Definability in Global Fields and Finitely Generated Fields

by

Kasper Dokter

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of

Master of Science

in the

Department of Mathematics
Utrecht University

at

December 11, 2013

Supervisor:

Dr. J. van Oosten

Second reader:

Prof. Dr. G. L. M. Cornelissen

Abstract

For algebraically closed fields, one cannot define characteristic zero by means of a single sentence in the language of rings. However, for global fields (i.e., finite separable extensions of $\mathbb{Q}$ or $\mathbb{F}_p[t]$) characteristic zero is definable. In other words, there is a sentence in the language of rings which is true in a global field precisely when that global field has characteristic zero. In fact there are many subsets of the set of global fields which have a first-order definition and they correspond to the arithmetically definable subsets of the natural numbers. It turns out that characteristic zero is also definable for infinite finitely generated fields. The characterization of all subsets of infinite finitely generated fields is still an open problem.

Preface

During the master course on model theory, I realized that there is a very strong connection between algebra and logic. Therefore, when I started to look for a subject for my thesis, I tried to find something which lies in the intersection of these two field. Jaap van Oosten suggested that I should study an article by B. Poonen [11], a number theorist who became interested in logic. I soon found out that his article was an extension of an article by R.M. Rumely [14]. Since I wanted my thesis to be self-contained, I started to work on this article, which unfortunately left no time to fully understand the results of Poonen. However, I hope that you will appreciate the beauty of the mathematics which is presented in this thesis.

Acknowedgements. First, I would like to thank Jaap van Oosten for his supervision the past year. I am grateful for his useful explanations and for the many other suggestions he made. It was a pleasure to be his student. I would also like to thank Gunther Cornelissen his time to read my thesis. Finally I would like to thank my parents for their support and interest during the past year.

Contents

Introduction

Mathematics is the art of finding proofs for statements about a given class of objects. For example, one may take the class of objects to be the set of all platonic polyhedra (this set consists of a tetrahedron, a cube, a octahedron, a dodecahedron and an icosahedron). It is easy to see that the statement "the number of faces equals six" is true for a cube, but false for any other polyhedron in this class. Euler discovered that the statement "the number of faces minus the number of edges plus the number of vertices equals two" is true for any of these polyhedra. We see how statements (or properties) interact with the objects from the class. We will investigate this interaction for some other, more involved, classes of objects.

In this thesis we will consider three classes of objects, namely

- *countable algebraically closed fields*;
- *global fields*;
- *infinite finitely generated fields.*

The objects in each of these classes are fields. A *field* is a set F, in which we can add ($+$) and multiply ($\times$) any two elements, with two special elements 0 and 1 such that some elementary properties about $+$, $\times$, 0 and 1 hold. See Definition 1.1.1 and Definition 1.1.3 for the precise definition of these properties. An example of a field is the set of rational numbers with the usual addition and multiplication and the two special elements 0 and 1. For the precise definition of the above classes we refer to Definition 1.11.11, Definition 2.1.1 and Definition 4.2.1.

Statements about a field are expressed in a mathematical language, namely the language of rings. The *language of rings* is the set of sequence of symbols from the following (infinite) list

$$0, 1, +, \times, =, \bot, \wedge, \vee, \rightarrow, \neg, \forall, \exists,), (, x, y, z, \ldots.$$

An example of a statement in this language is

$$\forall x(\neg(x = 0) \rightarrow \exists y(x \times y = 1))$$

which means (when *interpreted* in a field F)

"*for all* x in F we have that if *not* $x = 0$ then *there exists* a y in F such that $x \times y = 1$"

Clearly not all sequences of this symbols give a statement in the language of rings. Using the grammar of the language of rings, it can be seen whether a sequence of symbols is a well formed statement. This is defined explicitly in section 3.1.

Goals. Our goal is to investigate, for each of these classes of fields, the connection between the objects and its properties by means of the following three questions.

1) Is it decidable whether an arbitrary statement is true for a given object?

In this question we ask if there is a procedure which enables us to calculate whether a given statement is true for an arbitrary object of the class. This procedure should be independent from the statement.

2) Which subclasses can be distinguished by a single statement?

As seen in the example of the platonic polyhedra, the cube can be distinguished from any other polyhedron by the statement that the polyhedron has six faces. We now ask for which subclasses there exists a statement which is true for object if and only if that object is in that subclass.

If every single object can be distinguished by a single statement, then we get a positive answer to the following question.

3) Are two objects in a class with the same properties equal?

In this question we ask ourselves whether an object is completely determined by its properties. It could be the case that two objects are nearly the same, but that one cannot express their difference in the language. We see that we need a very precise definition of our language. This language will be the language of rings.

Structure. The first thing to do is to define what is meant by these three different classes of objects: countable algebraically closed fields, global fields and infinite finitely generated fields. This is done in chapter 1 and 2. In chapter 1 we introduce the basic commutative algebra which is needed in order to define these classes. Then in chapter 2 we study the properties of a global field.

After defining the objects we focus in chapter 3 on the statements about these objects. We first define what is meant by a statement, and also when it is true for a given object. We will prove some theorems (Theorem 3.9.8 and Corollary 3.10.8) towards the answer of the first question.

In chapter 4, 5 and 6 we will discuss the above questions for the countable algebraically closed fields, global fields and infinite finitely generated fields. There chapters are all independent from each other.

Own work. The major results of this thesis are already known for about thirty years or more. My work consists mainly of bundling those results into a single text. As each text has its own way to present the material, the bundling required to reformulate the results and fill in the details that are left unmentioned.

In this thesis introduced some new notation (like $\mathcal{O}_{\mathbb{K}}$, $\mathbb{K}$) and used the phrase 'non-integral t in a global field' instead of 'non-constant t in a function field' (c.f., section 4 of [14]). In this new notation, I extended proofs, which applied to number fields, to apply for all global fields (e.g., Lemma 2.3.5). I also generalized the notion of a (rank 1) valuation (compare Definition 2.5.5 with page 2 of [3]) and showed that every valuation on a global field is discrete. This more general approach enabled me to prove that the valuation rings of a global field admit a first-order definition (c.f., Corollary 2.5.16 and Lemma 5.3.1). This fact was assumed to be well-known by Rumely (c.f., page 204 of [14]).

Inspired by the questions of Poonen [11], I asked myself whether I could characterize the definable subsets of isomorphism classes of global fields. It turned out to be possible and I proved this in 5.8.

Prerequisites. The reader should have some basic knowledge about mathematics, say at bachelor level. More explicitly this means that you should be be familiar with the following:

- *Elementary set theory*: countable sets, equivalence relations/classes, total orders);
- *Complex numbers*;
- *Elementary theory of metric spaces*; convergent sequences, limits, Cauchy sequences.
- *Linear algebra*: vector spaces, linear maps, bases, matrices, determinants;
- *Elementary group theory*: normal subgroups;
- *Elementary number theory*: Bézout identity, quadratic reciprocity law, Legendre symbol.

Chapter 1

Commutative Algebra

A ring is a set in which you can add, subtract and multiply and a field is a ring in which you can divide. The goal of this chapter is to give an introduction into the theory of rings which will be used in the next chapters. To be more precise, consider the diagram

$$\begin{array}{ccc} K & \to & L \\ \uparrow & & \uparrow \\ R & \to & S \end{array} \tag{1.1}$$

where all maps are inclusions of rings, L/K is a field extension of finite degree, R is a Dedekind domain, S is the integral closure of R in L. In this setting we will study the arithmetic of the ring S.

The structure of this chapter is as follows. In section 1.1 we recall the definition of rings and fields, which are the objects in diagram (1.1). Then in section 1.2 and 1.3 we investigate some basis properties about the arithmetic in such rings: in section 1.2 we show the connection between divisors of zero in a ring and the existence of a field extending the ring. As we are considering diagram (1.1), we restrict our attention to integral domains, which are rings for which there exists a field extending it. Next, in section 1.3 we are considering factorizations of non-zero elements. We will conclude that an element in a general integral domain does not always admits factorization, because some elements in some integral domains are infinitely divisible or factorization is not unique. However, not all is lost if we pass to ideals, which generalizes the concept of an element. This is part of section 1.4. There we recall the definition of an ideal and show how we can do arithmetic with them, i.e. we define a product and define divisibility of ideals. Then in section 1.5 we give a condition such that no ideals are infinite divisible. Although ideals are already helpful, it turns out that ideals are not general enough. We generalize an ideal using modules, which are discussed in section 1.6. This will be used in section 1.10 to define a fractional ideal. We then focus on the constructions used in the rings R and S in diagram (1.1). We first study, in section 1.7, the properties of the integral closure and then give a quick introduction to local domains in section 1.8. These constructions allow us to describe the two kinds of rings which are most important for us: valuation domains and Dedekind domains which will be discussed in section 1.9 and 10 respectively. For now it seems that these two rings have little to do with each other. Finally we investigate the extension L/K of fields. First we examine the properties of a field extension, which is done in section 1.11.

1.1. Rings and homomorphisms

In this section we will define the most basic notions used in diagram (1.1), i.e., the notion of rings, subrings and fields and homomorphisms between them.

Rings and fields. Let us start with the definition of a ring.

Definition 1.1.1 (Rings)**.** A *ring* is an ordered tuple $(R, +, \cdot, 0, 1)$ consisting of a set R, two binary functions $+, \cdot$ and two (not necessarily distinct) elements $0, 1 \in R$ such that

1) $(R, +, 0)$ is an abelian group, i.e.,
   a) for all $x, y, z \in R$ we have $x + (y + z) = (x + y) + z$;
   b) for all $x \in R$ we have $x + 0 = x$;
   c) for all $x \in R$ there is a $y \in R$ such that $x + y = 0$;
   d) for all $x, y \in R$ we have $x + y = y + x$;
2) $\cdot$ is associative, i.e., for all $x, y, z \in R$ we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
3) $\cdot$ distributes over $+$, i.e., for all $x, y, z \in R$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$;
4) R is *unital*, i.e., for all $x \in R$ we have $x \cdot 1 = x$;
5) R is *commutative*, i.e., for all $x, y \in R$ we have $x \cdot y = y \cdot x$. △

For notational convenience we will denote $S = (R, +, \cdot, 0, 1)$ by R (e.g., we say that $\mathbb{Z}$ is a ring). This allows us to write "let R be a ring and $x \in R$". Without this convention this would mean that x is a set or a mapping or a constant. Furthermore the dot $\cdot$ is usually omitted (e.g. we write xy instead of $x \cdot y$).

Example 1.1.2 (Trivial ring)**.** Let R be a ring consisting of one element x. Then we have $0 = 1$, since $0, 1 \in \{x\}$. Let R be a ring with $0 = 1$. Then we have $x = 1 \cdot x = 0 \cdot x = 0$ for all $x \in R$ and hence $R = \{0\}$. In this case we call R *trivial* and otherwise R is called *non-trivial*. ◊

Definition 1.1.3 (Fields)**.** A *field* is a ring R such that

7) R is non-trivial, i.e., $1 \neq 0$;
8) for all $0 \neq x \in R$ there is a $y \in R$ such that $xy = 1$. △

The second property in the definition of a field may be stated as: every non-zero element x of R is *invertible*. Indeed the y in the definition acts as the inverse $1/x$ in R.

We now list some examples of rings and show some important constructions of rings out of a given one.

Example 1.1.4. The set of integers $\mathbb{Z}$ with usual addition and multiplication and interpretation of 0 and 1 is a ring, while the set of natural numbers with zero $\mathbb{N}$ is not.

The set of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ with usual addition and multiplication and interpretation of 0 and 1 are fields under the standard addition and multiplication. ◊

Example 1.1.5 (Number ring)**.** Let m be an integer. The subset

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

of the complex numbers $\mathbb{C}$ with induced addition and multiplication form a ring. This ring is an example of a *number ring*. ◊

Example 1.1.6. Let m be a positive integer. If $x, y \in \mathbb{Z}$ are integers, then x is *congruent* to y modulo m (notation: $x \equiv y \pmod{m}$) if and only if $m \mid x - y$. This defines an equivalence relation on $\mathbb{Z}$ and the set $\mathbb{Z}_m = \{0, \ldots, m - 1\}$ is a full set of representatives. Addition and multiplication in $\mathbb{Z}$ induces addition and multiplication modulo m in $\mathbb{Z}_m$: for all $x, y \in \mathbb{Z}_m$ there are unique $s, p \in \mathbb{Z}_m$ such that $x + y \equiv s$ and $xy \equiv p$ modulo m. Therefore $\mathbb{Z}_m$ is a ring. If m is prime, then $\mathbb{Z}_m$ is a field: for every non-zero $x \in \mathbb{Z}_m$ the greatest common divisor of x and m is 1. Bézouts identity gives $a, b \in \mathbb{Z}$ such that $ax + bm = 1$, which reduces modulo m to $ax \equiv 1$ modulo m. If p is prime then we write $\mathbb{F}_p := \mathbb{Z}_p$. ◊

Example 1.1.7 (Factor ring)**.** We mimic the previous example in a general ring R. Let $R^+ = (R, +, 0)$ denote the *additive group*. An *ideal* of a ring R is a subgroup $\mathfrak{a} < R^+$ such that $r\mathfrak{a} \subseteq \mathfrak{a}$ for all $r \in R$. An ideal $\mathfrak{a}$ of R is called *proper* if $\mathfrak{a} \neq R$. In section 1.4 we further investigate ideals. Let $\mathfrak{a}$ be a proper ideal of a ring R. If $x, y \in R$, then x is *congruent* to y modulo $\mathfrak{a}$ (notation: $x \equiv y \pmod{\mathfrak{a}}$) if and only if $x - y \in \mathfrak{a}$. This defines an equivalence relation on R and the equivalence classes are denoted by $x + \mathfrak{a}$, $x \in R$. The *factor ring* of R by $\mathfrak{a}$ is the set $R/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in R\}$ of all equivalence classes together with the addition and multiplication defined by $(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$ and $(x + \mathfrak{a}) \cdot (y + \mathfrak{a}) = x \cdot y + \mathfrak{a}$. It is easy to see that $R/\mathfrak{a}$ is a ring. ◊

Example 1.1.8 (Product ring)**.** Let R and S be rings. Then the set

$$R \times S = \{(r, s) \mid r \in R, s \in S\}$$

together with componentwise addition and multiplication (i.e.,

$$(r, s) + (r', s') = (r + r', s + s') \text{ and } (r, s) \cdot (r', s') = (r \cdot r', s \cdot s'))$$

is a ring. This ring is called the *product ring* of R and S. ◊

Example 1.1.9 (Polynomial ring)**.** Let R be a ring and X be a symbol. Then a *polynomial* f in X with coefficients in R is the sum

$$f = \textstyle\sum_{i \geq 0} a_i X^i$$

where $a_i \in R$ and $a_i \neq 0$ for finitely many $i \geq 0$. The elements a_i are called the *coefficients* of f. The element a_0 is called the *constant coeffient*. If all coefficients are zero, then f is called *zero* (notation: $f = 0$). In this case the *degree* of f is $-\infty$ (notation: $\deg(f) = -\infty$). If f is a non-zero polynomial, then the element a_d, with $d = \max(\{i \mid a_i \neq 0\})$ the *degree* of f (notation: $\deg(f) = d$), is called the *leading coefficient* of f and if $a_d = 1$ then f is called *monic*. Let $f = \sum_{i \geq 0} a_i X^i$ and $g = \sum_{i \geq 0} b_i X^i$ be polynomials. Then

$$f + g = \textstyle\sum_{i \geq 0}(a_i + b_i)X^i \qquad f \cdot g = \sum_{k \geq 0} \left(\sum_{i+j=k} a_i b_j \right) X^k,$$

define the sum and product of f and g. The *polynomial ring* in a symbol X over a ring R is the set

$$R[X] = \{\textstyle\sum_{i \geq 0} a_i X^i \mid a_i \in R, a_i \neq 0 \text{ for finitely many } i\}$$

of all polynomials in X (with coefficients in R) with respect to this sum and product. Notice that this sum and product are well-defined, i.e., only finitely many coefficients are non-zero. Furthermore we will choose the symbol X implicitly (e.g. we will not write "Let R be a ring and X a symbol and consider $R[X]$" but rather "Let R be a ring and consider $R[X]$") ◊

Example 1.1.10 (Group ring)**.** The *group ring* $R[G]$ of a group G over a ring R is the set

$$R[G] = \{\textstyle\sum_{g \in G} a_g g \mid a_g \in R, a_g \neq 0 \text{ for finitely many } g\}$$

with addition and multiplication of $r, s \in R[G]$ defined by

$$r + s = \textstyle\sum_{g \in G}(a_g + b_g)g \qquad r \cdot s = \sum_{g \in G} \sum_{xy=g} (a_x b_y) g$$ ◊

Homomorphisms. We now introduce the concept of a homomorphism, which is a structure preserving map between rings.

Definition 1.1.11 (Homomorphisms)**.** Let R and S be rings. A map $f : R \to S$ is a *(ring) homomorphism* and only if if for all $x, y \in R$ we have

1) $f(1) = 1$;

2) $f(x+y) = f(x) + f(y)$;

3) $f(xy) = f(x)f(y)$.

When R equals S, then a homomorphism is also called an *endomorphism*. △

Example 1.1.12. The following maps are homomorphisms:

1) Let A be a ring. The identity map $\mathrm{id}_A : A \to A$ is an endomorphism.

2) Let $f : A \to B$ and $g : B \to C$ be homomorphisms of rings. Then the *composition* $g \circ f : A \to C$ given by $x \mapsto g(f(x))$ is a homomorphism.

3) Let R and S be rings and $s \in S$. The *evaluation homomorphism/map* $e_s : R[X] \to S$ given by $P(X) \mapsto P(s)$ is a homomorphism.

The reader may check that the axioms of a homomorphism are satisfied. ◊

Using this example we may define the following:

Definition 1.1.13 (Isomorphisms)**.** A homomorphism $f : R \to S$ is a *(ring) isomorphism* if and only if there exists a homomorphism $g : S \to R$ such that $g \circ f = \mathrm{id}_R$ and $f \circ g = \mathrm{id}_S$. In this case R and S are called *isomorphic* (notation: $R \cong S$). A *(ring) automorphism* is a isomorphism $f : R \to R$. △

Now, at the end of this paragraph, we will focus on an important connection between rings and homomorphisms.

