CARL VON OSSIETZKY universität OLDENBURG

Asymptotically Fast Arithmetic in the Picard Group of Algebraic Curves & Related Topics

Von der Fakultät für Mathematik und Naturwissenschaften

der Carl von Ossietzky Universität Oldenburg

zur Erlangung des Grades und Titels eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

angenommene Dissertation

von

Matthias Junge

geboren am 22.11.1988

in Bremen

Gutachter

Prof. Dr. Florian Heß

Zweitgutachter

Dr. Jan Steffen Müller

Tag der Disputation

18.02.2022

Kurzfassung

Das Hauptergebnis der vorliegenden Arbeit sind Algorithmen, die einen vollständigen Satz an notwendigen Werkzeugen zu Verfügung stellen, um effizient in der Grad null Picard Gruppe $\mathrm{Pic}^0(X)$ einer reduzierten Überlagerung[1] X von $\mathbb{P}^1_k$ zu rechnen. Die vorgestellten Algorithmen haben eine asymptotische Laufzeit von $O^\sim(n^\omega c_X)$ Operationen im Grundkörper k wobei n der Grad eines endlichen Morphismus $\pi : X \to \mathbb{P}^1_k$ und c_X eine Invariante von X bezeichnet, für die gilt:

$$c_X \approx \begin{cases} \frac{g+\dim_k H^0(X,\mathcal{O}_X)+n}{n}, & X \text{ irreduzibel} \\ \max_{i=1}^m \{c_{i,X}\}, & X \text{ reduzibel} \end{cases} \quad \text{wobei}$$

$$c_{i,X} \approx \frac{g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + n_i + \varepsilon_i}{n_i}$$

Hierbei bezeichnen $X_1, \ldots, X_m$ die irreduziblen Komponenten von X, g und g_i jeweils die Geschlechter von X bzw. X_i, n und n_i jeweils den Grad von π bzw. $\pi_{|X_i}$ und ε_i ist eine positive ganze Zahl, die einzig davon abhängt, wie sich die irreduziblen Komponenten in X schneiden[2]. Dieses Resultat verallgemeinert das Ergebnis aus [Jun16] auf singuläre, reduzible und nicht-ebene projektive Kurven über k. Alle bisherigen Algorithmen funktionieren lediglich für irreduzible und nicht-singuläre Kurven über einen Körper k. Wir geben eine kurze Einordnung unseres Resultats im Vergleich zu bisherigen Arbeiten:[3]

(i) Die Laufzeit von $O^\sim(g^\omega)$ in [KM07] für integrales[4] und nicht-singuläres X hängt nicht von einem möglichen Grad n, sondern lediglich vom Geschlecht g ab. Daher können die dort vorgestellten Algorithmen auch nicht von dem Fall, dass n beschränkt ist aber g wächst, profitieren. In diesem Fall erreichen unsere Algorithmen eine überlegene Laufzeit von $O^\sim(c_X) \subseteq O^\sim(g + \dim_k H^0(X, \mathcal{O}_X))$. Statt linearer Algebra über dem Grundkörper k in Dimension g wie sie in [KM07] benutzt wird, benutzen wir lineare Algebra über dem Polynomring $k[x]$ in Dimension n und Grad c_X (welches in etwa dem größten der Werte g_i/n_i entspricht).

(ii) Für den Fall von integralen und nicht-singulären Kurven erreichen wir im Wesentlichen die gleiche Laufzeit wie in [Jun16], als wir (ebenfalls durch lineare Algebra über $k[x]$ in Dimension n, aber im Grad g/n) eine asymptotische Laufzeit von $O^\sim(n^\omega(g/n))$ erreichten. Die in dieser Arbeit vorgestellten Algorithmen funktionieren hingegen auch für singuläre Kurven.

(iii) Nach bestem Wissen des Autors sind die in dieser Arbeit vorgestellten Algorithmen die ersten Algorithmen, welche die Arithmetik in $\mathrm{Pic}^0(X)$ für die Klassen der singulären und reduziblen Kurven umsetzt. Darüber hinaus sind die vorgestellten Algorithmen für die Klasse der integralen und nicht-singulären projektiven Kurven mindestens so schnell wie die bereits existierenden Algorithmen. Somit erweitern wir nicht nur die Klasse der projektiven Kurven, für die es effiziente Algorithmen zur Umsetzung der Arithmetik in $\mathrm{Pic}^0(X)$ gibt, sondern wir können dieser Umsetzung für all diese Kurven eine einheitliche Laufzeit zuordnen.

[1] Dies sind reduzierte projektive Kurven über einen Körper k zusammen mit einem endlichen Morphismus auf $\mathbb{P}^1_k$. Für die konkrete Definition siehe Definition 2.1.3.

[2] Die Zahl ε_i ist durch $(\sum_{i=1}^m g_i) - g$ nach oben beschränkt. Hierfür siehe Lemma 2.4.3 zusammen mit Proposition 2.4.9.

[3] Für eine umfassendere Abhandlung über die bisherigen Arbeiten zur Arithmetik in $\mathrm{Pic}^0(X)$ siehe Abschnitt 1.1.

[4] Im Sinne von *irreduzibel* und *reduziert*.

Ferner beweisen wir in dieser Arbeit, dass die Grad null Picard Gruppe $\mathrm{Pic}^0(X)$ zu einer Idealklassengruppe isomorph ist, welche dem Koordinatenring einer überall dichten und affinen offenen Menge von X zugeordnet werden kann. Darüber hinaus zeigen wir, dass die Elemente in $\mathrm{Pic}^0(X)$ durch quadratische Polynommatrizen der Dimension n mit einem Grad, der nach oben linear durch c_X beschränkt ist, repräsentiert werden können. Falls X reduzibel ist, können wir die Elemente durch Matrizen in n-Blockform[5] repräsentieren, sodass der Grad des i-ten Zeilenblocks nach oben linear durch $c_{i,X}$ beschränkt ist. Nach bestem Wissen des Autors ist dies neu für den Fall dass X singulär und reduzibel ist und keinen k-rationalen Punkt besitzt.

Wir möchten betonen, dass wir insgesamt zwei Mengen von Algorithmen bereit stellen, die beide jeweils einen vollständigen Satz an Werkzeugen bereitstellen, um die Arithmetik in $\mathrm{Pic}^0(X)$ umzusetzen: Der erste lässt im Wesentlichen die irreduziblen Komponenten von X außer Betracht (und stellt damit einen eher generischen Ansatz dar) und der zweite versucht explizit die Existenz der Komponenten auszunutzen. Wir bezeichnen diese beiden als den komponentenunabhängigen bzw. den komponentenabhängigen Fall. Der komponentenunabhängige Satz an Algorithmen arbeitet mit Vertretern, die aus einer eher globalen und gröberen Perspektive größenoptimiert sind, und stellt damit einen tendenziell einfacheren Ansatz dar. Die Algorithmen des komponentenabhängigen Satzes arbeiten mit Vertretern aus $\mathrm{Pic}^0(X)$, deren Einschränkungen auf die irreduziblen Komponenten größenoptimiert sind. Hierfür ist es erforderlich, dass die lineare Algebra Algorithmen, die mit den entsprechend repräsentierenden Matrizen hantieren, etwas komplizierter werden. Dies liegt an dem Umstand, dass diese auf die Blockstruktur der Matrizen, welche die Einschränkungen auf die irreduziblen Komponenten von X widerspiegeln, eingehen müssen. Durch das voneinander unabhängige Arbeiten auf den verschiedenen Komponenten ergibt sich, dass diese Algorithmen einer möglicherweise parallelisierten Implementierung zugänglich sind.

In beiden Fällen stellt die Darstellung mithilfe der quadratischen Polynommatrizen die Möglichkeit bereit, eine Darstellung der Einschränkungen eines Elementes in $\mathrm{Pic}^0(X)$ auf die irreduziblen Komponenten von X effizient zu berechnen und damit ebenfalls Bilder unter dem Gruppenhomomorphismus $\mathrm{Pic}^0(X) \to \bigoplus_{i=1}^m \mathrm{Pic}^0(X_i)$.

Die vorliegende Arbeit liefert weiterhin Ergebnisse, die zwar nicht im gleichen Maß wie die Hauptergebnisse erwähnenswert sind, aber dennoch eigenen Wert haben. Zum Teil basieren die Hauptergebnisse dieser Arbeit auf diesen Ergebnissen. Im Folgenden geben wir einen kurzen Überblick über die erwähnten Ergebnisse und wie sie im Hauptunterfangen dieser Arbeit, der effizienten Umsetzung der Arithmetik in $\mathrm{Pic}^0(X)$, eingebettet sind.

Wir integrieren die Ergebnisse aus [Hes02, Theorem 7], welche die ersten expliziten Methoden zur Berechnung von Basen von Riemann-Roch Räumen vorgestellt und etabliert wurden, wie folgt: Wir erweitern den Geltungsbereich der dort gegebenen Ideen auf allgemeinere Garben und allgemeinere Kurven. Wir definieren verallgemeinerte Vektorbündel, welche im Wesentlichen solche Garben sind, für die es einen Struktursatz gibt, der ihre globalen Schnitte durch eine k-Basis angibt; im Wesentlichen sind verallgemeinerte Vektorbündel also solche Garben, für die [Hes02, Theorem 7] im Allgemeinen gilt. Darüber hinaus gilt all dies auch auf möglicherweise reduziblen und singulären Kurven. Dies ermöglicht es uns im Grunde, die Elemente in $\mathrm{Pic}^0(X)$ durch quadratische Polynommatrizen der Dimension n darzustellen.

Die durch die angegebene k-Basis beschriebene Dimension der globalen Schnitte eines verallgemeinerten Vektorbündels $\mathcal{F}$ hängt von den π-Invarianten von $\mathcal{F}$ ab, welche wiederum durch die Zerlegung von $\pi_*\mathcal{F}$ auf $\mathbb{P}^1_k$ in invertierbare Garben bestimmt sind. Diese hän-

[5] Falls $n = \sum_{i=1}^m n_i$ und $M \in k[x]^{n\times n}$ in n-Blockform ist, so gibt es Matrizen $M_i \in k[x]^{n_i \times n}$ sodass die Matrix M durch untereinander Schreiben der Matrizen $M_1, \ldots, M_m$ entsteht.

gen ebenfalls mit der Dimension von $H^1(X, \mathcal{F})$ als k-Vektorraum zusammen. Falls X integral und nicht-singulär ist, so erhält man üblicherweise Schranken für diese Invarianten durch Anwenden der Riemann-Roch Gleichung zusammen mit dem Verschwinden von $H^1(X, \mathcal{O}_X(D))$ für Divisoren D auf X dessen Grad $2g-2$ überschreitet. Wir verallgemeinern dies auf allgemeinere Kurven und auf verallgemeinerte Vektorbündel vom Rang 1 (welche wir $\mathcal{O}_X$-Ideale nennen). Im Falle von integralem X können wir auf recht elementare Weise Schranken angeben. Die Suche nach Schranken ist im reduziblen Fall hingegen sehr viel komplizierter. Nichtsdestotrotz können wir recht explizite Verfahren angeben, um Basen von $\mathcal{F}$ zu finden, welche in Bezug auf jede einzelne irreduzible Komponente klein sind. Die Existenz dieser Basen impliziert dann letztenendes die Schranken für die π-Invarianten. Ferner ist es von Bedeutung, dass die Schranken für die π-Invarianten obere Schranken für den minimalen Grad der die Elemente aus $\mathrm{Pic}^0(X)$ darstellenden Matrizen liefern. Daher sind wir schlussendlich dazu in der Lage, die Elemente in $\mathrm{Pic}^0(X)$ durch quadratische Polynommatrizen der Dimension n darzustellen, deren Grad nach oben linear durch c_X beschränkt ist.

Diese Schranken wiederum ermöglichen, dass wir eine Schranke $n_0 \in \mathbb{Z}$ angeben können, die von c_X und den Graden der Einschränkungen von $\mathcal{F}_{|X_i}$ auf die irreduziblen Komponenten von X abhängt, sodass die erste Kohomologiegruppe $H^1(X, \mathcal{F}(r(x)_\infty))$ für alle ganzen Zahlen $r \geq n_0$ verschwindet. Da der Poldivisor $(x)_\infty$ von x ample[6] ist, ist die Existenz einer solchen Schranke keine Überraschung.[7] Wir können jedoch im Falle von $\mathcal{O}_X$-Idealen $\mathcal{F}$ eine explizite Schranke angeben. Dies impliziert, dass das häufig auf die Riemann-Roch Gleichung angewandte Verschwinden der ersten Kohomologiegruppe (im Falle von integralem und nicht-singulärem X), welches das Vorhersagen der Dimension des Riemann-Roch Raums eines Divisors hinreichend großen Grades ermöglicht, auf $\mathcal{O}_X$-Ideale der Form $\mathcal{F}(r(x)_\infty)$ und seine globalen Schnitte verallgemeinert wird. Dieses Verschwindungsresultat kann wiederum zusammen mit einer allgemeinen Variante des Approximationssatzes dazu verwendet werden, um die Existenz von größenoptimierten Vertretern von $\mathrm{Pic}^0(X)$ zu begründen.

[6] Es findet der englische Ausdruck Verwendung, da es keine etablierte und einheitliche deutsche Interpretation des Wortes *ample* im mathematischen Kontext gibt.

[7] Siehe hierzu zum Beispiel [Liu02, 5.3.6].

Abstract

The main result of this thesis are algorithms that constitute a toolkit to efficiently compute in the degree zero Picard group $\mathrm{Pic}^0(X)$ of a reduced cover[8] X of $\mathbb{P}^1_k$ in an asymptotic running time of $O^\sim(n^\omega c_X)$ operations in the ground field k where n denotes the degree of a finite morphism $\pi : X \to \mathbb{P}^1_k$ and c_X is an invariant of X such that

$$c_X \approx \begin{cases} \frac{g+\dim_k H^0(X,\mathcal{O}_X)+n}{n}, & X \text{ irreducible} \\ \max_{i=1}^m \{c_{i,X}\}, & X \text{ reducible} \end{cases} \quad \text{where}$$

$$c_{i,X} \approx \frac{g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + n_i + \varepsilon_i}{n_i}.$$

Here $X_1, \ldots, X_m$ denote the irreducible components of X, g and g_i the respective genera, n and n_i the degrees of π respectively $\pi_{|X_i}$ and ε_i is an integer solely depending on how the components X_i intersect[9]. This generalises the result in [Jun16] to singular, reducible and non-plane projective curves over k. All previous algorithms only work for integral and non-singular curves over a field k. We give a short classification of our result in contrast to previous work:[10]

(i) The running time $O^\sim(g^\omega)$ of [KM07] for integral and non-singular X does not depend on n but solely on the genus g. Therefore, if n is bounded and g grows, then we obtain a superior running time of $O^\sim(c_X) \subseteq O^\sim(g + \dim_k H^0(X, \mathcal{O}_X))$. Instead of employing linear algebra in dimension g over k, as [KM07] does, we use linear algebra over the polynomial ring $k[x]$ in dimension n and degree c_X (which is roughly equal to the worst possible g_i/n_i).

(ii) In the case of integral and non-singular curves, our running time is essentially the same as the one in [Jun16] where the author obtained a running time of $O^\sim(n^\omega(g/n))$ (using linear algebra in dimension n over $k[x]$ in degree g/n). However, the algorithms we propose here work for singular curves as well.

(iii) Generally, to the author's best knowledge our algorithms are the first ones that implement the arithmetic in $\mathrm{Pic}^0(X)$ for the classes of singular and reducible curves. Moreover, our algorithms are essentially at least as fast as the fastest known algorithms for integral and smooth projective curves. That is, we do not only enlarge the class of curves X for which it is possible to compute efficiently in $\mathrm{Pic}^0(X)$, but we also provide a uniform running time for this task in general.

Furthermore, in this thesis we prove that the degree zero Picard group $\mathrm{Pic}^0(X)$ is isomorphic to an ideal class group associated to the coordinate ring of an affine and schematically dense open subset of X. Moreover, we show that the elements in $\mathrm{Pic}^0(X)$ can be represented by polynomial square matrices of dimension n with degree linearly bounded by c_X. If X is reducible, we can represent the elements by matrices in n-block-form[11] whose i-th row block has degree linearly bounded by $c_{i,X}$. To the author's best knowledge this is new in the case that X is singular, reducible and does not admit any k-rational points.

We want to emphasise that we provide two different sets of algorithms both constituting a complete toolkit to compute in $\mathrm{Pic}^0(X)$: The first one essentially does not take

[8] Those are reduced projective curves over a field k together with a suitable finite morphism onto $\mathbb{P}^1_k$, see Definition 2.1.3.

[9] The integer ε_i is bounded by $(\sum_{i=1}^m g_i) - g$, see Lemma 2.4.3 together with Proposition 2.4.9.

[10] For a more thorough treatment of the previous work on the arithmetic in $\mathrm{Pic}^0(X)$, see Section 1.1.

[11] If $n = \sum_{i=1}^m n_i$ and $M \in k[x]^{n \times n}$ is in n-block-form, then there are matrices $M_i \in k[x]^{n_i \times n}$ such that M is the matrix formed by writing the matrices $M_1, \ldots, M_m$ one below the other.

the irreducible components of X into account (and thus represents a more generic approach) and the second one explicitly does and tries to utilise them. We call these two the component independent respectively the component dependent case. The component independent toolkit works with representatives that are size-optimal from a more global and coarser perspective and provide a somehow less involved and more generic approach. However, the component dependent toolkit is comprised by algorithms that work with representatives of $\mathrm{Pic}^0(X)$ whose restrictions to each of the irreducible components of X are size-optimal. This requires the linear algebra algorithms that deal with the respective representing matrices to be a bit more involved since they need to take care of the block structure that reflects the restrictions to the irreducible components of X. But since they often work independently on the components, they are to some extent accessible for parallelisation. In both cases, the representation via polynomial square matrices enables us to efficiently compute representations of the restrictions of elements in $\mathrm{Pic}^0(X)$ to the irreducible components of X and thus to compute images under the group homomorphism $\mathrm{Pic}^0(X) \to \bigoplus_{i=1}^m \mathrm{Pic}^0(X_i)$.

There are further minor results upon which the main results rely (at least to some extent) and which, moreover, may have some significance on their own. In the following we give a brief overview of those and how these are embedded in the main endeavor of this thesis – efficiently implementing the arithmetic in $\mathrm{Pic}^0(X)$.

We incorporate the results of [Hes02, Theorem 7], which first gave explicit means to compute bases of Riemann-Roch spaces, in the following manner: We enlarge the ambit of the ideas given there to more general sheaves on more general curves. We define generalised vector bundles which are essentially those sheaves for which there is a structure theorem describing their global sections by means of a basis, i.e. essentially as those sheaves for which [Hes02, Theorem 7] holds in general. Moreover, all of this holds on possibly singular and reducible curves. This basically enables us to represent the elements of $\mathrm{Pic}^0(X)$ by polynomial square matrices of dimension n.

The dimension of the global sections of a generalised vector bundle $\mathcal{F}$ described by the stated k-basis depends on the π-invariants of $\mathcal{F}$ which themselves are determined by the decomposition of $\pi_*\mathcal{F}$ into invertible sheaves on $\mathbb{P}^1_k$. These also relate to the k-dimension of $H^1(X, \mathcal{F})$. In the case of an integral and non-singular curve X the Riemann-Roch equation together with the vanishing of $H^1(X, \mathcal{O}_X(D))$ for divisors D whose degree exceeds $2g-2$ provides bounds for these invariants. We generalise this to more general curves and to generalised vector bundles of rank 1 ($\mathcal{O}_X$-ideals). We rather easily provide bounds of these invariants if X is integral. The quest for effective bounds if X is reducible and decomposes into several irreducible components is much more involved. However, we give quite explicit instructions on how to find bases of $\mathcal{F}$ that are small with respect to each irreducible component. The existence of these bases then finally provides bounds for the π-invariants of $\mathcal{O}_X$-ideals. It is moreover important that we are able to prove that these bounds provide upper bounds of the minimal degree of polynomial matrices representing the elements in $\mathrm{Pic}^0(X)$. This finally establishes that we can represent the elements in $\mathrm{Pic}^0(X)$ by polynomial square matrices of dimension n with degree linearly bounded by c_X.

These bounds in turn provide that we are able to give a bound $n_0 \in \mathbb{Z}$, depending on c_X and the degrees of the restrictions $\mathcal{F}_{|X_i}$ of $\mathcal{F}$ to the irreducible components of X, such that for all integers $r \geq n_0$ the first cohomology group $H^1(X, \mathcal{F}(r(x)_\infty))$ vanishes. Since the pole divisor $(x)_\infty$ of x is ample, it is no surprise that such an integer n_0 exists.[12] However, we give an explicit bound in the case of $\mathcal{O}_X$-ideals $\mathcal{F}$. This establishes that the vanishing that is often employed in the Riemann-Roch equation (in the integral and smooth case) to predict the dimension of the Riemann-Roch space for divisors of sufficiently large

[12] See [Liu02, 5.3.6].

degree can be extended to $\mathcal{O}_X$-ideals of the form $\mathcal{F}(r(x)_\infty)$ and their global sections. This vanishing result in turn can be used to prove size-optimal representatives of $\mathrm{Pic}^0(X)$ by applying a general version of the Approximation Theorem 5.7.1.

Acknowledgement

I want to give great thanks to Florian Heß not only for his supervision and support of my PhD project, but also for introducing this beautiful subject to me. Whenever I had difficulties or only needed some new perspective on the material, I was always able to bring forward my issues and to profit from his expertise. I also want to thank Steffen Müller for being my second examiner and for his general advices with respect to possible applications of our algorithms.

I really appreciated the time I was able to spend with my office mates Dietrich Kuhn, Chrisitan Neurohr and Philipp Schläger. I also want to thank Malte Beer, Dietrich Kuhn and Philipp Schläger for the time they spent discussing my research problems. Big thanks to Benedikt Höpers, Anni Memmert and Philipp Schläger for valuable proofreading of my thesis.

I also want to thank the mathematicians all around the world that were open to provide me help without even knowing me: Kiran Kedlaya, János Kollár, Qing Liu, Vincent Neiger, Karl Schwede and Arne Storjohann.

Especially, I am much obliged that Benedikt Höpers has spent a great amount of his time discussing my research topics – I really enjoyed that time.

Finally and foremost, I am deeply grateful for all that Anni Memmert brings to my life. I want to thank her very much for being my safe haven and for her unconditional support.

Contents

Chapter 1

Introduction

The *Jacobian* $J(X)$ of an integral[1] and non-singular projective curve X over a field k is an algebraic group of dimension g (where g denotes the genus of X) that parameterises the degree zero divisors on X up to linear equivalence, see [Mil86] for a thorough treatment of Jacobians. If X has a k-rational point, then $J(X)$ is actually isomorphic to the degree zero Picard group $\mathrm{Pic}^0(X)$ consisting of degree zero divisors up to linear equivalence[2].

There has been quite an attention to the problem of computing efficiently in $J(X)$ of non-singular projective curves X over a field k – and still there is. In the cases of X being an *elliptic* or a *hyperelliptic* curve, this interest is tremendously boosted by the scientific community that works in the field of (applied) cryptography. This is due to the fact that (besides the problem of efficient integer factorisation which finds a use in the RSA cryptosystem) the discrete logarithm problem (DLP) is one of the main problems public key cryptosystem are based on. Instances of cryptosystems that rely on the DLP are the Diffie-Hellmann key exchange protocol [DH06] and the ElGamal cryptosystem [Elg85]. Both Neal Koblitz [Kob87] and Victor Miller [Mil85] proposed independently from one another to use the DLP in the group of points (which is essentially the same as the Jacobian) of an elliptic curve over a finite field for establishing cryptosystems. Since that time the research dealing with arithmetic aspects of elliptic curves has been intensified and also spread over to curves of higher genus, for instance, hyperelliptic curves of genus 2 or 3. The usage of Jacobians of such curves for cryptosystems was suggested again by Koblitz in [Kob89] and it has been studied in several occasions since then, for instance, in [Can87], [KGM+02] [MCT01] [Lan02], [PWGP03] and [Sut19]. Moreover, we refer the reader to the *handbook* [CFA+05] which is concerned with elliptic and hyperelliptic curve cryptography and covers lots of basic material as well as applied aspects.

In general, the Jacobian has been central in the study of projective curves as Mumford [AM04, p 260] has already put it straight:

> *"The Jacobian has always been a corner-stone in the analysis of algebraic curves and compact Riemann surfaces. [...] Weil's construction [of the Jacobian] was the basis of his epoch-making proof of the Riemann Hypothesis for curves over finite fields, which really put characteristic p algebraic geometry on its feet."*

In this thesis we focus on the algorithmic aspects of the arithmetic in the Jacobian (to be more precise, of the degree zero Picard group, see below) of far more general projective curves X over a field k. Implementing $J(X)$ algorithmically using an embedding into some projective space $\mathbb{P}^n_k$ is for almost all values of g impractical since either the dimension n grows exponentially in g or the equations cutting out $J(X)$ in $\mathbb{P}^n_k$ become very complicated.

[1] Note that the definition of a *curve* is not consistent in the literature in the sense that there is no consensus with respect to whether the curve (the scheme of dimension one in question) is assumed to be irreducible. However, in this thesis we will never assume a curve to be irreducible unless stated explicitly.

[2] See [Mil86, Theorem 1.1].

Therefore, most of the algorithms that work with $J(X)$ use the divisors representing the respective element in $J(X)$, keep track of linear equivalence and reduce resulting representatives (using a principal divisor) to obtain 'simple' ones after every arithmetic operation. This perfectly fits the endeavor of this thesis in which we actually care about the algorithmic implementation of the arithmetic in the degree zero Picard group of curves of large genus. Moreover, the Jacobian as defined in [Mil86] is only defined for non-singular projective curves over a field k, and we want to consider not only singular curves but also reducible ones[3]. All of this encourages us to consider the degree zero Picard group $\mathrm{Pic}^0(X)$ instead of the Jacobian.

We will present algorithms that cover the three essential ingredients that are necessary to be able to actually compute in $\mathrm{Pic}^0(X)$ (and more generally, these constitute the ingredients necessary to compute in an arbitrary abelian group):

Key ingredients of the arithmetic in an abelian group:

(i) Compute the composition of two group elements.

(ii) Compute the inverse of a given group element.

(iii) Test whether a given group element is the neutral element.

Some authors also provide an algorithm that provides a representation of the neutral element and thus we may also add this to the above key ingredients.

(iv) Provide a representation of the neutral element.

We will provide randomised algorithms to implement Items (i) and (ii) which are of *Las Vegas type*[4] and deterministic algorithms that implement Items (iii) and (iv).

In what follows next, we want to give a brief overview of the research that has been done with respect to efficient algorithms to compute in $\mathrm{Pic}^0(X)$ for general curves X (i.e., not assuming that X belongs to a rather restrictive class of curves, for instance the class of elliptic or the class of hyperelliptic curves) possibly having large genus. For a thorough treatment of the existing work, see Section 1.1. The existing research can be roughly divided into two different type of approaches, the *arithmetic* and the *geometric* approach.[5] The geometric approach assumes the curve X to be embedded into some projective space $\mathbb{P}_k^N$ and to be given by homogeneous equations where $N \in O(g)$ is possible. Starting from this setting [Vol94] and [HI94] both worked with as small values of N as possible, the most prominent one being $N = 2$.[6] Both used computations with polynomials of degree in the order of g and resulted in a total running time of $O(g^7)$ operations on the ground field k where g denotes the genus of X. The most prominent representative of the geometric approach is Kamal Khuri-Makdisi who presented in [KM07] the following way of representing the curve X and divisors on it. A fixed line bundle $\mathcal{L}$ that comes equipped with X of sufficiently large degree $\deg_k \mathcal{L} \geq 2g + 2$ provides the possibility to represent the curve X as the global sections of $\mathcal{L}$ and $\mathcal{L}^{\otimes 2}$ together with a multiplication map $\mu : \mathcal{L}(X) \otimes \mathcal{L}(X) \to \mathcal{L}^{\otimes 2}(X)$ between them. Moreover, divisors on X can then be interpreted as k-subvector spaces of $\mathcal{L}(X)$ and the arithmetic operations in $\mathrm{Pic}^0(X)$ can be carried out using linear algebra over k in dimension g. Using fast linear algebra over k this results in an asymptotic running time of $O^{\sim}(g^{\omega})$ operations in k and superseded the results in

[3] See Footnote 1.

[4] Our algorithms are randomised algorithms that either signal their failure or return a correct result. Moreover, the probability of failure can be influenced by input parameters and is upper bounded.

[5] We adopted the terminology *arithmetic vs. geometric* from [KM07] and the following distinction is inspired by the remarks made in [KM07].

[6] Both worked with a description of X as a possibly singular plane curve, see [KM04, p. 2].

[Vol94] and [HI94] by lengths. The arithmetic approach, whose most recent representative is Florian Heß, assumes X to come equipped with a finite morphism $\pi : X \to \mathbb{P}^1_k$ of degree n and interprets the function field F of X as a degree n field extension of $k(x)$. If X is non-singular, then $\mathrm{Pic}^0(X)$ is isomorphic to an ideal class group associated to F and the arithmetic in $\mathrm{Pic}^0(X)$ boils down to ideal arithmetic in the integral closure of $k[x]$ in F, see [Hes99] and [Hes02]. This results in a total running time which is polynomial in n and C_f where $f = y^n + a_1 y^{n-1} + \ldots + a_{n-1}y + a_n \in k[x, y]$ defines the function field of X and $C_f := \max\{\lceil \deg(a_i)/i \rceil \mid 1 \leq i \leq n\}$. Therefore, this approach is sensitive to the degree n of X over $\mathbb{P}^1_k$. In his master's thesis [Jun16] the author also followed the arithmetic approach. The author worked out ideas (that have been provided by Florian Heß[7]) in detail and came up with algorithms that implemented the arithmetic in $\mathrm{Pic}^0(X)$ for integral and non-singular projective curves X over finite fields. These theoretical algorithms were formulated in the function field setting mentioned above and resulted in a running time complexity of $O^{\sim}(n^{\omega-1}g)$ where g denotes the genus and n the degree of F over $k(x)$ as well as ω the matrix multiplication constant. Therefore, [Jun16] set a new best running time $O^{\sim}(g)$ in the case that n is bounded and g grows and it achieves the same asymptotic running time $O^{\sim}(g^{\omega})$ if $n \approx g$ as [KM07] did. Moreover, it interpolates between the two extremes and provides a compelling running time if n is neither constant (in terms of g) nor approximately equal to g. Under the quite reasonable assumption that $n \in O(g)$ it is at least as fast as all known algorithms and even faster if $n \not\approx g$ or n not bounded.

In a nutshell, the main goal of this thesis is to provide algorithms for the arithmetic in $\mathrm{Pic}^0(X)$ in the case that X is possibly singular and reducible and to achieve an analogous running time as in [Jun16]. This would provide a uniform running time for the arithmetic in $\mathrm{Pic}^0(X)$ for a wide range of projective curves X over fields. The previous work mentioned above (and pretty much every attempt made so far) concerned with the arithmetic in $\mathrm{Pic}^0(X)$ only considers *very nice* projective curves X over k and does not economise with assumptions imposed on X. That is, the authors assume X to be *irreducible*, *non-singular* and sometimes even to be *plane*.

Let us now describe the main difficulties we encounter trying to generalise the ideas from [Jun16] to curves that decompose into several irreducible components and that may have singularities. For this purpose, we assume for the moment that X is a non-singular and irreducible projective curve over the field k. One of the key ingredients for the results in [Jun16] (and implicitly for pretty much all of the previous work) was the theorem of Riemann-Roch together with a vanishing result. That is, for every divisor D on X there is the Riemann-Roch equation

$$\dim_k H^0(X, D) = \dim_k H^0(X, K - D) + \deg_k D + 1 - g \tag{0:1}$$

with K a canonical divisor on X. Moreover, whenever $\deg_k D \geq 2g - 1$ holds, we have $\dim_k H^0(X, K - D) = 0$. This provided means to argue that there are 'small' divisor class representatives of a specific form and implied that we are able to find principal divisors of the very same form. All of this laid the foundation to transport the task of computing with divisors into the realm of linear algebra in dimension n over the polynomial ring $k[x]$ with entries of degree in the order of g/n. There are several occasions in which the fact that X is non-singular and irreducible comes into play here. Since X is non-singular, the dualising respectively canonical sheaf ω_X is invertible and corresponds to the canonical divisor class, that is, we do have canonical divisors K. Moreover, the existence of K together with X being irreducible implies that $\deg_k D > \deg_k K = 2g - 2$ results in $K - D$ having negative degree and also that this implies that $H^0(X, K - D)$ vanishes. For singular curves the

[7] Florian Heß was the supervisor of the author's master's thesis.

dualising sheaf ω_X need not be invertible[8] and then the term $H^0(X, K-D)$ in Eq. (0:1) is replaced with $H^1(X, \mathcal{O}_X(D)) = H^0(X, \omega_X \otimes_{\mathcal{O}_X} \mathcal{O}_X(-D))$. However, for reducible curves the sheaf $\omega_X \otimes_{\mathcal{O}_X} \mathcal{O}_X(-D)$ might have global sections no matter what the degree of D is. Since we want to use similar ideas in this thesis as in [Jun16], we need to overcome these issues.

Let us now briefly describe how we addressed these issues. In contrast to the previous work, we will work with reduced covers of $\mathbb{P}^1_k$. Those are reduced projective curves X over a field k that admit a finite morphism[9] $\pi : X \to \mathbb{P}^1_k$ of degree n that is separable[10] and which satisfies that the intersection points of the irreducible components of X do not meet the fibre $\pi^{-1}(P_\infty)$ of a fixed point P_∞ of $\mathbb{P}^1_k$, the *point at infinity*.Then the direct image $\pi_*\mathcal{F}$ of every invertible sheaf $\mathcal{F}$ (being coherent and torsion-free indeed suffices to be locally free on $\mathbb{P}^1_k$) is a vector bundle of rank n on $\mathbb{P}^1_k$ and thus decomposes into a direct sum of twisted sheaves $\mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_1), \dots, \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_n)$. These integers $|\mathcal{F}|_1, \dots, |\mathcal{F}|_n$ are invariants of the isomorphism class of $\mathcal{F}$. Since finite morphisms are affine, we have $\chi_k(X, \mathcal{F}) = \chi_k(\mathbb{P}^1_k, \pi_*\mathcal{F})$[11] and thus we can interpret the dimension of both $H^0(X, \mathcal{F})$ and $H^1(X, \mathcal{F})$ in terms of the invariants $|\mathcal{F}|_1, \dots, |\mathcal{F}|_n$. In particular, proving bounds for them provide $H^1(X, \mathcal{F}) = 0$[12]. Whenever X is integral, we can quite easily provide bounds for these invariants in terms of g and n, no matter if X is singular[13]. An important part of this thesis is to prove bounds for the invariants in the case that X is reducible[14]. To do so, we need to investigate the connection between divisors on X and divisors on the irreducible components of X (in fact, we will do so for more general sheaves) extensively. The above then provides the vanishing of $H^1(X, \mathcal{F}(r(x)_\infty))$ where $\mathcal{F}$ is an invertible sheaf and r sufficiently large but bounded in terms of the degree of the restrictions of $\mathcal{F}$ to the irreducible components of X[15]. Despite the fact that we only need this result for invertible sheaves representing divisor classes, it does hold for far more general sheaves. We call these sheaves $\mathcal{O}_X$-ideals which are basically sheaves that are invertible at the generic points of X. It turned out to be the case that our definition of $\mathcal{O}_X$-ideals is congruent with the definition of generalised divisors given by Hartshorne in [Har07]. Furthermore, $\mathcal{O}_X$-ideals are instances of sheaves for which we can provide a structure theorem of their global sections[16], analogous to the one given in [Hes02] but for more general curves and sheaves. Moreover, the sections $\mathcal{F}(V)$ of an $\mathcal{O}_X$-ideal $\mathcal{F}$ over an affine open subset $V = \pi^{-1}(U)$, where $U \subseteq \mathbb{P}^1_k$ is an affine open, are free modules of rank n over $\mathcal{O}_{\mathbb{P}^1}(U)$. By fixing an affine open cover $\{U_0, U_\infty\}$ of $\mathbb{P}^1_k$ and setting $V_0 = \pi^{-1}(U_0)$, $V_\infty = \pi^{-1}(U_\infty)$, this provides that $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ are free $k[x]$- respective $k[x^{-1}]$-modules of rank n. Moreover, the $\mathcal{O}_X$-module $\mathcal{F}$ is represented by the pair $(\mathcal{F}(V_0), \mathcal{F}(V_\infty))$[17]. This provides that $\mathcal{O}_X$-ideals $\mathcal{F}$ with a prescribed behaviour along the fibre $\pi^{-1}(P_\infty)$ can be completely represented by $(n \times n)$-matrices over $k[x]$. Another very important feature of the invariants $|\mathcal{F}|_1, \dots, |\mathcal{F}|_n$ is that they determine the degree of the entries of the above matrices depending on the degree of $\mathcal{F}$.

[8] Indeed, it is invertible if and only if X is Gorenstein.

[9] Every projective curve over k admit a finite morphism to $\mathbb{P}^1_k$, see Theorem D.1.6. However, not every such morphism needs to satisfy the further properties we require.

[10] We call a morphism $X \to Y$ onto an irreducible curve Y *separable* if its restrictions to the irreducible components of X induce separable field extensions of the respective function fields.

[11] See Lemma B.5.12.

[12] See Proposition E.2.16.

[13] See Theorem 4.3.23.

[14] See Lemma 4.5.1.

[15] Since the pole divisor of x $(x)_\infty$ is an ample divisor, the existence of such an integer $r \in \mathbb{Z}$ is no surprise, see [Liu02, 5.3.6]. However, we are able to provide explicit bounds for r.

[16] We call these sheaves generalised vector bundles, see Definition 4.1.1.

[17] To be precise, to encode the $\mathcal{O}_X$-module structure we also need to compute multiplication tables, see Proposition 4.2.9.

All of the above then enables us to reduce the arithmetic in $\mathrm{Pic}^0(X)$ to linear algebra in dimension n over $k[x]$ with matrices having degree linearly bounded by an invariant c_X of X. The invariant c_X is roughly equal to g/n if X is irreducible and roughly equal to $\max_{i=1}^{m}\{g_i/n_i\} + \varepsilon$ if X is reducible. Here g resp. g_i denote the genera of X resp. X_i; n resp. n_i denote the degrees of X resp. X_i over $\mathbb{P}^1_k$ and ε depends on how the components X_i intersect. This results in an asymptotic running time of $O^{\sim}(n^{\omega}c_X)$ operations in k. Therefore, if X is irreducible but singular, we obtain a direct generalisation of the result in [Jun16] to singular curves. Moreover, if X decomposes into multiple irreducible components, then we obtain a running time that is roughly equal to the running time of the irreducible case applied to the irreducible component on which our algorithm is slowest. This pretty much looks like the best one could expect in general.

1.1 Existing Work

As already mentioned in the introductory text, there has been some effort in implementing the arithmetic in the degree zero Picard group $\mathrm{Pic}^0(X)$ for elliptic and hyperelliptic curves and, moreover, for more general curves as well. In this section we want to give a more thorough overview of the previous work and therefore supply insights of what is the state of the art with respect to efficient algorithms that implement the arithmetic in $\mathrm{Pic}^0(X)$ of general projective curves X over a field k.

In the following we want to divide the previous work roughly into two categories depending on the approach the authors used. By doing so, we use a terminology that we adopted from [KM07] where the author describes the two approaches as *arithmetic* and *geometric*. Roughly speaking, the arithmetic approach works with a degree n morphism $\pi : X \to \mathbb{P}^1_k$ and then tries to express $\mathrm{Pic}^0(X)$ either explicitly by rather simple objects (for instance using the Mumford representation as [Can87] does for hyperelliptic curves) or as an ideal class group attached to the function field of X. Then the arithmetic in $\mathrm{Pic}^0(X)$ boils down to ideal arithmetic. In contrast to this, the geometric approach, which is the one [KM07] used, uses an embedding of X into some projective space $\mathbb{P}^n$ with $n \in O(g)$. Then two Riemann-Roch spaces are needed to represent X and those are provided by the restrictions of linear and quadratic functions from the ambient projective space $\mathbb{P}^n$ to X. Then the arithmetic in $\mathrm{Pic}^0(X)$ boils down to linear algebra over k in dimension g inside these Riemann-Roch spaces.

Arithmetic Approaches

In [Can87] the author presents means to compute in the degree zero divisor class group (the Jacobian) of a *hyperelliptic curve* over a field k of characteristic not equal to 2. By a hyperelliptic curve the author refers to an integral, plane and non-singular projective curve X over k with an affine model given by $v^2 = f(u)$ where $f(u) \in k[u]$ is a separable polynomial of degree $2g + 1$ where $g > 0$. That is, the genus of X is the integer g and $n = 2$ denotes the degree of X over the projective line $\mathbb{P}^1_k$ (the gonality of X). Due to the relation $v^2 = f(u)$, every point $P = (x, y) \in X(\bar{k})$ not equal to the point ∞ at infinity satisfies that $P' = (x, -y)$ is also a point on X. This provides that for every such point P the relation $P + P' - 2 \cdot \infty = 0$ holds in the Jacobian of X. Therefore, every element in the Jacobian can be represented by a divisor of the form $(\sum_{i=1}^{r} P_i) - r \cdot \infty$ for some integer r and some further properties. These divisors are called *reduced* and every such divisor can be represented by two polynomials in $k[u]$ of degree at most g satisfying some greatest common divisor (gcd) conditions. This representation is called the Mumford representation. Finally, computing the sum of two divisors boils down to the computation of polynomial products and polynomial gcds of polynomials in $k[u]$ with degree bounded

by g. The author also provides an algorithm to reduce the resulting divisor class whose running time is also bounded by the number of required operations for computing the gcd of polynomials. Therefore, the overall running time is $O(g(\log g)^2) \subseteq O^{\sim}(g)$. Moreover, the algorithms are deterministic.

[Hes99] provides a method to compute the divisor class group of (an algebraic function field of) an integral and non-singular projective curve X over a field k. Moreover, the author develops an efficient method to compute Riemann-Roch spaces and provides an algorithm to reduce divisors. The latter provides an opportunity for finding representatives of a given specific form of classes in the degree zero divisor class group of X. This form is somewhat small in the sense that storing it on a computer requires bounded space. Furthermore, combining all of the above with a simple criterion for equality provides means to actually implement the group law in the degree zero divisor class group together with a test for equality deterministically. The running time of this application of the results in [Hes99] is polynomial in n and C_f where $f = y^n + a_1 y^{n-1} + \ldots + a_{n-1} y + a_n \in k[x, y]$ defines the function field of X and $C_f := \max\{\lceil \deg(a_i)/i \rceil \mid 1 \leq i \leq n\}$.

[Jun16], based on the ideas of Florian Heß, provides probabilistic algorithms to implement the group law in the degree zero Picard group $\mathrm{Pic}^0(X)$ where X denotes an integral and non-singular projective curve of genus g over a field k which has degree n over $\mathbb{P}^1_k$. After a precomputation that needs to be done once for X, the author reduces the group operations in $\mathrm{Pic}^0(X)$ to linear algebra over $k[x]$ in dimension n and degree linearly bounded by g/n which thus results in a total running time complexity of $O(n^\omega(g/n)) = O(n^{\omega-1}g))$ where ω denotes the matrix multiplication constant. The reduction to linear algebra over the polynomial ring $k[x]$ with $x \in k(X)$ is due to an isomorphism provided by the author between $\mathrm{Pic}^0(X)$ and an ideal class group associated to the integral closure $R = \mathrm{Cl}(k[x], k(X))$ of $k[x]$ in the function field $k(X)$ of X. To do so, it is shown that every class in $\mathrm{Pic}^0(X)$ admits a divisor representative which behaves as a common multiple of the pole divisor $(x)_\infty$ of x at the points lying over the point at infinity $P_\infty \in \mathbb{P}^1_k$. Moreover, [Hes02, Theorem 7] together with the theorem of Riemann-Roch and the vanishing of $H^1(X, \mathcal{O}_X(D))$ for divisors D with degree exceeding $2g - 2$ provides representatives of bounded size. These representatives are given by integral invertible ideals of R which are thus free of rank n over $k[x]$ and can therefore be represented by a polynomial square matrix of dimension n. The bounded size of the divisor representatives implies that the respective ideals have bounded degree and, moreover, that every such ideal admits a basis whose basis matrix has bounded degree as well. The principal ideals representing the zero element in the ideal class group correspond to principal divisors generated by functions that behave as powers of x at the points over P_∞. A key point for the presented algorithms is that they heavily rely on being able to compute for every given ideal such a function that is contained in that ideal.

Geometric Approaches

[KM07] provides probabilistic algorithms to implement the group law in the degree zero Picard group $\mathrm{Pic}^0(X)$ where X denotes a non-singular projective geometrically irreducible algebraic curve of genus g over a field k. After a precomputation that needs to be done once for X, the author reduces the group operations in $\mathrm{Pic}^0(X)$ to linear algebra over k in dimension $O(g) \times O(g^{1+\epsilon})$ which thus results in a total running time complexity of $O^{\sim}(g^\omega)$ where ω denotes the matrix multiplication constant.

The results of [KM07] rely on the former work [KM04] of the author where he introduced most of the theoretical foundation. The running time obtained in [KM04] is $O(g^4)$. The speedup from the results in [KM04] to those in [KM07] comes from replacing the representation of divisors by a k-basis with a representation by a smaller ideal generating set

which is obtained in a randomised way. This also implies that the algorithms in [KM07] are randomised algorithms.

In [KM07] the author assumes the curve X to be embedded into some projective space $\mathbb{P}_k^n$ with $n \in O(g)$ and that this embedding comes equipped with a line bundle $\mathcal{L}$ of degree $\deg \mathcal{L} \geq 2g+2$ but still with $\deg \mathcal{L} \in O(g)$. Then he fixes the k-vector spaces $H^0(X, \mathcal{L})$ and $H^0(X, \mathcal{L}^{\otimes 2})$ together with a multiplication map $H^0(X, \mathcal{L}) \otimes H^0(X, \mathcal{L}) \to H^0(X, \mathcal{L}^{\otimes 2})$ which provides a representation of X itself. After having established the above representation, every effective divisor D on X can be represented by the k-subvector space $H^0(X, \mathcal{L}(-D))$ of $H^0(X, \mathcal{L})$ which itself can be represented by a matrix over k via a k-basis. Alternatively, a k-basis as above can be replaced by an 'ideal generating set' (as the author calls it referring to the ideal a divisor defines on an affine open subset of X) which is a subset of $H^0(X, \mathcal{L})$ whose divisor of common zeros is D. This set may be way smaller than a basis of $H^0(X, \mathcal{L}(-D))$ scaling down the size of the involved matrices from $O(g) \times O(g^2)$ to $O(g) \times O(g^{1+\epsilon})$. To come up with such an ideal generating set, the author employs fundamental probabilistic statements about whether randomly chosen elements in a finite dimensional vector space lie in the finite union of proper subvector spaces. We mimic this method in this thesis to come up with ideal generating sets of ideals (indeed, exactly those ideals from above the author of [KM07] referred to). However, after representing divisors as above, the author is able to implement the group operations in $\mathrm{Pic}^0(X)$ only using the vector spaces $H^0(X, \mathcal{L}(-D))$ represented by a basis (or ideal generating set) and then using linear algebra over k in dimension $O(g) \times O(g^2)$ (respectively $O(g) \times O(g^{1+\epsilon})$). Hence, after the necessary precomputations, this results as mentioned above in the running time complexity of $O^{\sim}(g^{\omega})$.

In [IL12] the author generalises the main results of [KM04] to relative Jacobians of non-singular, projective $\mathrm{Spec}(R)$-schemes of relative dimension one where R is a noetherian *amenable*[18]ring. The author generalises the two main theorems [KM04, 2.2 and 2.3] upon which the representation and the arithmetic operations of effective Cartier divisors depend to relative effective Cartier divisors on relative $\mathrm{Spec}(R)$-schemes of relative dimension one. This yields the algorithmic realisations of the above statements and provides the arithmetic of divisors on relative curves and therefore the arithmetic on Jacobians of relative curves. All of this is done analogous to the proceeding in [KM04]. However, it seems to be the case that the speedup achieved in [KM07] over the result in [KM04] by working with ideal generating sets (obtained randomly) instead of bases over the ground field does not extend to amenable rings off-handedly. The overall running time for the arithmetic in the Jacobian is $O(g^4)$ (as in [KM04]) plus the running times $g\mathsf{S}(g)$, $\mathsf{K}(g, g)$ and $\mathsf{CK}(g, g, g)$[19]needed for computing *sums*, *kernels* and *common kernels*, respectively, see [IL12, pp 42-44].

We summarise the above reflections of the relevant work that each provides algorithms that implement the arithmetic in $\mathrm{Pic}^0(X)$ in Table 1.1. We explain the different columns that may need an explanation: The column *Curves* contains a brief description of the class of curves for which the respective algorithms work. The column *Type* lists whether the respective algorithm are deterministic (det.) or probabilistic (prob.) algorithms. The column *Approach* indicates which kind of approach the respective algorithms follow where *geom.* stands for the geometric and *arithm.* stands for the arithmetic approach.

[18]Roughly speaking, these are rings that admit effective linear algebra functions. The author defines a ring R to be *amenable* if the R-module operations *dual*, *composite*, *kernel*, *common kernel* and *sum* of projective R-modules can be computed effectively, see [IL12, pp 32-33]. Examples of amenable rings are fields with exact arithmetic, any domain with exact arithmetic and an effectively computable Euclidean function, a large class of principal ideal rings (not necessarily domains) containing finite semi-local rings and thus quotients of DVRs, Dedekind domains and certain quotients of $\mathbb{Z}_p[[u]]$, see [IL12, pp 33-34].

[19]for the notation $\mathsf{S}(g)$, $\mathsf{K}(g, g)$ and $\mathsf{CK}(g, g, g)$, see [IL12, p 33].

Source	Curves	Type	Complexity	Approach
[Can87]	hyperelliptic curves, i.e. non-singular, integral, plane, projective curve X over k, $\operatorname{char} k \neq 2$	det.	$O(g \log(g)^2)$, $n = 2$	arithm.
[Hes99], [Hes02]	non-singular, integral, projective curve X over k	det.	polynomial in n, C_f	arithm.
[Jun16]	non-singular, integral, projective curve X over k	prob.	$O^{\sim}(n^{\omega-1}g)$	arithm.
[KM07]	non-singular, geometrically irreducible, projective algebraic curve over k	prob.	$O^{\sim}(g^{\omega})$	geom.
[IL12]	non-singular, projective $\operatorname{Spec}(R)$-schemes of relative dimension one where R is noetherian	prob.	$O(g^4)+g\mathsf{S}(g)+$ $\mathsf{K}(g,g)$ + $\mathsf{CK}(g,g,g)$	geom.

Table 1.1: Overview of the running times of previous algorithms for the arithmetic in $\operatorname{Pic}^0(X)$

Besides the work that provided algorithms to efficiently compute in $\operatorname{Pic}^0(X)$ there has also been some efforts made with respect to computations that only relate to $\operatorname{Pic}(X)$. A work we need to mention in this context is [Bru13] which uses the geometric representation of [KM07] to present means to compute "desirable operations"[20] with respect to divisors over a finite field k. For instance, the decomposition of effective divisors into prime divisors, coming up with a uniformly random effective divisor of prescribed degree (if such exists) and computing images under the Frobenius map. Moreover, there are several operations when dealing with finite morphisms between non-singular curves that can be computed, for instance the pull-backs and push-forwards of divisors.

Another aspect that can be relevant for arithmetic in the Picard group is the efficient computation of Riemann-Roch spaces. Among others these can be used on integral curves to efficiently test whether a given divisor is principal. This in turn provides a possible zero test in $\operatorname{Pic}^0(X)$ and therefore a possible test for equality whenever there are algorithms at hand that can carry out the group law and compute inverses in $\operatorname{Pic}^0(X)$. The fundamental work was established in [Hes99]. However, over the last while some new algorithms have been proposed as those in [LGS20] and [ACL20] both for nodal plane projective curves. The algorithm in [LGS20] is a variant of the Brill-Noether algorithm and [ACL20] modifies this variant so as to improve known complexity bounds.

In [Bau14] the author worked out in detail the lattice theory that can be applied to lattices in function fields F/k of integral and non-singular projective curves X over a field k. The theory in particular applies to the invertible ideals which are free of rank $n = [F : k(x)]$ representing divisors on X. Especially the statements [Bau14, 4.0.1, 4.0.2] are similar to the methods described in [Hes02] and essentially interpret the Riemann-Roch space of a divisor D on X as a lattice space induced by the norm $|| \; ||_D$ which itself is induced by D. In Chapter 4 we will actually work with such lattices and their successive minima implicitly, but we will focus on how the latter can be upper bounded and how this affects the degree of matrices representing related bases. In contrast to [Bau14] we will not only work with the direct image $\pi_* \mathcal{O}_X(D)$ of the divisor D along the finite morphism corresponding to the finite function field extension $F/k(x)$ (which only admits the analysis on the level of k-vector spaces and free $k[x]$- respectively $\mathcal{O}_\infty$-modules) but will also respect that these vector spaces and free modules come from an $\mathcal{O}_X$-module.[21] In particular, we

[20] See [Bru13, p. 1711].

[21] Moreover, we will consider the whole situation on much more general curves and even for more general

will apply the insights gathered there to the problem of computing efficiently in $\mathrm{Pic}^0(X)$.

Finally, we would like to mention the work of Kohel [Koh12] that drew a connection between torus-based cryptography and the arithmetic in the (generalised) Jacobian of singular hyperelliptic curves. In the context of this thesis it is worth mentioning that Kohel also implemented algorithms[22] in the computer algebra systems Magma [BCP97] and Sage [S+20] that carry out the group law in the Jacobian of both possibly singular cubic and singular hyperelliptic curves by using the Mumford representation (with little to no modification) as in [Can87].

1.2 Complexity Model

We will analyse the running time of the algorithms we propose by bounding the number of required field operations from a field k on an *algebraic random access machine*[23] (algebraic RAM). Here we assume the test for equality $=$ and the operations $+$, $-$, $\times$ and "divide by a nonzero" involving two field elements to have unit cost. We decided to measure the running time complexity in operations in the ground field k instead of bit operations due to potential "coefficient explosion". Since adding elements of the Jacobian tends to increase their arithmetic height, this is a real and unavoidable issue if, for instance, k is any number field. Obviously, this is no issue if k is a finite field. Therefore, we treat k rather as a black box ground field whose arithmetic operations have unit cost.

Additionally to this complexity measure, we could also bound the number of integer operations required and bound the size of memory space used during the computations. However, we decided not to do so. The main reason for this is the lack of analysis on the side of the advanced linear algebra algorithms we employ coming up with our own algorithms. None of these come equipped with a complexity analysis that goes beyond bounding the number of ground field operations on an algebraic RAM. However, even the fastest algorithms dealing with the most fundamental task we will face in this thesis, namely the multiplication of two univariate polynomials, does not provide a space complexity analysis or any treatment of how many integer operations are required. However, it would still be possible to include the above aspect of complexity analysis by

1. assuming bounds both for the space complexity and the number of required integer operations of the most fundamental algorithms, for instance for *fast polynomial multiplication*, *fast matrix multiplication*, *division with remainder* etc., and

2. assuming bounds as above for the more advanced linear algebra algorithms over $k[x]$, for instance, algorithms that compute the *determinant*, *Popov form*, *reduction*, *basis of the kernel* and the *basis of the column space* of a matrix M and those that *solve a rational system* $M \cdot x = b$.

For the sake of brevity and since the number of operations in the ground field seems to be the more relevant parameter of complexity analysis, we decided not do so. However, we emphasise that the algorithms we propose in this thesis do not behave badly with respect to the above aspects of complexity analysis. Without profound analysis we claim that the space complexity is optimal, that is, the algorithms do not require more memory space than necessary by not exceeding the input/output size (asymptotically speaking). Moreover, in the algorithms we propose there is no single integer operation that cannot be associated with a call of an algorithm whose complexity analysis is solely measured in

sheaves than invertible ones corresponding to divisors on X.

[22] See http://iml.univ-mrs.fr/~kohel/alg/index.html.

[23] For further information and definitions regarding algebraic random access machines, we refer the reader to [Die09] and [Kal85].

terms of operations in the ground field. This means that the number of integer operations does indeed only count the calls of algorithms we will employ. Therefore, if there were bounds for the number of integer operations required in the algorithms we utilise, then the number of calling these already provides a bound for the number of integer operations we will use overall.

Note that since we do not explicitly bother with the space complexity and do not count the number of copy and move instructions on the algebraic RAM, algorithms as extracting a submatrix from a given matrix or concatenating matrices have constant cost in our cost model. Yet again, we could easily include this aspect of complexity analysis, but we decided not do so with the same reasons as above. Moreover, if we did include this aspect, the number of such operations required in our algorithms would be in $O(mnd) \subseteq O(n^2 d)$ where $m \leq n$ and $M \in k[x]^{m \times n}$ of degree d denotes the involved matrix.

Throughout this thesis, the integers g and n will denote the arithmetic genus of a scheme X (see Definition 2.4.8) and n the degree of a finite morphism $\pi : X \to \mathbb{P}^1_k$ (see Definition 2.2.2), respectively. Additionally, c_X denotes an invariant of X which depends on its irreducible components and how these intersect, see Definition 2.4.10. We will work with polynomial matrices of dimension n that have entries of degree in $O(c_X)$. These will be the parameters with respect to which we will count the number of operations in k needed for each algorithm. We will use the soft-O notation $O^{\sim}(f(g, n, c_X))$, $f \in \mathbb{Z}[x_1, x_2, x_3]$, which indicates that we neglect logarithmic terms in g,n and c_X.

We use ω to denote the exponent of matrix multiplication: two $n \times n$ matrices over k can be multiplied with $O(n^\omega)$ operations in k. We assume the cost of multiplying two polynomial matrices with dimension n and degree d is $O^{\sim}(n^w d)$ field operations, where the multiplication exponent ω is assumed to satisfy $2 < \omega \leq 3$.

Let $M : \mathbb{Z}_{\geq 0} \to \mathbb{R}_{>0}$ be a function such that polynomials in $k[x]$ of degree bounded by d can be multiplied using at most $M(d)$ field operations from k. Similarly, $B : \mathbb{Z}_{\geq 0} \to \mathbb{R}_{>0}$ bounds the cost of the extended greatest common divisor operation. That is, the extended greatest common divisor problem with two polynomials in $k[x]$ of degree bounded by d can be solved in time $O(B(d))$. By Proposition A.2.3, we have $M(d), B(d) \in O^{\sim}(d)$. We refer the reader to the book [GG03] for more details and reference about the cost of polynomial multiplication and matrix multiplication.

1.3 Main Results & Contributions

The main contribution of this thesis is a toolkit consisting of algorithms that we provide to compute in $\mathrm{Pic}^0(X)$. For reduced covers X of $\mathbb{P}^1_k$ these algorithms carry out the group law in $\mathrm{Pic}^0(X)$, compute the inverse of a given element and they test whether a given element is the neutral element. Our algorithms work with polynomial square matrices of dimension n over the polynomial ring $k[x]$ with degree bounded linearly by an invariant c_X of X. This results in an asymptotic running time of $O^{\sim}(n^\omega c_X)$ operations in k where k denotes the ground field of X, n the degree of a suitable finite morphism $\pi : X \to \mathbb{P}^1_k$, ω the matrix multiplication constant and c_X is determined by

$$c_X \approx \begin{cases} \frac{g + \dim_k H^0(X, \mathcal{O}_X) + n}{n}, & X \text{ irreducible} \\ \max_{i=1}^{m} \{c_{i,X}\}, & X \text{ reducible} \end{cases} \quad \text{where}$$

$$c_{i,X} \approx \frac{g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + n_i + \varepsilon_i}{n_i}.$$

For the rigorous definition of c_X and $c_{i,X}$, see Definition 2.4.10. The main result of this thesis is the following.

Theorem 6.6.1. *Let X be a reduced cover of $\mathbb{P}^1_k$. The elements in $\mathrm{Pic}^0(X)$ can be represented by matrices in $k[x]^{n\times n}$ with degree in $O(c_X)$. The combination of the Algorithms 19 and 20 provides randomised algorithms to compute both the group law in $\mathrm{Pic}^0(X)$ and the inverse of a given element. Moreover, Algorithms 21 and 22 provide a deterministic algorithm to test whether a given element in $\mathrm{Pic}^0(X)$ is the neutral element. All the above algorithms use at most $O^\sim(n^\omega c_X)$ operations in k and the randomised algorithms have positive constant success probability.*

To the best of the author's knowledge, our algorithms are the first ones that implement the arithmetic in $\mathrm{Pic}^0(X)$ for the rather general class of reducible and singular curves over k. Beyond that we do not only expand the range of curves for which such arithmetic is possible, but we also accomplish this in a running time that is at least as fast as the fastest known previous algorithms for nicer curves (integral, non-singular, sometimes even plane).

Source	Curves	Type	Complexity	Approach
[Can87]	hyperelliptic curves, i.e. non-singular, integral, plane, projective curve X over k, $\mathrm{char}\, k \neq 2$	det.	$O(g(\log g)^2)$, $n = 2$	arithm.
[Hes99], [Hes02]	non-singular, integral, projective curve X over k	det.	polynomial in n, C_f	arithm.
[Jun16]	non-singular, integral, projective curve X over k	prob.	$O^\sim(n^{\omega-1}g)$	arithm.
This thesis	reduced projective curve X over k with suitable[a] morphism $\pi : X \to \mathbb{P}^1_k$	prob.	$O^\sim(n^\omega c_X)$	arithm.
[KM07]	non-singular, geometrically irreducible, projective algebraic curve over k	prob.	$O^\sim(g^\omega)$	geom.
[IL12]	non-singular, projective $\mathrm{Spec}(R)$-schemes of relative dimension one where R is noetherian	prob.	$O(g^4)+g\mathsf{S}(g)+\mathsf{K}(g,g)+\mathsf{CK}(g,g,g)$	geom.

Table 1.2: Current overview of the running times for the arithmetic in $\mathrm{Pic}^0(X)$

To be precise, we generalise the results in [Jun16] (which has not yet been published) which only deals with integral and non-singular projective curves to integral projective curves in general and obtain essentially the same running time complexity of $O^\sim(n^\omega(g/n))$ operations in k. Moreover, the algorithms given in [KM07], that can only handle integral and non-singular curves over k, have a running time of $O^\sim(g^\omega)$ operations in k. In the case[24] that n is approximately equal to g, together with the reasonable assumption $\dim_k H^0(X, \mathcal{O}_X) \in O(g)$ our algorithms achieve essentially the same running time. Moreover, if n grows slower than g, we obtain an even better running time. For instance, if n is bounded and g grows, then we obtain a running time complexity of $O^\sim(g + \dim_k H^0(X, \mathcal{O}_X))$ which is essentially the same as [Can87] achieves for hyperelliptic curves.[25] Another example is the case when $n \leq g^\delta$ for $0 < \delta < 1$, for values of

[a] See Definition 2.1.3.

[24] Which might be true for "generic" non-singular curves over the complex numbers: On page 261 in [GH78], we find that the generic Riemann surface of genus g can be expressed as a branched cover of $\mathbb{P}^1_k$ with $n = \lceil g + 1/2 \rceil + 1$ sheets but not with less than that. That is, a generic Riemann surface of genus g has minimal degree $n \in \Theta(g)$ over $\mathbb{P}^1_k$. Furthermore, [Abr96] tells us that the gonality of a modular curve $X_0(N)$ over $\mathbb{C}$ grows linearly with the genus.

[25] Since for hyperelliptic curves we have $\dim_k H^0(X, \mathcal{O}_X) = 1$.

δ lower than ≈ 0.72 this even yields a sub-quadratic running time in g. Summarising the above, for integral curves over k we generalise the results of [Jun16] and [KM07] to possibly singular curves and even obtain better running times for suitable values of n.

One could say that we completed the big picture of the arithmetic in the Jacobian for quite general curves by assigning a uniform running time to the general problem of computing $\mathrm{Pic}^0(X)$. In contrast to Table 1.1 in Table 1.2 we include the result of *this thesis* and expressed "cover X of $\mathbb{P}^1_k$" in more comparable terms.

To reduce the original problem of computing in $\mathrm{Pic}^0(X)$ to linear algebra over $k[x]$, we prove that the degree zero Picard group is isomorphic to an ideal class group $\mathcal{I}_\pi/\mathcal{P}_\pi$ whose ideal representatives are ideals of the affine coordinate ring of an affine open subset induced by the morphism π. Moreover, we prove that each ideal class admits an integral representative that has degree linearly bounded by nc_X. In all of its generality, this size-optimal representation of $\mathrm{Pic}^0(X)$ is new.

1.3.1 Possible Applications

In this section we want to investigate where our results may be applied. Though one might say that the roots of computing in the Jacobian $J(X)$ respectively in $\mathrm{Pic}^0(X)$ of projective curves X may be seated in the possible application in cryptography, the author does not know of an explicit cryptographic application of fast arithmetic in the Jacobian of general curves of large genus. Exploiting the hardness of the DLP in the Jacobian of elliptic and hyperelliptic curves for cryptographic applications seems to be well suited. Nonetheless, being able to compute fast in the Jacobian of possibly reducible and singular curves with large genus might be worthwhile in case these might at some point enter the stage of cryptography. For instance, this would be the case if it was possible to reduce the DLP on a low genus curve to one with large genus whereby decreasing other parameters relevant for the running time of solving the DLP.

Besides being efficient for large genus curves, another important aspect of our results is that we are able to handle reducible and singular curves. Therefore, whenever it is necessary to compute in $\mathrm{Pic}^0(X)$ of a singular curve X since the related computation in $\mathrm{Pic}^0(\widetilde{X})$ for a non-singular model $\widetilde{X}$ of X does not provide the same information, one might use our algorithms. Furthermore, whenever we have a bunch of projective curves (singular or not), we may use the techniques introduced in [Sch05] to glue these schemes together in order to obtain a new scheme. The resulting curves make up examples of curves for which our algorithms may be applied since these become reducible curves that are highly probable singular. Reducible and singular curves also appear as the singular fibres of elliptic fibrations or fibrations of curves in general. For instance, in [NU73] a classification of the fibres in pencils of curves of genus 2 are given together with the configuration of their irreducible components.

Another possible area of research in which reducible and singular curves over finite fields appear is the research that deals with curves X of genus $g \geq 2$ over the rational numbers $\mathbb{Q}$ (or a number field $K/\mathbb{Q}$). Then there are primes p of $\mathbb{Q}$ of *bad reduction*, that is, the induced curve over $\mathbb{F}_p$ (the reduction of X modulo p) is singular. Though it is often possible to avoid dealing with reductions at bad primes there are cases in which this is worthwhile. For instance, Stoll and N. Bruin [BS10] use the Mordell-Weil sieve to prove statements about the rational points of a given non-singular curve X over $\mathbb{Q}$ using the "simple"[26] idea that the rational points embed into the Mordell-Weil group and that this can be detected algorithmically. For instance, the authors are able to prove that X has no rational points at all, that there are no rational points satisfying a given set of

[26] [BS10, p. 1].

congruence conditions or that there are no rational points mapping into a given coset[27] of the Mordell-Weil group. The Mordell-Weil sieve uses information about the Mordell-Weil group of X, together with local information obtained by reduction modulo p for many primes p. While Poonen in his heuristics [Poo06] originally only considered primes with good reduction, the authors of [BS10] also want to use the information that bad primes admit (and also of the kernel of the reduction at such) "*in order to keep the running time of the actual sieve computation within reasonable limits*" [BS10, p. 4]. To do so, the authors provide a variant of the Cantor algorithm [Can87] to implement the group law in the Jacobian of reductions at bad primes in the case of genus two curves in order to extract the above mentioned information. However, to the author's best knowledge there is no generalisation of this for curves of higher genus. Therefore, this is one explicit example in which the asymptotically fast algorithms for reducible and singular curves of large genus we propose in this thesis may be applied.

1.3.2 Implementation

At this point we like to note that, besides some fundamental code in Magma we came up together with Florian Heß, we did not implement our algorithms in any computer algebra system. As the reader will see, the implementation of our algorithms in any computer algebra system should be no trouble using the pseudo code we provide in this thesis. However, the main reason why we did not implement our algorithms is that these depend on algorithms that carry out fundamental linear algebra tasks over the polynomial ring $k[x]$. Some of these algorithms do have proven asymptotic running time complexity, but do not come along with an explicit implementation. Since the asymptotic running time of our algorithms relies on that of those algorithms, it is necessary to have an implementation of them at hand to come up with a useful implementation of our algorithms. In [HNES19], implementations of some algorithms are provided that carry out fundamental linear algebra tasks. For instance, there are implementations provided for polynomial multiplication, truncated inversion, approximants, interpolants, kernels, linear system solving, determinant and basis reduction. However, most prominently, the algorithm MatrixKernel given in [ZLS12] which is employed in our group law algorithm has no practical implementation yet, at least to the author's best knowledge.

[27] Which provides means to determine the set of all rational points on X if there is at most one rational point in each of the considered cosets, see [BS10, p. 2]

1.4 Commonly used Notation

All rings that will appear in this thesis will be commutative with 1. In Tables 1.3 and 1.4 we list notations we will use without further introduction in this thesis. Table 1.3 considers rather general notations whereas Table 1.4 deals with schemes and sheaves.

Notation	Description
$\mathbb{Z}$, $\mathbb{Z}_{\geq m}$, $\mathbb{Z}_{>m}$	Ring of integers, ring of integers a such that $a \geq m$ respectively the ring of integers a such that $a > m$
k	A field; occasionally used as an index
$\bar{k}$	Algebraic closure of the field k
$\mathbb{F}_q$	Finite field with q elements
$R^\times$	The group of units of the ring R
$S^{-1}R$, $S^{-1}M$	Localisations of the ring R and the R-module M with respect to the multiplicative subset $S \subseteq R$
M_P, R_P	Localisation of the R-module M respectively the ring R with respect to $S := R \setminus P$, that is $M_P = S^{-1}R$ and $R_P = S^{-1}R$
$\mathrm{Frac}(R)$	The total ring of fractions of R; this equals the localisation of R with respect to the multiplicative set of non-zero-divisors of R
$k[x]$	Univariate polynomial ring over the field k
$\ell c(f)$	Leading coefficient of $f \in k[x]$
$\deg f$	Degree of the polynomial $f \in k[x]$
$\deg M$	Degree of the matrix $M \in k[x]^{m\times n}$, defined as the maximum of the degrees of the entries of M
$M_1 \frown M_2$	Concatenation of the matrices $M_i \in k[x]^{m\times n_i}$, that is the matrix in $k[x]^{m\times(n_1+n_2)}$ resulting by writing M_2 right next to M_1; If no misconception is possible, we denote this by $[M_1 \mid M_2]$
$k((x^{-1}))$	Field of formal Laurent series in x^{-1}
$M \hookrightarrow N$	Injective map from M to N
$M \twoheadrightarrow N$	Surjective map from M to N
$M \leftrightarrow N$	Bijective map from M to N
$M \otimes_R N$	Tensor product of the R-modules M and N
$\phi_{\mathcal{B}} : V \to k^n$	Coordinate isomorphism of the n-dimensional k-vector space V with respect to the basis $\mathcal{B}$ of V
$\phi_{\mathcal{B}} : M \to R^n$	Coordinate isomorphism of the R-module M which is free of rank n with respect to the basis $\mathcal{B}$ of M
$M^\vee$, $\mathcal{F}^\vee$	Dual $\mathrm{Hom}_R(M, R)$ of the R-module M respectively the dual $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{O}_X)$ of the $\mathcal{O}_X$-module $\mathcal{F}$
ω	Matrix multiplication constant defined by the following: Computing the product of two $(n \times n)$-matrices over the field k requires $O(n^\omega)$ operations in k.

Table 1.3: General notation

Notation	Description
$\operatorname{Spec}(R)$	Set of prime ideals of the ring R or the affine scheme associated to R
$D_U(f)$	Basic open subset of the affine scheme U with respect to $f \in \mathcal{O}_U(U)$
X^0	Set of generic points of the irreducible components of the scheme X
X_0	Set of closed points of the scheme X
$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$	Tensor product of the $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$
$M^\sim$	Quasi-coherent sheaf on $\operatorname{Spec}(R)$ induced by the R-module M
$\mathbb{P}^N_R$	Projective space of dimension N over the affine base $\operatorname{Spec}(R)$
P_∞	Point at infinity on $\mathbb{P}^1_k$ with respect to a fixed standard affine open cover of $\mathbb{P}^1_k$
$\mathcal{O}_\infty = \mathcal{O}_{\mathbb{P}^1_k, P_\infty}$	Local ring at the point P_∞ at infinity on $\mathbb{P}^1_k$
$H^i(X, \mathcal{F})$	The i-th Čech cohomology group of the sheaf $\mathcal{F}$ on the topological space X
$\chi_k(X, \mathcal{F})$	Euler characteristic of the sheaf $\mathcal{F}$ on the scheme X over the affine base $\operatorname{Spec}(k)$, see also Definition B.5.13
$\operatorname{Ass}_{\mathcal{O}_X}(\mathcal{F})$	Set of associated points of the $\mathcal{O}_X$-module $\mathcal{F}$, if it is understood what X is, then we write $\operatorname{Ass}(\mathcal{F})$
$\operatorname{Ass}_R(M)$	Set of associated prime ideals of the R-module M
S_i	A sheaf $\mathcal{F}$ on a scheme X *is* S_i or *satisfies* S_i if for every point $P \in X$ the stalk $\mathcal{F}_P$ has depth (as an $\mathcal{O}_{X,P}$-module) of at least $\min\{i, \dim \operatorname{Supp}(\mathcal{F}_P)\}$, see [Sta18, Tag 0341]; moreover, X *is* S_i if $\mathcal{O}_X$ is S_i

Table 1.4: Scheme and sheaf related notation

The more involved notations are listed in the *List of Symbols* on page 313 sorted alphabetically with a page reference for their first appearance in this thesis. Moreover, in the *Glossary* on page 320 the reader finds an overview of terms and definitions that will occur throughout the thesis.

1.5 Outline of the Thesis

In this section we give a brief outline of the general structure of this thesis. We intend to give the reader a general map for an overview of the big picture.

This thesis is generally divided into two parts: the *main part* consisting of the chapters 1 to 6 and the *appendix* consisting of chapters A to G. The main part is dedicated to provide the means to compute efficiently in the degree zero Picard group $\operatorname{Pic}^0(X)$ including the algorithms constituting the arithmetic toolkit to do so. Frankly speaking, the main part is what one wants to see primarily when it comes to getting to the bottom of this thesis: the main result. The appendix somehow collects everything that does not fit into the main part in terms of being necessary to understand the origin of the main result. However, in the appendix we provide among other things some theory developed on our own necessary for the generality for some of the main statements along the road to the main result.

Now we will give a more detailed overview about both parts starting with the main part: In Chapter 2, "*Covers of* $\mathbb{P}^1_k$", we will give an as brief as possible introduction into

the notion of covers of $\mathbb{P}^1_k$ which are the type of projective curves we are going to work with and for which all of the results in this thesis will hold. Essentially, covers of $\mathbb{P}^1_k$ are projective curves that are possibly reducible and singular and that come equipped with a suitable finite morphism onto the projective line. We introduce a great deal of necessary notations we will use throughout the thesis.

In Chapter 3, "*Divisors, Invertible Sheaves and $\mathcal{O}_X$-Ideals*" we will recall the basic notions of Cartier divisors and introduce $\mathcal{O}_X$-ideals which can be regarded as the generalisation of the invertible sheaves corresponding to divisors. A significant number of results and statements we make in this thesis do not only hold for divisors, but also for $\mathcal{O}_X$-ideals. We provide the necessary theory behind moving divisors and sheaves back and forth between the several schemes that we associate to the given curve we are working on.

Chapter 4, "*Global Sections and π-invariants*", is one of the three most important chapters in this thesis and therefore we go into more detail here: We introduce generalised vector bundles (of which the rank one bundles are $\mathcal{O}_X$-ideals) $\mathcal{F}$ which essentially are those sheaves whose sections over V_0 and V_∞ (an affine open cover of X induced by a standard affine open cover on $\mathbb{P}^1_k$) are free $k[x]$- respectively $k[x^{-1}]$-modules. This is the main reason why their global sections can essentially be characterised by a reduced basis of $\mathcal{F}(V_0)$. We prove that $\mathcal{O}_X$-ideals respectively generalised vector bundles $\mathcal{F}$ can be represented by their sections over V_0 and V_∞ or even by their sections over V_0 and S (for the moment the reader may think of S as $X \setminus V_0$) . Moreover, the arithmetic operations necessary in the monoid of $\mathcal{O}_X$-ideals can be carried out using the latter pair $\mathcal{F}(V_0), \mathcal{F}(S)$ of ideals. We state a structure theorem for the global sections of $\mathcal{O}_X$-ideals respectively generalised vector bundles by providing a k-basis constituted by a specific reduced basis of $\mathcal{F}(V_0)$ combined with successive powers of x up to integer bounds depending on $\mathcal{F}$. These integers are called π-invariants and they provide first and foremost bounds for the possible degree of basis matrices of bases of $\mathcal{F}(V_0)$. This will be crucial since $\mathcal{O}_X$-ideals of a specific form can solely be represented by such a basis matrix. We illustrate the relation between $\mathcal{O}_X$-ideals and their restrictions to the irreducible components of a reduced reducible cover X of $\mathbb{P}^1_k$. This enables us to represent $\mathcal{O}_X$-ideals in terms of fixed reduced bases of $\mathcal{O}_{X_i}$ on the irreducible components X_i. We will prove that there are bases of $\mathcal{F}(V_0)$ that have bounded degree in terms of the above fixed bases. This proves the bounds for the π-invariants in the case of reducible covers of $\mathbb{P}^1_k$ which is one of the main results of this chapter. We provide algorithms that enable us to compute bases of $\mathcal{F}(V_0)$ in terms of basis matrices that have bounded degree on each irreducible component of X and thus can be regarded as being optimal with respect to the components of X. Finally, we give an equivalent criterion for when a divisor is principal which can be used for the test of equality in the Picard group.

In Chapter 5, "*Picard Group and its Structure*", we define the Picard group and its degree zero subgroup. Moreover, we examine its general structure by investigating how divisors on a curve X relate both to divisors on a schematically dense open subset U of X and to divisors on the irreducible components of X if X is reducible. Applying this we will see that the divisors on a cover X of $\mathbb{P}^1_k$ and divisors on V_0 together with the divisors on S are essentially the same. Furthermore, we can use all of this to prove that the degree zero Picard group $\mathrm{Pic}^0(X)$ is isomorphic to the degree zero divisor class group with specific representatives for each class. Moreover, this extends to an isomorphism between $\mathrm{Pic}^0(X)$ and an ideal class group $\mathcal{I}_\pi/\mathcal{P}_\pi$ associated to $\mathcal{O}_X(V_0)$. We will introduce the two approaches to compute in $\mathrm{Pic}^0(X)$ induced by two types of representatives of elements in $\mathcal{I}_\pi/\mathcal{P}_\pi$. The elements in $\mathcal{P}_\pi$ are called modification functions and we will analyse them, give proofs of their existence with bounded degree and we will also provide algorithms to compute them. The end of Chapter 5 is then dedicated to show that there are representatives of $\mathcal{I}_\pi/\mathcal{P}_\pi$ with bounded degrees (which implies that they can be represented on an algebraic RAM with bounded size) and provide first statements of how to compute

with them.

Chapter 6, "*Main Result – Computing Asymptotically Fast in* $\mathrm{Pic}^0(X)$", can be regarded as the most important and also the most algorithmic chapter. In this chapter we will provide the main result of this thesis. To do so, we will show that we can represent elements in $\mathcal{I}_\pi/\mathcal{P}_\pi$ (and thus in $\mathrm{Pic}^0(X)$) with polynomial square matrices with degree linearly bounded by c_X and show how to compute in $\mathcal{I}_\pi/\mathcal{P}_\pi$ (and thus in $\mathrm{Pic}^0(X)$) only using these matrices. For this purpose, we will show how to compute the quotient of two ideals if the quotient is an integral ideal by employing a fast algorithm that computes matrix kernels. To use this kernel algorithm efficiently, we introduce the necessary theory to come up randomly with ideal generating sets. To extend this to arbitrary ideal quotients, we need the representing matrices of elements in $\mathcal{P}_\pi$. Since the naive computation of such matrices has cubic running time complexity with respect to the degree n, we will show how to compute these matrices in a faster way. We will explain what precomputations need to be done once for X to establish a computational setup for our algorithms. Then we can finally propose Algorithms 19 to 22 which constitute the toolkit to compute in $\mathrm{Pic}^0(X)$ by providing means to carry out the group law, compute the inverse of elements and to test whether a given element is the neutral one. We give thorough analyses of the respective running time complexities of the proposed algorithms and can finally conclude with the main result: Theorem 6.6.1.

Let us now outline the appendix of this thesis. In Chapter A, "*Used Algorithms*", we collect the algorithms we will utilise for our own algorithms starting from some very naive to more involved ones which consider fast linear algebra over the polynomial ring $k[x]$.

In Chapter B, "*Foundational Theory*", we collect some fundamental statements about sheaves, algebraic geometry in general and some commutative algebra we will need throughout this thesis. All of the above is not intended to be self-contained, it is rather a collection of needed statements that the author did not find anywhere else in the literature.

Chapter C, "*Properties of R-Ideals and $\mathcal{O}_X$-Ideals*", provides the fundamental theory of $\mathcal{O}_X$-ideals by establishing theory about R-ideals for a specific class of one-dimensional rings R. These R-ideals are the local respectively affine variant of $\mathcal{O}_X$-ideals. We will present how these can be localised and restricted to irreducible components of $\mathrm{Spec}(R)$. Furthermore, we introduce the notion of degree of R-ideals which induces the global degree of $\mathcal{O}_X$-ideals which is congruent with the degree of divisors in the invertible case. Furthermore, we will show fundamental properties of these degree notions.

In Chapter D, "*Properties of Covers of* $\mathbb{P}^1_k$", we will prove basic properties of covers of $\mathbb{P}^1_k$ and give statements that are related to such. In particular, we give a prove of the existence of a finite morphism onto $\mathbb{P}^n_k$ for n-dimensional projective schemes over the field k. We will continuously and repeatedly make use of the presented statements throughout this thesis.

Chapter E, "*Dualising Sheaf and the Dual of $\mathcal{O}_X$-Ideals*", provides the duality theory which will be important along the road to the main result of this thesis. We introduce the general notion of r-dualising sheaves similar to the introduction in the *Grothendieck duality* section in [Liu02, 6.4.3]. We will use some more involved theory to prove some properties of the 1-dualising sheaf ω_X of a cover X of $\mathbb{P}^1_k$, for instance, that it is isomorphic to some $\mathcal{O}_X$-ideal whenever X is additionally reduced. Moreover, we will give a broader perspective on the theory of the π-invariants and relate them to the k-dimension of the first cohomology group $H^1(X, \mathcal{F})$ of $\mathcal{O}_X$-ideals $\mathcal{F}$. This together with the bound for the π-invariants that we prove in Chapter 4 provides an explicit bound $n_0 \in \mathbb{Z}_{\geq 1}$ such that $H^1(X, \mathcal{F}(r(x)_\infty))$ vanishes for all $r \geq n_0$ and all $\mathcal{O}_X$-ideals $\mathcal{F}$.

Chapter F, "*More on π-Invariants*", concludes this thesis by revealing a connection between the π-invariants of $\mathcal{O}_X$ and divisors on $\mathbb{P}^1_k$. Moreover, it ends with explicit (and more restrictive) bounds for the π-invariants of $\mathcal{O}_X$ if X is embedded in some projective

space $\mathbb{P}_k^N$ and the finite morphism $\pi : X \to \mathbb{P}_k^1$ of degree n is given by the projection onto two coordinates of $\mathbb{P}_k^N$. This result also provides means to compute the arithmetic genus of X in this case solely using the integers N, n and the degree of the homogeneous polynomials cutting out X in $\mathbb{P}_k^N$.

1.5.1 A Reading Guide

There are different options of how to read this thesis depending on how experienced the reader is with respect to arithmetic in Jacobians, algebraic geometry in general and with curves especially. Moreover, it may depend on what the reader wants to take away from reading this thesis.

(i) If the main interest of the reader is to extract the main statements of this thesis, then Section 6.6 is the place to go to.

(ii) If the reader is a more adept algebraic geometer whose main interest is to follow the road of achieving our main result, then reading the main part, together with following any link to the appendix which is necessary for the general understanding should be sufficient.

(iii) If the reader wants to comprehend the content of this thesis in all of its depth and generality, we clearly recommend to read the main part, together with following the links to the appendix. Once the reader ends up in the appendix by doing so, we advise the reader to try to get a general overview of the respective chapter/section of the appendix. Especially, the Chapters C and E should be read completely before proceeding with the main part.

(iv) The reader which is mostly interested in the explicit algorithms that implement the arithmetic in $\mathrm{Pic}^0(X)$ may proceed as follows: The reader should take the isomorphism $\mathrm{Pic}^0(X) \cong \mathcal{I}_\pi/\mathcal{P}_\pi$ and that the representatives in $\mathcal{I}_\pi$ can be represented by polynomial square matrices of dimension n (representing a basis) for granted (coming from a black box). By accepting these facts the reader obtains some bedrock from which it is possible to realise that the task of computing efficiently in $\mathcal{I}_\pi/\mathcal{P}_\pi$ is the one that needs to be carried out. Then it is obvious that we should care about computing the matrix representation of the elements in $\mathcal{P}_\pi$ and that we need to come up with linear algebra algorithms to compute the product (or quotient) of ideals in $\mathcal{I}_\pi$ in a manner that keeps the representatives in the same form (integral ideals only altered by elements in $\mathcal{P}_\pi$) as they are given as input for the algorithms. Finally, the zero test simply is accounted for by the theory established in Sections 4.7 and 5.9 and thus needs to be taken for granted. Chapter A contains a short introduction to the algorithms we will employ and should definitely be consulted by any reader who is interested in the explicit algorithms.

Moreover, we want to emphasise that the more generic approach (which we call the component independent case) we present can be considered to be less sophisticated and thus easier to comprehend and also to implement.

(v) If the reader is new in the context of algebraic geometry and is therefore not familiar with schemes, sheaves, divisors and so forth, then we recommend to follow the Chapter 3, Sections B.1 and B.2 together with one of the many textbooks and lecture notes on this topic, for instance, [Har77], [Liu02], [GW10] for standard textbooks and the lecture notes [Gat14] and [Gat20][28] of Andreas Gathmann. More comprehensive

[28] Here the former is an older version and the latter a newer one. They are in a sense complementary since [Gat14] treats divisors on curves (as Weil divisors though) and [Gat20] more generally treats schemes, $\mathcal{O}_X$-modules and cohomology.

lecture notes are those of Ravi Vakil [Vak18]. After the reader feels comfortable with those objects, we recommend to follow the reading approach in item (iii).

In general, it is possible to treat the appendix as a kind of black box and to mainly follow the main part and take the statements in the appendix which the main part refers to for granted. The possible danger following this approach is that the reader may fail to understand the content of this thesis in all of its generality. However, we recommend to read the Chapters C and E in any case.

Chapter 2

Covers of $\mathbb{P}^1_k$

In this chapter we will introduce the notion of "covers over $\mathbb{P}^1_k$", define all necessary notation and state some fundamental properties of covers of $\mathbb{P}^1_k$. Covers of $\mathbb{P}^1_k$ will be the class of schemes for which we state most of our results in this thesis. By definition, every cover X of $\mathbb{P}^1_k$ will come along with a finite morphism onto $\mathbb{P}^1_k$ (as every projective scheme over k of dimension one does) that satisfies two further properties. Throughout this thesis this will enable us to talk about fixed subschemes and other schemes related to the finite morphism. For instance, we can talk about the 'fibre of the point at infinity' or fix an affine open cover of the cover X of $\mathbb{P}^1_k$ induced by a standard affine open cover on $\mathbb{P}^1_k$. Once introduced the notations we give in this chapter will be a constant help dealing with the more involved topics later on.

The chapter is organised as follows: In Section 2.1 we define basic types of schemes we will work with throughout this thesis such as curves of finite residual-type over k, curves over k and covers of $\mathbb{P}^1_k$.

In Section 2.2 introduce a bunch of notations with respect to the finite morphism that comes along with a cover X of $\mathbb{P}^1_k$. These will, for instance, involve a fixed open cover of X consisting of the affine opens V_0 and V_∞ and also an affine scheme S whose closed points correspond bijectively to the fibre of the point at infinity.

In Section 2.3 we show that a given cover X of $\mathbb{P}^1_k$ together with its finite morphism can be represented by a commutative algebra setting condensed in a commutative diagram. We will use this representation throughout the rest of this thesis.

In Section 2.4 we introduce some basic notations and results with respect to the irreducible components of covers of $\mathbb{P}^1_k$. This will be used for iterative arguments that provide a statement on all of a cover X of $\mathbb{P}^1_k$ by applying some statement to the irreducible components of X iteratively.

2.1 Introduction to Covers of $\mathbb{P}^1_k$

In this section we will introduce the notion of "cover of $\mathbb{P}^1_k$" which will be separated schemes X over a field k of pure dimension one that are non-empty, noetherian, projective and Cohen-Macaulay together with a finite morphism onto $\mathbb{P}^1_k$. The fixed affine open cover of $\mathbb{P}^1_k$ will induce an affine open cover of X and the gluing data on $\mathbb{P}^1_k$ will provide gluing data on X. Moreover, the affine coordinate rings of X will be free modules of finite rank over the coordinate rings of $\mathbb{P}^1_k$. We will heavily use this fact for our algorithmic exploration of the Picard group and also for representing global sections of divisors (and even more general sheaves) in terms of bases. We will introduce our basic notations for this kind of setting and refer to and prove some foundational properties.

Let k be a field. In [GW10, Section 15.4] the notion of an **absolute curve** is introduced.

We will now define a *curve over k* as an absolute curve as in [GW10, Section 15.4] which is additionally separated and of finite type over k.

Definition 2.1.1. Let X be a scheme over the field k (with separated structure morphism $X \to \mathrm{Spec}(k)$) which is non-empty and noetherian. Let $X_1, \ldots, X_m$ denote its irreducible components and let X satisfy the following three equivalent properties (see [GW10, Prop. 15.1] and [GW10, Prop. 15.14]):

1. For every closed point $x \in X$, $\dim \mathcal{O}_{X,x} = 1$.
2. The closed irreducible subsets of X are the $X_1, \ldots, X_m$ and the closed points of X.
3. X is of *pure dimension one (or purely one-dimensional)*, i.e. $\dim X_i = 1$ for all $i = 1, \ldots, m$.

If X additionally satisfies that the residue class fields of its closed points have finite dimension over k, then we call X a **curve of finite residual-type over** k. If X is of finite type over k, then we call it an **absolute curve over** k or shorter a **curve over** k. △

Remark 2.1.2. Any curve over k is a curve of finite residual-type over k, see Lemma B.4.4. Moreover, if X is a curve of finite residual-type over k, then for any open subset $U \subseteq X$ we have that $\mathcal{O}_X(U)$ is a finite residual-type k-algebra, see Definition B.4.3 on page 239. △

We want to introduce the notion of a **cover of** $\mathbb{P}^1_k$. As the name suggests a cover X of $\mathbb{P}^1_k$ should be a projective curve over k together with a finite morphism $\pi : X \to \mathbb{P}^1_k$. In section Section D.1 of the appendix we will show that for projective schemes over k which are of pure dimension n there exists a finite and surjective morphism to $\mathbb{P}^n_k$. In particular, for curves over k there is a finite surjective morphism $\pi : X \to \mathbb{P}^1_k$, see Theorem D.1.6 and Proposition D.1.7. For the purposes we pursue in this thesis, we want this morphism to have further properties:

1. We want that $\pi_* \mathcal{O}_X$ is finite locally free over $\mathcal{O}_{\mathbb{P}^1}$. By Proposition D.2.4, this is equivalent to X being Cohen-Macaulay.
2. Let us fix an affine open cover $U_0 \cup U_\infty$ of $\mathbb{P}^1_k$ with $\{P_\infty\} = \mathbb{P}^1_k \setminus U_0$. For simplicity of the analysis we want that the preimage of the point at infinity $P_\infty \in \mathbb{P}^1_k$ contains no intersection points of the irreducible components of X.
3. The induced morphism $\pi_{|X_i} : X_i \to \mathbb{P}^1_k$ on the i-th irreducible component should induce a field extension $F_i/k(x)$ which is separable. Here F_i denotes the function field of X_i (endowed with the reduced subscheme structure) and $k(x)$ the function field of $\mathbb{P}^1_k$. By [Liu02, 3.2.15], this is equivalent to X_i being geometrically reduced.

Hence we will adopt these three criteria into the definition of a cover of $\mathbb{P}^1_k$.

Definition 2.1.3. A **cover of** $\mathbb{P}^1_k$ is a projective curve X over k together with a finite morphism $\pi : X \to \mathbb{P}^1_k$ and an affine open cover $U_0 \cup U_\infty$ of $\mathbb{P}^1_k$ (for which we set $\{P_\infty\} = U_\infty \setminus (U_0 \cap U_\infty)$) such that

(i) X is Cohen-Macaulay,

(ii) $\pi^{-1}(P_\infty)$ does not contain any intersection point of irreducible components of X, and

(iii) $\pi_{|X_i} : X_i \to \mathbb{P}^1_k$ induces a finite separable field extension $F_i/k(x)$ where X_i is endowed with the reduced subscheme structure and F_i denotes the function field of X_i.

Sometimes we want to consider projective curves X over k which do not satisfy all of the properties (i), (ii) and (iii) at the same time. Then we will explicitly exclude the respective properties of a cover of $\mathbb{P}^1_k$ we want to drop. △

Notation 2.1.4. Let $\mathcal{P}$ be a property of schemes. Let (X, π) be a cover of $\mathbb{P}^1_k$. Whenever we say *'let X satisfy respectively be $\mathcal{P}$'* or *'let X be a $\mathcal{P}$ cover of $\mathbb{P}^1_k$'*, then we mean that X as a scheme satisfies $\mathcal{P}$. For instance, *'let X be a reduced cover of $\mathbb{P}^1_k$'* or *'let X be irreducible'*. △

Let X be a cover of $\mathbb{P}^1_k$. By Corollary D.1.8, the morphism π will also be flat since X is Cohen-Macaulay. Note that by Corollary B.5.19, every scheme X of dimension $\dim(X) \leq 1$ over a field k is projective if and only if it is proper.

2.2 Finite Morphism to $\mathbb{P}^1_k$ and Notations

In the following we briefly describe what data comes equipped with the morphism and which we will assume to be part of *the input data* for our considerations. Unfortunately, this will involve a certain amount of notations we need to introduce to effectively work with covers of $\mathbb{P}^1_k$. The reader is referred to the *List of Symbols* on page 313 where there is also a collection of symbols that are solely related to covers of $\mathbb{P}^1_k$.

Definition 2.2.1. Let (X, π) be a cover of $\mathbb{P}^1_k$. With regards to the fixed standard open affine cover $U_0 \cup U_\infty$ of $\mathbb{P}^1_k$ we set $U_0 = \operatorname{Spec}(k[x])$, $U_\infty = \operatorname{Spec}(k[x^{-1}])$ and $U_{0,\infty} = U_0 \cap U_\infty = \operatorname{Spec}(k[x, x^{-1}])$ with x transcendental over k. By [GW10, 13.77], every finite morphism is affine and thus $V_0 := \pi^{-1}(U_0)$, $V_\infty := \pi^{-1}(U_\infty)$ form an affine open cover of X. Let R_0 and R_∞ be the affine coordinate rings of V_0 respectively V_∞. Furthermore, set $V_{0,\infty} = V_0 \cap V_\infty = \pi^{-1}(U_{0,\infty})$ which is also affine with coordinate ring $R_{0,\infty}$. By $i_0 : V_0 \to X$ and $i_\infty : V_\infty \to X$ we denote the corresponding open immersions. △

Definition 2.2.2. Let X be a cover of $\mathbb{P}^1_k$. We call the rank of $\pi_*\mathcal{O}_X$ over $\mathcal{O}_{\mathbb{P}^1}$ the **degree of** π. We will denote it by n. △

Remark 2.2.3. Moreover, the restrictions

$$\pi_{|V_0} : V_0 \to U_0, \quad \pi_{|V_\infty} : V_\infty \to U_\infty \quad \text{and} \quad \pi_{|V_{0,\infty}} : V_{0,\infty} \to U_{0,\infty}$$

will also be finite (and thus affine) morphisms (of affine schemes), see [Sta18, Tag 01WH]. △

By Lemma B.5.20, the morphisms $\pi_{|V_0}, \pi_{|V_\infty}$ and $\pi_{|V_{0,\infty}}$ correspond to finite ring extensions

$$k[x] \hookrightarrow R_0, \quad k[x^{-1}] \hookrightarrow R_\infty \quad \text{respectively} \quad k[x, x^{-1}] \hookrightarrow R_{0,\infty}. \tag{2:1}$$

Lemma 2.2.4. *The ring extensions in Eq. (2:1) make R_0, R_∞ and $R_{0,\infty}$ into free $k[x]$-, $k[x^{-1}]$- and $k[x, x^{-1}]$-modules of rank n, respectively.*

Proof. Note that since X is Cohen-Macaulay, by Proposition D.2.4 the sheaf $\pi_*\mathcal{O}_X$ is free of rank n and thus these extensions are also free of rank n over the respective ground rings. □

The open subscheme $U_{0,\infty}$ is both the basic open subset $D_{U_0}(x)$ in U_0 and the basic open subset $D_{U_\infty}(x^{-1})$ in U_∞ glued together representing the gluing data of $\mathbb{P}^1_k$. Now since the preimages of basic open subsets of affine morphisms are again basic open (the preimage of

a basic open subset of a regular function is given by the basic open subset of the pullback of that function), we have

$$\begin{aligned} V_{0,\infty} = V_0 \cap V_\infty &= \pi^{-1}_{|V_0}(D_{U_0}(x)) = D_{V_0}(x) \\ &= \pi^{-1}_{|V_\infty}(D_{U_\infty}(x^{-1})) = D_{V_\infty}(x^{-1}). \end{aligned}$$

This provides the isomorphisms

$$(R_0)_x \cong R_{0,\infty} \cong (R_\infty)_{x^{-1}}. \tag{2:2}$$

Roughly speaking, the gluing of the standard affine opens in $\mathbb{P}^1_k$ provides an affine open cover of X and also how the affine opens are glued together.

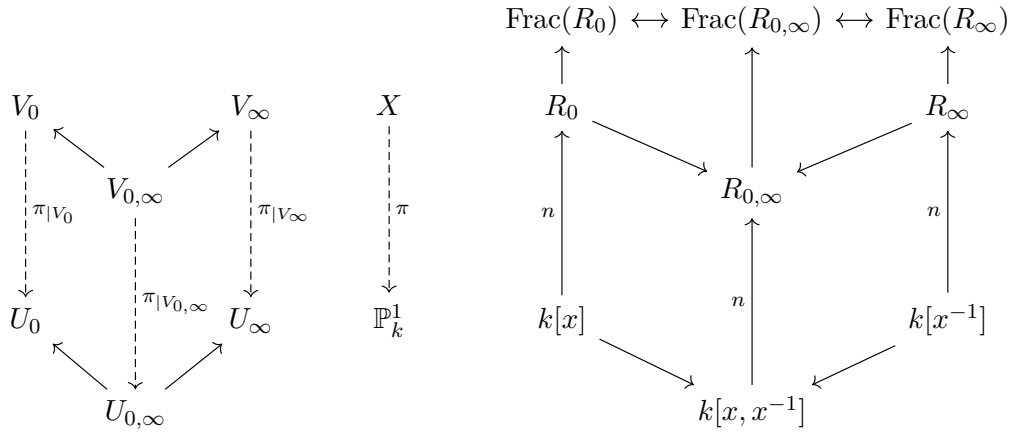


Figure 2.1: Open subsets and coordinate rings induced by finite morphism

Here $A \to B$ means $A \subseteq B$, $A \leftrightarrow B$ means $A \cong B$ and $A \dashrightarrow B$ indicates a morphism from A to B

The following statement and its proof will establish notation of covers of $\mathbb{P}^1_k$.

Proposition 2.2.5. *If (X, π) is a cover of $\mathbb{P}^1_k$, then the same is true for each $(X_i, \pi_{|X_i})$ of its finite irreducible components together with the restriction of π.*

Proof. Obviously, every irreducible component of a curve over k is a curve over k. Moreover, irreducible components of projective schemes are projective and since being Cohen-Macaulay is a local property, irreducible components of Cohen-Macaulay schemes are Cohen-Macaulay. Since X_i is an irreducible component of X, we have a closed immersion $\tau_i : X_i \to X$ and obtain thus a morphism $\pi_i := \pi_{|X_i} := \pi \circ \tau_i$ to $\mathbb{P}^1_k$. Since closed immersions are finite morphisms, see [Sta18, Tag 035C], and the composition of two finite morphisms is again finite, see [Sta18, Tag 01WK], $\pi_i : X_i \to \mathbb{P}^1_k$ is a finite morphism from X_i to $\mathbb{P}^1_k$. Moreover, the properties (ii) and (iii) from Definition 2.1.3 are clearly satisfied as well. □

We denote the degree of π_i by n_i.

Definition 2.2.6. As before, the morphism $\pi_i : X_i \to \mathbb{P}^1_k$ induces an affine cover of X_i by $V_{i,0} = \pi_i^{-1}(U_0) = \tau_i^{-1}(V_0)$ and $V_{i,\infty} = \pi_i^{-1}(U_\infty) = \tau_i^{-1}(V_\infty)$. We denote the corresponding coordinate rings by $R_{i,0}$ respectively $R_{i,\infty}$. Since closed subschemes of affine schemes are given by a unique ideal corresponding to the closed immersion, see [Sta18, Tag 01IH], there are unique prime ideals $P_{i,0}$ in R_0 and $P_{i,\infty}$ in R_∞ such that $R_{i,0} = R_0/P_{i,0}$ and $R_{i,\infty} = R_\infty/P_{i,\infty}$. We denote by $R_0^+ = \bigoplus_{i=1}^m R_{i,0}$ the affine coordinate ring corresponding to the disjoint union of the $V_{i,0}$. △

Remark 2.2.7. The canonical epimorphisms $R_0 \to R_{i,0}$ provide a homomorphism $R_0 \to R_0^+$ which is injective if and only if R_0 is reduced. △

Proposition 2.2.8. *Let (X, π) be a reduced cover of $\mathbb{P}^1_k$. Then $n = \sum_{i=1}^m n_i$.*

Proof. By definition, n equals the rank of $\pi_*\mathcal{O}_X$ and n_i the rank of $(\pi_i)_*\mathcal{O}_{X_i}$. In particular, $n = \operatorname{rk}_{k[x]} R_0$ and $n_i = \operatorname{rk}_{k[x]} R_{i,0}$. By Lemma B.5.6, we have an isomorphism

$$\phi : \operatorname{Frac}(R_0) \to \bigoplus_{i=1}^m \operatorname{Frac}(R_{i,0}).$$

Moreover, by Lemma B.4.10 we have $\operatorname{Frac}(R_0) = R_0 \otimes_{k[x]} k(x)$ as well as $\operatorname{Frac}(R_{i,0}) = R_{i,0} \otimes_{k[x]} k(x)$. Since $\operatorname{rk}_{k[x]} R_0 = \dim_{k(x)} \operatorname{Frac}(R_0)$ as well as $\operatorname{rk}_{k[x]} R_{i,0} = \dim_{k(x)} \operatorname{Frac}(R_{i,0})$, we find that the assertion follows from the isomorphism ϕ. □

On the level of topological spaces, the irreducible components of open subspaces are precisely given by the intersection of the irreducible components of the ambient space with the given subspace. Thus the $V_{i,0}$ and the $V_{i,\infty}$ are the irreducible components of the affine schemes V_0 and V_∞, respectively.

For completeness we also define the pole divisor of x here but refer the reader to Section 3.1 about divisors for the general treatment of divisors and to Definition 5.6.3 where the *generalised pole divisor of x* is defined.

Definition 2.2.9. We will denote the pole divisor of $x \in \mathcal{K}_X(X)$ on X, which is given by the configuration

$$\{(V_0, 1), (V_\infty, x^{-1})\},$$

by $(x)_\infty$. The multiples $r(x)_\infty$ correspond to the configuration $\{(V_0, 1), (V_\infty, x^{-r})\}$ and thus we will also use the notation $r(x)_\infty = (x^r)_\infty$. The pole divisor of $x \in \mathcal{K}_{X_i}(X_i)$ on the irreducible component X_i, which is given by the configuration

$$\{(V_{i,0}, 1), (V_{i,\infty}, x^{-1})\},$$

will be denoted by $(x)_{X_i,\infty}$. △

Until now everything is symmetric, but we will introduce some asymmetry by considering the fibre of the point P_∞ at infinity of $\mathbb{P}^1_k$ under π. We will define an affine scheme S whose set of closed points is one to one with $\pi^{-1}(P_\infty)$ and which comes with a birational injective morphism of schemes $\mu : S \to X$.

Definition 2.2.10. Let $T = k[x^{-1}] \setminus x^{-1}k[x^{-1}]$ be the complement of the maximal ideal of $k[x^{-1}]$ generated by x^{-1}. Then $\mathcal{O}_\infty = T^{-1}k[x^{-1}]$ is the local ring of the point at infinity $P_\infty \in \mathbb{P}^1_k$. We set $\mathcal{O}_S = T^{-1}R_\infty$ and $S = \operatorname{Spec}(\mathcal{O}_S)$. Furthermore, set $\mathcal{O}_{S_i} = T^{-1}(R_\infty/P_{i,\infty}) = T^{-1}R_\infty/T^{-1}P_{i,\infty}$ and $S_i = \operatorname{Spec}(\mathcal{O}_{S_i})$ where $P_{i,\infty}$ is a minimal prime of R_∞ as in Definition 2.2.6. By S we denote the affine scheme $(S, \mathcal{O}_S)$ and by S_i the affine scheme $(S_i, \mathcal{O}_{S_i})$. △

We immediately see that S_i are closed subschemes of S with closed immersions $\sigma_i : S_i \hookrightarrow S$ corresponding to the ring epimorphisms $\mathcal{O}_S \to \mathcal{O}_S/P_{i,\infty}\mathcal{O}_S = \mathcal{O}_{S_i}$ where $P_{i,\infty}$ denotes the minimal prime ideal of R_∞ corresponding to the irreducible component $X_i \cap V_\infty$ of V_∞. Moreover, $S = \bigcup_{i=1}^m S_i$.

Proposition 2.2.11. *The scheme S is finite and of dimension one. Its closed points are one to one with $\pi^{-1}(P_\infty)$ and its generic points are one to one with the generic points of X. Moreover, S is the disjoint union of the closed subschemes S_i and thus $\mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$.*

Proof. By definition, the prime spectrum of $\mathcal{O}_S$ is one to one with the prime ideals of R_∞ that have trivial intersection with T. Any maximal ideal $P\mathcal{O}_S$ of $\mathcal{O}_S$ therefore satisfies $P \cap k[x^{-1}] \subseteq k[x^{-1}] \setminus T = x^{-1}k[x^{-1}]$ and thus, since π maps closed points to closed points, see Corollary B.4.2, we must have $P \cap k[x^{-1}] = P_\infty$. Moreover, since any minimal prime ideal $P_{i,\infty}$ of R_∞ only consists of zero-divisors, see Corollary B.4.14, and R_∞ is torsion-free over $k[x^{-1}]$, we must have $P_{i,\infty} \cap T \subseteq P_{i,\infty} \cap (k[x^{-1}] \setminus \{0\}) = \emptyset$. That is, every minimal prime ideal of R_∞ corresponds to a minimal prime ideal of $\mathcal{O}_S$. Since $\pi : X \to \mathbb{P}^1_k$ is a finite morphism, the fibres of points under π are finite. This shows the first four assertions. Since X is a cover of $\mathbb{P}^1_k$, the points in $\pi^{-1}(P_\infty)$ do not lie on several irreducible components. This implies that the S_i have no intersection points and thus S is the disjoint union of the S_i. This provides $\mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$. □

Note that the same result as in Proposition 2.2.11 also holds for S_i. That is, S_i consists of finitely many points, its closed points are one to one to $\pi^{-1}(P_\infty) \cap X_i$ and its generic point corresponds to that of X_i.

Proposition 2.2.12. *The $\mathcal{O}_\infty$-module $\mathcal{O}_S$ is free of rank n. Moreover, every $k[x^{-1}]$-basis of R_∞ also constitutes an $\mathcal{O}_\infty$-basis of $\mathcal{O}_S$.*

Proof. By definition, we have $\mathcal{O}_S = T^{-1}R_\infty \cong R_\infty \otimes_{k[x^{-1}]} T^{-1}k[x^{-1}]$. By Lemma 2.2.4, R_∞ is a free $k[x^{-1}]$-module of rank n and thus we may write $R_\infty = \bigoplus_{i=1}^n \omega_i\, k[x^{-1}]$ for some $k[x^{-1}]$-basis $\omega_1, \dots, \omega_n$ of R_∞. Then $R_\infty \otimes_{k[x^{-1}]} T^{-1}k[x^{-1}] = \left(\bigoplus_{i=1}^n \omega_i\, k[x^{-1}]\right) \otimes_{k[x^{-1}]} T^{-1}k[x^{-1}]$ which is by [AM69, 2.14] isomorphic to $\bigoplus_{i=1}^n \omega_i\, T^{-1}k[x^{-1}] = \bigoplus_{i=1}^n \omega_i\, \mathcal{O}_\infty$ providing the assertion. □

Definition 2.2.13. By $\mu_a : S \to V_\infty$ we denote the morphism of schemes corresponding to the injective ring homomorphism $R_\infty \hookrightarrow T^{-1}R_\infty$. By μ we denote the composition of μ_a and the open immersion $V_\infty \hookrightarrow X$. △

Proposition 2.2.14. *Both μ_a and μ are morphisms of schemes that map the closed points of S bijectively onto the set of points $\pi^{-1}(P_\infty)$ lying over P_∞. Moreover, both morphisms are birational morphisms in the sense of [Sta18, Tag 01RO].*

Proof. By the properties of localisation, we see that the points of $\operatorname{Spec}(T^{-1}R_\infty)$ are the prime ideals $PT^{-1}R_\infty$ where $P \in \operatorname{Spec}(R_\infty)$ with $P \cap T = \emptyset$. By definition, μ_a maps $PT^{-1}R_\infty$ to P and hence by Proposition 2.2.11, we see that μ_a maps the closed points of S bijectively to $\pi^{-1}(P_\infty)$. The same is then obviously true for μ. That both μ_a and μ are birational also follows from Proposition 2.2.11. □

Notation 2.2.15. In the following we will treat S as a subset of X, that is we will use notations as $U \cap S$ for subsets $U \subseteq X$ of X. Moreover, note that since S contains every generic point of X, any non-empty open subset $U \subseteq X$ will have non-empty intersection $U \cap S \neq \emptyset$ with S. Hence, we will sometimes say that U is disjoint to S when their intersection does not contain any closed point of S. △

Remark 2.2.16. Note that by definition the morphism of sheaves $\mu^\# : \mathcal{O}_X \to \mu_*\mathcal{O}_S$ from the morphism $\mu : S \to V_\infty \to X$ of schemes factors through $(i_\infty)_*\mathcal{O}_{V_\infty}$ and thus we have for $U \subseteq X$ open:

$$\mu^\#(U) : \mathcal{O}_X(U) \to \mathcal{O}_X(U \cap V_\infty) \to T^{-1}\mathcal{O}_X(U \cap V_\infty)$$

Here, by abuse of notation, T denotes the image of $T = k[x^{-1}] \setminus x^{-1}k[x^{-1}] \subseteq \mathcal{O}_X(V_\infty)$ under the restriction homomorphism $\mathcal{O}_X(V_\infty) \to \mathcal{O}_X(U \cap V_\infty)$. In particular, if $U \cap V_\infty = \emptyset$, then $\mu^\#(U)$ is the zero map. If $U = V_\infty$, then $\mu^\#(U)$ is the localisation map $R_\infty \to \mathcal{O}_S$.

If $U = \pi^{-1}(U')$ with $U' \subseteq \mathbb{P}^1_k$ affine and $U \cap V_\infty \neq \emptyset$ but $U \cap S$ does not contain a closed point, then $\mu^\#(U)$ is an embedding $\mathcal{O}_X(U \cap V_\infty) \to \mathrm{Frac}(\mathcal{O}_X(U \cap V_\infty))$. Indeed, in that case $x^{-1} \in \mathcal{O}_X(U \cap V_\infty)^\times$ since its only zeros in V_∞ are the closed points of S. But then every non-zero element in $k[x^{-1}]$ is invertible in $T^{-1}\mathcal{O}_X(U \cap V_\infty)$ and thus $T^{-1}\mathcal{O}_X(U \cap V_\infty) \cong \mathcal{O}_X(U \cap V_\infty) \otimes_{k[x^{-1}]} k(x) = \mathrm{Frac}(\mathcal{O}_X(U \cap V_\infty))$, see Lemma B.4.10 and note that $\mathrm{Frac}(\mathcal{O}_{\mathbb{P}^1}(U')) = k(x)$. △

Definition 2.2.17. By $\mu_{a,i} : S_i \to V_{i,\infty}$ we denote the morphism of schemes corresponding to the injective ring homomorphism $R_{i,\infty} \hookrightarrow T^{-1}R_{i,\infty}$. By μ_i we denote the composition of $\mu_{a,i}$ and the open immersion $V_{i,\infty} \hookrightarrow X_i$. △

By applying the same lines of arguments as in the proof of Proposition 2.2.14, we can prove the same result for S_i and an irreducible component X_i of X.

Corollary 2.2.18. *Both $\mu_{a,i}$ and μ_i are morphisms of schemes that map the closed points of S_i bijectively onto the set of points $\pi^{-1}(P_\infty) \cap X_i$ in X_i lying over P_∞. Moreover, both morphism are birational morphisms in the sense of [Sta18, Tag 01RO].*

Remark 2.2.19. Obviously, μ_a and $\mu_{a,i}$ are affine morphisms. Since both the R_∞-module $T^{-1}R_\infty$ and the $R_{i,\infty}$-module $T^{-1}R_{i,\infty}$ are not finitely generated, the morphisms μ_a and $\mu_{a,i}$ are not finite. In particular, they are neither proper nor projective. △

Lemma 2.2.20. *Let X be a cover of $\mathbb{P}^1_k$. Then both V_0 and V_∞ are Cohen-Macaulay curves over k, that is curves over k which are Cohen-Macaulay. Moreover, the scheme S is a Cohen-Macaulay curve of finite residual-type over k.*

Proof. Being Cohen-Macaulay is defined locally, and thus all of the involved schemes are Cohen-Macaulay as asserted. Since $\mathbb{P}^1_k$ is non-empty and $\pi : X \to \mathbb{P}^1_k$ is surjective, all of the above schemes are non-empty as well. Open subschemes of locally noetherian schemes are locally noetherian, see [Sta18, Tag 01OW]. Moreover, affine schemes are quasi-compact, see [Sta18, Tag 01S7], and thus V_0 as well as V_∞ are noetherian. The restriction of $X \to \mathrm{Spec}(k)$ to V_0 or V_∞ is still a morphism of finite type, see [Sta18, Tag 01T2]. The first of the three equivalent properties in Definition 2.1.1 is a local condition and thus V_0 and V_∞ satisfy these. This shows that V_0 and V_∞ are curves over k.

Since S is affine with noetherian coordinate ring $\mathcal{O}_S$ (R_∞ is noetherian and localisations of noetherian rings are noetherian, see [Sta18, Tag 00FN]), S is noetherian. Now since V_∞ is of finite type over k, R_∞ is a finitely generated k-algebra, see [Sta18, Tag 01T2]. Thus by Lemma B.4.4 its residue class fields of closed points have finite dimensions over k. But since the residue class fields of closed points of $\mathcal{O}_S$ are isomorphic to those of the closed points of V_∞ lying over P_∞, the closed points of S have residue class fields of finite dimensions over k. □

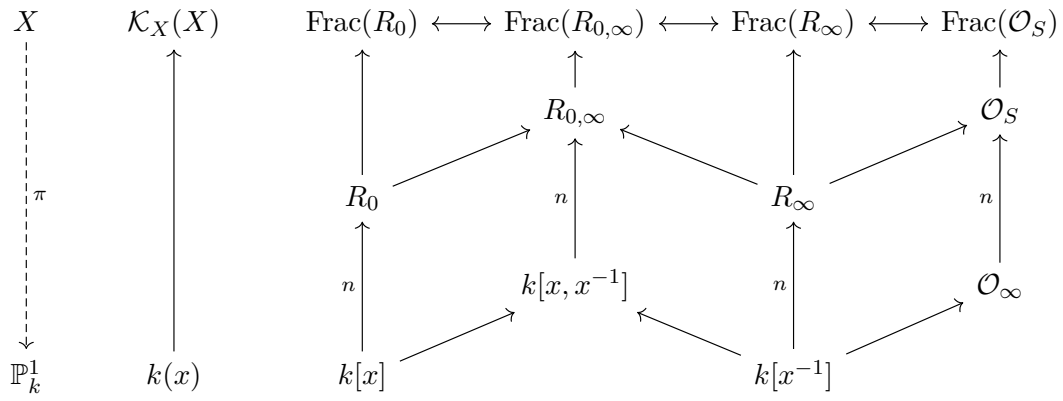


Figure 2.2: Coordinate rings and total ring of fractions induced by finite morphism

Here $A \to B$ means $A \subseteq B$ and $A \dashrightarrow B$ indicates a morphism from A to B

By introducing the scheme S with coordinate ring $\mathcal{O}_S$, we somehow introduced a possible asymmetry by symbolically replacing the second right column in Figure 2.2 with the most right column, that is replacing $k[x^{-1}] \hookrightarrow R_\infty \hookrightarrow \mathrm{Frac}(R_\infty)$ with $\mathcal{O}_\infty \hookrightarrow \mathcal{O}_S \hookrightarrow \mathrm{Frac}(\mathcal{O}_S)$. This idea will play an important role by coming up with solutions for the computation in the Picard group of a cover X of $\mathbb{P}^1_k$. One of the main reasons is the following: Both R_∞ and $\mathcal{O}_S$ are of Krull dimension one, but $\mathcal{O}_S$ is semi-local and thus every invertible ideal of it will be principal. We can use this fact to represent divisor classes on X (which otherwise are, at least to some extend (see chapter 4 for further information), represented by its sections over V_0 and V_∞) solely by its sections over V_0.

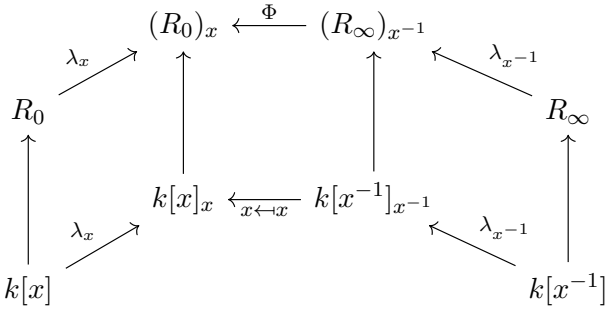
2.3 Representation of Covers of $\mathbb{P}^1_k$

Following the exposition of section 2.2, we have seen that any curve X over k with a finite morphism to $\mathbb{P}^1_k$ implies a certain commutative algebra setup:

Let X be a curve over k together with a finite morphism $\pi : X \to \mathbb{P}^1_k$. The isomorphisms Eq. (2:2) represented the gluing information of the affine curves V_0 and V_∞ over k along $V_{0,\infty}$. That is, the curve X over k is completely represented by the two coordinate rings R_0 and R_∞ together with an isomorphism $(R_\infty)_{x^{-1}} \to (R_0)_x$. This leads to commutative algebra characterisation of such curves over k together with a finite morphism to $\mathbb{P}^1_k$.

Lemma 2.3.1. *Any pair (X, π), where X is a projective curve over k and $\pi : X \to \mathbb{P}^1_k$ a finite morphism, can be represented by the commutative diagram of ring extensions*

Figure 2.3: Curve over k as a commutative diagram - not necessarily Cohen-Macaulay



The case that X is projective but not necessarily Cohen-Macaulay.

such that

(i) the affine schemes $\operatorname{Spec}(R_0)$ *and* $\operatorname{Spec}(R_\infty)$ *are curves over* k*,*

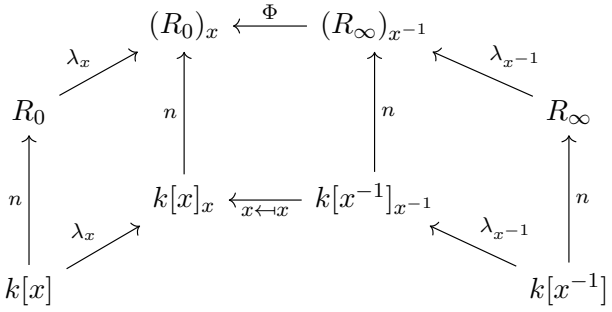
(ii) the homomorphisms λ_x *and* $\lambda_{x^{-1}}$ *are the localisation homomorphisms with regards to the elements* x *respectively* x^{-1}*, and*

(iii) Φ *is an isomorphism.*

Additionally, X *is Cohen-Macaulay if and only if we have the additional condition that*

(iv) the rings R_0 *and* R_∞ *are Cohen-Macaulay or, equivalently, the vertical arrows represent free extensions of the same rank* n*.*

Figure 2.4: Curve over k as a commutative diagram - Cohen-Macaulay case



The case that X is projective and Cohen-Macaulay.

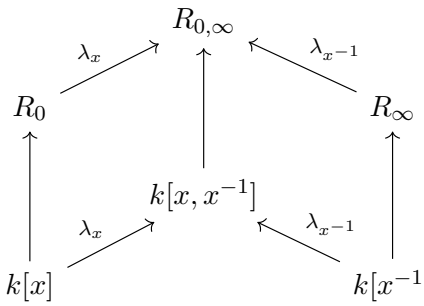
Proof. Assume (X, π) to be a pair as asserted. The finite morphism π provides the finite morphisms of affine schemes $\pi_{|V_0} : V_0 \to U_0$ and $\pi_{|V_\infty} : V_\infty \to U_\infty$ corresponding to the finite ring extensions $k[x] \hookrightarrow R_0$ respectively $k[x^{-1}] \hookrightarrow R_\infty$. The lower level of diagram Figure 2.3 is due to the gluing of the projective line and that gluing corresponds to the identification of $D_{U_0}(x)$ and $D_{U_\infty}(x^{-1})$, denoted by $U_{0,\infty}$. Since the preimage of basic open subsets under morphisms between affine schemes are again basic open, we have $\pi^{-1}(D_{U_0}(x)) = D_{V_0}(x)$ and $\pi^{-1}(D_{U_\infty}(x^{-1})) = D_{V_\infty}(x^{-1})$. Under the above identification we thus obtain $D_{V_0}(x) = D_{V_\infty}(x^{-1})$ in X which provides the isomorphism $(R_\infty)_{x^{-1}} \to (R_0)_x$. Moreover, if X is Cohen-Macaulay, then for any affine open subset of X the respective coordinate ring is Cohen-Macaulay. Equivalently, see Proposition D.2.4, we have that the respective ring extensions are free of the same rank n as $\pi_*\mathcal{O}_X$ over $\mathcal{O}_{\mathbb{P}^1}$.

Conversely, assume that we have given a commutative algebra setting as indicated in Figure 2.3. The affine curves $\operatorname{Spec}(R_0)$ and $\operatorname{Spec}(R_\infty)$ over k glue together along Φ to a curve X over k. The finite ring extensions $k[x] \hookrightarrow R_0$ and $k[x^{-1}] \hookrightarrow R_\infty$ correspond to finite morphisms $\pi_0 : \operatorname{Spec}(R_0) \to \operatorname{Spec}(k[x])$ and $\pi_\infty : \operatorname{Spec}(R_\infty) \to \operatorname{Spec}(k[x^{-1}])$. The lower level of diagram Figure 2.3 shows that the affine schemes $\operatorname{Spec}(k[x])$ and $\operatorname{Spec}(k[x^{-1}])$ glue together to a copy of $\mathbb{P}^1_k$. Then the diagram ensures that the two morphisms π_0 and π_∞ are compatible and provide a finite morphism $\pi : X \to \mathbb{P}^1_k$ as asserted. By [GW10, 12.89], this means that π is affine and proper. The structure morphism $\mathbb{P}^1_k \to \operatorname{Spec}(k)$ is proper, too. Since the composition of proper morphisms is proper, see [Liu02, 3.3.16], $X \to \operatorname{Spec}(k)$ is proper and thus by Lemma B.5.18, X is a projective scheme over k. The assertion considering (iv) now follows from Proposition D.2.4 again. □

Definition 2.3.2. Let (X, π) be represented as in Lemma 2.3.1. We use the isomorphism Φ to identify $(R_0)_x$ with $(R_\infty)_{x^{-1}}$ and denote it by $R_{0,\infty}$. Similarly, we identify $k[x]_x$ with $k[x^{-1}]_{x^{-1}}$ which can be written as $k[x, x^{-1}]$. Since both $(R_0)_x$ as well as $k[x, x^{-1}]$ are still

localisations of $k[x^{-1}]$ by x^{-1} we denote the composition of $\lambda_{x^{-1}}$ with Φ again by $\lambda_{x^{-1}}$. Then the diagram in Figure 2.3 becomes:

Figure 2.5: Curve over k as a commutative diagram - condensed gluing information



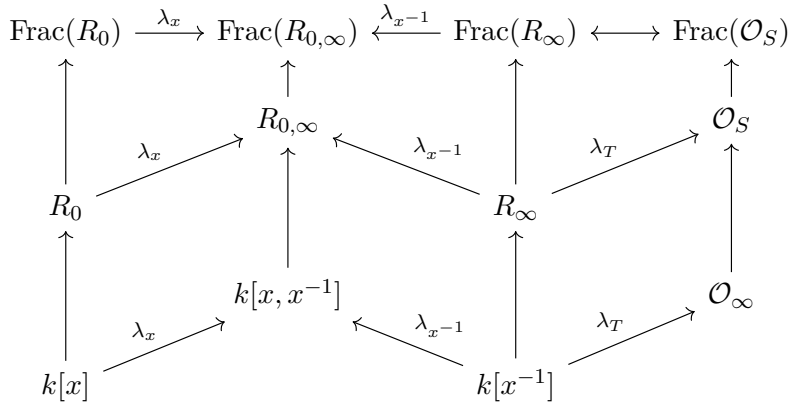
Gluing information condensed into $R_{0,\infty}$, together with the localisation homomorphisms λ_x and $\lambda_{x^{-1}}$

△

It turns out that the situation in Definition 2.3.2 extends to the respective total rings of fractions.

Lemma 2.3.3. *Let (X, π) be as in Definition 2.3.2. Then the localisation homomorphisms λ_x and $\lambda_{x^{-1}}$ extend to* $\mathrm{Frac}(R_0)$ *and* $\mathrm{Frac}(R_\infty)$*, respectively. In other words, we obtain a commutative diagram*

Figure 2.6: Curve over k as a commutative diagram - with total ring of fractions and $\mathcal{O}_S$



Localisation homomorphisms extend to total rings of fractions

Proof. Since the statement is symmetric, we only prove it for λ_x. The homomorphism λ_x extends to $\mathrm{Frac}(R_0)$ via $a/b \mapsto (a/b)/1$ where we identify the latter with the element a/b in $\mathrm{Frac}(R_{0,\infty})$. Hence $\lambda_x : \mathrm{Frac}(R_0) \to \mathrm{Frac}(R_{0,\infty})$ maps a/b to a/b. The embedding $R_{0,\infty} \hookrightarrow \mathrm{Frac}(R_{0,\infty})$ maps $a/b \in R_{0,\infty}$ to $(a/b)/1 = a/b$ in $\mathrm{Frac}(R_{0,\infty})$. This already shows that the asserted square commutes. □

We can thus represent a projective curve over k with finite morphism to $\mathbb{P}^1_k$ by a diagram as in Figure 2.6. The information on how to glue R_0 and R_∞ together is encoded in the fact that both embed via the localisation homomorphism into a common localisation $R_{0,\infty}$. This common embedding then also extends to the total rings of fractions and thus provides a common ambient $k[x, x^{-1}]$-module $\mathrm{Frac}(R_{0,\infty})$ in which everything takes place. We will see in Section 4.2 that this representation also enables us to give representations of so called $\mathcal{O}_X$-ideals.

Remark 2.3.4. By Lemma D.2.5, $V_{0,\infty}$ is schematically dense in X. Hence by [Liu02, 7.1.15], we have $\mathrm{Frac}(R_{0,\infty}) \cong \mathcal{K}_X(X)$ which underpins the understanding of $\mathrm{Frac}(R_{0,\infty})$ playing the role the function field plays in the integral case. △

2.4 Iterating on Irreducible Components

Let X be a reduced scheme with finitely many irreducible components $X_1, \ldots, X_m$. Here we fix the sequence $(X_1, \ldots, X_m)$ by which we mean that the order is relevant. In this section we will give definitions relative to the above sequence of irreducible components. We refer the reader also to section B.3 in the appendix where some statements and definitions about the irreducible components can be found.

We will use this setup and the statements that follow extensively in chapters 4 and 5 where we want to use results that hold for any of the X_i's to provide similar statements for X. To do so, we iterate over all X_i and include their intersection behaviour in our considerations to deduce the desired statement for the whole of X.

We will denote the closed immersions of the i-th irreducible component X_i by $\tau_i : X_i \hookrightarrow X$. The corresponding morphism of sheaves $\tau_i^{\#} : \mathcal{O}_X \to (\tau_i)_*\mathcal{O}_{X_i}$ induces a morphism of sheaves $\mathcal{O}_X \to \bigoplus_{i=1}^m (\tau_i)_*\mathcal{O}_{X_i}$. As it turns out, this morphism is injective if and only if X is reduced, see Proposition B.3.3.

Definition 2.4.1. Let $\mathscr{S}_X$ be such that the sequence

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \bigoplus_{i=1}^{m} (\tau_i)_*\mathcal{O}_{X_i} \longrightarrow \mathscr{S}_X \longrightarrow 0 \tag{4:3}$$

is exact, see Eq. (3:4). For $i = 1, \ldots, m$ let

$$Y_i = \bigcup_{j=1}^{i} X_i$$

denote the *scheme theoretic union of the* $X_1, \ldots, X_i$ *inside of* X, see [Sta18, Tag 0C4J]. Let Y_0 be the empty scheme with $\mathcal{O}_{Y_0} = 0$. By definition, $Y_m = X$. By definition, for every $i = 2, \ldots, m$ we have a natural surjective morphism of schemes

$$\upsilon_i : Y_{i-1} \sqcup X_i \to Y_i$$

compatible with the closed immersions $Y_{i-1} \hookrightarrow Y_i$ and $X_i \hookrightarrow Y_i$, i.e. the following diagram commutes:

$$\begin{array}{ccccc} & & Y_i & & \\ & {\scriptstyle h_{i-1}}\nearrow & \uparrow{\scriptstyle \upsilon_i} & \nwarrow{\scriptstyle j_i} & \\ Y_{i-1} & \longrightarrow & Y_{i-1} \sqcup X_i & \longleftarrow & X_i \end{array}$$

Locally, on any affine open subset $U = \mathrm{Spec}(R)$ of X, the corresponding morphism $\upsilon_i^{\#}$ is given by

$$\begin{array}{rccccc} \upsilon_i^{\#}(U): & R/I_i & \to & R/I_{i-1} & \oplus & R/P_i \\ & r + I_i & \mapsto & (r + I_{i-1} & , & r + P_i) \end{array}$$

where $I_\ell = P_1 \cap \ldots \cap P_\ell$ and P_ℓ denote the minimal prime ideal of R that correspond to the irreducible component $X_\ell \cap U$ of U. By Corollary B.4.42, we have that $\upsilon_i^{\#}(U)$ is injective since X was reduced. Moreover, Corollary B.4.42 provides the exact sequence

$$0 \longrightarrow R/I_i \xrightarrow{\phi_i} R/I_{i-1} \oplus R/P_i \xrightarrow{\psi_i} R/(I_{i-1} + P_i) \longrightarrow 0.$$

Let $\mathscr{S}_i$ denote the sheaf of $\mathcal{O}_{Y_i}$-algebras which makes the corresponding sequence of sheaves of $\mathcal{O}_{Y_i}$-algebras

$$0 \longrightarrow \mathcal{O}_{Y_i} \longrightarrow (h_{i-1})_*\mathcal{O}_{Y_{i-1}} \oplus (j_i)_*\mathcal{O}_{X_i} \longrightarrow \mathscr{S}_i \longrightarrow 0 \tag{4:4}$$

exact. Furthermore, let $\mathcal{J}_i \in \mathcal{O}_{X_i}$ denote the sheaf of $\mathcal{O}_{X_i}$-ideals that cuts out $Y_{i-1} \cap X_i$ in X_i, that is $V(\mathcal{J}_i) = Y_{i-1} \cap X_i$. △

Proposition 2.4.2. *The sheaves $\mathscr{S}$ and $\mathscr{S}_i$ as in Definition 2.4.1 are skyscraper sheaves and hence satisfy*

$$\begin{array}{lll} H^0(X, \mathscr{S}_X) = \bigoplus_{P\in X} (\mathscr{S}_X)_P & \text{with} & \chi(X, \mathscr{S}_X) = \sum_{P\in X} \dim_k (\mathscr{S}_X)_P \text{ and} \\ H^0(Y_i, \mathscr{S}_i) = \bigoplus_{P\in Y_i} (\mathscr{S}_i)_P & \text{with} & \chi(Y_i, \mathscr{S}_i) = \sum_{P\in Y_i} \dim_k (\mathscr{S}_i)_P. \end{array}$$

Moreover, all involved dimensions are finite.

Proof. The sheaf $\mathscr{S}$ is supported on the intersection points of the components X_i of X. By Lemma B.5.3, we know that these are finite in number and hence $\mathscr{S}$ is a skyscraper sheaf. The very same line of argument shows that $\mathscr{S}_i$ is a skyscraper sheaf on Y_i. The statements about the Euler characteristic now follow from Lemma B.2.8.

Note that all $\mathscr{S}$ and $\mathscr{S}_i$ are coherent $\mathcal{O}_X$- and $\mathcal{O}_{Y_i}$-modules (even algebras which are coherent as modules) and thus by [Sta18, Tag 02O6] we obtain that $H^0(Y_i, \mathscr{S}_i)$ and $H^0(X, \mathscr{S})$ are finite k-modules. □

Lemma 2.4.3. *Let X be a reduced cover of $\mathbb{P}^1_k$. Then*

$$\chi(X, \mathscr{S}_X) = \sum_{i=1}^{m} \chi(Y_i, \mathscr{S}_i).$$

Proof. Let $\pi : X \to \mathbb{P}^1_k$ be the finite morphism of degree n. Let $R = \mathcal{O}_X(V_0)$ where $V_0 = \pi^{-1}(U_0)$. Moreover, by P_i we denote the minimal prime ideal of R corresponding to the irreducible component $X_i \cap V_0$. It is easy to see that the irreducible components of an open subset U of a topological space X are given by the intersections of U with the irreducible components of X. Then $X_i \cap V_0 \cong \operatorname{Spec}(R/P_i)$ and $Y_i \cap V_0 \cong \operatorname{Spec}(R/(\bigcap_{j=1}^{i} P_j))$.

Moreover, by assumption $\operatorname{Supp}(\mathscr{S}_X)$ and $\operatorname{Supp}(\mathscr{S}_i)$ are disjoint to $\pi^{-1}(P_\infty)$ and hence we obtain by Proposition 2.4.2 the equalities

$$\begin{array}{lllllllll} S^m & := & H^0(X, \mathscr{S}_X) & = & \bigoplus_{P\in V_0} (\mathscr{S}_X)_P & , & \chi(X, \mathscr{S}_X) & = & \sum_{P\in V_0} \dim_k (\mathscr{S}_X)_P, \\ S_i & := & H^0(Y_i, \mathscr{S}_i) & = & \bigoplus_{P\in Y_i\cap V_0} (\mathscr{S}_i)_P & , & \chi(Y_i, \mathscr{S}_i) & = & \sum_{P\in Y_i\cap V_0} \dim_k (\mathscr{S}_i)_P. \end{array}$$

Note that by definition $Y_1 = X_1$ and hence $\mathscr{S}_1 = 0$ which implies $S_1 = 0$. Moreover, if $m = 1$, then $S^m = 0$, too. By Proposition 2.4.2, all involved dimensions are finite and thus $\dim_k S^m = \chi(X, \mathscr{S}_X)$ as well as $\dim_k S_i = \chi(Y_i, \mathscr{S}_i)$. Hence the assertion is now equivalent to

$$\dim_k S^m = \sum_{i=1}^{m} \dim_k S_i.$$

But as we have seen above, for $m = 1$ we even have $S^1 = S_1$. Then by Lemma B.1.36, the sequences Eq. (4:3) and Eq. (4:4), restricted to V_0, become

$$0 \longrightarrow R \longrightarrow \bigoplus_{i=1}^{m} R/P_i \longrightarrow S^m \longrightarrow 0 \tag{4:5}$$

respectively

$$0 \longrightarrow \frac{R}{P_1 \cap \ldots \cap P_i} \longrightarrow \frac{R}{P_1 \cap \ldots \cap P_{i-1}} \oplus \frac{R}{P_i} \longrightarrow S_i \longrightarrow 0. \tag{4:6}$$

Considering the involved R-modules only as k-vector spaces, the sequences of k-vector spaces split and we obtain the following isomorphisms of k-vector spaces

$$\bigoplus_{i=1}^{m} R/P_i \cong R \oplus S^m, \tag{4:7}$$

respectively

$$\frac{R}{P_1 \cap \ldots \cap P_{i-1}} \oplus \frac{R}{P_i} \cong \frac{R}{P_1 \cap \ldots \cap P_i} \oplus S_i, \tag{4:8}$$

which are true for all $m \geq 1$ and $i \leq m$. Now we claim that $S^m \cong \bigoplus_{i=1}^{m} S_i$ as k-vector spaces which would imply the assertion: We prove it by induction on m, the number of irreducible components of X. The case $m = 1$ is true by definition as we have seen above.

But first note that $R = R/(P_1 \cap \ldots \cap P_m)$ since X, and a fortiori R, is reduced and $P_1, \ldots, P_m$ denote all minimal primes of R.

Now let the hypothesis be true for $m-1$, i.e. $S^{m-1} \cong \bigoplus_{i=1}^{m-1} S_i$ as k-vector spaces and hence the sequence Eq. (4:5) provides the isomorphism

$$\bigoplus_{i=1}^{m-1} R/P_i \cong \frac{R}{P_1 \cap \ldots \cap P_{m-1}} \oplus \bigoplus_{i=1}^{m-1} S_i. \tag{4:9}$$

Now we only need to use known isomorphisms: By Eq. (4:7), we have

$$\begin{aligned}
\frac{R}{P_1 \cap \ldots \cap P_m} \oplus S^m \quad &\cong \quad \bigoplus_{i=1}^{m} R/P_i \quad \cong \quad R/P_m \oplus \bigoplus_{i=1}^{m-1} R/P_i \\
&\text{Eq. (4:9)} \rightsquigarrow \cong \quad R/P_m \oplus \frac{R}{P_1 \cap \ldots \cap P_{m-1}} \oplus \bigoplus_{i=1}^{m-1} S_i \\
&\text{Eq. (4:8)} \rightsquigarrow \cong \quad \frac{R}{P_1 \cap \ldots \cap P_m} \oplus \; S_m \oplus \bigoplus_{i=1}^{m-1} S_i
\end{aligned}$$

and thus, since the resulting homomorphism acts as an isomorphism on the first summand, $S^m \cong S_m \oplus \bigoplus_{i=1}^{m-1} S_i = \bigoplus_{i=1}^{m} S_i$ as desired. □

Remark 2.4.4. Lemma 2.4.3 shows that the sum of the $\chi(Y_i, \mathscr{S}_i)$ is independent of the order $(X_1, \ldots, X_m)$. But obviously, the $\chi(Y_i, \mathscr{S}_i)$ themselves may be unbalanced. △

Lemma 2.4.5. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{J} \leq \mathcal{O}_{Y_i}$ denote the ideal sheaf cutting out $Y_{i-1} \cap X_i$ in Y_i. Then we have*

$$\chi(Y_i, \mathscr{S}_i) = \dim_k \frac{\mathcal{O}_X(V_{i,0})}{\mathcal{J}(V_{i,0})} = \deg_k \mathcal{J}(V_{i,0}).$$

Proof. Let I and P be the ideals of $R = \mathcal{O}_{Y_i}(Y_i \cap V_0)$ that cut out $Y_{i-1} \cap V_0$ respectively $X_i \cap V_0$ in $Y_i \cap V_0$. Since Y_{i-1} and X_i only intersect at points in V_0, the support of the respective sheaves of $\mathcal{O}_X$-ideals cutting out Y_{i-1} respectively X_i in Y_i have support equal

to the support of I respectively P. Let $J = \mathcal{J}(Y_i \cap V_0)$. Then we have $J = I + P$. Since

$$R/J \cong \frac{R/I}{J/I} \cong \frac{R/P}{J/P},$$

the degree of $\mathcal{J}$ in Y_i can also be computed by computing the degree of its restriction to Y_{i-1} or X_i. By assumption, R is reduced and noetherian and thus by Corollary B.4.42 we obtain the exact sequence

$$0 \longrightarrow R \xrightarrow{\phi} R/I \oplus R/P \xrightarrow{\psi} R/J \longrightarrow 0$$

and therefore we have an isomorphism of R-modules $R/J \to \mathscr{S}_i(Y_i \cap V_0)$. Since $k \subseteq R$, this is also a k-vector space isomorphism and thus we finally obtain

$$\dim_k \mathscr{S}_i(Y_i \cap V_0) = \dim_k R/J = \deg_k J = \deg_k \mathcal{J}(V_0).$$

Since $\operatorname{Supp}(\mathscr{S}_i) \subseteq Y_i \cap V_0$, by Proposition 2.4.2, we have

$$\dim_k \mathscr{S}_i(Y_i \cap V_0) = \dim_k H^0(Y_i, \mathscr{S}_i) = \chi(Y_i, \mathscr{S}_i)$$

and thus the assertion follows. □

Remark 2.4.6. Note that the proof of Lemma 2.4.5 tells us that $\chi(Y_i, \mathscr{S}_i)$ is equal to the degree of $\mathcal{J}$, but also equal to the degree of the restriction of $\mathcal{J}$ to Y_{i-1} or X_i. △

Remark 2.4.7. Let X be a proper scheme of dimension one over a field k. There are several definitions of the genus of a scheme. In [Liu02, 7.3.19] the **geometric genus of** X is defined as $\dim_k H^1(X, \mathcal{O}_X)$. For the so called *arithmetic genus of* X there are several definitions. In [Liu02, 7.3.19] it is defined as $p_a(X) = 1 - \chi_k(X, \mathcal{O}_X)$. In [Sta18, Tag 0BY6] the definition of the genus is made dependent on the dimension of the globally regular functions over k, that is, dependent on $\dim_k H^0(X, \mathcal{O}_X)$. If $\dim_k H^0(X, \mathcal{O}_X) = 1$, which is equivalent to $H^0(X, \mathcal{O}_X) = k$, then by [Sta18, Tag 0BY5] we know that X is connected, Cohen-Macaulay and of pure dimension one. In this case the genus of X is defined as $\dim_k H^1(X, \mathcal{O}_X)$ and denoted by g. Note that this definition coincides with that of the arithmetic genus in [Liu02, 7.3.19].

In the case that $\dim_k H^0(X, \mathcal{O}_X) > 1$, [Sta18, Tag 0BY6] refers to [Ser55, p. 276] and [HHSB66, p. 2] where the arithmetic genus is defined as $\chi_k(X, \mathcal{O}_X)$. △

Definition 2.4.8. Since we do not want to impose the requirement $H^0(X, \mathcal{O}_X) = k$ on X, we will make the definition of the genus of X dependent on $\chi_k(X, \mathcal{O}_X)$. We call the integer $g = -\chi_k(X, \mathcal{O}_X)$ the **arithmetic genus of** X. Some formulas will look nicer using the notation $p_a(X) = 1 - \chi_k(X, \mathcal{O}_X) = 1 - g$ but, since we do not want to cause confusion, we will not give this invariant a name. △

Proposition 2.4.9. *Let X be a reduced proper scheme of dimension one over k and let $X_1, \dots, X_m$ be all of its components. By $\mathscr{S}_X$ we denote the sheaf defined in Definition B.3.4. Then $g = \sum_{i=1}^m g_i + \chi(\mathscr{S}_X)$ and therefore $p_a(X) = \sum_{i=1}^m p_a(X_i) + \chi(X, \mathscr{S}_X) + 1 - m$.*

Proof. By Definition B.3.4, we have an exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \bigoplus_{i=1}^m (\tau_i)_* \mathcal{O}_{X_i} \longrightarrow \mathscr{S}_X \longrightarrow 0.$$

Applying the Euler characteristic to the above sequence, we obtain by Lemma 2.4.3

$$\sum_{i=1}^{m} \chi(\mathcal{O}_{X_i}) = \chi\left(\bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{O}_{X_i}\right) = \chi(\mathcal{O}_X) + \chi(\mathscr{S}_X).$$

Subtracting the involved characteristics of structure sheaves we obtain

$$g = -\chi(\mathcal{O}_X) = -\sum_{i=1}^{m} \chi(\mathcal{O}_{X_i}) + \chi(\mathscr{S}_X) = \sum_{i=1}^{m} g_i + \chi(\mathscr{S}_X)$$

as desired. The last asserted equation now follows by adding m on both sides. □

The following definition will fix an invariant of X together with a fixed order $(X_1, \ldots, X_m)$ of its irreducible components if X is reducible and if it is irreducible it will define an invariant of X solely. This invariant will play an important role in this thesis since we will work with polynomial matrices whose entries have degree linearly bounded by that invariant.

Definition 2.4.10. Let X be an integral cover of $\mathbb{P}^1_k$. Then we define

$$c_X = \left\lceil \frac{2g + \dim_k H^0(X, \mathcal{O}_X) + n}{n} \right\rceil.$$

If X is a reduced but reducible cover of $\mathbb{P}^1_k$ with a fixed order $(X_1, \ldots, X_m)$ of irreducible components, we instead define

$$c_{i,X} := c_i(X, (X_1, \ldots, X_m)) := \left\lceil \frac{\chi(\mathscr{S}_i) + 2g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + n_i}{n_i} \right\rceil$$

and

$$c_X := c(X, (X_1, \ldots, X_m)) := \max_{i=1}^{m} \{c_{i,X}\}.$$

Note that the notions $c_{i,X}$ and c_X in the case of reducible X are misleading since they do depend on the fixed order $(X_1, \ldots, X_m)$ of the irreducible components of X. △

Lemma 2.4.11. *We have* $\sum_{i=1}^{m} c_{i,X} n_i \leq 2(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X)$.

Proof. It easy to see that $c_{i,X} n_i \leq \chi(\mathscr{S}_i) + 2g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + 2n_i$. Thus we obtain

$$\begin{aligned}
\sum_{i=1}^{m} c_{i,X} n_i &\leq \sum_{i=1}^{m} (\chi(\mathscr{S}_i) + 2g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + 2n_i) \\
&\leq 2g + \chi(\mathscr{S}_X) + 2n + \sum_{i=1}^{m} \dim_k H^0(X_i, \mathcal{O}_{X_i}) \\
&= 2(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X).
\end{aligned}$$

□

Chapter 3

Divisors, Invertible Sheaves and $\mathcal{O}_X$-Ideals

This chapter is organised as follows: In Section 3.1 we recall the basic definitions of Cartier divisors on arbitrary schemes. These involve the group of Cartier divisors and the group of Cartier divisor classes. Moreover, for curves over k we define the degree of divisors in a local sense using the degree of $\mathcal{O}_{X,P}$-ideals. Furthermore, we introduce the notion of $\mathcal{O}_X$-ideals which are a generalisation of sheaf of ideals on X. We show that the invertible $\mathcal{O}_X$-ideals form a group which is isomorphic to the group of Cartier divisors. This isomorphism is induced by the well known map $D \mapsto \mathcal{O}_X(D)$ which associates to each Cartier divisor an invertible sheaf. We will show some properties of the relation between divisors and invertible $\mathcal{O}_X$-ideals.

In Section 3.2 we analyse divisors on covers of $\mathbb{P}^1_k$. We will mainly be interested in how to move divisors between the different schemes that are involved when talking about covers of $\mathbb{P}^1_k$. That is, we take care of the question of how to restrict divisors on the cover X of $\mathbb{P}^1_k$ to V_0, V_∞ or S. Or if X is reducible with irreducible components $X_1, \ldots, X_m$, then about how to restrict divisors on X to a component X_i. Finally, we introduce a way of restricting $\mathcal{O}_X$-submodules of $\mathcal{K}_X$ in a way that is compatible with the above way of restricting divisors.

3.1 Cartier Divisors

Let X be a scheme. We start by defining the second most important sheaf (right after $\mathcal{O}_X$ itself) we will work with, the so called *sheaf of meromorphic functions* or *sheaf of stalks of meromorphic functions* which will be the sheaf whose sections admit the local equations defining a divisor on a scheme. About this sheaf there has been some misconceptions which have been illuminated by Kleiman in [Kle79]. We now provide its definition as in [Sta18, Tag 01X2] where it is defined as recommended in [Kle79].

Definition 3.1.1. Let $(X, \mathcal{O}_X)$ be a locally ringed space. For any open subset $U \subseteq X$ let $\mathcal{S}_X(U) \subseteq \mathcal{O}_X(U)$ denote the set of regular functions s on U such that the multiplication by s morphism $\mathcal{O}_U \to \mathcal{O}_U$, $f \mapsto f \cdot s$ is injective. The rule $U \mapsto \mathcal{S}_X(U)$ defines a subsheaf of sets of $\mathcal{O}_X$. Now $\mathcal{S}_X(U)$ is a multiplicative subset of $\mathcal{O}_X(U)$ and hence the localisation $\mathcal{S}_X(U)^{-1}\mathcal{O}_X(U)$ is defined. Then the rule

$$U \mapsto \mathcal{S}_X(U)^{-1}\mathcal{O}_X(U)$$

defines a presheaf $\mathcal{K}'_X$ of rings on X. We denote the sheafification of $\mathcal{K}'_X$ by $\mathcal{K}_X$ and call it the **sheaf of meromorphic functions on** X and denote it by $\mathcal{K}_X$. Moreover, a global section of $\mathcal{K}_X$ is called a **meromorphic function on** X. △

Remark 3.1.2. It is straightforward to show that $\mathcal{K}'_X$ is separated, see Lemma B.1.8. Thus we can apply Lemma B.1.22 (ii) to $\mathcal{K}_X$ to see that its sections over some open $U \subseteq X$ can be represented by an open cover $U = \cup_{i\in I} U_i$ and sections $f_i = r_i/s_i \in \mathcal{S}_X(U_i)^{-1}\mathcal{O}_X(U_i)$ of $\mathcal{K}'_X$ such that $(f_i)_{|U_i\cap U_j} = (f_j)_{|U_i\cap U_j}$ for all $i, j \in I$. The latter is equivalent to $(r_i s_j)_{|U_i\cap U_j} = (r_j s_i)_{|U_i\cap U_j}$ in $\mathcal{O}_X(U_i \cap U_j)$. △

The Definition 3.1.1 coincides with the one given in [Liu02, 7.1.13]. There are situations in which there is a well-defined pullback of meromorphic functions and as we will see later that will be the case every time we need that notion of pullback.

Definition 3.1.3. Let $f : Y \to X$ together with $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ be a morphism of schemes. We say that the **pullback of meromorphic functions along f is defined** if for every pair of open subsets $V \subseteq Y$ and $U \subseteq X$ such that $f(V) \subseteq U$, and if for any section $s \in \mathcal{S}_X(U)$ the pullback $f^\#(V)(s) \in \mathcal{O}_Y(V)$ actually lies in $\mathcal{S}_Y(V)$.

By definition of $\mathcal{S}_X$ and $\mathcal{K}_X$, the morphism $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ extends to a morphism $f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$ which we also denote by $f^\#$. Then we obtain two equivalent commutative diagrams

$$\begin{array}{ccc} f^{-1}\mathcal{O}_X & \xrightarrow{f^\#} & \mathcal{O}_Y \\ \downarrow & & \downarrow \\ f^{-1}\mathcal{K}_X & \xrightarrow{f^\#} & \mathcal{K}_Y \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathcal{O}_X & \xrightarrow{f^\#} & f_*\mathcal{O}_Y \\ \downarrow & & \downarrow \\ \mathcal{K}_X & \xrightarrow{f^\#} & f_*\mathcal{K}_Y. \end{array} \qquad \triangle$$

Remark 3.1.4. Note that if the morphism $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ extends to $f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$, or equivalently, $f^\# : \mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$, then the pullback of meromorphic functions along f is defined. This is due to the fact that the units in $\mathcal{K}_X(U)$ and $\mathcal{K}_Y(V)$ are given by quotients of elements in $\mathcal{S}_X(U)$ respectively $\mathcal{S}_Y(V)$ and that ring homomorphisms send units to units. Therefore, the pullback of meromorphic functions along f is defined if and only if $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ extends to $f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$. △

Note that by Lemma B.1.37, both $\mathcal{K}_X^\times$ and $\mathcal{O}_X^\times$ are sheaves of abelian groups. In the following we will denote the group law of the multiplicative group $H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$ additive.

Definition 3.1.5. Let X be a scheme. By $\mathrm{Div}(X) = H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$ we denote the **group of divisors** on X. An element of $\mathrm{Div}(X)$ is called **Cartier divisor** or short **divisor** on X. We have a natural morphism of sheaves

$$\mathcal{K}_X^\times \to \mathcal{K}_X^\times/\mathcal{O}_X^\times$$

providing a morphism $\phi : H^0\left(X, \mathcal{K}_X^\times\right) \to \mathrm{Div}(X)$. The image of ϕ is a subgroup of $\mathrm{Div}(X)$ and denoted by $\mathrm{Princ}(X)$. An element of it is called a **principal divisor** on X. Two divisors $D, E \in \mathrm{Div}(X)$ are called **linearly equivalent** if $D - E$ is a principal divisor. A divisor $D \in \mathrm{Div}(X)$ is called **effective**, denoted by $D \geq 0$, if it lies in the image of the map $H^0\left(X, \mathcal{O}_X \cap \mathcal{K}_X^\times\right) \to \mathrm{Div}(X)$. The quotient group $\mathrm{Div}(X)/\mathrm{Princ}(X)$ is denoted by $\mathrm{CaCl}(X)$ and is called the **group of Cartier divisor classes** on X. △

Since $\mathcal{K}_X^\times/\mathcal{O}_X^\times$ is the sheafification of the presheaf $U \mapsto \mathcal{K}_X(U)^\times/\mathcal{O}_X(U)^\times$, we may unravel the definition of Cartier divisors a bit by using our descriptions of sections of the sheafification of a presheaf, see Section B.1.

Remark 3.1.6. Following Section B.1, we see that every divisor $D \in \mathrm{Div}(X)$ is represented by a weakly matching family $(U_i, f_i \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$ where $X = \cup_{i\in I} U_i$, $f_i \in \mathcal{K}_X(U_i)^\times$ and for every $i, j \in I$ we have $f_{i|U_i\cap U_j} \cdot \mathcal{O}_X(U_i \cap U_j)^\times = f_{j|U_i\cap U_j} \cdot \mathcal{O}_X(U_i \cap U_j)^\times$, that is $f_{i|U_i\cap U_j}/f_{j|U_i\cap U_j} \in \mathcal{O}_X(U_i\cap U_j)^\times$. We call such a weakly matching family a **configuration** representing or inducing D.

Two configurations $(U_i, f_i \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$ and $(V_j, h_j \cdot \mathcal{O}_X(V_j)^\times)_{j\in J}$ define the same global section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$ and thus induce resp. represent the same divisor if and only if for all $(i,j) \in I \times J$ we have $f_{i|U_i\cap V_j}/h_{j|U_i\cap V_j} \in \mathcal{O}_X(U_i \cap V_j)^\times$.

