Carl von Ossietzky
Universität Oldenburg
Diplomstudiengang Mathematik

DIPLOMARBEIT

Elliptic Curves over Rings with a Point of View on Cryptography and Factoring

vorgelegt von:	Felix Fontein
Erster Betreuer:	Prof. Dr. Wiland Schmale
Zweiter Betreuer:	Prof. Dr. Heinz-Georg Quebbemann
Auswärtiger Berater bei Themenstellung und Betreuung:	Prof. Dr. Joachim Rosenthal
Oldenburg, den 28. Juni 2005	(Korrektur kleiner Fehler am 28.10.2005)

Contents

Acknowledgements

I would like to thank Prof. Dr. Joachim Rosenthal and Dr. Elisa Gorla for the idea of this thesis, for their support and encouragement.

I am deeply grateful to Dr. Elisa Gorla and Dr. Markus Dürr, who answered all my questions about algebraic geometry and the Theory of Schemes, and provided me with many hints and ideas. This thesis would not have been possible without them. I also appreciated the commitment of Prof. Dr. Markus Brodmann, Dr. Stefan Fumasoli and Dr. Mihai Halic very much.

I want to thank Jens Zumbrägel and Dr. Elisa Gorla for working through parts of my thesis and for giving me many helpful comments. Moreover, I acknowledge the proof-reading by Mirjam Langmann and Sue Landon-Jones.

I am much obliged to Prof. Dr. Wiland Schmale and Prof. Dr. Heinz-Georg Quebbemann for making all this possible and for their interest in my work.

I am indebted to the Institut für Mathematik at the University of Zurich for their hospitality and for providing me with the possibility to carry out many time-consuming computations with the computer algebra system MAGMA$^{\text{TM}}$. This thesis was typeset in LaTeX 2$_\varepsilon$, heavily using the packages AMS-TeX and XY-pic, and I would to like to thank their authors and maintainers for making these great tools freely available.

Last, but not least, I am deeply obliged to all my friends and to my family, who supported me all the time.

Chapter 1

Basics

1.1 Introduction

The idea to examine elliptic curves over (finite) rings came up between Prof. Dr. Joachim Rosenthal and Dr. Elisa Gorla during the 8th Workshop on Elliptic Curve Cryptography, which was held from September 20th to 22nd 2004 at the Ruhr-Universität Bochum, Germany.

In public key cryptography one often uses the discrete logarithm problem in a finite group as the underlying (mathematical) problem to create ciphers. The discrete logarithm problem for a group G can be formulated as follows: given two group elements $a, b \in G$, find an integer $x \in \mathbb{Z}$ such that $a^x = b$. Two kinds of groups are often used in practice: the multiplicative group of the integers modulo a huge composite number and the group of points of an elliptic curve over a finite field.

It turns out that the full structure of a group is not needed to perform public key cryptography: it is sufficient to have the structure of a semigroup or even only the structure of special kinds of loops. This is useful since most (mathematical) attacks on cryptosystems exploit the structure of the mathematical objects, like $\mathbb{Z}_n$ or the elliptic curve over a field. If objects are considered which are less structured, some kinds of attacks are not possible anymore or have to be modified at least.

The question which initiated this thesis can be formulated like this: if one drops the hypothesis that the underlying object of an elliptic curve is a field, and assumes that one only has the structure of a ring, what happens to the elliptic curve? Does their set of points still form a group? Do the addition formulae valid for elliptic curves over fields still work? What can one say about the structure of the group of points? And are there new attacks or reduction possibilities which have not been possible for elliptic curves over fields?

This thesis tries to answer these questions. We mainly concentrate on the case of commutative rings which have a unit, but also briefly consider the non-commutative case.

Before we continue we want to mention the preconditions for understanding this thesis. We assume the reader has an extensive knowledge of Linear Algebra and basic Algebra and of some basic definitions and results from Topology and Geometry. Although this thesis contains definitions of everything exceeding these essentialities, for better understanding it is recommended that the reader is familiar with Algebraic Geometry and in particular with the Theory of Schemes.

1.2 Outline of the Thesis

In this chapter we will present an overview of the results of this thesis, give some basic notations and short introductions to category theory and complexity theory.

Chapters 2 and 3 present a lot of material from Commutative Algebra and Algebraic Geometry that may not be known to everyone. In Chapter 2 many tools from Commutative Algebra, general Algebra and from Sheaf Theory are presented which are used later. Two important sections are: Section 2.4, where a requirement for doing arithmetic on elliptic curves over rings is discussed and characterized; and Section 2.5, where examples for constructing finite rings are given and which contains a discussion on how the required operations for doing arithmetic on elliptic curves over these rings can be effectively computed.

In Chapter 3 the basics of Algebraic Geometry over rings and fields are introduced, including some Theory of Schemes, curves and group schemes. Of special interest might be Sections 3.6, 3.8 and 3.9, which deal with how the affine and projective planes from the Theory of Schemes correspond to the definitions given in Section 3.1, which deal with curves over rings, and with group and Abelian schemes, respectively.

Chapter 4 deals with elliptic curves, first generally over schemes, then over fields and finally over rings. The main interest focuses on the group law, both its abstract definition using divisors and its geometric definition using Bézout's Theorem over algebraically closed fields. The structure of the group of points is analyzed and algorithms for determining the group order are given.

In the part about elliptic curves over rings an approach using the set of points is made first. The functoriality of this set is explicitly shown and used to extract information about the group structure. Then an arithmetic version of the group law is introduced, which allows the explicit computation of the sum of two points, and a geometric interpretation of elliptic curves over Artinian rings is given. Finally, an example is presented and analyzed.

Finally in Chapter 4, elliptic curves over non-commutative rings are discussed.

In Chapter 5 we will present applications for elliptic curves over rings. The chapter is divided into two parts: factoring and cryptography. In the section about factoring we will present Lenstra's Elliptic Curve Factorization Method for Integers and a generalization of this to arbitrary finite rings. The main results are the runtime analysis of this generalization, and the application of this algorithm to compute a primary decomposition of a zero-dimensional ideal in a polynomial ring $\mathbb{F}_q[x_1, \dots, x_n]$ over the Galois field $\mathbb{F}_q$ with q elements.

The second part of Chapter 5 first gives some general information on cryptography and how elliptic curves are used in cryptography. Then the hardness of two problems for elliptic curves over rings is discussed, and several existing encryption schemes using elliptic curves over rings are presented.

1.3 Results

In this section we want to give an overview of the main results developed in this thesis. The only new results are the application of elliptic curves over rings to factoring arbitrary finite rings, which is described and discussed in Section 5.1.4, and the discussion of elliptic curves over non-commutative rings in Section 4.4.

Let R be a ring. An *elliptic curve* over R is an equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \qquad a_i \in R,$$

satisfying that $\Delta(a_1, a_2, a_3, a_4, a_6) \in R^*$, where $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ is an expression introduced and explained in Chapter 4, together with the set of points $P = (x : y : z)$ in the projective plane $\mathbb{P}^2(R)$ satisfying this equation. The *projective plane* $\mathbb{P}^2(R)$ is defined as the set of triples $(x, y, z) \in R^3$ such that $\langle x, y, z\rangle = R$, and two such triples are identified if one results from the other after multiplication by an element of R; the equivalence class of the triple (x, y, z) is denoted by $(x : y : z)$. The elliptic curve is denoted by E_a with $a = (a_1, \dots, a_4, a_6)$, and the set of points by $E_a(R)$. If S is an R-algebra, one can consider the set of points $(x : y : z) \in \mathbb{P}^2(S)$, which satisfy the equation. They are denoted by $E_a(S)$.

The first result is that the mapping $S \mapsto E_a(S)$ is clearly functorial, where this *functor of points* respects products: we have $E_a(S \times S') = E_a(S) \times E_a(S')$ via the natural maps (Proposition 4.3.10). Moreover, if S is a local Artinian R-algebra with maximal ideal $\mathfrak{m}$, then the map $E_a(S) \to E_a(S/\mathfrak{m})$ is surjective and every preimage consists of exactly $|\mathfrak{m}|$ elements (Lemma 4.3.11). Therefore, if $R = \prod_{i=1}^k R_i$ is the product of local Artinian rings, and $\mathfrak{m}_i$ are the maximal ideals of R_i, we get the formula

$$|E_a(R)| = \prod_{i=1}^n |\mathfrak{m}_i| \cdot |E_a(R_i/\mathfrak{m}_i)|$$

in Corollary 4.3.12. Note that every Artinian ring can be uniquely written as such a product.

A more important result is that the set of points $E_a(S)$ can be turned into a group under the assumption that S satisfies a modest condition (see Sections 2.4 and 3.6), where the group structure is again functorial in S. While the group structure can be described very abstractly, as in Abel's Theorem 4.1.6, it can also be effectively computed using the formulae in Section 4.2.3 and the algorithm in Section 2.4 by the method described in Section 4.3.3. The proof that these two group laws are the same is of special interest: it reduces the case of any ring to the case of an algebraically closed field, where the group laws can be easily shown to be equivalent by the use of Bézout's Theorem.

There is another way to prove the result that $E_a(S)$ is functorially a group under this operation, for which the same properties hold except that one cannot know for sure that this group law is the same as the abstract one from Abel's Theorem. The idea for this proof originated from H. W. Lenstra and is described in [Len86]: the group laws can be checked by checking a set of identities in a quotient of the polynomial ring $\mathbb{Z}[a_1, \dots, a_4, a_6, x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3]$ using a computer algebra system. This idea is carried out in Proposition 4.2.19 and Corollary 4.3.17. Besides the fact that one cannot know whether this group law coincides with the algebraic one, this method has two more disadvantages: first, the proof is not very enlightening and, second, it is computationally very complex and takes a long time to verify, even with a fast computer.

By using the functoriality described above, one can partially describe the group structure for a curve over an Artinian ring by reducing it to the group structure of the residue fields $R/\mathfrak{m}$ for maximal ideals $\mathfrak{m}$ of R. The group structure for elliptic curves over finite fields is quite well-known (see, for example, Corollary 4.2.41 for the general form, Hasse's Theorem 4.2.43 for a boundary for the group cardinality, Theorem 4.2.46 for which exact cardinalities can appear, and [Sch87] and [Vol88] for the exact group structures that can appear). Only the structure of $E_a(R)$ for local Artinian rings R with maximal ideal $\mathfrak{m}$ is not known exactly, as only the structure of $E_a(R/\mathfrak{m})$ and the size of the kernel of the reduction map are known.

These results imply that problems concerning the group of elliptic curves over an Artinian ring can be split into smaller problems as soon as the Artinian ring can be effectively decomposed. Therefore, doing cryptography with elliptic curves over rings is only useful if decomposing the ring is hard (see the discussion in Section 5.2.3). Unfortunately this seems not to be the case, as for example we present a ring factorization algorithm based on Lenstra's Elliptic Curve Factorization Method for Integers in Section 5.1.4, which is conjectured to have a similar runtime estimate as Lenstra's method. The conjectures involved concern the distribution of integers with small prime factors, and they seem to be reasonable; one of them (Conjecture 5.1.9) was conjectured by H. W. Lenstra, the other (Conjecture 5.1.7) from the author of this thesis.

The last thing to mention is the discussion about elliptic curves over non-commutative rings. The first problem is how to define elliptic curves and, before that, how to define the projective plane over non-commutative rings; we stick to a naïve definition, which turns out to be of no use if one wants to use the classical formulae for adding points. The conclusion of Section 4.4 is that one probably needs to take another approach, which requires a good knowledge about non-commutative algebraic geometry that the author does not have.

1.4 Notations

We will use $A \subseteq B$ to denote that A is a subset of B or that A equals B, and $A \subsetneqq B$ if A is a subset of B but A does not equal B. We will use $|A|$ to denote the cardinality of a set A, and $A \setminus B$ to denote the difference set of two sets A and B. The natural numbers $\mathbb{N}$ include 0. We use the symbol $\sum'$ to denote a sum over a (possibly) infinite index set for which all but finitely many summands are zero.

All rings in this thesis, with the only exception being Section 4.4, are commutative and have a unit, always denoted by 1. Subrings have the same 1, and ring morphisms preserve the 1. Rings are denoted by capital letters R, S, T, etc., and ideals by old German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{m}$, etc.

If R is a ring, M an R-module and $T \subseteq M$ a subset, then $\langle T \rangle_R$ or $\langle T \rangle$ denotes the sub-R-module of M generated by T. If $T = \{x_1, \dots, x_n\}$ is finite, we often write $\langle x_1, \dots, x_n \rangle_R$ instead of $\langle \{x_1, \dots, x_n\} \rangle_R$.

The characteristic of a ring R is the uniquely determined non-negative generator of the kernel of the unique ring morphism $\mathbb{Z} \to R$. Fields are assumed to be commutative and to satisfy $1 \neq 0$. Therefore, their characteristic is either 0 or a prime. If q is a power of a prime we will write $\mathbb{F}_q$ for the finite field with q elements. If n is an integer, we will denote by $\mathbb{Z}_n$ the quotient of $\mathbb{Z}$ by the ideal $\langle n \rangle_{\mathbb{Z}}$. If p is a prime we will identify $\mathbb{Z}_p$ and $\mathbb{F}_p$.

The kernel of a morphism φ is denoted by $\ker \varphi$ and the image by $\operatorname{im} \varphi$.

If $A \in R^{n\times m}$ is a matrix, then $A_{\bullet j}$ will denote the j-th column of A, and $A_{i\bullet}$ the i-th row of A. More generally we will use $\bullet$ as a placeholder symbol; for example, $\sqrt{\bullet}$ will denote the square root map $x \mapsto \sqrt{x}$.

Zero objects, like the zero ring, the zero ideal, the zero group, the zero module, etc., are denoted simply by 0.

If a and b are elements of a commutative ring R, we say a divides b if there exists some $c \in R$ such that $ac = b$. If this is the case we write $a \mid b$ and otherwise $a \nmid b$.

Let $S = R[x_1, \dots, x_n]$ be a polynomial ring and $f \in S$. We write $\frac{\partial f}{\partial x_i}$ for the formal differentiation of f with respect to the indeterminate x_i. Furthermore, we write $f|_{x_i = a_i}$ for f evaluated in x_i with the value a_i.

If X is a set and $\sim$ an equivalence relation on X, we write $X/_\sim$ for the set of equivalence classes of $\sim$ and $[x]_\sim$ or $[x]$ for the equivalence class of $x \in X$ in $X/_\sim$.

1.5 A Short Introduction to Category Theory

In this thesis we require some category theory. We only want to give the definition of a category, of a functor, of a natural transformation, and of a product here and present several categories that we need. A more complete introduction can be found, for example, in [BW85, Chapter 1].

We will need one concept from Set Theory, namely the notion of a *class*. A class can be thought of as a "very big set" and in the cases appearing in this thesis one can simply think of classes as sets. The interested reader can find more information about this matter in many sources about Set Theory and Category Theory.

A *category* $\mathscr{C}$ is a class of *objects* $X \in \mathscr{C}$ together with a set $\mathrm{Hom}_{\mathscr{C}}(A, B)$ of *morphisms* associated to every two objects $A, B \in \mathscr{C}$, satisfying the following conditions (where we write $A \xrightarrow{f} B$ for a morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$):

(i) For every object $A \in \mathscr{C}$ there is a uniquely determined $\mathbf{id}_A \in \mathrm{Hom}_{\mathscr{C}}(A, A)$.

(ii) If $A \xrightarrow{f} B$ and $B \xrightarrow{f} C$ are morphisms for objects $A, B, C \in \mathscr{C}$, then one has a morphism $g \circ f \in \mathrm{Hom}_{\mathscr{C}}(A, C)$.

(iii) If $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ are morphisms for objects $A, B, C, D \in \mathscr{C}$, then $h \circ (g \circ f) = (h \circ g) \circ f$.

(iv) If $A \xrightarrow{f} B$ is a morphism, then $f \circ \mathbf{id}_A = f = \mathbf{id}_B \circ f$.

We will also write $f : A \to B$ for a morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$. A morphism $f : A \to B$ is an *isomorphism* if there exists a morphism $g : B \to A$ such that $f \circ g = \mathbf{id}_B$ and $g \circ f = \mathbf{id}_A$.

If $\mathscr{D}$ is another category, a *(covariant) functor* $\mathcal{F} : \mathscr{C} \to \mathscr{D}$ is a rule assigning every object $A \in \mathscr{C}$ an object $\mathcal{F}(A) \in \mathscr{D}$, and every morphism $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, $A, B \in \mathscr{C}$ a morphism $\mathcal{F}(f) \in \mathrm{Hom}_{\mathscr{D}}(\mathcal{F}(A), \mathcal{F}(B))$, such that the following relations hold:

(i) If $A \xrightarrow{f} B \xrightarrow{g} C$ are morphisms with $A, B, C \in \mathscr{C}$, then $\mathcal{F}(g \circ f) = \mathcal{F}(g) \circ \mathcal{F}(f)$.

(ii) For every $A \in \mathscr{C}$ we have $\mathcal{F}(\mathbf{id}_A) = \mathbf{id}_{\mathcal{F}(A)}$.

Thus, a functor $\mathcal{F} : \mathscr{C} \to \mathscr{D}$ induces a mapping $\mathrm{Hom}_{\mathscr{C}}(A, B) \to \mathrm{Hom}_{\mathscr{D}}(\mathcal{F}(A), \mathcal{F}(B))$ for all every pair of objects $A, B \in \mathscr{C}$. If this induced mapping is injective we call $\mathcal{F}$ *faithful*, and if it is surjective we call $\mathcal{F}$ *full*.

A *contravariant functor* $\mathcal{F} : \mathscr{C} \to \mathscr{D}$ is almost the same as a covariant functor, except that it induces a map $\mathrm{Hom}_{\mathscr{C}}(A, B) \to \mathrm{Hom}_{\mathscr{D}}(\mathcal{F}(B), \mathcal{F}(A))$ and $\mathcal{F}(g \circ f) = \mathcal{F}(f) \circ \mathcal{F}(g)$. For every category $\mathscr{C}$ one can define an *opposite category* $\mathscr{C}^{op}$ with the same objects as $\mathscr{C}$ such that the "identity functor" assigning every object to itself and every morphism to itself is a contravariant functor from $\mathscr{C}$ to $\mathscr{C}^{op}$. Clearly $(\mathscr{C}^{op})^{op} = \mathscr{C}$ and the contravariant functors $\mathscr{C} \to \mathscr{D}$ are in a natural one-to-one correspondence with the covariant functors $\mathscr{C}^{op} \to \mathscr{D}$.

If $\mathcal{F} : \mathscr{C} \to \mathscr{D}$ and $\mathcal{G} : \mathscr{D} \to \mathscr{E}$ are functors, one gets a functor $\mathcal{G} \circ \mathcal{F} : \mathscr{C} \to \mathscr{E}$. This construction yields the *Category of Categories*, whose objects are categories and whose morphisms are functors.

If $\mathscr{C}$ is a category, a *subcategory* $\mathscr{D}$ *of* $\mathscr{C}$ is a category $\mathscr{D}$, such that every object $A \in \mathscr{D}$ is also an object in $\mathscr{C}$ and for every two objects $A, B \in \mathscr{D}$, the set $\mathrm{Hom}_{\mathscr{D}}(A, B)$ is a subset of $\mathrm{Hom}_{\mathscr{C}}(A, B)$, where this inclusion preserves the identities $\mathbf{id}_A$, $A \in \mathscr{D}$ and the concatenation of morphisms. The inclusion map is a faithful functor called the *inclusion functor*. We say $\mathscr{D}$ is a *full* subcategory if the inclusion functor is full.

If $\mathcal{F}, \mathcal{G} : \mathscr{C} \to \mathscr{D}$ are two functors, a *natural transformation* $\mathscr{T} : \mathcal{F} \to \mathcal{G}$ is a rule assigning every object $A \in \mathcal{F}$ a morphism $\mathscr{T}(A) : \mathcal{F}(A) \to \mathcal{G}(A)$, such that for every morphism $f : A \to B$ the diagram

$$\begin{tikzcd}
\mathcal{F}(A) \arrow[r, "\mathscr{T}(A)"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{G}(A) \arrow[d, "\mathcal{G}(f)"] \\
\mathcal{F}(B) \arrow[r, "\mathscr{T}(B)"'] & \mathcal{G}(B)
\end{tikzcd}$$

commutes. If for every $A \in \mathscr{C}$ the morphism $\mathscr{T}(A) : \mathcal{F}(A) \to \mathcal{G}(A)$ is an isomorphism we say that $\mathscr{T}$ is an *isomorphism of* $\mathcal{F}$ *and* $\mathcal{G}$, and write $\mathcal{F} \cong \mathcal{G}$.

Let $\mathscr{C}$ and $\mathscr{D}$ be two categories and $\mathcal{F} : \mathscr{C} \to \mathscr{D}$ and $\mathcal{G} : \mathscr{D} \to \mathscr{C}$ be two functors (both either covariant or contravariant). Then $\mathscr{C}$ and $\mathscr{D}$ are called an *equivalence of categories*, and $\mathscr{C}$ and $\mathscr{D}$ are called *equivalent*, if there are isomorphisms of functors $\mathcal{F} \circ \mathcal{G} \cong \mathbf{id}_{\mathscr{D}}$ and $\mathcal{G} \circ \mathcal{F} \cong \mathbf{id}_{\mathscr{C}}$.

Let $\mathscr{C}$ be a category, I be an arbitrary index set, and for every $i \in I$, let an object $A_i \in \mathscr{C}$ be given. Then a *product* $\prod_{i \in I} A_i$ is an object $A \in \mathscr{C}$, together with morphisms $f_i : A \to A_i$ for every $i \in I$, such that for every other object $B \in \mathscr{C}$ and set of morphisms $g_i : B \to A_i$ there exists a unique morphism $g : B \to A$, such that for every i we have $f_i \circ g = g_i$. A *coproduct* $\coprod_{i \in I} A_i$ in $\mathscr{C}$ is a product of the A_i's in $\mathscr{C}^{op}$. One can easily show that if a product or coproduct exists, it is unique up to a unique isomorphism.

Finally, we want to introduce several categories:

(a) The *Category of Sets* $\mathscr{S}et$, whose objects are sets and whose morphisms are functions between these sets. Note that in literature this category is often also denoted by $\mathscr{E}ns$, standing for the French word *ensemble*.

The product in $\mathscr{S}et$ corresponds to the cartesian product, and the coproduct corresponds to the disjoint union.

(b) The *Category of Groups* $\mathscr{G}rp$ (respectively the *Category of Abelian Groups* $\mathscr{A}b$), whose objects are (Abelian) groups and whose morphisms are group morphisms.

The product in $\mathscr{A}b$ corresponds to the direct product, and the coproduct to the direct sum. In $\mathscr{G}rp$ the product corresponds to the direct product, and the coproduct of finitely many operands to the free group product.

(c) The *Category of R-algebras* $\mathscr{A}lg(R)$, R being a ring, whose objects are R-algebras and whose morphisms are R-algebra morphisms. The *Category of Rings* $\mathscr{R}ing$ is the category of $\mathbb{Z}$-algebras.

The product in $\mathscr{A}lg(R)$ corresponds to the direct product, and the coproduct of finitely many operands to the tensor product over R.

(d) If R is a ring, the *Category of R-modules* $\mathscr{M}od(R)$, whose objects are R-modules and whose morphisms are R-module morphisms.

The product in $\mathscr{M}od(R)$ corresponds to the direct product, and the coproduct to the direct sum.

1.6 A Short Introduction to Complexity Theory

In this section we want to give a small introduction to Complexity Theory. For more information see for example [HMU01] or [MvOV96, pp. 57–63, Section 2.3].

We call an algorithm *deterministic* if for every run with the same input, the same output is achieved; otherwise we call it *probabilistic* or *randomized*.

Let $f : \mathbb{N} \to \mathbb{R}_{>0}$ be a positively valued function. Define

$$\mathcal{O}(f) = \left\{ g : \mathbb{N} \to \mathbb{R}_{>0} \,\middle|\, \lim_{n\to\infty} \tfrac{g(n)}{f(n)} < \infty \right\}$$

and

$$o(f) = \left\{ g : \mathbb{N} \to \mathbb{R}_{>0} \,\middle|\, \lim_{n\to\infty} \tfrac{g(n)}{f(n)} = 0 \right\}.$$

We will often write $g = \mathcal{O}(f)$ respectively $g = o(f)$ instead of $g \in \mathcal{O}(f)$ respectively $g \in o(f)$, or simply say a function g is $\mathcal{O}(f)$ respectively $o(f)$.

Let $\mathcal{A}$ be an algorithm whose running time is bounded by $f(n) > 0$, where n is the size of the input. Then $\mathcal{A}$ is called *polynomial time bounded* if $f = \mathcal{O}(n^k)$ for some $k \in \mathbb{N}$, and *exponential time bounded* if $f = \mathcal{O}(e^n)$.

We say a problem is *deterministic* respectively *randomized bounded* by a function if there exists a deterministic respectively randomized algorithm solving the problem that is bounded by this function.

We say a problem A *reduces (in polynomial time)* to a problem B if there exists a deterministic polynomial time algorithm transforming instances of problem A into instances of problem B and converting the solution back. This means that problem A is *easier* than problem B. If A reduces to B and B reduces to A, we say that A and B are *(polynomial time) equivalent* problems. One similarly defines the notions of a *randomly polynomial time reduction* and of being *randomly polynomial time equivalent.*

Clearly, it might not only be important to consider the speed of an algorithm but also its memory consumption, but we will not discuss this here.

Chapter 2

Tools from Commutative Algebra

This chapter shall serve as a presentation of many tools from commutative algebra that are used in this thesis. Most proofs are omitted, but references to the literature are given in these cases. However, before we start with commutative algebra, we want to state an important result from group theory:

Theorem 2.0.1 (Structure Theorem for Finitely Generated Abelian Groups). *[SS88, part I, p. 261, Hauptsatz 39.8] Let G be a finitely generated Abelian group. Then there exist unique numbers $a_1, \dots, a_n \in \mathbb{N}_{>0}$ such that a_i divides a_{i+1}, $i = 1, \dots, n-1$ and either $a_1 > 1$ or $n = 1$, and a unique number $r \in \mathbb{N}$ such that*

$$G = \mathbb{Z}^r \oplus \bigoplus_{i=1}^{n} \mathbb{Z}_{a_i}.$$

From this theorem one easily gets the following corollary, which can also be proven on its own without much work, but which is of great help. Both the theorem and corollary will be intensively used in Chapter 4 to analyze the group structure of the group of points of an elliptic curve.

Corollary 2.0.2. *If G is a finite Abelian group and p a prime dividing $|G|$, then there exists an element of order p in G.*

As already stated, we will always mean a commutative ring with a unit when we talk about a ring. If R is a ring and $r \in R$, we use the following notations:

(a) We denote by R^* the group of *units* in R, i. e.

$$R^* = \{r \in R \mid \exists r' \in R : rr' = 1\}.$$

(b) If there is an element $r' \in R \setminus \{0\}$ such that $rr' = 0$, we call r a *zero-divisor.* A ring R whose only zero-divisor is 0 is called a *domain.*

(c) If r satisfies $r^2 = r$, we call r *idempotent.* As 0 and 1 are always idempotent, they are called the *trivial idempotents.*

(d) If r satisfies $r^n = 0$ for a natural number $n > 0$, we call r *nilpotent*. The smallest such n is called the *nilpotence index* of r. The set of all nilpotent elements is denoted by $\operatorname{Rad} R$, and is called the *radical* of R. In fact, it is an ideal, as we will see in Lemma 2.1.22.

(e) If $\operatorname{Rad} R = 0$ we say that R is *reduced.*

(f) We say that R is a *unique factorization domain* if it is a domain in which every non-unit $r \in R \setminus \{0\}$ can be uniquely (up to order and multiplication by units) written as the product of irreducible elements. Note that in this case every irreducible element is prime.

A very important theorem in commutative algebra is the Chinese Remainder Theorem, a generalization of the Chinese Remainder Theorem for Integers, which we will present later.

Proposition 2.0.3 (Chinese Remainder Theorem). *[Eis95, p. 79, exercise 2.6] Let R be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals in R such that $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $i \neq j$. Then*

$$R \Big/ \left(\bigcap_{i=1}^{n} \mathfrak{a}_i \right) \cong \prod_{i=1}^{n} R/\mathfrak{a}_i.$$

In commutative algebra, objects that satisfy a chain condition are of special interest. These chain conditions impose a lot of additional structure that is needed for many results. In particular the Artinian condition will turn out to be very strong, and the class of Artinian rings will be the class of rings for which all methods developed in this thesis will work.

Definition 2.0.4. *Let R be a ring.*

(a) *We call R* Artinian *if every descending chain of ideals eventually becomes stationary, i. e. if for every chain of ideals*

$$\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \mathfrak{a}_3 \supseteq \cdots$$

in R there is an $n_0 > 0$ such that $\mathfrak{a}_{n+1} = \mathfrak{a}_n$ for all $n \geq n_0$.

(b) *We call R* Noetherian *if every ascending chain of ideals eventually becomes stationary, i. e. if for every chain of ideals*

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$$

in R there is an $n_0 > 0$ such that $\mathfrak{a}_{n+1} = \mathfrak{a}_n$ for all $n \geq n_0$.

Remark 2.0.5. Clearly, every finite ring R is Artinian and Noetherian, as well as every field. On the other hand, the integers $\mathbb{Z}$ are Noetherian but not Artinian.

Note that finite rings are of main interest in applications (see Chapter 5). We next characterize the property of being Noetherian by the ideals in R and state two important mechanisms that can be used to generate new Noetherian rings from Noetherian rings.

Proposition 2.0.6. *Let R be a ring.*

(a) *[Eis95, pp. 46f, Exercise 1.1] A ring is Noetherian if, and only if, each of its ideals is finitely generated.*

(b) *[Eis95, p. 27, Theorem 1.2] (*Hilbert Basis Theorem*) If R is Noetherian, then so is $R[x_1, \ldots, x_n]$.*

(c) *[Eis95, p. 28, Corollary 1.3] If $\mathfrak{a} \subseteq R$ is an ideal in a Noetherian ring, then $R/\mathfrak{a}$ is Noetherian.*

2.1 Nilpotents, Ideals and Some Tools

2.1.1 Taylor Expansion and the Newton-Hensel Lemma

The material in this section is based on the books [SS88, parts I and II]. Our aim is to prove the Lemma of Newton-Hensel, which raises zeros of a polynomial in $R/\mathfrak{a}$ to zeros in R, where $\mathfrak{a}$ is an ideal only containing nilpotent elements. We will need this result in Chapter 4 and it will allow us to describe the points on an elliptic curve over a ring R if the points of the curve over $R/\mathfrak{a}$ are known.

For this we need an analogon to the Taylor expansion from analysis, which we will state first:

Proposition 2.1.1 (Taylor Expansion). *[SS88, part II, p. 26, 52.5] Let $f \in R[x_1, \ldots, x_n]$ and $a \in R^n$. Then there exists a unique family $(a_\alpha)_{\alpha \in \mathbb{N}^n} \in R^{\mathbb{N}^n}$ with only finitely many elements $\neq 0$, such that*

$$f = \sum_{\alpha \in \mathbb{N}^n}{}' a_\alpha (x - a)^\alpha \in R[x_1, \ldots, x_n],$$

where $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$. Moreover, one has $\alpha! \cdot a_\alpha = \frac{\partial^{|\alpha|} f}{\partial x^\alpha}(a)$, where $\alpha! = \prod_{i=1}^n \alpha_i$ and $\frac{\partial^{|\alpha|}}{\partial x^\alpha} = \frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_n}}{\partial x_n^{\alpha_n}}$.

Corollary 2.1.2. *Let $f \in R[y]$ and $x, t \in R$. Then there exists an $s \in R$ such that*

$$f(x + t) = f(x) + \frac{\partial f}{\partial y}(x)t + st^2.$$

In fact, if x is fixed, s is a polynomial over R in t.

As already mentioned, nilpotent ring elements and ideals play an important role in this thesis. We will now state some facts about nilpotent ideals and ideals consisting only of nilpotent elements.

Definition 2.1.3. *Let R be a ring and $\mathfrak{a} \subseteq R$ an ideal.*

(a) *If every element of $\mathfrak{a}$ is nilpotent, i. e. if $\mathfrak{a} \subseteq \operatorname{Rad} R$, then $\mathfrak{a}$ is called a* nilideal.

(b) *If $\mathfrak{a}^n = 0$ for some $n \in \mathbb{N}_{>0}$, then $\mathfrak{a}$ is called* nilpotent*. The smallest integer n, such that $\mathfrak{a}^n = 0$, is called the* nilpotence index *of $\mathfrak{a}$.*

Lemma 2.1.4. *Let R be a ring and $r \in R$ be nilpotent. Then for $a \in R$ we have $a - r \in R^*$ if, and only if, $a \in R^*$.*

Proof. Let $n > 0$ be the nilpotence index of $\mathfrak{a}$. We only have to show that $a \in R^*$ implies $a - r \in R^*$, the other direction follows by using the same argument with $(a - r)$ and $(a - r) - (-r)$. The remainder of the proof is shown in [SS88, part I, p. 91, 15.1(3)]. □

Lemma 2.1.5. *If $\mathfrak{a}$ is a nilpotent ideal in a ring R, then the sequence $\mathfrak{a}^n$ strictly decreases until it eventually becomes zero.*

Proof. Assume $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ for some n. Then $\mathfrak{a}^{n+k} = \mathfrak{a}^{n+1}\mathfrak{a}^{k-1} = \mathfrak{a}^n\mathfrak{a}^{k-1} = \mathfrak{a}^{n+k-1}$ if $k > 1$ and, therefore, $\mathfrak{a}^{n+k} = \mathfrak{a}^n$ for every $k \geq 0$. Thus, it must hold that $\mathfrak{a}^n = 0$ since $\mathfrak{a}$ is nilpotent. □

If an ideal is finitely generated, it is nilpotent if, and only if, it is a nilideal. We will show this in the following two lemmas:

Lemma 2.1.6. *Let R be a ring and $\mathfrak{a}$ a nilideal in R. If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}$ is nilpotent.*

Proof. We show this by induction on the number of generators. If $\mathfrak{a} = \langle r \rangle$, and r is nilpotent, then surely $\mathfrak{a}$ is nilpotent. Now assume $\mathfrak{a} = \mathfrak{a}_1 + \mathfrak{a}_2$, where $\mathfrak{a}_i$ is nilpotent with index n_i. Every element of $(\mathfrak{a}_1 + \mathfrak{a}_2)^{n_1+n_2}$ is a sum of elements of the form $r = \prod_{i=1}^{n_1+n_2} r_i$, where $r_i \in \mathfrak{a}_1 \cup \mathfrak{a}_2$. If more than n_1 of the r_i's are in $\mathfrak{a}_1$, then $r \in \mathfrak{a}_1^{n_1} = 0$, and otherwise $r \in \mathfrak{a}_2^{n_2} = 0$. □

Lemma 2.1.7. *Let R be a ring and $\mathfrak{a}$ an ideal in R generated by nilpotent elements. Then $\mathfrak{a}$ is a nilideal.*

Proof. Since the generators are a subset of $\operatorname{Rad} R$, clearly $\mathfrak{a} \subseteq \operatorname{Rad} R$ since $\operatorname{Rad} R$ is an ideal. □

Corollary 2.1.8. *In a Noetherian ring, an ideal is nilpotent if, and only if, it is a nilideal.*

Proof. Let R be a Noetherian ring and $\mathfrak{a} \subseteq R$ an ideal. If $\mathfrak{a}$ is a nilideal, by Lemma 2.1.6 it is nilpotent, since it is finitely generated by the Noetherian assumption. On the contrary, if $\mathfrak{a}$ is not a nilideal, it contains an element $x \in R$ which is not nilpotent. But then $0 \neq x^n \in \mathfrak{a}^n$ for every $n \in \mathbb{N}$. Hence, $\mathfrak{a}$ is not nilpotent either. □

We can now state the Lemma of Newton-Hensel, a version of the well-known Lemma of Hensel. This version can also be found in [SS88, part II, p. 727f].

Proposition 2.1.9 (Lemma of Newton-Hensel). *Let R be a ring and $\mathfrak{a} \subseteq R$ a nilideal. If $f \in R[x]$ is a polynomial and $a \in R$ such that $f(a) = 0$ in $R/\mathfrak{a}$, and $\frac{\partial f}{\partial x}(a)$ is a unit in $R/\mathfrak{a}$, then there exists a unique $\hat{a} \in R$ such that $a - \hat{a} \in \mathfrak{a}$ and $f(\hat{a}) = 0$ in R.*

Proof. First consider the case where $\mathfrak{a}$ is nilpotent. We construct a sequence $a_n \in R$, $n \in \mathbb{N}$, such that $a_n - a \in \mathfrak{a}$ and $f(a_n) \in \mathfrak{a}^{n+1}$. Since $\mathfrak{a}$ is nilpotent, eventually $f(a_n) = 0$.

Choose $g \in R$ such that $g = (\frac{\partial f}{\partial x}(a))^{-1}$ in $R/\mathfrak{a}$, and define $a_0 := a$ and $a_{n+1} := a_n - gf(a_n)$ for $n \in \mathbb{N}$. For $n = 0$, we clearly have $a_0 - a \in \mathfrak{a}$ and $f(a_0) \in \mathfrak{a}^1$. Now assume the assertions hold for some $n \geq 0$. Clearly we have $a_{n+1} - a_n = -gf(a_n) \in \mathfrak{a}$ and, hence, $a_{n+1} - a \in \mathfrak{a}$. By Corollary 2.1.2, for $x = a_n$ and $t = -gf(a_n)$ we get an $e \in R$ such that

$$\begin{aligned} f(a_{n+1}) &= f(x+t) = f(x) + \tfrac{\partial f}{\partial x}(x)t + et^2 \\ &= f(a_n) - g\tfrac{\partial f}{\partial x}(a_n)f(a_n) + e \cdot g^2 f(a_n)^2 \\ &= f(a_n)(1 - g\tfrac{\partial f}{\partial x}(a_n)) + g^2 f(a_n)^2 e. \end{aligned}$$

Now $1 - g\frac{\partial f}{\partial x}(a_n) \in \mathfrak{a}$, since $g\frac{\partial f}{\partial x}(a_n) = g\frac{\partial f}{\partial x}(a) = 1$ in $R/\mathfrak{a}$. Hence, $f(a_{n+1}) \in \mathfrak{a}^{(n+1)+1} + \mathfrak{a}^{2(n+1)} = \mathfrak{a}^{n+2}$. Thus, the assertions also hold for a_{n+1}.

If we consider the case where $\mathfrak{a}$ is a nilideal, the construction above still works, since one can operate in the subring R' of R generated by a, g, and by the coefficients of f. This ring is clearly Noetherian as being a finitely generated $\mathbb{Z}$-algebra. Thus, the nilideal $\mathfrak{a}' = \mathfrak{a} \cap R'$ is finitely generated and, hence, is nilpotent by Lemma 2.1.6. Since we still have $a_n - a \in \mathfrak{a}'$ and $f(a_n) \in (\mathfrak{a}')^{n+1}$ for all $n \in \mathbb{N}$, the sequence a_n still eventually gives a solution.

To show uniqueness, let $\hat{a}' \in R$ be another solution, i. e. we have $f(\hat{a}') = 0$ and $\hat{a}' - a \in \mathfrak{a}$. By plugging $x = \hat{a}$ and $t = \hat{a}' - \hat{a}$ into Corollary 2.1.2, we get an $e \in R$ such that

$$\begin{aligned} 0 = f(\hat{a}') &= f(x+t) = f(x) + \tfrac{\partial f}{\partial x}(x)t + et^2 \\ &= f(\hat{a}) + \tfrac{\partial f}{\partial x}(\hat{a})(\hat{a}' - \hat{a}) + (\hat{a}' - \hat{a})^2 e = (\hat{a}' - \hat{a})c, \end{aligned}$$

where $c := \frac{\partial f}{\partial x}(\hat{a}) + e(\hat{a}' - \hat{a})$. In $R/\mathfrak{a}$, we see that $c = \frac{\partial f}{\partial x}(\hat{a})$ is a unit and, therefore, there exists some $b \in R$ and $d \in \mathfrak{a}$ such that $bc = 1 + d$. Since d is nilpotent, we see that bc is a unit in R by Lemma 2.1.4. Therefore, c also has to be a unit and, hence, $\hat{a} = \hat{a}'$. □

Remark 2.1.10. Note that the proof gives a method to effectively compute $\hat{a}$ from a.

2.1.2 Resultants

Resultants allows to effectively compute whether two univariate polynomials have a common factor, by evaluating the determinant of a matrix. Moreover, resultants can be used to check whether a univariate polynomial has multiple roots in the algebraic closure. The latter will be the main use of resultants in this thesis, as we want to ensure for elliptic curves that a cubic polynomial has only simple roots.

Let $\mathbb{F}$ be an arbitrary field. We start with defining and characterizing what a multiple or simple root is for a univariate polynomial.

Definition 2.1.11. *Let $f \in \mathbb{F}[x]$. Then f has a* multiple root *in $a \in \mathbb{F}$ if we can write $f = (x-a)^2 h$, where $h \in \mathbb{F}[x]$. If $f(a) = 0$, but a is not a multiple root, we say f has a* simple root *in a.*

Lemma 2.1.12. *Let $f \in \mathbb{F}[x] \setminus \mathbb{F}$ a polynomial. Then f has a multiple root in $a \in \mathbb{F}$ if, and only if, $f(a) = 0 = \frac{\partial f}{\partial x}(a)$.*

Proof. This follows directly from Corollary 2.1.2. □

The next characterization of when a polynomial has no multiple roots over the algebraic closure can be used to effectively compute whether this is the case. However, this is not very useful as it does not easily allow the evaluation of a 'check polynomial' in the coefficients of the polynomial f and to simply test if the result is zero. This will be possible with resultants.

Lemma 2.1.13. *Let $f \in \mathbb{F}[x] \setminus \mathbb{F}$. Then f has no multiple roots over the algebraic closure of $\mathbb{F}$ if, and only if, f and $\frac{\partial f}{\partial x}$ are coprime.*

Proof. If f has a multiple root in $a \in \overline{\mathbb{F}}$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$, then $f = (x-a)^2 h$ where $h \in \overline{\mathbb{F}}[x]$, and $\frac{\partial f}{\partial x} = (x-a)\tilde{h}$ with $\tilde{h} \in \overline{\mathbb{F}}[x]$. Then the minimal polynomial of a over $\mathbb{F}$ divides both f and $\frac{\partial f}{\partial x}$ and, hence, they are not coprime.

For the other direction, assume f and $\frac{\partial f}{\partial x}$ have a common factor $h \in \mathbb{F}[x] \setminus \mathbb{F}$. Then h has a root in the algebraic closure $\overline{\mathbb{F}}$, which is thus a common root of f and $\frac{\partial f}{\partial x}$ and, therefore, it is a multiple root of f by Lemma 2.1.12. □

We will now define the resultant of two polynomials and state the main result.

Definition 2.1.14. *[CLO96, pp. 150f, Definition 7] Let $f, g \in \mathbb{F}[x]$, where $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ with $n = \deg f > 0$ and $m = \deg g > 0$. Define the* Sylvester matrix *of f and g as*

$$\operatorname{Syl}(f,g) := \left(\begin{array}{cccc|cccc} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ a_n & & \ddots & 0 & b_m & & \ddots & 0 \\ 0 & \ddots & & a_0 & 0 & \ddots & & b_0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{array}\right) \in \mathbb{K}^{(n+m)\times(n+m)}.$$

The resultant *of f and g is defined as*

$$\operatorname{Res}(f,g) := \det \operatorname{Syl}(f,g) \in \mathbb{F}.$$

Proposition 2.1.15. *[CLO96, p. 151, Proposition 8] Let $f, g \in \mathbb{F}[x] \setminus \mathbb{F}$ be two polynomials. Then f and g are coprime if, and only if, $\operatorname{Res}(f,g) \neq 0$.*

The following corollary provides a special case of this result, which is needed for our main application, namely testing whether a polynomial has multiple roots over the algebraic closure.

Corollary 2.1.16. *Let $f \in \mathbb{F}[x] \setminus \mathbb{F}$. Then f has no multiple roots over the algebraic closure of $\mathbb{F}$ if $\operatorname{Res}\big(f, \frac{\partial f}{\partial x}\big) \neq 0$. In particular:*

(a) *If $f = x^2 + ax + b$, then*

$$\operatorname{Res}\big(f, \tfrac{\partial f}{\partial x}\big) = \det \begin{pmatrix} b & a & 0 \\ a & 2 & a \\ 1 & 0 & 2 \end{pmatrix} = 4b + a^2 - 2a^2 = 4b - a^2.$$

(b) *If $f = x^3 + ax^2 + bx + c$, then*

$$\begin{aligned}\operatorname{Res}\big(f, \tfrac{\partial f}{\partial x}\big) &= \det \begin{pmatrix} c & 0 & b & 0 & 0 \\ b & c & 2a & b & 0 \\ a & b & 3 & 2a & b \\ 1 & a & 0 & 3 & 2a \\ 0 & 1 & 0 & 0 & 3 \end{pmatrix} \\ &= 4a^3c - 18abc + 27c^2 - a^2b^2 + 4b^3.\end{aligned}$$

Consider the special case $a = 0$. Then

$$\operatorname{Res}\big(f, \tfrac{\partial f}{\partial x}\big) = 27c^2 + 4b^3.$$

Proof. By Lemma 2.1.13 we know that f has no multiple roots over $\overline{\mathbb{F}}$ if, and only if, f and $\frac{\partial f}{\partial x}$ are coprime, which by Proposition 2.1.15 is the case if, and only if, the resultant is non-zero. □

2.1.3 Prime and Radical Ideals

In commutative algebra and algebraic geometry, prime ideals and radical ideals appear in many places. We want to state two facts about prime ideals, introduce radical ideals, and state some of their important properties.

The first result shows how to construct prime ideals with a certain property.

Definition 2.1.17. *Let R be a ring. A* multiplicative subset *of R is a subset $S \subseteq R$ such that $1 \in S$, and for every $a, b \in S$ we also have $ab \in S$.*

Example 2.1.18. Let R be a ring and $\mathfrak{a}$ an ideal in R. Then $R \setminus \mathfrak{a}$ is a multiplicative subset if, and only if, $\mathfrak{a}$ is prime.

Lemma 2.1.19. *[Eis95, p. 70, Proposition 2.11] Assume S is a multiplicative subset of a ring R and $\mathfrak{a}$ is an ideal not meeting S. Then there exists a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ but not meeting S.*

To be more exact, $\mathfrak{p}$ can be taken as an ideal maximal with respect to the property that it contains $\mathfrak{a}$ but does not meet S.

If $\mathfrak{p}$ is a prime ideal in R and $ab \in \mathfrak{p}$ for $a, b \in R$, then either $a \in R$ or $b \in R$. The same holds if one replaces a and b by arbitrary ideals $\mathfrak{a}$ and $\mathfrak{b}$ in R:

Lemma 2.1.20. *Let R be a ring, $\mathfrak{p} \subseteq R$ a prime ideal, and $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq R$ ideals such that $\prod_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$. Then there exists an i such that $\mathfrak{a}_i \subseteq \mathfrak{p}$.*

Proof. Assume that $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ for every i. Then for every i there exists an $a_i \in \mathfrak{a}_i$ such that $a_i \notin \mathfrak{p}$. Consider $\prod_{i=1}^n a_i \in \prod_{i=1}^n \mathfrak{a}_i$; since $\mathfrak{p}$ is prime, there must exist one i such that $a_i \in \mathfrak{p}$, which is a contradiction. □

We now proceed to define the radical of an ideal.

Definition 2.1.21. *Let R be a ring and $\mathfrak{a}$ an ideal in R. Define the* radical *of $\mathfrak{a}$ to be the set*

$$\sqrt{\mathfrak{a}} := \{f \in R \mid f^n \in \mathfrak{a} \textit{ for some } n \geq 1\}.$$

If $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then $\mathfrak{a}$ is called a radical ideal.

If $R = \mathbb{F}[x_1, \ldots, x_n]$ for a field and $\mathfrak{a}$ is an ideal in R, one can consider the set of common zeros of all $f \in \mathfrak{a}$. Then the set of the common zeros of all $f \in \sqrt{\mathfrak{a}}$ is the same as that of $\mathfrak{a}$. In fact, if $\mathbb{F}$ is algebraically closed we will see that $\sqrt{\mathfrak{a}}$ contains any other ideal sharing this property. Next, we want to state several properties of radicals and radical ideals:

Lemma 2.1.22. *[Eis95, p. 33] Let R be a ring and $\mathfrak{a}$ an ideal in R.*

(1) *We have that* $\operatorname{Rad} R = \sqrt{0}$.

(2) *The radical $\sqrt{\mathfrak{a}}$ of an ideal $\mathfrak{a}$ is again an ideal in R, and it is a radical ideal.*

(3) *If $\mathfrak{a} \subseteq \mathfrak{b}$ is a chain of ideals, then $\sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{b}}$.*

(4) *If $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ is radical.*

(5) *[Eis95, p. 71, Corollary 2.12] If $\mathfrak{a} \neq R$ is an ideal in R, then*

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \textit{ prime and } \mathfrak{a} \subseteq \mathfrak{p}\}.$$

2.1.4 Tensor Products

Let R be an arbitrary commutative ring with a unit. The tensor product is the coproduct in the category of R-algebras and has, similar to prime ideals, an important position in commutative algebra and algebraic geometry. We first state the definition and its existence before we show how it can be used.

Definition 2.1.23. *Let M and N be R-modules. An R-module T, together with an R-bilinear map $b : M \times N \to T$, is called the* tensor product of M and N *if it fulfills the following universal property:*

If L is another R-module and $\varphi : M \times N \to L$ a bilinear map, then there exists a unique R-linear map $\psi : T \to L$ such that $\psi \circ b = \varphi$.

We use the notation $x \otimes y$ for $b(x, y)$ if $x \in M$, $y \in N$, and write $M \otimes_R N$ for T, or simply $M \otimes N$ if R is clear from the context.

Remarks 2.1.24.

(a) [Eis95, p. 573] If the tensor product of two R-modules M and N exists, it is unique up to isomorphism. Thus, it is justified to talk about *the* tensor product of M and N.

(b) [Eis95, p. 573] Moreover, since the set of all bilinear maps from $M \times N$ to L is the same as $\operatorname{Hom}_R(M, \operatorname{Hom}_R(N, L))$, one can rephrase the universal property as
$$\operatorname{Hom}_R(M \otimes N, L) \cong \operatorname{Hom}_R(M, \operatorname{Hom}_R(N, L)).$$

(c) The tensor product of two R-algebras is again an R-algebra by $(a \otimes b)(c \otimes d) := (ac) \otimes (bd)$.

Proposition 2.1.25. *[Eis95, p. 573] In the category of R-modules, tensor products do exist.*

Sketch of Proof. Let M and N be two R-modules. Consider the free R-module $\tilde{T}$ generated by all formal objects of the form $x \otimes y$ for $x \in M$, $y \in N$, and consider the submodule T' generated by all elements of the form

$$(\lambda x + \lambda' x') \otimes (\mu y + \mu' y') - \lambda\mu(x \otimes y) - \lambda'\mu(x' \otimes y) - \lambda\mu'(x \otimes y') - \lambda'\mu'(x' \otimes y'),$$

where $x, x' \in M$, $y, y' \in N$ and $\lambda, \lambda', \mu, \mu' \in R$. We define $T := \tilde{T}/T'$ and $b : M \times N \to T$ by $(x, y) \mapsto x \otimes y$. From the definition of T' it follows directly that b is bilinear. One shows that T is the tensor product of M and N and that $b : M \times N \to T$ is the associated bilinear map. □

Now we will state several basic properties of the tensor product, beginning with its functoriality.

Proposition 2.1.26. *If M, N and L are R-modules and $\varphi : M \to N$ is a morphism, there exists a unique morphism $M \otimes L \to N \otimes L$, mapping $x \otimes z$ onto $\varphi(x) \otimes z$ for $x \in M$, $z \in L$. Hence, $\bullet \otimes_R L$ is a functor from the category of R-modules to the category of R-modules.*

Proof. It is easy to see that there is exactly one homomorphism $x \otimes z \mapsto \varphi(x) \otimes z$. □

Proposition 2.1.27. *See [Eis95, p. 574, Proposition A2.1]. Let M, N and L be R-modules.*

(1) *We have that $M \otimes (N \otimes L) \cong (M \otimes N) \otimes L$ by a natural isomorphism, given by $x \otimes (y \otimes z) \mapsto (x \otimes y) \otimes z$.*

(2) *We have that $M \otimes N \cong N \otimes M$ by a natural isomorphism, given by $x \otimes y \mapsto y \otimes x$.*

(3) *We have that $(\bigoplus_{i \in I} M_i) \otimes L \cong \bigoplus_{i \in I}(M_i \otimes L)$.*

(4) *If $M \to N \to P \to 0$ is a right-exact sequence with another R-module P, then $(M \otimes L) \to (N \otimes L) \to (P \otimes L) \to 0$ is right-exact.*

Flatness The property of being flat has a very important geometric interpretation (see for example Section 3.4.2 and [EH00, pp. 70–81]). We first want to cover the algebraic aspects.

Definition 2.1.28. *Let L be an R-module. Then L is called* flat *over R, or R-*flat*, if for every left-exact sequence of R-modules $0 \to M \to N \to P$ the sequence*

$$0 \longrightarrow (M \otimes L) \longrightarrow (N \otimes L) \longrightarrow (P \otimes L)$$

is still left-exact. A morphism $R \to S$ of rings is said to be flat *if it makes S flat as an R-module. An R-algebra S is* flat *if $R \to S$ is flat.*

Remark 2.1.29. Thus, by Proposition 2.1.27 (4), L is flat if, and only if, the functor $\bullet \otimes_R L$ is exact, i. e. it preserves short exact sequences.

We will now show that some rings which we will need later are flat over a base ring. We will later learn of another important class in Section 2.2.1.

Proposition 2.1.30. *Let R be a ring and let F be a free R-module. Then F is flat over R.*

Proof. This follows directly from $M \otimes_R R \cong M$ and Proposition 2.1.27 (3). □

Corollary 2.1.31. *Let R be a ring and $S = R[x_1, \dots, x_n]$. Then S is flat over R.*

Proof. Obviously, S is a free R-module (of infinite rank) and, therefore, flat over R by Proposition 2.1.30. □

To prove one of the main results of this subsection we first need two lemmas. One is the Snake Lemma from homological algebra, and the second one gives a criterion when tensoring preserves injections and surjections.

Lemma 2.1.32 (Snake Lemma). *[Eis95, pp. 640f, Exercise A3.10] Let R be a ring. Let the following diagram of R-modules be commutative and have exact rows:*

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

Then there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \ker\alpha \arrow[r] & \ker\beta \arrow[r] & \ker\gamma \arrow[dll] & \\
 & \operatorname{coker}\alpha \arrow[r] & \operatorname{coker}\beta \arrow[r] & \operatorname{coker}\gamma \arrow[r] & 0.
\end{tikzcd}$$

Lemma 2.1.33. *Let R be a ring, S an R-module, $\varphi : S \to S$ an R-module morphism and M another R-module. Consider the morphism $\varphi \otimes \mathbf{id}_M : S \otimes M \to S \otimes M$ from Proposition 2.1.26, which is defined by $s \otimes m \mapsto \varphi(s) \otimes m$.*

(a) *If φ is injective, then so is $\varphi \otimes \mathbf{id}_M$.*

(b) *If φ is surjective, then so is $\varphi \otimes \mathbf{id}_M$.*

(c) *If φ is bijective, then so is $\varphi \otimes \mathbf{id}_M$.*

Proof.

(a) Let N be the free R-module generated by the $s \otimes m$, $s \in S$, $m \in M$, and P the sub-R-module of N such that $N/P = S \otimes M$ (see the proof of Proposition 2.1.25 for the exact definition of P). One clearly sees that the R-linear map $\psi : N \to N$, $s \otimes m \mapsto \varphi(s) \otimes m$ is injective on N, and we have that $\psi(P) \subseteq P$ and $\psi(\complement P) \subseteq \complement P$. Therefore, ψ induces an injective map on $N/P = S \otimes M$, which is clearly $\varphi \otimes \mathbf{id}_M$.

(b) This follows from $\bullet \otimes_R M$ being right-exact by Proposition 2.1.27 (d).

(c) Follows from (a) and (b). □

The following result will be of great help in Proposition 2.3.17, which in turn will be useful in Section 3.8.2 where we present a class of curves over rings.

Proposition 2.1.34. *Let R be a ring, S a flat R-algebra and $f \in S$ a non-zero-divisor. Then $S/\langle f \rangle$ is flat over R.*

Proof. The idea for this proof is from [Bro05]. Consider the map "multiplication by f" on S, denoted by $\times f$, which is clearly injective since f is a non-zero-divisor. Consider the sequence

$$\begin{tikzcd}
0 \arrow[r] & S \arrow[r, hook, "\times f"] & S \arrow[r, two heads] & S/\langle f \rangle \arrow[r] & 0;
\end{tikzcd}$$

since $\operatorname{im}(\times f) = \langle f \rangle = \ker(S \to S/\langle f \rangle)$ it is exact. Let

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, hook] & N \arrow[r, two heads] & P \arrow[r] & 0
\end{tikzcd}$$

be an exact sequence of R-modules. Since tensoring is always right-exact, S is flat over R and, by the previous lemma, we know that all rows and columns in the following diagram are exact, where $K = \ker(M \otimes_R S/\langle f \rangle \to N \otimes_R S/\langle f \rangle)$:

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
K \arrow[r] & M \otimes_R S/\langle f \rangle \arrow[r] \arrow[u] & N \otimes_R S/\langle f \rangle \arrow[r, two heads] \arrow[u] & P \otimes_R S/\langle f \rangle \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & M \otimes_R S \arrow[r, hook] \arrow[u, two heads] & N \otimes_R S \arrow[r, two heads] \arrow[u, two heads] & P \otimes_R S \arrow[r] \arrow[u, two heads] & 0 \\
0 \arrow[r] & M \otimes_R S \arrow[r, hook] \arrow[u, hook, "\mathbf{id}_M \otimes (\times f)"'] & N \otimes_R S \arrow[r, two heads] \arrow[u, hook, "\mathbf{id}_N \otimes (\times f)"'] & P \otimes_R S \arrow[r] \arrow[u, hook, "\mathbf{id}_P \otimes (\times f)"'] & 0 \\
 & 0 \arrow[u] & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

Clearly this diagram is commutative. We have to show $K = 0$. However, by the Snake Lemma 2.1.32 with $\alpha = \mathbf{id}_M \otimes_R (\times f)$, $\beta = \mathbf{id}_N \otimes_R (\times f)$ and $\gamma = \mathbf{id}_P \otimes_R (\times f)$, we get that $K = \ker(\mathbf{id}_P \otimes_R (\times f)) = 0$. □

Tensoring of Polynomial Rings The tensor product is very powerful for modifying finitely generated R-algebras. We want to present several methods we will need later in this thesis.

Lemma 2.1.35. *[SS88, part II, pp. 591f, §82, Beispiel 7] Let R be a ring, $\varphi : R \to T$ a ring morphism and $S = R[x_1, \dots, x_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$ in $R[x_1, \dots, x_n]$. Then*

$$S \otimes_R T \cong S_T, \qquad \text{where } S_T := T[x_1, \dots, x_n]/\langle \varphi(\mathfrak{a}) \rangle_T .$$

Lemma 2.1.36. *[SS88, part II, pp. 591f, §82, Beispiel 7] Let R be a ring, $A = R[x_1, \dots, x_n]/\mathfrak{a}$, $B = R[y_1, \dots, y_m]/\mathfrak{b}$ and $S = R[x_1, \dots, x_n, y_1, \dots, y_m]/\langle \mathfrak{a}, \mathfrak{b} \rangle$. Then $A \otimes_R B \cong S$ by the isomorphism $f \otimes g \mapsto fg$.*

Multilinear Algebra Before closing this subsection we want to state some definitions from multilinear algebra, which are needed in algebraic geometry.

Definition 2.1.37. *[Eis95, p. 575] Let R be a ring and M be an R-module.*

(a) *The* tensor algebra $T_R(M)$ *is the graded (see Section 2.3.1), non-commutative R-algebra*

$$T_R(M) := \bigoplus_{n=0}^{\infty} M^{\otimes n},$$

where $M^{\otimes n}$ is the n-fold tensor product of M with itself, with the two special cases $M^{\otimes 0} = R$ and $M^{\otimes 1} = M$. The product of $x_1 \otimes \cdots \otimes x_n \in M^{\otimes n}$ and $y_1 \otimes \cdots \otimes y_m \in M^{\otimes m}$ is

$$x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_m \in M^{\otimes(n+m)}.$$

(b) *The* exterior algebra $\bigwedge_R M$ *is the algebra obtained from $T_R(M)$ by factoring by the two-sided ideal generated by the elements $x \otimes x$, $x \in M$.*

(c) *The* n-th exterior power $\bigwedge_R^n M$ *is the degree-n-component of the graded algebra $\bigwedge_R M$.*

2.2 Rings

In this section we want to look at several classes of rings. Local rings often appear in commutative algebra and algebraic geometry; they can, for example, be obtained from arbitrary rings by localizing at a prime ideal. This will be examined in Section 2.2.1. In the next section we will cover Artinian rings, which turn out to be Noetherian and have important properties. They share several properties with finite rings, which we need later in this thesis. Finally we will state some results from the Theory of Fields, which will also be needed later.

However, before looking at local rings, we want to emphasize two important properties of idempotent elements:

Remark 2.2.1. Let R be a ring, M be an R-module and $e \in \operatorname{End}(M)$ be an idempotent endomorphism. Then e is a projection onto $\operatorname{im} e$ in the sense that $e|_{\operatorname{im} e} = \mathbf{id}_{\operatorname{im} e}$:

Let $v = e(w) \in \operatorname{im} e$ for some $w \in M$. Then $e(v) = e(e(w)) = e^2(w) = e(w) = v$.

Assume $M = R$ and $e \in R$ to be idempotent. Then the map $x \mapsto ex$ is an idempotent R-module endomorphism. This can be used to decompose the ring if e is a non-trivial idempotent:

Proposition 2.2.2. *Let R be a ring and $e \in R$ be a non-trivial idempotent. Then R can be decomposed as the product of two non-zero rings R_1 and R_2, where $R_1 = eR$ and $R_2 = (1-e)R$.*

Proof. If e is idempotent, we have $(1-e)^2 = 1 - 2e + e^2 = 1 - e$, so $1 - e$ is also idempotent. In addition, it is clear that R_1 and R_2 are non-zero, since neither e nor $1 - e$ is 0.

To show that R_1 is a ring, it suffices to show that R_1 has a unit. If $er \in R_1$, then $e(er) = e^2 r = er$, and since $e = e1 \in R_1$, this is the unit element of R_1.

Furthermore, it is trivial to see that $r \mapsto er$ is a surjective ring morphism from R to R_1.

As the same is also true for R_2 and the surjective ring morphism $R \to R_2$, we will show next that the combined morphism $\varphi : R \to R_1 \times R_2$, $r \mapsto (er, (1-e)r)$ is a ring isomorphism. If $\varphi(r) = 0$, then $er = 0 = (1-e)r = r - er$ and, hence r must be 0 and φ is injective. If $(er_1, (1-e)r_2) \in R_1 \times R_2$, we get

$$\begin{aligned}\varphi(er_1 + (1-e)r_2) &= (e^2 r_1 + e(1-e)r_2, (1-e)er_1 + (1-e)^2 r_2)\\ &= (er_1, (1-e)r_2),\end{aligned}$$

so φ is also surjective. □

Next, we want to define two classes of rings that often appear, in particular in algebraic geometry:

Definition 2.2.3. *Let R denote a ring. We say that R is* local *if it has a unique maximal ideal.*

Definition 2.2.4. *Let G be a totally ordered Abelian group.*

(a) *A* valuation *on a field $\mathbb{F}$ is a group morphism $v : \mathbb{F}^* \to G$ that satisfies $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in \mathbb{F}^*$, $x \neq -y$.*

(b) *Let R be a local ring with maximal ideal $\mathfrak{m}$, which is a domain. Let $\mathbb{F}$ be the field of fractions of R. Then R is a* valuation ring *if there exists a valuation $v : \mathbb{F}^* \to G$ such that*

  (i) $R = \{0\} \cup \{x \in \mathbb{F}^* \mid v(x) \geq 0\}$ *and*

  (ii) $\mathfrak{m} = \{0\} \cup \{x \in \mathbb{F}^* \mid v(x) > 0\}$.

(c) *A valuation ring is called a* discrete valuation ring *if $G = (\mathbb{Z}, +, \leq)$.*

We will come back to valuations in Chapter 3. Before studying local rings in more detail we want to introduce a finiteness condition for R-algebras over an arbitrary ring R:

Definition 2.2.5. *Let R be a ring. An R-algebra S is* of finite presentation *if $S \cong R[x_1, \ldots, x_n]/\mathfrak{a}$ for some $n \in \mathbb{N}$ and some finitely generated ideal $\mathfrak{a} \subseteq R[x_1, \ldots, x_n]$.*

2.2.1 Local Rings and Localization

As already noted, local rings are an important class of rings. We want to characterize local rings and to introduce a powerful tool called localization. This tool allows several problems and questions to be reduced from arbitrary rings to local rings.

Proposition 2.2.6. *[SS88, part I, p. 248, §37, Aufgabe 13] Let R be a ring. Then the following are equivalent:*

(i) *The ring R is local.*

(ii) *The non-units of R form an ideal.*

(iii) *The non-units of R form an additive subgroup.*

(iv) *For every $r \in R$, at least one of r and $1 - r$ is in R^*.*

Hence, in a local ring R we have that $r \in R$ is a unit if, and only if, $r + s$ is a unit for any non-unit $s \in R$.

If R is an Artinian ring, more characterizations of being local can be given for R, as we will see in Section 2.2.2.

Next, we will concentrate on the concept of localization. We will follow the book of Eisenbud ([Eis95, pp. 59ff]). Localization generalizes the concept of forming the field of quotients of a domain to arbitrary rings.

Definition 2.2.7. *Let R be a ring.*

(1) *If S is a multiplicative subset of R and M is an R-module, denote by $S^{-1}M$ or $M[S^{-1}]$ the equivalence classes of elements $(s, m) \in S \times M$ under the equivalence relation*

$$(s, m) \sim (s', m') :\Longleftrightarrow \exists u \in S : u(ms' - m's) = 0.$$

We call $M[S^{-1}]$ the localization of M at S*, and we will write m/s for $[(s, m)]_\sim$.*

(2) *If $\mathfrak{p}$ is a prime ideal in R, by definition $S := R \setminus \mathfrak{p}$ is a multiplicative subset of R. Define $M_\mathfrak{p} := S^{-1}M$ as the* localization of M with respect to $\mathfrak{p}$.

(3) *For any $f \in R$ denote by R_f the localization at the multiplicative subset $S := \{f^i \mid i \in \mathbb{N}\}$.*

Remarks 2.2.8. [Eis95, pp. 59f] Let R be a ring, M be an R-module and $S \subseteq R$ be a multiplicative set.

(1) It is easy to see that $\sim$ is an equivalence relation.

(2) By defining $r(m/s) := (rm)/s$ and $(m/s)+(m'/s') := (ms'+ms)/(ss')$, we turn $S^{-1}M$ into an R-module.

(3) Since R is itself an R-module, we can also form $S^{-1}R$. By defining $(r/s) \cdot (r'/s') := (rr')/(ss')$, $S^{-1}R$ becomes a ring. Furthermore, $S^{-1}M$ has an $S^{-1}R$-module structure, given by $(r/s)(m/s') := (rm)/(ss')$.

(4) We have a natural map $M \to S^{-1}M$, $m \mapsto m/1$, which is an R-module homomorphism.

(5) The natural map $\varphi : R \to S^{-1}R$ is a ring homomorphism and it is injective if, and only if, S contains no zero-divisors. More precisely, an element $m \in M$ maps to zero if, and only if, it is annihilated by an element in S, i. e. $sm = 0$ for some $s \in S$.

(6) If $\mathfrak{p}$ is a prime ideal in R, then $R_\mathfrak{p}$ is a local ring with maximal ideal $\{r/s \in R_\mathfrak{p} \mid r \in \mathfrak{p},\ s \notin \mathfrak{p}\}$.

(7) If $\varphi : M \to N$ is a morphism of R-modules, then $S^{-1}\varphi := \tilde{\varphi} : S^{-1}M \to S^{-1}N$, $m/s \mapsto \varphi(m)/s$ is a morphism of $S^{-1}R$-modules, which commutes with the natural maps $M \to S^{-1}M$ and $N \to S^{-1}N$. Moreover, if $\psi : N \to L$ is another morphism of R-modules, then $S^{-1}(\psi \circ \varphi) = (S^{-1}\psi) \circ (S^{-1}\varphi)$.

Thus in categorical language, localization at S is a functor from the category of R-modules to the category of $S^{-1}R$-modules:

$$\mathscr{M}od(R) \to \mathscr{M}od(S^{-1}R), \qquad M \mapsto S^{-1}M.$$

We now give an important example of how a problem in arbitrary rings can be reduced to a problem in local rings obtained by localization:

Lemma 2.2.9. *[Eis95, pp. 67p, Lemma 2.8] Let R be a ring and M be an R-module.*

(a) *An element $m \in M$ is zero if, and only if, it goes to zero in each localization at a maximal ideal $\mathfrak{m}$ of R.*

(b) *We have that $M = 0$ if, and only if, $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of R.*

The case $M = R$ gives a useful corollary of (a):

Corollary 2.2.10. *Let R be a ring and $r \in R$. Then $r = 0$ if, and only if, for every maximal ideal $\mathfrak{m}$ of R, $r/1 = 0/1$ in $R_{\mathfrak{m}}$.*

For this reason we say that being zero is a *local property*: to show an element or module is zero, it is enough to show that it is zero in the localization at every prime ideal. There are several properties in commutative algebra and algebraic geometry that turn out to be local; this hints at why prime ideals are important.

We want to emphasize that the localization of an R-module can also be described in terms of the localization of R and tensoring:

Proposition 2.2.11. *Let S be a multiplicative subset of R.*

(1) *[Eis95, p. 65, Lemma 2.4] If M is an R-module, then $S^{-1}M \cong M \otimes_R S^{-1}R$.*

(2) *[Eis95, p. 66, Proposition 2.5] The R-module $S^{-1}R$ is flat.*

Remark 2.2.12. Let S be a multiplicative subset of R. We have that $(S^{-1}R)^n = S^{-1}(R^n) =: S^{-1}R^n$ for any $n \in \mathbb{N}$. More generally, if M_i, $i \in I$, are R-modules, then $S^{-1}\bigoplus_{i\in I} M_i = \bigoplus_{i\in I}(S^{-1}M_i)$.

Proof. This follows from Proposition 2.1.27 and Proposition 2.2.11. □

We introduce the following notation: if $\mathfrak{p}$ is a prime ideal in R, $v \in R^n$, and $A \in R^{n\times m}$, we write $v_{\mathfrak{p}} \in R_{\mathfrak{p}}^n$ and $A_{\mathfrak{p}} \in R_{\mathfrak{p}}^{n\times m}$ for the component-wise images of v and A under the natural map $R \to R_{\mathfrak{p}}$.

Lemma 2.2.13. *Let $v_1, \ldots, v_m \in R^n$, and let $P = \sum_i Rv_i$ be the R-module generated by the v_i's. Let $\mathfrak{p}$ be a prime ideal in R. Then $P_{\mathfrak{p}}$ is the $R_{\mathfrak{p}}$-module generated by the $v_{i,\mathfrak{p}}$'s.*

Proof. Let $v_i = (v_{i,j})_j \in R^n$ and, hence, $v_{i,\mathfrak{p}} = (v_{i,j}/1)_j \in R^n_{\mathfrak{p}}$. Now we have $P = \{\sum \lambda_i v_i \mid \lambda_i \in R\}$ and, according to Definition 2.2.7,

$$P_{\mathfrak{p}} = \left\{ \left(\sum\nolimits' \lambda_i v_i \right) / s \;\middle|\; \lambda_i \in R,\ s \notin \mathfrak{p} \right\}.$$

Since clearly $(\sum' \lambda_i v_i)/s = \sum' \lambda_i / s \cdot v_i / 1$, we have $P_{\mathfrak{p}} = \{\sum' \lambda_i / s \cdot v_{i,\mathfrak{p}} \mid \lambda_i \in R,\ s \notin \mathfrak{p}\}$ and, hence, $P_{\mathfrak{p}}$ is contained in the $R_{\mathfrak{p}}$-module generated by the $v_{i,\mathfrak{p}}$. But since $P_{\mathfrak{p}}$ also contains the $v_{i,\mathfrak{p}}$, these two modules must be the same. □

The next lemma shows that being injective, surjective or bijective for a R-module morphism is also a local property.

Lemma 2.2.14. *[Eis95, p. 68, Corollary 2.9] Let $\varphi : M \to N$ be a morphism of R-modules.*

(a) *Then φ is injective if, and only if, $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every prime $\mathfrak{p}$.*

(b) *Then φ is surjective if, and only if, $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for every prime $\mathfrak{p}$.*

(c) *Then φ is bijective if, and only if, $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is bijective for every prime $\mathfrak{p}$.*

These statements also hold if we replace "every prime $\mathfrak{p}$" by "every maximal ideal $\mathfrak{m}$".

There is a close connection between the ideals in the ring and the ideals in a localization of it. This will be in particular important in the Theory of Schemes, as it allows us to only look at all the prime ideals not meeting a given multiplicative system. If the multiplicative system is taken from a prime ideal $\mathfrak{p}$, this allows us to look at all prime ideals contained in $\mathfrak{p}$.

Proposition 2.2.15. *[Eis95, p. 61, Proposition 2.2] Let R be a ring and S a multiplicative subset of R, and let $\varphi : R \to S^{-1}R$ be the natural map.*

(a) *For any ideal $\mathfrak{a}$ of $S^{-1}R$ we have $\varphi^{-1}(\mathfrak{a})S^{-1}R = \mathfrak{a}$.*

(b) *The map $\mathfrak{a} \mapsto \varphi^{-1}(\mathfrak{a})$ is an injection from the set of ideals of $S^{-1}R$ into the set of ideals of R. This map preserves ordering by inclusion, intersections and the property of being prime.*

(c) *Let $\mathfrak{b}$ be an ideal of R. Then the following are equivalent:*

   (i) *There is an ideal $\mathfrak{a}$ of $S^{-1}R$ such that $\mathfrak{b} = \varphi^{-1}(\mathfrak{a})$.*

   (ii) *It is $\mathfrak{b} = \varphi^{-1}(\mathfrak{b}S^{-1}R)$.*

   (iii) *Every $s \in S$ is a non-zero-divisor modulo $\mathfrak{b}$, i. e. if $rs \in \mathfrak{b}$ for some $r \in R$, then $r \in \mathfrak{b}$.*

(d) *The map $\mathfrak{a} \mapsto \varphi^{-1}(\mathfrak{a})$ induces an order-preserving bijection between the primes of $S^{-1}R$ and the primes of R which do not meet S.*

This proposition also shows that the chain conditions we have introduced earlier are preserved by localization:

Corollary 2.2.16. *If R is Noetherian (respectively Artinian) and S is a multiplicative subset of R, then $S^{-1}R$ is Noetherian (respectively Artinian).*

Proof. This follows directly from Proposition 2.2.15 (b). □

2.2.2 Artinian Rings

In this section we will examine a class of rings that trivially contains all finite rings and which plays an important role in this thesis. We will begin by following Chapter 2 of [Eis95].

Definition 2.2.17. *Let R be a ring and M be an R-module.*

(a) *A* chain *of submodules of M of* length n *is a chain*

$$M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_0 = M,$$

where the M_i are submodules of M.

(b) *We call M* simple *if the only submodules of M are* 0 *and M itself.*

(c) *If $M_n \subseteq \cdots \subseteq M_0 = M$ is a chain of submodules and M_{i-1}/M_i is simple and non-trivial for $i = 1, \ldots, n$, then this chain is called a* composition series.

(d) *The* length of M *is the infimum of all lengths of composition series of M. If M has no finite composition series its lenght is ∞.*

(e) *We call M* Noetherian *respectively* Artinian *if every ascending respectively descending chain of submodules eventually becomes stationary.*

Remark 2.2.18. One directly sees that a ring R is Noetherian respectively Artinian if, and only if, it has the same property as an R-module. Moreover, an R-module is Noetherian if, and only if, every sub-R-module is finitely generated. Note that a non-zero, simple R-module is isomorphic to $R/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal.

The property of being Artinian can be characterized for a ring as follows. Interestingly, being Artinian implies being Noetherian.

Proposition 2.2.19. *[Eis95, p. 74, Theorem 2.14] For a ring R the following conditions are equivalent:*

(a) *The ring R is Artinian.*

(b) *The ring R is Noetherian and every prime ideal is maximal.*

(c) *Seen as an R-module, R has finite length.*

In every of these cases, R only has a finite number of prime ideals.

The first main result of this subsection is the structure theorem for Artinian rings, which will be used extensively in this thesis:

Corollary 2.2.20 (Structure Theorem for Artinian Rings). *[Eis95, p. 76, Corollary 2.16 and its proof] If R is an Artinian ring, then R is the finite product of local Artinian rings. To be exact, we have a ring isomorphism*

$$R \cong \bigoplus_{\mathfrak{m} \in \mathfrak{M}} R_{\mathfrak{m}},$$

where $\mathfrak{M}$ is the set of all maximal ideals of R.

We will now concentrate on local Artinian rings. Local Artinian rings can be characterized using nilpotent elements:

Lemma 2.2.21. *Let R be an Artinian ring. Then R is local if, and only if, every non-unit is nilpotent. Moreover, if R is a local Artinian ring, its maximal ideal is nilpotent.*

Proof. Since

$$\operatorname{Rad} R = \sqrt{0} = \bigcap \{\mathfrak{p} \mid \mathfrak{p} \text{ prime of } R\}$$

by Lemma 2.1.22, and since the primes of R are exactly the maximal ideals of R by Proposition 2.2.19, we see that every non-unit is nilpotent if, and only if, $\operatorname{Rad} R$ is the unique maximal ideal of R.

Now $\operatorname{Rad} R$ is clearly a nilideal. However, since R is Artinian, it is Noetherian by Proposition 2.2.19 and, hence, $\operatorname{Rad} R$ is finitely generated. The last statement follows from Lemma 2.1.6. □

The following property, being known from finite rings, shows that Artinian rings might be a good generalization of finite rings in a certain sense:

Lemma 2.2.22. *Let R be an Artinian ring and $r \in R$. Then r is either a zero-divisor or a unit.*

Proof. First assume R is local. Then, according to Lemma 2.2.21, every non-unit is nilpotent. If R is not local, write $R = \prod_{i=1}^{n} R_i$ with local Artinian rings R_i. If $r \in R$ is a unit, then its projection onto every R_i is a unit. If r is not a unit, the projection $r1_{R_i}$ onto one R_i is nilpotent and, therefore, a zero-divisor in R_i. For this i choose an element $s \in R_i \setminus \{0\}$ such that $s(r1_{R_i}) = 0$. But then $sr = (s1_{R_i})r = s(r1_{R_i}) = 0$ in R. □

Now we will state a useful characterization of when an Artinian ring is local:

Corollary 2.2.23. *Let R be an Artinian ring. The following are equivalent:*

(i) *The ring R is local.*

(ii) *The quotient $R/\operatorname{Rad} R$ is a field.*

(iii) *The only idempotents in R are the trivial ones.*

(iv) *If R can be decomposed into the product of two rings R_1 and R_2, then either $R_1 = 0$ or $R_2 = 0$.*

(v) *Every non-unit is nilpotent.*

Proof. We have already seen that (i) and (v) are equivalent (Lemma 2.2.21). Clearly, (v) implies (ii). If (ii) holds, then $\operatorname{Rad} R$ must be a maximal ideal. Since $\operatorname{Rad} R = \sqrt{0}$ is the intersection of all maximal ideals, R can only have one maximal ideal and is thus local.

We also have that (v) implies (iii), since if $a^2 = a$, then $a^n = a^{n-1} = \cdots = a^2 = a$ for all $n > 0$. If $a \neq 0$, then a must be a unit, but the only idempotent unit is 1.

If (iv) holds, then by Proposition 2.2.2, (iii) also holds. If (iv) does not hold, say $R = R_1 \times R_2$ with $R_1 \neq 0 \neq R_2$, then 1_{R_1} and 1_{R_2} are nontrivial idempotents in R; therefore (iii) implies (iv).

Assume R is not local. Then since R can be written as the product of local Artinian rings by Corollary 2.2.20, R must be the product of at least two non-zero rings. This shows that (iv) implies (i). □

2.2.3 Some Facts About Fields

In this subsection we want to present many facts about fields that will be particularly useful in Chapters 3 and 4.

Let $\mathbb{F}$ denote a field.

The Frobenius Morphism and Perfect Fields The Frobenius endomorphism is a very important endomorphism on rings with prime characteristic. For example it allows us to characterize finite fields, and it also has an important use in algebraic geometry. This finally leads us to Hasse's Theorem, which allows us to find a boundary for the number of $\mathbb{F}_q$-rational points of an elliptic curve.

Definition 2.2.24. *Let R be a ring of prime characteristic $p > 0$, and let $q \neq 1$ be a power of p. Then the* q-th power Frobenius morphism *is the map $R \to R$, $x \mapsto x^q$. If $q = p$, we simply call $x \mapsto x^p$ the* Frobenius morphism.

Remarks 2.2.25.

(a) The q-th power Frobenius morphism is indeed a ring morphism, since $\binom{i}{p} = 0 \in R$ for $1 \leq i < p$ and since $x \mapsto x^q$ is the n-fold concatenation of $x \mapsto x^p$ if $q = p^n$.

(b) If R is reduced, then the Frobenius morphism is injective.

Perfect fields are fields that behave well with respect to testing whether a polynomial is square-free using Euclid's algorithm. In fact, there is a close connection between perfect fields, the Frobenius endomorphism and the Galois Theory, which we will see later.

Definition 2.2.26. *A field $\mathbb{F}$ is* perfect *if the following holds: every polynomial $f \in \mathbb{F}[x] \setminus \mathbb{F}$ is square-free if, and only if, f and $\frac{\partial f}{\partial x}$ are coprime.*

Remark 2.2.27. For any field $\mathbb{F}$ we have that if $f \in \mathbb{F}[x] \setminus \mathbb{F}$ is not square-free, then f and $\frac{\partial f}{\partial x}$ are not coprime. (See also Lemma 2.1.13.)

Proposition 2.2.28.

(a) *[SS88, part II, p. 730, Satz 90.8] If $\mathbb{F}$ has characteristic zero, then $\mathbb{F}$ is always perfect.*

(b) *[SS88, part II, p. 730, Satz 90.9] Let $\mathbb{F}$ be of characteristic $p > 0$. Then $\mathbb{F}$ is perfect if, and only if, the Frobenius morphism $\mathbb{F} \to \mathbb{F}$, $x \mapsto x^p$ is surjective.*

(c) *[SS88, part II, p. 730, Satz 90.7] Algebraically closed fields are perfect.*

(d) *[SS88, part II, p. 731, Satz 90.12] Finite fields are perfect.*

Separable Field Extensions For field extensions of prime characteristic there is the notion of separability, which turns out to be important in algebraic geometry, for example, in the study of endomorphisms of elliptic curves over finite fields.

Definition 2.2.29. *[SS88, part II, pp. 726, 734, 741, 747, §§90–91]*

(a) *A polynomial $f \in \mathbb{F}[x]$ is called* separable *if f and $\frac{\partial f}{\partial x}$ are coprime.*

(b) *If $\mathbb{K}/\mathbb{F}$ is a field extension and $x \in \mathbb{K}$, then x is* separable *over $\mathbb{F}$ if x is algebraic over $\mathbb{F}$ and the minimal polynomial of x over $\mathbb{F}$ is separable. Otherwise, x is called* inseparable *over $\mathbb{F}$.*

(c) *A field extension $\mathbb{K}/\mathbb{F}$ is called* separable *if $\mathbb{K}$ is algebraic over $\mathbb{F}$ and if every element $x \in \mathbb{K}$ is separable over $\mathbb{F}$. Otherwise, $\mathbb{K}/\mathbb{F}$ is called* inseparable.

(d) *If $\mathbb{K}/\mathbb{F}$ is any field extension, then the* separated hull *of $\mathbb{F}$ in $\mathbb{K}$, denoted by $\mathbb{K}_{sep/\mathbb{F}}$, is the set of all elements $x \in \mathbb{K}$ that are separable over $\mathbb{F}$.*

(e) *If $\mathbb{K}/\mathbb{F}$ is a field extension and $\mathbb{F}$ is of characteristic $p > 0$, then $x \in \mathbb{K}$ is called* purely inseparable *if $x^{p^e} \in \mathbb{F}$ for some $e \in \mathbb{N}$.*

(f) *A field extension $\mathbb{K}/\mathbb{F}$ of characteristic $p > 0$ is called* purely inseparable *if every element of $\mathbb{K}$ is purely inseparable over $\mathbb{F}$.*

(g) *A field extension $\mathbb{K}/\mathbb{F}$ is called* normal *if $\mathbb{K}$ is algebraic over $\mathbb{F}$ and if every minimal polynomial of some $x \in \mathbb{K}$ over $\mathbb{F}$ splits into linear factors over $\mathbb{K}$.*

Note that every field extension $\mathbb{K}/\mathbb{F}$ of characteristic $p = 0$ is separable.

Proposition 2.2.30.

(a) *[SS88, part II, p. 730] A field $\mathbb{K}$ is perfect if, and only if, every prime polynomial $f \in \mathbb{K}[x]$ is separable, i. e. if $\overline{\mathbb{K}}/\mathbb{K}$ is separable where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$.*

(b) *[SS88, part II, pp. 741ff] If $\mathbb{K}/\mathbb{F}$ is an arbitrary field extension, then $\mathbb{K}_{sep/\mathbb{F}}/\mathbb{F}$ is a separable field extension.*

(c) *[SS88, part II, p. 747, Aufgabe 20(b)] A field extension $\mathbb{K}/\mathbb{F}$ of characteristic $p > 0$ is purely inseparable if, and only if, $\mathbb{K}_{sep/\mathbb{F}} = \mathbb{F}$.*

If one considers morphisms between curves defined over fields of characteristic $p > 0$, then the notion of being separable or inseparable are important in algebraic geometry. We will see this in Chapter 4, and this will be of use in the process of proving Hasse's Theorem, which allows us to bound the number of $\mathbb{F}_q$-rational points on an elliptic curve defined over a finite field $\mathbb{F}_q$. We continue with defining the separable and inseparable degree of a field extension, similar to the usual degree.

Definition 2.2.31. *[SS88, part II, pp. 747f] Let $\mathbb{K}/\mathbb{F}$ be a field extension.*

(a) *The* separable degree *of $\mathbb{K}/\mathbb{F}$ is defined as*

$$[\mathbb{K} : \mathbb{F}]_{sep} := [\mathbb{K}_{sep/\mathbb{F}} : \mathbb{F}].$$

(b) *The* inseparable degree *of* $\mathbb{K}/\mathbb{F}$ *is defined as*

$$[\mathbb{K} : \mathbb{F}]_{insep} := [\mathbb{K} : \mathbb{K}_{sep/\mathbb{F}}].$$

Remarks 2.2.32. Let $\mathbb{K}/\mathbb{F}$ be a field extension satisfying $[\mathbb{K} : \mathbb{F}] < \infty$.

(a) Clearly $[\mathbb{K} : \mathbb{F}]_{sep} \cdot [\mathbb{K} : \mathbb{F}]_{insep} = [\mathbb{K} : \mathbb{F}]$.

(b) The extension $\mathbb{K}/\mathbb{F}$ is separable if, and only if, $[\mathbb{K} : \mathbb{F}]_{sep} = [\mathbb{K} : \mathbb{F}]$, and it is inseparable if, and only if, $[\mathbb{K} : \mathbb{F}]_{sep} < [\mathbb{K} : \mathbb{F}]$.

(c) [SS88, part II, p. 747, Aufgabe 23] The separable degree is multiplicative.

The Galois Theory The Galois Theory draws a connection between subgroups of the relative automorphism group of a field extension and the lattice of intermediate fields. This allows the characterization of intermediate fields as fixed fields of certain subgroups of the group of automorphisms. Therefore, the Galois theory is of great importance in the theory of curves over finite fields. For example, the proof of Hasse's Theorem uses the fact that the algebraic closure of a finite field is a Galois extension over every finite subfield, and that all Galois groups are cyclic and generated by the Frobenius morphism. We begin by defining what the Galois group of a field extension is.

Definition 2.2.33. *Let* $\mathbb{K}/\mathbb{F}$ *be a field extension. Then the* Galois group *of* $\mathbb{K}$ *over* $\mathbb{F}$ *is the group*

$$G_{\mathbb{K}/\mathbb{F}} := \{\sigma : \mathbb{K} \to \mathbb{K} \mid \sigma \textit{ is a field automorphism, } \sigma|_{\mathbb{F}} = \mathbf{id}_{\mathbb{F}}\}.$$

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ *be a polynomial and* $\sigma \in G_{\mathbb{K}/\mathbb{F}}$*. Define* f^σ *to be the polynomial obtained from* f *by applying* σ *to all coefficients.*

Let $\mathbb{K}/\mathbb{F}$ be a field extension and $G := G_{\mathbb{K}/\mathbb{F}}$ its Galois group. The Galois Theory is built around the interlude between subgroups of G and intermediate fields of $\mathbb{K}/\mathbb{F}$.

Definition 2.2.34. *Define the* lattice of Galois subgroups*,*

$$\mathscr{G} := \mathscr{G}_{\mathbb{K}/\mathbb{F}} := \{H \subseteq G \mid H \textit{ subgroup } \},$$

and the lattice of intermediate fields*,*

$$\mathscr{K} := \mathscr{K}_{\mathbb{K}/\mathbb{F}} := \{L \mid \mathbb{F} \subseteq L \subseteq \mathbb{K} \textit{ tower of fields } \}.$$

For a subgroup $H \in \mathscr{G}$*, define*

$$\mathcal{L}_H := \{x \in \mathbb{K} \mid \sigma(x) = x \textit{ for all } \sigma \in H\},$$

and for an intermediate field $L \in \mathscr{K}$*, define*

$$\mathcal{H}_L := \{\sigma \in G \mid \sigma(x) = x \textit{ for all } x \in L\}.$$

Remark 2.2.35. For each $H \in \mathscr{G}$, $\mathcal{L}_H \in \mathscr{K}$, and for each $L \in \mathscr{K}$, $\mathcal{H}_L \in \mathscr{G}$.

Definition 2.2.36. *An intermediate field $L \in \mathscr{K}$ is called* Galois closed *if $\mathcal{L}_{\mathcal{H}_L} = L$. A field extension $\mathbb{K}/\mathbb{F}$ is called a* Galois extension *if it is normal and separable [SS88, part II, p. 754].*

We present one glimpse of the main theorem of the Galois theory we will need:

Proposition 2.2.37. *[SS88, part II, p. 755, Satz 92.12] Let $\mathbb{K}/\mathbb{F}$ be a Galois extension. Then every $L \in \mathscr{K}_{\mathbb{K}/\mathbb{F}}$ is Galois closed.*

Finally, we want to characterize in which case the algebraic closure of a field is Galois over the field itself. Recall that all finite fields are perfect.

Proposition 2.2.38. *Let $\mathbb{F}$ be a field and $\mathbb{K} = \overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. Then $\mathbb{K}/\mathbb{F}$ is a Galois extension if, and only if, $\mathbb{F}$ is perfect.*

Proof. Obviously $\mathbb{K}/\mathbb{F}$ is always normal, and by Proposition 2.2.30, it is separable if, and only if, $\mathbb{F}$ is perfect. □

Proposition 2.2.39. *[SS88, part II, p. 75, Satz 55.7] Let $\mathbb{F}_q$ be a finite field with q elements and $\overline{\mathbb{F}_q}$ its algebraic closure. Then $\overline{\mathbb{F}_q}/\mathbb{F}_q$ is Galois and $\mathbb{F}_q = \mathcal{L}_{\langle\varphi\rangle}$, where $\varphi : x \mapsto x^q$ is the Frobenius endomorphism.*

Roots of Polynomials Finally in this subsection we want to examine how polynomials can be parameterized by their roots in any extension of their splitting field. For this we need some basic information about symmetric polynomials.

Definition 2.2.40. *Let $\mathbb{F}$ be any field. Define the i-*th elementary symmetric polynomial in n indeterminates*, denoted by $s_{i,n}$, as*

$$s_{i,n} := \sum_{1 \le j_1 < \cdots < j_i \le n} \cdots \sum \prod_{k=1}^{i} x_{j_k} \in \mathbb{F}[x_1, \ldots, x_n].$$

Remark 2.2.41. We have the relation

$$s_{i,n}(x_1, \ldots, x_n) = s_{i,n-1}(x_1, \ldots, x_{n-1}) + x_n s_{i-1,n-1}(x_1, \ldots, x_{n-1}),$$

where $s_{i,j} = 0$ for $i < 0$ or $j < 0$.

The following proposition states how the roots of a polynomial are connected to its coefficients:

Proposition 2.2.42 (Vieta). *Let $f \in \mathbb{F}[x]$ be a polynomial that can be written as $f = \prod_{i=1}^{n}(x - \alpha_i)$ with $\alpha_i \in \mathbb{F}$. Then*

$$f = \sum_{i=0}^{n} (-1)^{n-i} s_{n-i,n}(\alpha_1, \ldots, \alpha_n) x^i.$$

Proof. This can easily be shown by induction on n and by using the formula from Remark 2.2.41. □

The following corollary is important. We will need it in Chapter 4 to develop explicit formulae for adding two points on an elliptic curve.