Definition 1.1.14 (Kernel and image)**.** Let $f : X \to Y$ be a map of sets. Then the *image* of f is set $f(X) = \{f(x) \mid x \in X\}$. The *kernel* of f is the set $\ker f = \{x \in X \mid f(x) = 0\}$. △

It is easily seen that the image of a homomorphism is a ring and that the kernel of a homomorphism is an ideal (c.f., Example 1.1.7). The following theorem shows a connection between the kernel and the image.

Theorem 1.1.15 (First isomorphism theorem)**.** *Let $f : R \to S$ be a homomorphism of rings. Then*

$$R/\ker(f) \cong f(R).$$

Proof. Consider that mappings

$$\bar{f} : R/\ker(f) \longrightarrow f(R), \qquad x + \ker(f) \mapsto f(x)$$

and

$$\bar{g} : f(R) \longrightarrow R/\ker(f), \qquad f(x) \mapsto x + \ker(f).$$

Note that for all $x, x' \in R$ the following statements are equivalent:

$$x + \ker(f) = x' + \ker(f) \;\Leftrightarrow\; x - x' \in \ker(f) \;\Leftrightarrow\; f(x - x') = 0 \;\Leftrightarrow\; f(x) = f(x').$$

This shows that both $\bar{f}$ and $\bar{g}$ are well-defined maps. It is trivial to check that both $\bar{f}$ and $\bar{g}$ are homomorphisms and that for all $x \in R$ we have $\bar{g}(\bar{f}(x + \ker(f))) = x + \ker(f)$ and $\bar{f}(\bar{g}(f(x))) = f(x)$. We conclude that $\bar{f}$ and $\bar{g}$ are isomorphisms, which proves the theorem. □

Subrings. Although rings and homomorphisms are interesting enough to study them one by one, it is fruitful to consider the extension of rings. Notice that the focus lies on interplay between the two rings rather then the arithmetic of a single ring.

Definition 1.1.16 (Ring extensions)**.** Let $(R, +, \cdot, 0_R, 1_R)$ and $(S, \oplus, \odot, 0_S, 1_S)$ be rings. Then R is an *extension* of S (notation: R/S) or S is a *subring* of R if and only if

1) $S \subseteq R$;

2) for all $x, y \in S$ we have $x \oplus y = x + y$ and $x \odot y = x \cdot y$;

3) $0_S = 0_R$;

4) $1_S = 1_R$.

If both R and S are fields, then R/S is called an *extension of fields*. △

We list some examples, non-examples and constructions of extensions of rings.

Example 1.1.17. The rationals $\mathbb{Q}$ and $\mathbb{Z}[\sqrt{m}]$ are extensions of the integers $\mathbb{Z}$. ◊

Example 1.1.18. Not every subset S of a ring R which is a ring with respect to the induced operations is a subring, since possibly $1_S \neq 1_R$. If R is a non-trivial ring and S is trivial, then we find $1_S = 0_S = 1_S \neq 0_R$. Hence, the trivial ring is never a subring of a field. A less obvious example is $R = \mathbb{Z}/6\mathbb{Z}$ and $S = \{0, 2, 4\}$, with $0_S = 0 \pmod 6$ and $1_S = 4 \pmod 6$. ◊

Example 1.1.19 (Prime subring)**.** Let R be a ring and Ω the set of all subrings of R. Then

$$S := \bigcap_{R' \in \Omega} R' = \{x \in R \mid x \in R' \text{ for all } R' \in \Omega\}$$

is a subring of R. It is the smallest one in the sense that it is a subring of every subring $R' \in \Omega$ of R. This subring is called the *prime subring* of R. Moreover if R is a field and Ω is the set of all subfields of R, then S is a field called the *prime subfield* of R. ◊

Example 1.1.20 (Field of fractions)**.** Let R be a subring of a field F and let $\Omega(R)$ be the set of all subfields K of F which contain R (the assumption of the existence of such a field F is non-trivial and in section 2 we will determine which rings are subrings of a field). Then

$$Q_F(R) := \bigcap_{K \in \Omega(R)} K = \{x \in F \mid x \in K \text{ for all } K \in \Omega(R)\}$$

is a subfield of F. This field is called the *(relative) field of fractions of* R. To be more explicit, the field of fractions of R in F is given by

$$Q := \{x \in F \mid x \in R \text{ or } 1/x \in R\}.$$

From the fact $x \in Q$ if and only if $1/x \in Q$, it is easily verified that Q is a subfield of F containing R. Hence $Q_F(R) \subseteq Q$. On the other hand suppose that $x \in Q$. If $x \in R$ then $x \in Q_F(R)$. If $x \notin R$, then $1/x \in R \subseteq Q_F(R)$. But since $Q_F(R)$ is a field we conclude $x = 1/(1/x) \in Q_F(R)$. Therefore $Q_F(R) = Q$.

The field of fractions of R in F is independent of F in the following sense: if F and F' are fields containing R, then $Q_F(R) \cong Q_{F'}(R)$. Indeed the map defined by $x \mapsto x$ if $x \in R$ and $x \mapsto 1/(1/x)$ for $x \notin R$ is an isomorphism.

The proof of Theorem 1.2.5 shows that there is a canonical choice for the field F containing R. Then $Q_F(R)$, for this F, is called the *field of fractions* of R and is denoted by $Q(R)$. ◊

The following example shows that it is possible to do some arithmetic with subrings. This will be applied to ideals in section 1.4.

Example 1.1.21 (Subring arithmetic)**.** Let S and T be subrings of a ring R. Then

$$S + T := \{s + t \mid s \in S \text{ and } t \in T\},$$

$$ST := \{\textstyle\sum_{i=1}^{k} s_i t_i \mid k \geq 1 \text{ and } s_i \in S, t_i \in T\},$$

$$S \cap T := \{r \in R \mid r \in S \text{ and } r \in T\},$$

are subrings of R called the *sum*, the *product* (or *compositum*) and the *intersection* of S and T respectively. ◊

Example 1.1.22. Let $f : R \to S$ be a homomorphism of rings. Then the kernel $\ker(f)$ is a subring of R and the image $f(R)$ is a subring of S. Moreover the kernel $\ker(f)$ is an ideal of R (c.f., Example 1.1.7). Hence we are able to define the factor ring $R/\ker(f)$. ◊

1.2. Integral domains

The structure of a ring allows us to determine the product of any two elements. The following definition inverts this process.

Definition 1.2.1 (Factorizations)**.** Let R be a ring and $x \in R$. A *factorization of x in R* is a sequence $x_1, \ldots, x_n$ of elements in R for some integer $n \geq 1$ such that $x = x_1 \cdots x_n$. In this case we say that x_i is a *factor of x* or that x_i *divides x* (notation: $x_i \mid x$) for all $1 \leq i \leq n$. △

In this section we investigate the factorizations of 0. We clearly find a whole list of factorizations which have a factor 0, which we will call the *trivial* factorizations of 0. There is no reason to assume that all factorizations of 0 are trivial.

Example 1.2.2. In the ring $\mathbb{Z}/4\mathbb{Z}$ we have the equality $2 \times 2 \equiv 0$ modulo 4 (c.f., Example 1.1.6). ♢

Now suppose we have a non-trivial factorization of 0. The factors in such a factorization are special and deserve a name:

Definition 1.2.3 (Zero divisors)**.** An element $x \neq 0$ in a ring R is a *zero divisor* if and only if there exists a $0 \neq y \in R$ such that $xy = 0$. △

We will show that the absence of zero divisors is related to fields. Let us first introduce some terminology:

Definition 1.2.4 (Integral domain)**.** A ring R is called an *integral domain* if and only if

1) R is non-trivial;

2) R has no zero divisors. △

It turns out that integral domains are exactly the rings used in the assumption in Example 1.1.20. Hence the relation between integral domains (or the absence of zero divisors) and fields is given by the following:

Theorem 1.2.5. *Let R be a ring. Then there exists a field F such that F/R is a ring extension if and only if R is an integral domain.*

Proof. Suppose there exists an extension F/R, with F a field. We will show that there are no zero divisors in F hence neither in R. By definition 0 is not a zero divisor. Let a be non-zero zero divisor. Then by definition of a field, there are $0 \neq b, c \in R$ such that $ba = 0$ and $ac = 1$. Hence $0 = 0 \cdot c = bac = b \cdot 1 = b$, which contradicts $b \neq 0$. This proves the claim. Furthermore note that R is non-trivial since $1 \neq 0$ in F and hence in R by definition of a subring. Therefore R is an integral domain.

Suppose R is an integral domain. For all $(r, s), (r', s') \in R \times (R - \{0\})$ we define: $(r, s) \sim (r', s')$ if and only if $rs' = r's$. This defines an equivalence relation on $R \times (R - \{0\})$ and the equivalence class of (r, s) is denoted by $\frac{r}{s}$. Consider the set

$$Q := \{\tfrac{r}{s} \mid r, s \in R \text{ and } s \neq 0\}$$

with addition and multiplication defined by

$$\tfrac{r}{s} + \tfrac{r'}{s'} = \tfrac{rs'+r's}{ss'}, \quad \text{and} \quad \tfrac{r}{s} \cdot \tfrac{r'}{s'} = \tfrac{rr'}{ss'}.$$

Note that the product is well defined, because R does not have zero divisors. It is easily seen that Q is a field. Now let F be a set which contains R and $f : F \to Q$ be a bijection such that $f(r) = \frac{r}{1}$ for all $r \in R$. Then define addition and multiplication on F as follows:

$$x \oplus y = f^{-1}(f(x) + f(y)), \quad \text{and} \quad x \odot y = f^{-1}(f(x) \cdot f(y)).$$

Then clearly F field and f is a homomorphism. Moreover F/R is a ring extension as $\oplus$ and $\odot$ coincide with the given addition and multiplication in R. □

Corollary 1.2.6. *Every field is an integral domain.*

Proof. Apply Theorem 1.2.5 for the trivial field extension. □

The converse is not true in general. However we do have the following:

Proposition 1.2.7. *Every finite integral domain is a field.*

Proof. Let R be a finite integral domain. Then it suffices to show that every non-zero r in R is invertible, since R is already non-trivial. Consider the ring homomorphism $\phi_r : R \to R$ given by $x \mapsto rx$. The kernel of ϕ_r is trivial, since R is an integral domain and r is non-zero. Therefore ϕ_r is injective. Now, since R is a finite ring, we can conclude that ϕ_r is also surjective. Hence we find some $s \in R$ with $rs = \phi_r(s) = 1$. This implies that R is a field. □

1.3. Unique factorization domains

Now we are going to examine the the existence and uniqueness of a factorization of a non-zero element x of an integral domain R. Recall that we restrict our attention to integral domains as we are studying diagram (1.1) on page 3, where the rings are subrings of a field extenstion.

Units. The existence of a factorization of x is trivial, as x is a factorization of x. We call this the *trivial* factorization. Uniqueness however does not hold. Clearly, as our rings are commutative (c.f., property 5 of Definition 1.1.1), the order of the factors is irrelevant. Moreover we have that 1 and $(-1)\cdot(-1\cdot 1)$ are two factorizations of 1 of different length. More general if u divides 1 (i.e., $uv = 1$ for some v), then both x and $u(vx)$ are factorizations of x. Hence divisors of 1 are special.

Definition 1.3.1 (Units)**.** An element x of an integral domain R is called a *unit* if and only if x divides 1. The set $R^\times$ of all units is called the *unit group* of R. △

It is easily seen that unit group is indeed a group with the induced multiplication of R.

Example 1.3.2. The unit group of the integers $\mathbb{Z}$ is given by $\mathbb{Z}^\times = \{-1, 1\}$ and the unit group of rationals $\mathbb{Q}$ is given by $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$. Generally, the unit group of a field F is given by $F^\times = F - \{0\}$. ♢

In the case of finite fields, the unit group has a simple structure:

Theorem 1.3.3. *The multiplicative group of a finite field is a cyclic group.*

Proof. Let F be a finite field of order q. Then $F^\times$ has order $q - 1$. Let m be the maximal order of the elements of $F^\times$. Then all elements of $F^\times$ are roots of $X^m - 1$, hence $m \geq q - 1$. Lagrange theorem implies that $m \mid (q - 1)$, so we have $m = q - 1$. Therefore $F^\times$ is cyclic. □

Despite the non-uniqueness of a factorization in a strict sense we may consider factorizations up to units, i.e., we want to consider the factorizations x and $u(vx)$ to be equal. The following definition enables us to make this precise.

Definition 1.3.4 (Associates)**.** Let x and y be non-zero elements of an integral domain R. Then x and y are called *associates* in R if and only if x/y is a unit in R. △

Notice that the notion of associates is an equivalence relation on R.

Definition 1.3.5. Let $p = x_1, \ldots, x_n$ and $q = y_1, \ldots, y_m$ be two factorizations of some element x in an integral domain R. Then we call p and q *identical (up to ordening and units)* if and only if for each non-unit x_i there exists an y_j such that x_i and y_j are associates in R. △

Now the factorizations x and $u(vx)$ are indeed identical.

Irreducibles. Given a non-zero non-unit element x of an integral domain R. Consider the following process of finding factorizations of x in R.

Let y be a factor of x. If y is a unit, then $y(x/y)$ a trivial factorization since it is identical to x. If however y is not a unit, then $y(x/y)$ and x are non-identical factorizations of x. We may repeat this process for each factor of this new factorization to obtain more and more factorizations of x which longer than the previous one.

This process stops precisely when every factor in the longest factorization of x has no non-trivial factorization. Then such factors are the most primitive factors of x and deserve a name.

Definition 1.3.6 (Irreducible elements)**.** An element x of an integral domain R is called *irreducible* if and only if x is a non-zero non-unit element and $y \mid x$ implies that $y = x$ or y is a unit for all y in R. △

Let us now discuss some examples.

Example 1.3.7. The irreducible elements of $\mathbb{Z}$ are of the form $\pm p$, with p a prime number. ◊

Example 1.3.8. The elements 3, 7 and $4 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$. We will show this by using the group homomorphism

$$\mathrm{N} : \mathbb{Z}[\sqrt{-5}]^\times \to \mathbb{Z}^\times \qquad a + b\sqrt{-5} \mapsto a^2 + 5b^2$$

This map is called the *norm map*, since it coincides with the norm $z \mapsto z\bar{z}$ on $\mathbf{C}$. Furthermore $\mathrm{N}(z) = 1$ implies $z\bar{z} = 1$. Therefore z is a unit in $\mathbb{Z}[\sqrt{-5}]$.

Suppose that $3 = \alpha\beta$ for some non-unit $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Then $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(3) = 3^2$ implies that $\mathrm{N}(\alpha), \mathrm{N}(\beta) \in \{1, 3, 9\}$. Furthermore $\mathrm{N}(\alpha) \neq 1 \neq \mathrm{N}(\beta)$, since α and β are non-units. Therefore $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 3$. But there are no elements of norm 3, since $a^2 + 5b^2 = 3$ has no integer solution: if $b = 0$, then 3 is a square and if $b \neq 0$ then $a^2 + 5b^2 \geq 5$. This shows that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

In similar fashion it is shown that 7 and $4 \pm \sqrt{-5}$ are irreducible. ◊

Unique factorization. There is no guarantee that the above process of finding new factorizations will stop at some point, because some elements are infinite divisible:

Definition 1.3.9. Let x be a non-zero non-unit element of an integral domain R. Then x is called *infinite divisible* if and only if there exists a sequence $(x_n)_{n\in\mathbb{N}}$, such that $x_0 = x$ and x_{n+1} is a non-trivial factor of x_n for all n in $\mathbb{N}$. △

Example 1.3.10. Let $R = \mathbb{Z}[x_0, x_1, x_2, \ldots]$ be the ring of polynomial expressions in the x_i with coefficients in $\mathbb{Z}$ and and let $\mathfrak{a} = (x_1 - x_0^2)R + (x_2 - x_1^2)R + \ldots$ be the ideal generated by the expressions $x_{i+1} - x_i^2$, for all $i \geq 0$. Consider the factor ring $R/\mathfrak{a}$ (see Example 1.1.7). Then x_0 is *infinite divisible* in $R/\mathfrak{a}$, because x_0 is a non-zero non-unit element and $x_0 = x_i^{2i}$ for all $i \geq 0$, where x_i is a non-zero non-unit element of $R/\mathfrak{a}$. ◊

There is also no guarantee that the above process of finding new factorizations leads to a unique factorization.

Example 1.3.11. We will show that in $\mathbb{Z}[\sqrt{-5}]$ we have

$$3 \cdot 7 = 21 = (4 + \sqrt{-5})(4 - \sqrt{-5}),$$

with 3, 7 and $4 \pm \sqrt{-5}$ pairwise non-associate irreducible elements.

By Example 1.3.8 we see that these elements are indeed irreducible. Furthermore the norms of 3, 7 and $4+\sqrt{-5}$ are respectively 9, 49 and 21. Therefore these elements are pairwise non-associate. Then norm of $4 - \sqrt{-5}$ is 21, hence it could only be an associate of $4 + \sqrt{-5}$. However

$$\frac{4 + \sqrt{-5}}{4 - \sqrt{-5}} = \frac{(4 + \sqrt{-5})^2}{21} = \frac{11}{21} + \frac{8}{21}\sqrt{-5}$$

is not in $\mathbb{Z}[\sqrt{-5}]^\times$. Therefore $4 + \sqrt{-5}$ and $4 - \sqrt{-5}$ are non-associate. ◊

If the process process of finding new factorizations stops at some point and leads to a unique factorization, then every element is generated by units and the irreducible elements. Therefore the units and the irreducible elements form the building blocks for all elements of the ring in the following type of rings:

Definition 1.3.12 (Unique factorization)**.** An integral domain R is called a *unique factorization domain* if and only if for all non-zero x in R

1) there exists a factorization of x into irreducibles;

2) any two factorizations of x into irreducibles are identical. △

Notice that unique factorization alone is not a sufficient condition to exclude zero divisors.