A divisor D on X is a principal divisor if and only if it may be represented by a configuration of the form $(X, f \cdot \mathcal{O}_X(X)^\times)$ for some $f \in \mathcal{K}_X(X)^\times$. △

Definition 3.1.7. By the above description, we see that a divisor D is effective if and only if can be represented by a configuration of the form $(U_i, f_i \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$ with $f_i \in \mathcal{O}_X(U_i)$. Given two divisors D and E by configurations $(U_i, f_i \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$ respectively $(V_j, g_j \cdot \mathcal{O}_X(V_j)^\times)_{j\in J}$, the sum $D + E$ is represented by the configuration

$$(U_i \cap V_j, f_i g_j \cdot \mathcal{O}_X(U_i \cap V_j)^\times)_{(i,j)\in I\times J}.$$

Thus the inverse $-D$ of a divisor D which is induced by $(U_i, f_i \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$ will be represented by $(U_i, f_i^{-1} \cdot \mathcal{O}_X(U_i)^\times)_{i\in I}$. For two divisors D and E on X we write $D \geq E$ if $D - E \geq 0$. The **support of** D, denoted by $\mathrm{Supp}(D)$, is defined to be the support of D as a section of the sheaf $\mathcal{K}_X^\times/\mathcal{O}_X^\times$, see Definition B.1.5. This comes down to

$$\mathrm{Supp}(D) = \{P \in X \mid D_P \neq 1\} = \{P \in X \mid (f_i)_P \notin \mathcal{O}_{X,P}{}^\times\}.$$ △

Lemma 3.1.8. *Let X be a scheme. Let D be a divisor on X. Then*

(i) $\mathrm{Supp}(D)$ *is a closed subset of X not containing any generic point of X.*

(ii) If X has additionally dimension one, then every point in $\mathrm{Supp}(D)$ *is a closed point of X.*

(iii) If X is additionally noetherian, then $\mathrm{Supp}(D)$ *is also finite.*

Proof. First of all, by Lemma B.1.6, the support of any section of a sheaf of abelian groups on X is a closed subset of X. Hence $\mathrm{Supp}(D)$ is closed. Let us now prove that it does not contain any generic point of X. Let $\eta \in X^0$ be a generic point of X. Then by [Sta18, Tag 0BA9], the local ring $\mathcal{O}_{X,\eta}$ is a zero-dimensional ring. In particular, the maximal ideal P of $\mathcal{O}_{X,\eta}$ is also the unique minimal prime ideal. Hence by Corollary B.4.14, it consists solely of zero-divisors. Therefore, every regular element of $\mathcal{O}_{X,\eta}$ is a unit and thus $\mathrm{Frac}(\mathcal{O}_{X,\eta}) \cong \mathcal{O}_{X,\eta}$. Now using Lemmas B.1.19 and B.1.37 provides

$$(\mathcal{K}_X^\times/\mathcal{O}_X^\times)_\eta \cong (\mathcal{K}_X^\times)_\eta/(\mathcal{O}_X^\times)_\eta \cong \mathcal{K}_{X,\eta}^\times/\mathcal{O}_{X,\eta}^\times.$$

Hence Proposition B.2.2 implies that $(\mathcal{K}_X^\times/\mathcal{O}_X^\times)_\eta$ is trivial. Therefore, every divisor (as a section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$) has zero germ at every generic point of X. This proves the first assertion.

The second assertion follows immediately since every point of X lies on at least one irreducible component of X and is thus by Lemma B.5.1, either a closed point or the generic point of that component. Whence any non-generic point of X and a fortiori every point of $\mathrm{Supp}(D)$ is closed in X.

Since $\mathrm{Supp}(D)$ solely consists of closed points of X, its points are its irreducible components. Since X is noetherian, the same is true for $\mathrm{Supp}(D)$ due to [Sta18, Tag 0052]. But again by [Sta18, Tag 0052], noetherian spaces only have finitely many irreducible components which thus proves the last assertion. □

Notation 3.1.9. Note that, by abuse of notation, we will mainly denote configurations that represent a divisor simply by (U_i, f_i) without mentioning that U_i, $i \in I$ for some index set I will form an open cover of X and also suppressing that the local representative f_i should actually be $f_i \cdot \mathcal{O}_X(U)^\times$. △

If X is a curve over k, see Definition 2.1.1, then in [Liu02, 7.3.1] the notion of degree of a Cartier divisor is introduced. We will not recall what that definition is at this point here, but refer the reader to Lemma C.4.8 where this is stated in the proof. Moreover, we have shown there that the notion introduced in [Liu02, 7.3.1] is equivalent to the following one.

Definition 3.1.10. Let X be a curve over k. Let $D \in \mathrm{Div}(X)$ and we denote its germ at $(\mathcal{K}_X^\times/\mathcal{O}_X^\times)_P = \mathcal{K}_{X,P}^\times/\mathcal{O}_{X,P}^\times$ by $D_P = a_P/b_P$ with $a_P, b_P \in \mathrm{Frac}(\mathcal{O}_{X,P})^\times$. We define the **degree of D over k**, or short **degree of D**, to be

$$\deg_k D = \sum_{P \in X_0} \dim_k \mathcal{O}_{X,P}/a_P\mathcal{O}_{X,P} - \dim_k \mathcal{O}_{X,P}/b_P\mathcal{O}_{X,P}.$$

This is well-defined since the elements a_P, b_P are unique up to multiplication with units in $\mathcal{O}_{X,P}$. △

Note that on more general schemes the notion of degree of a divisor is more involved and cannot (due to dimensional reasons) be stated solely in terms of multiplicities at closed points.

Remark 3.1.11. The degree of divisors establishes a group homomorphism $\deg_k : \mathrm{Div}(X) \to \mathbb{Z}$. Furthermore, in the proof of Lemma C.4.8 it is shown that

$$\deg_k D = \sum_{P \in X_0} \deg_k D_P\mathcal{O}_{X,P}$$

where $\deg_k D_P\mathcal{O}_{X,P}$ denotes the degree of the $\mathcal{O}_{X,P}$-ideal $D_P\mathcal{O}_{X,P}$, see Definition C.1.14 in Section C.1. Then the statement about being a group homomorphism follows from Proposition C.1.26. △

Lemma 3.1.12 ([Liu02], 7.3.18)**.** *If X is projective, then every principal divisor $\mathrm{div}_X(f) \in \mathrm{Div}(X)$ has degree zero.*

In Chapter 5 we will define and analyse the so called Picard group $\mathrm{Pic}(X)$ which is the set of isomorphism classes of invertible sheaves on X together with the tensor product of $\mathcal{O}_X$-modules as group law, see Definition 5.0.1. Recall that a sheaf $\mathcal{F}$ on a scheme X is called an *invertible sheaf* if it is a locally free $\mathcal{O}_X$-module of rank 1. That is, for every $P \in X$ there is an open neighborhood $U \subseteq X$ of P such that $\mathcal{F}_{|U}$ is isomorphic to $\mathcal{O}_U$.

We are now going to establish a 1-to-1 correspondence between divisors on X and so called invertible $\mathcal{O}_X$-ideals which will also be an isomorphism of abelian groups. In Chapter 5 we will link both divisors and invertible $\mathcal{O}_X$-ideals with the Picard group $\mathrm{Pic}(X)$. Throughout this thesis $\mathcal{O}_X$-ideals will play the role of a generalisation of divisors. We decided to care about those since many of the techniques we will use to cope with the computation in the Picard group even work for $\mathcal{O}_X$-ideals instead of for divisors only. Moreover, some theoretical results that are well known for divisors extend to $\mathcal{O}_X$-ideals as well. In Chapter 4 for instance, we will talk about the representation of global sections of $\mathcal{O}_X$-ideals and more generally for *generalised vector bundles*.

Definition 3.1.13. Let k be a field and let X be a curve of finite residual-type over k (e.g. X a cover of $\mathbb{P}^1_k$, see Remark 2.1.2). Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-submodule of $\mathcal{K}_X$. If $\mathcal{F}$ is invertible at the generic points of X, then we say that $\mathcal{F}$ is an **$\mathcal{O}_X$-ideal**. This is equivalent to $\mathcal{F}(U)$ being an $\mathcal{O}_X(U)$-ideal for every affine open subset $U \subseteq X$, see Definition C.1.2 on page 260. △

Example 3.1.14. Obviously, any invertible $\mathcal{O}_X$-submodule of $\mathcal{K}_X$ is an $\mathcal{O}_X$-ideal. Moreover, if $U \subseteq X$ is an open subset, then the restriction $\mathcal{F}_{|U}$ of an $\mathcal{O}_X$-ideal $\mathcal{F}$ to U is an $\mathcal{O}_U$-ideal. △

Definition 3.1.15. Let $\mathcal{F}, \mathcal{G} \leq \mathcal{K}_X$ be two $\mathcal{O}_X$-ideals. Since $\mathcal{K}_X$ is a sheaf of $\mathcal{O}_X$-algebras, the map $U \mapsto \mathcal{F}(U)\mathcal{G}(U)$ defines a presheaf using the restriction maps of $\mathcal{F}$ and $\mathcal{G}$ (that is, that of $\mathcal{K}_X$). We denote its sheafification by $\mathcal{FG}$ and call it the **product of the $\mathcal{O}_X$-ideals $\mathcal{F}$ and $\mathcal{G}$**. Since $\mathcal{K}_X$ is a sheaf, it is separated by definition. Now the presheaf $U \mapsto \mathcal{F}(U)\mathcal{G}(U)$ is a subpresheaf of $\mathcal{K}_X$ and hence by Lemma B.1.9 it is separated. By definition of the sheafification, see Definition B.1.14, and Lemma B.1.22 we have

$$(\mathcal{FG})(U) = \{(s_i, U_i)_{i\in I} \mid U = \cup_{i\in I} U_i, s_i \in \mathcal{F}(U_i)\mathcal{G}(U_i) : \ \forall i, j \in I \ s_{i|U_{i,j}} = s_{j|U_{i,j}}\}$$

where $U_{i,j} = U_i \cap U_j$ and the restriction $s_{i|U_{i,j}}$ is the image of $s_i \in \mathcal{K}_X(U)$ under the restriction map of $\mathcal{K}_X$ from U to $U_{i,j}$. Now since $\mathcal{F}(U_i), \mathcal{G}(U_i) \subseteq \mathcal{K}_X(U_i)$, we have $\mathcal{F}(U_i)\mathcal{G}(U_i) \subseteq \mathcal{K}_X(U_i)$ and thus the compatibility condition of the local section s_i above provide that (s_i, U_i) provide a section in $\mathcal{K}_X(U)$. This yields that $\mathcal{FG} \leq \mathcal{K}_X$ is also an $\mathcal{O}_X$-ideal. Now we obviously have $\mathcal{F} = \mathcal{F}\mathcal{O}_X = \mathcal{O}_X\mathcal{F}$ for any $\mathcal{O}_X$-ideal $\mathcal{F}$ and hence the set of $\mathcal{O}_X$-ideals together with the multiplication (which is associative) forms a monoid which we call **the monoid of $\mathcal{O}_X$-ideals** on X and denote by $\mathrm{MonoId}(X)$. △

Lemma 3.1.16. *Let $\mathcal{F}, \mathcal{G} \leq \mathcal{K}_X$ be two $\mathcal{O}_X$-ideals. Then for every $P \in X$ we have $(\mathcal{FG})_P = \mathcal{F}_P\mathcal{G}_P$.*

Proof. Since $(\mathcal{F}^{\#})_P = \mathcal{F}_P$ for every presheaf $\mathcal{F}$ on X and $P \in X$, see Lemma B.1.15 and Remark B.1.16, we only need to prove the equality for the presheaf $(\mathcal{FG})^p$. For every $P \in X$ we find an affine neighborhood U of P and since $\mathcal{F}$ and $\mathcal{G}$ are quasi-coherent, we have $\mathcal{F}_P = \mathcal{F}(U)_P$ and $\mathcal{G}_P = \mathcal{G}(U)_P$. Now it is obvious that $(\mathcal{F}(U)\mathcal{G}(U))_P = \mathcal{F}(U)_P\mathcal{G}(U)_P$ as subsets of $\mathrm{Frac}(\mathcal{O}_X(U)) = \mathcal{K}_X(U)$. Hence $(\mathcal{F}(U)\mathcal{G}(U))_P = \mathcal{F}_P\mathcal{G}_P$ as asserted. □

Lemma 3.1.17. *Let $\mathcal{F}, \mathcal{G}$ be two $\mathcal{O}_X$-ideals. Then for any affine open $U = \mathrm{Spec}(A)$ we have $(\mathcal{FG})(U) \cong \mathcal{F}(U)\mathcal{G}(U)$. In particular, $(\mathcal{FG})_{|U}$ is quasi-coherent with $(\mathcal{FG})_{|U} \cong (\mathcal{F}(U)\mathcal{G}(U))^{\sim}$.*

Proof. Since $\mathcal{F}$ and $\mathcal{G}$ are quasi-coherent, by [Liu02, 5.1.7], we have that $\mathcal{F}(U)^{\sim} \cong \mathcal{F}_{|U}$ and $\mathcal{G}(U)^{\sim} \cong \mathcal{G}_{|U}$. Moreover, we have $\mathcal{F}(U)_P \cong \mathcal{F}_P$, $\mathcal{G}(U)_P \cong \mathcal{G}_P$ and for all basic open subset $D(a) \subseteq U$ of U with $a \in A$ we have $\mathcal{F}(D(a)) = \mathcal{F}(U)_a$ as well as $\mathcal{G}(D(a)) = \mathcal{G}(U)_a$. Let us define a homomorphism $\phi : \mathcal{F}(U)\mathcal{G}(U) \to (\mathcal{FG})(U)$: By Corollary D.1.3, for every $P \in U$ we have a basic open neighborhood $V_P = D(a_P)$ with $a_P \in A$ and thus Definition B.1.14 together with Lemma B.1.22 provide that any section s of $\mathcal{FG}$ over U can be given by a weakly matching family $(s(V_P), V_P)_{P\in U}$ with $s(V_P) \in \mathcal{F}(V_P)\mathcal{G}(V_P) = \mathcal{F}(U)_{a_P}\mathcal{G}(U)_{a_P}$ and $s(V_P)_{|V_P\cap V_Q} = s(V_Q)_{|V_P\cap V_Q}$ in $\mathcal{F}(U)_{a_Pa_Q}\mathcal{G}(U)_{a_Pa_Q}$ for all $P, Q \in U$. Now let us define

$$\begin{array}{rccc} \phi: & \mathcal{F}(U)\mathcal{G}(U) & \to & (\mathcal{FG})(U) \\ & s & \mapsto & (s_{|V_P}, V_P)_{P\in U} \end{array}$$

where $V_P = D(a_P)$ with $a_P \in A$ and $s_{|V_P}$ denotes the image of s under the presheaf restriction map

$$\rho^U_{V_P}((\mathcal{FG})^p) : \mathcal{F}(U)\mathcal{G}(U) \to \mathcal{F}(V_P)\mathcal{G}(V_P) = \mathcal{F}(U)_{a_P}\mathcal{G}(U)_{a_P} = (\mathcal{F}(U)\mathcal{G}(U))_{a_P}.$$

Obviously, this restriction map is simply the localisation homomorphism λ_{a_P} by a_P. The induced homomorphism ϕ_P for $P \in X$ is obviously the homomorphism sending the germ s_P of s to $(s_{|V_P})_P = s_P$. Indeed, for given $s_P \in \mathcal{F}(U)_P\mathcal{G}(U)_P$ the homomorphism ϕ_P sends s_P to the image of s under the homomorphism

$$\mathcal{F}(U)\mathcal{G}(U) \longrightarrow (\mathcal{F}(U)\mathcal{G}(U))_{a_P} \longrightarrow ((\mathcal{F}(U)\mathcal{G}(U))_{a_P})_P \xrightarrow{\cong} (\mathcal{F}(U)\mathcal{G}(U))_P$$

which is obviously just the localisation homomorphism $\mathcal{F}(U)\mathcal{G}(U) \to (\mathcal{F}(U)\mathcal{G}(U))_P$ where the latter is by Lemma 3.1.16 isomorphic to $(\mathcal{F}\mathcal{G})_P$. Thus ϕ is an isomorphism. □

Lemma 3.1.18. *Let $\mathcal{F}, \mathcal{G} \leq \mathcal{K}_X$ be two invertible $\mathcal{O}_X$-ideals.*

1. *Then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} \cong \mathcal{F}\mathcal{G}$.*
2. *Let $\mathcal{H}$ be an invertible $\mathcal{O}_X$-ideal. Then $\mathcal{F} \leq \mathcal{G}$ implies $\mathcal{F}\mathcal{H} \leq \mathcal{G}\mathcal{H}$.*

   More precisely, let $\mathcal{F}$ be given by $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$ for $f_i \in \mathcal{K}_X(U_i)^\times$ and $i \in I$. Then for any embedding of $\mathcal{O}_X$-ideals $i : \mathcal{F} \hookrightarrow \mathcal{G}$ we have an embedding $i' : \mathcal{F}\mathcal{H} \hookrightarrow \mathcal{G}\mathcal{H}$ such that $i'(U_i) : \mathcal{F}(U_i)\mathcal{H}(U_i) \hookrightarrow \mathcal{G}(U_i)\mathcal{H}(U_i)$ maps f_ih to $i(f_i)h$ for $h \in \mathcal{H}(U_i)$.

Proof. We define a morphism of presheaves ϕ given by

$$\begin{array}{rccc} \phi(U): & \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U) & \to & \mathcal{F}(U)\mathcal{G}(U) \\ & f \otimes g & \mapsto & fg \end{array}$$

where the product fg is computed in $\mathcal{K}_X(U)$. Now since both $\mathcal{F}(U)$ and $\mathcal{G}(U)$ are invertible, by [Eis95, 11.6], $\phi(U)$ defines an isomorphism of $\mathcal{O}_X(U)$-modules. Hence ϕ is an isomorphism of presheaves. Since associating the sheafification of a presheaf to that presheaf defines a functor from the category of presheaves to the category of sheaves, see [GW10, 2.24], this isomorphism of presheaves results in an isomorphism of sheaves $\phi : \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} \to \mathcal{F}\mathcal{G}$ as asserted.

The particular part follows from the fact that the functor $- \otimes_{\mathcal{O}_X} \mathcal{H}$ is left-exact. Indeed, if $i : \mathcal{F} \to \mathcal{G}$ is injective, then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{H} \to \mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{H}$ is also injective. Then the above isomorphisms $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{H} \to \mathcal{F}\mathcal{H}$ and $\mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{H} \to \mathcal{G}\mathcal{H}$ provide an injective morphism $\mathcal{F}\mathcal{H} \to \mathcal{G}\mathcal{H}$ which by the construction of the above isomorphisms clearly maps f_ih to $i(f_i)h$ as asserted. □

Definition 3.1.19. Let $\mathcal{F}, \mathcal{G} \leq \mathcal{K}_X$ be two invertible $\mathcal{O}_X$-ideals. Then $\mathcal{F}\mathcal{G}$ is again an invertible $\mathcal{O}_X$-ideal since being locally free can be checked on the level of stalks. Now the product of invertible $\mathcal{O}_X$-ideals together with $\mathcal{O}_X$ as the neutral element defines a multiplicative abelian group, the **group of invertible $\mathcal{O}_X$-ideals**, denoted by $\mathrm{InvId}(X)$. Corollary 3.1.25 proves that there are indeed inverse elements. The invertible $\mathcal{O}_X$-ideals of the form $f\mathcal{O}_X$ with $f \in \mathcal{K}_X(X)^\times$ form a subgroup of $\mathrm{InvId}(X)$ which we call the subgroup of **principal invertible $\mathcal{O}_X$-ideals** and denote it by $\mathrm{PrincId}(X)$. We call the respective quotient group the **class group of invertible $\mathcal{O}_X$-ideals** and denote it by $\mathrm{ClInvId}(X)$. △

Remark 3.1.20. We will see in Chapter 4, Remark 4.1.5 that the notion of $\mathcal{O}_X$-ideals is equivalent with the notion of *generalised divisors* introduced in [Har07] for the schemes in question. Now considering $\mathcal{O}_X$-ideals up to linear equivalence, that is, up to isomorphism given by a regular global section $f \in \mathcal{K}_X(X)^\times$ (see for instance the upcoming Lemma 3.1.26), we obtain an equivalent of the so called *generalised line bundles*, see [Car20, p. 1]. △

Remark 3.1.21. In the appendix, in Section C.4 we will define the degree $\deg_k$ of $\mathcal{O}_X$-ideals for curves of finite residual-type over k, see Definition C.4.1. Similar to the degree of Cartier divisors introduced above, the degree of $\mathcal{O}_X$-ideals also establishes a group homomorphism $\deg_k : \mathrm{InvId}(X) \to \mathbb{Z}$, see Lemma C.4.7.

In Proposition 3.1.27 we will see that there is a correspondence between Cartier divisors on X and invertible $\mathcal{O}_X$-ideals. Moreover, we will also see there that the two notions of degree are also related. △

Remark 3.1.22. By definition, any invertible $\mathcal{O}_X$-ideal is an invertible $\mathcal{O}_X$-module on X and hence defines an element in $\mathrm{Pic}(X)$. This provides a map $\mathrm{InvId}(X) \to \mathrm{Pic}(X)$ which is by Lemma 4.1.2 surjective. △

Lemma 3.1.23. *Every $\mathcal{F} \in \mathrm{InvId}(X)$ comes with some open cover $\cup_{i\in I} U_i = X$ of X and $f_i \in \mathcal{K}_X(U_i)^\times$ such that $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$. In particular, we obtain a map $\mathrm{InvId}(X) \to \mathrm{Div}(X)$.*

Proof. Let $\mathcal{F}$ be an invertible $\mathcal{O}_X$-ideal. Then there is an open cover $\cup_{i\in I} U_i = X$ and isomorphisms $\gamma_i : \mathcal{O}_{U_i} \to \mathcal{F}_{|U_i}$ of $\mathcal{O}_{U_i}$-submodules of $\mathcal{K}_{U_i}$. Since γ_i is an isomorphism, the isomorphism $\gamma_i(U_i) : \mathcal{O}_X(U_i) \to \mathcal{F}(U_i)$ corresponds to the image of the unit section in $\mathcal{O}_X(U_i)$ which is a generator, say f_i, of $\mathcal{F}(U_i) \subseteq \mathcal{K}_X(U_i)$ as an $\mathcal{O}_X(U_i)$-module. The same holds for any open subset $V_i \subseteq U_i$ with generator $f_{V_i} \in \mathcal{K}_X(V_i)^\times$ of $\mathcal{F}(V_i)$. By definition of γ_i, the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_X(U_i) & \xrightarrow{\gamma(U_i)} & \mathcal{F}(U_i) = f_i\mathcal{O}_{U_i} \\ \downarrow{\scriptstyle \rho_{U_i,V_i,\mathcal{O}_X}} & & \downarrow{\scriptstyle \rho_{U_i,V_i,\mathcal{F}}} \\ \mathcal{O}_X(V_i) & \xrightarrow{\gamma(V_i)} & \mathcal{F}(V_i) = f_{V_i}\mathcal{O}_{V_i} \end{array}$$

In particular, $\gamma(V_i)(\rho_{U_i,V_i,\mathcal{O}_X}(1)) = \rho_{U_i,V_i,\mathcal{F}}(\gamma(U_i)(1))$ and thus $f_{V_i} = f_{i|V_i}$. This shows that $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$.

To prove the particular part let us denote $U_i \cap U_j$ by $U_{i,j}$. Now for all $i, j \in I$ we have that both the restrictions of f_i and of f_j to $U_{i,j}$ generate $\mathcal{F}_{|U_{i,j}}$ over $\mathcal{O}_{U_{i,j}}$, that is $f_{i|U_{i,j}} f_{j|U_{i,j}}^{-1} \in \mathcal{O}_X(U_{i,j})^\times$. Hence we can form the configuration (U_i, f_i^{-1}) which then defines a divisor $D \in \mathrm{Div}(X)$. It is obvious that any other open cover and local generators for $\mathcal{F}$ will provide by construction the same divisor and thus we obtain the asserted well-defined map. □

Lemma 3.1.24. *Let $\mathcal{F}, \mathcal{G} \in \mathrm{InvId}(X)$ be given by $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$ for $i \in I$ and $\mathcal{G}_{|V_j} = g_j\mathcal{O}_{V_j}$ for $j \in J$, respectively. Then $\mathcal{FG}$ is the $\mathcal{O}_X$-ideal given by $(\mathcal{FG})_{|U_i\cap V_j} = f_ig_j\mathcal{O}_{|U_i\cap V_j}$.*

Proof. By definition, we have

$$(\mathcal{FG})(U_i \cap V_j) = \{(s_k, W_k)_{k\in I} \mid U_i \cap V_j = \cup_{k\in I} W_k, s_k \in \mathcal{F}(W_k)\mathcal{G}(W_k) : \\ \forall\ k, h \in I\ s_{k|W_k\cap W_h} = s_{h|W_k\cap W_h} \}$$

and since $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$ and $\mathcal{G}_{|V_j} = g_j\mathcal{O}_{V_j}$ as well as $W_k \subseteq U_i \cap V_j$, we have $s_k \in \mathcal{F}(W_k)\mathcal{G}(W_k) = f_ig_j\mathcal{O}_X(W_k)$ and thus $s_k = f_ig_jw_k$ for some $w_k \in \mathcal{O}_X(W_k)$. Now the compatibility condition $s_{k|W_k\cap W_h} = s_{h|W_k\cap W_h}$ translates to $(f_ig_jw_k)_{|W_k\cap W_h} = (f_ig_jw_h)_{|W_k\cap W_h}$ which is equivalent to $(w_k)_{|W_k\cap W_h} = (w_h)_{|W_k\cap W_h}$. Thus (W_k, w_k) glues to a section of $\mathcal{O}_X(U_i \cap V_j)$ and hence we obtain

$$(\mathcal{FG})(U_i \cap V_j) = f_ig_j\mathcal{O}_X(U_i \cap V_j)$$

which provides the assertion. □

Corollary 3.1.25. *Let $\mathcal{F} \in \mathrm{InvId}(X)$ be given by $\mathcal{F}_{|U_i} = f_i\mathcal{O}_{U_i}$ for $i \in I$. Then the inverse $\mathcal{F}^{-1}$ of $\mathcal{F}$ is the element in $\mathrm{InvId}(X)$ defined by $(\mathcal{F}^{-1})_{|U_i} = f_i^{-1}\mathcal{O}_{U_i}$.*

Proof. Since $\mathcal{F} \in \mathrm{InvId}(X)$, there is a unique $\mathcal{G} \in \mathrm{InvId}(X)$ with $\mathcal{G}_{|U_i} = f_i^{-1}\mathcal{O}_{U_i}$. Moreover, $(\mathcal{FG})_{|U_i} = f_if_i^{-1}\mathcal{O}_{U_i} = \mathcal{O}_{U_i}$ by Lemma 3.1.24 and hence $\mathcal{FG} = \mathcal{O}_X$ as asserted. □

Lemma 3.1.26. *The subgroup $\mathrm{PrincId}(X)$ equals the set of invertible $\mathcal{O}_X$-ideals isomorphic to $\mathcal{O}_X$. In particular, two invertible $\mathcal{O}_X$-ideals are isomorphic if and only if they differ multiplicatively by an element in $\mathrm{PrincId}(X)$.*

Proof. Obviously, every principal $\mathcal{O}_X$-ideal $f\mathcal{O}_X$ is isomorphic to $\mathcal{O}_X$ by the isomorphism $\mathcal{O}_X \to f\mathcal{O}_X$ given by the multiplication with f.

Let $\mathcal{F}$ be an invertible $\mathcal{O}_X$-ideal isomorphic to $\mathcal{O}_X$ by the isomorphism $\gamma : \mathcal{O}_X \to \mathcal{F}$. In particular, $\gamma(X) : \mathcal{O}_X(X) \to \mathcal{F}(X)$ corresponds to a generator $f \in \mathcal{F}(X) \subseteq \mathcal{K}_X(X)$ of $\mathcal{F}(X)$. Since $\gamma(X)$ is an isomorphism, we have $f \in \mathcal{K}_X(X)^\times$. Now we argue that the restriction of f to any open subset $U \subseteq X$ is the generator of $\mathcal{F}(U)$. By the same line of argument as above, the morphism $\gamma(U) : \mathcal{O}_X(U) \to \mathcal{F}(U)$ corresponds to an element $f_U \in \mathcal{K}_X(U)^\times$ generating $\mathcal{F}(U)$. Since for any open subset $U \subseteq X$ the diagram

$$\begin{array}{ccc} \mathcal{O}_X(X) & \xrightarrow{\gamma(X)} & \mathcal{F}(X) \\ \downarrow{\scriptstyle \rho_{X,U,\mathcal{O}_X}} & & \downarrow{\scriptstyle \rho_{X,U,\mathcal{F}}} \\ \mathcal{O}_X(U) & \xrightarrow{\gamma(U)} & \mathcal{F}(U) \end{array}$$

commutes, we have

$$\rho_{X,U,\mathcal{F}}(\gamma(X)(1)) = \gamma(U)(\rho_{X,U,\mathcal{O}_X}(1))$$

and hence $f_{|U} = f_U$. This provides $\mathcal{F} = f\mathcal{O}_X$.

Let us now prove the second assertion. Let $\alpha : \mathcal{F} \to \mathcal{G}$ be an isomorphism of $\mathcal{O}_X$-modules. Since $\mathcal{F}$ is invertible and invertible $\mathcal{O}_X$-modules are flat, the induced morphism $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^{-1} \to \mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{F}^{-1}$ is again an isomorphism. Using Lemma 3.1.18 we thus have an isomorphism

$$\mathcal{O}_X = \mathcal{F}\mathcal{F}^{-1} \to \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^{-1} \to \mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{F}^{-1} \to \mathcal{G}\mathcal{F}^{-1}.$$

Using the first assertion thus provides $\mathcal{G}\mathcal{F}^{-1} = f\mathcal{O}_X$ for some $f \in \mathcal{K}_X(X)^\times$. Now multiplying both sides with $\mathcal{F}$ provides $\mathcal{G} = f\mathcal{F}$.

Conversely, if $\mathcal{G} = f\mathcal{F}$, then the multiplication with $f^{-1} \in \mathcal{K}_X(X)^\times$ morphism $\mathcal{G} = f\mathcal{F} \to \mathcal{F}$ yields an isomorphism. □

There is a natural relation between invertible $\mathcal{O}_X$-ideals and divisors which tells us that they are essentially the same.

Proposition 3.1.27. *Every divisor $D \in \operatorname{Div}(X)$ given by the configuration (U_i, f_i) induces a unique invertible $\mathcal{O}_X$-ideal $\mathcal{O}_X(D)$ given by $\mathcal{O}_X(D)_{|U_i} = f_i^{-1}\mathcal{O}_{U_i}$.*

(i) This induces an isomorphism of abelian groups

$$\begin{array}{rccc} \phi : & \operatorname{Div}(X) & \to & \operatorname{InvId}(X) \\ & D & \mapsto & \mathcal{O}_X(D) \end{array}$$

under which principal divisors $\operatorname{div}(f)$ with $f \in \mathcal{K}_X(X)^\times$ correspond to $f^{-1}\mathcal{O}_X$.

(ii) For every $D \in \operatorname{Div}(X)$ we have

$$D \geq 0 \quad \Leftrightarrow \quad \mathcal{O}_X \leq \mathcal{O}_X(D) \quad \Leftrightarrow \quad \mathcal{O}_X(-D) \leq \mathcal{O}_X.$$

(iii) For every $D \in \operatorname{Div}(X)$ we have $\deg_k D = -\deg_k \mathcal{O}_X(D)$ where the latter is defined in Section C.4.

(iv) If X is projective, then principal divisors and principal $\mathcal{O}_X$-ideals have degree zero.

Proof. Let us prove Item (i) first: Let $D \in \operatorname{Div}(X)$ be given by the configuration (U_i, f_i) for some open cover $\cup_{i\in I} U_i = X$. Since for all $i, j \in I$ we have $f_i f_j^{-1} \in \mathcal{O}_X(U_i \cap U_j)^\times$, setting $\mathcal{F}_i = f_i^{-1}\mathcal{O}_{U_i}$ does indeed define a sheaf $\mathcal{F}$ on X with the obvious restriction maps

such that $\mathcal{F}_{|U_i} = \mathcal{F}_i$. The sheaf $\mathcal{F}$ is obviously an $\mathcal{O}_X$-ideal. Now any other $\mathcal{O}_X$-ideal $\mathcal{G}$ with $\mathcal{G}_{|U_i} = f_i^{-1}\mathcal{O}_{U_i}$ need necessarily be equal to $\mathcal{F}$: Since both $\mathcal{F}$ and $\mathcal{G}$ are $\mathcal{O}_X$-subsheaves of $\mathcal{K}_X$, equality is a question of having the same stalk at every point of X, and this is obviously true. Taking any other configuration $(V_j, g_j)_{j\in J}$ of D does not change the induced sheaf: By hypothesis and the definition of divisors, we have for all i, j that $f_i g_j \in \mathcal{O}_X(U_i \cap V_j)^\times$. In particular, $f_{i|U_i\cap V_j}\mathcal{O}_{|U_i\cap V_j} = g_{j|U_i\cap V_j}\mathcal{O}_{|U_i\cap V_j}$ and thus the induced sheaves coincide. Hence for every divisor D on X we find a unique $\mathcal{O}_X$-ideal $\mathcal{O}_X(D)$ such that $\mathcal{O}_X(D)_{U_i} = f_i^{-1}\mathcal{O}_{U_i}$ which establishes the well-defined map ϕ. That assertion about the principal divisors and principal $\mathcal{O}_X$-ideals is evident from the construction of ϕ.

If $D \in \mathrm{Div}(X)$ with $\phi(D) = \mathcal{O}_X(D) = \mathcal{O}_X$, then by definition of ϕ, we have the equality $\mathcal{O}_X(D)_{U_i} = \mathcal{O}_{U_i}$ which is equivalent to $f_i \in \mathcal{O}_X(U_i)^\times$ for all $i \in I$. Therefore D was already the zero divisor on X and hence ϕ is injective.

The inverse map ϕ^{-1} is given by the map constructed in Lemma 3.1.23. That ϕ is a homomorphism of abelian groups is obvious, see [Liu02, 7.1.18]. This proves the first assertion.

Now we prove Item (ii): Let $D \in \mathrm{Div}(X)$. Then $D \geq 0$ if and only if D is induced by a configuration $(U_i, f_i)_{i\in I}$ with $f_i \in \mathcal{O}_X(U_i)$ for all $i \in I$. This is equivalent to $\mathcal{O}_X(U_i) \subseteq f_i^{-1}\mathcal{O}_X(U_i) = \mathcal{O}_X(D)_{|U_i}$ for all $i \in I$. Clearly, since ϕ is a group homomorphism, we have $\mathcal{O}_X(D)^{-1} = \mathcal{O}_X(-D)$. Note that by Lemma 3.1.18 $\mathcal{O}_X \leq \mathcal{O}_X(D)$ is equivalent to $\mathcal{O}_X(-D) \leq \mathcal{O}_X$ (via multiplication with $\mathcal{O}_X(D)^{-1}$ respectively $\mathcal{O}_X(D)$). This provides the second assertion. Item (iii) is due to Lemma C.4.8. Finally, consider Item (iv). That principal divisors have degree zero is Lemma 3.1.12 and then by the third assertion we can complete the proof. □

Definition 3.1.28. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal and $D \in \mathrm{Div}(X)$. Then we denote $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(D)$ by $\mathcal{F}(D)$. This is in accordance with the notation $\mathcal{O}_X(D)$ which clearly satisfies $\mathcal{O}_X(D) = \mathcal{O}_X \otimes_{\mathcal{O}_X} \mathcal{O}_X(D)$. △

Corollary 3.1.29. *The isomorphism* $\mathrm{Div}(X) \to \mathrm{InvId}(X)$ *extends to an isomorphism between* $\mathrm{CaCl}(X)$ *and* $\mathrm{ClInvId}(X)$.

Proof. Any principal divisor $D = \mathrm{div}(f)$ corresponds to $f^{-1}\mathcal{O}_X$ under the isomorphism ϕ in Proposition 3.1.27. Hence the subgroups $\mathrm{Princ}(X)$ and $\mathrm{PrincId}(X)$ are isomorphic under the isomorphism $\phi : \mathrm{Div}(X) \to \mathrm{InvId}(X)$ and hence the assertion follows. □

Remark 3.1.30. The isomorphism $\mathrm{Div}(X) \cong \mathrm{InvId}(X)$ provides a map $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ that is compatible with the map $\mathrm{InvId}(X) \to \mathrm{Pic}(X)$, see Remark 3.1.22. △

Lemma 3.1.31. *If X is a noetherian scheme without embedded points, then the homomorphisms* $\mathrm{InvId}(X) \to \mathrm{Pic}(X)$ *and* $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ *provide isomorphism* $\mathrm{ClInvId}(X) \cong \mathrm{CaCl}(X) \cong \mathrm{Pic}(X)$.

Proof. That $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ provides the isomorphism $\mathrm{CaCl}(X) \cong \mathrm{Pic}(X)$ is [Liu02, 7.1.19]. The rest of the assertion follows from Corollary 3.1.29. □

In the following lemma we collect some rather immediate relations between D and its corresponding invertible $\mathcal{O}_X$-ideal $\mathcal{O}_X(D)$.

Lemma 3.1.32. *The correspondence* $\mathrm{Div}(X) \leftrightarrow \mathrm{InvId}(X)$, $D \mapsto \mathcal{O}_X(D)$ *satisfies:*

(i) $\mathrm{Supp}(D) = \{P \in X \mid \mathcal{O}_X(D)_P \neq \mathcal{O}_{X,P}\}$,

(ii) For $f \in \mathcal{K}_X(X)^\times$ *and* $D \in \mathrm{Div}(X)$ *we have*

$$f \in \mathcal{O}_X(D)(X) \Leftrightarrow \mathrm{div}(f) + D \geq 0.$$

Proof.

(i) Let D be given by $\{(U_i, f_i)\}_{i\in I}$. Then $D_P = (f_i)_P\mathcal{O}_{X,P}$ for every i with $P \in U_i$. By Definition B.1.5, we have

$$\mathrm{Supp}(D) = \{P \in X \mid D_P \neq 1\} = \{P \in X \mid (f_i)_P \notin \mathcal{O}_{X,P}{}^\times\}$$

and by definition of $\mathcal{O}_X(D)$ we have $\mathcal{O}_X(D)_P \cong (f_i^{-1})_P\mathcal{O}_{X,P}$ which proves the first assertion.

(ii) Let D be given by $\{(U_i, f_i)\}_{i\in I}$. By definition we have $f \in \mathcal{O}_X(D)(X)$ if and only if for all $i \in I$ we have $f_{|U_i} \in \mathcal{O}_X(D)(U_i) = f_i^{-1}\mathcal{O}_X(U_i)$ since $\mathcal{O}_X(D)$ is a subsheaf of $\mathcal{K}_X$ and $f \in \mathcal{K}_X(X)$, see Lemma B.1.29. On the other hand, by definition we have that $\mathrm{div}(f) + D$ is the divisor given by $\{(U_i, f_{|U_i}f_i)\}_{i\in I}$ and this is is greater or equal to zero if and only if $f_{|U_i}f_i \in \mathcal{O}_X(U_i)$ for all $i \in I$. But this is equivalent to $f_{|U_i} \in f_i^{-1}\mathcal{O}_X(U_i)$ and thus the assertion follows.

□

3.2 Restricting Divisors

We will now turn to our setup in which we want to analyse how we can transport divisors between the appearing schemes. It turns out that there is a reasonable way of pulling back divisors along morphisms $f : Y \to X$ for which the pullback of meromorphic functions is defined, see Definition 3.1.3. We will see that this is the case for the Y in question. Moreover, this notion of pulling back divisors D is compatible with the notion of pulling back the corresponding invertible sheaf $\mathcal{O}_X(D)$.

Remark 3.2.1. Let $f : Y \to X$ be a morphism of schemes. Then f comes along with a morphism of sheaves $\mathcal{O}_X \to f_*\mathcal{O}_Y$ called the pullback map of regular functions along f. This datum of a pullback map along f (as a morphism of presheaves) is equivalent to the morphism of sheaves $f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$. Hence we denote both of them by $f^\#$. All of this follows from the fact that there is a bijection

$$\mathrm{Hom}_{\mathrm{Sh}(Y)}(f^{-1}\mathcal{G}, \mathcal{F}) \leftrightarrow \mathrm{Hom}_{\mathrm{PreSh}(X)}(\mathcal{G}, f_*\mathcal{F})$$

functorial in the sheaf $\mathcal{F}$ on Y and the presheaf $\mathcal{G}$ on X, see [GW10, 2.27]. △

We start with a corollary of Proposition B.1.44.

Corollary 3.2.2. *Let $f : Y \to X$ be a morphism of schemes. We have a natural map $\phi : f_*\mathcal{K}_Y^\times/f_*\mathcal{O}_Y^\times \longrightarrow f_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times)$ with $\phi(U)$ sending*

$$(U_i, s_i \cdot \mathcal{O}_Y^\times(f^{-1}(U_i))) \quad \text{to} \quad (f^{-1}(U_i), s_i \cdot \mathcal{O}_Y^\times(f^{-1}(U_i)))$$

where $s_i \in \mathcal{K}_Y^\times(f^{-1}(U_i))$ and $\{U_i \mid i \in I\}$ forms an open cover of the open subset $U \subseteq X$.

Proof. The assertion follows from Proposition B.1.44 where we replace $\mathcal{O}_X$ by $\mathcal{O}_X^\times$ and regard both $f_*\mathcal{O}_Y^\times$ and $f_*\mathcal{K}_Y^\times$ as sheaves of multiplicative abelian groups on X. □

Proposition 3.2.3. *Let $f : Y \to X$ be a morphism of schemes. Whenever the morphism $f^\# : \mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\varphi : \mathcal{K}_X \to f_*\mathcal{K}_Y$, we obtain a group homomorphism $f^* : \mathrm{Div}(X) \to \mathrm{Div}(Y)$ sending*

$$\left(U_i, \frac{a_i}{b_i} \cdot \mathcal{O}_X^\times(U_i)\right) \quad \text{to} \quad \left(f^{-1}(U_i), \frac{f^\#(U_i)(a_i)}{f^\#(U_i)(b_i)} \cdot \mathcal{O}_Y^\times(f^{-1}(U_i))\right).$$

Moreover, f^* satisfies the following properties:

(i) $\mathcal{O}_Y(f^*(D)) \cong f^*\mathcal{O}_X(D)$ *for all* $D \in \mathrm{Div}(X)$,

(ii) If $D \geq 0$ *in* $\mathrm{Div}(X)$, *then* $(f^*D) \geq 0$ *in* $\mathrm{Div}(Y)$.

.

Proof. By assumption we obtain a commutative diagram

$$\begin{array}{ccccccc} f_*\mathcal{O}_Y^\times & \hookrightarrow & f_*\mathcal{K}_Y^\times & \twoheadrightarrow & f_*\mathcal{K}_Y^\times/f_*\mathcal{O}_Y^\times & \xrightarrow{\phi} & f_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times) \\ {\scriptstyle f^\#}\uparrow & & {\scriptstyle \varphi}\uparrow & & & & \\ \mathcal{O}_X^\times & \hookrightarrow & \mathcal{K}_X^\times & & & & \end{array}$$

where ϕ is the natural morphism of Corollary 3.2.2. Then φ together with ϕ induce a morphism of sheaves

$$\mathcal{K}_X^\times/\mathcal{O}_X^\times \xrightarrow{\varphi} f_*\mathcal{K}_Y^\times/f_*\mathcal{O}_Y^\times \xrightarrow{\phi} f_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times). \tag{2:1}$$

Taking global sections provides a morphism of multiplicative groups

$$\mathrm{Div}(X) = H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) \to H^0\left(Y, f_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times)\right) = H^0\left(Y, \mathcal{K}_Y^\times/\mathcal{O}_Y^\times\right) = \mathrm{Div}(Y)$$

which we denote by f^*. Let $X = \bigcup_{i\in I} U_i$ be an open cover of X. By the above and Corollary 3.2.2, f^* works as follows:

$$\begin{array}{ccccc} (\mathcal{K}_X^\times/\mathcal{O}_X^\times)(X) & \to & (f_*\mathcal{K}_Y^\times/f_*\mathcal{O}_Y^\times)(X) & \to & (f_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times))(X) \\ (U_i, s_i \cdot \mathcal{O}_X^\times(U_i)) & \mapsto & (U_i, \varphi(U_i)(s_i) \cdot \mathcal{O}_Y^\times(f^{-1}(U_i))) & \mapsto & (f^{-1}(U_i), \varphi(U_i)(s_i) \cdot \mathcal{O}_Y^\times(f^{-1}(U_i))) \end{array} \tag{2:2}$$

By Remark 3.1.2, the sections of $\mathcal{K}_X^\times$ over some open $U \subseteq X$ are locally on U_i (with U_i forming an open cover of U) given by fractions of regular elements of $\mathcal{O}_X(U_i)$. Now since $\varphi : \mathcal{K}_X^\times \to f_*\mathcal{K}_Y^\times$ is the extension of $f^\# : \mathcal{O}_X^\times \to f_*\mathcal{O}_Y^\times$, we therefore have

$$\varphi(U_i)\left(\frac{a_i}{b_i}\right) = \frac{f^\#(U_i)(a_i)}{f^\#(U_i)(b_i)} \tag{2:3}$$

where both a_i and b_i are regular elements of $\mathcal{O}_X(U_i)$. Now combining Eq. (2:2) and Eq. (2:3) provides the main assertion.

The proof of (i) simplifies a lot if we assume X and Y to be projective over an affine base or affine itself since in both cases, by Corollaries D.1.3 and D.1.4, respectively, we find suitable affine open neighborhoods for a given finite set. The proof for the general case will be given in Remark B.5.8.

Let us now prove (i) in the above setting. Consider $D \in \mathrm{Div}(X)$ given by a configuration $\{(U_i, b_i/a_i)\}_{i\in I}$ with $a_i, b_i \in \mathcal{O}_X(U_i)$. Note that by Lemma B.5.7, we may choose an affine cover of X which is a refinement of the cover $\{U_i \mid i \in I\}$. Then taking the restrictions of a_i/b_i to the smaller affine opens as the local equations of D, we may without loss of generality assume that the cover $\{U_i \mid i \in I\}$ is an affine cover. We have $\mathcal{O}_X(D)_{|U_i} = (a_i/b_i)\mathcal{O}_{U_i}$. Now fix some U_i along with its open immersion $j : U_i \to X$ for which then $j^*\mathcal{O}_X(D) = \mathcal{O}_X(D)_{|U_i}$ holds. Then set $V_i = f^{-1}(U_i)$. By the simplifying assumption on Y, we may use Corollary D.1.4 or Corollary D.1.3 to find for every $P \in V_i$ an affine open subset $V_{i,P}$ such that $P \in V_{i,P} \subseteq V_i$ and thus $f(V_{i,P}) \subseteq U_i$. Now we can use Lemma 3.2.27 which provides

$$(f^*\mathcal{O}_X(D))_{|V_{i,P}} \cong (\mathcal{O}_X(D)(U_i) \otimes_{\mathcal{O}_X(U_i)} \mathcal{O}_Y(V_{i,P}))^\sim.$$

But since $\mathcal{O}_X(D)_{|U_i} = (a_i/b_i)\mathcal{O}_{U_i}$, we have

$$\begin{aligned}\mathcal{O}_X(D)(U_i) \otimes_{\mathcal{O}_X(U_i)} \mathcal{O}_Y(V_{i,P}) &\cong (a_i/b_i)\mathcal{O}_X(U_i) \otimes_{\mathcal{O}_X(U_i)} \mathcal{O}_Y(V_{i,P}) \\ &\cong \mathcal{O}_X(U_i) \otimes_{\mathcal{O}_X(U_i)} f^{\#}(V_{i,P})(a_i/b_i)\mathcal{O}_Y(V_{i,P}) \\ &= f^{\#}(V_{i,P})(a_i/b_i)\mathcal{O}_Y(V_{i,P}) \\ &= \frac{f^{\#}(V_{i,P})(a_i)}{f^{\#}(V_{i,P})(b_i)}\mathcal{O}_Y(V_{i,P})\end{aligned}$$

providing

$$(f^*\mathcal{O}_X(D))_{|V_{i,P}} \cong \frac{f^{\#}(V_{i,P})(a_i)}{f^{\#}(V_{i,P})(b_i)}\mathcal{O}_{V_{i,P}}.$$

The invertible sheaf $f^*\mathcal{O}_X(D)$ on Y defined by the above equation defines a divisor E on Y, see Proposition 3.1.27, via the configuration

$$\left(V_{i,P}, \frac{f^{\#}(V_{i,P})(a_i)}{f^{\#}(V_{i,P})(b_i)}\right)_{i\in I, P\in V_i}.$$

Now since $f^{\#}$ is a morphism of sheaves on Y, we have $f^{\#}(V_i)(a_i)_{|V_{i,P}} = f^{\#}(V_{i,P})(a_i)$ and similarly for b_i. This provides $E = f^*D$.

Let us now prove (ii). Let $D \in \mathrm{Div}(X)$ be effective, i.e. $D \geq 0$. Hence we may assume that it is given by $\{(U_i, a_i)\}_{i\in I}$ with $a_i \in \mathcal{O}_X(U_i)$. By assumption, the following diagram of morphisms of sheaves on X is commutative:

$$\begin{array}{ccc}\mathcal{O}_X^\times & \xrightarrow{f^{\#}} & f_*\mathcal{O}_Y^\times \\ \downarrow & & \downarrow \\ \mathcal{K}_X^\times & \xrightarrow{\varphi} & f_*\mathcal{K}_Y^\times\end{array}$$

By the main assertion, $f^*(D)$ is given by $\{(f^{-1}(U_i), \varphi(U_i)(a_i)\}_{i\in I}$. The commutativity of the above diagram now implies that $\varphi(U_i)(a_i) \in (f_*\mathcal{O}_Y^\times)(U_i) = \mathcal{O}_Y(f^{-1}(U_i))^\times$ and thus $f^*(D) \geq 0$ in $\mathrm{Div}(Y)$. □

Corollary 3.2.4. *Let the situation be as in Proposition 3.2.3. Then the pullback of principal divisors are principal and thus the restriction of the group homomorphism* $f^* : \mathrm{Div}(X) \to \mathrm{Div}(Y)$ *to the subgroup of principal divisors* $\mathrm{Princ}(X)$ *on* X *yields a group homomorphism*

$$f^*{}_{|\mathrm{Princ}(X)} : \mathrm{Princ}(X) \to \mathrm{Princ}(Y).$$

In particular, if $D \sim E$ *in* $\mathrm{Div}(X)$*, then* $f^*(D) \sim f^*(E)$ *in* $\mathrm{Div}(Y)$*.*

Proof. Let $D = \mathrm{div}(g)$ with $g \in \mathcal{K}_X(X)^\times$ be a principal divisor. By Proposition 3.2.3, the pullback $f^*(D)$ of D is given by the configuration $(Y, \varphi(X)(g))$ where $\varphi : \mathcal{K}_X \to f_*\mathcal{K}_Y$ is the extension of $\mathcal{O}_X \to f_*\mathcal{O}_Y$. In particular, $\varphi(X)(g) \in \mathcal{K}_Y(Y)^\times$ and hence $f^*(D)$ is principal.

The particular part follows from the fact that f^* is a group homomorphism, see Proposition 3.2.3, and the first assertion. Indeed, let $D - E = \mathrm{div}_X(g)$ for some $g \in \mathcal{K}_X(X)^\times$. Then the assertion follows from

$$f^*(D) - f^*(E) = f^*(D - E) = f^*(\mathrm{div}_X(g)) = \mathrm{div}_Y(\varphi(X)(g)).$$ □

We might summarise the above insight as follows: Whenever the pullback of regular functions along a morphism extends to quotients of regular functions, then pulling back

the local equations for a divisor yields a well-defined notion of *pullback of a divisor*.

Definition 3.2.5. Let $f : Y \hookrightarrow X$ be an injective morphism of schemes. Whenever the morphism $\mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$, we say that the **restriction of divisors from X to Y along f is defined**. In this case we may also just say that the **restriction of divisors from X to Y** or that the **restriction of divisors along f is defined**.

Sometimes we will also call the restriction of divisors more generally the pullback of divisors. We also denote the restricted divisor as $D_{|Y} = f^*D$.

Note that the restriction of divisors along f is defined if and only if the pullback of meromorphic functions is defined, see Definition 3.1.3 and Remark 3.1.4. △

Remark 3.2.6. Let (X, π) be a cover of $\mathbb{P}^1_k$. By Definition 2.2.9, we have that the pole divisor $(x)_{\mathbb{P}^1_k,\infty}$ on $\mathbb{P}^1_k$ (which together with the identity morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ is a cover of $\mathbb{P}^1_k$) is given by the configuration

$$\{(U_0, 1), (U_\infty, x^{-1})\}.$$

Thus by Proposition 3.2.3, we know that $\pi^*(x)_{\mathbb{P}^1_k,\infty}$ is given by the configuration

$$\{(V_0, 1), (V_\infty, x^{-1})\}$$

and thus equals the pole divisor $(x)_\infty$ of x on X. Since $\pi^* : \mathrm{Div}(\mathbb{P}^1_k) \to \mathrm{Div}(X)$ is a group homomorphism, this also provides $r(x)_\infty = \pi^*(r(x)_{\mathbb{P}^1_k,\infty})$. △

We will use the restriction of divisors respectively their corresponding invertible sheaves (and even more general $\mathcal{O}_X$-ideals) for several schemes Y which will come with an injective morphism of schemes $Y \to X$. Note that Y need not be a subscheme of X.

But first we give sufficient conditions such that $\mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$.

Lemma 3.2.7 ([Liu02], 7.1.33)**.** *Let $f : Y \to X$ be a morphism of schemes. We suppose that one of the following hypotheses is verified:*

1. *f is flat;*
2. *Y is reduced, having only a finite number of irreducible components, and every of these dominates one of X.*

Then the canonical morphism $\mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$.

Remark 3.2.8. In [Sta18, Tag 02OU] this is proved for more general cases and we list two of them here where the latter is an implication of the former:

1. X is locally Noetherian, and any associated point of X maps to a generic point of an irreducible component of Y,
2. X is locally Noetherian, has no embedded points and any generic point of an irreducible component of X maps to the generic point of an irreducible component of Y. △

Proposition 3.2.9. *Let $f : Y \to Z$ and $g : Z \to X$ be two morphisms of schemes. If both $\mathcal{O}_Z \to f_*\mathcal{O}_Y$ and $\mathcal{O}_X \to g_*\mathcal{O}_Z$ extend to $\mathcal{K}_Z \to f_*\mathcal{K}_Y$ respectively $\mathcal{K}_X \to g_*\mathcal{K}_Z$, then $\mathcal{O}_X \to (g \circ f)_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to (g \circ f)_*\mathcal{K}_Y$. Moreover, $\mathcal{O}_X \to (g \circ f)_*\mathcal{O}_Y$ factors through $g_*\mathcal{O}_Z$ and $\mathcal{K}_X \to (g \circ f)_*\mathcal{K}_Y$ factors through $g_*\mathcal{K}_Z$.*

Proof. The natural morphisms $\mathcal{O}_Z \to f_*\mathcal{O}_Y$ and $\mathcal{O}_X \to g_*\mathcal{O}_Z$ provide, via pushforward of the former by g, the morphism

$$\mathcal{O}_X \to g_*\mathcal{O}_Z \to g_*(f_*\mathcal{O}_Y) = (g \circ f)_*\mathcal{O}_Y$$

By assumption, we have the morphisms $\mathcal{K}_Z \to f_*\mathcal{K}_Y$ and $\mathcal{K}_X \to g_*\mathcal{K}_Z$. Hence we obtain a morphism $\mathcal{K}_X \to g_*\mathcal{K}_Z \to g_*(f_*\mathcal{K}_Y) = (g \circ f)_*\mathcal{K}_Y$. Using that the morphisms of the sheaf of stalks of meromorphic functions are the extension of the morphisms of structure sheaves, we obtain the commutative diagram

$$\begin{array}{ccccc} \mathcal{O}_X & \longrightarrow & g_*\mathcal{O}_Z & \longrightarrow & (g \circ f)_*\mathcal{O}_Y \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{K}_X & \longrightarrow & g_*\mathcal{K}_Z & \longrightarrow & (g \circ f)_*\mathcal{K}_Y \end{array}$$

which shows that $\mathcal{O}_X \to (g \circ f)_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to (g \circ f)_*\mathcal{K}_Y$. It also shows the last part of the assertion. □

Definition 3.2.10. Let X be a scheme. We call an open subscheme $U \subseteq X$ **schematically dense in** X if $\mathrm{Ass}(\mathcal{O}_X) \subseteq U$. △

Note Lemma B.2.5 for equivalent descriptions of schematically dense open subsets.

Lemma 3.2.11. *Let X be a locally noetherian scheme. Let $V \subseteq X$ be a schematically dense open subset with open immersion $i : V \hookrightarrow X$. Then $\mathcal{O}_X \hookrightarrow i_*\mathcal{O}_V$ extends to $\mathcal{K}_X \to i_*\mathcal{K}_V$ (which is an isomorphism) and hence the restriction of divisors from X to V is defined.*

Proof. This is Lemma B.2.6 and [Liu02, 7.1.15]. □

Remark 3.2.12. Proposition 3.2.3 shows that $\mathrm{Div}(X) \to \mathrm{Div}(V)$ locally works (on numerator and denominator) as the restriction $i^\#(U) : \mathcal{O}_X(U) \to \mathcal{O}_X(U \cap V)$ for $U \subseteq X$ open. Hence, if $(U_i, f_i/g_i)$ with $f_i, g_i \in \mathcal{O}_X(U_i)$ regular is a configuration of a divisor D on X, then $i^*(D)$ is given by the configuration

$$\left(U_i \cap V, \frac{i^\#(U_i)(f_i)}{i^\#(U_i)(g_i)}\right) = \left(U_i \cap V, \frac{(f_i)_{|U_i \cap V}}{(g_i)_{|U_i \cap V}}\right). \qquad \triangle$$

Lemma 3.2.13. *Let X be a scheme and Y an irreducible component of X with closed immersion $\tau : Y \hookrightarrow X$. Moreover, assume Y to be reduced. Then $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to \tau_*\mathcal{K}_Y$ and hence the restriction of divisors from X to Y is defined.*

Proof. Since Y is an irreducible component of X, it dominates (via τ) an irreducible component of X and is reduced. Hence the assertion follows from Lemma 3.2.7. □

Remark 3.2.14. Proposition 3.2.3 shows that $\mathrm{Div}(X) \to \mathrm{Div}(Y)$ locally works (on numerator and denominator) as the ring homomorphism

$$\tau^\#(U) : \mathcal{O}_X(U) \to \mathcal{O}_Y(\tau^{-1}(U))) = \mathcal{O}_X(U)/J$$

for $U \subseteq X$ open and $J = \mathcal{J}(U)$ where $\mathcal{J}$ is the sheaf of $\mathcal{O}_X$-ideals that cuts out Y in X. We also see that $\tau^\#(U)$ sends regular elements to regular elements since J is a minimal prime ideal of $\mathcal{O}_X(U)$ and thus only zero-divisors get send to zero-divisors, see Remark 3.2.8. If Y was only a closed subscheme of X, then locally J need not be a minimal prime ideal and hence regular elements may be sent to zero-divisors. △

Let X be a reduced scheme and $X_1, \ldots, X_m$ all of its irreducible components. By Y we denote the disjoint union of the X_i as in Definition B.3.1. Then we have a natural surjective morphism of schemes $\tau : Y \to X$. Now we can use Lemma 3.2.13 for all irreducible components and apply this to Y and τ.

Corollary 3.2.15. *Let X and Y be as above. Then $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to \tau_*\mathcal{K}_Y$ and hence the restriction of divisors from X to Y is defined.*

Proof. Obviously, as in Lemma 3.2.13, the second hypothesis of Lemma 3.2.7 is satisfied and hence the assertion follows. □

Remark 3.2.16. Proposition 3.2.3 shows that $\mathrm{Div}(X) \to \mathrm{Div}(Y)$ works locally, that is on every open $U \subseteq X$ (on numerator and denominator), as the diagonal map $\tau^\#(U)$ constituted of the ring homomorphisms

$$\tau_i^\#(U) : \mathcal{O}_X(U) \to \mathcal{O}_{X_i}(\tau_i^{-1}(U))) = \mathcal{O}_X(U)/J_i$$

for $J_i = \mathcal{J}_i(U)$ where $\mathcal{J}_i$ is the sheaf of $\mathcal{O}_X$-ideals that cuts out X_i in X. That is, locally it works as

$$\tau^\#(U) : \mathcal{O}_X(U) \hookrightarrow \bigoplus_{i=1}^m \mathcal{O}_{X_i}(\tau_i^{-1}(U))) = \bigoplus_{i=1}^m \mathcal{O}_X(U)/J_i$$

which maps a to $(a+J_1, \ldots, a+J_m)$. Note that $\tau^\#(U)$ is injective since X is reduced. △

Proposition 3.2.17. *Let X be a cover of $\mathbb{P}^1_k$. Then we have $(\mu_a)_*\mathcal{K}_S = \mathcal{K}_{V_\infty}$ and $\mu_*\mathcal{K}_S \cong \mathcal{K}_X$.*

Proof. The first assertion follows from the fact that $\mathrm{Frac}(T^{-1}R_\infty) = \mathrm{Frac}(R_\infty)$. The second from

$$\mu_*\mathcal{K}_S = (i_\infty \circ \mu_a)_*\mathcal{K}_S = (i_\infty)_*((\mu_a)_*\mathcal{K}_S) = (i_\infty)_*\mathcal{K}_{V_\infty} \cong \mathcal{K}_X$$

where the last isomorphism is due to Lemma B.2.6 and the last equality used the first assertion. □

Replacing X by X_i and S by S_i we obtain:

Corollary 3.2.18. *Let X be a cover of $\mathbb{P}^1_k$. Then we have $(\mu_{a,i})_*\mathcal{K}_{S_i} = \mathcal{K}_{V_{i,\infty}}$ and $(\mu_i)_*\mathcal{K}_{S_i} \cong \mathcal{K}_{X_i}$.*

Lemma 3.2.19. *The restriction of divisors from V_∞ to S and from $V_{i,\infty}$ to S_i is defined.*

Proof. Since both morphisms are given by localisation homomorphisms, they are flat, see [Sta18, Tag 00HT] and [Liu02, 4.3.3]. Thus the assertion follows from Lemma 3.2.7. □

Remark 3.2.20. Proposition 3.2.3 shows that μ^* locally, that is on every open $U \subseteq X$ (on numerator and denominator), works as

$$\mu^\#(U) : \mathcal{O}_X(U) \longrightarrow \mathcal{O}_S(\mu^{-1}(U)).$$

Note that by construction of S, we have $\mu^\#(V_\infty) : R_\infty \to T^{-1}R_\infty = \mathcal{O}_S$ is the localisation map. Moreover, if $U = D(h)$ with $h \in R_\infty$ is basic open, then

$$\mu^\#(U) : (R_\infty)_h \to (T^{-1}R_\infty)_h = (\mathcal{O}_S)_{\mu^\#(V_\infty)(h)}.$$ △

Proposition 3.2.21. *Let D be a divisor on X such that $D_{|S} = 0$ is the zero divisor on S. Then there is some open subset $W \subseteq V_\infty$ such that $\mu(S) \subseteq W$ with $D_{|W} = 0$.*

Proof. Since the restriction of divisors is transitive, see Corollary 3.2.23, any divisor that restricts to zero on S restricts to a divisor D on V_∞ whose restriction to S is the zero divisor. If $D = 0$, then we are done. Thus let D on V_∞ be given by a configuration $(U_i, f_i)_{i\in I}$. Let $P_1, \ldots, P_r$ denote the points of V_∞ that correspond to those in S. By

Lemma B.5.17, there is an affine open neighborhood $D(g_i)$ of P_i in V_∞ given by a regular element $g_i \in R_\infty$. Using these we may assume that D on V_∞ is given by open subsets U_j for which those with $P_i \in U_i$ will be of the form $D(g_i)$. Moreover, then $f_i = a_i/g_i^{r_i}$. Now the restriction of D to S is given by

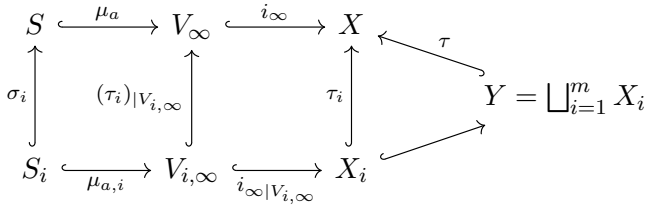
$$(\mu^{-1}(D(g_i)), \mu^{\#}(D(g_i))(f_i))$$

where $\mu^{\#}(D(g_i)) : (R_\infty)_{g_i} \to (T^{-1}R_\infty)_{g_i}$ is the localisation homomorphism, which is injective since g_i is regular. By assumption, D restricts to the zero divisor and thus

$$\mu^{\#}(D(g_i))(f_i) = \frac{a_i/g_i^{r_i}}{1} = \frac{a_i}{g_i^{r_i}}$$

is a unit in $(T^{-1}R_\infty)_{g_i}$. Hence a_i is of the form $p_i g_i^{\ell_i}$ for $p_i \in T$ and $\ell_i \in \mathbb{Z}$. But this means that the restriction of f_i to $D(g_i) \cap D(p_i) = D(g_i p_i)$ is a unit. Note that since $p_i \in T$, we have $x^{-1} \nmid p_i$ and thus $D(p_i)$ contains the point P_i. Thus the finite union of the $D(g_i p_i)$ provide an open subset $W \subseteq V_\infty$ which contains $\mu(S)$ such that D restricts to zero on W. □

Proposition 3.2.22. *Let X be a cover of $\mathbb{P}^1_k$. The following diagram of morphisms of schemes commutes. Moreover, the pullback of divisors along every one of the appearing morphisms is defined.*



Proof. Let R be a ring, P an ideal of R and $T \subset R$ a multiplicatively closed subset. Then, after identifying $T^{-1}(R/P)$ with $T^{-1}R/T^{-1}P$ the following diagram is commutative:

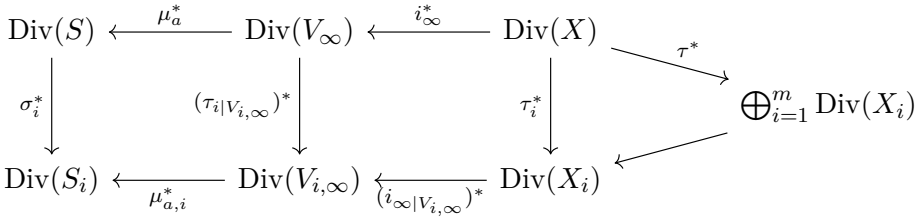
$$\begin{array}{ccc} T^{-1}R & \longleftarrow & R \\ \downarrow & & \downarrow \\ T^{-1}(R/P) & \longleftarrow & R/P. \end{array}$$

This provides the commutativity of the left square. The commutativity of the right square is evident as well as the commutativity of the triangle on the right hand side. That the restriction of divisors along i_∞ and $i_{\infty|V_{i,\infty}}$ are defined is Lemma 3.2.11. The same follows for the pullback along τ_i and $(\tau_i)_{|V_{i,\infty}}$ from Lemma 3.2.13. Since both S and S_i are finite schemes and S_i embeds as a closed subscheme, we see that every irreducible component of S_i (each of its points) dominates an irreducible component of S (one of its points). Since X is reduced, S_i is reduced and thus the restriction of divisors along σ_i is defined by Lemma 3.2.7. Finally, restriction of divisors from X to Y is defined by Corollary 3.2.15. □

Now we can conclude that restricting divisors from X to the various schemes involved in our context behaves very well in the following sense.

Corollary 3.2.23. *The following diagram of groups and group homomorphisms is com-*

mutative.



The map $\bigoplus_{i=1}^m \mathrm{Div}(X_i) \to \mathrm{Div}(X_i)$ *is simply the projection onto the* i*-th summand.*

Proof. The existence of the diagram with its maps follows from Proposition 3.2.22. That it is commutative follows from Proposition 3.2.9. □

Definition 3.2.24. For the readability we will denote the pullback/restriction of divisors naturally with the restriction symbol. For clarity, we list some examples of the notations explicitly below:

$D \in \mathrm{Div}(X)$	$D_{\|V_\infty}$	$:=$	$i_\infty^*(D)$
	$D_{\|V_0}$	$:=$	$i_0^*(D)$
	$D_{\|X_i}$	$:=$	$\tau_i^*(D)$
	$D_{\|V_{i,\infty}}$	$:=$	$((i_\infty)_{\|V_{i,\infty}} \circ \tau_i)^*(D)$
		$=$	$((\tau_i)_{\|V_{i,\infty}} \circ i_\infty)^*(D)$
$D \in \mathrm{Div}(X_i)$	$D_{\|V_{i,\infty}}$	$:=$	$(i_\infty)^*_{\|V_{i,\infty}}(D)$
$D \in \mathrm{Div}(V_\infty)$	$D_{\|V_{i,\infty}}$	$:=$	$(\tau_i)^*_{\|V_{i,\infty}}(D)$
	$D_{\|S_i}$	$:=$	$(\mu_{a,i} \circ (\tau_i)_{\|V_{i,\infty}})^*(D)$
		$=$	$(\sigma_i \circ \mu_a)^*(D)$

△

3.2.1 Restricting $\mathcal{O}_X$-submodules of $\mathcal{K}_X$

Let $f : Y \hookrightarrow X$ be a morphism of schemes. Whenever the restriction of divisors of X to Y (along f) is defined, we have seen in Proposition 3.2.3 that for any divisor D on X its restriction to Y satisfies $\mathcal{O}_Y(D_{|Y}) \cong f^*\mathcal{O}_X(D)$. Thus, if we define the restriction of an $\mathcal{O}_X$-module $\mathcal{F}$ to Y as the pullback $f^*\mathcal{F}$ along f, then this notion of restricting sheaves will be compatible with that of the restriction of divisors.

Definition 3.2.25. Let $f : Y \hookrightarrow X$ be an injective morphism of schemes. For any $\mathcal{O}_X$-module $\mathcal{F}$ set $\mathcal{F}_{|Y} := f^*\mathcal{F}$ and call it the **restriction of $\mathcal{F}$ to Y along f** or simply **restriction of $\mathcal{F}$ to Y** if the context already admits what f is. △

Remark 3.2.26. As mentioned above, if D is a divisor on X and the restriction of divisors along f is defined, we have

$$\mathcal{O}_X(D)_{|Y} \cong f^*\mathcal{O}_X(D) \cong \mathcal{O}_Y(f^*D) \cong \mathcal{O}_Y(D_{|Y}).$$ △

In the case of affine schemes and quasi-coherent $\mathcal{O}_X$-modules the pullback operation is very easily expressed using the extension of scalars.

Lemma 3.2.27 ([Liu02], 5.1.14 (b))**.** *Let $f : Y \to X$ be a morphism of schemes. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Let $U \subseteq Y$ be an affine open subset of Y such that $f(U) \subseteq V$ for some affine open $V \subseteq X$. Then*

$$(f^*\mathcal{F})_{|U} \cong (\mathcal{F}(V) \otimes_{\mathcal{O}_X(V)} \mathcal{O}_Y(U))^\sim.$$

In particular, $f^*\mathcal{F}$ is quasi-coherent.

If $f : Y \to X$ is an open immersion of an affine open Y into any X and $\mathcal{F}$ is a quasi-coherent $\mathcal{O}_X$-module, then we obviously have $f^*\mathcal{F} = f^{-1}\mathcal{F} = \mathcal{F}(Y)^\sim$.

This together with the property that "$(f \circ g)^* \cong g^* \circ f^*$" holds for the pullback functor of sheaves on locally ringed spaces, see [Sta18, Tag 0097], yields a very concrete description of what the restriction to S is.

Proposition 3.2.28. *Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Then*

$$\mathcal{F}_{|S} = (T^{-1}\mathcal{F}(V_\infty))^\sim = (\mathcal{F}(V_\infty) \otimes_{R_\infty} \mathcal{O}_S)^\sim.$$

In particular, $\mathcal{F}_{|S}(S) = T^{-1}\mathcal{F}(V_\infty)$ and $(\mathcal{F}_{|S})_P = \mathcal{F}_P$. Moreover, if $\mathcal{F} \leq \mathcal{K}_X$, then $\mathcal{F}_{|S}$ defines a unique $\mathcal{O}_S$-ideal which we also denote by $\mathcal{F}_{|S}$. If $\mathcal{F}_P$ is additionally invertible for all $P \in S$, then $\mathcal{F}_{|S}$ is free of rank one such that $\mathcal{F}_{|S}(S) = f\mathcal{O}_S$ with $f \in \operatorname{Frac}(\mathcal{O}_S)$.

Proof. By definition, we have $\mathcal{F}_{|S} = \mu^*\mathcal{F} = (i_\infty \circ \mu_a)^*\mathcal{F}$ and now applying [Sta18, Tag 0097] yields $(i_\infty \circ \mu_a)^*\mathcal{F} = \mu_a^*(i_\infty^*\mathcal{F})$ where the latter is equal to $\mu_a^*(\mathcal{F}(V_\infty)^\sim)$ by what we have said above. Since the ring homomorphism corresponding to $\mu_a : S \to V_\infty$ is the localisation homomorphism $R_\infty \to T^{-1}R_\infty = \mathcal{O}_S$, applying Lemma 3.2.27 with $U = S$ and $V = V_\infty$ finally yields

$$\mathcal{F}_{|S} = \mu_a^*(\mathcal{F}(V_\infty)^\sim) \cong (\mathcal{F}(V_\infty) \otimes_{R_\infty} T^{-1}R_\infty)^\sim \cong (T^{-1}\mathcal{F}(V_\infty))^\sim.$$

The particular part now follows by taking global sections and the fact that $\mathcal{F}_{|S}$ is the quasi-coherent $\mathcal{O}_S$-module given by $T^{-1}\mathcal{F}(V_\infty)$. Note that for $P \in S$ we have $P \cap T = \emptyset$ and thus $T \subseteq (R_\infty \setminus P)$ which provides $(T^{-1}\mathcal{F}(V_\infty))_P = \mathcal{F}(V_\infty)_P = \mathcal{F}_P$. The last assertion follows from the fact that

$$\mathcal{F}_{|S}(S) \cong T^{-1}\mathcal{F}(V_\infty) \subseteq T^{-1}\mathcal{K}_X(V_\infty) = T^{-1}\operatorname{Frac}(R_\infty) = \operatorname{Frac}(T^{-1}R_\infty) = \operatorname{Frac}(\mathcal{O}_S),$$

together with $\mathcal{F}_{|S} = (\mathcal{F}_{|S}(S))^\sim$ and the proof of Lemma C.4.10 telling us that $(\mathcal{F}_{|S}(S))^\sim \leq \mathcal{K}_S$. An alternative of proving it this way is to use the correspondence in Lemma C.4.10, the fact that $\mathcal{F}_{|S} \cong (\mathcal{F}_{|S}(S))^\sim = (T^{-1}\mathcal{F}(V_\infty))^\sim$ and that the localisation $T^{-1}M$ of an R-ideal M is an $T^{-1}R$-ideal, see Lemma C.1.7.

If $\mathcal{F}_P$ is invertible over $\mathcal{O}_{X,P}$ for all $P \in S$, then $\mathcal{F}_{|S}(S)$ is an invertible $\mathcal{O}_S$-ideal. Now since S is finite, $\mathcal{O}_S$ is a semi-local ring and therefore Lemma B.4.6 provides that every invertible ideal is principle. This completes the proof. □

Lemma 3.2.29. *Let $\mathcal{F}$ and $\mathcal{G}$ be two $\mathcal{O}_X$-ideals on a cover X of $\mathbb{P}^1_k$. Then $\mathcal{F} = \mathcal{G}$ if and only if $\mathcal{F}(V_0) = \mathcal{G}(V_0)$ and $\mathcal{F}(S) = \mathcal{G}(S)$.*

Proof. Note that by definition, both $\mathcal{F}$ and $\mathcal{G}$ are subsheaves of $\mathcal{K}_X$. Hence by Corollary B.1.30, we have $\mathcal{F} = \mathcal{G}$ as subsheaves of $\mathcal{K}_X$ if and only if $\mathcal{F}_P = \mathcal{G}_P$ as subsets of $\mathcal{K}_{X,P}$. Now $\mathcal{F}(V_0) = \mathcal{G}(V_0)$ implies $\mathcal{F}_P = \mathcal{G}_P$ for all $P \in V_0$ and $\mathcal{F}(S) = \mathcal{G}(S)$ implies $\mathcal{F}_P = \mathcal{G}_P$ for all $P \in S$ and hence we have $\mathcal{F}_P = \mathcal{G}_P$ for all $P \in X$. The other implication is trivial. □

Lemma 3.2.30. *Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Then $\mathcal{F}_{|X_i}$ is quasi-coherent with*

$$\mathcal{F}_{|X_i}(V_{i,0}) \cong \mathcal{F}(V_0) \otimes_{R_0} R_0/P_{i,0} = \mathcal{F}(V_0)/P_{i,0}\mathcal{F}(V_0).$$

Proof. This follows instantly using Lemma 3.2.27 with $V = V_0$ and $U = V_{i,0}$ and that both V_0 and $V_{i,0}$ are affine. □

Remark 3.2.31. In the case of $\mathcal{F}$ being an $\mathcal{O}_X$-subsheaf of $\mathcal{K}_X$ this resembles the construction of the restriction of divisors since it uses the morphism $\mathcal{K}_X \to f_*\mathcal{K}_Y$. △

Chapter 4

Global Sections and π-invariants

In this chapter we continue working with $\mathcal{O}_X$-ideals on covers of $\mathbb{P}^1_k$. We will analyse their global sections (which can be thought of generalised Riemann-Roch spaces), show how they can be represented using polynomial matrices and introduce their so called π-invariants. The insights we obtain in this chapter do have their own value, but we will definitely benefit from them in our approach to provide algorithms to compute in the Picard group. First and foremost, the bounds of the π-invariants will provide that we can represent the arithmetic objects by matrices with degree bounded by the invariant c_X.

The chapter is organised as follows: In Section 4.1 we introduce the notion of generalised vector bundles which are generalisations of $\mathcal{O}_X$-ideals to higher rank. These will essentially be those $\mathcal{O}_X$-modules on a cover X of $\mathbb{P}^1_k$ whose sections over V_0 and V_∞ are free over $k[x]$ respectively $k[x^{-1}]$.

In Section 4.2 we show how $\mathcal{O}_X$-ideals respectively generalised vector bundles can be represented by their sections over V_0 and V_∞ respectively by their sections over V_0 and S. Moreover, the arithmetic operations necessary in the monoid of $\mathcal{O}_X$-ideals can be carried out using the latter pair $\mathcal{F}(V_0), \mathcal{F}(S)$ of ideals. We will use this later on in the algorithms to compute in the Picard group to represent $\mathcal{O}_X$-ideals of a specific form only using a polynomial matrix of bounded degree.

In Section 4.3 we state a structure theorem for the global sections of $\mathcal{O}_X$-ideals respectively generalised vector bundles by providing a k-basis constituted by a specific reduced basis of $\mathcal{F}(V_0)$ combined with successive powers of x up to integer bounds depending on $\mathcal{F}$. These integers are called π-invariants and they provide first and foremost bounds for the possible degree of basis matrices of bases of $\mathcal{F}(V_0)$. The latter will be crucial since $\mathcal{O}_X$-ideals of a specific form can be solely represented by such a basis matrix. We will give first bounds for the π-invariants for integral covers of $\mathbb{P}^1_k$.

In Section 4.4 we examine the case when X is a reducible cover of $\mathbb{P}^1_k$. We illustrate the relation between $\mathcal{O}_X$-ideals $\mathcal{F}$ and their restrictions $\mathcal{F}_{|X_i}$ to the irreducible components of X. This enables us to represent $\mathcal{F}(V_0)$ in terms of fixed reduced bases of $\mathcal{O}_{X_i}$ on the irreducible component X_i. Then we prove that there are bases of $\mathcal{F}(V_0)$ that have bounded degree in terms of the above fixed bases.

In Section 4.5 we can use the insights of Section 4.4 to prove bounds for the π-invariants of $\mathcal{O}_X$-ideals and of X itself in the case of reducible X implying the existence of basis matrices of $\mathcal{F}(V_0)$ with degree bounded by the degree of $\mathcal{F}(V_0)$ and c_X.

Section 4.6 relates reduced bases of $\mathcal{O}_X$ to those of $\mathcal{O}_{X_i}$ for X_i being an irreducible component of X. Moreover, we will provide algorithms that compute a basis matrix of $\mathcal{F}(V_0)$ that has row-blocks whose degrees are linearly bounded by the degree of $\mathcal{F}_{|X_i}(V_{i,0})$ and $c_{i,X}$. This enables us to work with matrices that do not only have bounded degree but with matrices whose blocks have bounded degrees depending on the respective components.

Finally, in Section 4.7 we characterise when a divisor is principal which can be used

for the test of equality in the Picard group.

4.1 $\mathcal{O}_X$-Ideals and Generalised Vector Bundles

In this section we introduce the notion of generalised vector bundles $\mathcal{F}$ on a scheme X which are a generalisation of $\mathcal{O}_X$-ideals to a higher rank. Most the analysis in this chapter (having free sections over V_0 and V_∞, being represented by sections over V_0 and V_∞, structural theorem for the global sections) can be done for generalised vector bundles and not only for $\mathcal{O}_X$-ideals. But for the sake of brevity we decided to only define generalised vector bundles and then do the analysis only for $\mathcal{O}_X$-ideals which are generalised vector bundles of rank one. This also suits our primary goal to use the insights gathered in this chapter for computing with invertible $\mathcal{O}_X$-ideals in Chapter 6.

Definition 4.1.1. Let $\mathcal{F}$ be a coherent sheaf of $\mathcal{O}_X$-modules. We call $\mathcal{F}$ a **generalised vector bundle of rank** r on X if it is an $\mathcal{O}_X$-subsheaf of $\mathcal{K}_X^r$ which is free of rank r at the generic points of X. Note that a generalised vector bundle of rank one is an $\mathcal{O}_X$-ideal as defined in Definition 3.1.13. △

The following lemma shows that being free of a given rank r at the generic points of a scheme is enough for being isomorphic to a generalised vector bundle of rank r. But since we only want to deal with such sheaves which are already embedded in $\mathcal{K}_X^r$, our definition already requires being embedded in $\mathcal{K}_X^r$.

Lemma 4.1.2. *Let X be a noetherian S_1-scheme. Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module. If $\mathcal{F}$ is locally free of rank r at each generic point η of X, then the isomorphisms $\mathcal{F}_\eta \cong \mathcal{O}_{X,\eta}^r$ for $\eta \in X^0$ provide an $\mathcal{O}_X$-module embedding of $\mathcal{F}$ into $\mathcal{K}_X^r$.*

Proof. Since X is noetherian, by [Sta18, Tag 0BA8], we know that it only has a finite number m of irreducible components $X_1, \dots, X_m$ with respective generic points $P_1, \dots, P_m$. Due to the S_1-hypothesis on X, the set of generic points equals the set of associated points of X. For every $i \in \{1, \dots, m\}$ there is an open subset

$$U_i := X_i \setminus \bigcap_{j \neq i} (X_j \cap X_i) = X \setminus \bigcup_{j \neq i} X_j$$

of X such that $U_i \cap X_j = \emptyset$ for all $i \neq j$. By assumption, $\mathcal{F}_{P_i} \cong \mathcal{O}_{X,P_i}^r$ and thus due to Lemma B.4.26 and Remark B.4.27, for every generic point P_i there is some open neighborhood V_i such that $\mathcal{F}_{|V_i} \cong \mathcal{O}_{V_i}^r$. Now setting $W_i = U_i \cap V_i$ we obtain $\mathcal{F}_{|W_i} \cong \mathcal{O}_{W_i}^r$ with $W_i \cap X_j = \emptyset$ for all $j \neq i$. We set $W = \bigcup_{i=1}^m W_i$ and denote with $i : W \hookrightarrow X$ the inclusion morphism. We claim that the canonical morphism $\mathcal{F} \to i_*(\mathcal{F}_{|W})$ is an injection: First of all, being injective is a property of local nature since it can be checked at stalks. Moreover, we have that $\mathcal{O}_X \to i_*\mathcal{O}_W$ is injective as long as W is schematically dense, see Lemma B.2.5, and thus contains all associated points of X. The latter is satisfied by construction of W. Furthermore, the open set W was constructed such that

$$\mathcal{F}_{|W} \cong \bigoplus_{j=1}^m \mathcal{F}_{|W_j} \cong \bigoplus_{j=1}^m \mathcal{O}_{W_j}^r \cong \mathcal{O}_W^r$$

and hence $\mathcal{F}_{|W}$ is free of rank r. Hence we obtain

$$\mathcal{F} \hookrightarrow i_*(\mathcal{F}_{|W}) \cong i_*(\mathcal{O}_W^r) \hookrightarrow i_*(\mathcal{K}_W^r) \cong \mathcal{K}_X^r$$

where the last isomorphism is given by Lemma B.2.6. □

Proposition 4.1.3. *Let R be a noetherian Cohen-Macaulay ring of dimension one. Then any finite R-submodule M of $\operatorname{Frac}(R)$ is torsion-free and thus satisfies S_1.*

Proof. Since $M \subseteq \operatorname{Frac}(R)$, every element of M is of the form a/r with $a, r \in R$ and r regular. Now for any $s \in R$ we have $s \cdot (a/r) = (as)/r = 0$ in $\operatorname{Frac}(R)$ if and only if there is some $t \in R$ regular such that $t(as) = 0$. Hence $as = 0$ and thus s is a zero-divisor in R. Whence M is torsion-free. Since R is Cohen-Macaulay, it satisfies S_1 and thus by Corollary B.4.21, M also satisfies S_1. □

Definition 4.1.4. Let X be a scheme and $\mathcal{F}$ a quasi-coherent $\mathcal{O}_X$-module. We call $\mathcal{F}$ **torsion-free** if for every affine open $U \subseteq X$ the $\mathcal{O}_X(U)$-module $\mathcal{F}(U)$ is torsion-free. △

Remark 4.1.5. Hartshorne developed the theory of *generalised divisors* in several publications [Har86], [Har94] and [Har07]. In [Har07] he defined them for noetherian, equidimensional, embeddable schemes which satisfy S_2. He calls every coherent $\mathcal{O}_X$-submodule $\mathcal{I}$ of $\mathcal{K}_X$ a **fractional ideal** and **non-degenerate** if for all generic points $\eta \in X^0$ we have $\mathcal{I}_\eta = \mathcal{K}_{X,\eta}$. Moreover, a **generalised divisor on** X is a non-degenerate fractional ideal which satisfies S_2.

Let X be a noetherian projective scheme of pure dimension one which satisfies S_1. Thus the notion of generalised divisors on X is defined. Moreover, since X has dimension one, being S_1 and being S_d for $d \geq 0$ is equivalent. By Corollary B.4.21, any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ satisfies S_1 if it is torsion-free. By Proposition 4.1.3, any $\mathcal{O}_X$-submodule of $\mathcal{K}_X$ is torsion-free and thus every $\mathcal{O}_X$-ideal is indeed a generalised divisor on X. Moreover, every generalised divisor on X is an $\mathcal{O}_X$-ideal. Hence the two notions coincide for the schemes in question. △

Lemma 4.1.6. *Let S be a principal ideal domain and let $R \supseteq S$ be a ring extension such that R is free of rank n over S. Let $M \subseteq \operatorname{Frac}(R)$ be a finitely generated R-module which contains a regular element of R. Then M is a free S-module of rank n.*

Proof. Note that $M \subseteq \operatorname{Frac}(R)$ already implies that M is torsion-free over R. Indeed, any $c \in R$ annihilating $a/b \in M$ provides that $cad = 0$ for some regular $d \in R$. Hence $ac = 0$ and thus c was a zero-divisor. Let $K = \operatorname{Frac}(S)$. The freeness of R over S provides that R is torsion-free over S and hence the same is true for M by assumption. Analogously, M is finitely generated over S and thus free over S. Then by Lemma B.4.10, we have $\operatorname{Frac}(R) = R \otimes_S K$ and hence $\operatorname{rk}_K M \leq n$. Every regular element $b \in M$ provides $\operatorname{rk}_K M \geq \operatorname{rk}_K R$: Indeed, the R-module homomorphism $R \to M$ given by multiplication with b is injective. Then every S-basis of R will be mapped to an S-linear independent set. □

Now we replace $\operatorname{Frac}(R)$ by $\operatorname{Frac}(R)^m$.

Proposition 4.1.7. *Let R be a ring. Then $\operatorname{Frac}(R^m) = \operatorname{Frac}(R)^m$.*

Proof. By construction, $\operatorname{Frac}(R)$ is the localisation of R by its regular elements. The zero-divisors of R^m are such $(r_1, \ldots, r_m) \neq 0$ with at least one r_i is a zero-divisor or $r_i = 0$. Thus the regular elements are those $(r_1, \ldots, r_m) \neq 0$ with r_i non-zero regular elements for all $i = 1, \ldots, m$. Thus $\operatorname{Frac}(R^m) \subseteq \operatorname{Frac}(R)^m$. Now let $(r_1/a_1, \ldots, r_m/a_m) \in \operatorname{Frac}(R)^m$ be arbitrary. Then $(r_1/a_1, \ldots, r_m/a_m) = (r_1, \ldots, r_m) \cdot (a_1, \ldots, a_m)^{-1}$ and the former is in R^m and the latter is a unit in $\operatorname{Frac}(R^m)$. Hence $(r_1/a_1, \ldots, r_m/a_m) \in \operatorname{Frac}(R^m)$ and therefore $\operatorname{Frac}(R)^m \subseteq \operatorname{Frac}(R^m)$. □

Lemma 4.1.8. *Let S be a principal ideal domain and let $R \supseteq S$ be a ring extension such that R is free of rank n over S. Let $M \subseteq \operatorname{Frac}(R)^m$ be a finitely generated R-module which contains a regular element of R^m. Then M is a free S-module of rank nm.*

Proof. We want to use Lemma 4.1.6 with ground ring R^m. Since R^m is free of rank m over R and the latter is free of rank n over S, we deduce that R^m is free of rank nm over S. By Proposition 4.1.7, we have $M \subseteq \mathrm{Frac}(R)^m = \mathrm{Frac}(R^m)$. Finally, M is finitely generated over R^m since it is already finitely generated over R and the scalar multiplication $R \times M \to M$ factorises as needed, i.e. $R \times M \to R^m \times M \to M$ where $R \to R^m$, $r \mapsto (r, \dots, r)$. Now Lemma 4.1.6 provides the assertion. □

The following lemma is (to some extent) stated in the appendix as Proposition C.1.10 in the context of R-ideals and thus for a specific class of rings.

Lemma 4.1.9. *Let $M \subseteq \mathrm{Frac}(R)$ be a finitely generated R-module where R is a one-dimensional ring that satisfies S_1 and has finitely many minimal prime ideals (e.g. R noetherian and reduced). Then M contains a regular element of R if and only if M is invertible at all minimal primes of R.*

Proof. Let M contain no regular element of R. Then every numerator of M is a zero-divisor and thus by the finiteness assumption there is some regular $g \in R$ such that $gM \subseteq R$. Moreover, $gM \subseteq \bigcup_i P_i$ where P_i denote the finitely many associated primes of R which are exactly the minimal primes of R by the S_1 assumption. The prime avoidance lemma Lemma B.4.5 now provides that $gM \subseteq P$ for one minimal prime. Then $M \hookrightarrow gM_P \subseteq PR_P$ and therefore M_P cannot be isomorphic to R_P as an R_P-module since PR_P only contains zero-divisors. Conversely, let M contain a regular element $a \in R$. Again the finiteness assumption provides a regular $g \in R$ with $ga \in gM \subseteq R$ and therefore, for any minimal prime P the image of ga in M_P is a unit in R_P. Hence M_P is invertible at P. □

Lemma 4.1.9 can be generalised to R-submodules of $\mathrm{Frac}(R)^m$. Let M be an R-submodule of $\mathrm{Frac}(R)^m$, then $M = \bigoplus_{i=1}^m M_i$ with $M_i \subseteq \mathrm{Frac}(R)$ being a fractional ideal of R. The R-scalar multiplication $R \times M \to M$ maps $(r, (x_1, \dots, x_m))$ to $(rx_1, \dots, rx_m)$.

Lemma 4.1.10. *Let $M \subseteq \mathrm{Frac}(R)^m$ be a finitely generated R-module where R is a one-dimensional ring that satisfies S_1 and has finitely many minimal prime ideals (e.g. R noetherian). Then M contains a regular element of $\mathrm{Frac}(R)^m$ if and only if M is free of rank m at all minimal primes of R.*

Proof. Since M is a finite R-module, there is some regular $g \in R$ such that $gM \subseteq R^m$. Let P be a minimal prime ideal of R. Let M_P be free of rank m over R. Hence $M_P \cong gM_P = \bigoplus_{i=1}^m g(M_i)_P$ is free of rank m over R_P. Since $g(M_i)_P \subseteq R_P$, the rank of $g(M_i)_P$ over R_P is at most 1 and hence we deduce that $g(M_i)_P \cong R_P$ for all $i = 1 \dots, m$. But since $g(M_i)_P \subseteq R_P$, the former is a principal ideal of R_P generated by a regular element a_i of R_P. Therefore we obtain $gM_P = \bigoplus_{i=1}^m a_i R_P$ and the latter clearly contains $(a_1, \dots, a_m)$ which is no zero-divisor in R_P^m. Clearing out the denominator provides a regular in gM and hence a regular element in M.

Conversely, let $(a_1/b_1, \dots, a_m/b_m) \in M = \bigoplus_{i=1}^m M_i$ be a regular element of $\mathrm{Frac}(R)^m$. Hence $a_i \in R$ are regular for $i = 1, \dots, m$. Multiplying with the product of the denominators provides $a = (a_1, \dots, a_m) \in M$. The image of a under the localisation homomorphism $M \to M_P$ for a minimal prime ideal P of R yields an element in $\bigoplus_{i=1}^m (M_i)_P$ whose entries are regular elements in R_P. But since P was minimal, the regular elements of R_P are the invertible element of R_P and hence $M_P = \bigoplus_{i=1}^m (M_i)_P = \bigoplus_{i=1}^m R_P = R_P^m$. □

Corollary 4.1.11. *Let X be a noetherian, Cohen-Macaulay scheme of dimension one. Let $\mathcal{F}$ be a generalised vector bundle of rank m on X. Then for any affine open subset $U = \mathrm{Spec}(R)$ of X there exists a section of $\mathcal{F}$ over U which is a regular element of R^m.*

Proposition 4.1.12. *Let (X, π) be a cover of $\mathbb{P}^1_k$. Let $U \subseteq \mathbb{P}^1_k$ be a non-empty affine open subset of $\mathbb{P}^1_k$ with coordinate ring A and let $V = \mathrm{Spec}(R) = \pi^{-1}(U)$. Let $\mathcal{F}$ be a generalised vector bundle of rank m on X. Then $\mathcal{F}(V)$ is free of rank mn over A.*

Proof. First of all, for X as above, Theorem D.1.6 provides the existence of a finite morphism $\pi : X \to \mathbb{P}^1_k$. By [GW10, 13.77], π is also an affine morphism and hence V is indeed affine. Now by Lemma B.5.20, we have a ring extension $A \subseteq R$ with A being a principal ideal domain. By assumption, X is Cohen-Macaulay and thus by Proposition D.2.4, we see that R is free of rank n over A. By definition, $\mathcal{F}(V) \subseteq \mathcal{K}_X(V)^m = \mathrm{Frac}(R)^m$ where the last equality is Proposition B.2.2. Hence by Corollary 4.1.11, the requirements for Lemma 4.1.8 are met and we deduce that $\mathcal{F}(V)$ is free of rank mn over A. □

4.2 Representation of $\mathcal{O}_X$-Ideals

We have seen in Section 2.3 that any pair (X, π) with a projective curve X over k and a finite morphism $\pi : X \to \mathbb{P}^1_k$ can be completely represented by a commutative diagram as in Figure 2.6 in Lemma 2.3.3. See also Lemma 2.3.1 and Definition 2.3.2. This commutative algebra setting also enables us to represent $\mathcal{O}_X$-ideals by an R_0-ideal and an R_∞-ideal. To prove the asserted statement, we first prove that any $\mathcal{O}_X$-ideal is characterised by its sections over V_0 and V_∞. In the following let (X, π) be a cover of $\mathbb{P}^1_k$.

As mentioned in the beginning of Section 4.1, we would like to emphasise that all of the statements we make for $\mathcal{O}_X$-ideals in the following can be easily generalised to generalised vector bundles.

Lemma 4.2.1. *Every $\mathcal{O}_X$-ideal $\mathcal{F}$ is, as a sheaf of abelian groups, represented by its sections over V_0 and V_∞.*

Proof. By assumption, we have $\mathcal{F}(V_0) \subseteq \mathrm{Frac}(R_0)$ and $\mathcal{F}(V_\infty) \subseteq \mathrm{Frac}(R_\infty)$. The sections of $\mathcal{F}$ over any open subset $U \subseteq X$ can be given by a weakly matching family as follows

$$\mathcal{F}(U) = \left\{ (f_0, f_\infty) \in \mathcal{F}(U \cap V_0) \times \mathcal{F}(U \cap V_\infty) \mid \rho^{U\cap V_0}_{U\cap V_{0,\infty}}(\mathcal{F})(f_0) = \rho^{U\cap V_\infty}_{U\cap V_{0,\infty}}(\mathcal{F})(f_\infty) \right\}.$$

By assumption, $\mathcal{F}$ is quasi-coherent and thus the sections of $\mathcal{F}_{|V_0} = \mathcal{F}(V_0)^\sim$ over any open subset of V_0 are completely determined by $\mathcal{F}(V_0)$. Moreover, the same is true for the restriction maps of $\mathcal{F}_{|V_0}$. By symmetry, we see that the same is true for $\mathcal{F}_{|V_\infty}$ and therefore we obtain that both the sections of $\mathcal{F}$ over any open $U \subseteq X$ are characterised by $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ and the restriction maps as well. □

Remark 4.2.2. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ are R_0- respectively R_∞-submodules of $\mathrm{Frac}(R_0)$ respectively $\mathrm{Frac}(R_\infty)$. Since $\mathcal{F}$ is quasi-coherent, the same is true for $\mathcal{F}_{|V_0}$ and $\mathcal{F}_{|V_\infty}$. Moreover, we have that $V_{0,\infty}$, as an open subset of V_0, is basic open with $V_{0,\infty} = D_{V_0}(x)$. Similarly, $V_{0,\infty}$ is basic open in V_∞ with $V_{0,\infty} = D_{V_\infty}(x^{-1})$. Hence, we have

$$\begin{aligned}(\mathcal{F}_{|V_0})(V_{0,\infty}) = (\mathcal{F}_{|V_0})(V_0)_x = \mathcal{F}(V_0)_x \quad \text{and} \\ (\mathcal{F}_{|V_\infty})(V_{0,\infty}) = (\mathcal{F}_{|V_\infty})(V_\infty)_{x^{-1}} = \mathcal{F}(V_\infty)_{x^{-1}}.\end{aligned}$$

Since the left hand sides are clearly equal, we see that $\mathcal{F}(V_0)_x = \mathcal{F}(V_\infty)_{x^{-1}}$ represents the gluing condition for the modules $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ to be sections of the same sheaf. △

The above Remark and Lemma 4.2.1 show that $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ do not only suffice to represent $\mathcal{F}$ but we also have a gluing or compatibility condition imposed on $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$. Next we will show a somewhat converse.

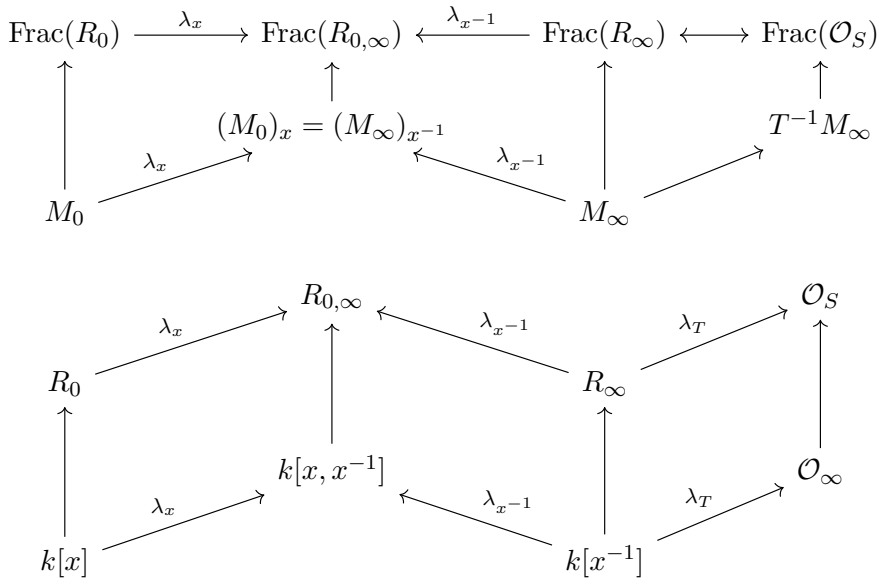
Lemma 4.2.3. *Let M_0 be an R_0-submodule of $\mathrm{Frac}(R_0)$ and let M_∞ be an R_∞-submodule of $\mathrm{Frac}(R_\infty)$. If $(M_0)_x = (M_\infty)_{x^{-1}}$, then there exists an $\mathcal{O}_X$-submodule $\mathcal{F}$ of $\mathcal{K}_X$ with $\mathcal{F}(V_0) = M_0$ and $\mathcal{F}(V_\infty) = M_\infty$. Moreover, if M_0 and M_∞ are R_0- respectively R_∞-ideals, then $\mathcal{F}$ is an $\mathcal{O}_X$-ideal.*

Proof. We consider the quasi-coherent sheaves $M_0^\sim = \mathcal{F}_0$ and $M_\infty^\sim = \mathcal{F}_\infty$ induced by M_0 on V_0 respectively by M_∞ on V_∞. Then $V_0 \cup V_\infty = X$ and the sheaves $\mathcal{F}_0$ and $\mathcal{F}_\infty$ are compatible on $V_{0,\infty}$ by assumption. Indeed, $(M_0)_x = (M_\infty)_{x^{-1}}$ shows that $(\mathcal{F}_\infty)_{|V_{0,\infty}}$ and $(\mathcal{F}_0)_{V_{0,\infty}}$ are isomorphic via Φ from diagram Figure 2.3 in Lemma 2.3.1. Thus the sheaves $\mathcal{F}_0$ and $\mathcal{F}_\infty$ glue together to a quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ on X. But since $\mathcal{K}_X$ is quasi-coherent, we have $\mathcal{F}_{|V_0} = \mathcal{F}_0 \leq (\mathcal{K}_X)_{|V_0}$ and $\mathcal{F}_{|V_\infty} = \mathcal{F}_\infty \leq (\mathcal{K}_X)_{|V_\infty}$. Thus we may glue $\mathcal{F}_0$ and $\mathcal{F}_\infty$ as well as $(\mathcal{K}_X)_{|V_0}$ and $(\mathcal{K}_X)_{|V_\infty}$ and the resulting sheaves will satisfy $\mathcal{F} \leq \mathcal{K}_X$. Finally, if M_0 and M_∞ are R_0- respectively R_∞-ideals, then they are invertible at the minimal prime ideals of R_0 respectively R_∞. This shows that $\mathcal{F}$ is invertible at the generic points of X and thus an $\mathcal{O}_X$-ideal. □

Corollary 4.2.4. *We have a bijection between the set of $\mathcal{O}_X$-submodules $\mathcal{F}$ of $\mathcal{K}_X$ and the set of pairs (M_0, M_∞) where M_0 is an R_0-submodule of* $\mathrm{Frac}(R_0)$ *and M_∞ an R_∞-submodule of* $\mathrm{Frac}(R_\infty)$ *such that $(M_0)_x = (M_\infty)_{x^{-1}}$. Moreover, if X is Cohen-Macaulay, then the $\mathcal{O}_X$-ideals correspond under this bijection the to the pairs (M_0, M_∞) with M_0 being an R_0-ideal and M_∞ being an R_∞-ideal.*

We may summarise the situation with a diagram:

Figure 4.1: $\mathcal{O}_X$-ideals on curve over k as a commutative diagram



Localisation homomorphisms extend to total rings of fractions.

Remark 4.2.5. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. The modules $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ can be embedded into $\mathrm{Frac}(R_{0,\infty})$ via the localisation maps $\lambda_x : \mathrm{Frac}(R_0) \to \mathrm{Frac}(R_{0,\infty})$ and $\lambda_{x^{-1}} : \mathrm{Frac}(R_\infty) \to \mathrm{Frac}(R_{0,\infty})$. Note that this is not the same as localising them by x respectively x^{-1}. But since λ_x and $\lambda_{x^{-1}}$ map as the identity map, see Lemma 2.3.3, we can already regard $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ as subsets of $\mathrm{Frac}(R_{0,\infty})$ (but not as $R_{0,\infty}$-submodules of $\mathrm{Frac}(R_{0,\infty})$ since we need to localise them to do so). In particular, we may consider the sets $\mathcal{F}(V_0) \cap \mathcal{F}(V_\infty) \subseteq \mathcal{F}(V_0) \cap \mathcal{F}(S)$. △

In terms of arithmetic representation and operations in the monoid $\mathrm{MonoId}(X)$, the pairs $(\mathcal{F}(V_0), \mathcal{F}(S))$ already suffice.

Lemma 4.2.6. *Every element $\mathcal{F}$ of the monoid of $\mathcal{O}_X$-ideals* $\mathrm{MonoId}(X)$ *on X, see Definition 3.1.15, can be represented by the pair $(\mathcal{F}(V_0), \mathcal{F}(S))$. Moreover, the arithmetic operations being relevant for the arithmetic in* $\mathrm{MonoId}(X)$*, that is, multiplication and checking for equality, can be carried out using that pair.*

Proof. First of all, by Lemma 3.2.29, the map $\mathcal{F} \mapsto (\mathcal{F}(V_0), \mathcal{F}(S))$ is injective. By Lemma 3.1.17, we know that $(\mathcal{F}\mathcal{G})(V_0)$ and $(\mathcal{F}\mathcal{G})(V_\infty)$ can be identified with $(\mathcal{F}\mathcal{G})(V_0)$ respectively $\mathcal{F}(V_\infty)\mathcal{G}(V_\infty)$. Thus

$$(\mathcal{F}\mathcal{G})(S) = T^{-1}(\mathcal{F}\mathcal{G})(V_\infty) = T^{-1}\mathcal{F}(V_\infty)\mathcal{G}(V_\infty) = T^{-1}\mathcal{F}(V_\infty)T^{-1}\mathcal{G}(V_\infty) = \mathcal{F}(S)\mathcal{G}(S)$$

which provides the assertion. □

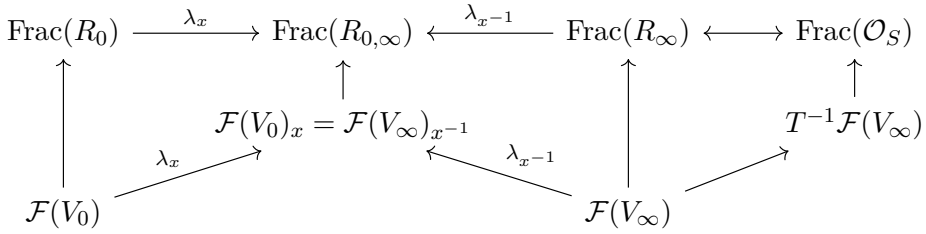
Remark 4.2.7. Though the pair $(\mathcal{F}(V_0), \mathcal{F}(S))$ does what we want in terms of arithmetic in $\mathrm{MonoId}(X)$, it does not provide in general a way to reconstruct $\mathcal{F}$. The latter would mean that we are able to compute $\mathcal{F}(V_\infty)$ from $(\mathcal{F}(V_0), \mathcal{F}(S))$ which in general is not possible. Given any $\mathcal{O}_\infty$-basis of $\mathcal{F}(S)$ which is not simultaneously a $k[x^{-1}]$-basis of $\mathcal{F}(V_\infty)$, we are in general only able to compute a $k[x^{-1}]$-submodule of $\mathcal{F}(V_\infty)$. △

Lemma 4.2.8. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\mathcal{F}(X) = \mathcal{F}(V_0) \cap \mathcal{F}(V_\infty) = \mathcal{F}(V_0) \cap \mathcal{F}(S)$ where we regard the involved sets as subsets of* $\mathrm{Frac}(R_{0,\infty})$ *as in Remark 4.2.5.*

Proof. Note that we have $\rho^{V_0}_{V_{0,\infty}}(\mathcal{F}) = \lambda_x : \mathcal{F}(V_0) \to \mathcal{F}(V_0)_x$ and $\rho^{V_\infty}_{V_{0,\infty}}(\mathcal{F}) = \lambda_{x^{-1}} : \mathcal{F}(V_\infty) \to \mathcal{F}(V_\infty)_{x^{-1}}$. Then the proof of Lemma 4.2.1 shows that

$$\mathcal{F}(X) = \{(f_0, f_\infty) \in \mathcal{F}(V_0) \times \mathcal{F}(V_\infty) \mid \lambda_x(f_0) = \lambda_{x^{-1}}(f_\infty)\}.$$

Since $\mathcal{F}$ is an $\mathcal{O}_X$-ideal, we have the following commutative diagram:



(2:1)

Therefore, after regarding f_0 and f_∞ as elements of $\mathrm{Frac}(R_{0,\infty})$, the commutativity of diagram (2:1) provides that they both lie in $\mathcal{F}(V_0)_x = \mathcal{F}(V_\infty)_{x^{-1}}$. Hence $f_0 = f_\infty$ as elements in $\mathrm{Frac}(R_{0,\infty})$ if and only if $\lambda_x(f_0) = \lambda_{x^{-1}}(f_\infty)$ as elements of $\mathcal{F}(V_0)$ respectively $\mathcal{F}(V_\infty)$. This provides $\mathcal{F}(X) = \mathcal{F}(V_0) \cap \mathcal{F}(V_\infty)$. The second equality in the assertion follows again by the commutativity of the diagram (2:1) and by the fact that $\mathcal{F}(V_\infty) \subseteq T^{-1}\mathcal{F}(V_\infty)$. □

Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. To represent the $\mathcal{O}_X$-module structure of $\mathcal{F}$, we need to encode the scalar multiplication $\mathcal{O}_X(V) \times \mathcal{F}(V) \to \mathcal{F}(V)$ for open $V \in \{V_0, V_\infty\}$. We have seen in Proposition 4.1.12 that if $\mathcal{F}$ is an $\mathcal{O}_X$-ideal, then $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ are free of rank n over $k[x]$ respectively $k[x^{-1}]$. Note that this also holds for $\mathcal{F} = \mathcal{O}_X$ and thus R_0 as well as R_∞ are free of rank n over $k[x]$ respectively $k[x^{-1}]$. We can use this to represent the $\mathcal{O}_X$-module structure. Let $(V, R) \in \{(V_0, R_0), (V_\infty, R_\infty)\}$. One possible way to go is to store a basis of $\mathcal{F}(V)$, a basis of R and a matrix which tells us how the products of these bases are represented again. But this sums up to storing a $(n \times n^2)$-matrix for each $\mathcal{F}(V)$.

But there is another way around this:

Proposition 4.2.9. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. By storing two $(n \times n^2)$-matrices once for all, both independent of $\mathcal{F}$, one over $k[x]$ and one over $k[x^{-1}]$, $\mathcal{F}$ can be represented by its sections over V_0 and V_∞.*

Proof. By the above discussion, we only need to show that we can represent the $\mathcal{O}_X$-module structure of $\mathcal{F}$. Let $(U, V, R) \in \{(U_0, V_0, R_0), (U_\infty, V_\infty, R_\infty)\}$. The task comes down to

storing the information of how the scalar product of a basis of $\mathcal{F}(V)$, say $v_1, \dots, v_n$, with a basis of R, say $\omega_1, \dots, \omega_n$, is again represented by the v_i. Now both $\mathcal{F}(V)$ and R are contained in the same $k(x)$-vector space $\mathrm{Frac}(R_{0,\infty})$ which is of dimension n. Hence there is some basis transformation matrix $M = (\mu_{ij})_{ij} \in k(x)^{n\times n}$ such that $(\omega_1, \dots, \omega_n)M = (v_1, \dots, v_n)$. Then the scalar product of v_j with some $f \in R$ with $f = \sum_{i=1}^n f_i\omega_i$ is given by $f\, v_j = \sum_{i=1}^n f_i(\omega_i v_j) = \sum_{i=1}^n f_i \left(\sum_{\ell=1}^n \mu_{\ell,j}\omega_\ell\omega_i\right) = \sum_{i,\ell}^n f_i\mu_{\ell,j}(\omega_\ell\omega_i)$. This means that if we are only working with coefficient vectors regarding a fixed basis $\omega_1, \dots, \omega_n$ of R, then, to represent the R-module structure of $\mathcal{F}(V)$, it is sufficient to know the matrix M and a *multiplication table* $T \in \mathcal{O}_{\mathbb{P}^1}(U)^{n^2\times n}$ in which the coefficients of the products $\omega_\ell\omega_i$ are stored. □

Thus to represent $\mathcal{O}_X$-ideals $\mathcal{F}$, there are two things to do: First, we need to fix two bases, one of R_0 over $k[x]$ and one of R_∞ over $k[x^{-1}]$, and then store the information about the products of the first kind in a multiplication table. Second, we represent both $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ with bases over $k[x]$ respectively $k[x^{-1}]$. The latter can be done by each storing a matrix, containing the coefficients of the basis elements regarding the fixed bases of R_0 and R_∞. Hence this provides a way to represent divisors D on X via its corresponding invertible sheaf $\mathcal{O}_X(D)$ and this in turn with its free modules $\mathcal{O}_X(D)(V_0)$ and $\mathcal{O}_X(D)(V_\infty)$.

Remark 4.2.10. Note that by Proposition 2.2.12, the $k[x^{-1}]$-basis of $\mathcal{F}(V_\infty)$ is also an $\mathcal{O}_\infty$-basis of $\mathcal{F}(S) = T^{-1}\mathcal{F}(V_\infty)$ and hence the latter is free of rank n as well. Hence the above representation via basis matrices provides a representation of $\mathcal{F}(S)$ as well. △

We will see in what follows that we might want to replace $\mathcal{F}(V_\infty)$ by $\mathcal{F}(S)$ (which by Remark 4.2.10 does not change the representation via bases at all) to be able to use matrix diagonalisation statements.

These will provide invariants of pairs (M_0, M_S) where M_0 is an R_0-ideal and M_S an $\mathcal{O}_S$-ideal. By what we have seen above, we thus obtain invariants for every $\mathcal{O}_X$-ideal.

4.3 Reduced Bases, π-Invariants and Global Sections

Consider the following situation: Let X be a integral and non-singular projective curve over k with function field $k(X)$. When dealing with (Weil) divisors D on X, one is mainly interested in the set of functions

$$\mathcal{L}(D) = \{f \in k(X) \mid v_P(f) + v_P(D) \geq 0\} \cup \{0\} \tag{3:2}$$

that satisfy the requirements (regarding orders of poles and zeros) the divisor prescribes. This k-vector space is called the *Riemann-Roch space* of the divisor D and it has finite dimension over k. These Riemann-Roch spaces and the theorem of Riemann-Roch which relates the dimension of $\mathcal{L}(D)$ with the degree of D (and even gives an equation that predicts the dimension of $\mathcal{L}(D)$ if the degree of D is large enough, we refer the reader to Section E.2 where we provide this kind of equation for a broader class of curves over k and broader class of sheaves) has huge areas of application in the geometry of curves over k. If $\mathcal{O}_X(D)$ denotes the invertible sheaf associated to D, see Proposition 3.1.27, then Lemma 3.1.32 provides that

$$\begin{aligned}\mathcal{O}_X(D)(X) &= \{f \in \mathcal{K}_X(X)^\times \mid \mathrm{div}_X(f) + D \geq 0\} \cup \{0\} \\ &= \mathcal{L}(D).\end{aligned} \tag{3:3}$$

On more general schemes, for instance if X is a projective curve over k, $\mathcal{L}(D)$ cannot be defined as in Eq. (3:2) (since for singular points P on X there is no discrete valuation

v_P available) and thus $\mathcal{O}_X(D)(X)$ seems to be the right replacement for $\mathcal{L}(D)$. But for reducible X, there may be elements from $\mathcal{K}_X(X) \setminus \mathcal{K}_X(X)^\times$ appearing in $\mathcal{O}_X(D)(X)$ which shows that the elements in the right hand side of Eq. (3:3) do not constitute all of $\mathcal{O}_X(D)(X)$.

However, the invertible sheaves $\mathcal{O}_X(D)$ associated to divisor can be regarded as a suitable class of sheaves for which it is worthwhile to examine the structure of their global sections. We go a bit further and want to analyse the global sections of $\mathcal{O}_X$-ideals. We will use the fact that $\mathcal{F}(V_0)$ and $\mathcal{F}(S)$ are both free or rank n over $k[x]$ respectively $\mathcal{O}_\infty$. This enables us to represent $\mathcal{F}(X)$ using a specific kind of basis of $\mathcal{F}(V_0)$ which is directly linked to and provides a basis of $\mathcal{F}(S)$ as well. Before we can introduce the above kind of basis, which we will call reduced, we need to introduce some of the mechanics used in the section *Lattices and Basis Reduction over $k[x]$* of [Hes02]. These will enable us to relate bases of $\mathcal{F}(V_0)$ and $\mathcal{F}(S)$ by a diagonal matrix with powers of x on its diagonal.

Definition 4.3.1. Let $k((x^{-1}))$ denote the field of formal Laurent series in x^{-1}. For $f \in k((x^{-1}))$ let $\deg(f)$ denote the largest power of x that appears in f. For $v \in k((x^{-1}))^n$ let $\deg(v)$ denote the maximum of the degrees of the entries of v. We call $\deg(v)$ the **(column) degree of** v. Let $M = (v_1 \dots v_n) = (v_{i,j})_{i,j} \in k((x^{-1}))^{m\times n}$ with $v_i \in k((x^{-1}))^m$. By $\mathrm{LC}(M) = (d_{i,j})_{i,j} \in k^{m\times n}$ we denote the matrix with

$$d_{i,j} = \begin{cases} \ell c(v_{i,j}), & \deg v_{i,j} = \deg(v_j) \\ 0, & \text{otherwise} \end{cases}$$

and call it the **leading coefficient matrix** of M. △

Remark 4.3.2. Note that we have $k(x) \subseteq k((x^{-1}))$ and for $f/g \in k(x)$ with $f, g \in k[x]$ we have $\deg(f/g) = \deg(f) - \deg(g)$ where the former degree is the one of the element in $k((x^{-1}))$ and the latter that of $k[x]$. Indeed, we can write $f = x^{\deg(f)}\widetilde{f}$ and $g = x^{\deg(g)}\widetilde{g}$ where both $\widetilde{f}, \widetilde{g} \in k[x^{-1}]$ not divisible by x^{-1}. In particular, both $\widetilde{f}$ and $\widetilde{g}$ have degree zero in $k((x^{-1}))$ which is equivalent to be a unit in $k((x^{-1}))$. Moreover, this yields $\widetilde{f}/\widetilde{g} = \varepsilon \in k((x^{-1}))^\times$ with ε having non-zero constant coefficient and all coefficients of positive powers of x are zero. Then

$$\frac{f}{g} = x^{\deg(f)-\deg(g)} \cdot \varepsilon$$

and thus the degree of the right hand side, as an element in $k((x^{-1}))$, is equal to $\deg(f) - \deg(g)$ as asserted. △

Definition 4.3.3. Let $M \in k((x^{-1}))^{n\times n}$ be a matrix with columns $v_1, \dots, v_n$. We say that M is **reduced** if it satisfies the following equivalent properties:

(i) No $k[x]$-unimodular column operation does decrease the sum of column degrees of M,

(ii) $\mathrm{LC}(M)$ has full rank,

(iii) $\sum_{i=1}^n \deg(\lambda_i v_i) = \max\{\deg(\lambda_i v_i))\}$, and

(iv) $\deg\det M = \sum_{i=1}^n \deg(v_i)$.

For the equivalence of these properties see [Hes02, Lemma 1]. △

Remark 4.3.4. For any $M \in k((x^{-1}))^{n\times n}$ we might perform $k[x]$-unimodular column operations on M which strictly decrease the sum of the column degrees of M. If this is not possible, then the result is reduced by Definition 4.3.3 (i). Moreover, this process needs to terminate since by Definition 4.3.3, (iv) the sum of the column degrees has as lower

bound the degree of the determinant of M (which does not change under $k[x]$-unimodular column operations). Hence any matrix might be reduced this way.

Moreover, if $M \in k(x)^{n\times n}$, then we may write $M = M_0/f$ with $f \in k[x]$ and $M_0 \in k[x]^{n\times n}$. In this case it is enough to reduce M_0, that is, if M_0' is a reduced right equivalent matrix of M_0, then M_0'/f is a reduced right equivalent matrix of M_0/f. △

We state a very important matrix diagonalisation lemma which is originally due to Birkhoff. To do so, we first cite a statement from [Hes02].

Lemma 4.3.5 (Corollary 3, [Hes02])**.** *Let $M \in k(x)^{n\times n}$. There exist unimodular matrices $T_1 \in \mathcal{O}_\infty^{n\times n}$ and $T_2 \in k[x]^{n\times n}$ and uniquely determined rational integers $d_1 \geq \ldots \geq d_n$ such that*

$$T_1 \cdot M \cdot T_2 = (x^{-d_j}\delta_{i,j})_{i,j}. \tag{3:4}$$

The matrix T_2 is the basis transformation matrix obtained by the reduction algorithm (as mentioned in Remark 4.3.4) performed on the columns of M. The column degree of the j-th column of $M \cdot T_2$ is equal to $-d_j$.

The following corollary is a slight adaptation of [Hes02, Corollary 4].

Corollary 4.3.6. *Let V be an n-dimensional $k(x)$-vector space. Let M_0 be a $k[x]$-module and M_∞ be an $\mathcal{O}_\infty$-module both free of rank n inside of V. To any such two modules we find bases $v_1, \ldots, v_n$ of M_0 and $b_1, \ldots, b_n$ of M_∞ such that*

$$(v_1, \ldots, v_n) = (b_1, \ldots, b_n) \cdot (x^{-d_j}\delta_{i,j})_{i,j}.$$

The sequence $d_1 \geq \ldots \geq d_n$ is uniquely determined by M_0 and M_∞ and we call them the $k(x)$-invariants of (M_0, M_∞).

Proof. Every $k[x]$-basis of M_0 and every $\mathcal{O}_\infty$-basis of M_∞ provide a $k(x)$-basis of V. Both the existence of the bases and the uniqueness of the integers $d_1 \geq \ldots \geq d_n$ is due to Lemma 4.3.5 applied to an arbitrary basis transformation matrix from a $k(x)$-basis provided by M_∞ to a $k(x)$-basis provided by M_∞. □

Remark 4.3.7. Note that if we want to compute the invariants $d_1 \geq \ldots \geq d_n$ of (M_0, M_∞), then we may start with any two bases of M_0 and M_∞. Then the transformation matrix can be reduced performing unimodular $k[x]$-column operations as in Lemma 4.3.5. The resulting matrix has column degrees $-d_1, \ldots, -d_n$.

In particular, since the above unimodular column operations do strictly decrease the sum of the column degrees of a transformation matrix, any given transformation matrix M with degree bounded by d provides an upper bound: $-d_1 \leq \ldots \leq -d_n \leq d$. △

Definition 4.3.8. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then by Corollary 4.2.4, $\mathcal{F}$ is represented by the pair $(\mathcal{F}(V_0), \mathcal{F}(V_\infty))$ which both in turn can be represented by bases over $k[x]$ respectively $k[x^{-1}]$. Following Remark 4.2.10, the pair $(\mathcal{F}(V_0), \mathcal{F}(V_\infty))$ given by bases induces the pair $(\mathcal{F}(V_0), \mathcal{F}(S))$. The basis of $\mathcal{F}(V_0)$ over $k[x]$ provides a $k(x)$-basis of $\mathrm{Frac}(R_{0,\infty})$ and that of $\mathcal{F}(S)$ over $\mathcal{O}_\infty$ (which comes from a $k[x^{-1}]$-basis of $\mathcal{F}(V_\infty)$) does the same. Thus Corollary 4.3.6 applies and provides $k(x)$-invariants of $(\mathcal{F}(V_0), \mathcal{F}(S))$ which we call the **π-invariants** of $\mathcal{F}$ and denote them by $|\mathcal{F}|_1 \geq \ldots \geq |\mathcal{F}|_n$. For the sake of readability we abbreviate $|X|_i := |\mathcal{O}_X|_i$ and $|D|_i := |\mathcal{O}_X(D)|_i$ for any divisor $D \in \mathrm{Div}(X)$. △

Remark 4.3.9. In Chapter E of the appendix we will talk about the invariants a finite morphism $\pi : X \to \mathbb{P}^1_k$ induces in general. We will see that the π-invariants defined above are essentially the same. △

Remark 4.3.10. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Any $k[x]$-basis of $\mathcal{F}(V_0)$ is an $k[x,x^{-1}]$-basis of $\mathcal{F}(V_0)_x$ and any $k[x^{-1}]$-basis of $\mathcal{F}(V_\infty)$ is an $k[x,x^{-1}]$-basis of $\mathcal{F}(V_\infty)_{x^{-1}}$. Now since $\mathcal{F}(V_0)_x = \mathcal{F}(V_\infty)_{x^{-1}}$, any two such bases provide $k[x,x^{-1}]$-bases of the same $k[x,x^{-1}]$-module. Hence there is a basis transformation matrix relating them which is an element in $\mathrm{GL}(n,k[x,x^{-1}])$. △

Lemma 4.3.11. *For $A \in \mathrm{GL}(n,k[x,x^{-1}])$ there are $T \in \mathrm{GL}(n,k[x^{-1}])$, $S \in \mathrm{GL}(n,k[x])$ and uniquely determined integers $d_1 \geq \ldots \geq d_n$ such that $TAS = (x^{-d_i}\delta_{i,j})_{i,j}$.*

Proof. By [Hes02, Corollary 3], there are matrices $T \in \mathrm{GL}(n,\mathcal{O}_\infty)$, $S \in \mathrm{GL}(n,k[x])$ and integers $d_1 \geq \ldots \geq d_n$ with $TAS = (x^{-d_i}\delta_{i,j})_{i,j}$. Hence $T^{-1} = AS(x^{d_i}\delta_{i,j})_{i,j}$ has determinant in $\mathcal{O}_\infty^\times \cap \{a \cdot x^m \mid a \in k, m \in \mathbb{Z}\} = k^\times$. Moreover, since all matrices A, S and $(x^{d_i}\delta_{i,j})_{i,j}$ have entries in $k[x,x^{-1}]$ and T^{-1} is defined over $\mathcal{O}_\infty$, its entries lie in $\mathcal{O}_\infty \cap k[x,x^{-1}] = k[x^{-1}]$.

The latter equality holds more general: Let R be a noetherian domain and let $f \in R$ be a prime element in R. Then $R_{(f)} \cap R_f = R$ where the intersections take place in the quotient field $\mathrm{Frac}(R)$ of R. Let $a/b = c/f^r$ with $r \geq 1$ hold in $\mathrm{Frac}(R)$ such that $f \nmid c$ in R and $b \notin fR$. Then by definition, we have $af^r = bc$ and thus $f \mid bc$ which is a contradiction. Thus we obtain $r = 0$ and hence $a/b = c \in R$ which implies the assertion. □

Lemma 4.3.12. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal.*

(i) There are bases $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta_n$ of $\mathcal{F}(V_0)$ respectively $\mathcal{F}(V_\infty)$ and integers $d_1 \geq \ldots \geq d_n$ such that $\alpha_i = \beta_i x^{-d_i}$.

(ii) For any two bases $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta_n$ as in Item (i), the set

$$\{x^j\alpha_i \mid 1 \leq i \leq n,\ 0 \leq j \leq d_i\}$$

is a k-basis of $\mathcal{F}(X)$.

Proof. We first prove Item (i). By Remark 4.3.10, any two bases of $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ are also $k[x,x^{-1}]$-bases of $\mathcal{F}(V_0)_x$ and $\mathcal{F}(V_\infty)_{x^{-1}}$ and hence there is a transformation matrix $A \in \mathrm{GL}(n,k[x,x^{-1}])$. Applying Lemma 4.3.11 to A provides bases $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta_n$ of $\mathcal{F}(V_0)$ respectively $\mathcal{F}(V_\infty)$ with $\alpha_i = \beta_i x^{-d_i}$. Now we prove Item (ii). By Lemma 4.2.8, the global sections of $\mathcal{F}$ consist of those elements in $\mathrm{Frac}(R_{0,\infty})$ that have both a preimage under λ_x in $\mathcal{F}(V_0)$ and one under $\lambda_{x^{-1}}$ in $\mathcal{F}(V_\infty)$. By Remark 4.3.10, we know that every $k[x]$-basis of $\mathcal{F}(V_0)$ is also a $k[x,x^{-1}]$-basis of $\mathcal{F}(V_{0,\infty})$ and every $k[x^{-1}]$-basis of $\mathcal{F}(V_\infty)$ is also a $k[x,x^{-1}]$-basis of $\mathcal{F}(V_{0,\infty})$. Hence $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta_n$ are $k[x,x^{-1}]$-bases of $\mathcal{F}(V_{0,\infty})$. Let $f \in \mathcal{F}(V_{0,\infty})$ be arbitrary. Now f has a preimage under λ_x if and only if $\phi_{(\alpha_i)}(f) \in k[x]^n$ and f has a preimage under $\lambda_{x^{-1}}$ if and only if $\phi_{(\beta_i)}(f) \in k[x^{-1}]^n$. Let $f = \sum_{i=1}^n \lambda_i\alpha_i$ with $\lambda_i \in k[x,x^{-1}]$. Then $\phi_{(\alpha_i)}(f) = (\lambda_1,\ldots,\lambda_n)^T$. Since $\alpha_i = \beta_i x^{-d_i}$, we have $\phi_{(\beta_i)}(f) = \mathrm{diag}(x^{d_i}) \cdot \phi_{(\alpha_i)}(f)$. This provides that $f \in \mathcal{F}(X)$ if and only if $\deg(\lambda_i) - d_i \leq 0$ and hence the assertion follows. □

Remark 4.3.13. Note that the integers d_i can (and will be, for instance, for $\mathcal{F} = \mathcal{O}_X$ we will have $0 \geq d_1 \geq \ldots \geq d_n$) be negative. △

Note that the $k[x^{-1}]$-basis $\beta_1,\ldots,\beta_n$ of $\mathcal{F}(V_\infty)$ will also be an $\mathcal{O}_\infty$-basis of $\mathcal{F}(S)$. Naturally, the question of how to obtain such nice bases as given in Lemma 4.3.12 is, at this point, still open. Theorem 4.3.15 will answer this question in an algorithmically insightful way.

Lemma 4.3.14. *Let $M = (v_1 \ldots v_n) \in k(x)^{n\times n}$ be a unimodular and reduced matrix. Let $-d_i$ denote the degree of the column v_i. Then $M \cdot \mathrm{diag}(x^{d_i})$ is unimodular over $\mathcal{O}_\infty$.*

Proof. First of all, $M \cdot \operatorname{diag}(x^{d_i})$ is defined over $\mathcal{O}_\infty$ since each column v_i of M is divided by $x^{\deg(v_i)}$ and thus has degree lower or equal to zero. Since M is reduced, by Definition 4.3.3 (iv), we have $\sum_{i=1}^n -d_i = \sum_{i=1}^n \deg(v_i) = \deg \det M$. Hence the determinant of $M \cdot \operatorname{diag}(x^{d_i})$ has degree zero and is thus a unit in $\mathcal{O}_\infty$. □

We now state one of the fundamental ingredients of our algorithms. The following theorem originates from [Hes02, Theorem 7] which is stated for the function field case of an integral, non-singular and plane projective curve. Theorem 4.3.15 also considers the reducible, singular and non-plane case, but the proof of [Hes02, Theorem 7] still works. However, we will give a slightly different and more constructive proof since it will provide some algorithmic insights.

Theorem 4.3.15. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal with π-invariants $|\mathcal{F}|_1 \geq \ldots \geq |\mathcal{F}|_n$. Then there is a $k[x]$-basis $v_1, \ldots, v_n$ of $\mathcal{F}(V_0)$ such that*

$$\left\{x^j v_i \mid 1 \leq i \leq n, 0 \leq j \leq |\mathcal{F}|_i + r\right\}$$

*forms a k-basis of $\mathcal{F}(r(x)_\infty)(X)$ for all $r \in \mathbb{Z}$. We call such a basis of $\mathcal{F}(V_0)$ a **reduced** basis of $\mathcal{F}$ respectively $\mathcal{F}(V_0)$.*

Proof. Note that by Lemma D.2.23 and Corollary D.2.24, we have $\mathcal{F}(r(x)_\infty)(V_0) = \mathcal{F}(V_0)$ and $\mathcal{F}(r(x)_\infty)(S) \cong x^r \mathcal{F}(S)$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $\mathcal{F}(V_0)$ and $\beta_1, \ldots, \beta_n$ be a basis of $\mathcal{F}(S)$. These are related by a transformation matrix $M \in k(x)^{n \times n}$ such that $(\beta_1, \ldots, \beta_n) \cdot M = (\alpha_1, \ldots, \alpha_n)$. We are interested in a basis $v_1, \ldots, v_n$ of $\mathcal{F}(V_0)$ such that $v_1\, x^{d_1}, \ldots, v_n\, x^{d_n}$ is a basis of $\mathcal{F}(S)$ and thus $v_1\, x^{d_1+r}, \ldots, v_n\, x^{d_n+r}$ is basis of $x^r \mathcal{F}(S)$. If we find such $v_1, \ldots, v_n$, then Lemma 4.3.12 (ii) already implies the assertion. To produce such a basis, let $g \in k[x]$ be a common denominator of the entries of M, i.e. gM is defined over $k[x]$. Now reduce the matrix gM by running RedMat, see Theorem A.2.7 and note Remark A.2.9, and then multiply the result with g^{-1} and call it N with column degrees $-d_i$. Note that N is reduced in the sense of Lemma 4.3.14. Since RedMat returns a matrix right equivalent to gM, $(v_1, \ldots, v_n) := (\beta_1, \ldots, \beta_n) \cdot N$ is again a basis of $\mathcal{F}(V_0)$. We multiply from the right with $\operatorname{diag}(x^{d_i})$ (this is just division of each column u_i by $x^{\deg(u_i)}$) and obtain $(v_1, \ldots, v_n) \cdot \operatorname{diag}(x^{d_i}) = (\beta_1, \ldots, \beta_n) \cdot N \cdot \operatorname{diag}(x^{d_i})$. By Lemma 4.3.14, $N \cdot \operatorname{diag}(x^{d_i})$ is unimodular over $\mathcal{O}_\infty$. This shows that $v_1 x^{d_1}, \ldots, v_n x^{d_n}$ is an $\mathcal{O}_\infty$-basis of $\mathcal{F}(S)$ and thus that $v_1 x^{d_1+r}, \ldots, v_n x^{d_n+r}$ is one of $x^r \mathcal{F}(S)$. Now Lemma 4.3.12 (ii) provides the assertion. The uniqueness of the d_i is proven in [Hes02]. □

Corollary 4.3.16. *We have*

$$\dim_k H^0(X, \mathcal{F}) = \sum_{|\mathcal{F}|_i \geq 0} (|\mathcal{F}|_i + 1) \geq \#\{i \in \{1, \ldots, n\} : |\mathcal{F}|_i = 0\}.$$

In particular,

$$\dim_k H^0(X, \mathcal{O}_X) \geq \#\{i \in \{1, \ldots, n\} : |X|_i = 0\} \quad \text{and} \quad |X|_1 \geq 0.$$

Proof. We apply Theorem 4.3.15 with $\mathcal{F} = \mathcal{O}_X$ and $r = 0$. This already provides the first assertion. The second follows immediately from the first and the fact that $\dim_k H^0(X, \mathcal{O}_X) \geq 1$. □

Definition 4.3.17. Let us from now on denote a reduced basis of $\mathcal{O}_X$ by $\Omega = (\omega_1, \ldots, \omega_n)$ and its corresponding basis of R_∞ by $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n$ with $\widetilde{\omega}_i = \omega_i x^{|X|_i}$. △

Definition 4.3.18. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Every $k[x]$-basis $\alpha_1, \ldots, \alpha_n$ of $\mathcal{F}(V_0)$ has a basis transformation matrix, which we usually denote by $T_\mathcal{F} = (\lambda_{i,j})_{i,j}$, satisfying

$$(\alpha_1, \ldots, \alpha_n) = \Omega \cdot T_\mathcal{F} = (\omega_1, \ldots, \omega_n) \cdot T_\mathcal{F},$$

by which we mean that $\alpha_j = \sum_{i=1} \lambda_{i,j}\omega_i$ for all $j = 1, \ldots, n$. After fixing the basis Ω, by Proposition 4.2.9, we can consider $T_\mathcal{F}$, independent of the basis itself, as the representation of the R_0-module $\mathcal{F}(V_0)$. △

Remark 4.3.19. From Theorem 4.3.15 we immediately deduce that $r \geq |\mathcal{F}|_i$ holds if and only if increasing r by one increases the dimension of $\mathcal{F}(r(x)_\infty)(X)$ by at least i, that is

$$r \geq -|\mathcal{F}|_i \Leftrightarrow \dim_k \mathcal{F}((r+1)(x)_\infty)(X) - \mathcal{F}(r(x)_\infty)(X) \geq i. \tag{3:5}$$

To be more precise, we have

$$\dim_k \mathcal{F}((r+1)(x)_\infty)(X) - \mathcal{F}(r(x)_\infty)(X) = \#\{i : r \geq -|\mathcal{F}|_i\}. \tag{3:6}$$

Moreover, $\mathcal{F}(r(x)_\infty)(X) \neq 0$ if and only if $r \geq -|\mathcal{F}|_1$. △

Corollary 4.3.20. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal such that $\mathcal{F}(S) = x^s \mathcal{O}_S$ and $\mathcal{F}(V_0) \subseteq R_0$. Let $T_\mathcal{F}$ denote the basis matrix of some $k[x]$-basis of $\mathcal{F}(V_0)$. Then* $\operatorname{diag}(x^{-|X|_i - s}) \cdot T_\mathcal{F}$ *is a basis transformation matrix from a basis of $\mathcal{F}(S)$ to one of $\mathcal{F}(V_0)$. Moreover, then*

(i) the degree of column i of $\textsc{RedMat}(\operatorname{diag}(x^{-|X|_i}) \cdot T_\mathcal{F}) \cdot x^{-s}$ *is equal to $|\mathcal{F}|_i$, and*

(ii) $\operatorname{diag}(x^{|X|_i}) \cdot \textsc{RedMat}(\operatorname{diag}(x^{-|X|_i}) \cdot T_\mathcal{F})$ *is the basis matrix of a reduced basis of $\mathcal{F}(V_0)$.*

Proof. Let $T_\mathcal{F}$ be the basis matrix of $\mathcal{F}(V_0)$ corresponding to the basis $\alpha_1, \ldots, \alpha_n$. Thus we have $(x^s\, \widetilde{w}_1, \ldots, x^s\, \widetilde{w}_n) \cdot \operatorname{diag}(x^{-|X|_i - s}) \cdot T_\mathcal{F} = (\alpha_1, \ldots, \alpha_n)$ and hence the desired transformation matrix is given by $\operatorname{diag}(x^{-|X|_i - s}) \cdot T_\mathcal{F}$ as asserted. Then with $N := \textsc{RedMat}(\operatorname{diag}(x^{-|X|_i}) \cdot T_\mathcal{F}) \cdot x^{-s}$ the proof of Theorem 4.3.15 together with noticing that the degrees of the columns of N will be the π-invariants of $\mathcal{F}$ provides (i). Again, following the proof of Theorem 4.3.15 and noticing that $\beta_i = x^s \widetilde{\omega}_i$ provides that $(x^s\, \widetilde{w}_1, \ldots, x^s\, \widetilde{w}_n) \cdot N$ is a reduced basis of $\mathcal{F}(V_0)$, that is, $\operatorname{diag}(x^{|X|_i}) \cdot \textsc{RedMat}(\operatorname{diag}(x^{-|X|_i}) \cdot T_\mathcal{F})$ is a basis matrix of that reduced basis. □

The insights of Corollary 4.3.20 immediately provide algorithms both to compute a basis matrix $T_\mathcal{F}$ of a reduced basis of $\mathcal{F}(V_0)$ and the π-invariants of $\mathcal{F}$ for an $\mathcal{O}_X$-ideal $\mathcal{F}$ given by an arbitrary basis matrix of $\mathcal{F}(V_0)$.

Algorithm 1 Computing basis matrix of a reduced basis

Precomputed	Reduced basis Ω of R_0; π-invariants $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ of X
Input	T basis matrix of $\mathcal{F}(V_0)$ where $\mathcal{F}$ is $\mathcal{O}_X$-ideal
Output	$T_\mathcal{F}$ basis matrix of $\mathcal{F}(V_0)$ representing a reduced basis

1: **procedure** $\textsc{RedBasMat}(T)$
2: $\quad T \leftarrow \textsc{ScaleRows}(T, x^{-|X|_1}, \ldots, x^{-|X|_n})$
3: $\quad T \leftarrow \textsc{RedMat}(T)$
4: $\quad$ **return** $\textsc{ScaleRows}(T, x^{|X|_1}, \ldots, x^{|X|_n})$

Algorithm 2 Computing π-invariants of $\mathcal{O}_X$-ideal

Precomputed	Reduced basis Ω of R_0; π-invariants $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ of X
Input	T basis matrix of $\mathcal{F}(V_0)$ where $\mathcal{F}$ is $\mathcal{O}_X$-ideal
Output	π-invariants $-\lvert\mathcal{F}\rvert_1 \leq \ldots \leq -\lvert\mathcal{F}\rvert_n$ of $\mathcal{F}$

1: **procedure** PiInvariants(T)
2: $s \leftarrow$ Degree(Determinant(T))
3: $T \leftarrow$ ScaleRows($T, x^{-\lvert X\rvert_1}, \ldots, x^{-\lvert X\rvert_n}$)
4: $T \leftarrow$ RedMat(T)
5: **for** $j = 1, \ldots, n$ **do**
6: $d_j \leftarrow$ Degree(SubMatrix($T, (1, j), (n, 1)$))
7: **return** $d_1 + s, \ldots, d_n + s$

Lemma 4.3.21. *The algorithms* RedBasMat *and* PiInvariants*, see Algorithm 1 respectively Algorithm 2, are correct. Moreover, if d is an upper bound for both $-\lvert X\rvert_n$ and the degree of the input matrix, then they both require at most $O^{\sim}(n^{\omega}d)$ operations in k. Moreover,* RedBasMat *returns a matrix with degree bounded by $2d$.*

Proof. The correctness of both algorithms follows from Corollary 4.3.20. Let us first consider the running time assertion of RedBasMat and the assertion regarding the output degree. By assumption, d is both an upper bound of $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ and of $\deg M$. Thus by Lemma A.1.2 (i), ScaleRows at line 2 requires at most $O^{\sim}(n^{\omega}d)$ operations in k and returns a matrix with degree bounded by $2d$. By Theorem A.2.7, RedMat thus requires at most $O^{\sim}(n^{\omega}d)$ operations in k and returns a matrix with degree bounded by $2d$ as well. Thus the argument from above applies again and ScaleRows at line 4 also requires at most $O^{\sim}(n^{\omega}d)$ operations in k. This proves both the assertion about the output degree as well as the running time assertion of RedBasMat.

By Lemma A.1.2 (ii), Determinant requires at most $O^{\sim}(n^{\omega}d)$ operations in k whereby Degree has constant cost, see Lemma A.1.2 (iv). As we have shown above, the calls of ScaleRows and RedMat in line 3 and 4 require at most $O^{\sim}(n^{w}d)$ operations in k and both return a matrix with degree bounded by $2d$. By Lemma A.1.2 (vi), SubMatrix has constant cost which finally provides the assertion. □

Assume for a moment that X is an integral and a local complete intersection (e.g. non-singular) projective scheme of dimension one over k. By K we denote a canonical divisor on X. Then for any divisor $D \in \operatorname{Div}(X)$ the Riemann-Roch space of $K - D$ (whose dimension equals that of $H^1(X, D)$) vanishes whenever $\deg_k D > \deg_k K$. This, together with the Riemann-Roch equation provides an explicit description of the dimension of the Riemann-Roch space of D solely dependent on $\deg_k D$ and the arithmetic genus of X whenever $\deg_k D > \deg_k K$. The following theorem generalises this to quite arbitrary integral projective schemes of dimension one over a field and to more general sheaves as well. The proof uses the theory of the dualising sheaf which we present in Chapter E of the appendix.

Theorem 4.3.22. *Let X be an integral projective scheme of dimension one over the field k. Let $\mathcal{F}$ be a coherent and torsion-free $\mathcal{O}_X$-module which is invertible at the generic point of X (i.e. $\mathcal{F}$ is isomorphic to an $\mathcal{O}_X$-ideal). Then $\deg_k \mathcal{F} < -2g - \dim_k H^0(X, \mathcal{O}_X)$ implies $H^1(X, \mathcal{F}) = 0$.*

Proof. By Lemma C.4.4, we have $\deg_k \mathcal{F} = -g - \chi(\mathcal{F})$ which implies

$$\deg_k \mathcal{F} \geq -g - \dim_k H^0(X, \mathcal{F}). \tag{3:7}$$

Assume that $0 \neq \dim_k H^1(X, \mathcal{F}) = \dim_k H^0(X, \mathcal{F}^*)$ where $\mathcal{F}^* = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$, see [Liu02, 6.4.20]. Then there is some non-zero $f \in \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$ which we claim to be injective: By [Sta18, Tag 0AVL], f is injective if f_P is injective for all $P \in \mathrm{Ass}(\mathcal{F})$. Since $\mathcal{F}$ is torsion-free, the latter is a subset of the generic points of X, see Lemma B.4.23, and hence we only need to show that f_η is injective for the generic point η of X. By Proposition E.1.19, we know that $\omega_{X,\eta} \neq 0$. Since X is integral, it is a fortiori reduced and thus Cohen-Macaulay. Hence, by Corollary E.1.15, we know that ω_X is torsion-free and since it is quasi-coherent, the same is true for $\omega_{X,\eta}$. By assumption, $\mathcal{F}_\eta$ is invertible and hence f_η is characterised by the image of the generator of $\mathcal{F}_\eta$. In particular, by assumption that image is not zero. Now the torsion-freeness of $\omega_{X,\eta}$ implies that f_η is injective. Thus f provides

$$\begin{aligned}\dim_k H^0(X, \mathcal{F}) &\leq \dim_k H^0(X, \omega_X) \\ &= \dim_k H^1(X, \mathcal{O}_X) \\ &= \dim_k H^0(X, \mathcal{O}_X) + g\end{aligned}$$

and this together with the Eq. (3:7) implies

$$\deg_k \mathcal{F} \geq -2g - \dim_k H^0(X, \mathcal{O}_X) = -g - \dim_k H^1(X, \mathcal{O}_X).$$

Therefore, $\deg_k \mathcal{F} < -2g - \dim_k H^0(X, \mathcal{O}_X)$ implies $H^1(X, \mathcal{F}) = 0$ as asserted. □

Whenever X is integral, we can use Theorem 4.3.22 to give some effective bounds for the π-invariants of $\mathcal{O}_X$-ideals.

Theorem 4.3.23. *Let X be an integral cover of $\mathbb{P}^1_k$. Then for any $\mathcal{O}_X$-ideal $\mathcal{F}$ its π-invariants satisfy*

(i) $\left\lceil \frac{\deg_k \mathcal{F}}{n} \right\rceil \leq -|\mathcal{F}|_1 \leq \ldots \leq -|\mathcal{F}|_n \leq \left\lceil \frac{\deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil$ *and*

(ii) $-|\mathcal{F}|_1 < \left\lceil \frac{\deg_k \mathcal{F} + g}{n} \right\rceil$.

Proof. We have $\deg_k \mathcal{F} = -g - \chi(\mathcal{F})$ and hence

$$\deg_k \mathcal{F}(r(x)_\infty) = \dim_k H^1(X, \mathcal{F}(r(x)_\infty)) - \dim_k H^0(X, \mathcal{F}(r(x)_\infty)) - g \tag{3:8}$$

and by Theorem 4.3.22, we know that $\dim_k H^1(X, \mathcal{F}(r(x)_\infty)) = 0$ as soon as $\deg_k \mathcal{F}(r(x)_\infty) < -2g - \dim_k H^0(X, \mathcal{O}_X)$. By Proposition D.2.10, we have

$$\deg_k \mathcal{F}(r(x)_\infty) = \deg_k \mathcal{F} - rn. \tag{3:9}$$

Therefore, the condition for $\dim_k H^1(X, \mathcal{F}(r(x)_\infty))$ to vanish becomes

$$\begin{aligned}&\deg_k \mathcal{F} - rn < -2g - \dim_k H^0(X, \mathcal{O}_X) \\ \Leftrightarrow\ &\deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X) < rn.\end{aligned}$$

Hence, for

$$r \geq \left\lceil \frac{\deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil \tag{3:10}$$

Eq. (3:8) becomes

$$\deg_k \mathcal{F} - rn = -\dim_k H^0(X, \mathcal{F}(r(x)_\infty)) - g$$

which is equivalent to

$$\dim_k H^0(X, \mathcal{F}(r(x)_\infty)) = -\deg_k \mathcal{F} + rn - g. \tag{3:11}$$

Now for r in the given order of magnitude as in Eq. (3:10) we have $rn - \deg_k \mathcal{F} \geq -2g$ and hence the right hand side of Eq. (3:11) is positive and thus increasing r by 1 in Eq. (3:11) does indeed increase $\dim_k H^0(X, \mathcal{F}(r(x)_\infty))$ by exactly rn. By Remark 4.3.19, this implies $r \geq -|\mathcal{F}|_n$ which proves the upper bound in (i).

To prove the lower bound in (i), note that by Remark 4.3.19, we have $\mathcal{F}(r(x)_\infty)(X) = 0$ if and only if $r < -|\mathcal{F}|_1$. Now Lemma C.4.6 provides that $\deg_k \mathcal{F}(r(x)_\infty) > 0$ already implies $H^0(X, \mathcal{F}(r(x)_\infty)) = 0$. By Eq. (3:9), we have $\deg_k \mathcal{F}(r(x)_\infty) = \deg_k \mathcal{F} - rn$ and thus $r < \left\lceil \frac{\deg_k \mathcal{F}}{n} \right\rceil$ is sufficient and hence the lower bound in (i) follows.

By Remark 4.3.19, $-|\mathcal{F}|_1 \leq r$ is equivalent to $\mathcal{F}(r(x)_\infty)(X) \neq 0$. Hence to find an upper bound for $-|\mathcal{F}|_1$ we are looking for a sufficiently large r such that the dimension of $\mathcal{F}(r(x)_\infty)(X)$ is at least one. From Eq. (3:8), we deduce

$$\begin{aligned}
\dim_k H^0(X, \mathcal{F}(r(x)_\infty)) &= \dim_k H^1(X, \mathcal{F}(r(x)_\infty)) - \deg_k \mathcal{F}(r(x)_\infty) - g \\
&\geq -\deg_k \mathcal{F}(r(x)_\infty) - g \\
\text{Proposition D.2.10} \rightsquigarrow &= -\deg_k \mathcal{F} + rn - g \\
&> 0
\end{aligned}$$

if $r > (\deg_k \mathcal{F} + g)/n$ which provides (ii). □

Corollary 4.3.24. *Let X be an integral cover of $\mathbb{P}^1_k$. Then we have*

$$0 = -|X|_1 \leq \ldots \leq -|X|_n \leq \left\lceil \frac{2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil \leq c_X.$$

Proof. All inequalities follow from plugging in $\mathcal{O}_X$ for $\mathcal{F}$ in Theorem 4.3.23 and noting that $\deg_k \mathcal{O}_X = 0$. Moreover, this also shows $|X|_1 \leq 0$. By Corollary 4.3.16, we have $|X|_1 \geq 0$ and combining this with the above provides $|X|_1 = 0$. The last inequality follows from the Definition 2.4.10 of c_X in the integral case. □

That $|X_i|_1$ vanishes for every irreducible component of a reduced cover of $\mathbb{P}^1_k$ also shows that the same is true for $|X|_1$.

Corollary 4.3.25. *Let X be an reduced cover of $\mathbb{P}^1_k$. Then $|X|_1 = 0$.*

Proof. By Corollary 4.3.16, we have $|X|_1 \geq 0$ and thus we are left to show that $|X|_1 \leq 0$. Assume $|X|_1 > 0$, then both ω_1 and $x\omega_1$ lie in $\mathcal{O}_X(X)$. By Corollary 4.3.24, we have $|X_i|_1 = 0$ for all irreducible components $X_1, \ldots, X_m$ of X. This provides that for all $i = 1, \ldots, m$ we have $\dim_k \mathcal{O}_{X_i}(X_i) = 1$. Since ω_1 is non-zero, there is an irreducible component X_i such that $(\omega_1)_{|X_i}$ is non-zero as well. The same then holds for $(x\omega_1)_{|X_i}$. But since $\dim_k \mathcal{O}_{X_i}(X_i) = 1$, $(\omega_1)_{|X_i}$ and $(x\omega_1)_{|X_i}$ are linearly dependent over k which provides $(\lambda - x)(\omega_1)_{|X_i} = 0$ for some $\lambda \in k$ and hence $x = \lambda$, a contradiction. □

Proposition 4.3.26. *Let $\mathcal{F}$ and $\mathcal{G}$ be two $\mathcal{O}_X$-ideals such that $\mathcal{F}(V_0) \subseteq \mathcal{G}(V_0)$ and $\mathcal{F}(S) \subseteq x^s \mathcal{G}(S)$ for some $s \in \mathbb{Z}$. Then $-|\mathcal{F}|_n \geq -|\mathcal{G}|_n - s$. Moreover, the basis transformation matrix from a reduced basis of $\mathcal{G}$ to a reduced basis of $\mathcal{F}$ has degree bounded by $-|\mathcal{F}|_n + s + |\mathcal{G}|_1$. In particular, if X is integral, then the above basis matrix has degree bounded by $s + c_X + \frac{-\deg_k \mathcal{G} + \deg_k \mathcal{F} + n}{n}$.*

Proof. Let $\beta_1, \dots, \beta_n$ be a reduced basis of $\mathcal{G}$ and let $\alpha_1, \dots, \alpha_n$ be a reduced basis of $\mathcal{F}$. Then there is a basis transformation matrix $T = (\lambda_{i,j})_{i,j} \in k[x]^{n\times n}$ of full rank such that

$$(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n) \cdot T.$$

By assumption and Lemma 4.2.8, we have

$$\mathcal{F}(r(x)_\infty)(X) = \mathcal{F}(V_0) \cap x^r \mathcal{F}(S) \subseteq \mathcal{G}(V_0) \cap x^{r+s}\mathcal{G}(S) = \mathcal{G}((r+s)(x)_\infty)(X). \tag{3:12}$$

Now set $r = -|\mathcal{F}|_n$. Then by the reducedness of $\alpha_1, \dots, \alpha_n$, we have $\alpha_1, \dots, \alpha_n \in \mathcal{F}(r(x)_\infty)(X)$ as well as $\alpha_1, \dots, \alpha_n \in \mathcal{G}((r+s)(x)_\infty)(X)$ by Eq. (3:12). Reducedness of $\beta_1, \dots, \beta_n$ yields

$$\mathcal{G}(V_0) \cap x^{r+s}\mathcal{G}(S) = \left\{ \sum_{i=1}^{n} \lambda_i \beta_i \mid \lambda_i = 0 \text{ or } 0 \le \deg(\lambda_i) \le r + s + |\mathcal{G}|_i \right\}.$$

In particular, $\alpha_i = \sum_{j=1}^{n} \lambda_{i,j}\beta_j$ with $\lambda_{i,j} = 0$ or $\deg(\lambda_{i,j}) \le r + s + |\mathcal{G}|_j$. Now for every $j = 1, \dots, n$ there is some i such that $\lambda_{i,j} \neq 0$. Otherwise, there is some β_j not appearing in any of the linear combinations of the α_i implying that T cannot have full rank. Therefore, for every $j = 1, \dots, n$ there is some $\lambda_{i,j} \neq 0$ and thus we have $0 \le \deg(\lambda_{i,j}) \le r + s + |\mathcal{G}|_j$. This provides $-|\mathcal{F}|_n + s = r + s \ge -|\mathcal{G}|_j$ for all $j = 1, \dots, n$. Since $|\mathcal{G}|_1 \ge \dots \ge |\mathcal{G}|_n$ this implies $-|\mathcal{F}|_n + s \ge -|\mathcal{G}|_n$.