Corollary 2.2.43. *Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x]$ be a monic polynomial of degree n, i. e. $a_n = 1$, and $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}$ be $n-1$ distinct roots of f. Then*

$$f = \prod_{i=1}^{n-1}(x - \alpha_i) \cdot \left(x + a_{n-1} + \sum_{i=1}^{n-1} \alpha_i \right).$$

Proof. Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ over which f splits into linear factors. Choose $\alpha_n \in \mathbb{K}$ such that $f = \prod_{i=1}^{n}(x - \alpha_i)$. Then by Proposition 2.2.42 we know that $s_1(\alpha_1, \dots, \alpha_n) = a_{n-1}$ over $\mathbb{K}$, where $f = \sum_{i=0}^{n} a_i x^i$. Therefore, we have $\alpha_n = -a_{n-1} - \sum_{i=1}^{n-1} \alpha_i \in \mathbb{F}$. □

Remark 2.2.44. If the $n-1$ roots for Corollary 2.2.43 are not distinct, but the multiplicities of the known roots are also known, then the formula can still be used.

2.3 More Tools

In this section we want to present graded rings, homogenous ideals, and Hilbert polynomials, as well as state some results from Dimension Theory, Kähler differentials and the Theory of Associated Primes.

2.3.1 Graded Rings and Homogenous Ideals

Graded rings are of great importance in projective algebraic geometry as we will see later. Recall the definition of a graded ring:

Definition 2.3.1. *Let S be a ring. Then S is called a* (positively) graded ring *if the additive group of S can be written as a direct sum $S = \bigoplus_{i \geq 0} S_i$, such that $S_i S_j \subseteq S_{i+j}$. The elements of S_i are called* homogenous of degree i. *If not specified otherwise we mean $f_i \in S_i$ if we write $f = \sum_{i \geq 0} f_i \in S$.*

If S is a graded ring, we will write S_i for the set of the homogenous elements in S which have degree i. In fact, then we have $S = \bigoplus_{i \geq 0} S_i$. Moreover, we will write S^h for the set of all homogenous elements in S.

Let R and S be two graded rings and $\varphi : R \to S$ a ring morphism. Then φ is a morphism of graded rings *or a* graded morphism *if $\varphi(R_i) \subseteq S_i$ for all i, i. e. if φ preserves degrees.*

The following example shows an important example for how graded rings appear in commutative algebra:

Example 2.3.2. Let R be any ring and $S = R[x_0, \dots, x_n]$ the ring of polynomials in $n+1$ indeterminates over R. Then S is a positively graded ring: for $\alpha = (\alpha_0, \dots, \alpha_n) \in \mathbb{N}^{n+1}$ let $x^\alpha := \prod_{i=0}^{n} x_i^{\alpha_i}$ and $|\alpha| := \sum_{i=0}^{n} \alpha_i$. Then

$$S = \bigoplus_{i \geq 0} S_i, \qquad \text{where} \qquad S_i = \bigoplus_{\substack{\alpha \in \mathbb{N}^{n+1} \\ |\alpha| = i}} R x^\alpha.$$

When we mention $R[x_0, \dots, x_n]$ as a graded ring, we will from now on mean this graduation.

We next introduce homogenous ideals, which make it possible to pass the grading to quotients of graded rings.

Definition 2.3.3. *Let $S = \bigoplus_{i\geq 0} S_i$ be a graded ring. An ideal $\mathfrak{a} \subseteq S$ is called* homogenous *if for every $f = \sum_{i\geq 0} f_i \in S$ we have that $f \in \mathfrak{a}$ if, and only if, $f_i \in \mathfrak{a}$ for every i. The ideal $S_+ := \bigoplus_{i>0} S_i$ is called the* irrelevant ideal *of S.*

Proposition 2.3.4. *Let S be a graded ring.*

(1) *Obviously $1 \in S_0$. Moreover, S_0 is a subring of S.*

(2) *[Eis95, p. 81, Exercise 2.14] An ideal $\mathfrak{a} \subseteq S$ is homogenous if, and only if, it is generated by its homogenous elements. If $\mathfrak{a}$ is finitely generated, then it is homogenous if, and only if, there exist homogenous $f_1, \dots, f_n \in \mathfrak{a}$ such that $\mathfrak{a} = \langle f_1, \dots, f_n \rangle$.*

(3) *An ideal $\mathfrak{a} \subseteq S$ is homogenous if, and only if, it has a decomposition $\mathfrak{a} = \bigoplus_{i\geq 0} \mathfrak{a}_i$ such that $\mathfrak{a}_i \subseteq S_i$.*

(4) *[Eis95, pp. 81f, Exercise 2.15 (c)] A homogenous ideal $\mathfrak{p} \subseteq S$ is prime if, and only if, for every two homogenous elements $f_1, f_2 \in S$ we have $f_1 f_2 \in \mathfrak{p}$ if, and only if, $f_1 \in \mathfrak{p}$ or $f_2 \in \mathfrak{p}$.*

(5) *[Har77, p. 9, ch. I] [Eis95, pp. 81f, Exercise 2.15 (a)] The finite product, arbitrary intersection and arbitrary sum of homogenous ideals is homogenous. Moreover, the radical of a homogenous ideal is homogenous.*

For graded rings, there exists a stronger version of the Hilbert Basis Theorem:

Proposition 2.3.5. *[Eis95, p. 47, Exercise 1.4] Let $S = \bigoplus_{i\geq 0} S_i$ be a graded ring. Then the following are equivalent:*

(i) *The ring S is Noetherian.*

(ii) *The ring S_0 is Noetherian and the irrelevant ideal S_+ is finitely generated.*

(iii) *The ring S_0 is Noetherian and S is a finitely generated S_0-algebra.*

We will first give some facts about graded morphisms and homogenous ideals. Then we will elaborate on how factoring a graded ring by a homogenous ideal turns the quotient into a graded ring.

Remark 2.3.6. Let $\varphi : S \to T$ be a graded morphism of graded rings S and T. If $\mathfrak{a}$ is a homogenous ideal in T, then $\mathfrak{b} := \varphi^{-1}(\mathfrak{a})$ is a homogenous ideal in S. If $\mathfrak{a}$ is prime, then so is $\mathfrak{b}$.

Proof. We already know that preimages of ideals are ideals, and preimages of prime ideals are prime ideals. Let $f \in \varphi^{-1}(\mathfrak{a})$ and write $f = \sum_{i\geq 0} f_i$ with $f_i \in S_i$. Then $\sum_{i\geq 0} \varphi(f_i) = \varphi(f) \in \mathfrak{a}$ and, since φ preserves degrees, we get $\varphi(f_i) \in \mathfrak{a}$ for every i. Therefore, $f_i \in \varphi^{-1}(\mathfrak{a}) = \mathfrak{b}$ for every i and $\mathfrak{b}$ is hence homogenous. □

Remark 2.3.7. Let S be a graded ring and $\mathfrak{p}$ be a homogenous prime ideal in S. Then $\mathfrak{p}_0 = \mathfrak{p} \cap S_0$ is a prime ideal in S_0.

Proposition 2.3.8. *[SS88, part II, p. 205, §62] Let S be a graded ring and $\mathfrak{a}$ be a homogenous ideal. Then $S/\mathfrak{a}$ is again a graded ring and the natural map $q : S \to S/\mathfrak{a}$ is a graded morphism.*

Since every ring can be seen as a module over itself, it is obvious that modules over graded rings can have a grading structure themselves.

Definition 2.3.9. *Let S be a graded ring and M be an S-module. Then M is called* graded *if there is a decomposition $M = \bigoplus_{i\in\mathbb{Z}} M_i$ such that for each i, M_i is an Abelian group and $R_j M_i \subseteq M_{i+j}$ for every i and j. We again write M^h for the set of homogenous elements of M.*

If M and N are graded S-modules and $\varphi : M \to N$ is a morphism of S-modules, then φ is called a graded morphism of degree n *if $\varphi(M_i) \subseteq N_{i+n}$.*

Remark 2.3.10. If S is a homogenous ring, then any homogenous ideal $\mathfrak{a}$ a graded S-module in a natural way, where $\mathfrak{a}_i = 0$ for $i < 0$. This includes the case $\mathfrak{a} = S$.

Next we define the twist of a graded module. This definition is important as it will be fundamental in describing all rational points of the scheme-theoretic projective space over a ring.

Definition 2.3.11. *Let S be a graded ring and $M = \bigoplus_{i\in\mathbb{Z}} M_i$ be a graded S-module. For any $n \in \mathbb{Z}$ define the* n-th twist of M *as*

$$M(n) := \bigoplus_{i\in\mathbb{Z}} M_{i+n}.$$

Remark 2.3.12. The n-th twist of M is, in fact, M when the grading is shifted by n: we have $M(n)_i = M_{n+i}$. It is clear that $M(n)$ is again a graded S-module.

If M and N are graded S-modules and $\varphi : M \to N$ is a graded morphism of degree n, then φ can be thought of as a graded morphism of degree 0 from M to $N(n)$ or from $M(-n)$ to N.

Localization behaves well with graded rings and modules if multiplicative systems that only contain homogenous elements are used:

Definition 2.3.13. *Let S be a graded ring, M a graded S-module, and A a multiplicative subset of S containing only homogenous elements. Then we define $A^{-1}M$ as the set of equivalence classes of $M \times A$ modulo the equivalence relation*

$$(m, a) \sim (m', a') :\Longleftrightarrow \exists h \in A : h(ma' - m'a) = 0.$$

Then $A^{-1}M$ is called the localization with respect to A. *We again write m/a for the equivalence class of (m, a).*

Remark 2.3.14. If S is a graded ring, M a graded S-module, and A a multiplicative subset of S as in the definition, then $A^{-1}M$ is a graded S-module, where the homogenous elements of $A^{-1}M$ are elements of the form m/a such that $m \in M$ is homogenous, having the degree $\deg m/a = \deg m - \deg a$. Moreover, $A^{-1}S$ is a graded ring and $A^{-1}M$ is a graded $A^{-1}S$-module.

If $\mathfrak{p}$ is a homogenous prime ideal in a graded ring R, the multiplicative set $R \setminus \mathfrak{p}$, in general, contains inhomogenous elements. Therefore $R_\mathfrak{p}$ would not be a graded ring.

Definition 2.3.15. *If S is a graded ring, M a graded S-module, and $\mathfrak{p}$ a homogenous prime ideal in S, then we write $M_{(\mathfrak{p})}$ for the elements of degree zero in the localization of M at A, where A is the set of homogenous elements in the complement of $\mathfrak{p}$. If $f \in S_+$, we write $S_{(f)}$ for the homogenous elements of degree zero in the localization of M at $\{f^n \mid n \in \mathbb{N}\}$.*

Remarks 2.3.16. Let S be a graded ring, M be a graded S-module, and $\mathfrak{p}$ be a homogenous prime ideal in S.

(1) Then $M_{(\mathfrak{p})}$ is an S_0-module. It consists of all m/a such that m is homogenous of degree $\deg a$.

(2) Again, $M_{(\mathfrak{p})}$ is a $S_{(\mathfrak{p})}$-module.

(3) The ring $S_{(\mathfrak{p})}$ is a local ring with maximal ideal $\mathfrak{m} = \{\frac{g}{h} \in S_{(\mathfrak{p})} \mid g \in \mathfrak{p},\ h \notin \mathfrak{p}\}$.

(The proofs are the same as in Remark 2.2.8.)

We want to close this subsection with the following proposition, which shows that a certain graded ring is flat over its degree zero component. This will later allow us to build curves over rings.

Proposition 2.3.17. *Let R be a ring, $S = R[x_0, \dots, x_n]$, and let $f \in S$ be homogenous of degree $d > 0$ and a non-zero-divisor in S. Let $\hat{S} = S/\langle f \rangle$ and $\hat{x}_i$ be the image of x_i in $\hat{S}$. Then*

$$\hat{S}_{(\hat{x}_i)} \cong R[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]/\langle f|_{x_i=1} \rangle =: \hat{S}^{(i)}$$

is flat over R.

Proof. Recall that $\hat{S}_{(\hat{x}_i)}$ are quotients in the form $\frac{g}{x_i^k}$, where $g \in \hat{S}$ is homogenous of degree k. Clearly, $x_i \mapsto 1$ gives a ring isomorphism from $\hat{S}_{(\hat{x}_i)}$ to $\hat{S}^{(i)}$.

The only thing left to show before we can apply Proposition 2.1.34 to complete the proof is that $\hat{f}_i := f|_{x_i=1}$ is a non-zero-divisor in the ring

$$\hat{S}^{[i]} := R[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n] \cong S_{(x_i)},$$

where the isomorphism again maps $x_i \mapsto 1$. But by this isomorphism, if $\hat{f}_i$ is a zero-divisor, then f must be a zero-divisor contrary to the assumption, since $g/x_i^k = 0$ in $S_{(x_i)}$ if, and only if, $g = 0$. □

2.3.2 Hilbert Polynomials

In projective algebraic geometry over fields the Hilbert polynomial plays an important role. We will see later that it can be used to define the arithmetic genus of a projective variety and to define the degree of a projective variety, which will allow the description of the intersection of a projective variety with a hyperplane.

Definition 2.3.18. *[Eis95, p. 42]*

(a) *Let $f \in \mathbb{Q}[t]$ be a polynomial. Then f is said to be a* numerical polynomial *if there exists some $t_0 \in \mathbb{Z}$ such that $f(t) \in \mathbb{Z}$ for all $t \in \mathbb{Z}$, $t \geq t_0$.*

(b) *Let $S = \mathbb{F}[x_0, \dots, x_n]$ be seen as a graded ring (see Example 2.3.2) and M be a finitely generated graded S-module. The* Hilbert function *of M is defined as*

$$H_M : \mathbb{Z} \to \mathbb{Z}, \qquad s \mapsto \dim_{\mathbb{F}} M_s.$$

Theorem 2.3.19 (Hilbert). *[Eis95, p. 42, Theorem 1.11] If M is a finitely generated graded S-module where $S = \mathbb{F}[x_0, \dots, x_n]$ for a field $\mathbb{F}$, then there exists a unique numerical polynomial f of degree at most n such that there is an $s_0 \in \mathbb{N}$ satisfying $f(s) = H_M(s)$ for all $s \in \mathbb{Z}$, $s \geq s_0$.*

Definition 2.3.20. *The polynomial in Theorem 2.3.19 is called the* Hilbert polynomial *of M.*

2.3.3 Dimension Theory

If a ring contains a field, one can consider the vector space dimension of the ring over this field. Unfortunately, in most cases this dimension is infinite. Therefore, we need other notions of dimensions for rings containing fields, but also for general rings. For field extensions there is the transcendence degree, and for arbitrary rings, the Krull dimension. We first define the latter, which turns out to be the right concept for dimension in algebraic geometry.

Definition 2.3.21. *Let R be a ring.*

(a) *Define the* height $\operatorname{ht} \mathfrak{p}$ *of a prime ideal $\mathfrak{p}$ of R to be the supremum of all lengths of properly ascending chains of prime ideals ending at $\mathfrak{p}$, where the length of a chain $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{p}$ is n.*

(b) *The* (Krull) dimension $\dim R$ *is the supremum of the heights of all prime ideals in R.*

(c) *If R is a graded ring, define* $\dim^h R$ *to be the supremum of all lengths of chains of homogenous prime ideals that do not contain the irrelevant ideal.*

Remarks 2.3.22.

(a) Note that from the definition it does not follow that a finite dimensional ring is Noetherian, nor that a Noetherian ring is finite dimensional.

(b) If R is Noetherian, then $\dim R = 0$ if, and only if, R is Artinian. This follows directly from Proposition 2.2.19.

Next we define the transcendence degree of a field extension.

Definition 2.3.23. *Let $\mathbb{K}/\mathbb{F}$ be a field extension.*

(a) *A set of elements $X \subseteq \mathbb{K}$ is* algebraically independent *over $\mathbb{F}$ if for any set of distinct elements $x_1, \dots, x_n \in X$ and any polynomial $f \in \mathbb{F}[t_1, \dots, t_n]$ we have that $f(x_1, \dots, x_n) = 0$ implies $f = 0$.*

(b) *A* transcendence basis *of $\mathbb{K}/\mathbb{F}$ is a set of elements $X \subseteq \mathbb{K}$ that is algebraically independent over $\mathbb{F}$, satisfying that every element of $\mathbb{K}$ is algebraic over $\mathbb{F}(X)$.*

(c) *The* transcendence degree *of $\mathbb{K}/\mathbb{F}$, denoted by $\operatorname{tr.deg.}_{\mathbb{F}} \mathbb{K}$, is the cardinality of any transcendence basis of $\mathbb{K}/\mathbb{F}$.*

Remarks 2.3.24.

(a) See [Eis95, pp. 561f] for a proof that the transcendence degree of a field extension is well-defined, i. e. transcendence bases exist and have the same length.

(b) If R is a domain that is a finitely generated $\mathbb{F}$-algebra, and $\mathbb{K}$ the field of fractions of R, then by [Har77, p. 6, ch. I, Theorem 1.8A] we have $\dim R = \operatorname{tr.deg.}_{\mathbb{F}} \mathbb{K}$.

Regular Rings We want to present the class of regular rings. Regularity turns out to be important for characterizing smoothness in algebraic geometry.

Definition 2.3.25. *Let R be a ring.*

(a) *If R is local with maximal ideal $\mathfrak{m}$ and if $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim R$, then we say that R is a* regular local ring.

(b) *If $R_\mathfrak{p}$ is a regular local ring for every prime $\mathfrak{p}$ of R, then R is said to be* regular.

We wil now present two results on regular rings we will need later.

Proposition 2.3.26 (Auslander-Buchsbaum). *[Mat80, p. 142, Theorem 48] Let R be a regular local ring. Then R is a unique factorization domain.*

Corollary 2.3.27. *A regular ring is reduced.*

Proof. Let R be regular and $x \in R$ such that $x^n = 0$. Then $x^n = 0$ in all localizations $R_\mathfrak{p}$, where $\mathfrak{p}$ is a prime of R. But the rings $R_\mathfrak{p}$ are regular local rings and, therefore, reduced by Proposition 2.3.26. Therefore, $x = 0 \in R_\mathfrak{p}$ for every $\mathfrak{p}$. By Lemma 2.2.9 we get $x = 0$ in R. □

2.3.4 Kähler Differentials

In differential geometry one can characterize smoothness at a point by examining the vector space of differential forms at this point; they form the tangent space. For varieties and schemes, an algebraic analogon can be used. In this subsection we define the module of relative differentials for an R-algebra. How this is connected to Kähler differentials on schemes will be noted in Remark 2.3.4 (b). We begin by investigating what a derivation is.

Definition 2.3.28. *Let R be a ring, S an R-algebra and M an S-module. A map $d : S \to M$ is called a* derivation *if $d(fg) = d(f)g + fd(g)$ for all $f, g \in S$. If d is a derivation and a morphism of R-modules, then d is called* R-linear*. The set of all R-linear derivations $d : S \to M$ is denoted by* $\mathrm{Der}_R(S, M)$*.*

Remark 2.3.29. The set $\mathrm{Der}_R(S, M)$ is in a natural way an S-module, where $d : S \to M$ multiplied by $s \in S$ is $sd : f \mapsto s \cdot d(f)$.

We now show the existence and uniqueness of the module of relative differentials and show how it can be constructed:

Proposition 2.3.30. *[Mat80, pp. 181ff] Let S be an R-algebra. There exists an S-module $\Omega_{S/R}$ and an R-linear derivation $d : S \to \Omega_{S/R}$ with the following universal property:*

If M is any S-module and $d' : S \to M$ is any R-linear derivation, then there exists a unique S-module morphism $\varphi : \Omega_{S/R} \to M$ such that $d' = \varphi \circ d$.

The module $\Omega_{S/R}$ is unique up to isomorphism.

Definition 2.3.31. *Let S be an R-algebra. The* module of relative differential forms *or* module of Kähler differentials *of S over R is the S-module $\Omega_{S/R}$ from the previous proposition.*

Remark 2.3.32. There are two methods that can be used to construct $\Omega_{S/R}$ for an R-algebra S:

(1) [Eis95, p. 386] Take the free S-module generated by symbols in the form $d(x) := dx$ for $x \in S$, modulo the sub-S-module generated by

$$d(xy) - xd(y) - yd(x), \qquad d(\lambda x + \mu y) - \lambda d(x) - \mu d(y),$$

where $x, y \in S$ and $\lambda, \mu \in R$.

(2) [Mat80, p. 182] Let $\varphi : S \otimes_R S \to S$ be the “diagonal” morphism defined by $x \otimes_R y \mapsto xy$, and let $\mathfrak{a} = \ker \varphi$. By the homomorphism $S \to S \otimes_R S$, $s \mapsto s \otimes_R 1$, $\mathfrak{a}$ becomes an S-module. Define $d : S \to \mathfrak{a}/\mathfrak{a}^2$ by $s \mapsto 1 \otimes s - s \otimes 1 \mod \mathfrak{a}^2$. Then $\mathfrak{a}/\mathfrak{a}^2$, together with the universal derivation d, is the module of relative differential forms.

Before concluding this subsection we want to present two results on how the relative module of differentials behaves with respect to tensoring and localization.

Proposition 2.3.33. *[Har77, p. 173, Proposition 8.2A] Let S and T be R-algebras and U a multiplicative subset of S.*

(a) *We have that $\Omega_{S/R} \otimes_R T \cong \Omega_{S_T/T}$, where $S_T = S \otimes_R T$.*

(b) *We have that $\Omega_{U^{-1}S/R} \cong U^{-1}\Omega_{S/R}$.*

2.3.5 Associated Primes

In this subsection we will introduce associated primes of a module. As they can be used to describe the zero-divisors of a ring, we will use them to state a result about zero-divisors in special algebras over Artinian rings.

Definition 2.3.34. *Let R be a ring, M be an R-module and N, P be sub-R-modules of M. Let*

$$(P : N) := (P :_R N) := \{r \in R \mid rN \subseteq P\}.$$

If $\mathfrak{a}$ is an ideal in R, then we write

$$(P :_M \mathfrak{a}) := \{m \in M \mid \mathfrak{a}m \subseteq P\}.$$

An element $r \in R$ is called a zero-divisor on M *if $(0 :_M r) := (0 :_M \langle r\rangle) \neq 0$. Otherwise it is a* non-zero-divisor on M*.*

Remark 2.3.35. Clearly, $(P :_R N)$ is an ideal in R and $(P :_M \mathfrak{a})$ a sub-R-module of M. Moreover, $r \in R$ is a zero-divisor on R (by Definition 2.3.34) if, and only if, r is a zero-divisor in R (by the usual definition).

Definition 2.3.36. *Let R be a ring and M an R-module. Let $\operatorname{Spec} R$ denote the set of prime ideals of R. The* associated primes *of M are the prime ideals of R in the set*

$$\operatorname{Ass}_R(M) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \exists m \in M : (0 :_R \langle m\rangle_R) = \mathfrak{p}\}.$$

The following proposition shows that for Noetherian rings and finitely generated modules, associated primes do exist. It also gives some more properties that we will need.

Proposition 2.3.37. *[Eis95, pp. 89f] Let R be a Noetherian ring and $M \neq 0$ be a finitely generated R-module.*

(a) *The set $\operatorname{Ass}_R(M)$ is finite and non-empty, and every $\mathfrak{p} \in \operatorname{Ass}_R(M)$ contains $(0 :_R M)$. If $\mathfrak{p} \in \operatorname{Spec} R$ is a prime minimal among all primes containing $(0 :_R M)$, then $\mathfrak{p} \in \operatorname{Ass}_R(M)$.*

(b) *Let S be the set of zero-divisors on M. Then $S = \bigcup\{\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M)\}$.*

(c) *If $S \subseteq R$ is a multiplicative subset, then*

$$\operatorname{Ass}_{S^{-1}R}(S^{-1}M) = \{\mathfrak{p}S^{-1}R \mid \mathfrak{p} \in \operatorname{Ass}_R(M),\ \mathfrak{p} \cap S = \emptyset\}.$$

We now want to present a result that reduces the problem of enumerating associated primes to do this in quotients of the ring.

Definition 2.3.38. *Let $\varphi : R \to S$ be a map of rings. We will denote the induced map $\operatorname{Spec} S \to \operatorname{Spec} R$, $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$ by φ^*.*

Proposition 2.3.39. *[Mat80, p. 58, Corollary] Let $\varphi : R \to S$ be a flat morphism of Noetherian rings. Then*

$$\mathrm{Ass}_S(S) = \bigcup\{\mathrm{Ass}_S(S/\mathfrak{p}S) \mid \mathfrak{p} \in \mathrm{Ass}_R(R)\}$$

and

$$\varphi^*(\mathrm{Ass}_S(S)) = \{\mathfrak{p} \in \mathrm{Ass}_R(R) \mid \mathfrak{p}S \neq S\}.$$

With the help of this proposition we can get the following result. which will be needed to obtain a result on the sheaf of meromorphic functions of a smooth curve over a local Artinian ring.

Proposition 2.3.40. *Let R be a local Artinian ring with maximal ideal $\mathfrak{m}$ and S be a flat Noetherian R-algebra containing R. Assume that S has a minimal prime ideal $\mathfrak{p}$ and that $\mathfrak{m}S = \mathfrak{p}$. Then $f \in S$ is a zero-divisor if, and only if, f is nilpotent. Moreover, the set of zero-divisors is exactly $\mathfrak{p}$.*

Proof. The idea is from [Bro05]. Clearly, every nilpotent element is a zero-divisor. Since the zero-divisors of S are exactly the elements in $\bigcup\{\mathfrak{q} \mid \mathfrak{q} \in \mathrm{Ass}_S(S)\}$ by Proposition 2.3.37 (b), and the nilpotent elements of S are exactly the elements of $\sqrt{0} = \bigcap\{\mathfrak{q} \mid \mathfrak{q} \in \operatorname{Spec} S\} = \mathfrak{p}$, we have to show that $\mathrm{Ass}_S(S) = \{\mathfrak{p}\}$. However,

$$\mathrm{Ass}_S(S) = \bigcup\{\mathrm{Ass}_S(S/\mathfrak{q}S) \mid \mathfrak{q} \in \mathrm{Ass}_R(R)\} = \mathrm{Ass}_S(S/\mathfrak{m}S) = \mathrm{Ass}_S(S/\mathfrak{p})$$

according to Proposition 2.3.39, since $\mathrm{Ass}_R(R) \subseteq \{\mathfrak{m}\}$ and $\mathrm{Ass}_R(R) \neq \emptyset$ by Proposition 2.3.37 (a). Since $0 = (0 :_S S) \subseteq \mathfrak{p}$, we have $\mathfrak{p} \in \mathrm{Ass}_S(S/\mathfrak{p})$ by Proposition 2.3.37 (a). But $S/\mathfrak{p}$ is a domain and, hence, if $\mathfrak{q} \in \mathrm{Ass}_S(S/\mathfrak{p})$ annihilates any non-zero element of $S/\mathfrak{p}$, it must be that $\mathfrak{q} \subseteq \mathfrak{p}$. □

2.4 Primitive Elements and Projective Modules

In this section we want to discuss a condition needed for defining an arithmetic addition law on elliptic curves over special rings. We will give a characterization of this condition using the Picard group of the ring and show several examples of rings satisfying this condition. This class of rings will include all Artinian and, therefore, all finite rings.

2.4.1 Primitive Elements

We will now define the notion of being primitive for a finite collection of elements of a ring. This property is needed to formulate the condition.

Definition 2.4.1. *Let R be a ring. Then $a_1, \ldots, a_n \in R$ are called* primitive *if $\langle a_1, \ldots, a_n \rangle_R = R$.*

Remarks 2.4.2.

(a) The elements $a_1, \ldots, a_n \in R$ are primitive if, and only if, there exist $b_1, \ldots, b_n \in R$ such that $\sum a_i b_i = 1$. Because of this property the term *unimodular* is sometimes used in the literature instead of primitive.

(b) If one of the a_i's is a unit, then $a_1, \dots, a_n$ are primitive. This implies that if R is a field, $a_1, \dots, a_n$ are not primitive if, and only if, all a_i's are zero.

(c) The notion of being primitive will be applied to vectors and matrices with coefficients in R in the following sense: we say a vector $(a_i)_i \in R^n$, respectively a matrix $(b_{ij})_{ij} \in R^{n \times m}$ is *primitive over* R, if $a_1, \dots, a_n$, respectively $b_{11}, \dots, b_{1m}, \dots, b_{n1}, \dots, b_{nm}$ are primitive over R.

We will now characterize the property of being primitive.

Lemma 2.4.3. *Let $a_1, \dots, a_n \in R$. The following are equivalent:*

(i) *The elements $a_1, \dots, a_n$ are primitive.*

(ii) *For every maximal ideal $\mathfrak{m}$ in R, at least one of the a_i's is not contained in $\mathfrak{m}$.*

(iii) *For every prime ideal $\mathfrak{p}$, the images of the a_i's under the natural map $R \mapsto R_{\mathfrak{p}}$ are primitive in $R_{\mathfrak{p}}$.*

(iv) *For every maximal ideal $\mathfrak{m}$, the images of the a_i's under the natural map $R \mapsto R_{\mathfrak{m}}$ are primitive in $R_{\mathfrak{m}}$.*

(v) *For every maximal ideal $\mathfrak{m}$, the images of the a_i's in $R/\mathfrak{m}$ are not all zero.*

This shows that being primitive is a local property. Note that in a local ring, $a_1, \dots, a_n$ are primitive if, and only if, at least one of them is a unit.

Proof. If (i) holds, then $1 = \sum r_i a_i$ with $r_i \in R$. If $\mathfrak{m}$ is an ideal containing all the a_i's, then $1 \in \mathfrak{m}$. Thus, $\mathfrak{m}$ cannot be maximal, and (ii) holds.

If (i) does not hold, $\langle a_1, \dots, a_n \rangle \subsetneqq R$. Then there exists a maximal ideal $\mathfrak{m}$ containing $a_1, \dots, a_n$. So (ii) does not hold.

If (i) holds, then $1 = \sum r_i a_i$ with $r_i \in R$. Since the natural map maps 1 in R onto 1 in $R_{\mathfrak{p}}$, the images of the a_i's are primitive in $R_{\mathfrak{p}}$. Therefore, (iii) holds.

It is clear that (iii) implies (iv).

If (ii) does not hold, the a_i's are contained in a maximal (and thus prime) ideal $\mathfrak{m}$. Since the image of $\mathfrak{m}$ under the natural map is contained in the maximal ideal of $R_{\mathfrak{m}}$, the images of the a_i's are also contained in it (see Remarks 2.2.8). Hence, by (i) $\Leftrightarrow$ (ii), they cannot be primitive in $R_{\mathfrak{m}}$ and (iv) does not hold.

We conclude by noting that (ii) and (v) are equivalent. □

Before continuing we will show that for polynomials over Artinian rings the notion of its coefficients being primitive is equivalent to being a zero-divisor.

Definition 2.4.4. *Let R be a ring and $f \in R[x_1, \dots, x_n]$ be a polynomial. Then f is* primitive *over R if the set of coefficients of f is primitive over R.*

Proposition 2.4.5. *Let R be an Artinian ring and $S = R[x_1, \dots, x_n]$. Then $f \in S$ is a non-zero-divisor if, and only if, f is primitive. Moreover, if R is local, then f is a zero-divisor if, and only if, it is nilpotent, which is the case if, and only if, all coefficients are contained in the maximal ideal of R.*

Proof. First assume R is local with maximal ideal $\mathfrak{m}$. Now $R[x_1, \ldots, x_n]/\langle \mathfrak{m} \rangle \cong (R/\mathfrak{m})[x_1, \ldots, x_n]$ and, therefore, $\langle \mathfrak{m} \rangle$ is prime. Since every element of $\mathfrak{m}$ is nilpotent, so is every element of $\langle \mathfrak{m} \rangle$ and, therefore, $\sqrt{0} = \langle \mathfrak{m} \rangle$ in $R[x_1, \ldots, x_n]$. By Corollary 2.1.31, $R[x_1, \ldots, x_n]$ is flat over R and, hence, we can conclude the local case by applying Proposition 2.3.40.

Now let R be an arbitrary Artinian ring. Write $R = \bigoplus_{i=1}^m R_i$, where R_i are local Artinian rings with maximal ideals $\mathfrak{m}_i$, and let $S_i = R_i[x_1, \ldots, x_n]$, $\mathfrak{m}_i' = \langle \mathfrak{m}_i \rangle_{S_i}$. Let $f = \sum_{i=1}^m f_i$, where $f_i \in S_i$. Assume f is primitive and $fg = 0$ with $g = \sum_{i=1}^m g_i$, $g_i \in S_i$. Then $fg = \sum_{i=1}^m f_i g_i$ and, thus, $f_i g_i = 0$ for all i. But since f is primitive, f_i is not contained in $\mathfrak{m}_i'$. By the first part of the proof, then $g_i = 0$ for all i and, hence, $g = 0$. Now let f not be primitive; therefore $f_i \in \mathfrak{m}_i'$ for some i. If $f_i = 0$, choose $g = 1_{S_i}$, and otherwise let $g \in \mathfrak{m}_i' \setminus \{0\}$ such that $f_i g = 0$. But then $fg = 0$, while $g \neq 0$. □

We will now formulate the condition needed for rings to define an arithmetic group law:

(∗) For all $n, m \in \mathbb{N}_{>0}$, and every matrix $(a_{ij})_{ij} \in R^{n \times m}$ primitive over R such that all two-by-two minors vanish, i. e. $a_{ij}a_{k\ell} - a_{i\ell}a_{kj} = 0$ for all i, j, k, ℓ with $1 \leq i < k \leq n$ and $1 \leq j < \ell \leq m$, there exists an R-linear combination of the columns that is primitive over R.

We will see in Section 4.3.3 why this condition is needed. Now we will continue to characterize this condition and we will also specify an algorithm that effectively computes the linear combination over finite rings.

2.4.2 Projective Modules

To define the Picard group of a ring we need to know what a projective R-module of rank one is. We also need several properties and characterizations of such modules.

Definition 2.4.6. *Let R be a ring and P an R-module. Then P is called* projective *if every exact sequence $M \xrightarrow{f} P \to 0$ of R-modules splits at P, i. e. if there exists an R-module homomorphism $g : P \to M$ such that $f \circ g = \mathbf{id}_P$.*

Remark 2.4.7. Let $A \xrightarrow{f} B \to 0$ be an exact sequence that splits at B by the morphism $g : B \to A$. Then $A \cong B \oplus \ker f$:

Consider the R-linear map $h : A \to B \oplus \ker f$, $x \mapsto (f(x), x - g(f(x)))$. Since it maps $\ker f$ onto $\ker f$, and since f is surjective, h itself is surjective. If $h(x) = 0$, then $h \in \ker f$ and, hence, $x = x - g(f(x)) = 0$. Hence h is injective.

Proposition 2.4.8. *Let P be a finitely generated R-module. The following are equivalent:*

(i) *The module P is projective.*

(ii) *The module P is a direct summand of a free module of finite rank.*

(iii) *There exists some $n \in \mathbb{N}$ and an idempotent $e \in \mathrm{End}(R^n)$ such that $P \cong eR^n$.*

(iv) *For all R-modules M, N and homomorphisms $h : P \to N$ and $f : M \to N$, where $\operatorname{im} h \subseteq \operatorname{im} f$, there exists a lift of h with respect to f, i. e. there exists an homomorphism $\tilde{h} : P \to M$ such that $h = f \circ \tilde{h}$.*

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\exists\tilde{h}"'] \arrow[d, "h"] \\
M \arrow[r, "f"'] & N
\end{tikzcd}$$

(v) *If $M \xrightarrow{f} N \to 0$ is exact, then the map*

$$\operatorname{Hom}(P, f) : \operatorname{Hom}_R(P, M) \to \operatorname{Hom}_R(P, N), \qquad \varphi \mapsto f \circ \varphi$$

is surjective.

Proof. Assume that (i) holds. Choose some $n \in \mathbb{N}$ such that there exists a surjective $f : R^n \to P$. This is possible since P is finitely generated. Then by assumption, the exact sequence $R^n \xrightarrow{f} P \to 0$ splits at P and so we get $R^n \cong \ker f \oplus P$. Thus (ii) holds.

Assume that (ii) holds. Let $R^n = P \oplus Q$ and define $e : R^n \to R^n$ by $p + q \mapsto p$, where $p \in P$ and $q \in Q$. Then $e \in \operatorname{End}(R^n)$, $e(R^n) = P$ and $e^2 = e$, so (iii) holds.

Assume that (iii) holds. Let $P = eR^n$ and define $Q := (1 - e)R^n$. We show that

$$\varphi : R^m \to P \oplus Q, \qquad x \mapsto (ex, (1 - e)x)$$

is an isomorphism: it is clear that it is a homomorphism and, since $\varphi(x) = 0$ implies $ex = 0 = x - ex$, i. e. $x = 0$, it is injective. Given $(ex, (1 - e)y) \in P \oplus Q$, it is

$$\begin{aligned}\varphi(ex + (1 - e)y) &= (e^2x + e(1 - e)y, (1 - e)ex + (1 - e)^2y) \\ &= (ex, (1 - e)y).\end{aligned}$$

So (ii) holds.

Assume that (ii) holds and let M, N, h and f be as in the assumptions for (iv). Let $\varphi : R^n = P \oplus Q \to P$ be the projection onto P and $\psi : P \to R^n = P \oplus Q$ the injection into $P \oplus Q$, so $\varphi \circ \psi = \mathbf{id}_P$. This show that it is enough to prove that R^n fulfills (iv), since in this case there exists a lift $g : R^n \to M$ of the mapping $h \circ \varphi : R^n \to N$ with respect to $f : M \to N$, i. e. $f \circ g = h \circ \varphi$ and, by setting $\tilde{h} := g \circ \psi$, we get

$$\begin{aligned}f \circ \tilde{h} &= (f \circ g) \circ \psi = (h \circ \varphi) \circ \psi \\ &= h \circ (\varphi \circ \psi) = h \circ \mathbf{id}_P = h,\end{aligned}$$

so that (iv) holds.

$$\begin{tikzcd}
R^n \arrow[r, bend left, "\varphi"] \arrow[d, dashed, "\exists g"'] & P \arrow[l, bend left, "\psi"] \arrow[d, "h"] \\
M \arrow[r, "f"'] & N
\end{tikzcd}$$

Hence, assume we have modules N, M and homomorphisms $h : R^n \to N$ and $f : M \to N$ such that $\operatorname{im} h \subseteq \operatorname{im} f$. Let $e_1, \dots, e_n$ be a basis of R^n. Since $\operatorname{im} h \subseteq \operatorname{im} f$, choose $x_i \in M$ such that $f(x_i) = h(e_i)$ and define a homomorphism $\tilde{h} : R^n \to M$ by mapping e_i onto x_i. Then $(f \circ \tilde{h})(e_i) = f(x_i) = h(e_i)$ for all i, so $f \circ \tilde{h} = h$. This completes the proof of (ii) ⇒ (iv).

Assume that (iv) holds. Let $M \xrightarrow{f} P \to 0$ be exact and choose $h = \mathbf{id}_P$ and $N = P$. Then by (iv), there exists a homomorphism $\tilde{h} : P \to M$ such that $f \circ \tilde{h} = h = \mathbf{id}_P$, which means that the sequence splits at P and, therefore, (i) holds.

To see that (iv) and (v) are equivalent, note that (v) means that for every $h \in \operatorname{Hom}_R(P, N)$ there is an $\tilde{h} \in \operatorname{Hom}_R(P, M)$ such that $h = f \circ \tilde{h}$ and, further, that (iv) can be reformulated by replacing N by $\operatorname{im} f$ such that the condition $\operatorname{im} h \subseteq \operatorname{im} f$ is no longer needed. □

Corollary 2.4.9. *Every free module of finite rank is projective.*

Proof. This directly follows from (ii) ⇒ (i). □

Example 2.4.10. Not every projective module is free: let $R = \mathbb{Z} \oplus \mathbb{Z}$ and $P = \mathbb{Z}$, where the action is given by $R \times P \to P$, $((r, r'), m) \mapsto rm$.

But there are cases where the converse holds true. Before we show this, we need the following result:

Proposition 2.4.11. *Let R be a ring and P be a finitely generated projective R-module. Then there exists an $n \in \mathbb{N}$ and an $A = (a_{ij})_{ij} \in R^{n\times n}$ such that $P \cong \operatorname{coker} A$, i. e. the following sequence is exact:*

$$\begin{tikzcd} R^n \arrow[r, "x\mapsto Ax"] & R^n \arrow[r] & P \arrow[r] & 0. \end{tikzcd}$$

Furthermore, A is idempotent, i. e. $A^2 = A$.

Thus, every finitely generated projective R-module P is *of finite presentation*, which means that it sits in an exact sequence $F_1 \to F_2 \to P \to 0$, where F_1 and F_2 are free R-modules of finite rank.

Proof. By Proposition 2.4.8, we can write $P \cong eR^n$ for some $n \in \mathbb{N}$ and some idempotent $e \in \operatorname{End}(R^n)$. Let $f := 1 - e \in \operatorname{End}(R^n)$. Then the sequence

$$\begin{tikzcd} R^n \arrow[r, "f"] & R^n \arrow[r, "e"] & R^n \end{tikzcd}$$

is exact. Let $e_1, \dots, e_n$ be a basis of R^n, and define the a_{ij}'s by the equations $\sum_j a_{ij} e_j = f(e_i)$, $i = 1, \dots, n$. Then the endomorphism f is represented by the matrix $A = (a_{ij})_{ij}$ in the sense that if $x = \sum_i \lambda_i e_i$ and $f(x) = \sum_i \mu_i e_i$, then $(\mu_i)_i = (a_{ij})_{ij}(\lambda_i)_i$. Thus, the sequence given in the proposition is exact. That A is idempotent follows directly from the fact that $f = 1 - e$ is idempotent. □

Proposition 2.4.12. *[Eis95, pp. 136f, Exercise 4.11 (a)] Let R be a local ring and P a finitely generated projective module over R. Then P is free.*

Corollary 2.4.13. *Let R be a ring and P a finitely generated projective module. If $\mathfrak{p}$ is a prime ideal of R, then the localization $P_{\mathfrak{p}}$ of P is free as an $R_{\mathfrak{p}}$-module, i. e. there exists an $n \in \mathbb{N}$ such that $R_{\mathfrak{p}}^n \cong P_{\mathfrak{p}}$.*

Proof. Since $R_\mathfrak{p}$ is local, it is enough to show that $P_\mathfrak{p}$ is projective. Then we can finish the proof by applying Proposition 2.4.12. By Proposition 2.4.8 we can write $R^n = P \oplus Q$ for some $n \in \mathbb{N}$ and some R-module Q. However, since $R^n_\mathfrak{p} = P_\mathfrak{p} \oplus Q_\mathfrak{p}$, by Proposition 2.4.8, $P_\mathfrak{p}$ is a finitely generated projective $R_\mathfrak{p}$-module. □

This implies that for every projective finitely generated R-module P we get a map

$$\varphi : \operatorname{Spec} R \to \mathbb{N}, \qquad \mathfrak{p} \mapsto \operatorname{rank}_{R_\mathfrak{p}} P_\mathfrak{p}.$$

Definition 2.4.14. *If R is a ring, P is a finitely generated projective R-module, and $n \in \mathbb{N}$, then P is called* projective of rank n *if, for every prime ideal $\mathfrak{p}$ in R, we have* $\operatorname{rank}_{R_\mathfrak{p}} P_\mathfrak{p} = n$.

Definition 2.4.15. *For a ring R let* $\operatorname{Pic} R$ *denote the* Picard group *of R, which is defined to be the set of isomorphism classes of projective R-modules of rank one.*

Note that we do not know (yet) that $\operatorname{Pic} R$ is a group. We need one further characterization of a module being projective:

Proposition 2.4.16. *[Eis95, pp. 136f, Exercise 4.11 (b)] Let R be a ring and P a finitely generated R-module. Then P is projective if, and only if, for every maximal ideal $\mathfrak{m}$ of R, $P_\mathfrak{m}$ is a projective (and hence free, by Proposition 2.4.12) $R_\mathfrak{m}$-module.*

Thus, being projective is also a local property.

2.4.3 Projective Modules and Matrices

We want to characterize the matrix condition $(*)$ from page 41 by projective R-modules of rank one. For that, we will first show that any finitely generated projective R-module of rank one can be represented by a primitive matrix $A \in R^{n \times m}$ for which every two-by-two minor vanishes.

Lemma 2.4.17. *Let P be a finitely generated projective R-module of rank one. Then $P \cong AR^m$ for a matrix $A \in R^{n \times m}$, which is primitive over R and for which every two-by-two minor vanishes.*

Proof. By Proposition 2.4.8 all finitely generated projective R-modules are up to isomorphism of the form $P = eR^n$, where $n \in \mathbb{N}_{>0}$ and $e \in \operatorname{End}(R^n)$ is idempotent. Let $A = (a_{ij})_{ij} \in R^{n \times n}$ be the matrix representation for $e \in \operatorname{End}(R^n)$. Hence, $P = AR^n$. Let $\mathfrak{p}$ be a prime ideal of R.

Since $P_\mathfrak{p}$ is free of rank one, we have $\sum A_{\bullet i,\mathfrak{p}} R_\mathfrak{p} = P_\mathfrak{p} = R_\mathfrak{p} v$ for some $v \in R^n_\mathfrak{p}$. Thus, for every i we get some $\lambda_{i,\mathfrak{p}} \in R_\mathfrak{p}$ such that $A_{\bullet i,\mathfrak{p}} = \lambda_{i,\mathfrak{p}} v$. Since $A_\mathfrak{p}$ is idempotent and $v \in A_\mathfrak{p} R^n_\mathfrak{p}$, we have $A_\mathfrak{p} v = v$ (see Remark 2.2.1).

Let $e_1, \dots, e_n$ be the canonical basis of $R^n_\mathfrak{p}$, and let $\lambda_i \in R_\mathfrak{p}$ such that $\lambda_i v = A_\mathfrak{p} e_i$. Then since

$$\Bigl(\sum_i \lambda_i v_i\Bigr) v = \sum_i \lambda_i v v_i = \sum_i A_\mathfrak{p} e_i v_i = A_\mathfrak{p} v = v,$$

we must have $\sum \lambda_i v_i = 1$ as the map $r \mapsto rv$ is injective (because $R_\mathfrak{p} v$ is free). Since $v = \sum_i \mu_i A_{\bullet i,\mathfrak{p}}$ for some $\mu_i \in R_\mathfrak{p}$, we have

$$1 = \sum_j \lambda_j v_j = \sum_j \lambda_j \sum_i \mu_i a_{ji,\mathfrak{p}}$$

and, therefore, $A_{\mathfrak{p}}$ is primitive. Since this is true for every prime ideal $\mathfrak{p}$, by Lemma 2.4.3 we get that A is primitive.

We now show that every two-by-two minor of A vanishes: This is clearly true for $A_{\mathfrak{p}}$, since $A_{\bullet i,\mathfrak{p}} = \lambda_{i,\mathfrak{p}} v$, so $a_{ji,\mathfrak{p}} = \lambda_{i,\mathfrak{p}} v_j$ and, thus,

$$a_{ji,\mathfrak{p}} a_{\ell k,\mathfrak{p}} - a_{\ell i,\mathfrak{p}} a_{jk,\mathfrak{p}} = \lambda_{i,\mathfrak{p}} v_j \lambda_{k,\mathfrak{p}} v_\ell - \lambda_{i,\mathfrak{p}} v_\ell \lambda_{k,\mathfrak{p}} v_j = 0.$$

Since this is true for every localization $A_{\mathfrak{p}}$, it is also true for A itself by Corollary 2.2.10. □

Lemma 2.4.18. *Let $A \in R^{n\times m}$ be a matrix that is primitive over R such that every two-by-two minor vanishes. Then $P = AR^m$ is a projective R-module of rank one.*

Proof. Assume $A = (a_{ij})_{ij} \in R^{n\times m}$ is primitive and every two-by-two minor of A vanishes. We will show that $P = AR^m \subseteq R^n$ is a projective R-module of rank one. We have that P is generated as an R-module by the columns of A, i. e. $P = \sum_i RA_{\bullet i}$.

By using the vanishing of all two-by-two minors, we get

$$\Big(\sum_i \mu_i a_{ik}\Big) A_{\bullet\ell} = \Big(\sum_i \mu_i a_{i\ell}\Big) A_{\bullet k}$$

for all $k, \ell \in \{1, \dots, m\}$ and all $(\mu_i)_i \in R^n$.

By Proposition 2.4.16 and Lemma 2.4.3, to conclude this proof we have to show that $P_{\mathfrak{p}}$ is free of rank one for every prime ideal $\mathfrak{p}$. Hence, for the rest of this proof, assume that R is local.

A collection of elements is primitive over a local ring if, and only if, one of them is a unit. Thus, there exist some $\hat{\imath}$ and k such that $a_{\hat{\imath}k} \in R^*$. Let $\mu_{\hat{\imath}} = a_{\hat{\imath}k}^{-1}$ and $\mu_j = 0$ for $j \neq \hat{\imath}$. Then $\sum_i \mu_i a_{ik} = 1$ and, therefore, we get

$$A_{\bullet\ell} = a_{\hat{\imath}k}^{-1} a_{\hat{\imath}\ell} A_{\bullet k}$$

for all ℓ. However, this means that $v := A_{\bullet k}$ generates AR^m, i. e. $AR^m = Rv$. Since $a_{\hat{\imath}k}$ is a unit, Rv is free: Indeed $\sum_i \lambda_i v_i = 1$ for some λ_i, and let

$$\varphi : R^n \to R, \qquad (w_i)_i \mapsto \sum_i \lambda_i w_i.$$

One can easily see that $\varphi(rv) = r$ for every $r \in R$, and thus Rv is isomorphic to R. □

We have shown the following proposition:

Proposition 2.4.19. *Let P be a finitely generated R-module. Then P is projective of rank one if, and only if, there exists a matrix $A \in R^{n\times m}$ that is primitive over R and for which every two-by-two minor vanishes such that $P \cong AR^m$.*

As a next step we characterize when a projective R-module of rank one is free by using this matrix representation.

Lemma 2.4.20. *Let $P = AR^m \subseteq R^n$ be a projective R-module of rank one, where $A \in R^{n\times m}$ is a matrix that is primitive over R such that every two-by-two minor of A vanishes. If there exists an R-linear combination of the columns of A that is primitive over R, then P is free.*

Proof. Let $A = (a_{ij})_{ij} \in R^{n\times m}$ be as in the assumptions. Let $\lambda_i \in R$ be such that $v := \sum_i \lambda_i A_{\bullet i}$ is primitive over R. We will show that $R \cong P$ by the isomorphism $r \mapsto rv$. Assuming that this map is surjective, the inverse is given by $\psi|_{Rv}$, where

$$\psi : R^n \to R, \qquad (w_i)_i \mapsto \sum \mu_i w_i$$

for some μ_i's satisfying $\sum \mu_i v_i = 1$.

To complete the proof we will now show that AR^m is contained in Rv. Fix one i, and let $1 \leq k, \ell \leq n$. Then $a_{ki}v_\ell - a_{\ell i}v_k = 0$ since all two-by-two minors of A vanish, and v is a linear combination of the columns of A. However this gives

$$\Big(\sum_i \mu_i a_{i\ell}\Big)v_j = \sum_i \mu_i a_{i\ell} v_j = \sum_i \mu_i v_i a_{j\ell} = \Big(\sum_i \mu_i v_i\Big) a_{j\ell} = a_{j\ell}$$

and, hence, $A_{\bullet\ell} = \alpha_\ell v \in Rv$ for $\alpha_\ell := \sum_i \mu_i a_{i\ell}$. □

Lemma 2.4.21. *Let $P = AR^m \subseteq R^n$ be a projective R-module of rank one, where $A \in R^{n\times m}$ is a matrix that is primitive over R such that every two-by-two minor of A vanishes. If P is free, then there exists an R-linear combination of the columns of A that is primitive over R. Moreover, the primitive R-linear combination is unique up to multiplication by units.*

Proof. Let $A = (a_{ij})_{ij} \in R^{n\times m}$ be as in the assumption. Since P is free, there exists a $v \in R^n$ such that $AR^m = P = Rv$.

Let $\mathfrak{p}$ be a prime ideal of R. Since $A_\mathfrak{p}$ is primitive, one of its columns contains a unit and, therefore, $A_{\bullet k,\mathfrak{p}}$ is primitive for one k. In the proof of Lemma 2.4.18, we saw that $P_\mathfrak{p} = R_\mathfrak{p} A_{\bullet k,\mathfrak{p}}$. Further, $R_\mathfrak{p} v_\mathfrak{p} = P_\mathfrak{p}$. Hence, there are $\alpha, \beta \in R$ such that $v_\mathfrak{p} = \alpha A_{\bullet k,\mathfrak{p}}$ and $A_{\bullet k,\mathfrak{p}} = \beta v_\mathfrak{p}$. This implies $A_{\bullet k,\mathfrak{p}} = \beta\alpha A_{\bullet k,\mathfrak{p}}$ and, since one component of $A_{\bullet k,\mathfrak{p}}$ is a unit, it follows that $\beta\alpha = 1$. Therefore, one component of $v_\mathfrak{p}$ is also a unit, and $v_\mathfrak{p}$ is primitive. By Lemma 2.4.3 v is primitive.

Now, since $AR^m = P = Rv$, there exist $\lambda_1, \dots, \lambda_m$ such that $v = \sum_i \lambda_i A_{\bullet i}$ and, thus, we have a linear combination of the columns of A that is primitive.

Assume $\tilde{v}$ is another linear combination of the columns of A, which is primitive. Then $\tilde{v} = \alpha v$ for some $\alpha \in R$. If α is not a unit, then every component of $\tilde{v}$ is contained in the ideal $R\alpha \subsetneqq R$, contradicting that $\tilde{v}$ is primitive. □

We have shown the following proposition:

Proposition 2.4.22. *Let $P = AR^m \subseteq R^n$ be a projective R-module of rank one, where $A \in R^{n\times m}$ is a matrix that is primitive over R such that every two-by-two minors of A vanish. Then P is free if, and only if, there exists an R-linear combination of the columns of A, which is primitive over R. If such a linear combination exists, it is unique up to multiplication by units of R.*

As a result of the two last propositions we get the following corollary which characterizes the matrix condition $(*)$ from the end of Section 2.4.1 (on page 41):

Corollary 2.4.23. *Let R be a ring. Then the following are equivalent:*

(i) *Every projective R-module of rank one is free, i. e.* $\operatorname{Pic} R = 0$.

(ii) *For every primitive matrix $A \in R^{n\times m}$, such that every two-by-two minor vanishes, there exists an R-linear combination of the columns of A that is primitive.* $(*)$

In this situation the linear combination in (ii) is unique up to multiplication by units.

2.4.4 Rings Satisfying $\operatorname{Pic} R = 0$

In this subsection we want to give several examples of rings R satisfying $\operatorname{Pic} R = 0$. First, we will describe how to calculate the primitive linear combination of the columns of a given primitive matrix over a finite ring R satisfying $(*)$. In particular, this proves that every finite ring R satisfies $\operatorname{Pic} R = 0$. Following [Len86], we begin with a lemma:

Lemma 2.4.24. *[Len86, p. 107, Lemma] Let R be a finite ring and choose $t \in \mathbb{N}$ such that $2^{t+1} > |R|$.*

(a) *For every $c \in R$ there exists an $x \in R$ such that $c^{t+1}x = c^t$.*

(b) *An element $c \in R$ is nilpotent if, and only if, $c^t = 0$.*

Proof.

(a) Consider the chain of ideals

$$Rc^{t+1} \subseteq Rc^t \subseteq \cdots \subseteq Rc \subseteq R.$$

If $Rc^{i+1} \subsetneqq Rc^i$ for $i = 0, \dots, t$, by Lagrange we get

$$|R| \geq 2\,|Rc| \geq 2\cdot 2\left|Rc^2\right| \geq \cdots \geq 2^{t+1}\left|Rc^{t+1}\right| \geq 2^{t+1} > |R|\,,$$

a contradiction. Hence, we have $Rc^i = Rc^{i+1}$ for some $i \in \{0, \dots, t\}$ and, therefore, $c^{i+1} = xc^i$ for some $x \in R$. By multiplying with c^{t-i} we complete the proof of (a).

(b) Note that (a) implies $c^u x = c^{u-1}$ for some $x \in R$ if $u > t$. So $c^u = 0$ implies $c^{u-1} = 0$ if $u > t$. If c is nilpotent and $i \in \mathbb{N}_{>0}$ is the smallest exponent such that $c^i = 0$, it must be $i \leq t$, therefore $c^t = 0$. □

Let $A = (a_{ij})_{ij} \in R^{n\times m}$ be a matrix that is primitive over R.

The algorithm works by recursion on the size of the ring. For the zero ring 0, any collection of elements is primitive, so any column of the matrix can be taken. Otherwise, the matrix must contain an element that is not nilpotent: if every entry is nilpotent, all elements lie in the ideal $\operatorname{Rad} R \subsetneqq R$, so the matrix cannot be primitive over R. Let c be a non-nilpotent entry.

Using the lemma, we can find an $x \in R$ such that $c^{t+1}x = c^t$. This implies

$$c^t = c^{t+1}x = c^t cx = (c^{t+1}x)cx = \cdots = c^{2t}x^t.$$

By letting $e := c^t x^t$, we have $e^2 = c^{2t}x^{2t} = x^t c^t = e$, so e is idempotent. Since $c \neq 0$, we have $e \neq 0$, as otherwise we would have $0 = ec^t = c^t$.

If $e = 1$, then c is a unit and the column containing c is primitive over R. If $e \neq 1$, then e is a non-trivial idempotent, so $R = Re \times R(1-e)$, where Re and

$R(1-e)$ are non-zero finite rings (see Proposition 2.2.2). Let $\pi_e : R \to Re$ and $\pi_{1-e} : R \to R(1-e)$ be the canonical surjections.

Now clearly $\pi_e(A)$ is a matrix primitive over Re, hence by recursion, we find an Re-linear combination of the columns of $\pi_e(A)$, which is primitive over Re. The same can be done for $\pi_{1-e}(A)$. Therefore, we get an $R(1-e)$-linear combination of the columns of $\pi_{1-e}(A)$, which is primitive over $R(1-e)$. These two linear combinations can be combined to form one in R by adding them together. The sum is primitive over R because the ideals in R are products of ideals in Re and $R(1-e)$.

For a first running-time analysis, note that $\pi_e(c)$ will be a unit, since

$$\pi_e(c)^t \pi_e(x)^t = \pi_e(1) = 1_{Re},$$

and $\pi_{1-e}(c)$ will be nilpotent, since

$$\pi_{1-e}(c)^t = \pi_{1-e}(c^t) = (1-e)c^t = c^t - c^{2t}x^t = 0.$$

This implies that the recursion is only needed for $\pi_{1-e}(A)$. Thus, the number of recursions is bounded by $n \cdot m$. Furthermore, the number of recursions is bounded by the number of maximal ideals in R: Since R can be written as the direct sum of local rings by Corollary 2.2.20, the number of local rings in the decomposition corresponds exactly to the number of maximal ideals in R.

If, for example, $R = \mathbb{Z}_n$ for $n = pq$, where p and q are distinct primes, there can be at most one recursion. (Note that in case a recursion is needed, we have factored n.)

We now want to sum up the requirements that are needed for this algorithm to work efficiently:

- It must be possible to store ring elements efficiently and that every ring element can be represented with a fixed maximum number of bits.

  This is important for both practical considerations and to determine a value of t in Lemma 2.4.24.

- Basic ring operations, such as multiplication, addition and subtraction, should be efficient.

- Testing whether an element is zero, or equivalently whether two elements are equal, should be efficient.

  This is important since an element can have several different representations.

- Solving an equation of the type $ax = b$ should be efficient, where the existence of a solution is known and where $a \in R$ is not necessarily a unit.

For special classes of rings one can find specialized algorithms that have less requirements. This is, for example, the case for $\mathbb{Z}_{pq}$, where p and q are distinct primes. How this can be done can be seen for some special classes of rings in Section 2.5.

Choose t as in Lemma 2.4.24 to be minimal. (In fact, choosing t as the smallest power of 2 satisfying the condition is more effective, since x^t can be computed easier by consecutive squaring.) The algorithm looks like this:

```
Algorithm ComputePrimitiveCombination($e, A$)
Parameters:
  • $e \in R$: An idempotent nonzero element of $R$. This will be the unit of
    the ring $Re$ we will work in.
  • $A = (a_{ij})_{ij} \in (Re)^{n \times m}$: A matrix that is primitive over $Re$ satisfying
    that every two-by-two minor vanishes.
Returns:
  • An element $(\lambda_j)_j$ of $(Re)^m$, such that $\sum_{j=1}^{m} \lambda_j A_{\bullet j}$ is primitive in $Re$.
The algorithm:
(1) For every pair $(i, j)$, where $1 \leq i \leq n$ and $1 \leq j \leq m$, do:
    (a) Let $c := e \cdot a_{ij}$.
    (b) Compute $c^t$ (for example, by consecutive squaring).
    (c) If $c^t = 0$, continue with the next $(i, j)$ pair.
    (d) Compute[a] some $x \in Re$ such that $c \cdot c^t \cdot x = c^t$.
    (e) Compute $x^t$ and let $\hat{e} := c^t \cdot x^t$.
    (f) If $\hat{e} = e$, then let $\lambda_{j'} = 0$ for $j' \neq j$ and $\lambda_j = e$, and return $(\lambda_{j'})_{j'}$.
    (g) Compute $A' := (a'_{i'j'})_{i'j'} \in (R\hat{e})^{n \times m}$ where $a'_{i'j'} := (e - \hat{e}) \cdot a_{i'j'}$.
    (h) Let $(\lambda'_{j'})_{j'}$ be the result of ComputePrimitiveCombination($e - \hat{e}, A'$).
    (i) Let $\lambda_{j'} := \lambda'_{j'}$ for $j' \neq j$ and $\lambda_j := \lambda'_j + \hat{e}$, and return $(\lambda_{j'})_{j'}$.
(2) If no pair $(i, j)$ was found such that $c^t \neq 0$, output "Matrix not primitive"
    and abort.
```

[a] In fact, this is the same as finding some $\tilde{x} \in R$ which satisfies $c^{t+1}\tilde{x} = c^t$ and then letting $x := \tilde{x}e$. This works since multiplying by e is a projection from R onto Re.

The initial call is `ComputePrimitiveCombination`$(1, A)$ for a primitive matrix $A \in R^{n \times m}$ of which every two-by-two minor vanishes.

In fact, this algorithm also works for an Artinian ring, since such a ring is the product of finitely many local Artinian rings, and for each of these the maximal ideal is nilpotent. By taking the maximum of the nilpotence indices of the maximal ideals in the local rings one obtains a value for t. That $c^t = xc^{t+1}$ always has a solution for every $c \in R$ can be seen in every local factor of R, since there either $c^t = 0$ or c^t is a unit.

From the discussion from the previous pages, we get the following result:

Proposition 2.4.25. *Let R be a finite ring. Then the condition $(*)$ is fulfilled. Moreover, given a primitive matrix $A \in R^{n \times m}$ whose two-by-two minors vanish, the primitive linear combination of the columns can be computed efficiently.*

We will now give some further conditions that imply $(*)$.

Lemma 2.4.26. *Let R be a ring and $\mathfrak{m}_1, \ldots, \mathfrak{m}_k, \mathfrak{m}$ distinct maximal ideals. Then there exists an*

$$m \in \bigcap_{i=1}^{k} \mathfrak{m}_i \qquad \text{such that} \qquad m \notin \mathfrak{m}.$$

Proof. For every i there exists an $m_i \in \mathfrak{m}_i$ such that $m_i \notin \mathfrak{m}$: otherwise $\mathfrak{m}_i$ would be a proper subset of $\mathfrak{m}$. Let $m := \prod_{i=1}^{k} m_i$. Then $m \in \mathfrak{m}_i$ for all i and, thus, $m \in \bigcap_{i=1}^{k} \mathfrak{m}_i$. Since every maximal ideal is prime, $m \in \mathfrak{m}$ would imply that one of the m_i's is in $\mathfrak{m}$, which would be a contradiction. □

Proposition 2.4.27. *Let R be a ring with a finite number of maximal ideals. Then the matrix condition $(*)$ is fulfilled.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ be the maximal ideals. By Lemma 2.4.26 there exist $x_1, \ldots, x_k$ such that $x_i \notin \mathfrak{m}_i$ and $x_i \in \bigcap_{j \neq i} \mathfrak{m}_j$. Hence, x_i maps onto a unit in $R/\mathfrak{m}_i$ and onto zero in $R/\mathfrak{m}_j$ for all $j \neq i$.

Let $A = (a_{ij})_{ij} \in R^{n \times m}$ be a primitive matrix. Then for every ℓ one of the a_{ij}'s is a unit in $R/\mathfrak{m}_\ell$; let j_ℓ be the column containing this element. Now let $v := \sum_{\ell=1}^{k} x_\ell A_{\bullet j_\ell}$; then v is the multiple of $A_{\bullet j_\ell}$ by a unit in $R/\mathfrak{m}_\ell$ and, therefore, v is primitive in $R/\mathfrak{m}_\ell$ for every ℓ. Using Lemma 2.4.3 we can conclude that v is primitive in R. □

Corollary 2.4.28. *Every Artinian ring satisfies $(*)$.*

Proof. By Proposition 2.2.19 every Artinian ring has finitely many maximal ideals and, therefore, satisfies $(*)$ by Proposition 2.4.27. □

Since every finite ring is Artinian we now have another proof of the first statement of Proposition 2.4.25. The proof of Proposition 2.4.27 can be turned into an algorithm to compute the linear combination, if the following constraints are satisfied:

(1) Efficient addition and multiplication in R;

(2) The maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ in the sense that k is known and for given $x \in R$ and $i \in \{1, \ldots, k\}$, one can efficiently compute whether $x \in \mathfrak{m}_i$ or not;

(3) The x_i's from the proof of Proposition 2.4.27.

The practical use of this algorithm can be questioned as it is desirable to hide as much information as possible about the structure of R. (Refer to Sections 5.1 and 5.2 for more information.)

Proposition 2.4.29. *Let R be a unique factorization domain. Then R fulfills $(*)$.*

Proof. Let $A = (a_{ij})_{ij} \in R^{n \times m}$ be a primitive matrix such that every two-by-two minor vanishes.

Let i be such that $A_{i\bullet}$ is non-zero. Let v_i be a greatest common divisor of $a_{i1}, \ldots, a_{im}$, and $v_i = \sum_j \mu_{ij} a_{ij}$ for some $\mu_{ij} \in R$. By the vanishing of the two-by-two minors we get

$$\Big(\sum_j \lambda_j a_{kj}\Big) A_{\ell\bullet} = \Big(\sum_j \lambda_j a_{\ell j}\Big) A_{k\bullet}$$

for all $k, \ell \in \{1, \dots, n\}$ and all $(\lambda_j)_j \in R^m$. Let k and ℓ be such that $A_{k\bullet}$ and $A_{\ell\bullet}$ are non-zero. For a fixed k choose $\lambda_j = \mu_{kj}$; then $\sum_j \lambda_j a_{kj} = v_k$ and, hence,

$$v_k A_{\ell\bullet} = \Big(\sum_j \mu_{kj} a_{\ell j}\Big) A_{k\bullet}.$$

Now $v_\ell v_k$ is a greatest common divisor for the components of the vector on the left side, and $v_k \sum_j \mu_{kj} a_{\ell j}$ is a greatest common divisor for the elements of the vector on the right side. Cancelling v_k gives $\sum_j \mu_{kj} a_{\ell j}$, and $v_\ell = \sum_j \mu_{\ell j} a_{\ell j}$ differ only by multiplication by a unit. This shows that for every i such that $A_{i\bullet}$ is non-zero, the combination $\sum_j \mu_{kj} a_{ij}$ is a greatest common divisor of $a_{i1}, \dots, a_{im}$. Therefore, we can assume without loss of generality, that $\mu_j := \mu_{kj} = \mu_{ij}$ for all k. Thus, we have $v_k = \sum_j \mu_j a_{kj}$ for all k such that $A_{k\bullet}$ is non-zero.

Now a greatest common divisor of all a_{ij}'s is also a greatest common divisor of $v_1, \dots, v_n$ and, hence, there exist $\lambda_1, \dots, \lambda_n \in R$ such that

$$1 = \sum_i \lambda_i v_i = \sum_i \lambda_i \sum_j \mu_j a_{ij}.$$

Therefore we have completed the proof since this shows that $\sum_j \mu_j A_{\bullet j}$ is primitive. □

2.5 Examples

In this section we will present some examples of finite rings. We will discuss how they can be represented so that the required operations for the `ComputePrimitiveCombination` algorithm can be computed effectively. We will also describe how this algorithm can be specialized for quotients of Euclidean rings.

2.5.1 Quotients of Euclidean Rings

Definition 2.5.1. *A domain R is called* Euclidean *if there exists a function* $\deg : R \setminus \{0\} \to \mathbb{N}$ *such that for every $f, g \in R$, $g \neq 0$ there exist $q, r \in R$ with $f = qg + r$, and where either $r = 0$ or* $\deg r < \deg g$.

The most important examples are the integers $\mathbb{Z}$, where $\deg x = |x|$, and the ring of polynomials in one indeterminate over a field with the usual degree function. One can show that every Euclidean ring is a principal ideal domain and, hence, a unique factorization domain.

For the remainder of this subsection let R denote an Euclidean ring with degree function deg, and let $\mathfrak{a} = \langle f \rangle$ be an ideal in R generated by $f \in R \setminus (\{0\} \cup R^*)$. Define

$$g \equiv g' \pmod f \;:\Longleftrightarrow\; g - g' \text{ is divisible by } f.$$

Next we will study some general properties of $R/\mathfrak{a}$. Note that while Euclidean rings are usually infinite, quotients $R/\mathfrak{a}$ can be finite. In the cases we will inspect more closely they are generally finite.

Lemma 2.5.2. *We have*

$$R/\mathfrak{a} = \{0 + \mathfrak{a}\} \cup \{r + \mathfrak{a} \mid r \in R \setminus \{0\},\ \deg r < \deg f\}.$$

Proof. It is clear that the set on the right is a subset of $R/\mathfrak{a}$. Conversely, let $g + \mathfrak{a} \in R/\mathfrak{a}$. Write $g = qf + r$ where $q, r \in R$ such that $r = 0$ or $\deg r < \deg f$. Therefore we have $g + \mathfrak{a} = r + \mathfrak{a}$. □

Recall that a *greatest common divisor* d of elements $r_1, \ldots, r_n$ satisfies that it divides $r_1, \ldots, r_n$, and for every other divisor d' of $r_1, \ldots, r_n$, we have that d' divides d.

Remarks 2.5.3.

(a) Since R is a unique factorization domain, the greatest common divisor exists for any finite collection of elements of R, where at least one is not zero.

(b) If d is a greatest common divisor of $g_1, \ldots, g_n$, then there exists $h_1, \ldots, h_n \in R$ such that

$$d = \sum_{i=1}^{n} h_i g_i.$$

Such an equation is called a *Bézout equation.* If one can write $1 = \sum_{i=1}^{n} h_i g_i$ where $h_1, \ldots, h_n \in R$, then 1 is a greatest common divisor of $g_1, \ldots, g_n$.

(c) For the case where $n = 2$, the greatest common divisor and the corresponding Bézout equation can be effectively computed by using the *Extended Euclidean Algorithm*, which we will state here without a proof of correctness:

Let $a_1, a_2 \in R$, both not zero. Compute the following divisions, where $q_i, a_j \in R$:

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3 && (a_3 = 0 \quad \text{or} \quad \deg a_3 < \deg a_2),\\
a_2 &= q_2 a_3 + a_4 && (a_4 = 0 \quad \text{or} \quad \deg a_4 < \deg a_3),\\
a_3 &= q_3 a_4 + a_5 && (a_5 = 0 \quad \text{or} \quad \deg a_5 < \deg a_4),\\
&\vdots\\
a_n &= q_n a_{n+1} + a_{n+2} && (a_{n+2} = 0 \quad \text{or} \quad \deg a_{n+2} < \deg a_{n+3}),\\
&\vdots
\end{aligned}$$

Eventually we get $a_{n+2} = 0$ for some n; stop the computations at this point. Then a_{n+1} is the greatest common divisor of a_1 and a_2. Now consider the equations:

$$\begin{aligned}
a_3 &= a_1 - q_1 a_2, && (3)\\
a_4 &= a_2 - q_2 a_3, && (4)\\
a_5 &= a_3 - q_3 a_4, && (5)\\
&\vdots\\
a_n &= a_{n-2} - q_{n-2} a_{n-1} && (n)\\
a_{n+1} &= a_{n-1} - q_{n-1} a_n && (n+1)
\end{aligned}$$

By iteratively substituting equation (3) into (4) and (5), ..., $(n-1)$ into (n) and $(n+1)$, and finally (n) into $(n+1)$, we get $a_{n+1} = \alpha a_1 + \beta a_2$ for some $\alpha, \beta \in R$. Thus, we computed a Bézout equation for a_1 and a_2.

We can characterize the units in $R/\mathfrak{a}$ by the following standard result from algebra:

Lemma 2.5.4. *The element $g + \mathfrak{a} \in R/\mathfrak{a}$ is invertible if, and only if, g and f are coprime. If $1 = g'g + f'f$ is a Bézout equation for g and f where $g', f' \in R$, then the inverse of $g + \mathfrak{a}$ in $R/\mathfrak{a}$ is $g' + \mathfrak{a}$.*

Proof. Clearly $(g+\mathfrak{a})(g'+\mathfrak{a}) = 1+\mathfrak{a}$ if, and only if, $1 = gg'+ff'$ for some $f' \in R$. □

Therefore, the Extended Euclidean Algorithm can be used to decide whether an element of $R/\mathfrak{a}$ is a unit and to compute its inverse if it is a unit.

We are now interested in whether a congruence $gx \equiv h \pmod{f}$ is solvable, i. e. if the equation $gx = h$ in $R/\mathfrak{a}$ is solvable, and how to compute a solution if that is possible. If g is a unit in $R/\mathfrak{a}$, the congruence is always solvable and, by using the Extended Euclidean Algorithm, the unique solution can be effectively computed. The following lemma gives a solution to the other cases:

Lemma 2.5.5. *Let $a, b \in R$. Denote by d a greatest common divisor of a and f. Then the congruence*

$$ax \equiv b \pmod{f}$$

has a solution $x \in R$ if, and only if, d divides b. If $x \in R$ is a solution, then all other solutions are given by

$$x + \frac{f}{d}g, \qquad \text{where } g \in R.$$

This lemma is a standard result in Elementary Number Theory (see for example [IR82, p. 32, Proposition 3.3.1]).

From the proof one obtains the following algorithm to decide whether $ax \equiv b \pmod{f}$ has a solution and to compute a solution if it is solvable:

(1) Compute a greatest common divisor d of a and f.

(2) If d does not divide b, output *"No solutions found"* and abort.

(3) Compute a/d, b/d and f/d.

(4) Use the Extended Euclidean Algorithm to compute $(a/d)^{-1}$ in $R/\langle f/d\rangle$.

(5) Compute $x := (a/d)^{-1}(b/d) \mod (f/d)$.

(6) Output x.

If $R/\mathfrak{a}$ fulfills all other requirements for the `ComputePrimitiveCombination` algorithm, it can be implemented as specified in Section 2.4. But it can also be improved if the elements of $R/\mathfrak{a}$ are represented by their residue modulo f. We first need a special version of the Chinese Remainder Theorem 2.0.3:

Proposition 2.5.6 (Chinese Remainder Theorem). *Let $f_1, \ldots, f_k \in R$ be pairwise coprime and let $f := f_1 \cdots f_k$ and $\mathfrak{a} = \langle f\rangle$. Then the map*

$$\psi : R/\mathfrak{a} \to R/\langle f_1\rangle \times \cdots \times R/\langle f_k\rangle, \qquad a + \mathfrak{a} \mapsto (a + \langle f_1\rangle, \ldots, a + \langle f_k\rangle)$$

is an isomorphism.

Note that the proposition as stated here works for every principal ideal domain. We state this proof instead of referring to Theorem 2.0.3 since it shows how to effectively compute the isomorphism and its inverse.

Proof. Consider the map

$$\varphi : R \to R/\langle f_1\rangle \times \cdots \times R/\langle f_k\rangle, \qquad a \mapsto (a + \langle f_1\rangle, \ldots, a + \langle f_k\rangle).$$

It is clear that φ is a ring homomorphism. In addition we have

$$\ker \varphi = \bigcap_{i=1}^{k} \ker(R \to R/\langle f_i\rangle\,,\ a \mapsto a + \langle f_i\rangle) = \bigcap_{i=1}^{k} \langle f_i\rangle = \langle f\rangle = \mathfrak{a},$$

since f is the least common multiple of the f_i's and R is a principal ideal domain. Hence, we have

$$R/\mathfrak{a} \cong \varphi(R) \subseteq R/\langle f_1\rangle \times \cdots \times R/\langle f_k\rangle\,.$$

We will now construct $a_i \in R$ such that $\varphi(a_i) = (0, \ldots, 0, 1, 0, \ldots, 0) =: e_i$, where the 1 is at the i-th position. This implies that φ and, hence, ψ is surjective.

It can easily be seen that f_i and $\hat{f}_i := \prod_{\substack{j=1\\ j\neq i}}^{n} f_j$ are coprime for every i. Thus, there exists a Bézout equation $1 = g_i f_i + \hat{g}_i \hat{f}_i$, where $g_i, \hat{g}_i \in R$. Let $a_i := 1 - g_i f_i$. Now $a_i + \langle f_i\rangle = 1 + \langle f_i\rangle$ and if $j \neq i$,

$$a_i + \langle f_j\rangle = \hat{g}_i \hat{f}_i + \langle f_j\rangle = \hat{g}_i \prod_{\substack{k=1\\ k\neq i}}^{n} f_k + \langle f_j\rangle = 0 + \langle f_j\rangle\,.$$

Therefore we have $\varphi(a_i) = e_i$. □

Assume $f = u f_1^{e_1} \cdots f_k^{e_k}$, where $u \in R^*$ and $e_i \in \mathbb{N}_{>0}$, is the factorization of f into pairwise distinct primes $f_1, \ldots, f_k$. By the Chinese Remainder Theorem we have

$$R/\mathfrak{a} \cong R/\langle f_1^{e_1}\rangle \times \cdots \times R/\left\langle f_k^{e_k}\right\rangle,$$

and both the isomorphism ψ and its inverse are effectively computable. If the factorization is known, the algorithm `ComputePrimitiveCombination` can be rewritten using this fact and the following result.

Lemma 2.5.7. *Let $f \in R$ be prime and $e \in \mathbb{N}_{>0}$. Then $S := R/\langle f^e\rangle$ is local, and S is a field if, and only if, $e = 1$.*

Proof. Note that an element $g + \langle f^e\rangle$ is not a unit in S if, and only if, f divides g. Thus, the non-units of S form a subgroup of $(S, +)$ and, hence, by Proposition 2.2.6, S is local.

For the equivalence note that $R/\mathfrak{a}$ is a field if, and only if, $\mathfrak{a}$ is a maximal ideal. Now $\langle f^e\rangle \subsetneqq \langle f\rangle \subsetneqq R$ if, and only if, $e > 1$. Therefore S can only be a field if $e = 1$. For $e = 1$ it is a field, because f is prime and, hence, $\langle f\rangle$ is a prime ideal; in any principal ideal domain every prime ideal is maximal. □

Recall that in local rings a collection of elements is primitive if, and only if, at least one of them is a unit.

We will now discuss how the algorithm `ComputePrimitiveCombination` can be optimized when the factorization of f is not known.

Let $A = (a_{ij})_{ij} \in (R/\mathfrak{a})^{k \times \ell}$ be a matrix primitive over $R/\mathfrak{a}$, for which every two-by-two minor of A vanishes. Let i, j be indices such that $a_{ij} \neq 0$. Compute a greatest common divisor d of a_{ij} and f. If d is a unit, a_{ij} is a unit in $R/\mathfrak{a}$ and the column $A_{\bullet j}$ is primitive. If d is not a unit, then d is a non-trivial factor of f. We distinguish two cases:

(a) If f contains at least two different prime factors we can write $f = f_1 f_2$, where f_1 and f_2 are coprime non-units. By the Chinese Remainder Theorem 2.5.6 we have $R/\mathfrak{a} \cong R/\langle f_1 \rangle \times R/\langle f_2 \rangle$, where the isomorphism is given by

$$\psi : R/\mathfrak{a} \to R/\langle f_1 \rangle \times R/\langle f_2 \rangle, \qquad a + \langle f \rangle \mapsto (a + \langle f_1 \rangle, a + \langle f_2 \rangle)$$

and, hence, is efficiently computable. We can then reduce the problem to two instances of computing a primitive linear combination of the columns, one over $R/\langle f_1 \rangle$ and one over $R/\langle f_2 \rangle$. If d divides f_1, then a_{ij} is a unit modulo f_2 and, thus, we only have to recurse on the instance over $R/\langle f_1 \rangle$.

(b) If $f = f_1^k$ where f_1 is prime and $k > 1$, the ring $R/\mathfrak{a}$ is local and, hence, there must be some i, j such that a_{ij} is a unit.

Therefore, the algorithm can be vastly simplified.

Next we want to give two important examples of Euclidean rings that are often used in practice:

Examples 2.5.8.

(1) As already mentioned, the integers $\mathbb{Z}$, together with the degree function $\deg x = |x|$, are a Euclidean ring.

If $n \in \mathbb{N}$ is greater than one, then $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ is a finite non-zero ring.

(2) Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. Consider the ring of polynomials in one indeterminate, $\mathbb{F}_q[x]$. As already mentioned, this ring is Euclidean, where the degree function is given by the usual polynomial degree, i. e. if $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{F}_q[x] \setminus \{0\}$, where $a_n \neq 0$, then $\deg f = n$.

If $f \in \mathbb{F}_q[x] \setminus \{0\}$ is not a unit, then $R/\langle f \rangle$ is a finite non-zero ring.

2.5.2 Quotients of Multivariate Polynomial Rings

In this section we will look at quotients of polynomial rings over finite fields, i. e. $R := \mathbb{F}_q[x_1, \dots, x_n]/\mathfrak{a}$, where $n > 1$, q is a prime power and $\mathfrak{a}$ is an ideal in $\mathbb{F}_q[x_1, \dots, x_n]$. Assume that operations in $\mathbb{F}_q$ can be computed effectively.

By the Hilbert Basis Theorem (Proposition 2.0.6 (b)) $\mathbb{F}_q[x_1, \dots, x_n]$ is Noetherian and, hence, every ideal $\mathfrak{a}$ in $R := \mathbb{F}_q[x_1, \dots, x_n]$ can be written as $\mathfrak{a} = \langle f_1, \dots, f_s \rangle$ for some $f_1, \dots, f_s \in \mathbb{F}_q[x_1, \dots, x_n]$. Fix $\mathfrak{a} = \langle f_1, \dots, f_s \rangle$. The question arises if there is an analogon to polynomial division in the univariate case, which would allow an effective representation of elements and efficient arithmetic in R. A solution for this problem is given by so called *Gröbner bases* and the *division algorithm.* We will recall the basics here; more information can be found for example in chapter 15 of [Eis95] and in the books [CLO96] and [CLO98].

Definition 2.5.9. *Let $\mathbb{F}$ be a field. Consider the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$.*

(a) *If $\alpha = (\alpha_i)_i \in \mathbb{N}^n$, we write x^α for $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.*

(b) *A* monomial order *$\leq$ is a total well-ordering*[1] *of $\mathbb{N}^n$ that is compatible with addition, i. e. for $\alpha, \beta, \gamma \in \mathbb{N}^n$, $\alpha \leq \beta$ if, and only if, $\alpha + \gamma \leq \beta + \gamma$. For $x^\alpha, x^\beta \in \mathbb{F}[x_1, \dots, x_n]$ we define*

$$x^\alpha \leq x^\beta :\Longleftrightarrow \alpha \leq \beta.$$

(c) *Let $\leq$ be a monomial order and $f \in \mathbb{F}[x_1, \dots, x_n] \setminus \{0\}$. Let $f = \sum_{i=1}^k a_i x^{\alpha_i}$, where $\alpha_1 > \cdots > \alpha_k$ and $a_i \in \mathbb{F} \setminus \{0\}$ for every i. Define*

$$\begin{aligned} \operatorname{mdeg}_\leq(f) &:= \alpha_1 && \textit{(multi degree)}, \\ \operatorname{LM}_\leq(f) &:= x^{\alpha_1} && \textit{(leading monomial)}, \\ \operatorname{LT}_\leq(f) &:= a_1 x^{\alpha_1} && \textit{(leading term)}. \end{aligned}$$

(d) *If $\mathfrak{a}$ is an ideal in $\mathbb{F}[x_1, \dots, x_n]$, we call the ideal*

$$\operatorname{in}_\leq(\mathfrak{a}) := \langle \{\operatorname{LM}_\leq(f) \mid f \in \mathfrak{a} \setminus \{0\}\} \rangle$$

the initial ideal *of $\mathfrak{a}$.*

(e) *Let $f_1, \dots, f_s \in \mathbb{F}[x_1, \dots, x_s]$ and $\mathfrak{a}$ be an ideal in $\mathbb{F}[x_1, \dots, x_n]$. We call $f_1, \dots, f_s$ a* Gröbner basis *of $\mathfrak{a}$ if $\operatorname{in}_\leq(\mathfrak{a}) = \langle \operatorname{LM}_\leq(f_1), \dots, \operatorname{LM}_\leq(f_s) \rangle$.*

Remarks 2.5.10. Let $\mathbb{F}$ be a field. Consider the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$. If not said otherwise, $\leq$ is an arbitrary monomial order on $\mathbb{N}^n$ and $\mathfrak{a}$ is an arbitrary ideal in $\mathbb{F}[x_1, \dots, x_n]$.

(a) [CLO96, pp. 52ff] There exist monomial orders for every n. For $n = 1$, there is exactly one, but for $n > 1$ there is an infinite number of monomial orders. An example is the lexicographic order: For $(\alpha_i)_i, (\beta_i)_i \in \mathbb{N}^n$ define

$$(\alpha_i)_i < (\beta_i)_i :\Longleftrightarrow \exists 1 \leq j \leq n \text{ such that } \alpha_i = \beta_i \text{ for all } i < j \text{ and } \alpha_j < \beta_j.$$

(b) [CLO96, p. 75, Corollary 6] If $f_1, \dots, f_s$ is a Gröbner basis of $\mathfrak{a}$, it can be shown that $\mathfrak{a} = \langle f_1, \dots, f_s \rangle$.

(c) [CLO96, p. 87, Theorem 2] If $\mathfrak{a} = \langle f_1, \dots, f_s \rangle$, then a Gröbner basis of $\mathfrak{a}$ can be computed from the f_i's by *Buchberger's algorithm*.

(d) [CLO96, p. 80] If $f_1, \dots, f_s$ is a Gröbner basis of $\mathfrak{a}$, every $f \in \mathbb{F}[x_1, \dots, x_n]$ can be represented as $f = \sum_{i=1}^s g_i f_i + r$, where $g_1, \dots, g_s, r \in \mathbb{F}[x_1, \dots, x_s]$ such that $\operatorname{mdeg}_\leq(f_i g_i) \leq \operatorname{mdeg}_\leq(f)$ if $f_i g_i \neq 0$ and none of the monomials of r is contained in the initial ideal of $\mathfrak{a}$. Further note that r is unique, and there exists an algorithm which efficiently computes such a representation. This algorithm allows to efficiently decide whether $f \in \mathbb{F}[x_1, \dots, x_n]$ is in $\mathfrak{a}$ or not: $f \in \mathfrak{a}$ if, and only if, $r = 0$. From now on, we write $\overline{f}^{\mathfrak{a}, \leq}$ for r, or simply $\overline{f}$ if $\leq$ and $\mathfrak{a}$ are clear from the context.

The algorithm that computes the representation is called the *division algorithm* [CLO96, pp. 61f, Theorem 3]. We will state it here without a proof of correctness:

[1] A total order $\leq$ on a set M is a *well-ordering* if every non-empty subset of M has a minimum with respect to $\leq$.

```
(1) Set $g_i := 0$ for all $i$ and $r := 0$.
(2) While $f \neq 0$ repeat the following:
    • If there is an $i \in \{1, \dots, s\}$ such that $\mathrm{LM}_\leq(f_i)$ divides $\mathrm{LM}_\leq(f)$:
        (1) Let $g_i := g_i + \frac{\mathrm{LT}_\leq(f)}{\mathrm{LT}_\leq(f_i)}$.
        (2) Let $f := f - \frac{\mathrm{LT}_\leq(f)}{\mathrm{LT}_\leq(f_i)} f_i$.
    • Otherwise:
        (1) Let $r := r + \mathrm{LT}_\leq(f)$.
        (2) Let $f := f - \mathrm{LT}_\leq(f)$.
(3) Output $\sum_{i=1}^{s} g_i f_i + r$.
```

(e) [CLO98, p. 36] Let $\mathcal{B}_{\mathfrak{a},\leq} := \{\alpha \in \mathbb{N}^n \mid x^\alpha \notin \mathrm{in}_\leq(\mathfrak{a})\}$. Then $\{x^\alpha + \mathfrak{a} \mid \alpha \in \mathcal{B}_{\mathfrak{a},\leq}\}$ is a $\mathbb{F}$-vector space basis of $\mathbb{F}[x_1, \dots, x_n]/\mathfrak{a}$.

From now on, let $\leq$ be an arbitrary, but fixed, monomial order on $\mathbb{N}^n$. We will write LT instead of $\mathrm{LT}_\leq$, $\mathcal{B}_\mathfrak{a}$ instead of $\mathcal{B}_{\mathfrak{a},\leq}$ etc.

The last remark shows that not every ideal $\mathfrak{a}$ is useful for our purposes, as we want $R = \mathbb{F}_q[x_1, \dots, x_n]/\mathfrak{a}$ to be finite. If a Gröbner basis $f_1, \dots, f_s$ of $\mathfrak{a}$ and, thus, a basis $\mathrm{LM}(f_1), \dots, \mathrm{LM}(f_s)$ of the initial ideal $\mathrm{in}(\mathfrak{a})$ is given, one can decide whether R is finite or not: If for every $i \in \{1, \dots, n\}$ there exists an $e_i \in \mathbb{N}$ such that $x_i^{e_i} \in \mathrm{in}(\mathfrak{a})$, R is finite (and vice versa). And it is $x_i^{e_i} \in \mathrm{in}(\mathfrak{a})$ if, and only if, $\mathrm{LM}(f_j)$ is a multiple of $x_i^{e_i}$ for a j. Therefore R is finite if, and only if, for every $i \in \{1, \dots, n\}$ there is some $j \in \{1, \dots, s\}$ such that $\mathrm{LM}(f_j) \in \mathbb{F}_q[x_i]$. (See [CLO98, p. 37].)

Note that ideals $\mathfrak{a} \neq \mathbb{F}[x_1, \dots, x_n]$ such that $\dim_\mathbb{F} \mathbb{F}[x_1, \dots, x_n]/\mathfrak{a} < \infty$ are called *zero-dimensional*. These are exactly the ideals such that the Krull dimension $\dim \mathbb{F}[x_1, \dots, x_n]/\mathfrak{a}$ is zero.

What is missing for the `ComputePrimitiveCombination` algorithm is the question of how to solve $fx = g \pmod{\mathfrak{a}}$ for $f, g \in \mathbb{F}_q[x_1, \dots, x_n]$, if a solution is known to exist. We will show that this question can be reduced to the problem of solving systems of linear equations over $\mathbb{F}_q$.

Fix $\mathfrak{a} = \langle f_1, \dots, f_s \rangle$ and let $\mathcal{B} := \mathcal{B}_\mathfrak{a}$. Let $\alpha_1 < \alpha_2 < \dots < \alpha_t$ be the elements of $\mathcal{B}$. Hence, $R := \mathbb{F}_q[x_1, \dots, x_n]/\mathfrak{a} \cong \mathbb{F}_q^t$ as an $\mathbb{F}_q$-vector space. For $f \in \mathbb{F}_q[x_1, \dots, x_n]$, let $M_f \in \mathbb{F}_q^{t \times t}$ be the matrix representation of the $\mathbb{F}_q$-vector space endomorphism $x \mapsto fx$ of R, where the basis is given by $(x^{\alpha_1} + \mathfrak{a}, \dots, x^{\alpha_t} + \mathfrak{a})$. It is clear that $\varphi : \mathbb{F}_q[x_1, \dots, x_n] \to \mathbb{F}_q^{t \times t}$, $f \mapsto M_f$ is a ring homomorphism whose kernel is $\mathfrak{a}$. Let $\psi : R \to \mathbb{F}_q^t$, $x^{\alpha_i} \mapsto e_i$ be the coordinate map[2] for the $\mathbb{F}_q$-basis $(x^{\alpha_1}, \dots, x^{\alpha_n})$ of R. It is easy to see that ψ can be extended to a vector space homomorphism $\mathbb{F}_q[x_1, \dots, x_n] \to \mathbb{F}_q^t$ by $f \mapsto \psi(\overline{f})$, with kernel $\mathfrak{a}$. By writing $f = \sum_{i=1}^{k} f_i x^{\beta_i}$, it can be easily seen that

$$\psi(fg) = \sum_{i=1}^{k} f_i \psi(x^{\beta_i} g) = \sum_{i=1}^{k} f_i M_{x^{\beta_i}} \psi(g) = M_f \psi(g).$$

This gives that $fg \equiv h \pmod{\mathfrak{a}}$ if, and only if, $\psi(fg) = \psi(h)$, which again is equivalent to $M_f \psi(g) = \psi(h)$. Moreover, since further ψ is surjective, this leads to a solution to the problem as to whether $fg \equiv h \pmod{\mathfrak{a}}$ holds for a $g \in \mathbb{F}_q[x_1, \dots, x_n]$:

[2] Let e_i denote the vector $(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{F}_q^t$, where the 1 is at the i-th position.

the congruence is solvable if, and only if, the system of linear equations

$$M_f \begin{pmatrix} g_1 \\ \vdots \\ g_t \end{pmatrix} = \psi(h), \qquad g_1, \ldots, g_t \in \mathbb{F}_q \tag{$*$}$$

over $\mathbb{F}_q$ is solvable. Furthermore, $(g_1, \ldots, g_t)$ is a solution of $(*)$ if, and only if, $g = \sum_{i=1}^{t} g_i x^{\alpha_i}$ is a solution for $fg \equiv h \pmod{\mathfrak{a}}$.