Example 1.3.13. In $\mathbb{Z}/4\mathbb{Z}$, 1 and 3 are units and 2 is not a unit. Furthermore 1×2 and 2×3 are all factorizations of 2. Thus $\mathbb{Z}/4\mathbb{Z}$ has unique factorization and is not an integral domain. ◊

Primes. There is one last property of an element we want to mention.

Definition 1.3.14 (Prime elements)**.** An element x in an integral domain R is called *prime* if and only if x is a non-zero non-unit element of R and $x \mid ab$ implies $x \mid a$ or $x \mid b$ for all a and b in R. △

In a unique factorization domain, property of being irreducible and the property of being prime coincides. In fact, this equivalence almost determines a unique factorization domain.

Theorem 1.3.15. *Let R be an integral domain. Then R is a unique factorization domain if and only if for all non-zero non-unit x in R*

1) x is not infinite divisible;

2) x prime if and only if x is irreducible.

Proof. Suppose that R is a unique factorization domain. Let x be an arbitrary non-zero non-unit element of R. Since x admits a factorization into irreducibles, x is not infinite divisible. Suppose that x is prime and $x = ab$. Then $x \mid a$ or $x \mid b$. Hence we find that either $1 = (a/x)b$ or $1 = a(b/x)$ or equivalently a or b is a unit. This shows that x is irreducible. Suppose that x is irreducible and $x \mid ab$. Then there is some c with $cx = ab$. Hence by the uniqueness of the factorization x is associate to a or b. Therefore $x \mid a$ or $x \mid b$, which means that x is prime.

Suppose R is an integral domain such that x is not infinite divisible and x prime if and only if x is irreducible for all non-zero non-unit x in R. Then every x in R admits a factorization into irreducibles as the process described at the beginning of the paragraph terminates after finitely many steps. Hence it suffices to show that this factorization is unique. Let $a_1 \cdots a_n$ and $b_1 \cdots b_m$ be two factorizations of x into irreducibles. Then for every irreducible a_i we have that $a_i \mid b_1 \cdots b_m$. This implies that $a_i \mid b_j$, since a_i is prime by the assumption on R. Now a_i and b_j are associates, because they are irreducible. We conclude that the factorization of x is unique. □

1.4. Ideals

In Example 1.1.7 we introduced the notion of an ideal. In this section we will view them as generalizations of elements of a ring. Then our goal is to translate every property about elements into a property about ideals. We will tackle properties like irreducibility and primeness. In section 1.5 we will translate the property of infinite divisibility to ideals.

However, in some integral domains we are able to prove unique factorization of ideals. These integral domains are called Dedekind domains. Those will be discussed in section 1.10, where we will show that ideals generalize elements of an integral domain and that ideals admit some arithmetic.

Principal ideal domains. Let us first recall the definition of an ideal, as it is such an important object.

Definition 1.4.1 (Ideals)**.** A subring $\mathfrak{a}$ of an integral domain R is an *ideal* if and only if $R\mathfrak{a} = \mathfrak{a}$. △

In this definition, $R\mathfrak{a}$ is the product of the subrings R and $\mathfrak{a}$ of R, which is defined in Example 1.1.21.

Let us now examine why ideals are generalizations of elements. First we show how to construct ideals.

Definition 1.4.2 (Finitely generated ideals)**.** Let R be an integral domain and $x_1, \ldots, x_n \in R$, with $n \geq 1$ an integer. Then the *ideal generated by* $x_1, \ldots, x_n$ is the set

$$(x_1, \ldots, x_n) := \{r_n x_n + \cdots + r_n x_n \mid r_i \in R\}.$$

For $n = 1$, this ideal is called a *principal ideal*. △

Clearly every element x in an integral domain R gives rise to a principal ideal (x) and by definition every principal ideal comes from some generator x in R. In general it is not true that every ideal is principal. However, in some rings, every ideal is principal:

Example 1.4.3. Let $\mathfrak{a}$ be an ideal in $\mathbb{Z}$. Then $\mathfrak{a} = (a)$ for some $a \in \mathbb{Z}$. Indeed, let $a > 0$ be the smallest positive element of $\mathfrak{a}$ and let $x \in \mathfrak{a}$ be arbitrary. Then division with remainder yields $x = qa + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < a$. Notice that $r = x - qa \in \mathfrak{a}$, hence by the minimality of a we conclude that $r = 0$. Thus $x \in (a)$ and $\mathfrak{a} \subseteq (a)$. Since trivially $(a) \subseteq \mathfrak{a}$, we conclude that $\mathfrak{a} = (a)$. ◊

In this example we conclude that elements in $\mathbb{Z}$ are just as general as ideals in $\mathbb{Z}$. This is a property of the ring $\mathbb{Z}$ which may be formulated as follows:

Definition 1.4.4 (Principal ideal domain)**.** A ring R is called a *principal ideal domain* if and only if R is an integral domain and every ideal in R is principal. △

We may wonder whether every integral domain is a principal ideal domain. This is not always the case.

Example 1.4.5. Consider the ideal $(2, X) \subseteq \mathbb{Z}[X]$. Suppose $(2, X) = (f)$ with $f \in \mathbb{Z}[X]$. Since $2 \in (2, X)$ we find $g \in \mathbb{Z}[X]$ with $2 = fg$. Hence $0 = \deg(2) = \deg(fg) = \deg(f) + \deg(g)$, which implies that $\deg(f) = \deg(g) = 0$, because $\deg(f), \deg(g) \geq 0$. Thus f, g are divisors of 2 in $\mathbb{Z}$. Note that $1 \notin (2, X)$ and hence $f \neq 1$, as every $h \in (2, X)$ satisfies $h(0) \equiv 0$ modulo 2. Furthermore $f \neq 2$, since otherwise $X \notin (2) = (2, X)$. This gives a contradiction which shows that $(2, X)$ is not principal. ◊

Example 1.4.6. Theorem 1.5.6 together with Example 1.3.11 show that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. ◊

Ideal arithmetic. By definition, elements in a ring admit some arithmetic, that is, we are able to add and multiply and talk about divisibility. Using Example 1.1.21, we are able to define arithmetic for ideals:

Definition 1.4.7 (Ideal arithmetic)**.** Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of an integral domain R. The sum $\mathfrak{a} + \mathfrak{b}$ and *product* $\mathfrak{ab}$ of $\mathfrak{a}$ and $\mathfrak{b}$ are defined as

$$\begin{aligned} \mathfrak{a} + \mathfrak{b} &:= \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}, \\ \mathfrak{ab} &:= \{a_1 b_1 + \cdots + a_k b_k \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}. \end{aligned}$$

We say that $\mathfrak{b}$ *divides* $\mathfrak{a}$ (notation: $\mathfrak{b} \mid \mathfrak{a}$) if and only if $\mathfrak{b} \supseteq \mathfrak{a}$. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime if and only if $\mathfrak{a} + \mathfrak{b} = R$. △

Remark that this definition of divisibility makes some sense: if there exists an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{bc}$ then $\mathfrak{b} \mid \mathfrak{a}$, because $\mathfrak{b}$ is an ideal. It is however not at all clear that the converse holds. In section 1.10 we will see that the converse is true for Dedekind domains.

The following example shows that for principal ideals the above arithmetic coincides with the arithmetic of elements.

Example 1.4.8. Let x and y be elements of an integral domain R. Then we have $(x)(y) = (xy)$. Therefore multiplication of ideals generalizes the multiplication of elements.

The sum however does not generalize in this way. The ideal $(x) + (y) = (x, y)$ need not be principal (c.f., Example 1.4.5). In some other integral domains the sum is principal for all x and y. Such integral domains are called Bèzout domains (e.g., a principal ideal domain). Take for example $R = \mathbb{Z}$ in which every ideal is principal. In such rings we find $(x) + (y) = (d)$, with $d = ax + by$ for some $a, b \in R$. Note that if r divides both a and b, then r divides d. Hence d is a multiple of the greatest common divisor of a and b. On the other hand $(x), (y) \subseteq (d)$ which means that d is a common divisor of x and y. Hence d is the greatest common divisor. This shows that, in the case that $(x) + (y)$ is principal, $(x) + (y) = R$ is equivalent to stating that x and y are coprime.

For the divisibility, suppose that (y) divides (x). Then $(x) \subseteq (y)$, hence $x = ry$ for some $r \in R$. Then clearly we find $(x) = (r)(y)$. Hence the notion of divisibility for ideals generalizes the divisibility for elements. ♢

Chinese remainder theorem. We will now turn our attention to coprime ideals. The following lemma gives an explicit description of the product of coprime ideals.

Lemma 1.4.9. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals of an integral domain R. Then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.*

Proof. Since $\mathfrak{a}$ and $\mathfrak{b}$ are both ideals, we have $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Since $\mathfrak{a}$ and $\mathfrak{b}$ be coprime we have $\mathfrak{a} + \mathfrak{b} = R$, i.e., there are a in $\mathfrak{a}$ and b in $\mathfrak{b}$ with $1 = a + b$. Hence for all $c \in \mathfrak{a} \cap \mathfrak{b}$ we find that $c = 1 \cdot c = ac + bc \in \mathfrak{ab}$. We conclude that $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$ and hence $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. □

We will now apply Lemma 1.4.9 in order to derive the following theorem.

Theorem 1.4.10 (Chinese remainder theorem)**.** *Let $n \geq 1$ an integer and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise coprime proper ideals in an integral domain R, i.e., $\mathfrak{a}_i + \mathfrak{a}_j = R$ for $i \neq j$. Then*

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_n \cong R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

Proof. Consider the map $\pi : R \to \prod_{j=1}^{n} R/\mathfrak{a}_j$ given by $a \mapsto (a + \mathfrak{a}_i)_{i=1}^{n}$. The factor groups $R/\mathfrak{a}_i$ are well-defined, since $\mathfrak{a}_i$ is a proper ideal. We will show that π is surjective. Let $(a_i + \mathfrak{a}_i)_{i=1}^{n}$ be an element in the codomain. It suffices to construct $c_i \in R$ with $c_i \equiv 1$ modulo $\mathfrak{a}_i$ and $c_i \equiv 0$ modulo $\mathfrak{a}_j$, for $j \neq i$. Indeed, then $a := \sum_{i=1}^{n} a_i c_i$ is mapped to $(a_i + \mathfrak{a}_i)_{i=1}^{n}$ under π, as $a \equiv \sum_{i=1}^{n} a_i c_i \equiv a_j$ modulo $\mathfrak{a}_j$ for all j. Given i, we find $x_j \in \mathfrak{a}_i$ and $y_j \in \mathfrak{a}_j$ with $x_j + y_j = 1$ for all $j \neq i$, because $\mathfrak{a}_i + \mathfrak{a}_j = R$. Hence we find $\prod_{j \neq i}(x_j + y_j) = 1$. If we expand the product we see that every term is, except $c_i = \prod_{j \neq i} y_j$, contained in $\mathfrak{a}_i$. Hence $c_i \equiv \prod_{j \neq i}(x_j + y_j) = 1$ modulo $\mathfrak{a}_i$ and $c_i \equiv 0$ modulo $\mathfrak{a}_j$, for $j \neq i$. We conclude that π is surjective.

The kernel of π is the set of $a \in R$ with $a \equiv 0$ modulo $\mathfrak{a}_i$ or equivalently $a \in \mathfrak{a}_i$, for all i. Hence $\ker(\pi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$. With induction on Lemma 1.4.9, we find that $\ker(\pi) = \bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. The theorem now follows from the first isomorphism theorem. □

Prime and maximal ideals. In section 1.3 we studied some basic types of elements: units, irreducibles and primes. We have seen above that ideals generalize elements, as elements correspond with principal ideals. A principal ideal (u) generated by a unit u in R contain 1 and hence $(u) = R$ is not proper. Therefore non-units correspond with proper principal ideals.

Definition 1.3.6 can be translated to the language of ideals as follows:

Definition 1.4.11 (Maximal ideals)**.** An ideal $\mathfrak{a}$ of a ring R is called *maximal* if and only if $\mathfrak{a}$ is non-zero proper ideal and $\mathfrak{b} \mid \mathfrak{a}$ implies $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = R$ for all ideals $\mathfrak{b}$. △

If we dissect this definition by using the definition of division and proper we see that an ideal $\mathfrak{a}$ of a ring R is maximal if and only if $(0) \neq \mathfrak{a} \neq R$ and $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$

implies $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = R$ for all ideals $\mathfrak{b}$. This explains where the term maximal comes from.

In other texts it is not assumed that a maximal ideal is non-zero. However this condition is automatic when R is not a field: if R is not a field, then there exists a non-zero non-unit element x in R. Hence (0) is not maximal, since $(0) \subsetneq (x) \subsetneq R$.

The following lemma shows that, in a principal ideal domain, maximal ideals are the correct translations of irreducibles.

Lemma 1.4.12. *Let R be a principal ideal domain. Then x is irreducible if and only if (x) is maximal.*

Proof. It is trivial that x is irreducible whenever (x) is maximal. Suppose that x is irreducible. Let $\mathfrak{b}$ be a proper ideal with $\mathfrak{b} \mid (x)$. Since R is a principal ideal domain, we find some b with $(b) = \mathfrak{b}$. Then b is a non-zero non-unit element of R, because $\mathfrak{b}$ is non-zero and proper. Furthermore we have $(b) \mid (x)$, hence we find some a with $x = ab$. But x is irreducible, hence a is a unit. This shows that $(x) = (ab) = (b) = \mathfrak{b}$. We conclude that (x) is maximal. □

The following theorem gives a nice tool to prove that a proper ideal is maximal.

Theorem 1.4.13. *Let $\mathfrak{a}$ be a non-zero proper ideal of a ring R. Then $\mathfrak{a}$ is maximal if and only if $R/\mathfrak{a}$ is a field.*

Proof. The assumption that $\mathfrak{a}$ is proper coincides with $R/\mathfrak{a}$ being non-trivial. The projection $\pi : R \to R/\mathfrak{a}$ induces a map between the ideals that contain $\mathfrak{a}$ and the ideals of $R/\mathfrak{a}$. Hence $\mathfrak{a}$ is maximal if and only if $\{0+\mathfrak{a}\}$ and $R/\mathfrak{a}$ are the only ideals of $R/\mathfrak{a}$. Thus if $R/\mathfrak{a}$ is a field, then $\mathfrak{a}$ is maximal. On the other hand, suppose that $\mathfrak{a}$ is maximal. If $x+\mathfrak{a}$ is a zero divisor, then $x+\mathfrak{a}$ is not a unit. Hence $(x+\mathfrak{a}) \neq R/\mathfrak{a}$ and $x + \mathfrak{a} \in (x + \mathfrak{a}) = \{0 + \mathfrak{a}\}$. Thus $R/\mathfrak{a}$ has no zero divisors. Therefore $R/\mathfrak{a}$ is a field. □

We now turn our attention to the generalizations of prime elements. Definition 1.3.14 generalizes as follows:

Definition 1.4.14 (Prime ideals)**.** An ideal $\mathfrak{p}$ of a ring R is called *prime* if and only if $\mathfrak{p}$ is a non-zero proper ideal and $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. △

The following lemma gives another characterization of prime ideals. Other texts use this as a definition.

Lemma 1.4.15. *Let $\mathfrak{a}$ be a non-zero proper ideal of a ring R. Then $\mathfrak{p}$ is prime if and only if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for all $x, y \in R$.*

Proof. If $\mathfrak{p}$ is prime, then for all $x, y \in R$ we have that $xy \in \mathfrak{p}$ or equivalently $\mathfrak{p} \mid (xy) = (x)(y)$ implies $\mathfrak{p} \mid (x)$ or $\mathfrak{p} \mid (y)$ or equivalently $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

On the other hand, suppose that $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ for all $x, y \in R$. Suppose that $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$. If $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p} \nmid \mathfrak{b}$, then there exists a in $\mathfrak{a}$ and b in $\mathfrak{b}$ with $a, b \notin \mathfrak{p}$. But since $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, we have a contradiction. This shows that either $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. □

The following lemma shows that, in a principal ideal domain, prime ideals generalize prime elements.

Lemma 1.4.16. *Let R be a principal ideal domain. Then x is prime if and only if (x) is prime.*

Proof. Using Lemma 1.4.15 we see that (x) is prime if and only if $ab \in (x)$ implies $a \in (x)$ or $b \in (x)$. Since $y \in (x)$ if and only if $x \mid y$, the lemma follows. □

Now we have the following:

Theorem 1.4.17. *Let $\mathfrak{a}$ be a non-zero proper ideal of a ring R. Then $\mathfrak{a}$ is prime if and only if $R/\mathfrak{a}$ is an integral domain.*

Proof. The assumption that $\mathfrak{a}$ is proper coincides with $R/\mathfrak{a}$ being non-trivial and the assumption that $\mathfrak{a}$ is prime coincides, using Lemma 1.4.15, with $R/\mathfrak{a}$ not having any zero divisors. □

If we now combine Theorem 1.4.17 and Theorem 1.4.13 with Theorem 1.2.6 we find the following corollary.

Corollary 1.4.18. *Every maximal ideal is a prime ideal.*

The converse is not true in general. However if we apply Proposition 1.2.7 we conclude the following:

Corollary 1.4.19. *Every non-zero prime ideal in a finite ring is maximal.*

1.5. Noetherian domains

Eventually we want to reformulate the definition of a unique factorization domain into the language of ideals. As seen in section 1.3 we need to exclude ideals which are infinite divisible and also show that factorization of ideals is unique. In this section we will tackle the first property.

We first introduce a new notion. An *(ascending) chain* C of ideals in a ring R is a sequence $(\mathfrak{a}_n)_{n\in\mathbb{N}}$ of ideals of R with $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ for all n in $\mathbb{N}$. A chain is called *stable* if and only if there exist some k in $\mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_k$ for all $n \geq k$. In this case we say that C *stabilizes* at k.

Definition 1.5.1 (Noetherian domains)**.** An integral domain R is *Noetherian* if and only if every chain is stable. △

There are multiple ways to define a Noetherian domain. The following proposition gives another characterization of Noetherian domain.