Moreover, all non-zero $\lambda_{i,j}$ have degree bounded by $-|\mathcal{F}|_n + s + |\mathcal{G}|_j \le -|\mathcal{F}|_n + s + |\mathcal{G}|_1$. We conclude that

$$\deg(T) = \max\{\deg(\lambda_{i,j}) \mid i, j \in \{1, \dots, n\}\} \le -|\mathcal{F}|_n + s + |\mathcal{G}|_1.$$

Now if X is integral, then by Theorem 4.3.23 (i), we have $|\mathcal{G}|_1 \le -\left\lceil \frac{\deg_k \mathcal{G}}{n} \right\rceil$ and

$$-|\mathcal{F}|_n \le \left\lceil \frac{\deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil$$

which yields

$$\begin{aligned}
\deg(T) &\le s - \left\lceil \frac{\deg_k \mathcal{G}}{n} \right\rceil + \left\lceil \frac{\deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil \\
&\le s + \frac{-\deg_k \mathcal{G} + \deg_k \mathcal{F} + 2g + \dim_k H^0(X, \mathcal{O}_X) + 2n}{n} \\
&\le s + c_X + \frac{-\deg_k \mathcal{G} + \deg_k \mathcal{F} + n}{n}.
\end{aligned}$$

□

Corollary 4.3.27. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal such that $\mathcal{F}(V_0) \subseteq R_0$ and $\mathcal{F}(S) = x^s\mathcal{O}_S$. Then $-|\mathcal{F}|_n \ge -|X|_n - s$. Moreover, the basis transformation matrix T from a reduced basis of $\mathcal{O}_X$ to a reduced basis of $\mathcal{F}$ has degree bounded by $-|\mathcal{F}|_n + s$. In particular, if X is integral, then the above matrix has degree bounded by $s + \frac{\deg_k \mathcal{F}}{n} + c_X$. If furthermore $\deg_k \mathcal{F} = 0$, then $\deg T \le \frac{\deg_k \mathcal{F}(V_0)}{n} + c_X$. Moreover, in this case $-|\mathcal{F}|_n \ge -|X|_n - \frac{\deg_k \mathcal{F}(V_0)}{n}$*

Proof. This is Proposition 4.3.26 with $\mathcal{G} = \mathcal{O}_X$. The particular part follows from Corollary C.4.13, together with Corollary D.2.9 which tell us that $\deg_k \mathcal{F}(V_0) = -\deg_k \mathcal{F}(S)$ and $\deg_k \mathcal{F}(S) = \deg_k x^s\mathcal{O}_S = -sn$. □

Lemma 4.3.28. *Let X be an integral cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Let $T_\mathcal{F}$ be any basis transformation matrix from a fixed reduced basis Ω of $\mathcal{O}_X$ to any basis of $\mathcal{F}(V_0)$, see*

Definition 4.3.18. Then $T_{\mathcal{F}}$ satisfies

$$\deg(\textsc{RedMat}(T_{\mathcal{F}})) \leq \frac{\deg_k \mathcal{F}(V_0)}{n} + c_X.$$

Moreover, if d is both an upper bound of $\deg(T_{\mathcal{F}})$, then the computation of $\textsc{RedMat}(T_{\mathcal{F}})$ requires at most $O^{\sim}(n^{\omega}d)$ operations in k.

Proof. By Theorem A.2.7, we know that $\textsc{RedMat}(T_{\mathcal{F}})$ has minimal column degrees among all $k[x]$-right equivalent matrices of $T_{\mathcal{F}}$. Now the matrix T from Corollary 4.3.27 is among these right equivalent matrices and thus $\deg(T)$ provides the asserted upper bound. By Corollary A.2.8, $\textsc{RedMat}$ requires at most $O^{\sim}(n^{\omega}d)$ operations in k where d is an upper bound of the degree of $T_{\mathcal{F}}$. □

Lemma 4.3.29. *Let $\Omega = (\omega_1, \ldots, \omega_n)$ be a reduced basis of $\mathcal{O}_X$. Without loss of generality we can assume that $\omega_1 = 1$.*

Proof. By Corollary 4.3.25, we have $|X|_i \leq 0$ for all $i = 1, \ldots, n$. Let $m = \dim_k \mathcal{O}_X(X)$. Hence, by Theorem 4.3.15, we know that $\omega_1, \ldots, \omega_m$ will span all of $\mathcal{O}_X(X)$ with coefficients in k. In particular, there are $\mu_i \in k$ such that $1 = \sum_{i=1}^{m} \mu_i \omega_i$. Without loss of generality we assume that $\mu_1 \neq 0$. Then we interchange ω_1 for 1 and see that we still have a $k[x]$-basis of $\mathcal{O}_X(V_0)$ since

$$\omega_1 = \mu_1^{-1} \cdot 1 + \sum_{i=2}^{m} \mu_i \mu_1^{-1} \omega_i \tag{3:13}$$

provides that we can still generate ω_1 over $k[x]$. Next we show that the new basis is still reduced in the sense of Theorem 4.3.15. To see this, it is enough to ensure that for arbitrary $r \in \mathbb{Z}$ every element of $\mathcal{O}_X(r(x)_\infty))(X)$ can be uniquely written as a $k[x]$-linear combination $\lambda_1 \cdot 1 + \lambda_2\omega_2 + \ldots + \lambda_n\omega_n$ with coefficients $\lambda_i \in k[x]$ such that $\deg \lambda_i \leq r + |X|_i$. Note that by assumption, the same is true for the elements $\omega_1, \ldots, \omega_n$. So let $a = \sum_{i=1}^{n} \lambda_i \omega_i \in \mathcal{O}_X(r(x)_\infty))(X)$ with $\deg \lambda_i \leq r + |X|_i$ be arbitrary. Now we substitute ω_1 following Eq. (3:13) and obtain

$$\begin{aligned} a = \sum_{i=1}^{n} \lambda_i \omega_i &= \lambda_1(\mu_1^{-1} \cdot 1 + \sum_{i=2}^{n} \mu_i \mu_1^{-1} \omega_i) + \sum_{i=2}^{n} \lambda_i \omega_i \\ &= \lambda_1 \mu_1^{-1} \cdot 1 + \sum_{i=2}^{n} (\lambda_i + \mu_i \mu_1^{-1}) \omega_i \end{aligned}$$

which tells us that $1, \omega_2, \ldots, \omega_n$ also generate $\mathcal{O}_X(r(x)_\infty))(X)$ as desired. □

Definition 4.3.30. Combining Lemma 4.2.8 and the definition of the pole divisor $(x)_\infty$ of x, see Definition 2.2.9, we see that $\mathcal{O}_X(r(x)_\infty)(X) = R_0 \cap x^r \mathcal{O}_S$. For $f \in R_0$ we define $\deg^*(f) = \min\{r \in \mathbb{Z} \mid f \in \mathcal{O}_X(r(x)_\infty)(X)\}$. △

We collect immediate consequences of the definition of $\deg^*$.

Corollary 4.3.31. *Let $\lambda \in k[x]$ and $f, g \in R_0$. Then*

(i) $\deg^*(\lambda) = \deg \lambda$,

(ii) $\deg^*(\omega_i) = -|X|_i$, *and*

(iii) $\deg^*(fg) \leq \deg^*(f) + \deg^*(g)$.

Proof. By Lemma 4.3.29, without loss of generality we have $\omega_1 = 1$. Moreover, by Corollary 4.3.24, we also have $|X|_1 = 0$. Hence, by Theorem 4.3.15, we have $\lambda \in \mathcal{O}_X(r(x)_\infty)(X)$ if and only if $\deg \lambda \leq r$ which provides (i). Property (ii) follows immediately from Theorem 4.3.15. To prove (iii), assume that $f \in x^r\mathcal{O}_S$ and $g \in x^s\mathcal{O}_S$ both numbers r, s being minimal with this property, that is $\deg^*(f) = r$ and $\deg^*(g) = s$. In particular, $fg \in R_0 \cap x^{r+s}\mathcal{O}_S$ and thus $\deg^*(fg) \leq r + s$ which finally provides (iii). □

Lemma 4.3.32. *Let $f = \sum_{i=1}^n \lambda_i\omega_i \in R_0$. Then*

$$\deg^*(f) + |X|_n \leq \deg \phi_\Omega(f) \leq \deg^*(f).$$

Proof. Theorem 4.3.15 tells us that $f \in R_0$ with $\lambda_i \in k[x]$ lies in $\mathcal{O}_X(r(x)_\infty)(X)$ if and only if $\deg \lambda_i \leq r + |X|_i$ for all $i = 1, \ldots, n$. Let $d = \deg \phi_\Omega(f)$. Then $r \geq d - |X|_n$ guarantees $f \in \mathcal{O}_X(r(x)_\infty)(X)$ and hence $\deg^*(f) \leq d - |X|_n$ providing the first inequality.

Let $r = \deg^*(f)$. Then $f \in \mathcal{O}_X(r(x)_\infty)(X)$ and thus $\deg \lambda_i \leq r + |X|_i$ for all $i = 1, \ldots, n$. Now since $|X|_i \leq 0$, see Corollary 4.3.16 and Theorem 4.3.15, we deduce $\deg \lambda_i \leq r$ for all $i = 1, \ldots, n$ and thus $\deg \phi_\Omega(f) \leq \deg^*(f)$ as asserted. □

Definition 4.3.33. The coefficients $\mu_{i,j,\ell} \in k[x]$ defined by $\omega_i\omega_j = \sum_{\ell=1}^n \mu_{i,j,\ell}\omega_\ell$ define the **multiplication table** given by the 3-dimensional array $(\mu_{i,j,\ell})_{i,j,\ell}$. △

Lemma 4.3.34. *The entries $\mu_{i,j,\ell}$ of the multiplication table satisfy*

$$\deg \mu_{i,j,\ell} \leq -|X|_i - |X|_j \leq -2|X|_n.$$

In particular, if X is integral, then

$$\deg \mu_{i,j,\ell} \leq 2\left\lceil \frac{2g + \dim_k H^0(X, \mathcal{O}_X)}{n} \right\rceil \leq 2c_X.$$

Proof. By Corollary 4.3.31 (ii), we have $\deg^*(\omega_i) = -|X|_i$. Moreover, Corollary 4.3.31 (iii) then provides $\deg^*(\omega_i\omega_j) \leq \deg^*(w_i) + \deg^*(w_j) = -|X|_i - |X|_j$. In particular, $\deg^*(\omega_i\omega_j) \leq -2|X|_n$. The particular part follows from Corollary 4.3.24 and the definition of c_X, see Definition 2.4.10. □

Lemma 4.3.35. *Let X be a cover of $\mathbb{P}^1_k$. Let $\Omega = (\omega_1, \ldots, \omega_n)$ be a reduced basis of $\mathcal{O}_X$. Let $f \in R_0$ with $\deg \phi_\Omega(f) \leq d$. Then the $k[x]$-basis $f\Omega = (f\omega_1, \ldots, f\omega_n)$ of fR_0 has a basis matrix T_f with $\deg(T_f) \leq d - 2|X|_n$. In particular, if X is integral, then $\deg(T_f) \leq d + 2c_X$.*

Proof. By definition, the j-th column of a basis matrix T_f of $f\Omega$ contains the coefficients of $f\omega_j$ with respect to Ω. If $f = \sum_{i=1}^n \lambda_i\omega_i$, then

$$f\omega_j = \sum_{i=1}^n \lambda_i\omega_i\omega_j = \sum_{i=1}^n \lambda_i \sum_{\ell=1}^n \mu_{i,j,\ell}\omega_\ell = \sum_{\ell=1}^n \left(\sum_{i=1}^n \lambda_i\mu_{i,j,\ell} \right) \omega_\ell.$$

By Lemma 4.3.34, we have $\deg \mu_{i,j,\ell} \leq -2|X|_n$ and by assumption $\deg(\lambda_i) \leq d$. Thus the j-th column of T_f has degree bounded by $d - 2|X|_n$ and thus the same is true for all of T_f. The particular part follows from Lemma 4.3.34. □

In general, if X is not integral and decomposes into several irreducible components, then it is not at all clear how to come up with bounds for both the π-invariants of X or $\mathcal{F}$ and the degree of basis matrices of reduced bases of $\mathcal{F}(V_0)$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal. In the next section we will investigate in how to come up with bases of $\mathcal{F}(V_0)$ that are not too far away from inducing reduced bases of $\mathcal{F}_{|X_i}(V_{i,0})$ on the components X_i of X.

4.4 $\mathcal{O}_X$-Ideals on Reducible Schemes

In this section we will explicitly assume that X is a reducible and reduced cover of $\mathbb{P}^1_k$ with irreducible components $X_1, \dots, X_m$. It turns out that we can restrict an $\mathcal{O}_X$-ideal $\mathcal{F}$ to an irreducible component X_i such that it is isomorphic to some $\mathcal{O}_{X_i}$-ideal $\mathcal{F}_{|X_i}$. Similarly to the injection

$$\mathcal{O}_X \longrightarrow \bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{O}_{X_i} \tag{4:14}$$

this will provide an injection

$$\mathcal{F} \longrightarrow \bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{F}_{|X_i}. \tag{4:15}$$

As we have already seen in this chapter, after fixing bases we can represent the sections of $\mathcal{F}$ over V_0 via a basis with respect to a basis of $\mathcal{O}_X$ over V_0 and we can do the same for the sections of $\mathcal{F}_{|X_i}$ over $V_{i,0}$ with respect to the sections of $\mathcal{O}_{X_i}$ over $V_{i,0}$ for all $i = 1, \dots, m$. Then the embeddings in Eqs. (4:14) and (4:15) provide that we can relate the above bases.

4.4.1 Connection to the Restrictions to Components

Lemma 4.4.1. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\mathcal{F}_{|X_i}$, see Definition 3.2.25, is isomorphic to some $\mathcal{O}_{X_i}$-ideal.*

Proof. By Lemma D.2.5, we know that V_0 is schematically dense in X. In particular, it contains all generic points $\eta_1, \dots, \eta_m \in X^0$ of X. By the quasi-coherence of $\mathcal{F}$, we therefore obtain $\mathcal{F}(V_0)_{P_{i,0}} \cong \mathcal{F}_{\eta_i} \cong \mathcal{O}_{X,\eta_i} \cong (R_0)_{P_{i,0}}$ where $P_{i,0}$ is the minimal prime of R_0 corresponding to η_i. The restriction $\mathcal{F}_{|X_i}$ of $\mathcal{F}$ to X_i is quasi-coherent and due to Lemma 3.2.30, it moreover satisfies

$$\mathcal{F}_{|X_i}(V_{i,0}) \cong \mathcal{F}(V_0) \otimes_{R_0} R_0/P_{i,0} = \mathcal{F}(V_0)/P_{i,0}\mathcal{F}(V_0).$$

Now we may apply Corollary B.4.33 to $M = \mathcal{F}(V_0)$ which provides that $\mathcal{F}_{|X_i}(V_{i,0})$ and thus $\mathcal{F}_{|X_i}$ is also invertible at η_i. Now Lemma 4.1.2 tells us that the isomorphism $\mathcal{F}_{|X_i,\eta_i} \to \mathcal{O}_{X_i,\eta_i}$ provides an $\mathcal{O}_{X_i}$-module embedding of $\mathcal{F}_{|X_i}$ into $\mathcal{K}_{X_i}$. □

By Definition B.3.1, we can relate $\mathcal{F}$ with its restrictions $\mathcal{F}_{|X_i}$ to the X_i: Let $\tau_i : X_i \to X$ denote the closed immersion corresponding to X_i. Then by Definition 3.2.25, we have $\mathcal{F}_{|X_i} = \tau_i^* \mathcal{F}$. In particular, $(\tau_i)_* \mathcal{F}_{|X_i} = (\tau_i)_*(\tau_i^* \mathcal{F})$ and for the latter there is a canonical morphism $\mathcal{F} \to (\tau_i)_*(\tau_i^* \mathcal{F})$, see [GW10, 7.8.10]. Hence we obtain canonical morphisms $\mathcal{F} \to (\tau_i)_* \mathcal{F}_{|X_i}$ which thus induces a canonical morphism $\phi : \mathcal{F} \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{F}_{|X_i}$.

Proposition 4.4.2. *Let $\mathcal{F}$ be a quasi-coherent, torsion-free $\mathcal{O}_X$-module. The morphism $\phi : \mathcal{F} \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{F}_{|X_i}$ introduced above is injective.*

Proof. First of all, by Remark B.1.11, we know that ϕ is injective if and only if ϕ_P is injective for all $P \in X$. Let $P \in X$ be arbitrary with affine open neighborhood $U = \operatorname{Spec}(R)$. Let P_i denote the minimal prime ideals of R that correspond to the irreducible components X_i meeting U. Then the morphism τ_i restricted to U, denoted by $\tau_{U,i}$, is given by the ring homomorphism $R \to R/P_i$. Since $\mathcal{F}$ is quasi-coherent, there is a torsion-free R-module M with $\mathcal{F}_{|U} = M^\sim$. Now by Lemma 3.2.30, we have $\tau_{U,i}^* \mathcal{F}_{|U} \cong (M \otimes_R R/P_i)^\sim \cong (M/P_i M)^\sim$. By [GW10, 7.24 (1)], in turn we have

$$(\tau_{U,i})_*(\tau_{U,i}^* \mathcal{F}_{|U}) \cong (\tau_{U,i})_*(M \otimes_R R/P_i)^\sim \cong (M \otimes_R R/P_i)^\sim$$

where in the latter $M \otimes_R R/P_i$ is regarded as an R-module via the map $R \to R/P_i$. Hence the morphism

$$\phi(U) : \mathcal{F}(U) \to \bigoplus_{i:X_i \cap U \neq \emptyset} ((\tau_{U,i})_* \mathcal{F}_{|X_i \cap U})(U)$$

is given by

$$M \to \bigoplus_{i:X_i \cap U \neq \emptyset} \underbrace{M \otimes_R R/P_i}_{= M/P_i M}, \quad m \mapsto (m + P_i M)_i$$

which is injective due to Proposition B.4.37 and M being torsion-free. This provides that the induced morphism on the level of stalks at $P \in U$ will be injective. Since the affine open subsets form a base of the topology of X, this shows that ϕ_P is injective for all $P \in X$ and thus the assertion follows. □

Remark 4.4.3. By Lemma 4.4.1, we know that $\mathcal{F}_{|X_i}$ is isomorphic to some $\mathcal{O}_{X_i}$-ideal and thus embeds into $\mathcal{K}_{X_i}$. Combining this with Proposition 4.4.2 we see that we have the $\mathcal{O}_X$-module embeddings

$$\mathcal{F} \hookrightarrow \bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{F}_{|X_i} \hookrightarrow \bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{K}_{X_i} \cong \mathcal{K}_X. \tag{4:16}$$

△

Notation 4.4.4. From now on we will assume that every $\mathcal{O}_X$-ideal $\mathcal{F}$ is an $\mathcal{O}_X$-submodule of $\mathcal{K}_X$ via the embedding given by Eq. (4:16). In particular, we also assume this for the $\mathcal{O}_X$-ideal $\mathcal{O}_X$. △

Remark 4.4.5. Notation 4.4.4 enables us to relate the bases of $\mathcal{F}_{|X_i}(V_{i,0})$ and those of $R_{i,0} = \mathcal{O}_{X_i}(V_{i,0})$. Both are $R_{i,0}$-submodules of $\mathcal{K}_{X_i}(V_{i,0}) = \mathrm{Frac}(R_{i,0})$ and the latter is free of rank n_i over $k(x)$. Now every $k[x]$-basis $v_{i,1}, \ldots, v_{i,n_i}$ of $\mathcal{F}_{|X_i}(V_{i,0})$ provides a $k(x)$-basis of $\mathrm{Frac}(R_{i,0})$ and the same is true for any basis $\omega_{i,1}, \ldots, \omega_{i,n_i}$ of $R_{i,0}$. Hence there is a basis transformation matrix $T_{\mathcal{F}_i} \in k(x)^{n \times n}$ such that

$$(v_{i,1}, \ldots, v_{i,n_i}) \cdot T_{\mathcal{F}_i} = (\omega_{i,1}, \ldots, \omega_{i,n_i})$$

similar to Definition 4.3.18. △

Remark 4.4.5 enables us to represent the $k[x]$-module $\mathcal{F}_{|X_i}(V_{i,0})$ via a basis transformation matrix $T_{\mathcal{F}_i}$ by fixing a reduced $k[x]$-basis of $R_{i,0}$. Moreover, by Notation 4.4.4, we have embeddings of $k[x]$-modules

$$R_0 \hookrightarrow R_0^+ = \bigoplus_{i=1}^{m} R_{i,0} \quad \text{and} \quad \mathcal{F}(V_0) \hookrightarrow \bigoplus_{i=1}^{m} \mathcal{F}_{|X_i}(V_{i,0})$$

and we know that both R_0 and $\mathcal{F}(V_0)$ are also free of rank n over $k[x]$. In particular, there are $k[x]$-basis transformation matrices $T_{0,\mathcal{F}}$ from a basis of $\bigoplus_{i=1}^m \mathcal{F}_{|X_i}(V_{i,0})$ to one of $\mathcal{F}(V_0)$, and $T_{0,\mathcal{O}_X}$ from a basis of R_0^+ to one of R_0. Note that the bases $v_{i,1}, \ldots, v_{i,n_i}$ and $\omega_{i,1}, \ldots, \omega_{i,n_i}$ for $i = 1, \ldots, m$ constitute a basis of $\bigoplus_{i=1}^m \mathcal{F}_{|X_i}(V_{i,0})$ respectively R_0^+. This provides a diagram that gives an overview of this basis transformation situation:

$$\begin{array}{ccc} R_0^+ & \longrightarrow & R_0 \\ \downarrow & & \downarrow \\ \bigoplus_{i=1}^m \mathcal{F}_{|X_i}(V_{i,0}) & \longrightarrow & \mathcal{F}(V_0) \end{array} \qquad \begin{array}{ccc} (\omega_{i,j})_{i,j} & \xrightarrow{T_{0,\mathcal{O}_X}} & (\omega_i) \\ {\scriptstyle \mathrm{diag}(T_{\mathcal{F}_1}, \ldots, T_{\mathcal{F}_m})} \downarrow & & \downarrow {\scriptstyle T} \\ (v_{i,j})_{i,j} & \xrightarrow{T_{0,\mathcal{F}}} & (v_i)_i \end{array}$$

We will now try to put this into a kind of definition (which is more a fixation of notation) that we will use throughout this thesis. Moreover, we will try to establish some notation with regards to the iterating process over the irreducible components of X fixed in an order $(X_1, \dots, X_m)$. We refer the reader to Section 2.4 where the notations and basic results regarding the iterating process over the components are provided.

Before we can write down the notations we try to fix, we first need to give a convenient definition of how we denote matrices that admit a block structure.

Definition 4.4.6. Let $n = \sum_{i=1}^{m} n_i$. Any $M \in k[x]^{n\times n}$ can be described by block matrices $M_{i,j} \in k[x]^{n_i \times n_j}$, $i, j = 1, \dots, m$. That is,

$$M = \left(\begin{array}{c|c|c|c} M_{1,1} & M_{1,2} & \dots & M_{1,m} \\ \hline M_{2,1} & M_{2,2} & \dots & M_{2,m} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \underbrace{M_{m,1}}_{n_1} & \underbrace{M_{m,2}}_{n_2} & \dots & \underbrace{M_{m,m}}_{n_m} \end{array}\right)$$

and we write $M = (M_{i,j})_{i,j}$. In the following we will often just specify the blocks $M_{i,j}$ to determine M in the given n-**block-form**. △

Notation 4.4.7. Let X be a reduced cover of $\mathbb{P}^1_k$ with irreducible components X_i for which we fix an order $(X_1, \dots, X_m)$. Let Y_i be defined as in Definition 2.4.1. Let $\mathcal{J}_i \in \mathcal{O}_{X_i}$ be the ideal sheaf of $\mathcal{O}_{X_i}$ cutting out $Y_{i-1} \cap X_i$ in X_i. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Let $v_1, \dots, v_n$ denote a basis of $\mathcal{F}(V_0)$. For $i = 1, \dots, m$ let

(i) n_i denote the degree of the restriction of π to X_i,

(ii) $\Omega_i = (\omega_{i,1}, \dots, \omega_{i,n_i})$ denote a reduced basis of $R_{i,0}$,

(iii) $\mathcal{F}_i := \mathcal{F}_{|X_i}$ denote the restriction of $\mathcal{F}$ to X_i, if $\mathcal{F} = \mathcal{O}_X(D)$, we set $D_i = D_{|X_i}$,

(iv) $v_{i,1}, \dots, v_{i,n_i}$ denote a reduced basis of $\mathcal{F}_i(V_{i,0})$,

(v) $c_{i,1}, \dots, c_{i,n_i}$ denote a reduced basis of $\mathcal{J}_i(V_{i,0})\mathcal{F}_i(V_{i,0})$,

(vi) C_i denote a basis transformation matrix from $\omega_{i,1}, \dots, \omega_{i,n_i}$ to $c_{i,1}, \dots, c_{i,n_i}$, that is

$$(c_{i,1}, \dots, c_{i,n_i}) = (\omega_{i,1}, \dots, \omega_{i,n_i}) \cdot C_i, \tag{4:17}$$

(vii) $T_{\mathcal{F}_i}$ denote a basis transformation matrix from $\omega_{i,1}, \dots, \omega_{i,n_i}$ to $v_{i,1}, \dots, v_{i,n_i}$, that is

$$(v_{i,1}, \dots, v_{i,n_i}) = (\omega_{i,1}, \dots, \omega_{i,n_i}) \cdot T_{\mathcal{F}_i}. \tag{4:18}$$

If $\mathcal{F} = \mathcal{O}_X(D)$, we also write T_{D_i}.

Moreover, let

(viii) $\Omega_i^m := (\omega_{i,j})_{i,j} := (\omega_{i,1}, \dots, \omega_{i,n_i})_{i=1,\dots,m}$ denote the corresponding basis of R_0^+,

(ix) $(v_{i,j})_{i,j} := (v_{i,1}, \dots, v_{i,n_i})_{i=1,\dots,m}$ denote the corresponding basis of $\bigoplus_{i=1}^m \mathcal{F}_i(V_{i,0})$,

(x) $T_{\mathcal{F}}$ denote the basis transformation matrix from $(\omega_{i,j})_{i,j}$ to $(v_{i,j})_{i,j}$, that is

$$(v_{i,j})_{i,j} = (\omega_{i,j})_{i,j} \cdot T_{\mathcal{F}}, \tag{4:19}$$

thus $T_{\mathcal{F}} = (T_{i,j})_{i,j}$ with

$$T_{i,j} = \begin{cases} T_{\mathcal{F}_i}, & i = j \\ 0, & i \neq j, \end{cases}$$

if $\mathcal{F} = \mathcal{O}_X(D)$, we also write T_D,

(xi) $T_{0,\mathcal{F}}$ denote a basis transformation matrix from $(v_{i,j})_{i,j}$ to $v_1, \ldots, v_n$, that is

$$(v_1, \ldots, v_n) = (v_{i,j})_{i,j} \cdot T_{0,\mathcal{F}}, \tag{4:20}$$

(xii) Let $M_{\mathcal{F}}$ denote the basis transformation matrix from $(\omega_{i,j})_{i,j}$ to $v_1, \ldots, v_n$, that is

$$(v_1, \ldots, v_n) = (\omega_{i,j})_{i,j} \cdot M_{\mathcal{F}}. \tag{4:21}$$

If $\mathcal{F} = \mathcal{O}_X(D)$, we also write M_D.

By definition, we thus have $M_{\mathcal{F}} = (M_{i,j})_{i,j} = T_{\mathcal{F}} \cdot T_{0,\mathcal{F}}$. If $T_{0,\mathcal{F}} = (T_{i,j})_{i,j}$, then $M_{i,j} = T_{\mathcal{F}_i} \cdot T_{i,j}$. △

Remark 4.4.8. By Notation 4.4.7, if $\mathcal{F}$ is an $\mathcal{O}_X$-ideal with basis matrix $M_{\mathcal{F}}$ with respect to Ω_i^m, then $M_{\mathcal{F}}$ is in n-block-form with row blocks $M_{i,\mathcal{F}} \in k[x]^{n_i \times n}$. The row block matrix $M_{i,\mathcal{F}}$ contains by definition the coefficients of the basis elements of $\mathcal{F}(V_0)$ restricted to X_i respectively regarded as elements in $\mathcal{F}_{|X_i}(V_{i,0})$ as column vectors. In particular, the columns of $M_{i,\mathcal{F}}$ represent a generating set of $\mathcal{F}_{|X_i}(V_{i,0})$ and thus ColumnBasis applied to $M_{i,\mathcal{F}}$ returns a basis matrix of $\mathcal{F}_{|X_i}(V_{i,0})$. Frankly speaking, the matrix $M_{\mathcal{F}}$ therefore does not only represent $\mathcal{F}(V_0)$ via a basis but does also provide the algorithmic possibility to compute the restrictions $\mathcal{F}_{|X_i}(V_{i,0})$. The algorithm ComputeComponentMatrices will compute these restrictions by computing the mentioned basis matrices, see Algorithm 5. △

What we have seen in Remark 4.4.8 that the representation of $\mathcal{F}(V_0)$ via a basis that itself is represented with respect to the basis Ω_i^m in contrast with a representation solely with respect to Ω has the advantage of being able to compute the restrictions to the irreducible components. This will turn out not only to be handy but also to be crucial if we want to see whether a given $\mathcal{O}_X$-ideal is isomorphic to $\mathcal{O}_X$. After we have proven the existence of *small bases* and thus be able to give bounds for the π-invariants $-|X|_n$ in the next section, we will see in Section 4.6 that the representation of a reduced basis Ω with respect to Ω_i^m will provide the possibility to efficiently change from a representation with respect to Ω to one with respect to Ω_i^m (note that the converse is not true in general, see the remarks we make in the introductory text of Section 6.3). This will give us access to the advantages revealed in Remark 4.4.8 of the latter representation in the case of the former representation.

4.4.2 Finding Small Bases in the Case of Reducible Schemes

In this section we will prove the existence of bases of $\mathcal{F}(V_0)$ over $k[x]$ whose basis matrix $M_{\mathcal{F}}$ as in Notation 4.4.7 (xii) has bounded row degrees in terms of $\deg_k \mathcal{F}_i(V_{i,0})$ and invariants of X. Here $\mathcal{F}$ is any $\mathcal{O}_X$-ideal. Moreover, we will give an effective algorithm that is able to compute the desired basis matrix $M_{\mathcal{F}}$ given any basis matrix of $\mathcal{F}(V_0)$ with respect to Ω_i^m. We will depend on this when it comes to computing basis matrices from which we compute so called modification functions, see Section 5.7.2. We will achieve all of the above by using linear algebra over $k[x]$ and the so called Popov form of polynomial matrices.

Furthermore, the following lemma tells us that any basis transformation matrix $T_{0,\mathcal{F}}$ will provide a transformation matrix from which we might compute the π-invariants of $\mathcal{F}$. This will enable us to give bounds for the π-invariants of general $\mathcal{O}_X$-ideals in Section 4.5.

Lemma 4.4.9. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Any basis transformation matrix $T_{0,\mathcal{F}}$ from $(v_{i,j})_{i,j}$ to a basis $v_1,\dots,v_n$ of $\mathcal{F}(V_0)$ yields a basis transformation matrix*

$$T = \operatorname{diag}(x^{-|\mathcal{F}_i|_j}) \cdot T_{0,\mathcal{F}}$$

from $\mathcal{F}(S)$ to $\mathcal{F}(V_0)$. Now if we drop the assumption that S is disjoint to the intersection points of X and assume that $\mathcal{F}_{|S} = \oplus_{i=1}^m \mathcal{F}_{|S_i}$, then T as before yields the same basis transformation matrix.

Proof. Let $v_1,\dots,v_n$ be a basis of $\mathcal{F}(V_0)$ and $(v_{i,1},\dots,v_{i,n_i})$ a reduced basis of $\mathcal{F}_i(V_{i,0})$, that is $(\widetilde{v}_{i,1},\dots,\widetilde{v}_{i,n_i}) = (v_{i,1}x^{|\mathcal{F}_i|_1},\dots,v_{i,n_i}x^{|\mathcal{F}_i|_{n_i}})$ is a basis of $\mathcal{F}_{|S_i}(S_i)$. In both cases, the assumptions provide that $\mathcal{F}_{|S}(S) = \bigoplus_{i=1}^m \mathcal{F}_{|S_i}(S_i)$ and thus we may choose $(\widetilde{v}_{i,j})_{i,j}$ to be a basis of the former. Then we have

$$\begin{aligned}(v_1,\dots,v_n) &= (v_{i,j})_{i,j} \cdot T_{0,\mathcal{F}} \\ &= (\widetilde{v}_{i,j})_{i,j} \cdot \operatorname{diag}(x^{-|\mathcal{F}_i|_j})_{i,j} \cdot T_{0,\mathcal{F}}\end{aligned}$$

which yields the assertion in both cases. □

Now Lemma 4.3.5 combined with Corollary 4.3.6 tells us that the column degrees of the reduction of T as above will constitute the π-invariants of $\mathcal{F}$. In particular, by Remark 4.3.7, the ordered column degrees of T will be an upper bound for the π-invariants of $\mathcal{F}$. By Theorem 4.3.23, we already know bounds for the π-invariants of $\mathcal{F}_i$ for all $i = 1,\dots,n$. Hence we are left to argue why we are able to find a basis of $\mathcal{F}(V_0)$ which is small in relation to the reduced bases $(v_{i,j})_{i,j}$ of $\bigoplus_{i=1}^m \mathcal{F}_i(V_{i,0})$.

The main idea to achieve this is the following: Assume X to have two irreducible components X_1 and X_2. Then we would like to find a basis of $\mathcal{F}(V_0)$ which is small both in terms of the reduced bases of $\mathcal{F}_1(V_{1,0})$ and $\mathcal{F}_2(V_{2,0})$. Since $\mathcal{F}(V_0)$ embeds into $\mathcal{F}_1(V_{1,0})\oplus\mathcal{F}_2(V_{2,0})$ and this embedding is compatible with the surjection $\mathcal{F}(V_0) \to \mathcal{F}_i(V_{i,0})$, we find a basis of $\mathcal{F}(V_0)$ mapping to a given one of $\mathcal{F}_1(V_{1,0})$. But its image in $\mathcal{F}_2(V_{2,0})$ may be arbitrary. But we are able to show that we might reduce that image by a reduced basis of the ideal cutting out $X_1 \cap X_2$ in X_2. The degree of this ideal only depends on X and its components (and how those intersect inside of X). For general X we can iterate this procedure to finally obtain the desired basis of $\mathcal{F}(V_0)$.

The line of argument here is a pure linear algebra one and only deals with bases of free modules. An important statement which will be used here is Proposition C.2.2.

We will start by introducing matrices that are not only reduced but also satisfy further properties, matrices in the so called Popov form.

Definition 4.4.10. Let $M = (v_{i,j})_{i,j} \in k[x]^{n\times n}$ be a reduced matrix with columns $v_1,\dots,v_n \in k[x]^{n\times 1}$. For every $j = 1,\dots,n$ we denote by $\operatorname{piv}_j(M) = \operatorname{piv}(v_j)$ the row index of the lowermost non-zero entry in $\operatorname{LC}(v_j)$ and call it the **pivot index of** v_j. Consider the following properties that M might satisfy:

(i) The pivot indices of $v_1,\dots,v_n$ are all distinct.

(ii) The entry $v_{\operatorname{piv}(v_j),j}$ is monic.

(iii) We have $\deg(v_1) \le \deg(v_2) \le \dots \le \deg(v_n)$ and if $\deg(v_j) = \deg(v_{j+1})$, then $\operatorname{piv}(v_j) < \operatorname{piv}(v_{j+1})$.

(iv) For all $j = 1, \dots, n$ and $\ell \in \{1, \dots, n\} \setminus \{j\}$ we have $\deg(v_{\mathrm{piv}(v_j),j}) > \deg(v_{\mathrm{piv}(v_j),\ell})$.

If M satisfies Item (i), then M is called in **weak Popov form**. If M satisfies Items (i) to (iv), then M is called in **Popov form**. △

Remark 4.4.11. Let $M \in k[x]^{n\times n}$ be a matrix in weak Popov form (resp. Popov form). Then for all $j = 1, \dots, n$ the matrix obtained by deleting row $\mathrm{piv}(v_j)$ and column j is still in weak Popov form (resp. Popov form). Indeed, deleting row $\mathrm{piv}(v_j)$ and column j from M does not affect the pivot indices of the columns v_ℓ for $\ell \neq j$ and, moreover, since M is in weak Popov form, all $\mathrm{piv}(v_j)$ are distinct which stays true after deleting. △

Lemma 4.4.12. *Let $b = (b_1, \dots, b_m)^T \in k[x]^m$, $P \in k[x]^{m\times m}$ be such that P is in Popov form. Let $d = \deg(b) = \max_{i=1}^m\{\deg(b_i)\} > \deg(P)$. We define the matrix*

$$M := \left(\begin{array}{c|c} \mathbf{0} & x^d \\ \hline & b_1 \\ P & \vdots \\ & b_n \end{array}\right)$$

and denote by $Q = \textsc{Popov}(M)$ its Popov form computed by algorithm Popov, see Theorem A.2.16. Let $U \in k[x]^{m+1\times m+1}$ denote the matrix with $Q = MU$. Then

$$Q = \left(\begin{array}{c|c} \mathbf{0} & x^d \\ \hline & b'_1 \\ P & \vdots \\ & b'_n \end{array}\right) \quad \text{and} \quad U = \left(\begin{array}{c|c} E_m & V_{m,1} \\ \hline \mathbf{0}_{1,m} & E_1 \end{array}\right)$$

with $V_{m,1} \in k[x]^{m\times 1}$ and for all $i = 1, \dots, m$ we have $\deg(b'_i) < \deg(p_{\mathrm{piv}(p_{j_i})})$ for some $j_i \in \{1, \dots, m\}$. In particular, for $b' = (b'_1, \dots, b'_m)^T$ we have $\deg(b') < \deg(P)$.

Proof. First of all, note that both the Popov form of a non-singular matrix and the transformation matrix providing the Popov form are unique. Moreover, its column degrees are unique and minimal under those of matrices right equivalent to the original matrix. The column degrees of the Popov form add up to the degree of the determinant since it is reduced, see Definition 4.3.3 (iv). Since P is reduced, $\mathrm{LC}(P)$ has full rank and thus obviously the same is true for $\mathrm{LC}(M)$ and therefore M is already reduced. Hence the column degrees of M equal the column degrees of its Popov form. Furthermore, by assumption, we have $\deg(P) < d$ and P is in Popov form, that is, the column degrees of M are already ordered non-decreasingly which will also be true for its Popov form. From the above we can deduce that Popov will neither change the order of the columns of M nor will it increase any column degree. This shows that the column operations that will be carried out by Popov on M (those that will not be reversed) can not involve the last column as one of the column that alters another one. Any alteration of the first m columns of M involving the last column produces an entry in the uppermost row with degree at least d which then increases the column degree of the column in which it appears. This is not possible since the column degrees of the Popov form of M are already determined by those of M. Therefore any such alteration need to be reversed with the appropriate action using the last column since it is the only column with non-zero uppermost entry. The above also shows that the pivot indices of the Popov form of M are already determined by those of P and that of the last column will be 1.

However, any column operations only involving the leftmost m columns of M need to be reversed since otherwise this contradicts that P is in Popov form. Therefore, the only possible (not-reversed) column operations that Popov will carry out on M are alterations

of the rightmost column by the leftmost m columns. Those will ensure that the degrees of the lowermost m entries of the rightmost column of the output matrix will be strictly bounded by the respective degrees of the entries of P at the pivot indices of P. This proves the assertion about the output matrix of Popov. The restrictions on the possible column operations carried out by Popov shows that the transformation matrix U with $\text{Popov}(M) = MU$ is indeed of the asserted form. □

Proposition 4.4.13. *Let $B = (b_{i,j})_{i,j} = (b_1, \ldots, b_n) \in k[x]^{m \times n}$, $P = (p_{i,j})_{i,j} \in k[x]^{m \times m}$ be two matrices such that P is in Popov form. Let $d_i := \deg(b_i) > d$ and assume $d_1 \leq \ldots \leq d_n$. We define the matrix*

$$M := \left(\begin{array}{c|ccc} \mathbf{0} & x^{d_1} & & \\ & & \ddots & \\ & & & x^{d_n} \\ \hline P & b_1 & \ldots & b_n \end{array}\right)$$

and denote by $Q = \text{Popov}(M)$ its Popov form computed by algorithm Popov, see Theorem A.2.16. Let $U \in k[x]^{m+n \times m+n}$ denote the matrix with $Q = MU$. Then

$$Q = \left(\begin{array}{c|ccc} \mathbf{0} & x^{d_1} & & \\ & & \ddots & \\ & & & x^{d_n} \\ \hline P & b'_1 & \ldots & b'_n \end{array}\right) \quad \text{and} \quad U = \left(\begin{array}{c|c} E_m & V_{m,n} \\ \hline \mathbf{0} & E_n \end{array}\right)$$

with $V_{m,n} \in k[x]^{m \times n}$ and, moreover, for all $i = 1, \ldots, n$ we have $\deg(b'_{i,j}) < \deg(p_{\text{piv}(p_j),j})$ for some $j \in \{1, \ldots, m\}$. In particular, $\deg(B + PV_{m,n}) < \deg(P)$.

Proof. We prove the assertion by induction on n. The base case $n = 1$ is proven by Lemma 4.4.12. Now let us assume that the assertion is true for every $(m - 1 \times m - 1)$ matrix M. Let

$$M_{m,n} = \left(\begin{array}{c|ccc|c} \mathbf{0} & x^{d_1} & & & \\ & & \ddots & & \\ & & & x^{d_{n-1}} & \\ \hline & & & & x^{d_n} \\ \hline P & b_1 & \ldots & b_{n-1} & b_n \end{array}\right) \quad \text{and} \quad M_{m,n-1} = \left(\begin{array}{c|ccc} \mathbf{0} & x^{d_1} & & \\ & & \ddots & \\ & & & x^{d_{n-1}} \\ \hline P & b_1 & \ldots & b_{n-1} \end{array}\right)$$

where $M_{m,n-1}$ originates from $M_{m,n}$ by deleting row n and column $n + m$. By induction hypothesis,

$$\begin{aligned} Q_{m,n-1} := \text{Popov}(M_{m,n-1}) &= M_{m,n-1} \cdot U_{m,n-1} \\ &= M_{m,n-1} \cdot \left(\begin{array}{c|c} E_m & V_{m,n-1} \\ \hline \mathbf{0} & E_{n-1} \end{array}\right) \\ &= \left(\begin{array}{c|ccc} \mathbf{0} & x^{d_1} & & \\ & & \ddots & \\ & & & x^{d_{n-1}} \\ \hline P & b'_1 & \ldots & b'_{n-1} \end{array}\right) \end{aligned}$$

for some $V_{m,n-1} \in k[x]^{m \times n-1}$, $b'_j = (b'_{1,j}, \ldots, b'_{m,j})^T$ and for all $i = 1, \ldots, m$ we have

$\deg(b'_{i,j}) < \deg(p_{\mathrm{piv}(p_j),j})$ for some $j \in \{1,\ldots,m\}$. Now we set

$$M_{m,1} = \left(\begin{array}{c|c} \mathbf{0} & x^{d_n} \\ \hline P & b_n \end{array}\right)$$

and apply Lemma 4.4.12 to obtain

$$\begin{aligned} Q_{m,1} &= \textsc{Popov}(M_{m,1}) \\ &= M_{m,1} \cdot U_{m,1} \\ &= M_{m,1} \cdot \left(\begin{array}{c|c} E_m & v_{m,1} \\ \hline \mathbf{0} & 1 \end{array}\right) \\ &= \left(\begin{array}{c|c} \mathbf{0} & x^{d_n} \\ \hline P & b'_n \end{array}\right) \end{aligned}$$

with $v_{m,1}, b'_n \in k[x]^m$, $b'_n = (b'_{1,n},\ldots,b'_{m,n})^T$ and for all $i = 1,\ldots,m$ we have $\deg(b'_{i,n}) < \deg(p_{\mathrm{piv}(p_j),j})$ for some $j \in \{1,\ldots,m\}$. Now we define

$$V_{m,n} = \left(\begin{array}{c|c} V_{m,n-1} & v_{m,1} \\ \mathbf{0} & \end{array}\right) \quad \text{and} \quad U_{m,n} = \left(\begin{array}{c|c} E_m & V_{m,n} \\ \hline \mathbf{0} & E_n \end{array}\right).$$

Then we easily see that

$$Q_{m,n} := M_{m,n} \cdot U_{m,n} = \left(\begin{array}{c|cccc} & x^{d_1} & & & \\ \mathbf{0} & & \ddots & & \\ & & & x^{d_{n-1}} & \\ & & & & x^{d_n} \\ \hline P & b'_1 & \ldots & b'_{n-1} & b'_n \end{array}\right).$$

By assumption, we have $d_1 \leq \ldots \leq d_n$ and $d_i > \deg(P)$ which now together with

$$\forall\ i = 1,\ldots,m\ \ \deg(b'_{i,j}) < \deg(p_{\mathrm{piv}(p_j),j})$$

provides that $Q_{m,n}$ is in Popov form. Since both the Popov form of non-singular matrices and the transformation matrix providing the Popov form are unique, we have

$$Q_{m,n} = \textsc{Popov}(M_{m,n})$$

with unique transformation matrix $U_{m,n}$ which finishes the proof. □

The following algorithm is the algorithmic implementation of Proposition 4.4.13. We will not need it in our algorithms and we only state it for completeness. Instead, we will only need the statement of Proposition 4.4.13 to come up with the basis we are looking for.

Algorithm 3 Reducing a matrix by a matrix in Popov form

Assumption:	The algorithm POPOV returns both the Popov form of the input matrix and the corresponding transformation matrix
Input	$B \in k[x]^{m\times n}$; $P = (p_{i,j})_{i,j} \in k[x]^{m\times m}$ in Popov form
Output	$U \in k[x]^{m\times n}$ and B' such that $B' := B + PU = (b'_{i,j})_{i,j}$ and for all $i = 1,\dots,n$ we have $\deg(b'_{i,\ell}) < \deg(p_{\mathrm{piv}(p_j),j})$ for some $j \in \{1,\dots,m\}$

1: **procedure** REDUCEBYPOPOV(B, P)
2: **for** $j = 1,\dots,n$ **do**
3: $d_j \leftarrow \max_{i=1}^{m}\{\deg(b_{i,j})\}$
4: $D \leftarrow \mathrm{diag}(x^{d_1},\dots,x^{d_n})$
5: $M \leftarrow \left(\begin{array}{c|c} \mathbf{0} & D \\ \hline P & B \end{array}\right)$
6: $Q, V \leftarrow$ POPOV(M)
7: $U \leftarrow$ SUBMATRIX($V, (1, m+1), (m, n)$)
8: **return** $U, B + PU$

Proposition 4.4.14. *The algorithm* REDUCEBYPOPOV*, see Algorithm 5, is correct. Moreover, if d is an upper bound of the degrees of both B and P, then* REDUCEBYPOPOV *requires at most $O^{\sim}((m+n)^{\omega}d)$ operations in k and returns matrices B' and U such that $B' = B + PU$ and $\deg(B') < \deg(P)$.*

Proof. The correctness of REDUCEBYPOPOV follows from Proposition 4.4.13. By construction, the matrix M in line 5 has degree bounded by d and thus POPOV requires at most $O^{\sim}((m+n)^{\omega}d)$ operations in k, see Theorem A.2.16. □

The following proposition shows that if we can find suitable unimodular column operations for a given matrix that result in row degree bounds, then by suitable scaling we can employ the POPOV algorithm to compute a matrix with the desired row degree bounds.

Proposition 4.4.15. *Let $M = (m_{i,j})_{i,j} \in k[x]^{m\times n}$ be a polynomial matrix. If there are unimodular column operations on M such that the i-th row of the resulting matrix has degree d_i and $d := \max_{i=1}^{m}\{d_i\}$, then*

$$M' = \mathrm{diag}(x^{d_1-d},\dots,x^{d_m-d}) \cdot \text{POPOV}(\mathrm{diag}(x^{d-d_1},\dots,x^{d-d_m}) \cdot M)$$

is a right equivalent matrix of M which has row degrees $e_1,\dots,e_m$ beginning from top such that $e_i \le d_i$ for all $i = 1,\dots,m$.

Proof. Let $U \in k[x]^{n\times n}$ denote the unimodular matrix such that $M \cdot U$ has row degrees $d_1,\dots,d_m$ beginning from top. Obviously, every row of

$$N := \mathrm{diag}(x^{d-d_1},\dots,x^{d-d_m}) \cdot M \cdot U$$

then has degree d. Note that since $\mathrm{diag}(x^{d-d_1},\dots,x^{d-d_m}) \cdot M$ and N are right equivalent, their Popov forms coincide. Moreover, the column degree of every column of N is bounded by d. Therefore, its Popov form has column degrees that are bounded by d as well. Moreover, due to the definition of the Popov form we know that the same holds for the row degrees of POPOV(N). Now we set $M' := \mathrm{diag}(x^{d_1-d},\dots,x^{d_m-d}) \cdot \text{POPOV}(N)$ and see that its row degrees $e_1,\dots,e_m$ satisfy $e_i \le d_i$ for all $i = 1,\dots,m$. Finally, that M' is right equivalent to M follows easily from the fact that POPOV computes a right equivalent

matrix, that is, we have

$$\begin{aligned} M' &= \operatorname{diag}(x^{d_1-d}, \dots, x^{d_m-d}) \cdot \textsc{Popov}(\operatorname{diag}(x^{d-d_1}, \dots, x^{d-d_m}) \cdot M) \\ &= \operatorname{diag}(x^{d_1-d}, \dots, x^{d_m-d}) \cdot (\operatorname{diag}(x^{d-d_1}, \dots, x^{d-d_m}) \cdot M) \cdot T \\ &= M \cdot T \end{aligned}$$

for some unimodular $T \in \mathrm{GL}(n, k[x])$. □

Proposition 4.4.16. *Let $n = \sum_{i=1}^{m} n_i$. For every matrix $M = (M_{i,j})_{i,j}$ in n-block-form there is a right equivalent matrix $M' = MU$ such that*

$$M' = \left(\begin{array}{c|c|c|c|c|c} C_1 & 0 & \dots & & & 0 \\ \hline N_{2,1} & C_2 & 0 & \dots & & 0 \\ \hline N_{3,1} & N_{3,2} & C_3 & 0 & \dots & 0 \\ \hline \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \hline N_{m-1,1} & N_{m-1,2} & \dots & N_{m-1,m-2} & C_{m-1} & 0 \\ \hline N_{m,1} & N_{m,2} & \dots & N_{m,m-2} & N_{m,m-1} & C_m \end{array}\right),$$

where C_i is in Popov form and for all $j = 1, \dots, m$ the ℓ-th row of $N_{i,j}$ has degree strictly bounded by the ℓ-th row of C_i. In particular, $\deg(N_{i,j}) < \deg(C_i)$ for all $i = 1, \dots, m$.

Proof. We compute a column basis of the first row block $(M_{i,j})_{j=1,\dots,m}$ using Column-Basis, compute its Popov form with Popov, call it C_1 and apply the necessary column operations to all of M. The resulting matrix now looks like

$$M_1 = \left(\begin{array}{c|c|c|c|c|c} C_1 & 0 & \dots & & & 0 \\ \hline N_{2,1} & N_{2,2} & \dots & & & N_{2,m} \\ \hline N_{3,1} & N_{3,2} & \dots & & & N_{3,m} \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline N_{m-1,1} & N_{m-1,2} & \dots & & & N_{m-1,m} \\ \hline N_{m,1} & N_{m,2} & \dots & & & N_{m,m} \end{array}\right).$$

Now we can apply the same method again and compute the Popov form of a basis of the column space of $[N_{2,2} | \dots | N_{2,m}]$ and apply the unimodular column operations to all of M_1 which then provides

$$M_2 = \left(\begin{array}{c|c|c|c|c|c} C_1 & 0 & \dots & & & 0 \\ \hline N'_{2,1} & C_2 & 0 & \dots & & 0 \\ \hline N'_{3,1} & N'_{3,2} & \dots & & & N'_{3,m} \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline N'_{m-1,1} & N'_{m-1,2} & \dots & & & N'_{m-1,m} \\ \hline N'_{m,1} & N'_{m,2} & \dots & & & N'_{m,m} \end{array}\right)$$

with C_2 in Popov form. Thus by Proposition 4.4.13, there are further unimodular column operations that reduces the row degrees of $N'_{2,1}$ accordingly. This shows that the assertion follows from induction over the number m of row blocks of M. □

Corollary 4.4.17. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal.*

There is a $k[x]$-basis $v_1, \dots, v_n$ of $\mathcal{F}(V_0)$ such that

$$M_{\mathcal{F}} = \left(\begin{array}{c|c|c|c|c|c} C_1 & 0 & & & & \\ \hline N_{2,1} & C_2 & 0 & & & \\ \hline N_{3,1} & N_{3,2} & C_3 & 0 & & \\ \hline \vdots & \vdots & \ddots & \ddots & \ddots & \\ \hline N_{m-1,1} & N_{m-1,2} & \dots & N_{m-1,m-2} & C_{m-1} & 0 \\ \hline N_{m,1} & N_{m,2} & \dots & N_{m,m-2} & N_{m,m-1} & C_m \end{array}\right),$$

is the basis matrix with respect to the basis Ω_i^m, that is,

$$(v_1, \dots, v_n) = \Omega_i^m \cdot M_{\mathcal{F}}.$$

Moreover, C_i is in Popov form and for all $j = 1, \dots, m$ the ℓ-th row of $N_{i,j}$ has degree strictly bounded by the ℓ-th row of C_i. If $\mathcal{F}$ is invertible or satisfies $\mathcal{F}_P = \mathcal{O}_{X,P}$ for all $P \in \operatorname{Supp}(\mathscr{S})$, then the matrices C_i satisfy

$$\deg(C_i) \leq \frac{\deg_k \mathcal{F}_i(V_{i,0})}{n_i} + c_{i,X}.$$

Proof. The existence of $M_{\mathcal{F}}$ in the asserted form follows from Proposition 4.4.16. We show the assertion about the C_i only for C_m since the general statement then follows by induction. In general, the i-th row block of $M_{\mathcal{F}}$ contains a generating set of $\mathcal{F}_i(V_{i,0})$. Moreover, by construction, $(N_{m,1} \mid \dots \mid N_{m,m-1} \mid C_m)$ has rank n_m and thus represents a $k[x]$-generating set of $\mathcal{F}_i(V_{m,0})$. Due to the form of $M_{\mathcal{F}}$, the matrix C_m represents a basis of the submodule of $\mathcal{F}_m(V_{m,0})$ of those elements vanishing on $X_1 \cup \dots \cup X_{m-1}$. This precisely is the submodule $\mathcal{J}_m(V_{m,0})\mathcal{F}_m(V_{m,0})$, see Proposition C.2.2. Let us now prove that the assumptions on $\mathcal{F}$ provide $\deg_k \mathcal{J}_i\mathcal{F}_i = \deg_k \mathcal{J}_i + \deg_k \mathcal{F}_i$ for $i = 1, \dots, m$. In the case that $\mathcal{F}$ is invertible, this is due to Lemma C.4.7. In the case that $\mathcal{F}_P = \mathcal{O}_{X,P}$ for all $P \in \operatorname{Supp}(\mathcal{O}_{X_i}/\mathcal{J}_i) \subseteq \operatorname{Supp}(\mathscr{S})$, we have

$$\mathcal{J}_{i,P}\mathcal{F}_{i,P} = \begin{cases} \mathcal{F}_{i,P}, & P \notin \operatorname{Supp}(\mathcal{O}_{X_i}/\mathcal{J}_i) \\ \mathcal{J}_{i,P}, & P \in \operatorname{Supp}(\mathcal{O}_{X_i}/\mathcal{J}_i) \end{cases}$$

which then provides

$$\begin{aligned} \deg_k \mathcal{J}_i\mathcal{F}_i = \sum_{P \in X} \mathcal{J}_{i,P}\mathcal{F}_{i,P} &= \sum_{P \in \operatorname{Supp}(\mathcal{O}_{X_i}/\mathcal{J}_i)} \mathcal{J}_{i,P} + \sum_{P \notin \operatorname{Supp}(\mathcal{O}_{X_i}/\mathcal{J}_i)} \mathcal{F}_{i,P} \\ &= \deg_k \mathcal{J}_i + \deg_k \mathcal{F}_i. \end{aligned}$$

Now by Lemmas 2.4.5 and 4.3.28, we have

$$\begin{aligned} \deg(C_i) &\leq \frac{\mathcal{J}_i(V_{i,0})\mathcal{F}_i(V_{i,0})}{n_i} + c_{X_i} \\ &\leq \frac{\deg_k \mathcal{F}_i(V_{i,0}) + \chi(Y_i, \mathscr{S}_i)}{n_i} + c_{X_i} \end{aligned}$$

which by Definition 2.4.10 yields

$$\deg(C_i) \leq \frac{\deg_k \mathcal{F}_i(V_{i,0})}{n_i} + c_{i,X}$$

and thus finishes the proof. □

Corollary 4.4.18. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. There is a $k[x]$-basis $v_1, \dots, v_n$ of $\mathcal{F}(V_0)$ such that*

$$T_{0,\mathcal{F}} = \begin{pmatrix} E_{n_1} & 0 & & & & \\ N_{2,1} & C_2 & 0 & & & \\ N_{3,1} & N_{3,2} & C_3 & 0 & & \\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ N_{m-1,1} & N_{m-1,2} & \dots & N_{m-1,m-2} & C_{m-1} & 0 \\ N_{m,1} & N_{m,2} & \dots & N_{m,m-2} & N_{m,m-1} & C_m \end{pmatrix},$$

is the basis transformation matrix regarding the basis $(v_{i,j})_{i,j}$

$$(v_1, \dots, v_n) = (v_{i,j})_{i,j} \cdot T_{0,\mathcal{F}}.$$

Moreover, C_i is in Popov form and for all $j = 1, \dots, m$ the ℓ-th row of $N_{i,j}$ has degree strictly bounded by the ℓ-th row of C_i. If $\mathcal{F}$ is invertible or satisfies $\mathcal{F}_P = \mathcal{O}_{X,P}$ for all $P \in \operatorname{Supp}(\mathscr{S})$, then the matrices C_i satisfy

$$\deg(C_i) \leq c_{X_i}.$$

Proof. The prove is the very same as the one of Corollary 4.4.17 with one exception: The matrices C_i are basis matrices of the free $k[x]$-modules $\mathcal{J}_i(V_{i,0})\mathcal{F}_i(V_{i,0})$ with respect to the reduced basis $v_{i,1}, \dots, v_{i,n_i}$ instead of $\omega_{i,1}, \dots, \omega_{i,n_i}$. In particular, $C_1 = E_{n_1}$. Both $\mathcal{J}_i\mathcal{F}_i$ and $\mathcal{F}_i$ are $\mathcal{O}_{X_i}$-ideals with $\mathcal{J}_i(V_{i,0})\mathcal{F}_i(V_{i,0}) \subseteq \mathcal{F}_i(V_{i,0})$ and $\mathcal{J}_i(S)\mathcal{F}_i(S) = \mathcal{F}_i(S)$. Thus we may apply Proposition 4.3.26 with $s = 0$ to obtain

$$\begin{aligned} \deg(C_i) &\leq \frac{-\deg_k \mathcal{F}_i + \deg_k \mathcal{J}_i\mathcal{F}_i + n_i}{n_i} + c_{X_i} \\ &= \frac{\deg_k \mathcal{J}_i(V_{i,0}) + n_i}{n_i} + c_{X_i} \end{aligned}$$

where we have used the assumption on $\mathcal{F}$ that provides $\deg_k \mathcal{J}_i\mathcal{F}_i = \deg_k \mathcal{J}_i + \deg_k \mathcal{F}_i$. Therefore, as in the proof of Corollary 4.4.17 we use Lemma 2.4.5 and Definition 2.4.10 to obtain $\deg(C_i) \leq c_{i,X}$ as asserted. □

Remark 4.4.19. We will later combine Corollaries 4.3.6 and 4.4.18 and Lemma 4.4.9 to obtain a bound for the π-invariants for general $\mathcal{O}_X$-ideals $\mathcal{F}$ and for $\mathcal{O}_X$. △

Proposition 4.4.20. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Let M be any basis matrix of $\mathcal{F}(V_0)$ with respect to Ω_i^m. Let $d_i = \left\lceil \frac{\deg_k \mathcal{F}_i(V_{i,0})}{n_i} + c_{i,X} \right\rceil$. Then*

$$\operatorname{diag}(x^{d_1-d}, \dots, x^{d_m-d}) \cdot \textsc{Popov}(\operatorname{diag}(x^{d-d_1}, \dots, x^{d-d_m}) \cdot M)$$

is a basis matrix of $\mathcal{F}(V_0)$ in n-block-form whose i-th row block has degree bounded by d_i. In particular, its degree is bounded by $\max_{i=1}^m \{\deg_k \mathcal{F}_i(V_{i,0})/n_i + c_{i,X}\}$.

Proof. Corollary 4.4.17 shows that there is a right equivalent matrix of M that has the desired bounded row block degrees. Therefore, the assertion follows from Proposition 4.4.15 which provides a right equivalent matrix of M and therefore another basis matrix of $\mathcal{F}(V_0)$. □

Algorithm 4 Compute component reduced basis matrix

Input	$M \in k[x]^{n\times n}$ in n-block-form; $n = \sum_{i=1}^{m} n_i$; $d_1, \dots, d_m$ desired row block degrees
Output	$T = (T_{i,j})_{i,j} \in k[x]^{n\times n}$ in n-block-form, right equivalent to M with $\deg(T_{i,j}) \leq d_i$ for all $j = 1, \dots, m$

1: **procedure** RowBlockReduce($M, d_1, \dots, d_m$)
2: $D \leftarrow \max\{d_1, \dots, d_m\}$
3: $M \leftarrow$ ScaleRows($M, x^{D-d_1}, \dots, x^{D-d_m}$)
4: $P \leftarrow$ Popov(M)
5: $P \leftarrow$ ScaleRows($P, x^{d_1-D}, \dots, x^{d_m-D}$)
6: **return** P

Proposition 4.4.21. *If there is a right equivalent matrix of M with row block degrees bounded by $d_1, \dots, d_m$, then the algorithm* RowBlockReduce*, see Algorithm 4, is correct. Moreover, if d is a common bound for D and $\deg M$, then* RowBlockReduce *requires at most $O^{\sim}(n^{\omega}d)$ operations in k. The output matrix has degree bounded by $\max_{i=1}^{m}\{d_i\} \leq d$.*

Proof. The correctness of RowBlockReduce follows from Proposition 4.4.20. This already provides $\deg(\text{RowBlockReduce}(M)) \leq \max_{i=1}^{m}\{d_i\}$. Note that after the first scaling the row block degrees are all equal to D and thus Popov does not increase the row block degrees (it may increase the degrees of columns but this can not exceed D) since otherwise the result would not be reduced. This provides $\max_{i=1}^{m}\{d_i\} \leq d$.

Scaling a square matrix N of dimension n with x^D requires at most n^2 polynomial multiplications of polynomials with degree bounded by $D + \deg(N)$. Therefore, it requires at most $O^{\sim}(n^2(D + \deg(N)))$ operations in k, see Proposition A.2.3. Applying this to M we obtain that line 3 requires at most $O^{\sim}(n^2 d)$ operations in k. Since d is an upper bound of both D and $\deg(M)$, $2d$ is an upper bound for the scaled version of M which is the input of Popov in line 4. Thus, by Theorem A.2.16, the computation of P at line 4 requires at most $O^{\sim}(n^{\omega}d)$ operations in k and provides by construction a matrix with degree bounded by D. Finally, the scaling argument from above applies again and we can finish the proof. □

4.5 Bounds for π-Invariants in the General Case

In this section we mainly use Corollary 4.4.18 to prove bounds of the π-invariants of a general $\mathcal{O}_X$-ideal. The same argument will be used to show that $-|X|_i$ are linearly bounded by c_X.

Lemma 4.5.1. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Assume that $\mathcal{F}$ is invertible or that $\mathcal{F}_P = \mathcal{O}_{X,P}$ for all $P \in \operatorname{Supp}(\mathscr{S})$. Then*

(i) $-|\mathcal{F}|_n \leq \max_{i=1}^{m}\left\{\frac{\deg_k \mathcal{F}_i}{n_i} + 2c_{X_i}\right\} \leq \max_{i=1}^{m}\left\{\frac{\deg_k \mathcal{F}_i}{n_i}\right\} + 2c_X$ *and*

(ii) $\max_{i=1}^{n}\{-\deg_k \mathcal{F}_i/n_i\} \leq -|\mathcal{F}|_1$.

Proof. We prove Item (i) first. We can write down a basis transformation matrix from a basis of $\mathcal{F}(S)$ to one of $\mathcal{F}(V_0)$ and then use the insights of Theorem 4.3.15. Let $(\widetilde{v}_{i,j})_{i,j}$ be the $\mathcal{O}_\infty$-basis of $\mathcal{F}(S) = \bigoplus_{i=1}^{m}\mathcal{F}(S_i)$ that is provided by the reduced bases of $\mathcal{F}(V_0)$, that is $\widetilde{v}_{i,j} = x^{|\mathcal{F}_i|_j}v_{i,j}$. Let $T_{0,\mathcal{F}}$ be as in Corollary 4.4.18 and let $(v_1, \dots, v_n)$ denote the

corresponding $k[x]$-basis of $\mathcal{F}(V_0)$. Then by Lemma 4.4.9, a basis transformation matrix M from the basis $(\widetilde{v}_{i,j})_{i,j}$ of $\mathcal{F}(S)$ to $(v_i)_i$, one of $\mathcal{F}(V_0)$, is provided by

$$M = \operatorname{diag}(x^{-|\mathcal{F}_i|_j} \mid i = 1, \dots, n, j = 1, \dots, n_i) \cdot T_{0,\mathcal{F}}.$$

By Corollary 4.4.18, we thus have

$$M = (M_{i,j})_{i,j} = \begin{cases} \operatorname{diag}(x^{-|\mathcal{F}_i|_\ell} \mid \ell = 1, \dots, n_1), & i = j = 1 \\ \operatorname{diag}(x^{-|\mathcal{F}_i|_\ell} \mid \ell = 1, \dots, n_i) \cdot C_i, & i = j > 1 \\ \operatorname{diag}(x^{-|\mathcal{F}_i|_\ell} \mid \ell = 1, \dots, n_i) \cdot N_{i,j}, & i > j \\ 0, & i < j. \end{cases}$$

In particular, the degree of M and thus the maximum of the column degrees of M is bounded by

$$\begin{aligned} \max_{i=1}^{m}\{\deg M_{i,i}\} &= \max_{i=1}^{m}\{\max_{j=1}^{n_i}\{-|\mathcal{F}_i|_j + \deg \operatorname{col}(j, C_i)\}\} \\ &\leq \max_{i=1}^{m}\{\max_{j=1}^{n_i}\{-|\mathcal{F}_i|_{n_i} + \deg C_i\}\} \\ &= \max_{i=1}^{m}\{-|\mathcal{F}_i|_{n_i} + \deg C_i\}\} \\ \text{Corollary 4.4.18} \rightsquigarrow &\leq \max_{i=1}^{m}\{-|\mathcal{F}_i|_{n_i} + c_{X_i}\}. \end{aligned}$$

By Remark 4.3.7, this provides the upper bounds for $-|\mathcal{F}|_i$.

Now let us prove Item (ii). By Remark 4.3.19, $r \geq -|\mathcal{F}|_1$ is equivalent to $\mathcal{F}(r(x)_\infty)(X) \neq 0$ and thus $r < -|\mathcal{F}|_1$ is equivalent to $\mathcal{F}(r(x)_\infty)(X) = 0$. Hence if we find $r \in \mathbb{Z}$ such that $\mathcal{F}(r(x)_\infty)(X)$ vanishes, r provides a lower bound for $-|\mathcal{F}|_1$. By Proposition 4.4.2, we have an embedding

$$\phi : \mathcal{F}(r(x)_\infty) \to \bigoplus_{i=1}^{m} (\tau_i)_* \mathcal{F}(r(x)_\infty)_{|X_i}. \tag{5:22}$$

By Definition 2.2.9, the pole divisor of x on X restricts to the pole divisor of x on X_i. This together with the fact that the pullback of sheaves respects the tensor product of sheaves provides $\mathcal{F}(r(x)_\infty)_{|X_i} = \mathcal{F}_{|X_i}(r(x)_{X_i,\infty})$. Now taking global sections in Eq. (5:22) provides

$$\mathcal{H}^0(X, \mathcal{F}(r(x)_\infty)) \to \bigoplus_{i=1}^{m} H^0(X, \mathcal{F}_{|X_i}(r(x)_{X_i,\infty})).$$

Now since X is reduced, X_i is integral and thus we may apply Lemma C.4.6 which tells us that $\mathcal{F}_{|X_i}(r(x)_{X_i,\infty})$ vanishes whenever $\deg_k \mathcal{F}_{|X_i}(r(x)_{X_i,\infty}) > 0$. By Lemma C.4.7, we have

$$\begin{aligned} \deg_k \mathcal{F}_{|X_i}(r(x)_{X_i,\infty}) &= \deg_k \mathcal{F}_{|X_i} + r \deg_k (x)_{X_i,\infty} \\ &= \deg_k \mathcal{F}_{|X_i} + r n_i > 0 \end{aligned}$$

if $r > -\deg_k \mathcal{F}_{|X_i}/n_i$. Since we need all $\mathcal{F}_{|X_i}(r(x)_{X_i,\infty})$ to vanish, the assertion follows. □

Corollary 4.5.2. *Let X be a reduced cover of $\mathbb{P}^1_k$. Then*

$$0 = -|X|_1 \leq \ldots \leq -|X|_n \leq c_X.$$

Proof. We apply Lemma 4.5.1 (i) and obtain $-|X|_n \leq c_X$ as desired. The equality $-|X|_1 =$

0 follows from Corollary 4.3.16. □

Corollary 4.5.3. *Let X be a cover of $\mathbb{P}^1_k$. Let $\Omega = (\omega_1, \dots, \omega_n)$ be a reduced basis of $\mathcal{O}_X$. Let $f \in R_0$ with $\deg \phi_\Omega(f) \leq d$. Then the $k[x]$-basis $f\Omega = (f\omega_1, \dots, f\omega_n)$ has a basis matrix T_f with $\deg(T_f) \leq d + 2c_X$.*

Proof. Combine Corollary 4.5.2 and Lemma 4.3.35. □

Corollary 4.5.4. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal such that $\mathcal{F}(V_0) \subseteq R_0$ and $\mathcal{F}(S) = x^s\mathcal{O}_S$. The basis transformation matrix T from a reduced basis of $\mathcal{O}_X$ to a reduced basis of $\mathcal{F}$ has degree bounded by*

$$\deg T \leq s + \max_{i=1}^{m} \left\{ \frac{\deg_k \mathcal{F}_i}{n_i} \right\} + 2c_X.$$

In particular, if $\deg_k \mathcal{F}_{|X_i} = 0$ for all $i = 1, \dots, m$, then the above basis matrix has degree bounded by

$$\deg T \leq \frac{\deg_k \mathcal{F}(V_0)}{n} + 2c_X.$$

Proof. By Corollary 4.3.27, we know that the respective basis matrix degree is bounded by $s - |\mathcal{F}|_n$ and thus Lemma 4.5.1 provides the assertion. The particular part follows from $\deg_k \mathcal{F}_{|X_i} = 0$ and

$$s = \frac{sn}{n} = \frac{-\deg_k \mathcal{F}(S)}{n} = \frac{\deg_k \mathcal{F}(V_0)}{n}$$

where the second and third equality are due to Corollaries C.4.13 and D.2.9, respectively. □

With the same line of argument as in Lemma 4.3.28 we obtain that we are always able to compute a basis matrix of $\mathcal{F}(V_0)$ with degree bounded in terms of the degree of $\mathcal{F}$.

Corollary 4.5.5. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal such that $\mathcal{F}(V_0) \subseteq R_0$ and $\mathcal{F}(S) = x^s\mathcal{O}_S$. Moreover, assume that $\deg_k \mathcal{F}_{|X_i} = 0$. Given any basis matrix $T_\mathcal{F}$ of $\mathcal{F}(V_0)$ with respect to a reduced basis of $\mathcal{O}_X$, we have that*

$$\deg(\textsc{RedMat}(T_\mathcal{F})) \leq \frac{\deg_k \mathcal{F}(V_0)}{n} + 2c_X.$$

Proof. By Theorem A.2.7, we know that $\textsc{RedMat}(T_\mathcal{F})$ has minimal column degrees among all $k[x]$-right equivalent matrices of $T_\mathcal{F}$. Now the matrix T from Corollary 4.5.4 is among these right equivalent matrices and thus $\deg(T)$ provides the asserted upper bound. □

4.6 Reduced Basis of $\mathcal{O}_X$ in the General Case

In this section we use Corollary 4.4.18 to see that a reduced basis Ω of $\mathcal{O}_X$ respectively R_0 has bounded degrees with respect to Ω_i^m. We also provide some fundamental properties of the multiplication table of Ω_i^m. Using the above we are able to show that the standard basis matrix of fR_0 with respect to Ω_i^m has bounded degrees as well. We will furthermore see how to compute basis matrices of reduced bases of $\mathcal{F}_i(V_{i,0})$ only given a basis matrix of $\mathcal{F}(V_0)$ with respect to a reduced basis of R_0.

Corollary 4.6.1. *There exists a $k[x]$-basis $\omega_1, \dots, \omega_n$ of R_0 with $\omega_\ell = \sum_{i=1}^{m} \sum_{j=1}^{n_i} \nu_{\ell,i,j}\omega_{i,j}$ such that $\nu_{\ell,i,j} \in k[x]$ and*

$$\deg \nu_{\ell,i,j} \leq c_{X_i}.$$

Moreover, let $\mu_{i,j,q,s}$ denote the multiplication tables of X_i, i.e. $\omega_{i,j}\omega_{i,q} = \sum_{s=1}^{n_i} \mu_{i,j,q,s}\omega_{i,s}$. Then

$$\deg(\nu_{\ell,i,j} \cdot \mu_{i,j,q,s}) \leq 3c_{X_i}.$$

Proof. We apply Corollary 4.4.18 to $\mathcal{O}_X$ and obtain a basis matrix $T_{0,\mathcal{O}_X}$ of a $k[x]$-basis $\omega_1, \ldots, \omega_n$ of $R_0 = \mathcal{O}_X(V_0)$ with regards to Ω_i^m. We denote its entries by $\nu_{\ell,i,j}$ where $\ell = 1, \ldots, n$ runs through the columns and $i = 1, \ldots, m$, $j = 1, \ldots, n_i$ together indicate the rows. That is, $\omega_\ell = \sum_{i=1}^{m} \sum_{j=1}^{n_i} \nu_{\ell,i,j}\omega_{i,j}$. Now by Corollary 4.4.18, this basis matrix has entries whose degree is bounded as asserted. By Lemma 4.3.34, $\mu_{i,j,q,s}$ satisfies

$$\deg \mu_{i,j,q,s} \leq 2 \cdot \frac{2g_i + \dim_k H^0(X_i, \mathcal{O}_{X_i}) + n_i}{n_i} \leq 2c_{X_i}$$

and hence we deduce

$$\deg(\nu_{\ell,i,j} \cdot \mu_{i,j,q,s}) \leq c_{X_i} + 2c_{i,X} \leq 3c_{X_i}.$$

as asserted. □

Not only did we find a $k[x]$-basis of R_0 which has small degree with respect to Ω_i^m, but this does also imply that a reduced basis of R_0 has small degree with respect to Ω_i^m, too.

Lemma 4.6.2. *There exists a reduced basis Ω of R_0 whose basis matrix T_Ω with respect to Ω_i^m has degree bounded by $2c_X$.*

Proof. Since X is a cover of $\mathbb{P}_k^1$, by Definition 2.1.3 (ii), we know that $\mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$ and thus $(\widetilde{\omega}_{i,j})_{i,j}$ with $\widetilde{\omega}_{i,j} = x^{|X_i|_j}\omega_{i,j}$ forms an $\mathcal{O}_\infty$-basis of $\mathcal{O}_S$. By Corollary 4.6.1, there exists a basis $\beta_1, \ldots, \beta_n$ of R_0 whose basis matrix T_0 with respect to Ω_i^m has degree bounded by c_X. In particular, $T := \operatorname{diag}(x^{-|X_i|_j}) \cdot T_0$ is a basis transformation matrix from a basis of $\mathcal{O}_S$ to one of R_0. By Corollary 4.3.24, we know that $-|X_i|_j \leq c_{X_i}$ for all $i, j \in \{1, \ldots, n\}$ and hence the degree of the diagonal matrix $\operatorname{diag}(x^{-|X_i|_j})$ is bounded by

$$\max_{i,j \in \{1,\ldots,n\}} \{-|X_i|_j\} \leq \max_{i \in \{1,\ldots,n\}} \{c_{X_i}\} \leq c_X.$$

In particular, $\deg T \leq 2c_X$. By the proof of Theorem 4.3.15, we know that $\textsc{RedMat}(T)$ is a basis matrix of a reduced basis of R_0 with respect to $(\widetilde{\omega}_{i,j})_{i,j}$. In particular, $\operatorname{diag}(x^{|X_i|_j}) \cdot \textsc{RedMat}(T)$ is the respective basis matrix with respect to $\Omega_i^m = (\omega_{i,j})_{i,j}$. Since $|X_i|_j \leq 0$ for all $i, j \in \{1, \ldots, n\}$ and $\deg(\textsc{RedMat}(T)) \leq \deg T$, see Theorem A.2.7. This provides the desired basis matrix of a reduced basis of R_0 with respect to Ω_i^m having degree bounded by $2c_X$. □

Definition 4.6.3. Let us fix a reduced basis Ω as in Lemma 4.6.2 and we denote its basis matrix with respect to Ω_i^m by T_Ω. Note that analogously to Corollary 4.6.1 the multiplication table entries of Ω have degree bounded by $4c_X$. △

Remark 4.6.4. As already advocated in the end of Lemma 4.4.1, the matrix T_Ω provides a possible change of representation, see Remark 4.4.8 and the text following it. If T is a basis matrix of the basis $\mathcal{B}$ with respect to Ω, then we obviously have

$$\mathcal{B} = \Omega \cdot T = \Omega_i^m \cdot T_\Omega \cdot T$$

and thus $M = T_\Omega \cdot T$ is a matrix representing the basis $\mathcal{B}$ with respect to Ω_i^m. This matrix representation now provides the advantage of computing the restrictions to the irreducible components as revealed in Lemma 4.4.1. The computation of the matrix product $M = T_\Omega \cdot T$ requires at most $O^\sim(n^\omega d)$ operations in k if d is a common bound of $2c_X$ and the

degree of T. That is, if T has degree in $O(c_X)$, then the change of representation can be computed using at most $O^{\sim}(n^{\omega}c_X)$ operations in k. △

The next algorithm computes the basis matrices $T_{\mathcal{F}_i}$ as in Notation 4.4.7 from a given basis matrix with respect to either Ω or Ω_i^m. We will pass the information whether the given basis matrix represents a basis with respect to Ω or Ω_i^m to the algorithm in form of a Boolean c. We will use this notation throughout this thesis and it could be read as

$$c = \begin{cases} \textit{true}, & \textbf{c}\text{omponents are relevant: with respect to } \Omega_i^m \\ \textit{false}, & \textbf{c}\text{omponents are irrelevant: with respect to } \Omega \end{cases}$$

Algorithm 5 From a basis matrix with respect to Ω to one with respect to Ω_i^m

Precomputed	Basis Ω_i^m of R_0^+; basis matrix T_Ω of a reduced basis Ω
Input	$M_{\mathcal{F}}$ basis matrix of $\mathcal{F}(V_0)$ either with respect to Ω ($c = \textit{false}$) or to Ω_i^m ($c = \textit{true}$) where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal; c Boolean whether $M_{\mathcal{F}}$ is with respect to Ω or to Ω_i^m
Output	$T_{\mathcal{F}_1}, \ldots, T_{\mathcal{F}_m}$ basis matrices of $\mathcal{F}_1(V_{1,0}), \ldots, \mathcal{F}_m(V_{m,0})$, respectively

1: **procedure** ComputeComponentMatrices(T, c)
2: **if** $c = \textit{false}$ **then**
3: $T \leftarrow T_\Omega \cdot T$
4: **for** $i = 1, \ldots, m$ **do**
5: $p_i \leftarrow 1 + \sum_{j=1}^{i-1} n_j$
6: $T_i \leftarrow$ SubMatrix($T, (p_i, 1), (n_i, n)$)
7: $T_i \leftarrow$ RedMat(ColumnBasis(T_i))
8: **return** $T_1, \ldots, T_m$

Proposition 4.6.5. *The algorithm* ComputeComponentMatrices*, see Algorithm 5, is correct. Moreover, if d is an upper bound of the degrees of both $T = M_{\mathcal{F}}$ and T_Ω, then* ComputeComponentMatrices *requires at most $O^{\sim}(n^{\omega}d)$ operations in k and returns matrices with degree bounded by d.*

Proof. If c equals *true*, then $T = M_{\mathcal{F}}$ is a basis matrix of $\mathcal{F}(V_0)$ with respect to Ω_i^m. Otherwise, if $\mathcal{B}$ denotes the basis that is represented by $M_{\mathcal{F}}$, we have

$$\mathcal{B} = \Omega \cdot M_{\mathcal{F}} = \Omega_i^m \cdot T_\Omega \cdot M_{\mathcal{F}}$$

and hence $T := T_\Omega \cdot M_{\mathcal{F}}$ is the basis matrix representing $\mathcal{B}$ with respect to Ω_i^m. In particular, if we write

$$T = \begin{bmatrix} T_1 \\ T_2 \\ \vdots \\ T_m \end{bmatrix},$$

with $T_i \in k[x]^{n_i \times n}$ of rank n_i, then the columns of T_i represent a $k[x]$-generating set of $\mathcal{F}(V_{i,0})$. In particular, its column space equals $\mathcal{F}(V_{i,0})$ and thus ColumnBasis(T_i) $\in k[x]^{n_i \times n_i}$ is a basis matrix of $\mathcal{F}(V_{i,0})$, see Theorem A.2.15. Now the correctness of RedMat finally provides the correctness of ComputeComponentMatrices, see Theorem A.2.7.

Let us consider the running time assertion. The computation of the matrix product $T = T_\Omega \cdot M_{\mathcal{F}}$ requires at most $O^{\sim}(n^{\omega}d)$ operations in k. By assumption, $2d$ is an upper bound of $\deg(T)$. We consider the running time complexity of each **for** loop iteration: By Lemma A.1.2 (vi), we know that SubMatrix has constant cost. Since T has degree

bounded by $2d$, the same holds for all T_i. In particular, the average column degree s_i of T_i is bounded by $\deg(T_i) \leq 2d$. Thus, by Theorem A.2.15, the computation of ColumnBasis(T_i) requires at most $O^{\sim}(n_i^{\omega-1}nd)$ operations in k and it has degree bounded by $2d$. Thus, by Theorem A.2.7, calling RedMat requires $O^{\sim}(n_i^{\omega}d)$ operations in k. Now since $n \geq n_i$, each **for** loop iteration requires at most $O^{\sim}(n_i nd)$ operations in k. A simple computation shows

$$\sum_{i=1}^{m}(n_i^{\omega-1}nd) = nd\sum_{i=1}^{m}(n_i^{\omega-1}) \leq nd(\sum_{i=1}^{m}n_i)^{\omega-1} \leq ndn^{\omega-1} = n^{\omega}d$$

and hence the **for** loop overall requires at most $O^{\sim}(n^{\omega}d)$ operations in k and hence the running time assertion follows. □

Now we can combine ComputeComponentMatrices and RowBlockReduce to compute a row block reduced matrix for a given basis matrix of some $\mathcal{O}_X$-ideal $\mathcal{F}$ with $\mathcal{F}(S_i) = x^{r_i}\mathcal{O}_{S_i}$.

Algorithm 6 Compute row block reduced basis matrix

Precomputed	Basis Ω_i^m of R_0^+; $n_1, \ldots, n_m$; $c_{1,X}, \ldots, c_{m,X}$
Input	M basis matrix of $\mathcal{F}(V_0)$ with respect to Ω_i^m where $\mathcal{F}$ is a degree zero $\mathcal{O}_X$-ideal such that $\mathcal{F}(S_i) = x^{r_i}\mathcal{O}_{S_i}$ for all $i = 1, \ldots, m$
Output	M basis matrix of $\mathcal{F}(V_0)$ in n-block-form with row blocks M_i such that $\deg M_i \leq (\deg_k \mathcal{F}_i(V_{i,0}))/n_i + c_{i,X}$

1: **procedure** CompWiseRedMat(M)
2: $M_1, \ldots, M_m \leftarrow$ ComputeComponentMatrices(M, true)
3: **for** $i = 1, \ldots, m$ **do**
4: $r_i \leftarrow$ (Degree(Determinant(M_i)))$/n_i$
5: $d_i \leftarrow r_i + c_{i,X}$
6: $M \leftarrow$ RowBlockReduce($M, d_1, \ldots, d_m$)
7: **return** M

Remark 4.6.6. Note that by Proposition 4.4.20, the desired row block degrees

$$d_i = \left\lceil \frac{\deg_k \mathcal{F}_i(V_{i,0})}{n_i} + c_{i,X} \right\rceil$$

are those we can achieve using RowBlockReduce in algorithm CompWiseRedMat. But Proposition 4.4.21 shows that every, maybe easier to compute, upper bound of row block degrees of a possible right equivalent matrix of M suffices. △

Proposition 4.6.7. *The algorithm* CompWiseRedMat*, see Algorithm 6, is correct. Moreover, if d is an upper bound of the degree of $M_{\mathcal{F}}$, then* CompWiseRedMat *requires at most $O^{\sim}(n^{\omega}d)$ operations in k. In addition, the output matrix has degree bounded by d.*

Proof. The correctness of ComputeComponentMatrices provides that the matrices M_i are the basis matrices of a reduced basis of $\mathcal{F}_i(V_{i,0})$, see Proposition 4.6.5. The correctness of Degree and Determinant, together with Proposition D.2.7 provides $\deg\det(M_i) = \deg_k \mathcal{F}_i(V_{i,0})$. Since $\mathcal{F}$ has degree zero, by Corollary C.4.13, the latter equals $-\deg_k \mathcal{F}(S_i) = r_i n_i$ and thus $r_i = (\deg\det(M_i))/n_i$. By Proposition 4.4.20, we know that $d_i = r_i + c_{i,X}$ is an upper bound for the degree of the i-th row block of some right equivalent matrix of M. Thus, by Proposition 4.4.21, the algorithm RowBlockReduce does indeed compute a right equivalent matrix of M whose i-th row block has degree

bounded by d_i. This proves the correctness of CompWiseRedMat. The statement about the degree of the output matrix follows directly from Proposition 4.4.21.

Next we prove the running time assertion. Let d be an upper bound of $\deg M$. Then by Proposition 4.6.5, the computation of the matrices $M_1, \dots, M_m$ require at most $O^{\sim}(n^\omega d)$ operations in k. The matrices M_i are reduced basis matrices of $\mathcal{F}_i(V_{i,0})$ and thus, by Lemma 4.3.28, they satisfy $\deg M_i \leq (\deg_k \mathcal{F}_i(V_{i,0}))/n_i + c_{X_i} = r_i + c_{X_i}$ where the last equality follows from what we have already seen above. Therefore, by Lemma A.1.2 (ii) and (iv), the computation of r_i at line 4 requires at most $O^{\sim}(n_i^\omega(r_i + c_{X_i}))$ operations in k. The following computation

$$\begin{aligned}\sum_{i=1}^{m} n_i^\omega (r_i + c_{X_i}) \leq \max_{i=1}^{m}\{r_i + c_{X_i}\} \cdot \sum_{i=1}^{m} n_i^\omega &\leq \max_{i=1}^{m}\{r_i + c_{X_i}\} \cdot (\sum_{i=1}^{m} n_i)^\omega \\ &\leq \max_{i=1}^{m}\{r_i + c_{X_i}\} \cdot n^\omega,\end{aligned}$$

together with Lemma 2.4.11 and $r_i = (\deg_k \mathcal{F}_i(V_{i,0}))/n_i$ provides

$$\sum_{i=1}^{m} n_i^\omega (r_i + c_{X_i}) \leq \max_{i=1}^{m}\{(\deg_k \mathcal{F}_i(V_{i,0}))/n_i + c_{i,X}\} \cdot n^\omega.$$

Therefore, the **for** loop requires overall at most $O^{\sim}(\max_{i=1}^{m}\{(\deg_k \mathcal{F}_i(V_{i,0}))/n_i + c_{i,X}\} \cdot n^\omega)$ operations in k. Since d is an upper bound of $\deg M$, Proposition 4.4.20 provides that $d \geq \deg M \geq \max_{i=1}^{m}\{(\deg_k \mathcal{F}_i(V_{i,0}))/n_i + c_{i,X}\}$ and thus d is an upper bound as required for Proposition 4.4.21. The latter therefore provides that RowBlockReduce requires at most $O^{\sim}(n^\omega d)$ operations in k. □

With RedMat and CompWiseRedMat we now have two algorithms at hand to compute, given any basis matrix M of $\mathcal{F}(V_0)$ (where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal), a right equivalent matrix of M with reduced degree. We can use RedMat if M represents a basis with respect to Ω and CompWiseRedMat if M represents a basis with respect to Ω_i^m. But both play the same role of reducing a given basis matrix and will in Chapter 6 be used in the very same moments. Therefore, we introduce the algorithm ReduceBasisMatrix which calls one of them depending on the fixed basis (Ω or Ω_i^m as above) with respect to which the matrix is defined.

Definition 4.6.8. Let ReduceBasisMatrix denote the algorithm that, given a matrix $M \in k[x]^n$ and a Boolean c, calls CompWiseRedMat(M) if $c = \mathit{true}$ and RedMat(M) if $c = \mathit{false}$ and then returns the result. △

Lemma 4.6.9. *The products of the $\omega_{i,j}$ satisfy*

(i) $\omega_{i,j} \cdot \omega_{h,\ell} = 0$ *if* $i \neq h$, *and*

(ii) $\deg \phi_{\Omega_i^m}(\omega_{i,j} \cdot \omega_{i,\ell}) \leq -|X_i|_j - |X_i|_\ell$.

Proof. As elements of $\bigoplus_{i=1}^{m} R_{i,0}$ we clearly have $\omega_{i,j} \cdot \omega_{h,\ell} = 0$ whenever $i \neq h$. Property (ii) follows from Lemma 4.3.34. □

Lemma 4.6.10. *Let $f, g \in R_0^+ = \bigoplus_{i=1}^{m} R_{i,0}$ with*

$$f = \sum_{i=1}^{m}\sum_{j=1}^{n_i} \lambda_{i,j}\omega_{i,j}, \quad \textit{and} \quad g = \sum_{k=1}^{m}\sum_{\ell=1}^{n_k} \varepsilon_{k,\ell}\omega_{k,\ell}.$$

Let us denote the entries of the multiplication table of X_i by $\mu_{i,j,q,s}$, that is $\omega_{i,j}\omega_{i,q} = \sum_{s=1}^{n_i} \mu_{i,j,q,s}\omega_{i,s}$. Then

$$fg = \sum_{i=1}^{m}\sum_{s=1}^{n_i}\left(\sum_{j=1}^{n_i}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{i,\ell}\mu_{i,j,\ell,s}\right)\omega_{i,s} \tag{6:23}$$

and thus

$$\deg \phi_{\Omega_i^m}(fg) \leq \deg \phi_{\Omega_i^m}(f) + \deg \phi_{\Omega_i^m}(g) + 2c_X.$$

In particular, Eq. (6:23) shows that $\sum_{j=1}^{n_i}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{i,\ell}\mu_{i,j,\ell,s}$ are the coefficients of $f_{|X_i}g_{|X_i}$ with respect to $\omega_{i,1},\dots,\omega_{i,n_i}$ and hence $\phi_{\Omega_i^m}(fg)$ is simply the concatenation of the vectors $\phi_{\Omega_i}(f_{|X_i}g_{|X_i})$.

Proof. A simple computation shows

$$\begin{aligned}
fg &= \left(\sum_{i=1}^{m}\sum_{j=1}^{n_i}\lambda_{i,j}\omega_{i,j}\right)\cdot\left(\sum_{k=1}^{m}\sum_{\ell=1}^{n_k}\varepsilon_{k,\ell}\omega_{k,\ell}\right)\\
&= \sum_{i=1}^{m}\sum_{j=1}^{n_i}\sum_{k=1}^{m}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{k,\ell}\omega_{i,j}\omega_{k,\ell}\\
\text{Lemma 4.6.9 (i)} \rightsquigarrow &= \sum_{i=1}^{m}\sum_{j=1}^{n_i}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{i,\ell}\omega_{i,j}\omega_{i,\ell}\\
&= \sum_{i=1}^{m}\sum_{j=1}^{n_i}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{i,\ell}\left(\sum_{s=1}^{n_i}\mu_{i,j,\ell,s}\omega_{i,s}\right)\\
&= \sum_{i=1}^{m}\sum_{s=1}^{n_i}\left(\sum_{j=1}^{n_i}\sum_{\ell=1}^{n_i}\lambda_{i,j}\varepsilon_{i,\ell}\mu_{i,j,\ell,s}\right)\omega_{i,s}.
\end{aligned}$$

By Lemma 4.3.34, we have

$$\deg \mu_{i,j,\ell,s} \leq 2\frac{2g_i + \dim_k H^0(X,\mathcal{O}_{X_i}) + n_i}{n_i} \leq 2c_{i,X}$$

and thus $\max_{i=1}^{m}\{\deg \mu_{i,j,\ell,s}\} \leq 2c_X$ which provides the assertion. □

Corollary 4.6.11. *Let $f = \sum_{i,j}\lambda_{i,j}\omega_{i,j} \in R_0 \subseteq R_0^+ = \bigoplus_{i=1}^{m} R_{i,0}$ satisfy $\deg \lambda_{i,j} \leq d$ for all $i = 1,\dots,m$ and $j = 1,\dots,n_i$. Then the $k[x]$-basis matrix M_f representing the $k[x]$-basis $f\Omega = (f\omega_1,\dots,f\omega_n)$ of fR_0 satisfies*

$$\deg M_f \leq d + 3c_X.$$

Proof. The entries of M_f are the coefficients of $f\omega_\ell$ with respect to Ω_i^m. By Lemma 4.6.10, we know that the above coefficients that are non-zero are $\sum_{j=1}^{n_i}\sum_{q=1}^{n_i}\lambda_{i,j}\nu_{\ell,i,q}\mu_{i,j,q,s}$. By Corollary 4.6.1, we have $\deg(\nu_{\ell,i,q}) \leq c_X$ and thus Lemma 4.6.10 provides the assertion. □

Remark 4.6.12. After fixing the bases $\Omega = \omega_1,\dots,\omega_n$ and $\Omega_i^m = (\omega_{i,j})_{i,j}$ and having the products $\nu_{\ell,i,q}\mu_{i,j,q,s}$ precomputed, the proof of Corollary 4.6.11 resp. Lemma 4.6.10 already shows that the computation of the basis matrix M_f requires the computation of $\sum_{i=1}^{m} n_i^3 \leq n^3$ polynomial products of degree $\max\{d, 3c_X\}$. We will see that this might be too many products and hence we will come up with an efficient way of computing the required coefficients with a complexity in the order of $\sum_{i=1}^{m} n_i^2$ respectively n^2. △

Proposition 4.6.13. *Let $f \in R_0$ be arbitrary. Then*

(i) $\deg \mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(f) \leq \deg \phi_{\Omega_i^m}(f) + 3c_X$ *and*

(ii) $\deg \mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(f) \leq \deg \phi_{\Omega}(f) + 2c_X$.

Proof. By definition, we have $\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(f) = \mathrm{Tr}(M_f)$ where M_f denote the $k[x]$-basis matrix of fR_0 representing the $k[x]$-basis $f\Omega = (f\omega_1, \ldots, f\omega_n)$. Hence

$$\deg(\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(f)) = \deg(\mathrm{Tr}(M_f)) \leq \deg M_f.$$

By Corollary 4.6.11, we have $\deg M_f \leq \deg \phi_{\Omega_i^m}(f) + 3c_X$ which provides (i). By Corollary 4.5.3, we have $\deg M_f \leq \deg \phi_{\Omega}(f) + 2c_X$ which provides (ii). □

4.7 Regular Global Sections and Test of Identity

In this section we look for the general analogue of the following statement which is standard for integral schemes. This establishes the theoretical background for deciding whether a given degree zero divisor is principal or not.

Lemma 4.7.1 ([Liu02], 7.3.25)**.** *Let X be an integral projective scheme over k. Let $D \in \mathrm{Div}^0(X)$. Then D is principal if and only if $\mathcal{O}_X(D)(X) \neq 0$.*

Remark 4.7.2. The proof of Lemma 4.7.1 reveals that any of the non-zero elements f in $\mathcal{O}_X(D)(X)$ will satisfy $\mathrm{div}(f^{-1}) = D$ in the case that D is principal. △

Lemma 4.7.3. *Let X be an integral cover of $\mathbb{P}^1_k$. Let $D \in \mathrm{Div}^0(X)$. Let $\alpha_1, \ldots, \alpha_n$ be a reduced basis of $\mathcal{O}_X(D)(V_0)$. Then the following are equivalent:*

(i) D is principal,

(ii) $\mathcal{O}_X(D)(X) \neq 0$, and

(iii) $\mathrm{div}(\alpha_1^{-1}) = D$.

Proof. The equivalence between (i) and (ii) is due to Lemma 4.7.1. The implication (iii) ⇒ (i) is obvious. Now assume that D is principal. Hence $\mathcal{O}_X(D)(X) \neq 0$ and thus, by Remark 4.3.19, we have $0 \geq -|D|_1$ providing $|D|_1 \geq 0$ and hence, by Theorem 4.3.15, this implies $\alpha_1 \in \mathcal{O}_X(D)(X)$. Now Remark 4.7.2 provides $D = \mathrm{div}(\alpha_1^{-1})$. □

In the more general case of reducible X this does not stay true anymore. But with a slight adaption in which we only care about regular global sections of $\mathcal{O}_X(D)$ it will, at least to some extent, still be true. For notational reasons we introduce the following notion:

Definition 4.7.4. Let $D \in \mathrm{Div}(X)$ be a Cartier divisor on X. Then set $\mathcal{L}_{\mathrm{reg}}(D) = \mathcal{O}_X(D)(X) \cap \mathcal{K}_X(X)^\times$. △

Lemma 4.7.5. *Let $D \in \mathrm{Div}(X)$. Then we have*

$$\mathcal{L}_{\mathrm{reg}}(D) = \{f \in \mathcal{K}_X(X)^\times \mid \mathrm{div}(f) + D \geq 0\}.$$

Proof. By Lemma 3.1.32, we have $f \in \mathcal{O}_X(D)(X)$ if and only if $\mathrm{div}(f) + D \geq 0$ for every $f \in \mathcal{K}_X(X)^\times$. □

Lemma 4.7.6 ([Liu02], 3.3.21)**.** *Let X be a reduced, connected projective scheme over a field k. Then $H^0(X, \mathcal{O}_X)$ is a finite field extension of k. Moreover, if X is geometrically reduced and geometrically connected, then $H^0(X, \mathcal{O}_X) = k$.*

Lemma 4.7.7. *Let X be a projective curve over k. Let $D \in \mathrm{Div}(X)$ be effective and have degree zero. Then $D = 0$.*

Proof. Then we have $\mathcal{O}_X(-D) \leq \mathcal{O}_X$ and by [Liu02, 7.3.5], we deduce $0 = \deg_k D = \sum_{P \in X} \dim_k \mathcal{O}_{X,P}/\mathcal{O}_X(-D)_P$ and thus $\dim_k \mathcal{O}_{X,P}/\mathcal{O}_X(-D)_P = 0$ which gives $\mathcal{O}_X(-D)_P = \mathcal{O}_{X,P}$ for all $P \in X$. Now Corollary B.1.30 already provides $\mathcal{O}_X(D) = \mathcal{O}_X$ and hence $D = 0$. □

Lemma 4.7.8. *Let X be a projective curve over k. Let $D \in \mathrm{Div}(X)$ and $f \in \mathcal{K}_X(X)^\times$. Then*

$$\mathcal{L}_{\mathrm{reg}}(D + \mathrm{div}(f)) \cong f^{-1}\mathcal{L}_{\mathrm{reg}}(D).$$

In particular,

$$\mathcal{L}_{\mathrm{reg}}(\mathrm{div}(f)) \cong f^{-1}H^0(X, \mathcal{O}_X)^\times.$$

If $H^0(X, \mathcal{O}_X) = k$, then $\mathcal{L}_{\mathrm{reg}}(\mathrm{div}(f)) \cong f^{-1}k^\times$.

Proof. By definition of Cartier divisors, we have $\mathrm{div}(g) + \mathrm{div}(f) = \mathrm{div}(gf)$ for any two $f, g \in \mathcal{K}_X(X)^\times$. Thus

$$\begin{aligned}\mathcal{L}_{\mathrm{reg}}(D + \mathrm{div}(f)) &= \{g \in \mathcal{K}_X(X)^\times \mid \mathrm{div}(g) + \mathrm{div}(f) + D \geq 0\} \\ &= f^{-1}\{g \in \mathcal{K}_X(X)^\times \mid \mathrm{div}(g) + D \geq 0\} \\ &= f^{-1}\mathcal{L}_{\mathrm{reg}}(D).\end{aligned}$$

To prove the particular part note that every $g \in \mathcal{L}_{\mathrm{reg}}(0)$ satisfies $\mathrm{div}(g) \geq 0$ and thus by Lemma 4.7.7 we deduce $\mathrm{div}(g) = 0$. This is equivalent to $g \in \mathcal{O}_X(X)^\times$ and hence $\mathcal{L}_{\mathrm{reg}}(0) = H^0(X, \mathcal{O}_X)^\times$. □

Lemma 4.7.9. *Let X be a projective curve over k. Let $D \in \mathrm{Div}^0(X)$ be a degree zero Cartier divisor on X. Then $\mathcal{L}_{\mathrm{reg}}(D) \neq \emptyset$ if and only if D is principal.*

Proof. By definition, we have $\mathcal{L}_{\mathrm{reg}}(D) = \{f \in \mathcal{K}_X(X)^\times \mid \mathrm{div}(f) + D \geq 0\}$. If $D = \mathrm{div}(g)$ for some $g \in \mathcal{K}_X(X)^\times$, then $\mathrm{div}(g^{-1}) + D = 0$ and thus $g^{-1} \in \mathcal{L}_{\mathrm{reg}}(D)$. Conversely, if $f \in \mathcal{L}_{\mathrm{reg}}(D)$, then $E := \mathrm{div}(f) + D \geq 0$ is effective and still has degree zero. Thus by Lemma 4.7.7, we have $E = 0$ and hence deduce $D = -\mathrm{div}(f) = \mathrm{div}(f^{-1})$. □

Chapter 5

Picard Group and its Structure

In this chapter we examine the so called Picard group and the associated degree zero Picard group of a scheme. First, we give the definitions of both groups. To do so, the reader may recall that invertible sheaves on a scheme X (or more generally, on a locally ringed space) are those $\mathcal{O}_X$-modules that are locally free of rank 1. These are $\mathcal{O}_X$-modules that are locally isomorphic to $\mathcal{O}_X$. That is, the $\mathcal{O}_X$-module $\mathcal{F}$ is invertible if and only if for every $P \in X$ there is an open neighborhood $U \subseteq X$ of P such that $\mathcal{F}_{|U}$ is isomorphic to $\mathcal{O}_U$. It is straightforward to prove that for every invertible sheaf $\mathcal{F}$, the $\mathcal{O}_X$-module $\mathcal{F}^\vee = \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{O}_X)$ is again invertible and satisfies $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{F}^\vee \cong \mathcal{O}_X$. This justifies that we also write $\mathcal{F}^{-1} := \mathcal{F}^\vee$ in this case.

Definition 5.0.1. Let X be a scheme. By $\mathrm{Pic}(X)$ we denote the set of isomorphism classes of invertible sheaves on X. As we have seen above, $\mathrm{Pic}(X)$ together with the tensor product $\otimes_{\mathcal{O}_X}$ of $\mathcal{O}_X$-modules form a group with neutral element $\mathcal{O}_X$. We call this group the **Picard group** of X. △

Note that the Picard group could also be defined for ringed spaces. To define the degree zero Picard group, we need to define the degree of invertible sheaves first. Since the sheaf $\mathcal{O}_X(D)$ associated to a divisor $D \in \mathrm{Div}(X)$ is invertible, the notion of degree of an invertible sheaf should be compatible with the degree of the divisor D and, moreover, compatible with the degree of the $\mathcal{O}_X$-ideal $\mathcal{O}_X(D)$. As we have already seen in Definition 3.1.10, the degree of divisors is only defined for divisors on curves over k. Moreover, the degree of $\mathcal{O}_X$-ideals, see Definition C.4.1, is defined for $\mathcal{O}_X$-ideals on curves of finite residual-type over k. These definitions do depend on the dimension of X and are only well-defined if X has dimension at most one. We want to use the degree of $\mathcal{O}_X$-ideals to define the degree of invertible sheaves on curves of finite residual-type over k. By Lemma 4.1.2, every invertible sheaf $\mathcal{L}$ is isomorphic to some $\mathcal{O}_X$-submodule $\mathcal{F}$ of $\mathcal{K}_X$ which is then by Definition 3.1.13 an $\mathcal{O}_X$-ideal. Therefore, we could define the degree of $\mathcal{L}$ to be the degree of $\mathcal{F}$. This makes sense since the degrees of two isomorphic $\mathcal{O}_X$-ideals are equal. Whenever X is additionally projective, by Lemma C.4.4, we have $\deg_k \mathcal{F} = \chi(\mathcal{O}_X) - \chi(\mathcal{F})$. We do only care about the degree zero Picard group in the case of projective curves over k and thus we define the degree of an invertible sheaf as follows.

Definition 5.0.2. Let X be a projective curve over k. Let $\mathcal{L}$ be an invertible sheaf on X. Then we define its **degree** as

$$\deg_k \mathcal{L} = \chi(\mathcal{O}_X) - \chi(\mathcal{L}).$$ △

In the literature, the degree zero Picard group of an irreducible scheme X is defined to be the subgroup of $\mathrm{Pic}(X)$ consisting of those isomorphism classes of degree zero. To expand this definition to the class of reducible schemes, we require the invertible sheaf to have

degree zero restrictions to every single irreducible component of X. This enables us to link the degree zero Picard group of a reducible scheme to those of its irreducible components.

Definition 5.0.3. Let X be a reduced projective curve over k. By $\mathrm{Pic}^0(X)$ we denote the subset of $\mathrm{Pic}(X)$ consisting of those isomorphism classes that have degree zero restriction to every irreducible component of X. By Proposition C.4.15 and Lemma C.4.7, we see that $\mathrm{Pic}^0(X)$ together with the tensor product of $\mathcal{O}_X$-modules forms a subgroup of $\mathrm{Pic}(X)$ which we call the **degree zero Picard group of** X. △

Remark 5.0.4. Moreover, this definition is not too far away from the more general definition which does not take into account what the degrees of the restrictions are and only requires the global degree to be zero. For instance, if $\bar{k}$ denotes an algebraic closure of k, then the above (more general) definition of the degree zero Picard group comes down to those isomorphism classes whose restriction to the i-th component of the base extended $X_{\bar{k}} = X \otimes_k \bar{k}$ has degree zero, see [BLR90, Chapter 9, Cor. 13]. In particular, our definition coincides with the general one for algebraically closed k. △

Definition 5.0.5. Analogously to Definition 5.0.3, we define the group $\mathrm{ClInvId}^0(X)$ of degree zero invertible $\mathcal{O}_X$-ideals. △

As we will see in what follows, the Picard group is very closely related to the group of Cartier divisor classes and also to the first cohomology group of $\mathcal{O}_X^\times$. Moreover, we will define the degree zero divisor class group and will see that it is essentially the same as $\mathrm{Pic}^0(X)$.

This chapter is organised as follows: In Section 5.1 we will try to give a characterisation of the Picard group in the affine case. In Section 5.2 we will see the close relation between the Picard group and $H^1(X, {\mathcal{O}_X}^\times)$ and will conclude that the groups

$$\mathrm{ClInvId}(X),\ \mathrm{CaCl}(X),\ H^1(X, {\mathcal{O}_X}^\times) \text{ and } \mathrm{Pic}(X)$$

are all isomorphic, see Corollary 5.2.12.

In Sections 5.3 and 5.4 we will examine the relation between divisors on a scheme and divisors on a schematically dense open subscheme respectively the relation between divisors on a reducible scheme and divisors on the irreducible components. Then in Section 5.5 we relate divisors on a cover X of $\mathbb{P}^1_k$ to divisors on V_0 and S to see that the former and the latter are essentially the same. In Section 5.6 we define $\mathrm{CaCl}^0(X)$, the group of degree zero Cartier divisor classes, and $\mathrm{CaCl}^0_\pi(X)$, the group of degree zero Cartier divisor classes with respect to π which only considers representatives of the former group of a specific form. We will conclude that $\mathrm{CaCl}^0(X) \cong \mathrm{CaCl}^0_\pi(X)$ are both isomorphic to a specific ideal class group $\mathcal{I}_\pi/\mathcal{P}_\pi$ which is a rather general result which to the best knowledge of the author has not been well known yet. Moreover, there will be two kinds of representatives, one which is somehow independent of the irreducible components of X and one which is component dependent. In what follows by then we will distinguish between these two representatives that reflect two different algorithmic approaches on how to compute in $\mathcal{I}_\pi/\mathcal{P}_\pi$. The elements by which we may alter representatives in the ideal class group $\mathcal{I}_\pi/\mathcal{P}_\pi$ are called modification functions and in Section 5.7 we will analyse those and give proofs of their existence with bounded degree and we will also provide algorithms to compute them. In Sections 5.8 and 5.9 we prove that each class in $\mathcal{I}_\pi/\mathcal{P}_\pi$ has a representative with bounded degree and we show how to compute with those representatives only using basis matrices.

5.1 Divisor Group and Picard Group in the Affine Case

In this section we will show how the Picard group looks like in the case of an affine scheme X.

Lemma 5.1.1. *Let R be a noetherian ring. The set of isomorphism classes of invertible R-modules together with the tensor product of R-modules forms a group, denoted by* $\mathrm{Pic}(R)$ *and called the Picard group of R.*

Proof. The name is suggested in [Eis95, p. 255] and the assertion follows entirely from [Eis95, 11.6]. □

But there is a certain subclass of invertible R-modules that do indeed form a group without considering equivalence classes. The set of invertible R-ideals M, which are all embedded in $\mathrm{Frac}(R)$, and thus yield a more explicit inverse $M^{-1} = \{x \in \mathrm{Frac}(R) \mid xM \subseteq R\}$ resulting in an equality $MM^{-1} = R$, yield a group with the ideal product being the group law.

Lemma 5.1.2. *Let R be a noetherian ring. The set of invertible R-ideals together with the product of R-ideals form a group. This group is sometimes denoted by $C(R)$ and called the group of Cartier divisors.*

Proof. Again, the name is suggested in [Eis95, p. 255 f.]. The assertion follows from [Eis95, 11.6]. □

Note that we have already proved in Proposition 3.1.27 that $\mathrm{InvId}(X)$ is isomorphic to the group $\mathrm{Div}(X)$ of Cartier divisors on X for any scheme X. Next we justify the above names by proving that $\mathrm{InvId}(\mathrm{Spec}(R)) \cong C(R)$ and $\mathrm{Pic}(\mathrm{Spec}(R)) \cong \mathrm{Pic}(R)$.

Proposition 5.1.3. *Let X be an affine curve of finite residual-type over k. Then*

$$\begin{array}{ccc} C(R) & \to & \mathrm{InvId}(X) \\ M & \mapsto & M^{\sim} \end{array}$$

defines an isomorphism of abelian groups.

Proof. By Lemma C.4.10, the map $M \mapsto M^{\sim}$ establishes an equivalence of categories between the category of R-ideals and the category of $\mathcal{O}_X$-ideals. Clearly, $M_P \cong (M^{\sim})_P$ for all $P \in \mathrm{Spec}(R)$ and thus M is invertible if and only if $M^{\sim}$ is invertible. Hence, the map $M \mapsto M^{\sim}$ gives a bijection between $C(R)$ and $\mathrm{InvId}(X)$. Finally, we prove that $M \mapsto M^{\sim}$ defines a group homomorphism. For all $P \in X$ we obviously have $(MN)_P = M_P N_P$ as subsets of $\mathrm{Frac}(R_P)$. This means that both $(MN)^{\sim}$ and $M^{\sim}N^{\sim}$ have equal stalks for all $P \in X$ (by definition, we have $(\mathcal{FG})_P = \mathcal{F}_P\mathcal{G}_P$ inside $\mathcal{K}_{X,P}$ for $\mathcal{O}_X$-ideals $\mathcal{F}$ and $\mathcal{G}$) and thus by Corollary B.1.30, they are equal as subsheaves of $\mathcal{K}_X$. □

Proposition 5.1.4. *Let X be an affine curve of finite residual-type over k. Then there is an isomorphism* $\mathrm{Pic}(R) \to \mathrm{Pic}(X)$ *given by* $C(R) \to \mathrm{InvId}(X)$ *from Proposition 5.1.3 on representatives.*

Proof. Since R is noetherian, [Eis95, 11.7] provides that the natural map $C(R) \to \mathrm{Pic}(R)$ sending an invertible R-ideal to its isomorphism class is surjective. Moreover, its kernel is given by principal R-ideals fR with $f \in \mathrm{Frac}(R)^{\times}$. Therefore, for every isomorphism class in $\mathrm{Pic}(R)$ we find a representative $M \in C(R)$ which corresponds by Proposition 5.1.3 to $M^{\sim} \in \mathrm{InvId}(X)$. Then the surjective map $\mathrm{InvId}(X) \to \mathrm{Pic}(X)$, see Remark 3.1.22, sending an invertible $\mathcal{O}_X$-ideal to its isomorphism class provides that we may associate to each element in $\mathrm{Pic}(R)$ an element in $\mathrm{Pic}(X)$. Now any two representatives $M, N \in C(R)$

of the same class in $\mathrm{Pic}(R)$ differ multiplicatively by some fR with $f \in \mathrm{Frac}(R)^\times$, due to [Eis95, 11.7]. Hence $M = fN$ and thus $M^\sim = (fN)^\sim = (fR)^\sim N^\sim = f\mathcal{O}_X N^\sim$ by Proposition 5.1.3. This provides that the multiplication with f morphism $N^\sim \to M^\sim$ is an isomorphism and hence we obtain a well-defined map $\phi : \mathrm{Pic}(R) \to \mathrm{Pic}(X)$. By construction, this provides a commutative diagram:

$$\begin{array}{ccc} C(R) & \xrightarrow[\cong]{M \mapsto M^\sim} & \mathrm{InvId}(X) \\ \downarrow & & \downarrow \\ \mathrm{Pic}(R) & \xrightarrow{\phi} & \mathrm{Pic}(X) \end{array}$$

Now ϕ is obviously surjective and its kernel is given by classes with representatives M such that $M^\sim \cong \mathcal{O}_X$. By Lemma 3.1.26, the latter is equivalent to $M^\sim = f\mathcal{O}_X$ and hence by Proposition 5.1.3, we have $M = (f\mathcal{O}_X)(X) = f\mathcal{O}_X(X) = fR \cong R$ providing the injectivity of ϕ. □

5.2 Picard Group and Cohomology

Sometimes the Picard group of a scheme is defined as $H^1(X, \mathcal{O}_X^\times)$, the first Čech cohomology group of the sheaf of invertible regular functions on X. We will see that this is justified by proving that $H^1(X, \mathcal{O}_X^\times)$ is isomorphic to $\mathrm{Pic}(X)$. Moreover, we will also show more isomorphic models of $\mathrm{Pic}(X)$.

In the following we will, very briefly, recall what the Čech cohomology is. To do so, we follow the exposition in and refer to [Liu02, Chapter 5.2] for more information and proofs of the statements we make.

Let X be a topological space, $\mathcal{U} = \{U_i \mid i \in I\}$ an open cover and we put $U_{i_0,\ldots,i_p} := U_{i_0} \cap \ldots \cap U_{i_p}$. For a sheaf $\mathcal{F}$ on X and $p \geq 0$ let the set of **p-cochains of $\mathcal{U}$ in $\mathcal{F}$** be

$$C^p(\mathcal{U}, \mathcal{F}) = \prod_{(i_0,\ldots,i_p) \in I^{p+1}} \mathcal{F}(U_{i_0,\ldots,i_p})$$

which comes with a map $d^p : C^p(\mathcal{U}, \mathcal{F}) \to C^{p+1}(\mathcal{U}, \mathcal{F})$ sending $(\alpha_{i_0,\ldots,i_p})$ to

$$(d^p \alpha_{i_0,\ldots,i_p})_{i_0\ldots,i_{p+1}} = \sum_{k=0}^{p+1} (-1)^k (\alpha_{i_0,\ldots,\widehat{i_k},\ldots,i_{p+1}})_{|U_{i_0,\ldots,i_{p+1}}}$$

where $\widehat{i_k}$ means "omitted". For all p we have $d^{p+1} \circ d^p = 0$, that is the $C^p(\mathcal{U}, \mathcal{F})$ with d^p form a *complex*. For $p \geq 0$ we set

$$H^p(\mathcal{U}, \mathcal{F}) = \frac{\ker(d^p : C^p(\mathcal{U}, \mathcal{F}) \to C^{p+1}(\mathcal{U}, \mathcal{F}))}{\mathrm{im}(d^{p-1} : C^{p-1}(\mathcal{U}, \mathcal{F}) \to C^p(\mathcal{U}, \mathcal{F}))} \tag{2:1}$$

and, by convention, $C^{-1}(\mathcal{U}, \mathcal{F}) = 0$ which implies $H^{-1}(\mathcal{U}, \mathcal{F}) = 0$.

For the cases $p = 0, 1$ we have by definition:

1. $H^0(\mathcal{U}, \mathcal{F}) = \mathcal{F}(X)$:

   By definition, $H^0(\mathcal{U}, \mathcal{F})$ equals the kernel of $d^0 : C^0(\mathcal{U}, \mathcal{F}) \to C^1(\mathcal{U}, \mathcal{F})$ which maps as follows:

   $$\begin{array}{rcl} \prod_{i \in I} \mathcal{F}(U_i) & \to & \prod_{i,j \in I} \mathcal{F}(U_i \cap U_j) \\ (f_i)_{i \in I} & \mapsto & ((f_i)_{|U_i \cap U_j} - (f_j)_{|U_i \cap U_j})_{i,j \in I} \end{array}$$

Hence its elements are given by local sections of $\mathcal{F}$ over an open covering of X which agree on the overlaps. This equals the definition of the global sections of $\mathcal{F}$.

2. $H^1(\mathcal{U}, \mathcal{F})$ consists of the group of α_{i_0,i_1} in $\prod_{(i_0,i_1)\in I^2} \mathcal{F}(U_{i_0,i_1})$ such that

$$\forall\ i_0, i_1, i_2 \in I^3 : \quad (\alpha_{i_0,i_1})_{U_{i_0,i_1,i_2}} = (\alpha_{i_0,i_2})_{U_{i_0,i_1,i_2}} - (\alpha_{i_1,i_2})_{U_{i_0,i_1,i_2}}$$

modulo the group of those α_{i_0,i_1} in $\prod_{(i_0,i_1)\in I^2} \mathcal{F}(U_{i_0,i_1})$ such that

$$\alpha_{i_0,i_1} = (\alpha_{i_0})_{|U_{i_0,i_1}} - (\alpha_{i_1})_{|U_{i_0,i_1}}$$

with $\alpha_{i_j} \in \mathcal{F}(U_{i_j})$, $j = 1, 2$, for all $i_0, i_1 \in I$.

For two covers $\mathcal{U} = \{U_i \mid i \in I\}$ and $\mathcal{V} = \{V_j \mid j \in J\}$ we say that $\mathcal{V}$ **is a refinement of** $\mathcal{U}$ if there is a map $\sigma : J \to I$ such that for every $j \in J$ we have $V_j \subseteq U_{\sigma(j)}$. This induces a homomorphism, which is also denoted by σ,

$$\sigma : C^p(\mathcal{U}, \mathcal{F}) \to C^p(\mathcal{V}, \mathcal{F}), \quad \sigma(\alpha)_{j_0,\ldots,j_p} = (\alpha_{\sigma(j_0),\ldots,\sigma(j_p)})_{|V_{j_0,\ldots,j_p}}.$$

Since σ commutes with the maps d^p, we obtain a homomorphism

$$\sigma^* : H^p(\mathcal{U}, \mathcal{F}) \to H^p(\mathcal{V}, \mathcal{F}). \tag{2:2}$$

It can be shown that the map σ^* is independent of the choice of σ, [Liu02, 5.2.8]. An implication of this is that if $\mathcal{U}$ is a refinement of $\mathcal{V}$ and vice versa, then σ^* is an isomorphism.

The "*is a refinement of*"-property defines a partial ordering on the family of open coverings of X which is filtering since for any two coverings $\mathcal{U} = \{U_i \mid i \in I\}$ and $\mathcal{V} = \{V_j \mid j \in J\}$ the open cover $\{U_i \cap V_j \mid i \in I, j \in J\}$ is a refinement of both $\mathcal{U}$ and $\mathcal{V}$. We call two coverings **equivalent** if and only if one is a refinement of the other and vice versa. Hence, up to isomorphism, $H^p(\mathcal{U}, \mathcal{F})$ only depends on the equivalence class of $\mathcal{U}$.

Definition 5.2.1. Let X be a topological space and $\mathcal{F}$ a sheaf on X. We set

$$H^p(X, \mathcal{F}) = \varinjlim_{\mathcal{U}} H^p(\mathcal{U}, \mathcal{F})$$

where $\mathcal{U}$ runs through the classes of open coverings of X. The group $H^p(X, \mathcal{F})$ is called the p**-th (Čech) cohomology group of** $\mathcal{F}$. △

The natural map $H^p(\mathcal{U}, \mathcal{F}) \to H^p(X, \mathcal{F})$ turns out to be an isomorphism of groups for all $p \geq 0$ whenever the objects involved are nice enough:

Proposition 5.2.2. *Let X be a separated scheme, $\mathcal{F}$ a quasi-coherent sheaf on X and $\mathcal{U}$ an affine cover of X. Then the natural map $H^p(\mathcal{U}, \mathcal{F}) \to H^p(X, \mathcal{F})$ is an isomorphism. In particular, for every two affine open covers $\mathcal{U}$ and $\mathcal{V}$ of X, we have for all $p \geq 0$*

$$H^p(\mathcal{U}, \mathcal{F}) \cong H^p(\mathcal{V}, \mathcal{F}).$$

Proof. This is [Liu02, 5.2.19]. □

That is, up to isomorphism, the cohomology groups of quasi-coherent modules are independent of the chosen affine cover on a separated scheme.

We shortly list some of the properties of the Čech cohomology groups we need.

Lemma 5.2.3. *Let X be a separated scheme and $\mathcal{F}$ a quasi-coherent sheaf on X. If there is an affine cover of X made up of n open sets, then $H^p(X, \mathcal{F}) = 0$ for all $p \geq n$.*

Proof. This is [Liu02, 5.2.19], together with [Liu02, 5.2.5]. □

Corollary 5.2.4. *Let X be a projective scheme of dimension n over the field k. Let $\mathcal{F}$ be a quasi-coherent sheaf on X. Then $H^p(X, \mathcal{F}) = 0$ for all $p > n$.*

Proof. By Theorem D.1.6, there is a finite morphism $\pi : X \to \mathbb{P}^n_k$ which is, by [Sta18, Tag 01WN], affine. Hence it induces an affine cover made up of $n+1$ open subsets by considering the affine open preimages of the standard affine patches of $\mathbb{P}^n_k$. Then the assertion follows from Lemma 5.2.3. □

Lemma 5.2.5 ([Liu02] 5.2.15)**.** *Let X be a topological space and let*

$$0 \to \mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H} \to 0 \tag{2:3}$$

be an exact sequence of sheaves on X. Then there exists a canonical homomorphism $\delta : H^0(X, \mathcal{H}) \to H^1(X, \mathcal{F})$ such that the sequence

$$0 \to \mathcal{F}(X) \to \mathcal{G}(X) \to \mathcal{H}(X) \xrightarrow{\delta} H^1(X, \mathcal{F}) \to H^1(X, \mathcal{G}) \to H^1(X, \mathcal{H})$$

*is exact. We call δ the **1-connecting morphism** or simply the **connecting morphism** of the sequence (2:3).*

Proof. We only want to highlight how the proof constructs the map δ and refer the reader for the rest of the proof to [Liu02, 5.2.15]. By the definition of surjectivity of a morphism of sheaves, the morphisms $\beta_P : \mathcal{G}_P \to \mathcal{H}_P$ for all $P \in X$ are surjective. Hence, for every global section $h \in \mathcal{H}(X)$ there is an open cover $\mathcal{U} = \{U_i \mid i \in I\}$ of X (which depends on h) and sections $g_i \in \mathcal{G}(U_i)$ such that $\beta(U_i)(g_i) = h_{|U_i}$. For $i, j \in I$ let $U_{i,j} = U_i \cap U_j$. Now for all $i, j \in I$ we have

$$\beta(U_{i,j})(g_{i|U_{i,j}} - g_{j|U_{i,j}}) = 0$$

and thus by the exactness of the sequence, there are $f_{i,j} \in \mathcal{F}(U_{i,j})$ such that

$$\alpha(U_{i,j})(f_{i,j}) = g_{i|U_{i,j}} - g_{j|U_{i,j}}.$$

Since $\mathcal{U}$ forms an open cover of X, the same is true for $\mathcal{V} := \{U_{i,j} \mid i, j \in I\}$. Therefore, the family $\{(U_{i,j}, f_{i,j}) \mid i, j \in I\}$ forms an element of $C^1(\mathcal{V}, \mathcal{F})$. Now the proof of [Liu02, 5.2.15] provides that this also induces an element of $H^1(\mathcal{V}, \mathcal{F})$ and thus one in $H^1(X, \mathcal{F})$. Moreover, it shows that the latter is independent of the choice of $\mathcal{U}$. Hence we obtain a well-defined morphism $\delta : H^0(X, \mathcal{H}) \to H^1(X, \mathcal{F})$. □

Remark 5.2.6. To summarise the construction on the connecting morphism δ, we may phrase it as a recipe: Once we are able to come up with local preimages of a global section of the right hand side sheaf, we take their pair-wise differences (or quotient whenever we work multiplicatively) and these define a well-defined element in the first Čech cohomology group of the left hand side sheaf. △

Proposition 5.2.7. *Let X be a locally noetherian scheme. Then the group homomorphism induced by the following map on representatives*

$$\begin{array}{rcl} \delta : H^0(X, \mathcal{K}_X^\times / \mathcal{O}_X^\times) & \to & H^1(X, \mathcal{O}_X^\times) \\ \left(U_i, \frac{f_i}{g_i}\right)_{i \in I} & \mapsto & \left(U_i \cap U_j, \frac{f_i g_j}{f_j g_i}\right)_{i,j \in I} \end{array}$$

is an isomorphism $\mathrm{CaCl}(X) \to H^1(X, \mathcal{O}_X^\times)$.

Proof. First of all, recall that $\mathrm{CaCl}(X)$ is defined as $H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$ modulo the image of the morphism $H^0\left(X, \mathcal{K}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$. We have the canonical exact sequence

$$0 \longrightarrow \mathcal{O}_X^\times \longrightarrow \mathcal{K}_X^\times \longrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times \longrightarrow 0.$$

By Lemma B.2.4, we have $H^1\left(X, \mathcal{K}_X^\times\right) = 0$ and thus the long exact sequence of cohomology groups from Lemma 5.2.5 derived from the sequence above is

$$0 \longrightarrow H^0\left(X, \mathcal{O}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) \xrightarrow{\delta} H^1\left(X, \mathcal{O}_X^\times\right) \longrightarrow 0.$$

The morphism δ is the connecting morphism and maps (which can be seen by examining the proof of Lemma 5.2.5 and following the recipe of how to compute the connecting morphism in Remark 5.2.6) representatives as follows:

$$\begin{array}{rcl} \delta : H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) & \to & H^1\left(X, \mathcal{O}_X^\times\right) \\ \left(U_i, \frac{f_i}{g_i}\right)_{i\in I} & \mapsto & \left(U_i \cap U_j, \frac{f_i g_j}{f_j g_i}\right)_{i,j\in I} \end{array}$$

Note that by Lemma 5.2.5, the morphism δ is well-defined and surjective.

Let $D = (U_i, f_i/g_i)_{i\in I}$ be a configuration of a divisor lying in the kernel of δ. That is, $\frac{f_i g_j}{f_j g_i} = 1$ and therefore $\frac{f_i}{g_i} = \frac{f_j}{g_j}$ over all $U_i \cap U_j$ and all $i, j \in J$. Hence, D lies in the image of $H^0\left(X, \mathcal{K}_X^\times\right) \to H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$ and is therefore a principal divisor. Conversely, let $D = (X, f)$ with $f \in \mathcal{K}_X(X)^\times$ be a principal divisor, then $\delta(D) = (U_i \cap U_j, 1)_{i,j\in I}$ is the trivial element in $H^1\left(X, \mathcal{O}_X^\times\right)$. Therefore, we obtain $\ker\delta = \mathrm{im}(H^0\left(X, \mathcal{K}_X^\times\right) \to H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right))$ and together with the surjectivity of δ this provides the desired isomorphism. □

Proposition 5.2.8 ([DG67])**.** *Let X be a scheme satisfying one of the following hypotheses:*

1. *X is locally noetherian and $\mathrm{Ass}(\mathcal{O}_X)$ is contained in an affine open subset, or*
2. *X is reduced and the number of irreducible components of X is locally finite.*

Then the canonical homomorphism $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ induced by ϕ from Proposition 3.1.27 (i) is surjective and induces an isomorphism

$$\mathrm{CaCl}(X) \cong \mathrm{Pic}(X).$$

Remark 5.2.9. The injectivity of $\mathrm{CaCl}(X) \to \mathrm{Pic}(X)$ can be deduced using the isomorphism $\mathrm{Div}(X) \to \mathrm{InvId}(X)$, see Proposition 3.1.27 (i). The surjectivity of $\mathrm{CaCl}(X) \to \mathrm{Pic}(X)$ then follows from the fact that every invertible sheaf is isomorphic to some $\mathcal{O}_X$-ideal, see Lemma 4.1.2. △

Remark 5.2.10. Note that by Remark 3.1.22, we have a surjective map $\mathrm{InvId}(X) \to \mathrm{Pic}(X)$. By Corollary 3.1.29, we have an isomorphism $\mathrm{CaCl}(X) \cong \mathrm{InvId}(X)$ and we deduce with Proposition 5.2.8 that the map above extends to an isomorphism $\mathrm{ClInvId}(X) \cong \mathrm{Pic}(X)$. △

Remark 5.2.11. In Definition 5.6.1 we will define the degree zero divisor class group $\mathrm{CaCl}^0(X)$ which is a subgroup of $\mathrm{CaCl}(X)$. Since ϕ is compatible with the respective notions of degree, the isomorphism $\mathrm{CaCl}(X) \cong \mathrm{Pic}(X)$ will provide an isomorphism $\mathrm{CaCl}^0(X) \cong \mathrm{Pic}^0(X)$. △

Corollary 5.2.12. *Let X satisfy one of the conditions in Proposition 5.2.8, then*

$$H^1\left(X, \mathcal{O}_X^\times\right) \cong \mathrm{CaCl}(X) \cong \mathrm{ClInvId}(X) \cong \mathrm{Pic}(X).$$

In particular, the above holds whenever X is a cover of $\mathbb{P}^1_k$.

Proof. The first assertion follows by combining Propositions 5.2.7 and 5.2.8. If X is noetherian and projective over some field k, then Theorem D.1.6 provides a finite morphism $\pi : X \to \mathbb{P}^1_k$. Since X is Cohen-Macaulay, [Sta18, Tag 0BXG] provides that X has no embedded points. Hence $\mathrm{Ass}(\mathcal{O}_X)$ equals X^0, the set of generic points of the irreducible components of X. By [Liu02, 7.3.10], π sends generic points to generic points and hence $\mathrm{Ass}(\mathcal{O}_X)$ is contained in the preimage of the affine open subset $U_0 \cap U_1$ of $\mathbb{P}^1_k$ where U_0 and U_1 form a standard affine open cover of $\mathbb{P}^1_k$. By [GW10, 13.77], finite morphisms are affine and thus the requirements of Proposition 5.2.8 are met. The isomorphism $\mathrm{ClInvId}(X) \cong \mathrm{Pic}(X)$ follows from Remark 5.2.10. □

5.3 Divisors and Open Subschemes

In this section we draw a connection between divisors on a scheme X and the divisors on a schematically dense open subscheme. The scheme X will at least be locally noetherian and typically $U \subseteq X$ will denote the schematically dense open subscheme of X, see Definition 3.2.10 and Lemma B.2.5 for a characterisation of schematically dense open subschemes. Note that we will use the term schematically dense open subset meaning schematically dense open subscheme.

Proposition 5.3.1. *Let X be a locally noetherian scheme and $U \subseteq X$ be a schematically dense open subset. The following diagram is commutative with exact rows and columns:*

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & i_*\mathcal{O}_U^\times & \hookrightarrow & i_*\mathcal{K}_U^\times & \xrightarrow{\xi} & i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times) & \longrightarrow & 1 \\
 & & \uparrow & & \alpha\uparrow & & \vdots\uparrow & & \\
1 & \longrightarrow & \mathcal{O}_X^\times & \hookrightarrow & \mathcal{K}_X^\times & \longrightarrow & \mathcal{K}_X^\times/\mathcal{O}_X^\times & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 1 & & 1 & & i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times & & \\
 & & & & & & \uparrow & & \\
 & & & & & & 1 & &
\end{array}$$

The morphism ξ is the composition of the projection $i_*\mathcal{K}_U^\times \to i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times$ with the natural isomorphism $i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times \to i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)$. The dashed morphism is the morphism induced by the composition of the isomorphism α with ξ. Moreover, it is equal to the morphism given in Eq. (2:1) in Proposition 3.2.3.

Proof. Since $U \subseteq X$ contains all associated points of X, by Lemma 3.2.11, the injective morphism $\mathcal{O}_X^\times \hookrightarrow i_*\mathcal{O}_U^\times$ extends to the isomorphism $\alpha : \mathcal{K}_X^\times \to i_*\mathcal{K}_U^\times$. This provides the left square and its commutativity. The sequence

$$1 \longrightarrow i_*\mathcal{O}_U^\times \longrightarrow i_*\mathcal{K}_U^\times \longrightarrow i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times \longrightarrow 1$$

is trivially exact. Composing the projection $i_*\mathcal{K}_U^\times \longrightarrow i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times$ with the natural morphism $i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times \to i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)$, which is an isomorphism by Corollary B.1.45, provides the surjective morphism ξ. It is obvious that the image of $i_*\mathcal{O}_U^\times \to i_*\mathcal{K}_U^\times$ is equal to the kernel of ξ and hence we obtain the exactness of the first row. The exactness of the second row is evident.

The kernel of $\xi \circ \alpha$ is the isomorphic preimage of $i_*\mathcal{O}_U^\times$ under α which, by the commutativity of the left square, contains $\mathcal{O}_X^\times$. Hence we deduce the existence of the dashed morphism, which is also surjective since the same is true for $\xi \circ \alpha$. After identifying $i_*\mathcal{O}_U^\times$

with its preimage under α it follows immediately that the kernel of the dashed morphism is $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times$. By construction, the dashed morphism $\mathcal{K}_X^\times/\mathcal{O}_X^\times \to i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)$ is, as asserted, the same as the morphism given in Eq. (2:1) in Proposition 3.2.3. □

Lemma 5.3.2. *Let X be a locally noetherian scheme and let $U \subseteq X$ be a schematically dense open subset. Then the elements of $H^0(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times)$ are given by collections of the form*

$$\left\{(U, 1\cdot\mathcal{O}_X(U)^\times), (V_i, s_i\cdot\mathcal{O}_X(V_i)^\times) \mid s_i \in \mathcal{O}_X(U\cap V_i)^\times, s_i/s_j \in \mathcal{O}_X(V_i\cap V_j)^\times\right\}$$

where U and the V_i together form an open cover of X.

Proof. By Lemma B.1.22 (ii), the global sections of $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times$ are given by collections of the form

$$\left\{(W_i, t_i\cdot\mathcal{O}_X(W_i)^\times) \mid t_i \in \mathcal{O}_X(U\cap W_i)^\times, t_i/t_j \in \mathcal{O}_X(W_i\cap W_j)\right\}$$

where the W_i form an open cover of X. Now for all $W_i \subseteq U$ we have $t_i \in \mathcal{O}_X(W_i)^\times$ and hence for any such W_i we deduce $(W_i, t_i\cdot\mathcal{O}_X(W_i)^\times) = (W_i, 1\cdot\mathcal{O}_X(W_i)^\times)$. That means that the restriction of the global section to U is given by the neutral element section and thus we may replace all those $(W_i, t_i\cdot\mathcal{O}_X(W_i)^\times)$ with $W_i \subseteq U$ by $(U, 1\cdot\mathcal{O}_X(U)^\times)$. Now we denote all those W_i with $W_i \not\subseteq U$ by V_i. Together with U these V_i form an open cover of X. This already provides the assertion. □

Proposition 5.3.3. *Let X be a noetherian scheme of dimension one and let $U \subseteq X$ be a schematically dense open subset. Then $(i_*\mathcal{O}_U)^\times/\mathcal{O}_X^\times$ is a skyscraper sheaf and thus we have $H^1\left(X, (i_*\mathcal{O}_U)^\times/\mathcal{O}_X^\times\right) = 0$.*

Proof. Since $\operatorname{Ass}(\mathcal{O}_X) \subseteq U$, we have that U meets every irreducible component X_i of X. Hence $X_i \setminus (U\cap X_i)$ is a proper closed subset of the one-dimensional irreducible scheme X_i and thus it is finite, see Proposition B.5.2. Since noetherian schemes have finitely many irreducible components, say $X_1, \dots, X_m$, see [Sta18, Tag 0BA8], $X\setminus U = \bigcup_{i=1}^m (X_i \setminus U\cap X_i)$ is finite, too.

Note that by Lemma B.1.37, we know that $(\mathcal{R}^\times)_P = \mathcal{R}_P^\times$ for every sheaf of rings $\mathcal{R}$ on X for which $\mathcal{R}^\times$ is indeed a sheaf. Let us examine how the stalks of the quotient $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times$ look like:

$$\left(\frac{i_*\mathcal{O}_U^\times}{\mathcal{O}_X^\times}\right)_P \cong \frac{((i_*\mathcal{O}_U)^\times)_P}{(\mathcal{O}_X^\times)_P} = \frac{(i_*\mathcal{O}_U)_P^\times}{\mathcal{O}_{X,P}^\times}$$

which is zero whenever $(i_*\mathcal{O}_U)_P = \mathcal{O}_{X,P}$ and thus whenever $P \in U$. Hence its support is contained in $X \setminus U$ which is finite by the above. Whence the quotient is a skyscraper sheaf and thus satisfies $H^1\left(X, (i_*\mathcal{O}_U)^\times/\mathcal{O}_X^\times\right) = 0$ by Lemma B.2.8. □

Lemma 5.3.4. *Let X be a locally noetherian scheme of dimension one and let $U \subseteq X$ be a schematically dense open subset. Let $i : U \hookrightarrow X$ denote the corresponding open immersion. Moreover, assume that $X = U \cup V$ for some open $V \subseteq X$. Then we have an exact sequence*

$$0 \to H^0(\mathcal{O}_X^\times) \to H^0(i_*\mathcal{O}_U^\times) \to H^0(i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times) \xrightarrow{\delta} \operatorname{CaCl}(X) \xrightarrow{i^*} \operatorname{CaCl}(U) \to 0.$$

The morphism δ sends a global section s of $H^0(i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times)$ given by

$$\{(U, 1\cdot\mathcal{O}_X(U)^\times), (V_i, h_i\cdot\mathcal{O}_X(V_i)^\times) \mid h_i \in \mathcal{O}_X(U\cap V_i)^\times, h_i/h_j \in \mathcal{O}_X(V_i\cap V_j)^\times, i \in I\}$$

to the divisor on X given by the configuration $\{(U,1),(V_i,h_i)_{i\in I}\}$. Moreover, the map $\mathrm{CaCl}(X)\to\mathrm{CaCl}(U)$ is induced by the pullback of divisors along i.

Proof. Since X is locally noetherian and $\mathrm{Ass}(\mathcal{O}_X)\subseteq U$, by Lemma B.2.6, the morphism $\mathcal{O}_X\to i_*\mathcal{O}_U$ is injective. Thus we may consider the exact sequence

$$1\longrightarrow\mathcal{O}_X^\times\longrightarrow(i_*\mathcal{O}_U)^\times\longrightarrow(i_*\mathcal{O}_U)^\times/\mathcal{O}_X^\times\longrightarrow 1$$

which, by Lemma 5.2.5, provides a long exact sequence by applying Čech cohomology:

$$\begin{array}{l} 0\longrightarrow H^0\left(X,\mathcal{O}_X^\times\right)\longrightarrow H^0\left(X,i_*\mathcal{O}_U^\times\right)\longrightarrow H^0\left(X,i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)\xrightarrow{\delta} \\ \quad H^1\left(X,\mathcal{O}_X^\times\right)\longrightarrow H^1\left(X,i_*\mathcal{O}_U^\times\right)\longrightarrow \underbrace{H^1\left(X,i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)}_{=0} \end{array} \tag{3:4}$$

Here we denoted the group laws additively and $H^1\left(X,(i_*\mathcal{O}_U)^\times/\mathcal{O}_X^\times\right)=0$ is due to Proposition 5.3.3. By Lemma 5.3.2, any element h in $H^0\left(X,i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)$ is given by

$$\{(U,1\cdot\mathcal{O}_X(U)^\times),(V_i,h_i\cdot\mathcal{O}_X(V_i)^\times)\mid h_i\in\mathcal{O}_X(U\cap V_i)^\times,h_i/h_j\in\mathcal{O}_X(V_i\cap V_j)^\times,i\in I\}$$

where the V_i together with U form an open cover of X. Now, following Remark 5.2.6 and Lemma 5.2.5, the elements $h_i/h_j\in\mathcal{O}_X(U_{i,j})^\times$ provide an element κ of $H^1(X,\mathcal{O}_X^\times)$ given by $\{(U_{i,j},h_i/h_j)\mid i,j\in I\}$.

We easily observe that the image of the global section h under the monomorphism $\delta':i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\hookrightarrow\mathcal{K}_X^\times/\mathcal{O}_X^\times$, see Lemma B.2.6, maps under the homomorphism

$$H^0\left(X,\mathcal{K}_X^\times/\mathcal{O}_X^\times\right)\to H^1\left(X,\mathcal{O}_X^\times\right)$$

given in Proposition 5.2.7 to the element κ constructed above. Therefore, the following diagram is commutative:

$$\begin{array}{ccccc} H^0\left(X,i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right) & \xrightarrow{\delta'(X)} & H^1\left(X,\mathcal{O}_X^\times\right) & \longrightarrow & H^1\left(X,i_*\mathcal{O}_U^\times\right) \\ & & \uparrow & & \uparrow \\ & & H^0\left(X,\mathcal{K}_X^\times/\mathcal{O}_X^\times\right) & \xrightarrow{i^*} & H^0\left(X,i_*\mathcal{K}_U^\times/i_*\mathcal{O}_U^\times\right) \end{array} \tag{3:5}$$

The morphisms in the top row are those provided by the sequence (3:4) and that of the bottom row is the one provided by Proposition 5.3.1. Note that the latter is the pullback of divisors on X to divisors on U along i, see Propositions 3.2.3 and 5.3.1 again. Hence, by Proposition 5.2.7, it allows us to replace $H^1\left(X,\mathcal{O}_X^\times\right)$ and $H^1\left(X,i_*\mathcal{O}_U^\times\right)$ in the sequence (3:4) by $\mathrm{CaCl}(X)$ respectively $\mathrm{CaCl}(U)$, such that we obtain the exact sequence

$$\begin{array}{l} 0\longrightarrow H^0\left(X,\mathcal{O}_X^\times\right)\longrightarrow H^0\left(X,i_*\mathcal{O}_U^\times\right)\longrightarrow H^0\left(X,i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)\xrightarrow{\delta} \\ \quad \mathrm{CaCl}(X)\longrightarrow\mathrm{CaCl}(U)\longrightarrow 0 \end{array} \tag{3:6}$$

where the morphism δ is now, on representatives, given by the map δ' from (3:5). That δ maps representatives as asserted can now easily be checked by examining how the map $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\hookrightarrow\mathcal{K}_X^\times/\mathcal{O}_X^\times$ works, see Lemma B.2.6. The last assertion is due to the fact that the morphism in the lower row of (3:5) was the pullback of divisors on X to divisors on U

along i. □

Corollary 5.3.5. *The kernel of the restriction morphism $i^* : \mathrm{CaCl}(X) \to \mathrm{CaCl}(U)$ consists of divisor classes given by representatives*

$$\{(U, 1 \cdot \mathcal{O}_X(U)^\times), (V_i, h_i \cdot \mathcal{O}_X(V_i)^\times) \mid h_i \in \mathcal{O}_X(U \cap V_i)^\times, h_i/h_j \in \mathcal{O}_X(V_i \cap V_j)^\times, i, j \in I\}$$

where U and the V_i, $i \in I$, form an open cover of X.

Corollary 5.3.6. *Let X be a cover of $\mathbb{P}^1_k$. Then we have an exact sequence*

$$0 \to H^0(\mathcal{O}_X^\times) \to H^0(i_*\mathcal{O}_{V_0}^\times) \to H^0(i_*\mathcal{O}_{V_0}^\times/\mathcal{O}_X^\times) \xrightarrow{\delta} \mathrm{CaCl}(X) \xrightarrow{\cdot|V_0} \mathrm{CaCl}(V_0) \to 0.$$

where δ sends a global section h of $H^0(i_*\mathcal{O}_{V_0}^\times/\mathcal{O}_X^\times)$ given by

$$\{(V_0, 1 \cdot R_0^\times), (V_i, h_i \cdot \mathcal{O}_X(V_i)^\times) \mid h_i \in \mathcal{O}_X(V_0 \cap V_i)^\times, h_i/h_j \in \mathcal{O}_X(V_i \cap V_j)^\times, i, j \in I\},$$

where $\bigcup_{i\in I} V_i$ contains the closed points of S, to the divisor on X given by the configuration $\{(V_0, 1), (V_i, h_i)_{i\in I}\}$. Moreover, the map $\mathrm{CaCl}(X) \to \mathrm{CaCl}(V_0)$ is induced by the pullback of divisors along $i_0 : V_0 \hookrightarrow X$.

Example 5.3.7. If X is a cover of $\mathbb{P}^1_k$, then the *generalised pole divisor of x*, which will be defined in Definition 5.6.3, will lie in the kernel of $i^* : \mathrm{CaCl}(X) \to \mathrm{CaCl}(V_0)$. △

Remark 5.3.8. Note that the assumption regarding the dimension of X is only necessary for $H^1\left(X, i_*\mathcal{O}_U^\times\right) = 0$ and thus for the surjectivity of the map $i^* : \mathrm{CaCl}(X) \to \mathrm{CaCl}(U)$. △

Lemma 5.3.9. *Let X be a noetherian scheme of dimension one over k and let $U \subseteq X$ be a schematically dense open subset. The following diagram is commutative with exact rows and columns:*

$$\begin{array}{ccccccccccc}
 & & & & & & 0 & & & & \\
 & & & & & & \downarrow & & & & \\
 & & & & & & H^0(\mathcal{O}_X^\times) & & & & \\
 & & & & & & \downarrow & & & & \\
 & & & & & 0 & H^0(i_*\mathcal{O}_U^\times) & & & & \\
 & & & & & \downarrow & \downarrow & & & & \\
 & & & & 0 & \longrightarrow & H^0(i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times) & \xrightarrow{\mathrm{id}} & H^0(i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times) & \longrightarrow & 0 \\
 & & & & & & \downarrow{\scriptstyle \delta'(X)} & & \downarrow{\scriptstyle \delta} & & \\
0 & \longrightarrow & H^0(\mathcal{O}_X^\times) & \longrightarrow & H^0(\mathcal{K}_X^\times) & \longrightarrow & \mathrm{Div}(X) & \longrightarrow & \mathrm{CaCl}(X) & \longrightarrow & 0 \\
 & & & & & & \downarrow{\scriptstyle i^*} & & \downarrow{\scriptstyle i^*} & & \\
0 & \longrightarrow & H^0(i_*\mathcal{O}_U^\times) & \longrightarrow & H^0(i_*\mathcal{K}_U^\times) & \longrightarrow & \mathrm{Div}(U) & \longrightarrow & \mathrm{CaCl}(U) & \longrightarrow & 0 \\
 & & & & & & \downarrow & & \downarrow & & \\
 & & & & & & 0 & & 0 & &
\end{array}$$

The morphism $i^* : \mathrm{Div}(X) \to \mathrm{Div}(U)$ is the pullback of divisors as in Proposition 3.2.3, see also Lemma 3.2.11. Note that we denoted the group laws additively.

Proof. For any scheme X we have the canonical exact sequence

$$1 \longrightarrow \mathcal{O}_X^\times \longrightarrow \mathcal{K}_X^\times \longrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times \longrightarrow 1$$

which extends to the long exact sequence provided by applying Čech cohomology

$$0 \longrightarrow H^0\left(X, \mathcal{O}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) \longrightarrow H^1\left(X, \mathcal{O}_X^\times\right) \longrightarrow \underbrace{H^1\left(X, \mathcal{K}_X^\times\right)}_{=0}$$

where $H^1\left(X, \mathcal{K}_X^\times\right) = 0$ by Lemma B.2.4. By definition, we have $H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) = \mathrm{Div}(X)$ and by Proposition 5.2.7, $H^1\left(X, \mathcal{O}_X^\times\right) = \mathrm{CaCl}(X)$ which finally provides the two exact row sequences.

Let us examine the left column: By Proposition 5.3.1, we have an exact sequence

$$1 \longrightarrow i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times \longrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times \longrightarrow i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times) \longrightarrow 1. \tag{3:7}$$

The corresponding long exact sequence, for which we denote the group laws additive, is

$$0 \longrightarrow H^0\left(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right) \longrightarrow H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) \longrightarrow H^0\left(X, i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)\right) \xrightarrow{\delta'(X)} \underbrace{H^1\left(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)}_{=0}$$

where $H^1\left(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right) = 0$ by Proposition 5.3.3. Note that the connecting morphism is indeed the morphism $\delta'(X)$ (notation as in the proof of Lemma 5.3.4) since δ' is the one induced by the sequence (3:7). By definition, we have

$$H^0\left(X, i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)\right) = H^0\left(U, \mathcal{K}_U^\times/\mathcal{O}_U^\times\right) = \mathrm{Div}(U)$$

and $H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times)\right) = \mathrm{Div}(X)$ which provides the exactness of the left column. Moreover, by Proposition 5.3.1, the morphism $\mathcal{K}_X^\times/\mathcal{O}_X^\times \to i_*(\mathcal{K}_U^\times/\mathcal{O}_U^\times)$ is the same as the morphism given in (2:1) in Proposition 3.2.3 and thus on the level of global sections it is equal to the pullback i^* of divisors along i as in Proposition 3.2.3.

The existence of the exact sequence on the right hand side is due to Lemma 5.3.4. Moreover, by Lemma 5.3.4, the morphism $\mathrm{CaCl}(X) \to \mathrm{CaCl}(U)$ is the pullback i^* of divisors along i and thus we obtain the commutativity of the lower square connecting all three exact sequences.

Finally, by the proof of Lemma 5.3.4, the morphism δ is the morphism induced by $\delta'(X)$ on representatives. □

To get a better grip on what the difference is between the divisors on X and those on an schematically dense open subset $U \subseteq X$ as in Lemma 5.3.9, we investigate the kernel of the map $\mathrm{Div}(X) \to \mathrm{Div}(U)$.

Corollary 5.3.10. *Let X be a noetherian scheme of dimension one over k and let $U \subseteq X$ be a schematically dense open subset. The kernel of the map $i^* : \mathrm{Div}(X) \to \mathrm{Div}(U)$ is given by the divisors D on X with configurations of the form*

$$\{(U, 1), (V_i, h_i) \mid h_i \in \mathcal{O}_X(U \cap V_i)^\times, h_i/h_j \in \mathcal{O}_X(V_i \cap V_j)^\times, i, j \in I\}$$

where the V_i together with U form an open cover of X. Those divisors D on X are exactly those whose ideal sheaf $\mathcal{O}_X(D)$ vanishes on U, i.e. $\mathcal{O}_X(D)_{|U} = \mathcal{O}_U$ or equivalently $\mathrm{Supp}(D) \subseteq X \setminus U$.

Proof. First of all, note that $\mathcal{O}_X(U \cap U_i) \subseteq \mathcal{K}_X(U \cap U_i) \cong \mathcal{K}_X(U_i)$ for any open $U_i \subseteq X$, see Lemma B.2.6, and thus the asserted configuration makes sense. Now the assertion is a direct consequence of the fact that the kernel is, by Lemma 5.3.9, the image of

$$H^0\left(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right) \to H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right),$$

how the morphism $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times \to \mathcal{K}_X^\times/\mathcal{O}_X^\times$ maps (using the mentioned embedding $\mathcal{O}_X(U \cap U_i) \hookrightarrow \mathcal{K}_X(U_i)$) and how the elements of $H^0\left(X, i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times\right)$ look like, see Lemma 5.3.2. The last part of the assertion follows immediately. □

We consider the following simple example to see how these divisors look like for the projective line and a standard affine open.

Example 5.3.11. Let $X = \mathbb{P}_k^1 = \operatorname{Proj}(k[x_0, x_1])$ with $U_0 = D_+(x_1) = X \setminus \{(1:0)\}$. Set $P_\infty = (1:0)$ and denote $x = x_0/x_1$, then we have $\mathcal{O}_X(U_0) = k[x]$. Moreover, X is covered by U_0 and $U_\infty := X \setminus (0:1)$ where $\mathcal{O}_X(U_\infty) = k[x^{-1}]$. Obviously, X satisfies the requirements for Corollary 5.3.10 and thus the divisors on X that restrict to zero on U_0 are given by configurations of the form

$$\{(U_0, 1), (U_i, f_i) \mid f_i \in \mathcal{O}_X(U_0 \cap U_i)^\times, f_i/f_j \in \mathcal{O}_X(U_i \cap U_j)^\times, i \in I\}$$

where $\bigcup_{i\in I} U_i$ contains $X \setminus U_0 = \{P_\infty\}$. Now we can drop every of the U_i except one since any of them contains P_∞ and we only need one to still induce the same divisor on X. Let W denote the open U_i which is left. Without loss of generality we may not only assume that $W \subseteq U_\infty$ holds but also (since U_∞ is affine and any open subset of an affine open is covered by a finite number of basic open subsets) we may also assume that W is a basic open subset of U_∞. We also denote f_i by f. Thus $W = D_{U_\infty}(g)$ with $g \in k[x^{-1}]$ and $x^{-1} \nmid g$. Removing the zeros of the denominator of $f \in \mathcal{K}_X(W) = \operatorname{Quot}(k[x^{-1}]_g) = k(x)$ by replacing g with the product of g and the denominator of f, we may also assume $f \in \mathcal{O}_X(W) = k[x^{-1}]_g$. Since $U_0 \cap U_\infty = D_{U_\infty}(x^{-1})$, the restriction map $\mathcal{O}_X(W) \to \mathcal{O}_X(U_0 \cap W)$ is the ring monomorphism $k[x^{-1}]_g \to k[x, x^{-1}]_g$. Thus $f_i \in \mathcal{O}_X(U_0 \cap W)^\times$ means that $f_i \in k[x^{-1}]_g^\times \cup \{x^r \mid r \in \mathbb{Z}\}$. If $f_i \in k[x^{-1}]_g^\times$, then the induced divisor is the zero divisor. Otherwise, f is of the form bx^r with $b \in \mathcal{O}_X(W)^\times$ and hence we may assume that f is a power of x. Therefore, we obtain that the kernel of $i^* : \operatorname{Div}(\mathbb{P}_k^1) \to \operatorname{Div}(U_0)$ consists of divisors on $\mathbb{P}_k^1$ provided by configurations of the form

$$\{(U_0, 1), (W, x^r) \mid P_\infty \in W \subseteq U_\infty\}.$$ △

We can generalise the previous example, at least to some extent, to covers of $\mathbb{P}_k^1$.