Now M_f respectively $\psi(h)$ can be effectively computed from f respectively h by using the division algorithm, and the Gaussian elimination algorithm can be used to effectively solve $(*)$ or to test whether a solution does exist. Therefore, we provided everything needed for the `ComputePrimitiveCombination` algorithm.

Remarks 2.5.11.

(1) We conclude that $f \in R = \mathbb{F}[x_1, \ldots, x_n]/\mathfrak{a}$ is invertible if, and only if, M_f is invertible, which is the case if, and only if, $\det M_f \neq 0$.

(2) When n and/or t are large, the algorithms presented here are not very efficient, both in running time and memory consumption.

(3) Instead of taking quotients of $\mathbb{F}[x_1, \ldots, x_n]$ there is another way to construct $\mathbb{F}$-algebras. Unfortunately, not every finitely generated $\mathbb{F}$-algebra can be represented by this construction.

Let $(M, \cdot, 1_M)$ be an Abelian monoid and let $R := \oplus_{\alpha \in M} \mathbb{F}$. Define a multiplication on R by

$$(x_\alpha)_{\alpha \in M} \cdot (y_\alpha)_{\alpha \in M} := (z_\alpha)_{\alpha \in M} \qquad \text{where} \qquad z_\gamma := \sum_{\substack{\alpha, \beta \in M \\ \alpha\beta = \gamma}} x_\alpha y_\beta.$$

By writing $\sum'_{\alpha \in M} x_\alpha \alpha$ for $(x_\alpha)_{\alpha \in M}$, it is easy to see that R is a commutative ring with the unit $1_{\mathbb{F}} 1_M$. Since $\mathbb{F}$ is embedded in R by $x \mapsto x 1_M$, R is an $\mathbb{F}$-algebra. Again, the determination of whether an element is a unit or whether an equation is solvable can be reduced to solving systems of linear equations over $\mathbb{F}$.

If $M = \{\alpha_1, \ldots, \alpha_n\}$ is finite and $n = |M|$, one can define a surjective $\mathbb{F}$-linear map $\varphi : \mathbb{F}[x_1, \ldots, x_n] \to R$ by $x_i \mapsto \alpha_i$. If $\mathfrak{a} := \ker \varphi$, then $\mathbb{F}[x_1, \ldots, x_n]/\mathfrak{a} \cong R$, and $\mathcal{B}_{\mathfrak{a}}$ corresponds to M. (Obviously this is not a good method to find such a representation as, in general, there are representations with substantially less indeterminates.)

Finally, we want to show why not every quotient of $\mathbb{F}[x_1, \ldots, x_n]$ can be described by this construction. Consider $\mathbb{F}[x]/\langle x^2 \rangle$, which is a local ring and not isomorphic to $\mathbb{F} \times \mathbb{F}$. Assume that the characteristic of $\mathbb{F}$ is $\neq 2$. Up to isomorphism there are only two monoids with two elements, namely $(\mathbb{Z}_2, +)$ and $G = \{1, a\}$ with $1 \oplus 1 = 1$ and $1 \oplus a = a \oplus a = a \oplus 1 = a$. The construction resulting from $(\mathbb{Z}_2, +)$ is

$$\mathbb{F}[x, y]/\langle x - 1, y^2 - x \rangle \cong \mathbb{F}[y]/\langle y^2 - 1 \rangle = \mathbb{F}[y]/\langle (y-1)(y+1) \rangle \cong \mathbb{F} \times \mathbb{F}$$

since $2 \neq 0$ in $\mathbb{F}$. The construction resulting from $(G, \oplus)$ is

$$\mathbb{F}[x,y]/\left\langle x-1, y^2-y\right\rangle \cong \mathbb{F}[y]/\left\langle y(y-1)\right\rangle \cong \mathbb{F}\times\mathbb{F}.$$

The reason why we mention this method is that it might lead to an easier implementation in some cases.

2.6 Sheaves

In this section we want to give a short introduction to the Theory of Sheaves. Sheaves are objects that collect local and global information about some other object. As a reference see [Har77, pp. 60ff, ch. II, Section 1 and Section 5]. We want to remark that one can also define sheaves in a different way that gives the same results. This is, for example, done in [Iit82].

2.6.1 Presheaves and Sheaves

Let $\mathscr{C}$ be an arbitrary category. For simplicity, we will assume that certain products and coproducts do exist in some parts. In the categories we will use later, namely $\mathscr{A}b$ and $\mathscr{R}ing$, such products do exist.

First we want to fix a notation:

Definition 2.6.1. *Let X be a topological space and $U \subseteq X$ an open set. Then one defines $\mathbb{U}_U$ as the set of open subsets of U. Moreover, if $V \subseteq U$ is any set, then we denote with $\mathbb{U}_{U,V}$ the open sets in $\mathbb{U}_U$ which contain V, and we write $\mathbb{U}_{U,p}$ for $\mathbb{U}_{U,\{p\}}$.*

Remark 2.6.2. In fact, $\mathbb{U}_U$ is the trace topology of X induced onto U.

For the remainder of this subsection, we will always mean a topological space when we write X. We begin by defining what a (pre)sheaf in $\mathscr{C}$ over X is.

Definition 2.6.3. *Let $\mathscr{C}$ be a category. A* presheaf $\mathcal{F}$ in $\mathscr{C}$ on X *is a map that assigns an object $\mathcal{F}(U) \in \mathscr{C}$ to every open set $U \in \mathbb{U}_X$, together with a set of morphisms $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ for each pair $U, V \in \mathbb{U}_X$ such that $V \subseteq U$, satisfying the following properties:*

(1) *We have $\rho_W^V \circ \rho_V^U = \rho_W^U$ if $U, V, W \in \mathbb{U}_X$ satisfy $W \subseteq V \subseteq U$.*

(2) *For every $U \in \mathbb{U}_X$, we have $\rho_U^U = \mathbf{id}_{\mathcal{F}(U)}$.*

For $f \in \mathcal{F}(U)$ we call $\rho_V^U(f)$ the restriction of f to V, *and also write $f|_V$ instead.*

Moreover, one calls the elements $f \in \mathcal{F}(U)$ sections, *and the elements $f \in \mathcal{F}(X)$* global sections. *When U is clear, one also writes $\bullet|_V$ for ρ_V^U.*

If one more condition is satisfied, we call $\mathcal{F}$ a sheaf in $\mathscr{C}$ on X:

(3) *If $U \in \mathbb{U}_X$, open sets $U_i \in \mathbb{U}_U$ and $f_i \in \mathcal{F}(U_i)$ are given for every $i \in I$, where I is an arbitrary index set that satisfies $\bigcup_{i\in I} U_i = U$, and $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ for every $i, j \in I$, then there exists a unique $f \in \mathcal{F}(U)$ such that for every $i \in I$ we have $f|_{U_i} = f_i$.*

For a sheaf $\mathcal{F}$, one also writes $\Gamma(U, \mathcal{F})$ instead of $\mathcal{F}(U)$.

We will mainly be interested in (pre-)sheaves of Abelian groups and rings, i. e. (pre-)sheaves in the categories $\mathscr{A}b$ and $\mathscr{R}ing$.

Remarks 2.6.4. Let $\mathcal{F}$ be a sheaf on X. Then $\mathcal{F}(\emptyset) = 0$ by property (3).

A third kind of sheaf will be important later in this thesis:

Definition 2.6.5. *Let $\mathcal{O}$ be a sheaf of rings on X, and $\mathcal{F}$ be a sheaf of Abelian groups on X. One says that $\mathcal{F}$ is an* $\mathcal{O}$-module *or a* sheaf of $\mathcal{O}$-modules *if for every $U \in \mathbb{U}_X$, the group $\mathcal{F}(U)$ is an $\mathcal{O}(U)$-module and the restriction maps $\bullet|_V : \mathcal{F}(U) \to \mathcal{F}(V)$ for $V \in \mathbb{U}_U$, $U \in \mathbb{U}_X$, $V \subseteq U$ are compatible with the module structure, i. e. one has $(r \cdot f)|_V = r|_V \cdot f|_V$ for every $r \in \mathcal{O}(U)$, $f \in \mathcal{F}(U)$.*

Next we define what a morphism between two sheaves over X is. With this we get the category of sheaves in $\mathscr{C}$ over X.

Definition 2.6.6. *Let $\mathcal{F}$ and $\mathcal{G}$ be two presheaves in $\mathscr{C}$ on X. A* morphism of presheaves *$f : \mathcal{F} \to \mathcal{G}$ is a collection of morphisms $f(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ for every $U \in \mathbb{U}_X$ that are compatible with the restrictions, i. e. if $U, V \in \mathbb{U}_X$ with $V \subseteq U$, then $\bullet|_V \circ f(U) = f(V) \circ \bullet|_V$. If both $\mathcal{F}$ and $\mathcal{G}$ are sheaves, one speaks of f as a* morphism of sheaves. *An* isomorphism *of (pre-)sheaves is a morphism of (pre-)sheaves having a two-sided inverse.*

To be able to express local properties we need the following definition:

Definition 2.6.7. *[Har77, p. 62, ch. II] Let $\mathcal{F}$ be a presheaf on X and $p \in X$. Then a* germ of $\mathcal{F}$ in p *is a pair $\langle U, f \rangle$, where $U \in \mathbb{U}_{X,p}$ and $f \in \mathcal{O}(U)$, where two germs $\langle U, f \rangle$ and $\langle V, g \rangle$ are identified if, and only if, there is some $W \in \mathbb{U}_{X,p}$ satisfying $W \subseteq U \cap V$ and $f|_W = g|_W$. The set of germs of $\mathcal{F}$ in p is called the* stalk of $\mathcal{F}$ in p, *denoted by $\mathcal{F}_p$. We also write f_p for the germ $\langle U, f \rangle$ in $\mathcal{F}_p$.*

Remarks 2.6.8.

(1) [Har77, p. 62, ch. II, paragraph after definition] Note that the identification of two germs is an equivalence relation. Moreover, the object $\mathcal{F}_p$ is of the same kind as the objects $\mathcal{F}(U)$, $U \in \mathbb{U}_X$, i. e. it is an Abelian group, ring or module if $\mathcal{F}$ is a presheaf of Abelian groups or rings or a sheaf of modules, respectively.

(2) [Har77, p. 63, ch. II, paragraph after definition] Moreover, if $\mathcal{F}$ and $\mathcal{G}$ are presheaves on X, $f : \mathcal{F} \to \mathcal{G}$ is a morphism of presheaves and $p \in X$, then f induces a canonical map $f_p : \mathcal{F}_p \to \mathcal{G}_p$, which again is compatible with the structure of the objects $\mathcal{F}(U)$, $\mathcal{G}(U)$, $U \in \mathbb{U}_X$.

(3) [Har77, p. 62, ch. II, Definition] In more fancy language, one can write $\mathcal{F}_p = \varinjlim \mathcal{F}(U)$, where the limit is taken over all $U \in \mathbb{U}_{X,p}$. (See Definition 2.6.19 for $\varinjlim$, and Remarks 2.6.20 (c).)

(4) [Har77, p. 63, ch. II, proof of Proposition 1.1] Let $s \in \mathcal{F}(U)$. If $s_p = 0$ for every $p \in U$, then $s = 0$.

We now want to define what a sub(pre)sheaf is:

Definition 2.6.9. *Let $\mathcal{F}$ be a presheaf in $\mathscr{C}$ on X. A* subpresheaf *$\mathcal{G}$ of $\mathcal{F}$ is a presheaf in $\mathscr{C}$ on X such that for every open set U we have that $\mathcal{G}(U)$ is a sub-object of $\mathcal{F}(U)$ and the restriction maps of $\mathcal{G}$ are induced by those of $\mathcal{F}$. If $\mathcal{F}$ and $\mathcal{G}$ are sheaves, one calls $\mathcal{G}$ a* subsheaf *of $\mathcal{F}$.*

Remark 2.6.10. Note that if $\mathcal{G}$ is a subsheaf of $\mathcal{F}$, then for every $x \in X$ we have that $\mathcal{G}_x$ is a sub-object of $\mathcal{F}_x$.

The next proposition constructs a sheaf for every presheaf whose sections are functions on X. In case the presheaf was already a sheaf, this construction is isomorphic to the sheaf itself. Hence, the proposition shows that every sheaf can be interpreted as a sheaf whose sections are functions on X. This construction is also often used as many constructions concerning sheaves result in presheaves; in that case the sheafification is usually added as a last step of the construction.

Proposition 2.6.11. *[Har77, p. 64, Proposition-Defintion 1.2 and its proof] Let $\mathcal{F}$ be a presheaf in $\mathscr{C}$ on X. Then we can construct a sheaf $\mathcal{F}'$ as follows: For every open set $U \in \mathbb{U}_X$, let*

$$\mathcal{F}'(U) := \left\{ (f^{(p)})_{p\in U} \in \prod_{p\in U} \mathcal{F}_p \;\middle|\; \begin{matrix} \forall p \in U \; \exists V \in \mathbb{U}_{U,p}, f \in \mathcal{F}(V) \\ \forall q \in V : f^{(q)} = \langle V, f \rangle \end{matrix} \right\},$$

and define the restriction maps by

$$(f^{(p)})_{p\in U}\Big|_V := (f^{(p)})_{p\in V} \qquad \text{for } U, V \in \mathbb{U}_X,\ V \subseteq U.$$

Moreover, we can construct a morphism of presheaves $\rho_{\mathcal{F}} : \mathcal{F} \to \mathcal{F}'$ by

$$\rho_{\mathcal{F}}(U) : \mathcal{F}(U) \to \mathcal{F}'(U), \qquad f \mapsto (\langle U, f \rangle)_{p\in U},$$

which satisfies the following universal property:

Given a sheaf $\mathcal{G}$ and a morphism of presheaves $\varphi : \mathcal{F} \to \mathcal{G}$, there exists a unique morphism of sheaves $\psi : \mathcal{F}' \to \mathcal{G}$ such that $\psi \circ \rho_{\mathcal{F}} = \varphi$.

$$\begin{tikzcd} \mathcal{F} \arrow[rr, "\varphi"] \arrow[dr, "\rho_{\mathcal{F}}"'] & & \mathcal{G} \\ & \mathcal{F}' \arrow[ur, "\psi"'] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$

Moreover, $\mathcal{F}'$ is determined by this universal property up to a unique isomorphism. The sheaf $\mathcal{F}'$ is called the sheaf associated to the presheaf $\mathcal{F}$ *or the* sheafification of $\mathcal{F}$. *If $\mathcal{F}$ is a sheaf, then $\mathcal{F}'$ is isomorphic to $\mathcal{F}$.*

Remarks 2.6.12. [Har77, p. 64, ch. II, Proposition-Definition 1.2 and its proof]

(a) One can interpret an element $f := (f^{(p)})_{p\in U} \in \mathcal{F}'(U)$ as a function

$$f : U \to \coprod_{p\in U} \mathcal{F}_p, \qquad p \mapsto f^{(p)}.$$

This shows that every sheaf can be interpreted as a sheaf whose sections are functions.

(b) From this construction one directly sees that for every $x \in X$ we have $(\mathcal{F}')_x = \mathcal{F}_x$. In particular if $\mathcal{F}_x = \mathcal{G}_x$ for two presheaves $\mathcal{F}$ and $\mathcal{G}$, their associated sheaves are the same.

We now want to present constructions involving sheaves that do not always result in sheaves, but in presheaves:

Remark 2.6.13. Let I be an index set and $\mathcal{F}_i$, $i \in I$, a family of sheaves in $\mathscr{C}$ on X. Then

$$\mathcal{F} : U \mapsto \bigoplus_{i \in I} \mathcal{F}_i$$

is a presheaf, where the restriction maps $\rho_V^U : \mathcal{F}(U) \to \mathcal{F}(V)$ are the direct sum of the restriction maps $\rho_V^U : \mathcal{F}_i(U) \to \mathcal{F}_i(V)$. The same construction can be made using the direct product instead of the direct sum. For the direct product, the presheaf is in fact a sheaf.

Definition 2.6.14. *Let I be an index set and $\mathcal{F}_i$, $i \in I$, a family of sheaves. Denote by $\bigoplus_{i \in I} \mathcal{F}_i$ the sheaf associated to the presheaf*

$$U \mapsto \bigoplus_{i \in I} \mathcal{F}_i(U),$$

called the direct sum *of the $\mathcal{F}_i$'s. Also denote by $\prod_{i \in I} \mathcal{F}_i$ the sheaf*

$$U \mapsto \prod_{i \in I} \mathcal{F}_i(U),$$

called the direct product *of the $\mathcal{F}_i$'s.*

Remark 2.6.15. [Iit82, p. 44, §1.12a] If I is a finite set, then the presheaf $U \mapsto \bigoplus_{i \in I} \mathcal{F}_i(U)$ is already a sheaf.

Another construction is the quotient of two sheaves.

Lemma 2.6.16. *[Iit82, p. 34] Let $\mathcal{F}$ be a presheaf and $\mathcal{G}$ a subpresheaf of $\mathcal{F}$. Then $U \mapsto \mathcal{F}(U)/\mathcal{G}(U)$ is a presheaf, with the restriction maps being the maps induced by the restriction maps of $\mathcal{F}$, i. e.*

$$\rho_V^U : \mathcal{F}(U)/\mathcal{G}(U) \to \mathcal{F}(V)/\mathcal{G}(V), \qquad f + \mathcal{G}(U) \mapsto f|_V + \mathcal{G}(V).$$

Definition 2.6.17. *The presheaf $U \mapsto \mathcal{F}(U)/\mathcal{G}(U)$ (from Lemma 2.6.16) is called the* quotient presheaf $\mathcal{F}//\mathcal{G}$. *If $\mathcal{F}$ and $\mathcal{G}$ are sheaves, the sheafification of $\mathcal{F}//\mathcal{G}$ is called the* quotient sheaf $\mathcal{F}/\mathcal{G}$

We close this subsection with the following remark:

Remark 2.6.18. If $U \in \mathbb{U}_X$ is an open set and $\mathcal{F}$ is a sheaf on X, then one can naturally restrict $\mathcal{F}$ to U and has a sheaf $\mathcal{F}|_U$ on U. This comes from the fact that the trace topology on U is exactly the set of open subsets of X which lie in U.

2.6.2 Transportation of Sheaves via Continuous Maps

We want to introduce two constructions of transporting a sheaf to other topological spaces via a continuous map. For this we need to introduce the *direct limit* $\varinjlim \bullet$, a construction from category theory. For example, it generalizes the following construction: if p is prime, one can see $\mathbb{F}_{p^n}$ as a subfield of $\mathbb{F}_{p^m}$ if n divides m. If one forms $\bigcup_{n=0}^{\infty} \mathbb{F}_{p^n}$, where two fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^{n'}}$ are naturally embedded in $\mathbb{F}_{p^m}$ where m is the least common multiple of n and n', one obtains a field containing all $\mathbb{F}_{p^n}$, $n \in \mathbb{N}$. Note that this field is, in fact, the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$.

Definition 2.6.19. *Let I be an arbitrary index set and $\mathscr{C}$ a category.*

(a) *We say that I is* preordered *by a binary relation $\leq$ on I if $\leq$ is reflexive and transitive, satisfying that for every $i, j \in I$, there exists some $k \in I$ such that $i \leq k$ and $j \leq k$.*

(b) *Let I be a preordered set. Assume that for every $i \in I$ an object $G_i \in \mathscr{C}$ is given, and for every pair $i, j \in I$ with $i \leq j$ there is a morphism $\varphi^i_j : G_i \to G_j$ satisfying that for $i \leq j \leq k$, where $i, j, k \in I$, we have that $\varphi^j_k \circ \varphi^i_j = \varphi^i_k$. Then the G_i's, together with the φ^i_j's, are called a* direct system in $\mathscr{C}$.

$$\begin{tikzcd}
G_i \arrow[dr, "\varphi^i_j"] \arrow[dd, "\varphi^i_k"'] & \\
\circlearrowleft & G_j \arrow[dl, "\varphi^j_k"] \\
G_k &
\end{tikzcd}$$

We write $(I, \leq, (G_i)_i, (\varphi^i_j)_{i,j})$ to specify the direct system, or simply $((G_i)_i, (\varphi^i_j)_{i,j})$ if I and $\leq$ are clear from the context.

(c) *Now let $(I, \leq, (G_i)_i, (\varphi^i_j)_{i,j})$ be a direct system. Another object $G \in \mathscr{C}$ (of the same type as the G_i's) with a set of morphisms $f_i : G_i \to G$ is called the* direct limit *of $(I, \leq, (G_i)_i, (\varphi^i_j)_{i,j})$, written $G = \varinjlim_{i \in I} G_i$ or simply $G = \varinjlim G_i$, if for every pair $i, j \in I$ satisfying $i \leq j$, we have $\varphi^i_j \circ f_i = f_j$, and the following* universal property *is satisfied:*

If $H \in \mathscr{C}$ is an object and the $h_i : G_i \to H$ are morphisms such that $h_j \circ \varphi^i_j = h_i$ for every pair $i, j \in I$ satisfying $i \leq j$, then there exists a unique morphism $\psi : G \to H$ such that $\psi \circ f_i = h_i$ for every i. We get the following commutative diagram:

$$\begin{tikzcd}
G_i \arrow[dr, "f_i"] \arrow[drr, bend left, "h_i"] \arrow[dd, "\varphi^i_j"'] & & \\
& G \arrow[r, dashed, "\exists!\psi"] & H \\
G_j \arrow[ur, "f_j"] \arrow[urr, bend right, "h_j"'] & &
\end{tikzcd}$$

Remarks 2.6.20.

(1) The universal property of the direct limit can be used to show that it is defined up to isomorphism if it exists.

(2) In Remarks 2.6.8 (c) we wrote $\mathcal{F}_p = \varinjlim \mathcal{F}(U)$, $U \in \mathbb{U}_{X,p}$. The preorder $\leq$ for this direct limit is defined by $U \leq V$ if, and only if, $V \subseteq U$.

The following proposition guarantees the existence of the direct limit in all situations we need:

Proposition 2.6.21. *[Eis95, pp. 705ff, Appendix 8] In both the category of Abelian groups and the category of rings, direct limits exist for every direct system.*

Let $((G_i)_i, (\varphi_j^i)_{i,j})$ be a direct system of Abelian groups respectively rings, and let $G := \varinjlim G_i$ and $g_i : G_i \to G$ be the canonical morphisms.

(1) *Then every $g \in G$ is of the form $g_i(x_i)$ for some $i \in I$ and $x_i \in G_i$.*

(2) *Two elements $g_i(a), g_j(b) \in G$, where $i, j \in I$ and $a \in G_i$, $b \in G_j$, are the same if, and only if, there exists a $k \in I$ satisfying $i \leq k$, $j \leq k$ such that $\varphi_k^i(a) = \varphi_k^j(b)$.*

Remark 2.6.22. Assume I is a preordered index set, and $((G_i)_i, (\varphi_j^i)_{i,j})$ and $((H_i)_i, (\psi_j^i)_{i,j})$ two direct systems whose direct limits exist. Moreover, let $f_i : G_i \to H_i$ be a morphism for every $i \in I$, satisfying $f_j \circ \varphi_j^i = \psi_j^i \circ f_i$ for every pair $i, j \in I$ where $i \leq j$. Denote by $g_i : G_i \to \varinjlim G_i$ and $h_i : H_i \to \varinjlim H_i$ the canonical maps. Then there exists a unique morphism $f : \varinjlim G_i \to \varinjlim H_i$ satisfying $f \circ g_i = h_i \circ f_i$ for every $i \in I$.

This basically shows that the direct limit is a functor from the category of direct systems over I whose direct limits do exist.

Now we will define the direct image and the inverse image of a sheaf. For the remainder of this subsection X and Y will always denote topological spaces.

Definition 2.6.23. *Let $f : X \to Y$ be a continuous map and $\mathcal{F}$ be a sheaf on X. Define the* direct image $f_*\mathcal{F}$ of $\mathcal{F}$ under f *to be the sheaf on Y given by $(f_*\mathcal{F})(U) = \mathcal{F}(f^{-1}(U))$, $U \in \mathbb{U}_Y$.*

Moreover, if $\mathcal{G}$ is another sheaf on X and $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, define $f_*\varphi : f_*\mathcal{F} \to f_*\mathcal{G}$ as the morphism of sheaves on Y given by $(f_*\varphi)(U) = \varphi(f^{-1}(U))$, $U \in \mathbb{U}_Y$.

Proof. It is obvious that $f_*\mathcal{F}$ is a sheaf and $f_*\varphi$ is a morphism of sheaves. □

Definition 2.6.24. *Let $f : X \to Y$ be a continuous map and $\mathcal{F}$ be a sheaf on Y. Define the* inverse image $f^{-1}(\mathcal{F})$ of $\mathcal{F}$ under f *as the sheaf associated with the presheaf $U \mapsto \varinjlim \mathcal{F}(V)$ on X; here the limit is taken over all $V \in \mathbb{U}_Y$ such that $f(U) \subseteq V$, and the preorder $\leq$ is defined by $V \leq V'$ if, and only if, $V' \subseteq V$.*

If $\mathcal{G}$ is another sheaf on Y and $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, then one can define a morphism of sheaves $f^{-1}\varphi : f^{-1}\mathcal{F} \to f^{-1}\mathcal{G}$ by using the universal property of $\varinjlim$.

Proof. It is a little harder than for f_*, but also not too difficult to see that $U \mapsto \varinjlim \mathcal{F}(V)$ gives a presheaf on X and that $f^{-1}\varphi$ is a morphism of sheaves. □

Remarks 2.6.25. Let $f : X \to Y$ be a continuous function.

(a) We have that f_* is a functor from the category of sheaves on X to the category of sheaves on Y.

(b) Let $\mathcal{F}$ be a sheaf on Y. For every $p \in X$, there is a natural map $(f_*\mathcal{F})_{f(p)} \to \mathcal{F}_p$.

(c) We have that f^{-1} is a functor from the category of sheaves on Y to the category of sheaves on X.

2.6.3 Morphisms of Sheaves

Let X be a topological space and $\mathscr{C}$ be one of the categories $\mathscr{A}b$ and $\mathscr{R}ing$. All sheaves considered here will be sheaves in $\mathscr{C}$ on X. The following proposition shows how local conditions naturally appear for sheaves:

Proposition 2.6.26. *[Har77, p. 63, Proposition 1.1] Let $f : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. Then f is an isomorphism if, and only if, $f_x : \mathcal{F}_x \to \mathcal{G}_x$ is an isomorphism for every $x \in X$.*

We continue by defining the kernel, image and cokernel of a morphism.

Definition 2.6.27. *Let $f : \mathcal{F} \to \mathcal{G}$ be a morphism of presheaves.*

(a) *The presheaf given by $U \mapsto \ker f(U)$ is called the* kernel presheaf *of f.*

(b) *The presheaf given by $U \mapsto \operatorname{im} f(U)$ is called the* image presheaf *of f. Note that if $\mathcal{F}$ and $\mathcal{G}$ are sheaves of rings, then the kernel presheaf is a sheaf of $\mathcal{F}$-modules.*

(c) *If the sheaves in question are sheaves of Abelian groups or modules, the presheaf given by $U \mapsto \mathcal{G}(U)/\operatorname{im} f(U)$ is called the* cokernel presheaf *of f.*

The restriction maps are the obvious ones.

Remark 2.6.28. If $\mathcal{F}$ and $\mathcal{G}$ are sheaves in the definition, then the kernel presheaf is also a sheaf. Note that in general the image presheaf and the cokernel presheaf are *no* sheaves.

Definition 2.6.29. *Let $f : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves.*

(a) *We define the* kernel $\ker f$ *of f to be the kernel presheaf of f.*

(b) *We define the* image $\operatorname{im} f$ *of f to be the sheaf associated with the image presheaf of f.*

(c) *If the sheaves in question are sheaves of Abelian groups or modules, we define the* cokernel $\operatorname{coker} f$ *of f to be the sheaf associated with the cokernel presheaf of f.*

These constructions can be used to define in which cases morphisms of sheaves are injective or surjective, and in which cases sequences of sheaves are exact.

Definition 2.6.30. *Let $f : \mathcal{F} \to \mathcal{G}$ a morphism of sheaves.*

(a) *We say that f is* injective *if* $\ker f = 0$*, i. e. if* $\ker f$ *is the zero sheaf.*

(b) *We say that f is* surjective *if* $\operatorname{im} f = \mathcal{G}$*.*

(c) *We say a sequence of sheaves*

$$\begin{tikzcd} \cdots \arrow[r] & \mathcal{F}^{(i-1)} \arrow[r, "\varphi^{(i-1)}"] & \mathcal{F}^{(i)} \arrow[r, "\varphi^{(i)}"] & \mathcal{F}^{(i+1)} \arrow[r] & \cdots \end{tikzcd}$$

is exact at i *if* $\ker \varphi^{(i)} = \operatorname{im} \varphi^{(i-1)}$*.*

Remark 2.6.31. [Har77, pp. 64f, ch. II, Definition] If $f : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves, then f is injective if, and only if, $f(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ is injective for every open set $U \subseteq X$. In general, for surjectivity only one direction holds: if $f(U)$ is surjective for every U, then f itself is surjective.

The following proposition shows that being exact is a local property. Note that being a local property can be defined in a much more general setting than for modules over rings by the use of sheaf theory. In particular it shows that our definitions of kernel, image, cokernel, injective and surjective have been chosen correctly.

Proposition 2.6.32. *[Har77, p. 66, ch. II, Exercise 1.2 (c)] A sequence of sheaves*

$$\begin{tikzcd} \cdots \arrow[r] & \mathcal{F}^{(i-1)} \arrow[r, "\varphi^{(i-1)}"] & \mathcal{F}^{(i)} \arrow[r, "\varphi^{(i)}"] & \mathcal{F}^{(i+1)} \arrow[r] & \cdots \end{tikzcd}$$

is exact at i if, and only, if the the induced exact sequences

$$\begin{tikzcd} \cdots \arrow[r] & \mathcal{F}_x^{(i-1)} \arrow[r, "\varphi_x^{(i-1)}"] & \mathcal{F}_x^{(i)} \arrow[r, "\varphi_x^{(i)}"] & \mathcal{F}_x^{(i+1)} \arrow[r] & \cdots \end{tikzcd}$$

are exact at i for every $x \in X$.

Corollary 2.6.33. *Let $f : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves.*

(a) *Then f is injective or surjective if, and only if, for every $x \in X$, the stalk f_x is injective or surjective, respectively.*

(b) *We have that f is an isomorphism if, and only if, it is both injective and surjective.*

Proof. The first claim directly follows from Proposition 2.6.32 and the second from Proposition 2.6.26 and (a). □

2.6.4 Ringed Spaces

Ringed space is an important concept. A special subclass of the class of ringed spaces consists of the schemes that we will define in Section 3.3.

Definition 2.6.34. *Let X be a topological space and $\mathcal{O}_X$ be a sheaf of rings on X. Then $(X, \mathcal{O}_X)$ is called a* ringed space*, and $\mathcal{O}_X$ is called the* structure sheaf *of $(X, \mathcal{O}_X)$. If no confusion can arise, we simply write X for $(X, \mathcal{O}_X)$. The elements of the topological space X are called* points*.*

A morphism of ringed spaces *is a pair $(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ consisting of a continuous map $f : X \to Y$ and a map of sheaves of rings $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$. Instead of $(f, f^{\#})$ we will simply write f if it is clear from the context.*

Remark 2.6.35. Note that if $f : X \to Y$ is a map of ringed spaces X and Y, then $f^{\#}$ induces a map on stalks

$$f_p^{\#} : \mathcal{O}_{Y,f(p)} \to \mathcal{O}_{X,p}, \qquad p \in X,$$

since by Remark 2.6.25 (b) there is a morphism $(f_*\mathcal{O}_X)_{f(p)} \to \mathcal{O}_{X,p}$.

2.6.5 Sheaves of Modules

Let $(X, \mathcal{O})$ be a ringed space. We have defined (see Definition 2.6.5) what a *sheaf of $\mathcal{O}$-modules* or an *$\mathcal{O}$-module* is. In this last subsection of the chapter we want to take a closer look at $\mathcal{O}$-modules. We begin by defining what a morphism of $\mathcal{O}$-modules is and what a sub-$\mathcal{O}$-module is.

Definition 2.6.36. *Let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}$-modules. Then a morphism of sheaves $f : \mathcal{F} \to \mathcal{G}$ is a* morphism of $\mathcal{O}$-modules *or an $\mathcal{O}$*-morphism *if $f(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ is an $\mathcal{O}(U)$-linear map for every $U \in \mathbb{U}_X$. The set of $\mathcal{O}$-morphisms from $\mathcal{F}$ to $\mathcal{G}$ is denoted by* $\mathrm{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$ *or shorter* $\mathrm{Hom}(\mathcal{F}, \mathcal{G})$ *if no confusion can arise.*

If $\mathcal{G}$ is a subsheaf of $\mathcal{F}$ and both $\mathcal{F}$ and $\mathcal{G}$ are $\mathcal{O}$-modules, then $\mathcal{G}$ is called a sub-$\mathcal{O}$-module *of $\mathcal{F}$.*

Remarks 2.6.37. Let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}$-modules.

(1) If $f : \mathcal{F} \to \mathcal{G}$ is an $\mathcal{O}$-morphism, then the kernel $\ker f$, the image $\operatorname{im} f$ and the cokernel $\operatorname{coker} f$ are again $\mathcal{O}$-modules.

(2) If $\mathcal{G}$ is a sub-$\mathcal{O}$-module of $\mathcal{F}$, then $\mathcal{F}/\mathcal{G}$ is again an $\mathcal{O}$-module.

(3) The arbitrary direct sum or direct product of $\mathcal{O}$-modules is again an $\mathcal{O}$-module.

(4) If $U \in \mathbb{U}_X$ is an open subset, then $\mathcal{G}|_U$ is an $\mathcal{O}|_U$-module.

Proof. The claims (1), (2) and (3) are clear. For (4) recall that the trace topology of an open subset is exactly the set of open sets that is contained in that subset. □

A powerful construction for $\mathcal{O}$-modules is the tensor product.

Definition 2.6.38. *Let $\mathcal{F}$ and $\mathcal{G}$ be two $\mathcal{O}$-modules. Let the* tensor product of $\mathcal{F}$ and $\mathcal{G}$, *denoted by $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G}$, be the sheaf associated to the presheaf*

$$U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U)$$

with the obvious restriction maps.

Proof. It is easy to see that this assignment gives a presheaf. □

As for modules over rings, the notion of being free is important for $\mathcal{O}$-modules. While for modules over rings the notion of a projective module turns out to be being free locally, for $\mathcal{O}$-modules this can be reached more easily.

Definition 2.6.39. *Let $\mathcal{F}$ be an $\mathcal{O}$-module.*

(a) *If $\mathcal{F}$ is isomorphic to a direct sum of copies of $\mathcal{O}$, then $\mathcal{F}$ is called* free. *The* rank *of $\mathcal{F}$ is the number of copies of $\mathcal{O}$ which were required.*

(b) *If there is an open cover U_i of X such that $\mathcal{F}|_{U_i}$ is a free $\mathcal{O}|_{U_i}$-module, then $\mathcal{F}$ is called* locally free. *The* rank of $\mathcal{F}$ on such an U_i *is defined to be the rank of $\mathcal{F}|_{U_i}$ as an $\mathcal{O}|_{U_i}$-module.*

If the rank is the same for every U_i, then one says $\mathcal{F}$ is locally free of rank n, *where n is the rank on one (and hence all) U_i.*

(c) *If $\mathcal{F}$ is a locally free sheaf of rank one, then $\mathcal{F}$ is called an* invertible sheaf.

Remark 2.6.40. Define the rank of a locally free $\mathcal{O}$-module at a point to be the rank of the module restricted to an open neighborhood of that point on which it is free. Then the rank is a continuous function $X \to \mathbb{N} \cup \{\infty\}$, where $\mathbb{N} \cup \{\infty\}$ has the discrete topology. (This means that it is locally constant.) Thus, if X is connected, the rank is constant.

Proof. Let $x \in X$ be a point and $U_1, U_2 \in \mathbb{U}_{X,p}$ two open sets such that $\mathcal{F}|_{U_i}$ is a free $\mathcal{O}|_{U_i}$-module for both i. Let $U := U_1 \cap U_2 \in \mathbb{U}_{X,p}$, then $\mathcal{F}|_{U_i}(U) = \mathcal{F}(U)$ and $\mathcal{O}|_{U_i}(U) = \mathcal{O}(U)$ for both i and, therefore, the rank of $\mathcal{F}|_{U_i}(U)$ as an $\mathcal{O}|_{U_i}(U)$-module does not depend on i. Hence, the function rank : $X \to \mathbb{N}$ is well-defined and, since it is locally constant, it is also continuous. □

As for modules over rings, one can define the tensor algebra, exterior algebra and exterior power for $\mathcal{O}$-modules. This will be important for defining Kähler differentials for schemes.

Definition 2.6.41. *[Har77, p. 127, ch. II, Exercise 5.16] For an $\mathcal{O}$-module $\mathcal{F}$ define the* tensor algebra $T_{\mathcal{O}}(\mathcal{F})$, *the* exterior algebra $\bigwedge_{\mathcal{O}} \mathcal{F}$ *and the* n-th exterior power $\bigwedge_{\mathcal{O}}^n \mathcal{F}$ *the same way as for modules over rings (see Definition 2.1.37).*

Remark 2.6.42. [Har77, p. 127, ch. II, Exercise 5.16(a)] If $\mathcal{F}$ is a locally free $\mathcal{O}$-module of rank n, the r-th component of $T_{\mathcal{O}}(\mathcal{F})$ is a locally free $\mathcal{O}$-module of rank n^r and $\bigwedge_{\mathcal{O}}^r \mathcal{F}$ is a locally free $\mathcal{O}$-module of rank $\binom{n}{r}$.

If one takes a look at the set of $\mathcal{O}$-module morphisms between two $\mathcal{O}$-modules, this set naturally has itself the structure of an $\mathcal{O}$-module.

Definition 2.6.43. *[Har77, p. 109, ch. II and p. 67, ch. II, Exercise 1.15] Let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}$-modules. The presheaf*

$$U \mapsto \operatorname{Hom}_{\mathcal{O}|_U}(\mathcal{F}|_U, \mathcal{G}|_U)$$

is, in fact, a sheaf and is denoted by $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$ and called the sheaf $\mathcal{H}om$.

If $\mathcal{F}$ is any $\mathcal{O}$-module, define its dual $\mathcal{O}$-module, *denoted by $\mathcal{F}^{\curlyvee}$, to be the $\mathcal{O}$-module $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{O})$.*

We next state two results for locally free $\mathcal{O}$-modules and invertible $\mathcal{O}$-modules.

Proposition 2.6.44. *[Har77, p. 123, Exercise 5.1] Let $\mathcal{F}$ be a locally free $\mathcal{O}$-module of finite rank n.*

(1) *We have $(\mathcal{F}^{\curlyvee})^{\curlyvee} \cong \mathcal{F}$.*

(2) *If $\mathcal{G}$ is any other $\mathcal{O}$-module, then*

$$\mathcal{H}om_{\mathcal{O}}(\mathcal{F},\mathcal{G}) \cong \mathcal{F}^{\curlyvee} \otimes_{\mathcal{O}} \mathcal{G}.$$

(3) *If $\mathcal{G}$ and $\mathcal{H}$ are $\mathcal{O}$-modules, then*

$$\operatorname{Hom}_{\mathcal{O}}(\mathcal{F} \otimes \mathcal{G}, \mathcal{H}) \cong \operatorname{Hom}_{\mathcal{O}}(\mathcal{G}, \mathcal{H}om_{\mathcal{O}}(\mathcal{F},\mathcal{H})).$$

Proposition 2.6.45. *[Har77, p. 143, Proposition 6.12] Let $\mathcal{F}$ and $\mathcal{G}$ be invertible sheaves on $(X, \mathcal{O})$.*

(1) *Then $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G}$ is again an invertible sheaf on $(X, \mathcal{O})$.*

(2) *We have that $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{F}^{\curlyvee} \cong \mathcal{O}$.*

By the latter proposition the following definition is well-defined:

Definition 2.6.46. *Let* $\operatorname{Pic} X$ *denote the* Picard group *of the ringed space X, defined as the group of isomorphism classes of invertible sheaves on X, the group operation being tensoring of representatives.*

We will see that the Picard group of special ringed spaces corresponds to the Picard group of rings.

Definition 2.6.47. *An $\mathcal{O}$-module $\mathcal{I}$ is called an* ideal sheaf *if it is a sub-$\mathcal{O}$-module of $\mathcal{O}$.*

Remark 2.6.48. This means that $\mathcal{I}(U)$ is an ideal in $\mathcal{O}(U)$ for every $U \in \mathbb{U}_X$.

Now let $(Y, \mathcal{O}_Y)$ be another ringed space and $f : (X, \mathcal{O}) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces given by a continuous map $f : X \to Y$ and a morphism of sheaves $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}$.

Remark 2.6.49. There exists a natural morphism $f^{-1}\mathcal{O}_Y \to \mathcal{O}$:

Recall that $f^{-1}\mathcal{O}_Y$ is the presheaf associated with the sheaf

$$U \mapsto \varinjlim_{V \in \mathbb{U}_{Y,f(U)}} \mathcal{O}_Y(V),$$

where $U \in \mathbb{U}_X$. For every $V \in \mathbb{U}_{Y,f(U)}$, we have a natural map

$$\begin{tikzcd} \mathcal{O}_Y(V) \arrow[r, "f^{\#}(V)"] & (f_*\mathcal{O})(V) \arrow[r, equal] & \mathcal{O}(f^{-1}(V)) \arrow[r, "\bullet|_U"] & \mathcal{O}(U), \end{tikzcd}$$

since $U \subseteq f^{-1}(V)$. Now since these maps commute with the restrictions on Y, we get a unique morphism

$$\varinjlim_{V \in \mathbb{U}_{Y,f(U)}} \mathcal{O}_Y(V) \to \mathcal{O}(U)$$

(see Definition 2.6.19). This map clearly defines a morphism of presheaves and, therefore, there exists a unique morphism of sheaves

$$f^{-1}\mathcal{O}_Y \to \mathcal{O}.$$

Definition 2.6.50.

(a) *Let $\mathcal{F}$ be an $\mathcal{O}$-module. Then $f_*\mathcal{F}$ is an $f_*\mathcal{O}$-module and, by the map $f^\#$, also an $\mathcal{O}_Y$-module. We call $f_*\mathcal{F}$ the* direct image *of $\mathcal{F}$ under the morphism f.*

(b) *Let $\mathcal{G}$ be an $\mathcal{O}_Y$-module. Then $f^{-1}\mathcal{G}$ is an $f^{-1}\mathcal{O}_Y$-module. By the morphism $f^{-1}\mathcal{O}_Y \to \mathcal{O}$ of sheaves (see Remark 2.6.49) we define $f^*\mathcal{G}$ to be*

$$f^{-1}\mathcal{G} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}$$

and, hence, $f^*\mathcal{G}$ is an $\mathcal{O}$-module called the inverse image *of $\mathcal{G}$ under the morphism f.*

Chapter 3

Algebraic Geometry

In this chapter we want to repeat all necessary definitions and results from algebraic geometry, including results from the Theory of Schemes, about curves over fields and rings and about representable group functors and group schemes.

3.1 Basic Affine and Projective Geometry

In this section we want to give basic definitions, like the affine space $\mathbb{A}^n(R)$ and projective space $\mathbb{P}^n(R)$ over a ring R, the notion of being irreducible and what a variety is. Moreover, we want to state fundamental results on $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$, for example their functoriality, the Zariski topology, relations of special hyperplanes, projective closure of varieties etc. We begin by introducing affine and projective space:

Definition 3.1.1. *Let R be a ring. The* affine n-space *over R, denoted by $\mathbb{A}^n(R)$, is the set of n-tuples of elements of R: hence, $\mathbb{A}^n(R) = R^n$.*

Definition 3.1.2. *Let R be a ring. The* projective n-space *over R, denoted by $\mathbb{P}^n(R)$, is the set of $(n+1)$-tuples of elements of R which are primitive over R, where two such tuples are identified if they differ by multiplication by a unit of R. Thus*

$$\mathbb{P}^n(R) = \{(a_0, \dots, a_n) \in R^{n+1} \mid \langle a_0, \dots, a_n \rangle = R\}/\sim,$$

where

$$(a_i)_i \sim (b_i)_i \iff \exists u \in R^* : a_i = ub_i \text{ for } i = 0, \dots, n.$$

We will write $(a_0 : \dots : a_n)$ for the equivalence class $[(a_0, \dots, a_n)]_\sim$.

Note that we will call the elements of $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$ *points.*

Remarks 3.1.3.

(a) It is easy to see that if R is a field, then this definition of the projective n-space is the same as the usual one (see [Har77, pp. 8f, ch. I]), since then a $(n+1)$-tuple is primitive if, and only if, at least one entry is non-zero.

(b) Note that $(a_0, \dots, a_n) \in R^{n+1}$ generates a free R-module which is a direct summand of R^{n+1} if, and only if, $(a_0, \dots, a_n)$ is primitive over R.

(The proof of this can be found in the proofs of Lemma 2.4.20 and Lemma 2.4.21.)

(c) Note that if $(a_i)_i$ and $(b_i)_i$ are two primitive tuples, then $\lambda(a_i)_i = (b_i)_i$ for any $\lambda \in R$ implies $(a_i)_i \sim (b_i)_i$.

(On the contrary, assume $\lambda \notin R^*$, which means $\langle \lambda \rangle \subsetneqq R$, and therefore $\lambda(a_i)_i = (\lambda a_i)_i$ cannot be primitive.)

The following lemma implies that $\mathbb{A}^n(\bullet)$ and $\mathbb{P}^n(\bullet)$ are functors from $\mathscr{R}ing$ to $\mathscr{S}et$:

Lemma 3.1.4. *Let $\varphi : R \to S$ be a morphism of rings. Then φ induces natural maps $\mathbb{A}^n(R) \to \mathbb{A}^n(S)$ and $\mathbb{P}^n(R) \to \mathbb{P}^n(S)$, defined by applying φ to the components of the tuples.*

Proof. This is clear for $\mathbb{A}^n(R) \to \mathbb{A}^n(S)$. If $(a_0, \dots, a_n) \in R^{n+1}$ is primitive over R, then $1 = \sum_{i=0}^n \lambda_i a_i$ for some $\lambda \in R$ and, hence, $1 = \varphi(1) = \varphi(\sum \lambda_i a_i) = \sum \varphi(\lambda_i)\varphi(a_i)$ and, therefore, $(\varphi(a_0), \dots, \varphi(a_n)) \in S^{n+1}$ is primitive over S. Since a morphism of rings maps units onto units, two primitive tuples $a, b \in R^{n+1}$ satisfying $a \sim b$ are mapped onto tuples $a', b' \in S^{n+1}$ satisfying $a' \sim b'$. □

Next we want to give a criterion when two points in projective space are the same:

Lemma 3.1.5. *Let R be a ring and $a = (a_0 : \dots : a_n), b = (b_0 : \dots : b_n) \in \mathbb{P}^n(R)$. Then $a = b$ if and only if $a_i b_j = a_j b_i$ for all $0 \leq i < j \leq n$.*

Proof. Assume $a = b$, i. e. there is a $u \in R^*$ such that $a_i = ub_i$, $0 \leq i \leq n$. Then clearly $a_i b_j = u a_i a_j = a_j b_i$ for all $0 \leq i < j \leq n$.

Conversely, let $a_i b_j = a_j b_i$, $0 \leq i < j \leq n$. Clearly this holds for every $0 \leq i, j \leq n$. We reduce to the case that R is local by localizing at every maximal ideal $\mathfrak{m}$ of R and using Corollary 2.2.10. But if R is local, a collections of elements if primitive if and only if one is a unit. Assume a_i is a unit. Then $b_j = a_j b_i a_i^{-1}$ for every j and, therefore, $(b_j)_j = \lambda(a_j)_j$ for $\lambda = b_i a_i^{-1}$. But, following the above remarks, we then have $\lambda \in R^*$ and, thus, $a = b$. □

We want to define a topology on $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$ for a certain class of rings R. In the case $R = \mathbb{R}$ or $R = \mathbb{C}$ one has the classical topologies from analysis, but we are not interested in these. The topology we will define is much coarser than the classical topology, and it can be defined for every domain R.

Remark 3.1.6. Let R be a ring and $f \in R[x_0, \dots, x_n]$ a homogenous polynomial. If $a = (a_0 : \dots : a_n) \in \mathbb{P}^n(R)$, then $f(a) := f(a_0, \dots, a_n) \overset{?}{=} 0$ is well-defined, as $f(\lambda a_0, \dots, \lambda a_n) = \lambda^d f(a_0, \dots, a_n)$, where d is the degree of f.

Definition 3.1.7. *Let R be a ring and $n \in \mathbb{N}_{>0}$.*

(a) *Let $\mathfrak{a} \subseteq R[x_1, \dots, x_n]$ be an ideal. The* vanishing set *of $\mathfrak{a}$ over R is defined as*

$$V_R(\mathfrak{a}) = \{a \in \mathbb{A}^n(R) \mid f(a) = 0 \textit{ for all } f \in \mathfrak{a}\}.$$

If $f_1, \dots, f_m \in R[x_1, \dots, x_n]$ are polynomials, we also write $V_R(f_1, \dots, f_m)$ instead of $V_R(\langle f_1, \dots, f_m \rangle)$.

(b) *Let $\mathfrak{a} \subseteq R[x_0, \ldots, x_n]$ be a homogenous ideal. The* vanishing set *of $\mathfrak{a}$ over R is defined as*

$$V_R(\mathfrak{a}) = \{a \in \mathbb{P}^n(R) \mid f(a) = 0 \textit{ for all homogenous } f \in \mathfrak{a}\}.$$

If $f_1, \ldots, f_m \in R[x_0, \ldots, x_n]$ are homogenous polynomials, instead of writing $V_R(\langle f_1, \ldots, f_m\rangle)$ we also write $V_R(f_1, \ldots, f_m)$.

(c) *Sets of the form $V_R(\mathfrak{a})$ in (a) and (b) are called* algebraic (sub-)sets.

Proposition 3.1.8. *Let R be a domain and $n \in \mathbb{N}_{>0}$.*

(a) *If one takes the algebraic subsets of $\mathbb{A}^n(R)$ as the closed sets, one obtains a topology on $\mathbb{A}^n(R)$.*

(b) *If one takes the algebraic subsets of $\mathbb{P}^n(R)$ as the closed sets, one obtains a topology on $\mathbb{P}^n(R)$.*

Definition 3.1.9. *The topologies defined in the last proposition are called the* Zariski topologies *on $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$.*

If from now on we speak of a topology on $\mathbb{A}^n(R)$ or $\mathbb{P}^n(R)$, we always mean the Zariski topology. Next we want to characterize the connection between algebraic sets and ideals.

Definition 3.1.10. *Let R be a ring and $n \in \mathbb{N}_{>0}$.*

(a) *For any subset $V \subseteq \mathbb{A}^n(R)$ define*

$$I_R(V) := \{f \in R[x_1, \ldots, x_n] \mid f(x) = 0 \textit{ for all } x \in V\}.$$

(b) *For any subset $V \subseteq \mathbb{P}^n(R)$ define*

$$I_R(V) := \Big\langle \{f \in R[x_0, \ldots, x_n]^h \mid f(x) = 0 \textit{ for all } x \in V\} \Big\rangle_{R[x_0,\ldots,x_n]}.$$

Proposition 3.1.11. *Let R be a ring and $n \in \mathbb{N}_{>0}$.*

(a) (1) *For any $V \subseteq \mathbb{A}^n(R)$, the set $I_R(V)$ is an ideal in $R[x_1, \ldots, x_n]$.*

(2) *If $V \subseteq \mathbb{A}^n(R)$, then $V \subseteq V_R(I_R(V))$.*

(3) *If $I \subseteq R[x_1, \ldots, x_n]$, then $I \subseteq I_R(V_R(I))$.*

(4) *For $V \subseteq \mathbb{A}^n(R)$ we have $V = V_R(I_R(V))$ if and only if V is an algebraic set.*

(b) (1) *For any $V \subseteq \mathbb{P}^n(R)$, the set $I_R(V)$ is a homogenous ideal in $R[x_0, \ldots, x_n]$.*

(2) *If $V \subseteq \mathbb{P}^n(R)$, then $V \subseteq V_R(I_R(V))$.*

(3) *If $I \subseteq R[x_0, \ldots, x_n]^h$, then $I \subseteq I_R(V_R(I))$.*

(4) *For $V \subseteq \mathbb{P}^n(R)$ we have $V = V_R(I_R(V))$ if and only if V is an algebraic set.*

For algebraically closed fields there is a very beautiful characterization of algebraic sets, given by Hilbert's Nullstellensatz.

Theorem 3.1.12 (Hilbert's Nullstellensatz). *[Eis95, p. 34, Theorem 1.6] Let $\mathbb{F}$ be an algebraically closed field and $\mathfrak{a}$ an ideal in $\mathbb{F}[x_1, \dots, x_n]$. Then*

$$\sqrt{\mathfrak{a}} = I_{\mathbb{F}}(V_{\mathbb{F}}(\mathfrak{a})).$$

Hence, if $f \in \mathbb{F}[x_1, \dots, x_n]$ satisfies $V_{\mathbb{F}}(\mathfrak{a}) \subseteq V_{\mathbb{F}}(f)$, then $f \in \sqrt{\mathfrak{a}}$.

Corollary 3.1.13 (Projective Nullstellensatz). *Let $\mathbb{F}$ be an algebraically closed field and $\mathfrak{a}$ a homogenous ideal in $\mathbb{F}[x_0, \dots, x_n]$, and let $f \in \mathbb{F}[x_0, \dots, x_n]^h$ satisfy $V_{\mathbb{F}}(\mathfrak{a}) \subseteq V_{\mathbb{F}}(f)$*

(a) *If $\mathfrak{a}$ does not contain $\mathbb{F}[x_0, \dots, x_n]_+$, then $f \in \sqrt{\mathfrak{a}}$. Thus, in this case $\sqrt{\mathfrak{a}} = I_{\mathbb{F}}(V_{\mathbb{F}}(\mathfrak{a}))$.*

(b) *If $\mathfrak{a}$ contains $\mathbb{F}[x_0, \dots, x_n]_+$, then $I_{\mathbb{F}}(V_{\mathbb{F}}(\mathfrak{a})) = \mathbb{F}[x_0, \dots, x_n]$.*

Therefore, if $\mathfrak{a} = I_{\mathbb{F}}(V_{\mathbb{F}}(\mathfrak{a}))$, then $f \in \mathfrak{a}$.

Proof.

(a) Treat $\mathfrak{a}$ as an inhomogenous ideal and f as an inhomogenous polynomial in $\mathbb{F}[x_1, \dots, x_{n+1}]$; then in affine space, $V_{\mathbb{F}}^{aff}(\mathfrak{a}) \subseteq V_{\mathbb{F}}^{aff}(f)$, since

$$V_{\mathbb{F}}^{aff}(\mathfrak{a}) = \{(x_1, \dots, x_{n+1}) \in \mathbb{F}^{n+1} \mid (x_1 : \dots : x_{n+1}) \in V_{\mathbb{F}}^{proj}(\mathfrak{a})\} \cup \{0\}$$

(here we use that $\mathbb{F}[x_0, \dots, x_n]_+ \not\subseteq \mathfrak{a}$), and the same for f. Therefore, Hilbert's Nullstellensatz 3.1.12 gives $f \in \sqrt{\mathfrak{a}}$.

(b) Now assume $\mathbb{F}[x_0, \dots, x_n]_+ \subseteq \mathfrak{a}$. If for some $a \in \mathbb{F}^{n+1}$ we have $g(a) = 0$ for all $g \in \mathfrak{a}$, then $a = 0$; therefore $V_{\mathbb{F}}^{proj}(\mathfrak{a}) = \emptyset$ and, hence, $I_{\mathbb{F}}(V_{\mathbb{F}}(\mathfrak{a})) = I_{\mathbb{F}}(\emptyset) = \mathbb{F}[x_0, \dots, x_n]$. □

Corollary 3.1.14. *[Eis95, p. 36, Corollary 1.10] If $\mathbb{F}$ is an algebraically closed field, the maps $I_{\mathbb{F}}$ and $V_{\mathbb{F}}$ give a one-to-one correspondence between algebraic subsets of $\mathbb{A}^n(\mathbb{F})$ and radical ideals in $\mathbb{F}[x_1, \dots, x_n]$. In particular we have $V_{\mathbb{F}}(\mathfrak{a}) = \emptyset$ for an ideal $\mathfrak{a} \subseteq \mathbb{F}[x_1, \dots, x_n]$ if and only if $\mathfrak{a} = \mathbb{F}[x_1, \dots, x_n]$.*

Moreover, the Nullstellensatz allows us to characterize the maximal ideals of $\mathbb{F}[x_1, \dots, x_n]$, since they correspond to minimal algebraic sets in $\mathbb{A}^n(\mathbb{F})$, which are points.

Corollary 3.1.15. *[Eis95, p. 35, Corollary 1.9] Let $\mathbb{F}$ be an algebraically closed field. Then the maximal ideals of $\mathbb{F}[x_1, \dots, x_n]$ have the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ for $(a_1, \dots, a_n) \in \mathbb{F}^n$.*

Next we want to introduce the notion of being irreducible, and give a characterization of when an algebraic subset is irreducible.

Definition 3.1.16. *A topological space X is called* irreducible *if $X = A \cup B$ with closed sets A and B implies $A = X$ or $B = X$. A subset of X is called* irreducible *if it is irreducible as a topological space with the induced trace topology.*

Note that in topological spaces which are Hausdorff the only irreducible sets are sets consisting of at most one point.

Proposition 3.1.17. *Let R be a domain and X be either $\mathbb{A}^n(R)$ or $\mathbb{P}^n(R)$. Let Z be a closed subset of X. If $I_R(Z)$ is prime, then Z is irreducible. If Z is irreducible and R is an algebraically closed field, then $I_{\mathbb{F}}(Z)$ is prime.*

Proof. Note that to check whether a homogenous ideal is prime, it is enough to check the homogenous elements (see Proposition 2.3.4).

First let $I_R(Z)$ be prime, and let U, V be closed sets such that $Z = U \cup V$. Then $I_R(U)I_R(V) \subseteq I_R(U \cup V) = I_R(Z)$. By Lemma 2.1.20 either $I_R(U) \subseteq I_R(Z)$ or $I_R(V) \subseteq I_R(Z)$. Assuming $I_R(U) \subseteq I_R(Z)$, we get $Z \supseteq U = V_R(I_R(U)) \supseteq V_R(I_R(Z)) = Z$, i.e. $Z = U$.

For the other implication, assume Z is irreducible and that $R = \mathbb{F}$ is an algebraically closed field. Let $fg \in I_{\mathbb{F}}(Z)$. Then $Z = V_{\mathbb{F}}(I_{\mathbb{F}}(Z)) \subseteq V_{\mathbb{F}}(fg) = V_{\mathbb{F}}(f) \cup V_{\mathbb{F}}(g)$, and as Z is irreducible, either $Z \subseteq V_{\mathbb{F}}(f)$ or $Z \subseteq V_{\mathbb{F}}(g)$. Assuming $Z \subseteq V_{\mathbb{F}}(f)$, by Hilbert's Nullstellensatz (Theorem 3.1.12 or Corollary 3.1.13), we get $f \in I_{\mathbb{F}}(Z)$. □

Now we come to define the notion of a variety.

Definition 3.1.18. *Let $\mathbb{F}$ be an algebraically closed field and X be either $\mathbb{A}^n(\mathbb{F})$ or $\mathbb{P}^n(\mathbb{F})$. An algebraic set $V \subseteq X$ is called an* affine, *or* projective variety *if $I_{\mathbb{F}}(V)$ is prime.*

In the rest of this section we will mean either an affine or a projective variety if we simply speak of a variety.

Definition 3.1.19. *Let R be any ring and X either $\mathbb{A}^n(R)$ or $\mathbb{P}^n(R)$. Then an algebraic set $V \subseteq X$ is called a* variety *if for every maximal ideal $\mathfrak{m}$ of R, the image of V under the map induced from X to $\mathbb{A}^n(\overline{R/\mathfrak{m}})$ or $\mathbb{P}^n(\overline{R/\mathfrak{m}})$ by $R \to \overline{R/\mathfrak{m}}$ is the intersection of a variety with the image of the induced map. Here $\overline{R/\mathfrak{m}}$ is the algebraic closure of $R/\mathfrak{m}$.*

Now we will introduce hyperplanes and lines.

Definition 3.1.20. *Let $\mathbb{F}$ be a field and $n \in \mathbb{N}_{>0}$. A* hyperplane *H in $\mathbb{P}^n(\mathbb{F})$ is the complement of the zero set of a homogenous linear polynomial of degree one, i. e. $H = \mathbb{P}^n(\mathbb{F}) \setminus V_{\mathbb{F}}(f)$ with $f = \sum_{i=0}^n a_i x_i$, $(a_0, \dots, a_n) \in \mathbb{F}^{n+1} \setminus \{0\}$. If $n = 2$, then a hyperplane is also called a* line.

For $i = 0, \dots, n$ let H_i be the hyperplane defined by x_i, i. e. $H_i = \mathbb{P}^n(\mathbb{F}) \setminus V_{\mathbb{F}}(x_i)$.

Proposition 3.1.21. *Let $\mathbb{F}$ be a field and $n = 2$. Let $P = (x_1 : y_1 : z_1), Q = (x_2 : y_2 : z_2) \in \mathbb{P}^2(\mathbb{F})$ with $P \neq Q$. Then the line through P and Q is given by the equation*

$$(y_1 z_2 - y_2 z_1)x + (z_1 x_2 - z_2 x_1)y + (x_1 y_2 - x_2 y_1)z = 0.$$

Proof. Since $P \neq Q$, by Lemma 3.1.5 the equation defines a line in $\mathbb{P}^2(\mathbb{F})$. Moreover plugging in (x_1, y_1, z_1) and (x_2, y_2, z_2) shows that P and Q satisfy this equation. □

Proposition 3.1.22. *[Har77, p. 10, ch. I, Proposition 2.2] Let $\mathbb{F}$ be a field and $n \in \mathbb{N}_{>0}$. Then there is a natural identification of $H_i \subseteq \mathbb{P}^n(\mathbb{F})$ with $\mathbb{A}^n(\mathbb{F})$, given by*

$$(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) \mapsto (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n).$$

Moreover:

(a) *We have $\bigcup_{i=0}^n H_i = \mathbb{P}^n(\mathbb{F})$, i. e. $\mathbb{P}^n(\mathbb{F})$ can be covered with $n+1$ hyperplanes.*

(b) *The induced topology on $\mathbb{A}^n(\mathbb{F})$ from the Zariski topology on $\mathbb{P}^n(\mathbb{F})$ is again the Zariski topology on $\mathbb{A}^n(\mathbb{F})$.*

There is a close connection between varieties in projective space and varieties in affine space which follows from this proposition. For this we need some properties of irreducible spaces:

Lemma 3.1.23. *Assume Z is an irreducible closed set in a topological space X, and U an open set meeting Z. Then the following holds:*

(1) *The intersection $Z \cap U$ is dense in Z; and*

(2) *The intersection $Z \cap U$ is an irreducible closed subset in U.*

Proof.

(1) Assume $Z_1 = \overline{Z \cap U} \subsetneqq Z$, and let $Z_2 = Z \setminus (Z \cap U) = Z \setminus U$; then Z_1 and Z_2 are closed, and $Z_i \neq Z$ for both i. But $Z = Z_1 \cup Z_2$ and, thus, Z is reducible.

(2) That $Z \cap U$ is closed in U is clear.

Assume $Z \cap U = (Z_1 \cap U) \cup (Z_2 \cap U)$, where Z_1, Z_2 are closed in X and $\emptyset \neq Z_i \cap U \subsetneqq Z \cap U$ for $i = 1, 2$. (I. e. $Z \cap U$ is a reducible closed subset in U.)

Let $\hat{Z}_i := (\complement U \cup Z_i) \cap Z$. Then $\hat{Z}_i$ is closed, since $\complement U$, Z_i and Z are closed, and $\hat{Z}_i \subseteq Z$, $i = 1, 2$. Further

$$\begin{aligned} \hat{Z}_1 \cup \hat{Z}_2 &= (\complement U \cup Z_1 \cup Z_2) \cap Z = (\complement U \cup ((Z_1 \cup Z_2) \cap U)) \cap Z \\ &= (\complement U \cup (Z \cap U)) \cap Z = (\complement U \cup Z) \cap Z = Z. \end{aligned}$$

But, as $\hat{Z}_i \cap U = Z_i \cap U \subsetneqq Z \cap U$, we get $\hat{Z}_i \cap Z \subsetneqq Z$, $i = 1, 2$ and, thus, Z is reducible. □

Proposition 3.1.24. *Let $\mathbb{F}$ be an algebraically closed field and $n \in \mathbb{N}_{>0}$.*

(a) *If V is an algebraic set in $\mathbb{A}^n(\mathbb{F})$, for every i there exists a unique algebraic set V' in $\mathbb{P}^n(\mathbb{F})$ such that V is $V' \cap H_i$ with the identification $H_i = \mathbb{A}^n(\mathbb{F})$ from the last proposition. This set V' is called the* projective closure *of V.*

(b) *If V is an algebraic set in $\mathbb{P}^n(\mathbb{F})$ and $0 \leq i \leq n$, then $V \cap H_i$ is an algebraic set in $\mathbb{A}^n(\mathbb{F})$. Moreover, if $V \cap H_i \neq \emptyset$ and V is a variety, the projective closure of $V \cap H_i$ is V.*

(c) *The projective closure of a variety is again a variety, and a variety in $\mathbb{P}^n(\mathbb{F})$ intersected with H_i is again a variety in $\mathbb{A}^n(\mathbb{F})$.*

Proof. By using part (b) of the previous proposition it is enough to prove this proposition as follows: let X be an irreducible topological space and $Y \subseteq X$ a irreducible subspace, where Y is X-open.

(a) If $H \subseteq Y$ is a Y-closed set and $H' = \overline{H}^X$ is the closure of H in X, then $H = \overline{H}^Y = \overline{H}^X \cap Y = H' \cap Y$.

(b) If $H \subseteq X$ is X-closed, clearly $H \cap Y$ is Y-closed and $\overline{H \cap Y}^X \subseteq \overline{H}^X = H$. Now assume additionally that H is irreducible. Then $Y \cap H$ is H-dense by part (b) of the previous lemma, where H has the trace topology from X and, therefore, $H \subseteq \overline{Y \cap H}^X$.

(c) If $H \subseteq Y$ is irreducible, clearly so is $\overline{H}^X$. And if $H \subseteq X$ is irreducible, so is $H \cap Y$ by part (b) of the previous lemma. □

Corollary 3.1.25. *Let $\mathbb{F}$ be an algebraically closed field. Any projective variety over $\mathbb{F}$ can be covered by a finite number of affine varieties.*

Finally we want to use another property which $\mathbb{P}^n(R)$ and $\mathbb{A}^n(R)$ have for certain domains R.

Definition 3.1.26. *Let X be a topological space.*

(a) *We call X* Noetherian *if every ascending chain of open subsets eventually becomes stationary.*

(b) *Let $U \subseteq X$ be a closed subset. An irreducible closed subset $C \subseteq U$ is called an* irreducible component *of U if for every irreducible closed subset $C' \subseteq U$ such that $C \subseteq C'$, we already have $C = C'$.*

Proposition 3.1.27. *[Har77, p. 5, ch. I, Proposition 1.5] In a Noetherian topological space every closed subset can be written as the finite union of pairwise distinct of irreducible components of itself. This decomposition is unique.*

Corollary 3.1.28. *Let R be a Noetherian domain. Then every algebraic set in $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$ can be uniquely written as the finite union of its irreducible components.*

Proof. By the Hilbert Basis Theorem (Proposition 2.0.6 (b)), $R[x_1, \dots, x_n]$ and $R[x_0, \dots, x_n]$ are Noetherian. If $V_1 \subseteq V_2 \subseteq V_3 \subseteq \cdots$ is an ascending chain of open subsets of $X = \mathbb{A}^n(R)$ or $X = \mathbb{P}^n(R)$, it corresponds to an ascending chain of ideals $I_R(X \setminus V_1) \subseteq I_R(X \setminus V_2) \subseteq \cdots$; this chain will eventually become stationary, and since $V_i = X \setminus V_R(I_R(X \setminus V_i))$ so will become the chain $V_1 \subseteq V_2 \subseteq \cdots$. □

3.2 Varieties over Algebraically Closed Fields

In this section we want to discuss varieties over algebraically closed fields. We have already seen that in this case varieties have especially good properties. We first want to give some definitions and results for affine and projective varieties, before we introduce regular functions on varieties. Regular functions play the role of differential functions $f : X \to \mathbb{R}$ on manifolds X in differential geometry. Then we define morphisms between varieties and rational maps between varieties. Finally we define when a variety is smooth, give a criterion for smoothness, and state the Theorem of Bézout, which will be important to define a geometric group law on elliptic curves in Section 4.2.2.

Let $\mathbb{F}$ always be an algebraically closed field in this section.

3.2.1 Affine Varieties

We first want to discuss affine varieties. Let therefore $V = V_{\mathbb{F}}(\mathfrak{a})$ be an affine variety, $\mathfrak{a} = \langle f_1, \ldots, f_n \rangle$. We have already seen that $V = V_{\mathbb{F}}(\sqrt{\mathfrak{a}})$ and $I_{\mathbb{F}}(V) = \sqrt{\mathfrak{a}}$, and that $\sqrt{\mathfrak{a}}$ is prime.

Definition 3.2.1. *Define the* affine coordinate ring *of V, denoted by $\mathbb{F}[V]$, to be $\mathbb{F}[x_1, \ldots, x_n]/I_{\mathbb{F}}(V)$.*

Remark 3.2.2. By the above remark $\mathbb{F}[V]$ is a domain.

Elements of $\mathbb{F}[V]$ can be seen as functions on V, since every polynomial in $I_{\mathbb{F}}(V)$ vanishes on V. We will see in Proposition 3.2.17 how $\mathbb{F}[V]$ is connected to the set of regular functions on V.

We define the dimension of an affine variety as follows:

Definition 3.2.3. *The* dimension *of V, denoted by $\dim V$, is the dimension of V as a topological space, i. e. the supremum of the lengths of all chains of irreducible subsets.*

Remark 3.2.4. We have $\dim V = \operatorname{ht} I_{\mathbb{F}}(V) = \dim \mathbb{F}[V]$.

Varieties of dimension $n-1$ in $\mathbb{A}^n(\mathbb{F})$ can be characterized as follows:

Proposition 3.2.5. *[Har77, p. 7, ch. I, Proposition 1.13] An affine variety in $\mathbb{A}^n(\mathbb{F})$ has dimension $(n-1)$ if, and only if, it is defined by one non-constant irreducible polynomial in $\mathbb{F}[x_1, \ldots, x_n]$.*

3.2.2 Projective Varieties

Next we want to discuss projective varieties. For this let $V = V_{\mathbb{F}}(\mathfrak{a})$ be a projective variety, $\mathfrak{a} = \langle f_1, \ldots, f_n \rangle$. We have already seen that $V = V_{\mathbb{F}}(\sqrt{\mathfrak{a}})$ and $I_{\mathbb{F}}(V) = \sqrt{\mathfrak{a}}$, and that $\sqrt{\mathfrak{a}}$ is prime.

Definition 3.2.6. *Define the* homogenous coordinate ring *of V, denoted by $\mathbb{F}[V]$, to be $\mathbb{F}[x_0, \ldots, x_n]/I_{\mathbb{F}}(V)$.*

The homogenous coordinate ring is also a domain. It is also an $\mathbb{F}[x_0, \ldots, x_n]$-algebra, and hence the following definition makes sense:

Definition 3.2.7. *Define the* Hilbert polynomial *of V, denoted by P_V, as the Hilbert polynomial of $\mathbb{F}[V]$ seen as an $\mathbb{F}[x_0, \ldots, x_n]$-module.*

The Hilbert polynomial will be needed later to define the degree of a projective variety of dimension $n-1$ in $\mathbb{P}^n(\mathbb{F})$. The degree will be important to state the Theorem of Bézout which characterizes the intersection of two such varieties in $\mathbb{P}^2(\mathbb{F})$. For a projective variety the dimension can be defined in the same manner as for affine varieties:

Definition 3.2.8. *The* dimension *of V, denoted by* $\dim V$*, is the dimension of V as a topological space.*

3.2.3 Regular Functions

To define morphisms between varieties we first want to define what kind of functions defined on a variety are of interest, since we want that such functions, concatenated with a morphism of varieties, are again functions defined on the other variety. We are interested in functions which 'locally look like fractions of polynomials'.

Definition 3.2.9. *A* quasi-affine *or* quasi-projective *variety is an open subset of an affine or projective variety, respectively.*

Definition 3.2.10.

(a) *Let $V \subseteq \mathbb{A}^n(\mathbb{F})$ be a quasi-affine variety and $x \in V$ a point. A function $f : V \to \mathbb{F}$ is* regular at x *if there is a neighborhood $U \in \mathbb{U}_{V,x}$ and polynomials $g, h \in \mathbb{F}[x_1, \dots, x_n]$ such that $f(y) = \frac{g(y)}{h(y)}$ for all $y \in U$. If f is regular at any $x \in V$, we say that f is* regular on V.

(b) *Let $V \subseteq \mathbb{P}^n(\mathbb{F})$ be a quasi-projective variety and $x \in V$ a point. A function $f : V \to \mathbb{F}$ is* regular at x *if there is a neighborhood $U \in \mathbb{U}_{V,x}$ and homogenous polynomials $g, h \in \mathbb{F}[x_0, \dots, x_n]$ of the same degree such that $f(y) = \frac{g(y)}{h(y)}$ for all $y \in U$. If f is regular at any $x \in V$, we say that f is* regular on V.

The regularity of a function implies that it is continuous:

Proposition 3.2.11. *[Har77, p. 15, ch. I, Lemma 3.1] Let $f : V \to \mathbb{F}$ be a regular function, where V is quasi-affine or quasi-projective. Then f is continuous with respect to the Zariski topology when seen as a function $V \to \mathbb{A}^1(\mathbb{F})$.*

As a variety is irreducible we get the following corollary:

Corollary 3.2.12. *Let $f, g : V \to \mathbb{F}$ be regular. If $f = g$ on a non-empty open subset of V, then $f = g$ everywhere on V.*

Definition 3.2.13. *A* variety over $\mathbb{F}$ *is an affine, quasi-affine, projective or quasi-projective variety over $\mathbb{F}$.*

We next want to define and describe the structure sheaf of a variety. We are also interested in regular functions that are only defined on a non-empty open subset; they can be thought of as rational functions on a variety.

Definition 3.2.14. *Let V be a variety. Define the* structure sheaf $\mathcal{O}_V$ *on V as follows: for every open subset $U \in \mathbb{U}_V$, let $\mathcal{O}_V(U)$ be the set of regular functions $f : U \to \mathbb{F}$. (Note that U is quasi-affine or quasi-projective.)*

Proof. It is clear that this gives a pre-sheaf. Since the elements of the rings $\mathcal{O}_V(U)$ are functions $U \to \mathbb{F}$, and the condition for an arbitrary function $f : U \to \mathbb{F}$ to be inside $\mathcal{O}_V(U)$ is local, $\mathcal{O}_V$ is obviously a sheaf. □

Definition 3.2.15. *Let V be a variety. Define the* function field $\mathbb{F}(V)$ *to be the set of equivalence classes of pairs $\langle U, f\rangle$, where $U \in \mathbb{U}_V$ is non-empty and $f : U \to \mathbb{F}$ is regular, and $\langle U, f\rangle$ and $\langle V, g\rangle$ are identified if $f|_{U\cap V} = g|_{U\cap V}$.*

Proposition 3.2.16. *If V is a variety, then $\mathbb{F}(V)$ is a field, where the operations are defined as follows:*

$$\begin{aligned} &\langle U, f\rangle + \langle V, g\rangle = \langle U\cap V, f|_{U\cap V} + g|_{U\cap V}\rangle\,; \\ \textit{and}\qquad &\langle U, f\rangle \cdot \langle V, g\rangle = \langle U\cap V, f|_{U\cap V} \cdot g|_{U\cap V}\rangle\,. \end{aligned}$$

Proof. Note that if $U, W \in \mathbb{U}_V$ are non-empty, we have $U\cap W \neq \emptyset$ as V is irreducible. Moreover, if $f : U \to \mathbb{F}$ is regular but not constantly zero, then $\{f \neq 0\} := V \setminus V_{\mathbb{F}}(f)$ is non-empty and open and, therefore, $1/f$ is defined and regular on the open non-zero set $U \cap \{f \neq 0\}$. □

We can now describe the structure sheaf and the function field of affine and projective varieties:

Proposition 3.2.17. *[Har77, p. 17, ch. I, Theorem 3.2] Let $V \subseteq \mathbb{A}^n(\mathbb{F})$ be an affine variety, and let $A = \mathbb{F}[V]$ be the affine coordinate ring.*

(a) *Then $A \cong \Gamma(V, \mathcal{O}_V)$.*

(b) *For $x \in V$ let $\mathfrak{m}_x$ be the ideal of functions $f \in A$ vanishing at x. Then $x \mapsto \mathfrak{m}_x$ gives a one-to-one correspondence between the points of V and the maximal ideals of A.*

(c) *For $x \in V$ we have that $\mathcal{O}_{V,x} \cong A_{\mathfrak{m}_x}$ and* $\dim \mathcal{O}_{V,x} = \dim V$.

(d) *The function field $\mathbb{F}(V)$ is isomorphic to the field of fractions of A. Therefore $\mathbb{F}(V)$ is a finitely generated extension field of $\mathbb{F}$, having transcendence degree* $\operatorname{tr.deg.}_{\mathbb{F}} \mathbb{F}(V) = \dim V$ *by Remarks 2.3.24 (b).*

Proposition 3.2.18. *[Har77, p. 18, ch. I, Theorem 3.4] Let $V \subseteq \mathbb{P}^n(\mathbb{F})$ be a projective variety, and let $A = \mathbb{F}[V]$ be the homogenous coordinate ring.*

(a) *Then $\Gamma(V, \mathcal{O}_V) = \mathbb{F}$.*

(b) *For $x \in V$ let $\mathfrak{m}_x$ be the ideal generated by the homogenous polynomials $f \in A$ vanishing at x. Then $\mathfrak{m}_x$ is prime and $\mathcal{O}_{V,x} \cong A_{(\mathfrak{m}_x)}$.*

(c) *We have $\mathbb{F}(V) \cong A_{(\langle 0\rangle)}$.*

3.2.4 Morphisms between Varieties

Now we will define what a morphism between two varieties is and state some results on morphisms.

Definition 3.2.19. *Let X and Y be varieties over $\mathbb{F}$. A* morphism of varieties *$f : X \to Y$ is a continuous map such that for every regular function $\varphi : V \to \mathbb{F}$, $V \in \mathbb{U}_Y$, the function $\varphi \circ f : f^{-1}(V) \to \mathbb{F}$ is regular.*

Remark 3.2.20. The varieties over $\mathbb{F}$ with the morphisms from Definition 3.2.19 form a category, denoted by $\mathscr{V}\!ar(\mathbb{F})$.

With this definition we can enhance Proposition 3.1.22:

Proposition 3.2.21. *[Har77, p. 18, ch. I, Proposition 3.3] Let $H_i \subseteq \mathbb{P}^n(\mathbb{F})$ be the hyperplanes defined by $x_i \neq 0$, $0 \leq i \leq n$. Then the maps $\varphi_i : H_i \to \mathbb{A}^n(\mathbb{F})$ from Proposition 3.1.22 are isomorphisms of varieties.*

Next we state a result on what morphisms to affine varieties look like. This helps to describe morphisms to projective varieties by the use of Propositions 3.1.22 and 3.2.21.

Proposition 3.2.22. *[Har77, p. 19, ch. I, Proposition 3.5] Let X be any variety and Y be an affine variety. Then there exists a natural bijective map*

$$\mathrm{Hom}_{\mathscr{V}\!ar(\mathbb{F})}(X, Y) \to \mathrm{Hom}_{\mathbb{F}\text{-}\mathscr{A}lg}(\mathbb{F}[Y], \Gamma(X, \mathcal{O}_X)).$$

If we restrict our attention to affine varieties, we get the following equivalence of categories:

Corollary 3.2.23. *[Har77, p. 20, ch. I, Corollary 3.8] The contravariant functor*

$$\mathscr{V}\!ar(\mathbb{F}) \to \mathbb{F}\text{-}\mathscr{A}lg, \qquad X \mapsto \mathbb{F}[X]$$

induces an equivalence of categories between the category of affine varieties over $\mathbb{F}$ and the category of finitely generated domains over $\mathbb{F}$.

Similarly to Corollary 3.2.12 we get the following result for morphisms:

Proposition 3.2.24. *[Har77, p. 24, ch. I, Lemma 4.1] Let X and Y be varieties, and $f, g : X \to Y$ morphisms such that $f = g$ on a non-empty open subset of X. Then $f = g$ on all of X.*

3.2.5 Rational Maps between Varieties

Since morphisms are somehow well-behaved in that they are defined for every point, in some situations one wants to deal with maps which look at almost every point as a morphism.

Definition 3.2.25. *Let X and Y be varieties.*

(a) *If $U, V \in \mathbb{U}_X$ and $f : U \to Y$, $g : V \to Y$ are morphisms, we say $\langle U, f\rangle$ and $\langle V, g\rangle$ are* equivalent *if $f = g$ on $U \cap V$.*

(b) *A* rational map *$\varphi : X \to Y$ is an equivalence class of such pairs $\langle U, f \rangle$.*

(c) *A rational map $\varphi : X \to Y$ is* dominant *if for one pair $\langle U, f \rangle$ belonging to φ, the image $f(U)$ is Zariski-dense in Y.*

Remarks 3.2.26.

(a) If $\varphi : X \to Y$ is a rational map such that for every $x \in X$ there is a representative $\langle U, f \rangle$ with $x \in U$, then one representative of φ is a morphism $X \to Y$. In this case we treat φ itself as a morphism.

(b) Note that if $\varphi : X \to Y$ is rational and $\langle U, f \rangle$ and $\langle V, g \rangle$ are representatives of φ, then $f(U)$ is dense if, and only if, $g(V)$ is dense in Y.

(c) Comparing with Definition 3.2.15, one sees that the functions in the function field of a variety X are exactly the rational functions $X \to \mathbb{A}^1(\mathbb{F})$.

3.2.6 Smoothness

As in differential geometry, one is especially interested in objects without singularities. As there are no differential forms defined a priori in affine or projective space over an arbitrary algebraically closed field, we need to find another definition. It turned out that the notion of being regular reflects what we want:

Definition 3.2.27. *Let V be a variety and $x \in V$. Then V is* smooth *at x if $\mathcal{O}_{V,x}$ is a regular local ring. If V is smooth at every point, we say V is* smooth*.*

Clearly this definition is not useful for checking whether a variety is smooth. We now want to state a very important criterion for smoothness:

Theorem 3.2.28. *[Har77, p. 32, ch. I, Theorem 5.1] Let $V \subseteq \mathbb{A}^n(\mathbb{F})$ be an affine variety and $x \in V$. Let $f_1, \dots, f_m$ be generators for the ideal $I_{\mathbb{F}}(V)$. Then V is smooth at x if, and only if,*

$$\operatorname{rank} \left(\frac{\partial f_i}{\partial x_j}(x) \right)_{\substack{1 \le i \le m \\ 1 \le j \le n}} = n - \dim V.$$

Remarks 3.2.29.

(a) Note that whether V is smooth at x or not does not depend on either which generators f_i are chosen or on how V is embedded in $\mathbb{A}^n(\mathbb{F})$.

(b) The matrix $\left(\frac{\partial f_i}{\partial x_j}(x) \right)_{ij}$ is called the *Jacobian matrix* of V at x.

We will use this criterion later to characterize which cubic curves of a special form defined over an algebraically closed field are smooth.

3.2.7 Theorem of Bézout

The Theorem of Bézout describes the intersection set between a variety in $\mathbb{P}^2(\mathbb{F})$ and a hypersurface. An important special case is the intersection of a hypersurface and a line: Bézout's theorem states for this case that the intersection consists of exactly d points, where d is the degree of the variety. But first we want to define what a hypersurface is and what the degree of a projective variety is.

Definition 3.2.30. *[Har77, p. 52, ch. I]*

(a) *Let $X \subseteq \mathbb{P}^n(\mathbb{F})$ be a projective variety and P_X the Hilbert polynomial of X having degree r and leading coefficient c. Then the* degree *of X is $c \cdot r!$.*

(b) *A* hypersurface *is a projective variety generated by one polynomial.*

Proposition 3.2.31. *[Har77, p. 52, ch. I, Proposition 7.6] The degree of a non-zero projective variety is a positive integer. Moreover, if V is a variety defined by one homogenous polynomial of degree d, then the degree of V is d.*

Next we want to give the definition of the intersection multiplicity between a projective variety and a hypersurface.

Definition 3.2.32.

(a) *[Har77, p. 51, ch. I] Let $S = \mathbb{F}[x_0, \ldots, x_n]$, M be a graded S-module and $\mathfrak{p}$ be a minimal prime of S, i. e. a minimal element of $\operatorname{Ass}_{\mathbb{F}[x_0,\ldots,x_n]}(M)$. Let the* multiplicity of M at $\mathfrak{p}$, *denoted by $\mu_{\mathfrak{p}}(M)$, be the length of the $\mathbb{F}[x_0, \ldots, x_n]_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$.*

(b) *[Har77, p. 53, ch. I] Let $X \subseteq \mathbb{P}^n(\mathbb{F})$ be projective variety, $Y \subseteq \mathbb{P}^n(\mathbb{F})$ a hypersurface, and Z an irreducible component of $X \cap Y$. Define the* intersection multiplicity of X and Y at Z, *denoted by $i_{X,Y}(Z)$, as $\mu_{I_{\mathbb{F}}(Z)}(\mathbb{F}[x_0, \ldots, x_n]/(I_{\mathbb{F}}(X) + I_{\mathbb{F}}(Y)))$.*

Now we can state Bézout's Theorem:

Theorem 3.2.33 (Bézout). *[Har77, p. 54, ch. I, Corollary 7.8] Let X and Y be hypersurfaces in $\mathbb{P}^2(\mathbb{F})$, where X has degree n and Y has degree m. Let $Z_1, \ldots, Z_\ell$ be the irreducible components of $X \cap Y$. Then the Z_i are points and*

$$\sum_{i=1}^{\ell} i_{X,Y}(Z) = n \cdot m.$$

3.3 Schemes

In this section we want to introduce schemes and give first properties. More advanced definitions and results from scheme theory are given in the next two sections.

Schemes are a generalization of varieties, which allow to model changes of the base field or ring and especially the locality of many geometric notions. Unfortunately, the definition of a scheme is quite complicated. We begin by introducing the spectrum of the ring and the category of locally ringed spaces, and define an affine scheme. As the name hints, affine schemes generalize affine varieties. A general scheme is a locally ringed space that locally 'looks like' an affine scheme. More about the motives of why schemes were introduced can be found in the book [EH00].

After that we describe another construction, which in a certain sense generalizes projective varieties. In the next section we will see another generalization.

Introductive books on the Theory of Schemes are [Har77], [Iit82] and [EH00]. The latter tries to mediate the geometric side of schemes, while the first two provide a rigorous introduction to the Theory of Schemes, not requiring any requisites from algebraic geometry. Most of the information from this and the next three sections can be found in these books.

3.3.1 Spectrum of a Ring

Let R be a ring in the following. Recall that by a ring we always mean a *commutative ring with a unit.*

In Definition 2.3.36 we defined $\operatorname{Spec} R$, and now we want to restate this definition:

Definition 3.3.1. *Define*

$$\operatorname{Spec} R := \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \textit{ prime ideal of } R\}$$

to be the spectrum of R*.*

Next we define a topology on $\operatorname{Spec} R$. It is related to the Zariski topology from the previous section, as for an algebraically closed field $\mathbb{F}$ we have a bijection of algebraic sets in $\mathbb{A}^n(\mathbb{F})$ and radical ideals in $\mathbb{F}[x_1, \dots, x_n]$ by Hilbert's Nullstellensatz.

Definition 3.3.2. *For any ideal $\mathfrak{a} \subseteq R$, let $V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. Moreover, for any $f \in R$, define $D(f) := \operatorname{Spec} R \setminus V(\langle f \rangle)$.*

Proposition 3.3.3. *[Har77, p. 70, ch. II, Lemma 2.1 and p. 80, ch. II, Exercise 2.13(c)] The sets of the form $V(\mathfrak{a})$ form the closed sets of a topology on* $\operatorname{Spec} R$*, called the* Zariski topology*. The following properties hold:*

(1) *We have $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ if, and only if, $\sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$. This implies $V(\mathfrak{a}) = V(\mathfrak{b})$ if, and only if, $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$.*

(2) *We have that*

$$\bigcap_{i \in I} V(\mathfrak{a}_i) = V\left(\sum_{i \in I} \mathfrak{a}\right) \qquad \textit{and} \qquad \bigcup_{i=1}^{n} V(\mathfrak{a}_i) = V\left(\prod_{i=1}^{n} \mathfrak{a}_i\right).$$

(3) *The open sets $D(f)$, $f \in R$ form a basis of the topology.*

(4) *The topological space* $\operatorname{Spec} R$ *is compact*[1]*.*

(5) *It is* $\dim \operatorname{Spec} R = \dim R$*, where* $\dim \operatorname{Spec} R$ *is the dimension of* $\operatorname{Spec} R$ *as a topological space.*

[1] A topological space X is *compact* if for every open cover $(U_i)_{i \in I}$ of X, where I is an arbitrary index set, there exists a finite subset $J \subseteq I$ such that $\bigcup_{i \in J} U_i = X$.

We now define a sheaf of rings over $\operatorname{Spec} R$, which will generalize the sheaf of regular functions for affine varieties.

Definition 3.3.4. *Define a sheaf of rings $\mathcal{O}$ on the topological space $\operatorname{Spec} R$ as follows: for an open set U, let $\mathcal{O}(U)$ be the set of functions $s : U \to \coprod_{\mathfrak{p} \in U} R_{\mathfrak{p}}$ such that $s(\mathfrak{p}) \in R_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Spec} R$, and such that s is locally a quotient of elements of R. Or formulated differently,*

$$\mathcal{O}(U) := \left\{ (s^{(\mathfrak{p})})_{\mathfrak{p} \in U} \in \prod_{\mathfrak{p} \in U} R_{\mathfrak{p}} \;\middle|\; \begin{array}{c} \forall \mathfrak{p} \in U \; \exists V \in \mathbb{U}_{U,\mathfrak{p}} \; \exists r, s \in R \\ \forall \mathfrak{q} \in V : s \notin \mathfrak{q} \text{ and } s^{(\mathfrak{q})} = \frac{r}{s} \in R_{\mathfrak{q}} \end{array} \right\}.$$

The restriction maps are the obvious ones. We call $\mathcal{O}$ the structure sheaf *of* $\operatorname{Spec} R$.

Proof. It is easy to see that the property is local, and since it is also obvious that the difference and the product of two elements of $\mathcal{O}(U)$ is again in $\mathcal{O}(U)$, one directly sees that $\mathcal{O}$ is a sheaf of rings. □

Proposition 3.3.5. *[Har77, p. 71, ch. II, Proposition 2.2] Let R be a ring, and $\mathcal{O}$ the structure sheaf on* $\operatorname{Spec} R$.

(1) *If $\mathfrak{p} \in \operatorname{Spec} R$, then $\mathcal{O}_{\mathfrak{p}}$ is isomorphic to $R_{\mathfrak{p}}$. Hence $\mathcal{O}_{\mathfrak{p}}$ is a local ring for every $\mathfrak{p} \in \operatorname{Spec} R$.*

(2) *If $f \in R$, then $\mathcal{O}(D(f))$ is isomorphic to R_f. In particular $\Gamma(\operatorname{Spec} R, \mathcal{O}) \cong R$.*

We will later see that if $V \subseteq \mathbb{A}^n(\mathbb{F})$ is a variety defined by an ideal $\mathfrak{a}$ over an algebraically closed field $\mathbb{F}$, then $\operatorname{Spec} \mathbb{F}[x_1, \dots, x_n]/\mathfrak{a}$ corresponds to V.

3.3.2 Locally Ringed Spaces

Recall the definition of a ringed space: it is a topological space X together with a sheaf of rings $\mathcal{O}_X$ on X. A morphism of ringed spaces $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ is a pair $(f, f^\#)$ where $f : X \to Y$ is a continuous map and $f^\# : \mathcal{O}_Y \to f_* \mathcal{O}_X$ is a morphism of sheaves. We next want to introduce the notion of a locally ringed space, which, together with spectra of rings, is enough to define what a scheme is.