Proposition 1.5.2. *An integral domain R is Noetherian if and only if every non-zero ideal $\mathfrak{a}$ in R is finitely generated.*

Proof. Let R be an integral domain and $\mathfrak{a}$ an ideal of R. Suppose that R is Noetherian. Choose inductively $a_n \in \mathfrak{a} - (a_1, \ldots, a_{n-1})$ whenever $\mathfrak{a} \neq (a_1, \ldots, a_{n-1})$ or take $a_n = 0$ otherwise. We will show that we have made only finitely many choices (avoiding the axiom of choice). Consider the chain of ideals

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots \subsetneq (a_1, \ldots, a_n) \subsetneq \cdots \subseteq \mathfrak{a}$$

Since R is Noetherian, we find some k such that $(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1})$. This implies that $a_{k+1} = 0$ and that $\mathfrak{a} = (a_1, \ldots, a_k)$ is finitely generated.

On the other hand, suppose that every non-zero ideal in R is finitely generated. Let $(\mathfrak{a}_i)_{i\geq 0}$ be a chain of ideals in R. Then the union $\mathfrak{b} = \bigcup_{i\geq 0} \mathfrak{a}_i$ is clearly an ideal in R. By assumption it is finitely generated: $\mathfrak{b} = (b_1, \ldots, b_n)$. Find $k \geq 0$ such that $b_i \in \mathfrak{a}_k$ for all i. Then the chain stabilizes at k. □

A consequence of this definition is the following theorem:

Proposition 1.5.3. *Let R be a Noetherian domain. Then for every proper ideal $\mathfrak{a}$ there exists a maximal ideal $\mathfrak{m}$ such that $\mathfrak{m} \mid \mathfrak{a}$.*

Proof. Define $\mathfrak{a}_0 := \mathfrak{a}$ and $\mathfrak{a}_n := \mathfrak{a}_{n-1} + x_n R$, with $x_n \in R$ is chosen such that $\mathfrak{a}_{n-1} \subsetneq \mathfrak{a}_n \subsetneq R$ whenever possible and $x_n = 0$ otherwise, for all $n \geq 1$. Since R is Noetherian, we find some k such that $\mathfrak{a}_{k+1} = \mathfrak{a}_k$ for all $n \geq k$. Notice that we have made k choices, hence we did not use the axiom of choice. Define $\mathfrak{m} = \mathfrak{a}_k$ and let $\mathfrak{b}$ be a proper ideal of R with $\mathfrak{m} \subseteq \mathfrak{b} \subsetneq R$. Then for all $x \in \mathfrak{b}$ we have that $x \in \mathfrak{a}_k + xR = \mathfrak{a}_k = \mathfrak{m}$, because $\mathfrak{a}_{k+1} = \mathfrak{a}_k$. Thus $\mathfrak{b} = \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal which contains $\mathfrak{a}$. □

This proposition has an analog in terms of elements.

Proposition 1.5.4. *Let R be a Noetherian domain. Then for every non-unit element a there exists an irreducible element x such that $x \mid a$.*

Proof. Define $x_0 := a$ and for all $n \geq 1$ choose x_n to be a non-trivial factor of x_{n-1} whenever possible or define $x_n = x_{n-1}$ otherwise. Consider the chain $\mathfrak{a}_n := (x_n)$. Since R is Noetherian, we find some k such that $\mathfrak{a}_{k+1} = \mathfrak{a}_k$ for all $n \geq k$. Notice that we have made k choices, hence we did not use the axiom of choice. By construction and the fact that $\mathfrak{a}_{k+1} = \mathfrak{a}_k$ we conclude that x_k is irreducible. □

It is clear that in a Noetherian domain, no elements are infinite divisible because any sequence of non-trivial factors gives rise to a non-stable chain. Now Proposition 1.5.4 implies that in a Noetherian domain every element admits a factorization into irreducibles, whenever one accepts the *countable axiom of choice*.

Theorem 1.5.5. *Let R be a Noetherian domain. Then every non-zero non-unit element x of R admits a factorization into irreducibles.*

Proof. Let x be non-zero non-unit element of a Noetherian domain R. Define $x_0 := x$ and for every $n \in \mathbb{N}$ choose x_{n+1} such that $\pi_n := x_n/x_{n+1}$ is irreducible whenever x_n is neither zero nor a unit and $x_{n+1} = 1$ otherwise. This is possible by Proposition 1.5.4, since there exist an irreducible $y \in R$ with $y \mid x_n$, whenever x_n is neither zero nor a unit. Then take $x_{n+1} = x_n/y$. Note that this definition requires the countable axiom of choice. Now consider the sequence $(x_0) \subseteq (x_1) \subseteq \cdots$. Then since R is Noetherian, we find that $(x_m) = (x_{m+1})$ for some $m \in \mathbb{N}$. Hence x_m/x_{m+1} is a unit, which implies that $x_{m+1} = 1$. Therefore $x = \pi_0 \cdots \pi_m$, where π_k is either irreducible or a unit. This induces a factorization of x into irreducibles. □

Theorem 1.5.6. *A principal ideal domain is a unique factorization domain.*

Proof. Let R be a principal ideal domain and let x in R. Using Proposition 1.5.2, we see that R is Noetherian. From the above discussion we conclude that x is not infinite divisible and admits a factorization into irreducibles. Hence it suffices to show that this factorization is unique.

Let $x_1 \cdots x_n$ and $y_1 \cdots y_m$ be two factorizations of x into irreducibles. and pick some x_i. Then $x_i \mid y_1 \cdots y_m$. By Lemma 1.4.12 we see that (x_i) is a maximal ideal, because R is a principal ideal domain. By Corollary 1.4.18 we conclude that (x_i) is a prime ideal. It is clear from the definition that x_i is now a prime element. This implies that $x_i \mid y_j$ for some y_j (using induction). Since x_i and y_j are both irreducible, they must be associate. □

To prove that some rings are Noetherian it may suffice to prove that some subring is Noetherian. To be more precise we have:

Theorem 1.5.7 (Hilbert basis theorem)**.** *Let R be a Noetherian domain. Then $R[X]$ is a Noetherian domain.*

Proof. From Proposition 1.5.2 we conclude that it suffices to show that every ideal non-zero $\mathfrak{a}$ is finitely generated. Let $\mathfrak{a}$ be a non-zero ideal in $R[X]$. Let f_1 be a non-zero polynomial of minimal degree in $\mathfrak{a}$. Choose inductively f_n to be a non-zero polynomial of minimal degree in $\mathfrak{a} - (f_1, \ldots, f_{n-1})$ whenever $\mathfrak{a} \neq (f_1, \ldots, f_{n-1})$ and take $f_n = 0$ otherwise. We will show that we have made only finitely many choices (avoiding the axiom of choice).

Let a_n be the leading coefficient and d_n be the degree of f_n. Then $d_n \leq d_m$ if $n < m$, because f_n has minimal degree. Consider the chain of ideals

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, \ldots, a_n) \subseteq \cdots$$

Since R is Noetherian we find some k with $(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1})$. Hence there exist $r_i \in R$ such that $a_{k+1} = r_1 a_1 + \cdots + r_k a_k$. Notice that the polynomial

$$g = f_{k+1} - \sum_{i=1}^{k} r_i X^{d_{k+1} - d_i} f_i$$

has degree less then d_{k+1} and is not contained in $(f_1, \ldots, f_k)$. This contradicts the minimality of the degree of f_{k+1}. Hence there does not exist $f_{k+1} \in \mathfrak{a} - (f_1, \ldots, f_k)$, which shows that $\mathfrak{a} = (f_1, \ldots, f_k)$. □

For future use we will show one more tool to prove that an integral domain is Noetherian.

Proposition 1.5.8. *Let $f : R \to S$ be a surjective ring homomorphism of integral domains. Then S is Noetherian whenever R is Noetherian.*

Proof. Let $(\mathfrak{a}_n)_{n\geq 0}$ be a chain of ideals in S. Then $f^{-1}(\mathfrak{a}_n)$ is an ideal for all n, since f is a homomorphism. Hence $(f^{-1}(\mathfrak{a}_n))_{n\geq 0}$ is a chain of ideals in R. But since R is Noetherian we find some k such that $f^{-1}(\mathfrak{a}_n) = f^{-1}(\mathfrak{a}_k)$ for all $n \geq k$. Now using that f is surjective we find for all n that $f(f^{-1}(\mathfrak{a}_n)) = \mathfrak{a}_n$. Therefore we conclude $\mathfrak{a}_n = f(f^{-1}(\mathfrak{a}_n)) = f(f^{-1}(\mathfrak{a}_k)) = \mathfrak{a}_k$ for all $n \geq k$. Thus S is Noetherian. □

1.6. Modules over a ring

In this section we recall the definition of a module and prove some elementary facts about them. This will be used to define fractional ideals in section 1.10 and it is used in section 2.1 to prove the finiteness of the class group.

A module is a generalization of a vector space, as the scalars of a module do not need to be a field.

Definition 1.6.1 (Modules)**.** A *module* over a ring R (or a *R-module*) is an abelian group M together with a group homomorphism $\phi : R \to \mathrm{End}(M)$ denoted by $r \mapsto \phi_r$. △

To see why this is really the definition of a vector space whenever R is a field, notice that addition of vectors is defined by the group structure on M and multiplication is defined by ϕ using the formula $rm := \phi_r(m)$ for all r in R and m in M. Indeed, associativity ($(m+n)+o = m+(n+o)$), commutativity ($m+n = n+m$), the identity element ($m+0 = m$) and the inverse elements of addition ($m+(-m) = 0$) are defined by the group structure on M. Distributivity of scalar multiplication over vector addition ($r(m+n) = rm + rn$ for all m) follows from the fact that ϕ_r is an endomorphism. Distributivity of scalar multiplication over field addition ($(r+s)m = rm + sm$), compatibility of scalar multiplication with field multiplication ($r(sm) = (rs)m$) and the identity element of scalar multiplication ($1m = m$) follow from the fact that ϕ is an homomorphism.

We list some examples of modules over a ring.

Example 1.6.2. Let R be a ring. Then both R and $\{0\}$ are modules over R. ◊

Example 1.6.3. Let M be an abelian group. Then M is a $\mathbb{Z}$-module by defining scalar multiplication by $k \cdot x = x + \cdots + x$ (k times). ◊

Example 1.6.4. Let R be a ring and $m, n \geq 1$ integers. Then the set $M(m \times n, R)$ of all $m \times n$-matrices (i.e., m rows and n columns) with coefficients in R and 'entry-wise' addition and scalar multiplication is an R-module. ◊

Just as we studied ring extensions and field extensions, we will now study extensions of models or dually submodules.

Definition 1.6.5 (Submodules)**.** Let $(M, +, \cdot, 0_M)$ and $(N, \oplus, \odot, 0_N)$ be modules over a ring R. Then N is a *submodule* of M if

1) $N \subseteq M$;

2) for all $r \in R$ and $x, y \in N$ we have $x \oplus y = x + y$ and $r \odot x = r \cdot x$;

3) $0_N = 0_M$. △

Note that the last item of this definition is redundant, since we have $x \oplus 0_N = x = x + 0_M = x \oplus 0_M$ for all x in N.

We list some examples of submodules.

Example 1.6.6. Let M be a module over a ring R. Then both M and $\{0\}$ are R-submodules of M. ◊

Example 1.6.7. Let R/S be an extension of rings. Then R and S are S-modules and S is a S-submodule of R. ◊

Example 1.6.8. Let M be a module over a ring R and let N_1 and N_2 be R-submodules of M. Then

$$N_1N_2 = \{n_1^1n_1^2 + \cdots + n_k^1n_k^2 \mid n_i^j \in N_j, k \geq 1\}$$

and

$$N_1 \cap N_2 = \{m \in M \mid m \in N_1, m \in N_2\}$$

are R-submodules of M. Note that N_1N_2 is the smallest R-submodule of M which contains both N_1 and N_2, while $N_1 \cap N_2$ is the largest R-submodule of M which is contained in both N_1 and N_2. ◊

The last important object we want to mention is the module homomorphisms, which generalizes the linear map.

Definition 1.6.9 (Module homomorphisms)**.** Let M and N be modules over a ring R. A group homomorphism $f : M \to N$ is a *R-module homomorphism* if and only if for all $r \in R$, $x \in M$

$$f(r \cdot x) = r \cdot f(x)$$ △

Rank of a module. For vector spaces we have the concepts of bases and dimensions. We will translate this to the language of modules. We first seek an analogue of a subset which spans the vector space.

Definition 1.6.10 (Generating subsets)**.** Let M be a module over a ring R and $A \subseteq M$ a subset. Then A is called a *generating subset* of M if and only if

$$M = RA := \{r_1a_1 + \cdots + r_ka_k \mid r_i \in R, a_i \in A\}.$$

A module is called *finitely generated* if and only if there exists some finite generating subset. △

Some generating subsets contain redundant elements in the sense that the subset stays a generating subset even when they are left out. Such minimal generating subsets are called bases:

Definition 1.6.11 (Module basis)**.** A generating subset A of a module M over a ring R is called a *basis* of M (plural: *bases*) if and only if $r_1a_1 + \cdots + r_ka_k = 0$ implies $r_1 = \cdots = r_k = 0$, for all $k \in \mathbb{N}$, $a_i \in A$ and $r_i \in R$. A module M is called *free* if and only if there exist a basis of M. △

The following definition generalizes the concept of dimension.

Definition 1.6.12 (Module rank)**.** Let M be a module and d a positive integer. Then d is called the *rank* of M (notation: $\operatorname{rank}(M)$) if and only if every basis of M has cardinality d. △

It is not clear from the definition whether the rank exists.

Theorem 1.6.13. *Let M be a finitely generated free module over a Noetherian ring R. Then M has a rank.*

Proof. See Corollary 4.3 on page 136 of [6]. □

Torsion free modules. Finally prove a theorem which is needed in section 2.1.

Theorem 1.6.14. *A finitely generated torsion free module over a principal ideal domain is free.*

Proof. Let X be a finite generating set of a torsion free module M over a principal ideal domain R. Let $B \subseteq X$ be a basis in X of maximal rank. Let $N = RB$ be the R-span of the basis B. Then N is a free submodule of M. Since B is of maximal rank there exist for all $x \in X$ some non-zero $r_x \in R$ such that $r_xx \in N$. Let $r = \prod_{x \in X} r_x$ and consider the left multiplication by r on M. Clearly this is an injective R-module homomorphism with $rM \subseteq N$. Hence by the first isomorphism theorem it suffices to show that rM is a free submodule of N. Write $B = \{b_1, \ldots, b_n\}$ and consider for all $1 \leq i \leq n$ the projection $\pi_i : N \to R$ given by $\sum_{k=1}^n r_kb_k \mapsto r_i$. This is an R-module homomorphism and thus $\pi_i(rM) \subseteq R$ is an ideal of R. Since R is a principal ideal domain we find $s_i \in R$ such that $\pi_i(rM) = s_iR$. Here $s_i \neq 0$, because $r = \pi_i(rb_i) \in \pi_i(rM)$ and $r \neq 0$. But now we conclude that $\{s_1b_1, \ldots, s_nb_n\}$ is a basis of rM, hence M is free. □

1.7. Integrally closed domains

We will now discuss a new construction, which is fruitfully used in section 2.1. We first introduce a property of extensions of integral domains.

Definition 1.7.1 (Integral extensions)**.** Let S/R be an extension of integral domains. An element $s \in S$ is called *integral* over R if and only if there exists a polynomial $f \in R[X]$ with f monic and $f(s) = 0$. Furthermore S/R is called *integral* if and only if every $s \in S$ is integral over R. △

This definition is very similar to the definition of the algebraic field extension from section 1.11. The next definition generalizes the relative algebraic closure of fields to integral domains.

Definition 1.7.2 (Integrally closed domains)**.** Let S/R be an extension of integral domains. Then R is called *integrally closed* in S if and only if every integral extension of R contained in S is trivial. We set $S = Q(R)$, whenever S is unspecified. △

The following theorem gives a whole class of examples of integrally closed domains.

Theorem 1.7.3. *Let R be a unique factorization domain. Then R is integrally closed.*

Proof. Let $x \in Q(R)$ be integral over R. Then there exists c_i such that $x^n = \sum_{i=0}^{n-1} c_i x^i$. Now write $x = r/s$, with r and s in R. Then we have that $r^n = \sum_{i=0}^{n-1} c_i x^i s^{n-i}$, which implies that s divides r^n. Since R is a unique factorization domain, we conclude that s is associate to r, which implies that $x \in R$. Therefore R is integrally closed. □

Let S/R be an extension of integral domains and consider the set

$$\tilde{R} = \{s \in S \mid s \text{ integral over } R\}.$$

Then the next theorem shows that $\tilde{R}$ is the smallest subring of S that contains R and is integrally closed in S.

Theorem 1.7.4. *Let S/R be an extension of integral domains. Then $\tilde{R}$ is an integrally closed subring of S. Moreover if T is an integrally closed subring of S that contains R, then $\tilde{R} \subseteq T$.*

Proof. For the first part see Proposition 5 at page 6 of [5]. For the second part, suppose that S is an integrally closed subring which contains R. Then for any $x \in \tilde{R}$ we have that x is integral over R, hence over $S \supseteq R$. Since S is integrally closed we conclude that $x \in S$. Thus $\tilde{R} \subseteq S$. □

1.8. Local domains

We now turn our attention to another type of integral domain.

Definition 1.8.1 (Local domains)**.** A integral domain R is called *local* if and only if R has an unique non-zero maximal ideal. △

Note that the fact that the maximal ideal is non-zero implies that a local ring is not a field. If we assume the axiom of choice, we have the following characterization of local rings.

Proposition 1.8.2. *A ring R is local if and only if the set of non-units is an ideal.*

Proof. Suppose that R is a local ring and let $\mathfrak{m}$ denote the unique non-zero maximal ideal. Then clearly $\mathfrak{m}$ consists of some non-units as $\mathfrak{m} \neq R$. Furthermore if x is a non-unit then $(x) \neq R$ is a proper ideal. Using the axiom of choice, one can construct a maximal ideal containing (x), which must be equal to $\mathfrak{m}$, as $\mathfrak{m}$ is unique. Hence we find $x \in \mathfrak{m}$. This proves the proposition. □

There is a canonical way to assign a local ring to any given ring with a given prime ideal.