Proposition 5.3.12. *Let X be a cover of $\mathbb{P}_k^1$. Let $P_1, \ldots, P_s$ be the finitely many closed points in the fibre of P_∞ under $\pi : X \to \mathbb{P}_k^1$. Then the kernel of $i^* : \operatorname{Div}(X) \to \operatorname{Div}(V_0)$ consists of divisors provided by configurations of the form*

$$\{(V_0, 1), (U_1, f_1), \ldots, (U_s, f_s) \mid U_i \subseteq V_\infty, U_i \cap \pi^{-1}(P_\infty) = P_i, \\ f_i \in \mathcal{O}_X(V_0 \cap U_i)^\times, \forall j \neq i : f_i \in \mathcal{O}_X(U_i \cap U_j)^\times\}.$$

Proof. Clearly, X satisfies the requirements of Corollary 5.3.10 and thus for $U = V_0 = \pi^{-1}(U_0)$ we obtain that the kernel of $i^* : \operatorname{Div}(X) \to \operatorname{Div}(V_0)$ is given by divisors with configurations of the form

$$\{(V_0, 1), (U_i, f_i) \mid f_i \in \mathcal{O}_X(U_0 \cap U_i)^\times, f_i/f_j \in \mathcal{O}_X(U_i \cap U_j)^\times, i, j \in I\}$$

where $\bigcup_{i\in I} U_i$ contains $X \setminus V_0 = \pi^{-1}(P_\infty)$. As in the proof of Example 5.3.11, we may

drop all U_i except for one for each $P \in \pi^{-1}(P_\infty)$. Since $\pi^{-1}(P_\infty) = \{P_1, \dots, P_s\}$ is finite, let U_i, $i = 1, \dots, s$, denote the open neighborhood of P_i. Without loss of generality we may remove any P_j, $j \neq i$, from U_i and may thus assume that $U_i \cap \pi^{-1}(P_\infty) = P_i$. Furthermore, we may also remove the points in $V_0 \setminus V_\infty$ from every U_i and can thus assume $U_i \subseteq V_\infty$. Therefore, the kernel is given by divisors with configurations of the form

$$\{(V_0, 1), (U_1, f_1), \dots, (U_s, f_s) \mid U_i \subseteq V_\infty, U_i \cap \pi^{-1}(P_\infty) = P_i, \\ f_i \in \mathcal{O}_X(V_0 \cap U_i)^\times, \forall j \neq i : f_i \in \mathcal{O}_X(U_i \cap U_j)^\times\}$$

with $f_i \in \mathcal{K}_X(U_i)^\times$. Since U_i are open subsets of an affine scheme V_∞, they are covered by a finite union of basic open subsets in V_∞. Now, for each $i = 1, \dots, s$, pick any of these covering basic open subsets that contain P_i and then we obtain the same divisor. Thus, we may assume U_i to be basic open subsets of V_∞. By further shrinking U_i to a smaller basic open subset (by removing the zeros of the denominator of the f_i), we may also assume $f_i \in \mathcal{O}_X(U_i)$. Now since both U_i and $V_{0,\infty}$ are basic open subsets of V_∞, the intersection $U_0 \cap U_i \subseteq U_i$ is basic open in U_i. Moreover, since $V_{0,\infty} = D_{V_\infty}(x^{-1})$ in V_∞, we have $U_0 \cap U_1 = D_{U_i}(x^{-1})$. Hence the restriction map from U_i to $U_0 \cap U_i$ is the injective localisation homomorphism $\mathcal{O}_X(U_i) \to \mathcal{O}_X(U_i)_{x^{-1}}$. Since the units in $\mathcal{O}_X(U_i)_{x^{-1}}$ are of the form bx^{-r_i} with $b \in \mathcal{O}_X(U_i)^\times$ and $r_i \in \mathbb{Z}$, we obtain

$$f_i = bx^{-r_i} \quad \text{with} \quad b \in \mathcal{O}_X(U_i)^\times.$$

Since we can always alter f_i multiplicatively with units in $\mathcal{O}_X(U_i)$, we may finally assume $f_i = x^{r_i}$ for some $r_i \in \mathbb{Z}$ which provides the assertion. □

The following lemma tells us that we can extend divisors from the complement of a finite set to all of the scheme by providing local equations on the finite set of points. It also implies the surjectivity of the morphisms $\mathrm{Div}(\mathbb{P}^1_k) \to \mathrm{Div}(U)$ and $\mathrm{Div}(X) \to \mathrm{Div}(V_0)$ from Example 5.3.11 and Proposition 5.3.12.

Lemma 5.3.13. *Let X be a noetherian scheme of dimension one. Let $P_1, \dots, P_s \in X_0$ whose open complement is denoted by U. Then for any Cartier divisor D on U and for arbitrary $f_i \in \mathcal{K}_X(V_i)^\times$, $i = 1, \dots, s$ where $V_i \subseteq X$ are open neighborhoods of P_i, there exists a divisor E on X with $E_{|U} = D$ and $E_{P_i} = f_i \mathcal{O}_{X,P_i}$.*

Proof. Let D be given by the data (U_j, g_j) where $U = \bigcup_j U_j$ and $g_j \in \mathcal{K}_X(U_j)^\times$. Since U is open in X, the same is true for the U_j. Since X is noetherian and of dimension one, by Lemma 3.1.8, the support of D is a finite set of closed points of X. By definition, we thus have

$$\mathrm{Supp}(D) = \cup_j \{P \in U_j \mid (g_j)_P \mathcal{O}_{X,P} \neq \mathcal{O}_{X,P}\} = \cup_j \{P \in U_j \mid g_j \notin \mathcal{O}^\times_{X,P}\}.$$

By assumption, $f_i \in \mathcal{K}_X(V_i)^\times$ and thus the respective images in $H^0(X, \mathcal{K}^\times_{V_i}/\mathcal{O}^\times_{V_i})$ are principal divisors on V_i which, by the same line of argument as above, have finite support. That is, for all i the sets $\{P \in V_i \mid f_i \notin \mathcal{O}^\times_{X,P}\}$ are finite sets of closed points, too. Therefore, the set

$$W := \{P \in \cup_{i,j} V_i \cap U_j \mid \forall\, i, j : f_i, g_j \in \mathcal{O}^\times_{X,P}\}$$

is open in X as the complement of the finite union of all these finite closed sets. Obviously, the complement of $W_i := W \cup \{P_i\}$ is finite and thus W_i is open. Now we have found an open cover of $X = \bigcup_j U_j \cup \bigcup_i W_i$ and we define the divisor E on X by using this cover and as the local functions we use g_j on U_j and f_i on W_i. This indeed defines a divisor since on the overlaps $U_j \cap W_i \subseteq W$ the condition $f_i/g_j \in \mathcal{O}_X(U_j \cap W_i)^\times$ is obviously satisfied

because the functions itself are already units at the considered points. The divisor E obviously satisfies the asserted properties. □

5.4 Divisors and Irreducible Components

In this section we draw a connection between the divisors on a reducible scheme X and the divisors on its irreducible components. This connection will be heavily used in our approach of computing in the Picard group. If not mentioned otherwise, in the following X denotes a scheme with finitely many irreducible components $X_1, \dots, X_m$ and Y denotes their disjoint union as introduced in Section B.3. Note that we will also use the notation introduced there.

Lemma 5.4.1. *Let X be a locally noetherian and reduced scheme. Then the rows and columns of the following diagram are exact and the squares commute.*

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \mathcal{O}_X^\times & \xrightarrow{\tau^\#} & \bigoplus_{i=1}^m (\tau_i)_*{\mathcal{O}_{X_i}}^\times & \longrightarrow & (\bigoplus_{i=1}^m (\tau_i)_*{\mathcal{O}_{X_i}}^\times)/\mathcal{O}_X^\times & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \mathcal{K}_X^\times & \xrightarrow{\tau^\#} & \bigoplus_{i=1}^m (\tau_i)_*\mathcal{K}_{X_i}^\times & \longrightarrow & 1 & & \\
 & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \rho} & & & & \\
 & & \mathcal{K}_X^\times/\mathcal{O}_X^\times & \overset{\phi}{\dashrightarrow} & \bigoplus_{i=1}^m (\tau_i)_*(\mathcal{K}_{X_i}^\times/{\mathcal{O}_{X_i}}^\times) & \longrightarrow & 1 & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array} \tag{4:8}$$

Moreover, ϕ is the pullback of divisors from X to Y, i.e. the component-wise restriction of a divisor on X to the irreducible components of X.

Proof. Note that by abuse of notation we denote the extension of $\tau^\# : \mathcal{O}_X \to \tau_*\mathcal{O}_Y$ to the morphism $\mathcal{K}_X \to \tau_*\mathcal{K}_Y$, see Corollary 3.2.15, again by $\tau^\#$. This already provides the commutativity of the top square. That the left column is exact follows immediately from the fact that $\mathcal{O}_X$ is a subsheaf of $\mathcal{K}_X$ and thus $\mathcal{O}_X^\times$ one of $\mathcal{K}_X^\times$. By Corollary B.1.45, we have

$$(\tau_i)_*(\mathcal{K}_{X_i}^\times/\mathcal{O}_{X_i}^\times) \cong (\tau_i)_*\mathcal{K}_{X_i}^\times/(\tau_i)_*\mathcal{O}_{X_i}^\times$$

and thus the exactness of the right column follows due to the isomorphism $\tau_*\mathcal{K}_Y/\tau_*\mathcal{O}_Y \cong \bigoplus_{i=1}^m (\tau_i)_*\mathcal{K}_{X,i}/(\tau_i)_*\mathcal{O}_{X_i}$. The top row is exact since, by Proposition B.3.3, $\tau^\# : \mathcal{O}_X \to \tau_*\mathcal{O}_Y$ is injective since X is reduced. That $\tau^\# : \mathcal{K}_X^\times \to \bigoplus_{i=1}^m (\tau_i)_*\mathcal{K}_{X_i}^\times = \tau_*\mathcal{K}_Y$ is an isomorphism, and thus the middle row is exact, is given by Corollary B.3.8.

Due to the commutativity of the top square, we see that $\mathcal{O}_X^\times$ is contained in the kernel of the map $\rho \circ \tau^\# : \mathcal{K}_X \to \bigoplus_{i=1}^m (\tau_i)_*(\mathcal{K}_{X_i}^\times/{\mathcal{O}_{X_i}}^\times)$ and thus we obtain a well-defined morphism

$$\phi : \mathcal{K}_X^\times/\mathcal{O}_X^\times \dashrightarrow \bigoplus_{i=1}^m (\tau_i)_*(\mathcal{K}_{X_i}^\times/{\mathcal{O}_{X_i}}^\times)$$

which is indeed surjective since $\tau^\#$ is an isomorphism between $\mathcal{K}_X$ and $\tau_*\mathcal{K}_Y$ and ρ is obviously surjective. By construction, the morphism ϕ is the induced morphism

$$\mathcal{K}_X^\times/\mathcal{O}_X^\times \to \tau_*\mathcal{K}_Y^\times/\tau_*\mathcal{O}_Y^\times = \tau_*(\mathcal{K}_Y^\times/\mathcal{O}_Y^\times)$$

given in (2:1) in Proposition 3.2.3. Thus ϕ is the pullback of divisors from X to Y and by Corollary 3.2.23, it is equal to the component-wise restriction of divisors on X to an irreducible component. The lower square commutes by construction. □

Proposition 5.4.2. *There is an exact sequence*

$$1 \longrightarrow \left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right)/\mathcal{O}_X^{\times} \xrightarrow{\alpha} \mathcal{K}_X^{\times}/\mathcal{O}_X^{\times} \xrightarrow{\phi} \bigoplus_{i=1}^{m}\mathcal{K}_{X_i}^{\times}/\mathcal{O}_{X_i}{}^{\times} \longrightarrow 1 \tag{4:9}$$

with ϕ, σ and τ as in diagram (4:8) in Lemma 5.4.1 and $\alpha = \sigma \circ (\tau^{\#})^{-1}$. In particular, ϕ is the component-wise restriction of divisors on X to the respective irreducible component.

Proof. Consider the commutative diagram (4:8). By construction of the morphism $\phi : \mathcal{K}_X^{\times}/\mathcal{O}_X^{\times} \to \bigoplus_{i=1}^{m}(\tau_i)_*(\mathcal{K}_{X_i}^{\times}/\mathcal{O}_{X_i}{}^{\times})$, its kernel is $(\ker\rho \circ \tau^{\#})/\mathcal{O}_X^{\times}$. Since $\tau^{\#} : \mathcal{K}_X^{\times} \to \tau_*\mathcal{K}_Y$ was an isomorphism, we have

$$\ker\rho \circ \tau^{\#} = (\tau^{\#})^{-1}\left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right).$$

Therefore, the kernel of ϕ is the image of $\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}^{\times}$ under the composition α of $(\tau^{\#})^{-1}$ with σ. The rest of the assertion follows from Lemma 5.4.1. □

Corollary 5.4.3. *Let X be a reduced, noetherian scheme of dimension one. Then the support of*

$$\left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right)/\mathcal{O}_X^{\times}$$

is contained in the set of intersection points of the irreducible components of X. In particular, it is a skyscraper and thus $H^1\left(X, \left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right)/\mathcal{O}_X^{\times}\right) = 0$.

Proof. By Lemma B.1.37, we have

$$\left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right)_P = \bigoplus_{i=1}^{m}(\mathcal{O}_{X,P}/\mathcal{J}_{i,P})^{\times}$$

where $\mathcal{J}_i$ denotes the ideal sheaf cutting out the component X_i and $\mathcal{J}_{i,P}$ its stalk at P. By Lemma B.1.37, we have $(\mathcal{O}_X^{\times})_P = \mathcal{O}_{X,P}^{\times}$. For P lying on exactly one irreducible component of X, the quotient $\bigoplus_{P\in X_i}(\mathcal{O}_{X,P}/\mathcal{J}_{i,P})/\mathcal{O}_{X,P}$ and thus $\bigoplus_{i=1}^{m}(\mathcal{O}_{X,P}/\mathcal{J}_{i,P})^{\times}/\mathcal{O}_{X,P}^{\times}$ vanishes. Therefore, as asserted, the support of the sheaf in question is contained in the set of intersection points of the irreducible components of X. Now by Lemma B.5.3, this set is finite and hence, by Lemma B.2.8, the assertion follows. □

Corollary 5.4.4. *Let X be a reduced, noetherian scheme of dimension one. Let $X_1, \ldots, X_m$ be its irreducible components. Then there is an exact sequence*

$$0 \longrightarrow H^0\left(X, \left(\bigoplus_{i=1}^{m}(\tau_i)_*\mathcal{O}_{X_i}{}^{\times}\right)/\mathcal{O}_X^{\times}\right) \longrightarrow \mathrm{Div}(X) \xrightarrow{\phi} \bigoplus_{i=1}^{m}\mathrm{Div}(X_i) \longrightarrow 0 \tag{4:10}$$

where we denoted the group laws additively. Here ϕ denotes the component-wise restriction of divisors on X to the respective X_i's, that is $\phi(D) = (D_{|X_1}, \ldots, D_{|X_m})$.

Proof. We consider the long exact sequence provided by taking cohomology of sequence

(4:9) in Proposition 5.4.2:

$$1 \to H^0\left(X, \frac{\bigoplus_{i=1}^m (\tau_i)_* {\mathcal{O}_{X_i}}^\times}{\mathcal{O}_X^\times}\right) \to H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right) \to H^0\left(X, \bigoplus_{i=1}^m \mathcal{K}_{X_i}^\times/{\mathcal{O}_{X_i}}^\times\right) \to 1$$

Here the sequence ends in the trivial multiplicative group since

$$H^1\left(X, (\bigoplus_{i=1}^m (\tau_i)_* {\mathcal{O}_{X_i}}^\times)/\mathcal{O}_X^\times\right) = 1$$

by Corollary 5.4.3. Note that taking cohomology commutes with direct sums, see [Har77, 2.9.1]. Now denoting the group laws additively and plugging in the definition $\mathrm{Div}(X) = H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$ for any scheme X, we see that Proposition 5.4.2 provides the assumption. □

Corollary 5.4.5. *The kernel of $\phi : \mathrm{Div}(X) \to \bigoplus_{i=1}^m \mathrm{Div}(X_i)$ is given by divisors given by configurations of the form*

$$\{(U_j, s_j)_{j\in J} \mid \cup_{j\in J} U_j = X, s_j = (s_{j,i})_{\{i|X_i\cap U_j\neq\emptyset\}}, s_{j,i} \in \mathcal{O}_{X_i}(X_i \cap U_j)^\times, \\ s_j/s_h \in \mathcal{O}_X(U_j \cap U_h)^\times, h, j \in J\}.$$

That is, the kernel consists of those divisors with local functions s on open subsets U that restrict to invertible regular functions $s_{|X_i\cap U}$ on all irreducible components X_i meeting U.

Proof. The kernel of ϕ is given by the image of $H^0\left(X, (\bigoplus_{i=1}^m (\tau_i)_* {\mathcal{O}_{X_i}}^\times)/\mathcal{O}_X^\times\right)$ under the embedding into $H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$. By Lemma B.1.22 (ii), the global sections of the sheaf $(\bigoplus_{i=1}^m (\tau_i)_* {\mathcal{O}_{X_i}}^\times)/\mathcal{O}_X^\times$ are given by collections $(U_j, s_j \cdot \mathcal{O}_X(U_j)^\times)_{j\in J}$ for some index set J and open $U_j \subseteq X$ such that

$$\bigcup_{j\in J} U_j = X, \quad s_j = (s_{j,i})_{\{i|X_i\cap U_j\neq\emptyset\}}, \quad s_{j,i} \in \mathcal{O}_{X_i}(X_i\cap U_j)^\times \quad \text{and} \quad s_j/s_h \in \mathcal{O}_X(U_j\cap U_h)^\times.$$

Here we identify s_j with its image $(s_{j,i})_{\{i|X_i\cap U_j\neq\emptyset\}}$ under the injection

$$\mathcal{O}_X(U_j) \hookrightarrow \bigoplus_{\{i|X_i\cap U_j\neq\emptyset\}} \mathcal{O}_X(X_i \cap U_j).$$

By Proposition 5.4.2, $\alpha(X)$ maps the above section using the above identification, which is given by $\tau^\# : \mathcal{K}_X^\times \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{K}_{X_i}^\times$ from the diagram (4:8) in Lemma 5.4.1, and the injection $\bigoplus_{i=1}^m (\tau_i)_* \mathcal{O}_{X_i}^\times \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{K}_{X_i}^\times$ as asserted to the configuration

$$\{(U_j, s_j)_{j\in J} \mid \cup_{j\in J} U_j = X, s_j = (s_{j,i})_{\{i|X_i\cap U_j\neq\emptyset\}}, s_{j,i} \in \mathcal{O}_{X_i}(X_i \cap U_j)^\times, \\ s_j/s_h \in \mathcal{O}_X(U_j \cap U_h)^\times, h, j \in J\}.$$ □

Lemma 5.4.6. *The restriction of $\phi : \mathrm{Div}(X) \to \bigoplus_{i=1}^m \mathrm{Div}(X_i)$ to the subgroup of principal divisors yields a group epimorphism $\phi_{|\mathrm{Princ}(X)} : \mathrm{Princ}(X) \to \bigoplus_{i=1}^m \mathrm{Princ}(X_i)$. Moreover, if $f \in \mathcal{K}_X(X)^\times$ corresponds to $(f_1, \ldots, f_m)$ under the identification $\mathcal{K}_X(X)^\times \cong \bigoplus_{i=1}^m \mathcal{K}_{X_i}(X_i)^\times$, then*

$$\phi(\mathrm{div}_X(f)) = (\mathrm{div}_{X_1}(f_1), \ldots, \mathrm{div}_{X_m}(f_m)).$$

Proof. That the restriction induces the asserted group homomorphism follows from Corollary 3.2.4. The surjectivity $\phi_{|\mathrm{Princ}(X)}$ follows easily: Consider the principal divisor in $\bigoplus_{i=1}^m \mathrm{Div}(X_i)$ given by $(f_1, \ldots, f_m) \in \bigoplus_{i=1}^m \mathcal{K}_{X_i}(X_i)^\times$. Let f denote the preimage of

$(f_1, \dots, f_m)$ under the isomorphism $\tau^\# : \mathcal{K}_X(X)^\times \cong \bigoplus_{i=1}^m \mathcal{K}_{X_i}(X_i)^\times$. Then the commutativity of diagram (4:8) in Lemma 5.4.1 provides that $\operatorname{div}_X(f)$ gets sent to the principal divisor given by $(f_1, \dots, f_m)$ under ϕ. □

In general, the map $\phi_{|\operatorname{Princ}(X)} : \operatorname{Princ}(X) \to \bigoplus_{i=1}^m \operatorname{Princ}(X_i)$ is not injective as the following example shows.

Example 5.4.7. Let k be a field with $\operatorname{char} k \neq 2$. Let $X = \operatorname{Spec}(R)$ with $R = k[x,y]/I$ where is I the ideal generated by xy. The affine scheme X has two irreducible components (the two coordinate axes in $\mathbb{A}^2_k$) corresponding to the two minimal prime ideals generated by $y + I$ respectively $x + I$. Since R is reduced, this provides the injection

$$R \hookrightarrow R_1 \times R_2 := k[x,y]/(y) \times k[x,y]/(x), \quad f + I \mapsto (f + (y), f + (x))$$

which extends to an isomorphism $\operatorname{Frac}(R) \to k(y) \times k(x)$. These two morphisms correspond to the morphisms of sheaves $\mathcal{O}_X \hookrightarrow (\tau_1)_* \mathcal{O}_{X_1} \oplus (\tau_2)_* \mathcal{O}_{X_2}$ and $\mathcal{K}_X \cong \mathcal{K}_{X_1} \oplus \mathcal{K}_{X_2}$ along which the local equations of divisors get mapped with ϕ. Consider the regular element $f = (x+2y) \cdot (x+y)^{-1} \in \operatorname{Frac}(R)^\times$ which defines a principal divisor on X. The image of f under the isomorphism above is the tuple $(f_1, f_2) := (1 + (y), 2 + (x))$. Obviously, we have $f_i \in R_i^\times$ and thus the image of $\operatorname{div}_X(f)$ under $\phi_{|\operatorname{Princ}(X)}$ is the tuple $(\operatorname{div}_{X_1}(1), \operatorname{div}_{X_2}(2)) = (0,0)$. This is also the image of the zero divisor $0 = \operatorname{div}_X(1)$ on X. Since $x + y$ is no unit in R, the same is true for f and, therefore, $\operatorname{div}_X(f) \neq \operatorname{div}_X(1)$ which provides that $\phi_{|\operatorname{Princ}(X)}$ is not injective. △

Lemma 5.4.8. *Let $\phi : \operatorname{Div}(X) \to \bigoplus_{i=1}^m \operatorname{Div}(X_i)$ denote the component-wise restriction of divisors from Corollary 5.4.4. Then for every $D \in \operatorname{Div}(X)$ we have*

$$\deg_k \phi(D) = \sum_{i=1}^m \deg_k D_{|X_i} = \deg_k D.$$

Proof. First of all, the first equality is obvious since $\operatorname{Div}(Y) = \bigoplus_{i=1}^m \operatorname{Div}(X_i)$ for Y being the disjoint union of the irreducible components X_i. By Proposition 3.2.3, we have $\mathcal{O}_{X_i}(D_{|X_i}) \cong (\tau_i)^* \mathcal{O}_X(D) = \mathcal{O}_X(D)_{|X_i}$. Thus, by Proposition 3.1.27, we see that $\deg_k D_{|X_i} = -\deg_k \mathcal{O}_{X_i}(D_{|X_i}) = -\deg_k \mathcal{O}_X(D)_{|X_i}$. Now Proposition C.4.15 provides $\deg_k \mathcal{O}_X(D) = \sum_{i=1}^m \deg_k \mathcal{O}_X(D)_{|X_i}$ and thus we finally obtain

$$\deg_k D = -\deg_k \mathcal{O}_X(D) = \sum_{i=1}^m -\deg_k \mathcal{O}_X(D)_{|X_i} = \sum_{i=1}^m -\deg_k \mathcal{O}_{X_i}(D_{|X_i}) = \sum_{i=1}^m \deg_k D_{|X_i}$$

where we have used $\mathcal{O}_X(D)_{|X_i} \cong \mathcal{O}_{X_i}(D_{|X_i})$, due to Proposition 3.2.3. □

Definition 5.4.9. Define $\mathfrak{K}$ to be the kernel of ϕ, i.e. $\mathfrak{K}$ are exactly those divisors on X restricting to the zero divisor on every component X_i of X. Let $\mathfrak{H} \subseteq \operatorname{Div}(X)$ denote the preimage of $\bigoplus_{i=1}^m \operatorname{Princ}(X_i)$ under ϕ in Corollary 5.4.4. That is, $\mathfrak{H}$ consists of those divisors on X whose restriction to every irreducible component is a principal divisor. By Lemma 5.4.6, $\mathfrak{H}$ thus consists of those divisors sharing the same restrictions as a principal divisor on X. Now Lemma 5.4.6 already provides $\operatorname{Princ}(X) \subseteq \mathfrak{H}$. Since the zero divisor is the principal divisor of $1 \in \mathcal{K}_X(X)^\times$, we have $\mathfrak{K} \subseteq \mathfrak{H}$. △

Lemma 5.4.10. *The morphism $\operatorname{Div}(X) \to \bigoplus_{i=1}^m \operatorname{Div}(X_i)$ extends to a surjective morphism $\psi : \operatorname{CaCl}(X) \to \bigoplus_{i=1}^m \operatorname{CaCl}(X_i)$ providing the exact sequence*

$$0 \longrightarrow \mathfrak{H}/\operatorname{Princ}(X) \longrightarrow \operatorname{CaCl}(X) \to \bigoplus_{i=1}^m \operatorname{CaCl}(X_i) \longrightarrow 0. \tag{4:11}$$

Proof. We can extend the homomorphism ϕ by the surjection

$$\bigoplus_{i=1}^{m} \operatorname{Div}(X_i) \to \frac{\bigoplus_{i=1}^{m} \operatorname{Div}(X_i)}{\bigoplus_{i=1}^{m} \operatorname{Princ}(X_i)} = \bigoplus_{i=1}^{m} \frac{\operatorname{Div}(X_i)}{\operatorname{Princ}(X_i)} = \bigoplus_{i=1}^{m} \operatorname{CaCl}(X_i)$$

and obtain an epimorphism $\operatorname{Div}(X) \to \bigoplus_{i=1}^{m} \operatorname{CaCl}(X_i)$ whose kernel is obviously $\mathfrak{H}$. Since $\operatorname{Princ}(X) \subseteq \mathfrak{H}$ by Lemma 5.4.6, this yields an epimorphism $\psi : \operatorname{CaCl}(X) \to \bigoplus_{i=1}^{m} \operatorname{CaCl}(X_i)$ with kernel $\mathfrak{H}/\operatorname{Princ}(X)$. □

Remark 5.4.11. Summarising the above, we see that the restriction of divisors and thus also of divisor classes is provided by the natural surjective map $\mathcal{K}_X^\times/\mathcal{O}_X^\times \to \bigoplus_i \mathcal{K}_{X_i}^\times/\mathcal{O}_{X_i}{}^\times$. That is, we just restrict the quotients of regular functions defining the divisor to the respective components which would also be the first intuitive way to restrict divisors in a geometric way. By the above we have seen that this is independent of the local representing functions and is therefore well-defined. △

5.5 Divisors on X, V_0 and S

In this section we investigate how we might express divisors on X in terms of divisors on V_0 and on S. Let X be a reduced cover of $\mathbb{P}_k^1$ as introduced in Section 2.2.

The following Lemma tells us that divisors on an affine scheme with finitely many points are given by principal divisors.

Lemma 5.5.1. *Let X be an affine scheme with finite underlying topological space. Then*

$$\operatorname{Div}(X) \cong \bigoplus_{P \in X} \mathcal{K}_{X,P}^\times/\mathcal{O}_{X,P}^\times \cong \mathcal{K}_X(X)^\times/\mathcal{O}_X(X)^\times = \operatorname{Frac}(\mathcal{O}_X(X))^\times/\mathcal{O}_X(X)^\times.$$

Proof. Set $X = \operatorname{Spec}(R)$. Combining Propositions 3.1.27 and 5.1.3 provides an isomorphism of abelian groups $\operatorname{Div}(X) \cong \operatorname{InvId}(R)$. By assumption, R only has finitely many maximal ideals and hence, by Lemma B.4.6, any non-zero invertible R-ideal is principal. Hence we have the desired isomorphism between Cartier divisors on X and principal R-ideals. Obviously, we can alter any principal R-ideal by units in R. □

Corollary 5.5.2. *Since both S and the S_i are affine schemes with finite underlying topological space, see Proposition 2.2.11, we have* $\operatorname{Div}(S) \cong \operatorname{Frac}(\mathcal{O}_S)^\times/\mathcal{O}_S^\times$ *and* $\operatorname{Div}(S_i) \cong \operatorname{Frac}(\mathcal{O}_{S_i})^\times/\mathcal{O}_{S_i}^\times$.

Proposition 5.5.3. *Let X be a scheme which is a finite disjoint union of schemes $X_1, \dots, X_m$. Then* $\operatorname{Div}(X) = \bigoplus_{i=1}^{m} \operatorname{Div}(X_i)$ *where a divisor D on X is equal to the tuple $(D_{|X_1}, \dots, D_{|X_m})$. Obviously, we then have* $\deg_k D = \sum_{i=1}^{m} \deg_k D_{|X_i}$.

Proof. This follows immediately from the fact that we can without loss of generality choose the open covers defining divisors to be the disjoint unions of covers of the X_i. □

Corollary 5.5.4. *We have* $\operatorname{Div}(S) = \bigoplus_{i=1}^{m} \operatorname{Div}(S_i)$.

Proof. By Proposition 2.2.11, we have $\mathcal{O}_S = \bigoplus_{i=1}^{m} \mathcal{O}_{S_i}$ and thus $S = \operatorname{Spec}(\mathcal{O}_S)$ is the disjoint union of the $S_i = \operatorname{Spec}(\mathcal{O}_{S_i})$. Now the assertion follows from Proposition 5.5.3. □

Lemma 5.5.5. *Restricting divisors to the open subset V_0 and restricting divisors to S, see Definition 3.2.24, provides an isomorphism of abelian groups*

$$\begin{array}{ccccc} \operatorname{Div}(X) & \to & \operatorname{Div}(V_0) & \times & \operatorname{Div}(S) \\ D & \mapsto & (D_{|V_0} & , & D_{|S}). \end{array}$$

Proof. We have already seen that the restriction (or pullback along morphisms as in Proposition 3.2.3) of divisors is a group homomorphism. Hence the product of these group homomorphisms is a group homomorphism $\mathrm{Div}(X) \to \mathrm{Div}(V_0) \times \mathrm{Div}(S)$.

The surjectivity is provided by Lemma 5.3.13. To prove injectivity, let $D \in \mathrm{Div}(X)$ get sent to 0 in $\mathrm{Div}(V_0) \times \mathrm{Div}(S)$. Now D is the zero divisor if and only if there is an open cover $\{U_i\}$ of X with $D_{|U_i} = 0$ for all i. By assumption, $D_{|V_0} = 0$ and $D_{|S} = 0$. By Proposition 3.2.21, the latter implies that there is some open subset $W \subseteq V_\infty$ with $S \subseteq W$ such that $D_{|W} = 0$. Hence V_0 and W form an open cover of X such that D restricts to zero on both of them and thus by the above we deduce $D = 0$. □

Remark 5.5.6. By Proposition 2.2.11, we have $\mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$ which implies $\mathrm{Div}(S) = \bigoplus_{i=1}^m \mathrm{Div}(S_i)$ and thus we also have an isomorphism of abelian groups

$$\begin{array}{ccccc} \mathrm{Div}(X) & \to & \mathrm{Div}(V_0) & \times & \bigoplus_{i=1}^m \mathrm{Div}(S_i) \\ D & \mapsto & (D_{|V_0} & , & D_{|S_1}, \ldots, D_{|S_m}). \end{array}$$

△

Therefore, by Lemma 5.5.5, we may uniquely represent every divisor on X as its restriction to V_0 and to S (or to V_0 and to all of the S_i). Moreover, we may also carry out the addition of divisors by adding their respective restrictions.

Notation 5.5.7. The above identification of a divisor D with its restrictions to V_0 and S will be denoted by $D = (D_{|V_0}, D_{|S}) = D_{|V_0} + D_{|S}$ or, equivalently, by

$$D = (D_{|V_0}, D_{|S_1}, \ldots, D_{|S_m}) = D_{|V_0} + D_{|S_1} + \ldots + D_{|S_m}.$$

This sum notation interprets $D_{|V_0}$ as a divisor on X by extending it by zero on S and $D_{|S}$ as a divisor on X by extending it by zero on V_0. That is, $D_{|V_0}$ is the short notation for $(D_{|V_0}, 0)$ and $D_{|S}$ for $(0, D_{|S})$. △

Lemma 5.5.8. *Let $V \subseteq X$ be a schematically dense open subset. Restricting divisors on X to divisors on V provides a surjective group homomorphism* $\mathrm{Princ}(X) \to \mathrm{Princ}(V)$.

Proof. By Lemma 3.2.11, the restriction of divisors from X to V is defined. From Corollary 3.2.4 we know that the restriction of principal divisors are principal. This gives the desired group homomorphism $\mathrm{Princ}(X) \to \mathrm{Princ}(V)$. The surjectivity follows from the fact that $\mathcal{K}_X \to i_*\mathcal{K}_V$ is an isomorphism for the open immersion $i : V \to X$, see Lemma B.2.6, and that the restriction of divisors maps the local defining functions along this isomorphism. □

Lemma 5.5.9. *The restriction of divisors* $\mathrm{Div}(V_\infty) \to \mathrm{Div}(S)$ *restricted to the group of principal divisors on V_∞ is a group epimorphism* $\mathrm{Princ}(V_\infty) \to \mathrm{Div}(S)$.

Proof. By Remark 3.2.20, the restriction of divisors from X to S is defined. By Lemma 5.5.1, all divisors on S are principal divisors and, by Proposition 3.2.17, we know that $\mathcal{K}_X \to \mu_*\mathcal{K}_S$ is an isomorphism. Thus any divisor D on S is given by some $f \in (\mu_*\mathcal{K}_S)(X) = \mathcal{K}_S(S)$ which is isomorphic to $\mathcal{K}_X(X)$. Since the restriction of divisors maps the local defining functions along this isomorphism, it is evident that the respective preimage of f provides a preimage of the divisor D which is principal. □

Corollary 5.5.10. *The restriction of divisors provides a surjective group homomorphism* $\mathrm{Princ}(X) \to \mathrm{Div}(S)$.

Proof. This is just the combination of Lemmas 5.5.8 and 5.5.9. □

Remark 5.5.11. Corollary 5.5.10 tells us that, for any given divisor D on X, we will find a principal divisor on X which has the same restriction to S as D. Hence we can always find representatives of classes in $\mathrm{CaCl}(X)$ that are only supported outside of S, i.e. that have support in V_0. This may suggest that the restriction map $\mathrm{Div}(X) \to \mathrm{Div}(V_0)$ extends to an isomorphism under linear equivalence, i.e. to an isomorphism $\mathrm{CaCl}(X) \to \mathrm{CaCl}(V_0)$. But this is false in general: Although the map is well-defined, for any divisor D with support in V_0 whose restriction to V_0 is a principal divisor on V_0, we find by Lemma 5.5.8 a principal divisor $\mathrm{div}_X(f)$ on X with $\mathrm{div}_X(f)_{|V_0} = D_{|V_0}$. But since the support of $\mathrm{div}_X(f)$ may meet S, the difference $D - \mathrm{div}_X(f) \in \mathrm{Div}(X)$ in general need not be zero. For instance, let X be integral and non-singular such that $S = \{P\}$. Choose $D \geq 0$ such that $D_{|V_0} = \mathrm{div}_{V_0}(f) \neq 0$. Then $f^{-1}R_0 = \mathcal{O}_X(D)(V_0) \subseteq R_0$ and thus $v_Q(f^{-1}) \geq 0$ for all points $Q \in V_0$. Since $f^{-1} \notin R_0^\times$, there is some $Q_0 \in V_0$ such that $v_{Q_0}(f^{-1}) \geq 1$ and since $\deg_k \mathrm{div}_X(f) = 0$, see Proposition 3.1.27 (iv), $v_P(f) < 0$ and hence $\mathrm{Supp}(\mathrm{div}_X(f)) \cap S \neq \emptyset$. Therefore the desired map is not injective though it is surjective by Lemma 5.3.13. △

As we have seen above, Corollary 5.5.10 ensures that we might always find representatives of elements in $\mathrm{CaCl}(X)$ which are only supported on V_0. Those would correspond to divisors in $\mathrm{Div}(V_0)$ which are thus given by elements in $\mathrm{InvId}(R_0)$, see Proposition 5.1.3. In the next section we want to find specific representatives of elements in $\mathrm{CaCl}(X)$ (we even want to find a suitable isomorphism of the degree zero part on $\mathrm{CaCl}(X)$) which ensure that we only need to deal with elements in $\mathrm{InvId}(R_0)$. Hence it seems to be the case that everything perfectly fits together. But we do not only want to work with elements $\mathrm{InvId}(R_0)$ but even with integral ideal representatives. But those would correspond to effective divisors on V_0, see Proposition 3.1.27, and therefore the above would imply that we are working with representatives (on X) which are effective and have degree zero. But the only divisor on X that has degree zero and is effective is the zero divisor, see Lemma 4.7.7. Hence we will see that we need to allow the representative to be non-zero on S but still of a specific form.

5.6 Isomorphic Models of the Picard Group

In this section we will define the degree zero divisor class group $\mathrm{CaCl}^0(X)$ analogously to the definition of $\mathrm{Pic}^0(X)$. Moreover, we will define the degree zero divisor class group $\mathrm{CaCl}^0_\pi(X)$ with respect to π by only considering representatives in $\mathrm{CaCl}^0(X)$ of a specific form. This will provide an isomorphism between the former and the latter. Furthermore, we will present two different types of representatives in $\mathrm{CaCl}^0_\pi(X)$ that will each correspond to an approach of computing in $\mathrm{CaCl}^0_\pi(X)$ later on in Chapter 6.

5.6.1 Degree Zero Divisor Class Group with Respect to π

As mentioned above, in this section we will define the degree zero divisor class group $\mathrm{CaCl}^0(X)$ and the degree zero divisor class group $\mathrm{CaCl}^0_\pi(X)$ with respect to π. To do so, we will introduce the generalised pole divisor of x. In this section (X, π) will denote a reduced cover of $\mathbb{P}^1_k$.

Note that if $D, E \in \mathrm{Div}(X)$ are two divisors whose restrictions $D_{|X_i}, E_{|X_i}$ to the irreducible component X_i have degree zero, then the sum $D+E$ also has degree zero restriction to X_i. This is due to the fact that the restriction map $\phi : \mathrm{Div}(X) \to \bigoplus_{i=1}^m \mathrm{Div}(X_i)$ and the degree map $\deg_k : \mathrm{Div}(X) \to \mathbb{Z}$ both are group homomorphisms, see Corollary 5.4.4 respectively Remark 3.1.11.

Definition 5.6.1. Let X be a reduced cover of $\mathbb{P}^1_k$. Let $\mathcal{D}_0(X) \subseteq \mathrm{Div}(X)$ denote the subset of those divisors whose restriction on each irreducible component has degree zero.

By what we have said above, $\mathcal{D}_0(X)$ forms a subgroup of $\mathrm{Div}(X)$. Note that the restriction of a principal divisor to an irreducible component is again a principal divisor, see Corollary 3.2.4, and since principal divisors on projective curves have degree zero, see Lemma 3.1.12, $\mathrm{Princ}(X)$ is a subgroup of $\mathcal{D}_0(X)$. Then we define the **degree zero divisor class group** of X as the quotient group $\mathrm{CaCl}^0(X) = \mathcal{D}_0(X)/\mathrm{Princ}(X)$. △

As already advocated by Remark 5.2.11, we now can state the following lemma.

Lemma 5.6.2. *The isomorphisms* $\mathrm{CaCl}(X) \to \mathrm{InvId}(X) \to \mathrm{Pic}(X)$ *from Proposition 5.2.8 provides the isomorphisms* $\mathrm{CaCl}^0(X) \cong \mathrm{ClInvId}^0(X) \cong \mathrm{Pic}^0(X)$.

Next we define the generalised pole divisor of x, a divisor on X that restricts to prescribed multiples of the pole divisor of x on X_i.

Definition 5.6.3. By Lemma D.2.15, there are regular $h_i \in R_\infty$ with $S_i \subseteq D(h_i) \subseteq V_\infty \setminus (S \setminus S_i)$. Fix such $h_1, \dots, h_m \in R_\infty$. By construction, for any $i = 1, \dots, m$ we have $(X \setminus S_i) \cap D(h_i) \subseteq V_{0,\infty}$. Moreover, $x^r \in (R_\infty)_{h_i}$ restricts to a unit in $\mathcal{O}_X(V_{0,\infty})$. Hence the configuration

$$\{(X \setminus S_i, 1), (D(h_i), x^{-r_i})\}$$

does define a divisor on X which we denote by $(x^{r_i})_{i,\infty}$. By mild abuse of notation, x^{-r_i} denotes the image of x^{-r_i} in $(R_\infty)_{h_i}$ under the injective localisation homomorphism $R_\infty \to (R_\infty)_{h_i}$. By definition, we have

$$\mathcal{O}_X((x^{r_i})_{i,\infty})_P = \begin{cases} \mathcal{O}_{X,P}, & P \notin S_i \\ x^{r_i}\mathcal{O}_{X,P}, & P \in S_i \end{cases}$$

and $\mathcal{O}_X((x^{r_i})_{i,\infty})(V) = \mathcal{O}_X(V)$ for all $V \subseteq V_0$ as well as $\mathcal{O}_X((x^{r_i})_{i,\infty})(D(h_i)) = x^{r_i}(R_\infty)_{h_i}$. The inclusion $D(h_i) \cap D(h_j) \subseteq V_{0,\infty}$ corresponds to the ring homomorphisms $(R_\infty)_{x^{-1}} \to (R_\infty)_{h_i h_j}$ under which the unit x^r, $r \in \mathbb{Z}$, gets sent to a unit. Hence for $A := \{1, \dots, m\}$ the divisor $\sum_{i \in A}(x^{r_i})_{i,\infty}$ is given by the configuration

$$\{(V_0, 1), (D(h_i), x^{-r_i})_{i \in A}\}$$

which implies

$$\mathcal{O}_X(\textstyle\sum_{i \in A}(x^{r_i})_{i,\infty})_P = \begin{cases} \mathcal{O}_{X,P}, & P \notin S \\ x^{r_i}\mathcal{O}_{X,P}, & P \in S_i \end{cases}$$

as well as $\mathcal{O}_X(\sum_{i \in A}(x^{r_i})_{i,\infty})(V) = \mathcal{O}_X(V)$ for all $V \subseteq V_0$ and $\mathcal{O}_X(\sum_{i \in A}(x^{r_i})_{i,\infty})(D(h_i)) = x^{r_i}(R_\infty)_{h_i}$. Note that by definition, we have $(x^r)_{i,\infty} = r(x)_{i,\infty}$ for all $r \in \mathbb{Z}$. △

Remark 5.6.4. We could have defined the divisors $(x^{r_i})_{i,\infty}$ without the basic open subsets $D(h_i)$ and use $V_\infty \setminus (S \setminus S_i)$ instead. But the advantage of the way we have done it, is that we can immediately see what the restriction to S_i will be. This is due to the fact that the morphism $S \to V_\infty$ resp. $S_i \to V_{i,0}$ is induced by the localisation homomorphism regarding $T = k[x^{-1}] \setminus x^{-1}k[x^{-1}]$ and hence we can clearly determine how it works on the level on basic opens. △

Proposition 5.6.5. *The restriction of* $(x^{r_i})_{i,\infty}$ *to* X_i *is equal to* $r_i(x)_{X_i,\infty}$ *and its restriction to* X_j *with* $j \neq i$ *is equal to the zero divisor on* X_j.

Proof. Note that $X_i \setminus S_i = V_{i,0}$. By Remark 3.2.14, the configuration $\{(X \setminus S_i, 1), (D(h_i), x^{-r_i})\}$ gets sent to the configuration $\{(V_{i,0}, 1), (D(h_i), x^{-r_i}\}$ where, by abuse of notation, h_i and x^{-r_i} also denote their images under the residue map $R_\infty \to R_{i,\infty}$. Since x gets sent to a unit in $V_{i,0} \cap D(h_i) \subseteq V_{i,0} \cap V_{i,\infty}$, this configuration induces the same divisor as the configuration $\{(V_{i,0}, 1), (V_{i,\infty}, x^{-r_i})\}$. But the latter configuration induces the r_i-multiple $r_i(x)_{X_i,\infty}$ of the pole divisor of x. The second assertion if obvious. □

Definition 5.6.6. Let us denote the restriction of $(x)_{X_i,\infty}$ to S_i by $(x)_{S_i,\infty}$. Moreover, we denote the restriction of $(x)_\infty$ to S by $(x)_{S,\infty}$. △

Corollary 5.6.7. *Let $A = \{1, \dots, m\}$. Then*

$$\left(\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty}\right)_{|X_j} = r_j(x)_{X_j,\infty}$$

and hence

$$\left(\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty}\right)_{|S_j} = r_j(x)_{S_j,\infty}.$$

Proof. The first statement follows immediately from Proposition 5.6.5 if we take into account that the restriction map $\tau_j^* : \mathrm{Div}(X) \to \mathrm{Div}(X_j)$ is a group homomorphism, see Proposition 3.2.3 and Lemma 3.2.13. The second assertion follows by further restricting to S_j and by Corollary 3.2.23. □

Remark 5.6.8. In particular, under the identification from Remark 5.5.6, the divisor $\sum_{i\in A}(x^{r_i})_{i,\infty}$ corresponds to $(0, r_1(x)_{S_1,\infty}, \dots, r_m(x)_{S_m,\infty})$. △

Proposition 5.6.9. *Let $A = \{1, \dots, m\}$. Then we have*

(i) $\deg_k \sum_{i\in A}(x^{r_i})_{i,\infty} = \deg_k \left(\sum_{i\in A}(x^{r_i})_{i,\infty}\right)_{|S} = \sum_{i\in A} r_i n_i$, *and*

(ii) $\deg_k(\sum_{i\in A}(x^{r_i})_{i,\infty})_{S_j} = \deg_k(x^{r_j})_{|S_j} = r_j n_j$.

Proof. Let us prove the first assertion. By Proposition C.4.18 (ii), we have

$$\deg_k \sum\nolimits_{i\in A}(x^{r_i})_{i,\infty} = \deg_k \left(\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty}\right)_{|V_0} + \deg_k \left(\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty}\right)_{|S}$$

and since, by definition, $\sum_{i\in A}(x^{r_i})_{i,\infty}$ restricts to the zero divisor on V_0, the first equality of the first assertion follows. Now by Proposition C.4.18 (iii), we have

$$\deg_k \sum\nolimits_{i\in A}(x^{r_i})_{i,\infty} = \sum\nolimits_{j\in A} \deg_k \left(\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty}\right)_{|X_j} = \sum\nolimits_{j\in A} \deg_k r_j(x)_{X_j,\infty}$$

where the last equality is due to Corollary 5.6.7. Now by Corollary D.2.14, we have $\deg_k r_j(x)_{X_j,\infty} = r_j n_j$ and thus the second equality of the first assertion follows as well. The second assertion is an immediate consequence of Corollary 5.6.7. □

Remark 5.6.10. Let $A = \{1, \dots, m\}$. If $r_i = r$ for all $i \in A$, then

$$\sum\nolimits_{i\in A}(x^{r_i})_{i,\infty} = r(x)_\infty.$$ △

Lemma 5.6.11. *Let $f = (f_1, \dots, f_m) \in \mathcal{K}_X(X)^\times$. Then*

1. $\mathrm{div}_X(f)_{|S} = \mathrm{div}_S(f)$ *where the latter f is the image of the former under the ring monomorphism $R_\infty \to \mathcal{O}_S$, and*
2. $\mathrm{div}_X(f)_{|S_i} = \mathrm{div}_{S_i}(f_i)$.

Proof. By definition, $\mathrm{div}_X(f)$ is given by the configuration $\{(X, f)\}$. By Corollary 3.2.23, we have $\mathrm{div}_X(f)_{|S} = (\mathrm{div}_X(f)_{|V_\infty})_{|S}$ and by Remark 3.2.12, $\mathrm{div}_X(f)_{|V_\infty}$ is given by the configuration $\{(V_\infty, f)\}$ where we identified f with its image under the isomorphism $\mathcal{K}_X(X) \cong \mathcal{K}_X(V_\infty)$. Therefore, by Remark 3.2.20, $(\mathrm{div}_X(f)_{|V_\infty})_{|S}$ and hence $\mathrm{div}_X(f)_{|S}$ is given by $\{(S, f)\}$ where we identified f with its image under the ring monomorphism

$R_\infty \to \mathcal{O}_S$. This proves the first assertion. To prove the second, recall that by Remark 3.2.14, the restriction of $\mathrm{div}_X(f)$ to the component X_i is given by $\{(X_i, f_{|X_i})\}$ where $f_{|X_i}$ denotes the image of f under the ring epimorphism $\mathcal{K}_X(V_\infty) \to \mathcal{K}_{X_i}(V_{i,\infty})$. But this equals f_i under the identification $\mathcal{K}_X(X) \cong \mathcal{K}_X(V_\infty) \cong \bigoplus_{i=1}^m \mathcal{K}_{X_i}(V_{i,\infty})$ and hence yields the second assertion. □

Proposition 5.6.12. *Let $A = \{1, \dots, m\}$. The various restrictions of $\sum_{i\in A}(x^{r_i})_{i,\infty}$ are given as follows:*

1. *The restriction to V_∞ is given by the configuration*

$$\{(V_{0,\infty}, 1), (D(h_i), x^{-r_i})_{i\in A}\}.$$

2. *The restriction to S is given by the configuration*

$$\{(S_i, x^{-r_i})_{i\in A}\} \tag{6:12}$$

and hence by the principal divisor on S given by $f = (x^{-r_1}, \dots, x^{-r_m}) \in \mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$.

3. *The restriction to S_i is given by the principal divisor of x^{-r_i} on S_i and is thus equal to $r_i(x)_{S_i,\infty}$.*

Proof. Since $D(h_i) \subseteq V_\infty$ for all $i = 1, \dots, m$, by Remark 3.2.12, the first assertion follows immediately. By Corollary 3.2.23, the restriction from X to S can be computed by first restricting from X to V_∞ and then from V_∞ to S. By Remark 3.2.20, the restriction map from $D(h_i)$ to $D(h_i) \cap S = S_i$ is given by the map $(R_\infty)_{h_i} \to (T^{-1}R_\infty)_{h_i}$. Moreover, the intersection of $V_{0,\infty}$ with S is empty. Hence the restriction to S is given by the asserted configuration where x^{-r_i} is the image of x^{-r_i} under the above ring homomorphism. That the principal divisor $\mathrm{div}_S(f)$ on S equals the one induced by the configuration (6:12) is due to Corollary 5.5.4 and the fact that $\mathrm{div}_S(f)_{|S_i} = \mathrm{div}_{S_i}(x^{-r_i})$ which follows from Lemma 5.6.11. The third assertion follows now immediately since we can (again with Corollary 3.2.23) just further restrict $\mathrm{div}_S(f)$ to S_i which yields the asserted principal divisor on S_i. □

Corollary 5.6.13. *Let $A = \{1, \dots, m\}$. Let $f = (f_1, \dots, f_m) \in \mathcal{K}_X(X)^\times$. Then the following are equivalent.*

1. $\mathrm{div}_X(f)_{|S} = (\sum_{i\in A} r_i(x)_{i,\infty})_{|S}$,
2. *for all $i \in A$ we have* $\mathrm{div}_{S_i}(f_i) = r_i(x)_{S_i,\infty}$, *and*
3. *for all $i \in A$ we have $f_i^{-1}\mathcal{O}_{S_i} = x^{r_i}\mathcal{O}_{S_i}$.*

Proof. By Corollary 5.5.4, two divisors on S are equal if and only if all of their restrictions to S_i are equal. Hence, we have $\mathrm{div}_X(f)_{|S} = (\sum_{i\in A} r_i(x)_{i,\infty})_{|S}$ if and only if for all $i = 1, \dots, m$

$$(\mathrm{div}_X(f)_{|S})_{|S_i} = ((\sum\nolimits_{i\in A} r_i(x)_{i,\infty})_{|S})_{|S_i}.$$

By Lemma 5.6.11 and Proposition 5.6.12, this is equivalent to

$$\mathrm{div}_{S_i}(f_i) = r_i((x)_{X_i,\infty})_{|S_i} = r_i(x)_{S_i,\infty}$$

for all $i = 1, \dots, m$. By Corollary D.2.14, the latter is the principal divisor of x^{-r_i} on S_i. By definition, these two principal divisors on S_i are equal if and only if their defining functions differ multiplicatively by a unit in $\mathcal{O}_{S_i}$. Equivalently, $f_i^{-1}\mathcal{O}_{S_i} = x^{r_i}\mathcal{O}_{S_i}$ for all $i = 1, \dots, m$. □

In what follows, we will define the degree zero divisor class group with respect to π which is closely related to $\mathrm{CaCl}^0(X)$ but requires its representatives to have the same restriction to S as the generalised pole divisor, see Definition 5.6.3. This will enable us to prove that it is isomorphic to some ideal class group associated to R_0.

Definition 5.6.14. Let (X, π) be a reduced cover of $\mathbb{P}^1_k$. We set

$$\mathrm{Div}^0_\pi(X) = \left\{ D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty} \in \mathcal{D}_0(X) \mid \mathrm{Supp}(D) \subseteq V_0 \right\}$$

which is obviously a subgroup of $\mathcal{D}_0(X)$. We call $\mathrm{Div}^0_\pi(X)$ the **degree zero divisor group of X with respect to π**. Analogously,

$$\mathrm{Princ}_\pi(X) = \mathrm{Div}^0_\pi(X) \cap \mathrm{Princ}(X)$$

is a subgroup of $\mathrm{Div}^0_\pi(X)$. The morphism $\mathrm{Div}^0_\pi(X) \hookrightarrow \mathcal{D}_0(X) \to \mathrm{CaCl}^0(X)$ then provides an embedding

$$\mathrm{CaCl}^0_\pi(X) := \mathrm{Div}^0_\pi(X)/\,\mathrm{Princ}_\pi(X) \hookrightarrow \mathrm{CaCl}^0(X).$$

We call $\mathrm{CaCl}^0_\pi(X)$ the **degree zero divisor class group of X with respect to π** △

Remark 5.6.15. Due to Proposition 5.6.9, the fact that the restrictions of $D+\sum_{i\in A} r_i(x)_{i,\infty}$ to any irreducible component have degree zero and Proposition C.4.18 (ii), we have $\deg_k D_{|V_{i,0}} = -r_i n_i$. Hence we deduce $\deg_k D_{|V_0} = \sum_{i\in A} -r_i n_i$, see Proposition C.4.18 (iii). △

Proposition 5.6.16. *The embedding $\mathrm{CaCl}^0_\pi(X) \hookrightarrow \mathrm{CaCl}^0(X)$ is an isomorphism of abelian groups.*

Proof. By Lemma 5.5.1, every divisor $D \in \mathrm{Div}(X)$ restricts to a principal divisor on S. By Corollary 5.5.10, there is some principal divisor on X which restricts to exactly that divisor on S. This provides that we find representatives of classes in $\mathrm{CaCl}^0(X)$ which are trivial on S. In particular, these representatives define a class in $\mathrm{CaCl}^0_\pi(X)$ since $\sum_{i\in A} r_i(x)_{i,\infty}$ where $r_i = 0$ for all $i \in A$ is the zero divisor on X. This provides the assertion. □

Remark 5.6.17. By abuse of naming, we will also call $\mathrm{CaCl}^0_\pi(X)$ the degree zero divisor class group of X. △

Remark 5.6.18. The isomorphism $\mathcal{K}_X \to (i_0)_*\mathcal{K}_{V_0}$ from Lemma B.2.6 provides that every principal divisor on V_0 given by some $f \in \mathcal{K}_{V_0}(V_0)^\times = \mathrm{Frac}(R_0)^\times$ provides an element in $\mathcal{K}_X(X)^\times$ and thus a principal divisor on X. Since the restriction of divisors from X to V_0 uses the isomorphism $\mathcal{K}_X \to (i_0)_*\mathcal{K}_{V_0}$ which is the extension of $\mathcal{O}_X \to (i_0)_*\mathcal{O}_{V_0}$, we see that the restriction of the above divisor to V_0 is the principal divisor on V_0 given by f again. △

Definition 5.6.19. Let $\mathcal{P}_\pi \subseteq \mathrm{InvId}(R_0)$ be the set of invertible R_0-ideals whose (regular) generator f provides (as in Remark 5.6.18) a principal divisor $\mathrm{div}_X(f)$ on X satisfying the equivalent properties in Corollary 5.6.13. That is

$$\mathrm{div}_X(f) = (\mathrm{div}_X(f)_{|V_0}, \mathrm{div}_X(f)_{|S}) = (\mathrm{div}_{V_0}(f), r_1(x)_{S_1,\infty}, \ldots, r_m(x)_{S_m,\infty}),$$

see Notation 5.5.7. We easily see that $\mathcal{P}_\pi$ together with the multiplication of ideals forms a subgroup of the abelian group $\mathrm{InvId}(R_0)$. △

Proposition 5.6.20. *Every element fR_0 in $\mathcal{P}_\pi$ with $f = (f_1, \ldots, f_m) \in \mathcal{K}_X(X)^\times$ satisfies $\deg f_i R_{i,0} = r_i n_i$ for some $r_i \in \mathbb{Z}$, $i = 1, \ldots, m$. In particular, $\deg_k fR_0 = \sum_{i=1}^m r_i n_i$.*

Proof. Principal divisors have degree zero, see Lemma 3.1.12. Hence, by Proposition 3.1.27, we have $\deg_k \operatorname{div}_X(f) = 0$ and $\deg_k \operatorname{div}_{X_i}(f_i) = 0$. Moreover, by Lemma C.1.28, we have

$$\deg_k fR_0 = \sum_{i=1}^{m} \deg_k fR_0/fP_i = \sum_{i=1}^{m} \deg_k f_i(R_0/P_i) \tag{6:13}$$

where we have used that fR_0/fP_i is isomorphic to the R_0/P_i-ideal $f_i(R_0/P_i)$. By assumption on f, we have $f_i\mathcal{O}_{S_i} = x^{-r_i}\mathcal{O}_{S_i}$, see Corollary 5.6.13. This together with $\deg_k \operatorname{div}_{X_i}(f_i) = 0$ and Corollary C.4.13 yields $\deg_k f_i(R_0/P_i) = \deg_k f_i\mathcal{O}_{S_i} = \deg_k x^{-r_i}\mathcal{O}_{S_i}$. The latter is equal to r_in_i by Corollary D.2.9 which, together with Eq. (6:13), provides the assertion. □

Definition 5.6.21. Let $\operatorname{Spec}(R_0)^0 = \{P_1, \dots, P_m\}$ denote the minimal prime ideals of R_0. Then we define

$$\mathcal{I}_\pi = \{M \in \operatorname{InvId}(R_0) \mid \deg_k M/P_iM = r_in_i\}.$$

By Lemma C.1.28, we have $\deg_k M = \sum_{i=1}^m r_in_i$ for every $M \in \mathcal{I}_\pi$. Then $\mathcal{I}_\pi$ together with the multiplication of R_0-ideals forms a subgroup of $\operatorname{InvId}(R_0)$. Indeed, by Proposition C.1.26, we have $\deg_k MN = \deg_k M + \deg_k N$ for any two $M, N \in \operatorname{InvId}(R_{i,0})$. By Proposition 5.6.20, $\mathcal{P}_\pi$ is a subgroup of $\mathcal{I}_\pi$. △

Proposition 5.6.22. *The map*

$$\begin{array}{rccc} \gamma: & \operatorname{Div}^0_\pi(X) & \to & \mathcal{I}_\pi \\ & D + \sum_{i\in A} r_i(x)_{i,\infty} & \mapsto & \mathcal{O}_X(D)(V_0) \end{array}$$

is a group isomorphism.

Proof. The representation $D + \sum_{i\in A} r_i(x)_{i,\infty}$ is unique, see Remark 5.5.6. Hence

$$D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty} \mapsto D$$

induces a group homomorphism $\operatorname{Div}^0_\pi(X) \to \operatorname{Div}(X)$ whose image consists of divisors D on X with $D_{|X_i}$ having degree equal to r_in_i for some $r_i \in \mathbb{Z}$, see Remark 5.6.15. Thus the isomorphism $\operatorname{Div}(X) \to \operatorname{InvId}(X)$ as in Proposition 3.1.27 followed by the homomorphism $\operatorname{InvId}(X) \to \operatorname{InvId}(R_0)$, $\mathcal{F} \mapsto \mathcal{F}(V_0)$ provides a group homomorphism $\operatorname{Div}^0_\pi(X) \to \operatorname{InvId}(R_0)$ sending $D + \sum_{i\in A} r_i(x)_{i,\infty}$ to $\mathcal{O}_X(D)(V_0)$. By Remark 5.6.15, we have $\deg_k D_{|V_{i,0}} = r_in_i$ for some $r_i \in \mathbb{Z}$ and thus with Lemma C.4.8 and Corollary C.4.12 we deduce

$$\deg_k \mathcal{O}_X(D_{|V_{i,0}})(V_{i,0}) = \deg_k \mathcal{O}_X(D_{|V_{i,0}}) = -\deg_k D_{|V_{i,0}} = -r_in_i.$$

In particular, by Lemma 3.2.30, we have

$$\deg_k \mathcal{O}_X(D)(V_0)/P_i\mathcal{O}_X(D)(V_0) = \deg_k \mathcal{O}_X(D_{|V_{i,0}})(V_{i,0}) = -r_in_i$$

and therefore $\mathcal{O}_X(D)(V_0) \in \mathcal{I}_\pi$. This proves that the above homomorphism is equal to γ which in turn proves that γ is a group homomorphism.

Now let us prove that γ is surjective. Let $I \in \mathcal{I}_\pi$ be an invertible R_0-ideal such that $\deg_k I/P_iI = r_in_i$ for all $i \in A$. Let D_0 denote the preimage of I under the isomorphism $\operatorname{Div}(V_0) \to \operatorname{InvId}(R_0)$ as in Proposition 3.1.27. That is $\mathcal{O}_{V_0}(D_0)(V_0) = I$ and

$$\deg_k (D_0)_{|V_{i,0}} = -\deg_k \mathcal{O}_{V_{i,0}}((D_0)_{|V_{i,0}})(V_{i,0}) = \deg_k I/P_iI = r_in_i.$$

Now using Lemma 5.3.13 with S being the finite set and $f_j = 1$ for all points $Q_j \in S$ we see that there is a divisor D on X such that $D_{|V_0} = D_0$ and $D_{|S} = 0$. Then, by construction, we have $D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$ as well as $\mathcal{O}_X(D)(V_0) = I$ which proves the surjectivity of γ.

The kernel of γ is given by divisors $D + \sum_{i\in A} r_i(x)_{i,\infty}$ with $\mathrm{Supp}(D) \subseteq V_0$ such that $\mathcal{O}_X(D)(V_0) = R_0$. The latter is equivalent to $\mathcal{O}_X(D)_{|V_0} = \mathcal{O}_{V_0}$ and thus to $D_{|V_0} = 0$. In particular, since the restriction map is a group homomorphism, see Corollary 3.2.23, we have

$$(D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty})_{|X_j} = D_{|X_j} + (\sum\nolimits_{i\in A} r_i(x)_{i,\infty})_{|X_j} = (\sum\nolimits_{i\in A} r_i(x)_{i,\infty})_{|X_j} = r_j(x)_{X_j,\infty}$$

where we have used Corollary 5.6.7. Now the former has, by assumption, degree zero. The latter has degree $r_j n_j$ and hence we deduce that $r_j = 0$ for all $j \in A$. That is, γ is injective as well and thus the assertion follows. □

Corollary 5.6.23. *We have an isomorphism of abelian groups* $\mathrm{CaCl}^0_\pi(X) \to \mathcal{I}_\pi/\mathcal{P}_\pi$ *given by*

$$\begin{array}{rccc} \phi: & \mathrm{CaCl}^0_\pi(X) & \to & \mathcal{I}_\pi/\mathcal{P}_\pi \\ & [D + \sum_{i\in A} r_i(x)_{i,\infty}] & \mapsto & [\mathcal{O}_X(D)(V_0)] \end{array}$$

where $\mathrm{Supp}(D) \subseteq V_0$. *In particular,* $\mathrm{Pic}^0(X) \cong \mathrm{CaCl}^0(X) \cong \mathcal{I}_\pi/\mathcal{P}_\pi$.

Proof. By Proposition 5.6.22, we have the isomorphism of abelian groups

$$\begin{array}{rccc} \gamma: & \mathrm{Div}^0_\pi(X) & \to & \mathcal{I}_\pi \\ & D + \sum_{i\in A} r_i(x)_{i,\infty} & \mapsto & \mathcal{O}_X(D)(V_0). \end{array}$$

We are left to prove that $\gamma(\mathrm{Princ}_\pi(X)) = \mathcal{P}_\pi$. But this is trivial since $\gamma(\mathrm{div}_X(f)) = \mathcal{O}_X(\mathrm{div}_X(f))(V_0) = f_{|V_0}R_0$ is a principal ideal and lies in $\mathcal{I}_\pi$ by Proposition 5.6.22. The particular part now follows from Proposition 5.6.16. □

Since we now see that the functions in Princ^0_π will be those by which we alter representatives in CaCl^0_π, we give them a name.

Definition 5.6.24. Let $f \in \mathcal{K}_X(X)^\times$. If $fR_0 \in \mathcal{P}_\pi$ or, equivalently, $\mathrm{div}_X(f) \in \mathrm{Princ}_\pi(X)$, f is called a **modification function**. Consider the following two cases:

1. $D \in \mathrm{Div}(X)$ and $f \in \mathrm{Princ}_\pi(X)$ such that $f \in \mathcal{O}_X(D)(V_0)$, and
2. $I \in \mathcal{I}_\pi$ and $f \in I$ such that $fR_0 \in \mathcal{P}_\pi$.

In these cases we call f a **modification function of** D respectively a **modification function of** I. By definition, f is a modification function of D if and only if f is a modification function of $\mathcal{O}_X(D)(V_0)$. △

Let $f \in R_0$ be arbitrary. The following Lemma provides a sufficient condition for fR_0 to lie in $\mathcal{P}_\pi$, that is for f to be a modification function. From an algorithmic point of view, it will be very convenient that this condition is entirely expressed in terms of the coefficients of f with respect to the fixed $k[x]$-basis Ω of R_0.

Lemma 5.6.25. *Let* $\Omega = (\omega_1, \ldots, \omega_n)$ *be a reduced basis of* R_0. *Then* $\widetilde{\omega}_i = \omega_i x^{|X|_i}$ *is a* $k[x^{-1}]$*-basis of* R_∞ *and* $\mathcal{O}_\infty$*-basis of* $\mathcal{O}_S$. *If* $f = \sum_{i=1}^n \lambda_i\omega_i$ *with* $\lambda_i \in k[x]$ *such that*

$$\deg(\lambda_i) < \deg(\lambda_1) + |X|_i \quad \textit{for} \quad i = 2, \ldots, n,$$

then it satisfies $f\mathcal{O}_S = x^{\deg(\lambda_1)}\mathcal{O}_S$. *Note that for* $\lambda_i = 0$ *there is no condition imposed on the degree of* λ_1 *with respect to* $-|X|_i$.

Proof. Let $f = \sum_{i=1}^{n} \lambda_i \omega_i$ with $\deg \lambda_1 = r$ and $\deg \lambda_i < r + |X|_i$. Note that for every $\lambda_i \in k[x] \setminus \{0\}$ we have a unique representation $\lambda_i = x^{\deg(\lambda_i)}\varepsilon_i$ with $\varepsilon_i \in k[x^{-1}] \setminus x^{-1}k[x^{-1}] \subseteq \mathcal{O}_\infty^\times$. Then we have

$$\begin{aligned} f &= \sum_{i:\lambda_i \neq 0}^{n} \lambda_i x^{-|X|_i} \cdot \widetilde{\omega}_i = x^r \cdot \sum_{i:\lambda_i \neq 0}^{n} \lambda_i x^{-r-|X|_i} \cdot \widetilde{\omega}_i \\ &= x^r \cdot \sum_{i:\lambda_i \neq 0}^{n} \varepsilon_i \; x^{\deg(\lambda_i)-r-|X|_i} \cdot \widetilde{\omega}_i \\ &= x^r \cdot \left(\varepsilon_1 \; x^{\deg(\lambda_1)-r-|X|_1} \cdot \widetilde{\omega}_1 + \sum_{i\geq 2:\lambda_i \neq 0}^{n} \varepsilon_i \; x^{\deg(\lambda_i)-r-|X|_i} \cdot \widetilde{\omega}_i \right) \\ &= x^r \cdot \left(\varepsilon_1 + \sum_{i\geq 2:\lambda_i \neq 0}^{n} \varepsilon_i \; x^{\deg(\lambda_i)-r-|X|_i} \cdot \widetilde{\omega}_i \right). \end{aligned}$$

Let $z := \sum_{i\geq 2:\lambda_i \neq 0}^{n} \varepsilon_i \; x^{\deg(\lambda_i)-r-|X|_i} \cdot \widetilde{\omega}_i$. Then by the above, we have $f = x^r \cdot (\varepsilon_1 + z)$. By assumption, we have $\deg(\lambda_i) - r - |X|_i < 0$ for all $i = 2, \ldots, n$. Thus $z \in x^{-1}R_\infty$ and therefore z is contained in every maximal prime ideal of $\mathcal{O}_S$. Moreover, since $\varepsilon_1 \in k[x^{-1}] \setminus x^{-1}k[x^{-1}]$, it is not contained in any of the maximal primes of $\mathcal{O}_S$ and hence $\varepsilon_1 + z \in \mathcal{O}_S^\times$. □

Note that Lemma 5.6.25 does indeed imply that f is a modification function, but its implications are even stronger: It says that the principal divisor of f (if $f \in \mathcal{K}_X(X)^\times$) corresponds to

$$(\mathrm{div}_{V_0}(f), \mathrm{div}_S(x^{\deg(\lambda_1)})) = (\mathrm{div}_{V_0}(f), \mathrm{div}_{S_1}(x^{\deg(\lambda_1)}), \ldots, \mathrm{div}_{S_m}(x^{\deg(\lambda_1)}))$$

under the identification in Notation 5.5.7. That is, choosing f as above implies that the coefficients of the generalised pole divisor in the representation of $\mathrm{div}_X(f)$ will all be the same. Thus we face the problem that this method does not provide any possibility to control the coefficients r_i of $r_i \mathrm{div}_{S_i}(x) = \mathrm{div}_{S_i}(x^{r_i})$. But we can overcome this disadvantage by applying Lemma 5.6.25 for all the irreducible components $X_1, \ldots, X_m$.

5.6.2 Component Dependent and Independent Representation

In this section we will distinguish between two possible types of representatives in $\mathrm{CaCl}_\pi^0(X)$, those that have the same restriction to every S_i and those who may have different restrictions to the S_i. We will call the approach of solely working with the former type of representatives the component independent case and working with the latter type of representatives is called the component dependent case.

As we have already mentioned in Remark 5.6.10, by putting $r_i = r$ for all $i \in A$, the generalised pole divisor $\sum_{i\in A} r_i(x)_{i,\infty}$ equals the pole divisor $r(x)_\infty$. That is, degree zero divisors of the form $D + r(x)_\infty \in \mathcal{D}_0$ with $\mathrm{Supp}(D) \subseteq V_0$ are possible representatives of classes in $\mathrm{CaCl}_\pi^0(X)$. The next theorem and its corollary show that every class in $\mathrm{CaCl}_\pi^0(X)$ admits such a representative.

Theorem 5.6.26. *Let X be a cover of $\mathbb{P}_k^1$. For every invertible $\mathcal{O}_X$-ideal $\mathcal{F}$ there is some invertible $\mathcal{O}_X$-ideal $\mathcal{L}$ and $s \in \mathbb{Z}$ such that*

$$\mathcal{F} \cong \mathcal{L}(s(x)_\infty), \quad \mathcal{L} \leq \mathcal{O}_X \quad \textit{and} \quad \mathrm{Supp}(\mathcal{L}) \subseteq V_0 \textit{ (resp. } \mathcal{L}_{|S} = \mathcal{O}_S\textit{).}$$

Proof. Let $\mathcal{F}$ be an invertible $\mathcal{O}_X$-ideal. Since $\mathcal{F}$ is invertible, the same is true for $\mathcal{F}_{|S}$ by Proposition 3.2.28. Also, by Proposition 3.2.28, we have $\mathcal{F}(S) = h\mathcal{O}_S$ for some regular $h \in \mathrm{Frac}(R_0)$. Then multiplication by $h^{-1}\mathcal{O}_X$ provides that we may without loss of generality assume that $\mathcal{F}_{|S} = \mathcal{O}_S$ and thus $\mathrm{Supp}(\mathcal{F}) \subseteq V_0$.

The next (and last) step is to find a regular global section which wedges $\mathcal{F}(V_0)$ into R_0 and behaves like a power of x over S. To do so, we set $\mathcal{G} := \mathcal{F}^{-1}((x^r)_\infty)$ and $\mathcal{H} := \mathcal{F}^{-1}((x^{r-1})_\infty)$. Note that by Proposition 3.1.27, we have $\mathcal{G}_P = x^r\mathcal{O}_{X,P}$ and $\mathcal{H}_P = x^{r-1}\mathcal{O}_{X,P}$ for all $P \in S$. Then any regular global section f of $\mathcal{G}$ satisfies $f\mathcal{O}_X \leq \mathcal{F}^{-1}((x^r)_\infty)$ and thus

$$\mathcal{L} := f\mathcal{F}((x^{-r})_\infty) \leq \mathcal{O}_X$$

will therefore satisfy $\mathcal{L}_{|V_0} \cong f\mathcal{F}(V_0) \subseteq R_0$. Moreover, since f is regular, $\mathcal{L} \cong \mathcal{F}((x^{-r})_\infty)$. If moreover, $f\mathcal{O}_S = x^r\mathcal{O}_S$, then $\mathcal{L}$ will also satisfy $\mathcal{L}_{|S} \cong \mathcal{O}_X(x^{r-r})_{|S} = \mathcal{O}_S$. Then $\mathcal{F} = f^{-1}\mathcal{O}_X \otimes_{\mathcal{O}_X} \mathcal{L}((x^r)_\infty) \cong \mathcal{L}((x^r)_\infty)$ with $\mathcal{L} \leq \mathcal{O}_X$ and $\mathrm{Supp}(\mathcal{L}) \subseteq V_0$ as asserted.

To find such global section, we want to employ the Approximation Theorem 5.7.1. To use it, $H^1(X, \mathcal{H}) = 0$ needs to be satisfied. By Proposition D.2.3, we have that $(x)_\infty$ is an ample divisor, i.e. $\mathcal{O}_X((x)_\infty)$ is an ample invertible sheaf on X. Since $\mathcal{F}^{-1}$ is coherent, by [Liu02, 5.3.6] there is n_0 such that for all $n \geq n_0$ and $p \geq 1$ we have

$$0 = H^p\left(X, \mathcal{F}^{-1} \otimes_{\mathcal{O}_X} \mathcal{O}_X((x)_\infty)^{\otimes n}\right).$$

By [Liu02, 7.1.18 (a)], we have $\mathcal{O}_X(D)^{\otimes r} \cong \mathcal{O}_X(rD)$ for every $r \in \mathbb{Z}$. Thus $\mathcal{O}_X((x)_\infty)^{\otimes n} \cong \mathcal{O}_X(r(x)_\infty) = \mathcal{O}_X((x^r)_\infty)$ which provides $H^1\left(X, \mathcal{F}^{-1}((x^r)_\infty)\right) = 0$ for some $r \in \mathbb{Z}$.

Now we require $0 \neq g_P = x^r \in \mathcal{G}_P$ for $P \in S$ with $r \in \mathbb{Z}$ as above and $g_P = f_P \in \mathcal{G}_P$ for $P \in V_0$ where $\mathcal{F}_P = f_P\mathcal{O}_{X,P}$ for all $P \in V_0$ (thus no further requirement in V_0). Then the Approximation Theorem 5.7.1 guarantees the existence of $g \in \mathcal{G}(X)$ with $g_P = x^r + x^{r-1}b_P$ for $b_P \in \mathcal{O}_{X,P}$ for all $P \in S$. Hence $g_P = x^r(1 + x^{-1}b_P)$ where $1 + x^{-1}b_P \in \mathcal{O}_{X,P}^\times$ since $x^{-1} \in P\mathcal{O}_{X,P}$. Whence $g_P\mathcal{O}_{X,P} = x^r\mathcal{O}_{X,P}$ for all $P \in S$ and hence $g\mathcal{O}_S = x^r\mathcal{O}_S$ as global sections of $\mathcal{K}_S$ as desired. In particular, g corresponds to a regular global section of $\mathcal{K}_X$ via the isomorphism $\mathcal{K}_X \to \mu_*\mathcal{K}_S$, see Proposition 3.2.17. □

In Corollary E.2.18 in the appendix we will provide bounds for the integers $n_0 \in \mathbb{Z}$ such that for all $r \geq n_0$ the term $H^1(X, \mathcal{F}(r(x)_\infty))$ vanishes. By the proof of Theorem 5.6.26, this gives the following corollary.

Corollary 5.6.27. *The integer s in Theorem 5.6.26 can be bounded by*

$$\max_{i=1}^{m}\{(\deg_k \mathcal{F}_{|X_i})/n_i + 2c_{i,X}\} \leq \max_{i=1}^{m}\{(\deg_k \mathcal{F}_{|X_i})/n_i\} + 2c_X.$$

Corollary 5.6.28. *For every divisor $D \in \mathrm{Div}(X)$ there is some divisor $E \in \mathrm{Div}(X)$ with $E \leq 0$ and $\mathrm{Supp}(E) \subseteq V_0$ such that D and $E + s(x)_\infty$ are linear equivalent for some $s \in \mathbb{Z}$. Moreover, there is E such that s is upper bounded by*

$$\max_{i=1}^{m}\{(-\deg_k D_{|X_i})/n_i + 2c_{i,X}\} \leq \max_{i=1}^{m}\{(-\deg_k D_{|X_i})/n_i\} + 2c_X.$$

Proof. Apply Theorem 5.6.26 to $\mathcal{O}_X(D)$ and obtain $\mathcal{O}_X(E + (x^r)_\infty) \cong \mathcal{O}_X(D)$ with $\mathcal{O}_X(E) \leq \mathcal{O}_X$ and $\mathrm{Supp}(E) \subseteq V_0$. Now $\mathcal{O}_X(E) \leq \mathcal{O}_X$ is equivalent to $E \leq 0$, see Proposition 3.1.27 (ii). Moreover, since any two invertible $\mathcal{O}_X$-ideals are isomorphic if and only if they differ multiplicatively by the invertible sheaf associated to a principal divisor, see Lemma 3.1.26, E satisfies the asserted properties. The last part follows from Corollary 5.6.27. □

Remark 5.6.29. In Section 5.8 we will see that the bound for the integer s in Corollary 5.6.28 can be obtained solely by the existence of a divisor of the form $D + r(x)_\infty$ with unbounded r using modification functions. The method introduced there has the advantage that it also tells us how to reduce a divisor class given by a representative of the form $D+r(x)_\infty$ by using modification functions. This will be crucial in our algorithms that implement the arithmetic in $\mathrm{Pic}^0(X)$. △

Remark 5.6.30. Corollary 5.6.28 shows that the group $\mathrm{CaCl}^0_\pi(X)$ is isomorphic to the group of divisor classes with representatives $D + r(x)_\infty \in \mathcal{D}_0$, $\mathrm{Supp}(D) \subseteq V_0$, modulo principal divisors $\mathrm{div}_X(f)$ with $\mathrm{div}_S(f) = r(x)_\infty$. If X is integral, these two groups are equal by definition. △

Therefore, we may either work with representatives of the form $D + r(x)_\infty \in \mathcal{D}_0$ or of the form $D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathcal{D}_0$ both with $\mathrm{Supp}(D) \subseteq V_0$. Since we want to work with both forms, we give these two types of approaches to compute in $\mathrm{CaCl}^0_\pi(X)$ names.

Notation 5.6.31. We call the approach of working with representatives of the form $D + r(x)_\infty \in \mathcal{D}_0$ the **component independent case**. The approach of working with representatives of the form $D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathcal{D}_0$ is called the **component dependent case**. △

In the component independent case one tries to avoid the irreducible components of X and rather treats X as if it was irreducible. Actually, after working out how one could compute fast enough in $\mathrm{CaCl}^0(X)$ in the case of irreducible X, this should be the first approach of dealing with the more general case of reducible X. But as we have seen in Section 4.5, especially in Lemma 4.5.1 and Corollary 4.5.2, to obtain effective bounds for the π-invariants of both divisors and X itself, it was necessary to examine the irreducible components of X and the restriction of divisors to those. We will see in Section 5.8 that the degree of the ideal representatives will depend on these bounds. Therefore, one could say that using the component dependent mindset to work out the above bounds and try to come up with algorithms to cope with the component dependent case finally provides the possibility to (almost) forget about the irreducible components at all.

Remark 5.6.32. We want to highlight some properties of working in the component independent case: Let $D + r(x)_\infty \in \mathcal{D}_0$ with $D \leq 0$ denote a representative of an element in $\mathrm{Div}^0_\pi(X)$. Then $\deg_k D = -rn$ and $\deg_k \mathcal{O}_X(D)(V_0) = rn$, see Lemma D.2.13 and Proposition C.4.18 (i), (ii). Moreover, since $D \leq 0$, we have $\mathcal{O}_X(D)(V_0) \subseteq R_0$, see Proposition 3.1.27 (ii). Therefore, in the component independent case we work with integral ideals that have degree which is a multiple of n. The same holds for the modification functions by which we alter the ideal representatives. △

In the rest of this section, we show how the definitions of $\mathcal{I}_\pi$, $\mathcal{P}_\pi$ and $\mathrm{CaCl}^0_\pi(X)$ play out in the case of X being integral. We will see that this resembles what we have already seen in Remark 5.6.32. Let (X, π) be an integral cover of $\mathbb{P}^1_k$. As already mentioned in Remark 5.6.10, setting all r_i to the same number r, the generalised pole divisor $\sum_{i\in A} r_i(x)_{i,\infty}$ defined in Definition 5.6.3 equals a multiple $r(x)_\infty$ of the pole divisor of x on X, see Definition 2.2.9. Then the definition of $\mathrm{Div}^0_\pi(X)$ and $\mathrm{Princ}^0_\pi(X)$ translate into

(i) $\mathrm{Div}^0_\pi(X) = \{D + r(x)_\infty \in \mathcal{D}_0 \mid \mathrm{Supp}(D) \subseteq V_0, r \in \mathbb{Z}\}$, and

(ii) $\mathrm{Princ}^0_\pi(X) = \{\mathrm{div}(f) \in \mathrm{Princ}(X) \mid \mathrm{div}(f)_{|S} = r((x)_\infty)_{|S}, r \in \mathbb{Z}\}$.

Moreover, the definitions of $\mathcal{I}_\pi$ and $\mathcal{P}_\pi$ still apply in the integral case and then translate into

(i) $\mathcal{I}_\pi = \{M \in \mathrm{InvId}(R_0) \mid \deg_k M = rn \text{ for some } r \in \mathbb{Z}\}$, and

(ii) $\mathcal{P}_\pi = \{fR_0 \in \mathrm{InvId}(R_0) \mid f \in \mathrm{Frac}(R_0), f\mathcal{O}_S = x^r\mathcal{O}_S \text{ for some } r \in \mathbb{Z}\}$.

Furthermore, the isomorphism γ in Proposition 5.6.22 translates into

$$\begin{array}{rccc} \gamma: & \mathrm{Div}^0_\pi(X) & \to & \mathcal{I}_\pi \\ & D + r(x)_\infty & \mapsto & \mathcal{O}_X(D)(V_0) \end{array} \tag{6:14}$$

finally providing the isomorphism

$$\begin{array}{rccc} \phi: & \mathrm{CaCl}^0_\pi(X) & \to & \mathcal{I}_\pi/\mathcal{P}_\pi \\ & [D + r(x)_\infty] & \mapsto & [\mathcal{O}_X(D)(V_0)]. \end{array} \tag{6:15}$$

Summarising the above, we deduce that we can carry out the group law in $\mathrm{CaCl}^0(X)$ by computing with invertible ideals of R_0 having a degree that is a multiple of n and be able to modify by principal ideals whose generator generates the same principal ideal over $\mathcal{O}_S$ as some power of x does.

Remark 5.6.33. Note that by construction the restriction map $\rho_i : \mathrm{InvId}(R_0) \to \mathrm{InvId}(R_{i,0})$, $I \mapsto I/P_{i,0}I$ sends elements in $\mathcal{I}_\pi$ to elements in $\mathcal{I}_{\pi_i}$. Moreover, the elements in $\mathcal{P}_\pi$ are those principal ideals fR_0 in $\mathcal{I}_\pi$ such that for all $i = 1, \ldots, m$ we have $\rho_i(fR_0) \in \mathcal{P}_{\pi_i}$. That is, the modification functions on X are exactly those functions that restrict to modification functions on all of the irreducible components $X_1, \ldots, X_m$ of X. Hence to find a modification function on X, it is sufficient to find a function that restricts to modification functions on the components. △

5.7 Modification Functions

In this section we will examine modification functions of divisors more closely. We will prove that for every divisor $D \leq 0$ on X with support away from S (that is, for all $r_i \in \mathbb{Z}$ we have $D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$) there is a modification function $f \in \mathcal{L}_{\mathrm{reg}}(D + \sum_{i\in A} r_i(x)_{i,\infty})$ with $fR_0 \subseteq \mathcal{O}_X(D)(V_0)$ and $fR_0 \in \mathcal{P}_\pi$.

Modification functions will play an eminent role in our algorithmic approach of computing in $\mathrm{CaCl}^0_\pi(X)$ as we will see in Chapter 6. However, also theoretically they provide fundamental insights. For instance, they enable us to find representatives for each class in $\mathcal{I}_\pi/\mathcal{P}_\pi$ (and thus in $\mathrm{CaCl}^0_\pi(X)$) that are *integral* and have *bounded degree*.

Since we want to work with two approaches, the component independent case and the component dependent case, we need to provide existential statements of modification functions in both cases. In Section 5.7.1 we will give the somewhat constructive proofs of their existence in both cases. These proofs have a very geometric character and are, at least with respect to their basic ideas, easy to follow. The proofs themselves are quite technical. They rely heavily on the Approximation Theorem 5.7.1 which we will provide in a very general sheaf theoretic fashion. Moreover, since the proof in the component dependent case uses an iterative argument, it relies on some commutative algebra which cares about characterising the image of the natural morphism $M \to \bigoplus_{i=1}^m M/P_iM$ which is treated in Section B.4 of the appendix.

The reader that is mainly interested in the algorithmic aspect of this thesis, that is, in the concrete computation in $\mathrm{CaCl}^0_\pi(X)$ may skip Section 5.7.1 altogether since in Section 5.7.2 we do not only provide the explicit algorithms for computing the desired modification functions but these algorithms do also provide the existential statements of the modification functions. The degree bounds there are not as good as the ones we can provide in Section 5.7.1, but they are asymptotically the same.

The main difference between the two approaches to prove the existence of modification functions is the following: The first and more geometric approach uses that we can come

up with modification functions on integral schemes and thus on the irreducible components of X. Given a modification function on the first (we will fix an order of the irreducible components to do so) irreducible component X_1 of X, we will try to find one on the second, say X_2, which agrees with the first one on $X_1 \cap X_2$. This provides a modification function on $X_1 \cup X_2$ and thus we can proceed iteratively in this manner which finally yields the desired modification function on all of X. While doing so, we follow the commutative algebra instructions given in Section B.4 that guarantee that the computed element f actually lies in $\mathcal{O}_X(D)(V_0)$. The second and very algorithmic approach uses the basis matrix of the ideal $\mathcal{O}_X(D)(V_0)$ with respect to Ω_i^m. It then finds a suitable element in the column space of that matrix such that its i-th row block (which contains the coefficients of the restriction of that element to the i-th irreducible component with respect to Ω_i) satisfies the sufficient conditions of Lemma 5.6.25. The latter provides that the respective restriction is indeed a modification function on that component.

Summarising the above, one approach uses an iterative procedure to successively find modification functions in $\mathcal{O}_{X_i}(D_{|X_i})(V_{i,0})$ on the irreducible components X_i such that the result actually lies in $\mathcal{O}_X(D)(V_0)$ and not only in $\bigoplus_{i=1}^m \mathcal{O}_{X_i}(D_{|X_i})(V_{i,0})$. The other approach constructs an element within the ideal $\mathcal{O}_X(D)(V_0)$ that satisfies the sufficient conditions in Lemma 5.6.25 on each irreducible component.

5.7.1 Existence of Modification Functions

We start by stating the Approximation Theorem 5.7.1 in a very general setting and for $\mathcal{O}_X$-ideals. We note that the Approximation Theorem 5.7.1 even holds for more general sheaves, see Remark 5.7.2.

Theorem 5.7.1 (Approximation Theorem)**.** *Let $\mathcal{L}, \mathcal{F}$ be non-zero $\mathcal{O}_X$-ideals with $\mathcal{F} \leq \mathcal{L}$ and $H^1(X, \mathcal{F}) = 0$. Then the following sequence is exact:*

$$0 \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^0(X, \mathcal{L}) \longrightarrow \coprod_{P \in X} \mathcal{L}_P / \mathcal{F}_P \longrightarrow 0.$$

Proof. By taking cohomology, the exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}/\mathcal{F} \longrightarrow 0,$$

provides the exact sequence

$$0 \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^0(X, \mathcal{L}) \longrightarrow H^0(X, \mathcal{L}/\mathcal{F}) \longrightarrow H^1(X, \mathcal{F}) = 0,$$

see Lemma 5.2.5. By Corollary C.3.3, we obtain $H^0(X, \mathcal{L}/\mathcal{F}) = \coprod_{P \in X} \mathcal{L}_P/\mathcal{F}_P$ and the result follows. □

Remark 5.7.2. The proof of the Approximation Theorem 5.7.1 shows that we do not rely on $\mathcal{F}$ and $\mathcal{L}$ being $\mathcal{O}_X$-ideals, but only on the fact that Cohomology is defined for such sheaves and that the quotient sheaf $\mathcal{L}/\mathcal{F}$ is a skyscraper sheaf. Thus the Approximation Theorem 5.7.1 may also be formulated for X a topological space and sheaves defined over a category that provides the possibility of subsheaves. △

Remark 5.7.3. The name "Approximation Theorem" is justified in the following sense: We may choose arbitrary elements $a_P \in \mathcal{L}_P$ for all $P \in X$ and then the exactness of the sequence provides the existence of $g \in \mathcal{L}(X)$ such that $g_P + \mathcal{F}_P = a_P + \mathcal{F}_P$. Thus, up to values in $\mathcal{F}_P$ we can approximate an element in $\mathcal{L}(X)$ with prescribed values in $\mathcal{L}_P$ for all $P \in X$. △

The following proposition tells us that for any given divisor $D \leq 0$ with support away from S there are functions $f \in \mathcal{L}_{\text{reg}}(D + r(x)_\infty)$ with $f\mathcal{O}_S = x^r\mathcal{O}_S$ where the power r

depends on $\max_{i=1}^{m}\{-(\deg_k D_{|X_i})/n_i\}$. That is we may find modification functions with a common power r on all irreducible components.

Proposition 5.7.4. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $D \in \mathrm{Div}(X)$ be a divisor on X with $D \leq 0$ and $\mathrm{Supp}(D) \subseteq V_0$. Let $r \in \mathbb{Z}$ be any integer with $r > \max_{i=1}^{m}\{-(\deg_k D_{|X_i})/n_i + 2c_{i,X}\}$. Then there is $f \in \mathcal{K}_X(X)^\times$ such that*

(i) $f \in \mathcal{L}_{\mathrm{reg}}(D + r(x)_\infty)$ and

(ii) $f\mathcal{O}_S = x^r\mathcal{O}_S$.

Proof. Let D be given by the data (U_i, h_i^{-1}) for which we know that $h_i \in \mathcal{O}_X(U_i)$ since $D \leq 0$. Then $\mathcal{O}_X(D)_{|U_i} = h_i\mathcal{O}_{U_i}$ and thus $\mathcal{O}_X(D)_P = h_i\mathcal{O}_{X,P}$ for every $P \in U_i$. We set $\mathcal{L} = \mathcal{O}_X(D + r(x)_\infty)$ and $\mathcal{F} = \mathcal{O}_X(D + (r-1)(x)_\infty)$. Then we have

$$\mathcal{L}_P = \begin{cases} x^r\mathcal{O}_{X,P}, & P \in S \\ h_i\mathcal{O}_{X,P}, & P \in V_0 \end{cases}, \quad \mathcal{F}_P = \begin{cases} x^{r-1}\mathcal{O}_{X,P}, & P \in S \\ h_i\mathcal{O}_{X,P}, & P \in V_0 \end{cases} \tag{7:16}$$

By Corollary E.2.18, we have $H^1(X, \mathcal{F}) = H^1(X, \mathcal{O}_X(D + (r-1)(x)_\infty) = 0$ if $r - 1 \geq \max_{i=1}^{m}\{(\deg_k \mathcal{O}_X(D)_{|X_i})/n_i + 2c_{i,X}\}$. By Lemma C.4.8, we have $\deg_k \mathcal{O}_X(D)_{|X_i} = -\deg_k D_{|X_i}$ and thus $r > \max_{i=1}^{m}\{-(\deg_k D_{|X_i})/n_i + 2c_{i,X}\}$ is sufficient for $H^1(X, \mathcal{O}_X(D + (r-1)(x)_\infty)$ to vanish. We set

$$a_P = \begin{cases} x^r + \sum_{i=2}^{n} x^{r-1+|X|_i}\omega_i, & P \in S \\ h_i, & P \in V_0 \end{cases} \in \mathcal{L}_P$$

and note that

$$x^r + \sum_{i=2}^{n} x^{r-1+|X|_i}\omega_i = x^r + \sum_{i=2}^{n} x^{r-1}\widetilde{\omega}_i = x^r\left(1 + \sum_{i=2}^{n} x^{-1}\widetilde{\omega}_i\right).$$

Hence $a_P = x^r \cdot \varepsilon_P$ where $\varepsilon_P \in \mathcal{O}_{X,P}^\times$ for all $P \in S$. Now for r in the asserted order of magnitude we obtain by the Approximation Theorem 5.7.1 the existence of $f \in \mathcal{L}(X)$ (which will turn out to be regular due to its behaviour on S) such that $f_P + \mathcal{F}_P = a_P + \mathcal{F}_P$ for all $P \in X$. Thus, by Eq. (7:16), we have $f_P = a_P + x^{r-1}b_P$ for some $b_P \in \mathcal{O}_{X,P}$ and hence $f_P = x^r\varepsilon_P + x^{r-1}b_P = x^r(\varepsilon_P + x^{-1}b_P)$. Now since $\varepsilon_P \in \mathcal{O}_{X,P}^\times$ and $x^{-1} \in P\mathcal{O}_{X,P}$ for all $P \in S$, we have $\varepsilon_P + x^{-1}b_P \in \mathcal{O}_{X,P}^\times$ and hence $f_P\mathcal{O}_{X,P} = x^r\mathcal{O}_{X,P}$ for all $P \in S$. Since $\mathcal{O}_{S_i}$ is an integral domain with field of fractions F_i, the function field of X_i, we see that $f_P\mathcal{O}_{X,P} = x^r\mathcal{O}_{X,P}$ for all $P \in S_i$ together with $\mathcal{O}_{S_i} = \cap_{P \in S_i}\mathcal{O}_{X,P}$ easily provides the equality $f\mathcal{O}_{S_i} = x^r\mathcal{O}_{S_i}$. Since $\mathcal{O}_S = \bigoplus_{i=1}^{m}\mathcal{O}_{S_i}$, we therefore obtain $f\mathcal{O}_S = \bigoplus_{i=1}^{m} f_i\mathcal{O}_{S_i} = \bigoplus_{i=1}^{m} x^r\mathcal{O}_{S_i} = x^r\mathcal{O}_S$. In particular, $f \in \mathcal{K}_X(X)^\times$. □

In general, the degree of the restrictions $D_{|X_i}$ of a divisor D may be independent of the degree of D and thus to effectively use Proposition 5.7.4 we need to ensure that we will deal with divisors D whose restrictions have bounded degrees.

To do so, we will tweak the proof of Proposition 5.7.4 and apply it to the irreducible components of a cover of $\mathbb{P}^1_k$.

Let X be an integral cover of $\mathbb{P}^1_k$ and let $D \leq 0$ be a divisor on X. We can use the Approximation Theorem 5.7.1 to find modification functions for D that are regular functions on V_0 and which agree with a given function on a given closed subscheme away from S. Moreover, we can ensure that the degree of that modification function is linearly bounded by the degree of D, the arithmetic genus of X and some term determined by the closed subscheme. This will be the main step to prove the existence of modification functions for a general reduced cover of $\mathbb{P}^1_k$.

Proposition 5.7.5. *Let X be an integral cover of $\mathbb{P}^1_k$. Let $Z \subsetneq X$ be a closed subscheme of X (which is thus zero-dimensional, see Proposition B.5.2) disjoint to S. Let $\mathcal{J} \leq \mathcal{O}_X$ be the ideal sheaf corresponding to Z. Let $D \in \mathrm{Div}(X)$, $D \leq 0$, be a non-zero divisor with support away from S and let $r > (-\deg(D) + \deg(\mathcal{J}))/n + c_X$. Then for any $g \in \mathcal{O}_Z(Z)$ there is $f \in F^\times$ such that*

(i) $f \in \mathcal{O}_X(D + r(x)_\infty)(X)$

(ii) $f_{|Z} = g$, *and*

(iii) $f = \sum_{i=1}^n \lambda_i \omega_i$ *where* $\lambda_i \in k[x]$, $\deg(\lambda_1) = r$ *is monic and* $\deg(\lambda_i) \leq r - 1 + |X|_i$ *for all* $i = 2, \ldots, n$.

In particular, $f\mathcal{O}_S = x^r \mathcal{O}_S$. Note that, by (iii), we have $f \in R_0$.

Proof. Let F denote the function field of X. The finite morphism π provides an affine cover V_0 and V_∞ of X where $S = V_\infty \setminus (V_0 \cap V_\infty)$. Since $Z = \mathrm{Supp}(\mathcal{O}_X/\mathcal{J})$ is disjoint to S, we have $\mathcal{J}_P = \mathcal{O}_{X,P}$ for all $P \in S$. Let D be given by the data (U_i, h_i^{-1}) for which we know that $h_i \in \mathcal{O}_X(U_i)$ since $D \leq 0$. Then $\mathcal{O}_X(D)_{|U_i} = h_i \mathcal{O}_{U_i}$ and thus $\mathcal{O}_X(D)_P = h_i \mathcal{O}_{X,P}$ for every $P \in U_i$. We set $\mathcal{L} = \mathcal{O}_X(D + r(x)_\infty)$ and $\mathcal{F} = \mathcal{J}(D + (r-1)(x)_\infty)$. Let R_0 denote the coordinate ring of V_0 and I resp. J the ideals corresponding to $\mathcal{O}_X(D)$ respectively $\mathcal{J}$ on V_0. We have

$$\mathcal{L}_P/\mathcal{F}_P \cong \begin{cases} (\mathcal{O}_X/\mathcal{J})_P, & P \in V_0 \\ x^r \mathcal{O}_{X,P}/x^{r-1}\mathcal{O}_{X,P}, & P \in S \end{cases}.$$

Indeed, for $P \in V_0 \cap U_i$ we have

$$\frac{\mathcal{L}_P}{\mathcal{F}_P} = \frac{\mathcal{O}_X(D)_P}{\mathcal{O}_X(D)_P J_P} = \frac{h_i \mathcal{O}_{X,P}}{h_i \mathcal{O}_{X,P} \mathcal{J}_P} \xrightarrow{\cong} \frac{\mathcal{O}_{X,P}}{J_P} = (\mathcal{O}_X/\mathcal{J})_P.$$

Further, by assumption on D, we have $\mathcal{O}_X(D)_P = \mathcal{O}_{X,P}$ for $P \in S$. Moreover, for $P \in S$ we have $\mathcal{J}_P = \mathcal{O}_{X,P}$ which provides

$$\frac{\mathcal{L}_P}{\mathcal{F}_P} = \frac{x^r \mathcal{O}_X(D)_P}{x^{r-1}\mathcal{O}_X(D)_P \mathcal{J}_P} = \frac{x^r \mathcal{O}_{X,P}}{x^{r-1}\mathcal{O}_{X,P}}.$$

The exactness of $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{L} \longrightarrow \prod_{P \in X} \mathcal{L}_P/\mathcal{F}_P \longrightarrow 0$ provides by Lemma B.1.36 the exact sequence

$$0 \longrightarrow \mathcal{F}(V_0) \longrightarrow \mathcal{L}(V_0) \longrightarrow \prod_{P \in V_0} \mathcal{L}(V_0)_P/\mathcal{F}(V_0)_P \longrightarrow 0.$$

By construction of $\mathcal{F}$ and $\mathcal{L}$, we have $\mathcal{L}(V_0) = I$ and $\mathcal{F}(V_0) = JI$. Hence we obtain an exact sequence

$$0 \longrightarrow JI \longrightarrow I \longrightarrow \prod_{P \in V_0} I_P/J_P I_P \longrightarrow 0.$$

We can argue as above with $\mathcal{J}$ instead of $\mathcal{F}$ and $\mathcal{O}_X$ instead of $\mathcal{L}$ to obtain the exact sequence

$$0 \longrightarrow J \longrightarrow R_0 \longrightarrow \prod_{P \in V_0} (R_0)_P/J_P \longrightarrow 0.$$

Both these sequences are compatible in the sense that we have a commutative diagram

with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & JI & \longrightarrow & I & \xrightarrow{\phi_1} & \prod_{P\in V_0} I_P/J_PI_P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \cong\downarrow\psi & & \\ 0 & \longrightarrow & J & \longrightarrow & R_0 & \xrightarrow{\phi_2} & \prod_{P\in V_0}(R_0)_P/J_P & \longrightarrow & 0 \end{array} \tag{7:17}$$

We may identify $g \in \mathcal{O}_Z(Z)$ with some element $g \in R_0$ which is only unique up to addition with some element in J. The image of g under $\psi^{-1} \circ \phi_2$ in diagram (7:17) has due to the exactness of the top sequence a preimage under ϕ_1, say f. Then, by construction, f and g map via ϕ_2 onto the same element and thus by the exactness of the bottom sequence, $f - g \in J$. If the sequence of global sections

$$0 \longrightarrow H^0(X, \mathcal{F}) \longrightarrow H^0(X, \mathcal{L}) \longrightarrow \coprod_{P\in X} \mathcal{L}_P/\mathcal{F}_P \longrightarrow 0$$

is exact, then we can add this as a top sequence to the diagram in (7:17) with the restriction maps connecting the sequences resulting in a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F}(X) & \longrightarrow & \mathcal{L}(X) & \xrightarrow{\phi_0} & \prod_{P\in X} \mathcal{L}_P/\mathcal{F}_P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & JI & \longrightarrow & I & \xrightarrow{\phi_1} & \prod_{P\in V_0} I_P/J_PI_P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \cong\downarrow\psi & & \\ 0 & \longrightarrow & J & \longrightarrow & R_0 & \xrightarrow{\phi_2} & \prod_{P\in V_0}(R_0)_P/J_P & \longrightarrow & 0 \end{array} \tag{7:18}$$

Now any global section f of $\mathcal{L}$ that maps via ϕ_0 to an element in $\prod_{P\in X} \mathcal{L}_P/\mathcal{F}_P$ that restricts to $(\psi^{-1} \circ \phi_2)(g)$, then $f_{|Z} = g_{|Z}$ as desired. Since $I_P/J_PI_P = h_{i,P}(R_0)_P/h_{i,P}J_P$ for $P \in U_i$ and the isomorphism ψ is given by mapping $h_{i,P}a + h_{i,P}J_P$ to $a + J_P$, we have $(\psi^{-1} \circ \phi_2)(g) = (h_{i,P}g + h_{i,P}J_P)_{P\in V_0}$. Finally, all of the above shows that the sufficient condition for $f_{|Z} = g_{|Z}$ is $f \in \mathcal{L}(X)$ such that its image in $\mathcal{L}_P$ is $h_{i,P}g$.[1]

Since X is integral, Theorem 4.3.22 provides that $\deg_k \mathcal{F} < -2g - \dim_k H^0(X, \mathcal{O}_X)$ implies $H^1(X, \mathcal{F}) = 0$. Thus for $\deg_k \mathcal{F} < -2g - \dim_k H^0(X, \mathcal{O}_X)$ we can apply the Approximation Theorem 5.7.1 5.7.1. By Proposition D.2.10, we have $\deg_k \mathcal{O}_X(D + (x^{r-1})_\infty) = \deg_k \mathcal{O}_X(D) + \mathcal{O}_X((x^{r-1})_\infty)$. Moreover, by Lemma D.2.13, we have $\deg_k(x^{r-1})_\infty = (r-1)n$ and thus Lemma C.4.8 provides $\mathcal{O}_X((x^{r-1})_\infty) = (1-r)n$ as well as $\deg_k \mathcal{O}_X(D) = -\deg_k D$. Note that both $\mathcal{O}_X(D + (x^{r-1})_\infty)$ and $\mathcal{J}$ are $\mathcal{O}_X$-ideals of which the former is invertible. Hence, by Lemma C.4.7, we deduce that

$$\begin{aligned} \deg_k \mathcal{F} = &\ \deg_k(\mathcal{O}_X(D + (x^{r-1})_\infty) \otimes_{\mathcal{O}_X} \mathcal{J}) \\ = &\ -\deg_k D + (1-r)n + \deg_k \mathcal{J} \\ < &\ -2g - \dim_k H^0(X, \mathcal{O}_X) \end{aligned}$$

[1] We want to note that the assumption $D \leq 0$ guarantees a common ambient structure R_0 of J and I such that we can argue with the diagram in (7:17) – this is the only place where we need this and thus there are may be other possible variants of this theorem.

if and only if

$$\begin{aligned} r &> \frac{-\deg_k D + \deg_k \mathcal{J} + 2g + \dim_k H^0(X, \mathcal{O}_X) + n}{n} \\ &= \frac{-\deg_k D + \deg_k \mathcal{J}}{n} + \underbrace{\frac{2g + \dim_k H^0(X, \mathcal{O}_X) + n}{n}}_{= c_X}. \end{aligned}$$

Hence for r as required in the assumption, the Approximation Theorem 5.7.1 Theorem 5.7.1 provides that for any given $(a_P)_{P \in X} \in \coprod_{P \in X} \mathcal{L}_P$ there is some $f \in \mathcal{L}(X) = \mathcal{O}_X(D + r(x)_\infty)(X)$ satisfying $f = a_P + b_P$ for some $b_P \in \mathcal{F}_P$. Note that this equation holds in F since all involved modules are submodules of F. Now we set

$$a_P = \begin{cases} x^r + \sum_{i=2}^n x^{r-1+|X|_i} \omega_i, & P \in S \\ h_{i,P} g, & P \notin S \text{ and } P \in U_i \end{cases}$$

and note that

$$x^r + \sum_{i=2}^n x^{r-1+|X|_i} \omega_i = x^r + \sum_{i=2}^n x^{r-1} \widetilde{\omega}_i = x^r \left(1 + \sum_{i=2}^n x^{-1} \widetilde{\omega}_i\right).$$

Hence $a_P = x^r \cdot \varepsilon$ where $\varepsilon \in \mathcal{O}_S^\times$ for all $P \in S$. Thus there is some $f \in \mathcal{L}(X)$ such that

$$f = \begin{cases} x^r \cdot \varepsilon + x^{r-1} \cdot c_P = x^r \cdot (\varepsilon + x^{-1} \cdot c_P), & P \in S \text{ where } c_P \in \mathcal{O}_{X,P} \\ g + j, & P \notin S \text{ where } j \in J. \end{cases}$$

Again, since these equations hold in F, we deduce that all c_P coincide in F. Thus $f = x^r(\varepsilon + x^{-1}c) = g + j$ with $c \in \bigcap_{P \in S} \mathcal{O}_{X,P} = \mathcal{O}_S$ and $j \in J$. To prove that f satisfies the third part of the assertion, note that $f \in \mathcal{O}_X(D + (x^r)_\infty)(X) = R_0 \cap x^r \mathcal{O}_S$. Note that by Corollary 4.3.24, we have $r > -(\deg_k D + \deg_k \mathcal{J})/n + c_X \geq -|X|_n + 1$ (since $-\deg_k D > 0$ because of $D \neq 0$) and thus we have

$$x^r \varepsilon = x^r \left(1 + \sum_{i=2}^n x^{-1} \widetilde{\omega}_i\right) = x^r + \sum_{i=2}^n x^{r-1+|X|_i} \omega_i \in R_0$$

since $\omega_1, \ldots, \omega_n$ was a reduced basis of $\mathcal{O}_X$, see Theorem 4.3.15 and Definition 4.3.17. Hence $x^r \varepsilon \in R_0 \cap x^r \mathcal{O}_S = \mathcal{O}_X((x^r)_\infty)(X)$. Thus we have $x^{r-1}c = f - x^r \varepsilon \in R_0 \cap x^r \mathcal{O}_S$ and since $c \in \mathcal{O}_S$, $x^{r-1}c \notin x^r \mathcal{O}_S$. That is $x^{r-1}c \in R_0 \cap x^{r-1}\mathcal{O}_S$ and, by Theorem 4.3.15, we have that

$$\{x^j \omega_i \mid 1 \leq i \leq n, 0 \leq j \leq r - 1 + |X|_i\}$$

is a k-basis of $\mathcal{O}_X((x^{r-1})_\infty)(X) = R_0 \cap x^{r-1}\mathcal{O}_S$. Therefore there are polynomials $\lambda_i \in k[x]$ of degree smaller than $r - 1 + |X|_i$ with $x^{r-1}c = \sum_{i=1}^n \lambda_i \omega_i$. Hence

$$\begin{aligned} f &= x^r + \sum_{i=2}^n x^{r-1+|X|_i}\ \omega_i + \sum_{i=1}^n \lambda_i\ \omega_i \\ &= (x^r + \lambda_1) + \sum_{i=2}^n (x^{r-1+|X|_i} + \lambda_i)\ \omega_i \end{aligned}$$

satisfies all asserted properties. From this we can immediately deduce the particular part of the assertion – which alternatively already followed by the equation $f = x^r(\varepsilon + x^{-1}c)$ with $\varepsilon \in \mathcal{O}_S^\times$. □

Applying Proposition 5.7.5 with the empty scheme Z provides the following.

Corollary 5.7.6. *Let X be an integral cover of $\mathbb{P}^1_k$. Let $D \in \operatorname{Div}(X)$, $D \leq 0$, be a divisor with support away from S and let $r = \lceil -\deg(D)/n + c_X \rceil$. Then there is $f \in F^\times$ such that*

(i) $f \in \mathcal{O}_X(D + r(x)_\infty)(X)$

(ii) $f = \sum_{i=1}^n \lambda_i \omega_i$ *where* $\lambda_i \in k[x]$, $\deg(\lambda_1) = r$ *is monic and* $\deg(\lambda_i) \leq r - 1 + |X|_i$ *for all* $i = 2, \dots, n$.

In particular, $f\mathcal{O}_S = x^r \mathcal{O}_S$. Note that by (ii), we have $f \in R_0$.

Corollary 5.7.7. *Let X be an integral cover of $\mathbb{P}^1_k$. Let $D \leq 0$ be a divisor on X with $\operatorname{Supp}(D) \subseteq V_0$ and set $I = \mathcal{O}_X(D)(V_0)$. Then the function f from Corollary 5.7.6 satisfies*

(i) $f \in I$, $fR_0 \in \mathcal{P}_\pi$, *and*

(ii) $\deg_k I \leq \deg_k fR_0 \leq \deg_k I + (c_X + 1)n$.

Proof. First we prove (i). By Corollary 5.7.6 (i), the function f satisfies

$$f \in \mathcal{L}_{\mathrm{reg}}(D + r(x)) = \mathcal{O}_X(D)(V_0) \cap x^r \mathcal{O}_S \cap \mathcal{K}_X(X)^\times$$

and thus $f \in I$ as asserted. The last part of (i) follows from Corollary 5.7.6. Now we prove (ii). Due to $fR_0 \subseteq I$, Lemma C.1.27 already provides $\deg_k fR_0 \geq \deg_k I$. By Proposition C.4.18 (ii), together with Proposition 3.1.27 (iv) and Corollary D.2.9, we know that

$$\deg_k fR_0 = \deg_k f\mathcal{O}_S = \deg_k x^r \mathcal{O}_S = rn \leq -\deg(D) + (c_X + 1)n$$

which together with $-\deg_k(D) = \deg_k I$, see Proposition C.4.18 (i), finally provides (ii). □

Remark 5.7.8. Note that the assumption that S does not meet the intersection points of the irreducible components, which is Definition 2.1.3 (ii), enables us to, at least to some extent, only work on the affine open V_0. Moreover, the assumption $Z \cap S = \emptyset$ also makes the considerations a bit easier. However, we are not convinced that these assumptions are necessary. △

From now on let X be a reduced cover of $\mathbb{P}^1_k$. Our aim is to use Proposition 5.7.5 successively to find functions on the irreducible components of X with prescribed behaviour given by an effective divisor on X. To do so, we need to introduce some (admittedly laborious) notation (which sometimes makes the whole idea look more difficult than it is) which makes it possible for us to effectively talk about functions on the union of (not all) irreducible components of X.

Definition 5.7.9. To shorten the notation, we set

$$\begin{aligned} g(X, \mathscr{S}_X) &:= 2p_a(X) + 2(m-1) - \chi(\mathscr{S}_X) \\ &= 2(g+m) - \chi(\mathscr{S}_X) \end{aligned}$$

and for $i = 2, \dots, m$

$$c_i = \begin{cases} \left\lceil \frac{2p_a(X_i)}{n_i} \right\rceil, & i = 1 \\ \left\lceil \frac{2p_a(X_i) + \chi(\mathscr{S}_i)}{n_i} \right\rceil, & i = 2, \dots, m. \end{cases}$$

△

Lemma 5.7.10. *We have* $\sum_{i=1}^{m} c_i n_i \leq g(X, \mathscr{S}_X) + n$.

Proof. In general, for $a, b \in \mathbb{Z}$ we have by division with remainder $a = bk + r$ with $r < b$. This yields

$$\left\lceil \frac{a}{b} \right\rceil = \left\lceil \frac{kb + r}{b} \right\rceil = \left\lceil k + \frac{r}{b} \right\rceil = \begin{cases} k, & r = 0 \\ k + 1, & r \neq 0. \end{cases}$$

Then for $r = 0$ we clearly have $\lceil a/b \rceil = a$ and otherwise

$$\left\lceil \frac{a}{b} \right\rceil \cdot b = kb + b = kb + r - r + b = a - r + b \leq a + b.$$

Applying this to $c_i n_i$ we obtain

$$c_i n_i \leq 2p_a(X_i) + \chi(\mathscr{S}_i) + n_i$$

and thus

$$\begin{aligned} \sum_{i=1}^{m} c_i n_i &\leq \sum_{i=1}^{m} (2p_a(X_i) + \chi(\mathscr{S}_i) + n_i) \\ &= 2\left(\sum_{i=1}^{m} p_a(X_i)\right) + \chi(\mathscr{S}_X) + n \\ \text{Lemma 2.4.3, Proposition 2.4.9} \rightsquigarrow \quad &= 2 \cdot (p_a(X) - \chi(\mathscr{S}_X) + m - 1) + \chi(\mathscr{S}_X) + n \\ &= 2p_a(X) + 2(m-1) - \chi(\mathscr{S}_X) + n \\ &= g(X, \mathscr{S}_X) + n. \end{aligned}$$

□

Theorem 5.7.11. *Let X be a reduced cover of $\mathbb{P}^1_k$. By $(X_1, \ldots, X_m)$ we fix an order of the irreducible components of X. We set*

$$r_i = \begin{cases} \lceil (2p_a(X_1) - \deg_k D_{|X_1})/n_1 \rceil, & i = 1 \\ \left\lceil (2p_a(X_i) - \deg_k D_{|X_i} + \chi(\mathscr{S}_i))/n_i \right\rceil, & i = 2, \ldots, m. \end{cases}$$

Then for any divisor $D \in \mathrm{Div}(X)$ with $D \leq 0$ and $\mathrm{Supp}(D) \subseteq V_0$ there is a regular $f \in R_0$, $f = (f_1, \ldots, f_m)$ with

(a) $f \in \mathcal{L}_{\mathrm{reg}}(D + \sum_{i \in A} r_i (x)_{i,\infty})$,

(b) $f_i \in \mathcal{O}_{X_i}(D_{|X_i} + r_i (x)_{X_i,\infty})(X_i)$,

(c) $f_i = \sum_{j=1}^{n_i} \lambda_{i,j}\, \omega_{i,j}$, $\deg(\lambda_{i,1}) = r_i$ *is monic,* $\deg(\lambda_{i,j}) \leq r_i - 1 + |X_i|_j$, *and*

(d) $\deg_k f R_0 \leq g(X, \mathscr{S}_X) - \deg_k D + n$.

In (d) the sheaf $\mathscr{S}_X$ is defined by the sequence (4:3) given in Definition 2.4.1.

Proof. We prove the assertion by induction on the number m of irreducible components X_i of X. The case $m = 1$ follows from Proposition 5.7.5 with $\mathcal{J} = \mathcal{O}_X$. Indeed, by Proposition 5.7.5, there is $f \in k(X)^\times$ such that $f \in \mathcal{O}_X(D + r(x)_\infty)(X)$ which thus results in $f \in \mathcal{L}_{\mathrm{reg}}(D + r(x)_\infty)$. Moreover, we have $r = \lceil (2p_a(X) - \deg_k D)/n \rceil$ and $f_{|S}\mathcal{O}_S = x^r \mathcal{O}_S$. Thus, by Proposition C.4.18 (i) and (ii), we have $\deg_k f_{|V_0} R_0 = -\deg_k f_{|S}\mathcal{O}_S = -\deg_k x^r \mathcal{O}_S$ and the latter is by Corollary D.2.9 equal to rn. By the proof of Lemma 5.7.10, we finally obtain

$$\deg_k f_{|V_0} R_0 = rn \leq 2p_a(X) - \deg_k D + n = g(X, \mathscr{S}_X) - \deg_k D + n$$

as asserted. Note that $m = 1$ and $\mathscr{S}_X = 0$ together imply $g(X, \mathscr{S}_X) = 2p_a(X)$.

We will now use the notations introduced in Section 2.4. Assume the assertion to be true for all reduced covers of $\mathbb{P}^1_k$ with $m-1$ irreducible components.

Let X be a reduced cover of $\mathbb{P}^1_k$ with irreducible components $X_1, \ldots, X_m$. For every $i = 1, \ldots, m$ we fix a reduced basis $\omega_{i,1}, \ldots, \omega_{i,n_i}$ of $R_{i,0}$. Let $D \in \mathrm{Div}(X)$ be a divisor on X with $D \leq 0$ and $\mathrm{Supp}(D) \subseteq V_0$. By definition, we have $X = Y_m$ and $Y_{m-1} = \cup_{i=1}^{m-1} X_i$ has $m-1$ irreducible components which can obviously be identified with $X_1, \ldots, X_{m-1}$. We immediately see that Y_{m-1} is also a reduced cover of $\mathbb{P}^1_k$. Set $D_{m-1} = D_{|Y_{m-1}}$ which satisfies $D_{m-1} \leq 0$ in $\mathrm{Div}(Y_{m-1})$ by Proposition 3.2.3 (ii). Since the restriction of divisors is transitive, see Proposition 3.2.9, we have $(D_{m-1})_{|X_i} = D_{|X_i}$. We set $W_0 = Y_{m-1} \cap V_0$. Hence, by induction hypothesis, there is $f_Y = (f_1, \ldots, f_{m-1}) \in \mathcal{K}_{Y_{m-1}}(Y_{m-1})^\times$ with $f_Y \in \mathcal{O}_{Y_{m-1}}(W_0)$ such that for all $i = 1, \ldots, m-1$ we have

(H1) $f_Y \in \mathcal{L}_{\mathrm{reg}}(Y_{m-1}, D_{m-1} + \sum_{i=1}^{m-1}(x^{r_i})_{Y_{m-1},\infty})$,

(H2) $f_i \in \mathcal{O}_{X_i}(D_{|X_i} + r_i(x)_{X_i,\infty})(X_i)$,

(H3) $f_i = \sum_{j=1}^{n_i} \lambda_{i,j}\, \omega_{i,j}$, $\deg(\lambda_{i,1}) = r_i$ is monic, $\deg(\lambda_{i,j}) \leq r_i - 1 + |X_i|_j$, and

(H4) $\deg_k f_Y \mathcal{O}_{Y_{m-1}}(V_0 \cap Y_{m-1}) \leq g(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) - \deg_k D_{m-1} + \sum_{i=1}^{m-1} n_i$.

Here $\mathscr{S}_{Y_{m-1}}$ is the sheaf defined by the exact sequence

$$0 \longrightarrow \mathcal{O}_{Y_{m-1}} \longrightarrow \bigoplus_{i=1}^{m-1} (\tau_i)_* \mathcal{O}_{X_i} \longrightarrow \mathscr{S}_{Y_{m-1}} \longrightarrow 0$$

in accordance with (4:3) in Definition 2.4.1. Hence, by Lemma 2.4.3, we have

$$\chi(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) = \sum_{i=1}^{m-1} \chi(Y_i, \mathscr{S}_i)$$

and thus, again by Lemma 2.4.3, this provides

$$\begin{aligned} \chi(X, \mathscr{S}_X) &= \sum_{i=1}^{m} \chi(Y_i, \mathscr{S}_i) \\ &= \sum_{i=1}^{m-1} \chi(Y_i, \mathscr{S}_i) + \chi(Y_m, \mathscr{S}_m) \\ &= \chi(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) + \chi(X, \mathscr{S}_m). \end{aligned} \tag{7:19}$$

Let $P_{1,0}, \ldots, P_{m,0}$ denote the minimal prime ideals of R_0. Set $M = \mathcal{O}_X(D)(V_0)$ and $I_{m-1} = \cap_{i=1}^{m-1} P_{i,0}$. Then we see that $\mathcal{O}_{Y_{m-1}}(W_0) = R_0/I_{m-1}$ as well as $\mathcal{O}_{X_m}(V_{m,0}) = R_0/P_{m,0}$. By Lemma 3.2.27 and Proposition B.4.8, we have

$$\mathcal{O}_{W_0}(D_{|W_0}) \cong \mathcal{O}_{V_0}(D_{|V_0})_{|W_0} \cong (M \otimes_{R_0} R_0/I_{m-1})^\sim \cong (M/I_{m-1}M)^\sim$$

as well as $\mathcal{O}_{V_{m,0}}(D_{|V_{m,0}}) \cong (M/P_{m,0}M)^\sim$. By Corollary B.4.47, we have an exact sequence of R_0-modules

$$0 \longrightarrow M \xrightarrow{\phi_m} M/I_{m-1}M \oplus M/P_{m,0}M \xrightarrow{\psi_m} M/(I_{m-1}M + P_{m,0}M) \longrightarrow 0 \tag{7:20}$$

where ϕ_m maps diagonal and ψ_m takes the difference of the representatives. Due to (H1), we have

$$f_Y \in \mathcal{O}_{W_0}(D_{|W_0})(W_0) \cap \oplus_{i=1}^{m-1} x^{r_i} \mathcal{O}_{S_i} = M/I_{m-1}M \cap \oplus_{i=1}^{m-1} x^{r_i} \mathcal{O}_{S_i}$$

where the intersection takes place in $\mathcal{K}_{Y_{m-1}}(Y_{m-1})$. Thus $f_Y = h + I_{m-1}M$ for some $h \in M$. Moreover, by (H3), together with Lemma 5.6.25, we have $f_i\mathcal{O}_{S_i} = x^{r_i}\mathcal{O}_{S_i}$ for all $i = 1, \dots, m-1$ and thus $f_Y(\oplus_{i=1}^{m-1}\mathcal{O}_{S_i}) = \oplus_{i=1}^{m-1}x^{r_i}\mathcal{O}_{S_i}$.

Let $\mathcal{J}_m \leq \mathcal{O}_{X_m}$ denote the sheaf of ideals that cuts out $Y_{m-1} \cap X_m$ as a closed subscheme of X_m. By construction, $\mathcal{J}_m(V_{m,0})$ equals the ideal in $R_0/P_{m,0}$ generated by I_{m-1}, that is $\mathcal{J}_m(V_{m,0}) = (I_{m-1} + P_{m,0})/P_{m,0}$. We apply Proposition 5.7.5 to

$$X = X_m, \quad D = D_{|X_m}, \quad \mathcal{J} = \mathcal{J}_m, \quad g = h + P_{m,0}$$

and obtain the existence of $f_m + P_{m,0} \in R_0/P_{m,0} \subseteq \mathcal{K}_{X_m}(X_m)^\times$ such that

(S1) $f_m + P_{m,0} \in \mathcal{L}_{\mathrm{reg}}(X_m, D_{|X_m} + (x^{r_m})_{X_m,\infty})$,

(S2) $f_m - h \in I_{m-1} + P_{m,0}$,

(S3) $f_m + P_{m,0} = \sum_{i=1}^{n} \lambda_{m,i}\omega_{m,i}$ where $\lambda_{m,i} \in k[x]$, $\deg(\lambda_{m,1}) = r_m$ is monic and $\deg(\lambda_{m,i}) \leq r_m - 1 + |X_m|_i$ for all $i = 2, \dots, n_m$.

where $r_m = \lceil (2p_a(X_m) - \deg_k D_{|X_m} - \deg_k \mathcal{J}_m)/n_m \rceil$. First of all, (S3) together with Lemma 5.6.25 provides $f_m\mathcal{O}_{S_m} = x^{r_m}\mathcal{O}_{S_m}$. Then (S1) tells us that $f_m + P_{m,0}M \in M/P_{m,0}M$ and (S2) says that $(h + I_{m-1}M, f_m + P_{m,0}M)$ lies in the kernel of ψ_m and thus, by the exactness of sequence (7:20), in the image of ϕ_m. Therefore, there is $f \in M$ such that $f + I_{m-1} = h + I_{m-1} = f_Y$ and $f + P_{m,0} = f_m + P_{m,0}$. Since the restriction f_i of f_Y to X_i for $i = 1, \dots, m-1$ is regular and f_m is regular, f is regular. As elements of $\mathrm{Frac}(R_0) = \bigoplus_{i=1}^{m} \mathrm{Frac}(R_{i,0})$ we have $f = (f_1, \dots, f_{m-1}, f_m)$. In particular, $f_{|S_i}\mathcal{O}_{S_i} = f_i\mathcal{O}_{S_i} = x^{r_i}\mathcal{O}_{S_i}$ for all $i = 1, \dots, m$.

Due to (H2) and (S1), f satisfies condition (b). By (H3) and (S3), f satisfies condition (c). By the above, we have $f \in M = \mathcal{O}_X(D)(V_0)$ regular with $f\mathcal{O}_S = \oplus_{i=1}^{m}x^{r_i}\mathcal{O}_{S_i}$. Thus $f \in \mathcal{O}_X(D)(V_0) \cap \oplus_{i=1}^{m}x^{r_i}\mathcal{O}_{S_i} = \mathcal{L}_{\mathrm{reg}}(D + \sum_{i\in A} r_i(x)_{i,\infty})$. Hence f satisfies property (a). Therefore, we are left to prove that f also satisfies property (d). By (H4), we have

$$\deg_k(h + I_{m-1})(R/I_{m-1}) \leq g(Y_{m-1}, \mathscr{S}_{m-1}) - \deg_k D_{m-1} + \sum_{i=1}^{m-1} n_i \tag{7:21}$$

and due to $f_m\mathcal{O}_{S_m} = x^{r_m}\mathcal{O}_{S_m}$, together with Proposition 3.1.27 (iv), Proposition C.4.18 (ii) and Corollary D.2.9, we have

$$\begin{aligned} \deg_k(f_m + P_{m,0})(R_0/P_{m,0}) &= -\deg_k f_m\mathcal{O}_{S_m} \\ &= -\deg_k x^{r_m}\mathcal{O}_{S_m} \\ &= r_m n_m \\ &\leq 2p_a(X_m) - \deg_k D_{|X_m} - \deg_k(I_{m-1} + P_{m,0}) + n_m. \end{aligned} \tag{7:22}$$

For the last inequality we have used Corollary D.2.12. By Lemma C.1.28, we have

$$\begin{aligned}\deg_k fR_0 &= \sum_{i=1}^{m} \deg_k f_{|X_i} R_{i,0} \\ &= \sum_{i=1}^{m-1} \deg_k f_i R_{i,0} + \deg_k f_m R_{m,0} \\ &= \deg_k(h - I_{m-1})(R_0/I_{m-1}) + \deg_k(f_m + P_{m,0})R_0/P_{m,0} \\ &\leq (g(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) - \deg_k D_{m-1} + \sum_{i=1}^{m-1} n_i) \\ &\quad + (2p_a(X_m) - \deg_k D_{|X_m} - \deg_k(I_{m-1} + P_{m,0}) + n_m).\end{aligned} \tag{7:23}$$

By definition and Eq. (7:19), we have

$$\begin{aligned}g(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) &= 2p_a(Y_{m-1}) + 2(m-2) - \chi(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) \\ &= 2p_a(Y_{m-1}) + 2(m-2) - \chi(X, \mathscr{S}_X) + \chi(X, \mathscr{S}_m).\end{aligned} \tag{7:24}$$

Note that by Lemma 2.4.5, we have

$$\chi(X, \mathscr{S}_m) = \chi(Y_m, \mathscr{S}_m) = \dim_k \frac{R_0/P_{m,0}}{I_{m-1} + P_{m,0}} = \deg_k I_{m-1} + P_{m,0} = \deg_k \mathscr{J}_m. \tag{7:25}$$

Now plugging Eq. (7:25) into Eq. (7:24) and then the result into Eq. (7:23) provides

$$\begin{aligned}\deg_k fR_0 \leq\ & 2p_a(Y_{m-1}) + 2(m-2) - \chi(X, \mathscr{S}_X) - \deg_k D_{m-1} + \sum_{i=1}^{m} n_i \\ & + 2p_a(X_m) - \deg_k D_{|X_m}.\end{aligned} \tag{7:26}$$

By Proposition C.4.18 (iii), we have $\deg_k D_{m-1} = \sum_{i=1}^{m-1} \deg_k D_{|X_i}$ and by Proposition 2.4.9, we have

$$\begin{aligned}p_a(Y_{m-1}) &= \sum_{i=1}^{m-1} p_a(X_i) + \chi(Y_{m-1}, \mathscr{S}_{Y_{m-1}}) + 1 - (m-1) \\ \text{Eq. (7:25)} \rightsquigarrow\ &= \sum_{i=1}^{m-1} p_a(X_i) + \chi(X, \mathscr{S}_X) - \chi(X, \mathscr{S}_m) - m + 2 \\ &\leq \sum_{i=1}^{m-1} p_a(X_i) + \chi(X, \mathscr{S}_X) - m + 2.\end{aligned} \tag{7:27}$$

Now plugging $\deg_k D_{m-1} = \sum_{i=1}^{m-1} \deg_k D_{|X_i}$ and Eq. (7:27) into Eq. (7:26) finally provides

$$\begin{aligned}\deg_k fR_0 &\leq 2(\sum_{i=1}^{m-1} p_a(X_i) + \chi(X, \mathscr{S}_X) - m + 2) \\ &\quad + 2(m-2) - \chi(X, \mathscr{S}_X) - \deg_k D + n + 2p_a(X_m) \\ &= 2(\sum_{i=1}^{m} p_a(X_i) + \chi(X, \mathscr{S}_X) + 1 - m) \\ &\quad + 2 + 2(m-2) - \chi(X, \mathscr{S}_X) - \deg_k D + n \\ \text{Proposition 2.4.9} \rightsquigarrow\ &= 2p_a(X) + 2(m-1) - \chi(X, \mathscr{S}_X) - \deg_k D + n \\ \text{Definition 5.7.9} \rightsquigarrow\ &= g(X, \mathscr{S}_X) - \deg_k D + n.\end{aligned}$$

□

Remark 5.7.12. Note that the proof of Theorem 5.7.11 shows that the statement is not only true for the chosen r_i but also for all $s_i \geq r_i$. △

Remark 5.7.13. Note that Theorem 5.7.11 requires a divisor defined on all of X whose support is contained V_0 or equivalently which is not supported in S. But by Lemma 5.3.13, we see that we may extend any divisor D_0 on V_0 uniquely to a divisor D on X which restricts to D_0 on V_0 and which is not supported in S. This establishes a 1-to-1 correspondence between divisors on X not supported in S and $\mathrm{Div}(V_0)$. Hence we will use Theorem 5.7.11 for both such divisors. Put in the notation introduced in Notation 5.5.7, we use Theorem 5.7.11 for divisors D of the form $(D_0, 0)$ with $D_0 \leq 0$. △

Corollary 5.7.14. *Let the situation be as in Theorem 5.7.11. Then f satisfies* $\mathrm{div}_X(f) = (\mathrm{div}_{V_0}(f_{|V_0}), \sum_{i\in A} -r_i(x)_{i,\infty})$. *In particular, $fR_0 \in \mathcal{P}_\pi$.*

Proof. By Theorem 5.7.11 (c), together with Lemma 5.6.25, we have $f_{|X_i}\mathcal{O}_{S_i} = x^{r_i}\mathcal{O}_{S_i}$ for all $i \in A$. Hence, by Corollary 5.6.13, we deduce

$$-\mathrm{div}_X(f)_{|S} = \mathrm{div}_X(f^{-1})_{|S} = (\sum\nolimits_{i\in A} r_i(x)_{i,\infty})_{|S}$$

which is equivalent to $\mathrm{div}_X(f)_{|S} = (\sum_{i\in A} -r_i(x)_{i,\infty})_{|S}$ and hence provides the assertion. The particular part follows from Definition 5.6.19. □

The function constructed in Theorem 5.7.11 does indeed provide a modification function of D.

Lemma 5.7.15. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $D \leq 0$ be a divisor on X with $\mathrm{Supp}(D) \subseteq V_0$ and set $I = \mathcal{O}_X(D)(V_0)$. Then the function f from Theorem 5.7.11 satisfies*

(i) $f \in I$, $fR_0 \in \mathcal{P}_\pi$, and

(ii) $\deg_k I \leq \deg_k fR_0 \leq \deg_k I + 2g + 2m + n - \chi(\mathscr{S}_X)$.

Proof. First we prove (i). By Theorem 5.7.11 (a), the function f satisfies

$$f \in \mathcal{L}_{\mathrm{reg}}(D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty}) = \mathcal{O}_X(D)(V_0) \cap (\oplus_{i\in A} x^{r_i}\mathcal{O}_{S_i}) \cap \mathcal{K}_X(X)^\times$$

and thus $f \in I$ as asserted. The last part of (i) follows from Corollary 5.7.14. Now we prove (ii). From $fR_0 \subseteq I$ Lemma C.1.27 already provides $\deg_k fR_0 \geq \deg_k I$. By Theorem 5.7.11 (d), we already know that

$$\deg_k fR_0 \leq g(X, \mathscr{S}_X) - \deg_k D + n.$$

Note that by Definitions 2.4.8 and 5.7.9, we have

$$\begin{aligned} g(X, \mathscr{S}_X) &= 2p_a(X) + 2(m-1) - \chi(\mathscr{S}_X) \\ &= 2(1+g) + 2(m-1) - \chi(\mathscr{S}_X) \\ &= 2g + 2m - \chi(\mathscr{S}_X). \end{aligned}$$

Moreover, by Proposition C.4.18 (i), we have $-\deg_k(D) = \deg_k \mathcal{O}_X(D)(V_0) = \deg_k I$ and thus combining the above provides the assertion. □

Corollary 5.7.16. *Let X be a reduced cover of $\mathbb{P}^1_k$. Let $D + r(x)_\infty \in \mathrm{Div}^0_\pi(X)$ with $D \leq 0$ and $I = \mathcal{O}_X(D)(V_0)$. Then the modification function f from Theorem 5.7.11 satisfies $f \in I$ and*

$$\deg_k I \leq \deg_k fR_0 \leq \deg_k I + 2g + 2m + n - \chi(\mathscr{S}_X).$$

Corollary 5.7.17. *Since* $f \in \mathcal{L}_{\text{reg}}(D + \sum_{i\in A} r_i(x)_{i,\infty})$*, we have*

$$\operatorname{div}(f) + D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty} \geq 0.$$

Moreover, by Corollary 5.7.14, we have $\operatorname{div}_S(f) = \sum_{i\in A} -r_i(x)_{i,\infty}$*. Hence*

$$\operatorname{div}_{V_0}(f) + D_{|V_0} \geq 0.$$

5.7.2 Computing Modification Functions

As already mentioned in the introduction to Section 5.7, in this section we provide algorithms to explicitly compute modification functions given a basis matrix of the R_0-ideal $\mathcal{O}_X(D)(V_0)$. Furthermore, these algorithms also provide existential statements of modification functions in general. We divide this endeavor into two cases, first we examine how to compute modification functions in the component independent case and then do the same in the component dependent case. We chose this order since, as we will see, the idea used in the component independent case can be extended to the component dependent one.

5.7.2.1 Component Independent Case

We start with some fundamental observations with regards to the leading coefficients matrix $\operatorname{LC}(M)$ of a matrix $M \in k[x]^{m\times n}$. The following shows why we do care about this. Let $f = \sum_{i=1}^{n} \lambda_i \omega_i \in R_0$ with $\lambda_i \in k[x]$. Then $\phi_\Omega(f) = (\lambda_1, \dots, \lambda_n)^T$ and we set $x^{-|X|}\phi_\Omega(f) := (x^{-|X|_1}\lambda_1, \dots, x^{-|X|_n}\lambda_n)^T$. Then f satisfies the sufficient conditions in Lemma 5.6.25 to be a modification function if and only if

$$\operatorname{LC}(\phi_\Omega(x^{-|X|}\phi_\Omega(f))) = (\mu, 0, \dots, 0)^T$$

for any $\mu \in k^\times$. This will help us to find a suitable linear combination of a given basis matrix which results in a modification function.

Remark 5.7.18. Let $\lambda = (\lambda_1, \dots, \lambda_n) \in k[x]^{1\times n}$ be a row vector. Let $d = \max_{i=1}^{n}\{\deg \lambda_i\}$ be its degree. Obviously, no unimodular column operation over $k[x]$ on λ can decrease the degree of λ below zero. In particular, no unimodular column operation over $k[x]$ on $f \cdot \lambda = (f \cdot \lambda_1, \dots, f \cdot \lambda_n)$ can decrease its degree below $\deg f - d$. Moreover, applying unimodular column operations over $k[x]$ on $f \cdot \lambda = (f \cdot \lambda_1, \dots, f \cdot \lambda_n)$ yields a row vector such that every non-zero entry is still a multiple of f. △

The following lemma is particularly useful for finding linear combinations of columns of a reduced matrix with prescribed LC-vector.

Lemma 5.7.19. *Let* $M \in k[x]^{m\times n}$ *be a reduced matrix with columns* $v_1, \dots, v_n \in k[x]^m$ *of degrees* $d_1, \dots, d_n$*, respectively. Let* $\mu = (\mu_1, \dots, \mu_n)^T \in k^n$ *be arbitrary and set* $d = \max\{d_i \mid \mu_i \neq 0\}$*. Then we have*

$$\operatorname{LC}(M) \cdot \mu = \operatorname{LC}\left(M \cdot \begin{pmatrix} \mu_1 x^{d-d_1} \\ \vdots \\ \mu_n x^{d-d_n} \end{pmatrix} \right).$$

Proof. Let $v_j = (v_{1,j}, \dots, v_{n,j})^T$, that is $M = (v_{i,j})_{i,j}$. We set $\operatorname{LC}(M) \cdot \mu = (\lambda_1, \dots, \lambda_n)^n$. Then

$$\lambda_i = \sum_{j=1}^{n} a_{i,j} \cdot \mu_j \quad \text{with} \quad a_{i,j} = \begin{cases} \ell c(v_{i,j}), & \deg(v_{i,j}) = \deg(v_j) = d_j \\ 0, & \text{otherwise.} \end{cases}$$

By definition, we have

$$N := M \cdot \begin{pmatrix} \mu_1 x^{d-d_1} \\ \vdots \\ \mu_n x^{d-d_n} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} \mu_j x^{d-d_j} v_{1,j} \\ \vdots \\ \sum_{j=1}^{n} \mu_j x^{d-d_j} v_{m,j} \end{pmatrix}.$$

Since M is reduced, we have

$$\max_{i=1}^{m}\{\deg(\sum\nolimits_{j=1}^{n} \mu_j x^{d-d_j} v_{i,j})\} = \deg(N) = \max_{i=1}^{n}\{\deg(\mu_j x^{d-d_j} \cdot v_j)\} = d.$$

Therefore, the non-zero entries of $\mathrm{LC}(N)$ do only depend on the coefficients of entries of N of degree d. The coefficient of x^d in $\sum_{j=1}^{n} \mu_j x^{d-d_j} v_{i,j}$ equals

$$\sum_{j:\deg(v_{i,j})=d_j} \ell c(v_{i,j}) \cdot \mu_j = \lambda_i$$

which thus proves the assertion. □

We can use Lemma 5.7.19 to give an algorithm that computes a modification function of an ideal given by its $k[x]$-basis matrix. Note that the suffix "CF" stands for *components free* and represents the component independent case.

Algorithm 7 Computing a modification function in the component independent case

Precomputed	Reduced basis Ω of R_0; π-invariants $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ of X
Input	T basis matrix of $\mathcal{F}(V_0)$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal
Output	$\phi_\Omega(f)$ where f is a modification function of $\mathcal{F}(V_0)$

1: **procedure** ModFctCF(T)
2: $T \leftarrow$ ScaleRows($T, x^{-\lvert X\rvert_1}, \ldots, x^{-\lvert X\rvert_n}$)
3: $N \leftarrow$ RedMat(T)
4: $L \leftarrow$ LeadCoeffMat(N)
5: $(\mu_1, \ldots, \mu_n) \leftarrow$ SolveLES$_k(L, (1, 0, \ldots, 0)^T)$
6: $I = \{i \mid \mu_i \neq 0\}$
7: $d_1, \ldots, d_n \leftarrow 0, \ldots, 0$
8: **for** $i \in I$ **do**
9: $d_i \leftarrow$ Degree(SubMatrix($N, (1, i), (n, i)$))
10: $D \leftarrow \max\{d_i \mid i \in I\}$
11: **for** $i = 1, \ldots, n$ **do**
12: $\mu'_i \leftarrow \mu_i x^{D-d_i}$
13: $f \leftarrow N \cdot (\mu'_1, \ldots, \mu'_n)^T$
14: $f \leftarrow$ ScaleRows($T, x^{\lvert X\rvert_1}, \ldots, x^{\lvert X\rvert_n}$)
15: **return** f

Theorem 5.7.20. *The algorithm* ModFctCF*, see Algorithm 7, is correct. Moreover, if d is a common bound of $\deg(T)$ and $-\lvert X\rvert_n$, then* ModFctCF *requires at most $O^{\sim}(n^\omega d)$ operations in k and returns a vector with degree bounded by $d - \lvert X\rvert_n \leq d + c_X$.*

Proof. We work with the notation as in Algorithm 7. Since RedMat does not increase the degree of the input matrix and computes a right equivalent of it, Remark 5.7.18 provides that every non-zero entry of the i-th row of N has at least degree $-\lvert X\rvert_i$. Moreover, $\deg N \leq \deg T - \lvert X\rvert_n$. Since N is reduced, there is a vector $\mu \in k^n$ such that $L \cdot \mu = (1, 0, \ldots, 0)^T$. By Lemma 5.7.19, we know that f from line 13 satisfies $\mathrm{LC}(f) = (1, 0, \ldots, 0)^T$. We have

seen above that every non-zero entry of the i-th row of N has at least degree $-|X|_i$ and thus the same is true for the i-th row of f. Moreover, by construction, the latter has degree $D \leq \deg N \leq \deg T - |X|_n \leq d - |X|_n$. Therefore, the output vector $f = (f_1, \ldots, f_n)^T$ satisfies $\deg f_i < \deg f_1 + |X|_i$ for all non-zero f_i and $\deg f = \deg f_1 \leq d - |X|_n$. This proves the correctness of Algorithm 7.

Now we prove the running time assertion. Let d be a common bound of $\deg(T)$ and $\max_{i=1}^{m}\{-|X_i|_{n_i}\}$. Hence, calling RedMat requires at most $O^{\sim}(n^{\omega}d)$ operations in k, see Theorem A.2.7. Therefore, any scaling of the rows of T by the appearing powers of x only produce matrices and vectors with degree bounded by $2d$. Hence the running time assertion follows from Lemma A.1.2 (i), (iv), (v) and (vi). □

Lemma 5.7.21. *The element $f \in \mathcal{K}_X(X)$ computed by* ModFctCF *satisfies $f \in \mathcal{F}(V_0) \cap x^e\mathcal{O}_S \cap \mathcal{K}_X(X)^{\times}$ where $e = \deg \phi_\Omega(f)$. In particular, $-\mathrm{div}_S(f) = e(x)_\infty$. If $\mathcal{F} = \mathcal{O}_X(D)$ for some $\mathrm{Supp}(D) \subseteq V_0$, then $f \in \mathcal{L}_{\mathrm{reg}}(D + e(x)_\infty)$.*

Proof. By construction, we have $f \in \mathcal{F}(V_0)$. Moreover, it is constructed such that $\mathrm{LC}(\phi_\Omega(f)) = (1, 0, \ldots, 0)^T$ and thus Lemma 5.6.25 provides $f\mathcal{O}_S = x^e\mathcal{O}_S$. The particular part follows from Corollary 5.6.13 and the fact that $f \neq 0$. □

5.7.2.2 Component Dependent Case

We want to generalise the procedure used in Algorithm 7 to compute modification functions in the component dependent case. To do so, we state a lemma that will help us prove the correctness of Algorithm 8.

Lemma 5.7.22. *Let $M \in k[x]^{n\times n}$ be in n-block-form with $\det(M) \neq 0$ and m row blocks $M_i \in k[x]^{n_i \times n}$ of degree d_i. Let $d = \max_{i=1}^{m}\{d_i\}$. Let N be the matrix we obtain by scaling the row blocks M_i in M by x^{d-d_i}. By N_1 we denote a reduction of N with columns $v'_1, \ldots, v'_n \in k[x]^n$. Let $\mu = (\mu_1, \ldots, \mu_n)^T \in k^n$ be a vector over k such that*

$$\mathrm{LC}(N_1) \cdot \mu = (1, 0, \ldots, 0 \mid \ldots \mid 1, 0, \ldots 0)^T.$$

Set $d' = \max\{\deg(\mu_j v'_j) \mid j \in \{1, \ldots, n\}\}$. Let N_2 be the matrix we obtain by scaling the i-th row block of N_1 by $x^{d_i - d}$. Then the vector

$$f := \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} := N_2 \cdot \begin{pmatrix} \mu_1 x^{d' - \deg(v'_1)} \\ \vdots \\ \mu_n x^{d' - \deg(v'_n)} \end{pmatrix}$$

satisfies $\mathrm{LC}(f_i) = (1, 0, \ldots, 0)^T$ and $\deg f_i \leq d_i$ for all $i = 1, \ldots, m$. Moreover, by construction, f lies in the column space of M.

Proof. By construction, the row blocks of N all have degree d. That is, $\deg N \leq d$. Therefore, $N_1 := (v'_1 \ldots v'_n) := \mathrm{RedMat}(N)$ has degree bounded by d as well. In particular, the degree of the row blocks $N_{1,i}$ of N_1 also have degree bounded by d. Since N_1 is reduced, $\mathrm{LC}(N_1)$ has full rank over k and thus there is a vector $\mu = (\mu_1, \ldots, \mu_n)^T \in k^n$ over k such that

$$\mathrm{LC}(N_1) \cdot \mu = (1, 0, \ldots, 0 \mid \ldots \mid 1, 0, \ldots 0)^T. \tag{7:28}$$

We set $v = N_1 \cdot (\mu_1 x^{d' - \deg(v'_1)}, \ldots, \mu_n x^{d' - \deg(v'_n)})^T$. By Lemma 5.7.19, we obtain

$$\mathrm{LC}(N_1) \cdot \mu = \mathrm{LC}(v).$$

By construction, $\deg(v) \leq d' \leq d$. Let N_2 be the matrix and f be the column vector we obtain by scaling the i-th row block of N_1 respectively of f by $x^{d_i - d}$. Then

$$f := \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} := N_2 \cdot \begin{pmatrix} \mu_1 x^{d' - \deg(v'_1)} \\ \vdots \\ \mu_n x^{d' - \deg(v'_n)} \end{pmatrix}$$

and the i-th row block f_i of f has degree bounded by $d' - d + d_i \leq d_i$. By Eq. (7:28), we know that the first entry of the i-th row block of v has strictly larger degree than the other entries of the i-th row block of v. Since f_i emerges by scaling the i-th row block of v, the same is true for f_i. Finally, that f lies in the column space of M follows from the fact that N_2 emerges from M by scaling columns from the left and reverse the very same scaling after applying some unimodular column operations. □

Algorithm 8 Computing a modification function in the component dependent case

Precomputed	Basis Ω_i^m of R_0^+; for all $i = 1, \ldots, m$: π-invariants $-\lvert X_i\rvert_1 \leq \ldots \leq -\lvert X\rvert_{n_i}$ of X_i
Input	M basis matrix of $\mathcal{O}_X$-ideal $\mathcal{F}$ with respect to Ω_i^m,
Output	$\phi_{\Omega_i^m}(f) = (\phi_{\Omega_1}(f_1), \ldots, \phi_{\Omega_m}(f_m))$ where f_i is a modification function of $\mathcal{F}_i(V_{i,0})$

1: **procedure** ModFctC(M)
2: **for** $i = 1, \ldots, m$ **do**
3: **for** $j = 1, \ldots, n_i$ **do**
4: $M \leftarrow \text{MultiplyRow}(M, j + \sum_{\ell=1}^{i-1} n_\ell, x^{-\lvert X_i\rvert_j})$
5: **for** $i = 1, \ldots, m$ **do**
6: $p_i \leftarrow 1 + \sum_{j=1}^{i-1} n_j$
7: $d_i \leftarrow \text{Degree}(\text{SubMatrix}(M, (p_i, 1), (p_i + n_i - 1, n)))$
8: $d \leftarrow \max\{d_1, \ldots, d_m\}$
9: **for** $i = 1, \ldots, m$ **do**
10: **for** $j = 1, \ldots, n_i$ **do**
11: $M \leftarrow \text{MultiplyRow}(M, j + \sum_{\ell=1}^{i-1} n_\ell, x^{d-d_i})$
12: $N_1 \leftarrow \text{RedMat}(M)$
13: $L \leftarrow \text{LeadCoeffMat}(N_1)$
14: **for** $i = 1, \ldots, m$ **do**
15: $e_{1,i} \leftarrow (1, 0, \ldots, 0) \in k^{n_i}$
16: $e \leftarrow \text{ColumnConcat}(e_{1,1}, \ldots, e_{1,m})$
17: $\mu = (\mu_1, \ldots, \mu_n) \leftarrow \text{SolveLES}_k(L, e)$
18: $d'_1, \ldots, d'_n \leftarrow 0, \ldots, 0$
19: **for** $i = 1, \ldots, n$ **do**
20: $d'_i \leftarrow \text{Degree}(\text{SubMatrix}(N_1, (1, i), (n, i)))$
21: $d' \leftarrow \max\{d'_i \mid i \in \{i \mid \mu_i \neq 0\}\}$
22: **for** $i = 1, \ldots, n$ **do**
23: $\mu'_i \leftarrow \mu_i \cdot x^{d'-d'_i}$
24: $\mu' \leftarrow (\mu'_1, \ldots, \mu'_n)^T$
25: $f' \leftarrow N_1 \cdot \mu'$
26: $f \leftarrow f'$
27: **for** $i = 1, \ldots, m$ **do**
28: **for** $j = 1, \ldots, n_i$ **do**
29: $f \leftarrow \text{MultiplyRow}(f, j + \sum_{\ell=1}^{i-1} n_\ell, x^{d_i-d+\lvert X_i\rvert_j})$
30: **return** f

Theorem 5.7.23. *The algorithm* ModFctC*, see Algorithm 8, is correct. Moreover, if d is a common bound of $\deg(M)$ and $\max_{i=1}^m\{-\lvert X_i\rvert_{n_i}\}$, then* ModFctC *requires at most $O^\sim(n^\omega d)$ operations in k and returns a vector*

$$\phi_{\Omega_i^m}(f) = (\phi_{\Omega_1}(f_1), \ldots, \phi_{\Omega_m}(f_m))^T$$

with $\deg \phi_{\Omega_i}(f_i) \leq a_i - \lvert X_i\rvert_{n_i} \leq a_i + c_{X_i}$ where a_i is a degree bound of the i-th row block of M. Moreover, $\phi_{\Omega_i}(f_i) = (f_{i,1}, \ldots, f_{i,n_i})^T$ with $f_{i,j} \in k[x]$ such that $\deg f_{i,j} < \deg f_{i,1} + \lvert X_i\rvert_j$ for all $i = 1, \ldots, m$ and $j = 2, \ldots, n_i$.

Proof. We work with the notation as in Algorithm 8. To prove the correctness, we can simply use Lemma 5.7.22: Let d_i denote the degree of the i-th row block of M after line 5. Hence $d_i \leq a_i - \lvert X_i\rvert_{n_i}$. By definition, $d = \max_{i=1}^m\{d_i\}$. By Lemma 5.7.22, we know that

$f' := (f'_1, \dots, f'_m)^T := N_1 \cdot \mu'$ satisfies $\deg f'_i \leq d' \leq d$ and $\mathrm{LC}(f'_i) = (1, 0, \dots, 0)^T \in k^{n_i}$.

Let $f'_i = (f'_{i,1}, \dots, f'_{i,n_i})^T$ for all $i = 1, \dots, m$. If we write $f := (f_1, \dots, f_m)$ for f, then

$$f_i := (f_{i,1}, f_{i,2} \dots, f_{i,n_i})^T = (x^{d_i - d} f'_{i,1}, x^{d_i - d + |X_i|_2} f'_{i,2}, \dots, x^{d_i - d + |X_i|_{n_i}} f'_{i,n_i})^T$$

and since $\deg f'_{i,j} < \deg f'_{i,1}$ for all $i = 1, \dots, n$ and $j = 2, \dots, n_i$, we deduce

$$\begin{aligned} \deg f_{i,j} &= \deg f'_{i,j} + |X_i|_j + d_i - d \\ &< \deg f'_{i,1} + |X_i|_j + d_i - d \\ &= \deg f_{i,1} - (d_i - d) + |X_i|_j + d_i - d \\ &= \deg f_{i,1} + |X_i|_j \end{aligned}$$

for all $i = 1, \dots, n$ and $j = 2, \dots, n_i$. Moreover, since $\deg f'_i \leq d$, we obtain

$$\begin{aligned} \deg f_i &= \max_{j=1}^{n_i} \{\deg f_{i,j}\} \\ &= \max_{j=1}^{n_i} \{\deg f'_{i,j} + |X_i|_j + d_i - d\} \\ &= \max_{j=1}^{n_i} \{\deg f'_{i,j} + |X_i|_j\} + d_i - d \\ &\leq \deg f'_i + d_i - d \\ &\leq d + d_i - d \\ &= d_i \\ &\leq a_i - |X_i|_{n_i} \end{aligned}$$

for all $i = 1, \dots, m$. This shows the correctness of ModFctC.