Definition 3.3.6. *Let R, S be two local rings with maximal ideals $\mathfrak{m}_R, \mathfrak{m}_S$, respectively, and $\varphi : R \to S$ is a ring morphism. Then φ is called a* local morphism *if $\varphi(\mathfrak{m}_R) \subseteq \mathfrak{m}_S$.*

Definition 3.3.7. *A ringed space X is called a* locally ringed space *if for every $p \in X$ we have that the stalk $\mathcal{O}_{X,p}$ is a local ring. If X and Y are locally ringed spaces and $f : X \to Y$ is a morphism of ringed spaces, then f is called a* morphism of locally ringed spaces *if for every $p \in X$ the induced map $f_p^\# : \mathcal{O}_{Y,f(p)} \to \mathcal{O}_{X,p}$ is a local morphism.*

With these definitions we can form the category of locally ringed spaces.

Now we show more properties of $\operatorname{Spec} R$, including that it gives a contravariant functor from $\mathscr{R}\mathit{ing}$ into the category of locally ringed spaces:

Proposition 3.3.8. *[Har77, p. 73, ch. II, Proposition 2.3] Let R and S be rings.*

(1) *If $\mathcal{O}$ is the structure sheaf of $\operatorname{Spec} R$, then $(\operatorname{Spec} R, \mathcal{O})$ is a locally ringed space. In the future we will simply write $\operatorname{Spec} R$ for $(\operatorname{Spec} R, \mathcal{O})$.*

(2) *If $\varphi : R \to S$ is a ring morphism, then this induces a morphism of locally ringed spaces $f : \operatorname{Spec} S \to \operatorname{Spec} R$.*

(3) *If $f : \operatorname{Spec} S \to \operatorname{Spec} R$ is a morphism of locally ringed spaces, then there exists a ring morphism $\varphi : R \to S$ which induces f as in (b).*

Moreover, $\mathbf{id}_R$ induces $\mathbf{id}_{\operatorname{Spec} R}$, and if T is another ring and $R \xrightarrow{\varphi} S \xrightarrow{\psi} T$ are ring morphisms, then the induced morphisms f of φ, g of ψ and h of $\psi \circ \varphi$ fulfill $h = f \circ g$:

$$\begin{tikzcd}
R \arrow[r, "\varphi"'] \arrow[rr, bend left, "\psi\circ\varphi"] \arrow[d, dotted] & S \arrow[r, "\psi"'] \arrow[d, dotted] & T \arrow[d, dotted] \\
\operatorname{Spec} R & \operatorname{Spec} S \arrow[l, "f"'] & \operatorname{Spec} T \arrow[l, "g"'] \arrow[ll, bend left, "h=f\circ g"]
\end{tikzcd}$$

Therefore $\operatorname{Spec} \bullet$ is a contravariant, fully faithful functor from the category of commutative rings with a unit to the category of locally ringed spaces.

Before we continue with the definition of a scheme in the next subsection, we want to recall the following topological definitions:

Definition 3.3.9. *Let X be a topological space.*

(1) *A point $x \in X$ is called a* closed point *if $\overline{\{x\}} = \{x\}$.*

(2) *Let Z be an irreducible closed subset of X. A* generic point *for Z is a point $x \in Z$, such that $\overline{\{x\}} = Z$.*

Remarks 3.3.10. In $\operatorname{Spec} R$, the closed points are exactly the maximal ideals. The irreducible subsets and their generic points are characterized later in Lemma 3.3.33.

3.3.3 Schemes

Now we are finally able to define what a scheme is:

Definition 3.3.11.

(1) *An* affine scheme *is a locally ringed space X such that X is isomorphic as a locally ringed space to $\operatorname{Spec} R$ for some ring R.*

(2) *A* scheme *X is a locally ringed space such that every $p \in X$ has an open neighborhood U such that $(U, \mathcal{O}_X|_U)$ is an affine scheme.*

(3) *A* morphism of schemes *$f : X \to Y$ for two schemes X, Y is a morphism of locally ringed spaces.*

With these definitions we can form the category of schemes and its full subcategory of affine schemes.

Remark 3.3.12. If R is a ring, then $\operatorname{Spec} R$ is an (affine) scheme.

Definition 3.3.13. *Let R be a ring. Define the* affine n-space over R *as* $\mathbb{A}_R^n := \operatorname{Spec} R[x_1, \dots, x_n]$.

We will see in Section 3.6 how this definition is related to the previous definition of affine n-space over R, namely $\mathbb{A}^n(R)$.

We can now define the notion of a scheme over a base scheme, and that of a scheme-theoretic point.

Definition 3.3.14. *Let S be any scheme. An* S-scheme *is a tuple (X, f) where X is a scheme and $f : X \to S$ is a morphism. If f is clear from the context, one can also simply say that X is an S-scheme, or that X is a* scheme over S. *The morphism f is also called the* structure morphism *of X over S. If (Y, g) is another S-scheme, then a morphism of schemes $h : X \to Y$ is a* morphism of S-schemes *if $g \circ h = f$.*

If X and Y are S-schemes, then an Y-rational point *or* section of X (over Y) *is an S-morphism $Y \to X$. The set of all S-rational points of X is denoted by $X(S)$. A* geometric point *of X is a morphism* $\operatorname{Spec} \mathbb{F} \to X$ *for an algebraically closed field $\mathbb{F}$.*

If $S = \operatorname{Spec} R$ for a ring R, one also speaks of schemes over R, R-morphisms *and* R-rational points.

Note that with this definition we have two kinds of points for a scheme X/S: its points $p \in X$ of the topological space, and its S-rational points. In some cases certain subsets of these points can be identified (see Section 3.6 for more information).

Remark 3.3.15. If R is a ring, then $\mathbb{A}_R^n$ is in a natural way an R-scheme.

The next remark will allow us to draw a connection between $\mathbb{A}_R^n(R) = \mathbb{A}_R^n(\operatorname{Spec} R)$ and $\mathbb{A}^n(R)$. A closer connection will be given in Section 3.6.

Proposition 3.3.16. *[Har77, p. 79, ch. II, Exercise 2.4] Let R be a ring, $n \in \mathbb{N}_{>0}$ and X a scheme over R. Then there is a one-to-one correspondence of R-morphisms $X \to \mathbb{A}_R^n$ and R-linear ring morphisms $R[x_1, \dots, x_n] \to \Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X)$. To be more exact,*

$$\operatorname{Hom}(X, \mathbb{A}_R^n) \cong \operatorname{Hom}_R(R[x_1, \dots, x_n], \Gamma(X, \mathcal{O}_X)).$$

Here $\Gamma(X, \mathcal{O}_X)$ has the structure of an R-algebra given by the structure morphism of X over R.

If R is a ring and M an R-module, we have seen that $\operatorname{Spec} R$ encapsulates the global and local information of R. To encapsulate the global and local information of M in a similar way, we need the following definition:

Definition 3.3.17. *Let R be a ring, $X = \operatorname{Spec} R$ and M an R-module. Define*

$$\tilde{M}(U) := \left\{ (s^{(\mathfrak{p})})_{\mathfrak{p}\in U} \in \prod_{\mathfrak{p}\in U} M_{\mathfrak{p}} \;\middle|\; \begin{array}{c} \forall \mathfrak{p} \in U \; \exists V \in \mathbb{U}_{U,\mathfrak{p}} \; \exists r \in M, s \in R \\ \forall \mathfrak{q} \in V : s \notin \mathfrak{q} \text{ and } s^{(\mathfrak{q})} = \frac{r}{s} \in M_{\mathfrak{q}} \end{array} \right\}.$$

With the obvious restriction maps this defines a sheaf $\tilde{M} : U \mapsto \tilde{M}(U)$, called the sheaf associated to *M.*

Proposition 3.3.18. *[Har77, p. 110, ch. II, Proposition 5.1] Let R be a ring, M an R-module and $X = \operatorname{Spec} R$.*

(a) *Then $\tilde{M}$ is an $\mathcal{O}_X$-module.*

(b) *Moreover $\tilde{M}_{\mathfrak{p}} \cong M_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Spec} R$.*

(c) *We have $\Gamma(X, \tilde{M}) = M$.*

As schemes are locally ringed spaces that locally look like spectra of rings, we are especially interested in $\mathcal{O}_X$-modules that locally look like sheaves associated to modules:

Definition 3.3.19. *Let X be a scheme and $\mathcal{F}$ an $\mathcal{O}_X$-module. Then $\mathcal{F}$ is* quasi-coherent *if X can be covered by open affine $U = \operatorname{Spec} R$, such that $\mathcal{F}|_U \cong \tilde{M}$ for some R-module M.*

3.3.4 Projective Spectrum

We next want to define a construction which generalizes the construction of projective varieties. Recall that for projective varieties graded rings play an important role. We begin with describing the equivalent of $\operatorname{Spec} R$ for graded rings and defining the Zariski topology in a similar way.

Definition 3.3.20. *Let S be a graded ring. Define*

$$\operatorname{Proj} S := \{\mathfrak{p} \subseteq S \mid \mathfrak{p} \text{ prime and homogenous, } S_+ \not\subseteq \mathfrak{p}\}$$

as the projective spectrum *of S.*

Definition 3.3.21. *Let S be a graded ring and $\mathfrak{a}$ a homogenous ideal in S. Define*

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Proj} S \mid \mathfrak{p}\mathfrak{a} \subseteq \mathfrak{p}\}.$$

If $f \in S$ is homogenous, define

$$D_+(f) := \operatorname{Proj} S \setminus V(\langle f \rangle).$$

Proposition 3.3.22. *[Har77, p. 76, ch. II, Lemma 2.4 and p. 76, ch. II, Proposition 2.5] The sets of the form $V(\mathfrak{a})$ form the closed sets of a topology on* $\operatorname{Proj} S$, *called the* Zariski topology. *The following properties hold:*

(1) *We have that*

$$\bigcap_{i\in I} V(\mathfrak{a}_i) = V\left(\sum_{i\in I} \mathfrak{a}\right) \qquad \text{and} \qquad \bigcup_{i\in I} V(\mathfrak{a}_i) = V\left(\prod_{i=1}^{n} \mathfrak{a}_i\right).$$

(2) *The $D_+(f)$, $f \in S_+$ homogenous, form a basis of the topology.*

(3) *It is* $\dim \operatorname{Proj} S = \dim^h S$.

We next want to associate a structure sheaf to $\operatorname{Proj} S$ in a similar way as for $\operatorname{Spec} R$:

Definition 3.3.23. *Let S be a graded ring. Define the* structure sheaf *of* $\operatorname{Proj} S$ *by*

$$\mathcal{O}(U) := \left\{ (s^{(\mathfrak{p})})_{\mathfrak{p}\in U} \in \prod_{\mathfrak{p}\in U} S_{(\mathfrak{p})} \;\middle|\; \begin{array}{r} \forall \mathfrak{p} \in U\ \exists V \in \mathbb{U}_{U,\mathfrak{p}}\ \exists r, s \in S^h \\ \forall \mathfrak{q} \in V : s \notin \mathfrak{q} \text{ and } s^{(\mathfrak{q})} = \frac{r}{s} \in S_{(\mathfrak{q})} \end{array} \right\}.$$

The restriction maps are the obvious ones.

Proof. Again it is easy to see that this is a sheaf of rings on $\operatorname{Proj} S$. □

Proposition 3.3.24. *[Har77, p. 76, ch. II, Proposition 2.5] Let S be a graded ring, and let $\mathcal{O}$ be the structure sheaf of* $\operatorname{Proj} S$.

(1) *For any $\mathfrak{p} \in \operatorname{Proj} S$ we get an isomorphism $\mathcal{O}_{\mathfrak{p}} \cong S_{(\mathfrak{p})}$. Therefore $\mathcal{O}_{\mathfrak{p}}$ is a local ring.*

(2) *For every homogenous $f \in S_+$ we have that $(D_+(f), \mathcal{O}|_{D_+(f)})$ is isomorphic as a locally ringed space to* $\operatorname{Spec} S_{(f)}$.

(3) *The locally ringed space* $(\operatorname{Proj} S, \mathcal{O})$ *is a scheme.*

We will now define projective space over a ring in a scheme theoretic way. Again we will not see the connection to $\mathbb{P}^n(R)$ from Section 3.1 yet, but later in Section 3.6.

Definition 3.3.25. *Let R be a ring and $n \in \mathbb{N}_{>0}$. Define the* projective n-space over R *as* $\mathbb{P}^n_R := \operatorname{Proj} R[x_0, \ldots, x_n]$.

If S is a graded ring which is an R-algebra, the following lemma allows us to see $\operatorname{Proj} S$ as an R-scheme:

Lemma 3.3.26. *[Iit82, p. 165] Let S be a graded ring and $R = S_0$. Then there is a natural map $f : \operatorname{Proj} S \to \operatorname{Spec} R$.*

If S is a graded ring and M a graded S-module, we again are interested in a similar construction for M over $\operatorname{Proj} S$ as in the previous section for modules over arbitrary rings.

Definition 3.3.27. *Let S be a graded ring, $X = \operatorname{Proj} S$ and M a graded S-module. Define*

$$\tilde{M}(U) := \left\{ (s^{(\mathfrak{p})})_{\mathfrak{p}\in U} \in \prod_{\mathfrak{p}\in U} M_{(\mathfrak{p})} \;\middle|\; \begin{array}{r} \forall \mathfrak{p} \in U\ \exists V \in \mathbb{U}_{U,\mathfrak{p}}\ \exists r \in M^h, s \in S^h \\ \forall \mathfrak{q} \in V : s \notin \mathfrak{q} \text{ and } s^{(\mathfrak{q})} = \frac{r}{s} \in M_{(\mathfrak{q})} \end{array} \right\}.$$

With the obvious restriction maps this defines a sheaf $\tilde{M} : U \mapsto \tilde{M}(U)$, called the sheaf associated to M.

Proposition 3.3.28. *[Har77, pp. 116f, ch. II, Proposition 5.11] Let S be a graded ring, M a graded S-module, and $X = \operatorname{Proj} S$.*

(a) *Then $\tilde{M}$ is a quasi-coherent $\mathcal{O}_X$-module.*

(b) *For any $\mathfrak{p} \in X$ we have $\tilde{M}_{\mathfrak{p}} \cong M_{(\mathfrak{p})}$.*

(c) *If $f \in S_+^h$, then $\tilde{M}|_{D_+(f)} \cong \widetilde{M_{(f)}}$.*

In Definition 2.3.11 we defined the twist of a graded module. We will now define a similar concept for sheaves of modules over $\mathcal{O}_X$. We will later need this to characterize the R-rational points of $\operatorname{Proj} S$.

Definition 3.3.29. *Let S be a graded ring and $X = \operatorname{Proj} S$, and let $z \in \mathbb{Z}$.*

(a) *Define $\mathcal{O}_X(z)$ to be $\widetilde{S(z)}$.*

(b) *If $\mathcal{F}$ is a sheaf of $\mathcal{O}_X$-modules, define $\mathcal{F}(z) := \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(z)$.*

Proposition 3.3.30. *[Har77, p. 117, ch. II, Proposition 5.12] Let S be a graded ring, $X = \operatorname{Proj} S$, and assume that S is generated by S_1 as an S_0-algebra.*

(a) *The sheaf $\mathcal{O}_X(z)$ is an invertible sheaf for every $z \in \mathbb{Z}$.*

(b) *If M is a graded S-module, then $\tilde{M}(z) = \widetilde{M(z)}$ for any $z \in \mathbb{Z}$.*

(c) *For $z, w \in \mathbb{Z}$ we have $\mathcal{O}_X(z) \otimes_{\mathcal{O}_X} \mathcal{O}_X(w) \cong \mathcal{O}_X(z + w)$.*

For later use we need the following proposition, which gives us information about the global sections of the twisted sheaf $\mathcal{O}_{\mathbb{P}^n_R}(k)$:

Proposition 3.3.31. *Let R be a ring and $n \in \mathbb{N}$, $k \in \mathbb{Z}$. Then $(\mathcal{O}_{\mathbb{P}^n_R}(k))(\mathbb{P}^n_R) = R[x_0, \ldots, x_n]_k$.*

Proof. For $n = 0$ note that $D_+(x_0) = \mathbb{P}^0_R$. We therefore assume $n > 0$.

Let $s \in (\mathcal{O}_{\mathbb{P}^n_R}(k))(\mathbb{P}^n_R)$, and consider $U_i = D_+(x_i)$. By Proposition 3.3.28 (c) we have $s|_{U_i} = \frac{f_i}{x_i^{d_i}}$ for some $f_i \in R[x_0, \ldots, x_n](k)_{d_i}$ and $d_i \in \mathbb{N}$. Moreover consider $U_{ij} = D_+(x_i x_j) \subseteq D_+(x_i) \cap D_+(x_j)$. Thus,

$$s|_{U_{ij}} = \frac{f_i x_j^{d_i}}{(x_i x_j)^{d_i}} = \frac{f_j x_i^{d_j}}{(x_i x_j)^{d_j}} \in R[x_0, \ldots, x_n]_{(x_i x_j)}.$$

But as $x_i x_j$ is a non-zero-divisor, this means that

$$f_j x_i^{d_j} (x_i x_j)^{d_i} = f_i x_j^{d_i} (x_i x_j)^{d_j},$$

and as x_i, x_j are non-zero-divisors, we get $f_j x_i^{d_i} = f_i x_j^{d_j}$. By choosing $i \neq j$ we see that $f_i = \tilde{f}_i x_i^{d_i}$ with a homogenous $\tilde{f}_i \in R[x_0, \ldots, x_n]_k$ for every i and, therefore,

$$s|_{D_+(x_i)} = \frac{\tilde{f}_i}{x_i^0} \in R[x_0, \ldots, x_n](k)_{(x_i)}$$

and, moreover, $\tilde{f}_i = \tilde{f}_j$ for all i, j. □

3.3.5 First Properties of Schemes

Before closing this section we want to state some first properties of schemes. The first results give information on the topological space of a scheme and about its irreducible subsets:

Lemma 3.3.32. *[Iit82, p. 13, Proposition 1.5] The topological space of a scheme is T_0, i. e. for every two distinct points there exists an open set containing one but not the other.*

Lemma 3.3.33. *[Iit82, p. 16, Proposition 1.8] The irreducible closed subsets of* $\operatorname{Spec} R$ *are exactly the sets of the form $V(\mathfrak{a})$, where $\mathfrak{a} \subseteq R$ is an ideal such that $\sqrt{\mathfrak{a}}$ is prime. In that case $\overline{\{\sqrt{\mathfrak{a}}\}}$ equals the irreducible closed subset. Hence the irreducible subsets are exactly the ones of the form $V(\mathfrak{p})$, where $\mathfrak{p} \in \operatorname{Spec} R$.*

Lemma 3.3.34. *[Har77, p. 80, ch. II, Exercise 2.9] If X is a scheme, then every non-empty irreducible closed subset has a unique generic point.*

The connectedness of an affine scheme can be characterized as follows:

Lemma 3.3.35. *[Har77, p. 82, ch. II, Exercise 2.19] Consider the topological space $S = \operatorname{Spec} R$ for a ring S. Then the following are equivalent:*

(i) *It is $R = R_1 \times R_2$ for two non-zero rings R_1, R_2; and*

(ii) *The topological space S is* disconnected, *i. e. it contains a non-trivial proper subset U which is both open and closed.*

If $R = \prod_{i=1}^{n} R_i$ is an Artinian ring with its decomposition into local Artinian rings, the lemma says that $\operatorname{Spec} R$ consists of n points, each corresponding to a maximal ideal $\mathfrak{m}_i$ of an R_i. Moreover, $\operatorname{Spec} R$ can be seen as the disjoint union of the $\operatorname{Spec} R_i$'s.

We next want to define some useful properties schemes can have.

Definition 3.3.36. *Let X be a scheme.*

(a) *Then X is* integral *if all rings $\mathcal{O}_X(U)$, $U \in \mathbb{U}_X$ are domains.*

(b) *The scheme X is* reduced *if all rings $\mathcal{O}_X(U)$, $U \in \mathbb{U}_X$ are reduced.*

(c) *The scheme X is* regular *if all local rings $\mathcal{O}_{X,x}$, $x \in X$ are regular local rings.*

(d) *The scheme X is* irreducible *if its topological space X is irreducible.*

(e) *The scheme X is* connected *if its topological space X is connected.*

Proposition 3.3.37. *[Har77, p. 82, ch. II, Proposition 3.1] A scheme is integral if, and only if, it is reduced and connected.*

Definition 3.3.38. *Let X be a scheme.*

(a) *We call X* locally Noetherian *if X can be covered by open affine subsets* $\operatorname{Spec} A_i$ *such that every A_i is a Noetherian ring.*

(b) *We call X* Noetherian *if it is locally Noetherian and compact.*

If R is a Noetherian ring, then clearly $\operatorname{Spec} R$ is Noetherian.

3.4 Morphisms of Schemes

In this section we want to present several results and constructions for morphisms of schemes, and further define and describe properties of morphisms.

3.4.1 Fibred Products

The first, very important construction is the fibred product of two S-schemes. It can also be seen as the product of two morphisms with the same destination.

Definition 3.4.1. *Let X and Y be schemes over a base scheme S. The* fibred product *of X and Y over S is an S-scheme $X \times_S Y$ with S-morphisms $f_X : X \times_S Y \to X$ and $f_Y : X \times_S Y \to Y$, such that for every scheme Z and S-morphisms $g : Z \to X$ and $h : Z \to Y$, there exists a unique morphism $Z \to X \times_S Y$, such that the following diagram commutes:*

$$\begin{tikzcd}
Z \arrow[dr, dashed, "\exists!"] \arrow[drr, bend left, "g"] \arrow[ddr, bend right, "h"'] & & \\
& X \times_S Y \arrow[r, "f_X"'] \arrow[d, "f_Y"] & X \arrow[d] \\
& Y \arrow[r] & S
\end{tikzcd}$$

Remarks 3.4.2.

(a) Note that by the universal property of the fibred product, it is unique up to a unique isomorphism, if it exists. Therefore, it is justified to speak of *the* fibred product.

(b) Since $\operatorname{Spec} \mathbb{Z}$ is the final object in the category of schemes [Har77, p. 79, ch. II, Exercise 2.5], the fibred product of two arbitrary schemes X and Y can always be taken over $\operatorname{Spec} \mathbb{Z}$, provided the fibred product exists. Therefore, define $X \times Y := X \times_{\operatorname{Spec} \mathbb{Z}} Y$.

(c) The fibred product $X \times_S Y$ is the usual categorical product of X and Y in the category of S-schemes.

Proposition 3.4.3. *[Har77, p. 87, ch. II, Theorem 3.3] For any two schemes X and Y over a scheme S, the fibred product $X \times_S Y$ exists.*

Remarks 3.4.4. [Har77, pp. 87f, ch. II, Proof of Theorem 3.3]

(a) If $S = \operatorname{Spec} R$, $X = \operatorname{Spec} A$, and $Y = \operatorname{Spec} B$ where A, B are R-algebras, then $X \times_S Y = \operatorname{Spec}(A \otimes_R B)$, and the projections $X \times_S Y \to X$ and $X \times_S Y \to Y$ correspond to the natural maps $A \to A \otimes_R B$ and $B \to A \otimes_R B$.

(b) Let X be covered by X_i's and Y be covered by Y_j's. Then $X \times_S Y$ is completely determined by the $X_i \times_S Y_j$'s. Moreover, if S is covered by S_i's, $f : X \to S$ and $g : Y \to S$, $X_i = f^{-1}(S_i)$ and $Y_i = g^{-1}(S_i)$, then $X \times_S Y$ is completely determined by the $X_i \times_{S_i} Y_i$'s.

The fibred product has many important uses in algebraic geometry. We want to present two cases which we will often need.

Base Extension The fibred product can be used for base extension: if one has a scheme X over a base S, and a morphism $T \to S$ of schemes, then one can consider X as a T-scheme using the fibred product. Note that since morphisms $T \to S$ correspond to ring morphisms $A \to B$ if $T = \operatorname{Spec} B$ and $S = \operatorname{Spec} A$, one can think of base extension as a mechanism transporting the defining relations of the scheme X over to another base.

Definition 3.4.5. *Let X be a scheme over S, and $f : T \to S$ a morphism. Then the scheme*

$$X_T := X \times_S T$$

is said to be the scheme obtained from X by base extension $T \to S$. *The projection $X_T \to T$ will be denoted by f_T.*

Corollary 3.4.6. *Let R be a ring and $R \to S$ a morphism. Let $X = \operatorname{Spec} R$ and $T = \operatorname{Spec} S$.*

(a) *If A is an R-algebra, $Y = \operatorname{Spec} A$, and $f : Y \to X$ is the structure morphism, then $Y_T = \operatorname{Spec}(A \otimes_R S)$ and $f_T : Y_T \to T$ is the structure morphism of Y_T over T.*

(b) *If $Y = \mathbb{A}^n_R$ for an $n \in \mathbb{N}$, then $Y_T = \mathbb{A}^n_S$.*

We can now define projective n-space over an arbitrary scheme:

Definition 3.4.7. *Let Y be a scheme and $n \in \mathbb{N}$. Then the* projective n-space *over Y, denoted by $\mathbb{P}^n_Y$, is defined as $\mathbb{P}^n_{\mathbb{Z}} \times_{\operatorname{Spec} \mathbb{Z}} Y$.*

Remark 3.4.8. [Har77, p. 103, ch. II] Note that if R is a ring, then $\mathbb{P}^n_R = \mathbb{P}^n_{\mathbb{Z}} \times \operatorname{Spec} R = \mathbb{P}^n_{\operatorname{Spec} R}$.

As base extension can be used to enlarge the ground field of a scheme defined over $\operatorname{Spec} \mathbb{F}$ to a field containing $\mathbb{F}$, one can use base extension to view such a scheme as a scheme over the algebraic closure of $\mathbb{F}$. This leads to the following definition:

Definition 3.4.9. *Let X be a scheme over a field $\mathbb{F}$, and let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$.*

(a) *Then X is* geometrically connected *if $X \times_{\mathbb{F}} \overline{\mathbb{F}}$ is connected.*

(b) *Then X is* geometrically irreducible *if $X \times_{\mathbb{F}} \overline{\mathbb{F}}$ is irreducible.*

The next proposition shows that base extension behaves functorial:

Proposition 3.4.10. *[Iit82, pp. 69, e. and Proposition 1.32 (v)] Let S be any scheme. Then any morphism $T \to S$ of schemes induces a functor $\mathscr{Sch}(S) \to \mathscr{Sch}(T)$ by $X \mapsto X_T = X \times_S T$, such that $f : X \to Y$ goes over to $f_T : X_T \to Y_T$. This functor preserves fibred products, i. e. $X \times_S Y$ goes over to $X_T \times_T Y_T$ and $f \times g : X \times_S Y \to X' \times_S Y'$ goes over to $f_T \times g_T : X_T \times_T Y_T \to X'_T \times_T Y'_T$.*

Moreover, for every S-scheme X there exists a unique morphism $X_T \to X$ such that the following diagram commutes for any S-morphism $f : X \to Y$:

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, dotted] & & Y \arrow[dl, dotted] & \mathscr{S}ch(S) \arrow[dd] \\
& S & & \\
X_T \arrow[uu] \arrow[rr, "f_T"] \arrow[dr, dotted] & & Y_T \arrow[uu] \arrow[dl, dotted] & \mathscr{S}ch(T) \\
& T \arrow[uu, dotted] & &
\end{tikzcd}$$

We now want to explicitly compute a base extension which we will need later.

Proposition 3.4.11. *Let A be a ring, $\mathfrak{a}$ be a homogenous ideal in $R[x_0, \dots, x_n]$, and $\varphi : A \to B$ be a ring morphism. Let $\mathfrak{b} = \langle \varphi(\mathfrak{a}) \rangle_B \subseteq B[x_0, \dots, x_n]$. Then*

$$\operatorname{Proj} A[x_0, \dots, x_n]/\mathfrak{a} \times_{\operatorname{Spec} A} \operatorname{Spec} B = \operatorname{Proj} B[x_0, \dots, x_n]/\mathfrak{b}.$$

Proof. We know that $X := \operatorname{Proj} A[x_0, \dots, x_n]/\mathfrak{a}$ is covered by the $D_+(x_i)$'s, and that

$$X|_{D_+(x_i)} = \operatorname{Spec}(A[x_0, \dots, x_n]/\mathfrak{a})_{(\langle x_i \rangle)},$$

and that

$$(A[x_0, \dots, x_n]/\mathfrak{a})_{(\langle x_i \rangle)} \cong A[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]/(\mathfrak{a}|_{x_i=1}).$$

Now $\langle \varphi(\mathfrak{a}|_{x_i=1}) \rangle_B = \mathfrak{b}|_{x_i=1}$, and therefore by Lemma 2.1.35 we have

$$(A[x_0, \dots, x_n]/\mathfrak{a})_{(\langle x_i \rangle)} \otimes_A B \cong (B[x_0, \dots, x_n]/\mathfrak{b})_{(\langle x_i \rangle)}.$$

Hence, by Remark 3.4.4 (b), we are done. □

Fibres Another important concept that can be realized with fibred products is the concept of fibres of a morphism. If one has a morphism $f : X \to Y$ of schemes, one can consider Y being a set which parameterizes X: for every $y \in Y$ one can look at $Z := X|_{f^{-1}(y)}$. Unfortunately, Z is not a scheme over a base. But one can rescue this concept by using the fibred product as we will see in the following.

Definition 3.4.12. *Let X be a scheme, and $p \in X$ a point. Consider the local ring $\mathcal{O}_{X,p}$ and its maximal ideal $\mathfrak{m}_{X,p}$. Define the* residue field $k(p)$ *of p on X to be the field $k(p) := \mathcal{O}_{X,p}/\mathfrak{m}_{X,p}$.*

Note that $\operatorname{Spec} k(y)$ is a Y-scheme [Har77, p. 80, ch. II, Exercise 2.7].

Definition 3.4.13. *Let $f : X \to Y$ be a morphism of schemes, and $y \in Y$.*

(a) *The* fibre *of f in y is the scheme*

$$X_y := X \times_Y \operatorname{Spec} k(y).$$

(b) *The* geometric fibre *of f in y is the scheme*

$$X \times_Y \operatorname{Spec} \overline{k(y)},$$

where $\overline{k(y)}$ is the algebraic closure of $k(y)$. (See [Mum99, p. 111].)

Remark 3.4.14. [Har77, p. 92, ch. II, Exercise 3.10(a)] The fibre of f in y is homeomorphic to $f^{-1}(y)$ and it is a scheme over $k(y)$. The geometric fibre of f in y is a scheme over the algebraic closure of $k(y)$.

A very interesting case is the *generic fibre* of a morphism, that is, the fibre of a morphism $X \to Y$ at the generic point of Y (for this we obviously need Y to be irreducible):

Proposition 3.4.15. *Assume S is an irreducible and integral scheme and ξ its generic point. Then the functor $\mathscr{S}ch(S) \to \mathscr{S}ch(k(\xi))$, $X \mapsto X_\xi$ from Proposition 3.4.10 is faithful, i. e. if X and Y are S-schemes, then the induced map $\operatorname{Hom}_S(X, Y) \to \operatorname{Hom}_{k(\xi)}(X_\xi, Y_\xi)$ is injective.*

The same is true for the functor $\mathscr{S}ch(S) \to \mathscr{S}ch(\overline{k(\xi)})$, where $\overline{k(\xi)}$ is the algebraic closure of $k(\xi)$.

Proof. This question is clearly local on S, therefore, assume $S = \operatorname{Spec} R$ and let $K = k(\xi)$ be the field of fractions of R. Moreover, the question is local on Y. Hence we can assume $Y = \operatorname{Spec} B$ for an R-algebra B by restricting to $f : f^{-1}(\operatorname{Spec} B) \to \operatorname{Spec} B$. Again the question is local on X and, therefore, we can assume $X = \operatorname{Spec} A$ for an R-algebra A. Thus, we have R-morphisms $f : \operatorname{Spec} A \to \operatorname{Spec} B$, which correspond to R-algebra morphisms $B \to A$. Now, applying the functor, these are going over to K-algebra morphisms $B_K \to A_K$, where $f : B \to A$ goes to $f \otimes 1 : B \otimes_R K \to A \otimes_R K$, $x \otimes 1 \mapsto f(x) \otimes 1$. By Lemma 2.1.33 (a) we get that the morphism $A \to A \otimes_R K$, $a \mapsto a \otimes 1$ (which is R-linear) is injective, since $R \to K$ is injective. With this we can conclude. □

3.4.2 Special Classes of Morphisms

In this subsection we want to present several types of morphisms, including characterizations and implications.

Immersions and Subschemes Immersions can be thought of as inclusion maps. We will define open and closed immersions and, using them, open and closed subschemes of a scheme. We will, moreover, characterize all closed subschemes using ideal sheaves.

Definition 3.4.16. *Let X be a scheme.*

(1) *An* open subscheme *of X is a scheme U whose topological subspace is an open subset of X and whose structure sheaf $\mathcal{O}_U$ is isomorphic to the restriction $\mathcal{O}_X|_U$.*

(2) *An* open immersion *is a morphism $f : X \to Y$ that induces an isomorphism of X with an open subscheme of Y.*

(3) *A* closed immersion *is a morphism $f : Y \to X$ that induces a homeomorphism of the topological space Y into a closed subset of the topological space X and, furthermore, the induced map $f^\#$ of sheaves is surjective.*

(4) *A* closed subscheme *of X is an equivalence class of closed immersions $f : Y \to X$, where two such immersions $f : Y \to X$, $f' : Y' \to X$ are identified if there is an isomorphism $\iota : Y \to Y'$ such that $f' \circ \iota = f$.*

(5) *Let Y be a closed subscheme of X with the inclusion $i : Y \to X$. The* ideal sheaf of Y*, denoted by $\mathscr{I}_Y$, is the kernel of the morphism $i^\# : \mathcal{O}_X \to i_*\mathcal{O}_Y$.*

(6) *An ideal sheaf $\mathscr{I}$ of $\mathcal{O}_X$ is called* locally principal *if there exists a cover of open affine subsets $U_i = \operatorname{Spec} R_i$ of X such that $\mathscr{I}|_{U_i}$ is generated by one section.*

Proposition 3.4.17. *[Har77, p. 116, ch. II, Proposition 5.9] Let X be a scheme.*

(a) *If Y is a closed subscheme of X, then its ideal sheaf $\mathscr{I}_Y$ is quasi-coherent.*

(b) *Any quasi-coherent ideal sheaf $\mathscr{I}$ determines a unique closed subscheme Y of X such that $\mathscr{I} = \mathscr{I}_Y$.*

Quasi-compact Morphisms

Definition 3.4.18. *[Har77, p. 91, ch. II, Exercise 3.2] Let $f : X \to Y$ be a morphism of schemes. Then f is* quasi-compact *if one can cover Y with open affine V_i such that $f^{-1}(V_i)$ is compact.*

Separated and Quasi-Separated Morphisms Being separated over a base corresponds to being Hausdorff. For example, if a scheme is separated over a field $\mathbb{F}$, then it cannot contain double points. More details can be found in the book of Eisenbud and Harris [EH00, pp. 93ff].

Definition 3.4.19. *Let $f : C \to S$ be a morphism of schemes. The* diagonal morphism *is the unique morphism $\Delta_f : C \to C \times_S C$ such that $p_i \circ \Delta_f = \mathbf{id}_C$ for both projections p_i:*

$$\begin{tikzcd}
C \arrow[dr, "\Delta_f", "\exists!"'] \arrow[drr, bend left, "\mathbf{id}_C"] \arrow[ddr, bend right, "\mathbf{id}_C"'] & & \\
& C \times_S C \arrow[r, "p_2"] \arrow[d, "p_1"'] & C \arrow[d, "f"] \\
& C \arrow[r, "f"'] & S
\end{tikzcd}$$

Definition 3.4.20. *Let $f : C \to S$ be a morphism of schemes. Then f is* separated *if the diagonal morphism Δ_f is a closed immersion.*

Proposition 3.4.21. *[Har77, p. 96, ch. II, Corollary 4.2] [Har77, p. 175, ch. II] Let $f : C \to S$ be a morphism of schemes. Then f is separated if, and only if, the image of Δ_f is closed in $C \times_S C$. Moreover, in any case the image is locally closed, i. e. it is the intersection of a closed with an open set.*

Definition 3.4.22. *[GD67, p. 226(322), Définition 1.2.1] Let $f : X \to Y$ be a morphism of schemes. Then f is said to be* quasi-separated *if the diagonal morphism $\Delta_f : X \to X \times_Y X$ is quasi-compact.*

Remark 3.4.23. If $f : X \to Y$ is separated, then according to [GD67, p. 226(322), following Définition 1.2.1] it is also quasi-separated.

Morphisms of Finite Type, Finite Morphisms In classical algebraic geometry a morphism between varieties is called finite if every preimage of a point is finite. See also [EH00, p. 92].

Definition 3.4.24. *Let $f : C \to S$ be a morphism of schemes.*

(a) *Then f is* locally of finite type *if S can be covered by open affine subsets $V_i = \operatorname{Spec} R_i$, such that for every i the preimage $f^{-1}(V_i)$ can be covered by open affine subsets $U_{ij} = \operatorname{Spec} S_{ij}$, such that S_{ij} is a finitely generated R_i-algebra.*

(b) *Then f is* of finite type *if it is locally of finite type and, additionally, for every i, the preimage $f^{-1}(V_i)$ can be covered with finitely many such subsets.*

(c) *Then f is* finite *if S can be covered by open affine subsets $V_i = \operatorname{Spec} R_i$, such that for every i the preimage $f^{-1}(V_i)$ is again an open affine subset* $\operatorname{Spec} S_i$, *where S_i is a finite*[2] *R_i-algebra.*

The notion of being of finite presentation ensures that if given a scheme X over a base S, we have that X can locally on S be described with a finite number of polynomials.

Definition 3.4.25. *[GD67, p. 230(326), Définition 1.4.2 and p. 234(330), Définition 1.6.1] Let $f : X \to Y$ be a morphism of schemes.*

(a) *Let $x \in X$ be a point and let $y = f(x)$. Then f is of* finite presentation at x *if there exists an open affine neighborhood $V = \operatorname{Spec} R$ of y and an open affine neighborhood $U = \operatorname{Spec} S$ of x, such that $f(U) \subseteq V$ and S is an R-algebra of finite presentation.*

(b) *We say that f is* locally of finite presentation *if it is of finite presentation at all points $x \in X$.*

(c) *We say that f is* of finite presentation *if:*

   (i) *the morphism f is locally of finite presentation;*

   (ii) *the morphism f is quasi-compact; and*

   (iii) *the morphism f is quasi-separated.*

Remarks 3.4.26. Let $f : X \to Y$ be a morphism of schemes.

(a) [GD67, p. 230(326), Définition 1.4.2] If Y is locally Noetherian, then f is locally of finite type if, and only if, f is locally of finite presentation.

(b) [GD67, p. 234(330), Définition 1.6.1] If f is locally of finite presentation, then f is quasi-compact if, and only if, it is of finite type.

[2] An R-algebra S is *finite* if it is a finitely generated R-module.

Proper Morphisms Proper morphisms correspond to being compact (for more details see [EH00, pp. 93ff]). In fact they are a generalization of being projective, a notion we introduce in the next paragraph.

Definition 3.4.27. *Let $f : C \to S$ be a morphism.*

(a) *We say that f is* closed *if the the image of any closed subset is closed.*

(b) *We say f is* universally closed *if it is closed and for any base extension $T \to S$ the corresponding morphism $f_T : C_T \to T$ is also closed.*

(c) *The morphism f is* proper *if it is:*

  (i) *separated;*

  (ii) *of finite type; and*

  (iii) *universally closed.*

Proposition 3.4.28. *[Iit82, p. 169, Theorem 3.1] Let S be a finitely generated graded R-algebra. Then $\operatorname{Proj} S \to \operatorname{Spec} R$ is proper.*

Projective Morphisms If a scheme is projective about a base, this simply means that it can be embedded as a closed subscheme into projective space over this base. This corresponds to being a projective variety.

Definition 3.4.29. *Let $f : X \to Y$ be a morphism of schemes.*

(a) *Then f is* projective *if there exists a closed immersion $\iota : X \to \mathbb{P}^n_Y$ for an $n \in \mathbb{N}_{>0}$, such that $f = g \circ \iota$ where $g : \mathbb{P}^n_Y \to Y$ is the canonical projection.*

(b) *The morphism f is* quasi-projective *if it can be factored as an open immersion $X \to X'$ followed by a projective morphism $X' \to Y$.*

Remarks 3.4.30.

(a) This definition is from [Har77, p. 103, ch. II], and there it is noted that this definition of a projective morphism is slightly different from the one in [GD61, 5.5], and that the two definitions are equal if there is a quasi-projective morphism $Y \to \operatorname{Spec} R$ for a ring R.

(b) Clearly a projective morphism is quasi-projective.

Proposition 3.4.31. *[Har77, p. 103, ch. II, Theorem 4.9]*

(a) *A projective morphism of Noetherian schemes is proper.*

(b) *A quasi-projective morphism of Noetherian schemes is of finite type and separated.*

We next want to give a result which allows to describe morphisms into projective space over a ring and, therefore, also into schemes which are projective over a ring.

Definition 3.4.32. *Let X be a scheme and $\mathcal{F}$ an $\mathcal{O}_X$-module. If $s_1, \dots, s_n \in \Gamma(X, \mathcal{F})$ are global sections, we say $s_1, \dots, s_n$* (locally) generate $\mathcal{F}$ *if $\mathcal{F}_x$ is generated by $s_{1,x}, \dots, s_{n,x}$ as an $\mathcal{O}_{X,x}$-module for every point $x \in X$.*

Proposition 3.4.33. *[Har77, p. 150, ch. II, Theorem 7.1] Let R be a ring and X be a scheme over R.*

(a) *If $\varphi : X \to \mathbb{P}^n_R$ is an R-morphism, then $\varphi^*(\mathcal{O}_{\mathbb{P}^n_R}(1))$ is an invertible sheaf on X, which is generated by the global sections $s_i = \varphi^*(x_i)$, $i = 0, \dots, n$.*

(b) *Conversely, if $\mathcal{L}$ is an invertible sheaf on X, and $s_0, \dots, s_n \in \Gamma(X, \mathcal{L})$ are global sections that generate $\mathcal{L}$, then there exists a unique R-morphism $\varphi : X \to \mathbb{P}^n_R$, such that $\mathcal{L} \cong \varphi^*(\mathcal{O}_{\mathbb{P}^n_R}(1))$ and $s_i = \varphi^*(x_i)$ under this isomorphism.*

We will now show that Proj indeed generalizes projective varieties in the sense that $\operatorname{Proj} S$ is projective over $\operatorname{Spec} R$ if S is a graded R-algebra.

Proposition 3.4.34. *[Har77, pp. 80f, ch. II, Exercise 2.14 (b) and pp. 92f, ch. II, Exercise 3.12 (a)] Let S and T be graded rings, and $\varphi : S \to T$ a graded surjective morphism of graded rings. Then φ induces a closed immersion $f : \operatorname{Proj} T \to \operatorname{Proj} S$.*

Corollary 3.4.35. *Let R be a ring, $S = R[x_0, \dots, x_n]$, $\mathfrak{a}$ be a homogenous ideal in S, $T = S/\mathfrak{a}$, and $\varphi : S \to T$ be the canonical projection. Then the corresponding morphism $\operatorname{Proj} T \to \operatorname{Spec} R$ is projective. If R is Noetherian, then so are $\operatorname{Proj} T$ and $\operatorname{Spec} R$.*

Proof. The previous proposition gives a closed immersion $\operatorname{Proj} T \to \operatorname{Proj} S = \mathbb{P}^n_R$ and, therefore, $\operatorname{Proj} T \to \operatorname{Spec} R$ (given by Lemma 3.3.26) is projective. If R is Noetherian, clearly $\operatorname{Spec} R$ is Noetherian. Since $\operatorname{Proj} T$ can be covered by the open sets $D_+(\varphi(x_i))$, $0 \le i \le n$, and $T_{(\langle \varphi(x_i) \rangle)}$ is Noetherian by Corollary 2.2.16 and Proposition 2.3.5, then $\operatorname{Proj} T$ is also Noetherian. □

Flat Morphisms Recall that a morphism $X \to Y$ can be seen as a parameterization of X by Y. If the morphism is flat, one can show that the fibres have 'much in common' (for details see for example [EH00, pp. 70–81]). We will not describe this in more detail.

Definition 3.4.36. *Let $f : X \to Y$ be a morphism.*

(a) *If $\mathcal{F}$ is an $\mathcal{O}_X$-module and $p \in X$ a point, we say that $\mathcal{F}$* is flat over Y at a point x *if the stalk $\mathcal{F}_x$ is a flat $\mathcal{O}_{Y,f(x)}$-module, where we consider $\mathcal{F}_x$ as an $\mathcal{O}_{Y,f(x)}$-module via the natural map $f^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ (note also Remark 2.6.35).*

(b) *If $\mathcal{F}$ is an $\mathcal{O}_X$-module, we say $\mathcal{F}$* is flat over Y *if it is flat at every point of X.*

(c) *We say X* is flat over Y *or f* is flat *if $\mathcal{O}_X$ is flat over Y.*

Proposition 3.4.37. *[Har77, p. 254, ch. II, Proposition 9.2]. Let $A \to B$ be a ring morphism, and M an B-module. Let $\operatorname{Spec} B \to \operatorname{Spec} A$ be the corresponding morphism of affine schemes, and $\mathcal{F} = \tilde{M}$. Then $\mathcal{F}$ is flat over $\operatorname{Spec} A$ if and only if M is flat over A.*

Smooth Morphisms Being smooth generalizes the notion of smooth varieties. This will become clear in Theorem 3.4.41. First we define when a morphism is of relative dimension n.

Definition 3.4.38. *[Har77, p. 268, ch. III, Definition] Let $f : X \to Y$ be a morphism of schemes. Then f is* of relative dimension k *if for every irreducible component $X' \subseteq X$ and $Y' \subseteq Y$, such that $f(X') \subseteq Y'$, we have $\dim X' = \dim Y' + k$.*

Next we define when a morphism is smooth. Note that this definition is very technical and we will not use it directly.

Definition 3.4.39. *Let $f : X \to Y$ be a morphism of schemes.*

(a) *[GD67, p. 56, Définition 17.1.1] Then f is* formally smooth *if the following condition holds:*

Let Y' be an arbitrary affine scheme and Y'_0 the closed subscheme of Y' defined by a nilpotent sheaf of ideals $\mathscr{I}$ of $\mathcal{O}_{Y'}$. Let $\iota : Y'_0 \to Y'$ be the embedding. Then the map

$$\mathcal{H}om_Y(Y', X) \to \mathcal{H}om_Y(Y'_0, X), \qquad g \mapsto g \circ \iota$$

is surjective. (Here nilpotent means that every ideal $\mathscr{I}(U)$ in $\mathcal{O}_{Y'}(U)$ is nilpotent, $U \in \mathbb{U}_{Y'}$.)

(b) *[GD67, p. 61, Définition 17.3.1] We call f* smooth *if it is locally of finite presentation and formally smooth.*

Remark 3.4.40. [GD67, p. 68, Corollaire 17.5.2 and before, and pp. 150f, Corollaire 6.7.8 and Définition 6.8.1] Let $f : X \to Y$ be a morphism of schemes. Then f is smooth if, and only if, all of the following conditions hold:

(i) The morphism f is flat;

(ii) The morphism f is of locally finite presentation;

(iii) For every $y \in Y$, the fibre X_y over $k(y)$ is a locally Noetherian scheme; and

(iv) For every $x \in X$, the fibre $X_{f(x)}$ over $k(f(x))$ is a regular scheme.

In particular if $f : X \to \operatorname{Spec} \mathbb{F}$ is a smooth morphism of schemes for a field $\mathbb{F}$, then $\mathcal{O}_{X,x}$ is a local regular ring for every $x \in X$.

The following theorem gives a very useful characterization of being smooth for morphisms which are of finite type. Combined with the Jacobian criterion, Theorem 3.2.28, this will be the way we use to show that a morphism is smooth.

Theorem 3.4.41. *[Mum99, p. 221, Theorem 3'] Let X, Y be schemes and $f : X \to Y$ be a morphism of finite type. Then f is smooth of relative dimension k if, and only if, f is flat and all its geometric fibres are disjoint unions of k-dimensional smooth varieties.*

3.5 Categories, Divisors and Differentials

This section contains advanced material from the Theory of Schemes. In the first subsection we will consider several categories which appear in the Theory of Schemes and describe equivalences between some of them.

In the next subsection we discuss the concept of divisors, which are very important in the study of elliptic curves. In the last subsection we give an overview over differentials and relative differentials. In the case of schemes over fields, they can be used to characterize smoothness.

3.5.1 Equivalences of Categories

We consider the following categories:

(a) The category $\mathscr{A}\!f\!f$ of affine schemes;

(b) The category $\mathscr{R}ing$ of rings (as always commutative and with a unit);

(c) The category $\mathscr{V}ar(\mathbb{F})$ of varieties over a field $\mathbb{F}$;

(d) The category $\mathscr{S}ch(S)$ of schemes over S;

(e) The category $\mathscr{M}od(R)$ of R-modules; and

(f) The category $\mathscr{Q}\mathscr{C}oh(\mathcal{O}_X)$ of quasi-coherent $\mathcal{O}_X$-modules.

Proposition 3.5.1. *The category of affine schemes and the category of rings are equivalent, where the equivalence is given by the contravariant functors*

$$\mathscr{R}ing \to \mathscr{A}\!f\!f, \qquad R \mapsto \operatorname{Spec} R$$

and

$$\mathscr{A}\!f\!f \to \mathscr{R}ing, \qquad X \mapsto \Gamma(X, \mathcal{O}_X).$$

Proposition 3.5.2. *Let $R \to S$ be a morphism of rings, $X = \operatorname{Spec} R$, $Y = \operatorname{Spec} S$ and $f : Y \to X$ the corresponding morphism of schemes.*

(a) *[Har77, p. 113, Corollary 5.5] The assignment $M \mapsto \tilde{M}$ gives an equivalence of categories between the category of R-modules and the category of quasi-coherent $\mathcal{O}_X$-modules:*

$$\mathscr{M}od(R) \to \mathscr{Q}\mathscr{C}oh(\mathcal{O}_X), \qquad M \mapsto \tilde{M}$$

and,

$$\mathscr{Q}\mathscr{C}oh(\mathcal{O}_X) \to \mathscr{M}od(R), \qquad \mathcal{F} \mapsto \Gamma(X, \mathcal{F}).$$

Moreover both functors are exact [Har77, p. 113, ch. II, Proposition 5.6].

(b) *[Har77, p. 110, Proposition 5.2(a)] If N is a S-module, and N_R the interpretation of N as an R-module using the map $R \to S$, then*

$$f_*\tilde{N} \cong \widetilde{N_R}.$$

(c) *[Har77, p. 110, Proposition 5.2(a)] If M is an R-module, then*

$$f^*\tilde{M} \cong \widetilde{M \otimes_R S}.$$

Corollary 3.5.3. *Let X be a scheme. A locally free sheaf $\mathcal{F}$ on X is quasi-coherent. If $\mathcal{F}$ is locally free of rank n and $X = \operatorname{Spec} R$, then $\mathcal{F} \cong \tilde{M}$ for a projective R-module of rank n.*

This in particular implies that $\operatorname{Pic}(\operatorname{Spec} R)$ corresponds to the set of isomorphism classes of projective R-modules of rank one, i. e. we have a natural bijection $\operatorname{Pic}(R) \cong \operatorname{Pic}(\operatorname{Spec} R)$ where $\operatorname{Pic}(R)$ is the Picard group of R as defined in Definition 2.4.15.

Proof. The first statement is clear. The second statement follows directly from Proposition 3.5.2 (b) and Proposition 2.4.16. □

Proposition 3.5.4. *[Har77, p. 78, ch. II, Proposition 2.6] Let $\mathbb{F}$ be an algebraically closed field. There is a natural, fully faithful functor from the category of varieties over $\mathbb{F}$ to the category of schemes over $\operatorname{Spec} \mathbb{F}$*

$$\mathscr{V}\!ar(\mathbb{F}) \to \mathscr{S}\!ch(\operatorname{Spec} \mathbb{F}).$$

If V is a variety and X the associated scheme, then the set of closed points of X is homeomorphic to the topological space of V. Moreover, the sheaf of regular functions on V is obtained by restricting the structure sheaf $\mathcal{O}_X$ by this homeomorphism. In particular, if the homeomorphism is induced by $\alpha : V \to X$, then $\mathcal{O}_X = \alpha_* \mathcal{O}_V$.

[Har77, p. 104, ch. II, Proposition 4.10] The image of this functor in $\mathscr{S}\!ch(\operatorname{Spec} \mathbb{F})$ is exactly the class of quasi-projective integral schemes over $\mathbb{F}$. The image of the class of projective varieties is exactly the class of projective integral schemes over $\mathbb{F}$.

Remarks 3.5.5.

(a) On affine varieties V the functor works as follows: if $A = \mathbb{F}[V]$ is the affine coordinate ring of V, then the associated $\mathbb{F}$-scheme is $\operatorname{Spec} A$. Each point $x \in V$ is mapped to the maximal ideal $\mathfrak{m}_x$ of A, i. e. the regular functions on V vanishing in x.

(b) On projective varieties V the functor works as follows: if $A = \mathbb{F}[V]$ is the homogenous coordinate ring of V, then the associated $\mathbb{F}$-scheme is $\operatorname{Proj} A$. Each point $x \in V$ is mapped to prime ideal $\big\langle \{f \in A^h \mid f(x) = 0\} \big\rangle$.

3.5.2 Divisors

There are two kinds of divisors: Weil divisors and Cartier divisors. Weil divisors can only be used for special schemes; in some cases Weil and Cartier divisors coincide. This is, for example, the case for smooth varieties over fields. For schemes over rings, which are required to discuss elliptic curves over rings, we need Cartier divisors. Before starting with divisors, we want to introduce a concept generalizing the concept of the function field of a variety.

Proposition 3.5.6. *[Har77, p. 91, ch. II, Exercise 3.6] Let X be an integral scheme and $x \in X$ its generic point. Then $K(X) := \mathcal{O}_{X,x}$ is a field, and for every affine open subset $U = \operatorname{Spec} R$, the field of fractions of R is isomorphic to $K(X)$.*

Definition 3.5.7. *Let X be an integral scheme. Then $K(X)$ from the previous proposition is called the* function field *of X.*

If X is a scheme which is not integral, we can proceed as follows:

Definition 3.5.8. *Let X be any scheme. For each $U \in \mathbb{U}_X$, let $S_X(U)$ be the elements of $\Gamma(U, \mathcal{O}_X)$, whose image is not a zero-divisor in every local ring $\mathcal{O}_{X,x}$, $x \in U$. Then*

$$U \mapsto S_X(U)^{-1}\Gamma(U, \mathcal{O}_X)$$

defines a presheaf, and the sheaf associated to it is called the sheaf of total quotient rings*, denoted by $\mathcal{K}_X$.*

Lemma 3.5.9. *[Har77, p. 140f, ch. II] Let X be a scheme and $U = \operatorname{Spec} R$ an affine open set. Then $\mathcal{K}_X(U)$ is isomorphic to the total quotient ring of R.*

The following proposition, together with Propositions 3.2.17, 3.2.18 and 3.5.4, shows that this concept is indeed a generalization of the function field of a variety.

Proposition 3.5.10. *[Har77, p. 145, ch. II, in the proof of Proposition 6.15] Let X be an integral scheme. Then $\mathcal{K}_X$ is the constant sheaf given by the function field of X, $K(X)$.*

Weil Divisors Compared to Cartier divisors, which we will define later, Weil divisors are simpler to work with and easier to understand. We first specify for which kind of schemes we define Weil divisors.

Definition 3.5.11. *A scheme X is* regular in codimension one *if every local ring $\mathcal{O}_{X,x}$ of X of dimension one is regular.*

In this paragraph we will only consider

$$\begin{array}{c}\textit{noetherian integral separated schemes}\\ \textit{which are regular in codimension one.}\end{array} \tag{$*$}$$

These are, for example, smooth varieties over a field [Har77, p. 130, ch. II].

Definition 3.5.12. *Let X be a scheme satisfying $(*)$.*

(a) *A* prime (Weil) divisor $[Y]$ *on X is a closed integral subscheme Y of codimension one.*

(b) *The* group of Weil divisors $\operatorname{WDiv}(X)$ *is the free Abelian group generated by the prime divisors on X.*

(c) *An* effective divisor *is a divisor $D = \sum n_Y[Y] \in \operatorname{WDiv}(X)$, such that for every prime divisor Y, $n_Y \geq 0$.*

Remark 3.5.13. If Y is a prime divisor on a scheme X satisfying $(*)$, then Y is irreducible. Assume $y \in Y$ is its generic point. Then $\mathcal{O}_{X,y}$ is a discrete valuation ring with quotient field K, being the same as the function field $K(X)$ of X.

Using this we can define the order of a rational function on X in a prime divisor.

Definition 3.5.14. *Let X be a scheme satisfying (*), Y a prime divisor of X and $f \in K(X)^*$. If $y \in Y$ is the generic point of Y, then the* valuation *induced by $\mathcal{O}_{X,y}$ on $K(X)^*$ is denoted by* ord_Y. *Therefore,* $\operatorname{ord}_Y : K(X)^* \to \mathbb{Z}$ *is a group morphism; if* $\operatorname{ord}_Y(f) < 0$, *one says f has a* pole *in Y; if* $\operatorname{ord}_Y(f) > 0$, *one says f has a* zero *in Y.*

We can use the order of a rational function at a prime divisor to define a divisor for a rational function. We first have to show that this is well-defined:

Proposition 3.5.15. *[Har77, p. 131, ch. II, Lemma 6.1] Let X be a scheme satisfying (*) and $f \in K(X)^*$. Then*

$$\operatorname{div}(f) := \sum \operatorname{ord}_Y(f)[Y]$$

is a well-defined Weil divisor on X. Moreover, if $g \in K(X)^*$ is another function, then $\operatorname{div}(f/g) = \operatorname{div}(f) - \operatorname{div}(g)$. *Therefore* $\operatorname{div} : K(X)^* \to \operatorname{WDiv}(X)$ *is a group homomorphism.*

Definition 3.5.16. *Let X be a scheme satisfying (*). A divisor of the form* $\operatorname{div}(f)$ *for an $f \in K(X)^*$ is called* principal. *Two divisors $D, D' \in \operatorname{WDiv}(X)$ are called* linearly equivalent *if $D - D'$ is principal. The* divisor class group *of X, denoted by* $\operatorname{Cl}(X)$, *is the quotient of* $\operatorname{WDiv}(X)$ *by the subgroup of principal divisors.*

Remark 3.5.17. Let X be a scheme satisfying $(*)$. Let K^* be the kernel of div. Then we have the following exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & K^* \arrow[r, hook] & K(X)^* \arrow[r, "f \mapsto \operatorname{div}(f)"] & \operatorname{WDiv}(X) \arrow[r, two heads] & \operatorname{Cl}(X) \arrow[r] & 0. \end{tikzcd}$$

We will look at Weil divisors on curves in section 3.7.4, and for that case we will also explicitly describe what K^* is.

Cartier Divisors Cartier divisors are technically more complicated than Weil divisors but contrary to Weil divisors they can be defined for every scheme. Cartier divisors are locally divisors of a function, hence locally principal. There is also the notion of a relative Cartier divisor, which is needed if one considers parameterizations $X \to Y$. In this case, a relative Cartier divisor can be seen as a family of Cartier divisors on the fibres.

Definition 3.5.18. *Let X be a scheme. The* group of Cartier divisors $\operatorname{CDiv}(X)$ *on X is the quotient sheaf $\mathcal{K}_X^*/\mathcal{O}_X^*$, and an element of it is called a* Cartier divisor. *We will write the group operation additively instead of multiplicatively.*

A Cartier divisor is principal *if it is in the image of the canonical map $\mathcal{K}_X^* \to \mathcal{K}_X^*/\mathcal{O}_X^*$. Two Cartier divisors are* linearly equivalent *if their difference is principal. The group of Cartier divisors factored by the subgroup of principal Cartier divisors is called the* Cartier divisor class group, *denoted by* $\operatorname{CaCl}(X)$.

Remark 3.5.19. [Har77, p. 141, ch. II] Let X be a scheme. A Cartier divisor on X can be described as a covering U_i, $i \in I$ of X and elements $f_i \in \mathcal{K}_X^*(U_i)$, $i \in I$, such that for two $i, j \in I$ we have $f_i/f_j \in \mathcal{O}_X^*(U_i \cap U_j)$.

This explains why Cartier divisors are called locally principal divisors: for every point $x \in X$ there is a neighborhood $U \in \mathbb{U}_{X,x}$ on which the divisor is principal. We will now give a result which shows that Weil and Cartier divisors coincide in one case:

Proposition 3.5.20. *[Har77, p. 141, ch. II, Proposition 6.11] Let X be an integral, separated Noetherian scheme, such that all local rings are unique factorization domains. Then* $\mathrm{WDiv}(X) \cong \mathrm{CDiv}(X)$*, and this isomorphism respects linearly equivalence and the property of being principal.*

Remark 3.5.21. [Har77, p. 142, ch. II, Remark 6.11.1A] The assumptions of the proposition are satisfied by every regular, integral, separated Noetherian scheme, where regular means that all local rings are regular.

Next we will define a map from $\mathrm{CDiv}(X)$ into $\mathrm{Pic}(X)$.

Definition 3.5.22. *[Har77, p. 144, ch. II] Let X be a scheme and $D \in \mathrm{CDiv}(X)$, represented by $(U_i, f_i)_{i \in I}$. Define a subsheaf $\mathcal{L}(D)$, the* sheaf associated to D*, of $\mathcal{K}_X$ by taking the sub-$\mathcal{O}_X$-module of $\mathcal{K}_X$ generated by f_i^{-1} on U_i, $i \in I$.*

Proposition 3.5.23. *[Har77, p. 144, ch. II, Proposition 6.13] Let X be a scheme.*

(a) *The map $D \mapsto \mathcal{L}(D)$ gives a one-to-one correspondence between* $\mathrm{CDiv}(X)$ *and invertible subsheaves of $\mathcal{K}_X$.*

(b) *For two divisors $D, D' \in \mathrm{CDiv}(X)$ we have $\mathcal{L}(D - D') \cong \mathcal{L}(D) \otimes \mathcal{L}(D')^{-1}$.*

(c) *Two divisors $D, D' \in \mathrm{CDiv}(X)$ are linearly equivalent if, and only if, $\mathcal{L}(D) \cong \mathcal{L}(D')$, where the isomorphism is in the category $\mathscr{M}od(\mathcal{O}_X)$, i. e. not taking into account the embedding into $\mathcal{K}_X$.*

Corollary 3.5.24. *[Har77, p. 144, ch. II, Corollary 6.14] If X is a scheme, the map $D \mapsto \mathcal{L}(D)$ gives an injective morphism from* $\mathrm{CaCl}(X)$ *into* $\mathrm{Pic}(X)$*.*

For certain schemes, this map is a bijection:

Proposition 3.5.25. *[Har77, p. 145, ch. II, Proposition 6.15] Let X be an integral scheme. Then* $\mathrm{CaCl}(X)$ *is isomorphic to* $\mathrm{Pic}(X)$*.*

Corollary 3.5.26. *[Har77, p. 145, ch. II, Corollary 6.16] If X is a Noetherian, integral, separated scheme, such that all local rings are unique factorization domains, then* $\mathrm{Cl}(X) \cong \mathrm{Pic}(X)$*.*

The next result simply states that the Picard group is functorial:

Proposition 3.5.27. *[Har77, p. 148, ch. II, Exercise 6.8(a)] Let $f : X \to Y$ be a morphism of schemes. Then*

$$\mathcal{L} \mapsto f^* \mathcal{L}$$

induces a morphism of Picard groups $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$.

We next want to define what an effective Cartier divisor is. We will see that in the above case, where $\mathrm{CDiv}(X)$ and $\mathrm{WDiv}(X)$ coincide, the notion of being effective is also the same for both kinds of divisors.

Definition 3.5.28. *Let X be a scheme and $D \in \mathrm{CDiv}(X)$ represented by $(U_i, f_i)_{i\in I}$. Then D is* effective *if $f_i \in \mathcal{O}_X^*(U_i)$ for all $i \in I$.*

Remark 3.5.29. [Har77, p. 145, ch. II, Remark 6.17] If X is a Noetherian, integral, separated scheme, such that all local rings are unique factorization domains, then the isomorphism $\mathrm{WDiv}(X) \cong \mathrm{CDiv}(X)$ from Proposition 3.5.20 respects the property of being effective.

There is a close connection between effective Cartier divisors on a scheme X and special closed subschemes of X:

Definition 3.5.30. *Let X be a scheme and D an effective Cartier divisor, given by $(U_i, f_i)_{i\in I}$. The* associated subscheme of codimension one *of D is the closed subscheme defined by the sheaf of ideals in $\mathcal{O}_X$ which is locally generated by the f_i's.*

Proposition 3.5.31. *[Har77, p. 145, ch. II, Proposition 6.18] Let X be a scheme, D be an effective Cartier divisor, and Y be its associated closed subscheme. Then $\mathscr{I}_Y \cong \mathcal{L}(-D) \cong \mathcal{L}(D)^{-1}$.*

Remark 3.5.32. An effective Cartier divisor is uniquely determined by the associated closed subscheme. Moreover, every locally principal closed subscheme determines a unique effective Cartier divisor (see [Har77, p. 145, ch. II, Remark 6.17.1]).

We will now define relative effective Cartier divisors and state some results. We will later use relative effective Cartier divisors for describing the group law on a generalized elliptic curve.

Definition 3.5.33. *Let X be a scheme over S, and D an effective Cartier divisor on X. Then D is* relative *if the associated closed subscheme of D is flat over S.*

Remarks 3.5.34.

(a) By using the fact that there is a one-to-one correspondence between effective Cartier divisors and locally principal closed subschemes, one can also define a relative effective Cartier divisor (as in [KM85, p. 1, Definition 1.1.1]) by the following:

A relative effective Cartier divisor D of X/S is a closed subscheme of X which is flat over S, and whose ideal sheaf $\mathscr{I}_D \subseteq \mathcal{O}_X$ is an invertible $\mathcal{O}_X$-module.

(b) [KM85, p. 3, Remark 1.1.1] The conditions for a closed subscheme D being an relative effective Cartier divisor is local on S in the sense that if $\operatorname{Spec} R$ is an open affine subset, one must be able to cover $f^{-1}(\operatorname{Spec} R)$ with open affine $U_i = \operatorname{Spec} A_i$ such that A_i is an R-algebra, $D \cap U_i$ is locally defined by one $f_i \in A_i$, and f_i is a non-zero-divisor in A_i and $A_i/\langle f\rangle$ is flat over R. (Here $f : X \to S$ is the structure morphism.)

Proposition 3.5.35. *Let X be a scheme over S.*

(a) *[KM85, pp. 3f, Remark 1.1.2] The sum of two relative effective Cartier divisors is again a relative effective Cartier divisor.*

(b) *[KM85, p. 4, Remark 1.1.3] Let D be an relative effective Cartier divisor. Then there is a tautological exact sequence*

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{O}_X \arrow[r] & \mathscr{I}_D^{-1} \arrow[r] & \mathscr{O}_D \otimes_{\mathscr{O}_X} \mathscr{I}_D^{-1} \arrow[r] & 0 \end{tikzcd},$$

and the image of $1 \in \mathscr{O}_X$ in $\mathscr{I}_D^{-1}$, denoted by ℓ_D, allows to recover D from $(\mathscr{I}_D^{-1}, \ell_D)$ as the scheme of zeros of $\ell_D \in \mathscr{I}_D^{-1}$.

(c) *[KM85, pp. 4f, Remark 1.1.3] The procedure in (b) gives a one-to-one correspondence between the following sets:*

(1) *Isomorphism classes of tuples $(\mathcal{L}, \ell)$, where $\ell \in \Gamma(X, \mathcal{L})$ is a global section such that*

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{O}_X \arrow[r, "f \mapsto f\ell"] & L \arrow[r] & \mathcal{L}/\mathscr{O}_X \arrow[r] & 0 \end{tikzcd}$$

is exact, and that $\mathcal{L}/\mathscr{O}_X$ is flat over S. Here two tuples $(\mathcal{L}, \ell)$ and $(\mathcal{L}', \ell')$ are said to be isomorphic if $\mathcal{L} \cong \mathcal{L}'$ and ℓ is mapped onto ℓ' by this isomorphism.

(2) *The set of relative effective Cartier divisors on X/S.*

If $D_i \mathrel{\hat{=}} (\mathcal{L}_i, \ell_i)$ are relative effective Cartier divisors on X/S, then $D_1 + D_2 \mathrel{\hat{=}} (\mathcal{L}_1 \otimes \mathcal{L}_2, \ell_1 \otimes \ell_2)$.

(d) *[KM85, p. 5, Remark 1.1.4] Let D be a relative effective Cartier divisor on X/S, represented by $(\mathcal{L}, \ell)$.*

(1) *Let $T \to S$ be any morphism of schemes. Then D_T is a relative effective Cartier divisor on X_T/T, represented by $(\mathcal{L}_T, \ell_T)$, where ℓ_T is the image of ℓ under the projection $\mathscr{O}_{\mathcal{L}} \to \mathscr{O}_{\mathcal{L}_T}$.*

(2) *Let $f : Y \to X$ be a flat S-morphism of S-schemes. Then f^*D is a relative effective Cartier divisor on Y/S.*

(e) *[KM85, p. 7, Corollary 1.1.5.2] Let S be locally Noetherian and $X \to S$ of finite type. Let D be a closed subscheme which is flat over X. Then D is a relative effective Cartier divisor if, and only if, for all geometric points $\operatorname{Spec} \mathbb{F} \to S$ of S the closed subscheme $D_{\operatorname{Spec} \mathbb{F}}$ of $X_{\operatorname{Spec} \mathbb{F}}$ is a relative effective Cartier divisor on $X_{\operatorname{Spec} \mathbb{F}} / \operatorname{Spec} \mathbb{F}$.*

The next two results emphasize the local nature of relative effective Cartier divisors:

Proposition 3.5.36. *Let X be a scheme over S with structure morphism $f : X \to S$, which is of finite presentation, and let D be a closed subscheme of X. Then the following are equivalent:*

(i) *The ideal sheaf $\mathscr{I}_D$ is invertible and D is flat over S, i. e. D is a relative effective Cartier divisor.*

(ii) *We have that X is flat over S, and for every $s \in S$ the restriction D_s of D onto the fibre X_s over s is an effective Cartier divisor on X_s.*

Proof. This follows directly from [BLR90, p. 213, Lemma 6]. Note also [MFK65, p. 24, e)]. □

Proposition 3.5.37. *Let X be a scheme over S with structure morphism $f : X \to S$, which is of finite presentation. Let D be a relative effective Cartier divisor on X over S. If U is an open subset of S and $V = f^{-1}(U)$, then $D|_V$ is a relative effective Cartier divisor on $X|_V$ over $S|_U$.*

Proof. This follows directly from Remark 3.5.32 and the local nature of flatness. □

3.5.3 Differentials

Kähler differentials play the role of differential forms on manifolds; they can be used to characterize smoothness in certain contexts. We also need the Kähler differentials to define what canonical divisors are on smooth varieties over fields.

Definition 3.5.38. *Let X be a scheme over S with structure morphism $f : X \to S$, and let $\Delta_f : X \to X \times_S X$ be the diagonal morphism. Let W be the open subscheme of $X \times_S X$, such that $\Delta_f(X)$ is a closed subscheme of W (see Proposition 3.4.21), and let $\mathscr{I}$ be the ideal sheaf of $\Delta_f(X)$ in W. Define $\Omega_{X/S} := \Delta_f^*(\mathscr{I}/\mathscr{I}^2)$ to be the* sheaf of relative differentials *of X over S.*

Remarks 3.5.39.

(a) [Har77, p. 175, ch. II, Remark 8.9.1] If $f : X \to S$ is a morphism of sheaves, then $\Omega_{X/S}$ has the structure of an $\mathcal{O}_X$-module. Moreover, it is quasi-coherent.

(b) [Har77, p. 175, ch. II, Remark 8.9.2] Let T be an R-algebra, and $S = \operatorname{Spec} R$, $X = \operatorname{Spec} T$ and $f : X \to S$ the structure morphism. Then $\Omega_{X/S}$ is the $\mathcal{O}_X$-module associated to the T-module $\Omega_{T/R}$. (See Section 2.3.4 for more information about $\Omega_{T/R}$.)

The following result shows how the module of Kähler differentials is connected to a scheme over a field being smooth:

Proposition 3.5.40. *[Har77, p. 177, ch. II, Theorem 8.15] Let X be an irreducible separated scheme of finite type over an algebraically closed field $\mathbb{F}$, and let $n = \dim X$. Then $\Omega_{X/\mathbb{F}}$ is a locally free $\mathcal{O}_X$-module of rank n if, and only if, X is a smooth variety over $\mathbb{F}$.*

Using this one can also define being smooth for a morphism of schemes over a field as follows:

Remark 3.5.41. [Har77, p. 268, ch. III, Definition] Let $f : X \to Y$ be a morphism of schemes of finite type over a field $\mathbb{F}$. Then f is smooth of relative dimension k if, and only if, all of the following conditions hold:

(i) The morphism f is flat;

(ii) The morphism f is of relative dimension k; and

(iii) For every point $x \in X$ we have

$$\dim_{k(x)}(\Omega_{X/Y} \otimes k(x)) = n.$$

Let $\mathbb{F}$ be an algebraically closed field. We will define the tangent sheaf, the canonical sheaf and the geometric genus for a smooth variety over $\mathbb{F}$. The canonical sheaf and the geometric genus will be needed to state the Theorem of Riemann-Roch, which helps computing the dimension of a linear system of a divisor and which is of great importance for showing results for elliptic curves over algebraically closed fields.

Definition 3.5.42. *Let X be a smooth variety over $\mathbb{F}$.*

(a) *The* tangent sheaf *of X is $\mathscr{T}_X := \mathcal{H}om_{\mathcal{O}_X}(\Omega_{X/\mathbb{F}}, \mathcal{O}_X) = \Omega^{\vee}_{X/\mathbb{F}}$.*

(b) *The* canonical sheaf *of X is $\omega_X := \bigwedge^n \Omega_{X/\mathbb{F}}$, the n-th exterior power of $\Omega_{X/\mathbb{F}}$, where $n = \dim X$. (See Definition 2.6.41.)*

(c) *If X is projective, the* geometric genus *of X is $p_g(X) = \dim_{\mathbb{F}} \Gamma(X, \omega_X)$.*

Remark 3.5.43. Let X be a smooth variety over $\mathbb{F}$ of dimension one. Then by Proposition 3.5.40, $\Omega_{X/F} = \omega_X$ is an invertible sheaf. Therefore, by Corollary 3.5.26, it corresponds to a linear equivalence class of Weil divisors on X. The divisors in this class are called *canonical divisors.*

3.6 Affine and Projective Geometry Revisited

In this section we want to inspect how the sets $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$ from the first section and their scheme theoretic counterparts $\mathbb{A}^n_R$ and $\mathbb{P}^n_R$ correspond to each other for several classes of rings R.

Let R be any ring. Recall that the scheme-theoretic affine n-space over R by Definition 3.3.13 is $\mathbb{A}^n_R = \operatorname{Spec} R[x_1, \ldots, x_n]$.

Proposition 3.6.1. *Let $\mathbb{F}$ be an algebraically closed field. Then the closed points of $\mathbb{A}^n_{\mathbb{F}}$ are in a natural one-to-one correspondence with the points in $\mathbb{A}^n(\mathbb{F}) = \mathbb{F}^n$.*

Proof. By Hilbert's Nullstellensatz 3.1.12 the maximal ideals in $\mathbb{F}[x_1, \ldots, x_n]$ are exactly of the form $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for $(a_1, \ldots, a_n) \in \mathbb{F}^n$. □

Remark 3.6.2. If $\mathbb{F}$ is not algebraically closed, or it is a ring, then this is not true.

Proposition 3.6.3. *The R-rational points of $\mathbb{A}^n_R$ are in a natural one-to-one correspondence with the points in $\mathbb{A}^n(R)$.*

Proof. Recall that the R-rational points of $\mathbb{A}^n_R$ are exactly the morphisms $\operatorname{Spec} R \to \mathbb{A}^n_R = \operatorname{Spec} R[x_1, \ldots, x_n]$, which commute with the structure morphism $\mathbb{A}^n_R \to \operatorname{Spec} R$. Since the category of affine schemes is equivalent to the category of rings (see Proposition 3.3.8), these morphisms correspond to ring morphisms $R[x_1, \ldots, x_n] \to R$ being the identity on R. Since every such morphism is uniquely determined by the images of the x_i in R, they clearly are in a one-to-one correspondence with the points in $\mathbb{A}^n(R) = R^n$. □

Next we are interested in the structure of $\mathbb{P}^n_R$, which is by Definition 3.3.25 equal to $\operatorname{Proj} R[x_0, \dots, x_n]$.

Proposition 3.6.4. *Let $\mathbb{F}$ be an algebraically closed field. Then the closed points of $\mathbb{P}^n_{\mathbb{F}}$ are in a natural one-by-one correspondence with the points in $\mathbb{P}^n(\mathbb{F})$.*

Proof. (See also [Har77, p. 77, ch. II, Example 2.5.1].) This follows from Corollary 3.1.13: if $\mathfrak{a}$ is a homogenous ideal not containing the irrelevant ideal, then $V_{\mathbb{F}}(\mathfrak{a})$ contains at least one point in $\mathbb{P}^n(\mathbb{F})$. This implies that the ideals

$$\langle \{a_i x_j - a_j x_i \mid 0 \le i < j \le n\} \rangle = \left\langle \{f \in \mathbb{F}[x_0, \dots, x_n]^h \mid f(a) = 0\} \right\rangle$$

for $a \in \mathbb{P}^n(\mathbb{F})$ are exactly the closed points in $\mathbb{P}^n_{\mathbb{F}}$. □

Proposition 3.6.5. *Let R be a ring with $\operatorname{Pic} R = 0$. (See Corollary 3.5.3.) Then the R-rational points of $\mathbb{P}^n_R$ are in a natural one-to-one correspondence with the points in $\mathbb{P}^n(R)$.*

Proof. If $(a_0, \dots, a_n) \in \mathbb{P}^n(R)$, then the a_i locally generate R as an R-module. Thus, treated as global sections of $\mathcal{O}_{\operatorname{Spec} R}$, they locally generate $\mathcal{O}_{\operatorname{Spec} R}$ and, hence, by Proposition 3.4.33, induce a unique A-rational point in $\mathbb{P}^n_R$. Since two points in $\mathbb{P}^n(R)$ are identified if there exists an R-module automorphism (these are exactly multiplication by a unit) of R mapping one representation onto the other, this shows that every point of $\mathbb{P}^n(R)$ induces a unique R-rational point in $\mathbb{P}^n_R$.

Conversely, let $f : \operatorname{Spec} R \to \mathbb{P}^n(R)$ be an R-rational point. By Proposition 3.4.33 it corresponds to an invertible sheaf on $\operatorname{Spec} R$ and $n+1$ global sections which locally generate it. Since every invertible sheaf is isomorphic to $\mathcal{O}_{\operatorname{Spec} R}$ by assumption, f corresponds to $n+1$ elements of R which locally generate R as an R-module, i. e. they are primitive over R. Moreover, they are unique up to R-automorphisms of R, which are exactly multiplication by units of R. □

We next explicitely construct the R-point morphisms $\operatorname{Spec} R \to \mathbb{A}^n_R$ and $\operatorname{Spec} R \to \mathbb{P}^n_R$ for given points in $\mathbb{A}^n(R)$ and $\mathbb{P}^n(R)$, respectively.

Proposition 3.6.6. *Let $a = (a_1, \dots, a_n) \in \mathbb{A}^n(R)$ be a point. Then the associated R-rational point $f : \operatorname{Spec} R \to \mathbb{A}^n_R$ is defined thus: a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ is mapped onto*

$$\{f \in R[x_1, \dots, x_n] \mid f(a) \in \mathfrak{p}\},$$

and a regular function $g \in \mathcal{O}_{\mathbb{A}^n_R}(U)$ is mapped onto $g(a)$.

Proof. This follows directly from the proof of Proposition 3.6.3. □

Proposition 3.6.7. *Let R be a ring and $a = (a_0 : \cdots : a_n) \in \mathbb{P}^n(R)$ be a point. Then the associated R-rational point $f : \operatorname{Spec} R \to \mathbb{P}^n_R$ is defined thus: a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ is mapped onto*

$$\left\langle \{f \in R[x_0, \dots, x_n]^h \mid f(a) \in \mathfrak{p}\} \right\rangle,$$

and a regular function $g \in \mathcal{O}_{\mathbb{P}^n_R}(U)$ is mapped onto $g(a)$.

Proof. Let $a = (a_0, \ldots, a_n) \in R^{n+1}$. We define a morphism $s_a : \operatorname{Spec} R \to \mathbb{P}^n_R$ thus:

Let $\mathfrak{p} \in \operatorname{Spec} R$. Define

$$\mathfrak{a}_{a,\mathfrak{p}} := \left\langle \{f \in R[x_0, \ldots, x_n]^h \mid f(a) \in \mathfrak{p}\} \right\rangle_{R[x_0,\ldots,x_n]}.$$

One can directly see that $\mathfrak{a}_{a,\mathfrak{p}}$ is a homogenous ideal and also that it is prime if it is not $R[x_0, \ldots, x_n]$. But if $\mathfrak{a}_{a,\mathfrak{p}} = R[x_0, \ldots, x_n]$, then it follows that $\langle a_0, \ldots, a_n \rangle \subseteq \mathfrak{p}$, which cannot be as $\langle a_0, \ldots, a_n \rangle = R$. Hence, $\mathfrak{a}_{a,\mathfrak{p}} \in \operatorname{Proj} R[x_0, \ldots, x_n]$. Define the topological map $s_a : \operatorname{Spec} R \to \mathbb{P}^n_R$ by $\mathfrak{p} \mapsto \mathfrak{a}_{a,\mathfrak{p}}$.

Let $V(\mathfrak{a})$ be a closed set in $\operatorname{Proj} R[x_0, \ldots, x_n]$, where $\mathfrak{a} \subseteq R[x_0, \ldots, x_n]$ is a homogenous ideal. Now we have that

$$\begin{aligned}\mathfrak{p} \in s_a^{-1}(V(\mathfrak{a})) &\iff s_a(\mathfrak{p}) \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{a}_{a,\mathfrak{p}} \iff \forall f \in \mathfrak{a} : f(a) \in \mathfrak{p} \\ &\iff \mathfrak{a}(f) := \{f(a) \mid f \in \mathfrak{a}\} \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\mathfrak{a}(a)),\end{aligned}$$

and hence s_a is continuous.

Now we are left to define $s_a^{\#} : \mathcal{O}_{\mathbb{P}^n_R} \to s_a^* \mathcal{O}_{\operatorname{Spec} R}$. Let $U := \operatorname{Proj} R[x_0, \ldots, x_n] \setminus V(\mathfrak{a})$ be an open set in $\mathbb{P}^n_R$, with $\mathfrak{a} \subseteq R[x_0, \ldots, x_n]$ a homogenous ideal. As we have already seen, $s_a^{-1}(U) = \operatorname{Spec} R \setminus V(\mathfrak{a}(a))$. Let $(s_a^{(\mathfrak{p})})_{\mathfrak{p} \in U} \in \prod_{\mathfrak{p} \in U} R[x_0, \ldots, x_n]_{(\mathfrak{p})}$ be an element of $\mathcal{O}_{\mathbb{P}^n_R}(U)$; we define its image $s_a^{\#}((s^{(\mathfrak{p})})_{\mathfrak{p} \in U})$ as

$$(s^{(\mathfrak{a}_{a,\mathfrak{p}})}(a))_{\mathfrak{p} \in s_a^{-1}(U)},$$

where

$$\frac{s}{f}(a) = \frac{s(a)}{f(a)} \in R_{\mathfrak{p}} \qquad \text{if} \qquad \frac{s}{f} \in R[x_0, \ldots, x_n]_{(\mathfrak{a}_{a,\mathfrak{p}})}.$$

We first need to check whether this is well-defined. As s and f are homogenous of the same degree, the fraction $\frac{s(a)}{f(a)} \in R_{\mathfrak{p}}$ is well-defined if $f(a) \notin \mathfrak{p}$. But this is the case since $f \notin \mathfrak{a}_{a,\mathfrak{p}}$.

Finally one must check that $f \circ s_a = \mathbf{id}_{\operatorname{Spec} R}$. As $\mathfrak{a}_{a,\mathfrak{p}} \cap R = \mathfrak{p}$, this is clear for the topological maps f and s_a. Let $U = \operatorname{Spec} R \setminus V(\mathfrak{a})$ be any open set in $\operatorname{Spec} R$, and $(s^{(\mathfrak{p})})_{\mathfrak{p} \in U}$ any element of $\mathcal{O}_{\operatorname{Spec} R}(U)$. We have to check that $(f \circ s_a)^{\#}((s^{(\mathfrak{p})})_{\mathfrak{p} \in U}) = (s_a^{\#} \circ f^{\#})((s^{(\mathfrak{p})})_{\mathfrak{p} \in U})$ is indeed $(s^{(\mathfrak{p})})_{\mathfrak{p} \in U}$. Now

$$f^{\#}((s^{(\mathfrak{p})})_{\mathfrak{p} \in U}) = (s^{(\mathfrak{p} \cap R)})_{\mathfrak{p} \in f^{-1}(U)}.$$

Applying $s^{\#}$, we get

$$\begin{aligned} s^{\#}\left(f^{\#}((s^{(\mathfrak{p})})_{\mathfrak{p} \in U})\right) &= s^{\#}\left((s^{(\mathfrak{q} \cap R)})_{\mathfrak{q} \in f^{-1}(U)}\right) \\ = (s^{(\mathfrak{a}_{a,\mathfrak{p}} \cap R)}(a))_{\mathfrak{p} \in s^{-1}(f^{-1}(U))} &= (s^{(\mathfrak{p})})_{\mathfrak{p} \in U},\end{aligned}$$

since $s^{(\mathfrak{p})}$ is the quotient of two elements of R and, hence, $s^{(\mathfrak{p})}(a) = s^{(\mathfrak{p})}$, and as $s_a^{-1}(f^{-1}(U)) = (f \circ s_a)^{-1}(U) = U$.

Now by Proposition 3.3.31 we have $(\mathcal{O}_{\mathbb{P}^n_R}(1))(\mathbb{P}^n_R) = \langle x_0, \ldots, x_n \rangle_R$, and by [Har77, p. 150, ch. II] we know that the global sections x_i generate $\mathcal{O}_{\mathbb{P}^n_R}(1)_{\mathfrak{p}}$ as an $\mathcal{O}_{\mathbb{P}^n_R,\mathfrak{p}}$-module for every $\mathfrak{p} \in \mathbb{P}^n_R$. Therefore, clearly $s_a^*(\mathcal{O}_{\mathbb{P}^n_R}(1)) = \mathcal{O}_{\operatorname{Spec} R}$ and $s_a^*(x_i) = a_i$. □

Before closing this section we want to explicitly describe the R-rational points of a closed subscheme of $\mathbb{P}^n_R$.

Proposition 3.6.8. *Let R be a ring, $n \in \mathbb{N}$, and $\mathfrak{a}$ be a homogenous ideal in $R[x_0, \ldots, x_n]$. Let $X = \operatorname{Proj} R[x_0, \ldots, x_n]/\mathfrak{a}$, $S = \operatorname{Spec} R$, and $Y = \mathbb{P}^n_R$. Let $f_X : X \to S$ and $f_Y : Y \to S$ be the structure morphisms and $i : X \to Y$ be the closed immersion. (See Proposition 3.4.34 and Corollary 3.4.35.) Then the R-rational points of X are exactly the R-rational points $s \in Y(S)$ which factor over X, i. e. there is an R-rational point $s' \in X(S)$ satisfying $i \circ s' = s$.*

$$\begin{tikzcd}
X \arrow[rr, "i"] \arrow[dr, "f_X"] & & Y \arrow[dl, "f_Y"'] \\
& S \arrow[ul, bend left, "s'"] \arrow[ur, bend right, "s"'] &
\end{tikzcd}$$

Moreover, if $\operatorname{Pic} R = 0$*, then the R-rational points of X correspond to the points $a \in \mathbb{P}^n(R)$, satisfying $g(a) = 0$ for all $g \in \mathfrak{a}^h$, i. e. to the points $a \in V_R(\mathfrak{a})$.*

Proof. Clearly every R-rational point $s' \in X(S)$ induces an R-rational point $s = i \circ s' \in Y(S)$. And if $s : S \to Y$ factors as $s = i \circ s'$ with $s' : S \to X$, then clearly $s' \in X(S)$.

For the second statement note that the R-rational points of X correspond to the insertion morphisms $R[x_0, \ldots, x_n] \to R$, which factor over $R[x_0, \ldots, x_n]/\mathfrak{a}$, i. e. which can be written as the concatenation of R-linear morphisms

$$R[x_0, \ldots, x_n] \longrightarrow R[x_0, \ldots, x_n]/\mathfrak{a} \longrightarrow R,$$

where the first map is the canonical projection (see Corollary 3.4.35). □

3.7 Curves

In this section we will study curves over algebraically closed fields. We are especially interested in morphisms between curves, in the Frobenius morphism, in how Weil divisors specialize on smooth curves, in the intersection of lines with curves and in tangent lines, and in how the genus of a curve is defined. As a final result in this section we will present the Riemann-Roch Theorem, which allows us to compute how many divisors are linearly equivalent to a given one.

Let $\mathbb{F}$ be an algebraically closed field. We want to begin by defining what a curve over a field $\mathbb{F}$ is. We first state two definitions, which turn out to be the same for smooth curves.

Definition 3.7.1. *A* curve over $\mathbb{F}$ *is a projective variety defined over $\mathbb{F}$ of dimension one.*

Definition 3.7.2. *[Har77, p. 136, ch. II]*

(a) *A* curve over $\mathbb{F}$ *is an integral separated scheme X of finite type over $\mathbb{F}$ of dimension one.*

(b) *A curve C is* complete *if the structure morphism $C \to \operatorname{Spec} \mathbb{F}$ is proper.*

(c) *A curve is* smooth *if all local rings are regular local rings.*

3.7.1 Some Facts about Curves

In this subsection we want to state some fundamental results on curves and show that the two above definitions for curves over $\mathbb{F}$ coincide for smooth curves.

Proposition 3.7.3. *[Har77, p. 136, ch. II, Proposition 6.7] Let C be a smooth curve over $\mathbb{F}$. Then the following are equivalent:*

(a) *The curve C is complete.*

(b) *The curve C is projective.*

(c) *The curve C is isomorphic to $t(C_{\mathbb{F}(C)})$, where $C_{\mathbb{F}(C)}$ is the abstract smooth curve associated with the function field $\mathbb{F}(C)$ [Har77, p. 42ff, ch. I] and t the functor $\mathscr{V}ar(\mathbb{F}) \to \mathscr{S}ch(\mathbb{F})$. (Compare Proposition 3.5.4 for t.)*

Proposition 3.7.4. *[Har77, p. 45, ch. I, Corollary 6.12] The following categories are equivalent:*

(a) *The category of smooth projective varieties of dimension one over $\mathbb{F}$, with dominant morphisms.*

(b) *The category of function fields of dimension one over $\mathbb{F}$, with $\mathbb{F}$-homomorphisms.*

The equivalence is given by assigning to C the function field $\mathbb{F}(C)$, and to a function field K the abstract smooth curve C_K.

Therefore the smooth curves, seen as varieties (Definition 3.7.1), are exactly the complete smooth curves, seen as schemes (Definition 3.7.2). In fact, the different definitions of a function field also coincide:

Proposition 3.7.5. *Let C be a smooth complete curve over $\mathbb{F}$ (as a scheme), and C' the corresponding smooth curve over $\mathbb{F}$ (as a variety). Then the function field of C is the same as the function field of C'.*

Proof. This follows from Proposition 3.2.18 (c) and Proposition 3.5.4. □

We want to close this subsection with an analogon to Liouville's Theorem from complex analysis for complete smooth curves:

Proposition 3.7.6. *[Sil86, p. 22, Proposition 1.2] Let C be a complete smooth curve and $f \in \mathbb{F}(C)$. Then f has no poles if, and only if, $f \in \mathbb{F}$, i. e. f is constant.*

Proof. By using Proposition 3.7.3 and Proposition 3.5.4, we get from Proposition 3.2.18 (a) that $\mathscr{O}_C(C) \cong \mathbb{F}$. □

3.7.2 Morphisms between Curves

In this subsection we want to study how a morphism between curves implies an inclusion of function fields, which allows classification of morphisms by using properties of the induced field extension. We are also interested in the (local) behavior of a morphism in a point.

Remarks 3.7.7.

(a) [Har77, p. 25, ch. I] Let X and Y be projective varieties over $\mathbb{F}$, and $f : X \to Y$ a dominant rational map. Let f be represented by $\langle U, f_U \rangle$ as in Section 3.2.5. If $g \in \mathbb{F}(Y)$ is a rational function represented by $\langle V, h \rangle$, $f_U^{-1}(V)$ is a non-empty (since $f_U(U)$ is dense) open set in X and, moreover, $f \circ f_U$ is a regular function on $f_U^{-1}(V)$. Therefore, $\left\langle f_U^{-1}(V), f \circ f_U \right\rangle$ represents a rational function in $\mathbb{F}(X)$.

(b) Let X and Y be integral schemes over $\mathbb{F}$, and $f : X \to Y$ a finite morphism. Let ξ be the generic point of X, and ζ the generic point of Y. Then $f(\xi) = \zeta$, as if $y \in Y$ is not ζ, then $\zeta \notin \overline{\{y\}}$, and hence $f^{-1}(\overline{\{y\}})$ is a proper closed subset of X. Therefore, $f^{-1}(\overline{\{y\}})$ cannot contain ξ, i. e. in particular we have $f(\xi) \neq y$. Thus, there is a well-defined map $f_\zeta^\# : \mathbb{F}(Y) = \mathcal{O}_{Y,\zeta} \to \mathcal{O}_{X,\xi} = \mathbb{F}(X)$.