Definition 1.8.3 (Localization)**.** Let $\mathfrak{p}$ be a prime ideal in an integral domain R. The *localization* of R at $\mathfrak{p}$ is the ring

$$R_{\mathfrak{p}} = \{x/y \in Q(R) \mid x \in R, y \in R - \mathfrak{p}\}. \qquad \triangle$$

Proposition 1.8.4. *Let $\mathfrak{p}$ be a prime ideal in an Noetherian integral domain R. Then the localization of R at $\mathfrak{p}$ is a local ring.*

Proof. The set of non-units in $R_{\mathfrak{p}}$ are precisely the elements x/y, with $x \in \mathfrak{p}$ and $y \in R - \mathfrak{p}$. This set is an ideal of $R_{\mathfrak{p}}$: if x_1/y_1 and x_2/y_2 are non-units, then both $x_1/y_1 - x_2/y_2 = (x_1y_2 - x_2y_1)/(y_1y_2)$ and $x_1/y_1 - x_2/y_2 = (x_1x_2)/(y_1y_2)$ are non-units. Proposition 1.8.2 now shows that $R_{\mathfrak{p}}$ is a local ring. $\square$

1.9. Valuation domains

Next we shall study a specific type of local ring, which will be of great importance for the following chapters. The terminology will be explained in section 2.5.

Definition 1.9.1 (Valuation domains)**.** An integral domain R is called a *valuation domain* if and only if $x \in R$ or $x^{-1} \in R$ for all x in the field of fractions $Q(R)$ of R. A valuation domain R is called *discrete* if and only if R is a principal ideal domain. $\triangle$

Example 1.9.2. Let π be an irreducible element of a Noetherian integral domain R. Then the localization $R_{(\pi)}$ is a valuation domain. Indeed, let $x/y \in Q(R)$ be arbitrary. Assume without loss of generelaty that x and y are coprime, i.e., $(x, y) = R$. If $x/y \notin R_{(\pi)}$, then π divides y. Hence π does not divide x, since x and y are coprime. Thus $y/x \in R_{(\pi)}$ which implies that $R_{(\pi)}$ is a valuation domain. $\Diamond$

Later on we will need the following properties of a valuation domains.

Proposition 1.9.3. *Let R be a valuation domain. Then*

1) R is a local domain;

2) R is integrally closed;

3) the ideals of R are totally ordered;

4) R is Noetherian if and only if R is discrete;

Proof. 1) We wish to apply Proposition 1.8.2. Let $\mathfrak{m}$ denote the set of non-units in R and let $a, b \in \mathfrak{m}$. Since R is a valuation domain we have $a/b \in R$ or $b/a \in R$. If $a/b \in R$, then $a + b = b(1 + a/b) \in \mathfrak{m}$, since otherwise $b \notin \mathfrak{m}$. Similarly if $b/a \in R$, then $a + b \in \mathfrak{m}$. Hence in both cases we find $a + b \in \mathfrak{m}$. If $r \in R$, then $ra \in \mathfrak{m}$ since otherwise $a \notin \mathfrak{m}$. Therefore $\mathfrak{m}$ is an ideal and R is a local ring.

2) Let $x \in K$ be integral over R. Then there exists $a_0, \ldots, a_{n-1} \in R$, $n \geq 1$, such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0.$$

Since R is a valuation domain we have $x \in R$ or $1/x \in R$. In the latter case we find from the above equation by multiplication by $(1/x)^{n-1}$ that

$$x = -a_{n-1} - \cdots - a_1(1/x)^{n-2} - a_0(1/x)^{n-1} \in R.$$

Therefore R is integrally closed.

3) Let $\mathfrak{a}, \mathfrak{b} \subseteq R$ be ideals. Then we have $\mathfrak{a} \subseteq \mathfrak{b}$ or there exists an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{b}$. In the latter case let $y \in \mathfrak{b}$. If $y = 0$, then $y \in \mathfrak{b}$. If $y \neq 0$ then $y/x \in \mathfrak{a}$, since otherwise $x = y(x/y) \in \mathfrak{b}$. Hence $y = x(y/x) \in \mathfrak{a}$. In both cases we find $y \in \mathfrak{a}$ hence $\mathfrak{b} \subseteq \mathfrak{a}$.

4) Trivially a principal ideal domain is Noetherian. Suppose that R is Noetherian and let $\mathfrak{a} \subseteq R$ be a non-zero ideal. Then there exists $a_1, \ldots, a_n$, $n \geq 1$, such that $\mathfrak{a} = (a_1, \ldots, a_n)$. Since the ideals of R are totally ordered we may renumber the a_i the obtain $(a_1) \subseteq \cdots \subseteq (a_n)$. Then $\mathfrak{a} = (a_1, \ldots, a_n) = (a_n)$, hence R is a principal ideal domain. $\square$

It turns out that valuation domains are strongly related to integral closures. The following proposition clarifies this connection.

Proposition 1.9.4. *Let R be a Noetherian subring of a field K, let $\{R_i\}_{i\in I}$ be the set of all valuation domains that contain R and $\tilde{R}$ the integral closure of R. Then $\tilde{R} = \bigcap_{i\in I} R_i$. Moreover R is integrally closed if and only if $R = \bigcap_{i\in I} R_i$.*

Proof. From the second item of Theorem 1.9.3 it follows that $\bigcap_{i\in I} R_i$ is integrally closed, as intersections of integrally closed rings are integrally closed. Using Proposition 1.7.4 and the construction of $\{R_i\}_{i\in I}$ we conclude that $\tilde{R} \subseteq \bigcap_{i\in I} R_i$.

On the other hand suppose $x \notin \tilde{R}$. Then $x \notin R[x^{-1}]$, since otherwise multiplication with a sufficient large power of x yields an integral relation for x over R. Therefore x is not a unit in R. We claim that $R[x^{-1}]$ is Noetherian. Indeed, since R is Noetherian we find that $R[X]$ is Noetherian. The surjectivity of the evaluation homomorphism then shows that $R[x^{-1}]$ is Noetherian. Therefore we apply Proposition 1.5.4 to find in $R[x^{-1}]$ an irreducible factor π of x^{-1}. Now let S denote the localization of $R[x^{-1}]$ at (π). Then S is a valuation ring, since (π) is principal. Furthermore $x = 1/x^{-1} \notin S$, as $x^{-1} \in (\pi)$. Finally R is clearly contained in S. Thus $S \in \{R_i\}_{i\in I}$ and $x \notin \bigcap_{i\in I} R_i$.

The last statement follows from Theorem 1.7.4. □

1.10. Dedekind domains

In section 1.4 we introduced the notion of an ideal and defined divisibility of ideals. We saw that this definition coincides with the usual definition, whenever the ring is a principal ideal domain, but we did not prove that if $\mathfrak{b} \mid \mathfrak{a}$ then there exists an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{bc}$ for all non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$. In this section we will study the rings for which this is true.

Fractional ideals. Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring R. We may form their product $\mathfrak{ab}$ which is the ideal consisting of all finite sums of products of elements of $\mathfrak{a}$ and $\mathfrak{b}$. Clearly the ideal R acts as the identity element: $\mathfrak{a}R = R\mathfrak{a} = \mathfrak{a}$. The set of ideals of R do not form a group under this multiplication, since we lack inverses.

Let us take a look at $R = \mathbb{Z}$ an let $\mathfrak{a}$ be a proper ideal which we try to invert. Let $\mathfrak{b}$ be an ideal such that $\mathfrak{ab} = \mathbb{Z}$. There are integers x and y such that $\mathfrak{a} = (x)$ and $\mathfrak{b} = (y)$, since $\mathbb{Z}$ is a principal ideal domain. We now have $\mathbb{Z} = \mathfrak{ab} = (xy)$. Therefore xy and hence x is a unit. This is impossible, since $\mathfrak{a}$ was chosen to be proper. Therefore no proper ideal of $\mathbb{Z}$ is invertible.

However, if we may choose $y = 1/x \in \mathbb{Q}$, then inverting is no problem. But now (y) is no longer an ideal (i.e., $\mathbb{Z}$-submodule) of $\mathbb{Z}$, but a $\mathbb{Z}$-submodule of $\mathbb{Q}$. Furthermore notice that not every $\mathbb{Z}$-submodule of $\mathbb{Q}$ is obtained this way, since we only find $\mathbb{Z}$-submodules $\mathfrak{b}$ of $\mathbb{Q}$ such that $x\mathfrak{b} \subseteq \mathbb{Z}$ for some $x \in \mathbb{Z}$. This excludes for example $\mathfrak{b} = \mathbb{Q}$.

This idea gives rise to the concept of fractional ideals.

Definition 1.10.1 (Fractional ideals)**.** Let R be a integral domain and K its field of fractions. A *fractional ideal* $\mathfrak{a}$ of R is a R-submodule of K such that $x\mathfrak{a} \subseteq R$ for some non-zero $x \in R$. △

If we wish to emphasize that an ideal R is not a fractional ideal, we will say that it is an *integral ideal*.

Dedekind domains. In general the set I_R of non-zero fractional ideals of R is still not a group.

Definition 1.10.2 (Dedekind domains)**.** Let R be an integral domain and I_R the set of non-zero fractional ideals of R. Then R is a *Dedekind domain* if and only if I_R is a group. △

Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero integral ideals of a Dedekind domain R and suppose that $\mathfrak{b} \mid \mathfrak{a}$. Then since $\mathfrak{b}$ is invertible, we find a fractional ideal $\mathfrak{b}^{-1}$ of R with $\mathfrak{c} := \mathfrak{ab}^{-1} \subseteq \mathfrak{bb}^{-1} = R$. Hence $\mathfrak{c}$ is an integral ideal with $\mathfrak{a} = \mathfrak{bc}$. This shows that in

a Dedekind domain we have $\mathfrak{b} \mid \mathfrak{a}$ if and only if there exists an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{bc}$, for all non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$.

The following theorem gives an equivalent definition of a Dedekind ring. Notice the similarity of this theorem with Theorem 1.3.15.

Theorem 1.10.3. *Let R be an integral domain. Then R is a Dedekind domain if and only if R is Noetherian, integrally closed and all non-zero prime ideals are maximal.*

Proof. See Proposition 14 at page 19 of [5]. □

The most important property of a Dedekind domain is that we have unique factorization of ideals.

Theorem 1.10.4. *Let R be a Dedekind domain. Then the set I_R of non-zero fractional ideals of R is a free abelian group generated by the non-zero prime ideals of R. In other words, every non-zero fractional ideal $\mathfrak{a}$ factors as a finite product*

$$\mathfrak{a} = \prod_{\mathfrak{p} \mid \mathfrak{a}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}.$$

Proof. Let R be a Dedekind domain and $\mathfrak{a}$ a non-zero integral ideal. Using Proposition 1.5.3 we find a maximal, hence prime, ideal $\mathfrak{p}_1$ which divides $\mathfrak{a}$. Since I_R is a group, we find a factorization $\mathfrak{a} = \mathfrak{p}_1(\mathfrak{a}\mathfrak{p}_1^{-1})$. Note that $\mathfrak{a}\mathfrak{p}_1^{-1}$ is an integral ideal, since $\mathfrak{p}_1$ contains $\mathfrak{a}$ and $\mathfrak{p}_1^{-1} = \{r \in Q(R) \mid r\mathfrak{p} \subseteq R\}$. If we repeat this process, we find a factorization of $\mathfrak{a}$ into prime ideals, because R is Noetherian by Theorem 1.10.3. □

1.11. Field extensions

As it is important to study extensions of rings and modules, it is also important to study extensions of fields, which is a special kind of ring extension where both rings are fields.

Degree of an extension. We start with the degree of an extension. Let L/K be a field extension. Then L is a vector space over K, as elements of L may be added and multiplied by scalars from K. This leads to the following definition.

Definition 1.11.1 (Degree)**.** Let L/K be a field extension. The *degree of L/K* (notation $[L : K]$) is the dimension of L as a K-vector space. The extension L/K is *finite* if and only if the degree is finite. △

Theorem 1.11.2 (Tower relation)**.** *Given a tower $M/L/K$ of field extensions. Then M/K is finite if and only if M/L and L/K are finite. Moreover, if M/K is finite, then $[M : K] = [M : L] \cdot [L : K]$.*

Proof. See Proposition 1.2 on page 224 of [6]. □

Algebraic extensions. We will now turn our attention to the arithmetic in a field extension.

Definition 1.11.3 (Algebraic extension)**.** Let L/K be a field extension and $x \in L$. Then x is called *algebraic over K* if and only if there exists a non-zero polynomial $f \in K[X]$ with $f(x) = 0$. We call x *transcendental over K* if and only if x is not algebraic over K. Moreover we call L/K *algebraic* if and only if every $x \in L$ is algebraic over K. △

Example 1.11.4. Consider the field extension $\mathbb{C}/\mathbb{Q}$. Then $\sqrt{2} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, since $\sqrt{2}$ is a zero of the non-zero polynomial $X^2 - 2$. ◊

Example 1.11.5. Consider the field extension $K(X)/K$. Then X is transcendental over K. Moreover, every non-constant polynomial f in $K[X]$ is transcendental over K. ◊

If L/K is a field extension and $x \in L$ is algebraic over K, then the ideal

$$I_x := \{f \in K[X] \mid f(x) = 0\}$$

is a non-zero proper ideal of $K[X]$. Since K is a field, $K[X]$ is a principal ideal domain. Hence we find some generator f_x of I_x. Clearly f_x has minimal degree in $I_x - \{0\}$. This explains the following definition.

Definition 1.11.6 (Minimal polynomial)**.** Let L/K be a field extension and $x \in L$ algebraic over K. The *minimal polynomial* of x is the generator of I_x. △

Notice that I_x is in fact a prime ideal of $K[X]$: if $(fg)(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$. Lemma 1.4.16 implies that f_x is a prime element of $K[X]$, as $K[X]$ is a principal ideal domain. Hence Theorem 1.3.15 and Theorem 1.5.6 imply that the minimal polynomial f_x is irreducible.

Separable extensions. As a preparation for the next section we will now study separable extensions. We first give a property of a polynomials.

Definition 1.11.7 (Separable polynomial)**.** Let L/K be a finite extension of fields and $f \in K[X]$. Then f is called *separable* over L if and only if $(X - a) \mid f$ implies $(X - a)^2 \nmid f$ for all $a \in L$. △

Loosely speaking, a polynomial f over K is separable over L precisely whenever f has no multiple roots in L. Via the minimal polynomial, this property extends to elements in an extension:

Definition 1.11.8 (Separable extensions)**.** Let L/K be a finite extension of fields and $x \in L$. Then x is called *separable* if and only if the minimal polynomial of x is separable over L. Moreover L/K is called *separable* if and only if all $x \in L$ are separable over K. △

We will give a nice criterion for determining whether an element is inseparable. For this we need the *formal derivative*:

$$d : L[X] \longrightarrow L[X], \qquad f \mapsto f'$$

which satisfies the following conditions:

1) d is normalized: $d(X) = 1$,

2) d is linear: $d(cf + g) = cd(f) + d(g)$ for all $f, g \in L[X]$ and $c \in L.$,

3) d satisfies the product rule: $d(fg) = d(f)g + fd(g)$ for all $f, g \in L[X]$.

Theorem 1.11.9. *Let L/K be a finite extension, let x in L and let f be the minimal polynomial of x over K. Then x is inseparable over K if and only if K has positive characteristic p and $f \in K[X^p]$.*

Proof. Suppose that $f \in K[X^p]$. Then there exists a $g \in K[Y]$ such that $f(X) = g(X^p)$ and $g(x^p) = 0$. Now using the factor theorem we find that $g = (Y - x^p)h(Y)$. Hence, using Newton's binomial in characteristic p, we have $f = (X - x)^p h(X^p)$. Thus x is a multiple zero of f.

Suppose that $f \in K[X] \subseteq L[X]$ has a multiple root a in L. Then we find a $g \in L[X]$ with $f = g \cdot (X - a)^m$ and $m \geq 2$. It is easily seen that

$$f' = (g \cdot (X - a)^m)' = (g'(X - a) + mg) \cdot (X - a)^{m-1}.$$

Thus we see that $(X - a)$ divides both f' and f, hence $\alpha f + \beta f' \neq 1$ for all $\alpha, \beta \in L[X]$. Hence f and f' are not coprime in $K[X]$, which implies that f divides f', because f is irreducible in $K[X]$. From $\deg(f') < \deg(f)$ is follows that $f' = 0$. If $a_n X^n$ is any non-zero term of f, then its derivative is $na_n X^n$ which is zero precisely when p divides n. Therefore $f \in K[X^p]$. □

Theorem 1.11.9 shows that every finite extension in characteristic 0 is separable.

Example 1.11.10. Let p be a prime power and t be transcendental over $\mathbb{F}_p$. Consider the extension $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$. Then $t^{1/p}$ is inseparable over $\mathbb{F}_p(t)$. Indeed, the minimal polynomial of $t^{1/p}$ over $\mathbb{F}_p(t)$ equals $f = X^p - t$. To see this, use the Eisenstein criterion over $\mathbb{F}_p[t]$. Now f factors over $\mathbb{F}_p(t^{1/p})$ as $(X - t^{1/p})^p$. Thus $t^{1/p}$ is a multiple root of $X^p - t$ in $\mathbb{F}_p(t^{1/p})$. ◊

Transcendence degree. Clearly not every field extension is algebraic. In this paragraph we will find a way to measure how far from being algebraic a given extension is. This is done via the transcendence degree.

Let L/K be a field extension and $A \subset L$. Then we will write $K(A)$ is the smallest intermediate field of L/K, which contains A. In other words

$$K(A) := \bigcap_{M \in \Omega} M,$$

where Ω is the set of all subfields M of L which contain both K and A. It is clear that $K(A)$ is a field.