Now we prove the running time assertion. Let d be a common bound of $\deg(M)$ and $\max_{i=1}^m \{-|X_i|_{n_i}\}$. Therefore, any scaling of the rows of M by the appearing powers of x only produce matrices and vectors with degree bounded by $2d$. Hence the running time assertion follows from Theorem A.2.7, Theorem A.2.12 and Lemma A.1.2 (i), (iv), (v), (vi), (viii). □

Example 5.7.24. We give an example that shows that the rescaling of f' with the powers $x^{|X_i|_j}$ does not necessarily decrease the degree of the i-th row block of f' to the degree a_i: Let M be given by

$$M = \left(\begin{array}{ccc} x & x & 0 \\ \hline 1 & 0 & x \\ x^2 & x^3 & x^5 \end{array}\right)$$

and let $-|X_i|_j$ be given by $-|X_1|_1 = -|X_2|_1 = 0$, see Corollary 4.3.24, and $-|X_2|_2 = 10$. First, we scale the third row of M by x^{10} which results in

$$\left(\begin{array}{ccc} x & x & 0 \\ \hline 1 & 0 & x \\ x^{12} & x^{13} & x^{15} \end{array}\right).$$

The maximal appearing row block degree is now 15 and thus we scale the first row block with x^{14} which results in

$$\left(\begin{array}{ccc} x^{15} & x^{15} & 0 \\ \hline 1 & 0 & x \\ x^{12} & x^{13} & x^{15} \end{array}\right).$$

We subtract the first column from the second and then we subtract the now second column multiplied with x^2 from the third which results in

$$\left(\begin{array}{ccc} x^{15} & 0 & 0 \\ \hline 1 & -1 & -x^2+x \\ x^{12} & x^{13}-x^{12} & 0 \end{array}\right) \quad \text{having leading coefficient matrix} \quad L := \left(\begin{array}{ccc} 1 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & 0 \end{array}\right)$$

and therefore it is reduced. The matrix L satisfies $L \cdot (1,0,-1)^T = (1,1,0)^T$ and thus we set

$$f' := \begin{pmatrix} f_1 \\ \hline f_2 \\ f_3 \end{pmatrix} := \begin{pmatrix} x^{15} \\ \hline 1 \\ x^{12} \end{pmatrix} - x^{13} \cdot \begin{pmatrix} 0 \\ \hline -x^2+x \\ 0 \end{pmatrix} = \begin{pmatrix} x^{15} \\ \hline x^{15}-x^{14}+1 \\ x^{12} \end{pmatrix}.$$

We rescale the first row block by x^{-14} and obtain

$$\begin{pmatrix} x \\ \hline x^{15}-x^{14}+1 \\ x^{12} \end{pmatrix}.$$

Now rescaling with the respective powers of x with respect to $-|X_i|_j$ in this case comes down to multiply the third row with x^{-10} which finally results in

$$f := \begin{pmatrix} x \\ \hline x^{15}-x^{14}+1 \\ x^2 \end{pmatrix}.$$

The row block degrees of M were 1 respectively 5. We see that f has row block degrees 1 and 15 where $15 = 10+5 = -|X_2|_2 + 5$. This shows that rescaling with $x^{|X_i|_j}$ need not necessarily decrease the row block degrees of f'. △

Lemma 5.7.25. *The element $f \in \mathcal{K}_X(X)$ computed by* ModFctC *satisfies*

(i) $f \in \mathcal{F}(V_0) \cap \bigoplus_{i=1}^m x^{e_i}\mathcal{O}_{S_i} \cap \mathcal{K}_X(X)^\times$ *where* $e_i = \deg \phi_{\Omega_i}(f_{|X_i})$ *and*

(ii) $f_{|X_i}\mathcal{O}_{S_i} = x^{e_i}\mathcal{O}_{S_i}$ *for all* $i = 1, \dots, m$.

In particular, $-\mathrm{div}_S(f) = \sum_{i\in A} e_i(x)_{i,\infty}$. *If* $\mathcal{F} = \mathcal{O}_X(D)$ *for* $\mathrm{Supp}(D) \subseteq V_0$, *then* $f \in \mathcal{L}_{\mathrm{reg}}(D + \sum_{i\in A} e_i(x)_{i,\infty})$.

Proof. By construction, we have $f \in \mathcal{F}(V_0)$. Moreover, it is constructed such that $\mathrm{LC}(\phi_{\Omega_i}(f_{|X_i})) = (1,0,\dots,0)^T$ and thus Lemma 5.6.25 provides $f_{|X_i}\mathcal{O}_{S_i} = x^{e_i}\mathcal{O}_{S_i}$. This shows both Items (i) and (ii). The particular part follows from Corollary 5.6.13 and the fact that $f_{|X_i} \neq 0$ for all $i = 1, \dots, m$. □

Remark 5.7.26. Let ModFct denote the algorithm that, given a matrix $M \in k[x]^n$ and a Boolean c, calls ModFctC(M) if $c = \mathit{true}$ and ModFctCF(M) if $c = \mathit{false}$ and then returns the result. By Theorems 5.7.20 and 5.7.23, we see that ModFct requires at most $O^\sim(n^\omega d)$ operations in k if d is a common bound of $\deg(M)$ and $\max_{i=1}^m\{-|X_i|_{n_i}\}$ ($c = \mathit{true}$) or of $\deg(M)$ and $-|X|_n$ ($c = \mathit{false}$). △

5.8 Reduced Class Representatives

In this section we will prove that for each class in $\mathrm{CaCl}^0_\pi(X)$ there is a representative whose restriction to V_0 has bounded degree. We will achieve this for both the component

independent case and the component dependent case by using modification functions. This is one of the very important applications of modification functions in this thesis. This is not only a nice theoretical result, but also the basis that we can assume the ideals that we get as input for our algorithms to have bounded degree, that is, degree in $O(nc_X)$. Moreover, we also show that the degree bound on the input ideal representatives provide bounds for the basis matrices representing those ideals. This implies that we may assume that the input matrices for our algorithms have degree in $O(c_X)$.

Furthermore, both Sections 5.8 and 5.9 provide the theoretical background for and justify why we can carry out the group law of $\mathrm{CaCl}^0_\pi(X)$ only using the basis matrices of $\mathcal{O}_X(D)$ where D is the respective representative of a given class.

5.8.1 Component Independent Representation

The main goal of this section is to provide for every class in $\mathrm{CaCl}^0_\pi(X)$ a representative of the form $D + r(x)_\infty \in \mathcal{D}_0$ with $D \leq 0$ and r linearly bounded by c_X. Moreover, the existence of a basis matrix representing $\mathcal{O}_X(D)(V_0)$ with degree in $O(c_X)$ will also be proven.

Notation 5.8.1. For the rest of this thesis we set

$$\mu_X = \begin{cases} 1, & \text{if } X \text{ is irreducible} \\ 2, & \text{if } X \text{ is reducible.} \end{cases} \quad \triangle$$

The following two statements provide the existence of basis matrices M_D of $\mathcal{O}_X(D)(V_0)$ for representatives of the form $D + r(x)_\infty$ with degree bounded by $r + \mu_X c_X$ and also bounds of the degree of modification functions that can be computed by ModFctCF using M_D.

For the rest of this section let X be a reduced cover of $\mathbb{P}^1_k$.

Lemma 5.8.2. *Let $D = D_0 + r(x)_\infty$ with $D_0 \leq 0$ be a representative of a class in $\mathrm{CaCl}^0_\pi(X)$. Then there exists a basis matrix M_D of $\mathcal{O}_X(D)(V_0)$ with respect to Ω such that $\deg M_D \leq r + \mu_X c_X$.*

Proof. By Corollaries 4.3.27 and 4.5.4, we know that there exists a basis matrix M_D with respect to Ω such that $\deg M_D \leq (\deg_k \mathcal{O}_X(D)(V_0))/n + \mu_X c_X$. Due to Corollary C.4.13 and Lemmas C.4.8 and D.2.13, we have

$$\deg_k \mathcal{O}_X(D)(V_0) = -\deg_k \mathcal{O}_X(D)(S) = -\deg_k \mathcal{O}_X(r(x)_\infty)(S) = \deg_k x^r \mathcal{O}_S = rn$$

and thus the assertion follows. □

Lemma 5.8.3. *Let $D = D_0 + r(x)_\infty$ be a representative of a class in $\mathrm{CaCl}^0_\pi(X)$ with basis matrix M_D as in Lemma 5.8.2. Then $\phi_\Omega(f) = \mathrm{ModFctCF}(M_D)$ satisfies $s := \deg \phi_\Omega(f) \leq r + (\mu_X + 1)c_X$. Moreover, we have $\mathrm{div}_S(f) = -s(x)_\infty$.*

Proof. By Lemma 5.8.2, we have $\deg M_D \leq r + \mu_X c_X$ and, by Theorem 5.7.20, we therefore obtain the bound for s. The algorithm ModFctCF computes f such that its coefficient vector $\phi_\Omega(f) = (f_1, \ldots, f_n)^T$ satisfies $\deg f_i < \deg f_1 - |X|_i$ and thus, by Lemma 5.6.25, this provides $f\mathcal{O}_S = x^s \mathcal{O}_S$ which in turn induces $\mathrm{div}_S(f) = -s(x)_\infty$ due to the definition of the pole divisor of x. □

Corollary 5.6.28 already provided representatives of classes in $\mathrm{CaCl}^0_\pi(X)$ that have the desired form $D + r(x)_\infty$ and bounded r. However, the following statement will also provide the desired representative. Moreover, it directly tells us how to compute a reduction of a representative which has too large degree. This will be used in the explicit arithmetic in $\mathrm{CaCl}^0_\pi(X)$.

Proposition 5.8.4. *Let $D = D_0 + a(x)_\infty \in \mathrm{Div}^0_\pi(X)$ with $D_0 \leq 0$. Let M_D be a basis matrix of $\mathcal{O}_X(D)(V_0)$ with respect to Ω such that $\deg M_D \leq a + \mu_X c_X$ (which exists due to Lemma 5.8.2). Let $\phi_\Omega(f) = \textsc{ModFctCF}(M_D)$ and set $E = -D - \mathrm{div}_X(f)$. Let M_E denote a basis matrix of $\mathcal{O}_X(E)(V_0)$ with respect to Ω as in Lemma 5.8.2 and let $\phi_\Omega(g) = \textsc{ModFctCF}(M_E)$. Then*

$$F = D + \mathrm{div}(fg^{-1}) = F_0 + r(x)_\infty$$

with $F_0 \leq 0$, $\mathrm{Supp}(F_0) \subseteq V_0$ and $r \leq (\mu_X+1)c_X$. In particular, $-\deg_k F_{|V_0} \leq (\mu_X+1)c_X n$.

Proof. By Lemma 5.8.3, f satisfies $\mathrm{div}_S(f) = -s(x)_\infty$, $s \leq a + (\mu_X+1)c_X$ and $\mathrm{div}_X(f) + D_0 + s(x)_\infty \geq 0$. By definition, we have $E = -D - \mathrm{div}_X(f) = -D_0 - a(x)_\infty - \mathrm{div}_X(f)$ and thus

$$\begin{aligned} E = & -(D_0)_{|V_0} - \mathrm{div}_{V_0}(f) - \mathrm{div}_S(f) - a(x)_\infty \\ = & -(D_0)_{|V_0} - \mathrm{div}_{V_0}(f) + (s-a)(x)_\infty. \end{aligned}$$

As above, by Lemma 5.8.3, g satisfies $\mathrm{div}_S(g) = -t(x)_\infty$, $t \leq (s-a) + (\mu_X+1)c_X$ and

$$\mathrm{div}_X(g) - (D_0)_{|V_0} - \mathrm{div}_{V_0}(f) + t(x)_\infty \geq 0.$$

In particular, $(D_0)_{|V_0} + \mathrm{div}_{V_0}(f) - \mathrm{div}_{V_0}(g) \leq 0$. Therefore, we finally obtain

$$\begin{aligned} D + \mathrm{div}_X(fg^{-1}) &= D_{|V_0} + a(x)_\infty + \mathrm{div}_X(f) - \mathrm{div}_X(g) \\ &= D_{|V_0} + a(x)_\infty + \mathrm{div}_{V_0}(f) + \mathrm{div}_S(f) - \mathrm{div}_{V_0}(g) - \mathrm{div}_S(g) \\ &= \underbrace{D_{|V_0} + \mathrm{div}_{V_0}(f) - \mathrm{div}_{V_0}(g)}_{\leq 0} + (a - s + t)(x)_\infty \end{aligned}$$

and $a - s + t \leq a - s + s - a + (\mu_X+1)c_X = (\mu_X+1)c_X$. The particular part now follows from Proposition C.4.18 (ii) and $\deg_k F = 0$. □

Corollary 5.8.5. *Let X be a reduced cover of $\mathbb{P}^1_k$. For every class in $\mathrm{CaCl}^0_\pi(X)$ there is a representative of the form $D = D_0 + r(x)_\infty$ with $D_0 \leq 0$, $\mathrm{Supp}(D_0) \subseteq V_0$ and $r \leq (\mu_X+1)c_X$.*

Proof. By Corollary 5.6.28, for every class in $\mathrm{CaCl}^0_\pi(X)$ there is a representative of the form $D = D_0 + r(x)_\infty$ with $D_0 \leq 0$, $\mathrm{Supp}(D_0) \subseteq V_0$. Now we only need to apply Proposition 5.8.4 to D and obtain the asserted representative. □

Corollary 5.8.6. *Let X be a reduced cover of $\mathbb{P}^1_k$. For every class in $\mathcal{I}_\pi/\mathcal{P}_\pi$ there is a representative $I \subseteq R_0$ with $(\deg_k I)/n \leq (\mu_X+1)c_X$. Moreover, there exists a basis matrix M_I of I with respect to Ω with $\deg M_I \leq (2\mu_X+1)c_X$.*

Proof. By Corollary 5.8.5, there is a representative for every class in $\mathrm{CaCl}^0_\pi(X)$ of the form $D = D_0 + r(x)_\infty$ with $D_0 \leq 0$, $\mathrm{Supp}(D_0) \subseteq V_0$ and $r \leq (\mu_X+1)c_X$. Hence $I = \mathcal{O}_X(D)(V_0) = \mathcal{O}_X(D_0)(V_0) \subseteq R_0$ by Proposition 3.1.27 (ii) and

$$\deg_k I = -\deg_k \mathcal{O}_X(D)(S) = -\deg_k x^r \mathcal{O}_S = rn$$

by Corollaries C.4.13 and D.2.9 which thus results in the asserted bound of $(\deg_k I)/n$. The existence of M_I is due to Corollaries 4.3.27 and 4.5.4. □

5.8.2 Component Dependent Representation

The main goal of this section is to prove that every class in $\mathrm{CaCl}^0_\pi(X)$ has a representative $D = D_0 + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathcal{D}_0$ with $\mathrm{Supp}(D_0) \subseteq V_0$ and $r_i \leq 2c_{i,X}$. Moreover, we prove that there is a basis matrix M_D in n-block-form representing $\mathcal{O}_X(D)(V_0)$ for D as above such that the i-th row block of M_D has degree bounded by $3c_{i,X}$. In particular, this yields $\deg M_D \leq 3c_X$.

Proposition 5.8.7. *Let $D = D_0 + \sum_{i\in A} a_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$ such that $D_0 \leq 0$ and $\mathrm{Supp}(D_0) \subseteq V_0$. Let M_D be a basis matrix of $\mathcal{O}_X(D)(V_0)$ with respect to Ω^m_i in n-block-form such that the i-th row block $M_{D,i}$ of M_D satisfies $\deg M_{D,i} \leq a_i + c_{i,X}$ (which exists due to Proposition 4.4.20). Let $\phi_{\Omega^m_i}(f) = \textsc{ModFctC}(M_D)$ be a modification function of D. We set $E = -(\mathrm{div}(f) + D)_{|V_0}$ and by M_E we denote a basis matrix of $\mathcal{O}_X(E)(V_0)$ with respect to Ω^m_i in n-block-form such that the i-th row block $M_{E,i}$ of M_E satisfies $\deg M_{E,i} \leq \deg_k \mathcal{O}_X(E_{|X_i})(V_{i,0})/n_i + c_{i,X}$ (as above, see Proposition 4.4.20). We set $\phi_{\Omega^m_i}(g) = \textsc{ModFctC}(M_E)$. Then*

$$F = D + \mathrm{div}(fg^{-1}) = F_0 + \sum\nolimits_{i\in A} s_i(x)_{i,\infty}$$

with $F_0 \leq 0$, $\mathrm{Supp}(F_0) \subseteq V_0$ and $s_i \leq 2c_{i,X}$. In particular,

$$-\deg_k F_{|V_0} \leq 4(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X).$$

Proof. By assumption, we have $\deg_k D_{|X_i} = -a_i n_i$. By Theorem 5.7.23 and Propositions 4.4.20 and 4.4.21, f satisfies

$$d_i := \deg \phi_{\Omega_i}(f_{|X_i}) \leq a_i + c_{i,X} - |X_i|_{n_i} \leq a_i + 2c_{i,X}.$$

By Lemma 5.7.25, f satisfies $-\mathrm{div}_S(f) = \sum_{i\in A} d_i(x)_{S_i,\infty}$ and $\mathrm{div}(f)+D+\sum_{i\in A} d_i(x)_{i,\infty} \geq 0$. Let us now add $\mathrm{div}(f)$ to the divisor we started with:

$$\begin{aligned}\mathrm{div}(f) + D + \sum\nolimits_{i\in A} a_i(x)_{i,\infty} &= \mathrm{div}_{V_0}(f) + D_{|V_0} + \mathrm{div}_S(f) + \sum\nolimits_{i\in A} a_i(x)_{S_i,\infty} \\ &= \underbrace{\mathrm{div}(f)_{|V_0} + D_{|V_0}}_{\geq 0} + \sum\nolimits_{i\in A} (\underbrace{a_i - d_i}_{\geq -2c_{i,X}})(x)_{S_i,\infty} \qquad (8{:}29)\end{aligned}$$

Set $E = -\mathrm{div}_{V_0}(f) - D_{|V_0} \leq 0$ which satisfies $-\deg_k E_{|X_i} = (d_i - a_i)n_i$ due to the fact that $\mathrm{div}_X(f) + D$ still has degree zero, see Eq. (8:29) and Proposition C.4.18 (ii). Now let M_E be a basis matrix of $\mathcal{O}_X(E)(V_0)$ as asserted and set $\phi_{\Omega^m_i}(g) = \textsc{ModFctC}(M_E)$ with $e_i := \deg \phi_{\Omega_i}(g_{|X_i})$. As above, by Theorem 5.7.23 and Propositions 4.4.20 and 4.4.21, g satisfies

$$\begin{aligned} e_i &\leq (\deg_k \mathcal{O}_X(E_{|X_i})(V_{i,0}))/n_i + 2c_{i,X} \\ \text{Proposition C.4.18 (i)} \rightsquigarrow\ &= (-\deg_k E_{|X_i})/n_i + 2c_{i,X} \\ &= (d_i - a_i) + 2c_{i,X}. \qquad (8{:}30)\end{aligned}$$

Moreover, by Lemma 5.7.25, g satisfies $-\mathrm{div}_S(g) = \sum_{i\in A} e_i(x)_{S_i,\infty}$ and $\mathrm{div}(g) + E + \sum_{i\in A} e_i(x)_{i,\infty} \geq 0$. In particular,

$$-\mathrm{div}(g) - E - \sum\nolimits_{i\in A} e_i(x)_{i,\infty} \leq 0. \qquad (8{:}31)$$

Now we consider $F := D + \operatorname{div}_X(fh^{-1}) = D_0 + \sum_{i\in A} a_i(x)_{i,\infty} + \operatorname{div}_X(fg^{-1})$: We have

$$\begin{aligned} F_{|V_0} &= -\operatorname{div}_{V_0}(g) + \operatorname{div}_{V_0}(f) + D_0 \\ &= -\operatorname{div}_{V_0}(g) - E_{|V_0} \leq 0 \end{aligned}$$

due to Eq. (8:31). Moreover,

$$\begin{aligned} F_{|S} &= \operatorname{div}_S(f) - \operatorname{div}_S(g) + \sum\nolimits_{i\in A} a_i(x)_{S_i,\infty} \\ &= \sum\nolimits_{i\in A} -d_i(x)_{S_i,\infty} + \sum\nolimits_{i\in A} e_i(x)_{S_i,\infty} + \sum\nolimits_{i\in A} a_i(x)_{S_i,\infty} \\ &= \sum\nolimits_{i\in A} (-d_i + e_i + a_i)(x)_{S_i,\infty}. \end{aligned}$$

Finally, Eq. (8:30) yields

$$-d_i + e_i + a_i \leq -d_i + (d_i - a_i) + 2c_{i,X} + a_i = 2c_{i,X}.$$

Thus $F = F_{|V_0} + F_{|S}$ with $F_{|V_0} \leq 0$ and $F_{|S} = \sum_{i\in A} s_i(x)_{S_i,\infty}$ such that $s_i \leq 2c_{i,X}$. In particular,

$$-\deg_k F_{|V_0} \leq \sum_{i=1}^{m} 2c_{i,X}n_i \leq 4(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X)$$

due to Lemma 2.4.11. □

Corollary 5.8.8. *Let $I \in \mathcal{I}_\pi$. Let M_I be a basis matrix of I with respect to Ω_i^m in n-block-form such that the i-th row block $M_{I,i}$ of M_I satisfies $\deg M_{I,i} \leq \deg_k I_i/n_i + c_{i,X}$ (which exists due to Proposition 4.4.20). Let $\phi_{\Omega_i^m}(f) = \text{ModFctC}(M_I)$ be a modification function of I. We set $J = fI^{-1}$ and by M_J we denote a basis matrix of J with respect to Ω_i^m in n-block-form such that the i-th row block $M_{J,i}$ of M_J satisfies $\deg M_{J,i} \leq \deg_k J_i/n_i + c_{i,X}$ (as above, see Proposition 4.4.20). We set $\phi_{\Omega_i^m}(g) = \text{ModFctC}(M_J)$. Then*

$$H = gf^{-1}I$$

satisfies $H \subseteq R_0$ and $\deg_k H_i/n_i \leq 2c_{i,X}$. In particular,

$$\deg_k H \leq 4(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X).$$

Proof. Let $D = \phi^{-1}(I) = D_0 + \sum_{i\in A} a_i(x)_{i,\infty}$ be the corresponding divisors of I under the isomorphism in Proposition 3.1.27. Note that

$$a_i = -(\deg_k(D_0)_{|X_i})/n_i = (\deg_k \mathcal{O}_{X_i}((D_0)_{|X_i}(V_{i,0})))/n_i = (\deg_k I_i)/n_i.$$

Let $E = -D_0 - \operatorname{div}_{V_0}(f)$. This equality becomes under ϕ, see Proposition 3.1.27, the equation

$$J = \mathcal{O}_X(E)(V_0) = fI^{-1}.$$

The product $H = gJ^{-1} = (gf^{-1})I$ corresponds under ϕ to $-\operatorname{div}_{V_0}(g) - E = -\operatorname{div}_{V_0}(g) + D + \operatorname{div}_{V_0}(f)$ and thus the rest of the assertion follows from Proposition 5.8.7 using the properties being preserved under ϕ, see for instance Proposition C.4.18. □

Corollary 5.8.9. *Every divisor class in $\operatorname{CaCl}_\pi^0(X)$ has a representative $D = D_0 + \sum_{i\in A} r_i(x)_{i,\infty}$ with $D_0 \leq 0$, $\operatorname{Supp}(D_0) \subseteq V_0$ and $r_i \leq 2c_{i,X}$ yielding $-\deg_k D_0 \leq 4(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X)$. Moreover, that representative has a basis matrix M_D in n-block-form with row blocks $M_{D,i}$ satisfying $\deg M_{D,i} \leq 3c_{i,X}$ yielding $\deg M_D \leq 3c_X$.*

Proof. By Corollary 5.6.28, there is a representative of the form $D+r(x)_\infty$ with $\mathrm{Supp}(D) \subseteq V_0$, $D \leq 0$ and some $r \in \mathbb{Z}$. Now since $r(x)_\infty = \sum_{i\in A} r(x)_{i,\infty}$, see Remark 5.6.10, we can apply Proposition 5.8.7 to that representative to obtain the new one with the desired properties. The statement about the basis matrix follows from Proposition 4.4.20 and $r_i \leq 2c_{i,X}$. □

Proposition 5.8.10. *Every ideal class in $\mathcal{I}_\pi/\mathcal{P}_\pi$ has a representative I with $I \subseteq R_0$ and $\deg_k I/P_iI \leq 2c_{i,X}$ yielding $\deg_k I \leq 4(g+n+\chi(\mathscr{S}_X)) + \dim_k H^0(X,\mathcal{O}_X)$. Moreover, that representative has a basis matrix M_I in n-block-form with row blocks $M_{I,i}$ satisfying $\deg M_{I,i} \leq 3c_{i,X}$ yielding $\deg M_I \leq 3c_X$.*

Proof. By Proposition 3.1.27, we have an isomorphism $\mathrm{CaCl}^0_\pi(X) \to \mathcal{I}_\pi/\mathcal{P}_\pi$ given by

$$[D + \sum\nolimits_{i\in A} r_i(x)_{i,\infty}] \mapsto [\mathcal{O}_X(D)(V_0)].$$

By Lemma 3.2.30, we have

$$\mathcal{O}_{V_{i,0}}(D_{|V_{i,0}})(V_{i,0}) \cong \mathcal{O}_X(D)_{|V_{i,0}}(V_{i,0}) \cong \frac{\mathcal{O}_X(D)(V_0)}{P_{i,0}\mathcal{O}_X(D)(V_0)}$$

which provides, if we write $I = \mathcal{O}_X(D)(V_0)$, that

$$\deg_k I/P_{i,0}I = \deg_k \mathcal{O}_{V_{i,0}}(D_{|V_{i,0}})(V_{i,0}) = -\deg_k D_{|V_{i,0}} = -\deg_k D_{|X_i} = r_in_i$$

where the second equality is due to Proposition C.4.18 (i) and the second last due to the fact that $\mathrm{Supp}(D_{X_i}) \subseteq V_{i,0}$. The last equality follows from the fact that $D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$ and Proposition C.4.18 (iii). Now everything follows from the isomorphism in Corollary 5.6.23 together with Corollary 5.8.9 and Lemma C.1.28. □

5.9 Arithmetic Operations in CaCl^0_π

While we have shown in Section 5.8 that there are representatives of bounded size, we want to prove in this section that computing the difference of two classes in CaCl^0_π respectively the quotient of two classes in $\mathcal{I}_\pi/\mathcal{P}_\pi$ using reduced representatives yields a representative of the resulting class that does not have too large degree. Moreover, we will establish statements concerning the arithmetic operations we will carry out later on with explicit algorithms in Chapter 6.

5.9.1 Component Independent Case

Proposition 5.9.1. *Let $D = D_0 + a(x)_\infty$, $E = E_0 + b(x)_\infty \in \mathrm{Div}^0_\pi(X)$ with $E_0, D_0 \leq 0$. Let M_D be a basis matrix of $\mathcal{O}_X(D)(V_0)$ with respect to Ω such that $\deg M_D \leq a + \mu_X c_X$ (which exists due to Lemma 5.8.2). Let $\phi_\Omega(f) = \textsc{ModFctCF}(M_D)$. Then*

$$F = E - D - \mathrm{div}(f) = F_0 + r(x)_\infty$$

with $F_0 \leq 0$, $\mathrm{Supp}(F_0) \subseteq V_0$ and $r \leq b + (\mu_X+1)c_X$. In particular,

$$-\deg_k F_{|V_0} \leq -\deg_k E_0 + (\mu_X+1)c_Xn.$$

Proof. By Theorem 5.7.20 and Lemma 5.8.3, we know that $f \in \mathcal{L}_{\mathrm{reg}}(D_0 + s(x)_\infty)$ where $s \leq a+(\mu_X+1)c_X$ such that $\mathrm{div}_S(f) = -s(x)_\infty$. In particular, $-\mathrm{div}_{V_0}(f) - D_0 \leq 0$. Thus

$$F = E - D - \mathrm{div}_X(f) = E_0 - D_0 - \mathrm{div}_{V_0}(f) + (b-a+s)(x)_\infty$$

with $F_{|V_0} = E_0 - D_0 - \mathrm{div}_{V_0}(f) \leq 0$ by the above and the fact that $E_0 \leq 0$. Moreover, $b-a+s \leq b-a+a+(\mu_X+1)c_X = b+(\mu_X+1)c_X$. Since $\deg_k F = 0$, by Proposition C.4.18 (ii), we finally have

$$\begin{aligned} -\deg_k F_{|V_0} = \deg_k F_{|S} = rn \leq bn + (\mu_X+1)c_X n = \deg_k E_{|S} + (\mu_X+1)c_X n \\ \text{Proposition C.4.18 (ii)} \rightsquigarrow \quad = -\deg_k E_0 + (\mu_X+1)c_X n. \end{aligned}$$ □

Corollary 5.9.2. *Let $I, J \in \mathcal{I}_\pi$ and let M_I be a basis matrix of I with respect to Ω such that $\deg M_I \leq \deg_k I/n + \mu_X c_X$. Let $f = \mathrm{ModFctCF}(M_I)$. Then $fJ/I \subseteq R_0$ and $\deg_k fJ/I \leq \deg_k J + (\mu_X+1)c_X n$.*

Proof. Let $E = \phi^{-1}(J) = E_0 + b(x)_\infty$ and $D = \phi^{-1}(I) = D_0 + a(x)_\infty$ be the corresponding divisors of J respectively I. Note that $a = -(\deg_k D_0)/n = (\deg_k I)/n$. Let $F = E - D - \mathrm{div}_X(f)$. Under ϕ this equality becomes, see Proposition 3.1.27, the equation

$$\mathcal{O}_X(F)(V_0) = fJ \cdot I^{-1} = fJ/I.$$

Now Proposition 5.9.1 implies $-\deg_k F_{|V_0} \leq -\deg_k E_{|V_0} + (\mu_X+1)c_X n$. By Proposition C.4.18 (i), we have

$$\begin{aligned} -\deg_k F_{|V_0} &= \deg_k \mathcal{O}_X(F)(V_0) = \deg_k fJ/I, \quad \text{and} \\ -\deg_k E_{|V_0} &= \deg_k \mathcal{O}_X(E)(V_0) = J \end{aligned}$$

which then completes the proof. □

Corollary 5.9.3 (of Proposition 5.8.4)**.** *Let $I \in \mathcal{I}_\pi$ and let M_I be a basis matrix of I with respect to Ω such that $\deg M_I \leq \deg_k I/n + \mu_X c_X$. Let $f = \mathrm{ModFctCF}(M_I)$ and set $J = fI^{-1} \subseteq R_0$. Let M_J be a basis matrix of J such that $\deg M_J \leq \deg_k J/n + \mu_X c_X$. Let $g = \mathrm{ModFctCF}(M_J)$ and set $H = gJ^{-1} = (gf^{-1})I$. Then $H \subseteq R_0$ and $\deg_k H \leq (\mu_X+1)c_X n$.*

Proof. Let $D = \phi^{-1}(I) = D_0 + a(x)_\infty$ be the corresponding divisors of I. Note that $a = -(\deg_k D_0)/n = (\deg_k I)/n$. Let $E = -D - \mathrm{div}_X(f)$. Under ϕ this equality becomes, see Proposition 3.1.27, the equation

$$J = \mathcal{O}_X(E)(V_0) = fI^{-1}.$$

The product $H = gJ^{-1} = (gf^{-1})I$ corresponds under ϕ to $-\mathrm{div}_X(g) - E = -\mathrm{div}_X(g) + D + \mathrm{div}_X(f)$ and thus the rest of the assertion follows from Proposition 5.8.4. □

Proposition 5.9.4. *Let X be integral. Let $D = D_0 + a(x)_\infty \in \mathrm{Div}_\pi^0(X)$ with $D_0 \leq 0$. Then D is principal if and only if $0 \geq -|D|_1$.*

Proof. By Lemma 4.7.9, D is principal if and only if $\mathcal{O}_X(D)(X) \neq 0$ and thus, by Remark 4.3.19, if and only if $0 \geq -|D|_1$. □

Remark 5.9.5. Note that if X is integral, given any basis matrix of $\mathcal{O}_X(D)(V_0)$, we can compute $-|D|_1$ using Algorithm 2. For reducible, reduced X, see Proposition 5.9.8. In particular, the *test of principality* or the *zero test* cannot be performed independent of the irreducible components. △

5.9.2 Component Dependent Case

Proposition 5.9.6. *Let $D = D_0 + \sum_{i\in A} a_i(x)_{S_i,\infty}$, $E = E_0 + \sum_{i\in A} b_i(x)_{S_i,\infty} \in \mathrm{Div}_\pi^0(X)$ with $E_0, D_0 \leq 0$. Let M_D be a basis matrix of $\mathcal{O}_X(D)(V_0)$ with respect to Ω_i^m in n-block-form with row blocks $M_{D,i}$ such that $\deg M_{D,i} \leq a_i + c_{i,X}$ (which exists due to*

Proposition 4.4.20). Let $\phi_\Omega(f) = \textsc{ModFctC}(M_D)$. *Then*

$$F = E - D - \operatorname{div}(f) = \left(F_{|V_0}, \sum_{i=1}^{m} (b_i + d_i)(x)_{i,\infty} \right)$$

with $F_{|V_0} \leq 0$ *and* $d_i \leq 2c_{i,X}$. *In particular,* $-\deg_k F_{|V_0} \leq -\deg_k E_0 + 4(g+n+\chi(\mathscr{S}_X)) + 2\dim_k H^0(X, \mathcal{O}_X)$.

Proof. By Theorem 5.7.23, the modification function f computed by ModFctC satisfies $e_i := \deg \phi_{\Omega_i}(f_i) \leq d_i + c_{i,X}$ where d_i is an upper bound of $\deg M_{D,i}$. Hence $e_i \leq a_i + 2c_{i,X}$. Moreover, by Lemma 5.7.25, we have

$$-\operatorname{div}_S(f) = \sum_{i \in A} e_i(x)_{i,\infty} \quad \text{and} \quad f \in \mathcal{L}_{\mathrm{reg}}(D_0 + \sum_{i \in A} e_i(x)_{i,\infty}) \tag{9:32}$$

where the latter provides $-\operatorname{div}_{V_0}(f) - D_0 \leq 0$. Hence from $E_0 \leq 0$ and Eq. (9:32), we deduce $F_{|V_0} = E_0 - \operatorname{div}(f)_{|V_0} - D_0 \leq 0$. By definition and Eq. (9:32), we have

$$F_{|S} = E_{|S} - D_{|S} - \operatorname{div}_S(f) = \sum\nolimits_{i \in A} (b_i - a_i + e_i)(x)_{S_i,\infty}.$$

Note that we have $d_i := -a_i + e_i \leq -a_i + a_i + 2c_{i,X} = 2c_{i,X}$. By assumption, we have $\deg_k(E_0)_{|X_i} = -b_i n_i$. Since E, D as well as $\operatorname{div}_X(f)$ have degree zero, the same is true for F and hence, by Proposition C.4.18 (ii) and Lemma 5.7.10, we obtain

$$\begin{aligned} -\deg_k F_{|V_0} = \sum_{i \in A} (b_i + d_i) n_i &= \sum_{i \in A} b_i n_i + \sum_{i \in A} d_i n_i \\ &= -\deg_k E_0 + \sum_{i \in A} d_i n_i \\ \text{Lemma 2.4.11} \rightsquigarrow \quad &\leq -\deg_k E_0 + 4(g+n+\chi(\mathscr{S}_X)) + 2\dim_k H^0(X, \mathcal{O}_X). \end{aligned}$$

□

Proposition 5.9.7. *Let* $I, J \in \mathcal{I}_\pi$. *Let* $f \in J$ *be given by* $\phi_{\Omega_i^m}(f) = \textsc{ModFctC}(M_J)$ *where* M_J *is a basis matrix of* J *with respect to* Ω_i^m *in* n*-block-form with row blocks* $M_{J,i}$ *such that* $\deg M_{J,i} \leq (\deg_k J_i)/n_i + c_{i,X}$ *(which exists due to Proposition 4.4.20). Then* $H := fI/J \subseteq R_0$ *with* $\deg_k H_i \leq \deg_k I_i + 2c_{i,X}$ *and* $\deg_k H \leq \deg_k I + 4(g+n+\chi(\mathscr{S}_X)) + 2\dim_k H^0(X, \mathcal{O}_X)$.

Proof. Let $E = \phi^{-1}(I) = (E_0, \sum_{i \in A} b_i(x)_{S_i,\infty})$ and $D = \phi^{-1}(J) = (D_0, \sum_{i \in A} a_i(x)_{S_i,\infty})$ be the corresponding divisors of I and J. Let $F = E - D - \operatorname{div}_X(f)$. Under ϕ this equality becomes, see Proposition 3.1.27, the equation

$$\mathcal{O}_X(F)(V_0) = (IfR_0) \cdot J^{-1} = fI/J = H$$

and hence the assertion follows from Proposition 5.9.6. □

Proposition 5.9.8. *Let* $E = D + \sum_{i \in A} r_i(x)_{i,\infty} \in \operatorname{Div}^0_\pi(X)$ *with* $D \leq 0$. *Let* $\alpha_{i,1}, \ldots, \alpha_{i,n_i}$ *for* $i = 1, \ldots, m$ *be a reduced basis of* $\mathcal{O}_X(E_{|X_i})(V_{i,0})$. *By* $\alpha \in \mathcal{K}_X(X)^\times$ *we denote the element corresponding to* $(\alpha_{1,1}, \ldots, \alpha_{m,1})$. *Then* E *is principal if and only if* $0 \geq -|E_{|X_i}|_1$ *for all* $i = 1, \ldots, m$ *and* $\alpha \in \mathcal{O}_X(E)(V_0)$.

Proof. By Lemma 4.7.9, E is principal if and only if $\mathcal{L}_{\mathrm{reg}}(E) \neq \emptyset$. Hence, if E is principal with $E = \operatorname{div}(\alpha^{-1})$, then, by Lemma 4.7.8, we have $\alpha \in \mathcal{L}_{\mathrm{reg}}(E) \subseteq \mathcal{O}_X(E)(X)$. Let $\alpha = (\alpha_1, \ldots, \alpha_m)$. Moreover, we have $E_{|X_i} = \operatorname{div}(\alpha_i^{-1})$ which provides $\alpha_i \in \mathcal{L}_{\mathrm{reg}}(E_{|X_i})$. In particular, $0 \geq -|E_{|X_i}|_1$ since this is equivalent to $\mathcal{O}_X(E_{|X_i})(X_i) \neq 0$, see Remark 4.3.19. By

Lemma 4.7.3, we see that $\alpha_i = \varepsilon_i \alpha_{i,1}$ with $\varepsilon_i \in k$. Finally, since $\mathcal{L}_{\mathrm{reg}}(E) \subseteq \mathcal{O}_X(E)(X) = \mathcal{O}_X(E)(V_0) \cap \bigoplus_{i=1}^m x^{r_i}\mathcal{O}_{S_i}$, we also have $\alpha \in \mathcal{O}_X(E)(V_0)$.

Conversely, let $0 \geq -|E_{|X_i}|_1$ hold. By Theorem 4.3.15 and Remark 4.3.19, this is equivalent to $\alpha_{i,1} \in \mathcal{O}_X(E_{|X_i})(X_i) \setminus \{0\} = \mathcal{L}_{\mathrm{reg}}(E_{|X_i})$ which together with $\deg_k E_{|X_i} = 0$ implies $E_{|X_i} = \mathrm{div}(\alpha_{i,1}^{-1})$, see Lemmas 4.7.8 and 4.7.9. Since $\alpha_{i,1} \neq 0$ for all $i = 1, \ldots, m$, we have that $\alpha = (\alpha_{1,1}, \ldots, \alpha_{m,1})$ is contained in $\mathcal{K}_X(X)^\times$. By assumption we have $\alpha \in \mathcal{O}_X(E)(V_0)$. Since $\mathrm{div}(\alpha_{|X_i}^{-1}) = E_{|X_i} = D_{|X_i} + r_i(x)_{i,\infty}$, we see that $\alpha_{|X_i} \in x^{r_i}\mathcal{O}_{S_i}$. In particular, $\alpha \in \bigoplus_{i=1}^m x^{r_i}\mathcal{O}_{S_i}$ which together with $\alpha \in \mathcal{O}_X(E)(V_0)$ yields $\alpha \in \mathcal{O}_X(E)(X)$. Now since $\alpha \in \mathcal{K}_X(X)^\times$, we finally have $\alpha \in \mathcal{L}_{\mathrm{reg}}(E)$. □

Remark 5.9.9. Note that, given basis matrices of $\mathcal{O}_X(E_{|X_i})(V_{i,0})$, we can compute the π-invariants $-|E_{|X_1}|_1, \ldots, -|E_{|X_m}|_1$ using Algorithm 2. Moreover, using Algorithm 1 we can compute a basis matrix of $\mathcal{O}_X(E_{|X_i})(V_{i,0})$ representing a reduced basis $\alpha_{i,1}, \ldots, \alpha_{i,n_i}$. Hence we are able to compute the coefficient vectors $\phi_{\Omega_1}(\alpha_{1,1}), \ldots, \phi_{\Omega_m}(\alpha_{m,1})$. △

Corollary 5.9.10. *Thus if we want to test whether E is principal, we might equivalently ask whether the linear system*

$$M_E \cdot \mu = \begin{pmatrix} \phi_{\Omega_1}(\alpha_{1,1}) \\ \vdots \\ \phi_{\Omega_m}(\alpha_{m,1}) \end{pmatrix}$$

has a solution $\mu \in k[x]^n$. For the definition of M_E, see Notation 4.4.7 (xii).

Chapter 6

Main Result – Computing Asymptotically Fast in $\mathrm{Pic}^0(X)$

In this chapter we will present the main result and contribution of this thesis: An algorithmic toolkit for computing asymptotically fast in the degree zero Picard group $\mathrm{Pic}^0(X)$ of X as follows.

> **Theorem 6.6.1.** *Let X be a reduced cover of $\mathbb{P}^1_k$. The elements in $\mathrm{Pic}^0(X)$ can be represented by matrices in $k[x]^{n\times n}$ with degree in $O(c_X)$. The combination of the Algorithms 19 and 20 provides randomised algorithms to compute both the group law in $\mathrm{Pic}^0(X)$ and the inverse of a given element. Moreover, Algorithms 21 and 22 provide a deterministic algorithm to test whether a given element in $\mathrm{Pic}^0(X)$ is the neutral element. All the above algorithms use at most $O^{\sim}(n^{\omega}c_X)$ operations in k and the randomised algorithms have positive constant success probability.*

In this chapter we will discuss the necessary theory behind the algorithms we will propose in this thesis to compute in $\mathrm{Pic}^0(X)$. It is organised as follows:

In Section 6.1 we will show that we can represent the elements in $\mathcal{I}_\pi/\mathcal{P}_\pi$ (and thus those in $\mathrm{Pic}^0(X)$) by matrices in $k[x]^{n\times n}$ with degree in $O(c_X)$. Moreover, we will outline the strategy we will follow in this chapter to actually compute in $\mathrm{Pic}^0(X)$.

In Section 6.2 we will provide an algorithm to compute the basis matrix of the quotient of two R-ideals that are themselves given by their basis matrices. Moreover, since the above algorithm requires an ideal generating set, we will provide probabilistic statements of how to find such a set.

Section 6.3 is solely devoted to computing the basis matrix of a principal R_0-ideal. We will compute the necessary products to do so by using fast polynomial multiplication in two indeterminates. In order to reduce to the polynomial multiplication, we need to provide a primitive element of $\mathcal{K}_X(X)$ over $k(x)$.

Section 6.4 gives an overview of precomputations that need to be done once before we can use the presented algorithms.

In Section 6.5 we introduce the algorithms that provide the toolkit to compute in $\mathrm{Pic}^0(X)$. Among these are the division algorithm, the algorithm that reduces a given class representative and the zero test.

Finally, in Section 6.6 we prove their correctness and that they can be used to compute asymptotically fast in $\mathrm{Pic}^0(X)$, see Theorem 6.6.1.

We have already stated in Chapter 5 that the groups $\mathrm{Pic}^0(X)$, $\mathrm{ClInvId}^0(X)$ and $\mathrm{CaCl}^0(X)$ are isomorphic, see Lemma 5.6.2. Moreover, as we have seen in Section 5.6, we have an

isomorphism $\mathrm{CaCl}^0(X) \to \mathrm{CaCl}^0_\pi(X)$, see Proposition 5.6.16. Moreover, we have an isomorphism $\mathrm{Div}^0_\pi(X) \to \mathcal{I}_\pi$ extending to an isomorphism $\mathrm{CaCl}^0_\pi(X) \to \mathcal{I}_\pi/\mathcal{P}_\pi$, see Proposition 5.6.22 and Corollary 5.6.23. Therefore, we may compute in $\mathcal{I}_\pi/\mathcal{P}_\pi$ instead of computing in $\mathrm{CaCl}^0_\pi(X)$ respectively in $\mathrm{Pic}^0(X)$ to carry out the group law of the degree zero Picard group.

In Section 5.8 we have shown that there are representatives of classes in both $\mathrm{CaCl}^0_\pi(X)$ and in $\mathcal{I}_\pi/\mathcal{P}_\pi$ that have bounded degree solely in terms of invariants of X. In the component independent case we have representatives D of the form

$$D = D_0 + r(x)_\infty, \quad D_0 \leq 0, \quad \mathrm{Supp}(D_0) \subseteq V_0, \quad r \leq (\mu_X + 1)c_X,$$

see Corollary 5.8.5, yielding ideal representatives

$$I \subseteq R_0, \quad (\deg_k I)/n \leq \mu_X c_X, \quad \deg M_I \leq (2\mu_X + 1)c_X,$$

see Corollary 5.8.6.

In the component dependent case we have representatives D of the form

$$\begin{aligned} D = D_0 + \sum\nolimits_{i \in A} r_i(x)_{i,\infty}, \quad D_0 \leq 0, \quad \mathrm{Supp}(D_0) \subseteq V_0, \quad r_i \leq 2c_{i,X}, \\ -\deg_k D_0 \leq 4(g + n + \chi(\mathscr{S}_X)) + \dim_k H^0(X, \mathcal{O}_X), \end{aligned}$$

see Corollary 5.8.9. This yields ideal representatives

$$I \subseteq R_0, \quad (\deg_k I/P_i I)/n_i \leq 2c_{i,X}$$

with basis matrix M_I in n-block-form with row blocks $M_{I,i}$ satisfying

$$\deg M_I \leq 3c_X, \quad \deg M_{I_i} \leq 3c_{i,X},$$

see Proposition 5.8.10. This has been done by proving that there is a way of reducing the respective given class representative by a suitably chosen modification function, see Proposition 5.8.7 and Corollary 5.8.8.

In Section 5.9 we have seen that we can subtract two divisor classes or divide two ideal classes which results in a class with a representative that again has bounded degree, see Proposition 5.9.6 and Proposition 5.9.7 in connection with Proposition 5.8.7. Moreover, also in Section 5.9 we have shown that there is a deterministic way of deciding whether a given representative in $\mathrm{CaCl}^0_\pi(X)$ or $\mathcal{I}_\pi/\mathcal{P}_\pi$ represents the trivial class, see Proposition 5.9.8.

To finally give concrete algorithms that carry out the group law, we need an algorithmic representation of the elements in $\mathrm{CaCl}^0_\pi(X)$ and $\mathcal{I}_\pi/\mathcal{P}_\pi$. This connection has already been established in Chapter 4 where we have discussed reduced bases of $\mathcal{F}(V_0)$ for any $\mathcal{O}_X$-ideal $\mathcal{F}$ on a cover X of $\mathbb{P}^1_k$. Moreover, we have shown that there are bases of $\mathcal{F}(V_0)$ in the case of a reducible and reduced cover X of $\mathbb{P}^1_k$ which are not too far away (in terms of degree) of reduced bases of $\mathcal{F}_i(V_{i,0})$. We will use the basis matrices of those bases to represent the elements in $\mathrm{CaCl}^0_\pi(X)$ respectively $\mathcal{I}_\pi/\mathcal{P}_\pi$.

6.1 Algorithmic Representation of Elements in $\mathrm{Pic}^0(X)$

Let X be a reduced cover of $\mathbb{P}^1_k$. To represent $\mathcal{O}_X$-ideals with basis matrices we need to fix bases of R_0 and $R_{i,0}$ for $i = 1, \ldots, m$ with respect to which we can represent the respective bases. The computation of those bases only need to be done once and can thus be precomputed as part of the algorithmic setup.

Notation 6.1.1. For all $i = 1, \dots, m$ let $\Omega_i = (\omega_{i,1}, \dots, \omega_{i,n_i})$ denote a reduced basis of $R_{i,0}$. The basis of $R_0^+ = \bigoplus_{i=1}^m R_{i,0}$ constituted by the Ω_i is denoted by Ω_i^m. By $\Omega = (\omega_1, \dots, \omega_n)$ we denote a reduced basis of R_0 as in Lemma 4.6.2. We denote the basis matrix of Ω with respect to Ω_i^m by T_Ω. By Lemma 4.6.2, we have $\deg T_\Omega \leq 2c_X$. We assume that we have computed the multiplication tables of all the above bases. △

Remark 6.1.2. We want to emphasise the flexibility that the precomputation of Ω and Ω_i^m together with T_Ω provides. Following Remarks 4.4.8 and 4.6.4, if $T_\mathcal{F}$ is a basis matrix of $\mathcal{F}(V_0)$ with respect to Ω, then the matrix $M_\mathcal{F} = T_\Omega \cdot T_\mathcal{F}$ represents the same basis with respect to Ω_i^m and thus enables us to compute the restrictions $\mathcal{F}_{|X_i}(V_{i,0})$ of $\mathcal{F}(V_0)$ applying ComputeComponentMatrices which employs ColumnBasis. Moreover, the computation of $M_\mathcal{F}$ given the matrix $T_\mathcal{F}$ is efficient using fast matrix multiplication as long as the degree of $T_\mathcal{F}$ lies in $O(c_X)$. △

In Section 4.2 we have seen that every $\mathcal{O}_X$-ideal $\mathcal{F}$ can be completely represented by the tuple $(\mathcal{F}(V_0), \mathcal{F}(V_\infty))$, see Corollary 4.2.4. Conversely, any pair (M_0, M_∞) where M_0 is an R_0-ideal and M_∞ is an R_∞-ideal for which we know that $(M_0)_x = (M_\infty)_{x^{-1}}$ holds represents an $\mathcal{O}_X$-ideal. Due to Lemma 4.2.6, we know that $(\mathcal{F}(V_0), \mathcal{F}(S))$ does represent $\mathcal{F}$ in terms of the arithmetic demands in the monoid of $\mathcal{O}_X$-ideals $\mathrm{MonoId}(X)$.

Since we have fixed the bases Ω and Ω_i^m, we may also represent $\mathcal{F}(V_0)$, $\mathcal{F}(V_\infty)$ and $\mathcal{F}(S)$ by a $k[x]$-, $k[x^{-1}]$- respectively $\mathcal{O}_\infty$-basis. But this means that we replace the tuple $(\mathcal{F}(V_0), \mathcal{F}(V_\infty))$ with a pair of matrices (T_0, T_∞) with $T_0 \in k[x]^{n\times n}$ and $T_\infty \in k[x^{-1}]^{n\times n}$ and the tuple $(\mathcal{F}(V_0), \mathcal{F}(S))$ with a pair of matrices (T_0, T_S) with $T \in k[x]^{n\times n}$ and $T_S \in \mathcal{O}_\infty^{n\times n}$. By Remark 4.2.10, we also see that T_∞ (regarded as a matrix over $\mathcal{O}_\infty$) also represents $\mathcal{F}(S)$. As already indicated by Lemma 4.2.6, we will use the arithmetic representation $(\mathcal{F}(V_0), \mathcal{F}(S))$ given by (T_0, T_S). We distinguish between the component independent and the component dependent case.

6.1.1 Component Independent Case

Let X be a reduced cover of $\mathbb{P}^1_k$. The following lemma shows that a $k[x]$-basis matrix of $\mathcal{F}(V_0)$ does already suffice to represent $\mathcal{F}$ in the case that $\deg_k \mathcal{F} = 0$ and $\mathcal{F}(S) = x^r\mathcal{O}_S$.

Lemma 6.1.3. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal of degree zero such that $\mathcal{F}(S) = x^r\mathcal{O}_S$. Then the pair $(\mathcal{F}(V_0), \mathcal{F}(S))$ can be solely represented by a $k[x]$-basis matrix of $\mathcal{F}(V_0)$.*

Proof. The pair $(\mathcal{F}(V_0), \mathcal{F}(S))$ may be represented by a pair of basis matrices (T_0, T_S) with $T_0 \in k[x]^{n\times n}$ and $T_S \in \mathcal{O}_\infty^{n\times n}$. But since $\mathcal{F}(S) = x^r\mathcal{O}_S$ for some $r \in \mathbb{Z}$, T_S is the diagonal matrix with x^r on the diagonal. Hence to compute T_S it is enough to know r.

First of all, by Corollary D.2.9, we have $\deg_k \mathcal{F}(S) = \deg_k x^r\mathcal{O}_S = -rn$. Moreover, by Corollary C.4.13, we deduce $\deg_k \mathcal{F}(S) = -\deg_k \mathcal{F}(V_0)$ which then finally provides $r = \deg_k \mathcal{F}(V_0)/n$. Since we can compute the degree of $\mathcal{F}(V_0)$ via its $k[x]$-basis matrix T_0, see Proposition D.2.7, we therefore have $(\deg \det T_0)/n = r$. □

Lemma 6.1.4. *For every class in $\mathrm{CaCl}^0_\pi(X)$ there is a representative of the form $E = D + r(x)_\infty$ with $r \leq (\mu_X + 1)c_X$ and if we set $\mathcal{F} = \mathcal{O}_X(E)$, then $\mathcal{F}$ can be represented by a basis matrix $T_\mathcal{F}$ of $\mathcal{F}(V_0)$ with degree bounded by $(2\mu_X + 1)c_X$.*

Proof. By Corollary 5.8.5, we always find representatives of classes in $\mathrm{CaCl}^0_\pi(X)$ in the asserted form. Moreover, by Lemma 5.8.2, there is a basis of $\mathcal{F}(V_0)$ whose basis matrix $T_\mathcal{F}$ has degree bounded by $r + \mu_X c_X \leq (2\mu_X + 1)c_X$. Now Lemma 6.1.3 tells us that $\mathcal{F}$ is represented by $T_\mathcal{F}$. □

6.1.2 Component Dependent Case

Let X be a reducible and reduced cover of $\mathbb{P}^1_k$. Recall the definitions we have made in Notation 4.4.7. In the case that $\mathcal{F} = \mathcal{O}_X(E)$ is the invertible $\mathcal{O}_X$-ideal of a divisor $E = D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$, things do not really get more complicated. As before, it turns out that we will only need a basis matrix of $\mathcal{F}(V_0)$ with respect to Ω^m_i to represent $\mathcal{F}$. The only difference here is that we need to be able to compute the restrictions $\mathcal{F}_i(V_{i,0}) := \mathcal{F}_{|X_i}(V_{i,0})$ from that given basis matrix. The following lemma shows how we represent the restrictions $\mathcal{F}_i$.

Lemma 6.1.5. *Let $E = D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$ and set $\mathcal{F} = \mathcal{O}_X(E)$. Then $\mathcal{F}_{|X_i}$ is solely represented by a $k[x]$-basis matrix $T_{\mathcal{F}_i}$ of $\mathcal{F}_{|X_i}(V_{i,0})$.*

Proof. By Corollary 5.6.7, we have $E_{|X_i} = (D_{|V_{i,0}}, r_i(x)_{S_i,\infty})$ with the notation as in Notation 5.5.7. That is $\mathcal{F}_{|X_i}(S_i) = \mathcal{O}_{X_i}(r_i(x)_{X_i,\infty})(S_i) = x^{r_i}\mathcal{O}_{S_i}$. Hence the requirements for Lemma 6.1.3 are met and thus we deduce that the $\mathcal{F}_{|X_i}$ are solely represented by a $k[x]$-basis matrix $T_{\mathcal{F}_i}$ of $\mathcal{F}_{|X_i}(V_{i,0})$, respectively. □

Now we consider a global representation of $\mathcal{F}(V_0)$ from which we are able to compute the restrictions and therefore yields a complete arithmetic representation of $\mathcal{F}$ in the component dependent case.

Lemma 6.1.6. *Let $E = D + \sum_{i\in A} r_i(x)_{i,\infty} \in \mathrm{Div}^0_\pi(X)$ and set $\mathcal{F} = \mathcal{O}_X(E)$. Then $\mathcal{F}$ is solely represented by $M_\mathcal{F}$ where $M_\mathcal{F}$ is any basis matrix of $\mathcal{F}(V_0)$ with respect to Ω^m_i.*

Proof. Following Lemma 4.2.6, we may represent $\mathcal{F}$ by the pair $(\mathcal{F}(V_0), \mathcal{F}(S))$. But since S is the disjoint union of the S_i, we have $\mathcal{F}(S) = \bigoplus_{i=1}^m \mathcal{F}_{|X_i}(S_i)$. Moreover, by assumption on $\mathcal{F}$, we have $\mathcal{F}_{|X_i}(S_i) = x^{r_i}\mathcal{O}_{S_i}$ and thus $(\mathcal{F}(V_0), r_1, \ldots, r_m)$ is enough to represent $\mathcal{F}$. Instead of representing $\mathcal{F}(V_0)$ via a $k[x]$-basis matrix with respect to Ω, we represent it with a basis matrix $M_\mathcal{F}$ with respect to Ω^m_i. Hence $\mathcal{F}$ is represented by $(M_\mathcal{F}, r_1, \ldots, r_m)$, and therefore we are left to argue that $M_\mathcal{F}$ already provides the integers $r_1, \ldots, r_m$. Due to Lemma 6.1.3, it is therefore enough to prove that we can compute a basis matrix of $\mathcal{F}_{|X_i}(V_{i,0})$ given $M_\mathcal{F}$. Finally, Proposition 4.6.5 shows that ComputeComponentMatrices exactly provides this feature. □

Remark 6.1.7. In the integral case the degree $\deg_k \mathcal{F}(V_0)$ can be determined by simply computing $\deg \det T_\mathcal{F}$, see Proposition D.2.7. But in the reducible case, we need to take care. By Proposition D.2.7, we have

$$\deg_k \mathcal{F}(V_0) = \deg \det M$$

where $M \in k(x)^{n\times n}$ is a basis transformation matrix from a basis of R_0 to one of $\mathcal{F}(V_0)$. The representation of $\mathcal{F}(V_0)$ by $M_\mathcal{F}$, a basis matrix with respect to Ω^m_i, does also provide $\deg_k \mathcal{F}(V_0)$ as follows: Let $\mathcal{B}$ denote the $k[x]$-basis of $\mathcal{F}(V_0)$. Since $\mathcal{F}(V_0) \subseteq R_0 \subseteq R_0^+$, we have

$$\mathcal{B} = \Omega \cdot M_{\Omega,\mathcal{F}}$$

for some matrix $M_{\Omega,\mathcal{F}} \in k[x]^{n\times n}$. Thus with $\Omega = \Omega^m_i \cdot T_\Omega$ we have

$$\mathcal{B} = \Omega^m_i \cdot T_\Omega \cdot M_{\Omega,\mathcal{F}}.$$

Now since $\mathcal{B} = \Omega^m_i \cdot M_\mathcal{F}$, this finally provides $M_\mathcal{F} = T_\Omega \cdot M_{\Omega,\mathcal{F}}$. In particular,

$$\deg \det M_\mathcal{F} = \deg \det T_\Omega + \deg \det M_{\Omega,\mathcal{F}}$$

and thus

$$\deg_k \mathcal{F}(V_0) = \deg \det M_{\Omega,\mathcal{F}} = \deg \det M_{\mathcal{F}} - \deg \det T_\Omega.$$

Note that $\deg \det T_\Omega$ can be precomputed. Moreover, by Lemma B.4.11, we have

$$\deg \det T_\Omega = \dim_k R_0^+/\tau^\#(V_0)(R_0)$$

where $\tau : \mathcal{O}_X \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{O}_{X_i}$ is the canonical monomorphism from Definition B.3.4. Since X is a cover of $\mathbb{P}^1_k$, we have $\operatorname{Supp} \mathscr{S}_X \subseteq V_0$ and thus, by Definition B.3.4, we have $\chi(\mathscr{S}_X) = \dim_k \mathscr{S}_X(X) = \dim_k R_0^+/\tau^\#(V_0)(R_0)$ where the first equality is due to the fact that $\mathscr{S}_X$ is a skyscraper sheaf. Therefore

$$\deg_k \mathcal{F}(V_0) = \deg \det M_{\mathcal{F}} - \chi(\mathscr{S}_X). \qquad \triangle$$

Remark 6.1.7 tells us that the degree will be computed in different ways dependent on with respect to which basis the given basis matrix represents $\mathcal{F}(V_0)$. Algorithm 9 provides the functionality of computing the degree of an R_0-ideal accordingly.

Algorithm 9 Computing the degree of an R_0-ideal

Precomputed	Ω fixed basis of R_0; Ω_i^m fixed basis of R_0^+; $\chi(\mathscr{S}_X)$
Input	M_I basis matrix of the ideal I; c Boolean whether M_I is a basis matrix with respect to Ω_i^m ($c = \mathit{true}$) or with respect to Ω ($c = \mathit{false}$)
Output	$\deg_k I$

1: **procedure** DegOfIdeal(M_I, c)
2: $d \leftarrow$ Degree(Determinant(M_I))
3: **if** c **then**
4: **return** $d - \chi(\mathscr{S}_X)$
5: **return** d

Lemma 6.1.8. *The algorithm* DegOfIdeal*, see Algorithm 9, is correct. Moreover, if d is an upper bound of the degree of M_I, then* DegOfIdeal *requires at most $O^\sim(n^\omega d)$ operations in k.*

Proof. The correctness of DegOfIdeal was discussed in Remark 6.1.7. The running time assertion follows from Notation A.1.1. □

Regarding the representation of an element in $\mathcal{I}_\pi$ we want to treat the modification functions, that is the elements in $\mathcal{P}_\pi$, differently.

Notation 6.1.9. Let $f \in R_0$ be a modification function, that is $fR_0 \in \mathcal{P}_\pi$. Let c be a Boolean encoding whether basis matrices of R_0-ideals are given with respect to Ω_i^m ($c = \mathit{true}$) or with respect to Ω ($c = \mathit{false}$). We assume the matrix $T_f := T_{fR_0}$ to be the basis matrix of the standard basis $f\Omega = (f\omega_1, \ldots, f\omega_n)$ with respect to

$$\begin{cases} \Omega, & \text{if } c = \mathit{false} \\ \Omega_i^m, & \text{if } c = \mathit{true}. \end{cases}$$

By Corollary 4.6.11, if $\deg \phi_\Omega(f) \leq d$, then $\deg T_f \leq d + 3c_X$ in the case $c = \mathit{true}$. By Lemma 4.3.34 and Corollary 4.5.2, the same bound holds in the case $c = \mathit{false}$. $\triangle$

6.1.3 Strategy

To carry out the group law in $\mathrm{CaCl}^0_\pi(X)$, we thus need to work basis matrices $M_\mathcal{F}$ over $k[x]$ of $\mathcal{F}(V_0)$ for which we know that they represent $\mathcal{F} = \mathcal{O}_X(E)$ for some representative $E = D + \sum_{i\in A} r_i(x)_{i,\infty}$ of a class in $\mathrm{CaCl}^0_\pi(X)$. Since $\mathrm{CaCl}^0_\pi(X) \to \mathcal{I}_\pi/\mathcal{P}_\pi$, $E \mapsto \mathcal{O}_X(E)(V_0)$ is an isomorphism of abelian groups, see Proposition 5.6.22 and Corollary 5.6.23, this is the same as to carry out the group law in $\mathcal{I}_\pi/\mathcal{P}_\pi$. The basis matrix $M_\mathcal{F}$ obviously represents the ideal $I = \mathcal{F}(V_0)$. Now the addition in $\mathrm{CaCl}^0_\pi(X)$ corresponds under ϕ to the multiplication in $\mathcal{I}_\pi/\mathcal{P}_\pi$ and being the neutral element in both groups is equivalent to have a principal representative. We will compute in $\mathcal{I}_\pi/\mathcal{P}_\pi$ using the matrices $M_\mathcal{F}$ which we might denote by M_I instead. Now to carry out the group law in $\mathcal{I}_\pi/\mathcal{P}_\pi$ means to be able to compute the product of two ideal classes given by some matrices T_1 and T_2 as above and then represent the product again as some matrix T_3 representing the result after applying the group law. Moreover, we need to do the same for the inverse of a class, which is given by the inverse of the ideal representative. And, finally, we need to be able to test whether the class a given pair represents is the trivial class which is the case if and only if the representative ideal lies in $\mathcal{P}_\pi$.

The main strategy we will pursue is the following:

Strategy 6.1.10. *Due to computational speed up, instead of computing the product, we compute the quotient of ideals in $\mathcal{I}_\pi$. If we are able to do this, we can compute the inverse of an element in $\mathcal{I}_\pi/\mathcal{P}_\pi$ as well. We will achieve this by the following steps:*

(I) The first step is to compute the quotient of J over I for which we know that the result $(J : I)$ satisfies $(J : I) \subseteq R_0$.

(II) The second step is to compute arbitrary quotients I over J by modifying with a suitable modification function f which makes the quotient integral again, that is $(fJ : I) \subseteq R_0$. To do so, we need to be able to compute the basis matrix of the standard basis of a principal R_0-ideal.

(III) After computing a quotient, the degree of the considered ideals may have grown and thus we need to come up with a method choosing a representative which has degree bounded by some invariants of X.

(IV) Finally, we need to introduce a method for deciding whether two given ideals represent the same class, or equivalently, whether a given ideal represents the trivial class.

Basically, we have already treated the theory behind Items (III) and (IV) in Sections 5.8 and 5.9 and we will simply write down the respective algorithms implementing the methods provided there. The algorithm that reduces the representative of a given class is given in Algorithm 20. Therefore, we are primarily left to come up with linear algebra algorithms that implement Items (I) and (II). Item (I) will be treated next in Section 6.2 and the computation of the basis matrices of principal ideals given by modification functions is examined in Section 6.3 which will provide Item (II).

6.2 Quotients of Ideals and Ideal Generating Sets

6.2.1 Quotients of Free Ideals

In this subsection we provide a lemma which shows how to compute a basis of the quotient of two ideals efficiently only given their respective bases. Since the procedure is not specifically dependent on our setup, we will consider the following situation:

Notation 6.2.1. Let R be a reduced ring such that all R-ideals are free of rank n over some ring A. For instance, this is the case if $R = R_0 = \mathcal{O}_X(V_0)$ where X is a reduced cover of $\mathbb{P}^1_k$ of degree n over $\mathbb{P}^1_k$. We fix some A-basis $\Omega = (\omega_1, \dots, \omega_n)$ of R. By $\phi_\Omega(f)$ we denote the coefficient vector of $f \in R$ with regards to Ω. Mostly, we will work with $A = k[x]$. △

Since we will use ideal generating sets instead of $A = k[x]$-bases, we need to be able to check whether a given set of elements of an ideal is actually an ideal generating set.

Lemma 6.2.2. *Let $f_1, \dots, f_h \in \mathrm{Frac}(R)$ be elements with $\deg \phi_\Omega(f_i), \deg T_{f_i} \leq d$ such that at least one $f_i R$ is invertible. Let $G = \sum_{i=1}^h f_i R$. Let $T = [T_{f_1} \mid \dots \mid T_{f_h}]$ denote the concatenated matrix of dimension $n \times hn$. Then G is an R-ideal, free of rank n over $k[x]$ and there exists a basis matrix T_G of G with degree bounded by d which is given by*

$$T_G = \textsc{ColumnBasis}(T) \in k[x]^{n \times n}.$$

Proof. First of all, since one of the $f_i R$ is invertible, the respective element f_i is a regular one and therefore G contains a regular element of R. By Proposition C.1.10, we therefore see that G is an R-ideal. Moreover, by Lemma 4.1.6, G is free of rank n over $k[x]$. Let $T = [T_{f_1} \mid \dots \mid T_{f_h}]$ denote the concatenated matrix of dimension $n \times hn$. Then, by construction, the column space of T is the $k[x]$-span of

$$\{f_i \omega_j \mid i = 1, \dots, h, j = 1, \dots, n\}$$

and thus equal to G. Hence the column space of T over $k[x]$ has rank n. By Theorem A.2.15,

$$T_G := \textsc{ColumnBasis}(T) \in k[x]^{n \times n}$$

is a basis matrix of the column space of T and its degree is bounded by the average column degree of T which is, by assumption, upper bounded by d. □

The next statement gives us a tool to test whether (randomly chosen) elements of an ideal constitute a generating system.

Lemma 6.2.3. *Let $J \subseteq I$ be two integral ideals of R_0, then $J = I$ if and only if $\deg_k J = \deg_k I$.*

Proof. The only if part is trivial. Therefore, let us assume $\deg_k J = \deg_k I$ and $J \subseteq I$. The latter implies that each basis of J can be represented by a basis of I. In terms of basis matrices this means that for all basis matrices M_I, M_J there is $T \in k[x]^{n \times n}$ such that $\Omega \cdot M_J = \Omega \cdot M_I \cdot T$. This implies $\deg_k I = \deg_k J + \deg \det(T)$ by Proposition D.2.7 Thus, by assumption, $\deg \det(T) = 0$ which is $\det(T) \in k$. Since M_J is invertible, $\det(T) \neq 0$. Thus $\det(T) \in k^\times$, that is, T is unimodular and hence $J = I$. □

Now we can use Lemmas 6.2.2 and 6.2.3 to provide an algorithm that test whether a given set of elements in an ideal constitute an ideal generating set of that ideal. Since we will use it for our algorithms that provide a toolkit to compute in $\mathrm{Pic}^0(X)$, we will formulate it for the two cases, the component independent and the component dependent. But it also works in the general setting described in Notation 6.2.1

Algorithm 10 Test for ideal generating set

Precomputed	Ω fixed basis of R_0; Ω_i^m fixed basis of R_0^+
Input	T_I basis matrix of I; $T_{\beta_1}, \dots, T_{\beta_h} \in k[x]^{n\times n}$ basis matrices of $\beta_i R$ such that $\beta_i \in I$; c Boolean whether T_I, T_{β_i} are basis matrices with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$)
Output	*true* if $I = \sum_{i=1}^h \beta_i R$, otherwise *false*

1: **procedure** TestIGS($T_I, T_{\beta_1}, \dots, T_{\beta_h}, c$)
2: $d_I = \text{DegOfIdeal}(T_I, c)$
3: $T_\beta = \text{ColumnBasis}(T_{\beta_1} \frown \dots \frown T_{\beta_h})$
4: $d_\beta = \text{DegOfIdeal}(T_\beta, c)$
5: **if** $d_I = d_\beta$ **then**
6: **return** *true*
7: **return** *false*

Lemma 6.2.4. *The algorithm* TestIGS*, see Algorithm 10, is correct if one of the $\beta_i R$ is invertible. Moreover, if d is a common bound for the degrees of the input matrices and $h \in O^\sim(1)$, then* TestIGS *requires at most $O^\sim(n^\omega d)$ operations in k.*

Proof. By assumption, $G = \sum_{i=1}^h \beta_i R \subseteq I$ and thus $G = I$ if and only if $\deg_k G = \deg_k I$, see Lemma 6.2.3. Since one of the $\beta_i R$ is invertible, ColumnBasis in line 3 does indeed compute a basis matrix T_G of G, see Lemma 6.2.2. By Lemma 6.1.8, DegOfIdeal in line 2 and 4 computes $d_I = \deg_k I$ respectively $d_\beta = \deg_k G$. Hence the correctness of TestIGS follows.

By assumption, d is a common upper bound for the degrees of all T_{β_i}, and thus Lemma 6.2.2 provides that T_β has degree bounded by d (it is even bounded by the average column degree of all the columns of the T_{β_i}). By Theorem A.2.15, we know that ColumnBasis in line 3 requires at most $O^\sim(n^{\omega-1}(hn)s)$ operations in k where $h \in O^\sim(1)$ by assumption and s is the average column degree of all the columns of the T_{β_i} which is bounded by d. In particular, ColumnBasis only requires $O^\sim(n^\omega d)$ operations in k. By Lemma 6.1.8, DegOfIdeal in line 2 and 4 requires at most $O^\sim(n^\omega d)$ operations in k since d is an upper bound of the input matrices. Hence TestIGS requires overall at most $O^\sim(n^\omega d)$ operations in k as asserted. □

To compute a basis of the integral quotient of two R-ideals, the following lemma represents the main statement we will use. The main idea is to switch from a basis (whose cardinality is n) of the denominator to an ideal generating system with asymptotically negligible cardinality (e.g. $\log(n)$). For the definition of the R-ideal quotient, see Definition C.1.5.

Proposition 6.2.5. *Let I, J be two integral R-ideals and let $\beta_1, \dots, \beta_h$ be an ideal generating set of I. Let T_J denote the basis matrix of the ideal J and for all $i = 1, \dots, h$ let T_{β_i} denote the standard basis matrix of $\beta_i R$. Then for every $f \in R_0$ the following equivalence holds:*

$$f \in (J : I) \Leftrightarrow \exists\ \mu_1, \dots, \mu_h \in A^n : \underbrace{\begin{pmatrix} T_{\beta_1} & T_J & 0 & \dots & 0 \\ T_{\beta_2} & 0 & T_J & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & 0 \\ T_{\beta_h} & 0 & \dots & 0 & T_J \end{pmatrix}}_{=:\ M(J,\beta_1,\dots,\beta_h)} \begin{pmatrix} \phi_\Omega(f) \\ \mu_1 \\ \vdots \\ \mu_h \end{pmatrix} = 0$$

Proof. By Definition C.1.5, $f \in (J : I)$ holds if and only if $fI \subseteq J$ and the latter is equivalent to $f\beta_i \in J$ for all $i = 1, \dots, h$ since $\beta_1, \dots, \beta_h$ is an ideal generating set of

I. The product $f\beta_i$ satisfies $\phi_\Omega(f\beta_i) = T_{\beta_i} \cdot \phi_\Omega(f)$. Indeed, column j of T_{β_i} contains the coefficients of $\beta_i\omega_j$ with respect to Ω. If we write $f = \sum_{j=1}^n \lambda_j\omega_j$ with $\lambda_j \in A$, then $f\beta_i = \sum_{j=1}^n \lambda_j\beta_j\omega_j$ as claimed. Now $f\beta_i \in J$ if and only if the equation $T_{\beta_i} \cdot \phi_\Omega(f) = T_J \cdot \mu_i$ has a solution $\mu_i \in A^n$. This already provides the assertion since the matrix equation formulates this for all $i = 1, \dots, h$ simultaneously. □

Definition 6.2.6. In the following we will denote the big matrix in Proposition 6.2.5 by $M = M(J, \beta_1, \dots, \beta_h)$. In Notation A.1.1 (vii) we define the algorithm BigMatrix that builds the *big matrix* M from above and which we will use in the rest of this thesis. △

Lemma 6.2.7. *Let the situation be as in Proposition 6.2.5. The kernel of the matrix $M = M(J, \beta_1, \dots, \beta_h)$ from Proposition 6.2.5 has rank n over A.*

Proof. Since the $hn \times hn$ diagonal submatrix of M built by the M_J has full rank and the number of rows of M is equal to hn, we obtain that M has rank hn. We can now use the rank-nullity theorem for free modules over principal ideal domains (which is a direct consequence of the facts that submodules of free modules over principal ideal domains are free again and that short exact sequences whose last (non-zero) module is free is split, see [Hun11, Thms. 3.4. and 6.1]) to see that $(h+1)n = \operatorname{rk}\ker M + \operatorname{rk} M$ and therefore $\operatorname{rk}\ker M = (h+1)n - hn = n$. □

Corollary 6.2.8. *As an A-module, the kernel of the big matrix $M = M(J, \beta_1, \dots, \beta_h)$ of Proposition 6.2.5 is of the form $\ker(M) = \{(\lambda\ \mu_1 \cdots \mu_h)^T \in A^{(h+1)n} \mid T_{\beta_i} \cdot \lambda = -T_J \cdot \mu_i\}$. The μ_i are the coefficient vectors of $f\beta_i$ in terms of the basis of J given by T_J. The top $(n \times n)$-matrix of a basis of $\ker(M)$ provides a basis matrix $T_{(J:I)}$ of $(J : I)$. Conversely, any basis matrix $T_{(J:I)}$ of $(J : I)$ provides a possible configuration of the top $(n \times n)$-matrix of a basis of $\ker(M)$.*

Proof. The proof of Proposition 6.2.5 shows the first two assumptions. We denote the column vectors of a basis of $\ker M$ by $g_j = (\lambda_j\ \mu_{1j}\ \dots\ \mu_{hj})^T$ for $j = 1, \dots, n$. Then, by Proposition 6.2.5, for every element α of $(J : I)$ there are $a_1, \dots, a_n \in A$ such that $\phi_\Omega(\alpha)$ is equal to the $(n \times 1)$-vector obtained by taking the top n entries of $\sum_{j=1}^n a_j g_j$. Thus $\lambda_1 \dots \lambda_n$ generate $(J : I)$ over A. By Lemma 6.2.7, the g_j are A-linearly independent. Assume there is a non-trivial linear combination $0 = \sum_{j=1}^n a_j\lambda_j$. By the second assertion, the latter hn entries of $\sum_{j=1}^n a_i g_j$ are the coefficients of $(\sum_{j=1}^n a_j\lambda_j)\beta_i = 0$ for all $i = 1, \dots, h$ with respect to the basis of J given by T_J and hence zero. That is, we also have $\sum_{j=1}^n a_i g_j = 0$ which provides $a_i = 0$ for all $i = 1, \dots, n$. Therefore $\lambda_1, \dots, \lambda_n$ is an A-basis of $(J : I)$. The converse statement is trivial. □

We can use Proposition 6.2.5 and Corollary 6.2.8 to provide an algorithm that computes a basis matrix of the quotient ideal of two R-ideals. It works in the general setting that is described in Notation 6.2.1 where $A = k[x]$.

Algorithm 11 Compute ideal quotient which is integral

Input	$T_J, T_f, T_{\beta_1}, \dots T_{\beta_h} \in k[x]^{n\times n}$ basis matrices of ideals $J, fR_0, \beta_1R_0, \dots, \beta_hR_0$, respectively
Output	$T_H \in k[x]^{n\times n}$ basis matrix of $H = (J : I)$ with $I = fR_0 + \sum_{i=1}^h \beta_iR_0$

1: **procedure** IdealQuotient($T_J, T_f, T_{\beta_1}, \dots T_{\beta_h}$)
2: $M \leftarrow$ BigMatrix($T_f, T_{\beta_1}, \dots, T_{\beta_h}, T_J$)
3: $K \leftarrow$ MatrixKernel(N)
4: $T_H \leftarrow$ RedMat(SubMatrix($K, (1,1), (n,n)$))
5: **return** T_H

Lemma 6.2.9. *The algorithm* IdealQuotient*, see Algorithm 11, is correct. If* $h \in O^{\sim}(1)$ *and* d *is an upper bound for both the degree of the input matrices and the minimal degree of basis matrices representing the kernel of* M*, then it requires at most* $O^{\sim}(n^{\omega}d)$ *operations in* k *and returns a matrix with degree in* $O(d)$*.*

Proof. That T_H is the asserted basis matrix of $(J : I)$ if $I = fR_0 + \sum_{i=1}^{h} \beta_i R_0$ follows from Corollary 6.2.8. This proves the correctness of IdealQuotient. By assumption, d is a bound for the minimal degree of basis matrices representing the kernel of M and thus for K as well, see Theorem A.2.6. By Theorem A.2.7, RedMat returns a matrix which also has degree bounded by d which proves the asserted degree of the output matrix.

Building the big matrix from Proposition 6.2.5 with BigMatrix has constant cost, see Lemma A.1.2 (vii). By Theorem A.2.6, the computation of K in step 3 requires at most $O^{\sim}(n^{\omega}d)$ operations in k and by assumption $\deg(K) \leq d$. Moreover, by Lemma A.1.2 (vi), SubMatrix has constant cost. Therefore, IdealQuotient requires overall at most $O^{\sim}(n^{\omega}d)$ operations in k. □

Therefore, to use IdealQuotient properly, we need to prove that for given J and I (by the ideal generating set $\beta_1, \ldots, \beta_h$) there is a basis of $\ker M(J, \beta_1, \ldots, \beta_h)$ that has degree in the same order of magnitude as a basis matrix $T_{(J:I)}$ of a reduced basis of $(J : I)$ does. We distinguish between the component independent and component dependent case.

Lemma 6.2.10. *Let* X *be a reduced cover of* $\mathbb{P}^1_k$*. Let* $J, I \in \mathcal{I}_\pi$ *be integral* R_0*-ideals with* $\deg_k I, \deg_k J \equiv 0 \bmod n$ *such that* $(J : I) \subseteq R_0$ *is integral again. Assume that* T_J *is reduced and has degree bounded by* d*. Let* $\beta_1, \ldots, \beta_h$ *be elements in* I *with* $\deg \phi_\Omega(\beta_i) \leq d$ *and* $I = \sum_{i=1}^{h} \beta_i R_0$*. Then there exists a basis matrix* $N \in k[x]^{hn \times n}$ *with degree in bounded by* $2d + (\mu_X + 2)c_X$ *representing the kernel of the big matrix* M *in Proposition 6.2.5 whose top* $(n \times n)$*-matrix is a basis matrix of* $(J : I)$ *which itself is degree upper bounded by* $d + \mu_X c_X$*.*

Proof. By Corollary 6.2.8, we know that every basis matrix $T_{(J:I)}$ of a basis $\delta_1, \ldots, \delta_n$ of $(J : I)$ together with the coefficients of $\beta_i \delta_j$ with regards to the basis of J represented by T_J provides a possible basis matrix of $\ker M(J, \beta_1, \ldots, \beta_h)$. By Definition C.1.5, we know that $(J : I)$ is an R_0-ideal and the same is true for $I^{-1} = (R_0 : I)$. Moreover, since $I \subseteq R_0$, we have by definition $I \subseteq R_0 \subseteq I^{-1}$ and thus from Lemma C.1.27, we obtain $\deg_k I^{-1} \leq 0$. Since J is invertible, Proposition C.1.26 provides

$$\deg_k(J : I) = \deg_k JI^{-1} = \deg_k J + \deg_k I^{-1} \leq \deg_k J.$$

Hence $\deg_k(J : I) \leq \deg \det T_J \leq dn$. By Corollaries 4.3.27 and 4.5.4, we know that there is a basis matrix $T_{(J:I)}$ of $(J : I)$ with

$$\deg(T_{(J:I)}) \leq \underbrace{\deg_k((J : I))/n}_{\leq d} + \mu_X c_X \leq d + \mu_X c_X.$$

By assumption, we have $\deg \phi_\Omega(\beta_i) \leq d$. Let $\delta_1, \ldots, \delta_n$ denote the basis of $(J : I)$ represented by the matrix $T_{(J:I)}$. Thus $\deg \phi_\Omega(\delta_j) \leq d + \mu_X c_X$. By Lemma 4.3.32, we have

$$\deg^*(\beta_i \delta_j) + |X|_n \leq \deg \phi_\Omega(\beta_i \delta_j) \leq \deg^*(\beta_i \delta_j),$$

and, by Corollary 4.3.31 (iii), we have $\deg^*(\beta_i \delta_j) \leq \deg^*(\beta_i) + \deg^*(\delta_j)$. Combining these two and Corollary 4.3.24 we obtain

$$\deg \phi_\Omega(\beta_i \delta_j) \leq \deg \phi_\Omega(\beta_i) + \deg \phi_\Omega(\delta_j) + 2c_X \leq 2d + (\mu_X + 2)c_X.$$

The coefficients of $\beta_i\delta_j$ with respect to the basis $\mathcal{B}$ of J represented by M_J satisfy

$$M_J \cdot \phi_{\mathcal{B}}(\beta_i\delta_j) = \phi_\Omega(\beta_i\delta_j).$$

We write $M_J = (v_1 \dots v_n)$ with $v_j \in k[x]^n$ as well as $\phi_{\mathcal{B}}(\beta_i\delta_j) = (\lambda_1, \dots, \lambda_n)^T$ and $\phi_\Omega(\beta_i\delta_j) = (\mu_1, \dots, \mu_n)^T$. Now we know that M_J is reduced and hence

$$\deg \mu_i = \max_{j=1}^{n}\{\deg(\lambda_j v_j)\} = \max_{j:\lambda_j \neq 0}\{\deg(\lambda_j) + \deg(v_j)\}.$$

By assumption, $\deg M_J \leq d$ and thus $\deg(v_j) \leq d$. Moreover, we have shown that $\deg(\mu_j) \leq 2d + (\mu_X + 2)c_X$. Therefore, $\deg(\lambda_j) \leq 2d + (\mu_X + 2)c_X$ as well. Therefore, we have found a possible basis matrix of $\ker M$ where its top $(n \times n)$-matrix has degree bounded by $d + \mu_X c_X$ and the lower $(hn \times n)$-matrix has degree bounded by $2d + (\mu_X + 2)c_X$. □

Remark 6.2.11. Note that the proof of Lemma 6.2.10 shows that I need not be invertible. It suffices that $I = \mathcal{F}(V_0)$ for some degree zero $\mathcal{O}_X$-ideal $\mathcal{F}$ with $\mathcal{F}(S) = x^r\mathcal{O}_S$ and $r = (\deg_k I)/n \in \mathbb{Z}$. Moreover, we can even circumvent to assume that J is invertible. The proof shows that it suffices that $\deg_k(J : I) \leq \deg_k J$ holds. One can prove that the R-ideal $(J : I)$ satisfies $(J : I) \supseteq J \cdot (R : I) \supseteq J$ since $I \subseteq R$ and thus we can apply Lemma C.1.27 to obtain $\deg_k(J : I) \leq \deg_k J$. △

Lemma 6.2.12. *Let X be a reducible and reduced cover of $\mathbb{P}^1_k$ with irreducible components $(X_1, \dots, X_m)$. Let $J, I \in \mathcal{I}_\pi$ be integral ideals such that $(J : I)$ is integral again. Assume that there are basis matrices T_{J_i} respectively T_{I_i} of all J_i respectively I_i with degree bounded by d. Moreover, assume that both M_I and M_J are reduced and have degree bounded by d as well. Let $\beta_1, \dots, \beta_h$ be elements of I with $\deg \phi_{\Omega_i^m}(\beta_j) \leq d$ and $I = \sum_{j=1}^h \beta_j R_0$. Then there exists a basis matrix with degree bounded by $2d + 3c_X$ representing the kernel of the big matrix M in Proposition 6.2.5 whose top $(n \times n)$-matrix is a basis matrix of $(J : I)$ which itself is degree upper bounded by $d + c_X$.*

Proof. The proof works completely analogous to that of Lemma 6.2.10. We only need to cite the appropriate statements for degree bounds in the reducible case.

As in the proof of Lemma 6.2.10 we have $0 \leq \deg_k J_i I_i^{-1} \leq \deg_k J_i \leq dn_i$. By Proposition 4.4.20, this provides the existence of a basis matrix $M_{(J:I)}$ with degree bounded by $d + c_X$. Let $\delta_1, \dots, \delta_n$ denote the basis of $(J : I)$ represented by the matrix $M_{(J:I)}$. Thus $\deg \phi_{\Omega_i^m}(\delta_j) \leq d + c_X$. Hence, by Lemma 4.6.10, we have

$$\begin{aligned}\deg \phi_{\Omega_i^m}(\beta_i\delta_j) &\leq \deg \phi_{\Omega_i^m}(\beta_i) + \deg \phi_{\Omega_i^m}(\delta_j) + 2c_X \\ &\leq d + (d + c_X) + 2c_X \\ &= 2d + 3c_X.\end{aligned}$$

Again, we have $M_J \cdot \phi_{\mathcal{B}}(\beta_i\delta_j) = \phi_{\Omega_i^m}(\beta_i\delta_j)$ and thus the very same argument using the reducedness of M_J as in Lemma 6.2.10 provides the assertion. □

Remark 6.2.13. Note that the proof of Lemma 6.2.12 shows that I need not necessarily be invertible. It suffices that $I = \mathcal{F}(V_0)$ for some degree zero $\mathcal{O}_X$-ideal $\mathcal{F}$ with $\mathcal{F}(S) = \bigoplus_{i=1}^m x^{r_i}\mathcal{O}_{S_i}$ and $\mathcal{F}_P = \mathcal{O}_{X,P}$ for all $P \in \mathrm{Supp}(\mathscr{S}_X)$. In particular, $\deg_k I_i \equiv 0 \bmod n_i$ is necessary. △

Corollary 6.2.14. *If d is an upper bound of the input matrices of Algorithm 11 and $c_X \in O(d)$, then Lemma 6.2.9 can be more precise: The required number of operations in k are still $O^\sim(n^\omega d)$, but the output matrix has degree bounded by $d + \mu_x c_X$.*

Proof. This follows from combining Lemmas 6.2.10 and 6.2.12 with Lemma 6.2.9. □

Let the situation be as in Notation 6.2.1.

Lemma 6.2.15. *Let I be an R-ideal with basis matrix T_I and let $f \in R$ be regular such that fR has basis matrix T_f. Then $T_{fI} := T_I \cdot T_f$ is a basis matrix of fI.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ denote the basis of I represented by T_I. Then $f\alpha_1, \ldots, f\alpha_n$ is a $k[x]$-basis of fI. Moreover, if $\alpha_j = \sum_{i=1}^n \lambda_{i,j}\omega_i$, then $f\alpha_j = \sum_{i=1}^n \lambda_{i,j} f\omega_i$. By definition, the coefficients of $f\omega_i$ with regards to $\omega_1, \ldots, \omega_n$ form the columns of T_f, and we have $T_I = (\lambda_{i,j})_{i,j} \in k[x]^{n\times n}$. Hence the j-th column of the product $T_I \cdot T_f$ contains the coefficients of $f\alpha_j$ which proves the assertion. □

6.2.2 Ideal Generating Sets

We want to use Proposition 6.2.5 to compute a basis of $(J : I)$ explicitly and hence we need a method to come up with a generating system of an integral invertible ideal.

Let $I \subseteq R_0$ be an invertible ideal and $s_1, \ldots, s_h \in I$. We can characterise whether the s_i are an ideal generating set of I or not by the "zeros of the s_i relative to I".

Definition 6.2.16. Let $I \subseteq R$ be an invertible ideal. For $f \in I$ we say that f **has a zero at** $P \in \operatorname{Spec}(R)$ **relative to** I if $f \in IP$. For any subset $T \subseteq R$ we call the set $V_I(T) = \{P \in \operatorname{Spec}(R) \mid T \subseteq PI\}$ the set of **common zeros of** T **relative to** I. △

Lemma 6.2.17. *Let $I \subseteq R$ be an invertible ideal. Let $s_1, \ldots, s_h \in I$ be arbitrary. Then $s_1, \ldots, s_h$ form a generating set of I if and only if they do not share a common zero relative to I.*

Proof. Let J denote the ideal generated by $s_1, \ldots, s_h$. Assume that $J = I$ and assume there is P such that $J \subseteq PI$, then $R = JI^{-1} \subseteq P$, a contradiction. Conversely, let $s_1, \ldots, s_n$ do not have any common zero relative to I, that is for all $P \in \operatorname{Spec}(R)$ we have $J \not\subset PI$ and therefore $JI^{-1} \not\subset P$. That is JI^{-1} is an integral ideal not contained in any prime ideal and therefore, by Zorn's lemma, it must be equal to R, hence $J = I$. □

Definition 6.2.18. Let W be a k-vector space of dimension n and let $\Sigma \subseteq k$ be a finite subset of the ground field k. Fix a k-basis $w_1, \ldots, w_n$ of W. Now a **Σ-random element** $s \in W$ or an element $s \in W$ which is chosen **Σ-randomly** is a linear combination $s = a_1 w_1 + \ldots + a_n w_n$ where the $a_i \in \Sigma$ are chosen independently and uniformly random from Σ. In the following, $\Pr(S)$ denotes the probability of the statement S to be true. △

Lemma 6.2.19 ([KM07], Lemma 4.2)**.** *Let W be a k-vector space with basis $w_1, \ldots, w_n$. Let $\Sigma \subseteq k$ be a finite subset of k and let $H_1, \ldots, H_r \subsetneq W$ be proper subspaces.*

(1) For a Σ-random element $s \in W$, $\Pr(s \in H_1 \cup \ldots \cup H_r) \leq r/\#\Sigma$.

(2) For a tuple $s_1, \ldots, s_j \in W^j$ of independent Σ-random elements $s_1, \ldots, s_j \in W$,

$$\Pr((s_1, \ldots, s_j) \in H_1^j \cup \ldots \cup H_r^j) \leq r/(\#\Sigma)^j.$$

Proposition 6.2.20. *Let R be a noetherian k-algebra of Krull dimension one. Let I be an invertible ideal of R and $f \in I$ a regular element. Then the set $V_I(f)$ of common zeros of f relative to I is finite, say $r = \#V_I(f)$. Let $\Sigma \subseteq k$ denote a finite set. Let $f_1, \ldots, f_h$ be Σ-randomly chosen elements. Then the probability that $f, f_1, \ldots, f_h$ form an ideal generating set of I is at least $1 - r/(\#\Sigma)^h$, that is*

$$\operatorname{Prob}\left(fR + \sum\nolimits_{i=1}^{h} f_i R = I\right) \geq 1 - r/(\#\Sigma)^h.$$

Proof. We obviously have $V_I(f) \subseteq V(f) = \{P \in \operatorname{Spec}(R) \mid T \subseteq P\}$. Since f is a regular element of R, by Corollary B.4.14, it cannot be contained in one of the minimal prime ideals of R. In particular, the Krull dimension of R/fR is zero. Since noetherian rings of Krull dimension zero have finite spectrum, see [Sta18, Tag 00KJ], $V(f)$ and a fortiori $V_I(f)$ is finite. Let $V_I(f) = \{P_1, \ldots, P_r\}$.

Let B be a finite ideal generating set of I and set $W = \operatorname{Span}_k(B)$. Then $B \not\subseteq IP_i$ since any ideal generating set does not share a common zero relative to I, see Lemma 6.2.17. Set $H_i = W \cap IP_i$. Now if $H_i = W$, then $B \subseteq W \subseteq IP_i$ which is a contradiction to what we have said above. Moreover, since IP_i are ideals of R, the H_i are indeed k-subvector spaces of W. Note that by definition, $H_1 \cup \ldots \cup H_r$ is the set of elements of W that share a common zero with f relative to I. By Lemma 6.2.17, for any $s \in W$ the pair f, s generates I if and only if the elements in f and s do not share a common zero relative to I. By the above, this is equivalent to $s \notin H_1 \cup \ldots \cup H_r$. Analogously, for every $f_1, \ldots, f_h \in W$, f together with $f_1, \ldots, f_h$ generate I if and only if $(f_1, \ldots, f_h) \notin H_1^h \cup \ldots \cup H_r^h$.

Let $f_1, \ldots, f_h \in W$ be Σ-randomly chosen. Then, by Lemma 6.2.19, we have

$$\operatorname{Prob}((f_1, \ldots, f_h) \in H_1^h \cup \ldots \cup H_r^h \leq r/(\#\Sigma)^h$$

and thus equivalently

$$\operatorname{Prob}((f_1, \ldots, f_h) \notin H_1^h \cup \ldots \cup H_r^h \geq 1 - r/(\#\Sigma)^h.$$

This yields $\operatorname{Prob}(fR + \sum_{i=1}^h f_i R = I) \geq 1 - r/(\#\Sigma)^h$ as asserted. □

Lemma 6.2.21. *Let R be a noetherian k-algebra of Krull dimension one. Let $f \in R$ be regular. Then $\#V(f) \leq \dim_k R/fR$.*

Proof. By Corollary B.4.14, f is not contained in any of the minimal prime ideals of R and thus R/fR has Krull dimension zero. Therefore $V(f)$ is finite, see [Sta18, Tag 00KJ]. Let $V(f) = \{P_1, \ldots, P_r\}$ and set $Q = \bigcap_{i=1}^r P_i$. Then $f \in Q$ and thus $R/fR \to R/Q$ is a surjection and therefore $\dim_k R/fR \geq \dim_k R/Q$. Since all elements of $V(f)$ are maximal, they are pairwise coprime and thus the Chinese Remainder Theorem provides

$$R/Q \cong \prod_{i=1}^r R/P_i$$

and since we have an injection $k \hookrightarrow R/P_i$ this already provides $r \leq \dim_k R/Q$ and hence the assertion follows. □

Corollary 6.2.22. *Let the situation be as in Proposition 6.2.20. Then*

$$\operatorname{Prob}(fR + \sum_{i=1}^h f_i R = I) \geq 1 - \frac{\dim_k R/fR}{(\#\Sigma)^h}.$$

Moreover, for every η such that $0 < \eta < 1$ we set

$$h = \left\lceil \frac{\log(\dim_k R/fR) - \log(\eta)}{\log(\#\Sigma)} \right\rceil.$$

Then $\operatorname{Prob}(fR + \sum_{i=1}^h f_i R = I) \geq 1 - \eta$.

Proof. The first assertion follows directly from Proposition 6.2.20, together with Lemma 6.2.21. Due to the first assertion, proving the second assertion reduces to prove

$$1 - \frac{\dim_k R/fR}{(\#\Sigma)^h} \geq 1 - \eta \tag{2:1}$$

for the asserted choice of h. Obviously, Eq. (2:1) is equivalent to

$$\eta \geq \frac{\dim_k R/fR}{(\#\Sigma)^h}.$$

Rearranging provides $(\#\Sigma)^h \geq (\dim_k R/fR)/\eta$ and then taking the logarithm for fixed base shows that Eq. (2:1) is equivalent to

$$h \cdot \log(\#\Sigma) \geq \log(\dim_k R/fR) - \log(\eta)$$

which finally provides the second assertion as well. □

Corollary 6.2.23. *Let the situation be as in Proposition 6.2.20. We consider the following three cases:*

(i) Let $\Sigma = \{0,1\}$. Choosing $h = \lceil \log_2(\dim_k(R/fR)) + r \rceil$ many Σ-random linear combinations $f_1, \ldots, f_h$ of elements in W provides an ideal generating set $f, f_1, \ldots, f_h$ of I with probability $\geq 1 - 2^{-r}$.

(ii) Assume that $k = \mathbb{F}_q$ is finite. Let $\Sigma = k$. Choosing $h = \lceil \log_q(\dim_k(R/fR)) + r \rceil$ many Σ-random linear combinations $f_1, \ldots, f_h$ of elements in W provides an ideal generating set $f, f_1, \ldots, f_h$ of I with probability $\geq 1 - q^{-r}$.

(iii) Assume that k is infinite and provides the functionality of giving out samples of elements of prescribed cardinality.

Then choosing $\Sigma \subseteq k$ such that $\log_2(\#\Sigma) \geq \log_2(\dim_k R/fR) + r$ provides that f, f_1 is an ideal generating set of I with probability $\geq 1 - 2^{-r}$.

Proof. Using Corollary 6.2.22 with $\Sigma = \{0,1\}$ and $\eta = 2^{-r}$ we obtain (i) and using Corollary 6.2.22 with $\Sigma = k$ and $\eta = 2^{-r}$ we obtain (ii). To prove (iii), note that by assumption, we can choose $\Sigma \subseteq k$ such that $\log_2(\#\Sigma) \geq \log_2(\dim_k R/fR) + r$ is always possible and thus the assertion follows from Corollary 6.2.22 with $\eta = 2^{-r}$. □

Now we formulate an algorithm that computes, given a basis matrix T of an invertible ideal I and a finite subset Σ of the ground field k, a set of random elements in the k-vector space spanned by the columns of T.

Algorithm 12 Randomised attempt to compute an ideal generating set

Input	$T \in k[x]^{n \times n}$; h number of elements to produce; Σ finite subset of k
Output	$\beta_1, \ldots, \beta_h \in k[x]^n$ with degree bounded by $\deg(T)$ which are Σ-randomly chosen k-linear combinations of the columns of T

```
1: procedure TryIGS(T, h, Σ)
2:     for j = 1, ..., n do
3:         for i = 1, ..., h do
4:             λ_{i,j} ← Random(Σ)
5:         β_j ← (λ_{1,j}, ..., λ_{n,j})
6:     return Tβ_1, ..., Tβ_h
```

Lemma 6.2.24. *The algorithm TryIGS, see Algorithm 12, is correct. Moreover, if d is an upper bound of $\deg(T)$ and $\#\Sigma \in O^{\sim}(1)$, then TryIGS requires at most $O^{\sim}(n^2dh)$ operations in k.*

Proof. The correctness is obvious. Since $\#\Sigma \in O^{\sim}(1)$, by Lemma A.1.2 (ix), RANDOM requires at most $O^{\sim}(1)$ operations in k. Hence running through the nested loops requires at most $O^{\sim}(nh)$ operations in k. Since $\beta_i \in k^n$, any of the multiplications $T\beta_i$ requires at most $O(n^2 d)$ operations in k and thus all of them require at most $O(n^2 dh)$ operations in k. □

We use TRYIGS, see Algorithm 12, to provide a randomised algorithm that tries to provide an ideal generating set for a given R_0-ideal. Using the insights of Corollary 6.2.23, we call TRYIGS while prescribing a sufficiently large number of generators such that the probability of successfully finding an ideal generating set is adequate for our purposes. The algorithm will either return a correct result or return that it failed.

Note that we assume for the moment that we have an algorithm PRINCBASMAT at hand that is able to compute the principal basis matrix T_f of a principal ideal fR_0 and that requires at most $O^{\sim}(n^{\omega} c_X)$ operations in k. We will justify this assumption in Section 6.3, see Remark 6.3.39. We will cite the respective statement of Section 6.3 in the proof of the correctness of Algorithm 13.

Algorithm 13 Providing an ideal generating set

Precomputed	Ω fixed basis of R_0; Ω_i^m fixed basis of R_0^+
Input	$T_I \in k[x]^{n\times n}$ basis matrix of ideal I; T_f standard basis matrix of the first regular generator; $r, t \in \mathbb{Z}_{\geq 1}$ probability parameters; Σ finite subset of k; c Boolean whether T_I, T_f are basis matrices with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$)
Output	Boolean 'igs' that informs whether the algorithm was successful and either 0 if igs equals *false* or $[(\beta_1, \ldots, \beta_h), (T_{\beta_1}, \ldots, T_{\beta_h})]$ if igs equals *true*; here $\beta_i \in k[x]^n$ and $T_{\beta_i} \in k[x]^{n\times n}$ is the basis matrix of $\beta_i R_0$

1: **procedure** PROVIDEIGS($T_I, T_f, r, t, \Sigma, c$)
2: $d_I \leftarrow$ DEGOFIDEAL(T_I, c)
3: **if** $d_I = 0$ **then** || $I = R_0$
4: **return** *true*, $[(1, 0, \ldots, 0)^T, (E_n)]$
5: $d_f \leftarrow$ DEGOFIDEAL(T_f, c)
6: $h \leftarrow \lceil (\log_2(d_f) + r)/\log_2(\#\Sigma) \rceil$
7: igs $\leftarrow$ *false*
8: $\ell \leftarrow 0$
9: **while** igs $=$ *false* **and** $\ell < t$ **do**
10: $\beta_1, \ldots, \beta_h \leftarrow$ TRYIGS(T_I, h, Σ)
11: **for** $i = 1, \ldots, h$ **do**
12: $T_{\beta_i} \leftarrow$ PRINCBASMAT(β_i, c)
13: igs $\leftarrow$ TESTIGS($T_I, T_f, T_{\beta_1}, \ldots, T_{\beta_h}$)
14: $\ell \leftarrow \ell + 1$
15: **if** igs $=$ *true* **then**
16: **return** igs, $[(\beta_1, \ldots, \beta_h), (T_{\beta_1}, \ldots, T_{\beta_h})]$
17: **return** igs, 0

Lemma 6.2.25. *The algorithm* PROVIDEIGS, *see Algorithm 13, is correct if f is regular. Moreover, if d is an upper bound for the degree of the input matrices, $c_X \in O(d)$ and $r, t \in O^{\sim}(1)$, then* PROVIDEIGS *requires at most $O^{\sim}(n^{\omega} d)$ operations in k and returns vectors and matrices whose degrees are bounded by d respectively $d + 2c_X$. The probability that* PROVIDEIGS *returns an ideal generating set is lower bounded by $1 - 2^{-rt}$. In particular, with $r = \log_2(n)$ the above probability becomes lower bounded by $1 - n^{-t}$.*

Proof. Let us prove the correctness of ProvideIGS first. Assume that $f \in R_0$ is a regular element. If $\deg \det T_I = 0$, then $\deg_k I = 0 = \deg_k R_0$ and thus $I \subseteq R_0$ together with Lemma 6.2.3 provides $I = R_0$. The correctness of the algorithms TryIGS, PrincBasMat and TestIGS, see Lemmas 6.2.4 and 6.2.24 and Theorems 6.3.32 and 6.3.38, provide that each iteration of the **while** loop comes up with a possible ideal generating set $f, \beta_1, \ldots, \beta_h$ of I and the Boolean *igs* storing whether it does indeed generate I. This already provides the correctness of ProvideIGS.

Let us now prove the asserted running time complexity. By assumption, d is an upper bound for the degrees of the input matrices and hence, by Lemma 6.1.8, the computation of d_I and d_f require at most $O^\sim(n^\omega d)$ operations in k. By assumption, $r \in O^\sim(1)$ and thus, by construction, we have $h \in O^\sim(1)$ as well. Let us examine the running time of each **while** loop iteration. Since $\deg(T_i) \leq d$ and $h \in O^\sim(1)$, Lemma 6.2.24 provides that TryIGS requires at most $O^\sim(n^\omega d)$ operations in k and that it returns coefficient vectors with degree bounded by d again. Therefore, Theorems 6.3.32 and 6.3.38 tell us that the computation of T_{β_i} requires at most $O^\sim(n^\omega d)$ operations in k. Since all of the input matrices of TestIGS are degree upper bounded by d, Lemma 6.2.4 tells us that TestIGS requires at most $O^\sim(n^\omega d)$ operations in k. The above shows that each iteration of the **while** loop requires at most $O^\sim(n^\omega d)$ operations in k and since we have at most $t \in O^\sim(1)$ many iterations, the **while** loop overall requires $O^\sim(n^\omega d)$ operations in k. This proves the asserted running time of ProvideIGS.

Next we prove the assertion concerning the degrees of the output vectors and matrices. By assumption, d is an upper bound of the input matrices and thus, by how TryIGS constructs the proposed ideal generating elements, we see that $\deg(\beta_i) \leq d$ as well. Therefore, by Theorems 6.3.32 and 6.3.38, we see that the output of PrincBasMat indeed has degree bounded by $d + 2c_X$.

We consider the assertion regarding the probability of ProvideIGS successfully returning an ideal generating set. First of all, by assumption, $\deg(T_f) \leq d$. Thus

$$\dim_k R_0/fR_0 = \deg_k fR_0 = \deg(\det(T_f)) \leq nd$$

and hence $\log_q(\dim_k R_0/fR_0), \log_2(\dim_k R_0/fR_0) \in O(\log nd) \subseteq O^\sim(1)$. Thus, by $r \in O^\sim(1)$, we have $h \in O^\sim(1)$. By Corollary 6.2.23 (i), we know that

$$\text{Prob}\left(fR_0 + \sum_{i=1}^{h} \beta_i R_0 = I\right) \geq 1 - 2^{-r}$$

for every one of the at most t loop iterations. Hence the probability that TryIGS does not return an ideal generating set in any of the loop iterations (and thus that ProvideIGS will not be successful) is upper bounded by 2^{-rt} providing the second last assertion. Moreover, let $r = \log_2(n) \in O^\sim(1)$. Then $2^{-rt} = 2^{-t\log_2(n)} = (2^{\log_2(n)})^{-t} = n^{-t}$ provides the last assertion. □

Remark 6.2.26. Note that according to Corollary 6.2.23, we could also always use $\Sigma = \{0, 1\}$ and then set $h = \lceil \log_2(d_f) + r \rceil$ to obtain the respective algorithm with the same probability of success. Moreover, in the respective cases, Corollary 6.2.23 (ii) and (iii) provide the respective lower bounds for the probability of success if we alter h accordingly. △

6.3 Computation of Basis Matrices of Principal Ideals

This section is dedicated to finding a way of computing the basis matrix T_f of the standard basis $f\omega_1, \ldots, f\omega_n$ of the principal ideal fR_0 for some $f \in \mathcal{K}_X(X)^\times$. By definition, we

therefore need to compute the products $f\omega_i$ for all $\omega_i \in \Omega$ while f and ω_i are given by coefficient vectors. Doing so naively would end up using n^3 many polynomial products which would exceed our running time goal of $O(n^\omega d)$ where d denotes the degree of the matrices respectively polynomials we are dealing with. The basic idea to circumvent this is to compute the respective products in an algebraic structure that is better suited for multiplication. We are going to represent the elements in question as polynomials in two indeterminates x and y where x generates $k[x]$ as a k-algebra and y is a primitive element of $\mathcal{K}_X(X)$ over $k(x)$. To be more precise, we want to find a plane affine curve given by $S = k[x, y]$ with $y \in R_0$ such that the corresponding index ν of the extension $S \subseteq R_0$ satisfies $S_\nu = (R_0)_\nu$. Then any element $h \in k[x]$ which is coprime to ν will satisfy $R_0/hR_0 \cong S/hS$ and thus we can use fast polynomial multiplication in two indeterminates with bounded degree in y (bounded by n) and bounded degree in x (given by the degree of h) to carry out the necessary multiplications steps. We will see that the degree of h depends on the choice of y. To be exact, the degree of h will depend on the degree of the trace of y and thus it is mandatory to find such y whose trace has sufficiently small degree.

Depending on which approach we use, the component independent or the component dependent case, we assume f to be given by either the coefficient vector $\phi_\Omega(f)$ with respect to Ω or by the coefficient vector $\phi_{\Omega_i^m}(f)$ with respect to Ω_i^m. We will start with the component independent case which completely forgets about X possibly being reducible. After we have shown how this works, we can use the obtained insights and the main idea mentioned above for the irreducible components of X simultaneously and work out the component dependent case.

At this point we want to emphasise why we indeed need two distinct approaches depending on whether we have to deal with the component independent or the component dependent case. Generally, to reduce both scenarios to only one algorithm, we need to be able to change efficiently between the representations of vectors $\phi_\Omega(f)$ and $\phi_{\Omega_i^m}(f)$ as well as respective basis matrices. The precomputed matrix T_Ω, see Lemma 4.6.2, such that $\Omega = \Omega_i^m \cdot T_\Omega$ and the principal basis matrix $f\Omega = \Omega \cdot T_f$ together provide

$$\phi_{\Omega_i^m}(f) = T_\Omega \cdot \phi_\Omega(f) \quad \text{and} \quad f\Omega = \Omega_i^m \cdot T_\Omega \cdot T_f.$$

That is, by multiplication with the matrix T_Ω of degree $2c_X$, see Lemma 4.6.2, we can change from the component independent to the component dependent case. But to change from the component dependent to the component independent case we need to multiply with $T_\Omega^{-1} = \det(T_\Omega)^{-1} \cdot \operatorname{adj}(T_\Omega)$ where $\operatorname{adj}(T_\Omega)$ may have degree nc_X. This implies that, in general, only one direction of change is efficient enough for our considerations and hence it does not suffice to come up with one algorithm in one of the cases, use it for the computations and then reinterpret the results by changing to the desired representation.

6.3.1 Existence of Primitive Element

In this section we prove that there is a primitive element $y \in R_0$ of $\mathcal{K}_X(X)$ over $k(x)$ with $\deg \phi_\Omega(y) \leq \log_q(n)$ if $k = \mathbb{F}_q$ and $\deg \phi_\Omega(y) \leq 1$ otherwise.

Let X be reduced cover of $\mathbb{P}_k^1$. We will accomplish this by using the isomorphism $\operatorname{Frac}(R_0) \cong \bigoplus_{i=1}^m \operatorname{Frac}(R_{i,0})$, see Proposition B.2.2, and by proving that there are primitive elements y_i of the function field extensions $\operatorname{Frac}(R_{i,0})$ over $k(x)$ of small degree using the constructive proof of the theorem of the primitive element. After that we prove that suitably altering the y_i suffices that the corresponding element in $\operatorname{Frac}(R_0)$ is actually a primitive element of $\operatorname{Frac}(R_0)$ over $k(x)$.

We will use the following statement iteratively to construct the needed primitive elements $y_i \in R_{i,0}$ such that $\operatorname{Frac}(R_{i,0}) = R_{i,0}[y_i]$ with $\deg \phi_{\Omega_i}(y_i) \leq 2\log_q(n_i)$ whenever

$k = \mathbb{F}_q$ is a finite field.

Proposition 6.3.1 (Theorem of the primitive element)**.** *Let A be an integral domain with field of fractions K. Let B be a finite A-algebra with $A \subseteq B$ which is an integral domain. Let $a, b \in B$ be such that a is separable over K. By $f_a, f_b \in K[t]$ we denote the minimal polynomials of a respectively b over K. Let $a = a_1, \ldots, a_r$ denote the zeroes of f_a and $b = b_1, \ldots, b_s$ those of f_b in a splitting field C of $f_a f_b$. We set*

$$E(y) = \{a_i y + b_j \mid 2 \leq i \leq \deg(f_a), 1 \leq j \leq \deg(f_b)\}.$$

Then every $y \in K$ with $c = ay + b \notin E(y)$ satisfies $K[a, b] = K[c]$. In particular, there are at most $(r-1)s$ elements y in K such that $c = ay + b$ is no primitive element of $K[a, b]$ over K.

Proof. By assumption, f_a is separable and thus $a, a_2, \ldots, a_r$ are all distinct. Moreover, by definition of $E(y)$, for every $c = ay + b \notin E(y)$ we have $\forall\ i, j : c - a_i y \neq b_j$. In particular, for such c we have

$$\forall\ i = 2, \ldots, r : f_b(c - a_i y) \neq 0. \tag{3:2}$$

Set h to be the greatest common divisor of f_a and $f_b(c - yt)$ in $K[c][t]$. Obviously, a is both a zero of f_a and of $f_b(c - yt)$ since $f_b(c - ay) = f_b(ay + b - ay) = f_b(b) = 0$. Therefore, $t - a$ divides h in $C[t]$ and no higher power of $t - a$ does divide h since f_a is separable. In $C[t]$, f_a splits into the linear factors $t - a_i$ and thus h is a product of these linear factors. If $t - a_i$ divides h, then it must divide $f_b(c - yt)$ and thus $f_b(c - a_i y) = 0$ in $C[t]$ which is not possible due to Eq. (3:2). Hence $t - a$ is the only possible factor of h and thus we deduce $h = t - a$. By definition of h, we have $h \in K[c][t]$ and thus $a \in K[c]$ which then provides $b = c - ay \in K[c]$ as well. Hence $K[a, b] \subseteq K[c]$. The other direction is obvious: Since $y \in K$, we have $c = ay + b \in K[a, b]$ and thus $K[c] \subseteq K[a, b]$.

The particular part follows easily: Every $y \in K$ with $c = ay + b \in E(y)$ satisfies $y = (b - b_j)(a - a_i)^{-1}$ for some $i = 2, \ldots, r$ and $j = 1, \ldots, s$. Therefore, there are at most $(r-1)s$ many such elements in K that do not provide c that is a primitive element. □

Now we can use Proposition 6.3.1 to provide primitive elements for the function fields of the irreducible components of X with bounded degree.

Lemma 6.3.2. *Let $F = k(x)[a_1, \ldots, a_\ell]$ be a field that is a finite and separable $k(x)$-algebra of dimension n over $k(x)$. Then there are polynomials $\lambda_2, \ldots, \lambda_\ell \in k[x]$ with*

$$\deg \lambda_j \leq \begin{cases} 2\log_q(n), & k = \mathbb{F}_q \\ 1, & k \text{ infinite} \end{cases}$$

such that for all $i = 1, \ldots, \ell$ the element $y_i := a_1 + \lambda_2 a_2 + \ldots + \lambda_i a_i$ satisfies

$$k(x)[a_1, \ldots, a_i] = k(x)[y_i].$$

In particular, there is $y = \sum_{i=1}^{\ell} \lambda_i a_i \in k[x][a_1, \ldots, a_\ell]$ with $F = k(x)[y]$ such that $\deg \lambda_i \leq 2\log_q(n)$ if $k = \mathbb{F}_q$ is finite and $\deg \lambda_i \leq 1$ otherwise.

Proof. We prove the assertion by induction on the number ℓ of generators of F over $k(x)$. The case $\ell = 1$ already provides a primitive element $y = a_1$ as asserted. Now assume that the statement is true for $\ell - 1 \geq 1$. That is, there are polynomials $\lambda_2, \ldots, \lambda_{\ell-1} \in k[x]$ with

$$\forall\ i = 2, \ldots, \ell - 1\ :\quad \deg \lambda_i \leq \begin{cases} 2\log_q(n), & k = \mathbb{F}_q \\ 1, & k \text{ infinite} \end{cases}$$

such that $y_i := a_1 + \lambda_2 a_2 + \ldots + \lambda_i a_i \in k(x)[a_1, \ldots, a_i]$ satisfies $k(x)[a_1, \ldots, a_i] = k(x)[y_i]$.

By definition, we have $F = k(x)[y_{\ell-1}, a_\ell]$. Let $f_{y_{\ell-1}}, f_{a_\ell} \in k(x)[t]$ denote the minimal polynomials of $y_{\ell-1}$ respectively a_ℓ over $k(x)$. Since both $K[y_{\ell-1}]$ and $K[a_\ell]$ are K-subvector spaces of F, we have $d := \deg f_{y_{\ell-1}}, e := \deg f_{a_\ell} \leq n$. Let $y_{\ell-1} = y_{\ell-1,1}, \ldots, y_{\ell-1,d}$ respectively $a_\ell = a_{\ell,1}, \ldots, a_{\ell,e}$ denote the respective zeros of $f_{y_{\ell-1}}$ and f_{a_ℓ} in a splitting field of $f_{y_{\ell-1}} f_{a_\ell}$. By Proposition 6.3.1, we know that every $\lambda \in k[x]$ with

$$\lambda \neq \frac{a_{\ell,j} - a_\ell}{y_{\ell-1} - y_{\ell-1,i}} \quad \forall\ i = 2, \ldots, d, j = 1, \ldots, e$$

satisfies $F = k(x)[y_{\ell-1}, a_\ell] = k(x)[y_{\ell-1} + \lambda a_\ell]$. Therefore, the number of possible elements in $k[x]$ that we wish to avoid is at most $(d-1)e \leq (n-1)n \leq n^2$. Hence if k is infinite, then there is an infinite number of polynomials of degree one. Hence in this case there is $\lambda \in k[x]$ of degree one such that

$$y_\ell := y_{\ell-1} + \lambda a_\ell = a_1 + \lambda_2 a_2 + \ldots + \lambda_{\ell-1} a_{\ell-1} + \lambda_\ell a_\ell$$

is a primitive element of F over $k(x)$ as asserted. For the rest of the proof we assume $k = \mathbb{F}_q$ to be a finite field with q elements. We examine what a degree bound $b \in \mathbb{N}$ is such that the cardinality of the set $P_b(k)$ of all polynomials over k of degree b exceeds $n^2 \geq (d-1)e$. Since k is a finite field with q elements, for every of the b (non-leading) coefficients in k of an arbitrary polynomial of degree b there are q possibilities in k and for the leading coefficient there are exactly $q-1$. Therefore, we obtain $\#P_b(k) = q^b(q-1)$. This implies that

$$\#P_b(k) = q^b(q-1) > n^2$$

is satisfied if $b + \log_q(q-1) > 2\log_q(n)$. Since $\log_q(q-1) \geq \log_q(1) = 0$, $b > 2\log_q(n)$ is a sufficient degree bound. Therefore, there is a polynomial $\lambda_\ell \in k[x]$ of degree at most $2\log_q(n)$ such that $y_\ell := y_{\ell-1} + \lambda_\ell a_\ell$ satisfies $k(x)[a_1, \ldots, a_\ell] = k(x)[y_{\ell-1}, a_\ell] = k(x)[y_\ell]$. The induction hypothesis already provides the asserted properties of y_i and λ_i for $i = 1, \ldots, \ell-1$ and thus y_ℓ provides the assertion. □

Using Lemma 6.3.2 for each $\mathrm{Frac}(R_{i,0})$ over $k(x)$ we obtain the following corollary.

Corollary 6.3.3. *For $i = 1, \ldots, m$ there are primitive elements $y_i \in R_{i,0}$ such that $\mathrm{Frac}(R_{i,0}) = k(x)[y_i]$ and $\deg_{\Omega_i} \phi(y_i) \leq \log_q(n_i)$ if $k = \mathbb{F}_q$ and $\deg_{\Omega_i} \phi(y_i) \leq 1$ otherwise.*

Next we alter the existing primitive elements $y_1, \ldots, y_m$ such that the corresponding element y in $R_{i,0}$ is a primitive element of $\mathrm{Frac}(R_{i,0})$. The following statement gives a sufficient criterion for whether this is the case only depending on the minimal polynomials $f_i \in k(x)[t]$ of y_i.

Lemma 6.3.4. *For $i = 1, \ldots, m$ let $f_i \in k(x)[t]$ be the minimal polynomial of α_i, the primitive element of $\mathrm{Frac}(R_{i,0})/k(x)$. If for all $i \neq j$ we have $\gcd(f_i, f_j) = 1$, then the corresponding element y of $(y_1, \ldots, y_m)$ is a primitive element of $\mathrm{Frac}(R_0)/k(x)$.*

Proof. Set $F := \mathrm{Frac}(R_0)$, $F_i := \mathrm{Frac}(R_{i,0})$ and $K := k(x)$. The element $y \in F$ is a primitive element of F over K if and only if for every $a \in F$ there is a polynomial $f \in K[t]$ such that $a = f(y)$. Therefore, it is enough to show that there are polynomials $g_i \in K[t]$, $i = 1, \ldots, m$, such that $g_i(y)$ gets sent to $(0, \ldots, 0, 1, 0, \ldots, 0)$ where 1 is at the i-th place. Because in this case the element $y \cdot g_i(y)$ gets sent to the tuple $(0, \ldots, 0, y_i, 0, \ldots, 0)$ which generates F_i over K and thus $t \cdot g_i \in K[t]$ yields the desired polynomial.

By assumption, there are $a_{i,j} \in K$ such that

$$1 = a_{i,j} f_i + a_{j,i} f_j \tag{3:3}$$

For each $i \in \{1, \dots, m\}$ define $h_i = \prod_{j \neq i} a_{j,i} f_j \in K[t]$. Then by equation (3:3), we have $h_i = \prod_{j \neq i}(1 - a_{i,j} f_i)$. By definition, we have $h_i(y_k) = \delta_{i,k}$ where $\delta_{i,k}$ denotes the Kronecker-Delta.

Let ρ denote the K-isomorphism $F \to \bigoplus_{i=1}^m F_i$ and let ρ_i denote the composition of ρ followed by the projection onto the i-th component. Then by definition of ρ and since it is a K-algebra homomorphism, we have

$$\rho(f(y)) = (f(\rho_1(y)), \dots, f(\rho_m(y))) = (f(y_1), \dots, f(y_m)) \tag{3:4}$$

for every $f \in K[t]$. In particular,

$$\begin{aligned} \rho(h_i(y)) &= (\underbrace{h_i(y_1)}_{=0}, \dots, \underbrace{h_i(y_{i-1})}_{=0}, \underbrace{h_i(y_i)}_{=1}, \underbrace{h_i(y_{i+1})}_{=0}, \dots, \underbrace{h_i(y_m)}_{=0}) \\ &= (0, \dots, 0, 1, 0, \dots, 0) \end{aligned}$$

and thus the assertion follows. □

By Lemma 6.3.4, we need to alter given $y_1, \dots, y_m$ such that their respective minimal polynomials are coprime over $k[x][t]$.

Lemma 6.3.5. *Let F/K be a finite field extension with $F = K[y]$. Let $f \in K[t]$ denote the minimal polynomial of y over K. Let $c \in K$, then $y + c$ has minimal polynomial $f(t - c)$. Obviously, $y + c$ is still a primitive element of F over K.*

Proof. The ring homomorphism $K[t] \to K[t]$, $g \mapsto g(t - c)$ is an isomorphism and hence $f \in K[t]$ is irreducible if and only if $f(t - c)$ is irreducible. Hence $f(t - c)$ is irreducible. That $f(t - c)(y + c) = f(y) = 0$ is obvious and thus the assertion follows. □

Remark 6.3.6. Let $f \in K[t]$ be arbitrary with $f = \sum_{i=0}^d a_i t^i$. For every $c \in K$ we have $f(t+c) = \sum_{k=0}^d t^k (\sum_{l=0}^{d-k} \binom{l+k}{k} c^l a_{l+k})$. In particular, the coefficient of t^0 in $f(t+c)$ equals $\sum_{l=0}^d c^l a_l$. △

For two irreducible polynomials in $k(x)[t]$ to be not equal it is enough that their respective coefficient of t^0 (which is non-zero since they are both irreducible) do not coincide. Hence for given $f \in k(x)[t]$ we face the task to choose $c \in k(x)$ such that $\sum_{l=0}^d c^l a_l \neq b$ for given $b \in k(x)$. At this point it is easy to see that if k is infinite, then there is an infinite number of polynomials over k of degree one. Therefore, we can alter the primitive elements $y_1, \dots, y_m$ successively by suitable polynomials $c_i \in k[x]$ of degree one such that at the end the resulting minimal polynomials $f_1, \dots, f_m$ are pairwise coprime. Only if the ground field k is finite, we need to give an argument that finding $c_i \in k[x]$ is still possible while keeping their respective degrees reasonably small.

Lemma 6.3.7. *Let K be a field. Let $f \in K[t]$ be non-zero and irreducible polynomial of degree d. For given $b \in K$ there are at most $d + 1$ possible distinct elements c in K such that $f(t + c)$ has constant coefficient b.*

Proof. For every c the constant coefficient of $f(t + c)$ is equal to $f(0 + c) = f(c)$. If for $d + 1$ distinct choices of $c \in K$ this equals the same $b \in K$, then $f - b$ has $d + 1$ zeros in K. Since f is of degree d, this implies $f = b \in K$ which is a contradiction to f being irreducible. □

Lemma 6.3.8. *Let $K = k(x)$ for some finite field k with q elements. Let $f_1, \dots, f_i \in K[t]$ be monic and irreducible polynomials and let $f \in K[t]$ of degree $d = \deg(f)$ be equal to one of the f_j. Then there is $c \in k[x]$ of degree bounded by $\lceil \log_q(d + 1 + i) \rceil$ such that $f(t + c)$ is not equal to any of the $f_1, \dots, f_i$.*

Proof. We will use Lemma 6.3.7 to alter f by a suitable c_1 of small degree. Without loss of generality we assume that $f = f_1$. There are q^s many polynomials over k having degree bounded by s. Therefore, there are $d+1$ distinct polynomials over k having degree bounded by $\lceil \log_q(d+1) \rceil$. Hence by Lemma 6.3.7, there is $c_1 \in k[x]$ of degree bounded by $\lceil \log_q(d+1) \rceil$ such that $f(t+c_1)$ has constant coefficient which is distinct to that of f_1 and hence $f(t+c_1) \neq f_1$. Now if $f(t+c_1)$ does not equal any of the remaining $f_2, \ldots, f_i$, then we are done. Otherwise, assume without loss of generality that $f(t+c_1) = f_2$. We can use the same argument as above to find $c_2 \in k[x]$ with $f(t+c_1+c_2) \neq f_2$. But we need to satisfy that $f(t+c_1+c_2) \neq f_1$ as well which is the case if and only if $c_2 = -c_1$. This additional condition prohibits at most one of the possible candidates for c_2 under those of degree bounded by $\lceil \log_q(d+1) \rceil$. Therefore, we are able to find c_2 such that $\deg(c_2) \leq \lceil \log_q(d+2) \rceil$. Proceeding in the same manner, in step j we need to ensure that c_j satisfies $c_j \neq -\sum_{l=r}^{j-1} c_l$ for all $r = 1, \ldots, j-1$. This provides that $f(t + \sum_{l=1}^{j} c_l)$ does not equal any of the $f(t + \sum_{l=1}^{h} c_l)$ for $h = 1, \ldots, j-1$. Thus in step j there are j polynomials that we need to avoid choosing c_j. Therefore, we are able to find $c_j \in k[x]$ with $\deg(c_j) \leq \lceil \log_q(d+1+j) \rceil$ such that $f(t + \sum_{l=1}^{j} c_l) \neq f_h$ for all $h = 1, \ldots, j-1$. This finally yields that for $c = \sum_{l=1}^{i} c_l$ we have that $f(t+c)$ does not equal any of the $f_1, \ldots, f_i$ and that $\deg(c_j) \leq \lceil \log_q(d+1+j) \rceil$. Whence $\deg(c) \leq \max_{l=1}^{i} \{ \lceil \log_q(d+1+l) \rceil \} = \lceil \log_q(d+1+i) \rceil$. □

Corollary 6.3.9. *Let X be a reduced cover of $\mathbb{P}^1_k$. Then for all $i = 1, \ldots, m$ there is a primitive element $y_i \in R_{i,0}$ of $\mathrm{Frac}(R_{i,0})$ over $k(x)$ with $\deg \phi_{\Omega_i}(y_i) \leq 3 \log_q(n)$ such that the corresponding element $y = (y_1, \ldots, y_m) \in \mathrm{Frac}(R_0)$ is a primitive element of $\mathrm{Frac}(R_0)$ over $k(x)$.*

Proof. By Corollary 6.3.3, there are primitive elements $y_1, \ldots, y_m$ with $\deg \phi_{\Omega_i}(y_i)$ bounded by $\log_q(n_i)$. Let $f_1, \ldots, f_m \in k(x)[t]$ denote the corresponding minimal polynomials. By Lemma 6.3.8, there is $c_2 \in k[x]$ with $\deg(c_2) \leq \lceil \log_q(n_2+2) \rceil$ such that $f_2(t+c_2) \neq f_1$. Using Lemma 6.3.8 successively, we see that for all $i = 2, \ldots, m$ there are $c_i \in k[x]$ with $\deg(c_i) \leq \lceil \log_q(n_i+i) \rceil$ such that $f_i(t+c_i) \neq f_j(t+c_j)$ for all $j = 1, \ldots, i-1$. This correponds to a change of the i-th primitive element by $-c_i \in k[x]$ and thus

$$\deg \phi_{\Omega_i}(y_i - c_i) \leq \deg \phi_{\Omega_i}(y_i) + \deg(c_i) \leq \log_q(n_i) + \log_q(n_i+i) \leq 3 \log_q(n)$$

which provides the assertion. □

Lemma 6.3.10. *There is a primitive element y of $\mathrm{Frac}(R_0)$ over $k(x)$ such that $y \in R_0$ and $\deg \phi_\Omega(y) \leq 2nc_X + 3 \log_q(n)$.*

Proof. By Corollary 6.3.9, there is a primitive element $y \in \mathrm{Frac}(R_0)$ of $\mathrm{Frac}(R_0)$ over $k(x)$ such that its restrictions $y_i \in R_0$ satisfy $\deg \phi_{\Omega_i}(y_i) \leq 3 \log_q(n)$. Obviously, y is not necessarily an element of R_0 just because its restrictions y_i lie in $R_{i,0}$ and in general we have $y = zf^{-1}$ where $z \in R_0$ and $f \in k[x]$ (since $\mathrm{Frac}(R_0) = R_0 \otimes_{k[x]} k(x)$). The transformation matrix $T_\Omega \in k[x]^{n \times n}$ satisfies $\phi_{\Omega_i^m}(f) = T_\Omega \cdot \phi_\Omega(f)$ for every $f \in \mathrm{Frac}(R_0)$ and $\deg T_\Omega \leq 2c_X$, see Lemma 4.6.2. Therefore,

$$\phi_\Omega(y) = T_\Omega^{-1} \cdot \phi_{\Omega_i^m}(y) = \det(T_\Omega)^{-1} \cdot \mathrm{adj}(T_\Omega) \cdot \phi_{\Omega_i^m}(y)$$

and since $\mathrm{adj}(T_\Omega)$ as well as $\phi_{\Omega_i^m}(y)$ are defined over $k[x]$, the denominators of the entries of $\phi_\Omega(y)$ have at most degree $\deg \det(T_\Omega) \leq 2nc_X$. Therefore, multiplying y with a polynomial in $k[x]$ of degree at most $2nc_X$ yields an element z of R_0 which is still a primitive element of $\mathrm{Frac}(R_0)$. By the above, we see that $\deg \phi_\Omega(z) \leq 2nc_X + \deg \phi_{\Omega_i^m}(y) \leq 2nc_X + 3 \log_q(n)$. □

6.3.2 Reducing Polynomial

In this section we provide the existence of the polynomial $h \in k[x]$ being coprime to the index of S in R_0 as already mentioned in the above introduction. If not mentioned otherwise, we assume that X is a reduced cover of $\mathbb{P}^1_k$.

Notation 6.3.11. In this section we will use the short notation $\deg_\Omega(f) = \deg \phi_\Omega(f)$ for all $f \in \mathcal{K}_X(X)$. △

Definition 6.3.12. Let $y \in R_0$ be a primitive element as in Lemma 6.3.10. For the following considerations let S denote the ring $k[x, y]$. By construction, we have $S \subseteq R_0$. The $k[x]$-module S has basis $1, y, \ldots, y^{n-1}$ and there is a basis transformation matrix $T \in k[x]^{n\times n}$ with $(1, y, \ldots, y^{n-1}) = (\omega_1, \ldots, \omega_n)\, T$. Let us denote $\nu = \det(T) \in k[x]$ and call it the **index of S in R_0**. △

We will need the following two properties of the index.

Proposition 6.3.13. *The index ν satisfies the equation $\nu^2 \mathrm{disc}(R_0)k[x] = \mathrm{disc}(S)k[x]$ and, regarding S and R_0 only as $k[x]$-modules, ν provides $\nu R_0 \subseteq S$.*

Proof. Let $\beta_1, \ldots, \beta_n$ denote a $k[x]$-basis of R_0 and $\gamma_1, \ldots, \gamma_n$ a $k[x]$-basis of S. The first assertion follows from the definition of the discriminant and observing that $(\mathrm{Tr}(\gamma_i\gamma_j)_{ij}) = T^t\, (\mathrm{Tr}(\beta_i\beta_j)_{ij})\, T$.[1] For the second we need to consider the Smith-Normal-Form $T_S = A\, T\, B$ with diagonal entries $\lambda_1, \ldots, \lambda_n \in k[x]$ and $A, B \in \mathrm{GL}(n, k[x])$. By definition of T, we have $(\gamma_i)_i = (\beta_i)_i\, A^{-1}\, A\, T$ which we multiply with B from the right to obtain $(\gamma_i)_i\, B = (\beta_i)_i\, A^{-1}\, A\, T\, B = (\beta_i)_i\, A^{-1}\, T_S$. Now if we denote the new bases as $(\gamma'_i)_i = (\gamma_i)_i\, B$ and $(\beta'_i)_i = (\beta_i)_i\, A^{-1}$, then we have $(\gamma'_i)_i = (\beta'_i)_i\, \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, that is $\gamma'_i = \beta'_i\, \lambda_i$. Finally, with $\nu = \det(T) = \mu \cdot \det(T_S) = \mu \cdot \prod_{i=1}^n \lambda_i$ where $\mu \in k^\times$ we obtain $\nu \sum_{i=1}^n \beta'_i\, k[x] \subseteq \sum_{i=1}^n \gamma'_i\, k[x]$ which provides the assertion. □

We will now show the existence of some $h \in k[x]$ with sufficiently small degree and which is coprime to the index ν. Note that if $\mathrm{char}(k) = 0$, then we can always take a linear polynomial $h \in k[x]$ which is not a divisor of ν.

Remark 6.3.14. Let $f \in \mathbb{F}_q[x]$, $f \neq 0$ be arbitrary. A simple counting argument shows that there exist a polynomial $h \in \mathbb{F}_q[x]$ with $\deg(h) \in \log_q \deg(f)$ such that $\gcd(h, f) = 1$. △

Following Remark 6.3.14, to show the existence of $h \in k[x]$ with $\deg(h) \in O(d)$ for some d and coprime to ν, we need to show the appropriate bound of $\deg(\nu)$.

Remark 6.3.15. From Proposition 6.3.13 we deduce $\deg(\nu) \leq \deg(\mathrm{disc}(S))$. By definition, the latter is given by $\mathrm{disc}(S) = \mathrm{disc}(1, y, \ldots, y^{n-1})$ and the latter is, by definition,

$$\det(\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}\, (y^{i+j})_{i,j})$$

and thus

$$\deg(\nu) \leq n \cdot \max_{0\leq i\leq 2n-2} \{\deg(\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(y^i))\}$$ △

Lemma 6.3.16. *The index ν satisfies*

$$\deg(\nu) \leq \begin{cases} 4n^3 c_X + 6n^2 \log_q(n), & k = \mathbb{F}_q \\ n^2 \cdot (4c_X + 2), & k \text{ infinite.} \end{cases}$$

Proof. By Proposition 4.6.13 (ii), we know that the degree of $\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(y^{2n-2})$ is bounded by

$$\deg(\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(y^{2n-2})) \leq \deg \phi_\Omega(y^{2n-2}) + 2c_X.$$

[1] Here T^t denotes the transpose of the matrix T.

By Lemma 4.3.32 and Corollary 4.3.31 (iii), we have

$$\deg \phi_\Omega(y^{2n-2}) \leq \deg^*(y^{2n-2}) \leq (2n-2) \cdot \deg^*(y) \leq (2n-2) \cdot (\deg_\Omega(y) - |X|_n)$$

and thus, by Corollary 4.5.2, we finally obtain

$$\deg \phi_\Omega(y^{2n-2}) \leq (2n-2) \cdot (\deg_\Omega(y) + 2c_X).$$

Since y is a primitive element of $\mathrm{Frac}(R_0)/k(x)$ as in Lemma 6.3.10, we have $\deg_\Omega(y) \leq 2nc_X + 3\log_q(n)$ if $k = \mathbb{F}_q$ is finite and $\deg_\Omega(y) \leq 1$ if k is infinite. Combining all the above we obtain

$$\begin{aligned}\deg(\mathrm{Tr}_{\mathrm{Frac}(R_0)/k(x)}(y^{2n-2})) &\leq \begin{cases}(2n-2)\cdot(2nc_X + 3\log_q(n) + 2c_X) + 2c_X, & k = \mathbb{F}_q\\ (2n-2)\cdot(1+2c_X) + 2c_X, & k \text{ infinite}\end{cases}\\ &\leq \begin{cases}4n^2c_X + 6n\log_q(n), & k = \mathbb{F}_q\\ n\cdot(4c_X+2), & k \text{ infinite.}\end{cases}\end{aligned}$$

Then Remark 6.3.15 provides the assertion. □

Corollary 6.3.17. *There exists $h \in k[x]$ coprime to ν with*

$$\deg(h) \in \begin{cases}O(\log_q(n) + \log_q(c_X)), & k = \mathbb{F}_q\\ O(1), & k \text{ infinite.}\end{cases}$$

Proof. If k is infinite, then there is an infinite number of polynomials in $k[x]$ of degree one which are coprime to h and we may choose one of them. Let $k = \mathbb{F}_q$ be finite. By Lemma 6.3.16, we have $\deg(\nu) \leq 4n^3c_X + 6n^2\log_q(n)$. Remark 6.3.14 shows that there is such a polynomial $h \in k[x]$ with

$$\deg(h) \in O(\log_q(4n^3c_X + 6n^2\log_q(n))) \subseteq O(\log_q(4n^3c_X)) = O(\log_q(n) + \log_q(c_X))$$

which provides the assertion. □

Lemma 6.3.18. *Let $m \in k[x]$ with $mR_0 \subseteq S$, $h \in k[x]$ with $\gcd(m,h) = 1$, then $S/hS \cong R_0/hR_0$.*

Proof. By assumption, there are $s,t \in k[x]$ such that $ms + th = 1$. Consider the homomorphism $\varphi : S \to R_0/hR_0$, $a \mapsto a + hR_0$ with kernel $\ker\phi = hR_0 \cap S$. Now $hS \subseteq hR_0 \cap S$ and further let $h\alpha \in hR_0 \cap S$ with $\alpha \in R_0$, then $1 = ms + th$ multiplied by α gives $\alpha = m\alpha \cdot s + h\alpha \cdot t \in S$ and hence $\ker\varphi = hS$. Thus $S/hS \cong \varphi(S)$ and now we are left to show that φ is surjective. For this purpose let $a + hR_0 \neq 0$ in R_0/hR_0 be arbitrary, then $ms \cdot a = (1-th)\cdot a = a - ath \equiv a \bmod hR_0$ and since $m \cdot sa \in S$ holds, we are done. □

Proposition 6.3.19. *There is some $h \in k[x]$ with $S/hS \cong R_0/hR_0$ such that*

$$\deg(h) \in \begin{cases}O(\log_q(n) + \log_q(c_X) + \log_q\log_q(n)), & k = \mathbb{F}_q\\ O(1), & k \textit{ infinite.}\end{cases}$$

Proof. This is a direct consequence of Corollary 6.3.17 and Lemma 6.3.18. □

6.3.3 Computation of Principal Basis Matrices

In this section we want to implement our plan and use the primitive element $y \in R_0$ of $\mathcal{K}_X(X)$ and $h \in k[x]$ coprime to the index of $k[x,y]$ in R_0 to provide algorithms to compute

the principal basis matrices T_f for given $f \in R_0$. We distinguish between the component independent and the component dependent case.

6.3.3.1 Component Independent Case

Let X be a reduced cover of $\mathbb{P}^1_k$ with $\mathcal{K}_X(X) = k(x)[y]$ as in Lemma 6.3.10. Let $h \in k[x]$ be a polynomial as in Proposition 6.3.19. Let $\Omega = (\omega_1, \ldots, \omega_n)$ denote a reduced basis of R_0. Let us denote the basis transformation matrix from Ω to $1, y, \ldots, y^{n-1}$ as in Definition 6.3.12 by T.

Definition 6.3.20. We will abbreviate

$$R := \bigoplus_{i=1}^{n} \omega_i \left(k[x]/(h)\right) \quad \textit{and} \quad R_y := \bigoplus_{i=1}^{n} y^{i-1} \left(k[x]/(h)\right). \qquad \triangle$$

Lemma 6.3.21. *The bases of R_0 and S as $k[x]$-modules will also provide $k[x]/hk[x]$-bases of the $k[x]/hk[x]$-modules R_0/hR_0 and S/hS. In particular, as $k[x]/hk[x]$-modules we have $R_0/hR_0 \cong R$ and $S/hS \cong R_y$.*

Proof. By Proposition B.4.8, we have $R_0/hR_0 \cong R_0 \otimes_{k[x]} k[x]/hk[x]$ as well as $S/hS \cong S \otimes_{k[x]} k[x]/hk[x]$. Now the isomorphisms $R_0 \to \bigoplus_{i=1}^n \omega_i k[x]$ and $S \to \bigoplus_{i=1}^n y^{i-1} k[x]$ provide the asserted $k[x]/hk[x]$-algebra isomorphisms

$$R_0/hR_0 \to R, \quad \text{and} \quad S/hS \to R_y.$$

Here we used that the direct sum and tensor product of modules behave distributively. □

Remark 6.3.22. Recall that the ring extension R_0/S comes with an $k[x]$-algebra monomorphism $\varphi : S \hookrightarrow R_0$ represented by the matrix T. In particular, T behaves multiplicative in the following sense: For given $f, g \in S$, we may on the one hand compute the product fg using the multiplication table in S (that is using polynomial multiplication in two indeterminates and division with remainder). Alternatively, we may compute $\phi_\Omega(f)$ and $\phi_\Omega(g)$ using T and the representations $\phi_{(y^{i-1})}(f)$ and $\phi_{(y^{i-1})}(g)$, then use the multiplication tables of R_0 and polynomial multiplication in $k[x]$ to compute $\phi_\Omega(fg)$ and then compute $\phi_{(y^{i-1})}(fg)$ via T^{-1}. We can reverse this scenario for any element in R_0 that is also an element of S. △

Remark 6.3.23. The isomorphism $S/hS \to R_0/hR_0$ in Proposition 6.3.19 is induced by the $k[x]$-algebra monomorphism $\varphi : S \hookrightarrow R_0$ acting on representatives. Now φ was represented by the matrix $T \in k[x]^{n \times n}$ with determinant ν coprime to h. Since the bases of S and of R_0 as $k[x]$-modules also provide bases of S/hS and R_0/hR_0 as $k[x^{-1}]/hk[x^{-1}]$-modules, see Lemma 6.3.21, we see that the matrix $T \in \mathrm{GL}(n, k[x^{-1}]/hk[x^{-1}])$ (invertible since its determinant ν is coprime to h) represents the $k[x^{-1}]/hk[x^{-1}]$-algebra isomorphism $\Phi^{-1} : R_y \to S/hS \to R_0/hR_0 \to R$. Moreover, as in Remark 6.3.22 the transport with T is multiplicative as it represents an algebra homomorphism. △

Remark 6.3.24. In Remark 6.3.23 we may replace h by a suitable power of it to allow coefficients of intended degree. △

Lemma 6.3.25. *The matrices $T, T^{-1} \in \mathrm{GL}(n, k[x]/hk[x])$ can be represented by the matrices $\textsc{Red}_h(T)$ respectively $\textsc{Red}_h(s \cdot \mathrm{adj}(T))$ defined over $k[x]$.*

Proof. Of course, the reduced representation of T is simply $\textsc{Red}_h(T)$. The matrix $T \in \mathrm{GL}(n, k[x]/hk[x])$ satisfies by Cramer's rule the identity $T^{-1} = \nu^{-1} \cdot \mathrm{adj}(T)$. To represent T with entries that has coefficients in $k[x]$ reduced modulo h, we do so to obtain a representation of T as a matrix defined over $k[x]$: Let $1 = th + s\nu$ be the Bézout identity of

$\gcd(h, \nu)$ in $k[x]$. Then $\nu = s^{-1} \cdot (1 - th)$ and thus $\nu^{-1} = s \cdot (1 - ht)^{-1} \equiv s \bmod h$. Hence the reduced representation of T^{-1} with entries in $k[x]$ is $\text{RED}_h(s \cdot \text{adj}(T))$. □

Definition 6.3.26. We abbreviate $T'_h = \text{RED}_h(T)$ and $T_h = \text{RED}_h(s\,\text{adj}(T))$. △

Corollary 6.3.27. *Assume we have precomputed the Bézout identity $1 = th + s\nu$ of h and ν with $\deg(t) < \deg(\nu)$ and $\deg(s) < \deg(h)$. Let $\Phi : R \to R_y$ be the isomorphism as in Remark 6.3.23. Let $\beta \in R$ be given by $\phi_\Omega(\beta) \in k[x]^n$ and let $\alpha \in R_y$ be given by $\phi_{(y^{i-1})}(\alpha) \in k[x]^n$. Then*

(i) $\phi_{(y^{i-1})}(\Phi(\beta)) = T_h \cdot \phi_\Omega(\beta)$, *and*

(ii) $\phi_\Omega(\Phi^{-1}(\alpha)) = T'_h \cdot \phi_{(y^{i-1})}(\alpha)$.

Here the coefficients of the right hand sides need be regarded as elements in $k[x]/hk[x]$ again.

Remark 6.3.28. Every element f of R_0 with $f = \sum_{i=1}^n \lambda_i \omega_i$ such that $\deg(\lambda_i) < \deg(h)$ for all $i = 1, \ldots, n$ (that is $\deg(\phi_\Omega(f)) < h$) can be regarded as an element of R. △

Remark 6.3.29. By construction, we have $y \in R_0$ and since R_0 is finite over $k[x]$, it is a fortiori integral over $k[x]$. Hence its minimal polynomial $f := f_y$ over $k(x)$ is an element of $k[x][t]$. Since $S \cong k[x][t]/fk[x]$, we can view the elements in S as polynomial representatives in $k[x, t]$ that are reduced modulo f. Altogether we can view the elements of R_y as such polynomial representatives in $k[x, t]$ that are reduced modulo h and f. △

By Remarks 6.3.28 and 6.3.29, we may regard elements in R_0 with suitable bounded coefficient degrees as elements in R and can thus transport those using the matrix $T_h \in k[x]^{n \times n}$, see Remark 6.3.23, to R_y where we can compute the product and then transport the result back to R using T'_h and reinterpret it as an element of R_0.

Proposition 6.3.30. *The multiplication of two elements in R_y given by reduced polynomial representatives in $(k[x]/(h))[t]/(f)$ can be carried out using $O^\sim(n \cdot \deg(h))$ many operations in k. Here "multiplication" in $(k[x]/(h))[t]/(f)$ includes the needed division with remainder. We denote the algorithm that computes such a product MULT_y.*

Proof. We regard the elements of R_y as elements in $(k[x]/(h))\,[t]/(f)$. Since f has degree n in t, by Lemma A.2.11, the multiplication can be carried out using $O^\sim(n)$ many operations in the coefficient ring $k[x]/(h)$. In the worst case those are multiplication itself which, by Proposition A.2.3, can be carried out using $O(\deg h)$ field operations in k. This completes the proof. □

Now we can describe an algorithm to compute the product of two elements in R_0 only using their coefficients with regards to Ω.

Theorem 6.3.31. *The algorithm CompEltProd, see Algorithm 14, is correct and uses at most $O^\sim(n^2 \deg(h))$ operations in k.*

Proof. If $f \in R_0$ is only given by its representation $(f_i + hk[x])_i$ as an element of R_0/hR_0, see Remark 6.3.28, but we do know that its coefficients with regards to Ω as an element of R_0 have degree strictly smaller than $\deg(h)$, then we may compute the latter by computing $f_i = f'_i + r_i h$ with $\deg f'_i < \deg(h)$ to obtain the unique $\phi_\Omega(f) = (f'_1, \ldots, f'_n) \in k[x]^n$.

Since $\deg_\Omega(f), \deg_\Omega(g) < \deg(h)$, we may regard f and g uniquely as elements of R, see Remark 6.3.28. Moreover, by Corollary 4.3.31 (iii) and Corollary 4.3.24, we know that

$$\deg_\Omega(fg) \le \deg^*(fg) \le \deg^*(f) + \deg^*(g) \le \deg_\Omega(f) + \deg_\Omega(g) + 2c_X$$

Algorithm 14 Computing product of elements

Precomputed	Reduced basis Ω of R_0; $y \in R_0$ primitive element of $\mathcal{K}_X(X)/k(x)$; $h \in k[x]$ coprime to the index ν of $k[x,y]$ in R_0; T_h and T'_h as in Definition 6.3.26
Input	$\phi_\Omega(f), \phi_\Omega(g)$ such that $\deg \phi_\Omega(f) + \deg \phi_\Omega(g) + 2c_X \leq \deg(h)$
Output	$\phi_\Omega(fg)$ such that $\phi_\Omega(fg) \leq \deg(h)$

1: **procedure** CompEltProd($\phi_\Omega(f), \phi_\Omega(g)$))
2: $(f_1, \ldots, f_n) \leftarrow \text{Red}_h(T_h \cdot \phi_\Omega(f))$
3: $(g_1, \ldots, g_n) \leftarrow \text{Red}_h(T_h \cdot \phi_\Omega(g))$
4: $(e_1, \ldots, e_n) \leftarrow \text{Mult}_y((f_1, \ldots, f_n), (g_1, \ldots, g_n))$
5: **return** $\text{Red}_h(T'_h \cdot e)$

which is, by assumption, smaller than $\deg(h)$. Hence fg as an element of R has a unique representation $\phi_\Omega(fg)$ with entries of degree smaller than $\deg(h)$. Hence, due to what we have said at the beginning of the proof, if we have a representation of fg as an element of R given by a representative coefficient vector over $k[x]$, we only need to reduce it entry-wise modulo h to compute the unique representation $\phi_\Omega(fg) \in k[x]^n$ we are after.

In particular, we may transport f and g to R_y using T_h, compute the product there using polynomial multiplication in two indeterminates with bounded degrees and transport it back to R using T'_h. This results in a coefficient vector with representative polynomial entries which we only need to reduce entry-wise modulo h to obtain the desired $\phi_\Omega(fg)$. This proves the correctness of CompEltProd.

The matrix by vector multiplications in step 2 and 3 use n^2 operations in $k[x]$, see Lemma A.2.5. Since all T_h and $\phi_\Omega(f)$, $\phi_\Omega(g)$ have degree smaller than $\deg(h)$, by Proposition A.2.3, the computation uses $O^\sim(n^2 \deg(h))$ operations in k and the result also has degree bounded by $2\deg(h) \in O(\deg(h))$. Thus, by Lemma A.1.2 (iii), the algorithm Red_h uses $O^\sim(n \deg(h))$ operations in k. By Proposition 6.3.30, the algorithm Mult_y in step 4 requires $O^\sim(n \deg(h))$ operations in k. The degree of the coefficients e_i are bounded by $\deg(h)$ and thus, as above, the matrix vector product computation uses $O^\sim(n^2 \deg(h))$ operations in k. Moreover, the result has degree in $O(\deg(h))$ and thus Red_h uses again $O^\sim(n \deg(h))$ operations in k. Thus the most expensive steps required $O^\sim(n^2 \deg(h))$ many operations in k and thus we can complete the proof. □

Now we want to use the fast bivariate polynomial multiplication to write down an algorithm that computes the basis matrix T_f representing the basis $f\Omega = (f\omega_1, \ldots, f\omega_n)$ with respect to Ω. If we do it naively, we end up using $n^3 \deg(h)$ many operations in k which we would like to avoid. Put it more concretely, we could use algorithm Algorithm 14 for every one of the products $f\omega_1, \ldots, f\omega_n$. But then we end up calling algorithm Algorithm 14 n times which yields a cubic complexity in n. We circumvent this issue by transporting all involved elements into R_y using fast matrix multiplication and then compute the products in R_y instead where one multiplication uses $O^\sim(n \deg(h))$ operations in k and thus we can easily afford to do this n times. Note that we formulated Algorithm 15 just for computing the products $f\omega_1, \ldots, f\omega_n$ but it works for all arbitrary products of the form $f\alpha_1, \ldots, f\alpha_n$. In this case, we need to compute $T_h \cdot M_\alpha$ where M_α contains the vectors $\phi_\Omega(\alpha_i)$ additionally and then use $T_h \cdot M_\alpha e_i$ instead of $T_h e_i$ at line 3.

Note that by definition, the i-th column of T_h equals $\phi_{(y^{i-1})}(\omega_i)$. If we denote by e_i the i-th standard vector in $k[x]^n$, then we obtain $T_h e_i = \phi_{(y^{i-1})}(\omega_i)$.

Theorem 6.3.32. *The algorithm* PrincBasMatCF*, see Algorithm 15, is correct. Moreover, if d is an upper bound of $\deg h$, then* PrincBasMatCF *requires at most $O^\sim(n^\omega d)$ operations in k.*

Algorithm 15 Computing basis matrix of principal ideal: component independent case

Precomputed	Reduced basis Ω of R_0; $y \in R_0$ primitive element of $\mathcal{K}_X(X)/k(x)$; $h \in k[x]$ coprime to the index ν of $k[x,y]$ in R_0; T_h and T'_h as in Definition 6.3.26
Input	$\phi_\Omega(f)$ such that $\deg \phi_\Omega(f) + 2c_X \leq \deg(h)$
Output	Basis matrix T_f representing $f\omega_1, \ldots, f\omega_n$ with $\deg(T_f) \leq \deg \phi_\Omega(f) + 2c_X$

1: **procedure** PrincBasMatCF($\phi_\Omega(f)$)
2: $f' \leftarrow \text{Red}_h(T_h \cdot \phi_\Omega(f))$
3: $M \leftarrow (\text{Mult}_y(f', T_h e_1), \ldots, \text{Mult}_y(f', T_h e_n))$
4: **return** $\text{Red}_h(T'_h \cdot M)$

Proof. In step 1 we compute $\Phi(f)$ as a coefficient vector with regards to $1, \ldots, y^{n-1}$. In step 2 we compute the products $\Phi(f)\Phi(\omega_1), \ldots, \Phi(f)\Phi(\omega_n)$ and write the respective coefficient vectors with regards to $1, \ldots, y^{n-1}$ column-wise in the matrix M. Hence the proof of Theorem 6.3.31 shows that T'_h multiplied with column i of M provides $\phi_\Omega(f\omega_i)$. Hence $T'_h \cdot M$ provides the asserted standard basis matrix of fR_0. The statement about the degree of the output matrix is due to Corollaries 4.3.24, 4.3.31 and 4.5.2 and Lemma 4.3.32.

The first step uses, as argued in the proof of Theorem 6.3.31, $O^\sim(n^2 \deg(h))$ operations in k and the resulting vector has coefficients with degree bounded by $2\deg(h) \in O(\deg(h))$. Thus, by Lemma A.1.2 (iii), the algorithm Red_h uses $O^\sim(n \deg(h))$ operations in k. By Proposition 6.3.30, the algorithm Mult_y in step 4 requires $O^\sim(n \deg(h))$ operations in k and hence calling it n times with the same input size requires $O^\sim(n^2 \deg(h))$ operations in k. Since the degree of f' and of T_h lie in $O(\deg(h))$, the same is true for the matrix M. Finally, the matrix product $T'_h \cdot M$ requires $O^\sim(n^\omega \deg(h))$ operations in k and is thus the most expensive step of the algorithm. Therefore, PrincBasMatCF requires $O^\sim(n^\omega \deg(h))$ operations in k. □

Remark 6.3.33. Let $T \in k[x]^{a \times a}$ and $M \in k[x]^{a \times b}$ have both degree d. Then the computation of the product $T \cdot M$ requires at most $O^\sim(\lceil b/a \rceil a^\omega d) = O^\sim(ba^{\omega-1}d)$ operations in k. Indeed, let $b = ca + r$ with $r < a$ be the division with remainder of b by a. We can split M into c square matrices $M_1, \ldots, M_c$ of dimension a and one which has dimension $a \times r$. We append zero columns to the latter to make it square and call it M_{c+1}. Then we can compute the product $T \cdot M$ by computing the products $T \cdot M_j$ and concatenate the result, that is

$$T \cdot M = (T \cdot M_1) \frown \ldots \frown (T \cdot M_c) \frown (T \cdot M_{c+1}).$$

Then the computation requires calling the square matrix multiplication algorithm in dimension a with degree d, which requires itself $O^\sim(a^\omega d)$ operations in k, a total number of $c + 1 = \lceil b/a \rceil$ times. Hence the complexity bound. △

The following adaptation of Algorithm 15 simply computes the products $f\alpha_1, \ldots, f\alpha_r$ with arbitrary r. We will need that in Algorithm 17.