(c) Let $f : X \to Y$ be a finite morphism of projective varieties. Then it gives the same injection of function fields in the sense of (a) as the corresponding injection of function fields in the sense of (b).

If, in the following, $f : X \to Y$ is a finite morphism, we will identify $\mathbb{F}(Y)$ as a subfield of $\mathbb{F}(X)$. We begin by characterizing what kind of morphisms $C \to C'$ between curves can appear if C is a complete smooth curve.

Proposition 3.7.8. *[Har77, p. 137, ch. II, Proposition 6.8] Let C be a complete smooth curve over $\mathbb{F}$ and let C' be an arbitrary curve over $\mathbb{F}$. If $f : C \to C'$ is a morphism, then one of the following cases occurs:*

(a) *either the image of f is a point, i. e. f is constant (and in particular not finite); or*

(b) *the image is C', f is a finite morphism, C' is complete and $\mathbb{F}(C')$ is a finite field extension of $\mathbb{F}(C)$.*

Next we want to define properties of non-constant morphisms based on their induced field extension:

Definition 3.7.9. *Let $f : X \to Y$ be a finite morphism of complete smooth curves.*

(a) *The* degree *of f, denoted by $\deg f$, is the degree of the field extension $\mathbb{F}(X)/\mathbb{F}(Y)$.*

(b) *We call f* separable *if $\mathbb{F}(X)/\mathbb{F}(Y)$ is separable.*

(c) *The* separable degree *of f, denoted by $\deg_s f$, is the separable degree of the field extension $\mathbb{F}(X)/\mathbb{F}(Y)$.*

(d) *We call f* inseparable *if $\mathbb{F}(X)/\mathbb{F}(Y)$ is inseparable.*

(e) *The* inseparable degree *of f, denoted by $\deg_i f$, is the inseparable degree of the field extension $\mathbb{F}(X)/\mathbb{F}(Y)$.*

(f) *If $\mathbb{F}$ has characteristic $p > 0$, we call f* purely inseparable *if $\mathbb{F}(X)/\mathbb{F}(Y)$ is purely inseparable.*

We can quickly conclude the following facts:

Corollary 3.7.10. *If $f : X \to Y$ is a morphism of complete smooth curves and $\deg f = 1$, then f is an isomorphism.*

Proof. Since $1 = \deg f = [\mathbb{F}(X) : \mathbb{F}(Y)]$, f induces an isomorphism $\mathbb{F}(C) \to \mathbb{F}(C')$ and, therefore, the claim follows from Proposition 3.7.4. □

Corollary 3.7.11. *Let $f : X \to Y$ and $g : Y \to Z$ be non-constant morphisms of complete smooth curves. Then $\deg(g \circ f) = \deg f \cdot \deg g$ and $\deg_s(g \circ f) = \deg_s f \cdot \deg_s g$.*

Proof. This follows directly from the multiplication formula for degrees of field extensions, $[\mathbb{K} : \mathbb{F}] = [\mathbb{F}' : \mathbb{F}] \cdot [\mathbb{K} : \mathbb{F}']$, where $\mathbb{K} \subseteq \mathbb{F}' \subseteq \mathbb{F}$ is a tower of fields. The same is true for the separable degree by Remark 2.2.32 (c). □

Note that a closed point $P \in C$ on a complete smooth curve C is a prime divisor and, therefore, one has a valuation ord_P on $\mathcal{O}^*_{C,P}$.

Definition 3.7.12. *Let C be a complete smooth curve and $P \in C$ a closed point. Then a* local parameter *of C at P is an element $t \in \mathcal{O}_{C,P}$ with valuation* $\operatorname{ord}_P(t) = 1$.

Remark 3.7.13. If C is a complete smooth curve, then local parameters exist for all closed points. (See Remark 3.5.13.)

We can now define what the ramification index of a morphism in a point is.

Definition 3.7.14. *[Har77, p. 299, ch. IV] Let $f : C \to C'$ be a non-constant morphism of smooth complete curves, and let $P \in C$. Let $Q = f(P)$ and $t \in \mathcal{O}_{C',Q}$ be a local parameter at Q. Consider t as an element of $\mathcal{O}_{C,P}$ by the natural map $f_Q^{\#} : \mathcal{O}_{C',Q} \to \mathcal{O}_{C,P}$, and define $e_P(f) := \operatorname{ord}_P(t) \in \mathbb{Z}$ to be the* ramification index *of f at P.*

If $e_P(f) > 1$, then f is said to be ramified *at P and Q is said to be a* branch point *of f, and if $e_P(f) = 1$ it is said to be* unramified *at P. If C is unramified at every $P \in C$, then C is said to be* unramified.

Proposition 3.7.15. *[Sil86, p. 28, Proposition 2.6] Let $\varphi : C_1 \to C_2$ be a non-constant morphism of smooth complete curves.*

(a) *For every $Q \in C_2$ we have*

$$\sum_{\varphi(P)=Q} e_P(\varphi) = \deg \varphi.$$

(b) *For all but finitely many $Q \in C_2$ we have*

$$\left|\varphi^{-1}(Q)\right| = \deg_s \varphi.$$

(c) *Let $\psi : C_2 \to C_3$ be another non-constant morphism of smooth complete curves. Then for all $P \in C_1$ we have*

$$e_P(\psi \circ \varphi) = e_{\varphi(P)}(\psi) \cdot e_P(\varphi).$$

We close this section with a result for rational maps from complete smooth curves to projective varieties. Some interesting special cases are rational maps $C \to \mathbb{P}^n_{\mathbb{F}}$ for a complete smooth curve C.

Proposition 3.7.16. *[Sil86, p. 23, ch. II, Proposition 2.1] Let $\varphi : C \to X$ be a rational map from a complete smooth curve C to a projective variety X. Then φ is a morphism.*

3.7.3 The Frobenius Morphism

If $\mathbb{F}$ is a field of prime characteristic p, and $q = p^n$, we have seen in Section 2.2.3 that the map $x \mapsto x^q$ is a field endomorphism. Moreover, for every $x \in \mathbb{F}$, $x^q = x$ if, and only if, $x \in \mathbb{F}_q$. In this subsection we will define the Frobenius endomorphism for schemes. This will allow us to determine later all $\mathbb{F}_q$-rational points of a curve as the kernel of $\mathbf{id} - \varphi$, where φ is the q-th power Frobenius morphism.

Definition 3.7.17. *[Har77, p. 301, ch. II] Let X be a scheme such that all local rings of X have prime characteristic $p > 0$, and let q be a power of p. Define the* Frobenius morphism *$F_q : X \to X$ as being the identity map on the topological space of X, and being the q-th power map on $F_q^\#(U) : \mathcal{O}_X(U) \to \mathcal{O}_X(U)$, $g \mapsto g^q$.*

Definition 3.7.18. *[Har77, p. 302, ch. II] Let X be a scheme with the structure morphism $\pi : X \to \operatorname{Spec} \mathbb{F}$, where there characteristic of $\mathbb{F}$ is $p > 0$, and let q be a power of p. Define the scheme $X^{(q)}$ over $\mathbb{F}$ as exactly the same scheme X but with structure morphism $\pi \circ F_q$. Then $F_q : X \to X$ becomes the $\mathbb{F}$-morphism $F_q : X^{(q)} \to X$, called the* $\mathbb{F}$-linear Frobenius morphism.

We will now state two results on the $\mathbb{F}$-linear Frobenius morphism and its connection to purely inseparable morphisms.

Proposition 3.7.19. *[Sil86, p. 30, Proposition 2.11] Let $\mathbb{F}$ be a field of characteristic $p > 0$ and C be a curve over $\mathbb{F}$, and let $F_q : C \to C^{(q)}$ be the $\mathbb{F}$-linear Frobenius morphism.*

(a) *Then F_q is purely inseparable.*

(b) *Moreover* $\deg F_q = q$.

(c) *If $\mathbb{F}$ is perfect, $\mathbb{F}(C^{(q)}) = \mathbb{F}(C)^q$.*

Proposition 3.7.20. *[Har77, p. 302, ch. II, Proposition 2.5] Let $f : X \to Y$ be a purely inseparable morphism of smooth complete curves over $\mathbb{F}$, where $\mathbb{F}$ has characteristic $p > 0$. Then $f = F_q$ for q being a power of p.*

3.7.4 Divisors

Since smooth curves satisfy the condition $(*)$ from Section 3.5.2, we can speak of Weil divisors on smooth curves. Moreover, the prime divisors on smooth curves are exactly the closed points ([Har77, p. 137, ch. II]).

Recall that a Weil divisor on a smooth curve C is a formal finite sum of prime divisors (hence points in this case) with multiplicities, i. e. $D = \sum_{P \in C} n_P[P]$, where

$n_P \in \mathbb{Z}$ and all but a finite number of n_P's are zero. To each function $f \in \mathbb{F}(V)^*$ we can associate a divisor $\mathrm{div}(f)$ by taking the valuation of $\mathcal{O}_{C,P}$ for f, denoted by $\mathrm{ord}_P(f)$, i. e. $\mathrm{div}(f) = \sum_{P\in C} \mathrm{ord}_P(f)[P]$. Such divisors $\mathrm{div}(f)$ are called principal and, if the difference of two arbitrary divisors is principal, they are called linearly equivalent. The group of divisors modulo the subgroup of principal divisors is the divisor class group $\mathrm{Cl}(C)$, which for smooth curves over $\mathbb{F}$ is isomorphic to $\mathrm{Pic}(C)$ and to $\mathrm{CaCl}(C)$. In the following we will identify $\mathrm{Cl}(C)$ with $\mathrm{Pic}(C)$ and $\mathrm{CaCl}(C)$, and also $\mathrm{WDiv}(C)$ with $\mathrm{CDiv}(C)$, the group of Cartier divisors.

We first state an exact sequence showing how all these definitions interact:

Remark 3.7.21. If C is a complete smooth curve, the kernel of $\mathrm{div}(\bullet)$ is $\mathbb{F}^*$ by Proposition 3.7.6 and, therefore, we have the following exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{F}^* \arrow[r, hook] & \mathbb{F}(C)^* \arrow[r, "f\mapsto\mathrm{div}(f)"] & \mathrm{WDiv}(C) \arrow[r, two heads] \arrow[d, equal] & \mathrm{Cl}(C) \arrow[r] \arrow[d, equal] & 0 \\
 & & & \mathrm{CDiv}(C) & \mathrm{CaCl}(C) \arrow[d, equal] & \\
 & & & & \mathrm{Pic}(C) &
\end{tikzcd}$$

Next we define the degree of a Weil divisor.

Definition 3.7.22. *Let C be a smooth curve and $D = \sum n_P[P]$ a divisor on C. Then the* degree *of D is $\deg D := \sum n_P$.*

Remark 3.7.23. Clearly $\deg : \mathrm{WDiv}(C) \to \mathbb{Z}$ is a surjective group homomorphism.

If $f : C \to C'$ is a morphism of curves, we want to transport Weil divisors on C' to C.

Remark 3.7.24. [Har77, p. 137, ch. II] Let $f : C \to C'$ be a finite morphism of smooth curves, $P \in C$ and $f(P) = Q \in C'$. Let $t \in \mathcal{O}_{C',Q}$ be a local parameter. Then t can be seen as an element of $\mathcal{O}_{C,P}$ by the natural map $f_Q^{\#} : \mathcal{O}_{C',Q} \to \mathcal{O}_{C,P}$. Moreover, $\sum_{f(P')=Q} \mathrm{ord}_{P'}(t)[P']$ is a well-defined Weil divisor on C, only depending on f and Q.

Definition 3.7.25. *Let $f : C \to C'$ be a finite morphism of smooth curves. Define a morphism $f^* : \mathrm{WDiv}(C') \to \mathrm{WDiv}(C)$ by*

$$f^*([Q]) = \sum_{f(P)=Q} \mathrm{ord}_P(t)[P],$$

where $Q \in C'$ and t is a local parameter at Q.

Remarks 3.7.26.

(a) [Har77, p. 137, ch. II] Note that $f^* : \mathrm{WDiv}(Y) \to \mathrm{WDiv}(X)$ preserves linear equivalence and, therefore, it induces a morphism $f^* : \mathrm{Cl}(Y) \to \mathrm{Cl}(X)$.

(b) [Har77, p. 148, ch. II, Exercise 6.8 or p. 299, ch. IV] If D is a divisor on Y, then $f^*(\mathcal{L}(D)) \cong \mathcal{L}(f^*D)$.

Proposition 3.7.27. *[Har77, p. 138, ch. II, Proposition 6.9] Let $f : C \to C'$ be a finite morphism of smooth curves, and $D \in \operatorname{WDiv}(C')$. Then $\deg(f^*D) = (\deg f) \cdot (\deg D)$.*

On complete smooth curves it turns out that principal divisors have degree zero. It therefore makes sense to restrict the above exact sequence to degree zero.

Corollary 3.7.28. *[Har77, p. 138, ch. II, Corollary 6.10] A principal divisor on a complete smooth curve has degree zero. Moreover, $\deg : \operatorname{Cl}(X) \to \mathbb{Z}$ is a well-defined and surjective group morphism.*

Definition 3.7.29. *Let C be a smooth curve. The subgroup of Weil divisors of degree zero is denoted by $\operatorname{WDiv}^0(C)$, and the quotient of $\operatorname{WDiv}^0(C)$ with the subgroup of principal divisors on C is denoted by $\operatorname{Pic}^0(C)$.*

Remark 3.7.30. If C is a complete smooth curve we have the following exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{F}^* \arrow[r, hook] & \mathbb{F}(C)^* \arrow[r, "f \mapsto \operatorname{div}(f)"] & \operatorname{WDiv}^0(C) \arrow[r, two heads] & \operatorname{Pic}^0(C) \arrow[r] & 0. \end{tikzcd}$$

We have seen that if $f : C \to C'$ is a non-constant morphism of complete smooth curves, we can transport Weil divisors from C' to C. We next want to show how to transport Weil divisors from C to C':

Definition 3.7.31. *Let $f : C \to C'$ be a non-constant morphism of smooth complete curves. Define the map*

$$f_* : \operatorname{WDiv}(C) \to \operatorname{WDiv}(C'), \qquad [P] \mapsto [f(P)].$$

Proposition 3.7.32. *Let $f : C \to C'$ be a finite morphism of smooth complete curves. Then $f_* : \operatorname{WDiv}(C) \to \operatorname{WDiv}(C')$ is a group morphism respecting linear equivalence and degree, i. e. $\deg f_*(D) = \deg D$ and if $D_1 \sim D_2$, then $f_*(D_1) \sim f_*(D_2)$.*

Proof. The only thing to show is that f_* respects linear equivalence. But this follows from [Har77, p. 306, ch. IV, Exercise 2.6]. □

3.7.5 Intersection with Lines

Recall the definition of the intersection multiplicity $i_{X,Y}(Z)$ from Definition 3.2.32. Using the Theorem of Bézout, we get the following result about the intersection of a smooth curve with a line:

Proposition 3.7.33. *Let C be a complete smooth curve in $\mathbb{P}^2_{\mathbb{F}}$ of degree d and let $L, L' \subseteq \mathbb{P}^2_{\mathbb{F}}$ be two lines defined by homogenous linear polynomials $f, f' \in \mathbb{F}[x, y, z]_1$. Assume that neither L nor L' is contained in C. Let $P_1, \dots, P_k$ be the intersection points of C with L, and $Q_1, \dots, Q_\ell$ be the intersection points of C with L'. Then $\frac{f}{f'} \in \mathbb{F}(C)$,*

$$\sum_{i=1}^{k} i_{C,L}(P_i) = d = \sum_{i=1}^{\ell} i_{C,L}(Q_i)$$

and

$$\operatorname{div}\left(\frac{f}{f'}\right) = \sum_{i=1}^{k} i_{C,L}(P_i)[P_i] - \sum_{i=1}^{\ell} i_{C,L}(Q_i)[Q_i].$$

Proof. This follows from the Theorem of Bézout (Theorem 3.2.33) and [Har77, p. 146, ch. II, Exercise 6.2]. □

We first need some preparation to be able to define the tangent hyperplane at one point of a smooth variety in $\mathbb{P}^n_{\mathbb{F}}$.

Lemma 3.7.34. *Let $f \in \mathbb{F}[x_0, \ldots, x_n]^h$ a homogenous polynomial and $P = (p_0 : \cdots : p_n) \in \mathbb{P}^n_{\mathbb{F}}$ such that $f(P) = 0$. If $p_j \neq 0$ for a $j \in \{0, \ldots, n\}$, then*

$$p_j \frac{\partial f}{\partial x_j}(P) = -\sum_{\substack{i=0 \\ i\neq j}}^{n} \frac{\partial f}{\partial x_i}(P) p_i.$$

Proof. Let f be homogenous of degree d. If $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{N}^{n+1}$ with $\sum_{i=0}^n \alpha_i = d$, then

$$\begin{aligned}
\sum_{\substack{i=0 \\ i\neq j}}^{n} \frac{\partial(x^\alpha)}{\partial x_i}(P)\frac{p_i}{p_j} &= \sum_{\substack{i=0 \\ i\neq j}}^{n} \left(\alpha_i x_i^{\alpha_i - 1} \prod_{\substack{k=0 \\ k\neq i}}^{n} x_k^{\alpha_k}\right)(P)\frac{p_i}{p_j} \\
= \sum_{\substack{i=0 \\ i\neq j}}^{n} \frac{p_i}{p_j}\alpha_i p_i^{\alpha_i - 1} \prod_{\substack{k=0 \\ k\neq i}}^{n} p_k^{\alpha_k} &= \sum_{\substack{i=0 \\ i\neq j}}^{n} \frac{\alpha_i}{p_j}(x^\alpha)(P) = \frac{d-\alpha_j}{p_j}(x^\alpha)(P) \\
= \frac{d}{p_j}(x^\alpha)(P) - \alpha_j \frac{\prod_{i=0}^n p_i^{\alpha_i}}{p_j} &= \frac{d}{p_j}(x^\alpha)(P) - \frac{\partial(x^\alpha)}{\partial x_j}(P).
\end{aligned}$$

Since differentiation and evaluation in P is $\mathbb{F}$-linear, we get

$$\sum_{\substack{i=0 \\ i\neq j}}^{n} \frac{\partial f}{\partial x_i}(P)\frac{p_i}{p_j} = \frac{d}{p_j}f(P) - \frac{\partial f}{\partial x_j}(P) = -\frac{\partial f}{\partial x_j}(P).$$

□

Assume C is a smooth variety in $\mathbb{P}^n_{\mathbb{F}}$ defined by a homogenous polynomial $f \in \mathbb{F}[x_0, \ldots, x_n]$, and let $P = (p_0 : \cdots : p_n) \in C(\mathbb{F})$. Moreover, assume that $p_i \neq 0$. Consider the part of C in the hyperplane defined by $x_i \neq 0$. It is defined by the inhomogenous polynomial $f|_{x_i=1} \in \mathbb{F}[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. Let $\hat{P} = (p_0/p_i, \ldots, p_{i-1}/p_i, p_{i+1}/p_i, \ldots, p_n/p_i) \in \mathbb{A}^n_{\mathbb{F}}$. Since we assumed C to be smooth, at least one of the partial differentiations $\frac{\partial f|_{x_i=1}}{\partial x_j}(\hat{P})$, $j \in \{0, \ldots, n\} \setminus \{i\}$, is not zero. Therefore, the tangent plane (in $\mathbb{A}^n_{\mathbb{F}}$) is defined by

$$\sum_{\substack{j=0 \\ j\neq i}}^{n} \frac{\partial f|_{x_i=1}}{\partial x_j}(\hat{P})x_j = \sum_{\substack{j=0 \\ j\neq i}}^{n} \frac{\partial f|_{x_i=1}}{\partial x_j}(\hat{P})\frac{p_i}{p_j}.$$

Extending to projective space $\mathbb{P}^n_{\mathbb{F}}$, this becomes the hyperplane defined by

$$\sum_{\substack{j=0 \\ j\neq i}}^{n} \frac{\partial f}{\partial x_j}(P)x_j - \sum_{\substack{j=0 \\ j\neq i}}^{n} \frac{\partial f}{\partial x_j}(P)\frac{p_i}{p_j}x_i = 0.$$

But by the lemma, this is exactly the hyperplane defined by

$$\sum_{j=0}^{n} \frac{\partial f}{\partial x_j}(P) x_j = 0,$$

which does not depend on i. This justifies the following definition:

Definition 3.7.35. *Let $C = V_{\mathbb{F}}(f)$, $f \in \mathbb{F}[x_0, \dots, x_n]^h$ be a smooth variety in $\mathbb{P}^n_{\mathbb{F}}$ and $P = (p_0 : \cdots : p_n) \in C$. Then the* tangent hyperplane *of C in P is the hyperplane given by the equation*

$$\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(P) x_i = 0.$$

If $n = 2$, then the tangent hyperplane is also called the tangent line*.*

We close with a result connecting the property of a line being tangent to a curve in the projective plane with the intersection multiplicities from Bézout's Theorem.

Proposition 3.7.36. *Let C be a complete smooth curve in $\mathbb{P}^2_{\mathbb{F}}$ of degree $d > 1$ and $P \in C$. Let L be the tangent line. Then $i_{C,L}(P) \geq 2$. Conversely, if L is a line meeting C in P such that $i_{C,L}(P) \geq 2$, then L is the tangent line of C in P.*

Proof. This follows from [Har77, p. 54, ch. I, Exercise 7.3]. □

3.7.6 Genus and the Riemann-Roch Theorem

Let C be a complete smooth curve. An important invariant of such curves is the genus. In topology the genus describes the number of holes something has; for example, a disk has genus zero and a torus has genus one. We now state the definition of the arithmetic genus of C, and show that it coincides with the geometric genus we have defined before.

Definition 3.7.37. *Let P_C be the Hilbert polynomial of C, seen as a variety in projective space. Define the* arithmetic genus *of C to be $p_a(C) := 1 - P_C(0)$.*

Proposition 3.7.38. *[Har77, p. 294, ch. IV, Proposition 1.1] Let C be a complete smooth curve. Then*

$$p_a(C) = p_g(C) = \dim_{\mathbb{F}} H^1(C, \mathcal{O}_C) \geq 0,$$

where $H^1(C, \mathcal{O}_C)$ is the first cohomology group of $\mathcal{O}_C$ (see [Har77, ch. III] for more information about cohomology) and $p_g(C)$ the geometric genus of C (see Definition 3.5.42).

Definition 3.7.39. *The* genus *of C is defined to be the arithmetic genus of C, being the same as the geometric genus or as* $\dim_{\mathbb{F}} H^1(C, \mathcal{O}_C)$*.*

The following proposition gives an easy way to determine the genus of a smooth plane curve:

Proposition 3.7.40. *[Har77, p. 54, ch. II, Exercise 7.2(b)] Let $C = V_{\mathbb{F}}(f) \subseteq \mathbb{P}^2_{\mathbb{F}}$ be a proper smooth curve, and let f be of degree d. (By Proposition 3.2.31, d is also the degree of C.) Then the genus of C is given by*

$$\frac{(d-2)(d-1)}{2}.$$

Our next aim is to state the Riemann-Roch Theorem. It allows to compute the dimension of the complete linear system of a divisor, which will be extremely useful in Chapter 4. But first we have to define complete linear systems and their dimensions.

Definition 3.7.41. *Let $D \in \mathrm{WDiv}(C)$ be a divisor. The* complete linear system *of D is the set*

$$|D| := \{D' \in \mathrm{WDiv}(C) \mid D' \geq 0,\ D' \sim D\}.$$

Remark 3.7.42. [Har77, p. 295, ch. IV and p. 157, ch. II, Proposition 7.7] If D is a divisor, then there is a one-by-one correspondence between $|D|$ and $(\Gamma(C, \mathcal{L}(D)) \setminus \{0\})/\mathbb{F}^*$. The set $\Gamma(C, \mathcal{L}(D)) \setminus \{0\}$ can be identified with all rational functions $f \in \mathbb{F}(C)$ such that either $f = 0$ or $\mathrm{div}(f) \geq -D$.

Definition 3.7.43. *Let $D \in \mathrm{WDiv}(C)$ be a divisor. Define*

$$\ell(D) := \dim_{\mathbb{F}} \Gamma(C, \mathcal{L}(D)).$$

The dimension $\dim |D|$ *of $|D|$ is $\ell(D) - 1$.*

Remark 3.7.44. [Har77, p. 295, ch. IV] For a divisor D the number $\ell(D)$ is finite.

Finally, we can state the Riemann-Roch Theorem.

Theorem 3.7.45 (Riemann-Roch). *[Har77, p. 295, ch. IV, Theorem 1.3] Let C be a complete smooth curve over an algebraically closed field $\mathbb{F}$ and let $D \in \mathrm{WDiv}(C)$ be a Weil divisor. Moreover, let K_C be a canonical divisor on C and g be the genus of C. Then*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

In practice we will need the following results, which mostly follow from the Riemann-Roch Theorem. Note that in literature sometimes statement (d) is called the Riemann-Roch Theorem, together with the inequality $\ell(D) \geq \deg D - g + 1$ for all Weil divisors D on C.

Proposition 3.7.46. *[Sil86, pp. 38f] Let C be a complete smooth curve of genus g with canonical divisor K_C.*

(a) *If $D \in \mathrm{WDiv}(C)$ and $\deg D < 0$, then $\ell(D) = 0$. If $D = 0$, then $\ell(D) = 1$.*

(b) *It is $\ell(K_C) = g$.*

(c) *It is $\deg K_C = 2g - 2$.*

(d) *If $\deg D > 2g - 2$ for $D \in \mathrm{WDiv}(C)$, then $\ell(D) = \deg D - g + 1$.*

3.8 Curves over Rings

In this section we will study curves over rings. In the first subsection, we will study curves over arbitrary fields, i. e. the fields do not have to be algebraically closed. In the next subsection we provide tools to give explicit examples of generalized smooth curves. We further give an interpretation of generalized smooth curves over Artinian rings and provide information on $\mathcal{K}_C$ and $\mathcal{O}_C$ for curves over local Artinian rings. In the last subsection we will state results for relative effective Cartier divisors on generalized smooth curves.

We begin by defining what a generalized smooth curve is supposed to be. Generalized elliptic curves will be curves of this class.

Definition 3.8.1. *[KM85, pp. 7f, Definition 1.2.1] Let S be any base scheme. A* generalized smooth curve *C over S is a scheme C such that $C \to S$ is separated, of finite presentation and smooth of relative dimension one.*

3.8.1 Curves over Perfect Fields

In Section 2.2.3 we saw that the Galois theory can be used to describe intermediate fields of a field extension $\mathbb{K}/\mathbb{F}$ as the set of elements of $\mathbb{K}$, which is fixed by a certain subgroup of the $\mathbb{F}$-automorphisms of $\mathbb{K}$. We will use this where $\mathbb{K}$ is the algebraic closure of $\mathbb{F}$ to inspect properties of curves over intermediate fields, when they are defined over $\mathbb{F}$. This will be important when we inspect elliptic curves over finite fields.

Let $\mathbb{F}$ be a perfect field, and $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$. Let $G_{\overline{\mathbb{F}}/\mathbb{F}}$ denote the Galois group of the field extension $\overline{\mathbb{F}}/\mathbb{F}$. By Proposition 2.2.38 we get that $\overline{\mathbb{F}}/\mathbb{F}$ is a Galois extension and, hence, $\mathbb{F}$ consists exactly of the elements in $\overline{\mathbb{F}}$ fixed by all $\sigma \in G_{\overline{\mathbb{F}}/\mathbb{F}}$.

We begin by defining when a curve and points of that curve are defined over (the not necessarily algebraically closed) field $\mathbb{F}$. (Note that in this definition, $\mathbb{F}$ does not necessarily needs to be perfect.)

Definition 3.8.2. *Let C be a curve over $\overline{\mathbb{F}}$. Then C is said to be* defined over $\mathbb{F}$ *if it can be defined by polynomials over $\mathbb{F}$. The* $\mathbb{F}$-rational points *of C are, in the affine case, points whose coordinates are in $\mathbb{F}$ and, in the projective case, points such that one representative exists whose coordinates are in $\mathbb{F}$.*

Remark 3.8.3. [Sil86, p. 6 and p. 10] If P is a point in $\mathbb{P}^n_{\overline{\mathbb{F}}}$ or $\mathbb{A}^n_{\overline{\mathbb{F}}}$, $G_{\overline{\mathbb{F}}/\mathbb{F}}$ induces a natural action on P by defining P^σ to be the point obtained from P by applying $\sigma \in G_{\overline{\mathbb{F}}/\mathbb{F}}$ to all components of P. The point P is then defined over $\mathbb{F}$ if, and only if, $P = P^\sigma$ for every $\sigma \in G_{\overline{\mathbb{F}}/\mathbb{F}}$.

Remark 3.8.4. Note that if C is a curve defined over $\mathbb{F}_q$, where q is a prime power, then the $\mathbb{F}_q$-linear q-th power Frobenius and the q-th power Frobenius coincide for C.

We next want to draw a connection between generalized smooth curves over $\operatorname{Spec} \mathbb{F}$ and complete smooth curves defined over $\mathbb{F}$.

Proposition 3.8.5. *A smooth curve C over $\overline{\mathbb{F}}$, which is defined over $\mathbb{F}$, is a generalized smooth curve over $S = \operatorname{Spec} \overline{\mathbb{F}}$ or $S = \operatorname{Spec} \mathbb{F}$. Moreover, if C is complete, then $C \to S$ is proper.*

Proof. By Proposition 3.5.4 we know that $C \to S$ is quasi-projective. Clearly C and S are Noetherian (see [Har77, p. 84, ch. II, Example 3.2.1]) and, thus, according to Proposition 3.4.31, $C \to S$ is separated and of finite type. According to Remark 3.4.26 (a), $C \to S$ is locally of finite presentation, and according to Remark 3.4.26 (b), $C \to S$ is hence quasi-compact. Since $C \to S$ is separated, it is also quasi-separated according to Remark 3.4.23, and, therefore, $C \to S$ is of finite presentation according to Definition 3.4.25.

We first handle the case $S = \operatorname{Spec} \overline{\mathbb{F}}$. Now $\overline{\mathbb{F}}$ is algebraically closed and, hence, the only geometric fibre of $C \to S$ is C/S itself. But by assumption C is a smooth variety of dimension one and, therefore, by Theorem 3.4.41, $C \to S$ is smooth of relative dimension one. For the case $S = \operatorname{Spec} \mathbb{F}$, note that the geometric fibre is the curve seen over $\operatorname{Spec} \overline{\mathbb{F}}$.

Now assume that C is complete. According to Proposition 3.7.3, in this case C is projective. Then according to Proposition 3.5.4, C is a projective scheme and, according to Proposition 3.4.31, the structure morphism $C \to S$ is proper. □

We are next interested in regular functions defined over $\mathbb{F}$, and in divisors defined over $\mathbb{F}$, which both turn out to have good properties.

Definition 3.8.6. *Let C be a curve defined over $\mathbb{F}$, and $f : U \to \overline{\mathbb{F}}$ be a regular function, where $U \subseteq C$ is an open subset. Then f is* defined over $\mathbb{F}$ *if f can be represented locally by a quotient of polynomials with coefficients in $\mathbb{F}$.*

Denote with $\mathbb{F}(C)$ the set of rational functions $f \in \overline{\mathbb{F}}(C)$, which are defined over $\mathbb{F}$, and with $\mathbb{F}[C]$ the set of regular functions $f \in \overline{\mathbb{F}}[C]$, which are defined over $\mathbb{F}$.

Remark 3.8.7. If C is a curve, then $\mathbb{F}(C)$ is a subfield of $\overline{\mathbb{F}}(C)$. If C is an affine variety defined by $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, then $\mathbb{F}[C] = \mathbb{F}[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$, and $\mathbb{F}(C)$ is the field of fractions of $\mathbb{F}[C]$.

Definition 3.8.8. *Let C be a curve defined over $\mathbb{F}$ and $D \in \operatorname{WDiv}(C)$. If $\sigma \in G_{\overline{\mathbb{F}}/\mathbb{F}}$ and $D = \sum_{P \in C} n_P[P]$, define $D^\sigma = \sum_{P \in C} n_P[P^\sigma]$. The divisor D is said to be* defined over $\mathbb{F}$ *if $D^\sigma = D$ for every $\sigma \in G_{\overline{\mathbb{F}}/\mathbb{F}}$.*

Proposition 3.8.9. *[Sil86, p. 40, Proposition 5.8] Let C be a complete smooth curve defined over $\mathbb{F}$ and $D \in \operatorname{WDiv}(C)$ defined over $\mathbb{F}$. Then there exists a basis of $\Gamma(C, \mathcal{L}(D))$, consisting of functions in $\mathbb{F}(C)$. If, moreover, $f \in \Gamma(C, \mathcal{L}(D))$ is defined over $\mathbb{F}$, it can be described as an $\mathbb{F}$-linear combination of this basis.*

3.8.2 A Class of Curves over Rings

Let R be any ring and $f \in R[x, y, z]^h \backslash R$ a homogenous polynomial which is primitive over R. Define $S = \operatorname{Spec} R$ and $C = \operatorname{Proj} R[x, y, z]/\langle f \rangle$. We will now analyze which properties are satisfied by C, S and the structure morphism $C \to S$. Our aim is to show that for certain choices of f we get that C/S is a proper smooth generalized curve.

As most of the following results hold for a more general case, we use a more general homogenous polynomial $f \in R[x_0, \dots, x_n]^h \setminus R$ and scheme

$$C = \operatorname{Proj} R[x_0, \dots, x_n]/\langle f\rangle$$

until Proposition 3.8.14, were we restrict to the case $n = 2$.

Proposition 3.8.10. *The morphism $C \to S$ is projective, proper and of finite presentation.*

Proof. That $C \to S$ is projective follows directly from Corollary 3.4.35, and that it is proper follows directly from Proposition 3.4.28. Note that separated morphisms are quasi-separated (Remark 3.4.23) and, since C is compact and S is affine, we get that $C \to S$ is quasi-compact. To see that $C \to S$ is locally of finite presentation (and, therefore, of finite presentation; see Definition 3.4.25 (c)), note that $S = \operatorname{Spec} R$ is affine and C can be covered by the $n+1$ open affine subsets

$$\operatorname{Spec}(R[x_0, \dots, x_n]/\langle f\rangle)_{(\langle x_i\rangle)},$$

and

$$(R[x_0, \dots, x_n]/\langle f\rangle)_{(\langle x_i\rangle)} \cong R[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]/\langle f|_{x_i=1}\rangle$$

are clearly R-algebras of finite presentations, $i = 0, \dots, n$. □

Proposition 3.8.11. *Assume f is a non-zero-divisor in $R[x_0, \dots, x_n]$. Then the morphism $C \to S$ is flat.*

Proof. Now by Corollary 2.3.17 (after defining $x_0 := x$, $x_1 := y$, $x_2 := z$ and $n := 2$) we get that $(R[x_0, \dots, x_n]/\langle f\rangle)_{(\hat{x}_i)}$, being isomorphic to

$$R[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]/\langle f|_{x_i=1}\rangle,$$

is flat over R for $0 \leq i \leq n$, where $\hat{x}_i$ is the image of x_i in $R[x_0, \dots, x_n]/\langle f\rangle$. But since $\operatorname{Proj} R[x_0, \dots, x_n]/\langle f\rangle$ is covered by the $D_+(\hat{x}_i)$'s the claim follows from Proposition 3.4.37. □

Remark 3.8.12. Let R be Artinian. Then since f is primitive it is a non-zero-divisor according to Corollary 2.4.5.

The (geometric) fibres of $C \to S$ are in fact varieties over (algebraically closed) fields:

Proposition 3.8.13. *Let $f \in R[x_0, \dots, x_n]^h \setminus R$. Assume that $f \mod \mathfrak{m}$ defines a variety over $\overline{R/\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R. Then the geometric fibre of $C \to S$ at a maximal ideal $\mathfrak{m}$ in R is the variety generated by $f \mod \mathfrak{m}$ over $\overline{R/\mathfrak{m}}$. Here $\overline{R/\mathfrak{m}}$ denotes the algebraic closure of $R/\mathfrak{m}$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of R, and $\varphi : R \twoheadrightarrow R/\mathfrak{m} \hookrightarrow \overline{R/\mathfrak{m}}$. By Proposition 3.4.11 we get

$$\begin{aligned} &\operatorname{Proj} R[x_0, \dots, x_n]/\langle f\rangle \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{R/\mathfrak{m}} \\ = \ &\operatorname{Proj} \overline{R/\mathfrak{m}}[x_0, \dots, x_n]/\langle \varphi(f)\rangle =: X. \end{aligned}$$

But now $R/\mathfrak{m} = k(\mathfrak{m})$ and, therefore, X is the geometric fibre of $C \to \operatorname{Spec} R$ at $\mathfrak{m}$. Since we have $\varphi(f) = f \mod \mathfrak{m}$, we get from Remark 3.5.5 (b) that X corresponds to the projective variety generated by $f \mod \mathfrak{m}$. □

We can now state a criterion when f defines a generalized smooth curve over R:

Proposition 3.8.14. *Assume that f is a non-zero-divisor in $R[x, y, z]$ (if R is Artinian, it is enough for f to be primitive over R). Moreover, assume that $f \mod \mathfrak{m}$ defines a smooth variety of dimension one over $\overline{R/\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of R. Then $C \to S$ is a proper generalized smooth curve. Again $\overline{R/\mathfrak{m}}$ denotes the algebraic closure of $R/\mathfrak{m}$.*

Proof. This follows directly from the previous Propositions 3.8.10, 3.8.11 and 3.8.13, and from Theorem 3.4.41. □

Remark 3.8.15. Assume R is an Artinian ring and, moreover, assume that f satisfies the assumptions of Proposition 3.8.14. Then C and S can be interpreted as follows:

(a) Since R is an Artinian ring, we can write $R = \prod_{i=1}^{n} R_i$ with local Artinian rings R_i, whose only prime ideal is their maximal ideal $\mathfrak{m}_i$. Therefore (see Lemma 3.3.35), S is a finite set of points, namely $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$, and the topology is the discrete topology.

(b) The fibre of $C \to S$ in a maximal ideal $\mathfrak{m}$ of R is the curve defined by $f \mod \mathfrak{m}$, now seen over the field $R/\mathfrak{m}$. The geometric fibre in $\mathfrak{m}$ is the curve defined by $f \mod \mathfrak{m}$ over the algebraic closure of $R/\mathfrak{m}$. These are curves in the "classical" sense, as in Section 3.7 or Section 3.8.1.

(c) An R-rational point $s \in C(S)$ is a "selection function": for every maximal ideal $\mathfrak{m}$ of R and, therefore, for every curve defined by $f_{\mathfrak{m}}$ over the local Artinian ring $R_{\mathfrak{m}}$, $\mathfrak{m} \in \operatorname{Spec} R$, it gives one $R_{\mathfrak{m}}$-rational point on this curve.

(d) One could interpret C/S as the "disjoint union" of the curves $C \times_{\operatorname{Spec} R} \operatorname{Spec} R_{\mathfrak{m}}$ over the local Artinian rings $R_{\mathfrak{m}}$, or as the "disjoint union" of the curves $C_{\mathfrak{m}} = C \times_{\operatorname{Spec} R} \operatorname{Spec} R/\mathfrak{m}$ over the fields $R/\mathfrak{m}$.

A more geometric interpretation for when R is a local Artinian ring can be found in Section 4.3.4.

Before continuing we want to give an example:

Example 3.8.16. Consider the Artinian ring $R = \mathbb{Z}_{12}$, whose decomposition is $R = \mathbb{Z}_4 \times \mathbb{Z}_3$ by the Chinese Remainder Theorem (Proposition 2.5.6), since $\mathbb{Z}_4$ is a local ring and $\mathbb{Z}_3$ is a field (see Lemma 2.5.7). Therefore, the maximal ideals of R are $\langle 2 \rangle$ and $\langle 3 \rangle$.

Consider the polynomial $f = y^2 z - x^3 \in R[x, y, z]$ (which is obviously a non-zero-divisor), and the curve $C = \operatorname{Proj} R[x, y, z]/\langle f \rangle$ over $S = \operatorname{Spec} R$. The curve C is thus the disjoint union of the curves

$$C_1 = \operatorname{Proj} \mathbb{Z}_3[x, y, z]/\langle f \rangle \qquad \text{and} \qquad C_2 = \operatorname{Proj} \mathbb{Z}_4[x, y, z]/\langle f \rangle$$

over the bases $S_1 = \operatorname{Spec} \mathbb{Z}_3$ and $S_2 = \operatorname{Spec} Z_4$, respectively, and the fibre of $C \to S$ in $\langle 2 \rangle$ is the curve $\operatorname{Proj} \mathbb{Z}_2[x, y, z]/\langle f \rangle$ over $\operatorname{Spec} \mathbb{Z}_2$, since $R_{\langle 2 \rangle} = \mathbb{Z}_4$ and $R_{\langle 2 \rangle}/\langle 2 \rangle R_{\langle 2 \rangle} \cong \mathbb{Z}_4/\langle 2 \rangle \cong \mathbb{Z}_2$.

Over $\mathbb{Z}_3$ the curve defined by $y^2z = x^3$ has the points

$$(0:0:1),\ (1:1:1) \text{ and } (0:1:0).$$

Over $\mathbb{Z}_2$ the curve has the points

$$(0:0:1),\ (1:1:1) \text{ and } (0:1:0).$$

And finally over $\mathbb{Z}_4$ the curve has the points

$$\begin{array}{llll} (0:0:1), & (0:2:1), & (2:2:1), & (2:0:1), \\ (1:1:1), & (1:3:1), & (0:1:0), & (2:1:0). \end{array}$$

Note that every point over $\mathbb{Z}_4$ reduces to a point over $\mathbb{Z}_2$ by the canonical reduction map. Moreover, this map is surjective and both the points $(1:1:1)$ and $(0:1:0)$ have exactly two preimages, while $(0:0:1)$ has four preimages. In Lemma 4.3.11 we will see that the first case is the usual one, while the second can only occur in points where the curve is not smooth over $\mathbb{Z}_2$. In fact, one can easily check that the curve $f = 0$ is not smooth in $(0:0:1)$ over any field $\mathbb{F}$.

From the above we now know that $|C(S)| = |C_1(S_1)| \cdot |C_2(S_2)| = 3 \cdot 8 = 24$.

From now on we will give some more information about $\mathcal{K}_C$ for the case that R is a local Artinian ring.

Proposition 3.8.17 (J. Walker). *[Wal99, p. 95, Lemma 4.1] Let $f : C \to S$ be a smooth morphism of locally Noetherian schemes, where $S = \operatorname{Spec} R$ with a local Artinian ring R, and let C be irreducible. Then $\mathcal{K}_C$ is constant, i. e. if U is an open connected subset of C, then $\mathcal{K}_C(U) \cong \mathcal{K}_{C,x}$ for every $x \in C$.*

Proof. Since C is irreducible, it has a unique generic point. Therefore, it is enough to show that $\mathcal{K}_C$ is locally constant. Let $C = \operatorname{Spec} T$ with an R-algebra T. Since f is flat, T is flat over R. Let $\mathfrak{m}$ be the maximal ideal of R. Clearly $T \otimes_R R/\mathfrak{m} \cong T/\mathfrak{m}T$ and, hence, by Remark 3.4.40 (d) we get that $T/\mathfrak{m}T$ is regular and, therefore, reduced by Corollary 2.3.27. Since $\operatorname{Spec} T$ has a unique generic point, T has a unique minimal prime $\mathfrak{p}$ and, therefore, we have $\mathfrak{p} \subseteq \mathfrak{m}T$. But $\mathfrak{m}$ is nilpotent by Lemma 2.2.21 and, therefore, $\mathfrak{p} = \mathfrak{m}T$. Since T is Noetherian, by Proposition 2.3.40, an element of T is a zero-divisor if, and only if, it is nilpotent.

Thus, every localization of T at a prime ideal is a subring of the total quotient ring of T and, therefore, the total quotient ring of any localization at a prime is equal to the total quotient ring of T itself. Therefore, $\mathcal{K}_{\operatorname{Spec} T}$ is constant. □

Corollary 3.8.18. *Let R be a local Artinian ring with maximal ideal $\mathfrak{m}$. Let $S = \operatorname{Spec} R$ and $C = \operatorname{Proj} T$, where $T := R[x_0, x_1, x_2]/\langle f\rangle$ and $f \in R[x_0, x_1, x_2]^h$ is as in Proposition 3.8.14. Then for every $x \in C$ we have*

$$\begin{aligned} \mathcal{K}_{C,x} &= \left\{ \frac{g}{h} \,\middle|\, g, h \in T^h,\ \deg g = \deg h,\ h \notin \mathfrak{m}T \right\} \\ \text{and} \qquad \mathcal{K}^*_{C,x} &= \left\{ \frac{g}{h} \,\middle|\, g, h \in T^h,\ \deg g = \deg h,\ g, h \notin \mathfrak{m}T \right\}. \end{aligned}$$

Moreover, if x belongs to a point $P \in \mathbb{P}^2_R$ in the sense of Proposition 3.6.7, we have

$$\begin{aligned} \mathcal{O}_{C,x} &= \left\{ \frac{g}{h} \,\middle|\, g, h \in T^h,\ \deg g = \deg h,\ h(P) \notin \mathfrak{m} \right\} \\ \text{and} \qquad \mathcal{O}^*_{C,x} &= \left\{ \frac{g}{h} \,\middle|\, g, h \in T^h,\ \deg g = \deg h,\ g(P), h(P) \notin \mathfrak{m} \right\}. \end{aligned}$$

(Note that it makes sense to ask $g(P) \in \mathfrak{m}$.)

Moreover, $g \in T^h$ is in $\mathfrak{m}T$ if, and only if, it is nilpotent, and this is the case if, and only if, it is a zero-divisor.

Proof. If $\mathcal{K}_{C,x}$ and $\mathcal{O}_{C,x}$ have the given form, clearly so have $\mathcal{K}^*_{C,x}$ and $\mathcal{O}^*_{C,x}$. Since f is prime modulo $\mathfrak{m}$, we have that $\langle \mathfrak{m}, f\rangle$ is a prime ideal in $R[x_0, x_1, x_2]$ and, hence, $\mathfrak{m}T$ is prime in T. By Proposition 3.3.24 (a),

$$\mathcal{O}_{C,\mathfrak{m}T} = \left\{ \frac{g}{h} \mid g, h \in T^h,\ \deg g = \deg h,\ h \notin \mathfrak{m}T \right\}$$

and, by Proposition 3.8.17 and its proof, the form of $\mathcal{K}_{C,x}$ for all $x \in C$ follows. The proof also implies the last statement. If x belongs to a point $P \in \mathbb{P}^2_R$, then $x = \big\langle \{f \in T^h \mid f(P) \in \mathfrak{m}\} \big\rangle$ and, therefore, the form of $\mathcal{O}_{C,x}$ follows again from Proposition 3.3.24. □

3.8.3 Relative Effective Divisors

As noted in Section 3.5.2 we cannot use Weil divisors on curves over rings; rather we have to use Cartier divisors. Since curves C over rings as in the last subsection can be seen as a flat family of curves over a base scheme $\operatorname{Spec} R$, we want to use relative effective Cartier divisors, since they in fact give families of effective Cartier divisors on the fibres of $C \to \operatorname{Spec} R$.

We first begin by associating a relative effective Cartier divisor with every point, and characterizing when a relative effective Cartier divisor is proper over S.

Proposition 3.8.19. *Let C be a generalized smooth curve over S.*

(a) *[KM85, p. 8, Lemma 1.2.2] Any S-rational point $s \in C(S)$ defines a relative effective Cartier divisor on C/S.*

(b) *[KM85, p. 8, Lemma 1.2.3] Let D be a closed subscheme of C, which is of finite type over S and of finite presentation over S. Then D is a relative effective Cartier divisor on C/S, which is proper over S.*

(c) *[KM85, p. 8, Lemma 1.2.3] If D is a relative effective Cartier divisor on C/S, which is proper over S, then D is of finite type over S and of finite presentation over S.*

Definition 3.8.20. *Let C be a generalized smooth curve over S and $s \in C(S)$ an S-rational point. The relative effective Cartier divisor defined by s as in the previous proposition, is denoted by $[s]$.*

Remark 3.8.21. [KM85, p. 9, Remark 1.2.4] If C is a proper generalized smooth curve over S, then every relative effective Cartier divisor is proper over S.

For Weil divisors it is easy to define a degree: it is simply the sum over all coefficients of the prime divisors. For proper relative effective Cartier divisors one can also define a degree:

Proposition 3.8.22. *[KM85, p. 9, Definition 1.2.5] Let C be a generalized smooth curve over S, and D a relative effective Cartier divisor on C/S, which is proper over S. Denote the structure morphism of C/S with f. If $U = \operatorname{Spec} R$ is an open affine subset of S, then the affine ring $\mathcal{O}_D(f^{-1}(U))$ of D is a locally free R-module of finite rank, and this rank is Zariski locally constant on S.*

Definition 3.8.23. *Let C be a generalized smooth curve over S and D a relative effective Cartier divisor on C/S. The* degree *of D, denoted by $\deg D$, is the Zariski locally constant function on S given by the previous proposition.*

It turns out that the proper relative effective Cartier divisors of (constant) degree one correspond to the S-rational points of C, if C/S is a generalized smooth curve:

Proposition 3.8.24. *Let C be a generalized smooth curve over S.*

(a) *[KM85, p. 9, Lemma 1.2.6] If D_1 and D_2 are relative effective Cartier divisors on C/S, which are proper over S, then $D_1 + D_2$ is again proper over S and $\deg(D_1 + D_2) = \deg D_1 + \deg D_2$.*

(b) *[KM85, p. 10, Lemma 1.2.7] If $s \in C(S)$ is an S-rational point, then $[s]$ is proper over S and has degree one.*

(c) *[KM85, p. 10, Lemma 1.2.7] If D is a relative effective Cartier divisor on C/S, which is proper over S and has degree one, than there exists a unique S-rational point $s \in C(S)$ such that $[s] = D$.*

Before closing this section we state two results on transporting relative effective Cartier divisors via S-morphisms between generalized smooth curves over S.

Proposition 3.8.25. *(See also Proposition 3.5.35 (d).)*

(a) *[KM85, p. 11, Lemma 1.2.8] Let C and C' be generalized smooth curves over S, and $f : C \to C'$ an S-morphism which is finite, flat, and of degree d. Let D be a relative effective Cartier divisor on C'/S, which is proper over S. Then $f^*(D)$ is a relative effective Cartier divisor on C/S, proper over S, having degree $\deg f^*(D) = d \cdot \deg D$.*

(b) *[KM85, p. 12, Lemma 1.2.9] If C is a generalized smooth curve over S, D is a relative effective Cartier divisor on C/S, which is proper over S, and $T \to S$ is an arbitrary morphism, then the base change D_T is a relative effective Cartier divisor on C_T/T, proper over T, of degree $\deg D$.*

3.9 Group Schemes and Abelian Schemes

In this section we want to present group schemes and Abelian schemes. For this we first start with looking at group objects in arbitrary categories. This will be done in Section 3.9.1, while in Section 3.9.2 we apply the results to the category of S-schemes for a base scheme S and state several results on special group objects in that category. The last subsection will give important examples that we will need later. But first, we want to point out some properties of the category of S-schemes.

Let S be a scheme, and consider the category $\mathscr{S}ch(S)$ of schemes over S. Clearly, in $\mathscr{S}ch(S)$ the base S is a *final object*, as for any S-scheme X there exists exactly one S-morphism $f : X \to S$, namely, the structure morphism of S. Moreover, note that in the category of S-schemes, the categorical product of two S-schemes X and Y is the fibred product $X \times_S Y$ over S (see also Remark 3.4.2 (c)).

3.9.1 Group Objects and Representable Functors

For any category $\mathscr{C}$ with a final object S we naturally have that $G \times S \cong G$ for every object G of $\mathscr{C}$. Recall that $\mathscr{C}^{op}$ denotes the *opposite category* of $\mathscr{C}$. Let $F : \mathscr{C}^{op} \to \mathscr{S}et$ be a functor. Then F is called *representable* by an object O of $\mathscr{C}$ if there exists an isomorphism $F \to \mathrm{Hom}_{\mathscr{C}}(-, O)$ of functors.

Definition 3.9.1. *Let $\mathscr{C}$ be a category with a final object S, and in which finite products $G \times G$ and $G \times G \times G$ exist for all objects G of $\mathscr{C}$.*

(a) *An object G of $\mathscr{C}$ is called a* group object *in $\mathscr{C}$ if there are morphisms $m : G \times G \to G$, $i : G \to G$ and $e : S \to G$ such that the following diagrams commute:*

$$\begin{tikzcd}
G \times G \times G \arrow[r, "m \times \mathbf{id}_G"] \arrow[d, "\mathbf{id}_G \times m"'] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "(\mathbf{id}_G{,}i)"] \arrow[d] & G \times G \arrow[d, "m"] \\
S \arrow[r, "e"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "(i{,}\mathbf{id}_G)"] \arrow[d] & G \times G \arrow[d, "m"] \\
S \arrow[r, "e"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\cong"] \arrow[d, "\mathbf{id}_G"'] & G \times S \arrow[d, "\mathbf{id}_G \times e"] \\
G & G \times G \arrow[l, "m"]
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\cong"] \arrow[d, "\mathbf{id}_G"'] & S \times G \arrow[d, "e \times id_G"] \\
G & G \times G \arrow[l, "m"]
\end{tikzcd}$$

If we use a group object G in the following, we will denote m by m_G, i by i_G and e by e_G, without specifying again what they are.

(b) *A group object G is* commutative *if $m_G \circ w = m_G$, where $w : G \times G \to G \times G$ switches the operands.*

(c) *Let G and H be two group objects in $\mathscr{C}$. A* homomorphism *of group objects is a morphism $f : G \to H$, such that $f \circ e_G = e_H \circ f$, $f \circ i_G = i_H \circ f$ and $f \circ m_G = m_H \circ (f \times f)$.*

Let $\mathscr{C}$ be a category and $X \in \mathscr{C}$. Define the functor

$$h_X : \mathscr{C} \to \mathscr{S}et, \qquad A \mapsto \mathrm{Hom}_{\mathscr{C}}(A, X), \qquad (A \xrightarrow{f} B) \mapsto (g \mapsto f \circ g).$$

Now let $f : X \to Y$ be a morphism in $\mathscr{C}$. Then there is a natural transformation $h_X \to h_Y$, defined by $\mathrm{Hom}_{\mathscr{C}}(A, X) \to \mathrm{Hom}_{\mathscr{C}}(A, Y)$, $g \mapsto f \circ g$ for every $A \in \mathscr{C}$.

Proposition 3.9.2 (Yoneda's Lemma). *[BLR90, p. 95, Proposition 1] Let $\mathscr{C}$ be a category and let $\hat{\mathscr{C}}$ denote the category $\mathrm{Hom}(\mathscr{C}^{\mathrm{op}}, \mathscr{S}et)$. Then for any $X \in \mathscr{C}$, and any $H \in \hat{\mathscr{C}}$, there is a natural bijection $H(X) \to \mathrm{Hom}_{\hat{\mathscr{C}}}(h_X, H)$, with the following property:*

If $u \in H(X)$, then u is mapped onto the natural transformation $h_X \to H$, which satisfies that $g \in h_X(A)$ is mapped onto $H(g)(u) \in H(A)$.

Corollary 3.9.3. *Let $\mathscr{C}$ be a category and let $\hat{\mathscr{C}}$ denote the category $\mathrm{Hom}(\mathscr{C}^{\mathrm{op}}, \mathscr{S}et)$. Define a functor*

$$h : \mathscr{C} \to \hat{\mathscr{C}}, \qquad X \mapsto h_X,$$

which maps a morphism $f : X \to Y$ to the natural transformation $h_X \to h_Y$. Then h is fully faithful.

Remark 3.9.4. The functor h from the corollary is called the *contravariant Yoneda embedding* of $\mathscr{C}$ into $\hat{\mathscr{C}} = \mathrm{Hom}(\mathscr{C}^{\mathrm{op}}, \mathscr{S}et)$.

Remark 3.9.5. [BLR90, p. 96] The functor h from the corollary commutes with direct products, i. e. if $X \times X$ exists in $\mathscr{C}$, then $h(X \times X) = h(X) \times h(X)$.

With Yoneda's Lemma we can draw a close connection between representable functors into $\mathscr{G}rp$ and group objects:

Proposition 3.9.6. *[Oor66, I.1-1f] Let $\mathscr{C}$ be a category as in Definition 3.9.1. Then group objects in $\mathscr{C}$ correspond to representable functors $F : \mathscr{C}^{\mathrm{op}} \to \mathscr{G}rp$; here $\mathscr{G}rp$ denotes the category of groups, and 'representable' means that the functor $U \circ F$ is representable, where $U : \mathscr{G}rp \to \mathscr{S}et$ is the forgetful functor[3]. The commutative group objects correspond to representable functors F, that factor through $\mathscr{A}b$, the category of Abelian groups, in the sense that there exists a functor $G : \mathscr{C}^{\mathrm{op}} \to \mathscr{A}b$ such that $F = \iota \circ G$, where $\iota : \mathscr{A}b \to \mathscr{G}rp$ is the inclusion functor.*

Proof. Given a group object G, one can make the functor $\mathrm{Hom}_{\mathscr{C}}(-, G)$ into a functor $\mathscr{C} \to \mathscr{G}rp$ by defining a composition law for every object $X \in \mathscr{C}$ by

$$\mathrm{Hom}_{\mathscr{C}}(X, G) \times \mathrm{Hom}_{\mathscr{C}}(X, G) \to \mathrm{Hom}_{\mathscr{C}}(X, G), \qquad (f, g) \mapsto m(f, g).$$

The commuting diagrams in the definition of a group object show that this composition law is a group law. Clearly, if the group object is commutative, then the resulting groups are also commutative.

Conversely, let $F : \mathscr{C} \to \mathscr{G}rp$ be a functor that is represented by an object $G \in \mathscr{C}$. The group law gives a natural map

$$\mathrm{Hom}_{\mathscr{C}}(A, G) \times \mathrm{Hom}_{\mathscr{C}}(A, G) \to \mathrm{Hom}_{\mathscr{C}}(A, G)$$

for every object $A \in \mathscr{C}$, which form a natural transformation $h_G \times h_G \to h_G$. Now, by Remark 3.9.5, we have $h_G \times h_G = h_{G \times G}$ and, therefore, by Corollary 3.9.3, we get that the natural transformation $h_G \times g_G \to h_G$ corresponds to a morphism $m : G \times G \to G$ in $\mathscr{C}$. By the same construction, the inversion morphism on $\mathrm{Hom}_{\mathscr{C}}(A, G)$,

[3] The *forgetful functor* $U : \mathscr{G}rp \to \mathscr{S}et$ assigns its underlying set to every group, and its underlying map between sets to every group morphism. Therefore, it "forgets the group structure".

$A \in \mathscr{C}$ gives a morphism $i : G \to G$. Now S is a final object in $\mathscr{C}$ and, therefore, $\mathrm{Hom}_{\mathscr{C}}(A, S) = 0$, $A \in \mathscr{C}$. But then there is a natural transformation $h_S \to h_G$ corresponding to a morphism $e : S \to G$.

We will show that G, together with the morphisms $m : G \times G \to G$, $i : G \to G$ and $e : S \to G$, defines a group object in $\mathscr{C}$. We show this exemplary for the first diagram in Definition 3.9.1 (a). Let $\hat{m} : h_G \times h_G \to h_G$ be the natural transformation corresponding to the group law. Consider the natural transformations

$$\hat{m} \times \mathbf{id} : (h_G \times h_G) \times h_G \to h_G \times h_G$$

and

$$\mathbf{id} \times \hat{m} : h_G \times (h_G \times h_G) \to h_G \times h_G.$$

Clearly the diagram

$$\begin{tikzcd}
(h_G \times h_G) \times h_G \arrow[r, "\hat{m}\times\mathbf{id}"] \arrow[d, equal] & h_G \times h_G \arrow[dd, "\hat{m}"] \\
h_G \times (h_G \times h_G) \arrow[d, "\mathbf{id}\times\hat{m}"'] & \\
h_G \times h_G \arrow[r, "\hat{m}"'] & h_G
\end{tikzcd}$$

of natural transformations commutes. But now, by using $h_G \times h_G = h_{G\times G}$ and $h_G \times h_G \times G = h_{G\times G\times G}$, we see that the first diagram in Definition 3.9.1 (a), mapped by h, results in this commuting diagram. Since h is fully faithful, the first diagram in Definition 3.9.1 (a) also commutes. □

3.9.2 Group Objects in the Category of S-Schemes

We now apply the results from the last subsection to the category $\mathscr{S}ch(S)$ of S-schemes. We saw at the beginning of this section that $\mathscr{S}ch(S)$ satisfies all assumptions of Proposition 3.9.6.

Definition 3.9.7. *A* group scheme *over S is a group object in the category $\mathscr{S}ch(S)$. Moreover, an* Abelian scheme *X over S is a group scheme of finite type over S, which has connected fibres and which is smooth and proper over S.*

Remark 3.9.8. [Oor66, I.1-3] For group schemes, 'geometrically connected fibres' and 'connected fibres' are the same concepts.

It turns out that Abelian schemes have many interesting properties, which also justify why they are called Abelian:

Proposition 3.9.9. *Let X be an Abelian scheme. Assume that S is Noetherian, and that X is locally Noetherian.*

(a) *[MFK65, p. 117, Corollary 6.4] Let G a group scheme over S, which is locally Noetherian, and let $f : X \to G$ be an S-morphism. Assume that f satisfies $f \circ e_X = e_G$. Then f is a homomorphism.*

(b) *[MFK65, p. 117, Corollary 6.5] The group structure of X is commutative.*

(c) *[MFK65, p. 117, Corollary 6.6] If m' is another group law on X with the same identity e_X, then $m' = m_X$.*

We will see in Chapter 4 that (generalized) elliptic curves are an example of an Abelian scheme.

3.9.3 Examples for Functors

We will now give three examples of functors. The third one will be the one we need in Chapter 4, where we will show how it can be represented in some cases.

Examples 3.9.10. Let $X \to S$ be a flat morphism of schemes, which is of finite presentation.

(a) According to [BLR90, p. 214], we have a functor

$$\mathrm{CDiv}_{X/S} : \mathscr{S}ch(S)^{op} \to \mathscr{S}et, \qquad S' \mapsto \mathrm{CDiv}(X_{S'}/S'),$$

where $\mathrm{CDiv}(X/S)$ denotes the set of relative effective Cartier divisors on X over S.

(b) Moreover, consider the functor

$$\mathrm{Pic}_{X/S} : \mathscr{S}ch(S)^{op} \to \mathscr{A}b, \qquad S' \mapsto \mathrm{Pic}(X_{S'})/\operatorname{Pic}(S'),$$

where $\mathrm{Pic}(S)$ is seen as a subgroup of $\mathrm{Pic}(X)$ by use of $f^* : \mathrm{Pic}(S) \to \mathrm{Pic}(X)$ (see Proposition 3.5.27).

Example 3.9.11. Let X be a generalized smooth curve, which is proper over S and has geometrically connected fibres, and let $k \in \mathbb{Z}$ be any integer. Note that for an invertible sheaf on X one can define a degree for every fibre over S (see [Har77, p. 149, ch. II, Exercise 6.12], as each fibre of X is a proper smooth curve over a field; or take a generalization of [KM85, p. 9, Definition 1.2.5] or Proposition 3.8.22 to arbitrary invertible sheaves). Consider the functor

$$\mathrm{Pic}^{(k)}_{X/S} : \mathscr{S}ch(S)^{op} \to \mathscr{S}et, \qquad S' \mapsto \mathrm{Pic}^{(k)}(X_{S'}/S') := \mathrm{Pic}^{(k)}(X_{S'})/_{\sim},$$

where $\mathrm{Pic}^{(k)}(X)$ denotes the subset of $\mathrm{Pic}(X)$ of isomorphism classes of invertible sheaves, which are fibre-by-fibre of degree k, and where $[\mathcal{L}] \sim [\mathcal{L}']$ if, and only if, there exists an invertible sheaf $\mathcal{L}_0$ on S', such that $\mathcal{L} \cong \mathcal{L}' \otimes f^*(\mathcal{L}_0)$ (see [KM85, p. 64]). For $k = 0$ the functor $\mathrm{Pic}^{(0)}_{X/S}$ factors through $\mathscr{A}b$.

We will see in the next chapter that if X is a generalized elliptic curve over S, then $\mathrm{Pic}^{(0)}_{X/S}$ is represented by X and, therefore, X/S is an Abelian scheme. This demonstrates how useful Proposition 3.9.6 is to show that an object $G \in \mathscr{C}$ is a group object, i.e. there exist morphisms $m : G \times G \to G$, $i : G \to G$ and $e : S \to G$ which satisfy the requirements of Definition 3.9.1 (a). One 'just' has to show that G represents a functor $\mathscr{C} \to \mathscr{A}b$.

Chapter 4

Elliptic Curves

4.1 Definition of Elliptic Curves

We now want to use the tools developed in the last chapters to analyze elliptic curves. The special property of an elliptic curve over a field $\mathbb{F}$ is that for any extension field $\mathbb{K}$ of $\mathbb{F}$, the set of $\mathbb{K}$-rational points can be turned into a group in a natural way. We begin by defining what an elliptic curve is.

Definition 4.1.1. *Let $\mathbb{F}$ be a field. An* elliptic curve E (defined over $\mathbb{F}$) *is a complete smooth curve of genus one defined over $\mathbb{F}$, given with an $\mathbb{F}$-rational point $\infty \in E(\mathbb{F})$.*

It is often useful to embed an object of interest into a larger context. An example are schemes: one embeds the category of varieties into the larger categories of schemes. For this we first want to generalize the notion of an elliptic curve to this larger category, by defining a "generalized" elliptic curve over a base scheme as in [KM85, Section 2].

Definition 4.1.2. *Let S be an arbitrary scheme, E be a proper smooth curve over S, and let $\infty \in E(S)$ be a global section. Then $(E/S, \infty)$ or simply E/S is called a* generalized elliptic curve *if the fibres of E are geometrically connected and of genus one.*

Remarks 4.1.3.

(a) Note that sometimes in the literature the terminus 'generalized elliptic curve' is used in another way. In this thesis we use the added 'generalized' to emphasize that the usual elliptic curves over a field are special cases of such elliptic curves.

(b) Let S be any scheme and E a proper smooth curve over S. The condition that the fibres of E are geometrically connected and of genus one means that the geometric fibres of E are elliptic curves (in sense of Definition 4.1.1) over an algebraically closed field. Moreover, the fibre is an elliptic curve defined over the residue field at that point.

That a generalized elliptic curve is indeed a generalization of an ordinary elliptic curve (over a field) can be seen from the following two results:

Proposition 4.1.4. *Let (E, ∞) be an elliptic curve over $\mathbb{F}$. Then E is a generalized elliptic curve.*

Proof. By Proposition 3.8.5, $E \to \operatorname{Spec} \mathbb{F}$ is a proper smooth curve. Since ∞ is a $\mathbb{F}$-rational point, it clearly is a section in $E(\operatorname{Spec} \mathbb{F})$ (see Proposition 3.6.8). □

Proposition 4.1.5. *Let (E, ∞) be a generalized elliptic curve over $S = \operatorname{Spec} \mathbb{F}$ for an algebraically closed field $\mathbb{F}$. Then (E, ∞) is an elliptic curve (in the sense of Definition 4.1.1). If $\mathbb{F}$ is not algebraically closed, then the geometric fibre of E at the only point of S is an elliptic curve (in the sense of Definition 4.1.1) defined over $\overline{\mathbb{F}}$.*

Proof. In this case E is equal to the fibre of E at the only point of S, which equals the geometric fibre of E at this point. But by Remark 4.1.3 (b) this is an elliptic curve. The second statement also follows from this remark. □

4.1.1 The Group Law

As already mentioned, there is a natural group structure associated to the $\mathbb{K}$-rational points of an elliptic curve over a field $\mathbb{F}$, where $\mathbb{K}$ is an extension field of $\mathbb{F}$. This is also true for generalized elliptic curves, as Katz and Mazur have shown with their following theorem:

Theorem 4.1.6 (Abel). *[KM85, p. 63, Theorem 2.1.2] Let (E, ∞) be a generalized elliptic curve over a base scheme S, with structure morphism $f : E \to S$. Then there exists a unique structure of commutative group scheme on E over S, such that for any S-scheme T, and any three points $P, Q, R \in E_T(T)$, we have $P + Q = R$ if, and only if, there exists an invertible sheaf $\mathcal{L}_0$ on T and an isomorphism of invertible sheaves on E_T such that*

$$\mathscr{I}_{[P]}^{-1} \otimes \mathscr{I}_{[Q]}^{-1} \otimes \mathscr{I}_{[\infty_T]} \cong \mathscr{I}_{[R]}^{-1} \otimes f_T^*(\mathcal{L}_0).$$

Idea of Proof (as in [KM85, pp. 63ff, Proof of Theorem 2.1.2]). Recall that in Example 3.9.11 we defined $\operatorname{Pic}^{(k)}(E_T/T)$ for $k \in \mathbb{N}$ and an S-scheme T as the set of isomorphism classes of invertible sheaves on E_T, which are fibre-by-fibre of degree k, modulo the relation $\mathcal{L} \sim \mathcal{L}'$ if there exists an invertible sheaf $\mathcal{L}_0$ on T, such that $\mathcal{L} \cong \mathcal{L}' \otimes f^*(\mathcal{L}_0)$. The proof proceeds in three steps:

(1) The idea is to show that the map

$$E(T) \to \operatorname{Pic}^{(1)}(E_T/T), \qquad P \mapsto [\mathscr{I}_{[P]}^{-1}]$$

is bijective. Then by composition with the bijection

$$\operatorname{Pic}^{(1)}(E_T/T) \to \operatorname{Pic}^{(0)}(E_T/T), \qquad [\mathcal{L}] \mapsto [\mathcal{L} \otimes \mathscr{I}_{[\infty]}],$$

we have a bijective map $E(T) \to \operatorname{Pic}^{(0)}(E_T/T)$. Now $\operatorname{Pic}^{(0)}(E_T/T)$ is an Abelian group and, moreover, this construction is clearly functorial (note Example 3.9.11) and hence gives a contravariant functor $\mathscr{S}ch(S)^{op} \to \mathscr{A}b$, which is represented by E. By Proposition 3.9.6 we have, therefore, shown the existence of the group law. Moreover, the uniqueness is given by the definition of $\operatorname{Pic}^{(0)}(E_T/T)$, the definition of the map $E(T) \to \operatorname{Pic}^{(0)}(E_T/T)$, and the relation

$$\mathscr{I}_{[P]}^{-1} \otimes \mathscr{I}_{[Q]}^{-1} \otimes \mathscr{I}_{[\infty_T]} \cong \mathscr{I}_{[R]}^{-1} \otimes f_T^*(\mathcal{L}_0)$$

for some invertible sheaf $\mathcal{L}_0$ on T.

(2) To show that $E(T) \to \operatorname{Pic}^{(1)}(E_T/T)$ is bijective, one first reduces to $T = S$ by base extension, as $E(T) = E_T(T)$.

The next step is to show that we can assume S to be affine by showing that the question is local on S: for that assume $\mathcal{L}_1$ and $\mathcal{L}_2$ are invertible sheaves on E, that U_i, $i \in I$, is an open covering of S, and that we have invertible sheaves $\mathcal{L}_{0,i}$ on U_i and isomorphisms $\mathcal{L}_1|_{f^{-1}(U_i)} \cong \mathcal{L}_2|_{f^{-1}(U_i)} \otimes_{f^{-1}(U_i)} f^*(\mathcal{L}_{0,i})$. We have to show that there exists an invertible sheaf $\mathcal{L}_0$ on S such that $\mathcal{L}_1 \cong \mathcal{L}_2 \otimes_{\mathcal{O}_E} f^*(\mathcal{L}_0)$.

For a proof of this see [KM85, pp. 65f].

(3) Thus, we can assume $S = \operatorname{Spec} R$, and R can be assumed to be Noetherian [GD67, p. 34, Proposition 8.9.1] since $f : E \to S$ is of finite presentation.

As the last step (which is the largest part of the proof), one shows that the map is bijective by explicitly constructing its inverse. This construction can be found in [KM85, pp. 66f]. □

Remarks 4.1.7.

(a) In the group law in the theorem, ∞_T is the neutral element, as for every $P \in E(T)$ we have

$$\mathscr{I}_{[P]}^{-1} \otimes \mathscr{I}_{[\infty_T]}^{-1} \otimes \mathscr{I}_{[\infty_T]} \cong \mathscr{I}_{[P]}^{-1} \cong \mathscr{I}_{[P]}^{-1} \otimes f_T^*(\mathcal{O}_{E_T}).$$

(b) By [KM85, p. 77, Theorem 2.5.1] this is the only way to make E/S into a commutative group scheme, which has ∞ as its neutral element. In the case that S is Noetherian and E is locally Noetherian, this also follows from Proposition 3.9.9 (c).

In Section 4.2.2 (Corollary 4.2.10) we will give a complete proof for the special case that (E, ∞) is an elliptic curve (in the sense of Definition 4.1.1) using the Riemann-Roch Theorem.

If R_1 and R_2 are two rings, then $S = \operatorname{Spec}(R_1 \times R_2)$ is the disjoint union of $\operatorname{Spec} R_1$ and $\operatorname{Spec} R_2$ by Lemma 3.3.35. If E is a curve over S with structure morphism f, then E is the disjoint union of $E_1 := f^{-1}(\operatorname{Spec} R_1)$ and $E_2 := f^{-1}(\operatorname{Spec} R_2)$. If E/S is a generalized elliptic curve, then $E_1/\operatorname{Spec} R_1$ and $E_2/\operatorname{Spec} R_2$ are also generalized elliptic curves. The following corollary relates the group scheme of E/S with the ones of $E_1/\operatorname{Spec} R_1$ and $E_2/\operatorname{Spec} R_2$.

Corollary 4.1.8. *Let (E, ∞) be a generalized elliptic curve over $S = \operatorname{Spec}(R_1 \times R_2)$, and let $f : E \to S$ be the structure morphism. Then $E_i := E|_{f^{-1}(\operatorname{Spec} R_i)}$ is a generalized elliptic curve over $S_i = \operatorname{Spec} R_i$, $i = 1, 2$, and the group law on E/S is the product of the group laws on E_1/S_1 and E_2/S_2, in the sense that the group $E(S)$ is naturally isomorphic to the product $E_1(S_1) \times E_2(S_2)$.*

Proof. There is a natural bijection $E(S) \cong E_1(S_1) \times E_2(S_2)$, since S is the disjoint union of S_1 and S_2 (see Lemma 3.3.35) and, therefore, E is the disjoint union of E_1 and E_2, and both S_i and E_i, $i = 1, 2$ are both closed and open in S or E, respectively.

To see that this bijection is a group morphism, note that by the Proof of Theorem 4.1.6, the group law is local on S. □

Now assume that $S = \operatorname{Spec} R$ with $\operatorname{Pic}(S) = 0$. (Recall that in Section 2.4 we characterized this condition; see also Corollary 3.5.3.) In this case every invertible sheaf on S is isomorphic to $\mathcal{O}_S$. Therefore, $f^*(\mathcal{L}_0)$ is always isomorphic to $\mathcal{O}_E$ for every invertible sheaf $\mathcal{L}_0$ on S (see Proposition 3.5.27). Therefore we have the following:

Corollary 4.1.9. *Let (E, ∞) be a generalized elliptic curve over a base $S = \operatorname{Spec} R$ with $\operatorname{Pic}(S) = 0$ (see Corollary 3.5.3). Then three sections $A, B, C \in E(S)$ satisfy $A + B = C$ if, and only if,*

$$\mathscr{I}_{[A]}^{-1} \otimes \mathscr{I}_{[B]}^{-1} \cong \mathscr{I}_{[C]}^{-1} \otimes \mathscr{I}_{[\infty]}^{-1},$$

where the isomorphism is a isomorphism of invertible sheaves on E. By Proposition 3.5.31, this is the case if, and only if,

$$\mathcal{L}([A] + [B]) \cong \mathcal{L}([C] + [\infty])$$

or, equivalently,

$$[A] + [B] \sim [C] + [\infty].$$

Recall that a field $\mathbb{F}$ trivially fulfills $\operatorname{Pic}(\operatorname{Spec} \mathbb{F}) = 0$ by Proposition 2.4.27 and Corollary 3.5.3.

4.2 Elliptic Curves over Fields

We first want to investigate the case of elliptic curves over fields. Most of the material in this section is quite standard and can be found in many textbooks, for example [Sil86]. It turns out that many of these results can be generalized for generalized elliptic curves, as in the book of Katz and Mazur (see [KM85, Chapter 2]). As we will not need these generalized results, we refer the interested reader to the book of Katz and Mazur. However, we will mention some of these results at appropriate places.

4.2.1 Weierstraß Equation

In this section we will investigate curves defined by so-called Weierstraß equations. We will get an explicit criterion when such a curve is smooth, and we will see that the smooth ones of these curves are, up to isomorphism, exactly the elliptic curves.

Definition 4.2.1. *Let R be any ring. Then a equation of the form*

$$y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3,$$

where $a_1, a_2, a_3, a_4, a_6 \in R$, is called a Weierstraß equation *over R. Define the values*

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1 a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24 b_4, \\
\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\
\text{and} \qquad j &= c_4^3/\Delta.
\end{aligned}$$

Then Δ *is called the* discriminant *and* j *the* j-invariant *for this Weierstraß equation. An equation of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is called an inhomogenous Weierstraß equation*.*

Definition 4.2.2. *Let* $P = (x : y : z) \in \mathbb{P}^2_{\mathbb{F}}$*. Then* P *is called* finite *or* affine *if* $z \neq 0$*, and otherwise* infinite *or a* point at infinity*.*

Let E be a curve defined by a Weierstraß equation over a field $\mathbb{F}$. Our aim is to show that the curve is smooth if, and only if, $\Delta \neq 0$. In this process we also derive some normal forms that can be assumed for special characteristics; the results will be presented in Corollary 4.2.8. We follow the discussion in [Sil86, pp. 46–51 and pp. 324ff].

To show this we use the Jacobian criterion from Theorem 3.2.28 and we distinguish the two cases whether the characteristic of $\mathbb{F}$ is two or not. But before that, note that if $(x : y : 0) \in E(\mathbb{F})$, then $0 = f(x, y, 0) = -x^3$ and, thus, $(x : y : 0) = (0 : y : 0)$. Therefore, E has exactly one infinite point $\infty := (0 : 1 : 0)$.

Characteristic of $\mathbb{F}$ is $\neq 2$: In this case 2 is invertible in $\mathbb{F}$ and we use this fact to complete the square:

$$\begin{aligned} y^2 + (a_1x + a_3z)y &= \left(y + \tfrac{a_1x+a_3z}{2}\right)^2 - \left(\tfrac{a_1x+a_3z}{2}\right)^2 \\ &= \left(y + \tfrac{a_1x+a_3z}{2}\right)^2 - \frac{a_1^2x^2 + 2a_1a_3xz + a_3^2z^2}{4}. \end{aligned}$$

Consider the linear map

$$\varphi : \langle x, y, z\rangle_{\mathbb{F}} \to \langle x, y, z\rangle_{\mathbb{F}}, \qquad \begin{cases} x \mapsto x, \\ y \mapsto \frac{1}{2}y - \frac{a_1x+a_3z}{2}, \\ z \mapsto z, \end{cases}$$

which is clearly bijective since the associated matrix has determinant $\frac{1}{2}$. We get

$$\begin{aligned} f \circ \varphi &= \tfrac{1}{4}y^2z - \tfrac{1}{4}a_1^2x^2z - \tfrac{1}{2}a_1a_3xz^2 - \tfrac{1}{4}a_3^2z^3 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \\ &= \tfrac{1}{4}y^2z - x^3 - \left(\tfrac{1}{4}a_1^2 + a_2\right)x^2z - \left(\tfrac{1}{2}a_1a_3 + a_4\right)xz^2 - \left(\tfrac{1}{4}a_3^2 + a_6\right)z^3 \\ &= \tfrac{1}{4}y^2z - x^3 - \tfrac{1}{4}b_2x^2z - \tfrac{1}{2}b_4xz^2 - \tfrac{1}{4}b_6z^3. \end{aligned}$$

Hence, E is smooth if, and only if, the curve $\hat{E}$ defined by $y^2z = 4x^3 + b_2x^2z + 2b_4xz^2 + b_6z^3$ is smooth (this follows from the Jacobian criterion in Theorem 3.2.28). Let $g := y^2z - 4x^3 - b_2x^2z - 2b_4xz^2 - b_6z^3$. Then we have

$$\begin{aligned} \frac{\partial g}{\partial x} &= -12x^2 - 2b_2xz - 2b_4z^2, \\ \frac{\partial g}{\partial y} &= 2yz \\ \text{and} \qquad \frac{\partial g}{\partial z} &= y^2 - b_2x^2 - 4b_4xz - 3b_6z^2. \end{aligned}$$

If we consider the only infinite point $\infty = (0 : 1 : 0) \in \hat{E}(\mathbb{F})$, we see that $\frac{\partial g}{\partial z}(0, 1, 0) = 1$, and therefore $\hat{E}$ is smooth at ∞. If we consider $(x : y : 1) \in \hat{E}(\mathbb{F})$ for $y \neq 0$, we see that $\frac{\partial g}{\partial y}(x,y,1) = 2y \neq 0$; thus the only points where $\hat{E}$ might not be smooth are the ones of the form $(x:0:1)$. Consider the polynomial

$$g(x,0,1) = -4x^3 - b_2x^2 - 2b_4x - b_6 \in \mathbb{F}[x].$$

The curve is smooth if, and only if, this polynomial and its derivative with respect to x have no common roots in $\overline{\mathbb{F}}$ (since $\frac{\partial g(x,0,1)}{\partial x}(x) = \frac{\partial g}{\partial x}(x,0,1)$), which is the case if, and only if, the polynomial has only simple roots. By Corollary 2.1.16 the polynomial has only simple roots if, and only if,

$$\begin{aligned} 0 \neq \operatorname{Res}\big(g, \tfrac{\partial g}{\partial x}\big) &= (-4)^5\big(4(\tfrac{1}{4}b_2)^3(\tfrac{1}{4}b_6) - 18(\tfrac{1}{4}b_2)(\tfrac{1}{2}b_4)(\tfrac{1}{4}b_6) \\ &\quad + 27(\tfrac{1}{4}b_6)^2 - (\tfrac{1}{4}b_2)^2(\tfrac{1}{2}b_4)^2 + 4(\tfrac{1}{2}b_4)^3\big) \\ &= \tfrac{1}{4^3}\big(-\tfrac{1}{4}b_2^3b_6 + 9b_2b_4b_6 - 27b_6^2 + \tfrac{1}{4}b_2^2b_4^2 - 8b_4^3\big)= \tfrac{\Delta}{2^6}. \end{aligned}$$

Thus, the curve is smooth if, and only if, $\Delta \neq 0$.

Characteristic of $\mathbb{F}$ is $= 2$: Let E be given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

In characteristic 2 we have

$$\begin{aligned} b_2 &= a_1^2, & b_4 &= a_1a_3, \\ b_6 &= a_3^2, & b_8 &= a_1^2a_6 + a_1a_3a_4 + a_2a_3^2 + a_4^2, \\ c_4 &= b_2^2, & \Delta &= b_2^2b_8 + b_6^2 + b_2b_4b_6 \\ & \text{and} & j &= c_4^3/\Delta. \end{aligned}$$

Hence

$$\Delta = a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_3^4 + a_1^3a_3^3 \quad \text{and} \quad j = \frac{a_1^{12}}{\Delta}.$$

We consider two sub-cases:

We have $a_1 = 0$: Consider the linear map

$$\varphi : \langle x,y,z\rangle_{\mathbb{F}} \to \langle x,y,z\rangle_{\mathbb{F}}, \qquad \begin{cases} x \mapsto x + a_2z, \\ y \mapsto y, \\ z \mapsto z. \end{cases}$$

This is clearly bijective, and we get

$$\begin{aligned} g := f \circ \varphi = y^2z &+ a_3yz^2 - (x + a_2z)^3 - a_2(x+a_2z)^2z \\ &- a_4(x+a_2z)z^2 - a_6z^3 \\ &= y^2z + a_3yz^2 - x^3 - a_2x^2z - a_2^2xz^2 - a_2^3z^3 \\ &- a_2x^2z - a_2^3z^3 - a_4xz^2 - a_2a_4z^3 - a_6z^3 \\ &= y^2z + a_3yz^2 - x^3 - (a_2^2 + a_4)xz^2 - (a_2a_4 + a_6)z^3. \end{aligned}$$

Moreover, we have that $\Delta = a_3^4$. Let $\hat{E}$ be the curve defined by g; again E is smooth if, and only if, $\hat{E}$ is smooth. We have

$$\begin{aligned} &\frac{\partial g}{\partial x} = x^2 + (a_2^2 a_4) z^2, \\ &\frac{\partial g}{\partial y} = a_3 z^2 \\ \text{and} \qquad &\frac{\partial g}{\partial z} = y^2 + (a_2 a_4 + a_6) z^2. \end{aligned}$$

Therefore, $\hat{E}$ is smooth at ∞, since $\frac{\partial g}{\partial z}(0,1,0) = 1$ and, if $\Delta \neq 0$, the curve $\hat{E}$ is smooth at every other point since $\frac{\partial g}{\partial y} = a_3 z^2$. On the contrary, assume $\Delta = 0$. Then the curve is smooth if, and only if, for every point $(x : y : 1) \in \hat{E}(\mathbb{F})$, $\frac{\partial g}{\partial x}(x,y,1) = x^2 + (a_2^2 a_4) \neq 0$. But in the algebraic closure of $\mathbb{F}$ we can clearly find an x satisfying $x^2 = -a_2^2 a_4$, and then a y satisfying $f(x,y,1) = 0$ with this x. Therefore, the curve is not smooth in this case.

We have $a_1 \neq 0$: Consider the linear map

$$\varphi : \langle x,y,z \rangle_{\mathbb{F}} \to \langle x,y,z \rangle_{\mathbb{F}}\,, \qquad \begin{cases} x \mapsto a_1^2 x + \frac{a_3}{a_1} z, \\ y \mapsto a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} z, \\ z \mapsto z. \end{cases}$$

This is clearly bijective and we get

$$\begin{aligned} \frac{1}{a_1^6} f \circ \varphi &= (a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3 z)^2 z \\ &\quad + a_1 (a_1^2 x + a_3/a_1 z)(a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3 z) z \\ &\quad + a_3 (a_1^3 y + (a_1^2 a_4 + a_3^2)/a_1^3 z) z^2 - (a_1^2 x + a_3/a_1 z)^3 \\ &\quad - a_2 (a_1^2 x + a_3/a_1 z)^2 z - a_4 (a_1^2 x + a_3/a_1 z) z^2 - a_6 z^3 \\ &= y^2 z + xyz - x^3 - \frac{a_3 + a_1 a_2}{a_1^3} x^2 z \\ &\quad - \frac{a_1^4 a_2 a_3^2 + a_1^5 a_3 a_4 + a_1^3 a_3^3 + a_3^4 + a_1^4 a_4^2 + a_1^6 a_6}{a_1^{12}} z^3 \\ &= y^2 z + xyz - x^3 - \frac{a_3 + a_1 a_2}{a_1^3} x^2 z - \frac{\Delta}{a_1^{12}} z^3 \end{aligned}$$

Define $g := y^2 z + xyz - x^3 - ((a_3 + a_1 a_2)/a_1^3) x^2 z - (\Delta / a_1^{12}) z^3 \in \mathbb{F}[x,y,z]$. Again we work with the curve $\hat{E}$ defined by g, which is smooth if, and only if, E is smooth. We have

$$\begin{aligned} &\frac{\partial g}{\partial x} = yz + x^2, \\ &\frac{\partial g}{\partial y} = xz \\ \text{and} \qquad &\frac{\partial g}{\partial z} = y^2 + xy - \frac{a_3 + a_1 a_2}{a_1^3} x^2 - \frac{\Delta}{a_1^{12}} z^2. \end{aligned}$$

The curve $\hat{E}$ is smooth at ∞ as $\frac{\partial g}{\partial z}(0,1,0) = 1$. Moreover, the curve is smooth at $(x : y : 1) \in \hat{E}(\mathbb{F})$ if, and only if, $x \neq 0$ or $y + x^2 \neq 0$. Thus, the only point where the curve can be singular is $(0 : 0 : 1)$. But $g(0,0,1) = \Delta / a_1^{12}$ and hence the curve has a singular point if, and only if, $\Delta = 0$.

Hence, we have gained the following proposition:

Proposition 4.2.3. *Let $\mathbb{F}$ be any field, and let E be the curve defined by the Weierstraß equation*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. Then the curve is smooth if, and only if, the discriminant Δ is $\neq 0$.

Moreover, if the characteristic of $\mathbb{F}$ is not two, then by the bijective linear transformation

$$\langle x, y, z\rangle_{\mathbb{F}} \to \langle x, y, z\rangle_{\mathbb{F}}, \qquad \begin{cases} x \mapsto x, \\ y \mapsto \frac{1}{2}(y - (a_1x + a_3z)), \\ z \mapsto z \end{cases}$$

the Weierstraß equation becomes

$$y^2z = 4x^3 + b_2x^2z + 2b_4xz^2 + b_6z^3.$$

(For the values b_i and Δ see Definition 4.2.1.)

From now on let $\mathbb{F}$ be a field that is perfect. By Proposition 2.2.28 this includes the case of algebraically closed fields. We will now prove that the elliptic curves defined over $\mathbb{F}$ are exactly the smooth curves given by a Weierstraß equation and, moreover, characterize their isomorphisms.

Proposition 4.2.4. *[Sil86, p. 63, ch. III, Proposition 3.1]*

(1) *Let (E, ∞) be an elliptic curve defined over $\mathbb{F}$. Then there exist functions $x, y \in \mathbb{F}(E)$ such that they define a map $E \to \mathbb{P}^2_{\overline{\mathbb{F}}}$, $P \mapsto (x(P) : y(P) : 1)$, which is an isomorphism of E with the curve defined by a Weierstraß equation, and that ∞ is mapped onto $(0 : 1 : 0)$. Moreover, $\mathbb{F}(E) = \mathbb{F}(x, y)$ and $[\mathbb{F}(E) : \mathbb{F}(x)] = 2$.*

    This Weierstraß equation is unique up to linear changes of coordinates by

    $$x' = u^2x + r, \qquad y' = u^3y + su^2x + t$$

    for $u, r, s, t \in \mathbb{F}$, $u \neq 0$.

(2) *If E is a smooth curve defined by a Weierstraß equation over $\mathbb{F}$, then it is an elliptic curve defined over $\mathbb{F}$, with $\infty = (0 : 1 : 0)$. (In fact, $\mathbb{F}$ can be* any *field for this part, and does not have to be perfect.)*

(3) *Two elliptic curves defined over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$, defined by Weierstraß equations, are isomorphic over $\overline{\mathbb{F}}$ if, and only if, their j-invariants are the same.*

Proof.

(1) Since ∞ is an $\mathbb{F}$-rational point, $n[\infty]$ is a divisor defined over $\mathbb{F}$ for any $n \in \mathbb{N}$. Therefore, $\Gamma(E, \mathcal{L}(n[\infty]))$ has a basis of functions defined over $\mathbb{F}$ according to Proposition 3.8.9. Since E has genus one, we get $\ell(n[\infty]) = n$ for every $n \geq 1$ according to Riemann-Roch (Proposition 3.7.46 (d)).

Now $\Gamma(E, \mathcal{L}(2[\infty]))$ has a basis $\{1, x\}$, where $x \in \mathbb{F}(E)$, and $\Gamma(E, \mathcal{L}(3[\infty]))$ has a basis $\{1, x, y\}$, where $y \in \mathbb{F}(E)$. The function x must have at least one pole and it can have at most a double pole at ∞. But if x had a single pole at ∞, then x^2 would also be in $\Gamma(E, \mathcal{L}(2[\infty]))$: a contradiction. Therefore x has a double pole at ∞. If y has a pole of order less than 3, then $y \in \Gamma(E, \mathcal{L}(2[\infty]))$, a contradiction.

Now one sees that 1, x, y and x^2 form a basis of $\Gamma(E, \mathcal{L}(4[\infty]))$, and 1, x, y, x^2 and xy form a basis of $\Gamma(E, \mathcal{L}(5[\infty]))$. Moreover, both the sets $\{1, x, y, x^2, xy, x^3\}$ and $\{1, x, y, x^2, xy, y^2\}$ form a basis of $\Gamma(E, \mathcal{L}(6[\infty]))$. Therefore, there exist $a_0, \ldots, a_6 \in \mathbb{F}$, not all zero, such that

$$a_0y^2 + a_1xy + a_3y + a_5x^3 + a_2x^2 + a_4x + a_6 = 0.$$

Now both a_0 and a_5 must be non-zero, since both the sets $\{1, x, y, x^2, xy, y^2\}$ and $\{1, x, y, x^2, xy, x^3\}$ are linearly independent. By replacing y by $a_0a_6^2y$ and x by a_0a_6x, and then dividing the resulting equation by $a_0^3a_6^4 \neq 0$, we obtain an equation $f \in \mathbb{F}[x, y]$ in inhomogenous Weierstraß form.