Definition 1.11.11 (Generating subset)**.** Let L/K be a field extension and $A \subseteq L$ a subset. Then A is called a *generating subset* if and only if $L = K(A)$. If A is finite, then L/K is called *finitely generated*. If A is a singleton, then L/K is called *primitive*. If K is unspecified, then K is the prime subfield of L. △

Example 1.11.12. A finite extension of fields is finitely generated. Indeed, let L/K be a finite field extension and let $x_1, \ldots, x_n$ be a K-basis of L, with $n = [L : K]$. Then $L = K(x_1, \ldots, x_n)$. ◊

The generating subset in this example is not minimal, as $1, x_2/x_1, \ldots, x_n/x_1$ is a K-basis of L which shows that $\{x_2/x_1, \ldots, x_n/x_1\}$ is a generating subset. Now since $x_1 \in L = K(x_2/x_1, \ldots, x_n/x_1)$, we see that $\{x_2, \ldots, x_n\}$ is also a generating subset.

Definition 1.11.13 (Transcendence basis)**.** Let L/K be a field extension and $A \subseteq L$ a subset. Then A is called *algebraically independent* if and only if for every integer $n > 0$ and every subset $a_1, \ldots, a_n \in A$ the kernel of the evaluation homomorphism

$$e : K[X_1, \ldots, X_n] \longrightarrow L, \qquad f \mapsto f(a_1, \ldots, a_n)$$

is trivial. Moreover A is called a *transcendence basis* of L/K if and only if $L/K(A)$ is algebraic and A is algebraically independent. △

Just as with modules and vector spaces, the cardinality of a basis is a fundamental property of an extension.

Definition 1.11.14 (Transcendence degree)**.** Let L/K be a field extension with basis A. Then the *transcendence degree* $\mathrm{trdeg}(L/K)$ of L over K is the cardinality of A. △

Just like the definition of the dimension of a module or vector space, we need to show that every basis of a field extension has the same cardinality. We refer for this to Theorem 1.1 on page 356 in [6].

Example 1.11.15. Let K be a field and L be the field of fractions of the polynomial ring $K[X]$. Then the transcendence degree of L/K equals 1. It can be shown that if $L/M/K$ is a tower of field extensions, then $\mathrm{trdeg}(L/K) = \mathrm{trdeg}(L/M) + \mathrm{trdeg}(M/K)$. We will not prove this, as we do not need it. Then, using induction, it is easy to show that the quotient field of $K[X_1, \ldots, X_n]$ has transcendence degree n over K, for any positive integer n. ◊

For future use, we will define the notion of Kronecker dimension. The reason for this definition will become apparent in section 2.1.

Definition 1.11.16 (Kronecker dimension)**.** Let K be a finitely generated field. Then the *Kronecker dimension* of K is defined by

$$\mathrm{Krdim}(K) = \begin{cases} \mathrm{trdeg}(K/\mathbb{F}_p) & \text{if } \mathrm{char}(K) = p > 0 \\ \mathrm{trdeg}(K/\mathbb{Q}) + 1 & \text{if } \mathrm{char}(K) = 0 \end{cases}$$ △

1.12. Galois theory

In this section we will define and study the group of structure preserving maps on a given finite field extension. This group will be called the Galois group. When this finite field extension is a splitting field we can relate the Galois group to the intermediate fields of the extension.

Splitting fields. Let f be a polynomial in $\mathbb{Q}[X]$. Then f factors into linear factors over the complex numbers. But $\mathbb{C}$ is not the only field extension of $\mathbb{Q}$ with this property. In fact, any extension of $\mathbb{Q}$, which contains all roots of f, suffices.

Definition 1.12.1 (Splitting fields)**.** Let L/K be a finite extension, $f \in K[X]$ a polynomial over K. Then L is called the splitting field of f if and only if there exists $a_1, \ldots, a_n$ in L such that

1) f *splits completely* in L, i.e., $f = (X - a_1) \cdots (X - a_n)$,

2) L is minimal, i.e., $L = K(a_1, \ldots, a_n)$. △

It turns out that the splitting field of f over K is unique up to an isomorphism f which fixes the elements of K, i.e., $f(x) = x$ for all $x \in K$. Such an isomorphism is called a *K-isomorphism*.

Theorem 1.12.2. *Let L and L' be two splitting fields of a polynomial f over K. Then there exists an K-isomorphism $\sigma : L \to L'$.*

Proof. See Theorem 3.1 on page 236 of [6]. □

As an application to finite fields, we have the following:

Theorem 1.12.3. *Let q be a power of a prime number. Then there is a unique finite field $\mathbb{F}_q$ with q elements.*

Proof. It suffices to see that $\mathbb{F}_q$ is the splitting field of $X^q - X$ over $\mathbb{F}_p$, as then Theorem 1.12.2 shows that $\mathbb{F}_q$ is unique. To see this notice that $\mathbb{F}_q^\times$ has order $q-1$. Hence the multiplicative order of any $x \in \mathbb{F}_q$ divides $q - 1$. Hence every non-zero $x \in \mathbb{F}_q$ satisfies $X^{q-1} = 1$ and every element of $\mathbb{F}_q$ is a root of $X^q - X$. □

Galois extensions. We will now define and study the group of structure preserving maps on a given finite extension of fields.

Let L/K be a finite field extension. A *K-automorphism of L* is a ring isomorphism $\sigma : L \to L$, such that $\sigma(x) = x$ for all $x \in K$. One can think of a K-automorphism of L as an automorphism of the extension L/K.

Example 1.12.4 (Frobenius automorphism)**.** Let L/K be an extension of finite fields of characteristic p. Then the map $\mathrm{Fr} : L \to L$ given by $x \mapsto x^{|K|}$ is K-automorphism of L. First of all notice that $\mathrm{Fr}(xy) = \mathrm{Fr}(x)\,\mathrm{Fr}(y)$ for all $x, y \in L$. Furthermore we have that

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p,$$

because $\binom{p}{k}$ is divisible by p for $k \neq 0, p$. Therefore $(x + y)^{p^n} = (x^p + y^p)^{p^{n-1}}$ and with induction on n we find that $\mathrm{Fr}(x + y) = \mathrm{Fr}(x) + \mathrm{Fr}(y)$ which implies that Fr is an homomorphism. Notice that $\ker(\mathrm{Fr}) = \{0\}$, which means that Fr is injective. Now since the domain and codomain of Fr are both of the same finite cardinality, we conclude that Fr is an automorphism.

It remains to check that Fr is trivial on K. To see this, notice that $|K^\times| = |K|-1$ implies that $x^{|K|-1} = 1$ for all $x \in K$. Hence $x^{|K|} = x$ for all $x \in K$, which shows that Fr is a K-automorphism of L. ◊

We will now study the set of all K-automorphisms of L, which is called the Galois group.

Definition 1.12.5 (Galois group)**.** Let L/K be a finite field extension. Then the *Galois group of L/K* (notation: $\mathrm{Gal}(L/K)$) is the group of K-automorphisms of L, i.e.,

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \text{ for all } x \in K\}.$$ △

It turns out the Galois group is a finite group. Moreover, the following theorem show that the order is bounded by the degree of the extension.

Theorem 1.12.6. *Let L/K be a finite extension. Then $|\operatorname{Gal}(L/K)| \leq [L:K]$.*

Proof. See Theorem 8.3.1 on page 94 of [1]. □

This theorem leads to the following definition.

Definition 1.12.7 (Galois extension)**.** A finite extension L/K of fields is called *Galois* if and only if $|\operatorname{Gal}(L/K)| = [L:K]$. △

We will now give some equivalent conditions for a finite field extension being Galois. Recall from Definition 1.12.1 that a polynomials is said to split completely over L if all roots are in L.

Definition 1.12.8 (Normal extensions)**.** Let L/K be a finite extension of fields. Then L/K is called *normal* if and only if every irreducible polynomial f in $K[X]$ with a root in L splits completely over L. △

Recall the definition of a seperable polynomial. We now have the following theorem:

Theorem 1.12.9. *Let L/K be a finite extension. Then the following are equivalent:*

1) L/K is a Galois extension;

2) L/K is a normal and separable extension;

3) L is the splitting field over K of a separable polynomial $f \in K[X]$.

Proof. See Theorem 8.3.5 on page 95 of [1]. □

Let L/K be a finite extension and $H < \operatorname{Gal}(L/K)$. Then the *fixed field of H in L* is the set

$$L^H = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Clearly, the fixed field L^H is an intermediate field. The following theorem gives a correspondence between intermediate fields L/K and subgroups of $\operatorname{Gal}(L/K)$, which is called *Galois correspondence*.

Theorem 1.12.10 (Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension. Then we have a one-to-one correspondence,*

$$\begin{array}{ccc} \{\textit{subgroups of } \operatorname{Gal}(L/K)\} & \longleftrightarrow & \{\textit{intermediate fields of } L/K\} \\ H & \mapsto & L^H \\ \operatorname{Gal}(L/M) & \leftarrow\!\shortmid & M \end{array}$$

Normal subgroups of $\operatorname{Gal}(L/K)$ correspond to normal intermediate fields M of L/K. Moreover if M is a normal intermediate field of L/K, then

$$\operatorname{Gal}(M/K) \cong \operatorname{Gal}(L/K)/\operatorname{Gal}(L/M).$$

Proof. See Theorem 1.1 on page 262 of [6]. □

Example 1.12.11 (Finite fields)**.** Let $\mathbb{F}_{p^n}/\mathbb{F}_p$ be an extension of finite fields, for some integer $n \geq 1$ and prime p. We will show that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a cyclic extension. A finite extension L/K is called *cyclic* if and only if L/K is Galois and $\operatorname{Gal}(L/K)$ is cyclic. Let k be the order of Fr in $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, where Fr is the Frobenius automorphism. Then $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and Theorem 1.12.6 implies that $k \leq |\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq n$. On the other hand suppose that $\mathrm{Fr}^k(x) = x$ for all $x \in \mathbb{F}_{p^n}$. Then $X^{p^k} - X$ has at least p^n solutions. Therefore we have that $p^k \geq p^n$ and $k \geq n$. We conclude that $k = |\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. In other words, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension with cyclic Galois group generated by the Frobenius automorphism.

We will now show that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is a cyclic extension. First of all we have that $d := n/m = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$ is an integer. Using Galois correspondence we find that $\operatorname{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$, because $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic and hence $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is normal. This shows that $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = d$, which implies that $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois. Now notice that $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ is generated by Fr^m, since clearly Fr^m is an $\mathbb{F}_{p^m}$-automorphism of $\mathbb{F}_{p^n}$ and $md = n$ which implies that $\mathrm{Fr}^m(x) = x^{p^m}$ has order d. Therefore $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is a Galois extension with cyclic Galois group generated by the m-th power of the Frobenius automorphism. ◊

The main theorem gives lots of information about the intermediate fields. In fact we can now show that all intermediate fields are primitive. Recall that a field extension is called primitive whenever it is generated by a single element.

Corollary 1.12.12 (Primitive element theorem)**.** *Let L/K be a finite separable field extension. Then L/K is primitive.*

Proof. We follow the proof of Theorem 9.4.1 on page 106 of [1]. If K is a finite field with characteristic p, then $L \cong K[X]/(f)$ for any irreducible separable $f \in K[X]$ with degree $[L : K]$. Therefore L/K is primitive, as it is generated by the image of X. Suppose that $|K| = \infty$ and write $L = K(a_1, \ldots, a_k)$ for some $k \geq 1$ and $a_i \in L$. Let g_i be the minimal polynomial of a_i over K and let f be the product of the distinct g_i. Let N be the splitting field of f. Then Galois correspondence applies to N/K, which shows that there are only finitely many intermediate fields, because $\mathrm{Gal}(N/K)$ is finite. Therefore there are only finitely many intermediate fields of L/K. Now we will show that L/K is primitive, with induction on k. For $k = 1$ this is trivial. Suppose that $K(a_1, \ldots, a_{k-1})/K$ is primitive. Then we find some $b \in L$ with $K(a_1, \ldots, a_{k-1}) = K(b)$. We show that $K(a_k, b)$ is primitive. Consider the intermediate fields $K(a_k + bc)$, with $c \in K$. Since K is infinite and there are at most finitely many intermediate fields, we find c and c' such that $K(a_k + bc) = K(a_k + bc')$. Clearly $a_k + bc \in K(a_k, b)$. On the other hand both $(a_k + bc) - (a_k + bc') = (c - c')b$ and $c'(a_k + bc) - c'(a_k + bc) = (c - c')a$ are in $K(a_k + bc)$. Since $c \neq c'$ this implies that $a_k, b \in K(a_k + bc)$. Hence $L = K(a_k, b) = K(a_k + bc)$ is primitive. □

Chapter 2

Algebraic Number Theory

In this chapter we investigate the properties of *global fields*, i.e., a finitely generated fields of Kronecker dimension one. The aim of this chapter is on the one hand the introduction of terminology such as the ring of integers, the class group, the ray class groups, places, ramification index and the residue class degree and on the one hand to prove some important results such as the finiteness of the class group, the finiteness of the ray class groups, the non-zero density of the prime ideals in a given ray class, the Hasse norm theorem and the Artin reciprocity law.

The study of these global fields is done in two ways, which are almost identical. The first approach is via the classical viewpoint: we study the ideals in the ring of integers, the class group and the ray class groups of a global field. We show that both of these groups are finite. In the second approach will be an idelic viewpoint: we will study the embeddings of a global field into *local fields*, which are completions of the global field with respect to an absolute value.

In the beginning of the chapter we will focus on the classical approach, as this is more intuitive. Later on we switch to the idelic viewpoint as we need to implement results from other texts such as Weil [17].

2.1. The ring of integers

We start of with the definition of the object which we will study in this chapter. Recall that a field is called finitely generated precisely when it is finitely generated over the prime subfield.

Definition 2.1.1 (Global field)**.** A field K is called a *global field* if and only if K is a finitely generated field of Kronecker dimension 1. △

We now introduce some basic notation. Let K be a global field. Then $t \in K$ is called *integral* if and only if t is integral over the prime subring of K (that is, t is integral over $\mathbb{Z}$ or $\mathbb{F}_p$ whenever $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$ respectively).

If K is a global field and $t \in K$ is non-integral, then we define the subring $\mathcal{O}_{\mathbb{K}} \subseteq K$ by

$$\mathcal{O}_{\mathbb{K}} := \begin{cases} \mathbb{Z} & \text{if } \mathrm{char}(K) = 0 \\ \mathbb{F}_p[t] & \text{if } \mathrm{char}(K) = p > 0 \end{cases} \tag{2.1}$$

Furthermore we define the subfield $\mathbb{K} \subseteq K$ by $\mathbb{K} = Q(\mathcal{O}_{\mathbb{K}})$. Then $K/\mathbb{K}$ is a finite extension of global fields.

Definition 2.1.2 (Ring of integers)**.** The *ring of integers* $\mathcal{O}_K$ of a global field K is the integral closure of $\mathcal{O}_{\mathbb{K}}$ in K. △

Ideal theory. We will now prove an important fact about the ring of integers, namely that it has *ideal theory*. This means that the set of fractional ideals of $\mathcal{O}_K$ is a free abelian group generated by the (integral) prime ideals.

The following lemma shows that every non-zero integral ideal of $\mathcal{O}_K$ extends (i.e., contains) a non-zero integral ideal of $\mathcal{O}_{\mathbb{K}}$. These extensions will be further investigated in the next paragraph.

For future use (c.f., Theorem 2.5.11), we will be a bit more general. If K is a global field and $R \subseteq K$ a subring of K, then R is called a *global ring* if and only if $\mathcal{O}_{\mathbb{K}} \subseteq R$.

Lemma 2.1.3. *Let $\mathfrak{a}$ be a non-zero integral ideal of a global ring R. Then $\mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}$ is a non-zero integral ideal of $\mathcal{O}_{\mathbb{K}}$.*

Proof. Let $\mathfrak{a}$ be an integral ideal of a global ring R. It is clear that $\mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}$ is an integral ideal of $\mathcal{O}_{\mathbb{K}}$. Now let x be a non-zero element of $\mathfrak{a}$. Then since $K/\mathbb{K}$ is finite, x is algebraic over $\mathbb{K}$. Since $\mathbb{K} = Q(\mathcal{O}_{\mathbb{K}})$ we find some $f = c \cdot f^x_{K/\mathbb{K}} \in \mathcal{O}_{\mathbb{K}}[X]$, where c is sufficiently large and f is irreducible in $\mathcal{O}_{\mathbb{K}}[X]$. More explicitly, we find $n \geq 1$ and $a_i \in \mathcal{O}_{\mathbb{K}}$ for $0 \leq i < n-1$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. But now we find $a_0 = -x^n - a_{n-1}x^{n-1} - \cdots - a_1 x \in \mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}$, because $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. Furthermore $a_0 = f(0) \neq 0$, since $x \neq 0$ and f is irreducible in $\mathcal{O}_{\mathbb{K}}[X]$. Thus $\mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}$ is a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. □

We also need the following important property about the non-zero integral ideals of a global ring R.

Lemma 2.1.4. *Every non-zero integral ideal $\mathfrak{a}$ of a global ring R is of finite index.*

Proof. Let $\mathfrak{a}$ be a non-zero integral ideal of a global ring R. We will follow the proof of Theorem 2.11 at page 19 of [16]. Using Lemma 2.1.3 we see that $\mathfrak{a}$ contains a non-zero element $a \in \mathcal{O}_{\mathbb{K}}$. Now it suffices to prove that R/aR is finite, since the canonical map $R/aR \to \mathcal{O}_K/\mathfrak{a}$ is surjective.

We will show that every finitely generated $\mathcal{O}_{\mathbb{K}}$-submodule of R/aR contains at most $\mathrm{N}_{\mathbb{K}}(a)^{[K:\mathbb{K}]}$ elements. Then $|R/aR| \leq \mathrm{N}_{\mathbb{K}}(a)^{[K:\mathbb{K}]}$, since we can construct larger $\mathcal{O}_{\mathbb{K}}$-submodules when R/aR is larger.