Lemma 6.3.34. *The Algorithm* CompEltProdList*, see Algorithm 16, is correct. It requires at most* $O^\sim(rn^{\omega-1} \deg(h))$ *operations in* k.

Proof. The correctness follows from all above considerations and the arguments in the proof of Theorem 6.3.32. By Remark 6.3.33, the matrix product $T_h \cdot M$ requires at most $O^\sim(rn^{\omega-1} \deg(h))$ operations in k. By the degree assumptions, we also know that the result has degree in $O(\deg(h))$ and thus Red_h requires, due to Lemma A.1.2 (iii), $O^\sim(rn \deg(h))$ operations in k. By assumption on the degrees of M and $\phi_\Omega(f)$, we know that the matrix

Algorithm 16 Computing products of given element with a list of elements

Precomputed	Reduced basis Ω of R_0; $y \in R_0$ primitive element of $\mathcal{K}_X(X)/k(x)$; $h \in k[x]$ coprime to the index ν of $k[x,y]$ in R_0; T_h and T'_h as in Definition 6.3.26
Input	$\phi_\Omega(f)$; $M = (\phi_\Omega(\alpha_1) \dots \phi_\Omega(\alpha_r)) \in k[x]^{n\times r}$ such that $\deg \phi_\Omega(f) + \deg(M) + 2c_X \leq \deg(h)$
Output	Matrix T representing $f\alpha_1, \dots, f\alpha_r$ with $\deg(T) \leq h$

1: **procedure** CompEltProdList($\phi_\Omega(f), M$)
2: $f' \leftarrow \text{Red}_h(T_h \cdot \phi_\Omega(f))$
3: $M' \leftarrow \text{Red}_h(T_h \cdot M)$
4: $N \leftarrow (\text{Mult}_y(f', M'e_1), \dots, \text{Mult}_y(f', M'e_r))$
5: **return** $\text{Red}_h(T'_h \cdot N)$

N computed in step 4 has degree in $O(\deg(h))$. Then Remark 6.3.33 again shows that the matrix product $T'_h \cdot N$ requires $O^\sim(rn^{\omega-1}\deg(h))$ operations in k. Moreover, the result has degree in $O(\deg(h))$ and thus Red_h requires, due to Lemma A.1.2 (iii), $O^\sim(rn\deg(h))$ operations in k. □

Remark 6.3.35. We could also use Algorithm 16 to compute the basis matrix of fR_0 by setting $M = E_n$ where E_n denotes the identity matrix in dimension n. But there is no need to do this since once we have computed the basis matrix M_f of fR_0, we can just compute $M_f \cdot M_I$ to compute the basis matrix of fI. △

6.3.3.2 Component Dependent Case

Let X be a reduced and reducible cover of $\mathbb{P}^1_k$ with irreducible components $(X_1, \dots, X_m)$. By $y_i \in R_{i,0}$ we denote a primitive element of $\mathcal{K}_{X_i}(X_i)$ over $k(x)$ as in Lemma 6.3.10. By $T_i \in k[x]^{n_i \times n_i}$ we denote the basis transformation matrix as in Definition 6.3.12, that is $(1, y_i, \dots, y_i^{n_i-1}) = \Omega_i \cdot T_i$. Moreover, let $h_i \in k[x]$ denote a polynomial which is coprime to the index of $S_i := k[x, y_i]$ in $R_{i,0}$. Furthermore, T_{h_i} denotes the matrix as in Definition 6.3.26.

Definition 6.3.36. Let $v = (v_1, \dots, v_m) \in R^m$ and $w = (w_1, \dots, w_n) \in R^n$ for R a commutative ring and $n, m \in \mathbb{N}$. By $v \frown w$ we denote the **concatenation of** v **and** w, that is $v \frown w = (v_1, \dots, v_m, w_1, \dots, w_n)$. △

Definition 6.3.37. Let X be a reduced cover of $\mathbb{P}^1_k$ with fixed order $(X_1, \dots, X_m)$ of irreducible components whose degrees over $\mathbb{P}^1_k$ are $n_1, \dots, n_m$, respectively, satisfying $\sum_{i=1}^m n_i = n$. We divide every $v \in k[x]^n$ into m vectors $v_1, \dots, v_m$ such that $v_i \in k[x]^{n_i}$ and $v = v_1 \frown \dots \frown v_m$. If $f \in R_0^+$ and $v = \phi_{\Omega_i^m}(f)$, then $v_i \in k[x]^{n_i}$ is the coefficient vector of $f_{|X_i}$ with regards to Ω_i, that is $v_i = \phi_{\Omega_i}(f_{|X_i})$. △

Note that Lemma 4.6.10 already told us that computing the product of $f, g \in R_0^+$ completely reduces to computing the products $f_{|X_i} g_{|X_i}$ where $f_{|X_i}$ denote the restriction of f with respect to the i-th irreducible component, that is to $R_{i,0}$. This already tells us how to compute the matrix T_f by computing the products $f_{|X_i}(w_j)_{|X_i}$.

Note that the suffix "C" in PrincBasMatC can be read as ***c**omponent dependent*.

Theorem 6.3.38. *The algorithm* PrincBasMatC*, see Algorithm 17, is correct. If d is an upper bound of $\max_{i=1}^m\{\deg(h_i)\}$ and $c_X \in O(d)$, it requires at most $O^\sim(n^\omega d)$ operations in k.*

Algorithm 17 Computing basis matrix of principal ideal: component dependent case

Precomputed	Basis Ω_i^m of R_0^+, T_Ω basis matrix of Ω with respect to Ω_i^m; for all $i = 1, \ldots, m$: $y_i \in R_{i,0}$ primitive elements of $F_i/k(x)$; $h_i \in k[x]$ coprime to the index ν_i of $k[x, y]$ in R_0; T_{h_i}, T'_{h_i} as in Definition 6.3.26
Input	$\phi_{\Omega_i^m}(f)$ such that for all $i = 1, \ldots, m$ and $j = 1, \ldots, m$ we have $\deg \phi_{\Omega_i^m}(f)_i + 3c_{X_i} \leq \deg(h_i)$
Output	T_f basis matrix of $f\omega_1, \ldots, f\omega_n$ with respect to Ω_i^m in n-block-form such that its i-th row block has degree bounded by $\deg \phi_{\Omega_i^m}(f)_i + 3c_{X_i}$

1: **procedure** PrincBasMatC($\phi_\Omega(f)$)
2: **for** $i = 1, \ldots, m$ **do**
3: $N_i \leftarrow$ SubMatrix$(M_\Omega, (1 + \sum_{j=1}^{i-1} n_j, 1), (n_i, n))$
4: $M_i \leftarrow$ CompEltProdList$(\phi_\Omega(f)_i, N_i)$
5: $T_f \leftarrow$ ColumnConcat$(M_1, \ldots, M_m)$
6: **return** T_f

Proof. We first prove the correctness: The matrix N_i computed in line 3 contains the coefficient vectors $\phi_{\Omega_i^m}(\omega_j)_i$ for $j = 1, \ldots, n$. Hence, by Lemma 6.3.34, the matrix M_i computed in step 4 contains the coefficient vectors of $f_{|X_i}(\omega_j)_{|X_i}$ for all $j = 1, \ldots, n$. By definition, the target matrix T_f contains as columns the vectors $\phi_{\Omega_i^m}(f\omega_j)$ for $j = 1, \ldots, n$. By Lemma 4.6.10, we have

$$\phi_{\Omega_i^m}(f\omega_j)^T = (\phi_{\Omega_1}((f\omega_j)_{|X_1}) \frown \ldots \frown \phi_{\Omega_m}((f\omega_j)_{|X_m}))^T,$$

and, moreover,

$$\begin{aligned} \deg \phi_{\Omega_i}((f\omega_j)_{|X_i}) &\leq \deg \phi_{\Omega_i}(f_{|X_i}) + \deg \phi_{\Omega_i}((\omega_j)_{|X_i}) + 2c_{i,X} \\ &\leq \deg \phi_{\Omega_i}(f_{|X_i}) + 3c_{i,X} \\ &\leq \deg h_i \end{aligned}$$

where we also used Corollary 4.6.1. In particular, T_f is in n-block-form whose i-th row block has degree bounded by $\deg \phi_{\Omega_i}(f_{|X_i}) + 3c_{i,X}$. Therefore, the matrix T_f equals the column style concatenated matrix obtained by the matrices $M_1, \ldots, M_m$ which finally proves the correctness of PrincBasMatC.

Now we prove the running time assertion. To do so, we investigate how many operations in k are needed to compute one of the m iterations in the **for** loop. By Definition 4.6.3 and Corollary 4.6.1, the matrices $N_1, \ldots, N_m$ have degree bounded by c_{X_i}, respectively. By Lemma A.1.2 (vi), the algorithm SubMatrix has constant cost. By Lemma 6.3.34, the computation of M_i requires $O^\sim(nn_i^{\omega-1}d_i)$ operations in k where $d_i = \deg \phi_{\Omega_i}(f)_i + \deg N_i + 2c_{X_i} \leq \deg \phi_{\Omega_i}(f)_i + 3c_{X_i} \leq \deg h_i$. Moreover, the result satisfies $\deg M_i \leq d_i \leq \deg h_i$. Hence the i-th iteration of the **for** loop requires, due to $n \geq n_i$ and $c_{X_i} \leq c_{i,X} \leq c_X$,

$$O^\sim\left(nn_i^{\omega-1}d_i\right) \subseteq O^\sim\left(nn_i^{\omega-1}d\right)$$

operations in k. Now the following simple computation

$$\sum_{i=1}^{m} nn_i^{\omega-1}d = nd\sum_{i=1}^{m} n_i^{\omega-1} \leq nd\left(\sum_{i=1}^{m} n_i\right)^{\omega-1} = ndn^{\omega-1} = n^\omega d$$

shows that the complete **for** loop requires $O^\sim(n^\omega d)$ operations in k. We have already argued above that $\deg(M_i) \leq d$ for all $i = 1, \ldots, m$ and thus, by Lemma A.1.2 (viii),

the computation of T_f has constant cost. Therefore, we obtain that PrincBasMatC requires, as asserted, at most $O^{\sim}(n^{\omega}d)$ operations in k. □

Remark 6.3.39. Let PrincBasMat denote the algorithm that, given a vector $v \in k[x]^n$ and a Boolean c, calls PrincBasMatC(v) if $c = true$ and PrincBasMatCF(v) if $c = false$ and then returns the result. △

Remark 6.3.40. By Remark 6.3.24, we may choose a suitable power of h_i to give it an intended degree such that the hypotheses

$$\deg \phi_{\Omega_i^m}(f)_i + \deg(\phi_{\Omega_i^m}(\omega_j)_i) + 2c_{X_i} \leq \deg(h_i) \tag{3:5}$$

for all $i = 1, \ldots, n$ are satisfied. Moreover, we know that $\deg(\phi_{\Omega_i^m}(\omega_j)_i) \leq c_X$, and if $\deg \phi_{\Omega_i^m}(f)_i \in O(c_X)$, then $\deg(h_i) \in O(c_X)$ is sufficient to satisfy the requirement Eq. (3:5). Hence the assumption in Theorem 6.3.38 is justified. Moreover, later on we will call the algorithms PrincBasMatC and PrincBasMatCF with input that has degree bounded by some d. Every time we do that, we assume that d is large enough to satisfy

$$\deg \phi_{\Omega_i^m}(f)_i + \deg(\phi_{\Omega_i^m}(\omega_j)_i) + 2c_{X_i} \leq \deg(h_i) \leq d$$

respectively

$$\deg \phi_{\Omega}(f) + 2c_X \leq \deg(h) \leq d.$$

Then both PrincBasMatC and PrincBasMatCF require at most $O^{\sim}(n^{\omega}d)$ operations in k. △

We want to end this section by noting that Algorithm 17 which computes the principal basis matrix in the component dependent case has the advantage over the algorithm applied in the component independent case that it is accessible for parallelisation.

6.4 Precomputations

As we have seen in the last section, there are some computations we need to carry out once to establish a computational respectively algorithmic environment in which we can use the presented algorithms to finally carry out the arithmetic in $\mathrm{Pic}^0(X)$. At the various points in this thesis where precomputed data was necessary, we already mentioned what needs to be precomputed. In the following we want to give an overview of what needs to be precomputed overall. Therefore, we briefly summarise what kind of such precomputations need to be done generally and which are necessary in the component independent respectively the component dependent case.

As mentioned in Notation 6.1.1, we compute and fix a reduced basis Ω of R_0 respectively $\mathcal{O}_X$ and reduced bases Ω_i of $R_{i,0}$ respectively $\mathcal{O}_{X_i}$. This implicitly includes the precomputation of the partition $n = \sum_{i=1}^{m} n_i$. The Ω_i then constitute the basis Ω_i^m. By T_Ω we compute the basis matrix of Ω with respect to Ω_i^m, that is, by definition we have $\Omega = \Omega_i^m \cdot T_\Omega$. By Lemma 4.6.2, we have $\deg T_\Omega \leq 2c_X$. Moreover, by Remark 4.6.4, we know that the change of representation with respect to Ω to a representation with respect to Ω_i^m can be done by multiplying with T_Ω. Furthermore, this change of representation is fast enough if the degree of the matrix respectively vector involved is linearly bounded by c_X. In Algorithm 6 we need explicit values or suitable bounds for the invariants $c_{i,X}$ for $i = 1, \ldots, m$ to compute a block-wise degree reduced basis matrix in the component dependent case. In Algorithm 9 we need the integer $\chi(\mathscr{S}_X)$ to be able to compute the degree of a given R_0-ideal regardless whether the ideal is represented by a matrix with respect to Ω or with respect to Ω_i^m. We have seen that the randomised algorithm ProvideIGS requires as input a finite subset Σ of the ground field k from which it chooses uniformly

random coefficients to come up with an ideal generating set. We can choose $\Sigma \subseteq k$ once and for all or use a separate one for every call of the randomised algorithms presented. In Section 6.3 we have seen that there are a number of necessary precomputations to deal with the computation of the basis matrices of principal ideals. First and foremost, we need to compute primitive elements $y \in R_0$ of $\mathcal{K}_X(X)$ over $k(x)$ respectively $y_i \in R_{i,0}$ of $\mathcal{K}_{X_i}(X_i)$ over $k(x)$ as in Lemmas 6.3.2 and 6.3.10. Then we need to compute the reducing polynomials $h, h_i \in k[x]$ which are coprime to the indices of $k[x,y]$ in R_0 respectively of $k[x,y_i]$ in $R_{i,0}$. Related to these, the matrices $T_h, T'_h \in k[x]^{n\times n}$ and $T_{h_i}, T'_{h_i} \in k[x]^{n_i\times n_i}$ as introduced in Definition 6.3.26 need be precomputed to transfer between the coefficient vector representation of elements in R_0 with respect to Ω respectively Ω_i^m to the bivariate polynomial representation in R_y, see Definition 6.3.20. This also involves the Bézout identity $1 = th + s\nu$ with respect to h and ν.

For the sake of the overview, we list the above precomputations enumerated and arranged by whether these are necessary in general or either for one of the two approaches, the component independent or the component dependent case.

Needed Precomputations:

(i) Generic precomputations:

(a) Reduced basis Ω of R_0 and reduced bases Ω_i of $R_{i,0}$ for all $i = 1, \dots, m$.

(b) The finite subset $\Sigma \subseteq k$ (not necessary).

(c) Basis transformation matrix T_Ω from Ω_i^m to Ω. We have $\deg T_\Omega \leq 2c_X$, see Lemma 4.6.2.

(d) The π-invariants $|X|_1, \dots, |X|_n$ of X and for all of its components $X_1, \dots, X_m$ the π-invariants $|X_i|_1, \dots, |X_i|_{n_i}$.

(ii) Precomputations in the component independent case:

(a) Primitive element $y \in R_0$ such that $\mathcal{K}_X(X) = k(x)[y]$.

(b) Basis transformation matrix T from Ω to $1, y, \dots, y^{n-1}$.

(c) Polynomial $h \in k[x]$ coprime to $\nu = \det(T)$ and the Bézout identity $1 = th + s\nu$.

(d) The matrices T_h and T'_h as in Definition 6.3.26,

$$T'_h = \textsc{Red}_h(T) \quad \text{and} \quad T_h = \textsc{Red}_h(s \operatorname{adj}(T)).$$

(iii) Precomputations in the component dependent case: For all $i = 1, \dots, m$ we compute

(a) $c_{1,X}, \dots, c_{m,X}$ and $\chi(\mathscr{S}_X)$.

(b) Primitive element $y_i \in R_{i,0}$ such that $F_i := \mathcal{K}_{X_i}(X_i) = k(x)[y_i]$.

(c) Basis transformation matrix T_i from Ω_i to $1, y_i, \dots, y_i^{n_i-1}$.

(d) Polynomial $h_i \in k[x]$ coprime to $\nu = \det(T_i)$ and the Bézout identity $1 = t_i h_i + s_i \nu_i$.

(e) The matrices T_{h_i} and T'_{h_i} as in Definition 6.3.26,

$$T'_{h_i} = \textsc{Red}_h(T_i) \quad \text{and} \quad T_{h_i} = \textsc{Red}_h(s_i \operatorname{adj}(T_i)).$$

Note that the multiplication tables for R_0 and $R_{i,0}$ for all $i = 1, \dots, m$ are strictly speaking necessary to represent the $\mathcal{O}_X$-module structure of an $\mathcal{O}_X$-ideal $\mathcal{F}$. But for the concrete computations within our algorithms we do not need them at all. That is, if we do not compute the multiplication tables, we solely represent the $\mathcal{O}_{\mathbb{P}^1}$-module $\pi_*\mathcal{F}$. But under the assumption that the input data of our algorithms represent an $\mathcal{O}_{\mathbb{P}^1}$-module $\pi_*\mathcal{F}$ with $\mathcal{F}$ being an $\mathcal{O}_X$-module, this suffices for our algorithms.

Remark 6.4.1. Moreover, note that we will not give a complete list of the necessary precomputations in every algorithm. We explicitly require that algorithm A which calls algorithm B has the precomputations available that algorithm B needs to have at hand for its own computations. △

6.5 Algorithms for Computing in the Picard group

In this section we will present the missing algorithms that enable us to compute in $\mathrm{Pic}^0(X)$. Further, we will discuss the respective running times of the algorithms. All presented algorithms can handle both the component independent and the component dependent case, see Section 5.6.2. We will give randomised algorithms for the computation of integral and arbitrary quotients and for reducing the degree of a class representative, see Algorithms 18 to 20. Moreover, we will provide deterministic algorithms (one for each case: component independent and component dependent) to determine whether a given representative of a class represents the trivial class, see Algorithms 21 and 22. Both together yield a deterministic algorithm to test whether a given class is the neutral one. All these algorithms will require at most $O^{\sim}(n^{\omega}d)$ operations in k where d is a suitable bound for the degree of the involved matrices and for the π-invariants of X. We will see in Section 6.6 that it can be shown that c_X is a valid value for d.

As outlined by Strategy 6.1.10, we start with an algorithm that computes the *integral* quotient of two R_0-ideals that represent elements in $\mathcal{I}_\pi/\mathcal{P}_\pi$, see Strategy 6.1.10 (I). Note that as already mentioned in Section 6.2, we need to come up with ideal generating sets of the involved denominator ideal to explicitly use Proposition 6.2.5 to compute a basis of the ideal quotient. See also Lemmas 6.2.10 and 6.2.12. As we have discussed in Section 6.2.2, we are able to provide an ideal generating set of an invertible ideal in a probabilistic way. That is, we may Σ-randomly choose k-linear combinations of a basis of the denominator ideal which together with a given modification function provides an ideal generating set with lower bounded probability, see Proposition 6.2.20 and Corollary 6.2.22. The algorithm ProvideIGS internally computes such an ideal generating set candidate and uses TestIGS to verify if it indeed is an ideal generating set. If so, it returns the respective ideal generating set and otherwise it returns that it failed. This provides a randomised algorithm IntegralDivision as follows in which we can plug in parameters that affect the probability of success.

Algorithm 18 Division of two ideals with integral result

Precomputed	Ω fixed reduced basis of R_0; Ω_i^m fixed basis of R_0^+; $\chi(\mathscr{S}_X)$; π-invariants $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ of X
Input	T_J, T_I, T_f matrices representing elements J, I, fR_0 in $\mathcal{I}_\pi/\mathcal{P}_\pi$, respectively, such that $JI^{-1} \subseteq R_0$; $f \in I$ a modification function of I; $r, t \in \mathbb{Z}_{\geq 1}$ probability parameters; Σ finite subset of k; c Boolean whether the matrices are basis matrices with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$)
Output	Basis matrix T_H where $H \subseteq R_0$ and $H \equiv JI^{-1}$ in $\mathcal{I}_\pi/\mathcal{P}_\pi$ if successful; otherwise 0

1: **procedure** IntegralDivision($T_J, T_I, T_f, r, t, \Sigma, c$)
2: $d_{JI^{-1}} \leftarrow$ DegOfIdeal(T_J, c) $-$ DegOfIdeal(T_I, c)
3: **if** $d_{JI^{-1}} = 0$ **then** || $I = J$
4: **return** E_n
5: isIGS, $[(\beta_1, \ldots, \beta_h), (T_{\beta_1}, \ldots, T_{\beta_h})] \leftarrow$ ProvideIGS($T_I, T_f, r, t, \Sigma, c$)
6: **if** isIGS $=$ *false* **then** || no IGS found
7: **return** 0
8: $T_H \leftarrow$ IdealQuotient($T_J, T_f, T_{\beta_1}, \ldots, T_{\beta_h}$)
9: **return** T_H

Lemma 6.5.1. *The algorithm* IntegralDivision*, see Algorithm 18, is correct. If $r, t \in O^\sim(1)$, d is an upper bound for all the degrees of the input matrices and $c_X \in O(d)$, then it requires at most $O^\sim(n^\omega d)$ operations in k and returns a matrix with degree bounded by $d + (\mu_X + 2)c_X \in O(d)$. The probability of* IntegralDivision *successfully returning a basis matrix is lower bounded by $1 - 2^{-rt}$. In particular, with $r = \log_2(n)$ the above probability becomes lower bounded by $1 - n^{-t}$.*

Proof. We consider the correctness of IntegralDivision first. By Lemma 6.1.8, we know that $d_{JI^{-1}} = \deg_k JI^{-1}$. Thus if $d_{JI^{-1}} = 0$, then by Lemma 6.2.3, it follows that $J = I$. Assume that ProvideIGS does not fail at line 5. By Lemma 6.2.25, we know that $I = fR_0 + \sum_{i=1}^h \beta_i R_0$. Therefore, by the correctness of IdealQuotient, see Lemma 6.2.9, T_H computed at line 8 is indeed a basis matrix of JI^{-1}. This proves the correctness of IntegralDivision.

Assume that d is an upper bound of the degrees of the input matrices. By Lemma 6.1.8, the computation of $d_{JI^{-1}}$ at line 2 requires at most $O^\sim(n^\omega d)$ operations in k. By the assumption on d, Lemma 6.2.25 provides that ProvideIGS requires at most $O^\sim(n^\omega d)$ operations in k and returns matrices with degrees bounded by $d + 2c_X$. By assumption on d, the latter is still in $O(d)$. Hence $d + 2c_X$ is now a common upper bound for the input matrices of IdealQuotient in line 8 and thus by Lemma 6.2.9 and Corollary 6.2.14, IdealQuotient requires at most $O^\sim(n^\omega d)$ operations in k and T_H has degree upper bounded by $d + 2c_X + \mu_X c_X = d + (\mu_X + 2)c_X$ which is still in $O(d)$ by assumption. This proves the assertions about the output degree and the running time.

Now we consider the assertion regarding the probability of IntegralDivision being successful. This is the case if and only if ProvideIGS in line 5 successfully provides and ideal generating set of I. By Lemma 6.2.25, the probability for the above is lower bounded by $1 - 2^{-rt}$ which provides the last part of the assertion. □

To be able to compute arbitrary quotients, we need to employ modification functions as indicated by Strategy 6.1.10 (II). The following algorithm provides the functionality of computing such arbitrary quotients. In addition to IntegralDivision it invokes the algorithm ModFct that provides a modification functions and the algorithm PrincBasMat

which computes the respective principal ideal basis matrix. This results in a randomised algorithm which again enables us to alter the lower bound of the probability of success.

Algorithm 19 Division of arbitrary ideals

Precomputed	Bases Ω of R_0 and Ω_i^m of R^+; π-invariants $-\lvert X\rvert_i$ of X and $-\lvert X_i\rvert_j$ of all X_i
Input	T_J, T_I matrices representing elements I respectively J in $\mathcal{I}_\pi$; $r, t \in \mathbb{Z}_{\geq 1}$ probability parameters; Σ finite subset of k; c Boolean whether the matrices are basis matrices with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$)
Output	Basis matrix T_H where $H \equiv JI^{-1}$ in $\mathcal{I}_\pi/\mathcal{P}_\pi$ and $H \subseteq R_0$ if successful; otherwise 0

1: **procedure** Division($T_J, T_I, r, t, \Sigma, c$)
2: $f \leftarrow$ ModFct(T_I, c)
3: $T_f \leftarrow$ PrincBasMat(f, c)
4: $T_H \leftarrow$ IntegralDivision($T_f \cdot T_J, T_I, T_f, r, t, \Sigma, c$)
5: **if** $T_H \neq 0$ **then**
6: **return** T_H || IntegralDivision failed
7: **return** 0 || IntegralDivision successful

Lemma 6.5.2. *The algorithm* Division*, see Algorithm 19, is correct. Moreover, if d is an upper bound both for the degree of the input matrices and for the π-invariants $-\lvert X\rvert_1, \ldots, -\lvert X\rvert_n$ and $-\lvert X_1\rvert_{n_1}, \ldots, -\lvert X_m\rvert_{n_m}$, then it requires at most $O^\sim(n^\omega d)$ operations in k and returns a matrix with degree in $O(d)$. The probability that* Division *is successful is lower bounded by $1-2^{-rt}$. In particular, with $r = \log_2(n^2)$ the above probability becomes lower bounded by $1 - n^{-t}$.*

Proof. Since d is an upper bound of the degrees of the input matrices, the computation of f in line 2 requires at most $O^\sim(n^\omega d)$ operations in k and returns a vector with degree bounded by $2d$, see Remark 5.7.26 and Theorems 5.7.20 and 5.7.23. Thus by Remark 6.3.39, PrincBasMat requires $O^\sim(n^\omega d)$ operations in k and returns a matrix with degree in $O(d)$. By Lemma 6.2.15, we know that the product $T_f \cdot T_J$ is a basis matrix of fJ and satisfies $\deg(T_f \cdot T_J) \in O(d)$. Therefore, by Lemma 6.5.1, the computation of T_H requires at most $O^\sim(n^\omega d)$ operations in k and returns a matrix with degree in $O(d)$ if it is successful. This provides the correctness of Division and proves the running time assertion. Moreover, by Lemma 6.5.1, we also know that the computation of T_H is successful with probability at least $1 - 2^{-rt}$ which completes the proof. □

In Strategy 6.1.10 (III) we have already mentioned that the degree of the representative resulting from computing the quotient of two ideals may increase. Moreover, by Propositions 5.9.1 and 5.9.6, we indeed see that the resulting representative has degree which is larger than the initial nominator in the order of nc_X and $g(X, \mathscr{S}_X)$, see Proposition 5.9.1 respectively Proposition 5.9.6. The following algorithm uses modification functions in accordance with the ideas presented in Proposition 5.8.7 and Corollary 5.9.3 as well as the algorithm ReduceBasisMatrix to compute a degree reduced representative of the input class. Since it uses the IntegralDivision algorithm twice, it is also a randomised algorithm similar to IntegralDivision and Division.

Algorithm 20 Reduction of the class representative

Precomputed	Bases Ω of R_0 and Ω_i^m of R^+; π-invariants $-\lvert X\rvert_i$ of X and $-\lvert X_i\rvert_j$ of all X_i
Input	T_I matrix representing an element I in $\mathcal{I}_\pi$; $r,t \in \mathbb{Z}_{\geq 1}$ probability parameters; Σ finite subset of k; c Boolean whether the matrices are basis matrices with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$)
Output	Basis matrix T_H if successful where $H \equiv I$ in $\mathcal{I}_\pi/\mathcal{P}_\pi$ such that $H \subseteq R_0$ and bounded degree, see Lemma 6.5.3; otherwise 0

1: **procedure** ReduceRepresentative(T_I, r, t, Σ, c)
2: $T_I \leftarrow$ ReduceBasisMatrix(T_I, c)
3: $f \leftarrow$ ModFct(T_I, c) || mod. fct. of I
4: $T_f \leftarrow$ PrincBasMat(f, c)
5: $T_J \leftarrow$ ReduceBasisMatrix(IntegralDivision($T_f, T_I, T_f, r, t, \Sigma, c$), c)
6: **if** $T_J = 0$ **then** || line 5 failed
7: **return** 0
8: $g \leftarrow$ ModFct(T_J, c) || mod. fct. of J
9: $T_g \leftarrow$ PrincBasMat(g, c)
10: $T_H \leftarrow$ ReduceBasisMatrix(IntegralDivision($T_g, T_J, T_g, r, t, \Sigma, c$), c)
11: **if** $T_H = 0$ **then** || line 10 failed
12: **return** 0
13: **return** T_H

Lemma 6.5.3. *The algorithm* ReduceRepresentative*, see Algorithm 20, is correct. We distinguish between the cases $c = true$ and $c = false$:*

(i) $c = true$: Let d be a common upper bound of: the degree of T_I, the invariants $-\lvert X_i\rvert_{n_i}$ and $(\deg_k I_i)/n_i + c_{i,X}$. Furthermore, assume that $c_X \in O(d)$. Then ReduceRepresentative *requires at most $O^\sim(n^\omega d)$ operations in k. Moreover, it returns a basis matrix T_H in n-block-form with row blocks $T_{H,i}$ such that $\deg T_{H,i} \leq 3c_{i,X}$.*

(ii) $c = false$: Let d be both an upper bound of the degree of T_I and for the π-invariants $\{-\lvert X\rvert_n,\ -\lvert X_i\rvert_{n_i} \mid i = 1,\dots,m\}$. Furthermore, assume that $c_X \in O(d)$. Then ReduceRepresentative *requires at most $O^\sim(n^\omega d)$ operations in k. Moreover, it returns a matrix T_H with degree bounded by $(\mu_X + 2)c_X$.*

The probability that ReduceRepresentative *is successful is lower bounded by $1-2^{-rt+1}$. In particular, with $r = \log_2(n^2)$ the above probability becomes lower bounded by $1 - n^{-t+1}$.*

Proof. We first prove the correctness of ReduceRepresentative. Due to the correctness of ModFct and PrincBasMat, T_f is indeed the basis matrix of a modification function of I, see Remarks 5.7.26 and 6.3.39. Thus the input of IntegralDivision in line 5 is correct and hence, by Lemma 6.5.1, we know that the ideal J, whose basis matrix T_J is computed in line 5, equals $fI^{-1} \subseteq R_0$. The same line of argument as above shows that T_H computed in line 10 is indeed the basis matrix of $H = gJ^{-1} = g(fI^{-1})^{-1} = (gf^{-1})I$.

By Corollaries 5.8.8 and 5.9.3, we see that the above steps do indeed compute a representative H of the same class as I in $\mathcal{I}_\pi/\mathcal{P}_\pi$ such that either $\deg_k H_{\lvert X_i} \leq 2c_{i,X}n_i$ if $c = true$ or $\deg_k H \leq (\mu_X+1)c_X n$ if $c = false$. By Corollary 4.5.5 and Lemma 4.3.28, we know that $\deg \mathrm{RedMat}(T_H)$ is bounded by $(\deg_k H)/n + \mu_X c_X \leq (2\mu_X+1)c_X$ in the case $c = false$. If $c = true$, by Propositions 4.4.20 and 4.4.21, we know that RowBlockReduce(T_H) is in n-block-form with row blocks $T_{H,i}$ satisfying $\deg T_{H,i} \leq (\deg_k H_{\lvert X_i})/n_i + c_{i,X} \leq 3c_{i,X}$. This proves the correctness of ReduceRepresentative.

Now we prove the assertion concerning the running time of ReduceRepresentative. First, assume that $c = \mathit{false}$. Since $\deg T_I \leq d$, Definition 4.6.8 and Theorem A.2.7 provide that ReduceBasisMatrix at line 2 requires at most $O^{\sim}(n^\omega d)$ operations in k and returns a matrix with degree bounded by $(\deg_k I)/n+\mu_X c_X$, see Lemma 4.3.28 and Corollary 4.5.5. In particular, its degree is still bounded by d. Therefore, the computation of f in line 3 requires at most $O^{\sim}(n^\omega d)$ operations in k and returns a vector with degree bounded by $2d$, see Theorem 5.7.20. Thus, to apply Theorem 6.3.32, the precomputed h need to satisfy $2d + 2c_X \leq \deg h$. Then PrincBasMat requires at most $O^{\sim}(n^\omega d)$ operations in k and returns a matrix with degree bounded by $2d+2c_X$. By Lemma 6.5.1, IntegralDivision requires at most $O^{\sim}(n^\omega(2d + 2c_X))$ operations in k and returns a matrix with degree bounded by $2d+2c_X+(\mu_X+2)c_X = 2d+(\mu_X+4)c_X$. Note that ReduceBasisMatrix in line 5 does nothing in the case $c = \mathit{false}$ since it only calls RedMat which is already called inside of IntegralDivision. Again, by Theorem 5.7.20, the computation of g at line 8 requires at most $O^{\sim}(n^\omega(2d+(\mu_X+4)c_X))$ operations in k and returns a vector with degree bounded by $4d+(2\mu_X+8)c_X$. Thus, to apply Theorem 6.3.32, the precomputed h need to satisfy $4d+(2\mu_X+8)c_X+2c_X = 4d+(2\mu_X+10)c_X \leq \deg h$. Then PrincBasMat requires at most $O^{\sim}(n^\omega(4d + (2\mu_X + 10)c_X))$ operations in k and returns a matrix with degree bounded by $4d + (2\mu_X + 10)c_X$. By Lemma 6.5.1, IntegralDivision at line 10 requires at most $O^{\sim}(n^\omega(4d + (2\mu_X + 10)c_X))$ operations in k and returns a matrix with degree bounded by $4d + (2\mu_X + 10)c_X + (\mu_X + 2)c_X = 4d + (3\mu_X + 12)c_X$. Finally, by Theorem A.2.7, RedMat at line 15 requires $O^{\sim}(n^\omega(4d + (3\mu_X + 12)c_X))$ operations in k. The running time is clearly bounded by $O^{\sim}(n^\omega(4d + (3\mu_X + 12)c_X))$ operations in k. The assumption $c_X \in O(d)$ now provides that the overall running time is bounded by $O^{\sim}(n^\omega d)$.

Let us now consider the case $c = \mathit{true}$. By Proposition 4.6.7, ReduceBasisMatrix at line 2 requires at most $O^{\sim}(n^\omega d)$ operations in k and provides a basis matrix T_I in n-block-form whose i-th row block has degree bounded by $(\deg_k I_i)/n_i + c_{i,X} \leq d$. By Theorem 5.7.23, the vector $f = (f_1, \ldots, f_m)^T$ computed in line 3 satisfies

$$\deg f_i \leq ((\deg_k I_i)/n_i + c_{i,X}) + c_{X_i} \leq (\deg_k I_i)/n_i + 2c_{i,X}. \tag{5:6}$$

To apply Theorem 6.3.38, the precomputed polynomials h_i need to satisfy $\deg h_i \geq \deg f_i + 3c_{X_i}$ and thus, by the above,

$$\deg h_i \geq (\deg_k I_i)/n_i + 5c_{i,X}$$

is sufficient. In this case PrincBasMat in line 4 returns a matrix whose i-th row block is degree bounded by $(\deg_k I_i)/n_i + 5c_{i,X}$ and it requires at most $O^{\sim}(n^\omega d)$ operations in k to do so. Now $(\deg_k I_i)/n_i + 5c_{i,X}$ is a common degree upper bound for the i-th row block of T_f and T_I. Thus $\delta := \max_{i=1}^{m}\{(\deg_k I_i)/n_i + 5c_{i,X}\} \leq d + 4c_X$ is a common degree upper bound of T_f and T_I. Therefore, by Lemma 6.5.1, IntegralDivision in line 5 requires at most $O^{\sim}(n^\omega\delta)$ operations in k and returns a matrix with degree bounded by $\delta + (\mu_X + 2)c_X \leq d + (\mu_X + 6)c_X \in O(d)$. Also in line 5, by Proposition 4.6.7, ReduceBasisMatrix returns a matrix whose i-th row block has degree bounded by

$$\begin{aligned}(\deg_k J_i)/n_i + c_{i,X} &= (\deg_k f_i R_{i,0} - \deg_k I_i)/n_i + c_{i,X}\\ \text{Eq. (5:6)} \rightsquigarrow &\leq (\deg_k I_i + 2c_{i,X}n_i - \deg_k I_i)/n_i + c_{i,X}\\ &= 3c_{i,X} \in O(d).\end{aligned}$$

In particular, $\deg T_J \leq 3c_X$. Since the input matrix had degree bounded by $d + (\mu_X + 6)c_X \in O(d)$, ReduceBasisMatrix requires at most $O^{\sim}(n^\omega d)$ operations in k to compute T_J. Now as before with f, we see that the vector $g = (g_1, \ldots, g_m)^T$ computed in line 8

satisfies

$$\deg g_i \leq (\deg_k J_i)/n_i + c_{i,X} + c_{X_i} = (\deg_k J_i)/n_i + 2c_{i,X} \leq 4c_{i,X}. \tag{5:7}$$

To apply Theorem 6.3.38, the precomputed polynomials h_i need to satisfy $\deg h_i \geq \deg g_i + 3c_{X_i}$ and thus, by the above, $\deg h_i \geq 7c_{i,X}$ is sufficient. In this case PrincBasMat in line 9 returns a matrix whose i-th row block is degree bounded by $7c_{i,X}$. Therefore, $7c_X \in O(d)$ is a common degree bound for both T_g and T_J. Therefore, by Lemma 6.5.1, IntegralDivision requires at most $O^{\sim}(n^{\omega}d)$ operations in k and returns a matrix with degree bounded by $7c_X + (\mu_X + 2)c_X = (\mu_X + 9)c_X \in O(d)$. By Proposition 4.6.7, ReduceBasisMatrix in line 10 returns a matrix whose i-th row block has degree bounded by

$$(\deg_k H_i)/n_i + c_{i,X} \leq 2c_{i,X} + c_{i,X} = 3c_{i,X},$$

see Corollary 5.8.8. Moreover, since the degree of the input matrix was bounded by $(\mu_X + 9)c_X \in O(d)$, it only requires at most $O^{\sim}(n^{\omega}d)$ operations in k. This proves the running time assertion.

ReduceRepresentative is successful if and only if the two calls of IntegralDivision are successful. This probability is lower bounded by

$$(1 - 2^{-rt})^2 = (1 - 2^{-rt+1} + 2^{-2rt}) \geq (1 - 2^{-rt+1})$$

which completes the proof. □

The algorithms IntegralDivision, Division and ReduceBasisMatrix together provide a toolkit to compute in $\mathcal{I}_\pi/\mathcal{P}_\pi$ and thus in $\mathrm{CaCl}^0_\pi(X)$, $\mathrm{CaCl}^0(X)$ as well as in $\mathrm{Pic}^0(X)$. The Division algorithm can either be seen to already carry out the group law of $\mathrm{Pic}^0(X)$ or it can be applied twice to compute products instead of quotients respectively sums instead of differences. Moreover, being able to compute quotients respectively differences of group elements using Division, we can therefore also compute the inverse of a given element. After every such operation, the algorithm ReduceBasisMatrix can be applied to reduce the resulting representative and to obtain one that is given by either a matrix in n-block-form with row blocks of degree bounded by $3c_{i,X}$ (in the component dependent case) or by a matrix with degree bounded by $(\mu_x + 2)c_X \leq 4c_X$ in the component independent case.

Therefore, the only missing part of a complete toolkit for the arithmetic in $\mathrm{Pic}^0(X)$ is to give an algorithm that tests whether a given element is the neutral one of the group or equivalently (given the possibility to carry out the group law and computing the inverse) one that decides whether two given elements are equal. This is what follows next.

Propositions 5.9.4 and 5.9.8 did already show what is needed to test whether a given representative $\mathcal{F}$ represents the trivial class in $\mathrm{Pic}^0(X)$. From this we deduce the following algorithms in the respective cases. We start with the component independent case.

Algorithm 21 Zero test if X is irreducible

Precomputed	Reduced basis Ω of R_0; π-invariants $-\lvert X\rvert_1 \leq \ldots \leq -\lvert X\rvert_n$ of X
Input	$T_{\mathcal{F}} \in k[x]^{n\times n}$ representing $\mathcal{O}_X$-ideal $\mathcal{F}$
Output	*true* if $\mathcal{F}$ represents the trivial element in $\mathrm{CaCl}^0_\pi(X)$; otherwise *false*

1: **procedure** ZeroTestIntegral($T_{\mathcal{F}}$)
2: $d_1, \ldots, d_n \leftarrow$ PiInvariants($T_{\mathcal{F}}$)
3: **if** $d_1 \leq 0$ **then**
4: **return** *true*
5: **return** *false*

Lemma 6.5.4. *The algorithm* ZeroTestIntegral*, see Algorithm 21, is correct. Moreover, if d is a common upper bound of $\deg T_{\mathcal{F}}$ and $-\lvert X\rvert_n$, then* ZeroTestIntegral *requires at most $O^{\sim}(n^\omega d)$ operations in k.*

Proof. By Lemma 4.3.21, the algorithm PiInvariants requires at most $O^{\sim}(n^\omega d)$ operations in k and thus the assertion follows. □

Now we state the respective algorithm in the component dependent case.

Algorithm 22 Zero test if X is reducible

Precomputed	Basis Ω_i^m of R_0^+ or basis Ω of R_0 dependent on the Boolean c; for all $i = 1, \ldots, m$: π-invariants $-\lvert X_i\rvert_1 \leq \ldots \leq -\lvert X_i\rvert_{n_i}$ of X_i
Input	$T_{\mathcal{F}}$ basis matrix of $\mathcal{O}_X$-ideal $\mathcal{F} = \mathcal{O}_X(D)$ with $D = D_0 + \sum_{i\in A} r_i(x)_{i,\infty}$ either with respect to Ω_i^m ($c = true$) or with respect to Ω ($c = false$); c Boolean whether $T_{\mathcal{F}}$ is with respect to Ω_i^m or Ω
Output	*true* if $\mathcal{F}$ represents the trivial element in $\mathrm{CaCl}^0_\pi(X)$, *false* otherwise

1: **procedure** ZeroTest(T, c)
2: $T_1, \ldots, T_m \leftarrow$ ComputeComponentMatrices(T, c)
3: **for** $i = 1, \ldots, m$ **do**
4: $\alpha_i \leftarrow$ SubMatrix($T_i, (1,1), (n_i, 1)$))
5: $d_i \leftarrow (d_{i,1}, \ldots, d_{i,n_i}) \leftarrow$ PiInvariants(T_i)
6: $r_i \leftarrow$ DegOfIdeal(T_i, c)$/n_i$
7: **if** $r_i < d_i$ **then**
8: **return** *false*
9: $\alpha \leftarrow$ ColumnConcat($\alpha_1, \ldots, \alpha_m$)
10: $(g\beta, g) \leftarrow$ RationalSystemSolve(T, α)
11: **if** $\deg(g) \neq 0$ **then**
12: **return** *false*
13: **return** *true*

Lemma 6.5.5. *The algorithm* ZeroTest*, see Algorithm 22, is correct whenever $T_{\mathcal{F}}$ represents an element of $\mathrm{CaCl}^0_\pi(X)$. Moreover, if $T_{\mathcal{F}}$ has degree bounded by d and d is also an upper bound for all $-\lvert X_1\rvert_{n_i}, \ldots, -\lvert X_m\rvert_{n_m}$, then* ZeroTest *requires at most $O^{\sim}(n^\omega d)$ operations in k.*

Proof. We first prove the correctness. Let $\mathcal{F} = \mathcal{O}_X(E)$ with $E = D + \sum_{i\in A} r_i(x)_{i,\infty}$. Note that $E = D + r(x)_\infty$ is possible. We abbreviate $\mathcal{F}_i := \mathcal{F}_{|X_i}$. For all $i = 1, \ldots, m$ let $\alpha_{i,1}, \ldots, \alpha_{i,n_i}$ denote a reduced basis of $\mathcal{F}_i(V_{i,0})$ and define α to satisfy $\phi_{\Omega_i^m}(\alpha) = \phi_{\Omega_1}(\alpha_{1,1}) \frown \ldots \frown \phi_{\Omega_m}(\alpha_{m,1})$. By Proposition 5.9.8, $\mathcal{F}$ represents the trivial class if and only if $\deg_k \mathcal{F}_i(V_{i,0})/n_i = r_i \geq -\lvert\mathcal{F}_i\rvert_1$ for all $i = 1, \ldots, m$ and $\alpha \in \mathcal{F}(V_0)$. Before the **for**

loop, ComputeComponentMatrices computes the basis matrices $T_{\mathcal{F}_i}$ of reduced bases $\alpha_{i,1}, \ldots, \alpha_{i,n_i}$ of $\mathcal{F}_i(V_{i,0})$. That ComputeComponentMatrices does indeed return the asserted matrices and that it at most requires $O^{\sim}(n^\omega d)$ operations in k, follows from Proposition 4.6.5.

The i-th iteration of the **for** loop computes

(i) by α_i the coefficient vector $\phi_{\Omega_i}(\alpha_{i,1})$, this is due to what SubMatrix does, see Notation A.1.1 (vi),

(ii) by r_i it computes the number r_i from the representation of E above; this is due to the fact that

$$\deg_k \mathcal{F}_i(V_{i,0})/n_i = r_i$$

and Proposition 5.6.9, Proposition C.4.18 (ii) as well as what DegOfIdeal does, see Algorithm 9,

(iii) by $d_i = -|\mathcal{F}_i|_1$ the respective first invariant of $\mathcal{F}_i$, this is due to the correctness of PiInvariants, see Lemma 4.3.21.

By what we have said above, see Proposition 5.9.8, if in some iteration of the **for** loop we have $r_i < d_i$, then $\mathcal{F}$ is indeed not principal. After we have passed the loop completely, we know that $r_i \geq -|\mathcal{F}_i|_1$ and thus $\mathcal{F}$ is principal if and only if $\alpha \in \mathcal{F}(V_0)$. Due to what ColumnConcat does, see Notation A.1.1 (viii), we know that the computation of α is indeed correct and has constant cost, see Lemma A.1.2 (viii). Since $T_{\mathcal{F}}$ has non-zero determinant, by Theorem A.2.13, we know that the algorithm RationalSystemSolve computes a tuple $(g\beta, g)$ where $\beta \in k(x)^n$ is a solution of $T_{\mathcal{F}} \cdot \beta = \alpha$ and $g \in k[x]$ of minimal degree such that $g\beta \in k[x]^n$. In particular, $\beta \in k[x]^n$ if and only if $\deg(g) = 0$. Therefore, $\alpha \in \mathcal{F}(V_0)$ if and only if $\deg(g) = 0$ which finally provides the correctness of ZeroTest.

Now we prove the asserted running time complexity. By assumption, the matrix T has degree bounded by d. Hence, by Proposition 4.6.5, the matrices $T_1, \ldots, T_m$ have degree bounded by d as well. By Lemma A.1.2 (vi), calling SubMatrix in line 4 has constant cost. Since $\deg T_i \leq d$, by Lemma 4.3.21, the algorithm PiInvariants in step 5 requires at most $O^{\sim}(n_i^\omega d)$ operations in k. Moreover, by Lemma 6.1.8, DegOfIdeal requires at most $O^{\sim}(n_i^\omega d)$ operations in k. Hence each iteration of the **for** loop requires at most $O^{\sim}(n_i^\omega d)$ operations in k. Now we have

$$\sum_{i=1}^{m} n_i^\omega d = d \cdot \sum_{i=1}^{m} n_i^\omega \leq d \cdot \left(\sum_{i=1}^{m} n_i \right)^\omega = d \cdot n^\omega$$

and therefore, the **for** loop altogether requires at most $O^{\sim}(n^\omega d)$ operations in k.

Since T_i has degree bounded by $2d$, the same is true for α_i computed in line 4. Again, calling ColumnConcat has constant cost as mentioned above. Therefore, the input matrix T has degree bounded by d and α has degree bounded by $2d$ and thus, by Corollary A.2.14, the algorithm RationalSystemSolve in step 10 requires at most $O^{\sim}(n^\omega d)$ operations in k which finally completes the proof. □

The algorithms presented in this section constitute a complete toolkit to compute in $\mathrm{Pic}^0(X)$ solely depending on the degree and the dimension of the input matrices (and bounds for the invariants $-|X|_n$ respectively $-|X_i|_{n_i}$) representing the respective elements in $\mathrm{Pic}^0(X)$. In the next section we summarise all of this in a theorem that represents the main result of this thesis.

6.6 Main Result

The following theorem summarises that the presented algorithms provide a complete toolkit to compute in $\mathrm{Pic}^0(X)$. It also represents the main result of this thesis.

Theorem 6.6.1. *Let X be a reduced cover of $\mathbb{P}^1_k$. The elements in $\mathrm{Pic}^0(X)$ can be represented by matrices in $k[x]^{n\times n}$ with degree in $O(c_X)$. The combination of the Algorithms 19 and 20 provides randomised algorithms to compute both the group law in $\mathrm{Pic}^0(X)$ and the inverse of a given element. Moreover, Algorithms 21 and 22 provide a deterministic algorithm to test whether a given element in $\mathrm{Pic}^0(X)$ is the neutral element. All the above algorithms use at most $O^{\sim}(n^\omega c_X)$ operations in k and the randomised algorithms have positive constant success probability.*

Proof. That we can represent every element in $\mathrm{CaCl}^0(X)$ with a matrix in $k[x]^{n\times n}$ follows from Lemma 6.1.4 in the case that X is integral and from Lemma 6.1.6 when X is reducible. By Corollaries 5.8.6 and 5.8.9, for each such representative there exists a basis matrix with degree in $O(c_X)$.

By Lemma 6.5.2, Algorithm 19 computes a matrix representation of the difference of two divisor representatives which is the same as the division of the corresponding R_0-ideals. Now we can use subtraction as the group law of $\mathrm{CaCl}^0(X)$ or just subtract twice to compute the sum of two given divisor representatives respectively the product of two given ideal representatives. Using Algorithm 20 after each call of Algorithm 19 guarantees that the degree of the respective divisor and representing matrix is still in the desired order. To compute the inverse of a given element in $\mathrm{CaCl}^0(X)$, we can call Algorithm 19 to divide the neutral element by the given representative. By Lemma 6.5.2, Algorithm 19 requires at most $O^{\sim}(n^\omega d)$ operations in k if d is an upper bound for both the degree of the input matrix and the invariants $-|X_i|_{n_i}$, $i = 1, \dots, m$, and $-|X|_n$. By Corollaries 4.3.24 and 4.5.2, we know that c_X itself is a bound for all the above invariants. As we have seen above, the input matrices have degree in $O(c_X)$ which thus provides that Lemma 6.5.2 requires at most $O^{\sim}(n^\omega c_X)$ operations in k. Also note that we precompute the polynomials $h_1, \dots, h_m$ such that their degree bounds the degree of all appearing instances of modification functions and still have degree in $O(c_X)$. The statement about the success probability follows immediately since we need to apply Algorithms 19 and 20 at most in succession, and therefore, the assertion follows from Lemmas 6.5.2 and 6.5.3. With the same arguments as above the asserted running time for Algorithms 21 and 22 follow from Lemmas 6.5.4 and 6.5.5. □

Theorem 6.6.1 states that the asymptotic running time complexity of the problem of computing in $\mathrm{Pic}^0(X)$ for a reduced cover X of $\mathbb{P}^1_k$ is bounded by $O^{\sim}(n^w c_X)$ operations in k where n denotes the degree of X over $\mathbb{P}^1_k$ and c_X an invariant of X defined in Definition 2.4.10. For simplicity, in the case of X being irreducible, c_X is roughly equal to g/n where g denotes the arithmetic genus of X and in the case of X being reducible, c_X is roughly equal to the maximum of the c_{X_i} of the irreducible components of X, see Remark E.2.21. For a thorough comparison of Theorem 6.6.1 with the existing algorithms, see Section 1.3 and Table 1.2.

Remark 6.6.2. We note that Theorem 6.6.1 does not discriminate between the component dependent and the component independent representation of the elements in $\mathrm{CaCl}^0_\pi(X)$ since the asymptotic running time is the same. Though the basis matrices in these two cases have the same degree (maximal appearing degree), we would like to emphasise that the component dependent representation is better than the component independent representation with respect to the following: In the component independent case the restrictions of the represented divisor satisfy the same degree bound which depends on a global invariant of X. But in the component dependent case each restriction satisfies a different

degree bound that only depends on an invariant of the component (and additionally on the order of the components). In a nutshell, this means that in the component independent case the degree bounds of the restrictions of the represented divisor are all the same and in the component dependent case they can be chosen to be optimal with respect to the respective component. △

Theorem 6.6.1 unites the results of the two approaches we presented in this thesis, the component independent and the component dependent case. Both cases are very similar in the sense that they both follow the strategy we outlined in Strategy 6.1.10. Though both work with different type of representatives of elements in $\mathrm{Pic}^0(X)$, we were able to prove the existence of representatives of both types that have bounded degree and therefore have representing matrices of bounded degree as well. In both cases we heavily rely on the modification functions which can be employed to reduce the general division of two ideals to the case of integral division of ideals, see Strategy 6.1.10 (II). Moreover, we can use them to find new representatives of a given class in $\mathrm{Pic}^0(X)$ that have bounded degree again, see Strategy 6.1.10 (III). Therefore, both approaches rely on modification functions, but they need to compute them in a different way due to the different representation types. However, the test whether a given element is the neutral element of $\mathrm{Pic}^0(X)$ is independent from modification functions and needs to be implemented differently depending on whether X is irreducible or reducible.

Additionally, we want to note that we can easily compute the neutral element of $\mathrm{Pic}^0(X)$ within our representation setup: The identity matrix of dimension n works in both the component independent and component dependent case.

Appendices

Appendix A

Used Algorithms

A.1 Basic Matrix Algorithms

In this section we collect some basic matrix algorithms that use naive attempts to solve simple tasks with respect to matrices over the polynomial ring $k[x]$. The reason we mention such algorithms and collect them here is the readability of the algorithms we propose throughout this thesis.

The following enumeration determines names of algorithms together with a description of what these algorithms compute. We will explicitly assume that we use the fastest known implementations of algorithms solving the described task. In Lemma A.1.2 we will give naive and known bounds for the running time of those algorithms.

Notation A.1.1.

(i) By MultiplyRow we denote an algorithm that computes, given a matrix $M \in k[x]^{m\times n}$, a polynomial $f \in k[x]$ and an index $i \in \{1,\dots,m\}$, the matrix obtained by multiplying the i-th row of M with f. Moreover, by ScaleRows we denote an algorithm that computes, given M as above and a list of polynomials $f_1,\dots,f_m \in k[x]$, the matrix we obtain by successively applying MultiplyRow(M,i,f_i) for $i = 1,\dots,m$.

(ii) By we Determinant denote an algorithm that computes, given a matrix $M \in k[x]^{n\times n}$, the determinant $\det M$ of M.

(iii) Let $h \in k[x]$. By Red_h we denote an algorithm that reduces any $M \in k[x]^{m\times n}$ entry-wise modulo h.

(iv) By Degree we denote an algorithm that computes, given a matrix $M \in k[x]^{m\times n}$, the degree $\deg M$ of M.

(v) By LeadCoeffMat we denote an algorithm that computes, given a polynomial matrix $M \in k[x]^{m\times n}$, the matrix $\mathrm{LC}(M)$. See Definition 4.3.1.

(vi) By SubMatrix we denote an algorithm that returns for given matrix $M = (m_{i,j})_{i,j}$ the submatrix SubMatrix$(M,(i,j),(m,n))$ of M whose top left entry is $m_{i,j}$ and which has dimension $m \times n$.

(vii) By BigMatrix denote an algorithm that computes, given matrices $T_{\beta_1},\dots,T_{\beta_h},T_J$, the big matrix $M(J,\beta_1,\dots,\beta_h)$ from Proposition 6.2.5, see Definition 6.2.6.

(viii) By ColumnConcat we denote an algorithm that returns, given matrices $M_1,\dots,M_r$ with $M_i \in k[x]^{r_i\times c}$, the concatenated block matrix $M \in k[x]^{\sum_{i=1}^{r} r_i\times c}$ whose i-th row block is given by M_i.

(ix) By RANDOM we denote an algorithm which returns, given a finite subset Σ of the field k, a uniformly random chosen element in Σ.

Since coming up with a random integer in the range $1, \ldots, \#\Sigma$ yields a random element in Σ, the cost of RANDOM in our cost model is constant. See Section 1.2. △

Now we give naive and more involved bounds for the running time of the above algorithms with respect to our cost model, see Section 1.2.

Lemma A.1.2.

(i) Let d be a common bound of the degree of the i-th row of M and of $\deg f$. Then MULTIPLYROW *requires at most $O^{\sim}(nd)$ operations in k.*

Let d be a common bound of $\deg M$ and $\max_{i=1}^{m}\{\deg f_i\}$. Then SCALEROWS *requires at most $O^{\sim}(mnd)$ operations in k.*

We note that the algorithms MULTIPLYROW *and* SCALEROWS *may also be applied for $f = x^{-i}$ with the same running time under the assumption that all the affected entries of M are multiples of x^i.*

(ii) Let $M \in k[x]^{n\times n}$ have degree d. Then DETERMINANT *requires at most $O^{\sim}(n^{\omega}d)$ operations in k.*

(iii) Let d be a common bound of the degree of $h \in k[x]$ and of the degree of $M \in k[x]^{m\times n}$. Then RED_h requires at most $O^{\sim}(mnd)$ operations in k.

(iv) DEGREE *has constant running time.*

(v) LEADCOEFFMAT *has constant running time.*

(vi) SUBMATRIX *has constant running time.*

(vii) BIGMATRIX *has constant running time.*

(viii) COLUMNCONCAT *has constant running time.*

Proof.

(i) Let d be a common bound of the degree of the i-th row of M and of $\deg f$. The algorithm MULTIPLYROW then obviously requires at most n multiplications in $k[x]$ of polynomials with degree bounded by d. These require at most $O^{\sim}(nd)$ operations in k, see Proposition A.2.3.

Let d be a common bound of $\deg M$ and $\max_{i=1}^{m}\{\deg f_i\}$. The algorithm SCALEROWS then calls MULTIPLYROW m times and thus obviously requires at most $O^{\sim}(mnd)$ operations in k, see Proposition A.2.3.

(ii) This is Theorem A.2.10.

(iii) Let $M \in k[x]^{m\times n}$ with $\deg h, \deg(M) \leq d$. Obviously, RED_h computes mn divisions with remainder with polynomials that have degree bounded by d. Therefore, by Proposition A.2.1, RED_h requires at most $O^{\sim}(mnd)$ operations in k.

(iv) Comparing degrees only require operations in $\mathbb{Z}$ and thus due to our cost model, these do not count. Since determining the degree of a polynomial has constant cost in our cost model, the same is true for DEGREE.

(v) That LEADCOEFFMAT has constant running time is due to our cost model, see Section 1.2.

(vi) That SubMatrix has constant running time is due to our cost model, see Section 1.2.

(vii) That BigMatrix has constant running time is due to our cost model, see Section 1.2.

(viii) That ColumnConcat has constant running time is due to our cost model, see Section 1.2. □

A.2 Linear Algebra Algorithms over Polynomial Rings

In contrast to Section A.1, we will collect statements about more advanced algorithms for solving more involved problems with regards to matrices over $k[x]$.

Recall that $2 \leq \omega \leq 3$ denotes the matrix multiplication constant, that is, multiplying two $n \times n$ matrices over a field k uses $O(n^\omega)$ operations in k. To the best knowledge of the author the best bound is $\omega \leq 2.373$, see [Wil12].

Proposition A.2.1. *Let $a, b \in R[x]$ be two polynomials over the commutative ring R. Assume $\deg(b) < \deg(a)$ and $\deg(a) \in O(\deg(b))$. Then division with remainder of a by b uses $O^\sim(\deg(b))$ operations in R.*

Proof. This follows directly from [GG03, Theorem 9.6]. □

Definition A.2.2. Let k be a field. By $M(d)$ we denote the number of operations in k needed for computing the product of two polynomials in one indeterminate over k of degree d. By $B(d)$ we denote the number of operations in k needed for computing the gcd of two polynomials in degree d over k. △

Proposition A.2.3. *Let k be a field. Then $M(d) \in O^\sim(d)$ and $B(d) \in O^\sim(d)$.*

Proof. The first assertion is the last Theorem (without numbering) in [CK91]. Regarding the second: The Euclidean algorithm uses at most $\log d$ many divisions with remainder of which each work with polynomials of degree at most d. But division with remainder in degree d uses $O^\sim(d)$ operations in k, see Proposition A.2.1. □

Remark A.2.4. Let M, $D \in R^{n \times n}$ be two square matrices over a ring R where D is diagonal. Moreover, let $b \in R^n$. Then the multiplication of M with D requires n^2 multiplications in R. Obviously, the transposed versions is also true. Moreover, computing the product $M \cdot b$ requires at most n^2 multiplications and $n(n-1)$ additions in R. △

Lemma A.2.5. *Let M, $D \in k[x]^{n \times n}$ with D diagonal. Moreover, let $b \in k[x]^n$. Assume that d is a bound for the degrees of M, D and b. Then computing the products $M \cdot D$ and $M \cdot b$ both require at most $O^\sim(n^\omega d)$ operations in k.*

Proof. By Remark A.2.4, we know that both computations requires at most $O(n^2)$ operations in $k[x]$. These operations are either additions or multiplications which by Proposition A.2.3 require at most $O^\sim(d)$ operations in k which already proves the assertion. □

Theorem A.2.6. *Let $M \in k[x]^{m \times n}$ be a matrix of degree d. Then there exist an algorithm* MatrixKernel *which computes a basis of the $k[x]$-module $\ker M = \{p \in k[x]^n \mid Mp = 0\}$ in form of a matrix $N \in k[x]^{n \times *}$ whose columns are the basis vectors. Moreover, the matrix N is column reduced, that is, the basis represented by N has the lowest degrees of all possible bases of M.[1] The computation of N uses $O^\sim_{n,g}(n^\omega \lceil md/n \rceil)$ operations in k.*

[1] This is congruent with our definition of a polynomial matrix being reduced, see Definition 4.3.3. Note that we only formulated the sqaure matrix case, but being reduced can be formulated for rectangular matrices as well, see [Hes02, p. 1].

Proof. Algorithm 1 in [ZLS12] computes $\ker M$ in form of the required matrix. That matrix is column reduced since Algorithm 1 in general computes a $\vec{s}$-reduced basis where $\vec{s} = [s_1, \ldots, s_m] \in \mathbb{Z}^m$. Regarding the definition see [ZLS12, 2.1]. We are only interested in the case $\vec{s} = [d, \ldots, d]$ from which one can deduce that N is column reduced. The fact that the running time of Algorithm 1 is indeed in the asserted order follows from [ZLS12, Cor. 4.6]. □

Now we turn to an algorithm which reduces a matrix over $k[x]$ in a sufficiently small amount of steps in k, see [GSSV12].

Theorem A.2.7 (See Theorem 18 in [GSSV12]). *There exist an algorithm* RedMat *which computes for given regular matrix $M \in k[x]^{n\times n}$ of degree d a right equivalent matrix of M such that it has minimal column degrees among all right equivalent matrices of M.*[2] *The algorithm* RedMat *uses $O\left(n^\omega \left((\log n)^2 M(d) + B(d)\right)\right)$ operations in k. Here $B(d)$ denotes the complexity of solving the gcd-problem in degree d and $M(d)$ denotes the complexity of multiplying two polynomials in one indeterminate of degree d.*

Corollary A.2.8. *If $\deg M \in O(d)$, then by Theorem A.2.7 and Proposition A.2.3* RedMat *uses $O^\sim(n^\omega d)$ operations in k to reduce M.*

Remark A.2.9. We can use algorithm RedMat to reduce any matrix $M \in k(x)^{n\times n}$ if we find $d \in k[x]$ such that $dM \in k[x]^{n\times n}$. Then RedMat provides a right equivalent matrix dMT of dM which has minimal column degrees among all right equivalent matrices of dM, and, evidently, the same is true for MT. △

Theorem A.2.10 (See [ZL14]). *Let $M \in k[x]^{n\times n}$ be of degree $O(d)$. Then there exists an algorithm* Determinant *which computes $\det(M)$ using $O^\sim(n^\omega d)$ operations in k.*

Lemma A.2.11 (9.7 in [GG03]). *Let R be a commutative ring with unity and let $f \in R[t]$ be a monic polynomial of degree n. Then the multiplication in $R[t]/fR[t]$ (including division with remainder) uses $O^\sim(n)$ operations in R.*

Theorem A.2.12 (Solution of Problem 2.3a (*LIN·SOLVE1*) on p. 104 in [BP94]). *Let A be an arbitrary $m \times n$ matrix over the field k and $b \in k^n$. Then there is an algorithm* SolveLES$_k$ *computing a solution vector $x \in k^n$ such that $Ax = b$ which requires at most $O(n^{\omega-1}m)$ operations in k.*

Theorem A.2.13 (Theorem 12 in [GSSV12]). *Let $M \in k[x]^{n\times n}$ be a polynomial matrix of degree d and non-zero determinant. Let $b \in k[x]^{n\times 1}$ have degree in $O(nd)$. If the solution $A^{-1}b$ satisfies $A^{-1}b \in k[x]^n$, then there is an algorithm* RationalSystemSolve *that computes $A^{-1}b$. If $A^{-1}b \notin k[x]^n$, then* RationalSystemSolve *computes $(gA^{-1}b, g)$ with $g \in k[x]$ with minimal degree such that $gA^{-1}b \in k[x]^n$. In both cases the algorithm has cost $O(n^\omega(\log n)^2 M(d) + nB(nd))$.*

Corollary A.2.14. *Let $M \in k[x]^{n\times n}$ be a polynomial matrix of degree d and non-zero determinant. Let $b \in k[x]^{n\times 1}$ have degree in $O(nd)$. Then the cost of computing $A^{-1}b$ is $O^\sim(n^\omega d)$.*

Proof. This is Theorem A.2.13, together with Proposition A.2.3. □

Theorem A.2.15 (Theorem 6.2 and lemma 5.1 in [ZL13]). *There exists an algorithm* ColumnBasis *that computes, given a matrix $M \in k[x]^{m\times n}$ of rank r such that $r \le m \le n$, a matrix $C \in k[x]^{m\times r}$ of full rank whose columns form a basis of the column space of M. If s denotes the average column degree of M, then* ColumnBasis *requires at most $O^\sim(m^{\omega-1}ns)$ operations in k and then C has degree bounded by s.*

[2] See Footnote 1.

Theorem A.2.16. *There exists an algorithm* Popov *that computes, given a non-singular matrix $M \in k[x]^{n\times n}$, a matrix $P \in k[x]^{n\times n}$ in Popov form. If $d = \deg(M)$, then* Popov *requires at most $O^{\sim}(n^{\omega}d)$ operations in k.*

Proof. By [SS11, Thm. 13 and 18], there exists an algorithm that computes for given reduced $M \in k[x]^{n\times n}$ (it even works for $m \times n$ with $M \geq n$) a matrix in Popov form and that requires at most $O^{\sim}(n^{\omega}d)$ operations in k. Hence we only need to reduce the input matrix by using RedMat which requires as well at most $O^{\sim}(n^{\omega}d)$ operations in k, see Theorem A.2.7. □

Appendix B

Foundational Theory

In this chapter we collect some of the foundational definitions and statement about some of the objects that are involved in this thesis. This chapter has evolved as a growing source of reference within this thesis and is not intended to be standalone. That is, we do not cover (in any sense) all of the material needed in this thesis. We rather state propositions we need and that we have not found in the literature (at least not in a way appropriate for this thesis).

This chapter is organised as follows: In Sections B.1 and B.2 we provide most of the basic definitions and statements for presheaves and sheaves on topological spaces and on schemes. Section B.3 provides the basic theory for treating the irreducible components of a scheme X in an iterative way. This will be key for examination of the relation of divisors on X and divisors on the irreducible components of X. In Sections B.4 and B.5 we provide rather foundational statements with respect to commutative algebra respectively algebraic geometry.

B.1 Presheaves and Sheaves

In this section we introduce (and mostly recall) the notion of sheaves, those objects which play a central role in this thesis and, of course, in all of algebraic geometry. We do not state every definition and proposition that is used in this thesis, and we do not claim to provide an introduction to sheaves as a whole. We only state those definitions and propositions which turned out to be useful to state in the context of this thesis. The interested reader is referred to the standard texts as [Liu02], [GW10], [Sta18], [Har77], [EH14], [THPlns75] as well as every other standard textbook on algebraic geometry.

We define sheaves the same way [Liu02] does, that is, as sheaves of abelian groups. This definition easily translates to the definition of sheaves of rings, of modules and algebras of a fixed ring etcetera. We want to keep the definition as brief as possible and do not want to define sheaves as functors in all of its generality.

Definition B.1.1. Let X be a topological space. A **presheaf on $\mathcal{F}$ (of abelian groups) on** X consists of the following data

- an abelian group $\mathcal{F}(U)$ for each open subset U of X and
- a group homomorphism $\rho_V^U(\mathcal{F}) : \mathcal{F}(U) \to \mathcal{F}(V)$ for every inclusion of open subsets $V \subseteq U$ called the **restriction morphism**

such that

1. $\mathcal{F}(\emptyset) = 0$,
2. $\rho_U^U(\mathcal{F}) = \mathrm{id}_{\mathcal{F}(U)}$,

3. if there are three open subsets $W \subseteq V \subseteq U$ of X, then $\rho^U_W(\mathcal{F}) = \rho^V_W(\mathcal{F}) \circ \rho^U_V(\mathcal{F})$.

The elements $s \in \mathcal{F}(U)$ are called **sections of $\mathcal{F}$ over U**. Let $V \subseteq U$ be open subsets of X. We also denote the image of $s \in \mathcal{F}(U)$ under the restriction map $\rho^U_V(\mathcal{F}) : \mathcal{F}(U) \to \mathcal{F}(V)$ by $s_{|V}$ and call it the **restriction of s to V**. Consider the following two conditions a presheaf $\mathcal{F}$ on X may (or may not) satisfy:

(a) (*Separatedness*) For any open subsets $U \subseteq X$ of X and open cover $U = \cup_{i\in I} U_i$ any two sections $s, t \in \mathcal{F}(U)$ are equal if and only if $\rho^U_{U_i}(\mathcal{F})(s) = \rho^U_{U_i}(\mathcal{F})(t)$ for all $i \in I$, i.e. $s_{|U_i} = t_{|U_i}$ for all $i \in I$.

(b) (*Gluing local sections*) For any open subset $U \subseteq X$ of X, open cover $U = \cup_{i\in I} U_i$ and sections $s_i \in \mathcal{F}(U_i)$ such that for all $i, j \in I$ we have $s_{i|U_i\cap U_j} = s_{j|U_i\cap U_j}$ in $\mathcal{F}(U_i \cap U_j)$ there exists $s \in \mathcal{F}(U)$ such that $s_{|U_i} = s_i$ for all $i \in I$. In this case we sometimes say that s *glues together from the sections* s_i.

A presheaf $\mathcal{F}$ on X is called **separated** if it satisfies condition (a). If $\mathcal{F}$ further satisfies condition (b), then it is called a **sheaf $\mathcal{F}$ on X**. A **subpresheaf** $\mathcal{G}$ of a presheaf $\mathcal{F}$ is a presheaf $\mathcal{G}$ such that for all open subsets $U \subseteq X$ we have that $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ is a subgroup and the restriction maps of $\mathcal{G}$ are induced by those of $\mathcal{F}$. If both $\mathcal{G}$ and $\mathcal{F}$ are sheaves, then $\mathcal{G}$ is called a **subsheaf of $\mathcal{F}$**. In both cases, $\mathcal{G}$ being a subpresheaf or subsheaf of $\mathcal{F}$, we write $\mathcal{G} \leq \mathcal{F}$. △

Example B.1.2. Let X be a topological space and $\mathcal{F}, \mathcal{G}$ be two subpresheaves of the presheaf $\mathcal{H}$, i.e. $\mathcal{F}, \mathcal{G} \leq \mathcal{H}$. Then the rule $U \mapsto \mathcal{F}(U) \cap \mathcal{G}(U)$ defines a subpresheaf $\mathcal{F} \cap \mathcal{G}$ of $\mathcal{H}$. Here the restriction maps are just those of $\mathcal{F}$ (or $\mathcal{G}$ and by definition those of $\mathcal{H}$ as well). Furthermore, if $\mathcal{F}$ and $\mathcal{G}$ are sheaves, then $\mathcal{F} \cap \mathcal{G}$ is a sheaf as well. △

Remark B.1.3. In a analogous way we define presheaves and sheaves (and all related definitions in Definition B.1.1) of rings, of modules or algebras over a given ring etcetera. If $\mathcal{F}$ is a sheaf on the topological space X, then the section s glued together is unique. Indeed, if there are $s, t \in \mathcal{F}(U)$ such that $s_{|U_i} = t_{|U_i}$ for all $i \in I$, then the separatedness axiom (a) in Definition B.1.1 ensures that $s = t$ in $\mathcal{F}(U)$. △

Definition B.1.4. Let X be a presheaf on the topological space X. Let $P \in X$ be arbitrary. We define the **stalk of $\mathcal{F}$ at P** as the direct limit

$$\mathcal{F}_P = \varinjlim_{U\subseteq X,\ P\in U} \mathcal{F}(U)$$

where U runs over all open neighborhoods of P in X. If $\mathcal{F}$ is a presheaf of R-modules, then $\mathcal{F}_P$ is an R-module and if $\mathcal{F}$ is a presheaf of rings, then $\mathcal{F}_P$ again is a ring. By definition, any element in $\mathcal{F}_P$ is given by some section s of $\mathcal{F}$ over U where $P \in U$, denoted by (U, s). Any two such representations (U, s) and (V, t) define the same element in $\mathcal{F}_P$ if and only if there is some open neighborhood $W \subseteq U \cap V$ such that $s_{|W} = t_{|W}$.

For any open subset $U \subseteq X$ such that $P \in U$ we have a natural map (group homomorphism) $\mathcal{F}(U) \to \mathcal{F}_P$ sending s to the element defined by (U, s) in $\mathcal{F}_P$. We denote the image of s under this map as s_P and call it the **germ of s at P**. △

Definition B.1.5. Let X be a topological space and $\mathcal{F}$ a presheaf on X. Then for any $f \in \mathcal{F}(X)$ we call the set

$$\mathrm{Supp}(f) := \mathrm{Supp}(\mathcal{F}, f) := \{P \in X \mid f_P \neq 0 \text{ in } \mathcal{F}_P\}$$

the **support of f on X**. △

Lemma B.1.6. *Let X be a topological space and $\mathcal{F}$ a presheaf on X. Then for any $f \in \mathcal{F}(X)$ the support* $\mathrm{Supp}(f)$ *is closed in X.*

Proof. Consider the complement $Z(f)$ of $\mathrm{Supp}(f)$ in X which consists of those points $P \in X$ for which $f_P = 0$. Then, by definition of the stalk $\mathcal{F}_P$ of $\mathcal{F}$, for every $P \in Z(f)$ there exists an open neighborhood U_P of P for which $f_{|U_P} = 0$ in $\mathcal{F}(U_P)$. Moreover, for every $Q \in U_P$ we obviously have $f_Q = 0$. In particular, $U_P \subseteq Z(f)$ and thus the open subsets $U_P \subseteq X$ for $P \in Z(f)$ cover $Z(f)$. Whence $Z(f)$ is open in X and therefore $\mathrm{Supp}(f)$ is closed in X. □

Remark B.1.7. Let $\mathcal{F}$ be a presheaf on the topological space X and $U \subseteq X$ an open subset of X. Let $s \in \mathcal{F}(U)$ be a sections of $\mathcal{F}$ over U. Then s defines a function which we (by slight abuse of notation) also denote by $s : U \to \coprod_{P \in U} \mathcal{F}_P$, $P \mapsto s_P$.

Now let $t \in \mathcal{F}(V)$ be another sections of $\mathcal{F}$ but over $V \subseteq X$ with $W = U \cap V \neq \emptyset$. Now if $s_{|W} = t_{|W}$ in $\mathcal{F}(W)$, then by construction the functions s and t agree on W and hence we may consider the function

$$u : U \cup V \to \coprod_{P \in U \cup V} \mathcal{F}_P, \quad P \mapsto \begin{cases} s_P, & P \in U \\ t_P, & P \in V \end{cases}$$

defined on $U \cup V$. This interpretation of sections of $\mathcal{F}$ as functions into the stalks of $\mathcal{F}$ does suggest that this function u should correspond to a section $u \in \mathcal{F}(U \cup V)$. But this need not hold in general. It does hold for arbitrary U and V if and only if $\mathcal{F}$ satisfies the *gluing local sections* condition (b) in Definition B.1.1.

This already suggests how we should overcome this missing property of $\mathcal{F}$, namely by adding such functions u as above. We will see this later in detail when talking about sheafification which does also want to ensure the *separatedness* condition (a) in Definition B.1.1. △

Lemma B.1.8. *Let $\mathcal{F}$ be a presheaf on the topological space X. Then $\mathcal{F}$ is separated if and only if the natural map $\mathcal{F}(U) \to \prod_{P \in U} \mathcal{F}_P$, $s \mapsto (s_P)_{P \in U}$ is injective for all open subsets $U \subseteq X$.*

Proof. Assume that $\mathcal{F}$ is separated. Let $U \subseteq X$ be any open subset of X and $s \in \mathcal{F}(U)$ with $s_P = 0$ in $\mathcal{F}_P$ for all $P \in U$. Thus, by definition, for every $P \in U$ there is an open neighborhood $U_P \subseteq U$ of P such that $s_{|U_P} = 0$. Since the U_P cover U, the separatedness of $\mathcal{F}$ provides $s = 0$ in $\mathcal{F}(U)$.

Conversely, let $\mathcal{F}(U) \to \prod_{P \in U} \mathcal{F}_P$ be injective. Let $s, t \in \mathcal{F}(U)$ satisfy $s_{|U_i} = t_{|U_i}$ for all $i \in I$ for some open cover $U = \cup_{i \in I} U_i$. In particular, $s - t$ restricts to zero on every U_i. Since the U_i cover U, the germ $(s - t)_P$ is zero for every $P \in U$ and hence $s - t$ must be zero by the injectivity assumption. □

Lemma B.1.9. *Let $\mathcal{F}$, $\mathcal{G}$ be presheaves (of abelian groups) on the topological space X such that $\mathcal{G} \leq \mathcal{F}$ as presheaves. If $\mathcal{F}$ is separated, then $\mathcal{G}$ is separated.*

Proof. By definition, for every open subset $U \subseteq X$ we have $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ is a subgroup and the restriction map $\mathcal{G}(U) \to \mathcal{G}(V)$ is simply the restriction of the restriction homomorphism $\mathcal{F}(U) \to \mathcal{F}(V)$ for every open subset $V \subseteq U$. Now let $U = \cup_{i \in I} U_i$ be an open cover, $s \in \mathcal{G}(U)$ such that $s_{|U_i} = 0$ for all $i \in I$. Since $s \in \mathcal{F}(U)$ and $s_{|U_i} = \rho_V^U(\mathcal{F})(s)$ we can use that $\mathcal{F}$ is separated which yields $s = 0$ in $\mathcal{F}(U)$. But since $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ and $s \in \mathcal{G}(U)$, this yields $s = 0$ in $\mathcal{G}(U)$ as well. Hence $\mathcal{G}$ is separated as asserted. □

Definition B.1.10. Let X be a topological space and $\mathcal{F}$, $\mathcal{G}$ two presheaves (of abelian groups) on X. A **morphism of presheaves** $f : \mathcal{F} \to \mathcal{G}$ is a collection of group homomorphism $f(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ for all open subsets $U \subseteq X$ such that for all open subsets $V \subseteq U$ the following diagram commutes.

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{f(U)} & \mathcal{G}(U) \\ {\scriptstyle \rho_V^U(\mathcal{F})}\downarrow & & \downarrow{\scriptstyle \rho_V^U(\mathcal{G})} \\ \mathcal{F}(V) & \xrightarrow{f(V)} & \mathcal{G}(V) \end{array}$$

If $\mathcal{F}$ and $\mathcal{G}$ are sheaves on X, then a **morphism of sheaves** $f : \mathcal{F} \to \mathcal{G}$ is a morphism of the presheaves $\mathcal{F}$ and $\mathcal{G}$. Every morphism of presheaves $f : \mathcal{F} \to \mathcal{G}$ provides for any $P \in X$ a morphism of the stalks $f_P : \mathcal{F}_P \to \mathcal{G}_P$ mapping (U, s) to $(U, f(U)(s))$ and satisfying $(f(U)(s))_P = f_P(s_P)$. We call f_P the **morphism induced by f on the stalks**. We say that f is **injective** if $f(U)$ is injective for all open subsets $U \subseteq X$. We say that f is **surjective** if the induced map on the stalks f_P is surjective for all $P \in X$. We say that $f : \mathcal{F} \to \mathcal{G}$ is an **isomorphism** if it has a two-sided inverse $g : \mathcal{G} \to \mathcal{F}$. A **morphism of sheaves** is just a morphism of presheaves $f : \mathcal{F} \to \mathcal{G}$ where $\mathcal{F}$ and $\mathcal{G}$ are sheaves. △

Remark B.1.11. If a morphism of presheaves is injective, then the induced map on the stalks is injective. The converse is true for a morphism of separated presheaves.

If for all open subsets $U \subseteq X$ the map $f(U)$ is surjective, then f is surjective. But if f is surjective, then $f(U)$ need not be surjective for all open subsets $U \subseteq X$. △

Whether a morphism of sheaves is an isomorphism or not can be checked on the level of stalks.

Lemma B.1.12 ([Liu02], 2.2.12)**.** *A morphism of sheaves $f : \mathcal{F} \to \mathcal{G}$ is an isomorphism if and only if f_P is an isomorphism for all $P \in X$.*

The same is not true for presheaves since we are not able to glue a preimage together from local sections that agree on overlaps.

Remark B.1.13. Morphisms of sheaves $\phi : \mathcal{F} \to \mathcal{G}$ on the topological space X provide some natural examples of presheaves on X. Let $U \subseteq X$ be any open subset of X. Then the following mappings define presheaves on X:

1. The **presheaf kernel of** ϕ defined by $U \mapsto \ker(\phi(U))$,
2. the **presheaf image of** ϕ defined by $U \mapsto \mathrm{im}(\phi(U))$,
3. the **presheaf cokernel of** ϕ defined by $U \mapsto \mathrm{coker}(\phi(U))$.

Here the presheaf kernel of ϕ is also a sheaf on X, but the presheaf cokernel and presheaf image of ϕ are no sheaves on X in general. The presheaf kernel of ϕ is a subsheaf of $\mathcal{F}$ and the presheaf image of ϕ is a subpresheaf of $\mathcal{G}$. If $\mathcal{F}, \mathcal{G}$ are two sheaves on the topological space X such that $\mathcal{G} \leq \mathcal{F}$, then we have an inclusion morphism $\mathcal{G} \hookrightarrow \mathcal{F}$ and its presheaf cokernel is separated. △

The next definition tries to come up with a sheaf $\mathcal{F}^\#$ starting from a presheaf $\mathcal{F}$ by adding those sections glued from local sections of $\mathcal{F}$ agreeing on intersections (ensuring the *gluing local sections* condition) and dropping those knocking out the *separatedness* condition.

Definition B.1.14. Let $\mathcal{F}$ be a presheaf (of abelian groups) on the topological space X. Consider

$$\mathcal{F}^{\#}(U) := \left\{ f : U \to \coprod_{P \in U} \mathcal{F}_P \mid \forall\ P \in U\ \exists\ V_P \subseteq U\ \exists\ s \in \mathcal{F}(V_P) : \forall\ Q \in V_P\ f(Q) = s_Q \right\}$$

for any open subset $U \subseteq X$. Taking the restriction of functions as the restriction maps this defines a presheaf (of abelian groups) on X. We call $\mathcal{F}^{\#}$ the **sheafification of** $\mathcal{F}$. △

The name already suggests that $\mathcal{F}^{\#}$ will indeed be a sheaf. The following lemma provides this fact and does also show that this construction of a sheaf from the presheaf $\mathcal{F}$ is universal.

Lemma B.1.15 ([Liu02], 2.2.15)**.** *Let $\mathcal{F}$ be a presheaf (of abelian groups) on the topological space X. Then $\mathcal{F}^{\#}$ is a sheaf (of abelian groups) on X and it comes with a morphism of presheaves $\theta : \mathcal{F} \to \mathcal{F}^{\#}$. Moreover, the pair $(\mathcal{F}^{\#}, \theta)$ satisfies the following universal property: For every morphism of presheaves $\beta : \mathcal{F} \to \mathcal{G}$, where $\mathcal{G}$ is a sheaf, there exists a unique morphism $\alpha : \mathcal{F}^{\#} \to \mathcal{G}$ such that $\beta = \alpha \circ \theta$.*

Remark B.1.16. The morphism of presheaves $\theta : \mathcal{F} \to \mathcal{F}^{\#}$ is the obvious one: For any open subset $U \subseteq X$ and $s \in \mathcal{F}(U)$ the section s defines a function $s : U \to \coprod_{P \in U} \mathcal{F}_P$ via $P \mapsto s_P$ as already introduced in Remark B.1.7. Note that $\theta_P : \mathcal{F}_P \to \mathcal{F}^{\#}_P$ is an isomorphism.

Moreover, if we identify the sections $s \in \mathcal{F}(U)$ over U for any given presheaf $\mathcal{F}$ with the functions $s : U \to \coprod_{P \in U} \mathcal{F}_P$ given by $P \mapsto s_P$, as in Remark B.1.7, then the sheafification $\mathcal{F}^{\#}$ simply adds those functions $U \to \coprod_{P \in U} \mathcal{F}_P$ such that there is an open cover $U = \cup_{i \in I} U_i$ and functions $s_i : U_i \to \coprod_{P \in U_i} \mathcal{F}_P$ given by sections $s_i \in \mathcal{F}(U_i)$ that agree (as functions to the stalks) on the overlaps $U_i \cap U_j$ for all $i, j \in I$. Then θ_P will not only be an isomorphism for all $P \in X$, but also the identity map. △

A morphism of presheaves that is an isomorphism on the level of stalks need not be an isomorphism of presheaves. But we will see now that the respective sheafifications are isomorphic.

Lemma B.1.17. *Let $f : \mathcal{F} \to \mathcal{G}$ be a morphism of presheaves on the topological space X. If the induced homomorphism f_P is an isomorphism for all $P \in X$, then $\mathcal{F}^{\#} \cong \mathcal{G}^{\#}$.*

Proof. We compose f with $\theta_{\mathcal{G}} : \mathcal{G} \to \mathcal{G}^{\#}$ and obtain a morphism of presheaves $\mathcal{F} \to \mathcal{G}^{\#}$ with the codomain being a sheaf. By Lemma B.1.15, this morphism factors through $\mathcal{F}^{\#}$ and hence we obtain a commutative diagram:

$$\begin{array}{ccc} \mathcal{F} & \xrightarrow{f} & \mathcal{G} \\ {\scriptstyle \theta_{\mathcal{F}}}\downarrow & & \downarrow{\scriptstyle \theta_{\mathcal{G}}} \\ \mathcal{F}^{\#} & \xrightarrow{f^{\#}} & \mathcal{G}^{\#} \end{array}$$

On the level of stalks this provides a commutative diagram

$$\begin{array}{ccc} \mathcal{F}_P & \xrightarrow{f_P} & \mathcal{G}_P \\ {\scriptstyle \theta_{\mathcal{F},P}}\downarrow & & \downarrow{\scriptstyle \theta_{\mathcal{G},P}} \\ (\mathcal{F}^{\#})_P & \xrightarrow{f^{\#}_P} & (\mathcal{G}^{\#})_P \end{array}$$

which together with the fact that $\theta_{\mathcal{F},P}$, $\theta_{\mathcal{G},P}$ and f_P are isomorphisms provides that the induced map $f^{\#}_P$ is an isomorphism as well. Then Lemma B.1.12 provides $f^{\#} : \mathcal{F}^{\#} \to \mathcal{G}^{\#}$ is an isomorphism of sheaves. □

Definition B.1.18. Let $\phi : \mathcal{G} \to \mathcal{F}$ be a morphism of sheaves on the topological space X. We denote the sheafifications of the presheaf kernel, presheaf cokernel and presheaf image by $\ker(\phi)$, $\operatorname{coker}(\phi)$ respectively $\operatorname{im}(\phi)$. If $\mathcal{G} \leq \mathcal{F}$ and ϕ is the inclusion morphism, then we define $\mathcal{F}/\mathcal{G} = \operatorname{coker}(\phi)$ to be the **quotient sheaf of $\mathcal{F}$ by $\mathcal{G}$**. △

The proof of the following lemma in the case of $\mathcal{O}_X$-modules can be found in every standard algebraic geometry textbook, for instance [GW10, (7.3.1)-(7.3.3)]. But the same line of argument works for sheaves of abelian groups where no $\mathcal{O}_X$-module structure need to be involved.

Lemma B.1.19. *Let $\phi : \mathcal{G} \to \mathcal{F}$ be a morphism of sheaves (of abelian groups) on the topological space X. Let $P \in X$ be arbitrary. Then $\ker(\phi)_P \cong \ker(\phi_P)$, $\operatorname{coker}(\phi)_P \cong \operatorname{coker}(\phi_P)$ and $\operatorname{im}(\phi)_P \cong \operatorname{im}(\phi_P)$. In particular, for $\mathcal{G} \leq \mathcal{F}$ we have $(\mathcal{F}/\mathcal{G})_P \cong \mathcal{F}_P/\mathcal{G}_P$.*

Definition B.1.20. Let $\mathcal{F}$ be a presheaf on the topological space X. Let $U \subseteq X$ be an open subset of X. For $f, g \in \mathcal{F}(U)$ we say that f and g are **equal on a cover**, denoted by $f \equiv_\cup g$, if and only if there is a cover $U = \bigcup_{i \in I} U_i$ such that for each $i \in I$ we have $f_{|U_i} = g_{|U_i}$. Being equal on a cover obviously defines an equivalence relation on $\mathcal{F}(U)$. △

Remark B.1.21. If $\mathcal{F}$ is a separated presheaf on the topological space X, then being equal on a cover and being equal is the same for sections of $\mathcal{F}$. That is, for every open subset $U \subseteq X$ two sections $f, g \in \mathcal{F}(U)$ we have $f \equiv_\cup g$ if and only if $f = g$ in $\mathcal{F}(U)$. △

Lemma B.1.22. *Let $\mathcal{F}$ be a presheaf on the topological space X.*

(i) For every open subset $U \subseteq X$ and $s, t \in \mathcal{F}(U)$ we have $s \equiv_\cup t$ if and only if $s_P = t_P$ for all $P \in U$. That is, two sections are equal on a cover if and only if their induced functions into the stalks are equal.

*(ii) Every section of $\mathcal{F}^\#$ over U can be represented by a family of sections of $\mathcal{F}$ that are pairwise equal on a cover. That is, for every $s \in \mathcal{F}^\#(U)$ there is an open cover $U = \cup_{i \in I} U_i$ and sections $s_i \in \mathcal{F}(U_i)$ such that $s_{i|U_i \cap U_j} \equiv_\cup s_{j|U_i \cap U_j}$ for all $i, j \in I$. Such a family of sections is often called a **weakly matching family of** $\mathcal{F}$ and denoted by $(U_i, s_i)_{i \in I}$.*

In particular, if $\mathcal{F}$ is separated, then for every $s \in \mathcal{F}^\#(U)$ there is an open cover $U = \cup_{i \in I} U_i$ and sections $s_i \in \mathcal{F}(U_i)$ such that $s_{i|U_i \cap U_j} = s_{j|U_i \cap U_j}$ in $\mathcal{F}(U_i \cap U_j)$ for all $i, j \in I$.

(iii) Two weakly matching families $(U_i, f_i)_{i \in I}$ and $(V_j, g_j)_{j \in J}$ of sections of $\mathcal{F}$ represent the same section of $\mathcal{F}^\#$ over U if and only if for all $(i, j) \in I \times J$ we have $f_{i|U_i \cap V_j} \equiv_\cup g_{j|U_i \cap V_j}$.

Proof.

(i) Let $f, g \in \mathcal{F}(U)$ be sections of $\mathcal{F}$ over the open subset $U \subseteq X$. Assume that $f \equiv_\cup g$, that is there is an open cover $U = \cup_{i \in I} U_i$ such that $f_{|U_i} = g_{|U_i}$ for all $i \in I$. Since the U_i cover U, for every $P \in U$ there is some $i \in I$ such that $P \in U_i$ and $f_P = g_P$.

Conversely, let $f_P = g_P$ for all $P \in U$. Then for every $P \in U$ there are open neighborhoods $U_{f,P}$ and $U_{g,P}$ of P such that $(U_{f,P}, f)$ and $(U_{g,P}, g)$ define the same element in $\mathcal{F}_P$. That is, there is some open subset $U_{f,g,P} \subseteq U_{f,P} \cap U_{g,P}$ containing P such that $f_{|U_{f,g,P}} = g_{|U_{f,g,P}}$. Obviously, these $U_{f,g,P}$ cover U and hence $f \equiv_\cup g$.

(ii) Let $f : U \to \coprod_{P \in U} \mathcal{F}_P$ be an element of $\mathcal{F}^\#(U)$. Hence for every $P \in U$ there is some $V_P \subseteq U$ and $s(P) \in \mathcal{F}(V_P)$ such that for all $Q \in V_P$ we have $f(Q) = s(P)_Q$. Now consider the family $(V_P, s(P))$ of sections of $\mathcal{F}$. Let $P, P' \in U$ be two distinct

points in U such that $W := V_P \cap V_{P'} \neq \emptyset$. Then by definition of $\mathcal{F}^\#(U)$, we have $s(P)_Q = s(P')_Q$ for all $Q \in W$ and hence, by Item (i), we obtain $s(P)_{|W} \equiv_\cup s(P')_{|W}$. The particular part now follows from Remark B.1.21.

(iii) Let $(V_P, s(P))_{P\in U}$ and $(W_P, t(P))_{P\in U}$ be two weakly matching families coming from $f : U \to \coprod_{P\in U} \mathcal{F}_P$, $f \in \mathcal{F}^\#(U)$, as above. That is, for all $Q \in V_P$ we have $s(P)_Q = f(Q)$ and for all $Q \in W_P$ we have $t(P)_Q = f(Q)$. In particular, for all $Q \in V_P \cap W_P$ we have $s(P)_Q = t(P)_Q$. By Item (i), this means $s_{|V_P\cap W_P} \equiv_\cup t_{|V_P\cap W_P}$.
Conversely, let $(V_P, s(P))_{P\in U}$ be a weakly matching family coming from $f : U \to \coprod_{P\in U} \mathcal{F}_P$, $f \in \mathcal{F}^\#(U)$, and $(W_P, t(P))_{P\in U}$ another weakly matching family coming from $g : U \to \coprod_{P\in U} \mathcal{F}_P$, $g \in \mathcal{F}^\#(U)$, such that $s(P)_{|V_P\cap W_P} \equiv_\cup t(P)_{|V_P\cap W_P}$. By Item (i) again, this yields that for all $Q \in V_P \cap W_P$ we have $s(P)_Q = t(P)_Q$ which means that $f(Q) = g(Q)$ for all $Q \in V_P \cap W_P$. Now since the intersections $V_P \cap W_P$ for $P \in U$ constitute an open cover of U, we obtain that f and g are equal as functions from U to the stalks of $\mathcal{F}$ and therefore as sections of $\mathcal{F}^\#$. □

Corollary B.1.23. *Let $\mathcal{G} \leq \mathcal{F}$ be two sheaves on the topological space X. Then every global sections of $\mathcal{F}/\mathcal{G}$ is represented by a weakly matching family $(U_i, f_i + \mathcal{G}(U_i))_{i\in I}$ where $X = \cup_{i\in I} U_i$, $f_i \in \mathcal{F}(U_i)$ and for every $i, j \in I$ we have $f_{i|U_i\cap U_j} + \mathcal{G}(U_i \cap U_j) = f_{j|U_i\cap U_j} + \mathcal{G}(U_i \cap U_j)$, that is $f_{i|U_i\cap U_j} - f_{j|U_i\cap U_j} \in \mathcal{G}(U_i \cap U_j)$. Two such representations $(U_i, f_i + \mathcal{G}(U_i))_{i\in I}$ and $(V_j, h_j + \mathcal{G}(V_j))_{j\in J}$ define the same global section of $\mathcal{F}/\mathcal{G}$ if and only if for all $(i, j) \in I \times J$ we have $f_{i|U_i\cap V_j} - h_{j|U_i\cap V_j} \in \mathcal{G}(U_i \cap V_j)$. Here we denoted the group law of $\mathcal{G}$ and $\mathcal{F}$ additively.*

Proof. By Remark B.1.13, the presheaf $U \mapsto \mathcal{F}(U)/\mathcal{G}(U)$ is separated. Moreover, $\mathcal{F}/\mathcal{G}$ is its sheafification. Thus Lemma B.1.22 already provides the assertion. □

If a presheaf is not separated, then being local equal on a cover is the most we can ask for in a representation of a section of the sheafification. That is the restrictions of the local sections do not agree on the intersection but only on some cover of the intersection. The following example shows a presheaf that is not separated and for which we find a section of the sheafification whose local sections of the presheaf do not agree on the intersection. Example B.1.24 is taken from a mathoverflow post[1].

Example B.1.24. Let X be the topological set $X = \{a, b, c, d\}$ where the open sets are given by $X, \emptyset, \{a\}, \{b\}, U = \{a, b, c\}, V = \{a, b, d\}, U \cap V = \{a, b\}$. Then we define

$$\mathcal{F}(W) = \begin{cases} \mathbb{Z}, & W \in \{X, U, V, U \cap V\} \\ \mathbb{Z}/2\mathbb{Z}, & W \in \{\{a\}, \{b\}\} \\ 0, & W = \emptyset \end{cases}$$

and the restriction maps $\mathcal{F}(W) \to \mathcal{F}(Y)$ for $Y \subseteq W$ are given by either the canonical surjection $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, the identity map on $\mathbb{Z}$ or the zero map. This defines a presheaf $\mathcal{F}$ on X. Since the points $a, b \in X$ form open subsets of X, the stalk $\mathcal{F}_P$ equals $\mathbb{Z}/2\mathbb{Z}$ for $P \in \{a, b\}$. The only two open neighborhoods of $c \in X$ are U and X. Hence every element of $\mathcal{F}_c$ is given by (U, s) with $s \in \mathcal{F}(U) = \mathbb{Z}$. Analogously, the only two open neighborhoods of $d \in X$ are V and X. Hence every element of $\mathcal{F}_d$ is given by (V, t) with $t \in \mathcal{F}(V) = \mathbb{Z}$. Consider the natural map

$$\mathbb{Z} = \mathcal{F}(U \cap V) \to \coprod_{P\in U} \mathcal{F}_P = \mathcal{F}_a \times \mathcal{F}_b \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

[1] https://mathoverflow.net/questions/31372/describing-global-sections-of-sheafifications

sending $s \in \mathcal{F}(U)$ to the sequence of its germs $(s_P)_{P\in U}$, that is $s \mapsto (s \bmod 2, s \bmod 2)$. Obviously, its kernel is $2\mathbb{Z}$ and hence it is not injective providing that $\mathcal{F}$ is indeed not separated, see Lemma B.1.8.

Let us now consider what the global sections $\mathcal{F}^\#(X)$ of the sheafification $\mathcal{F}^\#$ are. By definition those are maps

$$f : X = \{a, b, c, d\} \to \mathcal{F}_a \times \mathcal{F}_b \times \mathcal{F}_c \times \mathcal{F}_d \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

for which there are open neighborhoods V_P for every point $P \in X$ on which f is given by a section of $\mathcal{F}(V_P)$. The neighborhoods of c and d which are not all of X (in this case f is given by some $s \in \mathcal{F}(X) = \mathbb{Z}$, that is $f(P) = s$ for all $P \in X$) are U respectively V. Therefore, by definition, $f(P) = u$ for some $u \in \mathcal{F}(U) = \mathbb{Z}$ for all $P \in U$ and $f(P) = v$ for some $v \in \mathcal{F}(V) = \mathbb{Z}$ for all $P \in V$. In particular, $f(P) = u = v$ for all $P \in U \cap V = \{a, b\}$. That is, u and v coincide in the stalks $\mathcal{F}_a$, $\mathcal{F}_b$ which are both given by $\mathbb{Z}/2\mathbb{Z}$. Hence $u \equiv v \bmod 2$. Thus every $f \in \mathcal{F}^\#(X)$ is already completely determined by $(u, v) \in \mathbb{Z}^2$ such that $u \equiv v \bmod 2$. Consider $f \in \mathcal{F}^\#(X)$ given by $(0, 2)$, that is the map

$$\{a, b, c, d\} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

maps $a \mapsto (0, 0, 0, 0)$, $b \mapsto (0, 0, 0, 0)$, $c \mapsto (0, 0, 0, 0)$ and $d \mapsto (0, 0, 0, 2)$. Then f is represented by the weakly matching family $f_U = 0 \in \mathcal{F}(U)$ and $f_V = 2 \in \mathcal{F}(V)$ for which we obviously have $(f_U)_P = (f_V)_P$ for all $P \in U \cap V$ and thus $(f_U)_{|U\cap V} \equiv_\cup (f_V)_{|U\cap V}$ by B.1.22 (i). This can also be seen by covering $U \cap V = \{a, b\}$ by $\{a\} \cup \{b\}$ for which we then have $(f_U)_{|\{a\}} = (f_V)_{|\{a\}}$ and $(f_U)_{|\{b\}} = (f_V)_{|\{b\}}$ since the restriction map $\mathcal{F}(U) = \mathcal{F}(V) \to \mathcal{F}(\{a\}) = \mathcal{F}(\{b\})$ is the projection $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

But the restriction of $f_U = 0 \in \mathbb{Z} = \mathcal{F}(U)$ to $\mathcal{F}(U \cap V) = \mathbb{Z}$ is 0 again and that of $f_V = 2 \in \mathbb{Z} = \mathcal{F}(V)$ to $\mathcal{F}(U \cap V) = \mathbb{Z}$ is 2 and hence f_U and f_V do not coincide on $U \cap V$. △

There are ways of transporting sheaves along continuous maps of topological spaces.

Definition B.1.25. Let $f : X \to Y$ be a continuous map. Let $\mathcal{F}$ be a presheaf on X and let $\mathcal{G}$ be a presheaf on Y.

1. We define a presheaf $f_*\mathcal{F}$ on Y by the rule

   $$V \mapsto \mathcal{F}(f^{-1}(V))$$

   for any open subset $V \subseteq Y$. The restriction maps are given by those of $\mathcal{F}$. We call $f_*\mathcal{F}$ the **direct image of $\mathcal{F}$ under f** and sometimes the **pushforward of $\mathcal{F}$ by f**. Note that if $\mathcal{F}$ is a sheaf on X, then $f_*\mathcal{F}$ is a sheaf on Y.

2. We define a presheaf $f^{-1}\mathcal{G}$ on X by the rule

   $$U \mapsto \varinjlim_{V \supseteq f(U),\ V \subseteq Y \text{ open}} \mathcal{G}(V)$$

   for any open subset $U \subseteq X$ and take the restriction maps to be induced by those of $\mathcal{G}$. We denote it sheafification by $f^{-1}\mathcal{G}$ and call it the **inverse image of $\mathcal{G}$ under f**. △

Definition B.1.26. A sheaf $\mathcal{F}$ on a topological space X is called **flasque** if for every inclusion $U \subseteq V \subseteq X$ the restriction map $\mathcal{F}(V) \to \mathcal{F}(U)$ is surjective. △

Definition B.1.27. Let X be a topological space and $\mathcal{F}$ a sheaf (of abelian groups) on X. The **support of $\mathcal{F}$** is defined as $\mathrm{Supp}(\mathcal{F}) = \{P \in X \mid \mathcal{F}_P \neq 0\}$. We say that $\mathcal{F}$ is a **skyscraper sheaf** if it has finite support. △

Lemma B.1.28. *If $\mathcal{F}$ is a skyscraper sheaf on the topological space X with support consisting of closed points of X, then for all open $U \subseteq X$ we have $\mathcal{F}(U) = \coprod_{P \in U \cap \mathrm{Supp}(\mathcal{F})} \mathcal{F}_P$.*

Proof. Let $U \subseteq X$ be any open subset of X. As a sheaf is separated by definition, by Lemma B.1.8, the natural map

$$\mathcal{F}(U) \to \coprod_{P \in U} \mathcal{F}_P, \quad s \mapsto (s_P)_{P \in U}$$

is injective. Since the stalk of $\mathcal{F}$ at P is zero for every $P \notin \mathrm{Supp}(\mathcal{F})$, the map $\mathcal{F}(U) \to \coprod_{P \in U \cap \mathrm{Supp}(\mathcal{F})} \mathcal{F}_P$ is also injective. To prove the assertion, we show that this map is also surjective. Let $\{P_1, \dots, P_n\}$ be the finitely many closed points constituting $U \cap \mathrm{Supp}(\mathcal{F})$. Let $I = \{1, \dots, n\}$ and let $(s_i)_{i \in I} \in \coprod_{i \in I} \mathcal{F}_{P_i}$ be arbitrary. Then for every $i \in I$ there is an open neighborhood U_i of P_i and a section $s^i \in \mathcal{F}(U_i)$ such that $s^i_{P_i} = s_i$. Now since the points P_i are closed, we may remove every point P_j with $j \neq i$ from U_i and thus we may assume that the U_i, $i \in I$, form a disjoint open cover of U. This provides that the sections s^i agree on intersections (since those are empty) and thus the *gluing local sections* condition (b) in Definition B.1.1 provides a unique section $s \in \mathcal{F}(U)$ such that $s_{|U_i} = s^i$ and thus s gets mapped to $(s_i)_{i \in I}$ under the considered map. □

Lemma B.1.29. *Let $\mathcal{F}$ be a subsheaf of $\mathcal{H}$ on the scheme X. Then for any open subset $U \subseteq X$ and $h \in \mathcal{H}(U)$ we have $h \in \mathcal{F}(U)$ if and only if $h_P \in \mathcal{F}_P$ for all $P \in U$.*

Proof. By definition, if $h \in \mathcal{F}(U)$, then $h_P \in \mathcal{F}_P$. Conversely, let $h \in \mathcal{H}(U)$ satisfy $h_P \in \mathcal{F}_P$ for all $P \in U$. Thus for every $P \in U$ there is an open neighborhood U_P of P such that $h_{|U_P} \in \mathcal{F}(U_P) \subseteq \mathcal{H}(U_P)$. The U_P cover U and then we have $(h_{|U_P})_{|U_Q} = h_{|U_P \cap U_Q} = (h_{|U_Q})_{|U_P}$ as sections of $\mathcal{F}$ since $h \in \mathcal{H}(U)$ and the restriction maps of $\mathcal{F}$ are those induced by the restriction maps of $\mathcal{H}$. That is, we have a collection of sections of $\mathcal{F}$ on an open cover of U that agree on intersections and hence they glue to a section f in $\mathcal{F}(U)$. Now since gluing is unique, we have $f = h$ in $\mathcal{H}(U)$ and hence $h \in \mathcal{F}(U)$. □

Corollary B.1.30. *Let $\mathcal{F}, \mathcal{G} \leq \mathcal{H}$ be two subsheaves of $\mathcal{H}$ on the scheme X. Then $\mathcal{F} = \mathcal{G}$ as subsheaves of $\mathcal{H}$ if and only if $\mathcal{F}_P = \mathcal{G}_P$ as subsets in $\mathcal{H}_P$ for all $P \in X$.*

Proof. The only if part is trivial. Since both $\mathcal{F}$ and $\mathcal{G}$ are subsheaves of $\mathcal{H}$, their restriction maps are those induced by those of $\mathcal{H}$. Hence it suffices to prove that for all open subsets $U \subseteq X$ we have $\mathcal{F}(U) = \mathcal{G}(U)$ as subsets of $\mathcal{H}(U)$. Let $f \in \mathcal{F}(U) \subseteq \mathcal{H}(U)$. By Lemma B.1.29, this is equivalent to $f_P \in \mathcal{F}_P$ for all $P \in U$. Now since $\mathcal{F}_P = \mathcal{G}_P$, we have $f_P \in \mathcal{G}_P$ for all $P \in U$ and thus Lemma B.1.29 again provides $f \in \mathcal{G}(U)$. By symmetry, this proves the assertion. □

Proposition B.1.31. *Let $f : X \to Y$ be a morphism of schemes and $\mathcal{F}$ a sheaf on X. Then we have a natural morphism*

$$(f_* \mathcal{F})_{f(x)} \to \mathcal{F}_x$$

whose image consists of those pairs $(f^{-1}(U), s_{f^{-1}(U)})_\sim$ with $x \in f^{-1}(U)$ and $s_{f^{-1}(U)} \in \mathcal{F}(f^{-1}(U))$ for open subsets $U \subseteq Y$. Moreover,

$$(f^{-1}(U), s_{f^{-1}(U)})_\sim = (f^{-1}(V), s_{f^{-1}(V)})_\sim \Leftrightarrow (s_{f^{-1}(U)})_{|W} = (s_{f^{-1}(V)})_{|W}$$

for some $W \subseteq f^{-1}(U \cap V)$. Furthermore, if every open subset $W \subseteq f^{-1}(U)$ is of the form $W = f^{-1}(W')$ for some open subset $W' \subseteq X$, e.g. f open, then $(f_* \mathcal{F})_{f(x)} \to \mathcal{F}_x$ is bijective.

Proof. By definition, we have a map

$$(f_*\mathcal{F})_{f(x)} = \varinjlim_{U \ni f(x)} \mathcal{F}(f^{-1}(U)) = \varinjlim_{x \in f^{-1}(U)} \mathcal{F}(f^{-1}(U)) \to \varinjlim_{x \in V} \mathcal{F}(V) = \mathcal{F}_x$$

which sends a tuple $(f^{-1}(U), s_{f^{-1}(U)})_{\sim_1}$ to the tuple $(f^{-1}(U), s_{f^{-1}(U)})_{\sim_2}$. Here

$$(f^{-1}(U), s_{f^{-1}(U)})_{\sim_1} = (f^{-1}(V), s_{f^{-1}(V)})_{\sim_1} \Leftrightarrow (s_{f^{-1}(U)})_{|f^{-1}(W')} = (s_{f^{-1}(U)})_{|f^{-1}(W')}$$

for some open $W' \subseteq U \cap V$ and

$$(f^{-1}(U), s_{f^{-1}(U)})_{\sim_2} = (f^{-1}(V), s_{f^{-1}(V)})_{\sim_2} \Leftrightarrow (s_{f^{-1}(U)})_{|W} = (s_{f^{-1}(U)})_{|W}$$

for some open $W \subseteq f^{-1}(U \cap V)$. Thus if every open subset $W \subseteq f^{-1}(U)$ is of the form $W = f^{-1}(W')$ for some open $W' \subseteq X$, this provides injectivity. Moreover, the surjectivity also follows since the index sets over which the direct limits run coincide. □

Remark B.1.32. Let X be a topological space. We want to note that at least for sheaves, it is enough to define it on a base of the topology of X to obtain a unique sheaf on X. The reader is referred to the section Bases and sheaves in [Sta18, Tag 009H]. In particular, note the statements [Sta18, Tag 009R] and [Sta18, Tag 009U]. △

Definition B.1.33. A sequence

$$\ldots \xrightarrow{\alpha_{i-1}} \mathcal{F}_i \xrightarrow{\alpha_i} \mathcal{F}_{i+1} \xrightarrow{\alpha_{i+1}} \ldots$$

of sheaves is called exact if $\mathrm{im}(\alpha_i) = \ker(\alpha_{i+1})$ for all i. △

Lemma B.1.34. *Any exact sequence of sheaves $\mathcal{F}_i$ on X*

$$\ldots \xrightarrow{\alpha_{i-1}} \mathcal{F}_i \xrightarrow{\alpha_i} \mathcal{F}_{i+1} \xrightarrow{\alpha_{i+1}} \ldots$$

provides for any open $U \subseteq X$ an exact sequence

$$\ldots \xrightarrow{\alpha_{i-1|U}} (\mathcal{F}_i)_{|U} \xrightarrow{\alpha_{i|U}} (\mathcal{F}_{i+1})_{|U} \xrightarrow{\alpha_{i+1|U}} \ldots$$

Proof. Let $\alpha : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. Note that the presheaves defined by $V \mapsto \mathrm{im}(\alpha(V))$ and $W \mapsto \mathrm{im}(\alpha_{|U}(W))$ for $W \subseteq U$ open coincide if restricted to U. Hence $\mathrm{im}(\alpha)_{|U} = \mathrm{im}(\alpha_{|U})$ as sheaves where im denotes the sheafification of $V \mapsto \mathrm{im}(\alpha(V))$. The same is true for the kernel sheaf: $\ker(\alpha)_{|U} = \ker(\alpha_{|U})$. This provides the assertion. □

Definition B.1.35. Let X be a topological space and $\mathcal{O}$ a presheaf of rings on X. A **presheaf of $\mathcal{O}$-modules on** X is a presheaf $\mathcal{F}$ of abelian groups on X together with a morphism of presheaves of sets $\mathcal{O} \times \mathcal{F} \to \mathcal{F}$ such that for every open subset $U \subseteq X$ the map $\mathcal{O}(U) \times \mathcal{F}(U) \to \mathcal{F}(U)$ makes the group $\mathcal{F}(U)$ into an $\mathcal{O}(U)$-module. If additionally, both $\mathcal{O}$ and $\mathcal{F}$ are sheaves, then we call $\mathcal{F}$ a **sheaf of $\mathcal{O}$-modules on** X. If $(X, \mathcal{O}_X)$ is a ringed space, then we call any sheaf of $\mathcal{O}_X$-modules on X an **$\mathcal{O}_X$-module**. △

Lemma B.1.36. *Let*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0 \tag{1:1}$$

be an exact sequence of $\mathcal{O}_X$-modules where $\mathcal{F}$ is quasi-coherent. Let $U \subseteq X$ be an affine open subset. Then

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \mathcal{G}(U) \longrightarrow \mathcal{H}(U) \longrightarrow 0 \tag{1:2}$$

is an exact sequence of $\mathcal{O}_X(U)$-modules.

Proof. By Lemma B.1.34, the sequence

$$0 \longrightarrow \mathcal{F}_{|U} \longrightarrow \mathcal{G}_{|U} \longrightarrow \mathcal{H}_{|U} \longrightarrow 0$$

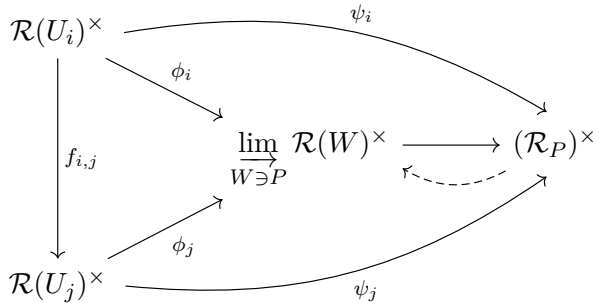
is exact and $\mathcal{F}_{|U}$ is still quasi-coherent. Then the assertion follows from [GW10, 12.34] since the global sections of $\mathcal{F}_{|U}$ are $\mathcal{F}(U)$. □

In the following lemma one should think of $\mathcal{R}$ as being the sheaf of regular functions on a scheme.

Lemma B.1.37 (Stalks of a sheaf of units)**.** *Let X be a topological space and $\mathcal{R}$ be a sheaf of rings on X. Then for any open subset $U \subseteq X$ the rule $U \mapsto \mathcal{R}(U)^\times$ defines a sheaf of abelian groups on X. Moreover, for any $P \in X$ we have $(\mathcal{R}^\times)_P = (\mathcal{R}_P)^\times$.*

Proof. First of all, since $\mathcal{R}$ is a sheaf of rings, $\mathcal{R}(U)^\times$ is an abelian group and a subset of $\mathcal{R}(U)$. Since units get sent to units under ring homomorphisms $\rho_V^U(\mathcal{R}) : \mathcal{R}(U) \to \mathcal{R}(V)$ for $U \subseteq V$, we have that $\rho_V^U(\mathcal{R})$ restricted to $\mathcal{R}(U)^\times$ yields a homomorphism of abelian groups $\mathcal{R}(U)^\times \to \mathcal{R}(V)^\times$. We take these homomorphisms as the restriction maps of $U \mapsto \mathcal{R}(U)^\times$. This easily defines a presheaf of abelian groups on X which we denote by $\mathcal{R}^\times$. To prove that $\mathcal{R}^\times$ is a sheaf, note that if $s \in \mathcal{R}^\times(U) = \mathcal{R}(U)^\times$ restricts to the unit in $\mathcal{R}^\times(U_i)$ for an open cover $U = \cup_{i\in I} U_i$, then the *separatedness* axiom of $\mathcal{R}$ provides $s = 1$ in $\mathcal{R}(U)$ and thus in $\mathcal{R}^\times(U)$. Thus $\mathcal{R}^\times$ satisfies the *separatedness* axiom. To prove the *gluing local sections* axiom, let $U = \cup_{i\in I} U_i$ be an open cover of an open subset U and write $U_{i,j} = U_i \cap U_j$. Then let $s_i \in \mathcal{R}^\times(U_i)$ be such that $s_{i|U_{i,j}} = s_{j|U_{i,j}}$ for all $i, j \in I$. The *gluing local sections* axiom of $\mathcal{R}$ provides the existence of a unique section $s \in \mathcal{R}(U)$ which restricts to the s_i on U_i. Hence we are left to prove that $s \in \mathcal{R}^\times(U)$. By assumption, we have $s_i \in \mathcal{R}^\times(U_i)$ for all $i \in I$. Therefore, there are $t_i \in \mathcal{R}^\times(U_i)$ such that $s_i t_i = 1$ in $\mathcal{R}^\times(U_i)$. In particular, for all $i, j \in I$ we also have $s_{i|U_{i,j}} \cdot t_{i|U_{i,j}} = 1$. Hence $t_{i|U_{i,j}}$ is the unique inverse of $s_{i|U_{i,j}}$ in $\mathcal{R}(U_i)$. But since this is also true for $t_{j|U_{i,j}}$ by construction, we obtain $t_{i|U_{i,j}} = t_{j|U_{i,j}}$ for all $i, j \in I$. We deduce that there is a unique section $t \in \mathcal{R}(U)$ such that $t_{|U_i} = (s_{|U_i})^{-1}$. Hence $(st)_{|U_i} = 1$ for all $i \in I$ and thus $st = 1$ in $\mathcal{R}(U)$ since $\mathcal{R}$ was a sheaf. This proves that $\mathcal{R}^\times$ indeed is a sheaf on X.

To prove the second assertion, consider the direct system consisting of the groups $(\mathcal{R}^\times)(U_i) = \mathcal{R}(U_i)^\times$ with group homomorphisms $f_{i,j} : \mathcal{R}(U_i)^\times \to \mathcal{R}(U_j)^\times$ for all $U_j \subseteq U_i$. Note that since $\mathcal{R}(U_i)^\times \subseteq \mathcal{R}(U_i)$, we obtain maps $\psi_i : \mathcal{R}(U_i)^\times \to (\mathcal{R}_P)^\times$ sending g_i to the germ (g_i, U_i) whose inverse in $(\mathcal{R}_P)^\times$ is given by (g_i^{-1}, U_i). Hence we obtain the commutative diagram (the dashed arrow is left out with respect to the commutativity) where $U_j \subseteq U_i$:



Now we argue that we find the dashed morphism making the whole diagram commute. Then, since the direct limit satisfies the universal property, the same would be true for $\mathcal{R}_P^\times$. This would prove, due to the uniqueness of the direct limit, that

$$(\mathcal{R}^\times)_P = \varinjlim_{W \ni P} \mathcal{R}(W)^\times \cong \mathcal{R}_P^\times.$$

Let $g \in \mathcal{R}_P^\times$ be arbitrary. Since $\mathcal{R}_P^\times \subseteq \mathcal{R}_P$ and the latter itself is a direct limit, we find a representation of g as (g, U_i) with U_i being an open neighborhood of P and (g^{-1}, U_i) being its inverse. Hence $(g, U_i) \in \mathcal{R}(U_i)^\times$ is a preimage of g under ψ_i and can thus be mapped to $\varinjlim_{W \ni P} \mathcal{R}(W)^\times$ via ϕ_i. Since both $(\mathcal{R}^\times)_P$ and $\mathcal{R}_P^\times$ are direct limits, the choice of the representation of g is irrelevant for the map and hence the latter is well-defined. □

Lemma B.1.38. *Let X be topological space and $U_i, i \in I$, an open cover of X. Let $\mathcal{F}_i$ be sheaves on U_i and assume that for each $i, j \in I$ with $U_{i,j} := U_i \cap U_j \neq \emptyset$ we have an isomorphism $\phi_{i,j} : (\mathcal{F}_i)_{|U_{i,j}} \to (\mathcal{F}_j)_{|U_{i,j}}$ satisfying the **cocycle conditions***

$$\phi_{i,i} = \mathrm{id} \quad \text{and} \quad \forall\ i, j, k \in I \text{ with } U_i \cap U_j \cap U_k \neq \emptyset : \ \phi_{j,k} \circ \phi_{i,j} = \phi_{i,k}.$$

Then there exists a sheaf $\mathcal{F}$ on X which is unique up to isomorphism such that there exists isomorphisms $\psi_i : \mathcal{F}_{|U_i} \to \mathcal{F}_i$, $i \in I$ with $\psi_j \circ \psi_i^{-1} = \phi_{i,j}$ on $U_{i,j}$.

The sections of $\mathcal{F}$ are defined as

$$\mathcal{F}(U) = \left\{ (s_i)_{i \in I} \in \coprod_{i \in I} \mathcal{F}_i(U_i \cap U) \mid (s_j)_{|U \cap U_{i,j}} = \phi_{i,j}((s_i)_{|U \cap U_{i,j}}) \right\}$$

*and $\mathcal{F}$ is called the **sheaf glued from the $\mathcal{F}_i$ along the $\phi_{i,j}$**.*

Proof. The assertion is easily verified with the definition of the sections of $\mathcal{F}$ given above. □

Definition B.1.39. Let $\mathcal{O}$ be a presheaf of rings on the topological space X. Let $\mathcal{F}, \mathcal{G}$ be two presheaves of $\mathcal{O}$-modules on X. Then we define the **presheaf tensor product of presheaves of $\mathcal{O}$-modules on** X by the rule

$$U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U)$$

for every open subset $U \subseteq X$ and denote it by $\mathcal{F} \otimes_{\mathcal{O}}^p \mathcal{G}$. If $\mathcal{O}$ is a sheaf of rings and both $\mathcal{F}$ and $\mathcal{G}$ are sheaves of $\mathcal{O}$-modules, then we call the sheafification of the above presheaf the **tensor product of $\mathcal{O}$-modules** and denote it by $\mathcal{F} \otimes_{\mathcal{O}}^s \mathcal{G}$ or more commonly by $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G}$. △

The following lemma shows that it does not matter if we sheafify the presheaves $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{O}$ and then form the tensor product or if we just sheafify right away the presheaf tensor product of $\mathcal{F}$ and $\mathcal{G}$ over $\mathcal{O}$.

Lemma B.1.40. *Let $\mathcal{O}$ be a presheaf of rings on the topological space X. Let $\mathcal{F}, \mathcal{G}$ be two presheaves of $\mathcal{O}$-modules on X. Then we have an isomorphism*

$$(\mathcal{F} \otimes_{\mathcal{O}}^p \mathcal{G})^\# \longrightarrow \mathcal{F}^\# \otimes_{\mathcal{O}^\#}^s \mathcal{G}^\#.$$

Proof. We have a natural morphism of presheaves

$$\begin{array}{ccccccc} \mathcal{F} & \otimes_{\mathcal{O}}^p & \mathcal{G} & \longrightarrow & \mathcal{F}^\# & \otimes_{\mathcal{O}^\#}^p & \mathcal{G}^\# \\ \mathcal{F}(U) & \otimes_{\mathcal{O}(U)}^p & \mathcal{G}(U) & \longrightarrow & \mathcal{F}^\#(U) & \otimes_{\mathcal{O}^\#(U)} & \mathcal{G}^\#(U) \end{array}$$

using the natural morphism $\theta : \mathcal{F} \to \mathcal{F}^\#$ as in Lemma B.1.15. Since θ_P is an isomorphism for all $P \in X$, it is obvious that the induced homomorphisms on the level of stalks are isomorphisms of $\mathcal{O}_P$-modules. Then Lemma B.1.17 provides that the sheafifications are isomorphic and since the sheafification of the codomain is by definition $\mathcal{F}^\# \otimes_{\mathcal{O}^\#}^s \mathcal{G}^\#$, the assertion follows. □

Let $f : Y \to X$ be a continuous map of topological spaces and $\mathcal{H}, \mathcal{F}$ be two sheaves on X such that $\mathcal{H} \leq \mathcal{F}$. For the restriction resp. pullback of divisors we will later need that we have a natural morphism of sheaves on X provided by the pushforward f_*:

$$f_*\mathcal{F}/f_*\mathcal{H} \longrightarrow f_*(\mathcal{F}/\mathcal{H})$$

To explicitly see how this map works, we unpack the definitions of the quotient sheaf (as a sheafification of a presheaf) in general and apply it to the quotients appearing above.

The definition of sheafification of a presheaf provides a description of the sections of a sheafification over some open subset, see Lemma B.1.22, and thus gives us, using Corollary B.1.23, the following lemma.

Lemma B.1.41. *Let $\mathcal{H}, \mathcal{F}$ be two sheaves (say of abelian groups) on a topological space X such that $\mathcal{H} \leq \mathcal{F}$. Then the sections of the quotient sheaf $\mathcal{F}/\mathcal{H}$ (whose group law we denote additively) over the open subset $U \subseteq X$ are classes of families $(U_i, s_i + \mathcal{H}(U_i))$ with $\{U_i \mid i \in I\}$ an open cover of U and $s_i + \mathcal{H}(U_i) \in \mathcal{F}(U_i)/\mathcal{H}(U_i)$ sections that agree on overlaps, that is*

$$(s_i)_{|U_i \cap U_j} - (s_j)_{|U_i \cap U_j} \in \mathcal{H}(U_i \cap U_j)$$

for all $i, j \in I$. Two such families $(U_i, s_i + \mathcal{H}(U_i))$ and $(V_j, t_j + \mathcal{H}(V_j))$ define the same class if and only if for all $i, j \in I$ we have $(t_j)_{|U_i \cap V_j} - (s_i)_{|U_i \cap V_j} \in \mathcal{H}(U_i \cap V_j)$.

Corollary B.1.42. *Let $f : Y \to X$ be a morphism of schemes and $\mathcal{F}$, $\mathcal{H}$ be $\mathcal{O}_Y$-modules or sheaves of abelian groups on Y. The sections of $f_*\mathcal{F}/f_*\mathcal{H}$ over $U \subseteq X$ open are classes of families*

$$(U_i, s_i + \mathcal{H}(f^{-1}(U_i)))$$

with $\{U_i \mid i \in I\}$ an open cover of U and $s_i + \mathcal{H}(f^{-1}(U_i)) \in \mathcal{F}(f^{-1}(U_i))/\mathcal{H}(f^{-1}(U_i))$ sections that agree on overlaps, i.e. $(s_i)_{|f^{-1}(U_i \cap U_j)} - (s_j)_{|f^{-1}(U_i \cap U_j)} \in \mathcal{H}(f^{-1}(U_i \cap U_j))$ for all $i, j \in I$. Two such families

$$(U_i, s_i + \mathcal{H}(f^{-1}(U_i))) \quad \text{and} \quad (V_j, t_j + \mathcal{H}(f^{-1}(V_j)))$$

define the same class if and only if for all i, j we have

$$(t_j)_{|f^{-1}(U_i \cap V_j)} - (s_i)_{|f^{-1}(U_i \cap V_j)} \in \mathcal{H}(f^{-1}(U_i \cap V_j)).$$

Corollary B.1.43. *Let $f : Y \to X$ be a morphism of schemes and $\mathcal{F}$, $\mathcal{H}$ be $\mathcal{O}_Y$-modules or sheaves of abelian groups on Y. Then $(f_*(\mathcal{F}/\mathcal{H}))(U) = (\mathcal{F}/\mathcal{H})(f^{-1}(U))$ consists of classes of families*

$$(V_i, s_i + \mathcal{H}(V_i))$$

with $\{V_i \mid i \in I\}$ an open cover of $f^{-1}(U)$ and $s_i + \mathcal{H}(V_i) \in \mathcal{F}(V_i)/\mathcal{H}(V_i)$ sections that agree on overlaps, i.e. $(s_i)_{|V_i \cap V_j} - (s_j)_{|V_i \cap V_j} \in \mathcal{H}(V_i \cap V_j)$ for all $i, j \in I$. Two such families

$$(V_i, s_i + \mathcal{H}(V_i)) \quad \text{and} \quad (W_j, t_j + \mathcal{H}(W_j))$$

define the same class if and only if for all i, j we have $(t_j)_{|V_i \cap W_j} - (s_i)_{|V_i \cap W_j} \in \mathcal{H}(V_i \cap W_j)$.

We have seen above that the sections of both $f_*(\mathcal{F}/\mathcal{H})$ and $f_*\mathcal{F}/f_*\mathcal{H}$ over the open subset $U \subseteq X$ are locally given by elements in $\mathcal{F}(V_i)/\mathcal{H}(V_i)$ where V_i form an open cover of $f^{-1}(U)$ and the local representations coincide on the overlaps. The difference is that for $f_*(\mathcal{F}/\mathcal{H})$ the open subsets V_i covering $f^{-1}(U)$ may be arbitrary and for $f_*\mathcal{F}/f_*\mathcal{H}$ they need to be preimages of an open cover U_i of U. But this tells us that we can find a natural map from the latter to the former.

Proposition B.1.44. *Let $f : Y \to X$ be a morphism of schemes and $\mathcal{F}$, $\mathcal{H}$ be $\mathcal{O}_Y$-modules or sheaves of abelian groups on Y. We have a natural map $\phi : f_*\mathcal{F}/f_*\mathcal{H} \longrightarrow f_*(\mathcal{F}/\mathcal{H})$ with $\phi(U)$ sending $(U_i, s_i + \mathcal{H}(f^{-1}(U_i)))$ to $(f^{-1}(U_i), s_i + \mathcal{H}(f^{-1}(U_i)))$.*

Proof. Let $(U_i, s_i + \mathcal{H}(f^{-1}(U_i))) \in (f_*\mathcal{F}/f_*\mathcal{H})(U)$ with $U = \bigcup_{i\in I} U_i$. Then $f^{-1}(U_i)$, $i \in I$ defines an open cover of $f^{-1}(U)$ and thus $(f^{-1}(U_i), s_i + \mathcal{H}(f^{-1}(U_i)))$, $i \in I$, does indeed define an element in $(f_*(\mathcal{F}/\mathcal{H}))(U)$. If $(W_j, t_j + \mathcal{H}(f^{-1}(W_j)))$, $j \in J$, defines the same element in $(f_*\mathcal{F}/f_*\mathcal{H})(U)$ as $(U_i, s_i + \mathcal{H}(f^{-1}(U_i)))$ does, then for all $i \in I$, $j \in J$ we have $(s_i)_{|f^{-1}(U_i\cap W_j)} - (t_j)_{|f^{-1}(U_i\cap W_j)} \in \mathcal{H}(f^{-1}(U_i \cap W_j))$. Now $(f^{-1}(W_j), t_j + \mathcal{H}(f^{-1}(W_j)))$, $j \in J$, defines the same element as $(f^{-1}(U_i), s_i + \mathcal{H}(f^{-1}(U_i)))$ does: For all $i \in I$, $j \in J$ we have

$$\begin{aligned}(t_j)_{|f^{-1}(U_i)\cap f^{-1}(W_j)} + \mathcal{H}(f^{-1}(U_i \cap W_j)) &= (t_j)_{|f^{-1}(U_i\cap W_j)} + \mathcal{H}(f^{-1}(U_i \cap W_j))\\ &= (s_i)_{|f^{-1}(U_i\cap W_j)} + \mathcal{H}(f^{-1}(U_i \cap W_j))\\ &= (s_i)_{|f^{-1}(U_i)\cap f^{-1}(W_j)} + \mathcal{H}(f^{-1}(U_i \cap W_j)).\end{aligned}$$

That ϕ is compatible with the restriction maps follows immediately since the sections in question stay the same: For (U_i, s_i) as a section of $f_*\mathcal{F}/f_*\mathcal{H}$ over U with cover U_i and $V \subseteq U$ we have the following diagram which obviously commutes and thus provides the assertion:

$$\begin{array}{ccc}(U_i, s_i + \mathcal{H}(f^{-1}(U_i))) & \xrightarrow{\phi(U)} & (f^{-1}(U_i), s_i + \mathcal{H}(f^{-1}(U_i)))\\ \Big\downarrow{\scriptstyle \mathrm{res}_{\mathcal{F}/\mathcal{H}, f^{-1}(U_i), f^{-1}(U_i\cap V)}} & & \Big\downarrow{\scriptstyle \mathrm{res}_{\mathcal{F}/\mathcal{H}, f^{-1}(U_i), f^{-1}(U_i\cap V)}}\\ (U_i \cap V, (s_i)_{|U_i\cap V} + \mathcal{H}(f^{-1}(U_i \cap V))) & \xrightarrow{\phi(V)} & (f^{-1}(U_i \cap V), (s_i)_{|U_i\cap V} + \mathcal{H}(f^{-1}(U_i \cap V)))\end{array}$$

□

Corollary B.1.45. *If every open cover of $f^{-1}(U)$ is induced by an open cover of U, e.g. f is the morphism embedding Y as a subscheme in X (open or closed), then the morphism in Proposition B.1.44 maps as the identity and induces an isomorphism.*

B.2 Sheaves on Schemes

We omit the definition of schemes and its fundamental properties.

Definition B.2.1. Let X be a scheme. By X^0 we denote the set of generic points of the irreducible components of X. By X_0 we denote the set of closed points of X. △

Proposition B.2.2. *Let X be a locally noetherian scheme with a finite number of irreducible components, e.g. X noetherian. Furthermore, assume that X has no embedded points. For $\eta \in X^0$ let $j_\eta : \mathrm{Spec}(\mathcal{O}_{X,\eta}) \to X$ denote the canonical map of schemes. Then*

(i) $\mathcal{K}_X = \bigoplus_{\eta\in X^0} (j_\eta)_*\mathcal{O}_{X,\eta} = \prod_{\eta\in X^0} (j_\eta)_*\mathcal{O}_{X,\eta}$,

(ii) $\mathcal{K}_X(U) = \bigoplus_{\eta\in U\cap X^0} \mathcal{O}_{X,\eta} = \bigoplus_{\eta\in U\cap X^0} \mathrm{Frac}(\mathcal{O}_{X,\eta})$, *for $U \subseteq X$ open,*

(iii) $\mathcal{K}_{X,P} := (\mathcal{K}_X)_P = \mathrm{Frac}(\mathcal{O}_{X,P})$,

(iv) $\mathcal{K}_X$ *is a quasi-coherent sheaf of $\mathcal{O}_X$-algebras, and*

(v) $\mathcal{K}_X(U) = \mathrm{Frac}(\mathcal{O}_X(U))$ *for every affine open $U \subseteq X$.*

Proof. Since X is locally noetherian, the weakly associated points of X coincide with the associated points of X, see [Sta18, Tag 05AR]. Moreover, each of these is by assumption a generic point of an irreducible component of X. Hence the requirements for X in [Sta18, Tag 0EMF] are met. All of the assertions are proven there. The only exception is Item (ii) which directly follows from Item (i) and the definitions:

$$((j_\eta)_*\mathcal{O}_{X,\eta})(U) = \mathcal{O}_{X,\eta}(j_\eta^{-1}(U)) = \begin{cases} \mathcal{O}_{X,\eta}(\operatorname{Spec}(\mathcal{O}_{X,\eta})) = \mathcal{O}_{X,\eta}, & \eta \in U \\ \mathcal{O}_{X,\eta}(\emptyset) = 0, & \eta \notin U \end{cases}$$

Note that the assumption we impose on X are stronger than the one given in [Sta18, Tag 0EMF], see [Sta18, Tag 05AR]. □

Corollary B.2.3. *Let X and the notation be as in Proposition B.2.2 with $X_1, \dots, X_m$ being the irreducible components of X. Let $\tau_i : X_i \to X$ denote the closed immersion corresponding to X_i. Then $\mathcal{K}_X = \bigoplus_{i=1}^m (\tau_i)_*\mathcal{K}_{X_i}$.*

Proof. Let η_i denote the generic point of X_i and by $j_i = j_{\eta_i} : \operatorname{Spec}(\mathcal{O}_{X_i,\eta_i}) \to X$ we denote the natural morphism. The latter obviously factors through X_i, i.e. $j_i = \tau_i \circ j_{i,\eta}$ with $j_{i,\eta_i} : \operatorname{Spec}(\mathcal{O}_{X_i,\eta_i}) \to X_i$. By definition, we have $\mathcal{K}_{X_i} = (j_{i,\eta_i})_*\mathcal{O}_{X_i,\eta_i}$ and by Proposition B.2.2 (i), we have

$$\mathcal{K}_X = \bigoplus_{i=1}^m (j_i)_*\mathcal{O}_{X,\eta_i} = \bigoplus_{i=1}^m (\tau_i \circ j_{i,\eta_i})_*\mathcal{O}_{X,\eta_i} = \bigoplus_{i=1}^m (\tau_i)_* \underbrace{((j_{i,\eta_i})_*\mathcal{O}_{X,\eta_i})}_{=\mathcal{K}_{X_i}}. \qquad \square$$

Lemma B.2.4. *The sheaves $\mathcal{K}_X$ and $\mathcal{K}_X^\times$ are both flasque and satisfy $H^i(X, \mathcal{K}_X) = 0$ and $H^i(X, \mathcal{K}_X^\times) = 1$ for all $i > 0$.*

Proof. The statement about the cohomology groups follows from [Har77, III 2.5] once we have shown the flasqueness of $\mathcal{K}_X$ and $\mathcal{K}_X^\times$. First of all, by Lemma B.1.37, $\mathcal{K}_X^\times$ is indeed a sheaf of rings on X. By Proposition B.2.2 (ii), the restriction maps $\mathcal{K}_X(V) \to \mathcal{K}_X(U)$ for open $U \subseteq V$ are given by the identity map whenever $U \cap X^0 = V \cap X^0$ and otherwise by projecting. Hence the restriction maps are surjective and thus $\mathcal{K}_X$ is flasque. By Proposition B.2.2 (ii), $\mathcal{K}_X(U)$ is the direct sum of its localisations at points in $U \cap X^0$. Thus

$$(\mathcal{K}_X^\times)(U) = \mathcal{K}_X(U)^\times = \left(\bigoplus\nolimits_{\eta \in U \cap X^0} \mathcal{K}_{X,\eta}\right)^\times = \bigoplus\nolimits_{\eta \in U \cap X^0} \mathcal{K}_{X,\eta}^\times = \bigoplus\nolimits_{\eta \in U \cap X^0} (\mathcal{K}_X^\times)_\eta$$

and hence for $\mathcal{K}_X^\times$, as for $\mathcal{K}_X$ before, its sections are given by a finite sum of its localisations which analogously to the argument above provide that the restriction maps of $\mathcal{K}_X^\times$ are surjective and therefore, that $\mathcal{K}_X^\times$ is flasque as well. □

Lemma B.2.5. *Let X be a locally noetherian scheme. Then for every open subscheme $U \subseteq X$ with open immersion $i : U \hookrightarrow X$ the following are equivalent.*

(i) U is schematically dense in X,

(ii) $i^\# : \mathcal{O}_X \to i_*\mathcal{O}_U$ is injective, and

(iii) for every open subscheme $V \subseteq X$ the only closed subscheme Y of V such that $U \cap V \subseteq Y$ is V itself.

Proof. The proof is the combination of [Liu02, 7.1.9] and [GW10, 9.19]. □

Lemma B.2.6. *Let X be a locally noetherian scheme. Let $i : U \hookrightarrow X$ be the open immersion of a schematically dense open subset $U \subseteq X$. Then*

(i) $\mathcal{K}_X \cong i_*\mathcal{K}_U$, $i_*\mathcal{K}_U^\times = (i_*\mathcal{K}_U)^\times \cong \mathcal{K}_X^\times$,

(ii) $\mathcal{O}_X \to i_*\mathcal{O}_U$ *as well as* $\mathcal{O}_X^\times \to (i_*\mathcal{O}_U)^\times = i_*\mathcal{O}_U^\times$ *are injective, and*

(iii) all the above provide a monomorphism $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times \hookrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times$.

Proof. The isomorphism $\mathcal{K}_X \cong i_*\mathcal{K}_U$ is [Liu02, 7.1.15] and the injectivity of $\mathcal{O}_X \to i_*\mathcal{O}_U$ (this is even an if and only if) is [Liu02, 7.1.9]. The identities $i_*\mathcal{K}_U^\times = (i_*\mathcal{K}_U)^\times$ and $(i_*\mathcal{O}_U)^\times = i_*\mathcal{O}_U^\times$ follow by definition. Now since injectivity can be checked at the level of stalks, Lemma B.1.37 provides the second assertion. Now we prove the last assertion. The monomorphism $\mathcal{O}_U^\times \hookrightarrow \mathcal{K}_U^\times$ provides the monomorphism $i_*\mathcal{O}_U^\times \hookrightarrow i_*\mathcal{K}_U^\times$ which composed with the isomorphism $i_*\mathcal{K}_U^\times \to \mathcal{K}_X^\times$ provides the monomorphism $i_*\mathcal{O}_U^\times \hookrightarrow \mathcal{K}_X^\times$. The latter morphism is compatible with the monomorphisms $\mathcal{O}_X^\times \hookrightarrow i_*\mathcal{O}_U^\times$ and $\mathcal{O}_X^\times \hookrightarrow \mathcal{K}_X^\times$ in the sense that the diagram

$$\begin{array}{ccc} i_*\mathcal{O}_U^\times & \hookrightarrow & \mathcal{K}_X^\times \\ \uparrow & & \uparrow \\ \mathcal{O}_X^\times & \xrightarrow{\mathrm{id}} & \mathcal{O}_X^\times \end{array}$$

is commutative. Now composing $i_*\mathcal{O}_U^\times \hookrightarrow \mathcal{K}_X^\times$ with the projection $\mathcal{K}_X^\times \to \mathcal{K}_X^\times/\mathcal{O}_X^\times$ provides the desired monomorphism $i_*\mathcal{O}_U^\times/\mathcal{O}_X^\times \hookrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times$. □

Remark B.2.7. For a more detailed and elaborated analysis of the third statement of Lemma B.2.6, we refer the reader to Proposition 5.3.1. △

Lemma B.2.8. *Let* $\mathcal{F}$ *be a skyscraper sheaf on the scheme* X*. Then for* $i > 0$ *we have* $H^i(X, \mathcal{F}) = 0$.

Proof. Obviously, skyscraper sheaves are flasque since their restriction maps are given by projecting. Now [Har77, III 2.5] provides the assertion. □

Lemma B.2.9 ([Sta18], Tag 0AVL)**.** *Let* X *be a locally noetherian scheme. Let* $\varphi : \mathcal{F} \to \mathcal{G}$ *be a map of quasi-coherent* $\mathcal{O}_X$*-modules. Assume that for every* $x \in X$ *at least one of the following happens*

1. $\mathcal{F}_x \to \mathcal{G}_x$ *is injective, or*
2. $x \notin \mathrm{Ass}(\mathcal{F})$.

Then φ *is injective.*

B.3 Irreducible Components

Let X and Y be two schemes. Let U_i form an open cover of Y and let $f_i : U_i \to X$ be morphisms of schemes. If the f_i agree on intersections, i.e. for all i, j we have $(f_i)_{|U_i \cap U_j} = (f_j)_{|U_i \cap U_j}$, then there is a unique morphism of schemes $f : Y \to X$ such that $f_{|U_i} = f_i$.

We can use this property of gluing morphisms of schemes to obtain a natural map from the disjoint union of the irreducible components of a scheme X to X itself: Let X be a scheme with finitely many irreducible components $X_1, \ldots, X_m$ and closed immersions $\tau_i : X_i \to X$. By Y we denote the disjoint union of the $X_1, \ldots, X_m$. Obviously, the X_i are open since their complements are finite unions of closed subsets (here we need that Y is the *disjoint* union). Moreover, they cover Y and we have morphisms $\tau_i : X_i \to X$ which

agree on intersections since these are empty. Hence there is a unique morphism $\tau : Y \to X$ such that the following diagram commutes:

$$\begin{array}{ccc} X_i & \xrightarrow{\upsilon_i} & Y = \bigsqcup_{i=1}^m X_i \\ \downarrow{\scriptstyle \tau_i} & \swarrow{\scriptstyle \tau} & \\ X & & \end{array}$$

Here υ_i denotes the inclusion map which is both an open and a closed immersion of the connected and irreducible component X_i of Y respectively.

The structure sheaf $\mathcal{O}_Y$ of Y is given by the direct sum of the structure sheaves of the X_i, that is $\mathcal{O}_Y = \bigoplus_{i=1}^m \mathcal{O}_{X_i}$ with $\mathcal{O}_Y(U) = \bigoplus_{i=1}^m \mathcal{O}_{X_i}(U \cap X_i)$. Moreover, the restriction map for $V \subseteq U$ is given by the sum of the restriction maps of $\mathcal{O}_{X_i}$.

The corresponding morphisms of structure sheaves $\mathcal{O}_X \to (\tau_i)_*\mathcal{O}_{X_i}$, $\mathcal{O}_Y \to (\upsilon_i)_*\mathcal{O}_{X_i}$ and $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ satisfy that the composed morphism

$$\mathcal{O}_X \to \tau_*\mathcal{O}_Y \to \tau_*((\upsilon_i)_*\mathcal{O}_{X_i}) = (\tau \circ \upsilon_i)_*\mathcal{O}_{X_i}$$

equals $\mathcal{O}_X \to (\tau_i)_*\mathcal{O}_{X_i}$. That is, for every open subset $U \subseteq X$ the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_X(U) & \xrightarrow{\tau^\#} & \bigoplus_{i=1}^m \mathcal{O}_{X_i}(U \cap X_i) \\ & \searrow^{\tau_i^\#} & \downarrow{\scriptstyle \upsilon_i^\#} \\ & & \mathcal{O}_{X_i}(U \cap X_i) \end{array}$$

We fix this situation in a definition where we intentionally omit the morphisms υ_i.

Definition B.3.1. Let X be a scheme with finitely many irreducible components X_i, $i = 1, \ldots, m$ and closed immersions $\tau_i : X_i \to X$. By Y we denote the disjoint union of the components of X and the morphism glued together from the closed immersions τ_i is denoted by $\tau : Y \to X$. It comes with a morphism of sheaves

$$\mathcal{O}_X \to \tau_*\mathcal{O}_Y = \bigoplus_{i=1}^m (\tau_i)_*\mathcal{O}_{X_i}$$

which is the product of the morphisms $\mathcal{O}_X \to (\tau_i)_*\mathcal{O}_{X_i}$. That is, for $U \subseteq X$ open with $I = \{i \in \{1, \ldots, m\} : U \cap X_i \neq \emptyset\}$ it maps

$$\begin{array}{rcl} \mathcal{O}_X(U) & \to & \bigoplus_{i \in I} \mathcal{O}_{X_i}(U \cap X_i) = \bigoplus_{i \in I} \mathcal{O}_X(U)/P_i \\ f & \mapsto & (f + P_i)_{i \in I} \end{array} \tag{3:3}$$

where $\{P_i \mid i \in I\}$ denote the minimal prime ideals of $\mathcal{O}_X(U)$. △

Proposition B.3.2. *The morphism $\tau : Y \to X$ as in Definition B.3.1 is finite.*

Proof. Note that being a finite morphism is a local property in the sense that it is equivalent to finding an affine open cover for which the induced morphisms are finite, see [Sta18, Tag 01WI]. Furthermore, closed immersions are finite morphisms, see [Sta18, Tag 035C]. Since the affine open covers of the X_i yield an affine open cover of Y, we obtain that $\tau : Y \to X$ is a finite morphism. □

Proposition B.3.3. *The morphism $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ as in Definition B.3.1 is injective if and only if X is reduced.*

Proof. The ring homomorphisms $\mathcal{O}_X(U) \to \bigoplus_{i \in I} \mathcal{O}_X(U)/P_i$ as in Eq. (3:3) have kernel $\bigcap_{i \in I} P_i$. Hence the kernel is the nilradical of $\mathcal{O}_X(U)$ which is zero if and only if $\mathcal{O}_X(U)$ is

reduced. By [Liu02, 2.4.2], this holds for every open subset $U \subseteq X$ of X if and only if X is reduced. □

Since the morphism $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ is injective whenever X is reduced, we consider the corresponding exact sequence of sheaves:

Definition B.3.4. Let X be a reduced scheme with finitely many irreducible components X_i, $i = 1, \dots, m$. Let $Y = \bigsqcup_{i=1}^m X_i$ be as in Definition B.3.1. By $\mathscr{S} = \mathscr{S}_{Y/X}$ we denote the cokernel of the injective morphism $\mathcal{O}_X \to \tau_*\mathcal{O}_Y = \bigoplus_{i=1}^m (\tau_i)_*\mathcal{O}_{X_i}$. Hence we have an exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \bigoplus_{i=1}^m (\tau_i)_*\mathcal{O}_{X_i} \longrightarrow \mathscr{S} \longrightarrow 0. \tag{3:4}$$

△

Lemma B.3.5. *Let the situation be as in Definition B.3.1. We have an isomorphism*

$$(\tau_*\mathcal{O}_Y)_P = \bigoplus_{P \in X_i} \mathcal{O}_{X,P}/\mathcal{J}_{i,P}$$

where $\mathcal{J}_i$ denotes the sheaf of ideals on X that cuts out the irreducible component X_i. Moreover, by $\mathcal{J}_{i,P}$ we denote the stalk of $\mathcal{J}_i$ at P.

Proof. Since direct limits commute with direct sums, we have

$$(\tau_*\mathcal{O}_Y)_P = \bigoplus_{i=1}^m ((\tau_i)_*\mathcal{O}_{X_i})_P = \bigoplus_{i=1}^m (\mathcal{O}_X/\mathcal{J}_i)_P,$$

and since $(\mathcal{O}_X/\mathcal{J}_i)_P = 0$ for all $P \notin X_i$, we obtain the desired result. □

Remark B.3.6. Let X be a scheme with finitely many irreducible components X_i, $i = 1, \dots, m$. Let $X^i := X \setminus \bigcup_{j \neq i}^m X_j \subseteq X_i$ and set $U^i := U \cap X^i$ for any $U \subseteq X$. Since there are only a finite number of irreducible components, X^i is open in X and hence U^i is open for any open $U \subseteq X$. By construction, U^i has no intersection with any other irreducible component of X. That is, the family of non-empty open subsets of X that meet X_i has a cofinal subfamily consisting of those open and non-empty subsets meeting X_i and no other irreducible component. Now computing direct limits for a given directed set is (up to isomorphism) the same as computing it for a cofinal subset. Therefore, whenever we consider a direct limit running over all open neighborhoods of a generic point η_i of X_i of X, then we might as well compute it via running over all open subsets of X that only meet X_i and no other irreducible component. △

In Corollary 3.2.15 we will see that the morphism $\mathcal{O}_X \to \tau_*\mathcal{O}_Y$ will extend to $\mathcal{K}_X \to \tau_*\mathcal{K}_Y$. But by the definition of the sheaf $\mathcal{K}_X$, we will see that the sheaves $\mathcal{K}_X$ and $\tau_*\mathcal{K}_Y$ are isomorphic when we take into account that the respective local rings at the same generic point of X are isomorphic as the following lemma shows.

Lemma B.3.7. *Let X be a reduced scheme with irreducible components $X_1, \dots, X_m$. Let Y denote the disjoint union of the X_i, see Definition B.3.1. Then for any generic point η_i of X_i we have*

$$\mathcal{O}_{X_i,\eta_i} \cong \mathcal{O}_{X,\eta_i} \cong \mathcal{O}_{Y,\eta_i}$$

where we identified the generic point η_i of X_i with the corresponding generic point of X and Y.

Proof. In Remark B.3.6 we have seen that we might compute the respective direct limits via the cofinal directed set of those open subsets which are contained in X_i and do not meet any other irreducible component of X. Hence

$$\begin{aligned}
\mathcal{O}_{Y,\eta_i} &= \varinjlim_{\bigsqcup_{j=1}^m U_j \subseteq Y \text{ open}} \mathcal{O}_Y(\bigsqcup_{j=1}^m U_j) = \varinjlim_{\bigsqcup_{j=1}^m U_j \subseteq Y \text{ open}} \bigoplus_{j=1}^m \mathcal{O}_{X_i}(U_i) \\
\text{Remark B.3.6} \rightsquigarrow \quad &\cong \varinjlim_{U_i \subseteq X_i \text{ open in } X_i} \mathcal{O}_{X_i}(U_i) \\
&= \mathcal{O}_{X_i,\eta_i}.
\end{aligned}$$

Now the surjective morphism $\mathcal{O}_X \to (\tau_i)_*\mathcal{O}_{X_i}$ gives a surjective homomorphism of rings $\mathcal{O}_{X,\eta_i} \to \mathcal{O}_{X_i,\eta_i}$. But since both X and X_i are reduced, the rings $\mathcal{O}_{X,\eta_i}$ and $\mathcal{O}_{X_i,\eta_i}$ are fields, see Lemma B.4.29. But any ring homomorphism of fields is clearly injective and thus we obtain the desired isomorphism. □

Corollary B.3.8. *The morphism $\mathcal{K}_X \to \tau_*\mathcal{K}_Y$ is an isomorphism of sheaves on X.*

Proof. This follows from Proposition B.2.2 and Lemma B.3.7. □

B.4 Commutative Algebra

The following Theorem is called the *Nullstellensatz* in its general form, it can be found in [Eis95, 4.5]. A **Jacobson** ring is a ring in which every prime ideal is the intersection of maximal ideals. This is trivially true for fields.