Define $\varphi : E \to V_{\overline{\mathbb{F}}}(f)$ by $P \mapsto (x(P) : y(P) : 1)$. According to Proposition 3.7.16 this defines a morphism. If $P = \infty$, then $\varphi(P) = (0 : 1 : 0)$, as y has a higher pole order than x. Since the only point mapped to $(0 : 1 : 0)$ is ∞ we see that φ is not constant. Therefore, by Proposition 3.7.8, it is finite and surjective, and $V_{\overline{\mathbb{F}}}(f)$ is smooth and, further, $\deg \varphi = [\mathbb{F}(E) : \mathbb{F}(x, y)] < \infty$. We have to show that $\deg \varphi = 1$, as then φ is an isomorphism.

But now x has exactly one double pole at ∞. Consider the map $\psi : E \to \mathbb{P}^1_{\mathbb{F}}$ defined by $P \mapsto (x(P) : 1)$. Then, according to Proposition 3.7.15 (a), we get $\deg \psi = 2$, i. e. $[\mathbb{F}(E) : \mathbb{F}(x)] = 2$. By the same argument we get $[\mathbb{F}(E) : \mathbb{F}(y)] = 3$. But since $[\mathbb{F}(E) : \mathbb{F}(x, y)]$ divides both $[\mathbb{F}(E) : \mathbb{F}(x)]$ and $[\mathbb{F}(E) : \mathbb{F}(y)]$, the former must be one. Therefore, we have $\mathbb{F}(E) = \mathbb{F}(x, y)$.

Let x', y' be two other functions defined over $\mathbb{F}$ which satisfy that $\{1, x'\}$ is a basis of $\Gamma(E, \mathcal{L}(2[\infty]))$ and $\{1, x', y'\}$ a basis of $\Gamma(E, \mathcal{L}(3[\infty]))$. Then we can write $x' = \alpha_0 + \alpha_1x$ and $y' = \beta_0 + \beta_1x + \beta_2y$ with $\alpha_i, \beta_j \in \mathbb{F}$. But since both x, y and x', y' satisfy a Weierstraß equation where the coefficients of x^3 and y^2 are one, it must be that $\beta_2^2 = \alpha_1^3$. Defining $u = \beta_2/\alpha_1$ and $s = \beta_1/u^2$ gives the form as in the statement.

(2) Let E be given by a smooth Weierstraß equation, and $\infty = (0 : 1 : 0)$. According to Proposition 3.7.40, the genus of E is $\frac{1}{2}(3-2)(3-1) = 1$ and, therefore, (E, ∞) is an elliptic curve.

Another proof to show that E has genus one is to use Proposition 4.2.29: it says that $0 \in \mathrm{WDiv}(E)$ is a canonical divisor and, therefore, the genus of E is $\frac{1}{2} \deg 0 + 1 = 1$ according to Riemann-Roch (Proposition 3.7.46 (c)).

(3) That the j-invariant is invariant under isomorphisms as in (a) can be verified by tedious calculations (see also [Sil86, p. 49, ch. III]). A proof for the converse can be found in [Sil86, pp. 50ff, ch. III, Proposition 1.4 (b) and pp. 325ff, A, Proposition 1.2 (b)]. □

Remark 4.2.5. If E is a generalized elliptic curve over $S = \operatorname{Spec} R$, Katz and Mazur have shown that E is up to isomorphism $\operatorname{Proj} R[x,y,z]/\langle f\rangle$, where f is a Weierstraß equation. Since the proof makes use of some tools which we have not introduced, we refer the interested reader to [KM85, pp. 67–69, Section 2.2].

By part (c) of the proposition, the following definition makes sense:

Definition 4.2.6. *Let E be an elliptic curve over a perfect field $\mathbb{F}$. Define the j-invariant of E, denoted by $j(E)$, to be the j-invariant of one (and thus of all) Weierstraß equations belonging to E.*

Finally in this subsection, we will show how the coordinates of the Weierstraß equation change after applying the isomorphisms from part (a) of the proposition and, moreover, we want to give special forms for different characteristics and j-invariants.

Remark 4.2.7. According to Proposition 4.2.4 (1), two elliptic curves given by Weierstraß equations over $\mathbb{F}$ are isomorphic over $\mathbb{F}$ if one curve can be obtained from the other by a coordinate transform of the form

$$x' = u^2x + rz, \qquad y' = u^3y + su^2x + tz, \qquad z' = z$$

for $u, r, s, t \in \mathbb{F}$, $u \neq 0$. Let

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0$$

be the Weierstraß equation of an elliptic curve. By plugging in the transformation and by dividing by u^6 we get

$$\begin{aligned}
0 &= \frac{(y')^2z + a_1x'y'z + a_3y'z^2 - (x')^3 - a_2(x')^2z - a_4x'z^2 - a_6z^3}{u^6}\\
&= y^2z + \frac{2su^5 + a_1u^5}{u^6}xyz + \frac{2u^3t + a_1u^3r + a_3u^3}{u^6}yz^2 - x^3\\
&- \frac{3u^4r + a_2u^4 - s^2u^4 - a_1su^4}{u^6}x^2z\\
&- \frac{-2su^2t - a_1u^2t - a_1su^2r - a_3su^2 + 3u^2r^2 + 2a_2u^2r + a_4u^2}{u^6}xz^2\\
&- \frac{-t^2 - a_1tr - a_3t + r^3 + a_2r^2 + a_4r + a_6}{u^6}z^3.
\end{aligned}$$

Therefore, we get the following coefficients for the new curve:

$$\begin{aligned}
a_1' &= \frac{2s + a_1}{u},\\
a_3' &= \frac{2t + a_1r + a_3}{u^3},\\
a_2' &= \frac{3r + a_2 - s^2 - a_1s}{u^2},\\
a_4' &= \frac{-2st - a_1t - a_1sr - a_3s + 3r^2 + 2a_2r + a_4}{u^4}\\
\text{and} \qquad a_6' &= \frac{-t^2 - a_1tr - a_3t + r^3 + a_2r^2 + a_4r + a_6}{u^6}.
\end{aligned}$$

Corollary 4.2.8. *Let $\mathbb{F}$ be a perfect field and $E/\mathbb{F}$ an elliptic curve defined over $\mathbb{F}$.*

(a) *If the characteristic of $\mathbb{F}$ is neither 2 nor 3, then E is isomorphic to a curve given by a Weierstraß equation*

$$y^2z = x^3 + a_4xz^2 + a_6z^3,$$

and we have

$$\Delta = -16(4a_4^3 + 27a_6^2) \neq 0 \qquad \textit{and} \qquad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

Any $\mathbb{F}$-isomorphism of two such Weierstraß equations has the form

$$x' = u^2x, \quad y' = u^3y, \quad z' = z, \qquad \textit{where } u \in \mathbb{F}^*,$$

and the coefficients of the new Weierstraß equation are

$$a_4' = \frac{a_4}{u^4} \quad \textit{and} \quad a_6' = \frac{a_6}{u^6}.$$

(b) *If the characteristic of $\mathbb{F}$ is 2 and $j(E) = 0$, then E is isomorphic to a curve given by a Weierstraß equation*

$$y^2z + a_3yz^2 = x^3 + a_4xz^2 + a_6z^3,$$

and we have

$$\Delta = a_3^4 \neq 0 \qquad \textit{and} \qquad j = 0.$$

Any $\mathbb{F}$-isomorphism of two such Weierstraß equations has the form

$$x' = u^2x + s^2z, \quad y' = u^3y + u^2sx + tz, \quad z' = z,$$

where $u \in \mathbb{F}^*$ and $s, t \in \mathbb{F}$, and the coefficients of the new Weierstraß equation are

$$a_3' = \frac{a_3}{u^3}, \quad a_4' = \frac{a_3s + s^4 + a_4}{u^4} \quad \textit{and} \quad a_6' = \frac{t^2 + a_3t + s^6 + a_4s^2 + a_6}{u^6}.$$

(c) *If the characteristic of $\mathbb{F}$ is 2 and $j(E) \neq 0$, then E is isomorphic to a curve given by a Weierstraß equation*

$$y^2z + xyz = x^3 + a_2x^2z + a_6z^3,$$

and we have

$$\Delta = a_6 \neq 0 \qquad \textit{and} \qquad j = \frac{1}{a_6}.$$

Any $\mathbb{F}$-isomorphism of two such Weierstraß equations has the form

$$x' = x, \quad y' = y + sx + a_3sz, \quad z' = z, \qquad \textit{where } s \in \mathbb{F},$$

and the coefficients of the new Weierstraß equation are

$$a_2' = a_2 + s(s+1) \quad \textit{and} \quad a_6' = a_6.$$

(d) *If the characteristic of* $\mathbb{F}$ *is* 3 *and* $j(E) = 0$*, then* E *is isomorphic to a curve given by a Weierstraß equation*

$$y^2 z = x^3 + a_4 x z^2 + a_6 z^3,$$

and we have

$$\Delta = -a_4^3 \neq 0 \qquad \textit{and} \qquad j = 0.$$

Any $\mathbb{F}$*-isomorphism of two such Weierstraß equations has the form*

$$x' = u^2 x + rz, \quad y' = u^3 y, \quad z' = z, \qquad \textit{where } u \in \mathbb{F}^* \textit{ and } r \in \mathbb{F},$$

and the coefficients of the new Weierstraß equation are

$$a_4' = \frac{a_4}{u^4} \quad \textit{and} \quad a_6' = \frac{r^3 + a_4 r + a_6}{u^6}.$$

(e) *If the characteristic of* $\mathbb{F}$ *is* 3 *and* $j(E) \neq 0$*, then* E *is isomorphic to a curve given by a Weierstraß equation*

$$y^2 z = x^3 + a_2 x^2 z + a_6 z^3,$$

and we have

$$\Delta = -a_2^3 a_6 \neq 0 \qquad \textit{and} \qquad j = -\frac{a_2^3}{a_6}.$$

Any $\mathbb{F}$*-isomorphism of two such Weierstraß equations has the form*

$$x' = u^2 x, \quad y' = u^3 y, \quad z' = z, \qquad \textit{where } u \in \mathbb{F}^*,$$

and the coefficients of the new Weierstraß equation are

$$a_2' = \frac{a_2}{u^2} \quad \textit{and} \quad a_6' = \frac{a_6}{u^6}.$$

Proof. See [Sil86, p. 324, A, Proposition 1.1], Proposition 4.2.4 and Remark 4.2.7, and the discussion in Section 4.2.1. □

4.2.2 (Geometric) Group Law

In Section 4.1.1 we saw that one can define a natural group law on the points of an elliptic curve, and we have seen in Corollary 4.1.9 that, for elliptic curves over fields, the group law of an elliptic curve E comes from $\mathrm{Pic}^0(E)$. In the first part of this subsection we will prove Corollary 4.1.9 for this case. Thus, let E denote an elliptic curve in the following, which is defined over a field $\mathbb{F}$.

Proposition 4.2.9. *Let* D *be a Weil divisor on* E *of degree zero. Then there exists a unique* $P \in E(\mathbb{F})$ *such that* $D \sim [P] - [\infty]$.

Proof. By Riemann-Roch (Proposition 3.7.46 (d)) we have $\dim \Gamma(E, \mathcal{L}([P])) = 1$ for every $P \in E(\mathbb{F})$ and, hence, $\Gamma(E, \mathcal{L}([P])) = \overline{\mathbb{F}}$, where $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$. Therefore, if $[P] \sim [Q]$ for some $P, Q \in E(\mathbb{F})$, and $f \in \overline{\mathbb{F}}(E)^*$ such that $\mathrm{div}(f) = [P] - [Q]$, then $f \in \overline{\mathbb{F}}^*$ and, therefore, $P = Q$. Thus, if $[Q] - [\infty] \sim D \sim [P] - [\infty]$ it follows that $P = Q$.

Now consider the divisor $D + [\infty]$, which has degree one. By Riemann-Roch (Proposition 3.7.46 (d)),

$$\dim \Gamma(E, \mathcal{L}(D + [\infty])) = 1.$$

Let $f \in \Gamma(E, \mathcal{L}(D + [\infty])) \setminus \{0\}$. Then $\operatorname{div}(f) \geq -D - [\infty]$, and since $\deg \operatorname{div}(f) = 0 = \deg(-D - [\infty]) - 1$, we see that $\operatorname{div}(f) - [P] = -D - [\infty]$ for some $P \in E(\mathbb{F})$. But this means $D \sim [P] - [\infty]$. □

Corollary 4.2.10. *Let E be an elliptic curve. Then the map*

$$\sigma : E \to \operatorname{Pic}^0(E), \qquad P \mapsto [[P] - [\infty]]$$

is a bijection.

It is a well-known fact that this "abstractly" defined group law has a geometric interpretation that leads to explicit formulae for adding two points. As at the beginning, it is not clear how this geometric group law is connected to the abstract group law from Theorem 4.1.6. As it is, in fact, a group law, we will at the beginning treat it as another operation on $E(\mathbb{F})$. This operation will be denoted by $\hat{+}$ and is defined as follows:

By the Theorem of Bézout (Theorem 3.2.33), every line meets the elliptic curve in exactly three (not necessarily distinct) points. We define an operation $\oplus$ on E such that $P \oplus Q$ is the third point on the line going through P and Q, where the tangent to E is taken instead of the line if $P = Q$. (Note that for this case it is important that E is smooth.) We further define another operation $\hat{+}$ on E by $P \hat{+} Q := (P \oplus Q) \oplus \infty$; this adds a so called *reflection* to $\oplus$. This operation is also called the *Chord and Tangent Law.*

The following proposition now draws the connection between the geometric addition $\hat{+}$ and the abstract addition $+$:

Proposition 4.2.11. *If $P, Q, R \in E(\mathbb{F})$ are three points, then $P \hat{+} Q = R$ if, and only if, $P + Q = R$.*

Proof. Assume that $P \hat{+} Q = R$. It is enough to show that $P + Q = R$, since for both operations $+$ and $\hat{+}$ there is exactly one R, which makes these statements true.

Let L_1 be the line through P and Q, which meets E in $P \oplus Q$, and let L_2 be the line through $P \oplus Q$ and ∞, which meets E in R. Let $f_i \in \mathbb{F}[x, y, z]_1$ be the defining equation of L_i, $i = 1, 2$. According to Proposition 3.7.33 we have

$$\begin{aligned} 0 \sim \operatorname{div}\left(\frac{f_1}{f_2}\right) &= ([P] + [Q] + [P \oplus Q]) - ([P \oplus Q] + [\infty] + [R]) \\ &= [P] + [Q] - [\infty] - [R] \end{aligned}$$

and, therefore, $P + Q = R$ by Corollary 4.1.9. □

The rest of this subsection is devoted to explicitly finding formulae for the group law on $E(\mathbb{F})$, and for computing the inverse of a point with respect to this group law. For this let $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$ be points on E, and assume E is given by

$$f := y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3 \in \mathbb{F}[x, y, z], \qquad (*)$$

where $\mathbb{F}$ is algebraically closed. We will later see that if $\mathbb{F}$ is any field over which the curve is defined, then $E(\mathbb{F})$ is a group.

Recall Corollary 2.2.43, which says that if $\sum_{i=0}^{n} a_i x^i$ is a monic polynomial in one indeterminate of degree n for which $n-1$ distinct roots $\alpha_1, \ldots, \alpha_{n-1}$ are known. Then

$$-a_{n-1} - \sum_{i=1}^{n-1} \alpha_i$$

is the remaining root. Also recall Remark 2.2.44.

The Inverse of a Point Let $P_2 = -P_1$ and assume that P_1 is finite. According to the definition of the Chord and Tangent Law we get P_2 by laying a vertical line through P_1. The line meets E in P_1, ∞ and P_2. Since $P_1 + \infty = \infty$ would imply $P_1 = \infty$, it must be that P_2 is finite. Therefore $x_2 = x_1$, $z_2 = z_1 = 1$, and we just need to find y_2. Consider the equation $f(x_1, y, 1) = 0$:

$$y^2 + (a_1 x_1 + a_3) y = x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6.$$

We know that the equation has the solution $y = y_1$ in $\mathbb{F}$ and, hence, according to Corollary 2.2.43, the second solution is given by

$$y_2 = -\left(a_1 x_1 + a_3 + y_1\right).$$

For an arbitrary point $(x_1 : y_1 : z_1) \neq \infty$ on E, we thus have

$$\begin{aligned} -(x_1 : y_1 : z_1) &= -\left(x_1/z_1 : y_1/z_1 : 1\right) \\ &= \left(x_1/z_1 : -a_1 x_1/z_1 - a_3 - y_1/z_1 : 1\right) \\ &= \left(x_1 : -a_1 x_1 - a_3 z_1 - y_1 : z_1\right). \end{aligned}$$

Note that if one plugs $(x_1 : y_1 : z_1) = (0 : 1 : 0)$ into this formula, one gets $(0 : -1 : 0) = (0 : 1 : 0)$. Therefore, this formula is valid for every point on the curve and we have the following proposition:

Proposition 4.2.12. *Let E be an elliptic curve over an algebraically closed field $\mathbb{F}$ defined by the Weierstraß equation $(*)$, and let $P = (x : y : z) \in E(\mathbb{F})$. Then*

$$-P = (x : -a_1 x - a_3 z - y : z).$$

Moreover, if both E and P are defined over a subfield $\mathbb{K}$ of $\mathbb{F}$, then $-P$ is also defined over $\mathbb{K}$.

The Line Through Two Points Since ∞ is the identity, it is enough to consider the case that both P_1 and P_2 are finite. Therefore, we can assume $z_1 = z_2 = 1$. Assume $x_1 \neq x_2$. Then the line through P_1 and P_2 has the slope

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2},$$

and the equation $y = \lambda x + v$, where $v = y_1 - \lambda x_1 = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$. Now, assume $x_1 = x_2$ and $P_1 \neq -P_2$ and, thus, in particular $y_1 = y_2$. By Definition 3.7.35, the tangent at E in $P_1 = P_2$ has the slope

$$\lambda = -\frac{\frac{\partial f}{\partial x}(P_1)}{\frac{\partial f}{\partial y}(P_1)} = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}.$$

Another way to write this is

$$\lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2(x_1 + x_2) + a_4 - a_1y_2}{y_1 + y_2 + a_1x_1 + a_3},$$

since $P_1 = P_2$. Moreover, if $P_1 \neq P_2$, then

$$\frac{x_1^2 + x_1x_2 + x_2^2 + a_2(x_1 + x_2) + a_4 - a_1y_2}{y_1 + y_2 + a_1x_1 + a_3} = \frac{y_1 - y_2}{x_1 - x_2}$$

when both sides are defined, as an elementary computation shows (since P_1 and P_2 lie on E, they satisfy the Weierstraß equation; by subtracting these and cancelling/adding terms one can reach this identity) (see [Sil86, pp. 69f, Remark 3.6.1]).

The Sum of Two Points Now assume that the line given by $y = \lambda x + v = \lambda x + (y_1 - \lambda x_1) = \lambda(x - x_1) + y_1$ meets the elliptic curve in the points $P_1 = (x_1 : y_1 : 1)$ and $P_2 = (x_2 : y_2 : 1)$. By the Theorem of Bézout we know that it meets the curve at a third point $P_3 = (x_3 : y_3 : 1)$. When plugging the equation of the line into $f(x, y, 1) = 0$, we get

$$\begin{aligned}0 &= f(x, \lambda(x - x_1) + y_1, 1)\\ &= \lambda^2(x - x_1)^2 + 2\lambda(x - x_1)y_1 + y_1^2\\ &\quad + (a_1x + a_3)(\lambda(x - x_1) + y_1) - x^3 - a_2x^2 - a_4x - a_6\\ &= -x^3 + \left(\lambda^2 + a_1\lambda - a_2\right)x^2 + \text{lower order terms.}\end{aligned}$$

Since we know that x_1 and x_2 are solutions for this equation, by Corollary 2.2.43 and Remark 2.2.44 we get

$$x_3 = -\left(-\lambda^2 - a_1\lambda + a_2 + x_1 + x_2\right) = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

By using $y = \lambda(x - x_1) + y_1$ we can hence compute $y_3^* = \lambda(x_3 - x_1) + y_1$. After reflecting this, we get

$$y_3 = -y_3^* - a_1x_3 - a_3 = -(\lambda + a_1)x_3 + \lambda x_1 - y_1 - a_3.$$

Therefore, we gained the following proposition, which describes the group law explicitly for all pairs (P_1, P_2) of points $P_1, P_2 \in E(\mathbb{F})$:

Proposition 4.2.13. *Let E be an elliptic curve over an algebraically closed field $\mathbb{F}$ defined by the Weierstraß equation (*). Let $P_i = (x_i : y_i : z_i) \in E(\mathbb{F})$, $i = 1, 2$.*

(a) *Assume that both $P_1 \neq \infty \neq P_2$ and, therefore, $z_1 = z_2 = 1$. If then $x_1 \neq x_2$, then we have $P_1 + P_2 = (x_3 : y_3 : 1)$, where*

$$\begin{aligned}\lambda &= \frac{y_1 - y_2}{x_1 - x_2},\\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2\\ \textit{and}\qquad y_3 &= -(\lambda + a_1)x_3 + \lambda x_1 - y_1 - a_3.\end{aligned}$$

(b) *Assume that both $P_1 \neq \infty \neq P_2$ and, therefore, $z_1 = z_2 = 1$. Moreover, assume that $P_1 \neq -P_2$. If then $y_1 + y_2 + a_1x_1 + a_3 \neq 0$ (which is always the case if $P_1 = P_2 \neq -P_1$), then we have $P_1 + P_2 = (x_3 : y_3 : 1)$, where*

$$\begin{aligned}\lambda &= \frac{x_1^2 + x_1x_2 + x_2^2 + a_2(x_1 + x_2) - a_1y_2 + a_4}{y_1 + y_2 + a_1x_1 + a_3},\\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2\\ \textit{and}\qquad y_3 &= -(\lambda + a_1)x_3 + \lambda x_1 - y_1 - a_3.\end{aligned}$$

(c) *If $P_1 = \infty$, then $P_1 + P_2 = P_2$; if $P_2 = \infty$, then $P_1 + P_2 = P_1$; and if $P_1 = -P_2$, then $P_1 + P_2 = \infty$.*

(d) *The cases (a)–(c) cover all possible pairs of points (P_1, P_2).*

If $\mathbb{K}$ is a subfield of $\mathbb{F}$ such that P_1, P_2 and E are defined over $\mathbb{K}$, then also $P_1 + P_2$ is defined over $\mathbb{K}$.

Corollary 4.2.14. *Let E be an elliptic curve defined over any field $\mathbb{F}$. Then the $\mathbb{F}$-rational points of E form a group, which is a subgroup of the $\overline{\mathbb{F}}$-rational points, where $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.*

Actually this is also implied by Theorem 4.1.6 and Proposition 4.1.4, as $E/\operatorname{Spec}\mathbb{F}$ is a generalized elliptic curve.

Corollary 4.2.15. *Let $P = (x : y : 1) \in E(\mathbb{F})$ and $(x' : y' : z') = Q := P + P \in E(\mathbb{F})$. Then*

$$\frac{x'}{z'} = \frac{x^4 + b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

if the denominator on the right side is non-zero.

We close this subsection by showing that the group law is a morphism, which can be seen as a part of the proof of Theorem 4.1.6 in the case of a generalized elliptic curve over $\operatorname{Spec}\mathbb{F}$, since in this special case we cannot use Yoneda's Lemma via Proposition 3.9.6. Note that if one assumes Theorem 4.1.6 to be true, then the following statement follows from Theorem 4.1.6 and Definition 3.9.1.

Proposition 4.2.16. *[Sil86, p. 68, Theorem 3.6] Let E be an elliptic curve over an algebraically closed field $\mathbb{F}$. Then the functions of the group law, $+ : E \times E \to E$ and $- : E \to E$, are morphisms of varieties. Moreover, the translation-by-P map $\tau_P : Q \mapsto Q + P$ is an isomorphism for every $P \in E(\mathbb{F})$.*

Moreover, one can get rational maps $\psi_i : E \times E \to E$, $1 \leq i \leq n$, such that

(i) *if ψ_i is defined for $P, Q \in E(\mathbb{F})$, then $\psi_i(P, Q) = P + Q$; and*

(ii) *for every pair $P, Q \in E(\mathbb{F})$ there is an i such that $\psi_i(P, Q)$ is defined.*

Proof. By Proposition 4.2.12 the map $- : E \to E$ is clearly a morphism. Consider the τ_P map, $P \in E(\mathbb{F}) \setminus \{\infty\}$. By Proposition 4.2.13, it can be given by a polynomial that is valid for all but the three points P, $-P$ and ∞. Therefore, τ_P is clearly a dominant rational map. By Proposition 3.7.16 it is, therefore, a morphism. Clearly $\tau_P \circ \tau_{-P} = \mathbf{id}_E = \tau_{-P} \circ \tau_P$ and, therefore, τ_P is an isomorphism.

Now let $P, Q \in E(\mathbb{F})$ be two points. Let $\varphi : E \times E \to E$ be the map defined by the formulae in Proposition 4.2.13(a). This is clearly a rational function that is undefined for pairs of the form (R, R), (∞, R), (R, ∞) and $(R, -R)$, $R \in E$. Consider $\psi_{P,Q} : E \times E \to E$, where

$$\psi_{P,Q} = \tau_P \circ \tau_Q \circ \varphi \circ (\tau_{-P} \times \tau_{-Q}).$$

Clearly $\psi_{P,Q}$ is a rational map, and $\psi_{P,Q}(R_1, R_2) = R_1 + R_2$ if $\psi_{P,Q}(R_1, R_2)$ is defined. But $\psi_{P,Q}$ is only undefined for pairs of points of the form $(R + P, R + Q)$, $(P, R + Q)$ and $(R + P, Q)$, $R \in E(\mathbb{F})$. Therefore, by varying P and Q, one gets a set of rational maps $\psi_1, \ldots, \psi_n : E \times E \to E$ which satisfy (i) and (ii). □

4.2.3 Complete Systems of Addition Laws

Let E be an elliptic curve over an algebraically closed field $\mathbb{F}$ given by the Weierstraß equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. In Proposition 4.2.13 we saw that the group law on elliptic curves over fields can be described by explicit formulae. Unfortunately, this set of formulae includes several special cases, or in more exact terms, some of the formulae are only defined on Zariski closed sets. By Proposition 4.2.16, it is possible to find a set of formulae that works on Zariski open subsets of $E \times E$. Unfortunately, the proposition gives no easy way to find a set of these formulae that not only works for all pairs of points, but is also parameterized by a_1 to a_6 and hence can be used for any elliptic curve. In this subsection we will see that it is possible to not only find formulae that are better with respect to the named criteria above but also work over every field and, as we will see later, also for curves over rings.

Definition 4.2.17. *(Compare [LR85, LR87, BL95].)*

(a) *A triple $\psi = (\psi_i)_{i=0,1,2} \in (\mathbb{F}[x_1, y_1, z_1, x_2, y_2, z_2])^3$ is called an* addition law *if the following conditions hold:*

  (i) *There exist positive integers $d_i > 0$, $i = 1, 2$, such that if seen as a polynomial in x_i, y_i, z_i, the ψ_j's are homogenous of degree d_i, $j = 0, 1, 2$. We then say that the ψ_j's are* bihomogenous *of* bidegree (d_1, d_2).

  (ii) *For every two points $P_1 = (x_1 : y_1 : z_1)$, $P_2 = (x_2 : y_2 : z_2) \in E(\mathbb{F})$, for $x_3 = \psi_1(P_1, P_2)$, $y_3 = \psi_2(P_2, P_2)$, $z_3 = \psi_3(P_1, P_2)$ we either have $x_3 = y_3 = z_3 = 0$ or $(x_3 : y_3 : z_3) = P_1 + P_2 \in E(\mathbb{F})$. In the second case we say that ψ is* defined *for P_1 and P_2.*

If $\psi = (\psi_i)_i$ is an addition law, let $D(\psi)$ denote the open subset of $E(\mathbb{F}) \times E(\mathbb{F})$ for which ψ is defined.

(b) *Two addition laws $\psi = (\psi_i)_i$ and $\varphi = (\varphi_i)_i$ are said to be* equivalent *if there exists an $\lambda \in \mathbb{F}^*$ such that $\psi_i = \lambda\varphi_i$ for all i.*

(c) *A* complete set of addition laws *is a set A of addition laws $\psi \in A$, such that $\bigcup\{D(\psi) \mid \psi \in A\} = E(\mathbb{F}) \times E(\mathbb{F})$.*

The formulae from Proposition 4.2.13 (a) can easily be used to obtain a group law that is defined on the Zariski open set

$$(E(\mathbb{F}) \times E(\mathbb{F})) \setminus \{(\infty, P), (P, \infty), (P, P), (P, -P) \mid P \in E(\mathbb{F})\},$$

by homogenization and using the common denominator $(x_1z_2 - x_2z_1)^3(z_1z_2)^3$. But one can do better by using the common denominator $(x_1z_2 - x_2z_1)^3(z_1z_2)$, and replacing x_i^3 by

$$y_i^2z_i + a_1x_iy_iz_i + a_3y_iz_i^2 - a_2x_i^2z_i - a_4x_iz_i^2 - a_6z_i^3.$$

This can be achieved for example by the following MuPAD$^{\text{TM}}$ [MuP05] code:

```
PRETTYPRINT := FALSE;
f := y^2*z + a_1*y*x*z + a_3*y*z^2 - a_2*x^2*z - a_4*x*z^2 - a_6*z^3
f1 := subs(f, {x=x_1,y=y_1,z=z_1});
f2 := subs(f, {x=x_2,y=y_2,z=z_2});
simp := g -> expand(subsex(expand(g), \
        x_1^3=f1, x_1^4=x_1*f1, x_2^3=f2, x_2^4=x_2*f2))

lambda := simplify((y_1/z_1 - y_2/z_2) / (x_1/z_1 - x_2/z_2));
xx_3 := (lambda^2 + a_1*lambda - a_2 - x_1/z_1 - x_2/z_2);
yy_3 := (-(lambda + a_1)*(lambda^2 + a_1*lambda - a_2 - x_1/z_1 \
        - x_2/z_2) + lambda*x_1/z_1 - y_1/z_1 - a_3);
z1_3 := simplify(lcm(denom(xx_3), denom(yy_3)))/(z_1*z_2)^2;
x1_3 := simplify(xx_3 * z1_3);
y1_3 := simplify(yy_3 * z1_3);
psi_0 := simp(simp(x1_3));
psi_1 := simp(simp(y1_3));
psi_2 := simp(simp(z1_3));
```

The resulting addition law is

$$\begin{aligned}\psi_0 &= 2x_1y_1y_2z_2 - 2x_2y_1y_2z_1 + 2a_3x_1y_2z_1z_2 - 2a_3x_2y_1z_1z_2\\ &\quad + x_1y_2^2z_1 - x_2y_1^2z_2 - a_1x_2^2y_1z_1 + a_2x_1x_2^2z_1 + a_1x_1^2y_2z_2\\ &\quad - a_2x_1^2x_2z_2 + a_3x_1y_1z_2^2 - a_3x_2y_2z_1^2 - 3a_6x_1z_1z_2^2 + 3a_6x_2z_1^2z_2\\ &\quad - a_4x_1^2z_2^2 + a_4x_2^2z_1^2,\end{aligned}$$

$$\begin{aligned}\psi_1 &= 2a_1x_2y_1y_2z_1 - 2a_1x_1y_1y_2z_2 + 2a_2x_1x_2y_1z_2 - 2a_2x_1x_2y_2z_1\\ &\quad - 2a_4x_1y_2z_1z_2 + 2a_4x_2y_1z_1z_2 - 2a_1a_3x_1y_2z_1z_2 + 2a_1a_3x_2y_1z_1z_2\\ &\quad + 3x_1x_2^2y_1 - 3x_1^2x_2y_2 + y_1y_2^2z_1 - y_1^2y_2z_2 + a_2x_2^2y_1z_1 + 3a_3x_1x_2^2z_1\\ &\quad - a_2x_1^2y_2z_2 - 3a_3x_1^2x_2z_2 + a_4x_1y_1z_2^2 - a_4x_2y_2z_1^2 + 3a_6y_1z_1z_2^2\\ &\quad - 3a_6y_2z_1^2z_2 - a_1a_2x_1x_2^2z_1 + a_1a_2x_1^2x_2z_2 + 3a_1a_6x_1z_1z_2^2\\ &\quad - a_3a_4x_1z_1z_2^2 - 3a_1a_6x_2z_1^2z_2 + a_3a_4x_2z_1^2z_2 + a_1a_4x_1^2z_2^2\\ &\quad - a_1a_4x_2^2z_1^2 - a_2a_3x_1^2z_2^2 + a_2a_3x_2^2z_1^2 + a_1^2x_2^2y_1z_1\\ &\quad - a_1^2x_1^2y_2z_2 + a_3^2y_1z_1z_2^2 - a_3^2y_2z_1^2z_2\end{aligned}$$

and

$$\begin{aligned}\psi_2 &= 3x_1^2x_2z_2 - 3x_1x_2^2z_1 - a_1x_1y_1z_2^2 + a_1x_2y_2z_1^2 - a_3y_1z_1z_2^2\\ &\quad + a_4x_1z_1z_2^2 + a_3y_2z_1^2z_2 - a_4x_2z_1^2z_2 - y_1^2z_2^2 + y_2^2z_1^2 + a_2x_1^2z_2^2\\ &\quad - a_2x_2^2z_1^2.\end{aligned}$$

Note that ψ_0, ψ_1 and ψ_2 are actually polynomials in the ring

$$\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x_1, y_1, z_1, x_2, y_2, z_2].$$

In [BL95], Bosma and Lenstra show that this system works for every pair $P_1, P_2 \in E(\mathbb{F})^2$ such that $P_1 \neq P_2$. In fact, they show much more: they show that there exists a complete set of addition laws with two addition laws and that these addition laws are necessarily of bidegree $(2, 2)$. Moreover, they characterize all such complete sets of addition laws and give a way to effectively compute them.

Note that before [BL95], Lange and Ruppert first gave a complete system of addition laws of bidegree $(2, 2)$, consisting of three formulae for elliptic curves of the form $y^2z = 4x^3 - g_2xz^2 - g_3z^3$ over fields of characteristic not equal to 2 or 3 in

[LR85, Section 3], and then a complete system of addition laws of bidegree $(2, 2)$ consisting of three formulae which works for elliptic curves, defined by a Weierstraß equation as in this thesis, and over arbitrary fields.

We now want to state the main results from [BL95] and show how a second addition formula can be computed, such that this new one with the one above forms a complete set of addition laws for every elliptic curve over every field.

Theorem 4.2.18 (W. Bosma, H. W. Lenstra). *Let E be an elliptic curve defined by a Weierstraß equation over any algebraically closed field $\mathbb{F}$.*

(a) *[BL95, p. 230, Theorem 1] A complete system of addition laws consists of at least two addition laws. If a complete system of addition laws has exactly two addition laws, both must be of bidegree $(2, 2)$.*

(b) *[BL95, p. 230, Theorem 2] There is a bijection between $\mathbb{P}^2(\mathbb{F})$ and the set of equivalence classes of addition laws with the following property:*

If $(a : b : c) \in \mathbb{P}^2(\mathbb{F})$ corresponds to the addition law ψ, then ψ is defined for $(P_1, P_2) \in E(\mathbb{F}) \times E(\mathbb{F})$ if, and only if, $P_1 - P_2$ does not lie on the line defined by $ax + by + cz = 0$ in $\mathbb{P}^2(\mathbb{F})$.

Since there are pairs of lines in $\mathbb{P}^2(\mathbb{F})$ that intersect outside $E(\mathbb{F})$, complete systems of addition laws with exactly two addition laws do exist. Two such lines are, for example, $y = 0$ and $z = 0$.

According to [BL95, pp. 236f], the addition law given above corresponds to the point $(0 : 0 : 1) \in \mathbb{P}^2(\mathbb{F})$, i.e. it is undefined exactly for the pairs of points (P_1, P_2) satisfying $P_1 = P_2$.

Finally, we want to specify a second addition law. To be more precise we will present the one corresponding to $(0 : 1 : 0)$, such that we get a complete system of addition laws. According to [BL95, p. 236], for this we can define

$$\psi_i' := \psi_i(P_1, -P_2) = \psi_i(x_1, y_1, z_1, x_2, -y_2 - a_1x_2 - a_3z_2, z_2),$$

and choose $\varphi_i := \psi_i \cdot \frac{\psi_1'}{\psi_2'}$. After simplifying the φ_i's and reducing as much as possible, one obtains (up to equivalence) the addition law corresponding to $(0 : 1 : 0)$.

To see that the φ_i's are polynomials one can proceed as follows. Note that $f = gh$ in $R/\langle g_1, \ldots, g_k\rangle$ means that one can write $f = gh + \sum g_ih_i$ with $h, h_i \in R$. In this case we have $R := \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, x_2, y_2, z_2]$, and with the help of the computer algebra system MAGMA$^{\text{TM}}$ [CAG04] we can write $\psi_i\psi_1' = \psi_2'g_i + f_1g_{1,i} + f_2g_{2,i}$ in R for polynomials $g_i, g_{1,i}, g_{2,i}$, where $f_1 = f(x_1, y_1, z_1)$ and $f_2 = f(x_2, y_2, z_2)$ are Weierstraß equations. Then $\varphi_i = g_i$. But first we need $\varphi_{i,numer} := \psi_i\psi_1'$, $i = 0, 1, 2$ and ψ_2', which can be computed, for example, in MuPAD$^{\text{TM}}$ with the following code:

```
phi_0numer := simplify(psi_0*subs(psi_1, y_2 = -y_2-a_1*x_2-a_3*z_2));
phi_1numer := simplify(psi_1*subs(psi_1, y_2 = -y_2-a_1*x_2-a_3*z_2));
phi_2numer := simplify(psi_2*subs(psi_1, y_2 = -y_2-a_1*x_2-a_3*z_2));
den := expand(subs(psi_2, y_2 = -y_2-a_1*x_2-a_3*z_2));
```

Before executing these lines one needs to execute the code listed above, which computes the ψ_i's.

Then in MAGMA$^{\text{TM}}$ one can proceed with the following code, where `phi_0numer`, `phi_1numer`, `phi_2numer` (the $\varphi_{i,numer}$'s) and `den` (the denominator, i. e. ψ_2') are replaced with the result from MuPAD$^{\text{TM}}$:

```
S<a_1,a_2,a_3,a_4,a_6,x_1,y_1,z_1,x_2,y_2,z_2> := PolynomialRing(IntegerRing(), 11);

f1 := a_1*x_1*y_1*z_1 - x_1^3 - a_6*z_1^3 + y_1^2*z_1 - a_2*x_1^2*z_1 \
      + a_3*y_1*z_1^2 - a_4*x_1*z_1^2;
f2 := a_1*x_2*y_2*z_2 - x_2^3 - a_6*z_2^3 + y_2^2*z_2 - a_2*x_2^2*z_2 \
      + a_3*y_2*z_2^2 - a_4*x_2*z_2^2;

J := IdealWithFixedBasis([den, f1, f2]);
phi_0 := Coordinates(J, phi_0numer)[1];
phi_1 := Coordinates(J, phi_1numer)[1];
phi_2 := Coordinates(J, phi_2numer)[1];
```

This gives the following results:

$$\begin{aligned}
\varphi_0 = {} & a_1^2a_3a_4x_1z_1z_2^2 - a_1^3a_6x_1z_1z_2^2 - a_1^2a_3a_6z_1^2z_2^2 - a_1^2a_3x_1^2x_2z_2 \\
& - a_1^2a_6y_1z_1z_2^2 - a_1^2a_6z_1^2y_2z_2 + a_1^2x_1y_1x_2^2 - a_1a_2a_3^2x_1z_1z_2^2 \\
& - 4a_1a_2a_6x_1z_1z_2^2 - a_1a_2x_1^2x_2^2 + a_1a_3^2a_4z_1^2z_2^2 - a_1a_3^2x_1^2z_2^2 \\
& - 2a_1a_3^2x_1z_1x_2z_2 + a_1a_3a_4y_1z_1z_2^2 + a_1a_3a_4z_1^2y_2z_2 - a_1a_3x_1^2y_2z_2 \\
& + a_1a_3y_1z_1x_2^2 + a_1a_4^2x_1z_1z_2^2 - 2a_1a_4x_1^2x_2z_2 - a_1a_4x_1z_1x_2^2 \\
& - 3a_1a_6x_1^2z_2^2 - 6a_1a_6x_1z_1x_2z_2 + 2a_1x_1y_1x_2y_2 + a_1y_1^2x_2^2 \\
& - a_2a_3^3z_1^2z_2^2 - a_2a_3^2y_1z_1z_2^2 - a_2a_3^2z_1^2y_2z_2 - 4a_2a_3a_6z_1^2z_2^2 \\
& - a_2a_3x_1z_1x_2^2 - 4a_2a_6y_1z_1z_2^2 - 4a_2a_6z_1^2y_2z_2 - a_2x_1^2x_2y_2 \\
& - a_2x_1y_1x_2^2 - a_3^3x_1z_1z_2^2 - a_3^3z_1^2x_2z_2 - a_3^2x_1y_1z_2^2 \\
& - 2a_3^2x_1z_1y_2z_2 + a_3a_4^2z_1^2z_2^2 - 2a_3a_4x_1z_1x_2z_2 - a_3a_4z_1^2x_2^2 \\
& - 3a_3a_6x_1z_1z_2^2 - 6a_3a_6z_1^2x_2z_2 + a_3y_1^2x_2z_2 + 2a_3y_1z_1x_2y_2 \\
& + a_4^2y_1z_1z_2^2 + a_4^2z_1^2y_2z_2 - a_4x_1^2y_2z_2 - 2a_4x_1y_1x_2z_2 \\
& - 2a_4x_1z_1x_2y_2 - a_4y_1z_1x_2^2 - 3a_6x_1y_1z_2^2 - 6a_6x_1z_1y_2z_2 \\
& - 6a_6y_1z_1x_2z_2 - 3a_6z_1^2x_2y_2 + x_1y_1y_2^2 + y_1^2x_2y_2,
\end{aligned}$$

$$\begin{aligned}
\varphi_1 = {} & a_1^4a_6x_1z_1z_2^2 - a_1^3a_3a_4x_1z_1z_2^2 + a_1^3a_3a_6z_1^2z_2^2 + a_1^3a_6y_1z_1z_2^2 + a_1^2a_2a_3^2x_1z_1z_2^2 \\
& + 5a_1^2a_2a_6x_1z_1z_2^2 + a_1^2a_2a_6z_1^2x_2z_2 - a_1^2a_3^2a_4z_1^2z_2^2 - a_1^2a_3a_4y_1z_1z_2^2 \\
& - a_1^2a_4^2x_1z_1z_2^2 + a_1^2a_4a_6z_1^2z_2^2 + a_1^2a_4x_1^2x_2z_2 + 3a_1^2a_6x_1^2z_2^2 \\
& + 6a_1^2a_6x_1z_1x_2z_2 + a_1a_2a_3^3z_1^2z_2^2 + a_1a_2a_3^2y_1z_1z_2^2 - a_1a_2a_3a_4x_1z_1z_2^2 \\
& - a_1a_2a_3a_4z_1^2x_2z_2 + 4a_1a_2a_3a_6z_1^2z_2^2 - 2a_1a_2a_3x_1^2x_2z_2 + 4a_1a_2a_6y_1z_1z_2^2 \\
& + a_1a_2x_1y_1x_2^2 - a_1a_3^3x_1z_1z_2^2 - 2a_1a_3a_4^2z_1^2z_2^2 - 2a_1a_3a_4x_1^2z_2^2 \\
& - 4a_1a_3a_4x_1z_1x_2z_2 - 3a_1a_3a_6x_1z_1z_2^2 + 3a_1a_3a_6z_1^2x_2z_2 - a_1a_4^2y_1z_1z_2^2 \\
& + 2a_1a_4x_1y_1x_2z_2 + a_1a_4y_1z_1x_2^2 + 3a_1a_6x_1y_1z_2^2 + 6a_1a_6y_1z_1x_2z_2 \\
& + a_1y_1^2x_2y_2 + a_2^2a_3^2x_1z_1z_2^2 + a_2^2a_3^2z_1^2x_2z_2 + 4a_2^2a_6x_1z_1z_2^2 + 4a_2^2a_6z_1^2x_2z_2 \\
& - a_2^2x_1^2x_2^2 + a_2a_3^2a_4z_1^2z_2^2 + a_2a_3^2x_1^2z_2^2 + 2a_2a_3^2x_1z_1x_2z_2 - 2a_2a_3x_1y_1x_2z_2 \\
& - a_2a_3y_1z_1x_2^2 - a_2a_4^2x_1z_1z_2^2 - a_2a_4^2z_1^2x_2z_2 + 4a_2a_4a_6z_1^2z_2^2 - a_2a_4x_1^2x_2z_2 \\
& - a_2a_4x_1z_1x_2^2 + 3a_2a_6x_1^2z_2^2 + 12a_2a_6x_1z_1x_2z_2 + 3a_2a_6z_1^2x_2^2 - a_3^4z_1^2z_2^2 \\
& - a_3^3y_1z_1z_2^2 - a_3^2a_4x_1z_1z_2^2 - 2a_3^2a_4z_1^2x_2z_2 - 6a_3^2a_6z_1^2z_2^2 + 3a_3^2x_1^2x_2z_2 \\
& - a_3a_4x_1y_1z_2^2 - 2a_3a_4y_1z_1x_2z_2 - 3a_3a_6y_1z_1z_2^2 - 3a_3x_1y_1x_2^2 + a_3y_1^2y_2z_2
\end{aligned}$$

$$\begin{aligned}
&- a_4^3z_1^2z_2^2 - a_4^2x_1^2z_2^2 - 4a_4^2x_1z_1x_2z_2 - a_4^2z_1^2x_2^2 - 3a_4a_6x_1z_1z_2^2 \\
&- 3a_4a_6z_1^2x_2z_2 + 3a_4x_1^2x_2^2 - 9a_6^2z_1^2z_2^2 + 9a_6x_1^2x_2z_2 + 9a_6x_1z_1x_2^2 + y_1^2y_2^2
\end{aligned}$$

and

$$\begin{aligned}
\varphi_2 = {} & a_1^3x_1^2x_2z_2 + a_1^2a_3x_1^2z_2^2 + 2a_1^2a_3x_1z_1x_2z_2 + a_1^2x_1^2y_2z_2 + 2a_1^2x_1y_1x_2z_2 \\
&+ 2a_1a_2x_1^2x_2z_2 + a_1a_2x_1z_1x_2^2 + 2a_1a_3^2x_1z_1z_2^2 + a_1a_3^2z_1^2x_2z_2 + 2a_1a_3x_1y_1z_2^2 \\
&+ 2a_1a_3x_1z_1y_2z_2 + 2a_1a_3y_1z_1x_2z_2 + a_1a_4x_1^2z_2^2 + 2a_1a_4x_1z_1x_2z_2 \\
&+ 3a_1a_6x_1z_1z_2^2 + 3a_1x_1^2x_2^2 + 2a_1x_1y_1y_2z_2 + a_1y_1^2x_2z_2 + 2a_2a_3x_1z_1x_2z_2 \\
&+ a_2a_3z_1^2x_2^2 + a_2x_1^2y_2z_2 + 2a_2x_1y_1x_2z_2 + 2a_2x_1z_1x_2y_2 + a_2y_1z_1x_2^2 \\
&+ a_3^3z_1^2z_2^2 + 2a_3^2y_1z_1z_2^2 + a_3^2z_1^2y_2z_2 + a_3a_4x_1z_1z_2^2 + 2a_3a_4z_1^2x_2z_2 \\
&+ 3a_3a_6z_1^2z_2^2 + 3a_3x_1z_1x_2^2 + a_3y_1^2z_2^2 + 2a_3y_1z_1y_2z_2 + a_4x_1y_1z_2^2 \\
&+ 2a_4x_1z_1y_2z_2 + 2a_4y_1z_1x_2z_2 + a_4z_1^2x_2y_2 + 3a_6y_1z_1z_2^2 + 3a_6z_1^2y_2z_2 \\
&+ 3x_1^2x_2y_2 + 3x_1y_1x_2^2 + y_1^2y_2z_2 + y_1z_1y_2^2.
\end{aligned}$$

Note that these formulae work for every elliptic curve E given by a Weierstraß equation over every field $\mathbb{F}$, since for developing these formulae we did not use any information on $\mathbb{F}$ or E except the coefficients of the Weierstraß equation, and the resulting polynomials are elements of $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, x_2, y_2, z_2]$.

Finally in this section we present a few properties about the complete system of addition laws presented here. These properties can later be used to define a group law for points of elliptic curves over rings R with $\operatorname{Pic} R = 0$.

Proposition 4.2.19. *Consider the ring*

$$R := \frac{\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3]}{\langle f(x_1, y_1, z_1), f(x_2, y_2, z_2), f(x_3, y_3, z_3)\rangle},$$

where

$$\begin{aligned}
f &= y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \\
&\in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x, y, z]
\end{aligned}$$

Define $P_i := (x_i, y_i, z_i)$, $-P_i := (x_i, -y_i - x_ia_1 - z_1a_3)$ and $\infty := (0, 1, 0)$. In this ring the following identities hold concerning the above polynomials ψ_0, ψ_1, ψ_2, φ_0, φ_1 and φ_2, seen as polynomials in the indeterminates $(x_1, y_1, z_1), (x_2, y_2, z_2)$:

(a) *We have $\varphi_i\psi_j = \varphi_j\psi_i$ for all $0 \le i, j \le 2$.*

(b) *We have $f(\varphi_0, \varphi_1, \varphi_2) = 0 = f(\psi_0, \psi_1, \psi_2)$.*

(c) *We have*

$$\psi_i(P_1, P_2) = -\psi_i(P_2, P_1)$$

and

$$\varphi_i(P_1, P_2)\varphi_j(P_2, P_1) = \varphi_j(P_1, P_2)\varphi_i(P_2, P_1)$$

for $0 \le i, j \le 2$.

(d) *We have*

$$\psi_i(P_1, -P_1) = 0 \qquad \text{and} \qquad \varphi_i(P_1, -P_1) = 0$$

for $i = 0$ and $i = 2$.

(e) *We have*

$$\begin{aligned} &\varphi_0(P_1,\infty) = x_1y_1, && \varphi_1(P_1,\infty) = y_1^2, && \varphi_2(P_1,\infty) = y_1z_1,\\ &\psi_0(P_1,\infty) = x_1z_1, && \psi_1(P_1,\infty) = y_1z_1, && \psi_2(P_1,\infty) = z_1^2. \end{aligned}$$

(f) *We introduce the notation* $\psi := (\psi_0, \psi_1, \psi_2)$ *and* $\varphi := (\varphi_0, \varphi_1, \varphi_2)$. *We then have*

$$\begin{aligned}
\psi_i(\psi(P_1,P_2),P_3)\psi_j(\psi(P_1,P_2),P_3) &= \psi_j(\psi(P_1,P_2),P_3)\psi_i(\psi(P_1,P_2),P_3),\\
\psi_i(\varphi(P_1,P_2),P_3)\psi_j(\psi(P_1,P_2),P_3) &= \psi_j(\varphi(P_1,P_2),P_3)\psi_i(\psi(P_1,P_2),P_3),\\
\varphi_i(\psi(P_1,P_2),P_3)\psi_j(\psi(P_1,P_2),P_3) &= \varphi_j(\psi(P_1,P_2),P_3)\psi_i(\psi(P_1,P_2),P_3),\\
\varphi_i(\varphi(P_1,P_2),P_3)\psi_j(\psi(P_1,P_2),P_3) &= \varphi_j(\varphi(P_1,P_2),P_3)\psi_i(\psi(P_1,P_2),P_3),\\
\psi_i(\psi(P_1,P_2),P_3)\psi_j(\varphi(P_1,P_2),P_3) &= \psi_j(\psi(P_1,P_2),P_3)\psi_i(\varphi(P_1,P_2),P_3),\\
\psi_i(\varphi(P_1,P_2),P_3)\psi_j(\varphi(P_1,P_2),P_3) &= \psi_j(\varphi(P_1,P_2),P_3)\psi_i(\varphi(P_1,P_2),P_3),\\
\varphi_i(\psi(P_1,P_2),P_3)\psi_j(\varphi(P_1,P_2),P_3) &= \varphi_j(\psi(P_1,P_2),P_3)\psi_i(\varphi(P_1,P_2),P_3),\\
\varphi_i(\varphi(P_1,P_2),P_3)\psi_j(\varphi(P_1,P_2),P_3) &= \varphi_j(\varphi(P_1,P_2),P_3)\psi_i(\varphi(P_1,P_2),P_3),\\
\psi_i(\psi(P_1,P_2),P_3)\varphi_j(\psi(P_1,P_2),P_3) &= \psi_j(\psi(P_1,P_2),P_3)\varphi_i(\psi(P_1,P_2),P_3),\\
\psi_i(\varphi(P_1,P_2),P_3)\varphi_j(\psi(P_1,P_2),P_3) &= \psi_j(\varphi(P_1,P_2),P_3)\varphi_i(\psi(P_1,P_2),P_3),\\
\varphi_i(\psi(P_1,P_2),P_3)\varphi_j(\psi(P_1,P_2),P_3) &= \varphi_j(\psi(P_1,P_2),P_3)\varphi_i(\psi(P_1,P_2),P_3),\\
\varphi_i(\varphi(P_1,P_2),P_3)\varphi_j(\psi(P_1,P_2),P_3) &= \varphi_j(\varphi(P_1,P_2),P_3)\varphi_i(\psi(P_1,P_2),P_3),\\
\psi_i(\psi(P_1,P_2),P_3)\varphi_j(\varphi(P_1,P_2),P_3) &= \psi_j(\psi(P_1,P_2),P_3)\varphi_i(\varphi(P_1,P_2),P_3),\\
\psi_i(\varphi(P_1,P_2),P_3)\varphi_j(\varphi(P_1,P_2),P_3) &= \psi_j(\varphi(P_1,P_2),P_3)\varphi_i(\varphi(P_1,P_2),P_3),\\
\varphi_i(\psi(P_1,P_2),P_3)\varphi_j(\varphi(P_1,P_2),P_3) &= \varphi_j(\psi(P_1,P_2),P_3)\varphi_i(\varphi(P_1,P_2),P_3),\\
\varphi_i(\varphi(P_1,P_2),P_3)\varphi_j(\varphi(P_1,P_2),P_3) &= \varphi_j(\varphi(P_1,P_2),P_3)\varphi_i(\varphi(P_1,P_2),P_3)
\end{aligned}$$

for all $0 \leq i, j \leq 2$.

Proof. We will check the claims with MAGMA$^{\text{TM}}$ since the polynomials that appear in the calculations are too huge. We need the following definitions:

```
S<a_1,a_2,a_3,a_4,a_6,x_1,y_1,z_1,x_2,y_2,z_2,x_3,y_3,z_3> := \
    PolynomialRing(IntegerRing(), 14);

f1 := a_1*x_1*y_1*z_1 - x_1^3 - a_6*z_1^3 + y_1^2*z_1 - a_2*x_1^2*z_1 \
      + a_3*y_1*z_1^2 - a_4*x_1*z_1^2;
f2 := a_1*x_2*y_2*z_2 - x_2^3 - a_6*z_2^3 + y_2^2*z_2 - a_2*x_2^2*z_2 \
      + a_3*y_2*z_2^2 - a_4*x_2*z_2^2;
f3 := a_1*x_3*y_3*z_3 - x_3^3 - a_6*z_3^3 + y_3^2*z_3 - a_2*x_3^2*z_3 \
      + a_3*y_3*z_3^2 - a_4*x_3*z_3^2;

I := ideal<S | f1, f2, f3>;
```

After that, one should define `psi_`i and `phi_`i, $0 \leq i \leq 2$, as above.

(a) The claim directly translates into the following expressions:

```
NormalForm(phi_0 * psi_1 - phi_1 * psi_0, I);
NormalForm(phi_0 * psi_2 - phi_2 * psi_0, I);
NormalForm(phi_1 * psi_2 - phi_2 * psi_1, I);
```

All three expressions evaluate to 0.

(b) The claim directly translates into the following expressions:

```
NormalForm(psi_1^2*psi_2 + a_1*psi_0*psi_1*psi_2 + a_3*psi_1*psi_2^2 - psi_0^3 \
          - a_2*psi_0^2*psi_2 - a_4*psi_0*psi_2^2 - a_6*psi_2^3, I);
NormalForm(phi_1^2*phi_2 + a_1*phi_0*phi_1*phi_2 + a_3*phi_1*phi_2^2 - phi_0^3 \
          - a_2*phi_0^2*phi_2 - a_4*phi_0*phi_2^2 - a_6*phi_2^3, I);
```

All two expressions evaluate to 0.

(c) We need the following intermediate results:

```
t0 := Evaluate(psi_0, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                        x_1, y_1, z_1, x_3, y_3, z_3 ]);
t1 := Evaluate(phi_1, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                        x_1, y_1, z_1, x_3, y_3, z_3 ]);
t2 := Evaluate(phi_2, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                        x_1, y_1, z_1, x_3, y_3, z_3 ]);
```

Then we can proceed as follows:

```
NormalForm(Evaluate(psi_0, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                             x_1, y_1, z_1, x_3, y_3, z_3 ]) + psi_0, I);
NormalForm(Evaluate(psi_1, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                             x_1, y_1, z_1, x_3, y_3, z_3 ]) + psi_1, I);
NormalForm(Evaluate(psi_2, [ a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                             x_1, y_1, z_1, x_3, y_3, z_3 ]) + psi_2, I);
NormalForm(t0 * phi_1 - t1 * phi_0, I);
NormalForm(t0 * phi_2 - t2 * phi_0, I);
NormalForm(t1 * phi_2 - t2 * phi_1, I);
```

All expressions evaluate to 0.

(d) The claim directly translates into the following expressions:

```
NormalForm(Evaluate(psi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
NormalForm(Evaluate(psi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
NormalForm(Evaluate(psi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            x_1, -y_1-a_1*x_1-a_3*z_1, z_1, x_3, y_3, z_3]), I);
```

The first, third, fourth and sixth expressions evaluate to 0, and the second and fifth do not evaluate to 0. This is as expected.

(e) The claim directly translates into the following expressions:

```
NormalForm(Evaluate(psi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
NormalForm(Evaluate(psi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
NormalForm(Evaluate(psi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
NormalForm(Evaluate(phi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                            0, 1, 0, x_3, y_3, z_3]), I);
```

The expressions evaluate to x_1z_1, y_1z_1, z_1^2, x_1y_1, y_1^2 and y_1z_1.

(f) We need the following intermediate results:

```
psi_0a := Evaluate(psi_0, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);
psi_1a := Evaluate(psi_1, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);
psi_2a := Evaluate(psi_2, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);
phi_0a := Evaluate(phi_0, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);
phi_1a := Evaluate(phi_1, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);
phi_2a := Evaluate(phi_2, [a_1, a_2, a_3, a_4, a_6, x_2, y_2, z_2, \
                           x_3, y_3, z_3, x_3, y_3, z_3]);

// Notation: psiphiA(P_1, P_2, P_3) := psi(P_1, phi(P_2, P_3))
psipsiA_0 := Evaluate(psi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
psipsiA_1 := Evaluate(psi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
psipsiA_2 := Evaluate(psi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
phipsiA_0 := Evaluate(phi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
phipsiA_1 := Evaluate(phi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
phipsiA_2 := Evaluate(phi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              psi_0a, psi_1a, psi_2a, x_3, y_3, z_3]);
psiphiA_0 := Evaluate(psi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);
psiphiA_1 := Evaluate(psi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);
psiphiA_2 := Evaluate(psi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);
phiphiA_0 := Evaluate(phi_0, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);
phiphiA_1 := Evaluate(phi_1, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);
phiphiA_2 := Evaluate(phi_2, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                              phi_0a, phi_1a, phi_2a, x_3, y_3, z_3]);

// Notation: psiphiB(P_1, P_2, P_3) := phi(psi(P_1, P_2), P_3)
psipsiB_0 := Evaluate(psi_0a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
psipsiB_1 := Evaluate(psi_1a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
psipsiB_2 := Evaluate(psi_2a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
phipsiB_0 := Evaluate(psi_0a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
phipsiB_1 := Evaluate(psi_1a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
phipsiB_2 := Evaluate(psi_2a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
psiphiB_0 := Evaluate(phi_0a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
psiphiB_1 := Evaluate(phi_1a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
psiphiB_2 := Evaluate(phi_2a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               psi_0, psi_1, psi_2, x_3, y_3, z_3]);
phiphiB_0 := Evaluate(phi_0a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
phiphiB_1 := Evaluate(phi_1a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
```

```
phiphiB_2 := Evaluate(phi_2a, [a_1, a_2, a_3, a_4, a_6, x_1, y_1, z_1, \
                               phi_0, phi_1, phi_2, x_3, y_3, z_3]);
```

Then we can proceed as follows:

```
NormalForm(psipsiA_0*psipsiB_1 - psipsiA_1*psipsiB_0, I);
NormalForm(psipsiA_0*psipsiB_2 - psipsiA_2*psipsiB_0, I);
NormalForm(psipsiA_1*psipsiB_2 - psipsiA_2*psipsiB_1, I);
NormalForm(psipsiA_0*phipsiB_1 - psipsiA_1*phipsiB_0, I);
NormalForm(psipsiA_0*phipsiB_2 - psipsiA_2*phipsiB_0, I);
NormalForm(psipsiA_1*phipsiB_2 - psipsiA_2*phipsiB_1, I);

NormalForm(psipsiA_0*psiphiB_1 - psipsiA_1*psiphiB_0, I);
NormalForm(psipsiA_0*psiphiB_2 - psipsiA_2*psiphiB_0, I);
NormalForm(psipsiA_1*psiphiB_2 - psipsiA_2*psiphiB_1, I);
NormalForm(psipsiA_0*phiphiB_1 - psipsiA_1*phiphiB_0, I);
NormalForm(psipsiA_0*phiphiB_2 - psipsiA_2*phiphiB_0, I);
NormalForm(psipsiA_1*phiphiB_2 - psipsiA_2*phiphiB_1, I);

NormalForm(phipsiA_0*psipsiB_1 - phipsiA_1*psipsiB_0, I);
NormalForm(phipsiA_0*psipsiB_2 - phipsiA_2*psipsiB_0, I);
NormalForm(phipsiA_1*psipsiB_2 - phipsiA_2*psipsiB_1, I);
NormalForm(phipsiA_0*phipsiB_1 - phipsiA_1*phipsiB_0, I);
NormalForm(phipsiA_0*phipsiB_2 - phipsiA_2*phipsiB_0, I);
NormalForm(phipsiA_1*phipsiB_2 - phipsiA_2*phipsiB_1, I);

NormalForm(phipsiA_0*psiphiB_1 - phipsiA_1*psiphiB_0, I);
NormalForm(phipsiA_0*psiphiB_2 - phipsiA_2*psiphiB_0, I);
NormalForm(phipsiA_1*psiphiB_2 - phipsiA_2*psiphiB_1, I);
NormalForm(phipsiA_0*phiphiB_1 - phipsiA_1*phiphiB_0, I);
NormalForm(phipsiA_0*phiphiB_2 - phipsiA_2*phiphiB_0, I);
NormalForm(phipsiA_1*phiphiB_2 - phipsiA_2*phiphiB_1, I);

NormalForm(psiphiA_0*psipsiB_1 - psiphiA_1*psipsiB_0, I);
NormalForm(psiphiA_0*psipsiB_2 - psiphiA_2*psipsiB_0, I);
NormalForm(psiphiA_1*psipsiB_2 - psiphiA_2*psipsiB_1, I);
NormalForm(psiphiA_0*phipsiB_1 - psiphiA_1*phipsiB_0, I);
NormalForm(psiphiA_0*phipsiB_2 - psiphiA_2*phipsiB_0, I);
NormalForm(psiphiA_1*phipsiB_2 - psiphiA_2*phipsiB_1, I);

NormalForm(psiphiA_0*psiphiB_1 - psiphiA_1*psiphiB_0, I);
NormalForm(psiphiA_0*psiphiB_2 - psiphiA_2*psiphiB_0, I);
NormalForm(psiphiA_1*psiphiB_2 - psiphiA_2*psiphiB_1, I);
NormalForm(psiphiA_0*phiphiB_1 - psiphiA_1*phiphiB_0, I);
NormalForm(psiphiA_0*phiphiB_2 - psiphiA_2*phiphiB_0, I);
NormalForm(psiphiA_1*phiphiB_2 - psiphiA_2*phiphiB_1, I);

NormalForm(phiphiA_0*psipsiB_1 - phiphiA_1*psipsiB_0, I);
NormalForm(phiphiA_0*psipsiB_2 - phiphiA_2*psipsiB_0, I);
NormalForm(phiphiA_1*psipsiB_2 - phiphiA_2*psipsiB_1, I);
NormalForm(phiphiA_0*phipsiB_1 - phiphiA_1*phipsiB_0, I);
NormalForm(phiphiA_0*phipsiB_2 - phiphiA_2*phipsiB_0, I);
NormalForm(phiphiA_1*phipsiB_2 - phiphiA_2*phipsiB_1, I);

NormalForm(phiphiA_0*psiphiB_1 - phiphiA_1*psiphiB_0, I);
NormalForm(phiphiA_0*psiphiB_2 - phiphiA_2*psiphiB_0, I);
NormalForm(phiphiA_1*psiphiB_2 - phiphiA_2*psiphiB_1, I);
NormalForm(phiphiA_0*phiphiB_1 - phiphiA_1*phiphiB_0, I);
NormalForm(phiphiA_0*phiphiB_2 - phiphiA_2*phiphiB_0, I);
NormalForm(phiphiA_1*phiphiB_2 - phiphiA_2*phiphiB_1, I);
```

All expressions evaluate to 0.

Note that checking (a)–(e) is very fast, but checking (f) involves a great deal of time.

The simplest case, namely checking

$$\psi_i(\psi(P_1,P_2),P_3)\psi_j(\psi(P_1,P_2),P_3) = \psi_j(\psi(P_1,P_2),P_3)\psi_i(\psi(P_1,P_2),P_3),$$

$0 \le i < j \le 2$, takes 220 minutes on one CPU of a 32 CPU SunFire 6800 machine with 144 GB RAM, where 16 CPUs have 900 MHz and 16 CPUs have 1050 MHz.

The most complex equation,

$$\varphi_i(\varphi(P_1,P_2),P_3)\varphi_j(\varphi(P_1,P_2),P_3) = \varphi_j(\varphi(P_1,P_2),P_3)\varphi_i(\varphi(P_1,P_2),P_3),$$

$0 \le i < j \le 2$, takes 1051.4 hours on the same machine, and during the computations up to 1.5 GB of RAM were used by MAGMA$^{\text{TM}}$. The second most complex equation took 840.6 hours to evaluate to 0. □

4.2.4 Isogenies

In this subsection we will study morphisms between elliptic curves that preserve the neutral element ∞. It turns out that these morphisms respect the group law.

Definition 4.2.20. *Let (E_i, ∞_i), $i = 1, 2$ be elliptic curves. A morphism $f : E_1 \to E_2$ is called an* isogeny *if $f(\infty_1) = \infty_2$. Denote the set of all isogenies $f : E_1 \to E_2$ as* $\mathrm{Hom}(E_1, E_2)$ *and define* $\mathrm{End}(E_1) := \mathrm{Hom}(E_1, E_1)$ *to be the* endomorphism ring *of E_1.*

Remarks 4.2.21.

(a) By Proposition 3.7.8, an isogeny is either finite and surjective, or constant. We denote the constant isogeny by 0 and call it the *zero isogeny*.

For a more general statement, also see [KM85, p. 76, Theorem 2.4.2].

(b) Recall that the *degree* of a non-constant isogeny, defined in Definition 3.7.9, is the degree of the field extension $\mathbb{F}(E_1)/\mathbb{F}(E_2)$. We define the degree of the zero isogeny to be 0.

The group law on elliptic curves induces a structure of Abelian groups on the set of isogenies between two elliptic curves:

Proposition 4.2.22. *If $\varphi, \psi : E_1 \to E_2$ are isogenies of elliptic curves, then $(\varphi + \psi)(P) := \varphi(P) + \psi(P)$ defines an isogeny $\varphi + \psi : E_1 \to E_2$. Moreover, $(-\varphi)(P) := -\varphi(P)$ also defines an isogeny $-\varphi : E_1 \to E_2$.*

Proof. Note that $\varphi + \psi$ is the same as the composition of the morphisms $(\varphi, \psi) : E_1 \to E_2 \times E_2$ and $+ : E_2 \times E_2 \to E_2$. For $-\varphi$ compose φ with the inversion $- : E_2 \to E_2$. □

Corollary 4.2.23. *If E_1 and E_2 are elliptic curves, then* $\mathrm{Hom}(E_1, E_2)$ *has the structure of an Abelian group.*

It turns out that isogenies respect the group law:

Proposition 4.2.24. *[Sil86, p. 75, Theorem 4.8] Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. Then $\varphi(P + Q) = \varphi(P) + \varphi(Q)$ for all $P, Q \in E(\mathbb{F})$.*

See also [KM85, p. 77, Theorem 2.5.1].

Proof. Assume $\varphi \neq 0$. Then φ induces a group morphism $\varphi_* : \operatorname{Pic}^0(E_1) \to \operatorname{Pic}^0(E_2)$ by Proposition 3.7.32, and clearly the diagram

$$\begin{tikzcd}
E_1 \arrow[r, "P\mapsto[[P]-[\infty_1]]"] \arrow[d, "\varphi"'] & \operatorname{Pic}^0(E_1) \arrow[d, "\varphi_*"] \\
E_2 \arrow[r, "Q\mapsto[[Q]-[\infty_1]]"'] & \operatorname{Pic}^0(E_2)
\end{tikzcd}$$

commutes. Now the maps $E_i \to \operatorname{Pic}^0(E_i)$ are isomorphisms and group morphisms, and therefore φ is a group morphism. □

An important corollary from this proposition is that the endomorphism ring of an elliptic curve is indeed a not necessarily commutative ring with unit **id**. We will investigate this ring structure in Section 4.2.8.

Recall that for any $P \in E(\mathbb{F})$ the translation-by-P map $\tau_P : E \to E$, defined by $Q \mapsto Q + P$, is an isomorphism.

Proposition 4.2.25. *[Sil86, p. 76, Corollary 4.9 and Theorem 4.10] Let $\varphi : E_1 \to E_2$ be a non-zero isogeny.*

(a) *The kernel* $\ker\varphi = \varphi^{-1}(\infty_2)$ *is a finite subgroup.*

(b) *For every $Q \in E_2$ we have $\left|\varphi^{-1}(Q)\right| = \deg_s \varphi$.*

(c) *For every $P \in E_1$ we have $e_P(\varphi) = \deg_i \varphi$.*

(d) *The map*

$$\ker\varphi \to G_{\overline{\mathbb{F}}(E_1)/\overline{\mathbb{F}}(E_2)}, \qquad T \mapsto \tau_T^*$$

is an isomorphism. Here $\tau_T^* : \overline{\mathbb{F}}(E_2) \to \overline{\mathbb{F}}(E_2)$ is the induced automorphism of the function field.

(e) *If φ is separable, then φ is unramified, $|\ker\varphi| = \deg\varphi$, and $\overline{\mathbb{F}}(E_1)$ is a Galois extension of $\overline{\mathbb{F}}(E_2)$.*

Of special interest are the endomorphisms of elliptic curves defined in the following definition.

Definition 4.2.26. *Let $m \in \mathbb{Z}$ be an integer and E an elliptic curve. Define the isogeny $[m] \in \operatorname{End}(E)$ for $m > 0$ by*

$$[m] : E \to E, \qquad \underbrace{P \mapsto P + \cdots + P}_{m\ times},$$

for $m < 0$ by $[m](P) := -([-m](P))$ and $[0] := 0$.

Proof. By Proposition 4.2.16 this is well-defined. □

Remark 4.2.27. Let E_1 and E_2 be elliptic curves. Then $\mathbb{Z}$ acts on $\operatorname{Hom}(E_1, E_2)$ by $m\varphi = [m] \circ \varphi$.

4.2.5 Invariant Differentials

In this subsection we will present some results on the invariant differential associated with a Weierstraß equation. These results are in particular important for Section 4.2.7, where we will determine the group structure. Proofs and more information can be found, for example, in [Sil86, ch. III, Section 5].

Definition 4.2.28. *Let*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^2$$

be a Weierstraß equation over $\mathbb{F}$. *Then a* invariant differential *of this Weierstraß equation is*

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

or any multiple by an element of $\mathbb{F}^*$.

Proposition 4.2.29. *[Sil86, p. 52, Proposition 1.5] Let E be a smooth curve given by a Weierstraß equation. Then the invariant differential ω is holomorphic and non-vanishing.*

The same can be shown for generalized elliptic curves. Let τ_P again be the translation-by-P map $Q \mapsto Q+P$. The following proposition explains the name of an invariant differential. Note that these two results can also be shown for generalized elliptic curves (see [KM85, p. 68, Remark 2.2.2]).

Proposition 4.2.30. *[Sil86, p. 80, Proposition 5.1] If ω is a translation invariant differential of an elliptic curve E, then for every $P \in E(\mathbb{F})$, we have $\tau_P^*\omega = \omega$.*

An invariant differential also respects the group structure of $\mathrm{Hom}(E_1, E_2)$:

Proposition 4.2.31. *[Sil86, p. 81, Theorem 5.2] Let E_1 and E_2 be elliptic curves, ω an invariant differential on E_1, and let $\varphi, \psi : E_1 \to E_2$ be isogenies. Then*

$$(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega.$$

Using this proposition one can state the following important results for the $[n]$ maps, $n \in \mathbb{Z}$:

Corollary 4.2.32. *Let E be an elliptic curve and ω an invariant differential on E.*

(a) *[Sil86, p. 83, Corollary 5.3] If $m \in \mathbb{Z}$ is an integer, then $[m]^*\omega = m\omega$.*

(b) *[Sil86, p. 83, Corollary 5.4] Assume $m \in \mathbb{Z}$ is non-zero. If the characteristic of $\mathbb{F}$ is $p > 0$, then further assume m is coprime to p. Then $[m]$ is a finite, separable endomorphism.*

(c) *[Sil86, p. 83, Corollary 5.5] Assume E is defined over $\mathbb{F}_q$, $q = p^e$ for a prime p. Let φ be the q-th power Frobenius endomorphism, and let $m, n \in \mathbb{Z}$. Then*

$$m + n\varphi : E \to E$$

is separable if, and only if, p does not divides m.

4.2.6 Dual Isogenies

In this subsection we will define the dual isogeny of an isogeny. This again will be needed for the next subsection, where we will analyze the group structure of an elliptic curve.

Theorem 4.2.33. *[Sil86, p. 84, Theorem 6.1] Let $\varphi : E_1 \to E_2$ be a non-constant isogeny of degree m.*

(a) *There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [m]$.*

(b) *As a group homomorphism $\hat{\varphi}$ is equal to the composition*

$$E_2 \xrightarrow{Q \mapsto [Q]-[\infty]} \mathrm{WDiv}^0(E_2) \xrightarrow{\varphi^*} \mathrm{WDiv}^0(E_1) \xrightarrow{\sum n_P[P] \mapsto \sum n_P P} E_1.$$

See [KM85, p. 81, Theorem 2.6.1 and p. 82, Corollary 2.6.1.1] for a generalization.

Definition 4.2.34. *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. The* dual isogeny *$\hat{\varphi}$ is the isogeny given by Theorem 4.2.33 (a) if $\varphi \neq 0$, and 0 otherwise.*

Proposition 4.2.35. *[Sil86, p. 86, Theorem 6.2] Let $\varphi : E_1 \to E_2$ be an isogeny between elliptic curves E_1 and E_2.*

(a) *It is*

$$\hat{\varphi} \circ \varphi = [\deg \varphi] : E_1 \to E_1 \qquad \textit{and} \qquad \varphi \circ \hat{\varphi} = [\deg \varphi] : E_2 \to E_2.$$

(b) *If $\psi : E_2 \to E_3$ is another isogeny, where E_3 is another elliptic curve, then $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.*

(c) *If $\psi : E_1 \to E_2$ is another isogeny, then $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.*

(d) *It is $\widehat{[m]} = [m]$ and $\deg[m] = m^2$ for all $m \in \mathbb{Z}$.*

(e) *We have $\hat{\hat{\varphi}} = \varphi$ and $\deg \hat{\varphi} = \deg \varphi$.*

See also [KM85, p. 82, Corollary 2.6.1.1, Theorem 2.6.2 and Corollary 2.6.2.1].

Remarks 4.2.36.

(a) Taking the dual isogeny induces a contravariant functor from and to the category of elliptic curves over $\mathbb{F}$ with isogenies as morphisms.

(b) The construction of the dual isogeny gives a group morphism $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(E_2, E_1)$ by (c), and by (e) it is an isomorphism.

The degree map on $\mathrm{Hom}(E_1, E_2)$ turns out to have a useful property which we will exploit in the proof of Hasse's Theorem.

Definition 4.2.37. *[Sil86, p. 88] A* quadratic form *on an Abelian group G is a map $\varphi : G \to \mathbb{R}$ satisfying*

(a) *$\varphi(x) = \varphi(-x)$ for all $x \in G$; and*

(b) *the induced pairing* $G \times G \to \mathbb{R}$, $(x, y) \mapsto d(x + y) - d(x) - d(y)$ *is bilinear.*

It is, moreover, positive definite *if* $d(x) \geq 0$ *for all* $x \in G$*, and if* $d(x) = 0$ *implies* $x = 0$.

Corollary 4.2.38. *[Sil86, p. 88, Corollary 6.3] If* E_1 *and* E_2 *are elliptic curves, then the degree map* $\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$, $\varphi \mapsto \deg \varphi$ *is a positive definite quadratic form.*

4.2.7 Group Structure and Order

By Theorem 4.1.6 we know that the points of an elliptic curve form a group. Next one can ask what the structure of the group is. Two cases are of special interest: firstly, if one fixes a natural number n, one can ask which points are annihilated by n, i. e. are in the kernel of $[n]$. Secondly, one can ask what the group structure is over a finite field or ring; in this case the group is finite. In this section we will completely answer the first question. The second question will be answered for the case of curves over finite fields $\mathbb{F}_q$.

Definition 4.2.39. *Let* E *be an elliptic curve.*

(a) *Define the* torsion subgroup *of* E *as*

$$\operatorname{Tors}(E) = \{P \in E(\mathbb{F}) \mid \operatorname{ord} P < \infty\}.$$

(b) *For an* $n \in \mathbb{N}_{>0}$ *define the* subgroup of n-torsion points *as*

$$E[n] = \ker[n] = \{P \in E(\mathbb{F}) \mid nP = \infty\} \subseteq \operatorname{Tors}(E).$$

Proposition 4.2.40. *Let* E *be an elliptic curve over an algebraically closed field* $\mathbb{F}$ *and* $n \in \mathbb{Z} \setminus \{0\}$.

(a) *If* n *is invertible in* $\mathbb{F}$ *(which is always the case when the characteristic of* $\mathbb{F}$ *is zero), then* $E[n] \cong \mathbb{Z}_{|n|} \times \mathbb{Z}_{|n|}$.

(b) *If the characteristic of* $\mathbb{F}$ *is* $p > 0$*, then either* $E[p^n] = 0$ *for all* $n \geq 1$*, or* $E[p^n] \cong \mathbb{Z}_{p^n}$ *for all* $n \geq 1$.

(c) *If* E *is defined over a finite field* $\mathbb{F}_q$*, then there exists an* $m > 0$ *such that* $E[n] \subseteq E(\mathbb{F}_{q^m})$.

See also [KM85, p. 73ff, Theorem 2.3.1 and Corollary 2.3.2]. (Note that in the proof in [KM85] the authors reduce to the case of an elliptic curve over $\mathbb{C}$, and in this case the problem is trivial since the group of points is non-canonically isomorphic to $\mathbb{C}/\Lambda$ for a lattice Λ.)

Proof. Note that by Proposition 4.2.35 (d) we have $\deg[n] = n^2$.

(a) Assume $|n| > 1$. By Corollary 4.2.32 (b) we know that $[n]$ is separable and finite. Therefore, $|E[n]| = |\ker[n]| = \deg[n] = n^2$. If d is a divisor of n, then clearly also $|E[d]| = d^2$. Now by the Structure Theorem for Finitely Generated Abelian Groups, Theorem 2.0.1,

$$E[n] \cong \prod_{i=1}^{k} \mathbb{Z}_{m_k}, \qquad 1 < m_1 \text{ divides } \cdots \text{ divides } m_k \text{ divides } |E[n]|\,.$$

If n is prime, clearly $k = 2$ and $m_1 = m_2 = n$ since every element of $E[n]$ has an order at most n. If n is composite, let d be a prime dividing m_1. As $\mathbb{Z}_d \times \mathbb{Z}_d \cong E[d] \subseteq E[n]$, it must be that $k = 2$ (see Corollary 2.0.2). But since every element of $E[n]$ has order at most n, it must be that $m_1 = m_2 = n$.

(b) Let $\varphi : E \to E^{(p)}$ be the $\mathbb{F}$-linear p-th power Frobenius. By Proposition 4.2.25 (b) $|E[p^n]| = \deg_s[p^n]$, which by Corollary 3.7.11 and Proposition 4.2.35 equals $\deg_s[p]^n = (\deg_s[p])^n = (\deg_s(\hat{\varphi} \circ \varphi))^n$. Now φ is purely inseparable by Proposition 3.7.19 (a) and, according to Proposition 3.7.11, we have $\deg_s(\hat{\varphi} \circ \varphi) = \deg_s \hat{\varphi}$. By Proposition 4.2.35 (e) we have $\deg \hat{\varphi} = \deg \varphi$.

If $\hat{\varphi}$ is separable, then $\deg_s \hat{\varphi} = \deg \varphi = p$ by Proposition 3.7.19. If $\hat{\varphi}$ is inseparable, then $\deg_s \hat{\varphi}$ must be 1, since p is prime. (Note that this does not depend on n!)

Hence, either $E[p^n] = 0$ for all $n \geq 1$, or $|E[p^n]| = p^n$ and, therefore, $E[p^n] \cong \mathbb{Z}_{p^n}$ by induction on n and by the Structure Theorem for Finitely Generated Abelian Groups (Theorem 2.0.1).

(c) This follows directly from the fact that $E[n]$ is always a finite subgroup. □

The proposition allows us to deduce the group structure of an elliptic curve over a finite field:

Corollary 4.2.41. *Let E be an elliptic curve over $\mathbb{F}_q$. Then $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_m$, where n divides m, and $1 \leq n \leq m$.*

Proof. By the Structure Theorem for Finitely Generated Abelian Groups (Theorem 2.0.1)

$$E(\mathbb{F}_q) \cong \prod_{i=1}^{n} \mathbb{Z}_{m_i},$$

where $1 < m_i \leq \cdots \leq m_n \leq |E(\mathbb{F}_q)|$ and m_i divides m_{i+1}, $1 \leq i < n$. If $n > 2$, let d be a prime factor of m_1. Then $E(\mathbb{F}_q)$ has a subgroup of type $\mathbb{Z}_d^n$ (see Corollary 2.0.2), which contradicts that $E[d]$ has an order of at most d^2 by Proposition 4.2.40. Thus $n \leq 2$. □

According to [Eng99, p. 107, Theorem 3.76] one can also show using the Weil pairing that the integer n in Corollary 4.2.41 divides $\left|\mathbb{F}_q^*\right| = q - 1$.

Next we want to prove the Theorem of Hasse, which gives an estimate for the size of the group of an elliptic curve over a finite field. Later we will see that this bound is optimal. But before we proceed to the theorem, we need an intermediate result on quadratic forms.

Lemma 4.2.42 (Cauchy-Schwarz). *[Sil86, pp. 131f, Lemma 1.2] Let G be an Abelian group, and $\varphi : G \to \mathbb{R}$ be a positive definite quadratic form. Then for all $x, y \in G$ we have*

$$|\varphi(x-y) - \varphi(x) - \varphi(y)| \leq 2\sqrt{\varphi(x)\varphi(y)}.$$

Theorem 4.2.43 (Hasse). *[Sil86, p. 131, Theorem 1.1] If E is an elliptic curve over $\mathbb{F}_q$, then $|E(\mathbb{F}_q)| = q + 1 - t$, where $|t| \leq 2\sqrt{q}$. (Here t is the* trace *of the Frobenius endomorphism; see Definition 4.2.60.)*

See also [KM85, p. 84f, Theorem 2.6.3 and Corollary 2.6.4].

Proof. Let $\varphi : E \to E$ be the q-th power Frobenius. Since $\overline{\mathbb{F}_q}/\mathbb{F}_q$ is Galois by Proposition 2.2.38 and Proposition 2.2.28 (d), we get $\ker(1-\varphi) = E(\mathbb{F}_q)$, together with Proposition 2.2.39. By Corollary 4.2.32 (c), $1 - \varphi$ is separable and, therefore, $|\ker(1-\varphi)| = \deg(1-\varphi)$. By Proposition 3.7.19 (b) it is $\deg\varphi = q$, and by Corollary 4.2.38 and Lemma 4.2.42 we get

$$\begin{aligned} ||E(\mathbb{F}_q)| - 1 - q| = {} & |\deg(1-\varphi) - \deg 1 - \deg\varphi| \\ & \leq 2\sqrt{\deg 1 \cdot \deg\varphi} = 2\sqrt{q}. \end{aligned}$$

□

For the rest of this subsection we will present results from papers of H. W. Lenstra and R. Schoof about which group sizes can appear for elliptic curves over $\mathbb{F}_q$, and how many non-isomorphic curves do exist which have a given group size. These results are based on results by M. Deuring and W. C. Waterhouse. From now on let $\mathbb{F}_q$ be a finite field of order $q = p^n$, where p is a prime and $n \in \mathbb{N}_{>0}$.

Definition 4.2.44. *In this definition all isomorphisms are taken as isomorphisms defined over $\mathbb{F}_q$.*

(a) *Denote with $\mathcal{E}_q$ the set of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$. Define $N_q := |\mathcal{E}_q|$ and*

$$N_q^* := \sum_{[E] \in \mathcal{E}_q} \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q} E|}.$$

(b) *Denote with $\mathcal{E}_q(t)$ the set of isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ that have exactly $q + 1 - t$ $\mathbb{F}_q$-rational points. Define $N(t) := N_q(t) := |\mathcal{E}_q(t)|$ and*

$$N_q^*(t) := \sum_{[E] \in \mathcal{E}_q(t)} \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q} E|}.$$

Remarks 4.2.45.

(a) We clearly have $N_q = \sum_{t=-\infty}^{\infty} N_q(t)$ and $\mathcal{E}_q = \bigcup_{t=-\infty}^{\infty} \mathcal{E}_q(t)$.

(b) From Hasse's Theorem 4.2.43 we know that $N_q(t) = 0$ if $|t| > 2\sqrt{q}$.

(c) By Proposition 4.2.4 (1) two elliptic curves given by Weierstraß equations over $\mathbb{F}$ are isomorphic over $\mathbb{F}$ if one curve can be obtained from the other by a coordinate transform of the form

$$x' = u^2 x + rz, \qquad y' = u^3 y + su^2 x + tz, \qquad z' = z$$

for $u, r, s, t \in \mathbb{F}$, $u \neq 0$.

The first theorem gives which numbers can appear for group sizes.

Theorem 4.2.46. *[Wat69, p. 536, Theorem 4.1] [Sch87, pp. 194f, Theorem 4.6] Assume $|t| \leq 2\sqrt{q}$. Then $N_q(t) \neq 0$ if, and only if, one of the following cases occurs:*

(a) *p does not divides t;*

(b) *q is not a square (i. e. if n is odd), and we have*

  (i) *$t = 0$;*

  (ii) *$t = \pm\sqrt{2q}$ and $p = 2$;*

  (iii) *$t = \pm\sqrt{3q}$ and $p = 3$; or*

(c) *q is a square (i. e. if n is even), we have*

  (i) *$t^2 = 4q$;*

  (ii) *$t^2 = q$;*

  (iii) *$t = 0$.*

In all other cases, $N_q(t) = 0$.

Examples 4.2.47.

(a) For $\mathbb{F} = \mathbb{Z}_2$, possible group sizes (by Hasse) are $1, \dots, 5$. By the previous theorem there are elliptic curves over $\mathbb{F}$ with 2 and 4 $\mathbb{F}$-rational points by (a), with 3 $\mathbb{F}$-rational points by (b) (i), and with 1 and 5 $\mathbb{F}$-points by (b) (ii).

(b) For $\mathbb{F} = \mathbb{Z}_3$, possible group sizes (by Hasse) are $1, \dots, 7$. By the previous theorem there are elliptic curves over $\mathbb{F}$ with 2, 3, 5 and 6 $\mathbb{F}$-rational points by (a), with 4 $\mathbb{F}$-rational points by (b) (i), and with 1 and 7 $\mathbb{F}$-rational points by (b) (iii).

(c) For $\mathbb{F} = \mathbb{F}_4$, possible group sizes (by Hasse) are $1, \dots, 9$. By the previous theorem there are elliptic curves over $\mathbb{F}$ with 2, 4, 6 and 8 $\mathbb{F}$-rational points by (a), with 5 $\mathbb{F}$-rational points by (c) (iii), with 3 and 7 $\mathbb{F}$-rational points by (c) (ii), and with 1 and 9 $\mathbb{F}$-rational points by (c) (i).

(d) For $\mathbb{F} = \mathbb{Z}_5$, possible group sizes (by Hasse) are $2, \dots, 10$. By the previous theorem there are elliptic curves over $\mathbb{F}$ with 2, 3, 4, 5, 7, 8, 9 and 10 $\mathbb{F}$-rational points by (a) and with 6 $\mathbb{F}$-rational points by (b) (i).

Hence if $|\mathbb{F}| \leq 5$, all sizes of groups of elliptic curves over $\mathbb{F}$ that are possible by Hasse's Theorem occur. The same happens for $\mathbb{F} = \mathbb{Z}_7$. But in the case where $\mathbb{F} = \mathbb{F}_8$, there is no elliptic curve over $\mathbb{F}$ having 7 or 11 $\mathbb{F}$-rational-points, even though by Hasse such cardinalities are possible.

Definition 4.2.48. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with characteristic $p > 0$. If p divides $t = q + 1 - |E(\mathbb{F}_q)|$, then E is called* supersingular.

We next want to state a theorem which states the exact number of non-isomorphic elliptic curves over $\mathbb{F}_q$ with a given group size. For that we first need two definitions:

Definition 4.2.49. *Let p be an odd prime and $n \in \mathbb{Z}$. Define the* Jacobi symbol

$$\left(\frac{n}{p}\right) := \begin{cases} 0 & \text{if } n \equiv 0 \pmod{p}, \\ 1 & \text{if } n \text{ is a non-zero square} \pmod{p}, \\ -1 & \text{if } n \text{ is not a square} \pmod{p}, \end{cases}$$

and for $p = 2$ define the Jacobi symbol

$$\left(\frac{n}{2}\right) := \begin{cases} 0 & \text{if } n \equiv 0 \pmod{2}, \\ 1 & \text{if } n \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

Definition 4.2.50. *Let $\Delta \in \mathbb{Z}$, $\Delta < 0$ with $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$.*

(a) *Define the* conductor *of Δ to be*

$$f := \max\{d \in \mathbb{Z} \mid \Delta/d^2 \equiv 0 \pmod 4 \text{ or } \Delta/d^2 \equiv 1 \pmod 4\},$$

and the fundamental discriminant *associated to Δ to be Δ/f^2.*

(b) *A* positive definite binary quadratic form of discriminant Δ *is a polynomial*

$$ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y],$$

where $a, b, c \in \mathbb{Z}$ satisfy $a > 0$ and $b^2 - 4ac = \Delta$. Denote the set of all such forms by $B(\Delta)$.

(c) *Let $f = ax^2 + bxy + cy^2 \in B(\Delta)$ and $\sigma = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Then*

$$f^\sigma := a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2$$

defines an action of $SL_2(\mathbb{Z})$ on $B(\Delta)$. Here $SL_2(\mathbb{Z})$ is the special linear group, i. e. the group of 2×2-matrices with entries in $\mathbb{Z}$ and determinant 1.

(d) *Define $CL(\Delta) := B(\Delta)/SL_2(\mathbb{Z})$ and denote $H(\Delta) := |CL(\Delta)|$ as the* Kronecker class number *for Δ.*

(e) *Denote with*

$$H^*(\Delta) := \sum_{[f] \in CL(\Delta)} \frac{1}{|\operatorname{Aut} f|}$$

the weighted Kronecker class number *for Δ. Here $\operatorname{Aut} f$ denotes the set of $\sigma \in SL_2(\mathbb{Z})$ such that $f^\sigma = f$.*

Remarks 4.2.51.

(a) Recall that $SL_2(\mathbb{Z}) = \{\sigma \in GL_2(\mathbb{Z}) \mid \det(\sigma) = 1\}$.

(b) [Sch87, p. 187] It can be shown that $CL(\Delta)$ is finite for every valid choice of Δ.

(c) By [Len87, pp. 654f] we have $2 \le |\operatorname{Aut} f| \le 6$ for all $f \in B(\Delta)$. Therefore

$$\frac{H(\Delta)}{6} \le H^*(\Delta) \le \frac{H(\Delta)}{2} \le 3H^*(\Delta).$$

We can now state the theorem:

Theorem 4.2.52. *[Sch87, pp. 194f, Theorem 4.6] The value $N_q(t)$ is given by the following if $|t| \leq 2\sqrt{q}$:*

(a) *if p does not divides t, we have $N_q(t) = H(t^2 - 4q)$;*

(b) *if q is not a square (i. e. if n is odd), we have*

   (i) $N_q(t) = H(-4p)$ *if* $t = 0$;

   (ii) $N_q(t) = 1$ *if* $t^2 = 2q$ *and* $p = 2$;

   (iii) $N_q(t) = 1$ *if* $t^2 = 3q$ *and* $p = 3$;

(c) *if q is a square (i. e. if n is even), we have*

   (i) $N_q(t) = \frac{1}{12}\left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right)$ *if* $t^2 = 4q$;

   (ii) $1 - \left(\frac{-3}{p}\right)$ *if* $t^2 = q$;

   (iii) $1 - \left(\frac{-4}{p}\right)$ *if* $t = 0$.