Let N be a finitely generated $\mathcal{O}_{\mathbb{K}}$-submodule of R/aR, generated by $(x_i + aR)_{i=1}^n$. Let M be the $\mathcal{O}_{\mathbb{K}}$-submodule R generated by $(y_i)_{i=1}^n$, for some $y_i \in x_i + aR$. Then the natural $\mathcal{O}_{\mathbb{K}}$-module homomorphism $\pi : M \to R/aR$ satisfies $\pi(M) = N$ and induces an $\mathcal{O}_{\mathbb{K}}$-module isomorphism $M/aM \cong N$. Hence is suffices to prove that M/aM contains at most $\mathrm{N}_{\mathbb{K}}(a)^{[K:\mathbb{K}]}$ elements.

Since R is an integral domain, M has no elements of finite order. Therefore M is a free $\mathcal{O}_{\mathbb{K}}$-module. Any set with more then $[K : \mathbb{K}]$ elements is linearly dependent over $\mathbb{K}$. Thus the rank k of M does not exceed $[K : \mathbb{K}]$ and we find that $|M/aM| = |\mathcal{O}_{\mathbb{K}}/a\mathcal{O}_{\mathbb{K}}|^k \leq \mathrm{N}_{\mathbb{K}}(a)^{[K:\mathbb{K}]}$. This concludes the proof of the lemma. □

We are now ready to prove that the ring of integers is a Dedekind domain.

Proposition 2.1.5. *The ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

Proof. We will show that Lemma 2.1.4 implies that $\mathcal{O}_K$ is Noetherian, integrally closed and every non-zero prime ideal of $\mathcal{O}_K$ is maximal. Then Theorem 1.10.3 implies that $\mathcal{O}_K$ is Dedekind.

Given a chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$ of ideals. Using Lemma 2.1.4 this gives rise to a decreasing sequence of natural numbers $|\mathcal{O}_K/\mathfrak{a}_0| \geq |\mathcal{O}_K/\mathfrak{a}_1| \geq \cdots$. Since $\leq$ is a well-order of $\mathbb{N}$, this sequence has a least element at which it stabilizes. But $\mathfrak{a}_i = \mathfrak{a}_j$ if and only if $|\mathcal{O}_K/\mathfrak{a}_i| = |\mathcal{O}_K/\mathfrak{a}_j|$, for all $i < j$. Therefore the chain stabilizes and $\mathcal{O}_K$ is Noetherian.

Since $\mathcal{O}_K$ is the integral closure of $\mathcal{O}_{\mathbb{K}}$ in K we conclude by Theorem 1.7.4 that $\mathcal{O}_K$ is integrally closed.

Furthermore let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then by Lemma 2.1.4 and Theorem 1.4.17 we find that $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain. Consider the left multiplication by a non-zero $a \in \mathcal{O}_K/\mathfrak{p}$. This map is injective, hence surjective by the finiteness of $\mathcal{O}_K/\mathfrak{p}$. Thus 1 is in the image which implies that a is invertible. Therefore $\mathcal{O}_K/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal by Theorem 1.4.13. □

The fact that the ring of integers $\mathcal{O}_K$ of a global field is a Dedekind domain implies that we have unique factorization of non-zero fractional ideals. We first illustrate this with an example.

Example 2.1.6. The set $I_{\mathbb{Q}}$ of non-zero fractional ideals of $\mathcal{O}_{\mathbb{Q}} := \mathbb{Z}$ is given by

$$I_{\mathbb{Q}} = \{q\mathbb{Z} \mid q \in \mathbb{Q}^{\times}\} \cong \mathbb{Q}^{\times}/\{\pm 1\}.$$

Hence every non-zero fractional ideal in $I_{\mathbb{Q}}$ factors as $q\mathbb{Z} = (p_1\mathbb{Z})^{n_1} \cdots (p_s\mathbb{Z})^{n_s}$, for some primes $p_i \in \mathbb{Z}$, integers $n_i \in \mathbb{Z}$ and $s \in \mathbb{N}$, with $q = \pm p_1^{n_1} \cdots p_s^{n_s}$. ◊

We can do the same for the function field $\mathbb{F}_p(t)$. In fact, this can be done in an arbitrary global field:

Theorem 2.1.7. *The set I_K of non-zero fractional ideals of $\mathcal{O}_K$ is a free abelian group generated by the non-zero prime ideals of $\mathcal{O}_K$, i.e., every non-zero fractional ideal $\mathfrak{a}$ factors uniquely as a finite product*

$$\mathfrak{a} = \prod_{\mathfrak{p} \mid \mathfrak{a}} \mathfrak{p}^{n_{\mathfrak{p}}}.$$

Proof. The result follows from Proposition 2.1.5 and Theorem 1.10.4. □

Extensions of primes. Given an extension L/K of global fields. We will investigate how the primes of L are related to the primes of K.

Definition 2.1.8 (Extensions of primes)**.** Let L/K be an extension of global fields, $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{P}$ *extends* $\mathfrak{p}$ or $\mathfrak{p}$ *lies over/above* $\mathfrak{p}$ (notation: $\mathfrak{P}/\mathfrak{p}$) if and only if $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. △

We will now study the relation between the primes $\mathfrak{P}$ of L which lie above a given prime $\mathfrak{p}$ of K.

Definition 2.1.9 (Ramification index)**.** Let L/K be a finite extension of global fields and $\mathfrak{P}$ a non-zero prime of $\mathcal{O}_L$ extending a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Then the *ramification index* $e(\mathfrak{P}/\mathfrak{p})$ of $\mathfrak{P}$ over $\mathfrak{p}$ is the multiplicity of $\mathfrak{P}$ in the factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$. △

For notational convenience we will also write $e_{\mathfrak{P}}$ instead of $e(\mathfrak{P}/\mathfrak{p})$.

Definition 2.1.10 (Residue class field)**.** Let $\mathfrak{p}$ be a non-zero prime ideal in the ring of integers $\mathcal{O}_K$ of a global field K. Then the *residue class field* is the field

$$\overline{K}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$$ △

In a finite extension L/K of global fields, we may consider the residue class field $\overline{K}_{\mathfrak{p}}$ at a prime $\mathfrak{p}$ and the residue class field $\overline{L}_{\mathfrak{P}}$ at some extension $\mathfrak{P}$ of $\mathfrak{p}$. This extension is finite, as L/K is finite. Hence we can define the following:

Definition 2.1.11 (Residue class degree)**.** Let L/K be a finite extension of global fields and $\mathfrak{P}$ a non-zero prime of $\mathcal{O}_L$ extending a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Then the *residue class degree* of $\mathfrak{P}$ over $\mathfrak{p}$ is the degree

$$f(\mathfrak{P}/\mathfrak{p}) = [\overline{L}_{\mathfrak{P}} : \overline{K}_{\mathfrak{p}}].$$ △

For notational convenience we will also write $f_{\mathfrak{P}}$ instead of $f(\mathfrak{P}/\mathfrak{p})$.

We are now ready to formulate the relation between the primes which lie above a given prime.

Theorem 2.1.12 (Fundamental formula)**.** *Let L/K be an extension of global fields. Then for all primes $\mathfrak{p}$ in $\mathcal{O}_K$ we have*

$$\sum_{\mathfrak{P}/\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} = [L : K].$$

Proof. See Proposition 8.2 on page 46 of [10] and notice that the proof applies not only to number field but function fields too. □

2.2. Ideal and field norm

In this section we will study the ideal norms. We distinguish two types of norms: the relative and the absolute ideal norm. Both of these maps give rise to a field norm, by considering principal ideals.

Relative norm. We will now study a map which connects, in a given extension L/K of global fields, the fractional ideals of L with those of K. Recall that the set I_L of fractional ideals of L is generated by the prime ideals of $\mathcal{O}_L$ (Theorem 2.1.7). Hence the following map is well-defined.

Definition 2.2.1 (Relative ideal norm)**.** Let L/K be a finite extension of global fields and let I_L and I_K be the groups of non-zero fractional ideals of L and K. The *(relative) ideal norm* from L to K is the group homomorphism

$$\mathrm{N}_{L/K} : I_L \longrightarrow I_K$$

determined by $\mathfrak{P} \mapsto \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$, for every prime $\mathfrak{P}$ in I_L and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. △

Using the fundamental formula, we find the following lemma.

Lemma 2.2.2. *Let L/K be a finite extension of global fields and $\mathfrak{a}$ a fractional ideal of K. Then $\mathrm{N}_{L/K}(\mathfrak{a}\mathcal{O}_L) = \mathfrak{a}^{[L:K]}$.*

Proof. Since the set I_K of non-zero fractional ideals of K is generated by the prime ideals of $\mathcal{O}_K$ it suffices to check the identity for some prime $\mathfrak{p}$. Write $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i}$, with $e_i = e(\mathfrak{P}_i/\mathfrak{p})$. Write $f_i = f(\mathfrak{P}_i/\mathfrak{p})$. Then we find by the fundamental formula that

$$\mathrm{N}_{L/K}(\mathfrak{p}\mathcal{O}_L) = \mathrm{N}_{L/K}(\textstyle\prod_{i=1}^{n} \mathfrak{P}_i^{e_i}) = \prod_{i=1}^{n} \mathrm{N}_{L/K}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{n} \mathfrak{p}^{e_i f_i} = \mathfrak{p}^{[L:K]},$$

which proves the lemma. □

We now come to an important property of the ideal norm, which will be used in Definition 2.2.4 and Theorem 2.12.8.

Theorem 2.2.3. *Let L/K be a finite extension of global fields. Then $\mathrm{N}_{L/K}(\mathfrak{A})$ is principal whenever $\mathfrak{A}$ is principal.*

Proof. See Proposition 22 on page 26 of [5]. □

Given an extension of global fields L/K. Then fractional ideals of $\mathcal{O}_K$ are generalizations of non-zero elements of K. Indeed, every element a in L a gives rise to a fractional ideal $a\mathcal{O}_L$ of L. Hence, in view of Proposition 2.2.3, we may define the following:

Definition 2.2.4 (Relative field norm)**.** Let L/K be a finite extension of global fields. The *(relative field) norm* from L to K is the group homomorphism $\mathrm{N}_{L/K} : L^\times \to K^\times$ which maps a to the generator of $\mathrm{N}_{L/K}(a\mathcal{O}_L)$. It is customary to extend this map with $\mathrm{N}_K(0) = 0$. △

The next theorem provides some alternative descriptions of this norm map.

Theorem 2.2.5. *Let L/K be a finite extension of global fields. Then for all a in L we have*

1) *$\mathrm{N}_{L/K}(a) = \det(M_a)$, with M_a the K-linear automorphism of L given by $x \mapsto ax$;*

2) *$\mathrm{N}_{L/K}(a) = \prod_\sigma \sigma(a)$, where σ runs over all K-homomorphism from L into a fixed algebraic closure $\overline{K}$ of K.*

Proof. From Proposition 22 on page 26 of [5] we know that $\mathrm{N}_{L/K}(a) = \det(M_a)$ holds, From page 40 and 41 of [16] we see that $\det(M_a) = \prod_\sigma \sigma(a)$. □

Absolute norm. We will now define an ideal norm, which depend on a single global field instead of an extension of global fields. Before we give the definition, recall that both $\mathcal{O}_K$ and $\mathfrak{a}$ are subgroups of K^+, the additive group of K. Hence we may speak about the index of $\mathfrak{a}$ in $\mathcal{O}_K$ as an additive subgroup.

Definition 2.2.6 (Absolute ideal norm)**.** Let K be a global fields and let I_K be the group of non-zero fractional ideals of K. The *(absolute) ideal norm* on K is the group homomorphism

$$\mathrm{N}_K : I_K \longrightarrow \mathbb{Q}_{>0}$$

determined by $\mathfrak{p} \mapsto [\mathcal{O}_K : \mathfrak{p}]$, for every prime $\mathfrak{p}$ in I_K. △

Notice that this definition is well-defined, because Theorem 2.1.7 shows that I_K is freely generated by the prime ideals of $\mathcal{O}_K$. Hence there exists a unique extension N_K of the assignment $\mathfrak{p} \mapsto [\mathcal{O}_K : \mathfrak{p}]$.

Example 2.2.7. Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}_{\mathbb{K}}$. Then since $\mathcal{O}_{\mathbb{K}}$ is a principal ideal domain, we find some $x \in \mathcal{O}_{\mathbb{K}}$ with $\mathfrak{p} = a\mathcal{O}_{\mathbb{K}}$. Hence we have that

$$\mathrm{N}_{\mathbb{K}}(\mathfrak{p}) = [\mathcal{O}_{\mathbb{K}} : a\mathcal{O}_{\mathbb{K}}] = \begin{cases} a & \text{if } \mathrm{char}(K) = 0 \\ p^{\deg(a)} & \text{if } \mathrm{char}(K) = p > 0 \end{cases},$$

where $\deg(a)$ is the degree of $a \in \mathcal{O}_{\mathbb{K}} = \mathbb{F}_p[t]$ as a polynomial in t. ◊

We will show that N_K is can also be characterized by the formula $\mathrm{N}_K(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$, where $\mathfrak{a}$ is any integral ideal of $\mathcal{O}_K$. We first prove a preliminary result:

Lemma 2.2.8. *Let K be a global field and $\mathfrak{p}$ a non-zero prime of $\mathcal{O}_K$. Then for all $n \in \mathbb{N}$ we have $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$ as $\mathcal{O}_K$-modules.*

Proof. Pick $a \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$, which is possible since $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ by the unique factorization. Define $\phi : \mathcal{O}_K \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ by $x \mapsto ax + \mathfrak{p}^{n+1}$. Then clearly ϕ is a $\mathcal{O}_K$-module homomorphism with $\mathfrak{p} \subseteq \ker(\phi)$. Suppose that $\phi(x) = 0 + \mathfrak{p}^{n+1}$. Then $ax \in \mathfrak{p}^{n+1}$ or $\mathfrak{p}^{n+1} \mid (a)(x)$ and $\mathfrak{p} \mid (x)$ since $\mathfrak{p}^{n+1}$ does not divide (a). Thus $\mathfrak{p} = \ker(\phi)$.

We now show that ϕ is surjective. Let $b \in \mathfrak{p}^n$. By the Chinese remainder theorem there exists $x_0 \in \mathcal{O}_K$ such that

$$x_0 \equiv b \pmod{\mathfrak{p}^{n+1}} \qquad \text{and} \qquad x_0 \equiv 0 \pmod{(a)/\mathfrak{p}^n}.$$

We have $\mathfrak{p}^n \mid (b)$ since $b \in \mathfrak{p}^n$ and $(a)/\mathfrak{p}^n \mid (x_0)$ by the second displayed condition. So $(a) = \mathfrak{p}^n \cdot (b)/\mathfrak{p}^n \mid (x_0)$, hence $x_0/a \in \mathcal{O}_K$. Finally

$$\varphi(x_0/a) = a(x_0/a) + \mathfrak{p}^{n+1} = x_0 + \mathfrak{p}^{n+1} = c + \mathfrak{p}^{n+1}.$$

Hence ϕ is surjective, and the lemma follows form the first isomorphism theorem for $\mathcal{O}_K$-modules. □

We will now give another, more explicit, characterization of the absolute ideal norm:

Theorem 2.2.9. *Let K be a global field and $\mathfrak{a}$ a non-zero integral ideal of $\mathcal{O}_K$. Then $\mathrm{N}_K(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$.*

Proof. Write $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$, with $n_i \geq 1$ an integer for all $1 \leq i \leq k$. By the Chinese remainder theorem we find that

$$\mathcal{O}_K/\mathfrak{a} \cong \prod_{i=1}^{n} \mathcal{O}_K/\mathfrak{p}_i^{n_i}.$$

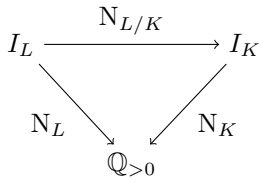
For each non-zero prime $\mathfrak{p}$ of $\mathcal{O}_K$ and each integer $n \geq 1$, consider the tower $\mathfrak{p}^{n+1} \subseteq \mathfrak{p}^n \subseteq \mathcal{O}_K$ of subgroups of K^+. From elementary group theory we have that $[\mathcal{O}_K : \mathfrak{p}^{n+1}] = [\mathcal{O}_K : \mathfrak{p}^n] \cdot [\mathfrak{p}^n : \mathfrak{p}^{n+1}]$. From Lemma 2.2.8 we see that $[\mathcal{O}_K : \mathfrak{p}] = [\mathfrak{p}^n : \mathfrak{p}^{n+1}]$. Hence, we have that $[\mathcal{O}_K : \mathfrak{p}^{n+1}] = [\mathcal{O}_K : \mathfrak{p}^n] \cdot [\mathcal{O}_K : \mathfrak{p}]$. By induction on n we find $[\mathcal{O}_K : \mathfrak{p}^n] = [\mathcal{O}_K : \mathfrak{p}]^n$, for all integers $n \geq 1$. We conclude that

$$[\mathcal{O}_K : \mathfrak{a}] = \prod_{i=1}^{n} [\mathcal{O}_K : \mathfrak{p}_i^{n_i}] = \prod_{i=1}^{n} [\mathcal{O}_K : \mathfrak{p}_i]^{n_i} = \prod_{i=1}^{n} \mathrm{N}_K(\mathfrak{p}_i)^{n_i}$$

The right hand side equals $\mathrm{N}_K(\mathfrak{a})$ by definition, which proves the theorem. □

The next proposition shows that relative and absolute norm commute.