Theorem B.4.1. *Let R be a Jacobson ring. Let $f : R \to S$ make the ring S into a finitely generated R-algebra. Then S is a Jacobson ring. Further, if $\mathfrak{n} \subseteq S$ is a maximal ideal, then $f^{-1}(\mathfrak{n})$ is a maximal ideal of R, and $S/\mathfrak{n}$ is a finite field extension of $R/f^{-1}(\mathfrak{n})$.*

Corollary B.4.2. *Let $f : A \to B$ be a k-algebra homomorphism of the finite k-algebras A and B. Then $f^{-1}(\mathfrak{m})$ is a maximal ideal of A for every maximal ideal $\mathfrak{m}$ of B.*

Proof. Without loss of generality, we assume that $k \subseteq A$ and $k \subseteq B$ such that the embedding is compatible with f. We can regard $C = A/f^{-1}(\mathfrak{m})$ as a k-subalgebra of the field $B/\mathfrak{m}$. Hence we have ring extensions $k \hookrightarrow C \hookrightarrow B/\mathfrak{m}$. By Theorem B.4.1, B is a Jacobson ring and the extension $B/\mathfrak{m}$ over k is a finite extension of fields. In particular, the dimension of $B/\mathfrak{m}$ over k is finite and thus the same is true for C. This already implies that C is a field: Every non-zero element in C provides via multiplication an injective k-vector space automorphism (since C is a domain as it is contained in a field) which is thus also surjective. This provides an inverse element and hence C is a field. Whence $A/f^{-1}(\mathfrak{m})$ is a field and therefore $f^{-1}(\mathfrak{m})$ a maximal ideal of A. □

Definition B.4.3. Let R be a k-algebra. We call R a **k-algebra of finite residual-type** or a **finite residual-type k-algebra** if for all maximal ideals $P \in \operatorname{Spec}(R)_0$ the k-vector space $R/P \cong R_P/PR_P$ has finite dimension. △

Lemma B.4.4. *Every finitely generated k-algebra is a finite residual-type k-algebra.*

Proof. Let $f : k \to R$ be the k-algebra homomorphism that makes R into a k-algebra. Then, by Theorem B.4.1, we see that for any maximal ideal $P \in \operatorname{Spec}(R)_0$ the k-vector space R/P has finite dimension. However, we have $R_P/PR_P \cong R/P$ as rings since localisation commutes with taking quotients, see [Sta18, Tag 00CT]. This proves the assertion. □

Lemma B.4.5 (Prime Avoidance lemma, see [Sta18] Tag 00DS)**.** *Let R be a ring. Let $I_i \subseteq R$, $i = 1, \dots, r$, and $J \subseteq R$ be ideals. Assume*

(i) $J \not\subseteq I_i$ for $i = 1, \dots, r$, and

(ii) all but two of I_i are prime ideals.

Then there exists an $x \in J$ such that $x \notin \cup_{i=1}^r I_i$. In particular, if $J \subseteq \cup_{i=1}^r I_i$, then $J \subseteq I_i$ for some i.

Lemma B.4.6. *Let R be a semi-local commutative ring, that is, R has only a finite number of maximal ideals. Then every invertible fractional ideal of R is principal.*

Proof. Suppose that $I \subseteq \mathrm{Frac}(R)$ is a non-zero invertible ideal of R with inverse $J \subseteq \mathrm{Frac}(R)$, i.e. $IJ = R$. We denote the maximal ideals by $\mathfrak{m}_1, \dots, \mathfrak{m}_\ell$. For all $j \in \{1, \dots, \ell\}$ there are $a_j \in I$ and $b_j \in J$ such that $a_j b_j \in R \setminus \mathfrak{m}_j$ since otherwise $IJ \subseteq \mathfrak{m}_j$. Moreover, we find $\lambda_{ji} \in \mathfrak{m}_j \setminus (\mathfrak{m}_j \cap \mathfrak{m}_i)$ for all $j \neq i$ and can set $\lambda_i = \prod_{j \neq i} \lambda_{ji}$ with $\lambda_i \in \mathfrak{m}_j$ for all $j \neq i$ and $\lambda_i \notin \mathfrak{m}_i$. Let $a = \sum_{i=1}^\ell \lambda_i a_i \in I$ and $b = \sum_{j=1}^\ell \lambda_j b_j \in J$. Then we have $ab = \sum_{i,j} \lambda_i \lambda_j a_i b_j$. By construction, $\lambda_i \lambda_i a_i b_i \notin \mathfrak{m}_i$ and for $j \neq i$ we have $\lambda_i \lambda_j a_i b_j \in \mathfrak{m}_i$, that is $ab \notin \mathfrak{m}_i$ for all $i \in \{1, \dots, \ell\}$. Whence ab is a unit in R and thus $I = abI \subseteq aIJ = aR$ which together with $aR \subseteq I$ yields the assertion. □

Lemma B.4.7. *Let k be a field. Let R be a noetherian k-algebra of Krull dimension one. Let I be an ideal of R such that R/I has Krull dimension zero. Then for all $A \in \{\mathrm{Spec}(R), V(I), \mathrm{Spec}(R)_0\}$ we have*

$$R/I \cong \bigoplus_{P \in A} R_P/I_P.$$

Moreover, if R is of finite residual-type (e.g. R is a finite k-algebra, see B.4.4), then for all such A the sum

$$\dim_k R/I = \sum_{P \in A} \dim_k R_P/I_P$$

is finite.

Proof. By assumption, the quotient R/I has Krull dimension zero. Since any noetherian ring of dimension zero is artinian, see [Sta18, Tag 00KH], R/I is artinian. Then, by [Sta18, Tag 00JB], we have $R/I \cong \bigoplus_{P \in V(I)} R_P/I_P$. For any $P \in \mathrm{Spec}(R)$ not contained in $V(I)$ the quotient R_P/I_P is trivial since I_P then is equal to R_P. Hence we might also let P run through all prime ideals of R. Every ideal in $V(I)$ is maximal and thus we might also let P only run over all maximal ideals of R. This proves the first assertion.

Now assume that the residue class fields of R, i.e. $R/P \cong R_P/PR_P$ for $P \in \mathrm{Spec}(R)$, have finite dimension over k. We are left to prove that $S = R_P/I_P$ has finite dimension over k. By [Sta18, Tag 00KJ], S is a zero-dimensional and local artinian ring whose maximal ideal $\mathfrak{m}$ is nilpotent. Denote by $\kappa = S/\mathfrak{m}$ the residue class field of S which is a finite dimensional k-vector space since it is isomorphic to R_P/PR_P. We obtain a filtration of the k-vector space S

$$0 = \mathfrak{m}^n \subsetneq \mathfrak{m}^{n-1} \subsetneq \dots \subsetneq \mathfrak{m}^2 \subsetneq \mathfrak{m} \subsetneq S$$

whose quotients κ and $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ have finite k-dimension: Indeed, $\dim_k \kappa$ is finite by assumption and the κ-vector spaces $\mathfrak{m}^i/\mathfrak{m}^{i+1} = \mathfrak{m}^i/\mathfrak{m}\mathfrak{m}^i$ are of finite dimension since $\mathfrak{m}$ (recall that R and thus S is noetherian) and thus $\mathfrak{m}^i$ is finitely generated as an S-module.

In particular, the multiplicativity of the dimension of vector spaces implies that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is also of finite dimension over κ. We have a short exact sequence of k-vector spaces

$$0 \longrightarrow \mathfrak{m} \longrightarrow S \longrightarrow \kappa \longrightarrow 0$$

which yields (since κ is a free module over k and thus projective, i.e. the short exact sequence splits) $S \cong \mathfrak{m} \oplus \kappa$ as k-vector spaces. Hence S is of finite k-dimension if both κ and $\mathfrak{m}$ are. Since κ is finite-dimensional over k, it is left to show that $\mathfrak{m}$ is finite-dimensional over k. But the same argument shows that $\mathfrak{m}$ is finite-dimensional over k if both $\mathfrak{m}^2$ and $\mathfrak{m}/\mathfrak{m}^2$ are. Proceeding as above (or using induction) we see that S is finite-dimensional over if all quotients $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ are (since $\mathfrak{m}^n = 0$) and this has already been proven above. □

Proposition B.4.8. *Let R be a ring with $I \subseteq R$ being an ideal. Let M be an R-module. Then $M \otimes_R R/I$ and M/IM are isomorphic as R-modules and as R/I-modules.*

Proof. We have the canonical exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

of R-modules. Now tensoring this sequence with M over R provides, by [Sta18, Tag 00DF], an exact sequence

$$I \otimes_R M \xrightarrow{\phi} R \otimes_R M \xrightarrow{\psi} R/I \otimes_R M \longrightarrow 0$$

with $\phi(r \otimes m) = r \otimes m$ and $\psi(r \otimes m) = (r + I) \otimes m$. We identify $R \otimes_R M$ with $RM = M$ and under this identification we have $\phi(I \otimes_R M) = IM$. Hence the exactness of the above sequence implies

$$M \otimes_R R/I \cong \psi(M) \cong M/\ker(\psi) = M/\phi(I \otimes_R M) = M/IM.$$

Clearly, both M/IM and $M \otimes_R R/I$ are R/I-modules. The isomorphism we obtain from above is given by

$$M \otimes_R R/I \to M/IM, \quad m \otimes (r + I) \mapsto rm + IM$$

which is clearly also R/I-linear providing the last part of the assertion. □

Lemma B.4.9. *Let $n = \sum_{i=1}^m n_i$. Given two matrices $A = (A_{i,j})_{i,j}, B = (B_{i,j})_{i,j} \in k[x]^{n\times n}$ in n-block-form, see Definition 4.4.6, we can multiply those by treating their block entries as entries of a normal matrix, that is*

$$AB = (C_{i,j})_{i,j} \quad \text{with} \quad C_{i,j} = \sum_{\ell=1}^{m} A_{i,\ell} \cdot B_{\ell,j}.$$

Proof. The (i, j)-entry of the product AB of two arbitrary matrices A, B with compatible dimensions is given by the product of the i-th row of A with the j-th column of B. This directly provides the assertion. □

Lemma B.4.10. *Let $B \supseteq A$ be a finite ring extension such that A is a domain with field of fractions $\mathrm{Frac}(A) = K$. Then $B \otimes_A K = \mathrm{Frac}(B)$.*

Proof. By assumption, $B \otimes_A K$ is a finite dimensional K-vector space. Since $B \subseteq B \otimes_A K$, we have $\mathrm{Frac}(B) \subseteq \mathrm{Frac}(B \otimes_A K)$ and hence it suffices to show $\mathrm{Frac}(B \otimes_A K) = B \otimes_A K$. To do this, we show that every regular element of $B \otimes_A K$ is invertible: By assumption, the linear map given by multiplying with a regular element is injective and hence by the

rank-nullity theorem also surjective. This provides an inverse linear map corresponding to an inverse element. □

Lemma B.4.11. *Let $N \subseteq M$ be two free $k[x]$-modules of the same rank n. Let T be a basis transformation matrix from a basis of M to a basis of N. Then* $\dim_k M/N = \deg\det T$.

Proof. Let $m_1, \dots, m_n$ and $n_1, \dots, n_n$ be bases of M respectively N such that

$$(m_1, \dots, m_n) \cdot T = (n_1, \dots, n_n). \tag{4:5}$$

Let $S = \operatorname{diag}(f_1, \dots, f_n)$ denote the Smith-Normal-Form of T, then Eq. (4:5) becomes

$$(\widetilde{m}_1, \dots, \widetilde{m}_n) \cdot S = (\widetilde{n}_1, \dots, \widetilde{n}_n). \tag{4:6}$$

with $\widetilde{m}_1, \dots, \widetilde{m}_n$ and $\widetilde{n}_1, \dots, \widetilde{n}_n$ bases of M respectively N. Note that we have $\deg\det T = \deg\det S = \sum_{i=1}^n \deg f_i$. Now we obviously have

$$M/N = \frac{\bigoplus_{i=1}^n \widetilde{m}_i k[x]}{\bigoplus_{i=1}^n \widetilde{n}_i k[x]} = \frac{\bigoplus_{i=1}^n \widetilde{m}_i k[x]}{\bigoplus_{i=1}^n \widetilde{m}_i f_i k[x]} \cong \bigoplus_{i=1}^n \frac{\widetilde{m}_i k[x]}{\widetilde{m}_i f_i k[x]} \cong \bigoplus_{i=1}^n \frac{k[x]}{f_i k[x]}$$

and the latter has dimension $\sum_{i=1}^n \deg f_i$ over k. This provides the assertion. □

Definition B.4.12. Let R be a noetherian ring and M a finite R-module. Let $i \geq 0$ be an integer. Then we say that M *has property* S_k or *is* S_k if for every prime ideal P of R we have $\operatorname{depth}_{R_P}(M_P) \geq \min\{i, \dim \operatorname{Supp}(M_P)\}$. △

To prove that every minimal prime ideal of any ring solely consist of zero-divisors, we cite a result which we will use.

Lemma B.4.13 ([Kap70], Theorem 84)**.** *Let R be a ring and let M be a non-zero R-module. Let P be a prime ideal of R which is minimal over $\operatorname{Ann}_R(M)$. Then P is contained in the set of zero-divisors of R.*

Corollary B.4.14. *Let R be a ring. Then any minimal prime ideal of R solely consists of zero-divisors.*

Proof. Consider $M = R$ as an R-module. Then $\operatorname{Ann}_R(M) = 0$ and thus, by Lemma B.4.13, any prime ideal of R which is minimal over 0 is contained in the set of zero-divisors of R. But the prime ideals of R that are minimal over 0 are exactly the minimal prime ideals of R. □

In a reduced ring, we also have that every zero-divisor is contained in some minimal prime ideal.

Lemma B.4.15 ([Sta18], Tag 00EW)**.** *Let R be a reduced ring. Then the union of the minimal prime ideals of R equals the set of zero-divisors of R.*

We can extend the definition of zero-divisor to modules.

Definition B.4.16. Let R be a ring and let M be an R-module. An element $a \in R$ is called a *zero-divisor on* M if there is some non-zero $m \in M$ such that $am = 0$ in M. △

We want to call a module M on which this cannot happen to be *torsion-free*. But since any zero-divisor pair a, b of R with $ab = 0$ provides (independently of M!) zero-divisors a, b on M with $a \cdot (bm) = 0$, we restrict the definition to those elements not being zero-divisors in R:

Definition B.4.17. Let R be a ring and let M be an R-module. We say M is a *torsion-free* R-module or *torsion-free over* R if any zero-divisor on M is a zero-divisor in R. △

Every annihilator $\mathrm{Ann}_R(m)$ of an element $m \in M$ is an ideal only consisting of zero-divisors on M. Obviously, the union of all such annihilators provides the set of zero-divisors on M. Whenever R is noetherian, the set of all such annihilator ideals has maximal elements which turn out to be prime ideals and are called the associated primes of M. This provides the following lemma.

Lemma B.4.18 ([Sta18], Tag 00LD)**.** *Let R be a noetherian ring and M an R-module. Then the set of zero-divisors on M is equal to $\bigcup_{P \in \mathrm{Ass}_R(M)} P$.*

Definition B.4.19. Let R be a ring and M an R-module. The elements of $\mathrm{Ass}_R(M)$ which are not minimal in $\mathrm{Ass}_R(M)$ are called the *embedded associated primes of M* or sometimes short *embedded primes of M*. △

The following lemma and its corollary draw a connection between being torsion-free and being S_1.

Lemma B.4.20 ([Sta18], Tag 031Q)**.** *Let R be a noetherian ring and M a finite R-module. Then M is S_1 if and only if M has no embedded primes.*

A direct implication of the definition of torsion-free and Lemma B.4.18 is:

Corollary B.4.21. *Let R be a noetherian ring satisfying S_1 and M a torsion-free R-module. Then every associated prime of M is a minimal prime ideal of R. In particular, M has no embedded primes and thus, if M is finite, by Lemma B.4.20, satisfies S_1.*

Proof. By definition, the set of zero-divisors on M is a subset of the set of zero-divisors in R. Since R satisfies S_1, it has no embedded primes and thus, by Lemma B.4.18, the set of zero-divisors in R is the union of the minimal primes of R. Hence every associated prime of M is contained in the union of the minimal primes of R. Thus the prime avoidance lemma Lemma B.4.5 provides that every associated prime of M is contained in and hence equal to a minimal prime of R. The particular part follows immediately from Lemma B.4.20. □

Lemma B.4.22 ([BH98], Proposition 1.2.1)**.** *Let R be a noetherian ring and M a finite R-module. If an ideal $I \subseteq R$ consists of zero-divisors on M, then $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}_R(M)$.*

Lemma B.4.23. *Let R be a noetherian ring satisfying S_1. Let M be an R-module. If M is torsion-free over R, then $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$. Conversely, if M is finite over R, then $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$ implies that M is torsion-free over R. In particular, any finite R-module M is torsion-free if and only if $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$.*

Proof. Let M be torsion-free and $P \in \mathrm{Ass}_R(M)$. By Corollary B.4.21, we have $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$ and M satisfies S_1. Conversely, let M be finite over R such that $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$. Let $a \in R$ be a zero-divisor on M with non-zero $m \in M$ such that $am = 0$. Then $aR \subseteq \mathrm{Ann}_R(m)$ and hence it solely contains zero-divisors on M. By Lemma B.4.22, aR is contained in an associated prime of M. Hence, by assumption, $a \in \bigcup_{\mathfrak{p} \in \mathrm{Spec}(R)^0} \mathfrak{p}$ is a zero-divisor. □

The following proposition shows that being torsion-free is a local property whenever the ground ring satisfies S_1, is noetherian and of dimension one.

Proposition B.4.24. *Let R be a noetherian ring of dimension one which satisfies S_1 and let M be a finite R-module. Then M is torsion-free over R if and only if M_P is torsion-free over R_P for all maximal ideals P in R.*

Proof. By Lemma B.4.23, M is torsion-free over R if and only if $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$. Since R is noetherian, by [Sta18, Tag 0310], we have $P \in \mathrm{Ass}_R(M)$ if and only if $PR_P \in \mathrm{Ass}_{R_P}(M_P)$. The minimal primes of R_P correspond to the minimal primes of R contained in P. Assume that M is torsion-free and thus $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$. Let P be a maximal ideal of R and $QR_P \in \mathrm{Ass}_{R_P}(M_P)$. Then QR_P is either a minimal prime in R_P and thus minimal in R or $Q = P$. If $Q = P$, by [Sta18, Tag 0310], $P \in \mathrm{Ass}_R(M)$ which is minimal by assumption.

Conversely, assume that $\mathrm{Ass}_{R_P}(M_P) \subseteq \mathrm{Spec}(R_P)^0$ for all maximal ideals P of R. Let $P \in \mathrm{Ass}_R(M)$ be arbitrary. By [Sta18, Tag 0310], we have that $PR_P \in \mathrm{Ass}_{R_P}(M_P) \subseteq \mathrm{Spec}(R)^0$ is minimal in R_P and thus minimal in R. □

Injectivity of module homomorphisms is decided at the prime ideals not associated to the domain. The proof was adopted from the statement [Sta18, Tag 0AVL] which states this fact for quasi-coherent $\mathcal{O}_X$-modules on a locally noetherian scheme.

Lemma B.4.25. *Let R be a noetherian ring and M, N two R-modules together with an R-module homomorphism $f : M \to N$. Then f is injective if and only if the induced homomorphism $f_P : M_P \to N_P$ is injective for all $P \in \mathrm{Ass}_R(M)$.*

Proof. Clearly, if f is injective, then $f_P : M_P \to N_P$ is injective for all prime ideals of R. Conversely, consider the R-module $K = \ker(f) \leq M$. By assumption, $K_P = 0$ for all $P \in \mathrm{Ass}_R(M)$. For every R-module, the associated primes are a subset of the support. Now any associated prime of K is an associated prime of M and hence $\mathrm{Ass}_R(K) = \emptyset$ which is only possible for the zero module since R is noetherian, see [Sta18, Tag 0587]. □

Lemma B.4.26. *Let R be a noetherian ring and M a finite R-module. If M_P is isomorphic to R_P as R_P-modules for some $P \in \mathrm{Spec}(R)$, then there is some $f \in R \setminus P$ such that $M_f \cong R_f$.*

Proof. First we choose $h \in R \setminus P$ such that $\lambda : M_h \to M_P$ is injective as follows: Consider the coherent sheaves $M^\sim$ and $M_P^\sim$ on $X = \mathrm{Spec}(R)$ where the latter is the skyscraper sheaf located at $P \in X$. The localisation homomorphism $\lambda_P : M \to M_P$ provides a morphism of sheaves $\phi : M^\sim \to M_P^\sim$. Obviously, $\phi_P = \mathrm{id}$ and thus the sheaf $\ker(\phi)$ satisfies $\ker(\phi)_P = 0$. Now since $\ker(\phi)_P = \varinjlim_{h \in R \setminus P} \ker(\phi)_h$, we know that there is some $h \in R \setminus P$ such that $\ker(\phi)_h = 0$ and thus $\lambda : M_h \to M_P$ is injective.

Let $x_1, \ldots, x_m$ be a generating set of M_h as an R_h-module and let m/r be a generator of M_P over R_P. There are are uniquely determined a_i/s_i such that

$$\lambda(x_i) = \frac{a_i}{s_i}\frac{m}{r}.$$

Now set $g = r\prod_{i=1}^m s_i$ and then we see that m generates M_{hg} over R_{hg}. In particular, we have an exact sequence

$$0 \to K \to R_{hg} \to M_{hg} \to 0$$

where the map $R_{hg} \to M_{hg}$ sends 1 to m. Now localising at P we see that $K_P = 0$ and since K is finitely generated, there is some $b \in R \setminus P$ such that $K_b = 0$. Now set $f = ghb \in R \setminus P$ and we obtain $M_f \cong R_f$ as asserted. □

Remark B.4.27. Lemma B.4.26 holds more generally. The statement stays true if we replace *M_P is isomorphic to R_P* with *M_P is isomorphic to R_P^r for some $r \geq 1$* which then provides $M_f \cong R_f^r$. The proof is basically the same and we just need to take care about the denominators of all of the basis elements of M_P. △

Proposition B.4.28 ([Sta18], Tag 0311)**.** *Let R be a noetherian ring and let M be an R-module. Then the canonical map $M \to \prod_{P \in \mathrm{Ass}_R(M)} M_P$ is injective.*

Lemma B.4.29 ([Sta18], Tag 00EU). *Let R be a reduced ring and let P be a minimal prime of R. Then R_P is a field.*

Corollary B.4.30. *Let R be a reduced ring and let P be a minimal prime of R. Let M be an R-module. Then $(M/PM)_P \cong M_P$.*

Proof. We know that $M/PM \cong M \otimes_R R/P$ and hence we obtain

$$(M/PM)_P \cong M_P \otimes_{R_P} R_P/PR_P = M_P \otimes_{R_P} R_P = M_P$$

where we have used $PR_P = 0$ since R_P was a field, see Lemma B.4.29. □

Lemma B.4.31. *Let R be a reduced noetherian ring and let P be a minimal prime ideal of R. Then*

$$\begin{array}{rcl} \phi : (R/P)_{P(R/P)} & \to & R_P \\ \frac{r+P}{s+P} & \mapsto & \frac{r}{s} \end{array} \tag{4:7}$$

is an isomorphism of rings.

Proof. By Lemma B.4.29, we know that $PR_P = 0$ and thus ϕ is well-defined. It is obviously surjective. Moreover, if $r/s = 0$ in R_P, then there is some $t \in R \setminus P$ such that $tr = 0$ in R. In particular, $t+P \neq 0+P$ and $(t+P)(r+P) = 0$ in R. Since R/P is an integral domain, ϕ is therefore injective as well. Finally, the homomorphism property is evident. □

Lemma B.4.32. *Let R be a reduced noetherian ring and let P be a minimal prime ideal of R. Let M be a finite R-module which is invertible at P. Then M_P can be considered as an R/P-module and*

$$\begin{array}{rcl} \phi : (M/PM)_{P(R/P)} & \to & M_P \\ \frac{m+PM}{r+P} & \mapsto & \frac{m}{r}. \end{array} \tag{4:8}$$

is an isomorphism of R/P-modules.

Proof. First of all, R_P is an R/P-algebra and as such, isomorphic to $\mathrm{Frac}(R/P)$. We have a map $R/P \to R_P$ that maps $r+P$ to $r/1$ and since PR_P is the zero ideal, see Lemma B.4.29, we see that it is indeed well-defined. Moreover, it is an injective ring homomorphism. The homomorphism property is evident and if $r/1 = 0$ in R_P, then there is some $s \in R \setminus P$ such that $rs = 0$ in R. In particular, $rs \in P$ and thus $r \in P$. This makes R_P into an R/P-algebra. Now since $M_P = M \otimes_R R_P$, we see that M_P also carries the structure of an R/P-module and we have $PM_P = 0$ since $PR_P = 0$, see Lemma B.4.29. The scalar multiplication is thus defined by $(s+P) \cdot (m/r) = (sm)/r$. Now consider the map ϕ from Eq. (4:8). Since $PM_P = 0$, we know that ϕ is well-defined. It is obviously surjective. If $m/r = 0$ in M_P, then there is some $s \in R \setminus P$ such that $sm = 0$ in M. In particular, $s+P \neq 0+P$ and $(s+P)(m+PM) = 0$ in M/PM. Hence ϕ is also injective. Finally, we prove that ϕ is R/P-linear. Let $s+P \in R/P$, $(m+PM)/(r+P)$ be arbitrary. Then

$$\phi\left((s+P) \cdot \frac{m+PM}{r+P}\right) = \phi\left(\frac{sm+PM}{r+P}\right) = \frac{sm}{r}.$$

Moreover,

$$(s+P) \cdot \phi\left(\frac{m+PM}{r+P}\right) = (s+P) \cdot \frac{m}{r} = \frac{sm}{r}$$

which completes the proof. □

Corollary B.4.33. *Let R be a reduced noetherian ring and let M be a torsion-free R-module. Let P be a minimal prime of R. If M is invertible at P, then M/PM is invertible at $P(R/P)$.*

Proof. By Lemma B.4.32, we have $(M/PM)_{P(R/P)} \cong M_P$ and, by Lemma B.4.31, we have $(R/P)_{P(R/P)} \cong R_P$. The latter isomorphism is also an isomorphism of R_P-modules and thus we obtain

$$(M/PM)_{P(R/P)} \cong M_P \cong R_P \cong (R/P)_{P(R/P)}$$

as asserted. □

Lemma B.4.34. *Let R be an integral domain and let M be a torsion-free R-module which is invertible at the zero ideal (0). Then*

$$M \hookrightarrow M_{(0)} \xrightarrow{\cong} R_{(0)} \xrightarrow{\cong} \operatorname{Frac}(R)$$

is an R-module embedding of M into $\operatorname{Frac}(R)$.

Proof. Since M is a torsion-free R-module, we know that the localisation homomorphism $M \to M_{(0)}$ is injective. By assumption, we have an isomorphism $M_{(0)} \to R_{(0)}$ and the latter is obviously isomorphic to $\operatorname{Frac}(R)$. Composing the above homomorphisms provides the asserted R-module embedding. □

We can even state a more general form of Corollary B.4.33.

Lemma B.4.35. *Let R be a noetherian reduced ring with minimal prime ideals $\{P_1, \dots, P_m\}$. Let $B \subseteq \{P_1, \dots, P_m\}$ and $I = \bigcap_{P \in B} P$. Let M be a torsion-free R-module which is invertible at the minimal primes of R. Then M/IM is invertible at the minimal prime ideals of R/I.*

Proof. The prime ideals of R/I are those given by $P + I$ with $P \in B$. Note that for a minimal prime $P+I$ the multiplicative set $(R/I) \setminus P+I$ is the image of the multiplicative set $R \setminus P$ under the canonical projection $R \to R/I$. Therefore, by [Sta18, Tag 00CT], we have

$$(R/I)_{P+I} \cong R_P/IR_P = R_P \tag{4:9}$$

where the latter equality is due to the fact that R_P is a field, see Lemma B.4.29. In particular,

$$\begin{aligned}(M/IM)_{P_i+I} \cong (M \otimes_R R/I) \otimes_{R/I} (R/I)_{P_i+I} &\cong (M \otimes_R R/I) \otimes_{R/I} R_{P_i} \\ &\cong M \otimes_R R_{P_i} \\ &\cong M_{P_i} \cong R_{P_i} \\ \text{Eq. (4:9)} \rightsquigarrow &\cong (R/I)_{P+I}\end{aligned}$$

providing the assertion. □

Remark B.4.36. We have seen in Lemma 4.1.2 that freeness of an R-module M at the minimal primes of R provide an R-module embedding into $\operatorname{Frac}(R)$. By Lemma B.4.35, we see that the same is true for M/IM as well. One should note that the proof of Lemma 4.1.2 embeds M into $\operatorname{Frac}(R)$ using the isomorphism $M_P \cong R_P$ for minimal primes $P \in \operatorname{Spec}(R)^0$. The proof of Lemma B.4.35 in turn shows that the isomorphism $(M/IM)_{P(R/I)} \cong (R/I)_{P(R/I)}$ stems from that of $M_P \cong R_P$. This provides a commutative

diagram as follows:

$$\begin{array}{ccc} \mathrm{Frac}(R) & \longrightarrow & \mathrm{Frac}(R/I) \\ \uparrow & & \uparrow \\ M & \xrightarrow{\mathrm{id}\otimes\pi} & M \otimes_R R/I = M/IM \end{array}$$

From this we can deduce that for any regular $g \in R$ such that $gM \subseteq R$, we have $(g + I)(M/IM) \hookrightarrow R/I$. Indeed, since the diagrams

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{Frac}(R) \\ \uparrow & & \uparrow \\ gM & \longrightarrow & M \end{array} \quad \text{and} \quad \begin{array}{ccc} R & \longrightarrow & \mathrm{Frac}(R) \\ \downarrow & & \downarrow \\ R/I & \longrightarrow & \mathrm{Frac}(R/I) \end{array}$$

commute as well, $(g+I)(M/IM) = (\mathrm{id}\otimes\pi)(gM)$ embeds into $\mathrm{Frac}(R/I)$ and has preimage under $\mathrm{Frac}(R) \to \mathrm{Frac}(R/I)$ which is contained in R and thus it embeds into R/I. △

Proposition B.4.37. *Let R be a reduced noetherian ring and let M be a finite and torsion-free R-module. Then the natural map $M \to \prod_{P\in \mathrm{Ass}_R(M)} M/PM$ is injective.*

Proof. By Lemma B.4.25, it suffices to show that the induced local homomorphism for all associated primes of M is injective. By Lemma B.4.23, we have $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$ and thus it suffices to show the injectivity at minimal primes of R. Let $\mathfrak{p} \in \mathrm{Spec}(R)^0$ be a minimal prime of R. Then the localised homomorphism is $M_\mathfrak{p} \to \prod_{P\in\mathrm{Spec}(R)^0}(M/PM)_\mathfrak{p}$. Now by Corollary B.4.30, we have $(M/PM)_\mathfrak{p} \cong M_\mathfrak{p}$ for $P = \mathfrak{p}$ and hence the homomorphism embeds $M_\mathfrak{p}$ as a direct summand in the codomain and is therefore injective. □

Remark B.4.38. The statement stays true for M being an R-algebra and the homomorphism $M \to \prod_{P\in\mathrm{Ass}(R)} M/PM$ being an R-algebra homomorphism. Moreover, note that since M is a torsion-free R-module, by Lemma B.4.23, we have $\mathrm{Ass}_R(M) \subseteq \mathrm{Spec}(R)^0$. Therefore, $M \to \prod_{P\in\mathrm{Spec}(R)^0} M/PM$ is injective. △

Corollary B.4.39. *Let R be a reduced noetherian ring and let M be a torsion-free R-module. Then $\bigcap_{P\in\mathrm{Ass}_R(M)} PM = 0$.*

Lemma B.4.40. *Let R be any ring and I, J two ideals in R with $I \cap J = 0$. Then the following sequence*

$$0 \longrightarrow R \xrightarrow{\phi} R/I \oplus R/J \xrightarrow{\psi} R/(I + J) \longrightarrow 0$$

with $\phi(a) = (a + I, a + J)$ and $\psi(a + I, b + J) = (a - b + I + J)$ is exact.

Proof. Obviously, $a \in \ker(\phi)$ if and only if $a \in I \cap J = 0$. Moreover, since ψ is taking the difference of the entries, $\psi \circ \phi = 0$. Now let $\psi(a + I, b + J)$ be zero, that is $a - b \in I + J$. Hence there are $a' \in I$ and $b' \in J$ such that $a - a' = b - b'$ in R. Then $(a + I, b + J) = (a - a' + I, b - b' + J) = \phi(a - a')$ and thus $\ker(\psi) \subseteq \mathrm{im}(\phi)$. □

Lemma B.4.41. *Let R be a reduced ring with minimal prime ideals $P_1, \dots, P_m$. Let $I = \bigcap_{i\in A} P_i$ and $J = \bigcap_{i\in B} P_i$ with $A, B \subseteq \{1, \dots, m\}$, $A \cup B = \{1, \dots, m\}$ and $A \cap B = \emptyset$. Then the injection $R \hookrightarrow R/I \oplus R/J$ extends to an isomorphism $\mathrm{Frac}(R) \to \mathrm{Frac}(R/I) \oplus \mathrm{Frac}(R/J)$.*

Proof. We use the fact that for reduced rings R, the injection $R \hookrightarrow \bigoplus_{i=1}^m R/P_i$ extends to an isomorphism $\mathrm{Frac}(R) \to \bigoplus_{i=1}^m \mathrm{Frac}(R/P_i)$, see [Liu02, 7.5.1]. So by assumption, we have

$$R/I \hookrightarrow \bigoplus_{i\in A} \underbrace{(R/I)/(P_i/I)}_{\cong\, R/P_i} \quad \text{and} \quad R/J \hookrightarrow \bigoplus_{i\in B} \underbrace{(R/J)/(P_i/J)}_{\cong\, R/P_i}$$

and these homomorphisms extend to isomorphisms

$$\mathrm{Frac}(R/I) \cong \bigoplus_{i\in A} R/P_i \quad \text{respectively} \quad \mathrm{Frac}(R/J) \cong \bigoplus_{i\in B} R/P_i.$$

In particular, the inclusion $R \hookrightarrow \bigoplus_{i\in A\cup B} R/P_i$, which does extend to an isomorphism $\mathrm{Frac}(R) \hookrightarrow \bigoplus_{i\in A\cup B} \mathrm{Frac}(R/P_i)$, factors through $R/I \oplus R/J$. Now since the homomorphisms $R \to \bigoplus_{i\in A\cup B} \mathrm{Frac}(R/P_i)$ and $R \to R/I \oplus R/J \hookrightarrow \bigoplus_{i\in A\cup B} \mathrm{Frac}(R/P_i)$ coincide, the assertion follows. □

Corollary B.4.42. *Let R be a reduced ring with minimal prime ideals $P_1, \dots, P_m$ and we set $I_i = \bigcap_{j=1}^{i} P_j$. Then for all $i = 2, \dots, m$ the following sequence*

$$0 \longrightarrow R/I_i \xrightarrow{\phi_i} R/I_{i-1} \oplus R/P_i \xrightarrow{\psi_i} R/(I_{i-1} + P_i) \longrightarrow 0$$

with $\phi_i(a + I_i) = (a + I_{i-1}, a + P_i)$ and $\psi_i(a + I_{i-1}, b + P_i) = (a - b + I_{i-1} + P_i)$ is exact.

Proof. Since R is reduced and $P_1, \dots, P_m$ are all the minimal prime ideals of R, we have $P_1 \cap \dots \cap P_m = 0$ in R. More general, R/I_i is also reduced since all its minimal prime ideals are $P_1 + I_i, \dots, P_i + I_i$ and thus their intersection equals the zero ideal I_i of R/I_i. Moreover, $I_{i-1} \cap P_i = I_i$ and hence we can use Lemma B.4.40 to deduce the assertion. □

Remark B.4.43. Let R be a ring and $I_1 \subseteq I_2 \subseteq \dots \subseteq I_m$ any chain of ideals. Let $f_i : R \to R/I_i$ denote the canonical epimorphism $r \mapsto r + I_i$. Then f_m factors through any R/I_i for $i = 1, \dots, m-1$. Moreover, we can naturally compose the f_i to obtain a homomorphism

$$R \to R/I_1 \to R/I_2 \to \dots \to R/I_{m-1} \to R/I_m$$

where $R/I_i \to R/I_{i-1}$ maps $r + I_i$ to $f_{i+1}(r) = r + I_{i+1}$. Then the above homomorphism equals f_m. △

Definition B.4.44. We can extend the homomorphisms ϕ_i by the sum $\mathrm{id}_i := \mathrm{id}^{\oplus i}$ of $m - i$ identity maps to obtain the maps

$$\phi_i \oplus \mathrm{id}_i : R/I_i \oplus \bigoplus_{j=i+1}^{m} R/P_j \longrightarrow R/I_{i-1} \oplus R/P_i \oplus \bigoplus_{j=i+1}^{m} R/P_j.$$

Now by Remark B.4.43, the composition $(\phi_2 \oplus \mathrm{id}_2) \circ \dots \circ (\phi_{m-1} \oplus \mathrm{id}_{m-1}) \circ \phi_m : R \to \bigoplus_{i=1}^{m} R/P_i$ equals the homomorphism $\phi : R \to \bigoplus_{i=1}^{m} R/P_i$ sending f to $(f + P_1, \dots, f + P_m)$. △

The following lemma just tells us that finding preimages of $(f_1+P_1, \dots, f_m+P_m)$ iteratively under $\phi_i \oplus \mathrm{id}_i$ yields a preimage under ϕ.

Lemma B.4.45. *Let the situation be as in Corollary B.4.42. Then $(f_1 + P_1, \dots, f_m + P_m) \in \bigoplus_{i=1}^{m} R/P_i$ lies in the image of $\phi : R \to \bigoplus_{i=1}^{m} R/P_i$ if and only if for all $i = 2, \dots, m$*

$$(f_1^{i-1} + I_{i-1}, f_i + P_i) \in \mathrm{im}(\phi_i). \tag{4:10}$$

Here $f_1^{i-1} + I_{i-1} = \phi_{i-1}^{-1}(f_1+P_1, \dots, f_{i-1}+P_{i-1}) \in R/I_{i-1}$ for $i \geq 3$ and $f_1^1 + I_{i-1} = f_1 + P_1$.

Proof. First of all, $(f_1^{i-1} + I_{i-1}, f_i + P_i) \in \mathrm{im}(\phi_i)$ if and only if

$$(f_1^{i-1} + I_{i-1}, f_i + P_i, \dots, f_m + P_m) \in \mathrm{im}(\phi_i \oplus \mathrm{id}_i).$$

We prove the assertion by induction on m, the number of minimal prime ideals of R. In the case $m = 2$ we have $I_1 = P_1$, $I_2 = P_1 \cap P_2$ and the homomorphism $\phi : R = R/I_2 \to$

$R/P_1 \oplus R/P_2$ coincides with the homomorphism $\phi_2 : R/I_2 \to R/P_1 \oplus R/P_2$. Hence the assertion is true for $m = 2$.

Now assume the assertion to be true for all rings with $m-1$ minimal prime ideals, $m \geq 2$. Then consider R to have m minimal prime ideals $P_1, \ldots, P_m$. Then $S := R/I_{m-1}$ has $m-1$ minimal prime ideals $P_1S, \ldots, P_{m-1}S$. Note that for all $i = 1, \ldots, m-1$ we have an isomorphism given by

$$\alpha_i : R/P_i \xrightarrow{\cong} S/P_iS, \quad r + P_i \mapsto (r + I_{m-1}) + P_i(R/I_{m-1}).$$

For $i = 2, \ldots, m-1$ we set

$$J_i = \cap_{j=1}^{i}(P_jS) = (\cap_{j=1}^{i}P_j)S = I_iS \subseteq S$$

for which

$$\beta_i : R/I_i \xrightarrow{\cong} S/J_i, \quad r + I_i \mapsto (r + I_{m-1}) + I_i(R/I_{m-1})$$

is an isomorphism for all $i = 1, \ldots, m-1$. Let $\psi_i : S/J_i \to S/J_{i-1} \oplus S/P_iS$ and $\phi_i : R/I_i \to R/I_{i-1} \oplus R/P_i$ denote the respective diagonal homomorphisms. Then we easily see that the following diagram commutes for all $i = 2, \ldots, m-1$:

$$\begin{array}{ccccc} S/J_i & \xrightarrow{\psi_i} & S/J_{i-1} & \oplus & S/P_iS \\ {\scriptstyle\beta_i}\uparrow & & \uparrow{\scriptstyle\beta_{i-1}} & & \uparrow{\scriptstyle\alpha_i} \\ R/I_i & \xrightarrow{\phi_i} & R/I_{i-1} & \oplus & R/P_i \end{array} \tag{4:11}$$

In particular, for $f_1^{i-1}, f_i \in R$ we have

$$(f_1^{i-1} + I_i, f_i + P_{i-1}) \in \mathrm{im}(\phi_i) \Leftrightarrow (f_1^{i-1} + J_i, f_i + P_{i-1}S) \in \mathrm{im}(\psi_i) \tag{4:12}$$

for all $i = 2, \ldots, m-1$. Here $f_1^{i-1} + J_i$ and $f_i + P_{i-1}S$ denote the respective elements induced by f_1^{i-1} and f_i in S/J_{i-1} respectively S/P_iS. The following diagram is rather obviously commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \xrightarrow{\phi_m} & S \oplus R/P_m & \longrightarrow & R/(I_{m-1} + P_m) & \longrightarrow & 0 \\ & & & \searrow^{\phi} & \downarrow{\scriptstyle \psi_{m-1}\oplus \mathrm{id}} & & & & \\ & & & & \bigoplus_{i=1}^{m-1} S/P_iS \oplus R/P_m & & & & \\ & & & & \downarrow{\scriptstyle \sum_{i=1}^{m-1}\alpha_i^{-1}\oplus \mathrm{id}} & & & & \\ & & & & \bigoplus_{i=1}^{m-1} R/P_i \oplus R/P_m & & & & \end{array} \tag{4:13}$$

Thus, by the commutative diagram in (4:13) and Corollary B.4.42, we have that

$$(f_1 + P_1, \ldots, f_{m-1} + P_{m-1}, f_m + P_m) \in \mathrm{im}(\phi)$$

if and only if

(i) $(f_1 + P_1S, \ldots, f_{m-1} + P_{m-1}S)$ lies in the image of ψ_{m-1}, with preimage, say f_1^{m-1}, and

(ii) $f_1^{m-1} - f_m \in I_{m-1} + P_m$.

By induction hypothesis, (i) is equivalent to

$$(f_1^{i-1} + J_i, f_i + P_{i-1}S) \in \mathrm{im}(\psi_i) \quad \text{for all} \quad i = 2, \dots, m-1$$

and thus, by Eq. (4:12), equivalent to

$$(f_1^{i-1} + I_i, f_i + P_{i-1}) \in \mathrm{im}(\phi_i) \quad \text{for all} \quad i = 2, \dots, m-1$$

where $f_1^{i-1} + I_{i-1} = \phi_{i-1}^{-1}(f_1 + P_1, \dots, f_{i-1} + P_{i-1}) \in R/I_{i-1}$. By Corollary B.4.42, we have that (ii) is equivalent to $(f_1^{m-1} + I_{m-1}, f_m + P_m) \in \mathrm{im}(\phi_m)$ which thus finally provides the assertion for the case m and thus finishes the proof. □

One wishes to extend the above insights into how to find preimages under the R-module homomorphism $M \to \prod_{P \in \mathrm{Ass}_R(R)} M/PM$ for suitable R-modules M. That is, can we replace R by M and R/I by M/IM in the above analysis? The answer in general is no. But if we consider M to be finite and torsion-free over R and R to be reduced and noetherian, then we can extend the above theory to such modules.

Lemma B.4.46. *Let R be a reduced noetherian ring with minimal prime ideals $P_1, \dots, P_m$. Let $I = \bigcap_{i \in A} P_i$ and $J = \bigcap_{j \in B} P_j$ for $A, B \subseteq \{1, \dots, m\}$ such that $A \cup B = \{1, \dots, m\}$. Let M be a finite, torsion-free R-module. Then the sequence of R-modules*

$$0 \longrightarrow M \xrightarrow{\phi} M/IM \oplus M/JM \xrightarrow{\psi} M/(IM + JM) \longrightarrow 0$$

with $\phi(m) = (m + IM, m + JM)$ and $\psi(m + IM, m' + JM) = m - m' + (IM + JM)$ is exact.

Proof. In general, we have

$$\left(\bigcap_{i \in A} P_i \right) M = \left\{ \sum_{j=1}^{m} a_j m_j \mid m_j \in M, a_j \in \bigcap_{i \in A} P_i, m \in \mathbb{N} \right\}.$$

Let $\sum_{j=1}^m a_j m_j \in (\bigcap_{i \in A} P_i)M$. Then $a_j \in P_i$ for all $i \in A$ and thus $a_j m_j \in \bigcap_{i \in A} P_i M$. Therefore

$$IM = \left(\bigcap_{i \in A} P_i \right) M \subseteq \bigcap_{i \in A} P_i M.$$

The kernel of ϕ is obviously $\ker(\phi) = IM \cap JM$. Therefore,

$$IM \cap JM \subseteq \bigcap_{i \in A \cup B} P_i M = \bigcap_{i=1}^{m} P_i M$$

and the latter is the zero submodule of M by Lemma B.4.23 and Corollary B.4.39. The kernel of ψ is

$$\ker(\psi) = \{(m + IM, n + JM) \mid m, n \in M, m - n \in IM + JM\}.$$

Let $(m + IM, n + JM) \in \ker(\psi)$. Then there are $a \in IM$ and $b \in JM$ such that $m + a = n + b$ in M. Hence

$$(m + IM, n + JM) = (m + a + IM, n + b + JM) = (m + a + IM, m + a + JM) = \phi(m + a)$$

and thus $\ker(\psi) \subseteq \mathrm{im}(\phi)$. Conversely, any $\phi(m) = (m + IM, m + JM)$ trivially satisfies $m - m = 0 \in \ker(\psi)$. The surjectivity of ψ is evident. □

Corollary B.4.47. *Let R be a reduced noetherian ring with finitely many minimal prime ideals $P_1, \dots, P_m$ and we set $I_i = \bigcap_{j=1}^{i} P_j$. Let M be an R-ideal. Then for all $i = 2, \dots, m$ the sequence of R-modules*

$$0 \longrightarrow M/I_iM \xrightarrow{\phi_i} M/I_{i-1}M \oplus M/P_iM \xrightarrow{\psi_i} M/(I_{i-1}M + P_iM) \longrightarrow 0$$

with $\phi_i(m + I_iM) = (m + I_{i-1}M, m + P_iM)$ and $\psi_i(m + I_{i-1}M, n + P_iM) = m - n + (I_{i-1}M + P_iM)$ is exact.

Proof. We use Lemma B.4.46 successively starting with $A = \{1, \dots, m-1\}$ and $B = \{m\}$. This provides the exact sequence

$$0 \longrightarrow M = M/I_mM \xrightarrow{\phi_m} M/I_{m-1}M \oplus M/P_mM \xrightarrow{\psi_m} M/(I_{m-1}M + P_mM) \longrightarrow 0.$$

By Lemma C.1.8, we know that the restriction $M/I_{m-1}M$ of the R-ideal M to R/I_{m-1} as defined in Definition C.1.9 is isomorphic to an R/I-ideal. This implies that we can apply Lemma B.4.46 again to $M/I_{m-1}M$ and thus the assertion follows by induction on the number m of minimal prime ideals of R. □

Lemma B.4.48. *Let R be a local ring containing a field k and whose maximal ideal is $\mathfrak{m}$. Let M be an R-module. Then $\operatorname{len}_R(M) \cdot \dim_k R/\mathfrak{m} = \dim_k(M)$.*

Proof. We prove the assertion by induction on the length of M over R. By [Sta18, Tag 00J2], we have that $\operatorname{len}_R(M) = 1$ if and only if $M \cong R/\mathfrak{m}$ as R-modules. Hence the assertion is true for $\operatorname{len}_R(M) = 1$. Now let the assertion be true for all modules of length n. Let M be any R-module of length $n+1$ and let

$$0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n \subsetneq M_{n+1} = M$$

be a composition series for M. Consider the short exact sequence

$$0 \longrightarrow M_n \longrightarrow M_{n+1} \longrightarrow M_{n+1}/M_n \longrightarrow 0. \tag{4:14}$$

Since the length is additive in short exact sequences, see [Sta18, Tag 00IV], we have

$$\operatorname{len}_R(M_{n+1}) = \operatorname{len}_R(M_n) + \operatorname{len}_R(M_{n+1}/M_n).$$

By definition, the quotient M_{n+1}/M_n is a simple R-module. Hence it has length one and now the induction hypothesis provides

$$\begin{aligned} \operatorname{len}_R(M_{n+1}) &= \frac{\dim_k(M_n)}{\dim_k R/\mathfrak{m}} + 1 \\ &= \frac{\dim_k(M_n)}{\dim_k R/\mathfrak{m}} + \frac{\dim_k R/\mathfrak{m}}{\dim_k R/\mathfrak{m}} \end{aligned}$$

and hence $\operatorname{len}_R(M_{n+1}) \cdot \dim_k R/\mathfrak{m} = \dim_k R/\mathfrak{m} + \dim_k(M_n)$. The exact sequence in (4:14) considered as a sequence of k-vector spaces splits and thus provides

$$\dim_k R/\mathfrak{m} + \dim_k(M_n) = \dim_k M_{n+1}$$

which completes the proof. □

Lemma B.4.49. *Let $(R, \mathfrak{m}, \kappa)$ be a local reduced k-algebra of dimension one where k is a field. Assume R to have finitely many minimal prime ideals $P_1, \dots, P_m$. Then for any*

regular element $a \in R$ we have

$$\dim_k R/aR = \sum_{i=1}^{m} \dim_k R/(aR + P_i).$$

Proof. The proof relies on the equality

$$\operatorname{len}_R(R/aR) = \sum_{i=1}^{m} \operatorname{len}_{R_{P_i}}(R_{P_i}) \cdot \operatorname{len}_{R/P_i}(R/aR + P_i) \tag{4:15}$$

which is proved for R in the proof of [Liu02, 7.5.7]. Note that since R is reduced, by Lemma B.4.29, we obtain that R_{P_i} is a field and thus $\operatorname{len}_{R_{P_i}}(R_{P_i}) = 1$. Moreover, by Lemma B.4.48, we obtain $\operatorname{len}_R(R/aR) = \dim_k R/aR \cdot (\dim_k \kappa)^{-1}$ and analogously

$$\begin{aligned}
\operatorname{len}_{R/P_i}(R/aR + P_i) &= \dim_k R/aR + P_i \cdot (\dim_k(R/P_i)/(\mathfrak{m}/P_i))^{-1} \\
&= \dim_k R/aR + P_i \cdot (\dim_k R/\mathfrak{m})^{-1} \\
&= \dim_k R/aR + P_i \cdot (\dim_k \kappa)^{-1}.
\end{aligned}$$

Plugging this into Eq. (4:15) provides the assertion. □

Lemma B.4.50. *Let R be a ring and let M be a finite R-module. Then for any two ideals $I, J \subseteq R$ of R we have $IM + JM = (I + J)M$.*

Proof. Let $m_1, \ldots, m_n$ be a generating set of M over R. Every element of the submodule IM of M has the form $\sum_{i=1}^{n} a_i m_i$ with $a_i \in I$. We have

$$IM + JM = \{a + b \mid a \in IM, b \in JM\}$$

and thus

$$\begin{aligned}
IM + JM &= \left\{ \sum_{i=1}^{n} a_i m_i + \sum_{i=1}^{n} b_i m_i \mid a_i \in I, b_i \in J \right\} \\
&= \left\{ \sum_{i=1}^{n} (a_i + b_i) m_i \mid a_i \in I, b_i \in J \right\} \\
&= \left\{ \sum_{i=1}^{n} c_i m_i \mid c_i \in I + J \right\} \\
&= (I + J)M.
\end{aligned}$$

□

B.5 Algebraic Geometry

Recall that a topological space is called **Kolmogorov** if for any two distinct points $x, x' \in X$, $x \neq x'$, there is a closed subset of X that contains exactly one of the two points. Since singletons $\{x\} \subseteq X$ of a topological space X are irreducible and the closure of irreducible sets is irreducible, $\overline{\{x\}}$ is a closed and irreducible subset of X. Therefore, if X is Kolmogorov, then any two distinct points have distinct closures. Furthermore, recall that a topological space X is called **sober** if every irreducible and closed subset of X has a unique generic point. Thus, by definition, a topological space X is Kolmogorov respectively sober if and only if the map

$$\begin{array}{ccc} X & \to & \{Y \mid Y \subseteq X \text{ closed and irreducible}\} \\ x & \mapsto & \overline{\{x\}} \end{array} \tag{5:16}$$

is injective respectively bijective. In particular, sober topological spaces are Kolmogorov. By [Sta18, Tag 01IS], a scheme is sober and thus Kolmogorov.

Lemma B.5.1. *Let X be non-empty, noetherian and irreducible topological space which is sober. Then X has a unique generic point ξ with $\overline{\{\xi\}} = X$. Furthermore, any proper closed subset $Y \subsetneq X$ does not contain ξ and any non-empty open subset $U \subseteq X$ contains ξ. If X is moreover of dimension one, then any point $x \in X$ with $x \neq \xi$ is a closed point. In particular, any finite set $Y \subseteq X$ which does not contain ξ is closed in X.*

Proof. Since X is sober, X has a unique generic point $\xi \in X$ and thus X is the smallest closed subset of X that contains ξ. Hence every proper closed subset $Y \subsetneq X$ can not contain ξ. Now if $U \subseteq X$ is a non-empty open in X, then its complement is a proper closed subset of X and thus it cannot contain ξ and hence $\xi \in U$.

Now assume X to be of dimension one. Since every noetherian space is quasi-compact, see [Sta18, Tag 04ZA], we deduce that X has a closed point, see [Sta18, Tag 005E]. Let $y \in X$ be distinct to ξ and set $Y = \overline{\{y\}}$. Since $\{y\}$ is irreducible, its closure $Y = \overline{\{y\}}$ is irreducible, see [Sta18, Tag 004W]. Since $y \neq \xi$, the injectivity of the map in (5:16) provides $Y \subsetneq X$. Thus, by [Liu02, 2.5.5], we deduce $\dim(Y) = 0$. Hence Y is a zero-dimensional, noetherian and irreducible topological space which is Kolmogorov. Hence there are no proper irreducible closed subsets of Y and thus $\overline{\{x\}} = Y$ for every $x \in Y$ and thus, by sobriety of Y, we deduce that $x = y$ for all $x \in Y$ and thus $Y = \{y\}$ is closed.

In particular, every set $Y \subseteq X$ not containing ξ only contains closed points and is thus closed itself if it is finite. □

Proposition B.5.2. *Let X be a noetherian and irreducible scheme of dimension at most one. Then any proper closed subset of X is finite.*

Proof. If X has dimension zero, every of its irreducible components has dimension zero as well. But irreducible schemes of dimension zero are singletons. Since X is noetherian, it has only finitely many irreducible components, see [Sta18, Tag 0BA8], and thus X itself is finite. Let us consider the case that X has dimension one. Since X is noetherian, it is quasi-compact, see [Sta18, Tag 04ZA]. Therefore, we can cover it by finitely many affine open subsets. Thus it suffices to prove the assertion for X being affine. So let $X = \operatorname{Spec}(R)$ such that R is a noetherian of dimension one with unique minimal prime ideal P_0. Now any proper closed subset $V(I)$, with $P_0 \subsetneq I \subsetneq R$ being an ideal of R, has only finitely many irreducible components, see [Sta18, Tag 0BA8]. Any such component corresponds to a prime ideal $P \supseteq I \supsetneq P_0$ which is thus maximal since R is of dimension one. Therefore, $V(I)$ is the finite union of its components which are all closed points by the above. Hence $V(I)$ itself is finite. □

Lemma B.5.3. *Let X be a noetherian scheme of dimension one and $X_1, \dots, X_m$ finitely many distinct closed irreducible subschemes of X. For all $i, j \in \{1, \dots, m\}$, $i \neq j$, the number $\#X_i \cap X_j$ of intersection points is finite. In particular, the total number of points lying in at least two of the subschemes is also finite.*

Proof. The intersection $X_i \cap X_j$ is closed in both X_i and X_j. Since X is one-dimensional, the subschemes X_i are at most one-dimensional. By assumption, $X_i \neq X_j$ for all $i \neq j$ and hence $X_i \cap X_j$ is a proper closed subset of a noetherian and irreducible scheme of dimension at most one. Therefore, Proposition B.5.2 provides the assertion. □

Lemma B.5.4. *Let M be an R-module and let $P \subseteq Q$ be two prime ideals of R. If $M_Q = 0$, then $M_P = 0$ as well. In particular, if $M_P \neq 0$, then $M_Q \neq 0$ for all $Q \supseteq P$.*

Proof. Since $P \subseteq Q$, we have $R \setminus Q \subseteq R \setminus P$. By definition, every element of M_Q can be written as m/r with $m \in M$ and $r \in R \setminus Q$. Moreover, $m/r = 0$ in M_Q if and only if there is some $s \in R \setminus Q$ such that $sm = 0$ in M. Assume $M_Q = 0$, then by the above, for all $m \in M$ there is $s \in R \setminus Q$ such that $sm = 0$. Let $m/r \in M_P$ with $r \in R \setminus P$ arbitrary be an arbitrary element of M_P. By assumption, there is $s \in R \setminus Q \subseteq R \setminus P$ such that $sm = 0$ and thus m/r is zero in M_P. Therefore, $M_Q = 0$ implies $M_P = 0$. In particular, $M_P \neq 0$ implies $M_Q \neq 0$. □

Corollary B.5.5. *Let X be a non-empty noetherian scheme and let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. If $\mathcal{F}_\xi \neq 0$ for some generic point of an irreducible component Z of X, then $Z \subseteq \operatorname{Supp}(\mathcal{F})$.*

Proof. Since the statement is of local nature, we may assume that $X = \operatorname{Spec}(R)$ is affine and since $\mathcal{F}$ is quasi-coherent, we have $\mathcal{F} = M^\sim$ for some R-module M. Then the statement follows from Lemma B.5.4. □

Lemma B.5.6. *Let X be a reduced scheme with irreducible components $X_1, \dots, X_m$. Then for any schematically dense open subset $U \subseteq X$ the ring monomorphism $\mathcal{O}_X(U) \hookrightarrow \bigoplus_{i=1}^m \mathcal{O}_{X_i}(U \cap X_i)$ extends to an isomorphism*

$$\operatorname{Frac}(\mathcal{O}_X(U)) \longrightarrow \bigoplus_{i=1}^m \operatorname{Frac}(\mathcal{O}_{X_i}(U \cap X_i)).$$

Proof. This follows from [Liu02, 7.5.2]. □

Lemma B.5.7. *Let X either be a projective scheme over an affine base or itself an affine scheme. Then for every open cover $\mathcal{U} = \{U_i \mid i \in I\}$ of X, there is an affine open cover $\mathcal{V} = \{V_j \mid j \in J\}$ which is a refinement of $\mathcal{U}$, that is, for all $j \in J$ there is some $i \in I$ such that $V_j \subseteq U_i$.*

Proof. In both cases, X being projective over an affine base or itself being affine, for every inclusion $\{P\} \subseteq U_i \subseteq X$ with $P \in X$ and open subset $U_i \subseteq X$ we find, due to Corollary D.1.4 and Corollary D.1.3, an affine open subset $V_{i,P}$ such that $\{P\} \subseteq V_{i,P} \subseteq U_i$. Obviously, the $V_{i,P}$ for $P \in U_i$ cover U_i. Thus $\mathcal{V} = \{V_{i,P} \mid i \in I, P \in U_i\}$ is an affine open cover of X which is a refinement of $\mathcal{U}$ as asserted. □

Remark B.5.8. Let the situation be as in Proposition 3.2.3. Then $\mathcal{O}_Y(f^*D) \cong f^*\mathcal{O}_X(D)$. We give the proof for the general Y and X as indicated in the proof of Proposition 3.2.3:

Consider $D \in \operatorname{Div}(X)$ given by a configuration $\{U_i, b_i/a_i\}_{i \in I}$ with $a_i, b_i \in \mathcal{O}_X(U_i)$. We have $\mathcal{O}_X(D)_{|U_i} = (a_i/b_i)\mathcal{O}_{U_i}$. Now fix some U_i along with its open immersion $j : U_i \to X$ for which then $j^*\mathcal{O}_X(D) = \mathcal{O}_X(D)_{|U_i}$ holds. Then set $V_i = f^{-1}(U_i)$ along with its open immersion $h : V_i \to Y$. Then, by construction, $f \circ h = j \circ f_{|V}$ and hence $(f \circ h)^*\mathcal{O}_X(D) = (j \circ f_{|V_i})^*\mathcal{O}_X(D)$. Since the pullback along the composition of morphisms is the reversed composition of pullbacks, we obtain

$$h^*(f^*(\mathcal{O}_X(D))) = (f \circ h)^*\mathcal{O}_X(D) = (j \circ f_{|V_i})^*\mathcal{O}_X(D) = f_{|V_i}^*(j^*\mathcal{O}_X(D)) = f_{|V_i}^*\mathcal{O}_X(D)_{|U_i}.$$

As above, we have $h^*(f^*(\mathcal{O}_X(D))) = f^*(\mathcal{O}_X(D))_{|V_i}$ and thus

$$f^*(\mathcal{O}_X(D))_{|V_i} = f_{|V_i}^*\mathcal{O}_X(D)_{|U_i} = f_{|V_i}^*(a_i/b_i)\mathcal{O}_{U_i}.$$

By definition of the pullback of sheaves of $\mathcal{O}_X$-modules along $f_{|V_i}$, we have

$$f_{|V_i}^*(a_i/b_i)\mathcal{O}_{U_i} = \mathcal{O}_{V_i} \otimes_{f_{|V_i}^{-1}\mathcal{O}_{U_i}} f_{|V_i}^{-1}(a_i/b_i)\mathcal{O}_{U_i}$$

where the tensor product is defined over $f_{|V_i}^{-1}\mathcal{O}_{U_i}$ and $\mathcal{O}_{V_i}$ is an $f_{|V_i}^{-1}\mathcal{O}_{U_i}$-module via the pullback morphism $f_{|V_i}^{\#} : f_{|V_i}^{-1}\mathcal{K}_{U_i} \to \mathcal{K}_{V_i}$ (being the extension of $f_{|V_i}^{\#} : f_{|V_i}^{-1}\mathcal{O}_{U_i} \to \mathcal{O}_{V_i}$) which itself is the restriction of the pullback morphism $f^{\#} : f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$. Now we are pretty much done since now *locally* the generator a_i/b_i can be pulled to the other factor of the tensor product using the morphism $f_{|V_i}^{\#} : f_{|V_i}^{-1}\mathcal{K}_{U_i} \to \mathcal{K}_{V_i}$ over which the tensor product is defined. The rest of the proof is the technical elaboration of the above idea.

By Lemma B.1.40, we have $\mathcal{F}^{\#} \otimes_{\mathcal{O}^{\#}} \mathcal{G}^{\#} \cong (\mathcal{F} \otimes_{\mathcal{O}}^{p} \mathcal{G})^{\#}$ where $\mathcal{O}$ is a sheaf of rings on X, $\mathcal{F}, \mathcal{G}$ are presheaves of $\mathcal{O}$-modules on X and $\otimes_{\mathcal{O}}^{p}$ denotes the presheaf tensor product as defined in Definition B.1.39. Applying this we obtain

$$\begin{aligned}\mathcal{O}_{V_i} \otimes_{f_{|V_i}^{-1}\mathcal{O}_{U_i}} f_{|V_i}^{-1}(a_i/b_i)\mathcal{O}_{U_i} &\cong \mathcal{O}_{V_i}^{\#} \otimes_{(f_{|V_i}^{-1,p}\mathcal{O}_{U_i})^{\#}} (f_{|V_i}^{-1,p}(a_i/b_i)\mathcal{O}_{U_i})^{\#} \\ &\cong (\mathcal{O}_{V_i} \otimes_{f_{|V_i}^{-1,p}\mathcal{O}_{U_i}}^{p} f_{|V_i}^{-1,p}(a_i/b_i)\mathcal{O}_{U_i})^{\#}\end{aligned}$$

where $f_{|V_i}^{-1,p}\mathcal{F}$ denotes the presheaf defined by $V \mapsto \varinjlim_{f_{|V_i}(V)\subseteq U} \mathcal{F}(U)$ whose sheafification is $f_{|V_i}^{-1}\mathcal{F}$. Now we can apply that the tensor product commutes with direct limits, that is, for $(A_i)_{i\in I}$ a direct system of rings and $(M_i)_{i\in I}$ as well as $(N_i)_{i\in I}$ direct systems of A_i-modules, we have

$$\varinjlim_{i\in I} M_i \otimes_{\varinjlim_{i\in I} A_i} \varinjlim_{i\in I} N_i \cong \varinjlim_{i\in I}(M_i \otimes_{A_i} N_i).$$

This provides an isomorphism of presheaves on V_i

$$\mathcal{O}_{V_i} \otimes_{f_{|V_i}^{-1,p}\mathcal{O}_{U_i}}^{p} f_{|V_i}^{-1,p}(a_i/b_i)\mathcal{O}_{U_i} \longrightarrow \left(V \mapsto \varinjlim_{U:\ f_{|V_i}(V)\subseteq U\subseteq U_i} \mathcal{O}_{V_i}(V) \otimes_{\mathcal{O}_X(U)} (a_i/b_i)_{|U}\mathcal{O}_X(U))\right)$$

where the tensor product on the right hand side is defined via the ring homomorphism $f_{|V_i}^{\#}(V) : \mathcal{K}_{U_i}(U) \to \mathcal{K}_{V_i}(V)$. Hence

$$\mathcal{O}_{V_i}(V) \otimes_{\mathcal{O}_X(U)} (a_i/b_i)_{|U}\mathcal{O}_X(U)) \cong f_{|V_i}^{\#}(V)(a_i/b_i)\mathcal{O}_{V_i}(V)$$

and therefore

$$\mathcal{O}_{V_i} \otimes_{f_{|V_i}^{-1,p}\mathcal{O}_{U_i}}^{p} f_{|V_i}^{-1,p}(a_i/b_i)\mathcal{O}_{U_i} \cong \left(V \mapsto \varinjlim_{U:\ f_{|V_i}(V)\subseteq U\subseteq U_i} f_{|V_i}^{\#}(V)((a_i/b_i)_{|U})\mathcal{O}_{V_i}(V)\right)$$

as presheaves. We easily see that the sheafification of the latter is the sheaf $f_{|V_i}^{\#}(V_i)(a_i/b_i)\mathcal{O}_{V_i}$ and thus isomorphic to the sheafification of the former, which is $f^*(\mathcal{O}_X(D))_{|V_i}$. Therefore

$$f^*(\mathcal{O}_X(D))_{|V_i} \cong f_{|V_i}^{\#}(V_i)(a_i/b_i)\mathcal{O}_{V_i} = \frac{f_{|V_i}^{\#}(V_i)(a_i)}{f_{|V_i}^{\#}(V_i)(b_i)}\mathcal{O}_{V_i} = \frac{f^{\#}(V_i)(a_i)}{f^{\#}(V_i)(g_i)}\mathcal{O}_{V_i}$$

as asserted. △

Lemma B.5.9 (Projection Formula, [Sta18], Tag 01E8)**.** *Let $f : X \to Y$ be a morphism of locally ringed spaces. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Let $\mathcal{G}$ be a finite locally free $\mathcal{O}_Y$-module. Then there are isomorphisms for all $r \geq 0$:*

$$\mathcal{G} \otimes_{\mathcal{O}_Y} R^r f_*\mathcal{F} \longrightarrow R^r f_*(\mathcal{F} \otimes_{\mathcal{O}_X} f^*\mathcal{G})$$

In particular, $\mathcal{G} \otimes_{\mathcal{O}_Y} f_*\mathcal{F} \longrightarrow f_*(\mathcal{F} \otimes_{\mathcal{O}_X} f^*\mathcal{G})$.

Theorem B.5.10 ([GW10], 11.51)**.** *Let* $\mathcal{F}$ *be a locally free sheaf of rank* r *on* $\mathbb{P}^1_k$*. Then there are uniquely determined integers* $d_1 \geq \ldots \geq d_r$ *such that* $\mathcal{F} = \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(d_i)$.

Lemma B.5.11. *Let* $\lambda \in \mathbb{Z}$*. Then we have*

$$\dim_k H^0\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(\ell)\right) = \begin{cases} 0, & \ell < 0 \\ \ell + 1, & \ell \geq 0 \end{cases}, \quad \dim_k H^1\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(\ell)\right) = \begin{cases} -\ell - 1, & \ell < 0 \\ 0, & \ell \geq 0. \end{cases} \tag{5:17}$$

Proof. This is the combination of [BPoMSS02, Lemmas 6.2, 6.7, 6.8, 6.9]. □

Lemma B.5.12 ([GW10], 12.37)**.** *Let* $f : X \to Y$ *be an affine morphism of schemes and let* $\mathcal{F}$ *be a quasi-coherent sheaf on* X*. Then* $H^1(Y, f_*\mathcal{F}) \cong H^1(X, \mathcal{F})$.

Definition B.5.13. Let k be a field. Let X be a proper scheme over k. Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module. The **Euler-Poincaré characteristic of** $\mathcal{F}$ **over** k or shorter the **Euler characteristic of** $\mathcal{F}$ **over** k is defined as the integer

$$\chi_k(X, \mathcal{F}) = \sum_{i \geq 0} \dim_k H^i(X, \mathcal{F}).$$

Sometimes if k and X is known from the context, we may write $\chi(\mathcal{F})$ instead of $\chi_k(X, \mathcal{F})$. △

Lemma B.5.14 ([Sta18], Tag 08AA)**.** *Let* k *be a field. Let* X *be a proper scheme over* k*. Let* $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ *be a short exact sequence of coherent* $\mathcal{O}_X$*-modules. Then*

$$\chi_k(X, \mathcal{F}_2) = \chi_k(X, \mathcal{F}_1) + \chi_k(X, \mathcal{F}_3).$$

Lemma B.5.15 ([Sta18], Tag 0AYT)**.** *Let* k *be a field. Let* X *be a proper scheme over* k*. Let* $\mathcal{F}$ *be a coherent sheaf with* $\dim(\mathit{Supp}(\mathcal{F})) \leq 0$*. Then*

(i) $\mathcal{F}$ *is generated by global sections,*

(ii) $H^i(X, \mathcal{F}) = 0$ *for* $i > 0$*,*

(iii) $\chi(X, \mathcal{F}) = \dim_k \Gamma(X, \mathcal{F})$*, and*

(iv) $\chi(X, \mathcal{F} \otimes \mathcal{E}) = n\chi(X, \mathcal{F})$ *for every locally free module* $\mathcal{E}$ *of rank* n*.*

Lemma B.5.16. *Let* $f : Y \to X$ *together with* $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ *be an affine morphism of schemes for which the restriction of divisors is defined (see Definition 3.2.5). Let* $\mathcal{H} = h\mathcal{O}_X$ *with* $h \in \mathcal{K}_X(X)^\times$ *be an* $\mathcal{O}_X$*-ideal. Then* $f^*\mathcal{H} = f^\#(X)(h)\mathcal{O}_Y$.

Proof. First of all, by Remark 3.2.1, we have a pullback map of regular functions $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$. By assumption on f, $\mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$ and, by [GW10, 2.27], we obtain that this datum is equivalent to $f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$. Here the latter indeed is the extension of $f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ and hence, by a bit more abuse of notation, we denote $f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$ also by $f^\#$.

By assumption on f, any affine open cover $X = \cup_{i \in I} U_i$ of X provides an affine open cover $Y = \cup_{i \in I} V_i$ of Y with $V_i = f^{-1}(U_i)$. Then, by definition, we have $(f^{-1}_{|V_i}\mathcal{F})(V_i) = \mathcal{F}(U_i)$. By [Liu02, 5.1.12], we have

$$\begin{aligned} (f^*\mathcal{F})(V_i) &= (\mathcal{O}_Y \otimes_{f^{-1}\mathcal{O}_X} f^{-1}\mathcal{F})(V_i) \\ &= (\mathcal{O}_Y(V_i) \otimes_{(f^{-1}\mathcal{O}_X)(V_i)} (f^{-1}\mathcal{F})(V_i) \\ &= \mathcal{O}_Y(V_i) \otimes_{\mathcal{O}_X(U_i)} \mathcal{F}(U_i) \\ &= \mathcal{O}_Y(V_i) \otimes_{\mathcal{O}_X(U_i)} h_{|U_i}\mathcal{O}_X(U_i). \end{aligned}$$

The tensor product is defined via the morphism $f^{\#} : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ which extends to $f^{\#} : f^{-1}\mathcal{K}_X \to \mathcal{K}_Y$. Hence

$$\begin{aligned}(f^*\mathcal{F})(V_i) = f^{\#}(V_i)(h_{|U_i})\mathcal{O}_Y(V_i) \otimes_{\mathcal{O}_X(U_i)} \mathcal{O}_X(U_i) &= f^{\#}(V_i)(h_{|U_i})\mathcal{O}_Y(V_i) \\ &= f^{\#}(X)(h)_{|V_i}\mathcal{O}_Y(V_i)\end{aligned}$$

and thus $(f^*\mathcal{F})_{|V_i} = f^{\#}(X)(h)_{|V_i}\mathcal{O}_{V_i} = (f^{\#}(X)(h)\mathcal{O}_Y)_{|V_i}$. That is, $f^*\mathcal{F}$ as an $\mathcal{O}_Y$-subsheaf of $\mathcal{K}_Y$ is equal to the sheaf $f^{\#}(X)(h)\mathcal{O}_Y$, see Corollary B.1.30. □

Lemma B.5.17. *Let X be a noetherian scheme. Then for every point $x \in X$ and affine open neighborhood U of x there is some non-zero-divisor $g \in \mathcal{O}_X(U)$ such that $x \in D_U(g)$.*

Proof. Since X is noetherian, it has finitely many irreducible components, say $X_1, \dots, X_m$ with unique generic points $\xi_1, \dots, \xi_m$, respectively. Set $E = \{x, \xi_1, \dots, \xi_m\}$. Since X is noetherian, it is quasi-compact and quasi-separated and thus we can apply Lemma D.1.2 to $E \subseteq W = U$ and $\mathcal{L} = \mathcal{O}_U$ and obtain $s \in \mathcal{O}_X(U)$ such that $E \subseteq X_s \subseteq U$. Since X_s contains E, s_{ξ_i} is non-zero for all $i = 1, \dots, m$ and thus no zero-divisor in $\mathcal{O}_X(U)$. Furthermore, we have $x \in D_U(s)$. □

Lemma B.5.18. *Let X be a proper scheme over a field k. If $\dim(X) \leq 1$, then X is projective over k.*

Proof. This is [Sta18, Tag 0A26] which says that X is H-projective and then we use [Sta18, Tag 0B45] which states the equivalence of being projective and H-projective for schemes over some field. □

Corollary B.5.19. *Let X be a scheme over a field k with $\dim(X) \leq 1$. Then X is projective if and only if X is proper.*

Proof. The only if part is [Liu02, 3.3.30] and the if part is B.5.18. □

Lemma B.5.20. *Let $\phi : A' \to A$ be a homomorphism of rings such that $\dim(A') = \dim(A)$. Let A' be an integral domain and let the corresponding morphism of affine schemes be finite. Then $\phi : A' \to A$ is injective.*

Proof. This follows from [DG67, I. 1.2.7]. □

Lemma B.5.21 ([KM98], 5.4)**.** *Let $f : X \to Y$ be a finite morphism of one-dimensional schemes. Let $\mathcal{F}$ be a coherent sheaf on X with $\operatorname{Supp}(\mathcal{F}) = X$. Then $f_*\mathcal{F}$ is S_1 if and only if $\mathcal{F}$ is S_1.*

Appendix C

Properties of R-Ideals and $\mathcal{O}_X$-Ideals

In this chapter we introduce the local respectively affine variants of $\mathcal{O}_X$-ideals, the so called R-ideals where R is the respective affine coordinate ring. Analogously to $\mathcal{O}_X$-ideals being a kind of generalisation of sheaves of ideals, R-ideals will be a kind of generalisation of ordinary ideals of the ring R (which do not solely consists of zero-divisors from R). To be precise, R-ideals will be fractional ideals of R that are invertible at the minimal prime ideals of R. We will define the degree of R-ideals and then use it to define the degree of divisors and the degree of $\mathcal{O}_X$-ideals. To properly define the degree of divisors, we have seen in Definition 3.1.10 that we need to work on a scheme that has dimension at most one. Therefore, we will introduce R-ideals for rings R of Krull dimension at most one. Moreover, we assume R to be an algebra over a field k since we will define the degree of R-ideals as the finite dimension of a quotient vector space over k. Frankly speaking, the theory behind R-ideals does form some of the important basis of working with divisors and $\mathcal{O}_X$-ideals.

The chapter is organised as follows: In Section C.1 we will define R-ideals and their degree. We will show that there are useful notions of restricting R-ideals to irreducible components of $\operatorname{Spec}(R)$, of how R-ideals may be localised and of the quotient of R-ideals. We will see that the degree of R-ideals satisfies useful properties. For instance, it may be computed locally, it behaves additively for products of R-ideals if one of the factors is invertible and the degree of an invertible R-ideal can be computed as the sum of the degrees of its restrictions to irreducible components of R.

In Section C.2 we provide a statement that characterises the image of the natural map $M \to \bigoplus_{i=1}^m M/P_iM$ where M is an R-ideal and $P_1, \dots, P_m$ denote the minimal prime ideals of R. This will be used in Section 5.7.1 to prove the existence of modification functions in a geometric fashion.

In Section C.3 we collect a few general properties of $\mathcal{O}_X$-ideals that are not concerned with their degree. For instance, we show that quotients of $\mathcal{O}_X$-ideals have finite support which can be used to apply the Approximation Theorem 5.7.1 in Section 5.7.1.

Finally, in Section C.4 we define the degree of $\mathcal{O}_X$-ideals and examine its properties. Since the degree of R-ideals could be computed locally, we define the degree of $\mathcal{O}_X$-ideals locally an then show that it can also be computed globally using the Euler characteristic of the respective $\mathcal{O}_X$-ideal. We will show that the degree of $\mathcal{O}_X$-ideals naturally inherits basically all of the properties of the degree of R-ideals. At the end of Section C.4 we translate the most important properties of the degree of $\mathcal{O}_X$-ideals to the degree of divisors.

C.1 Degree of R-Ideals over k

In this section k denotes a field and R a noetherian ring of Krull dimension one which is a finite residual-type k-algebra, see Definition B.4.3. A common example of such rings are the rings of regular functions $\mathcal{O}_X(U)$ for X a curve of finite residual-type over k and $U \subseteq X$ some open subset.

Remark C.1.1. Let X be a cover of $\mathbb{P}^1_k$. Then, by Lemma 2.2.20, the affine coordinate ring $R \in \{R_0, R_\infty, \mathcal{O}_S\}$ of V_0, V_∞ respectively S satisfies the above properties. Moreover, R is also Cohen-Macaulay. △

Definition C.1.2. Let M be a finitely generated R-submodule of $\mathrm{Frac}(R)$. We call M an **R-ideal** if it is invertible at the minimal primes of R. △

Example C.1.3. Let $I \subseteq \mathrm{Frac}(R)$ be an invertible ideal of R. Then I is an R-ideal since it is invertible at all primes of R and a fortiori at the minimal ones. △

Note that for an R-ideal M there always is, by taking the common denominator of a generating set, a regular element $f \in R$ such that $fM \subseteq R$.

Lemma C.1.4. *Let M be a finitely generated R-submodule of* $\mathrm{Frac}(R)$. *Then M is invertible at all minimal prime ideals of R if and only if for all regular $f \in R$ such that $fM \subseteq R$ we have R/fM has Krull dimension zero.*

Proof. Assume that M is invertible at all $P \in \mathrm{Spec}(R)^0$. We prove that the ideal $fM \subseteq R$ is not contained in any minimal prime of R. Otherwise, there is some minimal prime $P \in \mathrm{Spec}(R)^0$ such that $fM \subseteq P$ and thus $\lambda(f)M_P \hookrightarrow PR_P$ where $\lambda : R \to R_P$ denotes the localisation homomorphism. Moreover, by assumption, we have an isomorphism $\mu : R_P \to M_P$ which provides an R_P-module monomorphism $\varphi : \lambda(f)R_P \hookrightarrow PR_P$. Since φ is R_P-linear, it maps $\lambda(f)r \mapsto \lambda(f)\varphi(r)$ into PR_P. Since $f \in R$ is regular, by Lemma B.4.13, we have $f \notin P$ and thus $\lambda(f) \notin PR_P$. In particular, φ provides an R_P-module monomorphism $h : R_P \hookrightarrow PR_P$ which is absurd. Indeed, since PR_P only contains zero-divisors, see Corollary B.4.14, the generator $h(1)$ of $h(R_P)$ is a zero-divisor with $b \in R \setminus \{0\}$ such that $b \cdot h(1) = 0$. Hence $h(b) = b \cdot h(1) = 0$ and thus h maps b to zero. Therefore, if M is invertible at the minimal prime ideals of R, then $fM \not\subseteq P$ for all $P \in \mathrm{Spec}(R)^0$. In particular, R/fM has Krull dimension strictly lower than that of R, that is, dimension zero.

Conversely, assume that for all regular $f \in R$ such that $fM \subseteq R$ we have that R/fM has Krull dimension zero. In particular, for every minimal prime ideal $P \in \mathrm{Spec}(R)^0$ we have $fM \not\subseteq P$. Since $f \in R$ is regular, the R-module homomorphism $M \to fM$ given by the multiplication with f is an isomorphism and hence the localised homomorphism $M_P \to \lambda(f)M_P$ stays an isomorphism (due to localisation being exact). Moreover, since fM embeds into R, exactness of localisation provides again that we obtain a commutative diagram

$$\begin{array}{ccccc} M & \longrightarrow & fM & \hookrightarrow & R \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda} \\ M_P & \longrightarrow & \lambda(f)M_P & \hookrightarrow & R_P \end{array}$$

which thus provides that $\lambda(f)M_P$ embeds into R_P. Hence $\lambda(f)M_P$ is an ideal in R_P whose corresponding ideal fM in R is not contained in P and thus satisfies $\lambda(f)M_P \not\subseteq PR_P$. Hence $\lambda(f)M_P = R_P$ and thus M_P is isomorphic to R_P. □

If R does not only contain the field k but is also a finite ring extension of $k[x]$ of degree n for some transcendental x, then any R-ideal will be free of rank n over $k[x]$.

Definition C.1.5. Let R satisfy S_1. Let J, I be two R-ideals. Then the **R-ideal quotient of J by I** is defined as $(J : I) := \{a \in \mathrm{Frac}(R) \mid aI \subseteq J\}$. △

Lemma C.1.6. *Let R satisfy S_1. Let J, I be two R-ideals. Then $(J : I)$ is an R-ideal. Moreover, I is invertible if and only if $I(R : I) = R$. In particular, if I is invertible, then $(J : I) = JI^{-1}$ for all R-ideals J.*

Proof. It is straight forward to prove that $(J : I)$ is an R-submodule of $\mathrm{Frac}(R)$. Since R satisfies S_1, by Proposition C.1.10, we know that being invertible at the minimal primes of R is equivalent to containing a regular element of R. Thus there is some $f \in I$ and $g \in J$ which are regular. In particular, $gI \subseteq JI \subseteq J$ and thus $g \in (J : I)$. Thus we are left to prove that $(J : I)$ is finitely generated as an R-module. We have a natural R-module homomorphism

$$\begin{array}{rcl} \Psi : (J : I) & \to & \mathrm{Hom}_R(I, J) \\ a & \mapsto & \phi_a \end{array}$$

where $\phi_a : I \to J$, $b \mapsto ab$. If $\Psi(a) = \phi_a = 0$, then for all $b \in I$ we have $ab = 0$. But since $f \in I$ regular, we obtain $a = 0$. Hence Ψ is an R-module embedding. Since both I, J are finitely generated and R noetherian, the R-module $\mathrm{Hom}_R(I, J)$ is finitely generated and a fortiori the same is true for $(J : I)$.

By [Eis95, 11.6 (d)], we have that I is invertible if and only if $I(R : I) = R$. By definition, we have $J(R : I) \subseteq (J : I)$. Multiplying with I provides (since I is invertible) $J = J(R : I)I \subseteq (J : I)I \subseteq J$ and thus $(J : I)I = J$. Then multiplying with I^{-1} finally provides $(J : I) = JI^{-1}$ as asserted. □

Basic properties of localisation provide that being an R-ideal carries over to arbitrary localisations of R.

Lemma C.1.7. *Let M be an R-ideal and $S \subseteq R$ a multiplicative subset of R. Then $S^{-1}M$ can be considered as an $S^{-1}R$-ideal.*

Proof. First of all, since $M \subseteq \mathrm{Frac}(R)$ and $\mathrm{Frac}(R) = U^{-1}R$ for U being the set of regular elements of R, we have, by [Sta18, Tag 02C6], that $S^{-1}M \hookrightarrow \bar{S}^{-1}(U^{-1}R) \cong (SU)^{-1}R$. Here $SU = \{su \mid s \in S, u \in U\}$ for two multiplicative subsets S, U of R and $\bar{S}$ denotes the image of S under the localisation map $\lambda_U : R \to U^{-1}R$. By symmetry, we obtain $S^{-1}M \hookrightarrow (SU)^{-1}R \cong \bar{U}^{-1}(S^{-1}R)$ where $\bar{U}$ denotes the image of U under the localisation map $\lambda_S : R \to S^{-1}R$. Since λ_S sends regular elements to regular elements, we have that $\bar{U}$ is contained in the set $V \subseteq S^{-1}R$ of regular elements of $S^{-1}R$. Hence, by further localising, we obtain an embedding $\bar{U}^{-1}(S^{-1}R) \hookrightarrow V^{-1}(S^{-1}R) = \mathrm{Frac}(S^{-1}R)$ which finally yields $S^{-1}M \hookrightarrow \mathrm{Frac}(S^{-1}R)$ as $S^{-1}R$-modules. Hence we may regard $S^{-1}M$ as an $S^{-1}R$-ideal.

By assumption, we have $M_P \cong R_P$ for all $\mathrm{Spec}(R)^0$. The prime ideals $\mathrm{Spec}(S^{-1}R)$ in $S^{-1}R$ are exactly those of the form $S^{-1}P$ for $P \in \mathrm{Spec}(R)$ with $P \cap S = \emptyset$ and $\mathrm{Spec}(S^{-1}R)^0 = \{S^{-1}P \in \mathrm{Spec}(S^{-1}R) \mid P \in \mathrm{Spec}(R)^0\}$. Thus consider the localisation $(S^{-1}M)_{S^{-1}P}$ of $S^{-1}M$ at the minimal prime ideal $S^{-1}P$ of $S^{-1}R$. By [Sta18, Tag 02C6] again, we have $(S^{-1}M)_{S^{-1}P} \cong \lambda_P(S)^{-1}M_P$ where $\lambda_P : R \to R_P$ denotes the localisation homomorphism. Since $S^{-1}P \in \mathrm{Spec}(S^{-1}R)$, we have $P \cap S = \emptyset$ and thus $S \subseteq R \setminus P$ which provides $\lambda_P(S) \subseteq {R_P}^\times$. Moreover, by assumption, we have $M_P \cong R_P$ as R_P-modules for all $P \in \mathrm{Spec}(R)^0$. Hence $(S^{-1}M)_{S^{-1}P} \cong \lambda_P(S)M_P = M_P \cong R_P$ and the latter is isomorphic to $(S^{-1}R)_{S^{-1}P}$ due to [Sta18, Tag 02C6]. □

Lemma C.1.8. *Let M be an R-ideal. Let $P_1, \ldots, P_m$ denote all of the minimal prime ideals of R and set $I = \bigcap_{P \in B}$ for some $B \subseteq \{P_1, \ldots, P_m\}$. Then M/IM is isomorphic to an R/I-ideal.*

Proof. This is a combination of the Lemmas B.4.35 and 4.1.2. □

Definition C.1.9. Let M be an R-ideal. Let $I = \cap_{P\in B} P$ for some $B \subseteq \operatorname{Spec}(R)^0$. Then we define the **restriction of M with regards to** I as M/IM. If $I = P$ for $P \in \operatorname{Spec}(R)^0$, then we call M/PM the **restriction of M to the irreducible component** $\operatorname{Spec}(R/P)$ of $\operatorname{Spec}(R)$. Lemma C.1.8 shows that M/IM is isomorphic to an R/I-ideal. In general, we will identify M/IM with that R/I-ideal. △

Proposition C.1.10. *Let $M \subseteq \operatorname{Frac}(R)$ be a finitely generated R-module. If M contains a regular element, then M is an R-ideal. If R satisfies S_1 and M is an R-ideal, then M contains a regular element.*

Proof. Let M contain the regular element $a \in R$. The finiteness assumption provides a regular $g \in R$ with $ga \in gM \subseteq R$ being regular. In particular, by Corollary B.4.14, we have $ga \notin P$ for every minimal prime ideal P of R. Therefore for any minimal prime P the image of ga in M_P is a unit in R_P. Hence M_P is invertible at P.

Now assume R to satisfy S_1. Let M contain no regular element of R. Then every numerator of M is a zero-divisor and thus, by the finiteness assumption, there is some regular $g \in R$ such that $gM \subseteq R$. Moreover, by [Sta18, Tag 00LD], we have $gM \subseteq \bigcup_{P\in \operatorname{Ass}_R(R)} P$. But since R satisfies S_1, we have $\operatorname{Ass}_R(R) = \operatorname{Spec}(R)^0$. The prime avoidance lemma Lemma B.4.5 now provides that $gM \subseteq P$ for one minimal prime $P \in \operatorname{Spec}(R)^0$. Then $M_P \hookrightarrow gM_P \subseteq PR_P$ and therefore M_P cannot be isomorphic to R_P as an R_P-module since PR_P only contains zero-divisors and thus every R_P-module homomorphism $R_P \to PR_P$ fails to be injective (as in the proof of C.1.4). □

Corollary C.1.11. *Let R satisfy S_1. Then a finitely generated R-submodule of $\operatorname{Frac}(R)$ is an R-ideal if and only if it contains a regular element of R.*

Remark C.1.12. Let M be an R-submodule of $\operatorname{Frac}(R)$, i.e. M is a fractional ideal of R. Then M is torsion-free as an R-module. Indeed, assume $am = 0$ where $a \in R$ and $m \in M$. Write $m = b/c$ with $b, c \in R$. Then $ab/c = 0$ in $\operatorname{Frac}(R)$ which is equivalent to the existence of some regular $d \in R$ such that $abd = 0$. Since d is regular, this yields $ab = 0$ and thus a is a zero-divisor in R. △

Proposition C.1.13. *Let $N \subseteq M$ be two R-ideals. Then $\operatorname{Supp}(M/N)$ is finite.*

Proof. By [Eis95, Cor. 2.7], we have $\operatorname{Supp}(M/N) = V(\operatorname{Ann}(M/N))$. We have $\operatorname{Ann}(M/N) = \{x \in R \mid xM \subseteq N\}$. Moreover, N, $M \subseteq \operatorname{Frac}(A)$ and there is some regular $a \in R$ such that aM, $aN \subseteq R$. Then $xM \subseteq N$ if and only $xaM \subseteq aN$ and hence $\operatorname{Ann}(M/N) \supseteq \operatorname{Ann}(M) \cup aN$. Then

$$\operatorname{Supp}(M/N) \subseteq V(\operatorname{Ann}(M) \cup aN) \subseteq V(aN)$$

and since N is an R-ideal, R/aN is a zero-dimensional noetherian ring, see Lemma C.1.4, and hence artinian, due to [Sta18, Tag 00KH]. Moreover, by [Sta18, Tag 00JB], R/aN is equal to the finite product of its localisation at its maximal ideals. In particular, $V(aN)$ is finite. □

A lot of the analysis that follows can be easily extended to the more general case of **R-vector-bundles of rank r** which we may define analogously to R-ideals as finitely generated R-submodules of $\operatorname{Frac}(R^r) = \operatorname{Frac}(R)^r$ that are free of rank r at the minimal primes of R. These represent the affine respectively local model of generalised vector bundles which are introduced in Section 4.1 and defined in Definition 4.1.1. Analogously to the case of R-ideals, R-vector-bundles will be free over any principal ideal domain A if R is free over A, see Lemma 4.1.8. But similar to our treatment of generalised vector bundles in Section 4.1 and in this thesis in general, we also restrict ourselves in this section to the case of R-vector-bundles of rank 1 which are precisely the R-ideals.

We would like to define a degree of R-ideals over k. For integral R-ideals M we could define the degree of M in terms of the dimension of the k-vector space R/M. We can extend this to the general case by using a "wedging element" $f \in R$ with $fM \subseteq R$.

Definition C.1.14. Let M be an R-ideal and let $f \in R$ be regular with $fM \subseteq R$. We define the **degree of M over k** as

$$\deg_k M = \dim_k R/fM - \dim_k M/fM.$$

In the following we will call such an f a **wedging element of M**. The above definition itself depends on f, but we will show that it is independent of the choice of f. △

Remark C.1.15. In the case that both R and M have finite dimension over k, we can consider the two following exact sequences of k-vector spaces

$$\begin{array}{ccccccccc} 0 & \longrightarrow & fM & \longrightarrow & R & \longrightarrow & R/fM & \longrightarrow & 0 \\ 0 & \longrightarrow & fM & \longrightarrow & M & \longrightarrow & M/fM & \longrightarrow & 0 \end{array}$$

for any wedging element $f \in R$ for M. This provides

$$\begin{aligned} \dim_k R - \dim_k M &= \dim_k R/fM - \dim_k M/fM \\ &= \deg_k M. \end{aligned}$$ △

Next we want to show that the degree of R-ideals is finite. To do so, we need the following elementary statement.

Lemma C.1.16. *Let $N \leq M$ be two torsion-free R-modules. Let $a \in R$ be a regular element. Then*

$$\begin{array}{rccc} \phi: & M/N & \to & aM/aN \\ & m+N & \mapsto & am+aN \end{array}$$

is an isomorphism of R-modules.

Proof. Let $m+N = m+n+N \in M/N$ with $n \in N$. Then clearly $\phi(m+N) = \phi(m+n+N)$ and thus ϕ is well-defined. By definition, we have $aM = \{am \mid m \in M\}$. Thus the homomorphism is surjective. If $am + aN = \phi(m+N)$ is zero in aM/aN, then $am \in aN$ and thus, by the above, we have $am = an$ for some $n \in N$. In particular, $a(m-n) = 0$ and since a was regular and M is torsion-free, we must have $m = n$ which proves that ϕ is injective. □

Lemma C.1.17. *Let M be an R-ideal and let $f \in R$ be regular with $fM \subseteq R$. Then the degree $\deg_k M$ is finite. Moreover, the dimensions over k involved can be computed locally, that is*

$$\begin{array}{rcccccl} \dim_k R/fM & = & \sum_{P \in \operatorname{Spec}(R)_0} \dim_k R_P/fM_P & = & \sum_{P \in \operatorname{Spec}(R)_0} \deg_k fM_P & & \text{and} \\ \dim_k M/fM & = & \sum_{P \in \operatorname{Spec}(R)_0} \dim_k M_P/fM_P. & & & & \end{array}$$

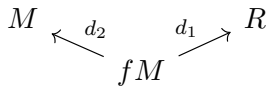
yielding

$$\deg_k M = \sum_{P \in \operatorname{Spec}(R)_0} \dim_k R_P/fM_P - \dim_k M_P/fM_P = \sum_{P \in \operatorname{Spec}(R)_0} \deg_k M_P.$$

Proof. Note that R is a finite residual-type k-algebra. Since M is an R-ideal, fM is an integral ideal of R such that R/fM has Krull dimension zero, see Lemma C.1.4. Thus, by Lemma B.4.7, $\dim_k R/fM$ is finite. Moreover, by Lemma C.1.16, we have a monomorphism of k-vector spaces $M/fM \xrightarrow{\cong} fM/f^2M \hookrightarrow R/f^2M$ and, by the above,

the latter has finite dimension over k. That is, both $\dim_k R/fM$ and $\dim_k M/fM$ and thus $\deg_k M$ is finite. The part about computing the dimension as the sum over the localisations is also due to Lemma B.4.7. □

To visualise this, consider the following diagram



in which the number along the arrow indicates the respective k-dimension of the quotient. Thus we have $\deg_k M = d_1 - d_2$. Note that if $M \subseteq R$, then we may take $f = 1$ and thus $d_2 = 0$ which then provides $\deg_k M = d_1$.

We now show that the definition is independent of the wedging element. To do so, we need the following elementary result.

Lemma C.1.18. *Let R be a ring and let M be an R-ideal with $fM \subseteq R$ and $f \in R$ regular. Then for all ideals $I \subseteq R$ we have the following exact sequences:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & fR/fIM & \longrightarrow & R/fIM & \longrightarrow & R/fR & \longrightarrow & 0 \\ 0 & \longrightarrow & fM/fIM & \longrightarrow & M/fIM & \longrightarrow & M/fM & \longrightarrow & 0 \end{array}$$

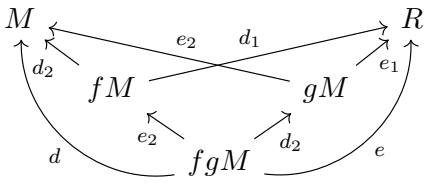
In particular, if R contains a field k and if $IM \subseteq R$ holds, then we obtain

$$\begin{array}{rcl} \dim_k R/fIM & = & \dim_k R/IM + \dim_k R/fM \\ \dim_k M/fIM & = & \dim_k M/IM + \dim_k M/fM. \end{array}$$

Proof. The exactness of the sequences is evident. The dimension implication follows by the additivity of the dimension along exact sequences of finite dimensional vector spaces and by the isomorphism given in Lemma C.1.16. Note that M is torsion-free by Remark C.1.12. □

Proposition C.1.19. *The definition of the degree of R-ideals is independent of the choice of the wedging element.*

Proof. Let M be an R-ideal. By assumption, there is some regular $f \in R$ with $fM \subseteq R$. Now take another regular $g \in R$ such that $gM \subseteq R$. Consider the following diagram in which the numbers attached to an arrow denote the k-dimension of the respective quotient:



By Lemma C.1.16, we have $M/fM \cong gM/gfM$ for all regular $g \in R$. By Lemma C.1.18, the numbers on the arrows in the diagram behave additively, that is, we have $d = d_2 + e_2$ and $e = e_1 + d_2$. In particular, $e - d = e_1 - e_2$. Moreover,

$$d_1 - d_2 = d_1 - d_2 + e_2 - e_2 = d_1 + e_2 - (d_2 + e_2) = e - d$$

which proves $e_1 - e_2 = d_1 - d_2$. □

Using the exact sequences of Lemma C.1.18 we obtain a surprising result:

Lemma C.1.20. *Let M be an R-ideal and $f \in R$ regular with $fM \subseteq R$. Then $\dim_k R/fR = \dim_k M/fM$. In particular,*

$$\begin{aligned}\deg_k M &= \dim_k R/fM - \dim_k R/fR \\ &= \deg_k fM - \deg_k fR.\end{aligned}$$

Proof. We consider the degree of M and expand the terms appearing by another wedging element g: Let $f, g \in R$ be two regular wedging elements for M. Then

$$\begin{aligned}\deg_k M &= \dim_k R/fM - \dim_k M/fM \\ \text{Lemma C.1.16} \rightsquigarrow \quad &= \dim_k gR/gfM - \dim_k gM/gfM \\ \text{Lemma C.1.18} \rightsquigarrow \quad &= (\dim_k R/gfM - \dim_k R/gR) - (\dim_k M/gfM - \dim_k M/gM) \\ &= \underbrace{(\dim_k R/gfM - \dim_k M/gfM)}_{=\deg_k M} + \dim_k M/gM - \dim_k R/gR.\end{aligned}$$

Now subtracting $\deg_k M$ on both sides provides $\dim_k M/gM = \dim_k R/gR$. □

Hence for integral R-ideals we see that Lemma C.1.20 can be applied to any regular element of R. This together with the isomorphism from Lemma C.1.16 provides the following result.

Proposition C.1.21. *Let M be an R-ideal. Then for any regular $a \in R$ we have $\dim_k M/aM = \dim_k R/aR$.*

Proof. Let $f \in R$ be regular with $fM \subseteq R$. We may apply Lemma C.1.20 to fM and any regular $a \in R$, since any such a is a wedging element for fM, to obtain $\dim_k fM/a(fM) = \dim_k R/aR$. Now by Lemma C.1.16, we have the isomorphism of R-modules $M/aM \cong fM/a(fM)$ which then finally provides the assertion. □

Combining Lemma C.1.20 and Lemma C.1.17 provides the following Corollary.

Corollary C.1.22. *Let M be an R-ideal and let $f \in R$ be regular with $fM \subseteq R$. Then*

$$\deg_k M = \sum_{P \in \operatorname{Spec}(R)} \deg_k M_P = \sum_{P \in \operatorname{Spec}(R)_0} \deg_k M_P$$

where M_P is regarded as an R_P-ideal, see Lemma C.1.7.

Proof. As mentioned above, the assertion is the combination of Lemmas C.1.17 and C.1.20. □

Lemma C.1.23. *Let M be an R-module and $a \in R$ regular. The map $\varphi : a^{-1}M/M \to M/aM$ with $\varphi(a^{-1}m + M) = m + aM$ is an R-module isomorphism.*

Proof. That φ is well defined follows from

$$a^{-1}m + m' + M = a^{-1}m + a^{-1}am' + M = a^{-1}(m + am') + M$$

and therefore

$$\begin{aligned}\varphi(a^{-1}m + m' + M) = \varphi(a^{-1}(m + am') + M) = m + am' + aM = m + aM \\ = \varphi(a^{-1}m + M).\end{aligned}$$

The map φ is obviously surjective and R-linear. Let $\varphi(a^{-1}m + M) = m + aM = aM$ which is equivalent to $m \in aM$. Then $m = am'$ for $m' \in M$ and thus $a^{-1}m \in M$ which finally provides the injectivity. □

Corollary C.1.24. *Let M be an R-ideal and let $a \in R$ be a regular element. Then*

$$\dim_k a^{-1}M/M = \dim_k M/aM = \dim_k R/aR.$$

Proof. Combining Lemma C.1.23 and Proposition C.1.21 provides the assertion. □

Proposition C.1.25. *Let M be an R-ideal and $I \subseteq R$ be an ideal of R. Then*

$$\dim_k M/IM = \deg_k IM - \deg_k M.$$

Proof. Let $f \in R$ be regular with $fM \subseteq R$. Consider the exact sequence

$$0 \longrightarrow fM/IfM \longrightarrow R/IfM \longrightarrow R/fM \longrightarrow 0$$

which, by Lemma C.1.16, provides

$$\dim_k M/IM = \dim_k R/IfM - \dim_k R/fM. \tag{1:1}$$

By Lemma C.1.20, we have

$$\deg_k M = \dim_k R/fM - \dim_k R/fR.$$

Since f is also a wedging element for IM, we analogously have

$$\deg_k IM = \dim_k R/IfM - \dim_k R/fR.$$

Therefore,

$$\begin{aligned} \deg_k IM - \deg_k M &= (\dim_k R/IfM - \dim_k R/fR) - (\dim_k R/fM - \dim_k R/fR) \\ &= \dim_k R/IfM - \dim_k R/fM \\ (1{:}1) \rightsquigarrow \; &= \dim_k M/IM. \end{aligned}$$

□

The following two results show that invertible R-ideals behave very well with respect to the degree. They show that the degree is additive if one of the factors is invertible and that the degree of an invertible R-ideal can be computed as the sum of the degrees of its restrictions to the irreducible components of $\operatorname{Spec}(R)$.

Proposition C.1.26. *If M is an invertible R-ideal and I any R-ideal, then*

$$\deg_k IM = \deg_k I + \deg_k M.$$

Proof. First, we prove the statement for $I \subseteq R$ and then extend the result to arbitrary R-ideals I. By Proposition C.1.25, we have $\deg_k IM = \deg_k M + \dim_k M/IM$ and thus we are left to prove that $\dim_k M/IM = \dim_k R/I$ since the latter is equal to $\deg_k I$. By Eq. (1:1) in the proof of Proposition C.1.25, we have

$$\dim_k M/IM = \dim_k R/IfM - \dim_k R/fM.$$

Hence, if we set $J = fM \subseteq R$, it suffices to show that

$$\dim_k R/IJ - \dim_k R/J = \dim_k R/I \tag{1:2}$$

holds for integral and invertible R-ideals J. By Proposition C.1.19, the degree of an

integral R-ideal I equals $\dim_k R/I$ and thus, by Corollary C.1.22, we have

$$\dim_k R/IJ = \sum_{P \in \operatorname{Spec}(R)} \dim_k R_P/I_P J_P.$$

Now since J is invertible, for all $P \in \operatorname{Spec}(R)$ we have $J_P = a_P R_P$ for some $a_P \in R_P$. For any two integral R-ideals I, J we have the exact sequence

$$0 \longrightarrow J/IJ \longrightarrow R/IJ \longrightarrow R/J \longrightarrow 0$$

which then provides

$$\dim_k R/IJ = \dim_k J/IJ + \dim_k R/J.$$

Applying this to I_P and $J_P = a_P R_P$ we obtain

$$\begin{aligned} \dim_k R_P/I_P J_P = \dim_k R_P/a_P I_P &= \dim_k a_P R_P/a_P I_P + \dim_k R_P/a_P R_P \\ \text{Lemma C.1.16} \rightsquigarrow \quad &= \dim_k R_P/I_P + \dim_k R_P/a_P R_P \\ &= \dim_k R_P/I_P + \dim_k R_P/J_P. \end{aligned}$$

Hence

$$\begin{aligned} \dim_k R/IJ &= \sum_{P \in \operatorname{Spec}(R)} \dim_k R_P/I_P J_P \\ &= \sum_{P \in \operatorname{Spec}(R)} \dim_k R_P/I_P + \dim_k R_P/J_P \\ &= \sum_{P \in \operatorname{Spec}(R)} \dim_k R_P/I_P + \sum_{P \in \operatorname{Spec}(R)} \dim_k R_P/J_P \\ &= \dim_k R/I + \dim_k R/J \end{aligned}$$

as desired. This proves the assertion in the case $I \subseteq R$.

Now let I be an arbitrary R-ideal. There are regular wedging elements $f, g \in R$ such that $fM \subseteq R$ and $gI \subseteq R$. Now using Lemma C.1.20 we obtain

$$\deg_k IM = \deg_k fgIM - \deg_k fgR. \tag{1:3}$$

Now since $fgI \subseteq R$, we can apply what we have shown above and have

$$\deg_k fgIM = \deg_k fgI + \deg_k M.$$

Plugging this into Eq. (1:3), we obtain

$$\deg_k IM = \deg_k fgI + \deg_k M - \deg_k fgR$$

and, by Lemma C.1.20 again, we have $\deg_k fgI - \deg_k fgR = \deg_k I$ which finally provides the assertion. □

Lemma C.1.27. *Let I, J be two R-ideals such that $J \subseteq I$. Then $\deg_k J \geq \deg_k I$.*

Proof. Let f be wedging elements of I, i.e. $fJ \subseteq fI \subseteq R$. Then the surjection $R/fJ \to R/fI$ provides an exact sequence of R-modules

$$0 \longrightarrow fI/fJ \longrightarrow R/fJ \longrightarrow R/fI \longrightarrow 0$$

where $fI/fJ \cong I/J$ by Lemma C.1.16. In particular, since all of the above k-vector spaces

are finite dimensional, we obtain

$$\underbrace{\dim_k R/fJ}_{=\deg_k J} = \underbrace{\dim_k R/fI}_{=\deg_k I} + \underbrace{\dim_k I/J}_{\geq 0}$$

and thus the assertion. □

Lemma C.1.28. *Let $M \in \mathrm{InvId}(R)$ be an invertible R-ideal. Then*

$$\deg_k M = \sum_{i=1}^{m} \deg_k M/P_iM$$

where $P_1, \ldots, P_m$ denote the minimal prime ideals of R and M/P_iM denotes the restriction of M to an R/P_i-ideal, see Lemma C.1.8 and Definition C.1.9.

Proof. First of all, by Corollary C.1.22, we may compute the degree of M as the sum of the degrees of M_P for $P \in \mathrm{Spec}(R)_0$. Since M is invertible, we have $M_P \cong R_P$ for every $P \in \mathrm{Spec}(R)$. There is some regular $f \in R$ such that $fM \subseteq R$ and thus $\lambda(f)M_P \subseteq R_P$ is an ideal of R_P and isomorphic to $M_P \cong R_P$. Here $\lambda : R \to R_P$ denotes the localisation homomorphism. So

$$(fM)_P = \begin{cases} \lambda_P(f)M_P, & fM \subseteq P \\ R_P, & \text{otherwise,} \end{cases}$$

and in the former case $\lambda_P(f)M_P$ is a proper ideal of R_P which is free of rank one over R_P. Hence $\lambda_P(f)M_P = \lambda_P(a)R_P$ for some $a \in R$ in that case. In the latter case we have $\deg_k M_P = 0$ and in the former we have

$$\begin{aligned} \deg_k M_P &= \deg_k \lambda_P(f)M_P - \deg_k \lambda_P(f)R_P \\ &= \deg_k a_P R_P - \deg_k \lambda_P(f)R_P \end{aligned}$$

where we set $a_P = \lambda_P(a)$. By Lemma B.4.49, the degree of a principal R-ideal can be computed as the sum of the degrees of the restrictions to the irreducible components of $\mathrm{Spec}(R_P)$, i.e.

$$\begin{aligned} \deg_k M_P &= \deg_k a_P R_P - \deg_k \lambda_P(f)R_P \\ &= \sum_{P_i \subseteq P} \left(\deg_k(a_P R_P + P_i R_P) - \deg_k(\lambda_P(f)R_P + P_i R_P)\right). \end{aligned} \tag{1:4}$$

Now fix some minimal prime $P_i \in \{P_1, \ldots, P_m\}$ such that $P_i \subseteq P$. By Remark B.4.36, we have that the $f \in R$ from above satisfies $(f + P_i)(M/P_iM) \hookrightarrow R/P_i$. Since M is invertible, we have $(M/P_iM)_P \cong R_P/P_iR_P \cong (R/P_i)_P$ and thus M/P_iM is invertible as an R/P_i-module as well. Similar to above, we have

$$((f + P_i)(M/P_iM))_P = \begin{cases} (\lambda_P(f) + P_i)(M_P/P_iM_P), & fM, P_i \subseteq P \\ (R/P_i)_P, & fM \not\subseteq P \vee P_i \not\subseteq P \end{cases}$$

and in the former case $(\lambda_P(f) + P_i)(M_P/P_iM_P) \cong (\lambda_P(a) + P_iR_P)(R_P/P_iR_P)$ with the same $a \in R$ as above. Therefore, with the same line of argument as above, we obtain

$$\begin{aligned} \deg_k M/P_iM &= \sum_{P \in \mathrm{Spec}(R/P_i)_0} \deg_k(M/P_iM)_P \\ &= \sum_{P_i \subseteq P} \deg_k(\lambda_P(a)R_P + P_iR_P) - \deg_k(\lambda_P(f)R_P + P_iR_P) \end{aligned}$$

which yields

$$\begin{aligned}\sum_{i=1}^{m} \deg_k M/P_iM &= \sum_{i=1}^{m} \sum_{P_i \subseteq P} \deg_k(\lambda_P(a)R_P + P_iR_P) - \deg_k(\lambda_P(f)R_P + P_iR_P) \\ &= \sum_{P \in \operatorname{Spec}(R)_0} \sum_{P_i \subseteq P} \deg_k(\lambda_P(a)R_P + P_iR_P) - \deg_k(\lambda_P(f)R_P + P_iR_P) \\ \text{Eq. (1:4)} \rightsquigarrow &= \sum_{P \in \operatorname{Spec}(R)_0} \deg_k M_P \\ &= \deg_k M\end{aligned}$$

as asserted. □

C.2 R-Ideals and Approximation of Elements and Bases

In this short section we provide the analogue of Lemma B.4.45 for R-ideals. The next lemma tells us how to construct elements in the restrictions M/P_iM of an R-ideal M that will actually come from an element of M itself.

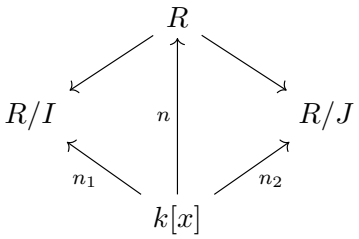
Lemma C.2.1. *Let R be a reduced ring with minimal prime ideals $P_1, \dots, P_m$ and we set $I_i = \bigcap_{j=1}^{i} P_j$. Let M be an R-ideal. Then $(m_1 + P_1M, \dots, m_m + P_mM) \in \bigoplus_{i=1}^{m} M/P_iM$ lies in the image of $\phi : M \to \bigoplus_{i=1}^{m} M/P_iM$ if and only if for all $i = 2, \dots, m$ we have*

$$(m_1^{i-1} + I_{i-1}M, m_i + P_iM) \in \operatorname{im}(\phi_i). \tag{2:5}$$

Here $m_1^{i-1} + I_{i-1}M = \phi_{i-1}^{-1}(m_1 + P_1M, \dots, m_{i-1} + P_{i-1}M) \in M/I_{i-1}M$ for $i \geq 3$ and $m_1^1 + I_{i-1}M = m_1 + P_1M$.

Proof. The proof is literally the same as the one of Lemma B.4.45. We only use Corollary B.4.47 instead of Corollary B.4.42. □

Proposition C.2.2. *Let the situation be as in Lemma B.4.46. Assume that R, R/I and R/J are free ring extensions of $k[x]$ such that*



commutes. Then $n = n_1 + n_2$. Assume M to be an R-ideal. Then M is free of rank n. Moreover, M/IM and M/JM are isomorphic to R/I- respectively R/J-ideals. In particular, they are free over $k[x]$ of rank n_1 respectively n_2. Then we have

$$\operatorname{im}(\phi) = \{(m + IM, m + z + JM) \mid m \in M, z \in IM + JM\}.$$

Fix any bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of M/IM respectively M/JM. Then $\operatorname{im}(\phi)$ has a $k[x]$-basis whose basis matrix with respect to $(\mathcal{B}_1, \mathcal{B}_2)$ is of the form

$$\left(\begin{array}{c|c} E_{n_1} & \mathbf{0} \\ \hline N & C \end{array}\right) \in k[x]^{(n_1+n_2)\times(n_1+n_2)}.$$

Here C can be chosen to be an arbitrary basis matrix of the free submodule $(IM+JM)/JM$.

Proof. By Lemma B.4.41, we have $n = n_1 + n_2$ since the rank of R over $k[x]$ is equal to the $k(x)$-dimension of $\mathrm{Frac}(R)$, see Lemma B.4.10. By Lemma 4.1.6, M is free of rank n. By Lemma C.1.8, M/IM and M/JM are isomorphic to R/I- respectively R/J-ideals, and thus Lemma 4.1.6 again provides the statement about the freeness.

Let $S = \{(m+IM, m+z+JM) \mid m \in M, z \in IM+JM\}$. Then $S \subseteq \ker(\psi) = \mathrm{im}(\phi)$ since $m-(m+z) = -z \in IM+JM$. Conversely, let $(m+IM, n+JM) \in \ker(\psi)$. Then $m-n \in IM+JM$ and thus $n = m+z$ with $z \in IM+JM$. This proves the assertion about $\mathrm{im}(\phi)$. In particular, this shows that if $\{m_i + IM\}$ is a generating set of M/IM over $k[x]$ and $\{z_i + IM + JM\}$ is a generating set of $(IM+JM)/JM$ over $k[x]$, then $\phi(\{m_i\} \cup \{z_i\})$ generates $\mathrm{im}(\phi)$ over $k[x]$. Let $\mathcal{B}_1 = (\alpha_1 + IM, \dots, \alpha_{n_1} + IM)$ and $z_1 + JM, \dots, z_{n_2} + JM$ be bases of M/IM respectively $(IM+JM)/JM$ over $k[x]$. Set $\mathcal{I} = (\alpha_1, \dots, \alpha_{n_1})$ and $\mathcal{Z} = (z_1, \dots, z_{n_2})$. Then

$$\mathcal{B} = (\phi(\mathcal{I}), \phi(\mathcal{Z})) = (\phi(\alpha_1), \dots, \phi(\alpha_{n_1}), \phi(z_1), \dots, \phi(z_{n_2}))$$

generates $\mathrm{im}(\phi)$. But since $\mathrm{im}(\phi)$ is free of rank $n = n_1 + n_2$, $\mathcal{B}$ need to be a basis of $\mathrm{im}(\phi)$ over $k[x]$. The basis transformation matrix T from $(\mathcal{B}_1, \mathcal{B}_2)$ to $\mathcal{B}$ is thus given by

$$T = \left(\begin{array}{c|c} E_{n_1} & \mathbf{0} \\ \hline N & C' \end{array}\right) \in k[x]^{(n_1+n_2)\times(n_1+n_2)}.$$

The top right zero matrix is due to $z_i \in IM + JM$ which means that z_i vanishes in M/IM. By construction, C' is the basis matrix of the basis $\phi(\mathcal{Z})$ of $(IM+JM)/JM$ over $k[x]$. Now we may reduce the matrix C' by unimodular column operations over $k[x]$ which finally yields

$$TU = \left(\begin{array}{c|c} E_{n_1} & \mathbf{0} \\ \hline N & C \end{array}\right)$$

with C being reduced. These unimodular column operations perform a base change of $\phi(\mathcal{Z})$ and $\mathrm{im}(\phi)$ and hence we deduce the assertion. □

Remark C.2.3. The key point here is that M (and thus $\phi(M)$) and $M/IM \oplus M/JM$ have the same rank over $k[x]$. This is the case whenever M is an R-ideal and thus embedded in $\mathrm{Frac}(R)$, see Lemma B.4.41. △

Remark C.2.4. Proposition C.2.2 can be used to find bases of the image of M in $M/IM \oplus M/JM$ that restricts to a given basis of M/IM and whose restriction in M/JM can be arbitrarily altered by any basis of $(IM+JM)/JM$. The algorithm ReduceByPopov enables us to reduce the image of the found basis in M/JM by that of $(IM+JM)/JM$ in terms of matrices. This results in finding a basis whose matrix representation as in Proposition C.2.2 satisfies $\deg N < \deg C$. We will rely on this in the endeavour of finding a suitable basis of $\mathcal{F}(V_0)$ for $\mathcal{O}_X$-ideals $\mathcal{F}$ that restricts to elements in $\mathcal{F}(V_{i,0})$ having coefficient vectors with respect to Ω_i with bounded degree. △

C.3 General Properties of $\mathcal{O}_X$-Ideals

If not mentioned otherwise, in this section X will denote a curve of finite residual-type over k, see Definition 2.1.1.

Lemma C.3.1. *Let $\mathcal{F} \leq \mathcal{L}$ be two $\mathcal{O}_X$-ideals. Then $\mathrm{Supp}(\mathcal{L}/\mathcal{F})$ is finite and thus $H^1(X, \mathcal{L}/\mathcal{F}) = 0$. In particular, if X is projective, then $\chi_k(X, \mathcal{L}/\mathcal{F}) = H^0(X, \mathcal{L}/\mathcal{F})$.*

Proof. By assumption, we can cover X by a finite set of affine opens. Hence the support of $\mathcal{L}/\mathcal{F}$ is finite if and only if the support of its restrictions to those affine opens are finite. Thus the first statement follows from Proposition C.1.13. But this means that $\mathcal{L}/\mathcal{F}$ is a skyscraper sheaf on X and thus, by Lemma B.2.8, we have $H^1(X, \mathcal{L}/\mathcal{F}) = 0$. This also proves the particular part. □

The sections of sheaves with finite support can easily be characterised by the stalks.

Lemma C.3.2. *Let X be a curve over k. Let $\mathcal{F}$ be a sheaf on X. If $\operatorname{Supp}(\mathcal{F})$ is finite, then $\mathcal{F}(U) \cong \coprod_{P \in U} \mathcal{F}_P$ for all open $U \subseteq X$.*

Proof. We can define a sheaf $\mathcal{F}^s$ by $\mathcal{F}^s(U) = \coprod_{P \in U} \mathcal{F}_P$ and obtain a canonical morphism of sheaves $\varphi : \mathcal{F} \to \mathcal{F}^s$. Since $\mathcal{F}$ is a sheaf, it is separated and thus by Lemma B.1.8 the morphism φ is injective. Thus, by Lemma B.1.12, φ is an isomorphism if and only if φ_P is surjective for all $P \in X$. For instance, this is the case whenever the stalk of $\mathcal{F}^s$ at P is isomorphic to $\mathcal{F}_P$. To show $\mathcal{F}^s_P \cong \mathcal{F}_P$, it suffices to show that there is some open subset U containing P but no other point of $S := \operatorname{Supp}\ \mathcal{F}$. For instance, this is the case if S solely consists of closed points of X since then we could just remove the other points. We will prove that this is the case which thus proves the assertion: Every irreducible component of X is again a curve over k and thus, by Lemma D.2.1, we see that each of them, and any non-empty affine open subset of it, contains infinitely many points. Therefore, since S is finite, it cannot contain an irreducible component of X (neither an affine open of a component). By Corollary B.5.5, we know that $\xi_i \in S_i \subseteq \operatorname{Supp}(\mathcal{F})$ implies $X_i \subseteq \operatorname{Supp}(\mathcal{F})$ which is not possible by the above. Hence S_i does not contain the unique generic point ξ_i of X_i and thus, by Lemma B.5.1, it consists solely of closed points of S_i. In particular, the same is true for S which proves the assertion. □

Corollary C.3.3. *Let X be a curve over k and let $\mathcal{F} \leq \mathcal{L}$ be two $\mathcal{O}_X$-ideals. Then $H^0(X, \mathcal{L}/\mathcal{F}) = \coprod_{P \in X} \mathcal{L}_P/\mathcal{F}_P$. In particular, if X is projective, then $\chi_k(X, \mathcal{L}/\mathcal{F}) = \sum_{P \in X} \dim_k \mathcal{L}_P/\mathcal{F}_P$.*

Proof. By Lemma C.3.1, $\operatorname{Supp}(\mathcal{L}/\mathcal{F})$ is finite and thus Lemmas C.3.1 and C.3.2 provide the assertions. □

Lemma C.3.4. *Let X be a Cohen-Macaulay curve of finite residual-type over k and let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-submodule of $\mathcal{K}_X$. Then $\mathcal{F}(U)$ contains a regular element of $\mathcal{O}_X(U)$ for all affine open $U \subseteq X$ if and only if $\mathcal{F}$ is invertible at the generic points of X if and only if there is an affine cover $\mathcal{U} = \{U_\alpha\}$ of X such that $\mathcal{F}(U_\alpha)$ contains a regular element of $\mathcal{O}_X(U_\alpha)$ for all $U_\alpha \in \mathcal{U}$.*

Proof. We prove the equivalence between the first two. Let $\mathcal{F}$ be invertible at the generic points of X and let $U \subseteq X$ be an affine open. Then the minimal primes of $\mathcal{O}_X(U)$ are in 1-to-1 correspondence to the generic points of X contained in U. Since $\mathcal{F}$ is quasi-coherent, $\mathcal{F}(U)$ is invertible at the minimal primes of $\mathcal{O}_X(U)$ and hence Proposition C.1.10 implies that $\mathcal{F}(U)$ contains a regular element of $\mathcal{O}_X(U)$. Conversely, let $\mathcal{F}(U)$ contain a regular element of $\mathcal{O}_X(U)$ for all open and affine $U \subseteq X$. Every generic point ξ of X lies in an affine open U and corresponds to a minimal prime P of $\mathcal{O}_X(U)$. By the coherence of $\mathcal{F}$, there is some regular $c \in \mathcal{O}_X(U)$ such that $c\mathcal{F}(U) \subseteq \mathcal{O}_X(U)$. Moreover, by assumption, there is some regular $a \in \mathcal{O}_X(U)$ contained in $\mathcal{F}(U)$. Hence $ac\mathcal{F}(U)_P$ is an integral ideal of $\mathcal{O}_{X,P}$ containing a regular element and since P was minimal, every regular element in $\mathcal{O}_{X,P}$ is invertible. Therefore, $\mathcal{F}_\xi \cong \mathcal{F}(U)_P \cong \mathcal{O}_{X,P}$. The same argument shows that one affine cover is sufficient and hence the last equivalence is trivial. □

C.4 Degree of $\mathcal{O}_X$-Ideals

After we have introduced the notion of degree for R-ideals for every finite residual-type k-algebra R, the next step is to enlarge this to $\mathcal{O}_X$-ideals for a curve X of finite residual-type over k. Since the degree of R-ideals can be computed locally in the sense of Corollary C.1.22, we might define the degree of an $\mathcal{O}_X$-ideal $\mathcal{F}$ as the sum of the degree of the $\mathcal{O}_{X,P}$-ideals $\mathcal{F}_P$.

Throughout this section, if not explicitly mentioned otherwise, k denotes a field and X a curve of finite residual-type over k.

Definition C.4.1. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. We define the **degree of $\mathcal{F}$ over k** as

$$\deg_k \mathcal{F} = \sum_{P \in X_0} \deg_k \mathcal{F}_P.$$

Here the definition makes sense since for every $P \in X$ there is some affine open neighborhood $U = \operatorname{Spec}(R)$ such that $\mathcal{F}(U) \cong M^\sim$, see [Liu02, 5.1.7], where M is a finitely generated R-submodule of $\mathcal{K}_X(U) = \operatorname{Frac}(R)$, see Proposition B.2.2. Hence M is an R-ideal and thus, via applying Lemma C.1.7, we see that $M_P = \mathcal{F}_P$ is an $R_P = \mathcal{O}_{X,P}$-ideal. △

Another possible way to define the degree of $\mathcal{O}_X$-ideals over k, one that is equivalent to the one we introduced above, is to find a wedging divisor instead of a wedging element. This resembles the idea of reducing the question to the integral ideal case. Moreover, in the definition introduced above we need a wedging element for every $\mathcal{F}_P$, and to give a regular element for every $P \in X$ strongly resembles the idea of a Cartier divisor.

Lemma C.4.2. *Let X be a curve of finite residual-type over k. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then there exists an (integral) invertible $\mathcal{O}_X$-ideal $\mathcal{G} \leq \mathcal{O}_X$ such that $\mathcal{F}\mathcal{G} \leq \mathcal{O}_X$. Note that we also have $\mathcal{F}\mathcal{G} \leq \mathcal{F}$.*

Proof. Since X is noetherian, it may be covered by finitely many affine opens. Take any finite affine open cover of X given by $U_i = \operatorname{Spec}(R_i)$ for $i \in I = \{1, \dots, m\}$. Since $\mathcal{F}$ is an $\mathcal{O}_X$-ideal, we have that $\mathcal{F}(U_i)$ is an R_i-ideal. Moreover, there is some regular $a_i \in R_i$ such that $a_i \mathcal{F}(U_i) \subseteq R_i$. The idea is now, roughly speaking, to collect all such a_i and form an invertible $\mathcal{O}_X$-ideal $\mathcal{G}$ which satisfies $\mathcal{G}(U_i) = a_i R_i$ and thus satisfies $(\mathcal{F}\mathcal{G})(U_i) \subseteq R_i$.

Since a_i is regular, it is not contained in any minimal prime ideal of R_i, see Corollary B.4.14. In particular, R_i/a_iR_i is the affine coordinate ring of the closed subscheme $V(a_i) \subseteq U_i$ and it is a noetherian ring of Krull dimension zero. Thus, by [Sta18, Tag 00KJ], it is a finite product of local artinian rings. In particular, $V(a_i)$ is not only closed in U_i, but also a finite union of closed points of X. Since $A_i := V(a_i)$ does not contain any minimal prime of R_i and thus no generic point of U_i, it does not contain any generic point of X at all. Let $X_1, \dots, X_m$ denote the finitely many irreducible components of X. Now $A_i \cap X_j$ is a finite set not containing the generic point of X_j and is thus closed in X_j by Lemma B.5.1. Thus $A_i = \cup_{j=1}^m (A_i \cap X_j)$ is closed in X as well. Then we define an $\mathcal{O}_X$-ideal $\mathcal{G}_i$ by $(\mathcal{G}_i)_{|U_i} = a_i \mathcal{O}_{U_i}$ and $(\mathcal{G}_i)_{X \setminus A_i} = \mathcal{O}_{X \setminus A_i}$. This does indeed define a sheaf of $\mathcal{O}_X$-modules since a_i restricts, by construction, to a unit in $(X \setminus A_i) \cap U_i$. Moreover, we even see that $(\mathcal{G}_i)_P$ is invertible for all $P \in X$ and thus $\mathcal{G}_i$ is an invertible $\mathcal{O}_X$-ideal. Now define the $\mathcal{O}_X$-ideal $\mathcal{G}$ as the finite product of the $\mathcal{G}_i$. Hence, by Lemma 3.1.24, $\mathcal{G}$ is the invertible $\mathcal{O}_X$-ideal given by $\mathcal{G}_{|U_J} = \prod_{j \in J} (a_j)_{|U_J} \mathcal{O}_{U_J}$ on every $U_J = \cap_{j \in J} U_j$ for arbitrary $J \subseteq I$. Note that $\{U_J \mid J \subseteq I\}$ form an open cover of X. Since X is separated with an affine base, by [Sta18, Tag 01KP], we have that U_J is an affine open subset of X. Therefore, by Lemma 3.1.17, we have an embedding

$$(\mathcal{F}\mathcal{G})(U_J) \cong \mathcal{F}(U_J)\mathcal{G}(U_J) = (\prod\nolimits_{j \in J} (a_j)_{|U_J}) \mathcal{F}(U_J) \subseteq \mathcal{O}_X(U_J). \tag{4:6}$$

Note that the embedding of $\mathcal{O}_X(U_J)$-modules in (4:6) provides an embedding of quasi-coherent $\mathcal{O}_{U_J}$-modules that are compatible with the restriction maps of the corresponding sheaves. Now since the homomorphisms $\mathcal{F} \to \mathcal{G}$ of general $\mathcal{O}_X$-modules $\mathcal{F}$ and $\mathcal{G}$ form a sheaf $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$, we obtain a morphism of $\mathcal{O}_X$-modules $\mathcal{FG} \to \mathcal{O}_X$ which is injective. □

In the case of X being a cover of $\mathbb{P}^1_k$, the proof simplifies a lot as the following remark shows.

Remark C.4.3. Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then there exist an effective divisor $D \geq 0$ such that $\mathcal{F}(-D) \leq \mathcal{O}_X$. Indeed, we have seen in Lemma 4.3.12 that for every $\mathcal{O}_X$-ideal $\mathcal{F}$ there are bases of $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ which are related by a matrix $\mathrm{diag}(x^{d_i})$. But this means that the common denominator $a_0 \in k[x]$ of the basis of $\mathcal{F}(V_0)$ and the common denominator $a_\infty \in k[x^{-1}]$ of the basis of $\mathcal{F}(V_\infty)$ will only differ by a power of x, which itself is a unit in $\mathcal{O}_{\mathbb{P}^1}(U_0 \cap U_\infty) = k[x, x^{-1}]$. This means we may define an effective divisor $D \geq 0$ by $\{(V_0, a_0), (V_\infty, a_\infty)\}$ since $a_0/a_\infty \in \mathcal{O}_X(V_0 \cap V_\infty)^\times$. Obviously, D satisfies $\mathcal{F}(-D) \leq \mathcal{O}_X$ since locally on V_0 we have $\mathcal{F}(-D)(V_0) \cong a_0\mathcal{F}(V_0) \subseteq R_0$ and on V_∞ we obtain $\mathcal{F}(-D)(V_\infty) \cong a_\infty\mathcal{F}(V_\infty) \subseteq R_\infty$. △

Lemma C.4.4. *Let X be a projective curve over k. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then for every invertible $\mathcal{O}_X$-ideal $\mathcal{G} \leq \mathcal{O}_X$ such that $\mathcal{FG} \leq \mathcal{O}_X$, we have*

$$\deg_k \mathcal{F} = \chi(\mathcal{O}_X/\mathcal{FG}) - \chi(\mathcal{F}/\mathcal{FG}).$$

Moreover, we also have

$$\deg_k \mathcal{F} = \chi(\mathcal{O}_X) - \chi(\mathcal{F}).$$

Proof. Let $\mathcal{G} \leq \mathcal{O}_X$ be an invertible $\mathcal{O}_X$-ideal such that $\mathcal{FG} \leq \mathcal{O}_X$. Then $\mathcal{FG} \leq \mathcal{F}$, see Lemma C.4.2. We first prove the equality

$$\chi(\mathcal{O}_X) - \chi(\mathcal{F}) = \chi(\mathcal{O}_X/\mathcal{FG}) - \chi(\mathcal{F}/\mathcal{FG}).$$

By the above, we have two short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{FG} & \longrightarrow & \mathcal{O}_X & \longrightarrow & \mathcal{O}_X/\mathcal{FG} & \longrightarrow & 0, \\ 0 & \longrightarrow & \mathcal{FG} & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{F}/\mathcal{FG} & \longrightarrow & 0. \end{array}$$

By assumption, X is projective and thus proper over k, see Corollary B.5.19. Hence the Euler characteristic $\chi_k(\mathcal{F}) := \chi_k(X, \mathcal{F})$ is defined, see Definition B.5.13. It behaves additively on short exact sequences, see Lemma B.5.14. This yields

$$\begin{aligned} \chi_k(\mathcal{O}_X) &= \chi_k(\mathcal{FG}) + \chi_k(\mathcal{O}_X/\mathcal{FG}) \quad \text{and} \\ \chi_k(\mathcal{F}) &= \chi_k(\mathcal{FG}) + \chi_k(\mathcal{F}/\mathcal{FG}). \end{aligned}$$

Now subtracting the latter from the former, we deduce

$$\chi_k(\mathcal{O}_X) - \chi_k(\mathcal{F}) = \chi_k(\mathcal{O}_X/\mathcal{FG}) - \chi_k(\mathcal{F}/\mathcal{FG}).$$

Next we prove that $\chi_k(\mathcal{O}_X/\mathcal{FG}) - \chi_k(\mathcal{F}/\mathcal{FG})$ is equal to $\deg_k \mathcal{F}$. Note that all $\mathcal{O}_X$, $\mathcal{F}$

and $\mathcal{FG}$ are $\mathcal{O}_X$-ideals. Then, by Corollary C.3.3, we obtain

$$\begin{aligned}\chi_k(\mathcal{O}_X/\mathcal{FG}) - \chi_k(\mathcal{F}/\mathcal{FG}) &= \sum_{P\in X} \dim_k \mathcal{O}_{X,P}/(\mathcal{FG})_P - \dim_k \mathcal{F}_P/(\mathcal{FG})_P \\ \text{Lemma 3.1.16} \rightsquigarrow &= \sum_{P\in X} \dim_k \mathcal{O}_{X,P}/\mathcal{F}_P\mathcal{G}_P - \dim_k \mathcal{F}_P/\mathcal{F}_P\mathcal{G}_P.\end{aligned}$$

Now since $\mathcal{G}$ is invertible, its stalks are principal $\mathcal{O}_{X,P}$-ideals $\mathcal{G}_P = a_P\mathcal{O}_{X,P}$ with $a_P \in \mathcal{O}_{X,P}$ and hence, by the definition of the degree of $\mathcal{O}_{X,P}$--ideals, we have

$$\begin{aligned}\dim_k \mathcal{O}_{X,P}/\mathcal{F}_P\mathcal{G}_P - \dim_k \mathcal{F}_P/\mathcal{F}_P\mathcal{G}_P &= \dim_k \mathcal{O}_{X,P}/a_P\mathcal{F}_P - \dim_k \mathcal{F}_P/a_P\mathcal{F}_P \\ &= \deg_k \mathcal{F}_P\end{aligned}$$

where the latter is the degree of $\mathcal{F}_P$ as an $\mathcal{O}_{X,P}$-ideal. Finally, this gives

$$\chi_k(\mathcal{O}_X/\mathcal{FG}) - \chi_k(\mathcal{F}/\mathcal{FG}) = \sum_{P\in X} \deg_k \mathcal{F}_P = \deg_k \mathcal{F}$$

as asserted. □

Corollary C.4.5. *Let $\mathcal{F} \leq \mathcal{G}$ be two $\mathcal{O}_X$-ideals. Then $\deg_k \mathcal{G} = \deg_k \mathcal{F} - \dim_k H^0(X, \mathcal{G}/\mathcal{F})$. In particular, $\deg_k \mathcal{F} \geq \deg_k \mathcal{G}$.*

Proof. By assumption, we have a short exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{G}/\mathcal{F} \longrightarrow 0$$

which together with Lemma B.5.14 provides $\chi(\mathcal{G}) = \chi(\mathcal{F}) + \chi(\mathcal{G}/\mathcal{F})$. Multiplying this equation with -1 and then adding $\chi(\mathcal{O}_X)$ on both sides, together with Corollary C.3.3 provides

$$\chi(\mathcal{O}_X) - \chi(\mathcal{G}) = \chi(\mathcal{O}_X) - \chi(\mathcal{F}) - \dim_k H^0(X, \mathcal{G}/\mathcal{F})$$

which is equivalent to

$$\deg_k \mathcal{G} = \deg_k \mathcal{F} - \dim_k H^0(X, \mathcal{G}/\mathcal{F}).$$ □

As is turns out, $\mathcal{O}_X$-ideals with positive degree on integral schemes do not have non-zero global sections.

Lemma C.4.6. *Let X be an integral and projective curve over k. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. If $\deg_k \mathcal{F} > 0$, then $\mathcal{F}(X) = 0$.*

Proof. Every non-zero global section f of $\mathcal{F}$ corresponds to a non-zero element of $\mathcal{K}_X(X) = F$, the function field of X. Thus $f\mathcal{O}_X$ is an invertible $\mathcal{O}_X$-ideal with $f\mathcal{O}_X \leq \mathcal{F}$. By Corollary C.4.5, this provides

$$\deg_k \mathcal{F} = \deg_k f\mathcal{O}_X - \dim_k H^0(X, \mathcal{F}/f\mathcal{O}_X).$$

By Lemma 3.1.12, we have $\deg_k f\mathcal{O}_X = 0$ and whence $\deg_k \mathcal{F} = -\dim_k H^0(X, \mathcal{F}/f\mathcal{O}_X) \leq 0$. Hence if $\deg_k \mathcal{F} > 0$, then we necessarily have $H^0(X, \mathcal{F}) = 0$. □

Proposition C.1.26 has shown that the degree of the product of two R-ideals is additive if one of the factors is invertible. This generalises to $\mathcal{O}_X$-ideals.

Lemma C.4.7. *Let $\mathcal{F}, \mathcal{G}$ be two $\mathcal{O}_X$-ideals such that for all closed points $P \in X$ at least one of the stalks of $\mathcal{F}$ or $\mathcal{G}$ is an invertible $\mathcal{O}_{X,P}$-ideal. For instance, this is the case if one of $\mathcal{F}$ and $\mathcal{G}$ is invertible. Then $\deg_k \mathcal{FG} = \deg_k \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} = \deg_k \mathcal{F} + \deg_k \mathcal{G}$.*

Proof. For all $P \in X$ we have $(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})_P \cong (\mathcal{F}\mathcal{G})_P = \mathcal{F}_P\mathcal{G}_P$. By assumption, $\mathcal{F}_P$ or $\mathcal{G}_P$ is invertible and hence Proposition C.1.26 provides that $\deg_k \mathcal{F}_P\mathcal{G}_P = \deg_k \mathcal{F}_P + \deg_k \mathcal{G}_P$ for all closed $P \in X$. By definition, this provides

$$\begin{aligned}\deg_k \mathcal{F}\mathcal{G} &= \sum_{P\in X,\ P \text{ cl.}} \deg_k \mathcal{F}_P\mathcal{G}_P \\ &= \sum_{P\in X,\ P \text{ cl.}} \deg_k \mathcal{F}_P + \deg_k \mathcal{G}_P \\ &= \sum_{P\in X,\ P \text{ cl.}} \deg_k \mathcal{F}_P + \sum_{P\in X,\ P \text{ cl.}} \deg_k \mathcal{G}_P \\ &= \deg_k \mathcal{F} + \deg_k \mathcal{G}.\end{aligned}$$

□

Lemma C.4.8. *For any $D \in \operatorname{Div}(X)$ we have $\deg_k D = -\deg_k \mathcal{O}_X(D)$.*

Proof. We refer the reader to [Liu02] for the definition of the degree of Cartier divisors. The degree of a divisor $D \in H^0\left(X, \mathcal{K}_X^\times\right)$ with $D_P = a_P/b_P$, $a_P, b_P \in \mathcal{O}_{X,P}$, is defined as

$$\deg_k D = \sum_{P\in X} (\operatorname{len}_{\mathcal{O}_{X,P}}(\mathcal{O}_{X,P}/a_P) - \operatorname{len}_{\mathcal{O}_{X,P}}(\mathcal{O}_{X,P}/b_P)) \cdot [\kappa(P) : k]$$

where $\kappa(P)$ denotes the residue class field of $\mathcal{O}_{X,P}$. However, by Lemma B.4.48, we have

$$\operatorname{len}_{\mathcal{O}_{X,P}}(\mathcal{O}_{X,P}/a_P) \cdot [\kappa(P) : k] = \dim_k \mathcal{O}_{X,P}/a_P$$

and since b_P is a wedging element for $D_P\mathcal{O}_{X,P}$, Lemma C.1.20 provides

$$\begin{aligned}\deg_k D &= \sum_{P\in X} \dim_k a_P\mathcal{O}_{X,P} - \dim_k b_P\mathcal{O}_{X,P} \\ &= \sum_{P\in X} \deg_k a_P\mathcal{O}_{X,P} - \deg_k b_P\mathcal{O}_{X,P} \\ &= \sum_{P\in X} \deg_k D_P\mathcal{O}_{X,P}.\end{aligned}$$

Now since $\mathcal{O}_X(D)_P \cong D_P^{-1}\mathcal{O}_{X,P}$, see Proposition 3.1.27, we therefore obtain

$$\begin{aligned}\deg_k \mathcal{O}_X(D) &= \sum_{P\in X} \deg_k \mathcal{O}_X(D)_P \\ &= \sum_{P\in X} -\deg_k D_P\mathcal{O}_{X,P} \\ &= -\deg_k D.\end{aligned}$$

□

Remark C.4.9. The degree of an invertible sheaf $\mathcal{L}$ is in [Liu02, Definition 7.29] defined as $\chi(\mathcal{L}) - \chi(\mathcal{O}_X)$ and thus the only difference to our definition of the degree of $\mathcal{O}_X$-ideals is the sign. △

Lemma C.4.10. *Let $X = \operatorname{Spec}(R)$ be an affine curve of finite residual-type over k. Then every $\mathcal{O}_X$-ideal $\mathcal{F}$ is given by some $M^\sim$ where M is an R-ideal. Conversely, every R-ideal M provides an $\mathcal{O}_X$-ideal $M^\sim$. This provides an equivalence of categories:*

$$\begin{array}{rcl} \boldsymbol{\mathcal{O}_X\text{-ideals}} & \to & \boldsymbol{R\text{-ideals}} \\ \mathcal{F} & \mapsto & \mathcal{F}(X) \\ M^\sim & \leftarrow\!\shortmid & M \end{array}$$

Proof. Since R is noetherian, by [Sta18, Tag 01OW], $X = \operatorname{Spec}(R)$ is locally noetherian. By [Har77, II, 5.5], there is an equivalence of the category of R-modules and the category of quasi-coherent $\mathcal{O}_X$-modules given by $M \mapsto M^\sim$ for any R-module M and its inverse $\mathcal{F} \mapsto \mathcal{F}(X)$ for any $\mathcal{O}_X$-module $\mathcal{F}$.

Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\mathcal{F} \leq \mathcal{K}_X$ implies $\mathcal{F}(X) \subseteq \mathcal{K}_X(X) = \operatorname{Frac}(R)$ since X is affine, see Proposition B.2.2. Since $\mathcal{F}$ is coherent and X locally noetherian, $\mathcal{F}(X)$ is finitely generated, see [Liu02, 5.1.11]. Moreover, we have $\mathcal{F}_P \cong \mathcal{F}(X)_P$ and thus $\mathcal{F}(X)$ is invertible at the minimal prime ideals of R since $\mathcal{F}$ is invertible at the generic points of X. Whence $\mathcal{F}(X)$ is an R-ideal such that $\mathcal{F} \cong \mathcal{F}(X)^\sim$.

Conversely, if M is an R-ideal, then $M \subseteq \operatorname{Frac}(R)$ and M is invertible at the minimal prime ideals of R. We claim that this implies that $M^\sim$ is an $\mathcal{O}_X$-submodule of $\mathcal{K}_X$: First of all, the basic affine open subsets $U = D(f)$ for some $f \in R$ form a base of the Zariski topology on X. By [GW10, 7.12], we have that $M^\sim(D(f)) = M_f$ defines a sheaf on the base of basic open subsets of X. By Remark B.1.32, this is enough to provide a sheaf $M^\sim$ of $\mathcal{O}_X$-modules on X such that $M^\sim(D(f)) = M_f$. Now by Proposition B.2.2, for any $U = D(f)$ we have $\mathcal{K}_X(U) = \operatorname{Frac}(R_f)$ and $\mathcal{K}_X$ is quasi-coherent on X. That is, $K := \mathcal{K}_X(X) = \operatorname{Frac}(R)$ satisfies $\mathcal{K}_X(U) \cong K_f$ and thus, again by [GW10, 7.12], $K^\sim$ defines a sheaf on the base of basic open subsets of X. However, we obviously have $M \subseteq K$ and thus [Sta18, Tag 009U] provides that $M^\sim \leq K^\sim \cong \mathcal{K}_X$ is an $\mathcal{O}_X$-submodule of $\mathcal{K}_X$. Since M is finitely generated and X locally noetherian, by [Liu02, 5.1.11], $M^\sim$ is coherent. Moreover, since M is invertible at minimal primes of R, $M^\sim$ is invertible at the generic points of X. Therefore, $M^\sim$ is an $\mathcal{O}_X$-ideal. □

Corollary C.4.11. *Let $X = \operatorname{Spec}(R)$ be an affine curve of finite residual-type over k. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\deg_k \mathcal{F} = \deg_k \mathcal{F}(X)$ where the former denotes the degree of the $\mathcal{O}_X$-ideal $\mathcal{F}$and the latter the degree of the R-ideal $\mathcal{F}(X)$.*

Proof. By Lemma C.4.10, we have $\mathcal{F} \cong \mathcal{F}(X)^\sim$ and thus $\mathcal{F}_P \cong \mathcal{F}(X)_P$ which then provides the equality due to the definitions of the degree of $\mathcal{O}_X$-ideals Definition C.4.1 and the degree of R-ideals Definition C.1.14. □

Corollary C.4.12. *Let X be a cover of $\mathbb{P}^1_k$ and $V \in \{V_0, V_\infty\}$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then*

$$\deg_k \mathcal{F}_{|V} = \deg_k \mathcal{F}(V) \quad \text{and} \quad \deg_k \mathcal{F}_{|S} = \deg_k \mathcal{F}_{|S}(S).$$

Proof. Due to Lemma 2.2.20, we have that V is an affine (Cohen-Macaulay) curve over k. In particular, V is an affine curve of finite residual-type over k. Moreover, $\mathcal{F}_{|V}$ is an $\mathcal{O}_V$-ideal, see Example 3.1.14. Hence, by Corollary C.4.11, the first identity follows. Moreover, by Proposition 3.2.28, we have that $\mathcal{F}_{|S}$ is an $\mathcal{O}_S$-ideal. By Lemma 2.2.20, we know that $\mathcal{O}_S$ is an affine curve of finite residual-type over k. Therefore, again by Corollary C.4.11, the second identity follows. □

An immediate consequence of Corollary C.4.12 is the following statement which enables us to compute the degree of an $\mathcal{O}_X$-ideal locally on the affine schemes V_0 and S.

Corollary C.4.13. *Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then*

$$\deg_k \mathcal{F} = \deg_k \mathcal{F}(V_0) + \deg_k \mathcal{F}(S).$$

Proof. By Proposition 3.2.28, we have for all closed points $P \in S_0$ the identity $(\mathcal{F}_{|S})_P =$

$\mathcal{F}_P$ and thus we obviously have

$$\begin{aligned}\deg_k \mathcal{F} = \sum_{P\in X_0} \deg_k \mathcal{F}_P &= \sum_{P\in (V_0)_0} \deg_k \mathcal{F}_P + \sum_{P\in S_0} \deg_k \mathcal{F}_P \\ &= \sum_{P\in (V_0)_0} \deg_k (\mathcal{F}_{|V_0})_P + \sum_{P\in S_0} \deg_k (\mathcal{F}_{|S})_P \\ &= \deg_k \mathcal{F}_{|V_0} + \deg_k \mathcal{F}_{|S}\end{aligned}$$

which then together with Corollary C.4.12 provides the assertion. □

We shall note that in general, the degree of $\mathcal{O}_X$-ideals does not behave additively with regards to the restriction to irreducible components. But if the irreducible components are also the connected components (i.e. they are disjoint) or if the respective $\mathcal{O}_X$-ideal is invertible, then the degree does indeed behave additively.

Remark C.4.14. The proof in the case of disjoint irreducible components is trivial since we can compute the degree as the sum over all degree of stalks and no such stalk appears multiple times due to the disjointness. △

Proposition C.4.15. *Let X be a reduced and proper scheme over a field k. Let $X_1, \dots, X_m$ be all of X irreducible components. Let $\mathcal{F}$ be an invertible sheaf on X. Then* $\deg_k \mathcal{F} = \sum_{i=1}^m \deg_k \mathcal{F}_{|X_i}$.

Proof. We denote by $\tau_i : X_i \to X$ the closed immersion corresponding to the closed subscheme X_i. The injection $\mathcal{O}_X \to \bigoplus_{i=1}^m (\tau_i)_* \mathcal{O}_{X_i}$ from Definition B.3.1 provides, due to Proposition B.3.3, an exact sequence

$$0 \longrightarrow \mathcal{O}_X \longrightarrow \bigoplus_{i=1}^m (\tau_i)_* \mathcal{O}_{X_i} \longrightarrow \mathscr{S} \longrightarrow 0, \tag{4:7}$$

where $\mathscr{S}$ is a skyscraper sheaf by Lemma B.5.3. Since $\mathcal{F}$ is invertible, it is flat, see [Liu02, 5.2.31 b], and hence tensoring sequence (4:7) with $\mathcal{F}$ provides an exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{F} \longrightarrow \bigoplus_{i=1}^m (\tau_i)_* \mathcal{F}_{|X_i} \longrightarrow \mathscr{S} \otimes_{\mathcal{O}_X} \mathcal{F} \longrightarrow 0.$$

Now applying the Euler characteristic, see Lemma B.5.14, yields

$$\sum_{i=1}^m \chi(X, (\tau_i)_* \mathcal{F}_{|X_i}) = \chi(X, \mathcal{F}) + \chi(X, \mathscr{S} \otimes_{\mathcal{O}_X} \mathcal{F}).$$

By Lemma B.5.15 (iv), we have $\chi(X, \mathscr{S} \otimes_{\mathcal{O}_X} \mathcal{F}) = \chi(X, \mathscr{S})$ and, by Lemma B.5.12, we deduce

$$\chi(X, (\tau_i)_* \mathcal{F}_{|X_i}) = \chi(X_i, \mathcal{F}_{|X_i}),$$

which together provides

$$\sum_{i=1}^m \chi(X_i, \mathcal{F}_{|X_i}) = \chi(X, \mathcal{F}) + \chi(X, \mathscr{S}). \tag{4:8}$$

Applying the Euler characteristic to sequence in (4:7) and using again the additivity on short exact sequences, see Lemma B.5.14, we obtain

$$\sum_{i=1}^m \chi(X_i, \mathcal{O}_{X_i}) = \chi(X, \mathcal{O}_X) + \chi(X, \mathscr{S}). \tag{4:9}$$

Now subtracting $\sum_{i=1}^m \chi(X_i, \mathcal{F}_{|X_i})$ from Eq. (4:9) and using Eq. (4:8), we deduce

$$\begin{aligned}\sum_{i=1}^m \chi(X_i, \mathcal{O}_{X_i}) - \sum_{i=1}^m \chi(X_i, \mathcal{F}_{|X_i}) &= \chi(X, \mathcal{O}_X) + \chi(X, \mathscr{S}) - (\chi(X, \mathcal{F}) + \chi(X, \mathscr{S})) \\ &= \chi(X, \mathcal{O}_X) - \chi(X, \mathcal{F})\end{aligned}$$

which implies

$$\sum_{i=1}^m \deg_k \mathcal{F}_{|X_i} = \sum_{i=1}^m \chi(X_i, \mathcal{O}_{X_i}) - \chi(X_i, \mathcal{F}_{|X_i}) = \chi(X, \mathcal{O}_X) - \chi(X, \mathcal{F}) = \deg_k \mathcal{F}. \qquad \square$$

Remark C.4.16. There is a proof of this fact in [Liu02, 7.5.7] where the degree of $\mathcal{L}$, as already mentioned in Remark C.4.9, is set as $\deg_k \mathcal{L} = \chi_k(X, \mathcal{L}) - \chi_k(X, \mathcal{O}_X)$ in contrast to our definition, see Definition C.1.14 and Lemma C.4.4, $\deg_k \mathcal{F} = \chi_k(X, \mathcal{O}_X) - \chi_k(X, \mathcal{F})$. Moreover, in [Liu02, 7.5.7] X need not be reduced, but then the equation becomes

$$\deg_k \mathcal{F} = \sum_{i=1}^m d_i \deg_k \mathcal{F}_{|X_i}$$

where $d_i = \operatorname{len}_{\mathcal{O}_{X,\eta_i}}(\mathcal{O}_{X,\eta_i})$ is the minimal power n_i such that the maximal ideal $\mathfrak{m}_i$ satisfies $\mathfrak{m}_i^{n_i} = 0$ in $\mathcal{O}_{X,\eta_i}$ (which is equal to one if X is reduced and thus $\mathcal{O}_{X,\eta_i}$ a field, see Lemma B.4.29). Also note that the author endows the components X_i with the reduced subscheme structure. $\triangle$

Remark C.4.17. Another proof that only works locally can be derived using Lemma C.1.28 which shows the respective statement for the case of R-ideals where R is local and reduced. In that case we only need that X is reduced at closed points since computing the degree can be done only using closed points, see Definition 3.1.13 and Corollary C.1.22. $\triangle$

In the following proposition we collect the most important properties of the degree of $\mathcal{O}_X$-ideals we have stated above in the special case of divisors on covers of $\mathbb{P}^1_k$.

Proposition C.4.18. *Let X be a curve of finite residual-type over k with irreducible components $X_1, \dots, X_m$. Let $D, E \in \operatorname{Div}(X)$. Then the following assertions are true.*

(i) Let X be affine. Then $\deg_k(D) = -\deg_k \mathcal{O}_X(D)(X)$.

(ii) Let X be a cover of $\mathbb{P}^1_k$. Then

$$\deg_k D = \deg_k D_{|V_0} + \deg_k D_{|S} = \deg_k D_{|V_0} + \sum_{i=1}^m \deg_k D_{|S_i}.$$

In particular, if $\deg_k D = 0$, then

$$\deg_k D_{|V_0} = -\deg_k D_{|S} = -\sum_{i=1}^m \deg_k D_{|S_i}.$$

(iii) $\deg_k D = \sum_{i=1}^m \deg_k D_{|X_i}$ and if X is a cover of $\mathbb{P}^1_k$, then

$$\deg_k D = \sum_{i=1}^m \deg_k D_{|X_i} = \sum_{i=1}^m \deg_k D_{|V_{i,0}} + \deg_k D_{|S_i}.$$

(iv) $\deg_k(D + E) = \deg_k D + \deg_k E$.

Proof. First of all, we will use the fact $\deg_k D = -\deg_k \mathcal{O}_X(D)$, see Lemma C.4.8. Then (i) follows from Corollary C.4.11. The former equality from (ii) is the combination of Corollaries C.4.12 and C.4.13 and the latter is due to the fact that S is the disjoint union of the S_i, see Proposition 5.5.3. The first equality of (iii) is due to Proposition C.4.15 and the second one is the result of applying (ii) to $D_{|X_i}$ since X_i is a cover of $\mathbb{P}^1_k$, see Proposition 2.2.5. Assertion (iv) follows from Lemma C.4.7. □

Appendix D

Properties of Covers of $\mathbb{P}^1_k$

In this chapter we provide some of the fundamental properties of covers of $\mathbb{P}^1_k$. For instance, due to the lack of reference, we provide a proof of the existence of a finite morphism onto $\mathbb{P}^n_k$ for every projective scheme over k of dimension n. We deduce from this that for every projective scheme X over k of dimension one there is a finite and surjective morphism to $\mathbb{P}^1_k$ which additionally is flat if and only if X is Cohen-Macaulay. Moreover, such morphisms send closed points to closed points and generic points to generic points.

The chapter is organised as follows: In Section D.1 we provide the existence of the finite morphism onto $\mathbb{P}^1_k$ and show some of its properties. In Section D.2 we provide a wide range of properties of covers of $\mathbb{P}^1_k$ that will be used frequently throughout this thesis.

D.1 Finite Morphism to Projective Space

To prove the existence of a finite morphism onto projective space, we need some existence lemmas for global sections of ample sheaves whose zero loci have codimension one.