In all other cases, $N_q(t) = 0$.

Remark 4.2.53. According to [Len87, p. 654, (1.5)] at least for the case that if $p > 3$ is prime and $|t| \leq 2\sqrt{p}$, then $N_p^*(t) = H^*(t^2 - 4p)$ and $N_p^* = p$.

Note that it is actually possible to describe the group structure more exact than we did in Corollary 4.2.41. R. Schoof described the possible group structures for supersingular curves in [Sch87] and J. F. Voloch described the possible group structures for non-supersingular curves in [Vol88].

Finally, we give a lower boundary for $H(\Delta)$, which will be useful later during the runtime analysis of Lenstra's Elliptic Curve Factorization Method.

Proposition 4.2.54. *[Len87, p. 656, Proposition 1.8] There exist effectively computable positive constants c, c' such that for every $z \in \mathbb{Z}_{>1}$ there exists an $\Delta^*(z) < -4$ such that*

$$\frac{c\sqrt{-\Delta}}{\log z} \leq H^*(\Delta) \leq c'\sqrt{-\Delta} \cdot \log|\Delta| \cdot (\log\log|\Delta|)^2$$

for all $\Delta \in \mathbb{Z}_{<0}$ with $-z \leq \Delta$, $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$, and the fundamental discriminant $\Delta_0 \neq \Delta^*(z)$. If Δ satisfies all conditions except $\Delta_0 \neq \Delta^*(z)$, the inequality on the left might be invalid, but the one on the right side is still valid.

Remark 4.2.55. [Len87, p. 656, before Proposition 1.8] If the generalized Riemann hypothesis is assumed to be true, then $\frac{c\sqrt{-\Delta}}{\log z}$ on the left can be replaced by $\frac{c\sqrt{-\Delta}}{\log\log z}$, and the inequality on the left is true for any Δ satisfying all conditions except $\Delta \neq \Delta^*(z)$.

4.2.8 Some More Facts About End(E) and [m]

Before we will present algorithms that compute the group order of an elliptic curve over $\mathbb{F}_q$ in the next subsection, we need some more facts about the endomorphism ring and about division polynomials, which are in close connection to the [n] maps, $n \in \mathbb{Z}$.

The Endomorphism Ring

Proposition 4.2.56. *[Sil86, p. 71, Proposition 4.2] Let E, E_1 and E_2 be elliptic curves.*

(a) *If $m \in \mathbb{Z}$ is not zero, then the map $[m]$ is non-constant.*

(b) *The $\mathbb{Z}$-module $\operatorname{Hom}(E_1, E_2)$ is torsion-free.*

(c) *The endomorphism ring $\operatorname{End}(E)$ is a zero-divisor-free, not necessarily commutative ring with unit of characteristic zero.*

Proof.

(a) This follows directly from Proposition 4.2.40 (a) and (b), since $\ker[m] = E[m] = E[-m]$.

(b) Assume that $[m]\circ\varphi = m\varphi = 0$ for $m \in \mathbb{Z}$, $\varphi \in \operatorname{Hom}(E_1, E_2)$. By Corollary 3.7.11 we get $0 = \deg([m]\circ\varphi) = \deg[m]\cdot\deg\varphi$ and, thus, either $\deg[m] = 0$ or $\deg\varphi = 0$. If $\varphi \neq 0$ then $\deg\varphi \neq 0$, but then by (a) we get $m = 0$.

(c) Let $\varphi, \psi \in \operatorname{End}(E)$ such that $\varphi \circ \psi = 0$. By the same degree argument as in (b) we get either $\varphi = 0$ or $\psi = 0$. Hence, $\operatorname{End}(E)$ has no zero-divisors. Moreover by (b) $\operatorname{End}(E)$ has characteristic zero. □

The units in the endomorphism ring of E are exactly the automorphisms of E. The following proposition shows that for most elliptic curves the only units are ±1.

Proposition 4.2.57. *[Sil86, p. 103, Theorem 10.1] Let E be an elliptic curve defined over a perfect field $\mathbb{F}$. Then we have*

(a) $|\operatorname{Aut}(E)| = 2$ *if* $j(E) \notin \{0, 1728\}$*;*

(b) $|\operatorname{Aut}(E)| = 4$ *if* $j(E) = 1728$ *and* $6 \in \mathbb{F}^*$*;*

(c) $|\operatorname{Aut}(E)| = 6$ *if* $j(E) = 0$ *and* $6 \in \mathbb{F}^*$*;*

(d) $|\operatorname{Aut}(E)| = 12$ *if* $j(E) = 0 = 1728$ *and* $3 = 0 \in \mathbb{F}$*;*

(e) $|\operatorname{Aut}(E)| = 24$ *if* $j(E) = 0 = 1728$ *and* $2 = 0 \in \mathbb{F}$.

These automorphisms are automorphisms over the algebraic closure of $\mathbb{F}$.

What is more important is that we now have an upper boundary for the number of automorphisms of an elliptic curve. We can, therefore, relate the quantities $N_q(t)$ and $N_q^*(t)$ from Definition 4.2.44:

Remark 4.2.58. We have that

$$\frac{N_q(t)}{24} \leq N_q^*(t) \leq \frac{N_q(t)}{2} \leq 12N_q^*(t).$$

If one fixes a natural number n, which is invertible in $\mathbb{F}$, then one can see that every endomorphism $\varphi \in \operatorname{End}(E)$ restricted to $E[n] \cong \mathbb{Z}_n^2$ is a group morphism. Since $\mathbb{Z}_n^2$ can be seen as a $\mathbb{Z}_n$-module, by the Theorem of Cayley-Hamilton, the $\mathbb{Z}_n$-module endomorphism $\varphi|_{E[n]}$ satisfies an equation $x^2 + ax + b$, where $a, b \in \mathbb{Z}_n$. Clearly a and b can be seen as elements of $\mathbb{Z}$ instead, but they still can depend on n. The following proposition shows that they can be chosen independent of n:

Proposition 4.2.59. *[KM85, p. 84, Corollary 2.6.2.2 and Theorem 2.6.3] Let E be an elliptic curve and $\varphi \in \operatorname{End}(E)$. Then φ satisfies the equation $x^2 - tx + d = 0$, where $t = \varphi + \hat{\varphi} \in \mathbb{Z}$ and $d = \deg\varphi = \varphi\hat{\varphi}$.*

Again, this theorem holds in a more general manner (see [KM85]).

Proof. Using Proposition 4.2.35, we see that

$$\deg(1+\varphi) = (\widehat{1+\varphi})(1+\varphi) = (1+\hat{\varphi})(1+\varphi) = 1 + \deg(\varphi) + (\varphi + \hat{\varphi}),$$

and, therefore, $\varphi + \hat{\varphi} \in \mathbb{Z}$. Moreover,

$$\varphi^2 - (\hat{\varphi} + \varphi)\varphi + \hat{\varphi}\varphi = 0.$$

□

If one views $\varphi|_{E[n]}$ as an $\mathbb{Z}_n$-modulo endomorphism of the free $\mathbb{Z}_n$-module $\mathbb{Z}_n^2$, one can represent it by a two-by-two matrix. The trace of this matrix is now the value t in the equation $x^2 - tx + d$, which is annihilated by $\varphi|_{E[n]}$. This leads to the following definition:

Definition 4.2.60. *Let E be an elliptic curve and $\varphi \in \operatorname{End}(E)$. Then* trace$(\varphi) :=$ $\varphi + \hat{\varphi} \in \mathbb{Z}$ *is called the* trace *of φ.*

This also explains why the integer t in $|E(\mathbb{F}_q)| = q + 1 - t$ is called the *trace of the Frobenius*: it is simply trace(φ) for $\varphi : E \to E$ the q-th power Frobenius, since as in the proofs of Theorem 4.2.43 and Theorem 4.2.59 we have

$$1 + q - \operatorname{trace}(\varphi) = 1 + \deg(-\varphi) + \operatorname{trace}(-\varphi) = \deg(1-\varphi) = |E(\mathbb{F}_q)|\,.$$

Division Polynomials Let E be an elliptic curve given by the Weierstraß equation

$$y^2 = x^3 + ax + b, \qquad \text{where } a, b \in \mathbb{F}.$$

Assume that the characteristic of $\mathbb{F}$ is neither 2 nor 3. The case of division polynomials for all characteristics is handled for example in [Eng99, pp. 84ff].

Definition 4.2.61. *[Sil86, p. 105, Exercise 3.7] The* division polynomials *on E are the polynomials $\psi_n \in \mathbb{Z}[a,b,x,y]$ defined by*

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \textit{for } n \geq 2\\
\textit{and} \qquad \psi_{2n} &= \frac{\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)}{2y} \qquad \textit{for } n > 2.
\end{aligned}$$

The connection between the map $[n]$ and ψ_n is given by the following proposition:

Proposition 4.2.62. *[Sil86, p. 105, Exercise 3.7] [Sch85, pp. 3f] [Eng99, pp. 84ff]*

(a) *For odd n we have that ψ_n is a polynomial in $\mathbb{Z}[a,b,x,y^2]$; for even n we have that $\psi_n/2y$ is a polynomial in $\mathbb{Z}[a,b,x,y^2]$. Define*

$$f_n := \begin{cases} \frac{\partial(\psi_n|_{y^2=x^3+ax+b})}{\partial x}, & n \text{ odd} \\ \frac{1}{y} \cdot \frac{\partial(\psi_n|_{y^2=x^3+ax+b})}{\partial x}, & n \text{ even.} \end{cases}$$

(b) *As polynomials in x we can write $\psi_n^2 = n^2 x^{n^2-1}$ + lower order terms. Moreover assume that n is invertible in $\mathbb{F}$. Then*

$$\deg f_n = \begin{cases} \frac{1}{2}(n^2-1) & \text{if } n \text{ is odd,} \\ \frac{1}{2}(n^2-4) & \text{if } n \text{ is even.} \end{cases}$$

(c) *A point $P = (x : y : 1) \in E(\mathbb{F})$, $2P \neq \infty$, satisfies $nP = \infty$ if, and only if, $f_n(x) = 0$.*

(d) *If $nP \neq \infty$ for $P = (x : y : 1) \in E(\mathbb{F})$, let $nP = (x' : y' : 1)$. Then*

$$x' = x - \frac{\psi_{n-1}(x,y)\psi_{n+1}(x,y)}{\psi_n^2(x,y)}$$

$$\text{and} \qquad y' = \frac{\psi_{n+2}(x,y)\psi_{n-1}^2(x,y) - \psi_{n-2}(x,y)\psi_{n+1}^2(x,y)}{4y\psi_n^3(x,y)}.$$

4.2.9 How to Count Points

In Section 4.2.7 we have seen several results about the group of points of an elliptic curve. We know that it has the form $\mathbb{Z}_n \times \mathbb{Z}_m$, where n divides m and n might be 1, and we know exactly which group orders are possible and which are not. What is missing is an effective method to compute the order of the group for a given elliptic curve. The first method is mostly of theoretical interest:

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 3$, and E an elliptic curve defined over $\mathbb{F}_q$ by

$$y^2 = x^3 + ax + b, \qquad \text{where } a, b \in \mathbb{F}.$$

Let

$$\chi : \mathbb{F}_q \to \mathbb{N}, \qquad x \mapsto \begin{cases} 1 & \text{if } (x^3+ax+b)^{(q-1)/2} = 0, \\ 0 & \text{if } (x^3+ax+b)^{(q-1)/2} = -1, \\ 2 & \text{if } (x^3+ax+b)^{(q-1)/2} = 1. \end{cases}$$

Then for each $x \in \mathbb{F}_q$ the number $\chi(x)$ gives the number of $y \in \mathbb{F}_q$ such that $y^2 = x^3 + ax + b$. Then

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} \chi(x).$$

This method is also described in [Len86, p. 109], and originally credited to S. Lang and H. Trotter. It is only useful if q is small, since it has running time $\mathcal{O}(q^{1+\varepsilon})$ for any constant $\varepsilon > 0$ and is therefore exponential.

One application of this to find a random point: choose a random $x \in \mathbb{F}_q$ such that $\chi(x) > 0$. Then use a square-root-finding algorithm to find a $y \in \mathbb{F}_q$ such that $y^2 = x^3 + ax + b$. (On how to effectively compute square roots, see for example [Sch85, pp. 490–494].)

Generic Methods

Generic methods are methods which work for arbitrary groups, specialized to the group of points of elliptic curves. This specialization is usually made by exploiting the fact that inversions are fast, and that a boundary for the group size is given.

The best example for a generic method is probably the following variation of the Shanks baby-step giant-step algorithm, due to Shanks and Mestre. It can be used to compute both the order of a point $P \in E(\mathbb{F}_q)$ and the group order. Note that the variation is that the boundaries for $|E(\mathbb{F}_q)|$ from Hasse's Theorem are used. Moreover, note that for this algorithm the characteristic can also be 2 and 3.

Let $\mathbb{F}_q$ be a finite field and E an elliptic curve defined over $\mathbb{F}_q$. According to [BSS99, p. 104, Section VI.3] and [Ros05], the algorithm works as follows:

(1) Repeat the following steps:

  (a) Find a random point $P \in E(\mathbb{F}_q)$, define $Q := (q+1)P$ and choose an $m \in \mathbb{Z}$ such that $m > \sqrt[4]{q}$.

  (b) Compute all values jP for $j = 0, \dots, m$, and store them. (This is the *baby step*.)

  (c) Compute $Q + k(2mP)$ for $k = -m, \dots, m$, until $Q + k(2mP) = \pm jP$ for some $0 \le j \le m$. (This is the *giant step*.)

  (d) Compute $M := q + 1 - 2mk \mp j$. This integer satisfies $MP = \infty$.

  (e) Factor $M = \prod_{i=1}^{\ell} p_i^{e_i}$, where the p_i's are distinct prime numbers and $e_i \in \mathbb{N}_{>0}$.

  (f) For every $i \in \{1, \dots, \ell\}$ test whether $\frac{M}{p_i}P = \infty$. If it does, divide M by p_i and try this i again.

  (g) Now $M = \operatorname{ord} P$, which is a divisor of $E(\mathbb{F}_q)$.

(2) Continue repeating step (1) until the least common multiple of the M's computed in (1) is in $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$, and twice its value is greater than $q+1+2\sqrt{q}$.

The running time is $\mathcal{O}(q^{1/4+\varepsilon})$ for any constant $\varepsilon > 0$. Note that this algorithm can also be used to compute information about the structure of $E(\mathbb{F}_q)$ (for more information see [Ros05]).

Schoof's Algorithm

The main reference for this paragraph is [Sch85, pp. 487–490], but a lot of information on Schoof's algorithm can be found also, for example, in [BSS99, Chapter VII] or [Eng99, pp. 133–141, Section 5.2]. In his book [Eng99] A. Enge also covers the cases of characteristic 2 and 3.

Let $\mathbb{F}_q$ be a finite field of characteristic $p > 3$. Let E be an elliptic curve defined by

$$y^2 = x^3 + ax + b, \qquad \text{where } a, b \in \mathbb{F}_q.$$

Let t denote the trace of the q-th power Frobenius morphism $\varphi \in \operatorname{End}(E)$. We know $|E(\mathbb{F}_q)| = q + 1 - t$, and $|t| \le 2\sqrt{q}$ by Theorem 4.2.43. If ℓ is prime, let φ_ℓ

denote $\varphi|_{E[\ell]}$. Now $\varphi_\ell^2 - t'\varphi_\ell + q \equiv 0$ on $E[\ell]$ if, and only if, $t \equiv t' \pmod{\ell}$. (For more details, see [Sch85, p. 486].)

Note that by Proposition 4.2.62 (d), for any $P = (x : y : 1) \in E[\ell]$, where $\ell \in [3, p-1]$ is prime, we have that $\varphi_\ell^2 + q = \tau\varphi_\ell$ for $\tau \in \mathbb{Z}_\ell$ if and only if

$$\left(x^{q^2}, y^{q^2}\right) + \left(x - \tfrac{\psi_{q-1}\psi_{q+1}}{\psi_q^2}, \quad \tfrac{\psi_{q+2}\psi_{q-1}^2 - \psi_{q-2}\psi_{q+1}^2}{4y\psi_q^3}\right)$$

is equal to ∞ if $\tau = 0 \in \mathbb{Z}_\ell$, or is equal to

$$\left(x^q - \left(\tfrac{\psi_{\tau-1}\psi_{\tau+1}}{\psi_\tau^2}\right)^q, \quad \left(\tfrac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3}\right)^q\right)$$

otherwise.

We will just describe the algorithm without explaining why it works.

(a) For $L \in \mathbb{N}$ denote by $\mathscr{P}_L$ all odd primes $\leq L$ excluding p. Compute an L such that

$$\prod_{\ell \in \mathscr{P}_L} \ell > 4\sqrt{q}.$$

We will determine $t \mod \ell$ for all $\ell \in \mathscr{P}_L$, which allows us to compute t by the restrictions known on t in step (d).

(b) Compute the polynomials $f_1, f_2, \ldots, f_L$.

(c) For every $\ell \in \mathscr{P}_L$, compute $t \mod \ell$ as follows:

(1) Test whether there is a point $P = (x : y : 1) \in E[\ell]$ satisfying $\varphi_\ell^2(P) = \pm kP$, where $k = (q \mod \ell) \in \{1, \ldots, \ell - 1\}$.

For this compute

$$\gcd\Big((x^{q^2} - x)f_k^2(x)(x^3 + ax + b) + f_{k-1}(x)f_{k+1}(x), \psi_\ell\Big)$$

if k is even, or

$$\gcd\Big((x^{q^2} - x)f_k^2(x) + f_{k-1}(x)f_{k+1}(x)(x^3 + ax + b), \psi_\ell\Big)$$

if k is odd. Now such a point exists if and only if the greatest common divisor is not one.

(a) Case 1: for some $P = (x : y : 1) \in E[\ell]$ we have $\varphi_\ell^2(P) = \pm qP$.

Go step by step through these cases, until $t \pmod{\ell}$ is determined:

(I) If the Jacobi symbol $\left(\frac{q}{\ell}\right) = -1$ we have $t \equiv 0 \pmod{\ell}$. Otherwise, compute a square root w of q modulo ℓ.

(II) If

$$(x^{q^2} - x)f_w^2(x)(x^3 + ax + b) + f_{w-1}(x)f_{w+1}(x)$$

is coprime to $f_\ell(x)$ in case k is even, or if

$$(x^{q^2} - x)f_w^2(x) + f_{w-1}(x)f_{w+1}(x)(x^3 + ax + b)$$

is coprime to $f_\ell(x)$ in case k is odd, then $t \equiv 0 \pmod{\ell}$. (In this case, neither $-w$ nor w is an eigenvalue of φ_ℓ.)

(III) Define

$$\Lambda := -f_{w+2}^2(x)f_{w-1}(x) + f_{w-2}^2(x)f_{w+1}(x).$$

If

$$\gcd\Big(4(x^3+ax+b)^{(q-1)/2}f_w^3(x) + \Lambda, f_\ell(x)\Big) = 1$$

if w is even, or

$$\gcd\Big(4(x^3+ax+b)^{(q+3)/2}f_w^3(x) + \Lambda, f_\ell(x)\Big) = 1$$

if w is odd, then $t \equiv -2w \pmod{\ell}$. (In this case $-w$ is an eigenvalue.)

(IV) Otherwise $t \equiv 2w \pmod{\ell}$. (In this case w is an eigenvalue.)

(b) Case 2: $\psi_\ell^2(P) \neq \pm qP$ for all $P \in E[\ell]$.
We will test which of the relations $\varphi_\ell^2 + q = \tau\varphi_\ell$ hold for $\tau \in \{1, 2, \ldots, \ell - 1\}$.
For this, one has to evaluate polynomials modulo $f_\ell(x)$ and test whether they are zero modulo $f_\ell(x)$. The polynomials to test if they are zero modulo $f_\ell(x)$ are

$$\Big(\big(\psi_{k-1}\psi_{k+1} - \psi_k(x^{q^2} + x^q + x)\big)\beta^2 + \psi_k^2\alpha^2\Big)\psi_\tau^{2q} + \psi_{\tau-1}^q\psi_{\tau+1}^q\beta^2\psi_k^2$$

and

$$4y^q\psi_\tau^{3q}\Big(\alpha\big((2x^{q^2}+x)\psi_k^2 - \psi_{k-1}\psi_{k+1}\big) \\ - y^{q^2}\beta\psi_k^2\Big) - \beta\psi_k^2(\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2)^q,$$

after first eliminating y^2 using $y^2 = x^3 + ax + b$ and dividing by y if necessary. Here

$$\alpha = \psi_{k+2}\psi_{k-1}^2 - \psi_{k-1}\psi_{k+1}^2 - 4y^{q^2+1}\psi_k^3$$

and

$$\beta = \Big((x - x^{q^2})\psi_k^2 - \psi_{k-1}\psi_{k+1}\Big)4y\psi_k.$$

(d) Compute t from the $t \mod \ell$, $\ell \in \mathscr{P}_L$, using the Chinese Remainder Theorem (see also Proposition 2.5.6) and Hasse's Theorem, which asserts $|t| \leq 2\sqrt{q}$.

Proposition 4.2.63. *[Sch85, p. 490] This algorithm has deterministic running time $\mathcal{O}(\log^9 q)$ and a memory consumption of $\mathcal{O}(\log^5 q)$.*

4.3 Elliptic Curves over Rings

In this section we treat elliptic curves over rings. Clearly these are the generalized elliptic curves over a base $\operatorname{Spec} R$, where R is a ring. In Section 3.6 we saw that if $\operatorname{Pic} R$ is trivial, all points of $\mathbb{P}_R^2$ and, hence, of an elliptic curve over R, are of the form $(x : y : z) \in \mathbb{P}^2(R)$. As this condition is satisfied by the rings that are of special interest for applications, i. e. for Artinian rings, we focus only on such points even if $\operatorname{Pic} R \neq 0$.

We begin this section by defining some notations for handling elliptic curves over a ring R. Then we first look at the points of the curve in $\mathbb{P}^2(R)$ and we will describe the functorial behavior of an elliptic curve. Then a "geometric" group law is introduced on the points for the case that $\operatorname{Pic} R = 0$. Finally, we show that this group law is the same as the one from Theorem 4.1.6. At the end we will give a geometric interpretation of elliptic curves over Artinian rings.

Now we will begin with a notation for treating elliptic curves by their coefficients of the defining Weierstraß equation.

Definition 4.3.1. *Let R be any ring. A* defining vector *for an elliptic curve is an element $a = (a_1, a_2, a_3, a_4, a_6) \in R^5$ such that the discriminant $\Delta = \Delta(a_1, a_2, a_3, a_4, a_6)$ for the Weierstraß equation*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

is a unit in R. The curve defined by this Weierstraß equation in $\mathbb{P}^2(R)$ is denoted by E_a, and the discriminant *by Δ_a. To denote that E_a is a curve with $a \in R^5$, we will use the notation E_a/R. To denote the set of R-valued points of E_a, we write $E_a(R)$.*

Moreover, we will identify E_a with the projective R-scheme $\operatorname{Proj} R[x, y, z]/\langle f_a\rangle$, *where*

$$f_a := y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3,$$

if $\operatorname{Pic}(\operatorname{Spec} R) = 0$ *(see Corollary 3.5.3).*

Remark 4.3.2. Note that $E_a(R)$ always contains $\infty = (0 : 1 : 0)$.

We next want to show that an elliptic curve E_a/R with $a \in R^5$ is, as a scheme, a generalized elliptic curve over $\operatorname{Spec} R$. For this we begin by showing that f_a is prime modulo every maximal ideal of R. We need two lemmas for this, and the fact that a polynomial over a field is prime if, and only if, it is irreducible if, and only if, the ideal it generates is prime.

Lemma 4.3.3. *Let $\mathbb{F}$ be a field, and $f \in \mathbb{F}[x_0, \dots, x_n]$ be a homogenous polynomial of positive degree. Then the following are equivalent:*

(i) *The polynomial f is prime in $\mathbb{F}[x_0, \dots, x_n]$.*

(ii) *There exists an i such that x_i does not divide f and that $f|_{x_i=1}$ is prime in $\mathbb{F}[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$.*

Proof. If x_i divides f and f is prime, then clearly $f = \lambda x_i$ with $\lambda \in \mathbb{F}^*$. In this case chose another i. Assume that x_i does not divide f. If then $x_i^j g \in \langle f\rangle$ for $j \in \mathbb{N}$ and $g \in \mathbb{F}[x_0, \dots, x_n] =: R$, we have that $g \in \langle f\rangle$. Therefore, we have that f is prime in R if, and only if, $f/1$ is prime in R_{x_i} by Proposition 2.2.15 (c) and (b). Now $f/1$ is prime in R_{x_i} if, and only if, f/x_i^j is prime for $j = \deg f$. Next, $f/x_i^j \in R_{x_i}$ is prime if, and only if, $f/x_i^j \in R_{(x_i)}$ is prime, since for primality testing one can restrict to homogenous elements by Proposition 2.3.4 (d), and $x_i \in R_{x_i}$ is a unit. Now we can conclude with $R_{(x_i)} \cong \mathbb{F}[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$. □

We use this lemma to show that the homogenous Weierstraß equation is prime in $\mathbb{F}[x, y, z]$ by showing that the dehomogenization for $z = 1$ is prime in $\mathbb{F}[x, y]$:

Lemma 4.3.4. *Let $\mathbb{F}$ be a field and $f = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6 \in \mathbb{F}[x,y]$, where $a_i \in \mathbb{F}$. Then f is prime in $\mathbb{F}[x,y]$.*

Proof. Assume that $f = -gh$ with $g, h \in \mathbb{F}[x,y]$.

Write g, h as polynomials in $(\mathbb{F}[y])[x]$ and assume $\deg_x g \geq \deg_x h$. Since $\deg_x g + \deg_x h = \deg_x f = 3$ and both are integers, either $\deg_x g = 3$ or $\deg_x g = 2$. We can assume that both g and h are monic, seen as polynomials over $\mathbb{F}[y]$.

If $\deg_x g = 3$, then $\deg_x h = 0$. As h is monic, it must be 1 and, therefore, $-g = f$. If $\deg_x g = 2$, then $\deg_x h = 1$. Thus $g = x^2 + \hat{g}$, $h = x + \hat{h}$, where $\hat{g} = \hat{g}_1 x + \hat{g}_0$ and $\hat{g}_0, \hat{g}_1, \hat{h} \in \mathbb{F}[y]$. Therefore, $gh = x^3 + x^2(\hat{h}+\hat{g}_1) + x(\hat{g}_0 + \hat{g}_1\hat{h}) + \hat{g}_0\hat{h}$. By comparing coefficients we get

$$\hat{h} + \hat{g}_1 = a_2, \qquad \hat{g}_0 + \hat{g}_1\hat{h} = a_4 - a_1 y, \qquad \hat{g}_0\hat{h} = a_6 - a_3 y - y^2.$$

Now $\deg_y \hat{h} = \deg_y \hat{g}_1$ by the first equation. First, consider $\deg_y \hat{h} = \deg_y \hat{g}_1 = 0$; then $\deg_y \hat{g}_0 = 1$ by the second equation, contradicting the third equation.

Hence, $\deg_y \hat{h} = \deg_y \hat{g}_1 > 0$. By the second equation we get $\deg_y \hat{g}_0 = \deg_y \hat{h} + \deg_y \hat{g}_1 \geq 2$, but this contradicts the third equation. □

Therefore, we can conclude:

Corollary 4.3.5. *Let R be a ring and $f = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in R[x,y,z]$, where $a_i \in R$. If $\mathfrak{m}$ is a maximal ideal of R, then $f \mod \mathfrak{m}$ is prime over $\overline{R/\mathfrak{m}}$, where $\overline{R/\mathfrak{m}}$ is the algebraic closure of $R/\mathfrak{m}$. Moreover, f is a non-zero-divisor.*

Proof. That f is a non-zero-divisor can be seen by taking a monomial order $\leq$ on $\mathbb{N}^3$ such that x^3 is the leading term of f. □

Together with the results from Section 3.8.2 we can conclude:

Corollary 4.3.6. *Let E_a/R be an elliptic curve over a ring R. Then the scheme E_a over $\operatorname{Spec} R$ is a generalized elliptic curve.*

Proof. This follows from Corollary 4.3.5, Proposition 3.8.14 and Proposition 4.2.4 (b). □

Remark 4.3.7. As already noted it can be shown that every generalized elliptic curve over $\operatorname{Spec} R$ has this form (see [KM85, pp. 67–69, Section 2.2]).

4.3.1 The Set of Points

In the Theory of Schemes there is the concept of the Functor of Points for a scheme: assume X is a scheme over a base S. Then $\operatorname{Hom}_S(-, X)$ is a contravariant functor from the category $\mathscr{S}ch(S)$ of S-schemes to the category $\mathscr{S}et$ of sets. Combining this with the contravariant equivalence of categories of rings and affine schemes, we get a covariant functor from $\mathscr{R}ing/R$, the category of R-algebras, to $\mathscr{S}et$, if $S = \operatorname{Spec} R$. We will now show this directly for elliptic curves over rings, where we only consider points of the form $(x : y : z) \in \mathbb{P}^2(R)$. Note that most of this section is applicable for any kind of smooth variety over rings, if one defines this correctly.

We first show that an elliptic curve E_a/R gives a covariant functor:

Proposition 4.3.8. *Let $\varphi : R \to S$ be a morphism of rings and $a \in R^5$ the defining vector for an elliptic curve over R. Then $E_{\varphi(a)}$ is an elliptic curve over S with defining vector $\varphi(a)$ and then φ extends naturally to a map $\tilde{\varphi} : E_a(R) \to E_{\varphi(a)}(S)$.*

Proof. That $E_{\varphi(a)}$ is an elliptic curve follows directly from the fact that ring morphisms map units onto units. For the next statement compare Lemma 3.1.4, and note that if $(x : y : z) \in E_a(R)$ satisfies a Weierstraß equation, then $\tilde{\varphi}(x : y : z) = (\varphi(x) : \varphi(y) : \varphi(z))$ clearly satisfies the image of the Weierstraß equation under φ. □

Remark 4.3.9. Let R be a ring and $\mathfrak{m}$ a maximal ideal, and $\varphi : R \to R/\mathfrak{m}$ the canonical projection. Since $E_{\varphi(a)}$ is an elliptic curve over a field if E_a is an elliptic curve over R, one sees at once that every point of the form $(x : y : z) \in E_a(R)$ with $z \in \mathfrak{m}$ must satisfy $x \in \mathfrak{m}$, since $(0 : 1 : 0) \in E_{\varphi(a)}(R/\mathfrak{m})$ is the only infinite point.

We next show that this functor preserves direct products:

Proposition 4.3.10. *Let $R = R_1 \times R_2$ be a ring, and let $\varphi_i : R \to R_i$, $i = 1, 2$ the projections. Let E_a be an elliptic curve over R and let $\tilde{\varphi}_i : E_a(R) \to E_{\varphi_i(a)}(R_i)$, $i = 1, 2$ be the induced maps. Then there is a natural bijection*

$$E_a(R) \cong E_{\varphi_1(a)}(R_1) \times E_{\varphi_2(a)}(R_2)$$

given by $(\tilde{\varphi}_1, \tilde{\varphi}_2)$.

Proof. Since $x_1 + x_2 \in R^*$ for $x_i \in R_i$ if and only if $x_i \in R_i^*$ for both i, and $R = R_1 \times R_2$, one easily sees that the induced maps $\mathbb{P}^2(R) \to \mathbb{P}^2(R_1) \times \mathbb{P}^2(R_2)$ and $E_a(R) \to E_{\varphi_1(a)}(R_1) \times E_{\varphi_2(a)}(R_2)$ are bijections. □

Next we present an important result which gives more information in a special case of Remark 4.3.9, which is extremely important for applications:

Lemma 4.3.11. *Let R be a local Artinian ring with maximal ideal $\mathfrak{m}$, and $R \to R/\mathfrak{m}$ be the canonical projection. If E_a is an elliptic curve over R, the induced map $E_a(R) \to E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$ is surjective, and for every point in $E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$ there is a bijection between its preimage and $\mathfrak{m}$.*

Proof. Let $q : R \to R/\mathfrak{m}$ be the projection and $\tilde{q} : E_a(R) \to E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$ the induced map. Let

$$f = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 - y^2z - a_1xyz - a_3yz^2 \in R[x, y, z]$$

be the defining polynomial of E_a/R, and let $(\hat{x} : \hat{y} : \hat{z}) \in E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$.

If $\hat{z} = 0$, we know that $\hat{x} = 0$ and $\hat{y} = 1$ since the only infinite point is $\infty = (0 : 1 : 0)$. So we are first interested in all $(x : y : z) \in E_a(R)$ which are mapped onto $(0 : 1 : 0)$ by $\hat{q}$. Clearly y must be a unit, and x and z non-units. We can assume that $y = 1$. Hence, we are trying to count the non-unit solutions x and z to the equation $f(x, 1, z) = 0$. Let x be any element of $\mathfrak{m}$. Then $f(x, 1, z) = x^3 + axz^2 + bz^3 - z \in R[z]$ and $\frac{df}{dz}(x, 1, 0) \equiv -1 \pmod{\mathfrak{m}}$ and, thus, by Proposition 2.1.9 (note that $\mathfrak{m}$ is nilpotent by Lemma 2.2.21) we know that there is exactly one $z \in \mathfrak{m}$ such that $(x : 1 : z) \in E_a(R)$.

If $\hat{z} \neq 0$, we are interested in all $(x : y : 1) \in E_a(R)$ such that $x + \mathfrak{m} = \hat{x}$ and $y + \mathfrak{m} = \hat{y}$. Since $E_{a \mod \mathfrak{m}}(R/\mathfrak{m})$ is a smooth curve, we know that $(\frac{df}{dx}, \frac{df}{dy})(\hat{x}, \hat{y}, 1) \neq (0,0)$. Therefore, by either fixing $x \in \hat{x}$ or $y \in \hat{y}$, we find exactly one $y \in \hat{y}$ or $x \in \hat{x}$, respectively, such that $(x : y : 1) \in E_a(R)$. □

We are now able to provide a formula for the number of points of an elliptic curve over a finite ring R, which reduces the problem of counting points over a ring to the problem of counting points over a field in case that the decomposition of R into local rings and their maximal ideals are known.

Corollary 4.3.12. *Let $R = \prod_{i=1}^n R_i$, where the R_i's are finite local rings with maximal ideals $\mathfrak{m}_i$. Let E_a be an elliptic curve over R, where $a = a_1 + \cdots + a_n$, $a_i \in R_i^5$. Then*

$$|E_a(R)| = \prod_{i=1}^n |E_{a_i}(R_i)| = \prod_{i=1}^n |\mathfrak{m}_i| \cdot |E_{a_i \mod \mathfrak{m}_i}(R_i/\mathfrak{m}_i)|\,.$$

In this formula, the $E_{a_i \mod \mathfrak{m}_i}(R_i/\mathfrak{m}_i)$ are elliptic curves over the finite fields $R_i/\mathfrak{m}_i$.

Remark 4.3.13. Note that by Corollary 2.2.20, every finite ring R can be written as the product of finite local rings. If this isomorphism can be effectively computed and the reductions $R_i \to R_i/\mathfrak{m}_i$ can also be effectively computed, then one can compute $|E_a(R)|$ for an elliptic curve E_a over R by computing $|E_{a \mod \mathfrak{m}}(R/\mathfrak{m})|$ over the finite field $R/\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of R. And for this case we know effective algorithms (see Section 4.2.9).

Corollary 4.3.14. *Let R be a finite ring. If E_a is an elliptic curve over R, then*

$$\frac{|E_a(R)|}{|R|} = \prod_{\mathfrak{m} \in \operatorname{Spec} R} \frac{|E_{a \mod \mathfrak{m}}(R/\mathfrak{m})|}{|R/\mathfrak{m}|}.$$

Proof. By the Structure Theorem for Artinian Rings write $R = \prod_{i=1}^n R_i$, with the R_i's finite local rings with maximal ideals $\mathfrak{m}_i \subseteq R_i$. Then the $\mathfrak{m}^{(i)} := R_1 \times \cdots \times R_{i-1} \times \mathfrak{m}_i \times R_{i+1} \times \cdots \times R_n$ are exactly the maximal ideals of R, and $\operatorname{Spec} R = \{\mathfrak{m}^{(1)}, \dots, \mathfrak{m}^{(n)}\}$. Therefore, we have

$$\begin{aligned}\frac{|E_a|}{|R|} &= \prod_{i=1}^n \frac{|\mathfrak{m}_i|\,|E_{a \mod \mathfrak{m}^{(i)}}(R_i/\mathfrak{m}_i)|}{|R_i|} = \prod_{i=1}^n \frac{|E_{a \mod \mathfrak{m}^{(i)}}(R_i/\mathfrak{m}_i)|}{|R_i/\mathfrak{m}_i|} \\ &= \prod_{i=1}^n \frac{|E_{a \mod \mathfrak{m}^{(i)}}(R/\mathfrak{m}^{(i)})|}{|R/\mathfrak{m}^{(i)}|} = \prod_{\mathfrak{m} \in \operatorname{Spec} R} \frac{|E_{a \mod \mathfrak{m}}(R/\mathfrak{m})|}{|R/\mathfrak{m}|}.\end{aligned}$$

□

We will now fix a notation we will use quite often:

Notation 4.3.15. *If $R = \bigoplus_{i=1}^n R_i$ with projections $p_i : R \to R_i$, or $\mathfrak{a}$ is an ideal of R, and E_a/R an elliptic curve, we will write E_a/R_i or $E_a/(R/\mathfrak{a})$ instead of the (formally correct) $E_{p_i(a)}/R_i$ or $E_{a \mod \mathfrak{a}}/(R/\mathfrak{a})$, respectively. The same also holds for $E_a(R_i)$ and $E_a(R/\mathfrak{a})$.*

Remark 4.3.16. With the help of Proposition 4.3.10, Lemma 4.3.11 and by Remark 2.1.10 we can describe an effective method for finding a point on an elliptic curve E_a/R over an Artinian ring in case that its decomposition $R = \prod_{i=1}^{n} R_i$ into local Artinian rings and their maximal ideals are given. If the $\mathfrak{m}_i$'s are the maximal ideals of the R_i's, we first find points $P_i \in E_a(R_i/\mathfrak{m}_i)$. By Remark 2.1.10 and the Proof of Lemma 4.3.11 we can effectively lift these to points $\hat{P}_i \in E_a(R_i)$, i. e. modulo $\mathfrak{m}_i$ we have that $\hat{P}_i$ reduces to P_i for $1 \leq i \leq n$. By the bijection from Proposition 4.3.10 we then obtain a point $P \in E_a(R)$ from the $\hat{P}_i$'s.

4.3.2 The Group of Points

Before trying to find explicit formulae for computing the group law we inspect what consequences the group law has in our context. In this subsection we will always work with rings R such that $\operatorname{Pic}(\operatorname{Spec} R) = 0$. By Corollary 3.5.3 and the results from Section 2.4 this is, for example, fulfilled if R has finitely many maximal ideals, hence, this includes the case of fields, Artinian rings and finite rings.

Let E_a be an elliptic curve defined over R. Then by Corollary 4.3.6, the scheme

$$E_a/\operatorname{Spec} R$$

is a generalized elliptic curve. By Proposition 3.6.5 there is a natural one-to-one correspondence between points $P \in E_a(R)$ and between R-valued points $s \in E_a(\operatorname{Spec} R)$ (scheme-theoretic points). Thus, we will identify $E_a(R)$ and $E_a(\operatorname{Spec} R)$ from now on.

By Corollary 4.1.9 the (scheme-theoretic) points of E_a form an Abelian group, where for three points $s_1, s_2, s_3 \in E_a(R)$ we have $s_1 + s_2 = s_3$ if, and only if,

$$[s_1] + [s_2] \sim [s_3] + [\infty],$$

where $\infty = (0 : 1 : 0)$ is the base point. From Corollary 4.1.8 we know that if $R = R_1 \times R_2$, then $E_a(R) \cong (E_a)_{R_1}(R_1) \times (E_a)_{R_2}(R_2)$. But now by Proposition 3.4.11 we know $(E_a)_{R_i} = E_{\varphi_i(a)}$, where $\varphi_i : R \to R_i$ is the projection. Therefore,

$$E_a(R) \cong E_{\varphi_1(a)}(R_1) \times E_{\varphi_2(a)}(R_2).$$

Moreover, if $\varphi : R \to S$ is an arbitrary ring morphism, then since E_a/R is a group scheme, the induced morphism $E_a(R) \to E_{\varphi(a)}(S)$ is compatible with the group structure. Hence, the bijection in Proposition 4.3.8 is the map of points for the isomorphism $E_a(R) \cong E_{\varphi_1(a)}(R_1) \times E_{\varphi_2(a)}(R_2)$ as schemes.

Now, assume that S is an arbitrary ring extension of R, i. e. it does not necessarily satisfy $\operatorname{Pic}(\operatorname{Spec} S) = 0$. Then for all points $P_1, P_2 \in E_a(S)$ satisfying that there is an intermediate ring $\hat{S}$ between R and S such that $\operatorname{Pic}(\operatorname{Spec} \hat{S}) = 0$ and $P_1, P_2 \in \mathbb{P}^2(\hat{S})$, the sum $P_1 + P_2 \in E_a(S)$ lies in $\mathbb{P}^2(\hat{S}) \subseteq \mathbb{P}^2(S)$ because of the natural injection $E_a(\hat{S}) \hookrightarrow E_a(S)$. Therefore, theoretically, we could also work with rings R, which do not satisfy $\operatorname{Pic}(\operatorname{Spec} R) = 0$, by restricting to certain points of $E_a(R)$, which would form a subgroup.

4.3.3 A "Geometric" Group Law on $E_a(R)$

We now want to define a "geometric" group law on $E_a(R)$ for R, a ring satisfying $\operatorname{Pic} R = 0$. The definition originated with H. W. Lenstra in [Len86]. It turns out that this group law satisfies the same properties as the ones we found for the natural group law on the generalized elliptic curve E_a/R, as seen in the last subsection. We will ultimately see that this group law corresponds to the group law as defined previously in Abel's Theorem 4.1.6.

Before we start we want to explain why we have decided to call this group law "geometric": it uses the formulae developed from the geometric Chord and Tangent Law of elliptic curves over fields in Section 4.2.2.

Let R be a ring such that $\operatorname{Pic}(\operatorname{Spec} R) = 0$. We characterized the latter property in Section 2.4 (see also Corollary 3.5.3). One of the main results which is essential for defining the group law is Corollary 2.4.23, which says that for a ring R the following conditions are equivalent:

(i) Every projective R-module of rank one is free. (By Corollary 3.5.3, this is equivalent to $\operatorname{Pic}(\operatorname{Spec} R) = 0$.)

(ii) For every primitive matrix $A \in R^{n\times m}$, such that every two-by-two minor vanishes, there exists an R-linear combination of the columns (or alternatively the rows) of A, which is primitive. Moreover, the linear combination is unique up to multiplication by units.

Recall that we have a complete set of addition laws for elliptic curves, which is parameterized by the coefficients of the Weierstraß equation (see Section 4.2.3). Let this be given by the polynomials $\varphi_{i,j} \in S$, $1 \leq i \leq 2$ and $0 \leq j \leq 2$, where

$$S = \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][x_1, y_1, z_1, x_2, y_2, z_2].$$

Then $\varphi_{i,a} := (\varphi_{i,0}(a), \varphi_{i,1}(a), \varphi_{i,2}(a)) \in (R[x_1, y_1, z_1, x_2, y_2, z_2])^3$ is one addition formula for the definition vector $a \in R^5$.

Let E_a be a curve over R and let $P_1, P_2 \in E_a(R)$. Consider the matrix

$$M_a(P_1, P_2) = \Big(\varphi_{i,a}(P_1, P_2)\Big)_{1\leq i\leq 2}.$$

If $\mathfrak{m}$ is a maximal ideal of R, then modulo $\mathfrak{m}$ these are the addition formulae for the elliptic curve $E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$ over the field $R/\mathfrak{m}$. Since $P_1 \mod \mathfrak{m}$ and $P_2 \mod \mathfrak{m}$ are valid points on $E_{a \bmod \mathfrak{m}}(R/\mathfrak{m})$, this matrix is nonzero modulo $\mathfrak{m}$. Therefore, $M_a(P_1, P_2)$ is primitive. By Proposition 4.2.19 (a) all two-by-two minors vanish. Then, by the assumption on R, there exists a unique primitive R-linear combination of the rows of M_a, which is uniquely determined up to multiplication by units. Therefore it defines a unique point in $\mathbb{P}^2(R)$ and, since $f_a(\varphi_{i,a}) = 0$ by Proposition 4.2.19 (b), it is a point in $E_a(R)$. Define this point as $P_1 \oplus P_2$. We get the following result:

Corollary 4.3.17. *For any ring R satisfying $\operatorname{Pic} R = 0$, and any elliptic curve E_a/R, the set of R-rational points $E_a(R)$ becomes an Abelian group under the operation $\oplus$.*

Proof. This follows from Proposition 4.2.19. □

As showing this by explicit computations carried out by a computer algebra system is not very enlightening, we will show this in a completely different way.

Before continuing we want to remark why the requirement $\operatorname{Pic} R = 0$ is needed:

(a) If $\operatorname{Pic} R \neq 0$, then by Corollary 2.4.23 one cannot necessarily compute a primitive linear combination from the rows of $M_a(P_1, P_2)$.

(b) A more intrinsic reason is that by Proposition 3.4.33, points on an elliptic curve over an arbitrary ring R are, in general, represented by projective R-modules of rank one and three elements of it, which generate the module. Hence, locally, every point is of the form $(x : y : z) \in \mathbb{P}^2(R_\mathfrak{p})$, $\mathfrak{p} \in \operatorname{Spec} R$, but not globally and, therefore, the sum of two points $P_1, P_2 \in \mathbb{P}^2(R)$ might not again be in $\mathbb{P}^2(R)$ but only locally in $\mathbb{P}^2(R_\mathfrak{p})$, $\mathfrak{p} \in \operatorname{Spec} R$.

For the moment let us assume that we have shown that $\oplus$ defines a valid group law. If R is a finite ring, with the tools developed earlier, like the algorithm `ComputePrimitiveCombination` (see page 49) or specializations for special rings, one can efficiently compute $P_1 \oplus P_2$, especially as we have a 2×3 matrix. (See also the discussion before the description of the algorithm.)

Moreover, if $\varphi : R \to S$ is a ring morphism, where S is also a ring satisfying $\operatorname{Pic}(\operatorname{Spec} S) = 0$, consider the induced map $\tilde{\varphi} : E_a(R) \to E_{\varphi(a)}(S)$. One can easily see that it becomes a group morphism under the operation $\oplus$.

Now we come to a construction that will ultimately show that $\oplus$ is the same as $+$ on $E_a(R)$.

Let R be any ring. Clearly R is a $\mathbb{Z}$-algebra and, therefore, can be written as a quotient $S/\mathfrak{a}$ of $S = \mathbb{Z}[\{x_i \mid i \in I\}]$, where I is some (possibly very large) index set and $\mathfrak{a}$ is an ideal in S. Now S is an integral domain and, therefore, it has a field of fractions $K = K(S)$, which clearly has an algebraic closure $\overline{K}$. As for elliptic curves over $\overline{K}$, the addition formulae clearly work, and we will ultimately reduce to this case. Let E_a/R be any elliptic curve with defining vector $a \in R^5$, and let $\hat{a} \in S^5$ be a lift of a, i. e. a vector such that $\hat{a}_i \mod \mathfrak{a} = a_i$ for every i. Let $\hat{\Delta} = \Delta_{\hat{a}}$ be the discriminant of $E_{\hat{a}}/S$, define $U := \{\hat{\Delta}^n \mid n \in \mathbb{N}\}$ and let $\hat{S} = U^{-1}S$; as $\Delta \neq 0$ (otherwise $\Delta_a = 0$ and, therefore, E_a/R would not be an elliptic curve) $\hat{S}$ is an intermediate ring between S and K, and K is the field of fractions of both $\hat{S}$ and S. Moreover, $E_{\hat{a}}/\hat{S}$ is an elliptic curve.

We now have that the scheme E_a/R is a closed subscheme of $E_{\hat{a}}/\hat{S}$ (in the sense that both E_a is a closed subscheme of $E_{\hat{a}}$, and $\operatorname{Spec} R$ is a closed subscheme of $\operatorname{Spec} \hat{S}$, since $\Delta_a \in R$ is invertible), and $E_{\hat{a}}$ and $\operatorname{Spec} \hat{S}$ are both integral schemes. We also have that the integral scheme $E_{\hat{a}}/\overline{K}$ is the geometric fibre of $E_{\hat{a}}/\hat{S}$ at the generic point of $\operatorname{Spec} \hat{S}$ and, therefore, by Proposition 3.4.15 and the functoriality of the group law (Theorem 4.1.6), the group law of $E_{\hat{a}}/\hat{S}$ is determined by the one of $E_{\hat{a}}/\overline{K}$. As again by the functoriality of the group law, the group law on E_a/R is determined by the one on $E_{\hat{a}}/\hat{S}$ (if $m : E_{\hat{a}} \times_{\hat{S}} E_{\hat{a}} \to E_{\hat{a}}$ is the group law on $E_{\hat{a}}/\hat{S}$, then $m_{\operatorname{Spec} R}$ is the group law on E_a/R; see also Proposition 3.4.10). Then the formulae for the group law on elliptic curves over fields from Section 4.2.3 can also be used for elliptic curves over rings.

As a last step we will explicitly construct the $\hat{S}$-morphism $m : E_{\hat{a}} \times E_{\hat{a}} \to E_{\hat{a}}$ given by the formulae from Section 4.2.3. This finally shows that these addition laws can be used (in some way) for any ring, since by the above argument this morphism is identical to the group law given by Theorem 4.1.6. (In fact, since any generalized elliptic curve over an arbitrary base scheme can be obtained by glueing generalized elliptic curves over rings, and since the base scheme can be obtained by glueing affine $\operatorname{Spec} R$'s, the group law on any generalized elliptic curve over an arbitrary base scheme is determined by the formulae from Section 4.2.3.)

Clearly $E_{\hat{a}}$ can be covered by $D_+(y)$ and $D_+(z)$, since if $\mathfrak{p}$ is a homogenous prime of $\hat{S}[x,y,z]/\langle f\rangle$, with f a Weierstraß equation, which is not in $D_+(y)\cup D_+(z)$, then it contains both y and z. But then it also contains x^3 since $f(x,y,z)=0$ in $\hat{S}[x,y,z]/\langle f\rangle$ and, since $\mathfrak{p}$ is prime, it therefore contains x. But then $\mathfrak{p}$ contains the irrelevant ideal and is therefore not in $\operatorname{Proj}\hat{S}[x,y,z]/\langle f\rangle$ anyway.

Therefore, we can cover $E_{\hat{a}}\times E_{\hat{a}}$ by the four affine subsets

$$\begin{array}{lcl} D_+(y)\times D_+(y), & & D_+(y)\times D_+(z), \\ D_+(y)\times D_+(z) & \text{and} & D_+(z)\times D_+(z). \end{array}$$

(See Proposition 3.3.24 (b) and Remark 3.4.2.) We construct the map $m|_U : U\to E_{\hat{a}}$ exemplary with $U := D_+(z)\times D_+(z)$. By the same method the other maps from the affine subsets of $E_{\hat{a}}\times E_{\hat{a}}$ to $E_{\hat{a}}$ can be constructed, and clearly they coincide on the intersections and, therefore, define m.

Let the formulae from Section 4.2.3 be denoted by

$$\begin{aligned} \varphi_{i,j} &\in ((\hat{S}[x_1,y_1,z_1,x_2,y_2,z_2]/\langle f(x_1,y_1,z_1),f(x_2,y_2,z_2)\rangle)_{(z_1)})_{(z_2)} \\ &\cong \hat{S}[x_1,y_1,x_2,y_2]/\langle f(x_1,y_1,1),f(x_2,y_2,1)\rangle =: \tilde{S}, \end{aligned}$$

where f is the Weierstraß equation for $E_{\hat{a}}$ and $1\le i\le 2$, $0\le j\le 2$. We have $U=\operatorname{Spec}\hat{S}[x_1,y_1,x_2,y_2]/\langle f(x_1,y_1,1),f(x_2,y_2,1)\rangle = \operatorname{Spec}\tilde{S}$ by Lemma 2.1.36. Define $U_i := U\setminus V(\langle\varphi_{i,0},\varphi_{i,1},\varphi_{i,2}\rangle)$; we claim these sets cover U. Let $\mathfrak{p}\in U\setminus(U_1\cup U_2)$. Then $\varphi_{i,j}\in\mathfrak{p}$ for all i,j. Let $\hat{\mathfrak{p}} := \hat{S}\cap\mathfrak{p}$ and $\tilde{\mathfrak{p}} := \langle\hat{\mathfrak{p}}\rangle_{\tilde{S}}$. Then $\mathfrak{p}$ goes into a prime ideal in $\tilde{S}/\tilde{\mathfrak{p}}\otimes_{\hat{S}/\hat{\mathfrak{p}}}\overline{L}$, where $\overline{L}$ is the algebraic closure of L, which is the field of fractions of $\hat{S}/\hat{\mathfrak{p}}$, by the map $\tilde{S}\to\tilde{S}/\tilde{\mathfrak{p}}\to\tilde{S}/\tilde{\mathfrak{p}}\otimes\overline{K}$. Moreover, by choosing a maximal homogenous ideal of $\tilde{S}/\tilde{\mathfrak{p}}\otimes\overline{K}$ containing the image of $\mathfrak{p}$ but not the irrelevant ideal, we can assume that $\hat{S}$ is an algebraically closed field and $\mathfrak{p}$ is a closed point. But then $\varphi_{i,j}\in\mathfrak{p}$ for all i,j means that the $\varphi_{i,j}$'s simultaneously vanish at one point (in the classical sense; see Proposition 3.5.4) on an elliptic curve over $\overline{K}$, which contradicts that the $\varphi_{i,j}$'s come from a complete system of addition laws (see Theorem 4.2.18).

We now define maps $U_i\to E_{\hat{a}}$ by use of the formulae $\varphi_{i,j}$, $j=0,1,2$. We show this for $i=1$. Assume that the formulae $\varphi_{1,0},\dots,\varphi_{1,2}$ do not give results with $z=0$ (see Theorem 4.2.18 and the definition of φ_j after the theorem). We define $U_i\to E_{\hat{a}}$ by the affine morphism $U_i\to D_+(z)$ by the $\hat{S}$-linear ring morphism

$$(\hat{S}[x,y,z]/\langle f\rangle)_{(z)}\to\mathcal{O}_{E_{\hat{a}}\times E_{\hat{a}}}|_{U_1}(U_1), \qquad \begin{cases} \frac{x}{z}\mapsto\frac{\varphi_{1,0}}{\varphi_{1,2}}, \\ \frac{y}{z}\mapsto\frac{\varphi_{1,1}}{\varphi_{1,2}} \end{cases}$$

(note that $U_1\subseteq D_+(z)\times D_+(z)$, and see [Har77, p. 79, ch. II, Exercise 2.4]).

We have shown the following theorem:

Theorem 4.3.18. *Let E be a generalized elliptic curve over a base scheme S. Then the group law $m: E\times E\to E$ from Theorem 4.1.6 is locally on S given by the addition formulae from Section 4.2.3.*

In particular if $S = \operatorname{Spec} R$ with a local ring R, all S-points of E are of the form $(x : y : z) \in \mathbb{P}^2(R)$, and the formulae from Section 4.2.3 can be directly used to compute the sum of two points.

If $S = \operatorname{Spec} R$ with an arbitrary ring R satisfying $\operatorname{Pic} R = 0$, we also have that all S-points of E are of the form $(x : y : z) \in \mathbb{P}^2(R)$. In this situation the addition law on E can be computed using the algorithm described at the beginning of this section.

The negation formula $P \mapsto -P$ from Proposition 4.2.12 can be used for any R-point of the form $(x : y : z) \in \mathbb{P}^2(R)$ for any affine $S = \operatorname{Spec} R$, without any restrictions on R.

Proof. By Remark 4.2.5 the curve E is, locally on S, given by a Weierstraß equation; by the preceeding discussion we can conclude the first part of the claim.

For the second part of the claim note that by Proposition 2.4.12, we have $\operatorname{Pic} R = 0$ for every local ring R. Therefore, all S-points of E have the required form by Proposition 3.6.8. Let $P, Q \in E(R)$ be two R-points and $\varphi_{i,j}$ a complete set of addition laws. Since primitive in a local ring means that one element is a unit, we see that for one i the tuple $(\varphi_{i,j}(P, Q))_{0 \leq j \leq 2}$ is primitive and, therefore, this tuple gives the sum of P and Q; with this we can conclude the second claim.

For the third claim note that points on E are given by a projective R-module P with three elements of P which locally generate P; as P is free by assumption, there exists one element which generates P, and by the matrix condition (see Lemma 2.4.21) the resulting primitive vector globally generates P and thus defines a point (see the proof of Proposition 3.6.5). Since by the first claim the group law is locally given by the formulae from Section 4.2.3, the algorithm at the beginning of this section therefore computes the sum correctly.

The last claim can be shown by the same methods as in the discussion above. Therefore, we omit the proof. □

Before closing this chapter we want to sketch a more elementary way to prove this result, at least for Artinian rings. By Corollary 2.2.20, Corollary 2.2.23, Corollary 4.1.8 and Proposition 4.3.10, it is enough to show this for local Artinian rings. By Proposition 3.8.17 and Corollary 3.8.18, one sees that the structure of $\mathcal{K}$ and the local rings in this case are very close to that of a field. If $P = (x_1 : y_1 : z_1) \in E(R)$ is an R-valued point, we have, moreover:

(a) If $z_1 \notin \mathfrak{m}$ and $y_1 \not\equiv -y_1 - a_1x_1 - a_3z_1 \pmod{\mathfrak{m}}$, a local parameter of P is given by

$$\frac{x_1z - z_1x}{z} \in \mathcal{K}^*_{E,P}.$$

(b) If $z_1 \notin \mathfrak{m}$ and $y_1 \equiv -y_1 - a_1x_1 - a_3z_1 \pmod{\mathfrak{m}}$, a local parameter of P is given by

$$\frac{y_1z - z_1y}{z} \in \mathcal{K}^*_{E,P}.$$

(c) If $z_1 \in \mathfrak{m}$, a local parameter of P is given by

$$\frac{y_1x - x_1y}{y} \in \mathcal{K}^*_{E,P}.$$

By this, the Cartier divisor induced by the point P can be explicitly described: in some neighborhood of P it is defined by the local parameter, and on the complement of $\overline{\{P\}}$ it is locally defined by 1 (see [Wal99, p. 96]). Using this representation one can explicitly compute the tensor product in Theorem 4.1.6, and for every formula one can show that it remains valid. Unfortunately, even when one wants to show that $-(x_1 : y_1 : z_1)$ is given by $(x_1 : -y_1 - a_1x_1 - a_3z_1 : z_1)$, this computation is long and requires, moreover, explicit computation of the connecting line of every two points $P, Q \in E(R)$, which is a non-trivial task as, similarly to Section 4.2.3, finding an open cover of $E_{\hat{a}} \times E_{\hat{a}}$ and a formula for every set of the cover can be hard.

4.3.4 A "Geometric" Interpretation over Artinian Rings

We will now try to give a geometric interpretation of elliptic curves over Artinian rings. Let $R = \bigoplus_{i=1}^{n} R_i$ be the decomposition of an Artinian ring R into the product of local Artinian rings R_i, and assume E_a/R is an elliptic curve. From the discussion in Remark 3.8.15 we know that E_a/R can be seen as the disjoint union of the curves E_a/R_i, $i = 1, \ldots, n$. Therefore, we want to concentrate on the case that R is local.

We have seen that if R is local with maximal ideal $\mathfrak{m}$, and E_a/R is an elliptic curve, then $E_a/(R/\mathfrak{m})$ is an elliptic curve over the residue field $R/\mathfrak{m}$ and there is a surjective homomorphism $E_a(R) \to E_a(R/\mathfrak{m})$, which maps exactly $|\mathfrak{m}|$ points of $E_a(R)$ onto every point of $E_a(R/\mathfrak{m})$.

If one sees nilpotent elements of R as "infinitesimal" elements, one could interpret the R-rational points E_a as the $R/\mathfrak{m}$-rational points of E_a together with an infinitesimal neighborhood of points for every $R/\mathfrak{m}$-rational point.

4.3.5 Examples

In this subsection we consider examples of curves over the finite ring $\mathbb{Z}_{12}$, which is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$ by the Chinese Remainder Theorem. Note that $\mathbb{Z}_{12}$ is the smallest commutative non-local ring with a unit that is not a product of fields and which can be represented by a quotient of $\mathbb{Z}$.

By computer experiments we found the following curves over $\mathbb{Z}_{12}$ with the given number of $\mathbb{Z}_{12}$-rational points:

(a) $y^2z + xyz = x^3 - xz^2$ with 48 points.

(b) $y^2z - 5xyz + 2yz^2 = x^3 + 4x^2z + 5xz^2 + 6z^3$ with 40 points;

(c) $y^2z - 4xyz - yz^2 = x^3 + 6x^2z - 4xz^2 + 3z^3$ with 36 points;

(d) $y^2z + 6xyz + 3yz^2 = x^3 + 5x^2z - 5xz^2 + 4z^3$ with 30 points;

(e) $y^2z - 3xyz + 4yz^2 = x^3 + 1x^2z + 5xz^2 - 4z^3$ with 24 points;

(f) $y^2z + 4xyz - 5yz^2 = x^3 + 3x^2z + 5xz^2 - 5z^3$ with 18 points;

(g) $y^2z + xyz - 2yz^2 = x^3 - x^2z + 2xz^2 - 5z^3$ with 16 points;

(h) $y^2z - 5xyz - 3yz^2 = x^3 - 2x^2z - 5xz^2 + 5z^3$ with 8 points;

(i) $y^2z + xyz + 2yz^2 = x^3 - x^2z + xz^2 + 4z^3$ with 4 points.

In the following we want to inspect the curve in (f), namely

$$y^2z + 4xyz - 5yz^2 = x^3 + 3x^2z + 5xz^2 - 5z^3,$$

which has 18 $\mathbb{Z}_{12}$-rational points. Hence, with $a = (4, -5, 3, 5, -5)$, this is the curve $E_a/\mathbb{Z}_{12}$ using the notation from Definition 4.3.1.

The Curve over $\mathbb{Z}_2$

The equation reads $y^2z + yz^2 = x^3 + x^2z + xz^2 + z^3$ modulo 2. One quickly finds the three $\mathbb{Z}_2$-rational points

$$P_{2,0} = (0:1:0), \quad P_{2,1} = (1:0:1) \quad \text{and} \quad P_{2,2} = (1:1:1),$$

and the group of $\mathbb{Z}_2$-rational points is isomorphic to $\mathbb{Z}_3$ with the identity being $P_{2,0}$.

The Curve over $\mathbb{Z}_4$

The equation reads $y^2z - yz^2 = x^3 - x^2z + xz^2 - z^3$ modulo 4. We already know by Lemma 4.3.11 that the $\mathbb{Z}_4$-rational points of this curve are all lifts of the $\mathbb{Z}_2$-rational points of the curve in Section 4.3.5. A quick computer search finds the following points:

$$\begin{array}{llll} P_{4,0} = (0:1:0), & P_{4,1} = (1:0:1), & & P_{4,2} = (3:0:1), \\ P_{4,3} = (1:1:1), & P_{4,4} = (3:1:1) & \text{and} & P_{4,5} = (2:1:0). \end{array}$$

The natural reduction map $E_a/\mathbb{Z}_4 \to E_a/\mathbb{Z}_2$ looks as follows:

$$\begin{array}{llll} P_{4,0} \mapsto P_{2,0}, & P_{4,1} \mapsto P_{2,1}, & & P_{4,2} \mapsto P_{2,1}, \\ P_{4,3} \mapsto P_{2,2}, & P_{4,4} \mapsto P_{2,2} & \text{and} & P_{4,5} \mapsto P_{2,0}. \end{array}$$

The kernel of this map has cardinality 2 and, therefore, the kernel is isomorphic to $\mathbb{Z}_2$. The composition table for the $\mathbb{Z}_4$-rational points looks as follows:

$+$	$P_{4,0}$	$P_{4,1}$	$P_{4,2}$	$P_{4,3}$	$P_{4,4}$	$P_{4,5}$
$P_{4,0}$	$P_{4,0}$	$P_{4,1}$	$P_{4,2}$	$P_{4,3}$	$P_{4,4}$	$P_{4,5}$
$P_{4,1}$	$P_{4,1}$	$P_{4,4}$	$P_{4,3}$	$P_{4,0}$	$P_{4,5}$	$P_{4,2}$
$P_{4,2}$	$P_{4,2}$	$P_{4,3}$	$P_{4,4}$	$P_{4,5}$	$P_{4,0}$	$P_{4,1}$
$P_{4,3}$	$P_{4,3}$	$P_{4,0}$	$P_{4,5}$	$P_{4,2}$	$P_{4,1}$	$P_{4,4}$
$P_{4,4}$	$P_{4,4}$	$P_{4,5}$	$P_{4,0}$	$P_{4,1}$	$P_{4,2}$	$P_{4,3}$
$P_{4,5}$	$P_{4,5}$	$P_{4,2}$	$P_{4,1}$	$P_{4,4}$	$P_{4,3}$	$P_{4,0}$

One can see that the group $E_a(\mathbb{Z}_4)$ is isomorphic to $\mathbb{Z}_6$ by the isomorphism

$$\begin{array}{llll} P_{4,0} \mapsto 0 + 6\mathbb{Z}, & P_{4,1} \mapsto 1 + 6\mathbb{Z}, & & P_{4,2} \mapsto 4 + 6\mathbb{Z}, \\ P_{4,3} \mapsto 5 + 6\mathbb{Z}, & P_{4,4} \mapsto 2 + 6\mathbb{Z} & \text{and} & P_{4,5} \mapsto 3 + 6\mathbb{Z}. \end{array}$$

Moreover, it is obvious that the natural reduction $E_a(\mathbb{Z}_4) \to E_a(\mathbb{Z}_2)$ is a group morphism.

The Curve over $\mathbb{Z}_3$

The equation reads $y^2z + xyz + yz^2 = x^3 - xz^2 + z^3$ modulo 3. One quickly finds the three $\mathbb{Z}_3$-rational points

$$P_{3,0} = (0:1:0), \quad P_{3,1} = (2:2:1) \quad \text{and} \quad P_{3,2} = (2:1:1),$$

and the group of $\mathbb{Z}_3$-rational points is isomorphic to $\mathbb{Z}_3$ with the identity being $P_{3,0}$.

The Curve over $\mathbb{Z}_{12}$

Since $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ we get $E_a(\mathbb{Z}_{12}) \cong E_a(\mathbb{Z}_4) \times E_a(\mathbb{Z}_3)$, and hence the curve is expected to have $18 = 6 \cdot 3$ $\mathbb{Z}_{12}$-rational points. A quick computer search finds the following points, here given with their reduction modulo 4 and 3:

mod 12	mod 4	mod 3
$P_{12,0} = (0:1:0)$	$P_{4,0}$	$P_{3,0}$
$P_{12,1} = (5:5:1)$	$P_{4,3}$	$P_{3,1}$
$P_{12,2} = (5:8:1)$	$P_{4,1}$	$P_{3,1}$
$P_{12,3} = (11:8:1)$	$P_{4,2}$	$P_{3,1}$
$P_{12,4} = (5:1:1)$	$P_{4,3}$	$P_{3,2}$
$P_{12,5} = (11:5:1)$	$P_{4,4}$	$P_{3,1}$
$P_{12,6} = (5:4:1)$	$P_{4,1}$	$P_{3,2}$
$P_{12,7} = (11:4:1)$	$P_{4,2}$	$P_{3,2}$
$P_{12,8} = (11:1:1)$	$P_{4,4}$	$P_{3,2}$
$P_{12,9} = (2:1:4)$	$P_{4,5}$	$P_{3,2}$
$P_{12,10} = (10:1:8)$	$P_{4,5}$	$P_{3,1}$
$P_{12,11} = (3:1:9)$	$P_{4,4}$	$P_{3,0}$
$P_{12,12} = (3:4:3)$	$P_{4,1}$	$P_{3,0}$
$P_{12,13} = (3:4:9)$	$P_{4,2}$	$P_{3,0}$
$P_{12,14} = (9:1:9)$	$P_{4,3}$	$P_{3,0}$
$P_{12,15} = (4:1:8)$	$P_{4,0}$	$P_{3,1}$
$P_{12,16} = (8:1:4)$	$P_{4,0}$	$P_{3,2}$
$P_{12,17} = (6:1:0)$	$P_{4,5}$	$P_{3,0}$

The composition table is as follows, where we write i instead of $P_{12,i}$:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	1	7	16	9	13	6	0	17	12	11	8	2	15	10	3	4	14	5
2	2	16	8	4	0	9	11	14	17	13	7	10	5	1	15	6	12	3
3	3	9	4	8	17	16	14	11	0	12	6	15	1	5	10	7	13	2
4	4	13	0	17	3	12	15	10	2	5	11	6	16	9	7	14	1	8
5	5	6	9	16	12	7	17	0	13	14	4	3	10	15	2	8	11	1
6	6	0	11	14	15	17	5	1	10	3	13	9	8	4	16	12	2	7
7	7	17	14	11	10	0	1	5	15	2	12	16	4	8	9	13	3	6
8	8	12	17	0	2	13	10	15	3	1	14	7	9	16	6	11	5	4
9	9	11	13	12	5	14	3	2	1	15	0	4	7	6	8	17	10	16
10	10	8	7	6	11	4	13	12	14	0	16	1	3	2	5	9	17	15
11	11	2	10	15	6	3	9	16	7	4	1	13	17	0	12	5	8	14
12	12	15	5	1	16	10	8	4	9	7	3	17	11	14	0	2	6	13
13	13	10	1	5	9	15	4	8	16	6	2	0	14	11	17	3	7	12
14	14	3	15	10	7	2	16	9	6	8	5	12	0	17	13	1	4	11
15	15	4	6	7	14	8	12	13	11	17	9	5	2	3	1	16	0	10
16	16	14	12	13	1	11	2	3	5	10	17	8	6	7	4	0	15	9
17	17	5	3	2	8	1	7	6	4	16	15	14	13	12	11	10	9	0

Since the natural bijection $E_a(\mathbb{Z}_{12}) \cong E_a(\mathbb{Z}_4) \times E_a(\mathbb{Z}_3)$ is a group morphism, we know by the previous paragraphs that $E_a(\mathbb{Z}_{12}) \cong \mathbb{Z}_6 \times \mathbb{Z}_3$.

Finally we want to demonstrate cases where the addition formulae from Section 4.2.3 return two triples in $\mathbb{Z}_{12}^3$, which are both not primitive, but can be used to form a primitive element. This is the case if, and only if, one formula gives $(0, 0, 0)$ modulo 2, while the other gives $(0, 0, 0)$ modulo 3. For example, if one adds $P_{12,17} = (6:1:0)$ and $P_{12,11} = (3:1:9)$, one gets the results $A := (3, 3, 3)$ and $B := (0, 4, 0)$. For modulo 2, we have $P_{12,17} = (0:1:0)$ and $P_{12,11} = (1:1:1)$, while for modulo 3 we have $P_{12,17} = (0:1:0)$ and $P_{12,11} = (0:1:0)$. We now want to apply algorithm `ComputePrimitiveCombination` (see page 49) to this situation, i. e. to the matrix

$$\begin{pmatrix} 3 & 3 & 3 \\ 0 & 4 & 0 \end{pmatrix} \in \mathbb{Z}_{12}^{2\times 3}.$$

It is clearly primitive, as $\langle 3, 4\rangle_{\mathbb{Z}_{12}} = \mathbb{Z}_{12}$, and the two-by-two minors all vanish since $3 \cdot 0 = 3 \cdot 4 = 0 \in \mathbb{Z}_{12}$. As $|\mathbb{Z}_{12}| = 12$, for $t = 3$ we have $2^{t+1} = 16 > |\mathbb{Z}_{12}|$. For the first entry $c := 3$, we have $c^t = 3 \in \mathbb{Z}_{12}$. Thus, c is not nilpotent. Now we need an $x \in \mathbb{Z}_{12}$ such that $9 = c^{t+1}x = c^t = 3$. This is satisfied by $x = 3$ and $x = 7$. Choosing $x := 7$, we get $x^t = 7$ and $\hat{e} := c^t x^t = 9$. Clearly $\hat{e} \neq 1$ and, hence, $\hat{e}$ is a non-trivial idempotent. Indeed, $9^2 = 9 \in \mathbb{Z}_{12}$. We compute

$$A' := (1 - \hat{e})A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} \in (\mathbb{Z}_{12}(1 - \hat{e}))^{2\times 3}.$$

By applying this algorithm to $A' \in (\mathbb{Z}_{12}(1-\hat{e}))^{2\times 3}$, we get the primitive combination $0A'_{1\bullet} + (1 - \hat{e})A'_{2\bullet}$ over $\mathbb{Z}_{12}(1 - \hat{e})$ and, hence, the algorithm terminates with the primitive combination

$$\hat{e}A_{1\bullet} + (1 - \hat{e})A_{2\bullet} = (3, 7, 3) \in \mathbb{Z}_{12}^3.$$

Clearly $7 \in \mathbb{Z}_{12}^*$ and $7^{-1} = 7 \in \mathbb{Z}_{12}^*$ and, thus, this is the point $(9 : 1 : 9) = P_{12,14}$, which is the same result as in the above composition table.

4.4 The Non-Commutative Case

We have seen in the commutative case that being able to reduce rings leads to a method to reduce the groups of points of elliptic curves over these rings. Therefore, it would be good that such reductions are not possible. But a commutative ring with no non-trivial ideals is a field, so we will not get anything new in contrast to the Theory of Elliptic Curves over Fields.

The situation is different if one does not require the rings to be commutative. We first want to describe all finite non-commutative rings that are simple in the sense that they have no non-trivial ideals. For this section with *ring* we mean a not necessarily commutative ring that has a unit.

Definition 4.4.1.

(a) *A ring R is a* division ring *if every non-zero element has a multiplicative inverse.*

(b) *A ring R whose only two-sided ideals are R and 0 is called* simple. *This is equivalent to saying that 0 is a maximal ideal.*

(c) *A ring R is* Artinian *if both descending chains of left-ideals and descending chains of right-ideals stabilize.*

Theorem 4.4.2 (Wedderburn). *[SS88, II, p. 76, Satz 55.9] A finite division ring is commutative.*

Theorem 4.4.3 (Artin-Wedderburn). *[Jac68, p. 39, ch. III, Theorem 1] An Artinian ring R is simple if, and only if, $R \cong K^{n\times n}$ for an integer $n \in \mathbb{N}_{>0}$ and a division ring K.*

Corollary 4.4.4. *A finite ring R is simple if, and only if, $R \cong \mathbb{F}_q^{n \times n}$ for some prime power q and some integer $n \in \mathbb{N}_{>0}$.*

As $\mathbb{F}_q^{n \times n}$ is commutative if and only if $n = 1$, the smallest example for a non-commutative simple ring is $R := \mathbb{F}_2^{2 \times 2}$, which has 16 elements.

In the following we want to consider if it makes sense to consider elliptic curves over such rings, and in particular over this example $R = \mathbb{F}_2^{2 \times 2}$. But when trying to consider elliptic curves over non-commutative rings, we are faced with several problems:

- The reason to use elliptic curves C over fields $\mathbb{F}$ is that there is a natural bijection $\mathrm{Pic}^0(C/\mathbb{F}) \overset{\cong}{\to} C(\mathbb{F})$. If one wants to work over non-commutative rings (even division rings), one first has to define what a curve over such rings is, and find a family of curves, a (natural) group attached to each of these curves, and a (natural) bijection between this group and the rational points over this ring. This involves a deep understanding of algebraic geometry and will not be done in this thesis.

- A simpler approach would be to try to take the definitions from commutative rings over to non-commutative rings. But this is problematic for several reasons, the most important one being the following:

  How to define a ring of polynomials over a non-commutative ring? If, for example, x and y are indeterminates over a ring R, and one assumes that $xy = yx$, then the insertion map $R[x, y] \to R$, $x \mapsto a$, $y \mapsto b$ for an arbitrary tuple $(a, b) \in R^2$ is not well-defined in the cases $ab \neq ba$. But if $xy \neq yx$, then monomials like xyx cannot be simplified, which is an awkward situation.

  Note that with $R[x, y]$ we mean the non-commutative algebra generated by the indeterminates x and y; in the case that R is commutative, this does *not* correspond to the usual meaning of $R[x, y]$ in (almost) all other parts of this thesis! (The only exception is Definition 2.1.37 (a).)

- Moreover, a polynomial $axbxc$ with $a, b, c \in R$ can also not be simplified to $abcx^2$. If one assumes that a, b, c are in the center of R, i. e. they commute with any other element in R, one could try to define $ax = xa$, $bx = xb$ and $cx = xc$ and so on, but what if one extends the ring to a larger ring S in which a, b, c are no longer in the center? In this case, the natural inclusion $R[x] \hookrightarrow S[x]$ is not a ring morphism!

  One way to circumvent this problem in order to get a functorial behavior is to use coefficients that come from the natural map $\mathbb{Z} \to R$.

For the rest of this section we want to examine the idea of using an elliptic curve defined over $\mathbb{Z}_2$ with the usual addition formulae, but where the points have coordinates in the non-commutative simple ring $R = \mathbb{F}_2^{2 \times 2}$. We denote the center of R by

$$C(R) := \{x \in R \mid xa = ax \text{ for all } a \in R\}.$$

Lemma 4.4.5. *We have $C(R^{n \times n}) = R1_{R^{n \times n}} = \{r1_{R^{n \times n}} \mid r \in R\}$ for any ring R.*

Proof. Clearly $R1_{R^{n\times n}} \subseteq C(R^{n\times n})$. Let $(a_{ij})_{ij}, (b_{ij})_{ij} \in R^{n\times n}$. If one writes down the equations for $(a_{ij})_{ij}(b_{ij})_{ij} = (b_{ij})_{ij}(a_{ij})_{ij}$, one can quickly see that this is only valid for a fixed $(a_{ij})_{ij}$ and any $(b_{ij})_{ij}$, if $a_{ij} = 0$ is satisfied for any pair (i, j) with $i \neq j$. Now, if $a_{kk} \neq a_{\ell\ell}$, we see that if $b_{ij} = 0$ for all i, j except $b_{k\ell} = 1$, we get $(a_{ij})_{ij}(b_{ij})_{ij} \neq (b_{ij})_{ij}(a_{ij})_{ij}$. □

Next we must define what we mean by points of an elliptic curve over a ring. If one defines the projective plane over a non-commutative ring the same way as over a commutative ring, one has several problems:

- What does primitive mean? If one takes the same definition as for commutative rings, i. e. the elements generate the ring as an ideal, one first has to decide whether as a left, right or two-sided ideal. If one considers two-sided ideals, since R is simple, any triple $(x, y, z) \in R^3$, where x, y, z are not all zero, would be primitive. We postpone this question until later.

- Which elements are identified? One could define $(a_i)_i \sim (b_i)_i$ if, and only if, there are $\lambda, \mu \in R^*$ such that $\lambda a_i \mu = b_i$ for all i. Alternatively, one could restrict oneself to multiplying only from the left or only from the right side. The problem with this is that, in general, in none of these cases $\sim$ is transitive. One might want to consider a subgroup of R^* which lies in the center of R, or in the image of $\mathbb{Z}$ in R.

  Another reason why this question is problematic is that if $(a_i)_i \sim (b_i)_i$, then $f(a)$ should vanish if, and only if, $f(b)$ vanishes for a homogenous polynomial f. As above, if the coefficients of the polynomial commute with any element of a ring extension, in general most $\lambda \in R^*$ do *not* commute with any element of R.

  Therefore, it seems to be good decision to restrict to elements of $C(R)^* := R^* \cap C(R)$. In this case it also does not matter if one multiplies from the left or from the right. In our case ($R = \mathbb{F}_2^{2\times 2}$), we have $C(R)^* = \{1_R\}$, i. e. $(a_i)_i \sim (b_i)_i$ if, and only if, $(a_i)_i = (b_i)_i$.

We consider the curve

$$y^2 z + \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) xyz + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) yz^2 = x^3 + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) x^2 z + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) xz^2 + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) z^3$$

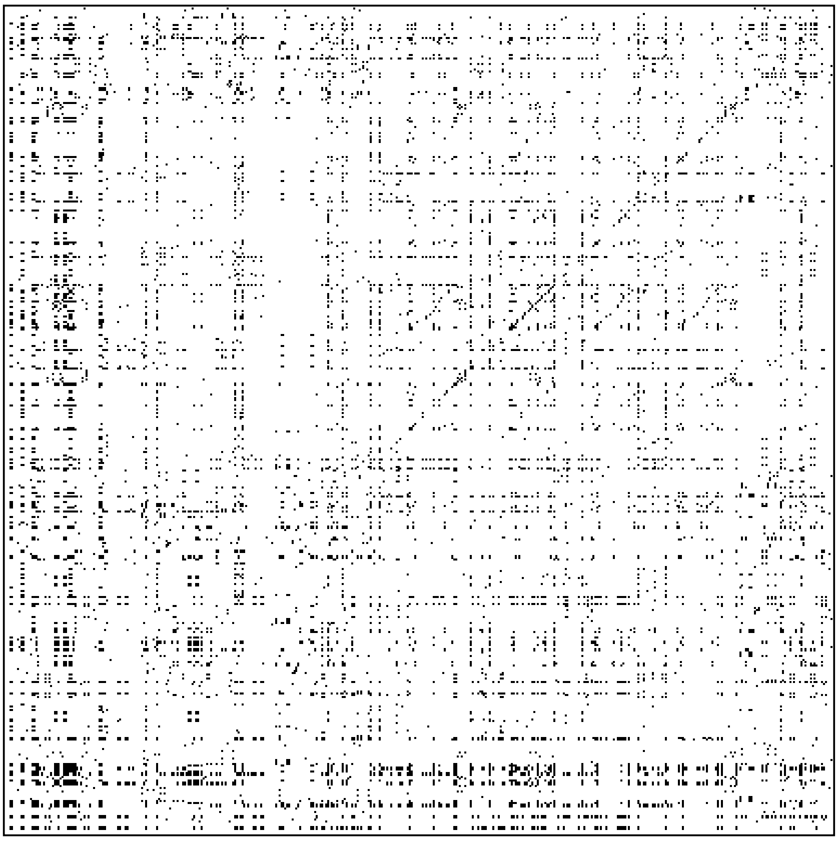
over $\mathbb{F}_2^{2\times 2}$. A quick computer search finds 447 points, where we ad-hoc define points as triples $(a_0, a_1, a_2) \in \mathbb{F}_2^{2\times 2} \setminus \{(0, 0, 0)\}$, where two of them are identified if they are equal. (Note that this is the same curve as in Section 4.3.5.)

It turns out that for 9600 pairs of such points, the addition formulae work in the sense that

- both produce a point on the curve (tested by plugging into the curve equation); and

- if both formulae give non-zero results, the results are the same.

The working pairs are shown as black dots in the following image, where the origin is in the lower left corner:



(Note that the black border is not part of the pairs of points.)

Finding a subset of the points with the property that

(a) for every two points in the set the addition is defined;

(b) the result lies in the subset; and

(c) the cardinality of this subset is maximal

is a hard problem that is easily seen to be $\mathcal{NP}$ complete (the Clique problem can be reduced to this problem; for information about Clique see for example [HMU01, p. 462, Exercise 10.4.1]). Finding large such sets is not feasible, especially if one uses curves over large simple rings with many points. It is also important that if one chooses a subset of the set of points, the coordinates of the points of this subset do not lie in a proper subring of R, which would be either $\mathbb{F}_q$ (in this case we are in the case of usual elliptic curves over fields) or a non-simple ring (which is not what we want).

For these reasons I conclude that one should study some non-commutative geometry before continuing in the direction of groups of points of curves over non-commutative finite rings.

Before closing this section we want to note that there are three embeddings of the usual group of points over $\mathbb{F}_q$ into the group of points over $\mathbb{F}_q^{2\times 2}$, which are correspond to the embeddings $\mathbb{F}_q \hookrightarrow \mathbb{F}_q^{2\times 2}$ given by $1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $1 \mapsto \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. By Lagrange's Theorem this implies that, not depending on how exactly $\mathbb{P}^2(\mathbb{F}_q^{n\times n})$ is defined, it is always possible to find subgroups in the group of points that correspond to the group of points of an elliptic curve over a field.

Chapter 5

Applications in Factoring and Cryptography

5.1 Factoring

The first use of elliptic curves over rings was to factor large integers $n \in \mathbb{N}$: H. W. Lenstra took the idea of Pollard's $(p-1)$-Method and replaced the multiplicative group $\mathbb{Z}_p^*$, p being a factor of n, with the group of points of an elliptic curve over $\mathbb{Z}_p$. The reason is that for an elliptic curve over $\mathbb{Z}_p$, the order of the group varies around $p+1$ and is not fixed as for $\mathbb{Z}_p^*$, where it is always $p-1$. We will describe both the Pollard $(p-1)$-Method and Lenstra's Elliptic Curve Method in Section 5.1.2.

In fact, Lenstra's method can be described without knowing what an elliptic curve over a ring is. But it turns out that there is a close connection between factoring an integer n and counting points of an elliptic curve over $\mathbb{Z}_n$. We will treat this in Section 5.1.3. Moreover, the Elliptic Curve Method by Lenstra can be generalized and used to decompose Artinian rings into local Artinian rings; we will present this generalization and a runtime analysis in Section 5.1.4. Finally, we show that this can be used to solve another problem, namely, computing a primary decomposition of a zero-dimensional ideal in $\mathbb{F}_q[x_1, \ldots, x_n]$. This will be investigated in Section 5.1.5.

5.1.1 Smooth Numbers

Before we start with factoring integers, we want to introduce a concept from Number Theory. This concept is the notion of an integer being smooth. Informally this should express that it only has small prime factors. It is clear that such numbers are relatively easy to factor, for example, by trial division. We will need results on smooth numbers during the process of analyzing the running time of the ring decomposition algorithm, and we need information on how they are distributed through the set of natural numbers. Unfortunately, we will use two conjectures about the distribution of smooth numbers in the runtime analysis. One is by H. W. Lenstra and is, in fact, based on a theorem by Norton, Canfield, Erdős and Pomerance, which we cite below. Before that we have to give the exact definition of an integer being smooth:

Definition 5.1.1. *Let $B > 0$ be a positive integer. Then another integer $n > 0$ is called* B-smooth *if every prime factor of n is less or equal than B.*

Theorem 5.1.2 (Norton, Canfield, Erdős, Pomerance). *[Coh96, p. 473, Theorem 10.2.1] Let $\psi(x, y) := |\{n \leq x \mid n \in \mathbb{N},\ n \text{ is } y\text{-smooth}\}|$. Then, if we set $u = \frac{\log x}{\log y}$, we have*

$$\psi(x, y) = xu^{-u(1+o(1))}$$

uniformly for $x \to \infty$ if $(\log x)^{\varepsilon} < u < (\log x)^{1-\varepsilon}$ for a fixed $\varepsilon \in \,]0, 1[$.

In particular, if we set $L(x) = e^{\sqrt{\log x \cdot \log \log x}}$, then

$$\psi(x, L(x)^a) = xL(x)^{-1/(2a)+o(1)}.$$

5.1.2 Factoring Integers

Factoring integers is a very old problem, and also a hard one. It is simple to find an algorithm that solves this problem, namely trial division, but it is too slow for large numbers. In the past there have been many proposals for faster factoring algorithms, for example Pollard's $(p-1)$-Method, Lenstra's Elliptic Curve Method, and the Generalized Number Field Sieve.

In this section we want to present Lenstra's Elliptic Curve Method. The main references for this subsection are [Len86] and [Len87]. Since Lenstra's method is a generalization of Pollard's $(p-1)$-Method, we first want to explain Pollard's method.

The Pollard $(p-1)$-Method (See for example [Len86, p. 103f], [MvOV96, pp. 92–93, Section 3.2.3] or [Ros05].)

Let $n > 1$ be a composite integer.

(a) Pick an $a \in \mathbb{Z}_n^*$.

(b) Select an integer $k > 0$, which is divisible by many small prime powers.

(c) Evaluate $a_k = a^k \mod n$.

(d) Compute $\gcd(a_k - 1, n)$.

(e) If the computation gives no factor, repeat the algorithm.

But how to choose k? Lenstra gives $k = \operatorname{lcm}\{1, \dots, w\}$ for a suitable bound w as an example [Len86, p. 103]. Another method would be to fix a bound $B > 0$, to take the set $\mathcal{P}_B$ of primes less or equal than B, and to define

$$k = \prod_{p \in \mathcal{P}_B} p^{\left\lfloor \frac{\log n}{\log p} \right\rfloor},$$

as suggested in [MvOV96, p. 92] and [Ros05].

To see why this method works, assume p is a prime factor of n such that $p - 1$ divides k, but p does not divide a (i.e. $a \in \mathbb{Z}_p^*$). Then $a^k \equiv 1 \pmod{p}$ since $\left|\mathbb{Z}_p^*\right| = p - 1$; therefore, p divides $\gcd(a^k - 1, n)$. If now n does not divides $\gcd(a^k - 1, n)$, we have found a factor. If there is another prime factor q of n such that $q - 1$ does not divide k, then $a^k \not\equiv 1 \pmod{q}$ and, hence, q does not divide $a^k - 1$. Therefore with a high probability, this gives a factor. If k is chosen as suggested in [MvOV96] and [Ros05], then $p-1$ divides k if, and only if, it is B-smooth.

Another way to understand this method is by the Chinese Remainder Theorem. We have

$$\mathbb{Z}_n^* = \prod_{i=1}^{\ell} \mathbb{Z}_{p_i^{e_i}}^*, \qquad \text{where } n = \prod_{i=1}^{\ell} p_i^{e_i} \text{ with distinct primes } p_i.$$

Now assume $p_i - 1$ is k-smooth for some i; then $a^k \mod p_i^{e_i}$ lies in the kernel of the reduction map $\mathbb{Z}_{p_i^{e_i}}^* \to \mathbb{Z}_{p_i}^*$ and, therefore, $a^k - 1$ is divisible by p_i. Now assume $p_j - 1$ is not k-smooth for some j; then $a^k \mod p_j^{e_j}$ does not lie in the kernel of the reduction map $\mathbb{Z}_{p_j^{e_j}}^* \to \mathbb{Z}_{p_j}^*$ and, therefore, $a^k - 1$ is not divisible by p_j. If there is such a pair (i, j), we hence have that

$$\gcd(a^k - 1, n) = \prod_{m=1}^{\ell} \gcd(a^k - 1, p_m^{e_m})$$

is divisible by p_i and not by p_j. Therefore $1 < \gcd(a^k - 1, n) < n$ and, thus, $\gcd(a^k - 1, n)$ is a non-trivial factor of n.

Unfortunately, this method relies on the fact that $p - 1$ has no large prime factors for one prime factor p of n. And even more unfortunately, the chances of this happening for a random p is rather low according to [Ros05], as one can deduce from Theorem 5.1.2.

Lenstra's Elliptic Curve Method Let $n \in \mathbb{N}$ be a composite integer, and let

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

be the factorization of n, where $p_1, \dots, p_k$ are distinct primes greater than 3, and $e_1, \dots, e_k$ are positive integers.

Restricting to primes $p > 3$ is not a problem, since the prime factors 2 and 3 can be found very easily by trial division. In fact, one could also allow prime factors of 2 or 3, but in this case one has to use a more general form for the elliptic curve.

Choose a random pair $(a, b) \in \mathbb{Z}_n$. If $E = E_c$ with $c = (0, 0, 0, a, b)$ defines an elliptic curve over $\mathbb{Z}_n$, we already know that

$$E_c(\mathbb{Z}_n) = \prod_{i=1}^{k} E_c(\mathbb{Z}_{p_i^{e_i}})$$

and

$$|E_c(\mathbb{Z}_n)| = \prod_{i=1}^{k} \left| E_{c \mod p_i^{e_i}}(\mathbb{Z}_{p_i^{e_i}}) \right| = \prod_{i=1}^{k} p_i^{e_i - 1} \, |E_{c \mod p_i}(\mathbb{Z}_{p_i})|$$

by Proposition 4.3.10 and Corollary 4.3.14. If we have chosen a pair (a, b) that does not define an elliptic curve, the discriminant is either 0 in $\mathbb{Z}_n$ or a non-zero non-unit, and hence gives a factor of n.

Next, one randomly picks a point $(\alpha : \beta : 1) \in E(\mathbb{Z}_n)$. (One could also randomly choose a, α, β and then choose b such that $P \in E_{(0,0,0,a,b)}(\mathbb{Z}_n)$, and then check whether $\Delta_{(0,0,0,a,b)} \in \mathbb{Z}_n^*$. Since computing square roots in $\mathbb{Z}_n$ is a hard problem, this is the preferred way to pick E_a and P.)