Proposition D.1.1. *Let X be a proper scheme over k where k is a field. Let $\mathcal{L}$ be an ample invertible sheaf on X and let $s \in \mathcal{L}(X)$ be a section of $\mathcal{L}$. Then $X_s = \{P \in X \mid s_P \mathcal{O}_{X,P} = \mathcal{L}_P\}$ is an affine open subset of X.*

Proof. By assumption, there is some $m > 0$ such that $\mathcal{L}^{\otimes m}$ is very ample for a closed immersion $\phi : X \to \mathbb{P}^n_k$. Then ϕ corresponds to global sections $s_0, \dots, s_n \in \mathcal{L}^{\otimes m}(X)$. We show that the morphism $\psi : X \to \mathbb{P}^{n+1}_k$ given by the sections $s^{\otimes m}, s_0, \dots, s_n \in \mathcal{L}^{\otimes m}(X)$ is a closed immersion. Let $Y := \mathbb{P}^{n+1}_k \setminus \{(1 : 0 : \dots : 0)\}$ and consider the morphism $p : Y \to \mathbb{P}^n_k$ given by forgetting the first coordinate which was due to $s^{\otimes m}$. Then $\phi = p \circ \psi$. Let $\mathcal{P}$ be a property of morphisms of schemes such that a closed immersions satisfy $\mathcal{P}$ and $\mathcal{P}$ is stable under composition and base change. Let $f : X \to Y$ and $g : Y \to Z$ be morphisms of schemes such that g is separated and $g \circ f$ satisfies $\mathcal{P}$. Then [Liu02, 3.3.15] provides that f satisfies $\mathcal{P}$. By [Sta18, Tag 01JY and Tag 02V0] and [Sta18, Tag 01KU and Tag 01KU], being separated and a closed immersion are examples for $\mathcal{P}$. Thus it suffices to show that p is separated. By [Sta18, Tag 0DVA], the inclusion $Y \hookrightarrow \mathbb{P}^{n+1}_k$ is separated and hence the composition $Y \hookrightarrow \mathbb{P}^{n+1}_k \to \operatorname{Spec}(k)$ of separated morphisms is separated. Therefore, we may use [Liu02, 3.3.15] again on $Y \xrightarrow{p} \mathbb{P}^n_k \to \operatorname{Spec}(k)$ to complete the proof. □

Lemma D.1.2 ([GW10] 13.49)**.** *Let X be a quasi-compact and quasi-separated scheme. Let $\mathcal{L}$ be an ample $\mathcal{O}_X$-module. For every finite subset E of X and open neighborhood W of E there exists an $n > 0$ and a section $s \in \mathcal{L}^{\otimes n}(X)$ such that X_s is affine and $E \subseteq X_s \subseteq W$.*

Corollary D.1.3. *Let X be an affine scheme. Then for any finite subset E of X and open neighborhood W of E there exists $h \in \mathcal{O}_X(X)$ such that $E \subseteq D(h) \subseteq W$.*

Proof. Note that an affine scheme is quasi-separated and quasi-compact, see [Sta18, Tag 01KN] and [GW10, 2.5]. In particular, any affine scheme is quasi-affine, see the definition in [Sta18, Tag 01P6]. Moreover, by [Sta18, Tag 01QE], a scheme X is quasi-affine if and only if $\mathcal{O}_X$ is ample. Hence we may apply Lemma D.1.2 to X and $\mathcal{L} = \mathcal{O}_X$ which clearly provides the assertion. □

Corollary D.1.4. *Let X be a projective scheme over an affine base scheme $\operatorname{Spec}(R)$. Then for any finite subset E of X and open neighborhood W of E there exists an affine open subset $U \subseteq X$ such that $E \subseteq U \subseteq W$.*

Proof. First of all, every affine scheme has an ample line bundle: Let $\mathcal{L}$ be an invertible sheaf on an affine scheme X. Let $\mathcal{F}$ be a quasi-coherent sheaf on X. Then $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{F}$ is quasi-coherent by [Liu02, 5.1.12] and quasi-coherent sheaves on affine schemes are obviously generated by global sections. Hence $\mathcal{L}$ is ample on X. Hence we may apply [Sta18, Tag 0B45] which tells us that any projective scheme $X \to S$ over an affine base S has an ample invertible sheaf. By [Sta18, Tag 0B45], we see that X is proper and a fortiori separated. By [Sta18, Tag 04XU], every universally closed morphism is quasi-compact. Hence every proper scheme and thus X is quasi-compact. Therefore the requirements of Lemma D.1.2 are met and we can deduce the assertion. □

Proposition D.1.5. *Let X be a noetherian scheme and Z a non-empty, closed subset of X. Let $\mathcal{L}$ be an ample invertible sheaf on X. Then there exists an $n > 0$ and a section $s \in \mathcal{L}^{\otimes n}(X)$ such that s does not vanish identically on any irreducible component of Z.*

Proof. Since X is noetherian and Z is closed, Z decomposes into finitely many, distinct irreducible components $Z_1, \dots Z_m$ which are closed in X. For each i there is $x \in X_i \setminus \cup_{j \neq i}^m Z_j$. As a noetherian scheme, X is quasi-compact by definition and quasi-separated by [Sta18, Tag 01OY]. We apply Lemma D.1.2 with $E = \{x\}$ and $W = X \setminus \cup_{j \neq i}^m Z_j$. This gives $s_i \in \mathcal{L}^{\otimes n_i}(X)$ for some $n_i > 0$ such that $x \in X_{s_i} \subseteq W$. Now s_i vanishes at $y \in X$ if and only if $y \notin X_{s_i}$, so s_i vanishes on every Z_j but not on X_i. Then for $n = n_1 \cdots n_m$, the section $s = \sum_{i=1}^m s_i^{\otimes (n/n_i)} \in \mathcal{L}^{\otimes n}(X)$ satisfies the assertion. □

Theorem D.1.6. *Let X be a projective scheme of dimension n over the field k. Then there exists a finite morphism $\pi : X \to \mathbb{P}_k^n$.*[1]

Proof. Let $n = \dim(X)$. We will show that there is an ample invertible sheaf $\mathcal{L}$ and global sections $s_0, \dots, s_n \in \mathcal{L}(X)$ which will define the desired finite morphism $X \to \mathbb{P}_k^n$.

As a first step we now prove by induction that for each i with $0 \leq i \leq n$ there exists an ample invertible sheaf $\mathcal{L}_i$ and global sections $s_0, \dots, s_i$ such that the intersection $Z_i := \bigcap_{j=0}^i V(s_j)$ of their zero loci satisfies $\operatorname{codim}(X_i, X) = i + 1$. Then $Z_n = \emptyset$ and hence $\bigcup_{i=0}^n X_{s_i} = X$. By assumption, there is an ample invertible sheaf $\mathcal{L}_0$ corresponding to a closed immersion $X \to \mathbb{P}_k^N$ for $N > 0$. The case $i = 0$ is provided by Proposition D.1.5. Now assume there is an ample invertible sheaf $\mathcal{L}_{i-1}$ on X and global sections $s_0, \dots, s_{i-1} \in \mathcal{L}_{i-1}(X)$. Then, by Proposition D.1.5, there is $s_i \in \mathcal{L}_{i-1}^{\otimes m}(X)$ for some $m > 0$ such that s_i does not vanish identically on any irreducible component of Z_{i-1}. Thus $\operatorname{codim}(Z_{i-1} \cap V(s_i), X) \geq \operatorname{codim}(Z_{i-1}, X) + 1$. Moreover, equality holds by Krull's Hauptidealsatz, see [Liu02, 2.5.12]. The ample invertible sheaf $\mathcal{L}_{i-1}^{\otimes m}$ and its sections $s_0^{\otimes m}, \dots, s_{i-1}^{\otimes m}, s_i$ complete the induction.

The first step provides an ample invertible sheaf $\mathcal{L}$ and $s_0, \dots, s_n \in \mathcal{L}(X)$ such that $X = \bigcup_{i=0}^n X_{s_i}$. Therefore $\mathcal{L}$ is globally generated by the s_i. From [Liu02, 5.1.31]

[1] Thanks to Kiran Kedlaya for his useful input.

we obtain a morphism of k-schemes $\pi : X \to \mathbb{P}^n_k$ such that $X_{s_i} = \pi^{-1}(U_i)$, $U_i = \operatorname{Spec}(k[T_0/T_i, \dots, T_n/T_i])$ and $\pi^\#(U_i)(T_j/T_i) = s_j/s_i$. We will show that this morphism is finite by showing that it is affine and projective, see [GW10, 13.77] for the equivalence of these properties. By Proposition D.1.1, the X_{s_i} are affine and thus, by [GW10, 12.1], it follows that π is affine. Since X is projective over k, π followed by the structure morphism of $\mathbb{P}^n_k$ is projective. The structure morphism of $\mathbb{P}^n_k$ is separated and thus, by [Liu02, 3.3.32], we obtain that π is projective. □

We will see that the finite morphism constructed above will be surjective and, moreover, flat if we additionally require X to be Cohen-Macaulay.

Proposition D.1.7. *Let X, Y be two schemes of the same finite dimension and Y irreducible. Then every finite morphism $\pi : X \to Y$ is surjective.*

Proof. We can restrict π to a morphism $\psi : X \to Z$, where Z is the scheme theoretic image of π. Since π is finite and $Z \to Y$ is closed and separated, ψ is also finite. Moreover, finite morphisms are closed, so $\pi(X)$ is a closed subset of Y, thus $Z = \pi(X)$ and ψ is surjective. Finite morphisms are also integral, so [Sta18, Tag0ECG] applied to ψ provides $\dim(Z) = \dim(X)$. By assumption, $\dim(Z) = \dim(Y)$ and Y irreducible and therefore we finally obtain $Z = Y$. □

Corollary D.1.8. *Let X be a proper scheme of dimension one over k. Then there exist a finite and surjective morphism $\pi : X \to \mathbb{P}^1_k$. If X is additionally Cohen-Macaulay, then any finite morphism to $\mathbb{P}^1_k$ is flat.*

Proof. First of all, due to Corollary B.5.19, X is projective over k. The existence of π is then given by Theorem D.1.6 and Proposition D.1.7. The second assertion is a consequence of the so called *Miracle Flatness Theorem*, see [GW10, 14.128]. □

Remark D.1.9. Let X be a projective scheme over k of dimension n with a finite and surjective morphism $\pi : X \to \mathbb{P}^n_k$ as in Theorem D.1.6. Let Z be one of its irreducible components with closed immersion $i : Z \to X$. Then $\pi \circ i : Z \to \mathbb{P}^n_k$ is also finite. But if $\dim Z < n$, then $\pi \circ i$ cannot be surjective. Therefore, if X is of pure dimension n, then every finite and surjective morphism from X to $\mathbb{P}^n_k$ provides such a morphism for every of its irreducible components. △

Proposition D.1.10. *Let $f : X \to Y$ be a morphism of projective curves over k. Then f sends closed points to closed points. It also sends generic points to generic points if and only if it is finite.*

Proof. By [Liu02, 7.3.10], a morphism of projective curves over k is finite if and only if it sends generic points to generic points.

Since the statement is of local nature, it is enough the prove the statement about the closed points for the k-algebra homomorphisms induced by an affine open cover of Y. That is, for any affine open $U = \operatorname{Spec}(A)$ of Y, we know that $V = f^{-1}(U)$ is again affine with $V = \operatorname{Spec}(B)$ and then $f_{|V}$ is given by a homomorphism of finite k-algebras $A \to B$. Therefore it is enough to prove that the preimage of a maximal ideal of B under $A \to B$ is a maximal ideal of A. This statement is Corollary B.4.2 of the Nullstellensatz Theorem B.4.1. □

D.2 Miscellaneous Properties

Lemma D.2.1. *Every non-empty affine open subset of a curve over k has infinitely many points. In particular, every curve over k has infinitely many points.*

Proof. Let $U \subseteq X$ be an affine open subset of X. Since X is of finite type over k, i.e. the structure morphism $X \to \operatorname{Spec}(k)$ is of finite type, by [Sta18, Tag 01T2], we have that $k \to \mathcal{O}_X(U) =: R$ is a ring map of finite type. That is, R is a finitely generated k-algebra and thus, by [Sta18, Tag 00OY], we obtain a subring $S \subseteq R$ such that $S \cong k[x]$ and the ring extension R/S is finite. In particular, every prime ideal of S lies under some and at most under finitely many prime ideals of R. Thus R has at least as many primes as S does. But Euclid's proof of the existence of infinitely many primes in $\mathbb{Z}$ extends to the case of S and thus yields the assertion. □

Corollary D.2.2. *Let X be a cover of $\mathbb{P}^1_k$. Then each $V_{i,0}$ and $V_{i,\infty}$ has infinitely many closed points. In particular, each irreducible component of X has infinitely many closed points.*

We recall the definition of the set where a global section of an invertible sheaf does generate the stalk of that sheaf. Let $\mathcal{F}$ be an invertible sheaf on the scheme X. Let $s \in \mathcal{F}(X)$. Then we set

$$X_s = \{x \in X \mid \mathcal{F}_x = s_x \mathcal{O}_{X,x}\}.$$

If X is affine and $\mathcal{F} = \mathcal{O}_X$, then $X_s = D(s)$.

Proposition D.2.3. *Let X be a cover of $\mathbb{P}^1_k$ with finite morphism $\pi : X \to \mathbb{P}^1_k$. The pole divisor $(x)_\infty$ of x (given by $\mathcal{O}_{\mathbb{P}^1}(U_0) = k[x]$) is ample.*

Proof. By [Liu02, 5.1.35], it suffices to show that there are global sections $s_1, \dots, s_r \in \mathcal{O}_X((x)_\infty)(X)$ such that X_{s_i} are affine subsets of X which cover X. By Lemma 4.2.8, we have

$$\mathcal{O}_X((x)_\infty)(X) = \mathcal{O}_X((x)_\infty)(V_0) \cap \mathcal{O}_X((x)_\infty)(V_\infty) = R_0 \cap xR_\infty$$

where the intersection takes place in $\operatorname{Frac}(R_0) \cong \operatorname{Frac}(R_\infty)$. Now π implies that

$$k[x] \cap xk[x^{-1}] \subseteq R_0 \cap xR_\infty$$

and we claim that $x, x-1 \in k[x] \cap xk[x^{-1}]$ satisfy the desired properties. By definition, we have

$$\mathcal{O}_X((x)_\infty)_P = \begin{cases} \mathcal{O}_{X,P}, & P \in V_0 \\ x\mathcal{O}_{X,P}, & P \in S \end{cases}$$

and thus $X_x = \{P \in V_0 \mid \mathcal{O}_{X,P} = x\mathcal{O}_{X,P}\} \cup \{P \in S \mid x\mathcal{O}_{X,P} = x\mathcal{O}_{X,P}\}$. The former set is the set of points where x does not vanish on V_0, that is, the preimage of the basic open subset $D_{U_0}(x)$ which is $V_0 \setminus \pi^{-1}(P_0)$. The latter is all of S. Hence

$$X_x = V_0 \setminus \pi^{-1}(P_0) \cup S = V_0 \setminus \pi^{-1}(P_0) \cup V_\infty = X \setminus \pi^{-1}(P_0) = \pi^{-1}(D_+(x_0)) = V_\infty$$

is affine. Completely analogous we obtain

$$X_{x-1} = \{P \in V_0 \mid \mathcal{O}_{X,P} = (x-1)\mathcal{O}_{X,P}\} \cup \{P \in S \mid x\mathcal{O}_{X,P} = (x+1)\mathcal{O}_{X,P}\}$$

where the former set is the set where $x - 1 \in R_0$ does not vanish and the latter is again all of S since $x - 1 = x(1 - x^{-1})$ and $1 - x^{-1}$ is a unit in $\mathcal{O}_{X,P}$ for all $P \in S$. Thus

$$X_{x-1} = V_0 \setminus V(x-1) \cup S = (V_0 \cup V_\infty) \setminus V(x-1) = X \setminus V(x-1)$$

where $V(x-1) \subseteq V_0$. Now $X = (X \setminus V(x-1)) \cup V_\infty$ since we even have $V(x-1) \subseteq V_{0,\infty}$. Hence we are left to show that $X \setminus V(x-1)$ is affine.

To do so, we use that the elements x and $x-1$ are pullbacks of functions on $\mathbb{P}^1_k$ and that the $\pi : X \to \mathbb{P}^1_k$ is affine (since it is finite). Let $\mathbb{P}^1_k = \operatorname{Proj}(k[x_0, x_1])$ and set $x = x_1/x_0$.

Then $\mathbb{P}^1_k$ is covered by the affine subsets $U_0 = D_+(x_0)$ and $U_\infty = D_+(x_1)$ with coordinate rings $k[x]$ respectively $k[x^{-1}]$. We consider the open subset $D_+(x_0 - x_1)$ of $\mathbb{P}^1_k$ which is affine, see [Liu02, 2.3.36 (a)], and which in turn is covered by $D_+((x_0 - x_1) \cdot x_0) \subseteq U_0$ and $D_+((x_0 - x_1) \cdot x_1) \subseteq U_\infty$. By [Liu02, 2.3.36 (b)], we have that $D_+((x_0 - x_1) \cdot x_0)$ is isomorphic to the basic open subset

$$D\left(\frac{(x_0 - x_1) \cdot x_0}{x_0^2}\right) = D\left(\frac{x_0 - x_1}{x_0}\right) = D\left(1 - \frac{x_1}{x_0}\right) = D(1 - x)$$

in U_0, that is $D_+((x_0 - x_1) \cdot x_0) \cong \operatorname{Spec}(k[x]_{1-x})$. Analogously, we have that $D_+((x_0 - x_1) \cdot x_1)$ is isomorphic to the basic open subset

$$D\left(\frac{(x_0 - x_1) \cdot x_1}{x_1^2}\right) = D\left(\frac{x_0 - x_1}{x_1}\right) = D\left(\frac{x_0}{x_1} - 1\right) = D(x^{-1} - 1)$$

in U_∞, that is $D_+((x_0 - x_1) \cdot x_1) \cong \operatorname{Spec}(k[x^{-1}]_{x^{-1}-1})$. Note that $V(1 - x) = V(x - 1)$ inside of $U_0 \cap U_\infty = \operatorname{Spec}(k[x, x^{-1}])$ since $1 - x = x(x^{-1} - 1)$ and $x \in k[x, x^{-1}]^\times$. In particular,

$$D_+(x_0 - x_1) = (U_0 \setminus V(1 - x)) \cup (U_\infty \setminus V(x^{-1} - 1)) = \mathbb{P}^1_k \setminus V_{U_0}(1 - x).$$

Therefore, the preimage $\pi^{-1}(D_+(x_0 - x_1))$ is

$$X \setminus V_{\pi^{-1}(U_0)}(\pi^\#(U_0)(1 - x)) = X \setminus V_{V_0}(1 - x) = X_{1-x} = X_{x-1}$$

and hence X_{x-1} is affine. □

The next statement basically says that covers of $\mathbb{P}^1_k$ have coordinate rings $\mathcal{O}_X(V)$ that are free over $\mathcal{O}_{\mathbb{P}^1}(U)$.

Proposition D.2.4. *Let X be a proper scheme over k of dimension one with finite surjective morphism $\pi : X \to Y = \mathbb{P}^1_k$. Then the following are equivalent:*

1. *$\pi_*\mathcal{O}_X$ is a locally free $\mathcal{O}_Y$-module,*
2. *X is Cohen-Macaulay, and*
3. *X has no embedded points.*

If the above statements are true, then we say that π has degree d where d is rank of $\pi_*\mathcal{O}_X$ over $\mathcal{O}_Y$.

Proof. Any proper scheme over k is noetherian. The equivalence between the last two statements is thus given by [Sta18, Tag 0BXG].

Let X be Cohen-Macaulay. Then, by Corollary D.1.8, $\pi : X \to \mathbb{P}^1_k$ is flat. By [Sta18, Tag 02KB], this is equivalent to $\pi_*\mathcal{O}_X$ being a locally free $\mathcal{O}_{\mathbb{P}^1}$-module.

Conversely, assume that $\pi_*\mathcal{O}_X$ is locally free over $\mathcal{O}_{\mathbb{P}^1}$. By [Sta18, Tag 02KB] again, $\pi : X \to \mathbb{P}^1_k$ is flat and hence the local homomorphisms $\mathcal{O}_{\mathbb{P}^1_k, \mathfrak{p}} \hookrightarrow \mathcal{O}_{X,P}$ with $\pi(P) = \mathfrak{p}$ are flat ring maps. Now since $\mathcal{O}_{\mathbb{P}^1_k, \mathfrak{p}}$ is Cohen-Macaulay and both X and $\mathbb{P}^1_k$ are noetherian, [Sta18, Tag 00R5] provides that $\mathcal{O}_{X,P}$ is Cohen-Macaulay, too. Now since X is Cohen-Macaulay if and only if $\mathcal{O}_{X,P}$ is Cohen-Macaulay for all $P \in X$, see [Sta18, Tag 02IP], we deduce that X indeed is Cohen-Macaulay. □

Lemma D.2.5. *Let $f : X \to Y$ be a finite morphism of projective curves with Y integral and X without embedded points. Then for all non-empty open subsets $U \subseteq Y$ its preimage $f^{-1}(U)$ is schematically dense in X.*

Proof. By [Liu02, 7.3.10], f sends generic points to generic points. Since $U \subseteq Y$ is non-empty, it contains the generic point of Y and hence $f^{-1}(U)$ contains all generic points of X. Since X has no embedded points, $\mathrm{Ass}(\mathcal{O}_X)$ equals the set of generic points of X. Therefore $\mathrm{Ass}(\mathcal{O}_X) \subseteq f^{-1}(U)$ and thus $f^{-1}(U)$ is a schematically dense open subset of X. □

Lemma D.2.6. *The open immersions $i_0 : V_0 \hookrightarrow X$ and $i_\infty : V_\infty \hookrightarrow X$ are affine morphisms.*

Proof. The situation is completely symmetric and thus we only consider $i_0 : V_0 \hookrightarrow X$. The affine open subset V_0 and V_∞ cover X and obviously, $i_0^{-1}(V_0) = V_0$ is affine. Moreover, $i_0^{-1}(V_\infty) = V_0 \setminus V(x)$ which is an affine basic open subset. Thus we have found an affine open cover of X whose preimages under i_0 are again affine. Then [Sta18, Tag 01S8] provides the assertion. □

Proposition D.2.7. *Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Let $U \in \{U_0, U_\infty\}$, $A = \mathcal{O}_{\mathbb{P}^1}(U)$ and $R = \mathcal{O}_X(V)$ with $V = \pi^{-1}(U)$. For $a \in A$ let $\deg(a)$ denote the degree in the respective polynomial ring. Let $M_\mathcal{F}$ denote a basis matrix of $\mathcal{F}(V)$ regarding a fixed basis of R. Then $\deg_k \mathcal{F}(V) = \deg \det M_\mathcal{F}$ where $\deg f/g = \deg f - \deg g$ for $f, g \in A$.*

Proof. Assume that $I = \mathcal{F}(V_0) \subseteq R$. Then Lemma B.4.11 provides the assertion. Now let I be arbitrary with wedging element $w \in R$ such that $wI \subseteq R$. Thus we have $\deg_k wR = \dim_k R/wR = \deg \det M_w$ and $\deg_k wI = \dim_k R/wI = \deg \det M_{wI}$. Now the definition of the degree of R-ideals provides

$$\deg_k I = \dim_k R/wI - \dim_k R/wR = \deg \det M_{wI} - \deg \det M_w.$$

Since the basis matrix of M_{wI} is simply the product of M_w and M_I, we obtain

$$\begin{aligned} \deg \det M_{wI} - \deg \det M_w &= \deg \det M_w + \deg \det M_I - \deg \det M_w \\ &= \deg \det M_I \end{aligned}$$

which finally provides $\deg_k I = \deg \det M_I$. □

Lemma D.2.8. *For any $r \in \mathbb{Z}_{\geq 0}$ we have $\dim_k \mathcal{O}_S/x^{-r}\mathcal{O}_S = \dim_k R_\infty/x^{-r}R_\infty$.*

Proof. Let $R := R_\infty$. Obviously, since $R \subseteq \mathcal{O}_S$, we have $\dim_k \mathcal{O}_S/x^{-r}\mathcal{O}_S \geq \dim_k R/x^{-r}R$. We show that a basis of $R/x^{-r}R$ is a generating set of $\mathcal{O}_S/x^{-r}\mathcal{O}_S$ over k which then provides equality: By definition of $\mathcal{O}_S$, we only need to show that we can generate elements of the form $1/h$ where $h \in T$ (recall that $T = k[x^{-1}] \setminus x^{-1}k[x^{-1}]$). Now h is a unit in $k[x^{-1}]/(x^{-r})$ since it is coprime to x^{-1}. Thus there is some $f \in k[x^{-1}]$ with $\deg f < r$ such that $h \cdot f = 1$ in $k[x^{-1}]/(x^{-r})$. We use this to generate $1/h$ with $1, x^{-1}, \ldots, x^{-r+1}$ over k: $1/h = h \cdot f/h = f$ in $\mathcal{O}_S/x^{-r}\mathcal{O}_S$. □

Corollary D.2.9. *For any $s \in \mathbb{Z}$ we have $\deg_k x^s R_\infty = -sn$ and $\deg_k x^s R_0 = sn$. In particular, $\deg_k x^s \mathcal{O}_S = \deg_k x^s R_\infty = -sn$.*

Proof. Note that for $g = x^s$ with $s \in \mathbb{Z}$ we have $s = \deg_x g = -\deg_{x^{-1}} g$. Then the first assertion is provided by applying Corollary D.2.12 with $g = x^s$.

Now we prove the particular part. Assume $s \geq 0$. By C.1.20 and the fact that x^{-s} is a wedging element, we have

$$\deg_k x^s \mathcal{O}_S = -\dim_k x^s \mathcal{O}_S/\mathcal{O}_S = -\dim_k \mathcal{O}_S/x^{-s}\mathcal{O}_S = -\dim_k R_\infty/x^{-s}R_\infty$$

where the second last equality is due to Corollary C.1.24 and the last is due to Lemma D.2.8. Now since $s \geq 0$, we have $\dim_k R_\infty/x^{-s}R_\infty = \deg_k x^{-s}R_\infty = sn$ by the first assertion.

Hence $\deg_k x^s\mathcal{O}_S = -\deg_k x^{-s}R_\infty = -sn$. If $s \leq 0$, then $x^s\mathcal{O}_S$ is an integral ideal of $\mathcal{O}_S$ and hence

$$\deg_k x^s\mathcal{O}_S = \dim_k \mathcal{O}_S/x^s\mathcal{O}_S = \dim_k R_\infty/x^sR_\infty = \deg_k x^sR_\infty = -sn$$

where the second equality is due to Lemma D.2.8 and the last equality is due to the first assertion we have already proven. □

Proposition D.2.10. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\deg_k \mathcal{F}((x^r)_\infty) = \deg_k \mathcal{F} - rn$.*

Proof. By Proposition 5.6.9, we have $\deg_k \sum_{i\in A} r_i(x)_{i,\infty} = \sum_{i\in A} r_i n_i$. By Lemma C.4.8, we obtain $\deg_k \mathcal{O}_X(\sum_{i\in A} r_i(x)_{i,\infty}) = \sum_{i\in A} -r_i n_i$. Note that, by Remark 5.6.10, we have $\sum_{i\in A} r(x)_{i,\infty} = (x^r)_\infty$ and thus $\deg_k \mathcal{O}_X((x^r)_\infty) = -rn$. By Lemma C.4.7, we thus have

$$\deg_k \mathcal{F}((x^r)_\infty) = \deg_k \mathcal{F} + \deg_k \mathcal{O}_X((x^r)_\infty) = \deg_k \mathcal{F} - rn.$$ □

Proposition D.2.11. *Set $f_P = [\kappa(P) : k]$ for $P \in S$, then $\sum_{P\in S} f_P \leq n$.*

Proof. [GW10, 12.21] with $Y = \mathbb{P}^1_k$ and $y = P_\infty$ says that $n = \deg(\pi) = \sum_{P\in S} e_P \cdot [\kappa(P) : k]$ where $e_P \geq 1$ (since $\mathcal{O}_{X,P} \neq 0$ for $P \in S$) if π is *finite locally free*. Now [GW10, 12.19] provides that π is *finite locally free* if π is finite and flat which is the case due to Corollary D.1.8. □

Corollary D.2.12. *Let X be a cover of $\mathbb{P}^1_k$. Let $f, g \in k(x)$ with $f = a/b$, $g = c/d$ and $a, b \in k[x]$, $c, d \in k[x^{-1}]$. Then $\deg_k fR_0 = n \cdot (\deg_x(a) - \deg_x(b))$ and $\deg_k gR_\infty = n \cdot (\deg_{x^{-1}}(c) - \deg_{x^{-1}}(d))$. In particular,*

$$\deg_k x^rR_0 = rn \quad \text{and} \quad \deg_k x^rR_\infty = n \cdot \deg_{x^{-1}} x^r = -rn.$$

Proof. Since X is a cover of $\mathbb{P}^1_k$, we have $k(x)^\times \subseteq \mathcal{K}_X(X)^\times$. Set $\mathcal{F} = \mathcal{O}_X(-\mathrm{div}(f))$ which satisfies $\mathcal{F}(V_\infty) = fR_\infty$. Now apply Proposition D.2.7 to $\mathcal{F}(V_0)$ which yields

$$\begin{aligned}
\deg_k \mathcal{F}(V_0) &= \deg_k fR_0 \\
&= \deg_k aR_0 - \deg_k bR_0 \\
&= \deg_x \det M_a - \deg_x \det M_b \\
&= n \cdot \deg_x(a) - n \cdot \deg_x(b) \\
&= n \cdot (\deg_x(a) - \deg_x(b)).
\end{aligned}$$

Now set $\mathcal{G} = \mathcal{O}_X(-\mathrm{div}(g))$ which satisfies $\mathcal{G}(V_\infty) = gR_\infty$. Analogously, we have

$$\begin{aligned}
\deg_k \mathcal{G}(V_\infty) &= \deg_k gR_\infty \\
&= \deg_k cR_\infty - \deg_k dR_\infty \\
&= \deg_{x^{-1}} \det M_c - \deg_{x^{-1}} \det M_d \\
&= n \cdot \deg_{x^{-1}}(d) - n \cdot \deg_{x^{-1}}(d) \\
&= n \cdot (\deg_{x^{-1}}(d) - \deg_{x^{-1}}(d)).
\end{aligned}$$

The particular part now follows immediately. □

Lemma D.2.13. *Let X be a cover of $\mathbb{P}^1_k$ of degree n. The pole divisor $(x)_\infty$ of x on X satisfies*

1. $\mathrm{Supp}((x)_\infty) \subseteq S$,
2. $\deg_k(x)_\infty = n$,

3. $((x)_\infty)_{|S} = \operatorname{div}_S(x^{-1})$.

Proof. By definition, $D := (x)_\infty$ is given by the configuration $\{(V_0, 1), (V_\infty, x^{-1})\}$. Since on the level of closed points we have $S = X \setminus V_0$, the first assertion follows immediately from the definition. We have seen in Lemma C.4.8 that we have $\deg_k D = -\deg_k \mathcal{O}_X(D)$. Moreover, by Corollary C.4.13, we have $\deg_k \mathcal{O}_X(D) = \deg_k \mathcal{O}_X(D)_{|V_0} + \deg_k \mathcal{O}_X(D)_{|S}$. However, by the first assertion, we have $\deg_k \mathcal{O}_X(D)_{|V_0} = \deg_k \mathcal{O}_{X|V_0} = 0$. By Proposition 3.2.3, we furthermore have $\deg_k \mathcal{O}_X(D)_{|S} = \deg_k \mathcal{O}_S(D_{|S})$. By Corollary 3.2.23, the restriction of D to S is given by $D_{|S} = (D_{|V_\infty})_{|S}$. By Remark 3.2.12, $D_{|V_\infty}$ is given by the configuration $\{(V_\infty, x^{-1})\}$ and then, by Remark 3.2.20, we have that $(D_{|V_\infty})_{|S}$ is given by $\{(S, x^{-1})\}$. Hence $D_{|S}$ is the the principal divisor of x^{-1} on S. Therefore

$$\deg_k \mathcal{O}_X(D)_{|S} = \deg_k \mathcal{O}_S(D_{|S}) = \deg_k \mathcal{O}_S(\operatorname{div}_S(x^{-1})) = \deg_k x\mathcal{O}_S.$$

Now x^{-1} is a wedging element for the $\mathcal{O}_S$-ideal $x\mathcal{O}_S$ and hence, by definition, we obtain

$$\begin{aligned} -\deg_k D = \deg_k x\mathcal{O}_S = &\dim_k \mathcal{O}_S/x^{-1}x\mathcal{O}_S - \dim_k x\mathcal{O}_S/x^{-1}x\mathcal{O}_S \\ = &-\dim_k x\mathcal{O}_S/\mathcal{O}_S. \end{aligned}$$

By Corollary C.1.24, the latter is equal to $-\dim_k \mathcal{O}_S/x^{-1}\mathcal{O}_S$ and hence we obtain $\deg_k D = \dim_k \mathcal{O}_S/x^{-1}\mathcal{O}_S$. Moreover, by Lemma D.2.8, $\dim_k \mathcal{O}_S/x^{-1}\mathcal{O}_S = \dim_k R_\infty/x^{-1}R_\infty$. By Proposition D.2.7, the latter equals $\dim_k R_\infty/x^{-1}R_\infty = \deg_{x^{-1}} \det M$. Here $M \in k[x^{-1}]^{n\times n}$ is the basis transformation matrix from any $k[x^{-1}]$-basis of R_∞ to one of $x^{-1}R_\infty$. Obviously, M can be chosen to be the diagonal matrix with x^{-1} on the diagonal and hence we finally obtain $\deg_k D = \deg_{x^{-1}} \det M = \deg_{x^{-1}}(x^{-n}) = n$.

We prove the third assertion. By Remark 3.2.20, the configuration $\{(V_0, 1), (V_\infty, x^{-1})\}$ gets sent to $\{(S, x^{-1})\}$ since V_0 has no closed points in common with S. Here we identified x^{-1} with its image under the ring monomorphism $R_\infty \to \mathcal{O}_S$. But $\{(S, x^{-1})\}$ induces obviously the principal divisor of x^{-1} on S. □

Corollary D.2.14. *Since any irreducible component X_i of X is also a cover of $\mathbb{P}^1_k$ of degree n_i and in this case $(x)_{X_i,\infty}$ equals the pole divisor of x on X_i, we also have*

1. $\operatorname{Supp}((x)_{X_i,\infty}) \subseteq S_i$,
2. $\deg_k(x)_{X_i,\infty} = n_i$,
3. $((x)_{X_i,\infty})_{|S_i} = \operatorname{div}_{S_i}(x^{-1})$.

Lemma D.2.15. *Let X be a cover of $\mathbb{P}^1_k$. For every $i \in \{1, \dots, m\}$ there is a basic open subset $D(h_i)$ of V_∞ such that $S_i \subseteq D(h_i) \subseteq V_\infty \setminus (\bigcup_{j\neq i}^m S_j)$. Moreover, we may assume h_i to be a regular element of R_∞.*

Proof. Since V_∞ is affine, it is quasi-affine and hence $\mathcal{O}_{V_\infty}$ is ample, see [Sta18, Tag 01QE]. Since V_∞ is affine, it is separated, see [Sta18, Tag 01KN]. Moreover, since V_∞ is noetherian, it is quasi-compact. By Corollary D.2.2, any irreducible component $V_{i,\infty}$ of V_∞ has infinitely many closed points. Hence for each $i = 1, \dots, m$ we may choose $m-1$ closed points $y_j \in V_{j,\infty}$ which are not contained in S_i. We denote them by $M_i = \{y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_m\}$.

Now the requirements for Lemma D.1.2 are met and we can plug in V_∞ for X, $S_i \cup M_i$ for E, $V_\infty \setminus (\bigcup_{j\neq i}^m S_j)$ for W and $\mathcal{O}_{V_\infty}$ for $\mathcal{L}$ to obtain $h_i \in \mathcal{O}_{V_\infty}(V_\infty) = R_\infty$ such that $S_i \cup M_i \subseteq D(h_i) \subseteq V_\infty \setminus (\bigcup_{j\neq i}^m S_j)$. Since h_i does not vanish identically on any of the irreducible components of V_∞, it need be a regular element of R_∞. □

Proposition D.2.16. *We have $\mathcal{O}_X(V_{0,\infty}) \cong \mathcal{O}_X(V_0)_x$ and $\mathcal{O}_X(V_{0,\infty}) \cong \mathcal{O}_X(V_\infty)_{x^{-1}}$.*

Proof. The proof is obvious since the preimage of basic open subsets is basic open. □

Corollary D.2.17. *Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. The restrictions*

$$\rho^{V_0}_{V_{0,\infty}} : \mathcal{F}(V_0) \to \mathcal{F}(V_{0,\infty}) \quad \text{and} \quad \rho^{V_\infty}_{V_{0,\infty}} : \mathcal{F}(V_\infty) \to \mathcal{F}(V_{0,\infty})$$

are localisation by x respectively x^{-1}.

Proof. The open subsets V_0, V_∞ and $V_{0,\infty}$ are all affine by construction and thus the restriction map $\rho^{V}_{V_{0,\infty}} : \mathcal{F}(V) \to \mathcal{F}(V_{0,\infty})$ is given by localisation, i.e. $\mathcal{F}(V) \to \mathcal{F}(V) \otimes_{\mathcal{O}_X(V)} \mathcal{O}_X(V_{0,\infty})$, see [Liu02, 5.1.14 (b)]. Thus we have $\rho^{V_0}_{V_{0,\infty}} : \mathcal{F}(V_0) \to \mathcal{F}(V_0)_x$ and $\rho^{V_\infty}_{V_{0,\infty}} : \mathcal{F}(V_\infty) \to \mathcal{F}(V_\infty)_{x^{-1}}$. □

Remark D.2.18. By [Sta18, Tag 00KJ], every zero-dimensional, noetherian ring R is isomorphic to $\bigoplus_{P \in \operatorname{Spec}(R)} R_P$.

The following proposition collects facts about the points lying over the point at infinity P_∞ of Y.

Proposition D.2.19. *For $P \in \operatorname{Spec}(R_\infty)$ the following are equivalent: (i) $P \cap T = \emptyset$, (ii) $P \cap k[x^{-1}] = P_\infty$, (iii) $P \supseteq P_\infty$.*

Proof. The proof is immediate since f maps closed points to closed points, see Proposition D.1.10. □

Remark D.2.20. Obviously, for any $P \in \{\text{quasi-coherent, coherent, invertible}\}$ we know that $\mathcal{F}_{|S}$ is P if $\mathcal{F}$ was P.

Lemma D.2.21. *Let X be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\mathcal{F}_{|S}$ is (as a sheaf of $\mathcal{O}_S$-modules) an $\mathcal{O}_S$-ideal and $\mathcal{F}_{|S}(S)$ is (as an $\mathcal{O}_S$-module) an $\mathcal{O}_S$-ideal.*

Proof. By Example 3.1.14, we know that $\mathcal{F}_{|V_\infty}$ is an $\mathcal{O}_\infty$-ideal. By Lemma C.4.10, this implies that $\mathcal{F}(V_\infty)$ is an R_∞-ideal. By definition, we have $\mathcal{F}_{|S}(S) = T^{-1}\mathcal{F}(V_\infty)$. Therefore, by Lemma C.1.7, $\mathcal{F}_{|S}(S)$ can be considered as an $\mathcal{O}_S$-ideal and, by Lemma C.4.10 again, this also provides that $\mathcal{F}_{|S}$ is an $\mathcal{O}_S$-ideal. □

Corollary D.2.22. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Then*

$$\mathcal{F}_{|S} \cong (\mathcal{F}(V_\infty) \otimes_{R_\infty} \mathcal{O}_S)^\sim \cong (T^{-1}\mathcal{F}(V_\infty))^\sim.$$

Moreover, if $\mathcal{F}$ is invertible, then $\mathcal{F}_{|S} \cong h\mathcal{O}_S$ for some $h \in \mathcal{K}_X(X)^\times$.

Proof. By basic properties of the pullback of sheaves, we have

$$\mu^*(\mathcal{F}) = (\mu_a^* \circ \iota^*)(\mathcal{F}) = \mu_a^*(\mathcal{F}_{|V_\infty}) \cong \mathcal{F}(V_\infty) \otimes_{R_\infty^\sim} \mathcal{O}_S^\sim \cong (\mathcal{F}(V_\infty) \otimes_{R_\infty} \mathcal{O}_S)^\sim \cong (T^{-1}\mathcal{F}(V_\infty))^\sim$$

where the first appearing isomorphism is [GW10, 7.24]. Now if $\mathcal{F}$ is invertible, we may assume (see [Liu02, 7.1.19]) that $\mathcal{F} \leq \mathcal{K}_X$ and hence $\mathcal{F}(V_\infty) \subseteq \mathcal{K}_X(V_\infty) = \operatorname{Frac}(\mathcal{O}_S)$. Thus $M_\infty := \mathcal{F}(V_\infty) \otimes_{R_\infty} \mathcal{O}_S \subseteq \operatorname{Frac}(\mathcal{O}_S)$. By Remark D.2.20, we know that $\mathcal{F}_{|S}$ is an invertible $\operatorname{Spec}(\mathcal{O}_S)$-module and hence $M_\infty \subseteq \operatorname{Frac}(\mathcal{O}_S)$ is invertible. Hence, by Lemma B.4.6, $M_\infty = h\mathcal{O}_S$ is a principal ideal with $h \in \mathcal{K}_S(S)^\times$. But since $\mathcal{K}_S(S) \cong \operatorname{Frac}(\mathcal{O}_S) = \operatorname{Frac}(R_\infty) \cong \mathcal{K}_X(X)$, h corresponds to a regular element in $\mathcal{K}_X(X)^\times$ as asserted. □

Lemma D.2.23. *For every quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ we have*

$$\mathcal{F}((x^r)_\infty)(V_0) = \mathcal{F}(V_0) \quad \text{and} \quad \mathcal{F}((x^r)_\infty)(V_\infty) \cong x^r\mathcal{F}(V_\infty).$$

Moreover,

$$\mathcal{F}(\mathrm{div}(x^r)_0)(V_0) \cong x^{-r}\mathcal{F}(V_0) \quad \textit{and} \quad \mathcal{F}(\mathrm{div}(x^r)_0)(V_\infty) = \mathcal{F}(V_\infty).$$

Proof. By definition, we have $\mathcal{O}_X(\mathrm{div}(x^r)_0)_{V_0} = x^{-r}\mathcal{O}_{V_0}$ and $\mathcal{O}_X(\mathrm{div}(x^r)_0)_{V_\infty} = \mathcal{O}_{V_\infty}$ and similarly $\mathcal{O}_X((x^r)_\infty)_{V_0} = \mathcal{O}_{V_0}$ and $\mathcal{O}_X((x^r)_\infty)_{V_\infty} = x^r\mathcal{O}_{V_\infty}$. The assertion now follows from the fact that the restriction to affine opens of the tensor product of quasi-coherent sheaves is given by the product of the restrictions, see [Liu02, 5.1.12]. □

Corollary D.2.24. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-module and let $(x^r)_\infty$ denote the pole divisor of x. Then $\mathcal{F}((x^r)_\infty)_{|S} \cong x^r\mathcal{F}(S)^\sim$.*

Proof. By Corollary D.2.22, we have $\mathcal{F}((x^r)_\infty)_{|S} \cong [T^{-1}\mathcal{F}(V_\infty)\otimes_{\mathcal{O}_X(V_\infty)}\mathcal{O}_X((x^r)_\infty)(V_\infty)]^\sim$. From Lemma D.2.23 we know $\mathcal{O}_X((x^r)_\infty)_{|V_\infty} \cong x^r\mathcal{O}_{V_\infty}$ and thus we obtain $\mathcal{F}((x^r)_\infty)_{|S} \cong x^r\mathcal{F}(S)^\sim$. □

Appendix E

Dualising Sheaf and the Dual of $\mathcal{O}_X$-Ideals

In this chapter we will recall some basic notions of the dualising (r-dualising) sheaf of a proper morphism of schemes. The 1-dualising sheaf ω_X helps us to express the first cohomology term of any quasi-coherent sheaf $\mathcal{F}$ on a scheme X over a field k as the global sections of its ω_X-dual $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$. In particular, these have the same dimension as k-vector spaces and thus the first cohomology term of $\mathcal{F}$ vanishes if and only if its ω_X-dual vanishes. We will use this connection and the decomposition of vector bundles over $\mathbb{P}^1_k$ into a direct sum of invertible sheaves to deduce a vanishing theorem for the first cohomology term of $\mathcal{F}(r(x)_\infty)$ for r sufficiently large in terms of the degree of $\mathcal{F}_{|X_i}$ and the invariant c_X. This establishes a variant of the Riemann-Roch equation for $\mathcal{O}_X$-ideals which makes it possible to give an explicit formula for the dimension of the global sections of $\mathcal{O}_X$-ideals of the form $\mathcal{F}(r(x)_\infty)$ and r sufficiently large.

This chapter is organised as follows: In Section E.1 we define the r-dualising sheaf, refer to proofs of its existence in the case of $r = 1$ for noetherian projective schemes of dimension one and prove and provide some fundamental properties. Moreover, we will see that the 1-dualising is isomorphic to an $\mathcal{O}_X$-ideal for reduced, projective curves over k. In Section E.2 we will define the degree of coherent and torsion-free sheaves which extends the definition of the degree of $\mathcal{O}_X$-ideals and already provides a Riemann-Roch equation. We will define the ω_X-dual, prove some of its fundamental properties and define the decomposition invariants of coherent and torsion-free sheaves $\mathcal{F}$ that uniquely determine the pushdown $\pi_*\mathcal{F}$ to the projective line. In the case of $\mathcal{O}_X$-ideals these coincide with the π-invariants. This enables us to draw a connection between the π-invariants of $\mathcal{O}_X$-ideals and the decomposition invariants of its ω_X-dual. This culminates in a description of the dimension of $H^1(X, \mathcal{F}(r(x)_\infty))$ solely in terms of the π-invariants of $\mathcal{F}$ and r. This description provides sufficient condition for $H^1(X, \mathcal{F}(r(x)_\infty))$ to vanish. The latter implies the mentioned Riemann-Roch equation providing an explicit description of the dimension of the global sections of $\mathcal{F}(r(x)_\infty)$ solely in terms of invariants of X, the degree of $\mathcal{F}$ and r for $\mathcal{O}_X$-ideals $\mathcal{F}$ and r sufficiently large in terms of the degree of its restrictions to the irreducible components of X. To the best of the author's knowledge, there is no such explicit formula present in the relevant literature.

E.1 The Dualising Sheaf and its Properties

Throughout this section, if not mentioned otherwise, X will be a noetherian, projective Cohen-Macaulay scheme of dimension one over the field k. By Corollary D.1.8, for such curves there is a finite and surjective morphism $\pi : X \to \mathbb{P}^1_k$ which is also flat. Examples for such curves are reduced curves over k. Now we define the r-dualising sheaf for a proper

morphism of schemes which is, for instance, introduced in [Liu02, Section 6.4].

Definition E.1.1. Let $\psi : X \to Y$ be a proper morphism of schemes with fibres of dimension $\leq r$ where Y is locally noetherian. The **r-dualising sheaf of** ψ is a quasi-coherent sheaf ω_ψ on X, endowed with a morphism of $\mathcal{O}_Y$-modules

$$\mathrm{tr}_\psi : R^r\psi_*\omega_\psi \to \mathcal{O}_Y$$

such that for any quasi-coherent sheaf $\mathcal{F}$ on X, the natural bilinear map

$$\psi_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F},\omega_\psi) \times R^r\psi_*\mathcal{F} \to R^r\psi_*\omega_\psi \overset{\mathrm{tr}_\psi}{\to} \mathcal{O}_Y$$

induces an isomorphism

$$\psi_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F},\omega_\psi) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(R^r\psi_*\mathcal{F},\mathcal{O}_Y). \tag{1:1}$$

Here $R^r\psi_*\mathcal{F}$ denotes the higher direct image of $\mathcal{F}$, for further information see [Liu02, 5.2.28]. △

Remark E.1.2. Since $R^0\psi_*\mathcal{F} = \psi_*\mathcal{F}$, see [Liu02, 5.2.29], the 0-dualising ω_ψ of ψ satisfies

$$\psi_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F},\omega_\psi) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(\psi_*\mathcal{F},\mathcal{O}_Y). \qquad \triangle$$

The definition of $R^r\psi_*\mathcal{F}$ for $\psi : X \to \mathrm{Spec}(A)$ with A some ring provides the following property of ω_ψ we will heavily use later on. We will only use it for A being a field.

Lemma E.1.3. *Let X be any scheme. Let $\psi : X \to \mathrm{Spec}(k)$ be a proper morphism with fibres of dimension $\leq r$ (e.g. $\dim(X) \leq r$). Then for every quasi-coherent sheaf $\mathcal{F}$ on X we have an isomorphism*

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F},\omega_\psi) \cong H^r(X,\mathcal{F})^\vee$$

where the dual is seen as the dual of the k-vector space $H^r(X,\mathcal{F})$. In particular,

$$\dim_k H^0(X,\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F},\omega_\psi)) = \dim_k H^r(X,\mathcal{F}).$$

Proof. This is [Liu02, 6.4.20]. □

Lemma E.1.4 ([Liu02] 6.4.25)**.** *Let $f : X \to Y$ be a finite morphism of locally noetherian schemes. For every quasi-coherent sheaf $\mathcal{G}$ on Y we set*

$$f^!\mathcal{G} = \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_*\mathcal{O}_X,\mathcal{G})$$

which is canonically endowed with the structure of a quasi-coherent $\mathcal{O}_X$-module. Moreover, there is a morphism $\mathrm{tr}_\mathcal{G} : f_*(f^!\mathcal{G}) \to \mathcal{G}$. Then $f^!\mathcal{O}_Y$ together with $\mathrm{tr}_{\mathcal{O}_Y}$ is the 0-dualising sheaf for f.

Example E.1.5. Let $\phi : \mathbb{P}^1_k \to \mathrm{Spec}(k)$ be the projective and smooth structure morphism. By [Liu02, 6.4.22, 6.4.32 and 6.1.22], the 1-dualising sheaf ω_ϕ exists and is isomorphic to $\mathcal{O}_{\mathbb{P}^1}(-2)$. In particular, it is invertible and thus the same is true for $\pi^*\omega_\phi$ for every morphism $\pi : X \to \mathbb{P}^1_k$. △

Since we know that the 1-dualising exists for $\mathbb{P}^1_k$, we can show that the 1-dualising of every noetherian projective scheme $\psi : X \to \mathrm{Spec}(k)$ exists and that it is related to that of $\phi : \mathbb{P}^1_k \to \mathrm{Spec}(k)$.

Proposition E.1.6. *Let X be a noetherian projective scheme of dimension one over the field k. Let $\psi : X \to \mathrm{Spec}(k)$ denote the projective structure morphism which decomposes*

into a finite morphism $\pi : X \to \mathbb{P}^1_k$ followed by $\phi : \mathbb{P}^1_k \to \mathrm{Spec}(k)$, see Theorem D.1.6. Then the 1-dualising ω_ψ exists and satisfies

$$\omega_\psi = \pi^! \omega_\phi = \omega_\pi \otimes_{\mathcal{O}_X} \pi^* \omega_\phi$$

where ω_π is the 0-dualising sheaf for π and ω_ϕ the 1-dualising sheaf for ϕ as in Example E.1.5.

Proof. By [Liu02, 6.4.26], ω_ψ does indeed exist and satisfies $\omega_\psi = \pi^! \omega_\phi$. By definition of $\pi^! \omega_\phi$, see Lemma E.1.4, we have $\pi^! \omega_\phi = \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_* \mathcal{O}_X, \omega_\phi)$ and since ω_ϕ is locally free, we obtain by how $\mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_* \mathcal{O}_X, \omega_\phi)$ is considered an $\mathcal{O}_X$-module, the isomorphism

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_* \mathcal{O}_X, \omega_\phi) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_Y}(f_* \mathcal{O}_X, \mathcal{O}_Y) \otimes_{\mathcal{O}_X} \pi^* \omega_\phi$$

which finally with Lemma E.1.4 provides that $\omega_\psi = \omega_\pi \otimes_{\mathcal{O}_X} \pi^* \omega_\phi$ where ω_π denotes the 0-dualising sheaf for π. □

Notation E.1.7. Let X be a noetherian projective scheme of dimension one over the field k. If the morphism $\psi : X \to \mathrm{Spec}(k)$ is given by the context, we denote the 1-dualising sheaf for ψ simply by ω_X. For instance, if (X, π) is a cover of $\mathbb{P}^1_k$, then $\psi = \phi \circ \pi$ where $\phi : \mathbb{P}^1_k \to \mathrm{Spec}(k)$. △

For the sake of the argument, we will now introduce the notion of TfS_2-sheaves and of TfS_2-dualising sheaves which are introduced in [Kol18] as the "correct analogs" of reflexive sheaves on non-normal schemes, see [Kol18, p. 1,4]. We will see in Proposition E.1.13 that the 1-dualising sheaf ω_X on a projective Cohen-Macaulay scheme of dimension one over a field k is also a TfS_2-dualising sheaf on X. This enables us to deduce some properties for ω_X, see for instance Corollaries E.1.15 and E.2.3

Definition E.1.8. Let X be a scheme. Let $\mathcal{F}$ be a coherent sheaf on X. Then $\mathcal{F}$ is called **torsionfree** if $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{F}) \subseteq X^0$, i.e. if the associated points of $\mathcal{F}$ are generic points of X. Sheaves that are coherent, torsionfree and S_2 are called TfS_2-sheaves. △

Remark E.1.9. The notion of being torsionfree, as in Definition E.1.8, coincides with our notion of being torsion-free if X is S_1, see Lemma B.4.23. Thus if X is a Cohen-Macaulay scheme of dimension one, then, by Corollary B.4.21, $\mathcal{F}$ is TfS_2-sheaf if and only if $\mathcal{F}$ is coherent and torsion-free. △

Definition E.1.10. A **TfS_2-dualising sheaf on** X is a TfS_2-sheaf $\widetilde{\omega}_X$ such that for all TfS_2-sheaves $\mathcal{F}$ the natural map

$$\mathcal{F} \longrightarrow \mathrm{Hom}_{\mathcal{O}_X}(\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}, \widetilde{\omega}_X), \widetilde{\omega}_X)$$

is an isomorphism. If $X = \mathrm{Spec}(R)$ and $\widetilde{\omega}_X$ is TfS_2-dualising on X given by the module R-module $\widetilde{\omega}_R$, then $\widetilde{\omega}_R$ is called a **TfS_2-dualising module on** R. △

Remark E.1.11. If X is non-empty and the TfS_2-dualising sheaf exists, it is non-zero. Indeed, by definition, we have $\mathcal{O}_X \cong \mathrm{Hom}_{\mathcal{O}_X}(\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \widetilde{\omega}_X), \widetilde{\omega}_X)$ and if $\widetilde{\omega}_X = 0$, then $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \widetilde{\omega}_X) = 0$ and thus $\mathcal{O}_X = 0$ which is absurd. △

Proposition E.1.12 ([Kol18], Cor. 40)**.** *Let X be a regular scheme. Then a coherent sheaf $\mathcal{F}$ is TfS_2-dualising if and only if $\mathcal{F}$ is invertible.*

Proposition E.1.13. *Let X be a noetherian, projective Cohen-Macaulay scheme of dimension 1 over the field k. Then the 1-dualising sheaf ω_X on X is also a TfS_2-dualising sheaf on X.*

Proof. By Corollary D.1.8, we know that there is a finite morphism $\pi : X \to \mathbb{P}^1_k$ which is surjective and flat. Since X is Cohen-Macaulay, by Proposition D.2.4, we know that $\pi_*\mathcal{O}_X$ is a free $\mathcal{O}_Y$-module. Now any torsion-free $\mathcal{O}_X$-module $\mathcal{F}$ thus satisfies that $\pi_*\mathcal{F}$ is torsion-free over $\pi_*\mathcal{O}_X$. Now since $\pi_*\mathcal{O}_X$ is free over $\mathcal{O}_{\mathbb{P}^1}$, it is a fortiori torsion-free over $\mathcal{O}_{\mathbb{P}^1}$ and hence the same is true for $\pi_*\mathcal{F}$. If $\mathcal{F}$ is coherent, by [Liu02, 5.1.14 (d)], $\pi_*\mathcal{F}$ is coherent as $\mathcal{O}_{\mathbb{P}^1}$-module. In particular, each stalk of $\pi_*\mathcal{F}$ is a finitely generated and torsion-free module over a principal ideal domain and thus free. Hence $\pi_*\mathcal{F}$ is locally free. Thus $\pi_*\mathcal{F}$ is locally free if $\mathcal{F}$ is coherent and torsion-free on X. In particular, the same holds true for all TfS_2-sheaves $\mathcal{F}$. Clearly, any locally free sheaf is a TfS_2-sheaf and thus we may apply [Kol18, Prop. 32] and see that $\pi^!\widetilde{\omega}_{\mathbb{P}^1_k}$ is a TfS_2-dualising sheaf on X for every TfS_2-dualising sheaf $\widetilde{\omega}_{\mathbb{P}^1_k}$ on $\mathbb{P}^1_k$. By [Kol18, Cor. 40], being TfS_2-dualising is equivalent to being invertible. Now let $\omega_{\mathbb{P}^1_k} = \mathcal{O}_{\mathbb{P}^1}(-2)$ be the 1-dualising sheaf on $\mathbb{P}^1_k$, which is invertible and thus, by [Kol18, Cor. 40], a TfS_2-dualising sheaf on $\mathbb{P}^1_k$. By [Liu02, 6.4.26 (a)], we know that $\omega_X = \pi^!\omega_{\mathbb{P}^1_k}$ is the 1-dualising sheaf on X and, by [Kol18, Prop. 32], it is also a TfS_2-dualising sheaf on X. □

Remark E.1.14. By Proposition E.1.6, we know that ω_X exists. Moreover, if X is additionally Cohen-Macaulay, by Proposition E.1.13, ω_X is also a TfS_2-dualising sheaf on X and therefore Remark E.1.11 provides that it is non-zero. △

Corollary E.1.15. *Let X be a noetherian, projective Cohen-Macaulay scheme of dimension 1 over the field k. Then the 1-dualising sheaf ω_X on X is also a TfS_2-sheaf on X and thus coherent, S_2 and satisfies $\mathrm{Ass}_{\mathcal{O}_X}(\omega_X) \subseteq X^0$. Since X is Cohen-Macaulay, by Lemma B.4.23, the latter is equivalent to ω_X being torsion-free.*

Definition E.1.16. Let X be a scheme of dimension one. We say that X is **Gorenstein in codimension 0**, denoted by "X is G_0", if the local rings $\mathcal{O}_{X,P}$ for all generic points $P \in X^0$ of X are local Gorenstein rings. △

Remark E.1.17. A local noetherian ring $(R, \mathfrak{m}, \kappa)$ is, by definition, a Gorenstein ring if it has finite injective dimension, that is, if $\sup\{i \mid \mathrm{Ext}^i_R(\kappa, R) \neq 0\}$ is finite. Now since $\mathrm{Ext}^0_R(\kappa, R) = \mathrm{Hom}_R(\kappa, R)$, we know that if R is itself a field, then $R = \kappa$ and thus $\mathrm{Hom}_R(\kappa, R) \neq 0$ providing that fields are local Gorenstein rings. In particular, by Lemma B.4.29, every reduced scheme is both Cohen-Macaulay and Gorenstein in codimension 0. △

Proposition E.1.18. *Let X be a projective curve over k which is Cohen-Macaulay and Gorenstein in codimension 0 (e.g. X reduced). Let ω_X be the 1-dualising sheaf on X. Then ω_X is isomorphic to some $\mathcal{O}_X$-ideal.*

Proof. Since X is reduced, it is S_1 and since it is of dimension 1, it also satisfies S_d for all $d \geq 1$. Thus, by [Kol18, Lem. 27], we know that $\mathcal{F}$ is a TfS_2-dualising sheaf on X if and only if $\mathcal{F}_P$ is a TfS_2-dualising module on $\mathcal{O}_{X,P}$ for all $P \in X$. By Corollary E.1.15, the 1-dualising ω_X is also a TfS_2-dualising sheaf on X and hence $\omega_{X,P}$ is a TfS_2-dualising module on $\mathcal{O}_{X,P}$. In particular, this holds for the generic points of X as well. Since X is noetherian, the local ring $\mathcal{O}_{X,P}$ for $P \in X^0$ is a zero-dimensional noetherian ring and thus, by [Sta18, Tag 00KH], it is artinian. Now the TfS_2-duality on artinian schemes is the same as the Matlis-duality since on such a scheme every coherent sheaf is S_2. Now combine [BH98, 3.2.12] and [Eis95, 21.1 and 21.2] to see that every TfS_2-dualising module Ω on a local artinian ring $(A, \mathfrak{m}, \kappa)$ is isomorphic to the injective hull $E(\kappa)$ of κ. See also [Kol18, Lem. 35]. Therefore, $\omega_{X,P}$ is isomorphic to the injective hull $E(\kappa(P))$. By [BH98, 3.2.12], we know that any finite faithful R-module (where $(R, \mathfrak{m}, \kappa)$ is a noetherian local ring) of type 1 is isomorphic to $E(\kappa)$. Moreover, by [BH98, 3.3.13], if R is additionally

Cohen-Macaulay, then the so called canonical module of R is a faithful maximal Cohen-Macaulay R-module of type 1 and thus, by the above, isomorphic to $E(\kappa)$. Finally, since X is reduced, by Lemma B.4.29, $\mathcal{O}_{X,P}$ is a field for every $P \in X^0$ and therefore, by Remark E.1.17, it is a local Gorenstein ring. Now [BH98, 3.3.7] provides that the canonical module of a local Gorenstein ring R is isomorphic to R and hence we deduce that $\omega_{X,P} \cong E(\kappa(P)) \cong \mathcal{O}_{X,P}$. Now since ω_X is invertible at the generic points of X and the latter is Cohen-Macaulay, we can apply Lemma 4.1.2 to deduce that there is an $\mathcal{O}_X$-module embedding $\omega_X \hookrightarrow \mathcal{K}_X$. By Corollary E.1.15, we know that ω_X is coherent and thus we conclude that ω_X is isomorphic to some $\mathcal{O}_X$-ideal, see Definition 3.1.13. □

Proposition E.1.19. *Let X be an integral, noetherian and projective Cohen-Macaulay scheme of pure dimension over the field k. Let $\eta \in X$ be the generic point of X. Then $\omega_{X,\eta} \neq 0$.*

Proof. By [Sta18, Tag 0587], we have $\omega_X \neq 0$ if and only if $\operatorname{Ass}_{\mathcal{O}_X}(\omega_X) \neq \emptyset$. By Corollary E.1.15, we know that $\operatorname{Ass}_{\mathcal{O}_X}(\omega_X) \subseteq X^0 = \{\eta\}$. Moreover, by Remark E.1.14, we know that $\omega_X \neq 0$ and hence, by the above, $\operatorname{Ass}_{\mathcal{O}_X}(\omega_X) \neq \emptyset$. Therefore, $\operatorname{Ass}_{\mathcal{O}_X}(\omega_X) = \{\eta\}$ and [Sta18, Tag 05AD] tells us that that $\operatorname{Ass}_{\mathcal{O}_X}(\omega_X) \subseteq \operatorname{Supp}(\omega_X)$ which provides the assertion. □

E.2 The ω_X-Dual and the Riemann-Roch Equation

Throughout this section, if not mentioned otherwise, X will be a noetherian, projective Cohen-Macaulay scheme of dimension one over the field k. By $\pi : X \to \mathbb{P}^1_k$ we denote a finite morphism which does exist due to Corollary D.1.8.

As a generalisation of the degree of $\mathcal{O}_X$-ideals we define analogously the degree of coherent and torsion-free sheaves on X.

Definition E.2.1. Let $\mathcal{F}$ be a coherent and torsion-free sheaf on X. Then we define

$$\deg_k \mathcal{F} = \chi(\mathcal{O}_X) - \chi(\mathcal{F}).$$

If $\mathcal{F}$ is an $\mathcal{O}_X$-ideal, then the above degree coincides with the degree of $\mathcal{F}$ as an $\mathcal{O}_X$-ideal. △

In the usual sense, the Riemann-Roch equation connects the Euler characteristic of an invertible sheaf (resp. that of a divisor) with its degree (resp. the degree of the corresponding divisor). Moreover, one wishes that the first cohomology term vanishes if the degree is large enough and thus one can predict the exact dimension of the global sections of the given sheaf (the Riemann-Roch space of the divisor) over k. There are two ways of coming up with such an equation:

(i) One defines the degree of such a sheaf independent of its Euler characteristic (e.g. as the degree of the corresponding divisor), then proves the Riemann-Roch equation and tries to find a way to show that the first cohomology term vanishes for large enough degree, or

(ii) one defines the degree of the given class of sheaves such that a Riemann-Roch equation holds by definition and proves the vanishing of the first cohomology term for large enough degree.

Definition E.2.1 provides a notion of degree for coherent and torsion-free sheaves which immediately provides an equation in the sense of Riemann-Roch. The reader should note that the degree of $\mathcal{O}_X$-ideals coincides with the definition of degree given in Definition E.2.1,

see Lemma C.4.4, and thus $\mathcal{O}_X$-ideals naturally satisfy a Riemann-Roch equation. The reader may compare with [Liu02, 7.3.17 and 7.3.26] where such an equation is provided for invertible sheaves corresponding to divisors on projective schemes of dimension one over a field k. Moreover, if X is an integral and local complete intersection projective curve over k, [Liu02, 7.3.33] states the vanishing of the first cohomology term if the degree of the given divisor exceeds $2p_a(X)-2$. In this section we will show a sufficient condition for the first cohomology term to vanish if we increase the degree of a given sheaf by tensoring with a suitable multiple of the pole divisor of x. We emphasise that the mentioned vanishing works for the large class of schemes X as mentioned in the beginning of this section (noetherian, projective Cohen-Macaulay scheme of dimension one over the field k).

To prove what we have said above, we need to introduce the ω_X-dual of coherent $\mathcal{O}_X$-modules and prove some of its fundamental properties.

Definition E.2.2. For every coherent $\mathcal{O}_X$-module $\mathcal{F}$ we define its **ω_X-dual** or simply **dual** by $\mathcal{F}^* = \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$. △

Corollary E.2.3 (of Proposition E.1.13)**.** *For all coherent and torsion-free sheaves $\mathcal{F}$ on X we have $\mathcal{F}^{**} \cong \mathcal{F}$.*

Proof. By Proposition E.1.13, the statement is true for all TfS_2-sheaves on X. By Remark E.1.9, the assertion holds for all coherent and torsion-free sheaves on X. □

Lemma E.2.4. *Let X be any scheme. If $\mathcal{F}, \mathcal{G}$ are coherent $\mathcal{O}_X$-modules, then the same is true for $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$. If $\mathcal{F}, \mathcal{G}$ are invertible at a common set $Y \subseteq X$ of points in X, then the same is true for $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$.*

Proof. Since $\mathcal{F}$ and $\mathcal{G}$ are coherent, by [Sta18, Tag 01CQ], the same is true for $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$. By definition, any coherent $\mathcal{O}_X$-module is finitely presented and thus, by [Sta18, Tag 01CP], we know that

$$\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})_P \to \mathrm{Hom}_{\mathcal{O}_{X,P}}(\mathcal{F}_P, \mathcal{G}_P)$$

is an isomorphism for all $P \in X$. Now for all $P \in Y$ let $f_P\mathcal{O}_{X,P} = \mathcal{F}_P$ and $g_P\mathcal{O}_{X,P} = \mathcal{G}_P$ be the generators of $\mathcal{F}_P$ respectively $\mathcal{G}_P$. Then every element in

$$\mathrm{Hom}_{\mathcal{O}_{X,P}}(\mathcal{F}_P, \mathcal{G}_P) = \mathrm{Hom}_{\mathcal{O}_{X,P}}(f_P\mathcal{O}_{X,P}, g_P\mathcal{O}_{X,P})$$

corresponds uniquely to an element in $\mathcal{O}_{X,P}$ (ϕ corresponds to $\phi(f_P)$) providing

$$\mathrm{Hom}_{\mathcal{O}_{X,P}}(f_P\mathcal{O}_{X,P}, g_P\mathcal{O}_{X,P}) \cong \mathcal{O}_{X,P}$$

and thus the assertion. □

Proposition E.2.5. *Let X be a noetherian scheme. Let $\mathcal{F}, \mathcal{G}$ be coherent $\mathcal{O}_X$-modules. Then*

$$\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})) \subseteq \mathrm{Ass}_{\mathcal{O}_X}(\mathcal{G}).$$

Proof. First of all, since X is locally noetherian, by [Sta18, Tag 05AG], we have $\mathcal{G} \neq 0$ if and only if $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{G}) \neq \emptyset$. Thus if $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{G}) = \emptyset$, then $\mathcal{G} = 0$ and thus $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}) = 0$ as well which again provides $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})) = \emptyset$. Hence suppose that both $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}))$ and $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{G})$ are non-empty. Let $P \in \mathrm{Ass}_{\mathcal{O}_X}(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}))$, then $P\mathcal{O}_{X,P} \in \mathrm{Ass}_{\mathcal{O}_{X,P}}(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})_P)$ by definition. Since $\mathcal{F}$ is of finite presentation, by [Sta18, Tag 01CP], we have the isomorphism

$$(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}))_P \to \mathrm{Hom}_{\mathcal{O}_{X,P}}(\mathcal{F}_P, \mathcal{G}_P).$$

Hence $P\mathcal{O}_{X,P}$ is the annihilator of a non-zero homomorphism $f : \mathcal{F}_P \to \mathcal{G}_P$. In particular, $\mathcal{F}_P, \mathcal{G}_P \neq 0$. Therefore, for all $p \in P\mathcal{O}_{X,P}$ we have $pf(a) = 0$ for all $a \in \mathcal{F}_P$. Hence $P\mathcal{O}_{X,P}$

annihilates the non-zero (otherwise $\mathcal{F}_P = 0$ or $f = 0$) $\mathcal{O}_{X,P}$-submodule $f(\mathcal{F}_P) \subseteq \mathcal{G}_P$. In particular, $P\mathcal{O}_{X,P}$ only consists of zero-divisors on $\mathcal{G}_P$ and since the latter is finitely generated over $\mathcal{O}_{X,P}$, by Lemma B.4.22, we know that $P \subseteq Q$ for some $Q \in \mathrm{Ass}_{\mathcal{O}_{X,P}}(\mathcal{G}_P)$. Since P was maximal in $\mathcal{O}_{X,P}$, we have $P = Q$ and thus $P \in \mathrm{Ass}_{\mathcal{O}_{X,P}}(\mathcal{G}_P)$. □

Proposition E.2.6. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module. Then the same is true for $\mathcal{F}^*$. Moreover, if X is Gorenstein in codimension 0 and $\mathcal{F}$ is invertible at the generic points of X, then same is true for $\mathcal{F}^*$ as well.*

Proof. First of all, by Corollary E.1.15, we know that ω_X is coherent and satisfies

$$\mathrm{Ass}_{\mathcal{O}_X}(\omega_X) \subseteq X^0.$$

Now since $\mathcal{F}$ is coherent by assumption, by Lemma E.2.4, we know that $\mathcal{F}^*$ is coherent, too. Moreover, since X is Cohen-Macaulay, by Lemma B.4.23, we know that a coherent $\mathcal{O}_X$-module $\mathcal{H}$ is torsion-free if and only if $\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{H}) \subseteq X^0$. By Proposition E.2.5, we have

$$\mathrm{Ass}_{\mathcal{O}_X}(\mathcal{F}^*) \subseteq \mathrm{Ass}_{\mathcal{O}_X}(\omega_X) \subseteq X^0$$

and hence $\mathcal{F}^*$ is torsion-free. By Proposition E.1.18, we know that if X is Gorenstein in codimension 0, then ω_X is isomorphic to some $\mathcal{O}_X$-ideal. In particular, ω_X is invertible at all generic points of X. Thus, if $\mathcal{F}$ is invertible at P for all $P \in X^0$, then, by Lemma E.2.4, we know that the same is true for $\mathcal{F}^*$ as well. □

Corollary E.2.7. *Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. By Lemma E.1.3, we obtain*

$$\dim_k H^1(X, \mathcal{F}) = \dim_k H^0(X, \mathcal{F}^*).$$

Proposition E.2.8. *Let $\mathcal{F}$ be a coherent and torsion-free $\mathcal{O}_X$-module. Then $\pi_*\mathcal{F}$ is free of finite rank r and there are uniquely determined integers $|\mathcal{F}|_1 \geq \ldots \geq |\mathcal{F}|_r$ such that*

$$\pi_*\mathcal{F} \cong \bigoplus_{i=1}^{r} \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i).$$

Proof. By [Liu02, 5.1.14], $\pi_*\mathcal{F}$ is a coherent $\mathcal{O}_{\mathbb{P}^1}$-module since $\mathbb{P}^1_k$ is locally noetherian. Since X is Cohen-Macaulay, the finite morphism π is flat, see Corollary D.1.8. By [Sta18, Tag 00NX], finitely generated modules over noetherian rings are locally free if and only if they are flat. Hence $\pi_*\mathcal{O}_X$ is a locally free $\mathcal{O}_{\mathbb{P}^1}$-module. Hence the torsion-freeness of $\mathcal{F}$ as an $\mathcal{O}_X$-module implies that $\pi_*\mathcal{F}$ is a torsion-free $\mathcal{O}_{\mathbb{P}^1}$-module. That is, each stalk of $\pi_*\mathcal{F}$ is a torsion-free and finitely generated module over a principal ideal domain of rank r (since $\mathbb{P}^1_k$ is regular) and hence $\pi_*\mathcal{F}$ is locally free of some rank r. That is, $\pi_*\mathcal{F}$ is a locally free $\mathcal{O}_{\mathbb{P}^1}$-module and thus, by Theorem B.5.10, it is isomorphic to a direct sum of r invertible sheaves $\mathcal{O}_{\mathbb{P}^1}(d_i)$ for unique integers $d_1 \geq \ldots \geq d_r$ on $\mathbb{P}^1_k$ which provides the assertion. □

Remark E.2.9. The notation $|\mathcal{F}|_i$ was already used for the π-invariants of $\mathcal{O}_X$-ideals. But as we will see in Corollary E.2.13, these notions will coincide if $\mathcal{F}$ is an $\mathcal{O}_X$-ideal. △

Corollary E.2.10. *Let (X, π) be a Cohen-Macaulay cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $\pi_*\mathcal{F}$ is free of rank n and there are uniquely determined integers $|\mathcal{F}|_1 \geq \ldots \geq |\mathcal{F}|_n$ such that*

$$\pi_*\mathcal{F} \cong \bigoplus_{i=1}^{n} \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i).$$

Proof. We only need to prove that the rank of $\pi_*\mathcal{F}$ over $\mathcal{O}_{\mathbb{P}^1}$ is equal to n since the rest follows from Proposition E.2.8. However, by Proposition 4.1.12, we know that $(\pi_*\mathcal{F})(U) = \mathcal{F}(\pi^{-1}(U))$ is free of rank n for all non-empty affine open subsets $U \subseteq \mathbb{P}^1_k$. □

Proposition E.2.11. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module. Then $\pi_*\mathcal{F}^*$ and $\pi_*\mathcal{F}$ have the same rank r and*

$$\pi_*\mathcal{F}^* \cong \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(-|\mathcal{F}|_i - 2) \quad \text{and thus} \quad |\mathcal{F}^*|_i = -|\mathcal{F}|_i - 2$$

Proof. Let $\pi_*\mathcal{F}$ have rank r. Due to Proposition E.1.6 we have $\omega_X = \omega_\pi \otimes_{\mathcal{O}_X} \pi^*\omega_\phi$ where ω_π is the 0-dualising sheaf for π and ω_π is the 1-dualising sheaf for $\phi : \mathbb{P}^1_k \to \operatorname{Spec}(k)$. Moreover, by Example E.1.5, we know that $\omega_\phi \cong \mathcal{O}_{\mathbb{P}^1}(-2)$ and thus $\pi^*\omega_\phi$ is invertible. In particular, we deduce

$$\mathcal{F}^* = \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_X) \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_\pi) \otimes_{\mathcal{O}_X} \pi^*\omega_\phi,$$

see [GW10, 7.7]. Since both $\mathcal{F}$ and ω_π are coherent, $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_\pi)$ is coherent, see Lemma E.2.4. Since ω_ϕ is invertible and hence flat, we can use the Projection Formula B.5.9 to deduce

$$\pi_*(\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_\pi) \otimes_{\mathcal{O}_X} \pi^*\omega_\phi) \cong \pi_*\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_\pi) \otimes_{\mathcal{O}_{\mathbb{P}^1}} \omega_\phi.$$

The defining property of the 0-dualising ω_π, see Eq. (1:1) in Definition E.1.1, provides

$$\pi_*\mathcal{F}^* \cong \mathcal{H}\mathrm{om}_{\mathcal{O}_{\mathbb{P}^1}}(\pi_*\mathcal{F}, \mathcal{O}_{\mathbb{P}^1}) \otimes_{\mathcal{O}_{\mathbb{P}^1}} \omega_\phi.$$

Plugging in $\omega_\phi \cong \mathcal{O}_{\mathbb{P}^1}(-2)$ and $\mathcal{H}\mathrm{om}_{\mathcal{O}_{\mathbb{P}^1}}(\pi_*\mathcal{F}, \mathcal{O}_{\mathbb{P}^1}) = (\pi_*\mathcal{F})^\vee$ provides

$$\pi_*\mathcal{F}^* \cong (\bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i))^\vee \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(-2). \tag{2:2}$$

Now obviously

$$(\bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i))^\vee \cong \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i)^\vee \cong \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i)^{-1} \cong \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(-|\mathcal{F}|_i)$$

since $\mathcal{F}^\vee \cong \mathcal{F}^{-1}$ for invertible sheaves $\mathcal{F}$. Plugging this into Eq. (2:2) finally provides

$$\pi_*\mathcal{F}^* \cong \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(-|\mathcal{F}|_i - 2). \tag{2:3}$$

This proves that $\pi_*\mathcal{F}^*$ also is locally free of rank r. □

Lemma E.2.12. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module. For $r \in \mathbb{Z}$ we have $|\mathcal{F}(r(x)_\infty)|_i = |\mathcal{F}|_i + r$.*

Proof. By Remark 3.2.6, we have $r(x)_\infty = \pi^*(r(x)_{\mathbb{P}^1_k,\infty})$. By Proposition 3.2.3 (i), we have $\mathcal{O}_X(r(x)_\infty) \cong \pi^*\mathcal{O}_{\mathbb{P}^1}((x)_{\mathbb{P}^1_k,\infty})$. Since $\mathcal{O}_Y(\mathrm{div}_Y(x^r)_\infty)$ is invertible, we may use the Projection Formula B.5.9 to deduce

$$\begin{aligned}\pi_*(\mathcal{F}(r(x)_\infty)) &= \pi_*(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(r(x)_\infty)) \\ &= \pi_*(\mathcal{F} \otimes_{\mathcal{O}_X} \pi^*\mathcal{O}_{\mathbb{P}^1}(r(x)_{\mathbb{P}^1_k,\infty})) \\ &= \pi_*\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_{\mathbb{P}^1}(r(x)_{\mathbb{P}^1_k,\infty}).\end{aligned} \tag{2:4}$$

By Theorem B.5.10, we have $\mathcal{O}_{\mathbb{P}^1}(r(x)_{\mathbb{P}^1_k,\infty})) \cong \mathcal{O}_{\mathbb{P}^1}(\ell)$ for some uniquely determined $\ell \in \mathbb{Z}$.

Now due to Lemma C.4.4, the degree of the $\mathcal{O}_{\mathbb{P}^1}$-ideal satisfies

$$\begin{aligned}\deg_k \mathcal{O}_{\mathbb{P}^1}(\ell) &= \chi(\mathcal{O}_{\mathbb{P}^1}) - \chi(\mathcal{O}_{\mathbb{P}^1}(\ell)) \\ &= \chi(\mathcal{O}_{\mathbb{P}^1}) + \dim_k H^1\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(\ell)\right) - \dim_k H^0\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(\ell)\right) \\ &= -\ell. \end{aligned} \tag{2:5}$$

where the last equation is due to Lemma B.5.11. Since $\mathbb{P}^1_k$ has degree one as a cover of $\mathbb{P}^1_k$, by Lemma D.2.13, we have $\deg_k(r(x)_{\mathbb{P}^1_k,\infty}) = r$ and hence, by Proposition 3.1.27 (iii), we obtain $\deg_k \mathcal{O}_{\mathbb{P}^1}(r(x)_{\mathbb{P}^1_k,\infty})) = -r$. Therefore, by Eq. (2:5), this means $\mathcal{O}_{\mathbb{P}^1}(r(x)_{\mathbb{P}^1_k,\infty})) \cong \mathcal{O}_{\mathbb{P}^1}(r)$. Plugging this into Eq. (2:4) provides

$$\begin{aligned}\pi_*(\mathcal{F}(r(x)_\infty)) &= \pi_*\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_{\mathbb{P}^1}(r) \\ &= \bigoplus_{i=1}^{m} \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i) \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(r) \\ &= \bigoplus_{i=1}^{m} \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i + r)\end{aligned}$$

where m is the rank of $\pi_*\mathcal{F}$. By the uniqueness of the integers $|\mathcal{F}|_i + r$, see Theorem B.5.10, we deduce that $|\mathcal{F}(r(x)_\infty)|_i = |\mathcal{F}|_i + r$. □

Corollary E.2.13. *Let (X, π) be a cover of $\mathbb{P}^1_k$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then the uniquely determined integers $d_1 \geq \ldots \geq d_n$ such that*

$$\pi_*\mathcal{F} \cong \bigoplus_{i=1}^{n} \mathcal{O}_{\mathbb{P}^1}(d_i)$$

equal the π-invariants of $\mathcal{F}$, see Definition 4.3.8 and Theorem 4.3.15, that is, for all $i = 1, \ldots, n$ we have $|\mathcal{F}|_i = d_i$.

Proof. By Theorem 4.3.15, the integers $|\mathcal{F}|_1 \geq \ldots \geq |\mathcal{F}|_n$ are uniquely determined by the property

$$\dim_k H^0\left(X, \mathcal{F}(r(x)_\infty)\right) = \sum_{|\mathcal{F}|_i + r \geq 0} (|\mathcal{F}|_i + r + 1)$$

for all $r \in \mathbb{Z}$. By definition, $H^0\left(\mathbb{P}^1_k, \pi_*\mathcal{F}(r(x)_\infty)\right) = H^0\left(X, \mathcal{F}(r(x)_\infty)\right)$ and thus, by Lemmas B.5.11 and E.2.12, we do have

$$\dim_k H^0\left(X, \mathcal{F}(r(x)_\infty)\right) = \sum_{d_i + r \geq 0} (d_i + r + 1)$$

which therefore provides that for all $i = 1, \ldots, n$ we have $|\mathcal{F}|_i = d_i$ as asserted. □

Proposition E.2.14. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module on X. Then $\chi(\mathcal{F}^*) = -\chi(\mathcal{F})$. In particular, $\deg_k \mathcal{F}^* = \deg_k \mathcal{F} + 2\chi(\mathcal{F})$.*

Proof. This first assertion follows from Propositions E.2.11 and E.2.16. By Proposition E.2.6, $\mathcal{F}^*$ is also coherent and torsion-free and thus $\deg_k \mathcal{F}^*$ is defined. To prove the latter assertion, we obtain by Lemma C.4.4 and Definition E.2.1

$$\begin{aligned}\deg_k \mathcal{F} - \deg_k \mathcal{F}^* &= (\chi(\mathcal{O}_X) - \chi(\mathcal{F})) - (\chi(\mathcal{O}_X) - \chi(\mathcal{F}^*)) \\ &= -\chi(\mathcal{F}) + \chi(\mathcal{F}^*)\end{aligned}$$

and thus, by the first assertion, this becomes

$$\deg_k \mathcal{F} - \deg_k \mathcal{F}^* = -2\chi(\mathcal{F})$$

and hence $\deg_k \mathcal{F}^* = \deg_k \mathcal{F} + 2\chi(\mathcal{F})$ as asserted. □

Corollary E.2.15. *For coherent, torsion-free $\mathcal{O}_X$-modules $\mathcal{F}$ we have*

$$\deg_k \mathcal{F}^* + \deg_k \mathcal{F} = -2g.$$

In particular, $\deg_k \omega_X = -2g$.

Proof. By definition, we have

$$\deg_k \mathcal{F}^* + \deg_k \mathcal{F} = \chi(\mathcal{O}_X) - \chi(\mathcal{F}^*) + \chi(\mathcal{O}_X) - \chi(\mathcal{F})$$

and, by Proposition E.2.14, we have $-\chi(\mathcal{F}^*) = \chi(\mathcal{F})$ and thus this becomes

$$\deg_k \mathcal{F}^* + \deg_k \mathcal{F} = 2\chi(\mathcal{O}_X)$$

as asserted. Now we plug in $\mathcal{F} = \mathcal{O}_X$ in the equation above and note that $\omega_X = \mathcal{O}_X^*$ as well as $\deg_k \mathcal{O}_X = 0$. Thus we obtain $\deg_k \omega_X = -2g$. □

Since $\mathcal{O}_{\mathbb{P}^1}(\ell)(\mathbb{P}^1_k) = 0$ for $\ell < 0$, we see that if r is chosen appropriately, then $\mathcal{F}(r(x)_\infty)$ has no global sections. We can use this together with the dualising property of ω_X to deduce that $H^1(X, \mathcal{F}(r(x)_\infty)) = 0$ for appropriate $r \in \mathbb{Z}$.

Proposition E.2.16. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module on X such that $\pi_*\mathcal{F}$ has rank r. Then*

$$\dim_k H^0(X, \mathcal{F}) = \textstyle\sum_{|\mathcal{F}|_i \geq 0}(|\mathcal{F}|_i + 1) \quad \text{and} \quad \dim_k H^0(X, \mathcal{F}^*) = -\sum_{|\mathcal{F}|_i < 0}(|\mathcal{F}|_i + 1).$$

Therefore, we have $\chi(\mathcal{F}) = \sum_{i=1}^{r}(|\mathcal{F}|_i + 1)$.

Proof. Since $\mathcal{F}(X) = (\pi_*\mathcal{F})(\mathbb{P}^1_k)$, we have $\dim_k \mathcal{F}(X) = \sum_i \dim_k \mathcal{O}_{\mathbb{P}^1}(|\mathcal{F}|_i)(\mathbb{P}^1_k)$. Then, by Lemma B.5.11, we directly obtain $\dim_k H^0(X, \mathcal{F}) = \sum_{|\mathcal{F}|_i \geq 0}(|\mathcal{F}|_i + 1)$. Now using Proposition E.2.11 we analogously obtain

$$\dim_k \mathcal{F}^*(X) = \sum_{|\mathcal{F}^*|_i \geq 0}(|\mathcal{F}^*|_i + 1) = \sum_{-|\mathcal{F}|_i - 2 \geq 0}(-|\mathcal{F}|_i - 1)$$

and since $-|\mathcal{F}|_i - 2 \geq 0$ is equivalent to $|\mathcal{F}|_i < -1$ and the summand $-|\mathcal{F}|_i - 1$ for $|\mathcal{F}|_i = -1$ does not change the sum, we finally obtain $\dim_k \mathcal{F}^*(X) = \sum_{|\mathcal{F}|_i < 0}(-|\mathcal{F}|_i - 1)$. By the dualising property of the 1-dualising ω_X, see Lemma E.1.3, we have

$$\begin{aligned}
\chi(\mathcal{F}) &= \dim_k H^0(X, \mathcal{F}) - \dim_k H^1(X, \mathcal{F}) \\
&= \dim_k H^0(X, \mathcal{F}) - \dim_k H^0(X, \mathcal{F}^*) \\
&= \sum_{|\mathcal{F}|_i \geq 0}(|\mathcal{F}|_i + 1) - \sum_{|\mathcal{F}|_i < 0}(-|\mathcal{F}|_i - 1) \\
&= \sum_{i=1}^{r}(|\mathcal{F}|_i + 1).
\end{aligned}$$

□

Proposition E.2.16 characterises exactly when the first cohomology term of a coherent and torsion-free sheaf $\mathcal{F}$ vanishes. It does if and only if $|\mathcal{F}|_i \geq 0$ for all $i = 1, \ldots, r$ where r is the rank of $\pi_*\mathcal{F}$. Meeting the wish of the vanishing of $H^1(X, \mathcal{F})$ just if the

degree of $\mathcal{F}$ is large enough is simply not possible for reducible X in general. But the following statement shows that if we tensor with $\mathcal{O}_X(r(x)_\infty)$ for r large enough, then $H^1(X, \mathcal{F}(r(x)_\infty))$ vanishes independently of X being reducible or not.

Corollary E.2.17. *Let $\mathcal{F}$ be a coherent, torsion-free $\mathcal{O}_X$-module on X such that $\pi_*\mathcal{F}$ has rank n. Then*

$$\dim_k H^1(X, \mathcal{F}(r(x)_\infty)) = \sum_{-|\mathcal{F}|_i > r} (-|\mathcal{F}|_i - r - 1).$$

In particular, $H^1(X, \mathcal{F}(r(x)_\infty)) = 0$ if and only if $r \geq -|\mathcal{F}|_n$.

Proof. By Proposition E.2.16, we have

$$\dim_k H^1(X, \mathcal{F}(r(x)_\infty)) = -\sum_{|\mathcal{F}(r(x)_\infty)|_i < 0} (|\mathcal{F}(r(x)_\infty)|_i + 1)$$

and, by Lemma E.2.12, we have $|\mathcal{F}(r(x)_\infty)|_i = |\mathcal{F}|_i + r$ and thus we obtain

$$\begin{aligned} \dim_k H^1(X, \mathcal{F}(r(x)_\infty)) &= -\sum_{|\mathcal{F}|_i + r < 0} (|\mathcal{F}|_i + r + 1) \\ &= \sum_{-|\mathcal{F}|_i > r} (-|\mathcal{F}|_i - r - 1) \end{aligned}$$

providing both assertions. □

We have shown in Lemma 4.5.1 (i) that there is an upper bound for the π-invariants of an $\mathcal{O}_X$-ideal $\mathcal{F}$ depending on the degree of $\mathcal{F}$ and thus we obtain the following result for $\mathcal{O}_X$-ideals.

Corollary E.2.18. *Let X be reducible with irreducible components $X_1, \ldots, X_m$. Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $H^1(X, \mathcal{F}(r(x)_\infty)) = 0$ if*

$$r \geq \max_{i=1}^{m} \left\{ \frac{\deg_k \mathcal{F}_{|X_i}}{n_i} + 2c_{i,X} \right\}.$$

In particular, if $r \geq \max_{i=1}^m \{(\deg_k \mathcal{F}_{|X_i})/n_i\} + 2c_X$, then $H^1(X, \mathcal{F}(r(x)_\infty)) = 0$.

Proof. This follows from Lemma 4.5.1 (i) and Corollary E.2.17. □

Remark E.2.19. Note that if X is integral, then a similar result was already provided by Theorem 4.3.22. △

Corollary E.2.20. *Recall the definition of the arithmetic genus $g = -\chi(\mathcal{O}_X)$ in Definition 2.4.8. By Proposition E.2.16, we have $g = (\sum_{i=1}^n -|X|_i) - n$ where n denotes the rank of $\pi_*\mathcal{O}_X$. Now Corollaries 4.3.24 and 4.5.2 provide $g \leq nc_X - n = n(c_X - 1)$ and thus $g/n \leq c_X$.*

Remark E.2.21. Hence, by Definition 2.4.10, we see that if X is integral, then c_X is quite a good approximation of g/n since we have

$$\frac{g}{n} \leq c_X \leq \frac{2(g+n) + \dim_k H^0(X, \mathcal{O}_X)}{n}.$$

Moreover, if X is reducible, then we have

$$\frac{g}{n} \leq c_X \leq \max_{i=1}^{m} \left\{ \frac{2(g_i + n_i) + \dim_k H^0(X, \mathcal{O}_{X_i}) + \chi(\mathscr{S}_i)}{n_i} \right\}. \qquad \triangle$$

By Corollary E.2.17, we know that an upper bound s of the invariants $-|\mathcal{F}|_i$ shows that $H^1(X, \mathcal{F}(r(x)_\infty))$ vanishes for $r \geq s$. To give such a bound requires a bit of work, see Section 4.4.2 and Lemma 4.5.1 (i). But a lower bound can be easily derived as we will see now.

Proposition E.2.22. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then*

$$-|\mathcal{F}|_n \geq \frac{\deg_k \mathcal{F} + g}{n}.$$

Proof. By Corollary E.2.17, we have $r \geq -|\mathcal{F}|_n$ if and only if $H^1(X, \mathcal{F}(r(x)_\infty)) = 0$. Since $\mathcal{F}$ and $\mathcal{O}_X(r(x)_\infty)$ are $\mathcal{O}_X$-ideals, by Definition 3.1.15, the same is true for $\mathcal{F}(r(x)_\infty)$. Therefore, by Lemma C.4.4, we have

$$\begin{aligned}\deg_k \mathcal{F}(r(x)_\infty) &= \chi(\mathcal{O}_X) - \chi(\mathcal{F}(r(x)_\infty)) \\ &= -g - \dim_k H^0(X, \mathcal{F}(r(x)_\infty))) + \dim_k H^1(X, \mathcal{F}(r(x)_\infty)))\end{aligned}$$

which, by rearranging, provides

$$\begin{aligned}\dim_k H^1(X, \mathcal{F}(r(x)_\infty))) &= \deg_k \mathcal{F}(r(x)_\infty) + g + \dim_k H^0(X, \mathcal{F}(r(x)_\infty))) \\ &\geq \deg_k \mathcal{F}(r(x)_\infty) + g. \qquad (2{:}6)\end{aligned}$$

Now since $\mathcal{F}(r(x)_\infty) = \mathcal{F} \cdot \mathcal{O}_X(r(x)_\infty)$ and $\mathcal{O}_X(r(x)_\infty)$ is an invertible $\mathcal{O}_X$-ideal, by Lemma C.4.7, we obtain $\deg_k \mathcal{F}(r(x)_\infty) = \deg_k \mathcal{F} + \deg_k \mathcal{O}_X(r(x)_\infty)$. By combining Lemmas C.4.8 and D.2.13, we obtain $\deg_k \mathcal{O}_X(r(x)_\infty) = rn$. In particular, if

$$\dim_k H^1(X, \mathcal{F}(r(x)_\infty))) = 0,$$

by Eq. (2:6), we obtain $r \geq (\deg_k \mathcal{F} + g)/n$. Now plugging in $r = -|\mathcal{F}|_n$ we obtain the desired result. □

Corollary E.2.23. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-ideal. Then $H^1(X, \mathcal{F}) = 0$ implies $(\deg_k \mathcal{F})/n \leq -g/n$.*

Proof. By Proposition E.2.22, we have $-|\mathcal{F}|_n \geq (\deg_k \mathcal{F} + g)/n$ and, by Corollary E.2.17, we see that $H^1(X, \mathcal{F}) = 0$ if and only if $0 \geq -|\mathcal{F}|_n$. Thus $H^1(X, \mathcal{F}) = 0$ implies $0 \geq (\deg_k \mathcal{F} + g)/n$ and hence the assertion follows. □

In this section we have defined the degree of coherent and torsion-free sheaves which satisfies a kind of Riemann-Roch equation by definition. Moreover, this degree coincides with the degree of $\mathcal{O}_X$-ideals and thus we saw that $\mathcal{O}_X$-ideals do satisfy with the local definition of their degree a Riemann-Roch equation. We have characterised in Corollary E.2.17 the vanishing of $H^1(X, \mathcal{F}(r(x)_\infty))$ in terms of the π-invariants of the $\mathcal{O}_X$-ideal $\mathcal{F}$. This allowed us to give a sufficient criterion for the vanishing of $H^1(X, \mathcal{F}(r(x)_\infty))$ only dependent on the maximum of the degree of the restrictions $\mathcal{F}_{|X_i}$ and the invariant c_X. The latter part need to be emphasised since without further investigation it is not at all clear how to prove the vanishing without choosing r as large as $m \cdot \max_{i=1}^m \{\deg_k \mathcal{F}_{|X_i}\}$. We have seen in Corollary E.2.23 that $\mathcal{F}$ does indeed need to satisfy a degree condition for $H^1(X, \mathcal{F})$ to vanish, but we do not know how to provide a condition solely dependent on the degree of $\mathcal{F}$ such that $H^1(X, \mathcal{F})$ vanishes in general. Thus we have come up with a vanishing result for $H^1(X, \mathcal{F}(r(x)_\infty))$ which mimics the degree growth by multiples of n which eventually leads to the vanishing of $H^1(X, \mathcal{F}(r(x)_\infty))$. That is, instead of "*a large enough degree leads to vanishing H^1-term*" we have "*we may tensor with $\mathcal{O}_X(r(x)_\infty)$ with sufficiently large r such that the H^1-term of the resulting sheaf vanishes*".

If X is projective over k (or proper over any affine base) and $\mathcal{L}$ an ample and invertible sheaf on X, then for every coherent $\mathcal{F}$ on X there is an integer $n_0(\mathcal{F})$ such that $H^1(X, \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{L}^n) = 0$ for all $n \geq n_0(\mathcal{F})$. Moreover, in this case $\mathcal{L}^r$ is very ample for $X \to \mathrm{Spec}(k)$ for sufficiently large r. For further information, see [Liu02, 5.3.6]. Therefore, since $(x)_\infty$ is an ample divisor on X, see Proposition D.2.3, we have proven a bound for $n_0(\mathcal{F})$ dependent on the degree of $\mathcal{F}$.

Appendix F

More on π-Invariants

In this chapter we provide some more observations regarding the π-invariants $-|X|_1 \leq \ldots \leq -|X|_n$ for some cover X of $\mathbb{P}^1_k$.

In Section F.1 we observe that giving an upper bound of $-|X|_n$ is equivalent to the existence of a divisor on $\mathbb{P}^1_k$ whose pullback to X has vanishing first cohomology term. In Section F.2 we examine the explicit case of (X, π) being a cover of $\mathbb{P}^1_k$ which is embedded in $\mathbb{P}^N_k$ such that $\pi : X \to \mathbb{P}^1_k$ is given by the projection onto two coordinates. In this case we provide an explicit formula for the invariant $-|X|_n$ from which we can also give an explicit formula for the arithmetic genus of X solely in terms of its defining polynomials, N and n. If not mentioned otherwise, (X, π) will denote a cover of $\mathbb{P}^1_k$.

F.1 Relation to Divisors on $\mathbb{P}^1_k$

In this section we prove the simple observation that every upper bound for $-|X|_n$ is given by an integer $d \in \mathbb{Z}$ such that $\pi^*\mathcal{O}_{\mathbb{P}^1}(d)$ has vanishing first cohomology term.

Lemma F.1.1. *For every $d \geq 0$ there is some effective divisor $D \geq 0$ on $\mathbb{P}^1_k$ such that $\mathcal{O}_{\mathbb{P}^1}(d) \cong \mathcal{O}_{\mathbb{P}^1}(D)$.*

Proof. By [GW10, 11.14.3], we have the isomorphism $\deg : \mathrm{CaCl}(\mathbb{P}^1_k) \to \mathbb{Z}$ and thus every divisor class is characterised by its degree. Since

$$\begin{aligned}\deg \mathcal{O}_{\mathbb{P}^1}(d) &= \chi(\mathcal{O}_{\mathbb{P}^1}(d)) - \chi(\mathcal{O}_{\mathbb{P}^1}) \\ &= \underbrace{\dim_k H^0\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(d)\right)}_{=\, d+1} - \underbrace{H^1\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(d)\right)}_{=\, 0} - \underbrace{\chi(\mathcal{O}_{\mathbb{P}^1})}_{=\, 1} \\ &= d,\end{aligned}$$

we know that there is some divisor $D \in \mathrm{Div}(\mathbb{P}^1_k)$ of degree d such that $\mathcal{O}_{\mathbb{P}^1}(D) \cong \mathcal{O}_{\mathbb{P}^1}(d)$. By the theorem of Riemann-Roch, there is some homogeneous polynomial $f \in \mathcal{O}_{\mathbb{P}^1}(d)(\mathbb{P}^1_k) = k[x_0, x_1]_d$ of degree d and hence $f\mathcal{O}_{\mathbb{P}^1} \leq \mathcal{O}_{\mathbb{P}^1}(d)$. Therefore we have $\mathcal{O}_{\mathbb{P}^1}(D) \cong f^{-1}\mathcal{O}_{\mathbb{P}^1}(d) \geq \mathcal{O}_{\mathbb{P}^1}$ for some divisor D of degree d. But $\mathcal{O}_{\mathbb{P}^1}(-D) \leq \mathcal{O}_{\mathbb{P}^1}$ is equivalent to $D \geq 0$. □

Lemma F.1.2. *Let $d \in \mathbb{Z}$. Then*

$$H^1\left(X, \pi^*\mathcal{O}_Y(d)\right) \cong H^0(\mathbb{P}^1_k, \bigoplus\nolimits_{i=1}^{n} \mathcal{O}_{\mathbb{P}^1}(-|X|_i - 2 - d)).$$

Proof. Since π is finite, it is affine and thus, by [Sta18, Tag 089W], we have $H^p\left(X, \mathcal{F}\right) \cong H^p\left(\mathbb{P}^1_k, \pi_*\mathcal{F}\right)$ for every quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$. Therefore,

$$H^1\left(X, \pi^*\mathcal{O}_Y(d)\right) \cong H^1\left(\mathbb{P}^1_k, \pi_*\pi^*\mathcal{O}_Y(d)\right).$$

By [Liu02, Ex. 5.1.1 (c)], we have $\pi_*\pi^*\mathcal{O}_Y(d) \cong \pi_*\mathcal{O}_X \otimes_{\mathcal{O}_Y} \mathcal{O}_Y(d)$. Combining this with Grothendieck duality on $\mathbb{P}^1_k$ we deduce

$$\begin{aligned} H^1\left(X, \pi^*\mathcal{O}_{\mathbb{P}^1}(d)\right) &\cong H^1\left(X, \pi_*\pi^*\mathcal{O}_{\mathbb{P}^1}(d)\right) \\ &\cong H^1\left(\mathbb{P}^1_k, \pi_*\mathcal{O}_X \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(d)\right) \\ &\cong H^0\left(\mathbb{P}^1_k, (\pi_*\mathcal{O}_X \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(d))^\vee \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(-2)\right) \\ &\cong H^0(\mathbb{P}^1_k, (\bigoplus\nolimits_{i=1}^n \mathcal{O}_{\mathbb{P}^1}(-|X|_i) \otimes_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_{\mathbb{P}^1}(-d-2)) \\ &\cong H^0(\mathbb{P}^1_k, \bigoplus\nolimits_{i=1}^n \mathcal{O}_{\mathbb{P}^1}(-|X|_i - 2 - d) \end{aligned}$$

as asserted. □

Corollary F.1.3. *Let $d \in \mathbb{Z}$. Then*

$$-|X|_n < d + 2 \Leftrightarrow H^1\left(X, \pi^*\mathcal{O}_Y(d)\right) = 0.$$

Proof. By Lemma B.5.11, we have $\dim_k H^0\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1}(r)\right) = 0$ if and only if $r < 0$ and ≥ 1 otherwise. Taking dimensions in Lemma F.1.2, we therefore obtain

$$0 = \dim_k H^1\left(X, \pi^*\mathcal{O}_Y(d)\right) = \sum_{i=1}^n \dim_k \mathcal{O}_{\mathbb{P}^1}(-|X|_i - 2 - d)$$

if and only if we have $-|X|_n < d + 2$. □

F.2 Finite Morphism is the Projection onto Coordinates

In this section we examine the special case of a cover X of $\mathbb{P}^1_k$ which is embedded in some projective space $\mathbb{P}^N$ and endowed with a finite morphism onto $\mathbb{P}^1_k$ which is just the projection onto two of the coordinates of $\mathbb{P}^N$. In this case we can explicitly prove what the π-invariants are and how we may compute the arithmetic genus g from a given set of generators of the ideal cutting out X in $\mathbb{P}^N$.

Proposition F.2.1. *Let $X \subseteq \mathbb{P}^N_k$ be a cover of $\mathbb{P}^1_k$ such that*

$$X = \operatorname{Proj}(k[x_0, x_1, \ldots, x_N]/I)$$

where I is a homogeneous ideal. Assume that $I = (f_2, \ldots, f_s)$ where

$$f_i = \alpha_i\, x_i^{a_i} + \sum_{(j_0, j_1, \ldots, j_i) : \sum_{\ell=0}^i j_\ell = a_i} \alpha_{j_0, j_1, \ldots, j_i}\, x_0^{j_0} x_1^{j_1} \cdots x_i^{j_i}$$

is homogeneous of degree $a_i \geq 2$ and $\alpha_i, \alpha_{j_0, j_1, \ldots, j_i} \in k$. Moreover, assume that $\pi : X \to \mathbb{P}^1_k$ is given by projection onto the first two coordinates x_0, x_1. Then

$$g = \frac{n \cdot (\sum_{i=2}^N a_i - (N-1)) + 2n}{2} \quad \text{and} \quad -|X|_n = \sum_{i=2}^N a_i - (N-1)$$

which provides

$$-|X|_n = 2 \cdot \left(\frac{g}{n} - 1\right) \in O\left(\frac{g}{n}\right)$$

Proof. Let $A = k[x_1, x_1, \ldots, x_N]$. Let $U_i = D_+(x_i) \subseteq \mathbb{P}^1_k$ for $i = 1, 2$ be the standard affine open cover of $\mathbb{P}^1_k$ with $\mathcal{O}_{\mathbb{P}^1}(U_0) = k[x_1/x_0]$ and $\mathcal{O}_{\mathbb{P}^1}(U_1) = k[x_0/x_1]$. By assumption,

this induces the affine open cover $V_0 = D_+(x_0) \subseteq \mathbb{P}^N_k$ and $V_\infty = D_+(x_1) \subseteq \mathbb{P}^N_k$. Then, by [Liu02, 2.3.36], we have $V_0 \cong \operatorname{Spec}(A/I_{(x_0)})$ and $V_\infty \cong \operatorname{Spec}(A/I_{(x_1)})$ where $I_{(x_0)} = IA_{x_0} \cap A_{(x_0)}$ and $I_{(x_1)} = IA_{x_1} \cap A_{(x_1)}$. By Lemma 2.2.4, $\mathcal{O}_X(V_0)$ and $\mathcal{O}_X(V_\infty)$ are both free of rank n over $k[x_1/x_0]$ respectively $k[x_0/x_1]$. Moreover, by assumption, for all $i = 2, \dots, N$ the following relation holds

$$\frac{x_i}{x_0} = \frac{x_i}{x_0} \cdot \frac{x_1}{x_1} = \frac{x_i}{x_1} \cdot \frac{x_1}{x_0}.$$

Now let $x = x_1/x_0$ and $y_i = x_i/x_0$, $i \geq 2$, as well as $x^{-1} = x_0/x_1$ and $z_i = x_i/x_1$, $i \geq 2$. Then the above gives $y_i = z_i x$ for all $i = 2, \dots, N$. By assumption, we have

$$I_{(x_0)} = (f_{2,0}, \dots, f_{s,0}) \quad \text{and} \quad I_{(x_1)} = (f_{2,1}, \dots, f_{s,1})$$

where

$$\begin{aligned} f_{i,0} &= \alpha_i \, y_i^{a_i} + \sum_{(j_0, j_1, \dots, j_i) : \sum_{\ell=0}^{i} j_\ell = a_i} \alpha_{j_0, j_1, \dots, j_i} \, x^{j_1} y_2^{j_2} \cdots y_i^{j_i} \\ f_{i,1} &= \alpha_i \, z_i^{a_i} + \sum_{(j_0, j_1, \dots, j_i) : \sum_{\ell=0}^{i} j_\ell = a_i} \alpha_{j_0, j_1, \dots, j_i} \, (x^{-1})^{j_0} z_2^{j_2} \cdots z_i^{j_i}. \end{aligned}$$

Set $B_{i,0} = k[x, y_2, \dots, y_i]/(f_{2,0}, \dots, f_{i,0})$ and $B_{i,1} = k[x^{-1}, z_2, \dots, z_i]/(f_{2,1}, \dots, f_{i,1})$. Then, by the above, we have that $B_{i,0}$ is finite free of rank a_i over $B_{i-1,0}$ with basis $1, y_i, \dots, y_i^{a_i - 1}$. And similarly that $B_{i,1}$ is finite free of rank a_i over $B_{i-1,1}$ with basis $1, z_i, \dots, z_i^{a_i - 1}$. Hence $B_{N,0}$ is finite free over $k[x]$ of rank $\prod_{i=2}^N a_i$ with basis

$$\{y_2^{j_2} \cdots y_N^{j_N} \mid 0 \leq j_i \leq a_i - 1\}$$

over $k[x]$. Analogously, $B_{N,1}$ is finite free over $k[x^{-1}]$ of rank $\prod_{i=2}^N a_i$ with basis

$$\{z_2^{j_2} \cdots z_N^{j_N} \mid 0 \leq j_i \leq a_i - 1\}.$$

These two bases are now related by the relation

$$y_2^{j_2} \cdots y_N^{j_N} \cdot x^{(-\sum_{i=2}^N j_i)} = z_2^{j_2} \cdots z_N^{j_N}.$$

Now since we have found bases of R_0 and R_∞ over $k[x]$ respectively $k[x^{-1}]$ which are related by a diagonal transformation matrix whose diagonal elements are $x^{\sum_{i=2}^N j_i}$ where $0 \leq j_i \leq a_i - 1$, the set $\{\sum_{i=2}^N j_i \mid 0 \leq j_i \leq a_i - 1\}$ coincides with $\{-|X|_i \mid i = 1, \dots, n\}$, see Corollary 4.3.6. Now since $g - n = \sum_{i=1}^n -|X|_i$, we thus have

$$\begin{aligned} g - n &= \sum_{\{(j_2, \dots, j_N) \mid 0 \leq j_i \leq a_i - 1\}} \sum_{i=2}^N j_i \\ &= \sum_{(j_2, \dots, j_N)} j_2 + \ldots + \sum_{(j_2, \dots, j_N)} j_N. \end{aligned} \tag{2:1}$$

For a fixed $k \in \{2, \dots, N\}$ we have

$$\sum_{(j_2, \dots, j_N)} j_k = \sum_{(j_2, \dots, j_N), j_k = 0} j_k + \sum_{(j_2, \dots, j_N), j_k = 1} j_k + \ldots + \sum_{(j_2, \dots, j_N), j_k = N} j_k \tag{2:2}$$

and for $\ell \in \{1, \ldots, a_k - 1\}$ we have

$$\begin{aligned}\sum_{(j_2,\ldots,j_N), j_k=\ell} j_k &= \ell \cdot \#\{(j_2, \ldots, j_N) \mid j_k = \ell, 0 \leq j_i \leq a_i - 1\} \\ &= \ell \cdot \prod_{i \neq k}^{N} a_i = \ell \cdot \frac{n}{a_k}.\end{aligned}$$

We substitute this back into Eq. (2:2) and obtain

$$\sum_{(j_2,\ldots,j_N)} j_k = \sum_{\ell=1}^{N} \ell \cdot \frac{n}{a_k} = \sum_{\ell=1}^{N} \ell \cdot \frac{n}{a_k} = \frac{n}{a_k} \cdot \sum_{\ell=1}^{N} \ell = \frac{n}{a_k} \cdot \frac{a_k(a_k+1)}{2} = \frac{n(a_k+1)}{2}. \quad (2:3)$$

Substituting this back into Eq. (2:1) we finally obtain

$$\begin{aligned}g - n &= \sum_{(j_2,\ldots,j_N)} j_2 + \ldots + \sum_{(j_2,\ldots,j_N)} j_N \\ &= \frac{n(a_2+1)}{2} + \ldots + \frac{n(a_N+1)}{2} \\ &= \sum_{i=2}^{N} \frac{n(a_i+1)}{2} \\ &= \frac{n}{2} \cdot \left(\left(\sum_{i=2}^{N} a_i \right) - (N-1) \right).\end{aligned}$$

Now let $a = \sum_{i=2}^{N} a_i$. Then the above implies

$$\frac{2g}{n} = (a - (N-1)) + 2.$$

We obviously have

$$-|X|_n = \max\{\sum_{i=2}^{N} j_i \mid 0 \leq j_i \leq a_i - 1\} = \sum_{i=2}^{N} (a_i - 1) = a - (N-1)$$

which thus provides

$$-|X|_n = 2 \cdot \left(\frac{g}{n} - 1 \right) \in O\left(\frac{g}{n} \right). \qquad \square$$

Appendix G

Conclusion and Future Work

In this thesis we provide a toolkit to compute asymptotically fast in the degree zero Picard group $\mathrm{Pic}^0(X)$ of rather general algebraic curves X over a field k. In particular, these may have large genus, have singularities, be non-plane and be reducible. To the authors' best knowledge our algorithms are the first ones that implement the group law in $\mathrm{Pic}^0(X)$ for this kind of curves. Moreover, our algorithms require $O^{\sim}(n^{\omega}c_X)$ operations in k where n denotes the degree of a finite morphism $X \to \mathbb{P}^1_k$ and c_X is an invariant of X which is roughly equal to g/n where g denotes the arithmetic genus of X. In particular, our algorithms do not only enlarge the class of curves for which fast arithmetic in $\mathrm{Pic}^0(X)$ is available, but they are also at least as fast as the fastest known algorithms for irreducible, plane and non-singular curves over k.[1] Therefore, our main contribution is that we gave the problem of how to compute fast in $\mathrm{Pic}^0(X)$ a comprehensive answer by providing algorithms that implement the arithmetic in $\mathrm{Pic}^0(X)$ and that have a uniform running time.

At this point we would like to briefly discuss possible future work that may generalise our contribution to science. First of all, we can not imagine another way of implementing the arithmetic in $\mathrm{Pic}^0(X)$ which is significantly faster than ours. But there might be slight improvements and also generalisations. We conject that our general idea should work out the same way if we drop the assumption that the intersection points of irreducible components of covers of $\mathbb{P}^1_k$ do not meet S, see Definition 2.1.3 (ii). Alternatively, we believe that it should not be too hard to argue that every reduced projective curve over k admits a finite morphism to $\mathbb{P}^1_k$ satisfying Definition 2.1.3 (ii). Another possible way to generalise our result is to work over an affine base $\mathrm{Spec}(A)$ given by a ring A that is not necessarily a field k. That is, analogous to Ivey-Law who generalised in [IL12] the ideas of Khuri-Makdisi given in [KM04], there might be a way to generalise our result to suitable rings A. In [IL12] the new ground rings A (which the author called *amenable* rings) needed to admit fast linear algebra of projective modules over A. Analogously, the new ground ring for our approach should admit fast linear algebra over $A[x]$. Although this should be hard enough, another point where this should get difficult is by coming up randomly with ideal generating sets of ideals by using the probabilistic statements given in Section 6.2.2. These methods do not apply to more general rings A off-handedly. This seems to be the same reason why [IL12] could not profit from the speedup Khuri-Makdisi gave in [KM07] in contrast to [KM04].

[1] For a more thorough classification of our result with respect to the previous work, see the Abstract at the beginning of this document and Section 1.1.

List of Algorithms

List of Figures

List of Tables

List of Symbols

What follows is an overview of symbols used in this document together with the page number where they first appear.

Ideal arithmetic related symbols

$(J : I)$ $:= \{a \in \mathrm{Frac}(R) \mid aI \subseteq J\}$ quotient of two R-ideals, page 255

$V_I(T)$ $= \{P \in \mathrm{Spec}(R) \mid T \subseteq PI\}$, page 176

Divisor related symbols

$(D_{|V_0}, D_{|S_1}, \ldots, D_{|S_m})$ image of the divisor D on the cover X of $\mathbb{P}^1_k$ under the embedding $\mathrm{Div}(X) \hookrightarrow \mathrm{Div}(V_0) \times \bigoplus_{i=1}^m \mathrm{Div}(S_i)$; also denoted by $D_{|V_0} + D_{|S_1} + \ldots + D_{|S_m}$, page 128

$(D_{|V_0}, D_{|S})$ image of the divisor D on the cover X of $\mathbb{P}^1_k$ under the embedding $\mathrm{Div}(X) \hookrightarrow \mathrm{Div}(V_0) \times \mathrm{Div}(S)$; also denoted by $D_{|V_0} + D_{|S}$, page 128

$(x^{r_i})_{i,\infty}$ extension by zero of pole divisor of x on irreducible component X_i to X; given by configuration $\{(X \setminus S_i, 1), (D(h_i), x^{-r_i})\}$, page 130

$\mathrm{CaCl}(X)$ $= \mathrm{Div}(X)/\mathrm{Princ}(X)$, group of Cartier divisor classes on X, page 52

$\mathrm{CaCl}^0(X)$ $= \mathcal{D}_0(X)/\mathrm{Princ}(X)$, degree zero divisor class group of X, page 129

$\mathrm{CaCl}^0_\pi(X)$ $= \mathrm{Div}^0_\pi(X)/\mathrm{Princ}_\pi(X)$; degree zero divisor class group of X with respect to π, page 132

$\mathrm{ClInvId}(X)$ class group of invertible $\mathcal{O}_X$-ideals, page 56

$\mathrm{ClInvId}^0(X)$ group of degree zero invertible $\mathcal{O}_X$-ideals, see Definition 5.0.5, page 110

$\mathrm{Div}(X)$ $= H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$, group of Cartier divisors on X, page 52

$\mathrm{Div}^0_\pi(X)$ degree zero divisor group of X with respect to π, page 132

$\mathcal{I}_\pi$ invertible R_0-ideals whose restriction to an irreducible component $X_i \cap V_0$ of V_0 has degree $r_i n_i$ for some $r_i \in \mathbb{Z}$, page 133

$\mathrm{InvId}(X)$ group of invertible $\mathcal{O}_X$-ideals, page 56

$\mathcal{D}_0(X)$ divisors on X with degree zero restrictions to the irreducible components of X, page 129

$\mathfrak{H}$ those divisors on X restricting to a principal divisor on every component of X, page 126

$\mathfrak{K}$ kernel of the divisor restriction map $\mathrm{Div}(X) \to \bigoplus_{i=1}^m \mathrm{Div}(X_i)$, page 126

$\mathrm{MonoId}(X)$	the monoid of $\mathcal{O}_X$-ideals on X, see Definition 3.1.15, page 55
$\mathrm{Pic}(R)$	the Picard group of the ring R; the group of isomorphism classes of invertible R-modules, page 111
$\mathrm{Pic}(X)$	Picard group of the scheme X, see Definition 5.0.1, page 109
$\mathrm{Pic}^0(X)$	degree zero Picard group of X, see Definition 5.0.3, page 110
$\mathcal{P}_\pi$	principal invertible R_0-ideals whose generator satisfies the conditions of Corollary 5.6.13, page 133
$\mathrm{Princ}(X)$	subgroup of principal Cartier divisors on X, page 52
$\mathrm{Princ}_\pi(X)$	$= \mathrm{Div}^0_\pi(X) \cap \mathrm{Princ}(X)$, page 132
$\mathrm{PrincId}(X)$	group of principal invertible $\mathcal{O}_X$-ideals, page 56
$C(R)$	the group of Cartier divisors of the ring R; the group of invertible R-ideals, page 111
$D_{\|Y}$	restriction of the divisor $D \in \mathrm{Div}(X)$ to the scheme Y where $f : Y \to X$ is a morphism of schemes for which the restriction of divisors is defined; see Definition 3.2.5, page 67

Sheaf related symbols

$\mathrm{Ass}(\mathcal{F})$	associated points of the sheaf $\mathcal{F}$, page 230
$\chi_k(X, \mathcal{F})$	or $\chi(\mathcal{F})$; Euler characteristic of the $\mathcal{O}_X$-module $\mathcal{F}$ on the proper k-scheme X, page 250
$\mathcal{F}$	presheaf or sheaf (of abelian groups, rings, modules or algebras (for a fixed ring)) on a topological space X, page 215
$\mathcal{F}/\mathcal{G}$	quotient sheaf of $\mathcal{F}$ by the subsheaf $\mathcal{G}$, defined as the sheafification of $U \mapsto \mathcal{F}(U)/\mathcal{G}(U)$, page 219
$\mathcal{F}\mathcal{G}$	product of the $\mathcal{O}_X$-ideals $\mathcal{F}$ and $\mathcal{G}$, page 55
$\mathcal{F}^*$	$= \mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$ where ω_X denotes the 1-dualising sheaf on X, page 288
$\mathcal{F}^\#$	sheafification of the presheaf $\mathcal{F}$, page 219
$\mathcal{F}_P$	stalk of the presheaf or sheaf $\mathcal{F}$ at the point P, page 216
$\mathcal{F}_{\|Y}$	restriction of the sheaf $\mathcal{F}$ on X to the scheme Y where $f : Y \hookrightarrow X$ is a morphism of schemes, see Definition 3.2.25, page 67
$\mathcal{G} \leq \mathcal{F}$	the presheaf or sheaf $\mathcal{G}$ is a subpresheaf or subsheaf of $\mathcal{F}$, page 216
$\mathcal{K}_X$	sheaf of stalks of meromorphic functions of X, page 52
$\mathcal{K}'_X$	presheaf whose sheafification is $\mathcal{K}_X$, page 52
$\mathcal{R}$	sheaf of rings, page 225
$\rho^U_V(\mathcal{F})$	restriction map $\mathcal{F}(U) \to \mathcal{F}(V)$ of the presheaf $\mathcal{F}$, page 215

$\mathscr{S}$	Skyscraper sheaf sitting at intersection points of irreducible components, page 45
$\mathscr{S}_i$	Skyscraper sheaf sitting at intersection points, page 46
$\mathrm{Supp}(\mathcal{F})$	support of the sheaf $\mathcal{F}$, page 222
$f \equiv_{\cup} g$	the sections $f, g \in \mathcal{F}(U)$ of the presheaf $\mathcal{F}$ are *equal on a cover*, page 220
$f : \mathcal{F} \to \mathcal{G}$	morphism of the presheaves or sheaves $\mathcal{F}$ and $\mathcal{G}$, page 218
$f^{-1}\mathcal{G}$	inverse image of $\mathcal{G}$ under the map f, page 222
$f_*\mathcal{F}$	direct image of $\mathcal{F}$ under the map f, page 222
$f_P : \mathcal{F}_P \to \mathcal{G}_P$	morphism induced by $f : \mathcal{F} \to \mathcal{G}$ on the stalks, page 218
s_P	the germ of $s \in \mathcal{F}(U)$ at the point $P \in U$ of the presheaf $\mathcal{F}$, page 216
$s_{\|V}$	$= \rho_V^U(\mathcal{F})(s)$, restriction of the section s of $\mathcal{F}$ over U to a section of $\mathcal{F}$ over V, page 216
$\|\mathcal{F}\|_i$	the i-th π-invariant of the $\mathcal{O}_X$-ideal $\mathcal{F}$ defined in Definition 4.3.8 , page 78
$\|D\|_i$	the i-th π-invariant of the $\mathcal{O}_X$-ideal $\mathcal{O}_X(D)$ corresponding to the divisor D defined in Definition 4.3.8, page 78

Algorithm input related symbols

Σ	finite subset of the ground field k from which the randomised algorithms that try to provide ideal generating sets choose uniformly random elements to compute a Σ-random element, page 178
c	Boolean that encodes whether the input basis matrices of ideals represent the respective basis with respect to Ω_i^m (in this case, the representation depends on the **c**omponents, thus $c =$*true*) or with respect to Ω (then $c =$*false*) , page 103
$r, t \in \mathbb{Z}_{\geq 1}$	probability parameters of randomised algorithms that affect the lower bound of the probability of the respective algorithm to be successful. Here r affects the number of Σ-randomly chosen elements trying to come up with ideal generators and t affects the total number of tries coming up with an ideal generating set , page 179

Linear algebra related symbols

$(M_{i,j})_{i,j}$	matrix $M \in k[x]^{n\times n}$ defined by matrices $M_{i,j} \in k[x]^{n_i \times n_j}$ where $n = \sum_{j=1}^{m} n_j$, see Definition 4.4.6, page 89
$\mathrm{LC}(M)$	**L**eading **C**oefficient matrix of the polynomial matrix $M \in k((x^{-1}))^{n\times n}$, page 77

Running time related symbols

$\Sigma-random$	see Definition 6.2.18, page 176

$B(d)$ number of operations in a ground field k needed for computing the greatest common divisor of two univariate polynomials with degree at most d, page 211

$M(d)$ number of operations in a ground field k needed for computing the product of two univariate polynomials with degree at most d, page 211

Scheme related symbols

μ_X integer depending on whether X is irreducible or not, see Notation 5.8.1, page 156

c_i $= \left\lceil \frac{2p_a(X_i)+\chi(\mathscr{S}_i)}{n_i} \right\rceil$; invariant of the scheme X with regards to a fixed order of irreducible components $X_1, \ldots, X_m$ of X, page 145

g $= -\chi(X, \mathcal{O}_X)$; arithmetic genus of X, see Definition 2.4.8 and the discussion in Remark 2.4.7, page 48

$g(X, \mathscr{S}_X)$ $= 2p_a(X) + 2(m-1) - \chi(\mathscr{S}_X) = 2(g+m) - \chi(\mathscr{S}_X)$; invariant of the scheme X, page 145

G_0 a scheme X of dimension one is G_0 if its local rings $\mathcal{O}_{X,P}$ for $P \in X^0$ are local Gorenstein rings, page 286

$p_a(X)$ $= 1 - \chi(X, \mathcal{O}_X)$, see Definition 2.4.8, page 48

X^0 set of generic points of the irreducible components of X, page 228

X_0 set of closed points of X, page 228

$|X|_i$ the i-th π-invariant of the $\mathcal{O}_X$defined in Definition 4.3.8 , page 78

Symbols Related to *Covers of* $\mathbb{P}^1_k$

$(\omega_{i,j})_{i,j}$ $= (\omega_{i,1}, \ldots, \omega_{i,n_i})_{i=1,\ldots,m}$ basis of $\bigoplus_{i=1}^m R_{i,0}$ constituted by the reduced bases of $R_{i,0}$, page 90

$(v_{i,j})_{i,j}$ $= (v_{i,1}, \ldots, v_{i,n_i})_{i=1,\ldots,m}$ basis of $\bigoplus_{i=1}^m \mathcal{F}_i(V_{i,0})$ constituted by the reduced bases of $\mathcal{F}_i(V_{i,0})$, page 90

$(x)_\infty$ Pole divisor of the function $x \in \mathcal{K}_X(X)$ on X, page 39

$(x)_{S_i,\infty}$ $= ((x)_{X_i,\infty})_{|S_i}$, page 130

$(x)_{X_i,\infty}$ Pole divisor of the function $x \in \mathcal{K}_{X_i}(X_i)$ on X_i, page 39

$(x^r)_\infty$ $= r(x)_\infty$ multiple of the pole divisor of x of the function $x \in \mathcal{K}_X(X)$ on X, page 39

$\mathcal{F}_i$ $= \mathcal{F}_{|X_i}$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal on the cover X of $\mathbb{P}^1_k$, page 90

$\mathcal{J}_i$ $\leq \mathcal{O}_{X_i}$, sheaf of ideals on X_i cutting out $Y_{i-1} \cap X_i$ in X_i, page 89

μ $= \mu_a \circ i_\infty$; Morphism $S \to V_\infty \to X$, page 40

μ_a Morphism $S \to V_\infty$, page 40

$\mu_{a,i}$ Morphism $S_i \to V_{i,\infty}$ corresponding to $R_{i,\infty} \hookrightarrow T^{-1}R_{i,\infty}$, page 41

μ_i	Morphism $S_i \to X_i$, page 41
ν	index of $S = k[x, y]$ in R_0 where y is primitive element of $\mathcal{K}_X(X)/k(x)$ and X a cover of $\mathbb{P}^1_k$, page 186
$\mathcal{O}_\infty$	$= T^{-1}k[x^{-1}]$; local ring of $P_\infty \in \mathbb{P}^1_k$, page 40
$\mathcal{O}_S$	$= T^{-1}R_\infty$; structure sheaf of S; $\mathcal{O}_S = \bigoplus_{i=1}^m \mathcal{O}_{S_i}$, page 40
Ω	$= (\omega_1, \ldots, \omega_n)$ a fixed reduced basis of $\mathcal{O}_X$ respectively R_0, see Notation 6.1.1, page 167
Ω_i	$= (\omega_{i,1}, \ldots, \omega_{i,n_i})$ a fixed reduced basis of $\mathcal{O}_{X_i}$ respectively $R_{i,0}$, see Notation 6.1.1, page 167
Ω_i^m	$= (\omega_{i,j})_{i,j}$ the fixed basis of R_0^+ constituted by $\Omega_1, \ldots, \Omega_m$, see Notation 6.1.1, page 167
$\mathcal{O}_{S_i}$	$= T^{-1}R_{i,\infty}$; structure sheaf of S_i, page 40
$\mathbb{P}^1_k$	Projective line over the field k, page 37
π	Finite morphism $X \to \mathbb{P}^1_k$ of the cover X of $\mathbb{P}^1_k$, see Definition 2.2.1, page 37
π_i	Restriction of the finite morphism $\pi : X \to \mathbb{P}^1_k$ to X_i, page 39
$\Omega_i = \omega_{i,1}, \ldots, \omega_{i,n_i}$	fixed reduced basis of $R_{i,0}$, page 90
Ω_i^m	$= (\omega_{i,1}, \ldots, \omega_{i,n_i})_{i=1,\ldots,m}$ basis of $\bigoplus_{i=1}^m R_{i,0}$ constituted by the reduced bases of $R_{i,0}$, page 90
C_i	basis transformation matrix from $\omega_{i,1}, \ldots, \omega_{i,n_i}$ to $c_{i,1}, \ldots, c_{i,n_i}$, page 90
c_X	$\max_{i=1}^m \{c_{i,X}\}$, here X denotes a cover of $\mathbb{P}^1_k$ and $X_1, \ldots, X_m$ its irreducible components; if X is integral, then $c_X = \frac{2g+\dim_k H^0(X,\mathcal{O}_X)+n}{n}$, page 49
$c_{i,1}, \ldots, c_{i,n_i}$	reduced basis of $\mathcal{J}_i(V_{i,0})\mathcal{F}_i(V_{i,0})$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal on the cover X of $\mathbb{P}^1_k$, page 90
$c_{i,X}$	$\frac{\chi(\mathcal{S}_i)+2g_i+\dim_k H^0(X_i,\mathcal{O}_{X_i})+n_i}{n_i}$, here X denotes a cover of $\mathbb{P}^1_k$ and X_i its i-th irreducible component, page 49
D_i	$= D_{\mid X_i}$ where D is a divisor on the cover X of $\mathbb{P}^1_k$, page 90
i_∞	Open immersion $V_\infty \to X$, see Definition 2.2.1, page 37
i_0	Open immersion $V_0 \to X$, see Definition 2.2.1, page 37
m	Number of irreducible components of the cover X of $\mathbb{P}^1_k$, page 38
$M_\mathcal{F}$	basis transformation matrix from $(\omega_{i,j})_{i,j}$ to $v_1, \ldots, v_n$, page 90
M_D	basis transformation matrix from $(\omega_{i,j})_{i,j}$ to $v_1, \ldots, v_n$ for $\mathcal{F} = \mathcal{O}_X(D)$, page 90
n	Degree of the cover X of $\mathbb{P}^1_k$; equal to $\sum_{i=1}^m n_i$, page 37
n_i	Degree of the curve X_i over $\mathbb{P}^1_k$, page 39

P_∞	Point at infinity of $\mathbb{P}^1_k$, page 40
$P_{i,\infty}$	Minimal prime ideal of R_∞ corresponding to the irreducible component $V_{i,\infty}$, see Definition 2.2.6, page 39
$P_{i,0}$	Minimal prime ideal of R_0 corresponding to the irreducible component $V_{i,0}$, see Definition 2.2.6, page 39
r-dualising	of a proper morphism $\psi : X \to Y$ satisfies a duality property, see Definition E.1.1, page 284
R_∞	Coordinate ring of the affine open patch V_∞ of the cover X of $\mathbb{P}^1_k$, see Definition 2.2.1, page 37
$R_{i,\infty}$	Coordinate ring of $V_{i,\infty}$, see Definition 2.2.6, page 39
$R_{0,\infty}$	Coordinate ring of the affine open patch $V_{0,\infty}$ of the cover X of $\mathbb{P}^1_k$, see Definition 2.2.1, page 37
R_0	Coordinate ring of the affine open patch V_0 of the cover X of $\mathbb{P}^1_k$, see Definition 2.2.1, page 37
R_0^+	$= \bigoplus_{i=1}^m R_{i,0}$, coordinate ring of disjoint union of the $V_{i,0}$, see Definition 2.2.6, page 39
$R_{i,0}$	Coordinate ring of $V_{i,0}$, see Definition 2.2.6, page 39
S	Affine scheme with closed points corresponding to $\pi^{-1}(P_\infty)$, page 40
S_i	Affine scheme with closed points corresponding to $\pi_i^{-1}(P_\infty)$; irreducible component of S, page 40
T	$= k[x^{-1}] \setminus x^{-1}k[x^{-1}]$, page 40
$T_\mathcal{F}$	basis transformation matrix from $(\omega_{i,j})_{i,j}$ to $(v_{i,j})_{i,j}$, page 90
T_D	$= T_\mathcal{F}$ for $\mathcal{F} = \mathcal{O}_X(D)$, page 90
$T_{0,\mathcal{F}}$	basis transformation matrix from $(v_{i,j})_{i,j}$ to $v_1, \ldots, v_n$, page 90
$T_{\mathcal{F}_i}$	basis transformation matrix from $\omega_{i,1}, \ldots, \omega_{i,n_i}$ to $v_{i,1}, \ldots, v_{i,n_i}$, page 90
T_{D_i}	basis transformation matrix from $\omega_{i,1}, \ldots, \omega_{i,n_i}$ to $v_{i,1}, \ldots, v_{i,n_i}$ where the latter is a reduced basis of $\mathcal{O}_{X_i}(D_i)(V_{i,0})$, page 90
U_∞	Standard affine patch of $\mathbb{P}^1_k$ with coordinate ring $k[x^{-1}]$, see Definition 2.2.1, page 37
$U_{0,\infty}$	Intersection of U_0 and U_∞ with coordinate ring $k[x, x^{-1}]$, see Definition 2.2.1, page 37
U_0	Standard affine patch of $\mathbb{P}^1_k$ with coordinate ring $k[x]$, see Definition 2.2.1, page 37
V_∞	Affine patch of the cover X of $\mathbb{P}^1_k$ lying over U_∞, see Definition 2.2.1, page 37
$V_{i,\infty}$	$= V_\infty \cap X_i = \pi_i^{-1}(U_\infty)$, page 39
$V_{0,\infty}$	$= V_0 \cap V_\infty$, see Definition 2.2.1, page 37

V_0	Affine patch of the cover X of $\mathbb{P}^1_k$ lying over U_0, see Definition 2.2.1, page 37
$v_1, \ldots, v_n$	basis of $\mathcal{F}(V_0)$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal on the cover X of $\mathbb{P}^1_k$, page 89
$V_{i,0}$	$= V_0 \cap X_i = \pi_i^{-1}(U_0)$, page 39
$v_{i,1}, \ldots, v_{i,n_i}$	reduced basis of $\mathcal{F}_i(V_{i,0})$ where $\mathcal{F}$ is an $\mathcal{O}_X$-ideal on the cover X of $\mathbb{P}^1_k$, page 90
X_i	The i-th irreducible component of the cover X of $\mathbb{P}^1_k$, page 38

Glossary

Notation	Description
R-ideal	an R-ideal of the finite residual-type k-algebra R is a finitely generated R-submodule of $\mathrm{Frac}(R)$ that is invertible at the minimal primes of R, see Definition C.1.2.
Σ-random	for the subset $\Sigma \subseteq k$ of the field k, an element w of the k-vector space W with basis $w_1, \ldots, w_n$ is chosen Σ-randomly if $w = \sum_{i=1}^{n} \lambda_i w_i$ where $\lambda_1, \ldots, \lambda_n \in \Sigma$ are chosen independently and uniformly random from Σ, see Definition 6.2.18.
π-invariants	π-invariants $\lvert\mathcal{F}\rvert_1 \geq \ldots \geq \lvert\mathcal{F}\rvert_n$ of an $\mathcal{O}_X$-ideal $\mathcal{F}$ as defined in Definition 4.3.8.
ω_X-dual	for a coherent $\mathcal{O}_X$-module $\mathcal{F}$ the ω_X-dual $\mathcal{F}^*$ of $\mathcal{F}$ is given by $\mathcal{H}\mathrm{om}_{\mathcal{O}_X}(\mathcal{F}, \omega_X)$, see Definition E.2.2.
n-block-form	a matrix $M \in k[x]^{n \times n}$ is in n-block form, if there is a partition $n = \sum_{j=1}^{m} n_j$ and $M_{i,j} \in k[x]^{n_i \times n_j}$ such that $M = (M_{i,j})_{i,j}$, see Definition 4.4.6.
r-dualising	see Definition E.1.1.
$\mathcal{O}_X$-ideal	is a coherent $\mathcal{O}_X$-submodule of $\mathcal{K}_X$ which is invertible at the generic points of X, see Definition 3.1.13.
absolute curve over k	a curve of finite residual-type over k which is of finite type over k; the same as a curve over k.
arithmetic genus	arithmetic genus of the one-dimensional scheme X over k, defined as $g = -\chi_k(X, \mathcal{O}_X)$; see Definition 2.4.8.
common zeros relative to I	$V_I(T) = \{P \in \mathrm{Spec}(R) \mid T \subseteq PI\}$, see Definition 6.2.16.

Notation	Description
component dependent case	this is the approach of computing in $\mathrm{CaCl}^0_\pi(X)$ by working with representatives of the form $D + \sum_{i\in A} r_i(x)_{i,\infty}$, see Notation 5.6.31.
component independent case	this is the approach of computing in $\mathrm{CaCl}^0_\pi(X)$ by working with representatives of the form $D + r(x)_\infty$, see Notation 5.6.31.
configuration	a configuration is a weakly matching family of a global section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$ and thus represents a divisor on X.
cover of $\mathbb{P}^1_k$	a curve X over k which is projective and Cohen-Macaulay together with a finite morphism onto $\mathbb{P}^1_k$ satisfying specific conditions, see Definition 2.1.3.
curve of finite residual-type over k	separated, non-empty and noetherian scheme of dimension one over k whose irreducible components have dimension one as well.
curve over k	the same as absolute curve over k.
degree of a divisor	the degree of a divisor D on X over k is defined in Definition 3.1.10.
degree of a morphism	degree of $\pi : X \to \mathbb{P}^1_k$, where X is Cohen-Macaulay, is defined as the rank of $\pi_*\mathcal{O}_X$ as an $\mathcal{O}_{\mathbb{P}^1}$-module, see for instance Definition 2.2.2 for the case of X being a cover of $\mathbb{P}^1_k$.
degree of an $\mathcal{O}_X$-ideal	the degree of an $\mathcal{O}_X$-ideal is defined in Definition C.4.1.
degree of an R-ideal	the degree of an R-ideal is defined in Definition C.1.14.
degree zero divisor class group	defined as the quotient group $\mathrm{CaCl}^0(X) = \mathcal{D}_0(X)/\operatorname{Princ}(X)$, see Definition 5.6.1.
divisor	a global section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$, see Definition 3.1.5.
effective	a divisor D is effective if $D \geq 0$, or equivalently, if it lies in the image of $H^0\left(X, \mathcal{O}_X \cap \mathcal{K}_X^\times\right) \to \operatorname{Div}(X)$.
equal on a cover	two sections $f, g \in \mathcal{F}(U)$ are equal on a cover if there is an open cover $\{U_i \mid i \in I\}$ of U such that $f_{\mid U_i} = g_{\mid U_i}$ for all $i \in I$.

Notation	Description
Euler characteristic	the Euler characteristic of the $\mathcal{O}_X$-module $\mathcal{F}$ is defined as $\chi(\mathcal{F}) = \chi_k(X, \mathcal{F})$, see Definition B.5.13.
finite residual-type	a k-algebra R is of finite residual-type if its residual class fields have finite dimension over k, see Definition B.4.3; there is also the notion of curves of finite residual-type over k.
flasque	a sheaf $\mathcal{F}$ is *flasque* or *flabby* if every restriction map of $\mathcal{F}$ is surjective. For instance, skyscraper sheaves are flasque.
generalised vector bundle	a generalised vector bundle of rank r on a cover X of $\mathbb{P}^1_k$ is an $\mathcal{O}_X$-subsheaf of $\mathcal{K}_X^{\oplus r}$ which is free of rank r at the generic points of X.
Gorenstein in codimension 0	a scheme X of dimension one is Gorenstein in codimension 0 if $\mathcal{O}_{X,P}$ is a local Gorenstein ring for all generic points $P \in X^0$, see Definition E.1.16.
group of degree zero Cartier divisor classes	group of degree zero Cartier divisor classes is the quotient of the degree zero group of divisors by the group of principal divisors .
group of divisors	the abelian group $H^0\left(X, \mathcal{K}_X^\times / \mathcal{O}_X^\times\right)$.
group of Cartier divisor classes	group of Cartier divisor classes is the quotient of the group of divisors by the group of principal divisors .
index of N in M	for $N \subseteq M$ being free modules over the ring R, the index denotes the determinant of a basis transformation matrix from M to N, see Definition 6.3.12 for the application.
linearly equivalent	two divisors D, E are linearly equivalent if they differ additively by a principal divisor.
modification function	generators f of elements in $\mathrm{Princ}_\pi(X)$ are called modification function. If furthermore $f \in \mathcal{O}_X(D)(V_0)$ holds, then f is called modification function of D respectively $\mathcal{O}_X(D)(V_0)$, see also Definition 5.6.24.
monoid of $\mathcal{O}_X$-ideals	the monoid of $\mathcal{O}_X$-ideals on X with neutral element $\mathcal{O}_X$ and the product of $\mathcal{O}_X$-ideals as binary operation, see Definition 3.2.25.

Notation	Description
Picard group	group of isomorphism classes of invertible sheaves on a scheme X, see Definition 5.0.1.
pivot index	the pivot index of a column $v \in k[x]^{n\times 1}$ is the row index of the lowermost non-zero entry in $\mathrm{LC}(v)$, see Definition 4.4.10.
pole divisor of x	see Definition 2.2.9.
Popov form	a reduced matrix with further properties, see Definition 4.4.10.
principal divisor	a divisor defined by an element of $\mathcal{K}_X(X)^\times$; an element in the image of $H^0\left(X, \mathcal{K}_X^\times\right) \to H^0\left(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times\right)$.
pullback of meromorphic functions	along the morphism $f : Y \to X$ of schemes is defined if the morphism $f^\# : f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$ sends elements of $\mathcal{S}_X$ to $\mathcal{S}_Y$, see Definition 3.1.3.
reduced basis	a $k[x]$-basis $v_1, \ldots, v_n$ of $\mathcal{F}(V_0)$ is reduced if $\{x^j v_i \mid 1 \le i \le n, 0 \le j \le r + \lvert\mathcal{F}\rvert_i\}$ forms a k-basis of $\mathcal{F}(r(x)_\infty)(X)$ for all $r \in \mathbb{Z}$, see Theorem 4.3.15.
reduced matrix	a matrix $M \in k((x^{-1}))^{n\times n}$ is reduced if it satisfies the equivalent conditions of Definition 4.3.3.
restriction of $\mathcal{O}_X$-module	the restriction of an $\mathcal{O}_X$-module $\mathcal{F}$ along a morphism of schemes $f : Y \hookrightarrow X$ is defined as $\mathcal{F}_{\lvert Y} = f^*\mathcal{F}$, see Definition 3.2.25.
restriction of divisors	along the morphism $f : Y \hookrightarrow X$ of schemes is defined if the morphism $\mathcal{O}_X \to f_*\mathcal{O}_Y$ extends to $\mathcal{K}_X \to f_*\mathcal{K}_Y$, see Definition 3.2.5.
schematically dense	an open subset $U \subseteq X$ is schematically dense in X if it satisfies the equivalent conditions of Lemma B.2.5, see also Definition 3.2.10.
separated	a presheaf is separated if it satisfies the separatedness condition (a) in Definition B.1.1.
sheafification	the sheafification of a presheaf is defined in Definition B.1.14.
skyscraper	a sheaf is a skyscraper sheaf if it has finite support.
support of a divisor	the support of a divisor is defined as the support of it as a global section of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$.

Notation	Description
support of a section	the support of a section s of a presheaf $\mathcal{F}$ on X is the set of points $P \in X$ where the germ s_P is non-trivial (not equal to the neutral element).
support of a sheaf	the support of a sheaf $\mathcal{F}$ on X is the set of points where the stalk of $\mathcal{F}$ is non-zero.
torsion-free R-module	an R-module M is *torsion-free* if the only zero-divisor on M in R are zero-divisors of R.
torsion-free $\mathcal{O}_X$-module	a quasi-coherent sheaf $\mathcal{F}$ is *torsion-free* if for every open affine U the $\mathcal{O}_X(U)$-module M is torsion-free.
weak Popov form	a reduced matrix with whose pivot indices are distinct, see Definition 4.4.10.
weakly matching family	a weakly matching family of a global section of a presheaf $\mathcal{F}$ is a collection of sections of $\mathcal{F}$ on an open cover which are pairwise equal on a cover.
wedging element	$f \in R$ is a wedging element of $M \subseteq \mathrm{Frac}(R)$ if $fM \subseteq R$ holds.
zero relative to I	$f \in R$ has a zero at $P \in \mathrm{Spec}(R)$ relative to I if $f \in IP$, see Definition 6.2.16.

Bibliography

[Abr96] Dan Abramovich, **A linear lower bound on the gonality of modular curves**, Internat. Math. Res. Notices (1996).

[ACL20] Simon Abelard, Alain Couvreur, and Grégoire Lecerf, **Sub-Quadratic Time for Riemann-Roch Spaces: Case of Smooth Divisors over Nodal Plane Projective Curves**, Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '20, Association for Computing Machinery, 2020, p. 14–21.

[AM69] M. F. Atiyah and I. G. Macdonald, **Introduction to Commutative Algebra**, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802

[AM04] E. Arbarello and D. Mumford, **The Red Book of Varieties and Schemes: Includes the Michigan Lectures (1974) on Curves and their Jacobians**, Lecture Notes in Mathematics, Springer Berlin Heidelberg, 2004.

[Bau14] Jens-Dietrich Bauch, **Lattices over Polynomial Rings and Applications to Function Fields**, Ph.D. thesis, University of Barcelona, 2014.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, **The Magma algebra system. I. The user language**, Journal of Symbolic Computation **24** (1997), no. 3-4, 235–265.

[BH98] W. Bruns and H.J. Herzog, **Cohen-Macaulay Rings**, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1998.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, **Néron models**, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, Springer Berlin Heidelberg, 1990.

[BP94] Dario Bini and Victor Y. Pan, **Polynomial and Matrix Computations (Vol. 1): Fundamental Algorithms**, Birkhauser Verlag, Basel, Switzerland, Switzerland, 1994.

[BPoMSS02] F. Bogomolov, T. Petrov, Courant Institute of Mathematical Sciences, and American Mathematical Society, **Algebraic Curves and One-Dimensional Fields**, Courant Lecture Notes, Courant Institute of Mathematical Sciences, 2002.

[Bru13] Peter Bruin, **Computing in Picard groups of projective curves over finite fields**, Math. Comput. **82** (2013), no. 283, 1711–1756.

[BS10] Nils Bruin and Michael Stoll, **The Mordell–Weil sieve: proving non-existence of rational points on curves**, LMS Journal of Computation and Mathematics **13** (2010), 272–306.

[Can87] David G. Cantor, **Computing in the Jacobian of a hyperelliptic curve**, Mathematics of Computation **48** (1987), no. 177, 95–101.

[Car20] Raffaele Carbone, **The direct image of generalized divisors and the Norm map between compactified Jacobians**, 2020.

[CFA+05] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, **Handbook of Elliptic and Hyperelliptic Curve Cryptography**, Discrete Mathematics and Its Applications, CRC Press, 2005.

[CK91] David G. Cantor and Erich Kaltofen, **On Fast Multiplication of Polynomials over Arbitrary Algebras**, Acta Inf. **28** (1991), no. 7, 693–701.

[DG67] Jean Dieudonné and Alexander Grothendieck, **Éléments de géométrie algébrique**, Inst. Hautes Études Sci. Publ. Math. **4, 8, 11, 17, 20, 24, 28, 32** (1961–1967).

[DH06] W. Diffie and M. Hellman, **New Directions in Cryptography**, IEEE Trans. Inf. Theor. **22** (2006), no. 6, 644–654.

[Die09] Claus Diem, **On the discrete logarithm problem for plane curves**, Habilitation, University of Leipzig, 2009.

[EH14] D. Eisenbud and J. Harris, **The Geometry of Schemes**, Springer, 2014.

[Eis95] David Eisenbud, **Commutatve Algbra With A View Toward Algebraic Geometry**, Springer Verlag GmbH, 1995.

[Elg85] T. Elgamal, **A public key cryptosystem and a signature scheme based on discrete logarithms**, IEEE Transactions on Information Theory **31** (1985), no. 4, 469–472.

[Gat14] Andreas Gathmann, **Algebraic Geometry**, Lecture Notes, 2014, Available at https://www.mathematik.uni-kl.de/~gathmann/de/alggeom.php.

[Gat20] _____, **Algebraic Geometry**, Lecture Notes, 2020, Available at https://www.mathematik.uni-kl.de/~gathmann/de/alggeom.php.

[GG03] Joachim Von Zur Gathen and Jürgen Gerhard, **Modern Computer Algebra**, 2 ed., Cambridge University Press, New York, NY, USA, 2003.

[GH78] P. Griffiths and J. Harris, **Principles of Algebraic Geometry**, Wiley, 1978.

[GSSV12] Somit Gupta, Soumojit Sarkar, Arne Storjohann, and Johnny Valeriote, **Triangular X-basis Decompositions and Derandomization of Linear Algebra Algorithms over** $K[x]$, J. Symb. Comput. **47** (2012), no. 4, 422–453.

[GW10] Ulrich Görtz and Torsten Wedhorn, **Algebraic Geometry I**, Advanced Lectures in Mathematics, Vieweg + Teubner, Wiesbaden, 2010, Schemes with examples and exercises. MR 2675155

[Har77] Robin Hartshorne, **Algebraic Geometry**, Graduate texts in mathematics, Springer, New York, 1977.

[Har86] _____, **Generalized divisors on Gorenstein curves and a theorem of Noether**, J. Math. Kyoto Univ. **26** (1986), no. 3, 375–386.

[Har94] ———, **Generalized Divisors on Gorenstein Schemes**, K-Theory **8** (1994), 287–339.

[Har07] ———, **Generalized Divisors and Biliaison**, Illinois J. Math. **51** (2007), no. 1, 83–98.

[Hes99] F. Hess, **Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern**, Dissertation, Technische Universität Berlin, 1999.

[Hes02] ———, **Computing Riemann-Roch spaces in algebraic function fields and related topics**, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR 1890579

[HHSB66] F. Hirzebruch, R. Hirzebruch, R.L.E. Schwarzenberger, and A. Borel, **Topological Methods in Algebraic Geometry**, Classics in mathematics, Springer-Verlag, 1966.

[HI94] Ming-Deh A. Huang and Doug Ierardi, **Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve**, J. Symb. Comput. **18** (1994), no. 6, 519–539.

[HNES19] Seung Gyu Hyun, Vincent Neiger, and Éric Schost, **Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants**, 2019.

[Hun11] Thomas W. Hungerford, **Algebra (Graduate Texts in Mathematics)**, Springer, 2011.

[IL12] Hamish Ivey-Law, **Algorithmic Aspects of Hyperelliptic Curves and their Jacobians**, Ph.D. thesis, 2012.

[Jun16] Matthias Junge, **Asymptotisch schnelle Arithmetik in der Divisorenklassengruppe von Funktionenkörpern großen Geschlechts**, Master's thesis, University of Oldenburg, Oldenburg, Germany, 2016.

[Kal85] E Kaltofen, **Computing with Polynomials given by Straight-Line Programs I: Greatest Common Divisors**, Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '85, Association for Computing Machinery, 1985, p. 131–142.

[Kap70] I. Kaplansky, **Commutative Rings**, Allyn and Bacon, 1970.

[KGM+02] Junichi Kuroki, Masaki Gonda, Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, **Fast genus three hyperelliptic curve cryptosystems**, The 2002 Symposium on Cryptography and Information Security, Japan–SCIS 2002, 2002.

[Kle79] Steven L. Kleiman, **Misconceptions About K_X**, L'Enseignement Mathématique **25** (1979), 203–206.

[KM98] J. Kollár and S. Mori, **Birational Geometry of Algebraic Varieties**, Cambridge Tracts in Mathematics, Cambridge University Press, 1998.

[KM04] Kamal Khuri-Makdisi, **Linear algebra algorithms for divisors on an algebraic curve**, Math. Comput. **73** (2004), no. 245, 333–357.

[KM07] ———, **Asymptotically fast group operations on Jacobians of general curves**, Math. Comp. **76** (2007), no. 260, 2213–2239. MR 2336292

[Kob87] Neal Koblitz, **Elliptic Curve Cryptosystems**, Mathematics of Computation **48** (1987), 203–209.

[Kob89] _____, **Hyperelliptic Cryptosystems**, J. Cryptol. **1** (1989), no. 3, 139–150.

[Koh12] David R. Kohel, **Constructive and destructive facets of torus-based cryptography**, 2012.

[Kol18] János Kollár, **Duality and normalization, variations on a theme of Serre and Reid**.

[Lan02] Tanja Lange, **Efficient Arithmetic on Genus 2 Hyperelliptic Curves over Finite Fields via Explicit Formulae**.

[LGS20] Aude Le Gluher and Pierre-Jean Spaenlehauer, **A fast randomized geometric algorithm for computing Riemann-Roch spaces**, Mathematics of Computation **89** (2020), no. 325, 2399–2433.

[Liu02] Qing Liu, **Algebraic Geometry and Arithmetic Curves**, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232

[MCT01] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, **Fast genus two hyperelliptic curve cryptosystems**.

[Mil85] Victor S. Miller, **Use of Elliptic Curves in Cryptography**, Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings (Hugh C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer, 1985, pp. 417–426.

[Mil86] J. S. Milne, **Jacobian Varieties**, pp. 167–212, Springer New York, New York, NY, 1986.

[NU73] Yukihiko Namikawa and Kenji Ueno, **The complete classification of fibres in pencils of curves of genus two**, Manuscripta Mathematica **9** (1973), 143–186.

[Poo06] Bjorn Poonen, **Heuristics for the Brauer–Manin Obstruction for Curves**, Experiment. Math. **15** (2006), no. 4, 415–420.

[PWGP03] Jan Pelzl, Thomas Wollinger, Jorge Guajardo, and Christof Paar, **Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves**, Cryptographic Hardware and Embedded Systems - CHES 2003 (Berlin, Heidelberg), Springer Berlin Heidelberg, 2003, pp. 351–365.

[S$^+$20] W. A. Stein et al., **Sage Mathematics Software (Version x.y.z)**, The Sage Development Team, 2020, `http://www.sagemath.org`.

[Sch05] Karl Schwede, **Gluing schemes and a scheme without closed points**.

[Ser55] Jean-Pierre Serre, **Faisceaux Algebriques Coherents**, Annals of Mathematics **61** (1955), no. 2, 197–278.

[SS88] G. Scheja and U. Storch, **Lehrbuch der Algebra: Unter Einschluß der linearen Algebra**, Mathematische Leitfäden, no. Teil 2, Vieweg+Teubner Verlag, 1988.

[SS11] Soumojit Sarkar and Arne Storjohann, **Normalization of row reduced matrices**, Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '11, Association for Computing Machinery, 2011, p. 297–304.

[Sta18] The Stacks project authors, **The Stacks project**, https://stacks.math.columbia.edu, 2018.

[Sut19] Andrew Sutherland, **Fast Jacobian arithmetic for hyperelliptic curves of genus 3**, The Open Book Series **2** (2019), no. 1, 425–442.

[THPlns75] B.R. Tennison, N.J. Hitchin, Cambridge University Press, and London Mathematical Society lecture note series, **Sheaf theory**, Cambridge books online, Cambridge University Press, 1975.

[Vak18] Ravi Vakil, **Foundations of Algebraic Geometry**, Lecture Notes, 2018, Available at http://math.stanford.edu/~vakil/216blog/.

[Vol94] Emil J. Volcheck, **Computing in the Jacobian of a plane algebraic curve**, Algorithmic Number Theory (Berlin, Heidelberg) (Leonard M. Adleman and Ming-Deh Huang, eds.), Springer Berlin Heidelberg, 1994, pp. 221–233.

[Wil12] Virginia Vassilevska Williams, **Multiplying matrices faster than Coppersmith-Winograd**, Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012, 2012, pp. 887–898.

[ZL13] Wei Zhou and George Labahn, **Computing column bases of polynomial matrices**, Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '13, Association for Computing Machinery, 2013, p. 379–386.

[ZL14] ———, **Fast and deterministic computation of the determinant of a polynomial matrix**, CoRR **abs/1409.5462** (2014).

[ZLS12] Wei Zhou, George Labahn, and Arne Storjohann, **Computing Minimal Nullspace Bases**, ISSAC, 2012, pp. 366–373.