Now let $\varphi_i : E_c(\mathbb{Z}_n) \to E_{c \bmod p_i}(\mathbb{Z}_{p_i})$ be the canonical reductions of the elliptic curve, and let $P_i := \varphi_i(P)$ and $\ell_i := \operatorname{ord}_{E_c(\mathbb{Z}_{p_i})} P_i$. Assume that ℓ_i is B-smooth for some bound $B > 0$, and ℓ_j is not B-smooth. If

$$k = \prod_{p \in \mathcal{P}_B} p^{\left\lfloor \frac{\log n}{\log p} \right\rfloor}, \qquad \text{where } \mathcal{P}_B = \{p \mid p \text{ prime}, p \leq B\};$$

then $kP_i = \infty$ while $kP_j \neq \infty$. Thus, if $kP = (x : y : z) \in \mathbb{P}^2(\mathbb{Z}_n)$, then $z \not\equiv 0 \pmod{p_j}$ while $z \equiv 0 \pmod{p_i}$, i. e. $\gcd(n, z)$ gives a factor of n since it is divisible by p_i but not by p_j.

Note that while computing kP in $E_c(\mathbb{Z}_n)$, one can use inhomogenous coordinates and treat $\mathbb{Z}_n$ as a field, until at one point one wants to divide by a non-unit. If B and k are chosen as above, this will happen since at this point the result of the addition in the curve over $\mathbb{Z}_{p_i}$ is ∞, while the result of the addition in the curve over $\mathbb{Z}_{p_j}$ is not ∞.

One possible way to speed this up is to compute kP iteratively, by evaluating the product for k iteratively.

The algorithm now does these computations for several pairs (E_c, P). Since the ℓ_i vary in the interval $[p_i + 1 - 2\sqrt{p_i}, p_i + 1 + 2\sqrt{p_i}]$, there is a chance that for one pair, one ℓ_i is B-smooth while another is not, and hence one gets a factor.

As this is a special case of the algorithm presented and discussed in Section 5.1.4, we do not analyze the running time here and simply state the result from [Len87], which uses a conjecture about the distribution of numbers which are B-smooth (see also Section 5.1.4). The result states that if p is the smallest prime factor of n, and h the number of tries, then a non-trivial factor of n can be found with probability at least $1 - e^{-h}$ in at most

$$\mathcal{O}\left(h \cdot e^{\sqrt{(2+o(1)) \cdot \log p \cdot \log \log p}} \cdot (\log n)^2\right)$$

expected bit operations.

5.1.3 Factoring Integers and Counting Points

As already mentioned there is a close connection between factoring an integer n and counting points of an elliptic curve over $\mathbb{Z}_n$. According to [MMV01] and [KK98], counting the points of an elliptic curve over $\mathbb{Z}_n$ is randomly polynomial time equivalent to factoring n.

Clearly, if the factorization of n is known, one can reduce with the Chinese Remainder Theorem and Corollary 4.3.14 to the case of counting points of an elliptic curve over a finite field, and we have deterministic polynomial time algorithms for counting points of curves over fields (see Section 4.2.9 for Schoof's algorithm). Since the number of prime factors of n is bounded by $\log_2 n$, counting points of a curve over $\mathbb{Z}_n$ can be done in deterministic polynomial time if the factorization of n is known.

For the converse we want to give the algorithm from [KK98, Proof of Theorem 1]. Given is a composite square-free integer n, and assume it is coprime to 6. The output is a non-trivial factor of n. Assume that we are given an oracle that computes $|E_a(\mathbb{Z}_n)|$ for an elliptic curve $E_a/\mathbb{Z}_n$.

(1) Choose S to be the largest prime less than $\lfloor \log n \rfloor$.

(2) Choose a random point $P = (x : y : 1) \in \mathbb{P}^2(\mathbb{Z}_n)$ and a random $a \in \mathbb{Z}_n$.

(3) Compute $b = y^2 - x^3 - ax \in \mathbb{Z}_n$, i. e. a b such that $P \in E_{(0,0,0,a,b)}(\mathbb{Z}_n)$.

(4) If $\Delta_{(0,0,0,a,b)} \notin \mathbb{Z}_n^*$, either a non-trivial factor is found or the discriminant is zero. In the second case continue with step (2).

(5) Compute $\left|E_{(0,0,0,a,b)}(\mathbb{Z}_n)\right|$.

(6) If S does not divide $\left|E_{(0,0,0,a,b)}(\mathbb{Z}_n)\right|$ or if S^2 divides $\left|E_{(0,0,0,a,b)}(\mathbb{Z}_n)\right|$, go to step (2).

(7) Let $m = \frac{\left|E_{(0,0,0,a,b)}(\mathbb{Z}_n)\right|}{S} \in \mathbb{Z}$.

(8) Try to compute mP. If `ComputePrimitiveCombination` has to do a recursion, or if the z-coordinate of the resulting point is neither zero nor coprime to n, a non-trivial factor is found.

(9) Go to step (2).

By [KK98, Proof of Theorem 1] the expected running time is $\mathcal{O}(\log^5 n)$. The result can be strengthened in the sense that if a multiple of $\left|E_{(0,0,0,a,b)}(\mathbb{Z}_n)\right|$ is known, then n can be factored in randomly polynomial time. For details see [KK98, Lemma 1].

Before we close this subsection we want to explain why this algorithm works. Assume $n = \prod_{i=1}^k p_i$ with primes p_i. Let $c = (0,0,0,a,b)$ and $P \in E_c(\mathbb{Z}_n)$. Now $|E_c(\mathbb{Z}_n)| = \prod_{i=1}^k |E_c(\mathbb{Z}_{p_i})|$ and, hence, if S is a prime dividing $|E_c(\mathbb{Z}_n)|$ only once, for exactly one i we have that S divides $|E_c(\mathbb{Z}_{p_i})|$. Thus, for all $j \neq i$ we have $\frac{|E_c(\mathbb{Z}_n)|}{S} P = \infty \in E_c(\mathbb{Z}_{p_j})$ but in $E_c(\mathbb{Z}_{p_i})$ it can happen that $\frac{|E_c(\mathbb{Z}_n)|}{S} P \neq \infty \in E_c(\mathbb{Z}_{p_i})$ and, therefore, we may find a factor. For an explanation why this second case can happen, and how good the chances are that step (7) is reached, we need results on how the number of points of a random elliptic curve over $\mathbb{Z}_p$ are distributed in the interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. This can be found, for example, in [Len87], and lower bounds can be found with some of the tools in the Sections 4.2.7 and 5.1.4.

5.1.4 Factoring Rings

Let R be a finite ring. By the structure theorem for Artinian rings, Corollary 2.2.20, we know that R can be written as a finite product of local Artinian rings. But we do not know yet an effective way how to compute this decomposition. In fact, since factoring an integer n is the same as decomposing the ring $\mathbb{Z}_n$, this problem is at least as hard as factoring integers.

We have seen in Section 2.4 that as soon as the algorithm `ComputePrimitiveCombination` does a recursion, it in fact decomposes the ring into two factors. (A numerical example of this can be found in Section 4.3.5.) Therefore, we can try to do arithmetic on random elliptic curves over R, as in Section 5.1.2, in the hope that this will lead to a factorization. It turns out that indeed this method works for arbitrary finite rings and, in fact, the same runtime estimate can be set up as in Section 5.1.2.

We have seen that factoring rings is equal to finding non-trivial idempotents in the ring (for example see Proposition 2.2.2). Therefore, our algorithm will have as input an arbitrary finite ring R and will output—if successful—a non-trivial idempotent $e \in R$.

If 2 or 3 is non-zero in R but not a unit, then, by the method from the algorithm `ComputePrimitiveCombination`, one can split R into two rings R_1 and R_2 such that 2 or 3, respectively, is nilpotent in one, and a unit in the other. Therefore, we can assume without loss of generality that in R we either have that 2 or 3 is a unit, or that it is nilpotent. In the case 2 or 3 is nilpotent, the characteristic of R is a power of 2 or 3, respectively. (The exact characteristic can then be found by consecutive squaring in at most $\log_2 |R|$ or $\log_3 |R|$ steps, respectively, but this result is not needed here.)

Selecting a Random Elliptic Curve Before describing the algorithm in detail, we want to inspect the process of randomly choosing an elliptic curve E_a/R and a point $(x : y : 1) = P \in E_a(R)$ more closely. By first choosing $a_1, \dots, a_4, x, y$ randomly and then computing a_6 such that $P \in E_a(R)$, the problem of finding one point on the curve is solved. (Note that in general, the problem of finding a point on an elliptic curve over a ring is hard.) In the case $6 \in R^*$ we can set $a_1 = a_2 = a_3 = 0$, and if $3 \in R^*$, we can set $a_1 = a_3 = 0$ without loss of generality (see Proposition 4.2.8). Next, one can compute $j(E_a)$ and Δ_a. If Δ_a is a non-unit, one either finds a non-trivial idempotent if Δ_a is not nilpotent or, for some rings such as $\mathbb{Z}_n$, one can still factor if Δ_a is a non-zero nilpotent element. Otherwise, one should choose another curve. If $\Delta_a \in R^*$ one can check whether $j(E_a) \in R^*$. In that case, one can try to transform the curve into one of the forms, as in Proposition 4.2.8 (c) and (e). This has the advantage that more coefficients are zero (which simplifies the addition formulae) or some coefficients are non-units, in which case one can again try to find factors. If $j(E_a)$ is a non-nilpotent non-unit one can again factor R; and if $j(E_a)$ is nilpotent, one can transform the curve into one of the forms as in Proposition 4.2.8 (b) and (d), with the same benefits as above.

Note that selecting random coefficients $a_1, \dots, a_4, a_6 \in \mathbb{F}_q$ whose discriminant is $\neq 0$ is roughly equivalent to choosing a random isomorphism class of elliptic curves over $\mathbb{F}_q$, since every curve E given by Weierstraß coefficients, is by Proposition 4.2.4 (1), isomorphic to exactly $\frac{(q-1)q^3}{|\operatorname{Aut} E|}$ other such curves, and the number of possibilities for $\operatorname{Aut}(E)$ is restricted by Proposition 4.2.57 to a number between 2 and 24 in the general case, or between 2 and 6 if $6 \in R^*$, and in most cases it is 2.

The Algorithm The algorithm works as follows: first one chooses an elliptic curve E_a/R and a point $P \in E_a(R)$ as described above. If the ring can be factored nothing more need be done. Otherwise, compute ℓP, where ℓ is a large integer that is the product of 'enough' small primes. (We will spend more detail on ℓ later.) Nothing more need be done if, during the computation of ℓP, the situation occurs that `ComputePrimitiveCombination` factors the ring. If ℓP can be computed without finding a non-trivial idempotent, one restarts the algorithm.

Assume that $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are distinct maximal ideals in R. Denote the natural maps $E_a(R) \to E_a(R/\mathfrak{m}_i)$ with φ_i, and define $P_i := \varphi_i(P)$ and $\ell_i := \operatorname{ord}_{E_a(R/\mathfrak{m}_i)} P_i$. If now ℓ_1 divides ℓ, but ℓ_2 does not, then $\ell P_1 = \infty \in E_a(R/\mathfrak{m}_1)$, while $\ell P_2 \neq$

$\infty \in E_a(R/\mathfrak{m}_2)$. If one looks at the projective coordinates of ℓP, we see that the z-coordinate lies in $\mathfrak{m}_1$ but not in $\mathfrak{m}_2$. But then the z-coordinate is a non-nilpotent non-unit in R, and therefore leads to a non-trivial idempotent. (Of course, if the x- or y-coordinate is in $\mathfrak{m}_1$ but not in $\mathfrak{m}_2$, or the other way around, we can also factor.)

Selection of ℓ Therefore, our aim is to choose ℓ such that the probability that the situation above happens is maximized. An example how to choose ℓ is to fix a "smoothness bound" $B \in \mathbb{N}$ as in Section 5.1.2, and then set

$$\ell = \prod_{p \in \mathcal{P}_B} p^{\left\lfloor \log_p\left(v+1+2\cdot\sqrt{v}\right)\right\rfloor}$$

where $\mathcal{P}_B = \{p \in \mathbb{N} \mid p \leq B,\ p \text{ prime}\}$ and $v \in \mathbb{Z}$ is an upper boundary for the smallest value of $|R/\mathfrak{m}|$, where $\mathfrak{m}$ is a maximal ideal of R. For example, one could choose $v = \sqrt{|R|}$. Since $\operatorname{ord} P_i$ divides $|E_a(R/\mathfrak{m}_i)|$ by Lagrange, and by Hasse's Theorem 4.2.43 we have $|E_a(R/\mathfrak{m}_i)| \leq |R/\mathfrak{m}_i| + 1 + 2\sqrt{|R/\mathfrak{m}_i|}$, this factor ℓ will annihilate every $P \in E_a(R/\mathfrak{m}_i)$ if, and only if, $|E_a(R/\mathfrak{m}_i)|$ is B-smooth. Since R is assumed not to be local, the smallest residue field $R/\mathfrak{m}$ can have at most $\sqrt{|R|}$ elements.

A Useful Notation In the remainder of this subsection we extensively make use of the fact that if $(a_1, \dots, a_4, x, y) \in R^6$ is given, there exists a unique $a_6 \in R$ such that with $a = (a_1, \dots, a_4, a_6)$ the point $P = (x : y : 1)$ satisfies the Weierstraß equation with the coefficient vector a. If given a tuple $(a_1, \dots, a_4, x, y) \in R^6$, we write $(a, P) = (a_1, \dots, a_4, x, y)$ when we mean that a and P should be chosen this way. If we speak of a valid tuple $(a_1, \dots, a_4, x, y)$, we mean that the discriminant associated with the Weierstraß equation is a unit.

Running Time Analysis Unfortunately, the proof by Lenstra in [Len87] has to be modified at several points, since it relies on the fact that for any maximal ideal $\mathfrak{m}$ of R, we have that $R/\mathfrak{m} \cong \mathbb{Z}_p$ for a prime p. Lenstra shows that there exists a universal effectively computable constant $c > 0$ such that for any ring R, the number of the valid tuples $(a_1, \dots, a_4, x, y) \in R$ as above, for which the algorithm finds a factor, is at least $|R|^6 \frac{c}{\log p} \cdot \frac{u-2}{2\lceil\sqrt{p}\rceil+1}$, where $p = \min\{|R/\mathfrak{m}| \mid \mathfrak{m} \text{ maximal ideal of } R\}$ is prime and

$$u = \left|\left\{ s \in \mathbb{Z} \;\middle|\; |s-(p+1)| \leq \sqrt{p},\ s \text{ is } B\text{-smooth} \right\}\right|.$$

This result is based on two other results:

(1) [Len87, p. 662, Proposition 1.16 (a)] There exists a universal effectively computable constant $c_1 > 0$ such that given a prime $p > 3$, and a set $S \subseteq \mathbb{Z}$ with $|s - p - 1| \leq \sqrt{p}$ for all $s \in S$, the number of valid tuples $(a_1, \dots, a_4, x, y) \in \mathbb{Z}_p^6$ as above, satisfying $|E_a(\mathbb{Z}_p)| \in S$, is at least $c_1(|S| - 2)\frac{p^{5/2}}{\log p}$.

(2) [Len87, p. 662, Proposition 1.16 (b)] There exists a universal effectively computable constant $c_2 > 0$ such that given two primes $p > 3$ and ℓ, the number of valid tuples $(a_1, \dots, a_4, x, y) \in \mathbb{Z}_p^6$ as above, satisfying that ℓ does not divide $|E_a(\mathbb{Z}_p)|$, is at least $c_2 p^3$.

For the case that $q = p^n$ is a power of an arbitrary prime p, there are examples for both (1) and (2) that show that one cannot change $\mathbb{Z}_p$ into $\mathbb{F}_q$ and p into q in the formulae, which would be required to generalize Lenstra's result for general finite rings:

(1) Let $q = 2^n$ and $S = \{s \in 2\mathbb{Z} + 1 \mid |s - (q + 1)| \leq \sqrt{q}\}$. By Theorem 4.2.46 all elliptic curves E over $\mathbb{F}_q$ satisfying $|E(\mathbb{F}_q)| \in S$ are supersingular.

(2) In the case $q = 2^n$ and $\ell = 2$, all elliptic curves E over $\mathbb{F}_q$ that satisfy that 2 does not divide $|E(\mathbb{F}_q)|$ are supersingular by Theorem 4.2.46.

In the case $q = 2^n$, by Theorem 4.2.52 the number of non-isomorphic supersingular curves over $\mathbb{F}_q$ are:

(a) if n is even, i. e. q is a square, there are 4 non-isomorphic supersingular curves; or

(b) if n is odd, i. e. q is not a square, there are 3 non-isomorphic supersingular curves (see [Sch87, p. 208, Table 1] for the value of $H(-8)$).

In any case, these numbers are neither growing with $|S|$ nor with q or $\log q$. But during the running time analysis, the set S is the set of integers in $[q + 1 - \sqrt{q}, q + 1 + \sqrt{q}]$ that are B-smooth for a large enough B, and for this set it turns out that a similar result can be stated. And the second problem turns out to only occur in such a drastic way if $p = \ell = 2$.

Lemma 5.1.3. *Let ℓ and p be primes, and $q = p^n$. Assume that not both p and ℓ are* 2.

Let S be the set of integers $s \in [q + 1 - \sqrt{q}, q + 1 + \sqrt{q}]$, such that p does not divide $t = q + 1 - s$ and ℓ does not divide s. Then

$$|S| \geq \begin{cases} (2\sqrt{q} - 1)\frac{p-2}{p} - 2 & \textit{if } p = \ell \neq 2, \\ (2\sqrt{q} - 1)\frac{p\ell - p - \ell + 1}{p\ell} - 3 & \textit{if } p \neq \ell. \end{cases}$$

In any case $|S| \geq \frac{2\sqrt{q}-10}{3}$.

Proof. Define $I := [q+1-\sqrt{q}, q+1+\sqrt{q}] \cap \mathbb{Z}$. Let $S_p := \{s \in I \mid p \text{ divides } q+1-s\}$ and $S_\ell := \{s \in I \mid \ell \text{ divides } s\}$. We are interested in the value

$$N = |I \setminus (S_p \cup S_\ell)| = |I| - |S_p \cup S_\ell| = |I| - |S_p| - |S_\ell| + |S_p \cap S_\ell| .$$

Clearly

$$\left\lfloor \tfrac{|I|}{p} \right\rfloor + 1 \geq |S_p| \qquad \text{and} \qquad \left\lfloor \tfrac{|I|}{\ell} \right\rfloor + 1 \geq |S_\ell| .$$

Moreover, $|I| = 2\left\lfloor \sqrt{q} \right\rfloor + 1 \geq 2(\sqrt{q} - 1) + 1 = 2\sqrt{q} - 1$. If $p = \ell$, then $S_p \cap S_\ell = \emptyset$, since $q + 1 \equiv 1 \pmod{p}$. Hence, we have

$$\begin{aligned} N &\geq |I| - \left(\left\lfloor \tfrac{|I|}{p} \right\rfloor + 1 \right) - \left(\left\lfloor \tfrac{|I|}{\ell} \right\rfloor + 1 \right) \\ &= |I| - \left\lfloor \tfrac{|I|}{p} \right\rfloor - \left\lfloor \tfrac{|I|}{\ell} \right\rfloor - 2 \\ &\geq |I| \left(1 - \tfrac{1}{p} - \tfrac{1}{\ell} \right) - 2 = |I| \left(1 - \tfrac{2}{p} \right) - 2. \end{aligned}$$

If $p \neq \ell$, then $s \in S_\ell$ if, and only if, $s \equiv 0 \pmod{\ell}$, and $s \in S_p$ if, and only if, $s \equiv 1 \pmod{p}$. Since ℓ and p are coprime, $s \in S_\ell \cap S_p$ if, and only if, $s \equiv \lambda \pmod{p\ell}$ for a $\lambda = \lambda(p, \ell) \in \mathbb{Z}$. Therefore $|S_p \cap S_\ell| \geq \left\lfloor \frac{|I|}{p\ell} \right\rfloor$ and we have

$$\begin{aligned} N &\geq |I| - \left(\left\lfloor \tfrac{|I|}{p} \right\rfloor + 1 \right) - \left(\left\lfloor \tfrac{|I|}{\ell} \right\rfloor + 1 \right) + \left\lfloor \tfrac{|I|}{p\ell} \right\rfloor \\ &= |I| - \left\lfloor \tfrac{|I|}{p} \right\rfloor - \left\lfloor \tfrac{|I|}{\ell} \right\rfloor + \left\lfloor \tfrac{|I|}{p\ell} \right\rfloor - 2 \\ &\geq |I| \left(1 - \tfrac{1}{p} - \tfrac{1}{\ell} + \tfrac{1}{p\ell} \right) - 3. \end{aligned}$$

For the last inequality, note that $1 - \frac{1}{p} - \frac{1}{\ell} + \frac{1}{p\ell}$ for distinct primes $p, \ell \geq 2$ takes the minimum for $\{p, \ell\} = \{2, 3\}$, and the minimum value is $1/3$. Moreover, $\frac{p-2}{p} \geq \frac{1}{3}$ for $p > 2$. □

Lemma 5.1.4. *There exists an effectively computable constant $c > 0$ such that the following holds:*

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, where p is prime. Let $S \subseteq \mathbb{Z}$ be a subset such that for every $s \in S$ we have that p does not divide $q + 1 - s$, and that $|q + 1 - s| \leq \sqrt{q}$. Denote with $N_{q,S}$ the number of pairs $(a, P) = (a_1, \ldots, a_4, x, y) \in \mathbb{F}_q^6$ with the property that $E_a/\mathbb{F}_q$ is an elliptic curve and $|E_a(\mathbb{F}_q)| \in S$. Then

$$N_{q,S} \geq c(|S| - 2) \frac{q^{11/2}}{\log q}.$$

Proof. We first inspect the number $N'_{q,S}$, which we define to be the number of non-isomorphic elliptic curves E over $\mathbb{F}_q$ such that $|E(\mathbb{F}_q)| \in S$. For this we are following [Len87, p. 657, Proof of Proposition 1.9 (b)]. Note that $N'_{q,S} = \sum_{s \in S} H((q + 1 - s)^2 - 4q)$ by Theorem 4.2.52. By applying Proposition 4.2.54 with $z = 4q$, we get a universal effectively computable constant $c' > 0$ and a $\Delta^* < 4$ such that $H(\Delta) \geq \frac{c'\sqrt{-\Delta}}{\log(4q)}$ for all $-4q \leq \Delta < 0$, $\Delta_0 \neq \Delta^*$ satisfying $\Delta \equiv 0 \pmod{4}$ or $\Delta \equiv 1 \pmod{4}$. Hence, if $((q + 1 - s)^2 - 4q)_0 \neq \Delta^*$, we have

$$H((q + 1 - s)^2 - 4q) \geq \frac{c'\sqrt{4q - (q + 1 - s)^2}}{\log(4q)}.$$

Now $\left|(q + 1 - s)^2 - 4q\right| \geq 3q$ for $s \in S$ since $(q + 1 - s)^2 \leq q$ and, thus, $H((q + 1 - s)^2 - 4q) \geq \frac{c'\sqrt{3q}}{\log(4q)}$ for $((q + 1 - s)^2 - 4q)_0 \neq \Delta^*$.

We next show that we have $\Delta(s)_0 = \Delta^*$ for at most two $s \in S$, where $\Delta(s) = q + 1 - s$. Assume $\Delta = t^2 - 4q$ with $t := q + 1 - s$ and $\Delta_0 = \Delta^*$ for an $s \in S$. Consider the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta^*}) \subseteq \mathbb{C}$ and its ring of algebraic integers A. By [Coh96, pp. 185f] A is a Dedekind ring and, therefore, every ideal can be written as a unique product of prime ideals [Coh96, p. 186, Theorem 4.6.14 (3)]. Consider the polynomial $x^2 - tx + q \in \mathbb{Z}[x]$. It clearly has its roots in K and, therefore, in A. Denote them by α and $\bar{\alpha}$ and note that they are complex conjugates as the coefficients of the polynomial are real. We have $\alpha + \bar{\alpha} = t$ and $\alpha\bar{\alpha} = q = p^n$. Now we have $\Delta \equiv t^2 \pmod{p}$, and since p does not divide t we get $\left(\frac{\Delta^*}{p}\right) = \left(\frac{\Delta}{p}\right) = 1$. Hence, by [Coh96, p. 224, Proposition 5.1.4 (3)] we have that $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ for two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in A. Therefore, we have $\langle \alpha \rangle = \mathfrak{p}_1^i \mathfrak{p}_2^j$ and $\langle \bar{\alpha} \rangle = \mathfrak{p}_1^{n-i} \mathfrak{p}_2^{n-j}$ for $i, j \in \{0, \ldots, n\}$. If $0 < i, j < n$, then $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ divides both the ideals $\langle \alpha \rangle$ and $\langle \bar{\alpha} \rangle$, which implies that p divides α and α' and therefore also

$t = \alpha + \alpha'$, which is a contradiction. Therefore, at least one of i and j is in $\{0, n\}$. Now $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are also complex conjugates as one can see in the representation in [Coh96, p. 224, Proposition 5.1.4 (3)] and, thus,

$$\mathfrak{p}_1^i \mathfrak{p}_2^j = \langle \alpha \rangle = \overline{\langle \bar{\alpha} \rangle} = \overline{\mathfrak{p}_1^{n-i} \mathfrak{p}_2^{n-j}} = \mathfrak{p}_2^{n-i} \mathfrak{p}_1^{n-j},$$

and hence $i + j = n$. Therefore, $\{\langle \alpha \rangle, \langle \bar{\alpha} \rangle\} = \{\mathfrak{p}_1^n, \mathfrak{p}_2^n\}$. As $A^* = \{1, -1\}$ by [Coh96, p. 231, Proposition 5.3.1] and $t = \alpha + \bar{\alpha}$, we see that t is determined up to sign by $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ only depend on K and p, and K only depends on Δ^*, we can conclude that there are at most two exceptional $s \in S$. Therefore, we have shown

$$N'_{q,S} \geq \hat{c}(|S| - 2)\frac{\sqrt{q}}{\log q}$$

for some effectively computable constant $\hat{c} > 0$.

For the last part we follow [Len87, pp. 662f, Proof of Proposition 1.16 (a)]. By Proposition 4.2.4 (a) every elliptic curve given by a vector $(a_1, \ldots, a_4, a_6)$ is over $\mathbb{F}_q$ isomorphic to $\frac{(q-1)q^3}{|\mathrm{Aut}_{\mathbb{F}_q} E_{(a_1,\ldots,a_4,a_6)}|}$ such pairs. Recall that $\mathcal{E}_q$ denotes the set of isomorphism classes of elliptic curves over $\mathbb{F}_q$. Then we have (using Proposition 4.2.57)

$$\begin{aligned} N_{q,S} &= \sum_{\substack{[E] \in \mathcal{E}_q \\ |E(\mathbb{F}_q)| \in S}} \frac{(q-1)q^3(|E(\mathbb{F}_q)| - 1)}{|\mathrm{Aut}_{\mathbb{F}_q} E|} \\ &\geq (q - \sqrt{q})(q-1)q^3 \sum_{\substack{E \in \mathcal{E}_q \\ |E(\mathbb{F}_q)| \in S}} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q} E|} \\ &\geq (q - \sqrt{q})(q-1)q^3 \frac{1}{24} \sum_{\substack{E \in \mathcal{E}_q \\ |E(\mathbb{F}_q)| \in S}} 1 \\ &= (q - \sqrt{q})(q-1)q^3 \frac{1}{24} N'_{q,S} \\ &\geq \frac{\hat{c}}{24}(|S| - 2)\frac{(q - \sqrt{q})(q-1)q^{7/2}}{\log q}. \end{aligned}$$

Now $(q - \sqrt{q})(q - 1) \geq \tilde{c}q^2$ for some $\tilde{c} > 0$ and all $q \geq 2$ and, therefore, the claim follows. □

In the case of characteristic 2 we need a result to establish an upper boundary for the number of cases in which $p = \ell = 2$ occurs.

Lemma 5.1.5.

(a) *There are at most two elements in the interval* $[q + 1 - \sqrt{q}, q + 1 + \sqrt{q}]$ *that are a power of* 2.

(b) *Let* G *be a finite Abelian group whose order is not a power of two. Then at least* $\frac{1}{3}|G|$ *of the elements do not have an order that is a power of two.*

Proof.

(a) The number is at most

$$\begin{aligned} &\lfloor \log_2(q + 1 + \sqrt{q}) \rfloor - \lceil \log_2(q + 1 - \sqrt{q}) \rceil + 1 \\ \leq\ &\log_2(q + 1 + \sqrt{q}) - \log_2(q + 1 - \sqrt{q}) + 1 \\ =\ &\log_2\left(1 + \frac{2}{\sqrt{q} + 1/\sqrt{q} - 1}\right) + 1 < \log_2(4) + 1 = 3. \end{aligned}$$

The inequality $\frac{2}{\sqrt{q}+1/\sqrt{q}-1} < 3$ follows from an elementary discussion of the maxima of the function on the left.

(b) By the Structure Theorem for Abelian Groups and the Chinese Remainder Theorem for integers (Proposition 2.5.6) we can write $G = \mathbb{Z}_{p^n} \times G'$ for a prime $p > 2$, $n \in \mathbb{N}_{>0}$ and an Abelian group G'. Now all elements in $\mathbb{Z}_{p^n}$ have as an order a power of p, and only the identity has order one. Therefore, the elements of G whose order is not a power of two is at least $(p^n - 1)\,|G'|$. Now $|G'| = \frac{|G|}{p^n}$ and, hence, the number is at least $(1 - \frac{1}{p^n})\,|G|$. We can conclude since $\frac{1}{p^n}$ is maximal for $p^n = 3$. □

Corollary 5.1.6. *There exists an effectively computable constant $c > 0$ such that the following holds:*

Let R be any finite ring and v, B and ℓ be as above. Let N denote the number of tuples $(a, P) = (a_1, a_2, a_3, a_4, x, y) \in R^6$ such that E_a/R is an elliptic curve and the algorithm described above finds an idempotent element in one round with the given choices of E_a/R and $P \in E_a(R)$.

Let $\mathfrak{m}$ be a maximal ideal of R such that $R/\mathfrak{m}$ is minimal; thus, in particular $v \geq |R/\mathfrak{m}| = p^n$, where p is prime. Denote with u the cardinality of the set

$$\left\{ s \in \mathbb{Z} \,\middle|\, \begin{array}{c} |s - |R/\mathfrak{m}| - 1| \leq \sqrt{|R/\mathfrak{m}|}, \\ s \textit{ is } B\textit{-smooth}, \ p \nmid (s - |R/\mathfrak{m}| - 1) \end{array} \right\}.$$

Then

$$\frac{N}{|R|^6} \geq c \frac{u - 4}{(2\lfloor\sqrt{|R/\mathfrak{m}|}\rfloor + 1) \cdot \log |R/\mathfrak{m}|}.$$

Proof. Assume that E_a/R is such a curve, $P \in E_a(R)$, and $\mathfrak{m}'$ is another maximal ideal of R. Furthermore, assume that $|E_a(R/\mathfrak{m})|$ is B-smooth, but $|E_a(R/\mathfrak{m}')|$ is not divisible by the largest prime factor of $\operatorname{ord}_{E_a(R/\mathfrak{m})} P$. Then, the algorithm will find a non-trivial idempotent of R. (For this also see [Len87, p. 667, Proof of Proposition 2.6].)

We want to use this to find a lower boundary for N. Denote with T_s the set of tuples $(a, P) = (a_1, \ldots, a_4, x, y) \in (R/\mathfrak{m})^6$ such that $E_a/(R/\mathfrak{m})$ is an elliptic curve and $|E_a(R/\mathfrak{m})| = s$.

For every such a and P define $\ell_{a,P}$ to be the largest prime factor of $\operatorname{ord}_{E_a(R/\mathfrak{m})} P$, and define $U_{a,P}$ as the set of tuples $(a', P') = (a'_1, \ldots, a'_4, x', y') \in (R/\mathfrak{m}')^5$ such that $E_{a'}/(R/\mathfrak{m}')$ is an elliptic curve and $|E_{a'}(R/\mathfrak{m}')|$ is not divisible by $\ell_{a,P}$.

In the case that the characteristic of $R/\mathfrak{m}'$ is 2, exclude all tuples $(a, P) = (a_1, \ldots, a_4, x, y) \in T_s$ for whom $\ell_{a,P} = 2$.

Let $V_{a,P,a',P'}$ denote the set of all $(a''_1, \ldots, a''_4, x'', y'') \in R^6$, which by reduction modulo $\mathfrak{m}$ is equal to $(a_1, \ldots, a_4, x, y)$, and by reduction modulo $\mathfrak{m}'$ is equal to $(a'_1, \ldots, a'_4, x', y')$. Since R is finite and $\mathfrak{m}$ and $\mathfrak{m}'$ are distinct maximal ideals, the Chinese Remainder Theorem (Theorem 2.0.3) gives $\left|V_{a,P,a',P'}\right| = \frac{|R|^6}{(|R/\mathfrak{m}||R/\mathfrak{m}'|)^6}$. Moreover, let $\mathcal{S}_B$ be the set of B-smooth integers such that p does not divide $|R/\mathfrak{m}|+1-s$ for all $s \in \mathcal{S}_B$.

(Note that where we have a tuple $(a'', P'') = (a''_1, \ldots, a''_4, x'', y'')$ such that $\Delta_{a''}$ is not a unit in R, then it is also not nilpotent and, therefore, we found a factor. Hence, we can simply neglect this case.)

Then, by the remark at the beginning of the proof, we get the inequality

$$\begin{aligned} N &\geq \sum_{s\in\mathcal{S}_B} \sum_{(a,P)\in T_s} \sum_{(a',P')\in U_{a,P}} \left|V_{a,P,a',P'}\right| \\ &\geq \sum_{\substack{s\in\mathcal{S}_B \\ \overline{|s-|R/\mathfrak{m}|-1|\leq\sqrt{|R/\mathfrak{m}|}}}} \sum_{(a,P)\in T_s} |U_{a,P}| \frac{|R|^6}{(|R/\mathfrak{m}|\,|R/\mathfrak{m}'|)^6}. \end{aligned}$$

First, assume $|R/\mathfrak{m}'| \geq 68$. By Lemma 5.1.3 and Lemma 5.1.4 we get

$$|U_{a,P}| \geq c\left(\tfrac{2}{3}\sqrt{|R/\mathfrak{m}'|} - \tfrac{16}{3}\right)\frac{|R/\mathfrak{m}'|^{11/2}}{\log|R/\mathfrak{m}'|}$$

for the universal, effectively computable constant c in Lemma 5.1.4. Now $\frac{2}{3}\sqrt{|R/\mathfrak{m}'|} - \frac{16}{3} \geq \frac{1}{64}\sqrt{|R/\mathfrak{m}'|}$ if $|R/\mathfrak{m}'| \geq 68$. Hence, we get

$$|U_{a,P}| \geq \frac{c}{7}\frac{|R/\mathfrak{m}'|^6}{\log|R/\mathfrak{m}'|} \geq \frac{c}{7}\frac{1}{\log 2}\left|R/\mathfrak{m}'\right|^6.$$

If $|R/\mathfrak{m}'| \leq 67$, for every prime ℓ there is at least one elliptic curve E over $R/\mathfrak{m}'$ satisfying $\ell \nmid |E(R/\mathfrak{m}')|$ (this follows from Theorem 4.2.46 and Examples 4.2.47), and since these are finitely many cases there exists a universal, effectively computable constant $\hat{c} > 0$ such that

$$|U_{a,P}| \geq \hat{c}\left|R/\mathfrak{m}'\right|^6$$

for any residue field $R/\mathfrak{m}'$. Together we get

$$\begin{aligned} \frac{N}{|R|^6} &\geq \sum_{\substack{s\in\mathcal{S}_B \\ \overline{|s-|R/\mathfrak{m}|-1|\leq\sqrt{|R/\mathfrak{m}|}}}} \sum_{(a,P)\in T_s} \hat{c}\left|R/\mathfrak{m}'\right|^6 \frac{1}{(|R/\mathfrak{m}|\,|R/\mathfrak{m}'|)^6} \\ &= \sum_{\substack{s\in\mathcal{S}_B \\ \overline{|s-|R/\mathfrak{m}|-1|\leq\sqrt{|R/\mathfrak{m}|}}}} \sum_{(a,P)\in T_s} \frac{\hat{c}}{|R/\mathfrak{m}|^6} \\ &= \frac{\hat{c}}{|R/\mathfrak{m}|^6} \sum_{\substack{s\in\mathcal{S}_B \\ \overline{|s-|R/\mathfrak{m}|-1|\leq\sqrt{|R/\mathfrak{m}|}}}} |T_s|. \end{aligned}$$

First, assume that the characteristic of $R/\mathfrak{m}'$ is > 2. By Lemma 5.1.4 (note that $|T_s| = N_{q,\{s\}}$) we get

$$\frac{N}{|R|^6} \geq c\hat{c}\frac{1}{|R/\mathfrak{m}|^6}(u-2)\frac{|R/\mathfrak{m}|^{11/2}}{\log|R/\mathfrak{m}|} = c\hat{c}\frac{(u-2)}{\sqrt{|R/\mathfrak{m}|}\log|R/\mathfrak{m}|}.$$

Now assume that the characteristic of $R/\mathfrak{m}'$ is 2. By Lemma 5.1.5 (b) we see

$$\frac{N}{|R|^6} \geq \hat{c}\frac{1}{|R/\mathfrak{m}|^6} \sum_{\substack{s\in\mathcal{S}_B\setminus\{2^k|k\in\mathbb{N}\} \\ \overline{|s-|R/\mathfrak{m}|-1|\leq\sqrt{|R/\mathfrak{m}|}}}} \frac{1}{3}N_{q,\{s\}},$$

with $N_{q,\{s\}}$ as in Lemma 5.1.4 and, using the Lemmas 5.1.4 and 5.1.5 (a), we get

$$\frac{N}{|R|^6} \geq c\hat{c}\frac{1}{3\,|R/\mathfrak{m}|^6}(u-4)\frac{|R/\mathfrak{m}|^{11/2}}{\log|R/\mathfrak{m}|} = \frac{c\hat{c}}{3}\cdot\frac{u-4}{\sqrt{|R/\mathfrak{m}|}\log|R/\mathfrak{m}|}.$$

As a last step, note that

$$\frac{1}{\sqrt{|R/\mathfrak{m}|}} \geq \tilde{c}\frac{1}{2\left\lfloor\sqrt{|R/\mathfrak{m}|}\right\rfloor + 1}$$

for some universal constant $\tilde{c}$. By taking the constant c from the claim as the maximum of the constants for both the cases of the characteristic of $R/\mathfrak{m}'$, multiplied by $\tilde{c}$, we can conclude. □

Unfortunately, we now need a conjecture to reach the same estimate as in [Len87]:

Conjecture 5.1.7. *Let $q = p^n$ be a power of the prime p, where $n > 1$, and S be the set of all B-smooth integers in the interval $[q+1-\sqrt{q}, q+1+\sqrt{q}]$, where $B > 11$. Define*

$$S' = \{s \in S \mid p \textit{ does not divides } q+1-s\},$$

and assume $|S| > 1$. Then $|S'| \geq \frac{2}{5}|S|$.

Note that computer experiments have shown that for $q \leq 1\,000\,000$ this conjecture holds. In fact, it also holds for $B \leq 5$ and $q = p$ as soon as $|S| > 1$. The constant $\frac{2}{5}$ appears to be the lowest boundary for this conjecture to work; it is attained, for example, if $q = 4$ or $q = 8$. If $p > 2$ one can chose $\frac{1}{2}$ and, in general for larger p, the constant can be chosen much nearer to 1. This is why I believe the conjecture will hold with the stated assumptions.

We have collected enough to prove an analogon to Corollary 2.8 in [Len87, p. 669]:

Corollary 5.1.8. *There exists an effectively computable constant $c > 1$ with the following property.*

Let R be a finite ring which is not local, $\mathfrak{m}$ be a maximal ideal of R such that $|R/\mathfrak{m}|$ is minimal, and $v > 1$ be an integer such that $v \geq |R/\mathfrak{m}|$. Choose $B > 1$ such that

$$u := \left|\left\{s \in \mathbb{Z} \;\middle|\; |s - |R/\mathfrak{m}| - 1| \leq \sqrt{|R/\mathfrak{m}|},\ s \textit{ is } B\textit{-smooth}\right\}\right|$$

is at least 11. Let $f(B) = \frac{u}{2\left\lfloor\sqrt{|R/\mathfrak{m}|}\right\rfloor+1}$ denote the probability that a random integer in the interval

$$\left[|R/\mathfrak{m}| + 1 - \sqrt{|R/\mathfrak{m}|}, |R/\mathfrak{m}| + 1 + \sqrt{|R/\mathfrak{m}|}\right]$$

is B-smooth. Then for any $h > 1$ the success probability for the above algorithm, with h different choices for the curve and point, is at least

$$1 - c^{-h\frac{f(B)}{3\log v}}.$$

Proof. With Corollary 5.1.6 and Conjecture 5.1.7 we get (with N as in the Corollary)

$$\frac{N}{|R|^6} \geq c'\frac{\frac{2}{5}u - 4}{\left(2\left\lfloor\sqrt{|R/\mathfrak{m}|}\right\rfloor + 1\right) \cdot \log|R/\mathfrak{m}|} \geq c''\frac{f(B)}{\log v}$$

for effectively computable universal positive constants c'' and c', since $u - 10 \geq \frac{1}{11}u$. The failure probability for the algorithm with h choices for the curve and point is $(1 - N/|R|^6)^h$, and

$$\left(1 - \frac{N}{|R|^6}\right)^h \leq (e^{-N/|R|^6})^h = e^{-hN/|R|^6} \leq e^{-hc''\frac{f(B)}{\log v}},$$

such that with $c = e^{c''/3} > 1$ (since $c'' > 0$) we can conclude. □

Define

$$L : [e, \infty[\to \mathbb{R}, \qquad x \mapsto e^{\sqrt{\log x \cdot \log\log x}}.$$

Then, by Theorem 5.1.2, for any $x > e$ we have that the probability for a random positive integer $s \in [1, x]$ to be $L(x)^a$-smooth is $L(x)^{-1/(2a)+o(1)}$ for any positive $a \in \mathbb{R}$ and for $x \to \infty$. In the paper [Len87] Lenstra conjectures:

Conjecture 5.1.9 (Lenstra). *[Len87, p. 670] Let $a > 0$ be a real number. Then the probability that a random positive integer in the interval $]x + 1 - \sqrt{x}, x + 1 + \sqrt{x}[$ is $L(x)^a$-smooth is $L(x)^{-1/(2a)+o(1)}$ for $x \to \infty$.*

Assuming this conjecture, we can conclude the estimated running time for the algorithm as in [Len87, p. 670], where h different choices for curve and point are used. It turns out that optimal choices for B and h are

$$B = L(|R/\mathfrak{m}|)^{\frac{1}{\sqrt{2}}+o(1)} \qquad \text{and} \qquad h \sim \frac{B}{f(B)} = L(|R/\mathfrak{m}|)^{\sqrt{2}+o(1)}$$

for $|R/\mathfrak{m}| \to \infty$. Since $|R/\mathfrak{m}|$ is not known before, one can replace it with v and choose an increasing sequence of values for v. We get the following conjecture for the running time of this algorithm:

Conjecture 5.1.10. *(See [Len87, p. 670, Conjecture 2.10].) Assume that R is a finite ring that is not local. Let $\mathfrak{m}$ be a maximal ideal of R such that $|R/\mathfrak{m}|$ is minimal. Let h be any positive integer. Then the above algorithm, with h choices of a curve and point, and with suitable values for B, v and h (see above), returns a non-trivial idempotent with probability $1 - e^{-h}$ in time*

$$h \cdot K(|R/\mathfrak{m}|) \cdot M(|R|),$$

where

$$K(n) = e^{\sqrt{(2+o(1))\cdot \log n \cdot \log\log n}}$$

and $M(n)$ is the cost for one addition on the elliptic curve over a ring with n elements. In the case of $R = \mathbb{Z}_n$ with n coprime to 6, one can choose $M(n) = \mathcal{O}((\log n)^2)$.

Note that if $R = \mathbb{Z}_n$ where n is coprime to 6, we can also choose

$$M(n) = \mathcal{O}((\log n)(\log\log n)^2(\log\log\log n))$$

according to [Len87, p. 669, Paragraph 2.9].

Improvements There are several improvements possible for this algorithm. If one uses curves for which some information about the group structure is known, one can considerably speed up the algorithm. For example, A. O. L. Atkin and F. Morain consider in [AM93] a family of curves E such that $|E(\mathbb{F}_p)|$ is divisible by 16. A problem is that one might use a family of curves that are limited in some way, such that the algorithm might not work for some kind of rings. For the case where $R = \mathbb{Z}_n$, Atkin and Morain mention that their experiments [AM93, p. 403, Paragraph 3.6] have shown that their family of curves seems to work well in practice; they use a family of curves parameterized by D. S. Kubert.

There are also many improvements for Lenstra's original algorithm, like adding a second phase. Some improvements are described in [Mon87, Section 8 and 9]; references to other improvements can also be found in this paper. More information about selecting optimal parameters for the case $R = \mathbb{Z}_n$ can be found in [SW93].

An Unsuccessful Idea for Improving the Elliptic Curve Factorization Method for Integers In integer factoring one sometimes uses the ring of integers of number fields instead of $\mathbb{Z}$, for example, $\mathbb{Z}[\sqrt{p}]$ for some prime p. This motivates one to look at finite ring extensions of $\mathbb{Z}_n$, where n is an integer to be factored, for example, at $\mathbb{Z}_n[\sqrt{k}] = \mathbb{Z}_n[x]/\left\langle x^2 - k\right\rangle$ if k is not a square in any $\mathbb{Z}_p$, p a prime factor of n. Unfortunately, this is of no help for the Elliptic Curve Factorization Method. Assume $n = n_1 n_2$ with coprime integers n_1 and n_2. Then $\mathbb{Z}_n[\sqrt{k}] \cong \mathbb{Z}_{n_1}[\sqrt{k}] \times \mathbb{Z}_{n_2}[\sqrt{k}]$ by the Chinese Remainder Theorem, and $\mathbb{Z}_{p^n}[\sqrt{k}]$, p a prime and $n > 0$, is a local ring with residue field $\mathbb{Z}_p[\sqrt{k}] = \mathbb{Z}_p[x]/\left\langle x^2 - k\right\rangle$, since $x^2 - k$ is irreducible over $\mathbb{Z}_p$. Thus, in $\mathbb{Z}_{p^n}[\sqrt{k}]$ the ratio of nilpotents to ring elements is the same as in $\mathbb{Z}_p[\sqrt{k}]$, which is $\frac{1}{p^2}$, compared to $\frac{1}{p}$ in $\mathbb{Z}_p$. Hence, the ratio of elements that help factoring to ring elements is less in $\mathbb{Z}_n[\sqrt{k}]$ than in $\mathbb{Z}_n$. If one also considers that computations in $\mathbb{Z}_n[\sqrt{k}]$ are more expensive than in $\mathbb{Z}_n$, it is worthless to try to apply the factoring method to $\mathbb{Z}_n[\sqrt{k}]$ instead of $\mathbb{Z}_n$ itself. For other extensions of $\mathbb{Z}_n$ similar results can be shown.

5.1.5 Primary Decomposition

As an application of the algorithm in the last section, we want to show how it can be used to compute the primary decomposition of a zero-dimensional ideal over $\mathbb{F}_q$. First, we want to define what a primary decomposition is. See, for example, [Mat80, pp. 52–57] or [Eis95, pp. 94–113, Chapter 3] for more information on primary decomposition. In the following let R be a Noetherian ring and M a finitely generated R-module.

Definition 5.1.11. *Let N be a submodule of M.*

(a) *An R-module P is called* co-primary *if* $|\mathrm{Ass}_R(P)| = 1$.

(b) *We say N is a* primary *submodule (of M) if M/N is co-primary. If* $\mathrm{Ass}_R(M/N) = \{\mathfrak{p}\}$, *we say N is* $\mathfrak{p}$-primary.

(c) *A* primary decomposition *of N is an equation $N = \bigcap_{i=1}^k N_i$, where the N_i are primary submodules of M.*

(d) *A primary decomposition $N = \bigcap_{i=1}^k N_i$ is* irredundant *if $N \subsetneqq \bigcap_{\substack{i=1\\i\neq j}}^k N_i$ for every j, and if the associated primes of M/N_i are all distinct.*

We also need the following characterization for a module being co-primary and an ideal being primary:

Proposition 5.1.12. *[Mat80, pp. 52f, Proposition 8.B] The module M is co-primary if, and only if, all of the following conditions hold:*

(i) *we have that $M \neq 0$; and*

(ii) *if $x \in R$ is a zero-divisor on M, then for every $y \in M$ there exists an $n > 0$ such that $x^n y = 0$.*

[Mat80, p. 53, Remark] If $M = R$ and $N = \mathfrak{a}$ for some ideal $\mathfrak{a}$ in R, then N is primary if, and only if, all zero-divisors of $R/\mathfrak{a}$ are nilpotent.

The following proposition shows that every submodule N of M has a primary decomposition:

Proposition 5.1.13. *[Mat80, p. 56, Corollary and p. 54, Definition 8.D and Lemma 8.E] Every submodule N of M has an irredundant primary composition. If $N = \bigcap_{i=1}^k N_i$ is such a decomposition, then $\operatorname{Ass}_R(M/N)$ is the disjoint union of the $\operatorname{Ass}_R(M/N_i)$.*

From now on we consider the case $M = R = \mathbb{F}_q[x_1, \dots, x_n]$ and $N = \mathfrak{a}$.

Remark 5.1.14. According to [EHV92, pp. 86ff] one can reduce the problem of finding a primary decomposition of any ideal $\mathfrak{a}$ in $R = \mathbb{F}[x_1, \dots, x_n]$ to the case where $\dim R/\mathfrak{a} = 0$, i. e. to the case where $R/\mathfrak{a}$ is Artinian.

Therefore, it is enough to concentrate on the case where $R/\mathfrak{a}$ is Artinian. The next lemma and its corollary link the primary decomposition of $\mathfrak{a}$ with the decomposition of $R/\mathfrak{a}$ into local Artinian rings:

Lemma 5.1.15. *Let $R = \mathbb{F}[x_1, \dots, x_n]$ and $\mathfrak{a}$ be an ideal in R. Assume $R = \bigcap_{i=1}^k \mathfrak{b}_i$ is an irredundant primary decomposition of $\mathfrak{a}$.*

(a) *We have that $\sqrt{\mathfrak{b}_i}$ is prime for every i. In fact, $\operatorname{Ass}_R(R/\mathfrak{b}_i) = \sqrt{\mathfrak{b}_i}$. If $\dim R/\mathfrak{a} = 0$, then $\mathfrak{a}$ is primary if, and only if, $\sqrt{\mathfrak{a}}$ is prime.*

(b) *If $\dim R/\mathfrak{a} = 0$, we have that $R/\mathfrak{a} \cong \prod_{i=1}^n R/\mathfrak{b}_i$. The ring $R/\mathfrak{a}$ is Artinian and the $R/\mathfrak{b}_i$'s are local Artinian rings.*

(c) *Let $R/\mathfrak{a}$ be an Artinian ring and $R/\mathfrak{a} \cong \prod_{i=1}^m R_i$ be the decomposition into local Artinian rings, and let $\mathfrak{c}_i = \ker(R/\mathfrak{a} \to R_i)$. Then $\mathfrak{a} = \bigcap_{i=1}^m \mathfrak{c}_i$ is an irredundant primary decomposition of $\mathfrak{a}$.*

Proof.

(a) By the last statement in Proposition 5.1.12 we see that every zero-divisor of $R/\mathfrak{b}_i$ is nilpotent. Therefore, the only zero-divisor in $R/\sqrt{\mathfrak{b}_i} \cong (R/\mathfrak{b}_i)/(\sqrt{0}/\mathfrak{b}_i)$ is 0 and, hence, $\sqrt{\mathfrak{b}_i}$ is prime.

For the second statement note that $R/\mathfrak{b}_i$ has the minimal prime $\sqrt{\mathfrak{b}_i}/\mathfrak{b}_i$ and, therefore, $\sqrt{\mathfrak{b}_i} \in \operatorname{Ass}_R(R/\mathfrak{b}_i)$ by Proposition 2.3.37 (a).

The last statement follows from the first and the fact that if $\sqrt{\mathfrak{a}}$ is prime and $\dim R/\mathfrak{a} = 0$, then $R/\mathfrak{a}$ is a local Artinian ring; by Lemma 2.2.21 and the last statement of Proposition 5.1.12 we therefore get that $\mathfrak{a}$ is primary in this case.

(b) We have to show $\mathfrak{b}_i + \mathfrak{b}_j = R$ for $i \neq j$, then we can conclude with the Chinese Remainder Theorem (Theorem 2.0.3). This is equivalent to $\sqrt{\mathfrak{b}_i} + \sqrt{\mathfrak{b}_j} = R$, since if $a+b=1$ with $a^n \in \mathfrak{b}_i$, $b^n \in \mathfrak{b}_j$, we have $1=(a+b)^{2n}=\tilde{a}+\tilde{b}$ with $\tilde{a} \in \mathfrak{b}_i$ and $\tilde{b} \in \mathfrak{b}_j$.

As the primary decomposition is irredundant, the $\sqrt{\mathfrak{b}_i}$'s are pairwise distinct primes. And as $\dim R/\mathfrak{a}=0$, the $\sqrt{\mathfrak{b}_i}$'s are maximal ideals. But then, clearly, $\sqrt{\mathfrak{b}_i}+\sqrt{\mathfrak{b}_j}=R$ for $i \neq j$.

The last statement is clear by Remarks 2.3.22 (b), by the last statement of Proposition 5.1.12, and by Lemma 2.2.21.

(c) Clearly, the $\mathfrak{c}_i$'s are primary by Lemma 2.2.21 and the last statement of Proposition 5.1.12. Since $R/\mathfrak{a} \cong \prod_{i=1}^m R/\mathfrak{c}_i$ it follows that $\mathfrak{a}=\bigcap_{i=1}^m \mathfrak{c}_i$ is an irredundant primary decomposition. □

Corollary 5.1.16. *If $R/\mathfrak{a}$ is an Artinian ring, any irredundant primary decomposition of $\mathfrak{a}$ corresponds to the decomposition of $R/\mathfrak{a}$ into local Artinian rings.*

The next lemma shows how to use the algorithm for finding idempotents in Artinian rings from Section 5.1.4 to find a primary decomposition of a zero-dimensional ideal $\mathfrak{a} \subseteq \mathbb{F}[x_1,\ldots,x_n]$:

Lemma 5.1.17. *Let $e \in R$ be an element such that $e^2=e \in R/\mathfrak{a}$, and it is $e \neq 1 \in \mathfrak{a}$ and $e \neq 0 \in \mathfrak{a}$. Then*

$$\mathfrak{a}=(\mathfrak{a}+\langle e\rangle)\cap(\mathfrak{a}+\langle e-1\rangle) \quad \textit{and} \quad R/\mathfrak{a} \cong R/(\mathfrak{a}+\langle e\rangle)\times R/(\mathfrak{a}+\langle e-1\rangle).$$

Moreover, if $\mathfrak{a}+\langle e\rangle=\bigcap_{i=1}^{\ell}\mathfrak{c}_i$ and $\mathfrak{a}+\langle 1-e\rangle=\bigcap_{i=1}^{m}\mathfrak{d}_i$ are primary decompositions, then a primary decomposition of $\mathfrak{a}$ is given by $\mathfrak{a}=\bigcap_{i=1}^{\ell}\mathfrak{c}_i\cap\bigcap_{i=1}^{m}\mathfrak{d}_i$.

Proof. As $1=e-(e-1)$ we have $(\mathfrak{a}+\langle e\rangle)+(\mathfrak{a}+\langle e-1\rangle)=R$ and, therefore, the second statement follows from the first by the Chinese Remainder Theorem (Theorem 2.0.3). Clearly $\mathfrak{a} \subseteq (\mathfrak{a}+\langle e\rangle)\cap(\mathfrak{a}+\langle e-1\rangle)$. Let $f=a+(e-1)g \in \mathfrak{a}+\langle e\rangle$, where $a \in \mathfrak{a}$ and $g \in R$. Since $a+eg \in \mathfrak{a}+\langle e\rangle$, we get $g \in \mathfrak{a}+\langle e\rangle$ and, therefore, can write $g=a'+eh$, where $a' \in \mathfrak{a}$ and $h \in R$. But then $f=(a+(1-e)a')+(e^2-e)h \in \mathfrak{a}$, since $e^2-e \in \mathfrak{a}$ by assumption. The last statement follows from the previous corollary. □

Note that one could also prove this lemma by using Lemma 5.1.15 and Proposition 2.2.2.

This directly leads to a recursive algorithm:

(1) Input is a zero-dimensional ideal $\mathfrak{a}$ in a ring $\mathbb{F}[x_1,\ldots,x_n]$ over a field $\mathbb{F}$.

(2) Find a non-trivial idempotent $e \in R/\mathfrak{a}$.

   (a) If no non-trivial idempotent could be found, return $\mathfrak{a}$ (which is primary in this case).

   (b) Compute primary decompositions $\mathfrak{a}+\langle e\rangle=\bigcap_i \mathfrak{c}_i$ and $\mathfrak{a}+\langle 1-e\rangle=\bigcap_j \mathfrak{d}_j$ by applying this algorithm recursively, and then return $\bigcap_i \mathfrak{c}_i \cap \bigcap_j \mathfrak{d}_j$.

Note that $\mathbb{F}$ should be a finite field. Otherwise, the algorithm from Section 5.1.4 for finding non-trivial idempotents is not usable.

There are two drawbacks:

(a) Note that detecting the case where $\mathfrak{a}$ is primary is hard, since the algorithm from Section 5.1.4 cannot prove that there are no non-trivial idempotents.

(b) For computations in $R/\mathfrak{a}$ a Gröbner basis of $\mathfrak{a}$ has to be computed, which is cost intensive. Fortunately, if one wants to compute a Gröbner basis for $\mathfrak{a} + \langle e \rangle$, one already has a Gröbner basis for $\mathfrak{a}$, which simplifies the computation.

An idea would be to give up finding a non-trivial idempotent after some time, and then either apply another algorithm for primary decomposition in the hope it produces better results (see for example [EHV92] and [Vas98, Chapters 3 and 4]), or to simply treat $\mathfrak{a}$ as a primary ideal and to warn the user that this might be wrong.

For implementation it might be useful not to do this recursively, but using four lists: `todo`, `done` and `hard` and `failed`. At startup all are empty, except `todo` which only contains $\mathfrak{a}$. Then in every iteration step, one ideal $\mathfrak{b}$ is removed from `todo` and one tries to find non-trivial idempotents e in $R/\mathfrak{b}$. If this fails after a given time, the ideal is put onto the `hard` list; otherwise the ideals $\mathfrak{b} + \langle e \rangle$ and $\mathfrak{b} + \langle 1 - e \rangle$ are put on the `todo` list. When the `todo` list is empty but the `hard` list is not, take the first ideal from the `hard` list. Either by applying another algorithm or applying the idempotent-finding algorithm for a longer time, one tries to split this. If the outcome is that $\mathfrak{b}$ is primary, it can be put onto the `done`; if $\mathfrak{b}$ can be split, put the factors onto the `todo` or `done` list, depending on whether they are known to be primary; otherwise put $\mathfrak{b}$ onto the `failed` list.

At the end the `done` list contains the successfully found primary ideals of a primary decomposition, and the `failed` list all ideals which may not be primary yet. In any case, the ideal $\mathfrak{a}$ is the intersection of all ideals in the `done` and `failed` lists, and if a primary decomposition of all ideals in `failed` is known, a primary decomposition of $\mathfrak{a}$ is given by the intersection of all ideals in `done` and the primary ideals from the decompositions of the ideals on the `failed` list.

We want to close this section with two remarks:

Remarks 5.1.18.

(a) It might be possible to generalize a primality test for integers using elliptic curves to a test for an ideal being primary or prime. Such a test, combined with the above algorithm, would result in a much more complete algorithm, which only has to rely on other algorithms when both the idempotent finding and the primary/prime checking algorithm do not give any results after several tries.

(b) The algorithm relies on the fact that it is fast to check whether an $x \in R = \mathbb{F}[x_1, \dots, x_n]/\mathfrak{a}$ is invertible or not, and that it is fast to find a solution to an equation $ax = b$ for which one knows one solution exists. (See the description of the algorithm `ComputePrimitiveCombination` on page 49.)

This can be done, for example, by the methods explained in Section 2.5.2, which are slow if $\dim_{\mathbb{F}} R$ is large. But for small $\dim_{\mathbb{F}} R$ there are other fast algorithms for primary decomposition (for example, see [Mon02]).

5.2 Cryptography

Cryptography is the area in cryptology where ciphers are designed; ciphers are algorithms which transform an input message, the *plaintext*, into an output message, the *ciphertext*, which can only be transformed back to the plaintext with the knowledge of a secret key. One of the very interesting areas of cryptography is the field of public key cryptography, which is relatively young. The first work in this area was done around 1976 by W. Diffie and M. Hellman; we will describe some of their ideas and of others in Section 5.2.1. More information can be found in [MvOV96], [Sin01] and [Ros05].

The idea to use elliptic curves in cryptography originated with N. Koblitz and V. Miller in 1985 (see [MvOV96, p. 316]). We will describe the ideas of how to use elliptic curves (over fields) in Section 5.2.2.

In 1991 K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone invented a public key scheme using elliptic curves over the ring $\mathbb{Z}_n$, where n is the product of two distinct primes. Their paper started the interest in using elliptic curves over rings in cryptography, which resulted in several other cryptosystems. We will discuss the hardness of problems in Section 5.2.3, and in Section 5.2.4 we will present several cryptographic schemes using elliptic curves over rings, including the one by Koyama et al.

5.2.1 General Cryptography

In classical cryptography only secret key systems were known and in use; in such systems, both the sender and the recipient of a message have to fix a secret key in advance, and both are able to encrypt and decrypt messages with this key. A different approach is used in public key cryptography, where the sender and the recipient have different keys, and the key to encrypt can in fact be known to everyone without being of much help for reconstructing the corresponding secret key. The main concept on which public key cryptography relies is the concept of a *one-way trapdoor function*, which we will describe in the first paragraph, together with how such a function is used. In the next paragraph we present the concept of a *discrete logarithm problem*, which allows the construction of such one-way trapdoor functions, together with an example. Later we will see how elliptic curves can be used to construct hard discrete logarithm problems.

One-Way Trapdoor Functions

A *one-way trapdoor function* is an injective function $f : X \to Y$ having the following properties:

- The image $\varphi(x)$ can be effectively computed for every $x \in X$.
- For almost all $y \in Y$ it is almost infeasible to compute $x = f^{-1}(y)$ without knowing a secret.
- If one knows the secret, one can effectively compute $x = f^{-1}(y)$ for every $y \in \operatorname{im} f$.

There are many applications of one-way trapdoor functions; we describe the two probably most important ones:

(a) **Public Key Cryptography** A key consists of a public and a secret part. The public part is needed for encryption, but is useless for decryption. The decryption can only be done effectively if the secret part is known.

In fact, this can be directly realized by one-way trapdoor functions: the public part is the function itself, and the secret part is its secret.

(b) **Digital Signatures** A digital signature is the analogon to a real signature: it should ensure that a document is authentic. To attach a digital signature to a document, one needs to put some information about the document into the signature. Otherwise the signature could be simply copied into any other document. This is usually done by placing a hash value of the document into the signature.

A one-way trapdoor function serves as the public key of the signature, whereas the secret of the function is used to sign a document: one takes a hash value of the document, appends a text which identifies oneself, and uses the secret to generate a value $s \in X$. This signature can be verified by anyone by simply applying the function to it: if the result is meaningful (i. e. the hash value belongs to the document, and the appended text is correct), the signature and the document is authentic.

Discrete Logarithm Problems

Let G be a (multiplicatively written) group. A *discrete logarithm problem*, abbreviated to *DLP*, consists of two elements $x, y \in G$ and the task to find an $z \in \mathbb{N}$ such that $x^z = y$. One says that a discrete logarithm problem is *hard* if it is hard to compute such a z, and one says that the discrete logarithm problem for the group G is *hard* if for most choices of two elements $x, y \in G$, the discrete logarithm problem (G, x, y) is hard.

If G is a group for which the discrete logarithm problem is hard, it can be used for doing cryptography. We want to present two applications for such groups:

(a) **Key Exchange** In 1976 Diffie and Hellman proposed a secret key exchange based on the hardness of the discrete logarithm problem.

- The setup is a cyclic group G and a generator $g \in G$.
- Both parties pick an exponent e, compute g^e, and send this to the other party.
- Both parties raise the value from the other party to their own exponent; this new value serves as the secret key.

If a third party was able to collect the g^{e_i}'s which were sent around, it is, in general, not able to compute $g^{e_1 e_2} = (g^{e_1})^{e_2} = (g^{e_2})^{e_1}$ without solving one of the two DLPs $g^x = h_i$, where $h_i = g^{e_i}$.

(b) **One-Way Trapdoor Functions** In 1985 ElGamal constructed a one-way trapdoor function based on the discrete logarithm problem.

- The setup is a cyclic group G and a generator $g \in G$.
- The key generator chooses a random $a \in \mathbb{N}$ and computes $h := g^a$.
- The public information is (G, g, h).
- To encrypt an element $m \in G$, one chooses a random $b \in \mathbb{N}$ and computes $(g^b, mh^b) \in G^2$.
- To decrypt a pair $(g_1, g_2) \in G^2$, one computes $m = g_2 g_1^{-a}$.

Since similar constructions are used later, we want to describe the *RSA one-way trapdoor function.* Let p and q be two distinct primes and $n = pq$. Choose $e \in \mathbb{Z}_{\phi(n)}^*$, where $\phi(n) = |\mathbb{Z}_n^*| = (p-1)(q-1)$, and compute $d = e^{-1} \mod \phi(n)$. Then there exists a Bézout equation $1 = ed + k\phi(n)$ for some $k \in \mathbb{Z}$, and given an arbitrary $x \in \mathbb{Z}_n$, one can show that $(x^e)^d = x \cdot x^{k\phi(n)} \equiv x \pmod n$ using the Chinese Remainder Theorem (Proposition 2.5.6) and Little Fermat's Theorem.

The public information is now n and e, and d and the factorization $n = pq$ are the secret. The trapdoor function is $m \mapsto m^e \mod n$.

5.2.2 Elliptic Curves over Fields

The group of points of an elliptic curve over a finite field $\mathbb{F}_q$ is obviously finite. Moreover, the group operation is effectively computable but quite complex compared to the basic operations in $\mathbb{F}_q$. As it also seems that the discrete logarithm problem is hard for general curves, the groups of points of elliptic curves are suitable to be used for constructing discrete logarithm problems as described in Section 5.2.1. The discrete logarithm problem for elliptic curves is sometimes called the *Elliptic Curve Discrete Logarithm Problem*, abbreviated to *ECDLP*.

Besides this there are noteworthy constructions for elliptic curves, namely the Weil and the Tate pairing. A *pairing* is a bilinear map $G \times G \to H$ for two groups G and H. For information on the Weil pairing see, for example, [Sil86, pp. 95–99, Chapter III, Section §8] and [MOV93].

There are both constructive and destructive applications for the pairings: for example, they can be used for signature schemes with very short signatures, as described in [BLS04], or to create identity-based encryption schemes, as described in [BF03]. A destructive use is the *MOV Reduction*, as described in [MOV93]: it can be used to reduce the discrete logarithm problem from $E[k]$ to a discrete logarithm problem in a finite field $\mathbb{F}_{q^n}$, where $\mathbb{F}_q$ is the field of definition for the curve and n an integer depending on k and the curve. For special classes of curves, for example for supersingular curves, this index is bounded upwards by 6 (see [MOV93, p. 1642, Table 1]). And if, for example, the trace of Frobenius is 0, this index is at most 2. Therefore for curves with $q + 1$ points, the discrete logarithm problem is relatively easy. For details see [MOV93].

We want to note that pairings can also be defined for a generalized elliptic curve (see [KM85, pp. 87–91, Section 2.8]). From here on we are no longer interested in pairings.

5.2.3 Hardness of Problems over Rings

In this section we will discuss the hardness of two problems for elliptic curves over rings, namely counting the number of points and solving the discrete logarithm problem.

Counting the Points

In Section 5.1.3 we saw that in the case where $R = \mathbb{Z}_n$, n being a composite square-free integer, the problem of counting the number of points of an elliptic curve over R is randomly polynomial time equivalent to factoring n.

Consider the general case, i. e. R is an arbitrary finite ring. If the decomposition $R = \bigoplus_{i=1}^{n} R_i$ into finite local rings is known and, moreover, the reduction $R \to R_i/\mathfrak{m}_i$ can be effectively computed, where $\mathfrak{m}_i$ is the maximal ideal of R_i, then the points of a curve over R can be counted in deterministic polynomial time using Schoof's algorithm.

The same technique as in [KK98] can be used to factor R, given that one has an oracle that computes $|E_c(R)|$ for an arbitrary elliptic curve E_c over R. Since it is unlikely to have such an oracle, we will not investigate this problem any further. For related topics see Sections 5.1.3 and 5.1.4.

The Discrete Logarithm Problem

Consider again $R = \mathbb{Z}_n$ for a composite square-free integer n. By [KK98, Theorem 3], if the discrete logarithm problem in any group $E_c(\mathbb{Z}_n)$ can be solved, then n can be factored in randomly polynomial time. Moreover, if n can be factored, the discrete logarithm problem in an arbitrary group $E_c(\mathbb{Z}_n)$ can be reduced to discrete logarithm problems in $E_{c \bmod p}(\mathbb{Z}_p)$ for all prime factors p of n. This reduction can be done in deterministic polynomial time.

Clearly, the second reduction generalizes to elliptic curves over arbitrary finite rings $R = \prod_{i=1}^{k} R_i$: if the reductions $R \to R_i$ and $R_i \to R_i/\mathfrak{m}_i$ are known and can be effectively computed, where the $\mathfrak{m}_i$ is the maximal ideal of the local ring R_i, then the discrete logarithm problem in $E_c(R)$ can be reduced to the discrete logarithm problems in $E_c(R_i)$. Moreover, to solve the discrete logarithm problems in $E_c(R_i)$, one can first solve the discrete logarithm problem in $E_{c \bmod \mathfrak{m}_i}(R_i/\mathfrak{m}_i)$ and then exploit the following fact:

If G and H are groups, $f : G \to H$ is a group morphism, and $g^a = h$ a discrete logarithm problem in G, one obtains the discrete logarithm problem $f(g)^a = f(h)$ in H. If $b \in \mathbb{N}$ is a solution for this second problem, then $a \equiv b \pmod{\operatorname{ord} f(g)}$ for any solution a of the DLP $g^x = h$, and $\operatorname{ord} f(g)$ is a divisor of $\operatorname{ord} g$.

Conclusion

Elliptic curves are used in cryptography because with relatively small fields $\mathbb{F}_q$ one can get a good security level, i. e. the DLPs are 'hard enough'. Using elliptic curves over large fields $\mathbb{F}_q$ with sizes one has to use for RSA is not a good idea, since one operation on an elliptic curve is costly compared to one in $\mathbb{F}_q$ itself.

If now a finite ring R is used that has approximately the same cardinality as $\mathbb{F}_q$, and R can be effectively decomposed, then the discrete logarithm problem and the point counting problem for elliptic curves over R is easier by several magnitudes than for elliptic curves over $\mathbb{F}_q$.

To prevent this, one has two options:

(a) Use a ring R whose components are large enough such that the discrete logarithm problem over them is still hard.

But as mentioned this is not a good idea, since adding two points is a complex operation compared to one multiplication in R, and the advantage of elliptic curves was that the ground field can be relatively small.

(b) One has to use rings R, which cannot be decomposed. These are, by Corollary 2.2.23, exactly the local rings. Moreover, it must be very hard to effectively compute $R/\mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of R.

As the first option is not really useful, one has to look for finite local rings where the residue field is hard to compute. We will not investigate this topic any further, as for the two important classes of finite local rings R we introduced in Section 2.5 computing $R/\mathfrak{m}$ is relatively easy:

- Rings of the form $R = S/\langle f^n \rangle$, where S is an Euclidean domain, f an irreducible element in S and $n > 1$ an integer. In that case $R/\mathfrak{m} = S/\langle f \rangle$, and f can be found from f^n by computing roots; in the case of integers or polynomials over a finite field, this is relatively easy.
- Rings of the form $\mathbb{F}_q[x_1, \dots, x_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a zero-dimensional primary ideal. In this case $R/\mathfrak{m} = \mathbb{F}_q[x_1, \dots, x_n]/\sqrt{\mathfrak{a}}$, and computing $\sqrt{\mathfrak{a}}$ is not too hard; see [EHV92] and [Vas98, p. 104, Theorem 4.2.3].

Therefore, our conclusion is that using elliptic curves over rings for cryptography is not useful. This opinion is also expressed in [Gal02] for the case $R = \mathbb{Z}_n$.

5.2.4 Existing Schemes over Rings

There have been a few cryptosystems that use elliptic curves over rings. In most cases the ring $\mathbb{Z}_n$ is used, which by Section 5.1.2 and the notes from Section 5.2.3 seems not to be a good idea.

The System by Koyama, Maurer, Okamoto and Vanstone (KMOV)

This system, described in the 1991 paper [KMOV91], was the first cryptosystem using elliptic curves over rings. The ring used is $\mathbb{Z}_n$, where $n = pq$ is the product of two distinct primes. In the paper the authors basically use the Chinese Remainder Theorem (Proposition 2.5.6) to reduce to the case of elliptic curves over $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Moreover, the authors use the usual addition formulae for fields over $\mathbb{Z}_n$, noting that the chance that they fail is low enough to be ignored in practice: the authors argue that otherwise computing with points would be a feasible factoring algorithm, which they assume not to exist [KMOV91, p. 255]. The authors chose trace zero curves, i. e. curves over $\mathbb{Z}_p$ or $\mathbb{Z}_q$, which have exactly $p + 1$ or $q + 1$ points, respectively (the trace of Frobenius is zero; compare Theorem 4.2.43 and see Section 5.2.2 why this is not a good idea). More exactly the authors use

- curves of the form $E_{(0,0,0,0,b)}/\mathbb{Z}_p$, where $p \equiv 2 \pmod 3$; and
- curves of the form $E_{(0,0,0,a,0)}/\mathbb{Z}_p$, where $p \equiv 3 \pmod 4$.

The group of points for the first type is cyclic, and the one for the second type is either cyclic or $\mathbb{Z}_m \times \mathbb{Z}_2$, depending on whether a is a quadratic residue modulo p or not. For details see [KMOV91, p. 254, Lemma 1 and Lemma 2].

In the paper three schemes are described:

(a) [KMOV91, pp. 255f, Section 4] The first scheme is a simple generalization of the RSA trapdoor function:

(1) One first chooses n and a curve E_c over $\mathbb{Z}_n$.

(2) Then one determines the order k_p, k_q of the group of points over $\mathbb{Z}_p$, $\mathbb{Z}_q$, and takes k as the least common multiple of k_p and k_q.

(3) Next one chooses a (publicly known) encryption exponent $e \in \mathbb{Z}_k^*$ and the corresponding (private) decryption exponent $d = e^{-1} \in \mathbb{Z}_k^*$.

Then, if $P \in E_c(\mathbb{Z}_n)$, we have $d(eP) = (de)P = P$.

This system is only useful for signature schemes, since the knowledge of the secret key is required to be able to generate a point on $E_c(\mathbb{Z}_n)$. For this scheme, curves of full generality are used, i. e. both a and b might be non-zero.

(b) [KMOV91, pp. 256f, Section 5] The second scheme uses curves with a definition vector of the form $(0, 0, 0, 0, b)$. This scheme works by using the fact that the full information on the curve needed for adding two points is contained in the points themselves, as b can be computed from a point (x, y) by using the fact that $y^2 = x^3 + b$ and, therefore, for every point of the affine plane $\mathbb{A}^2(\mathbb{Z}_n)$ one can choose a b such that the point lies on the curve $E_{(0,0,0,0,b)}$. Hence, one works with a family of curves over $\mathbb{Z}_n$ instead of with a fixed curve. Encryption and decryption are done as in the first scheme.

Note that the affine plane $\mathbb{A}^2(\mathbb{Z}_n)$ is the disjoint union of the sets $E_{(0,0,0,0,b)}(\mathbb{Z}_n) \setminus \{\infty\}$, where b ranges over $\mathbb{Z}_n^*$.

(c) [KMOV91, pp. 257–260, Section 6] The third scheme works in the same way as the second scheme, except that the encryption exponent is fixed to 2. For decryption one reduces the problem using the secret key to two halving problems over curves over a finite field. The drawback is that for one point $P \in E_c(\mathbb{Z}_n)$ there might be four points $Q_i \in E_c(\mathbb{Z}_n)$ satisfying $2Q_i = P$. The halving algorithm is an adaption of an algorithm by Adleman, Manders and Miller for computing square roots in $\mathbb{Z}_p$.

As input data, the algorithm is given p, $E_c/\mathbb{Z}_p$, $|E_c(\mathbb{Z}_p)|$, and a point $Q \in E_c(\mathbb{Z}_p)$, which is known to be the double of another point in $E_c(\mathbb{Z}_p)$.

(1) First one writes $|E_c(\mathbb{Z}_p)| = 2^h c$ with integers h and c such that c is odd.

(2) Next choose a random point $T \in E_c(\mathbb{Z}_p)$ that is not a double point, i. e. which cannot be written as $T = 2T'$ for some $T' \in E_c(\mathbb{Z}_p)$. Moreover, T should be in the maximum cyclic subgroup of $E_c(\mathbb{Z}_p)$, which contains Q.

(3) Define $Y := Q$ and $H := \frac{c+1}{2} Q \in E_c(\mathbb{Z}_p)$.

(4) Find the least k such that $2^k cY = \infty$.

(5) If $k = 0$, output H.

(6) Otherwise, define $Y := Y - 2^{h-k}T$ and $H := H - 2^{h-k-1}cT$ and go to step (4).

To find a non-double point, Koyama et al. give two algorithms:

- Algorithm 1 for the case where $E_c = E_{(0,0,0,a,b)}$ over $\mathbb{Z}_p$, and $E_c(\mathbb{Z}_p)$ is cyclic:
  Choose a random point $T \in E_c(\mathbb{Z}_p)$. If $\frac{|E_c(\mathbb{Z}_p)|}{2}T \neq \infty$, output T. Otherwise, restart.
- Algorithm 2 for the case where $E_c = E_{(0,0,0,a,0)}$, over $\mathbb{Z}_p$, and $E_c(\mathbb{Z}_p) \cong \mathbb{Z}_2 \times \mathbb{Z}_{(p+1)/2}$:
  This algorithm needs to compute the Weil pairing
  $$e_n : E_c(\mathbb{Z}_p)[n] \times E_c(\mathbb{Z}_p)[n] \to \mathbb{Z}_p^*,$$
  where $n := \frac{p+1}{2}$. See [MOV93] for a description of the pairing and for an algorithm to efficiently compute it.
  Choose a random point $T \in E_c(\mathbb{Z}_p)$ such that $e_n(T, Q) = 1$. If $\frac{p+1}{4}T \neq \infty$ output T. Otherwise, restart.

For the security of the second and the third schemes, the authors show the following [KMOV91, p. 260f, Section 7]:

- Computing $|E_c(\mathbb{Z}_n)|$ is computationally equivalent to factoring n [KMOV91, p. 260, Theorem 8].
- Computing d from e (as in the first and second scheme) is computationally equivalent to factoring n [KMOV91, p. 260, Theorem 9].
- Completely breaking the second scheme is computationally equivalent to factoring n [KMOV91, p. 260, Theorem 10].

Koyama et al. moreover discuss several attack types:

(a) Homomorphism attacks [KMOV91, p. 261, Section 7.4]: note that the second and third scheme have the property that if $M_1, M_2 \in E_c(\mathbb{Z}_n)$ are two plaintexts, and $E : E_c(\mathbb{Z}_n) \to E_c(\mathbb{Z}_n)$ is the encryption function, then $E(M_1) + E(M_2) = E(M_1 + M_2)$. The same holds for decryption. But for this we need that M_1 and M_2 lie on the same curve $E_c/\mathbb{Z}_p$; if M_1 and M_2 lie on different curves, which is the case with a high probability, then encryption and decryption do not have this property.

It is still possible to exploit the homomorphism property (see [KMOV91] for more details and how to avoid this).

(b) Isomorphism attacks [KMOV91, pp. 261f, Section 7.5]: an isomorphism is a coordinate transformation and can be used by an attacker to make someone sign a seemingly "random" message. By applying the isomorphism to the point, one gets a signature for the plain text obtained from the original plaintext after applying the isomorphism. This again can be avoided (for details see [KMOV91]).

(c) Low Multiplier Attack [KMOV91, p. 263, Section 7.6]: for the original RSA system there have been attacks where small encryption exponents were used, like $e = 2$ as in the third scheme above. Koyama et al. argue that the methods used for RSA cannot be applied to this case.

The Meyer-Müller Cryptosystem

At the Eurocrypt'96 conference, B. Meyer and V. Müller [MM96] presented another cryptosystem based on elliptic curves over $\mathbb{Z}_n$, based on the scheme by Koyama et al. [KMOV91]. M. Joye and J.-J. Quisquater have shown in [JQ98] that the Meyer-Müller system can be reduced to the Rabin-William cryptosystem.

We will describe how the system works. One chooses n to be the product of two distinct primes that are congruent to 11 modulo 12. Meyer and Müller use the fact that one can uniquely determine one of the possible four square roots of $k \in \mathbb{Z}_n$ by two bits, which store whether the square root is odd or even, and whether the Jacobi symbol is 1 or -1. See [MM96, Section 3] for details.

To encrypt a message $m \in \mathbb{Z}_n$ one randomly chooses a $\lambda \in \mathbb{Z}_n \setminus \{0\}$ and defines a point $P = (m^2 : \lambda m^3 : 1) \in \mathbb{P}^2(\mathbb{Z}_n)$. Moreover, one defines $a = \lambda^3$ and computes $b = (\lambda^2 - 1)m^6 - am^2$, and checks whether $\Delta_{(0,0,0,a,b)} \in \mathbb{Z}_n^*$. If this is not the case, one chooses another λ. Otherwise, one computes $(x : y : 1) = 2P$, and sends a, b, x, the Jacobi symbol $\left(\frac{y}{n}\right)$ and whether y is odd or even.

For decryption one computes the square root y of $x^3 + ax + b$ determined by the Jacobi symbol and the odd/even bit. Then one computes all $P_i = (x_i : y_i : 1) \in E_{(0,0,0,a,b)}$ such that $2P_i = (x : y : 1)$. Next, compute all i such that $a^2 = y_i^6 x_i^{-9} \mod n$. If there is more than one such i, this is a protocol failure. Otherwise $m = y_i^3 x_i^{-4} a^{-1} \mod n$.

If in encryption or decryption any operation fails, this is also a protocol failure. Meyer and Müller note that the probability that there is more than one i and that one cannot factor n at the same time is at most $118^2/(n-1)$ (see [MM96, Theorem 2]).

What is left is how to compute a $P \in E_c(\mathbb{Z}_n)$ such that $2P = Q$ for a given $Q \in E_c(\mathbb{Z}_n)$. If the factorization of n is known, one can reduce to $P, Q \in E_c(\mathbb{Z}_p)$ for a prime p [MM96, Section 5.2]. For this case Meyer and Müller provide an algorithm (see [MM96, Algorithm 4]) that computes the roots of a polynomial of degree four and tries whether there are y-coordinates for every root x such that $2(x : y : 1) = Q$.

Moreover, Meyer and Müller show that factoring n and decrypting arbitrary messages is randomly polynomial time equivalent (see [MM96, Theorem 6]).

This system has several disadvantages. Decryption is more complicated, as in the system by Koyama et al. from above. Also, Joye and Quisquater pointed out in [JQ98, Section 1] that if a message is sent twice to different receivers, one can reconstruct the plaintext from the two ciphertexts.

Paillier Schemes

In his paper [Pai00] S. D. Paillier presents three cryptosystems based on elliptic curves over rings. The first one is a variant of the encryption scheme of Naccache and Stern and uses a curve over the ring $\mathbb{Z}_n$, with $n = pq$ for two distinct primes p and q. The second is an analogon to the Okamoto-Uchiyama encryption scheme and uses curves over the ring $\mathbb{Z}_{p^2q}$ for two distinct primes p and q. The third is a variant of the Paillier cryptosystem and uses curves over the ring $\mathbb{Z}_{n^2}$, where $n = pq$ is the product of two distinct primes.

S. D. Galbraight shows that the third scheme in [Pai00] is not secure (see [Gal02, Section 6]) and that the second one cannot be implemented securely (see [Gal02, Section 7]). Then he presents another variation of the original Paillier cryptosystem (see [Gal02, Section 9]). Note that Galbraight remarks that cryptosystems based on elliptic curves over $\mathbb{Z}_n$ for large n are practically irrelevant, since their performance is much worse than those of non-elliptic curve schemes over $\mathbb{Z}_n$, for example RSA.

Extensions of Previous Schemes

Let n be the product of two distinct primes p and q. A cryptosystem is *semantically secure* if, given two ciphertexts and one plaintext, it is impossible to determine which ciphertext corresponds to the plaintext.

(a) In [GMMV02] a semantically secure RSA system based on elliptic curves over $\mathbb{Z}_{n^2}$ is presented. In this scheme only the x-coordinate of a point is stored, and a curve of the type $E_{(0,0,0,a,b)}/\mathbb{Z}_{n^2}$ is used.

(b) In [GMMV03] a semantically secure extension of the KMOV scheme over $\mathbb{Z}_{n^2}$ is presented. As in the KMOV scheme, points are taken from a family of curves of the form $E_{(0,0,0,0,b)}/\mathbb{Z}_{n^2}$.

(c) In [GMTV04] a semantically secure scheme is presented that also works with a family of curves of the form $E_{(0,0,0,0,b)}/\mathbb{Z}_{n^2}$. This scheme uses ideas from both Paillier schemes and Rabin related schemes.

Bibliography

[AM93] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, January 1993.

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615 (electronic), 2003.

[BL95] Wieb Bosma and Hendrik W. Lenstra, Jr. Complete systems of two addition laws for elliptic curves. *Journal of Number Theory*, 53(2):229–240, 1995.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. Number 21 in Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, Berlin, 1990.

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, 17(4):297–319, 2004.

[Bro05] Markus Brodmann. Personal communication, January 2005.

[BSS99] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves and Cryptography*. Cambridge University Press, Cambridge, UK, 1999.

[BW85] Michael Barr and Charles Wells. *Toposes, Triples and Theories*. Number 278 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, New York, 1985.

[CAG04] Computational Algebra Group at the University of Sydney. The Magma computational algebra system. Available at `http://magma.maths.usyd.edu.au/magma/`, 1993–2004.

[CLO96] David A. Cox, John B. Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, 1996.

[CLO98] David A. Cox, John B. Little, and Donal O'Shea. *Using Algebraic Geometry*. Number 185 in Graduate Texts in Mathematics. Springer, 1998.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Number 138 in Graduate Texts in Mathematics. Springer-Verlag, Berlin, third corrected edition, 1996.

[EH00] David Eisenbud and Joe Harris. *The Geometry of Schemes.* Number 197 in Graduate Texts in Mathematics. Springer, New York, 2000.

[EHV92] David Eisenbud, Craig Huneke, and Wolmer V. Vasconcelos. Direct methods for primary decomposition. *Inventiones mathematicae*, 110:207–235, 1992.

[Eis95] David Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry.* Number 150 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.

[Eng99] Andreas Enge. *Elliptic Curves and their Applications to Cryptography. An Introduction.* Kluwer Academic Publishers, Boston, 1999.

[Gal02] Steven D. Galbraith. Elliptic curve paillier schemes. *Journal of Cryptology*, 15:129–138, 2002.

[GD61] Alexandre Grothendieck and Jean Dieudonné. *Éléments de Géométrie Algébrique, chapter II: Étude globale élémentaire de quelques classes de morphismes.* Number 8 in Publications Mathématiques. Institut des Hautes Études Scientifiques, 1961. Freely available in digitalized form at `http://www.numdam.org`.

[GD67] Alexandre Grothendieck and Jean Dieudonné. *Éléments de Géométrie Algébrique, chapter IV: Étude locale des schémas et des morphismes de schémas.* Number 20, 24, 28 and 32 in Publications Mathématiques. Institut des Hautes Études Scientifiques, 1964–1967. Freely available in digitalized form at `http://www.numdam.org`.

[GMMV02] David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar. A semantically secure elliptic curve RSA scheme with small expansion factor. Cryptology ePrint Archive, Report 2002/083, June 2002. `http://eprint.iacr.org/`.

[GMMV03] David Galindo, Sebastià Martín, Paz Morillo, and Jorge L. Villar. An efficient semantically secure elliptic curve cryptosystem based on KMOV. In *Proceedings of International Workshop on Coding and Cryptography WCC*, pages 213–221, 2003.

[GMTV04] David Galindo, Sebastià Martín, Tsuyoshi Takagi, and Jorge L. Villar. A provably secure elliptic curve scheme with fast encryption. In *Proceedings of INDOCRYPT*, number 3348 in Lecture Notes in Computer Science, pages 245–259, Chennai, India, 2004.

[Har77] Robin Hartshorne. *Algebraic Geometry.* Number 52 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1977.

[HMU01] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, second edition, 2001.

[Iit82] Shigeru Iitaka. *Algebraic Geometry.* Number 76 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1982.

[IR82] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory.* Number 84 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1982.

[Jac68] Nathan Jacobson. *Structure of Rings*, volume 37 of *Colloquium Publications.* American Mathematical Society, Providence, R. I., revised edition, 1968.

[JQ98] Marc Joye and Jean-Jacques Quisquater. Reducing the elliptic curve cryptosystem of Meyer-Müller to the cryptosystem of Rabin-Williams. *Designs, Codes and Cryptography*, 14(1):53–56, April 1998.

[KK98] Noboru Kunihiro and Kenju Koyama. Equivalence of counting the number of points on elliptic curve over the ring $\mathbb{Z}_n$ and factoring n. In *Advances in Cryptology - Eurocrypt '98*, number 1070 in Lecture Notes in Computer Science, pages 47–58, 1998.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves.* Princeton University Press, Princeton, New Jersey, 1985.

[KMOV91] Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, and Scott A. Vanstone. New public-key schemes based on elliptic curves over the ring $\mathbb{Z}_n$. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 252–266, 1991.

[Len86] Hendrik W. Lenstra, Jr. Elliptic curves and number-theoretic algorithms. In *Proceedings of the International Congress of Mathematicians*, volume 1, pages 99–120, 1986.

[Len87] Hendrik W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics. Second Series*, 126(3):649–673, 1987.

[LR85] Herbert Lange and Wolfgang M. Ruppert. Complete systems of addition laws on abelian varieties. *Inventiones mathematicae*, 79:603–610, 1985.

[LR87] Herbert Lange and Wolfgang M. Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *Journal of Algebra*, 107(1):106–116, 1987.

[Mat80] Hideyuki Matsumura. *Commutative Alebra.* The Benjamin/Cummins Publishing Company, Reading, Massachusetts, second edition, 1980.

[MFK65] David B. Mumford, John Fogarty, and Frances Kirwan. *Geometric Invariant Theory.* Number 34 in Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, Berlin, third enlarged edition, 1965.

[MM96] Bernd Meyer and Volker Müller. A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring. In *Advances in Cryptology - Eurocrypt '96*, number 1070 in Lecture Notes in Computer Science, 1996.

[MMV01] Sebastià Martín, Paz Morillo, and Jorge L. Villar. Computing the order of points on an elliptic curve modulo N is as difficult as factoring N. *Applied Mathematics Letters*, 14:341–346, 2001.

[Mon87] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, January 1987.

[Mon02] Chris Monico. Computing the primary decomposition of zero-dimensional ideals. *Journal of Symbolic Computation*, 34(5):451–459, 2002.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, September 1993.

[Mum99] David B. Mumford. *The Red Book of Varieties and Schemes.* Number 1358 in Springer Lecture Notes in Mathematics. Springer-Verlag, Berlin Heidelberg, second expanded edition, 1999.

[MuP05] MuPAD Forschungsgruppe Universität Paderborn. MuPAD. The open computer algebra system. Available at `http://www.mupad.de/`, 1997–2005.

[MvOV96] Alfred J. Menezes, Paul van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[Oor66] Frans Oort. *Commutative Group Schemes.* Number 15 in Lecture Notes in Mathematics. Springer-Verlag, New York, 1966.

[Pai00] Pascal Paillier. Trapdooring discrete logarithms on elliptic curves over rings. In T. Okamato, editor, *Advances in Cryptology – ASIACRYPT 2000*, number 1976 in Lecture Notes in Computer Science, pages 573–584. Springer-Verlag, 2000.

[Ros05] Joachim Rosenthal. Cryptography. Personal notes available at `http://www.math.unizh.ch/aa/uploads/media/crypto.pdf`, winter term 2004–2005.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, April 1985.

[Sch87] René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory, Series A*, 46:183–211, 1987.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.

[Sin01] Simon Singh. *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets.* Deutscher Taschenbuch Verlag, München, 2001.

[SS88] Günter Scheja and Uwe Storch. *Lehrbuch der Algebra, Teile I und II.* Teubner, Stuttgart, 1980, 1988.

[SW93] Robert D. Silverman and Samuel S. Wagstaff, Jr. A practical analysis of the elliptic curve factoring algorithm. *Mathematics of Computation*, 61(203):445–462, 1993.

[Vas98] Wolmer V. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry.* Number 2 in Algorithms and Computations in Mathematics. Springer-Verlag, Berlin, 1998.

[Vol88] J. F. Voloch. A note on elliptic curves over finite fields. *Bulletin de la Société Mathématique de France*, 116(4):455–458, 1988. Freely available in digitalized form at `http://www.numdam.org`.

[Wal99] Judy L. Walker. Algebraic geometric codes over rings. *Journal of Pure and Applied Algebra*, 144:91–110, 1999.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969. Freely available in digitalized form at `http://www.numdam.org`.

Index

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel und Quellen benutzt habe.