Proposition 2.2.10. *Let L/K be an extension global fields. Then the diagram*



commutes. In other words: for all prime ideals $\mathfrak{P}$ of L we have

$$\mathrm{N}_L(\mathfrak{P}) = \mathrm{N}_K(\mathrm{N}_{L/K}(\mathfrak{P})).$$

Proof. Write $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. From Theorem 2.2.9 we conclude that

$$\mathrm{N}_K(\mathrm{N}_{L/K}(\mathfrak{P})) = \mathrm{N}_K(\mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}) = \mathrm{N}_K(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}$$

Using the definition of $f(\mathfrak{P}/\mathfrak{p})$ and $\mathrm{N}_K(\mathfrak{p})$ we find that

$$\mathrm{N}_K(\mathrm{N}_{L/K}(\mathfrak{P})) = |\mathcal{O}_K/\mathfrak{p}|^{[\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]} = |\mathcal{O}_L/\mathfrak{P}| = \mathrm{N}_L(\mathfrak{P}),$$

which concludes the proof. □

Just as the relative ideal norm of an extension L/K of global fields induces the field norm from $L^\times$ to $K^\times$, the absolute ideal norm from a global field K induces a map from $K^\times$:

Definition 2.2.11 (Absolute field norm)**.** Let L/K be a finite extension of global fields. The *(absolute field) norm* from K is the group homomorphism $\mathrm{N}_K : K^\times \to \mathbb{Q}_{>0}$ determined by $a \mapsto \mathrm{N}_K(a\mathcal{O}_K)$ for all $a \in \mathcal{O}_K$. It is customary to extend this map with $\mathrm{N}_K(0) = 0$. △

Example 2.2.12. Let $x \in \mathcal{O}_\mathbb{K}$. Then using Theorem 2.2.9 we have that

$$\mathrm{N}_\mathbb{K}(x) = [\mathcal{O}_\mathbb{K} : x\mathcal{O}_\mathbb{K}] = \begin{cases} |x| & \text{if } \mathrm{char}(K) = 0 \\ p^{\deg(x)} & \text{if } \mathrm{char}(K) = p > 0 \end{cases}.$$

Here $\deg(x)$ is the degree of $x \in \mathcal{O}_\mathbb{K} = \mathbb{F}_p[t]$ as a polynomial in t. For all $a = x/y \in \mathbb{K}$ we now have that

$$\mathrm{N}_\mathbb{K}(a) = \frac{[\mathcal{O}_\mathbb{K} : x\mathcal{O}_\mathbb{K}]}{[\mathcal{O}_\mathbb{K} : y\mathcal{O}_\mathbb{K}]} = \begin{cases} |a| & \text{if } \mathrm{char}(K) = 0 \\ p^{\deg(a)} & \text{if } \mathrm{char}(K) = p > 0 \end{cases}.$$

It is easy to see that the absolute field norm $\mathrm{N}_\mathbb{K}$ is an absolute value (c.f., Definition 2.4.1). ◊

2.3. Class group

Let K be a global field and let I_K denote the set of non-zero fractional ideals of $\mathcal{O}_K$. Consider the subgroup

$$P_K = \{k\mathcal{O}_K \mid k \in K^\times\}$$

of principal fractional ideals in I_K. This is a normal subgroup, since I_K is abelian. Hence we may consider their quotient.

Definition 2.3.1 (Ideal class group)**.** Let K be a global field. Then the *(ideal) class group* $\mathcal{C}l(K)$ of K is the quotient I_K/P_K. Elements $\mathfrak{R}$ of $\mathcal{C}l(K)$ are called *ideal classes*. The *class number* h is order of the class group. Two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *linear equivalent* if $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal principal fractional ideal. △

We will show that the order of the class group is finite. We follow page 100 of [5].

Lemma 2.3.2. *Every ideal class contains an integral ideal.*

Proof. Let $\mathfrak{R}$ be an ideal class in $\mathcal{C}l(K)$ and fix some fractional ideal $\mathfrak{a}$ in $\mathfrak{R}$. By definition of a fractional ideal there exists some $x \in \mathcal{O}_K$ such that $x\mathfrak{a} \subseteq \mathcal{O}_K$. Notice that $\mathfrak{b} = (x)\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$, with $\mathfrak{a} \sim \mathfrak{b}$. Therefore $\mathfrak{R}$ contains an integral ideal $\mathfrak{b}$. □

The next lemma shows that $\mathcal{O}_K$ is not very large.

Lemma 2.3.3. *The ring of integers $\mathcal{O}_K$ is a free $\mathcal{O}_\mathbb{K}$-module of rank $[K : \mathbb{K}]$.*

Proof. Clearly $\mathcal{O}_K$ is an $\mathcal{O}_\mathbb{K}$-module which is torsion free since $\mathcal{O}_K$ is an integral domain. Since $\mathcal{O}_\mathbb{K}$ is a unique factorization domain we conclude from Theorem 1.7.3 that $\mathcal{O}_\mathbb{K}$ is integrally closed. Now $\mathcal{O}_K$ is finitely generated by Proposition 6 at page 6 of Lang [5]. Now Theorem 1.6.14 implies that $\mathcal{O}_K$ is a free $\mathcal{O}_\mathbb{K}$-module, since $\mathcal{O}_\mathbb{K}$ is a principal ideal domain and K is a finite separable extension of the quotient field $\mathbb{K}$ of $\mathcal{O}_\mathbb{K}$.

It remains to show that $\mathcal{O}_K$ has rank $[K : \mathbb{K}]$. Since $K/\mathbb{K}$ is separable, the primitive element theorem (Corollary 1.12.12) implies the existence of an $x \in K$ of degree $n = [K : \mathbb{K}]$. By Proposition 1 at page 5 of Lang [5] we find a $c \in \mathbb{K}$ such that $cx \in \mathcal{O}_K$. But now $1, cx, \ldots, (cx)^{n-1}$ is an $\mathbb{K}$-linearly independent subset of $\mathcal{O}_K$, since the degree of cx equals the degree of x. Hence $\mathcal{O}_K$ has rank at least $[K : \mathbb{K}]$. Clearly the rank of $\mathcal{O}_K$ cannot exceed $[K : \mathbb{K}]$, which concludes the proof. □

Lemma 2.3.4. *There exist a $C > 0$ such that every non-zero integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ contains an element a with $\mathrm{N}_K(a) \leq C \cdot \mathrm{N}_K(\mathfrak{a})$.*

Proof. We rewrite the proof on page 100 of [5] using our notations. Recall the definition of $\mathbb{K}$ from section 2.1 and consider the finite extension $K/\mathbb{K}$. We know by Lemma 2.3.3 that the ring of integers is a finitely generated $\mathcal{O}_\mathbb{K}$-module of rank $N \geq 1$. Let $b_1, \ldots, b_N$ be an $\mathcal{O}_\mathbb{K}$-basis of $\mathcal{O}_K$ and define for any $d \in \mathbb{Q}_{>0}$

$$S_d = \{\textstyle\sum_{i=1}^N r_i b_i \in \mathcal{O}_K \mid r_i \in \mathcal{O}_\mathbb{K}, \mathrm{N}_\mathbb{K}(r_i) \leq d\}.$$

Then there are more then d^N elements in S_d. Indeed, we have that $|S_d| = g^N$, with

$$g = |\{r \in \mathcal{O}_\mathbb{K} \mid \mathrm{N}_\mathbb{K}(r) \leq d\}|.$$

If K is a number field then g is the number of $r \in \mathbb{Z}$ with $\mathrm{N}_\mathbb{K}(r) = |r| \leq d$. Hence $g = 2d + 1 > d$. If K is a function field then g is the number of $r \in \mathbb{F}_p[t]$ with $\mathrm{N}_\mathbb{K}(r) = p^{\deg(r)} \leq d$ or equivalently $\deg(r) \leq \lfloor \log_p(d) \rfloor$. Hence $g = p^{\lfloor \log_p(d) \rfloor + 1} > d$. In both cases we find $g > d$, which implies that $|S_d| > d^N$.

Choose $d = \mathrm{N}_K(\mathfrak{a})^{1/N}$. Then S_d contains more then $\mathrm{N}_K(\mathfrak{a})$ elements, while $\mathcal{O}_K/\mathfrak{a}$ contains precisely $\mathrm{N}_K(\mathfrak{a})$ elements by Theorem 2.2.9. Therefore the projection $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{a}$ is not injective on S_d. Hence we find two distinct elements x and y in S_d such that $\pi(x) = \pi(y)$. Define $a = x - y$. Then clearly $a \in \ker \pi = \mathfrak{a}$. Suppose that $x = \sum_{i=1}^N x_i b_i$ and $y = \sum_{i=1}^N y_i b_i$. Then $a = \sum_{i=1}^N a_i b_i$, with $a_i = x_i - y_i$ for all i. Hence, using the triangle inequality (Example 2.2.12), we see that

$$\mathrm{N}_\mathbb{K}(a_i) \leq \mathrm{N}_\mathbb{K}(x_i) + \mathrm{N}_\mathbb{K}(-y_i) \leq 2\,\mathrm{N}_K(\mathfrak{a})^{1/N}.$$

We now estimate the norm of a from K. By Proposition 2.2.10 and Theorem 2.2.5 we have

$$\mathrm{N}_K(a) = \mathrm{N}_\mathbb{K}(\mathrm{N}_{K/\mathbb{K}}(a)) = \mathrm{N}_\mathbb{K}(\prod_\sigma \sigma(a)) = \prod_\sigma \mathrm{N}_\mathbb{K}(\sigma(a)),$$

where σ runs through $\hom_\mathbb{K}(K, \overline{\mathbb{K}})$. Now using the triangle inequality (Example 2.2.12) and the fact that any σ fixes $\mathbb{K}$ we conclude that

$$\mathrm{N}_K(a) = \prod_\sigma \mathrm{N}_\mathbb{K}(\sigma(\sum_{i=1}^N a_i b_i)) \leq \prod_\sigma \sum_{i=1}^N \mathrm{N}_\mathbb{K}(a_i)\,\mathrm{N}_\mathbb{K}(\sigma(b_i))$$

Let M be the maximum of $\mathrm{N}_{\mathbb{K}}(\sigma(b_i))$ over all σ in $\hom_{\mathbb{K}}(K, \overline{\mathbb{K}})$ and all $1 \leq i \leq N$. Then we find that

$$\mathrm{N}_K(a) \leq \prod_{\sigma} \sum_{i=1}^{N} 2\,\mathrm{N}_K(\mathfrak{a})^{1/N} M \leq C \cdot \mathrm{N}_K(\mathfrak{a}),$$

with $C = (2M)^N N$, because $|\hom_{\mathbb{K}}(K, \overline{\mathbb{K}})| = N$. □

Lemma 2.3.5. *There exist only finitely many integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $\mathrm{N}_K(\mathfrak{a}) \leq C$, for some given $C > 1$.*

Proof. Let $\mathfrak{a}$ be a integral ideal of $\mathcal{O}_K$ with $\mathrm{N}_K(\mathfrak{a}) \leq C$. By Theorem 2.1.7 we may factor $\mathfrak{a}$ into positive powers of prime ideals $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. Hence we find by definition

$$\mathrm{N}_K(\mathfrak{a}) = \mathrm{N}_K(\mathfrak{p}_1)^{n_1} \cdots \mathrm{N}_K(\mathfrak{p}_k)^{n_k} \leq C$$

Notice that $\mathrm{N}_K(\mathfrak{p}_i) = [\mathcal{O}_K : \mathfrak{p}_i] \geq 2$ for all indices i, which implies that all n_i are bounded from above. Since $\mathfrak{a}$ is integral, we also have $n_i > 0$. Now consider

$$\mathrm{N}_K(\mathfrak{p}) = \mathrm{N}_{\mathbb{K}}(\mathrm{N}_{K/\mathbb{K}}(\mathfrak{p})) = \mathrm{N}_{\mathbb{K}}((\pi)^f) = \begin{cases} |\pi|^f & \text{if } \mathrm{char}(K) = 0 \\ p^{f \deg(\pi)} & \text{if } \mathrm{char}(K) = p > 0 \end{cases},$$

with $(\pi) = \mathfrak{p} \cap \mathcal{O}_{\mathbb{K}}$ and $f = f(\mathfrak{p}/(\pi))$. We see that there are only finitely many π with $\mathrm{N}_{\mathbb{K}}((\pi)^f) \leq C$. The fundamental formula shows that there are at most $[K : \mathbb{K}]$ for every (π). Hence we find only finitely many $\mathfrak{p}_i$ with $\mathrm{N}_K(\mathfrak{p}_i) \leq C$, which proves the claim. □

We are now ready to prove our main result:

Theorem 2.3.6. *The ideal class group $\mathcal{C}l(K)$ of a global field is finite.*

Proof. We will show that there exist a constant C such that for any non-zero integral ideal $\mathfrak{a}$ there exist a integral ideal $\mathfrak{b}$ in the linear equivalence class of $\mathfrak{a}$ such that $\mathrm{N}_K(\mathfrak{a}) \leq C$.

Use Lemma 2.3.4 to find some $C > 0$ such that every non-zero integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ contains an element a with $\mathrm{N}_K(a) \leq C \cdot \mathrm{N}_K(\mathfrak{a})$. Let $\mathfrak{R}$ be an ideal class and find using Lemma 2.3.2 an integral ideal $\mathfrak{a}$ in $\mathfrak{R}^{-1}$. Then choose $a \in \mathfrak{a}$ such that $\mathrm{N}_K(a) \leq C \cdot \mathrm{N}(\mathfrak{a})$. Let $\mathfrak{b} = a\mathcal{O}_K/\mathfrak{a} \in \mathfrak{R}$. Then

$$\mathrm{N}_K(\mathfrak{b}) = \mathrm{N}_K(a\mathcal{O}_K/\mathfrak{a}) = \mathrm{N}_K(a)/\,\mathrm{N}_K(\mathfrak{a}) \leq C.$$

Moreover $\mathfrak{b}$ is in integral ideal, because $\mathfrak{a}$ divides $a\mathcal{O}_K$, as $a\mathcal{O}_K \subseteq \mathfrak{a}$. Since there are only finitely many ideals of bounded norm by Lemma 2.3.5, the class group is finite. □

2.4. Absolute values and places

In this section we introduce the most fundamental notion in the idelic viewpoint: the places of field. We furthermore prove some properties of places.

Definition 2.4.1 (Absolute values)**.** An *absolute value* on a field K is a map $|\cdot| : K \to \mathbb{R}$ which is

1) positive: $|x| \geq 0$ for all $x \in K$;

2) non-degenerate: $|x| = 0$ if and only if $x = 0$ for all $x \in K$;

3) multiplicative: $|xy| = |x||y|$ for all $x, y \in K$;

4) additive: $|x + y| \leq |x| + |y|$ for all $x, y \in K$. △

Example 2.4.2 (Trivial absolute value)**.** Let K be a global field and consider the map $|\cdot|$ defined by $|x| = 1$ for all $x \neq 0$. Then $|\cdot|$ is an absolute value. This absolute value is called the *trivial* absolute value. ◊

Example 2.4.3 (Absolute field norm)**.** From Example 2.2.12, the absolute field norm $\mathrm{N}_{\mathbb{K}} : \mathbb{K} \to \mathbb{Q}_{\geq 0} \cup \infty$ is an absolute value of $\mathbb{K}$. ◊

Example 2.4.4 ($\mathfrak{p}$-adic absolute value)**.** Let K be a global field and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Then consider the map $\mathrm{ord}_{\mathfrak{p}} : K \to \mathbb{Z} \cup \infty$ given by $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$ and $\mathrm{ord}_{\mathfrak{p}}(x) = n_{\mathfrak{p}}$, where $n_{\mathfrak{p}}$ satisfies $x\mathcal{O}_K = \prod_{\mathfrak{q}} \mathfrak{q}^{n_{\mathfrak{q}}}$. Then the map $\mathrm{ord}_{\mathfrak{p}}$ is called the *order at* $\mathfrak{p}$ and satisfies

1) $\mathrm{ord}_{\mathfrak{p}}(x) = \infty$ if and only if $x = 0$;

2) $\mathrm{ord}_{\mathfrak{p}}(xy) = \mathrm{ord}_{\mathfrak{p}}(x) + \mathrm{ord}_{\mathfrak{p}}(y)$;

3) $\mathrm{ord}_{\mathfrak{p}}(x + y) \geq \min\{\mathrm{ord}_{\mathfrak{p}}(x), \mathrm{ord}_{\mathfrak{p}}(y)\}$,

for all $x, y \in K$. Then the map $|x|_{\mathfrak{p}} := \mathrm{N}_K(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)}$ is called the $\mathfrak{p}$-*adic absolute value on* K. From the above properties it is easy to see that $|x|_{\mathfrak{p}}$ is an absolute value. ◊

Let us state some elementary properties of absolute values.

Definition 2.4.5 (Archimedian absolute values)**.** An absolute value $|\cdot|$ on a field is *Archimedian* if and only if $|n|$ is unbounded on the subring generated by 1. △

This subring can not be identified with $\mathbb{Z}$ when the global field has a positive characteristic. The following proposition gives a characterization of Archimedian absolute values.

Proposition 2.4.6. *Let $|\cdot|$ be an absolute value on a field K. Then $|\cdot|$ is non-Archimedian if and only if $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.*

Proof. We will follow the proof in [3]. If $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$, then $|n| \leq 1$ for all n in the subring generated by 1. Thus $|\cdot|$ is non-Archimedian.

Suppose that $|\cdot|$ is non-Archimedian. Then $|n| \leq 1$ for all n in the subring generated by 1, because if $n > 1$ for some n in this subring, we find that $\lim_{k\to\infty} |n^k| = \infty$ which contradicts the fact that $|\cdot|$ is non-Archimedian.

Now let $x, y \in K$ and suppose without loss of generality that $|x| \geq |y|$. Then $|y/x| \leq 1$ and

$$|1 + y/x|^n = |(1 + y/x)^n| \leq \sum_{k=0}^{n} \left| \binom{n}{k} \right| |y/x|^k \leq 1 + \cdots + 1 = n + 1.$$

Thus we find that

$$|1 + y/x| = \lim_{n\to\infty} \sqrt[n]{|1 + y/x|^n} \leq \lim_{n\to\infty} \sqrt[n]{n + 1} = 1 = \max\{1, |y/x|\}.$$

We conclude that $|x + y| \leq \max\{|x|, |y|\}$. □

Notice that an absolute value $|\cdot|$ of a field K induces a topology on K: the coarsest topology such that the sets $\{x \mid |x - a| < r\}$, for all $a \in K$ and $r > 0$, are open.

Definition 2.4.7 (Discrete absolute values)**.** An absolute value $|\cdot|$ on a field is *discrete* if and only if 1 is isolated in the induced topology. △

Places. We will now introduce an equivalence relation on the set of all absolute values of a field. The (non-trivial) equivalence classes are then called the *places* of K.

Definition 2.4.8 (Equivalent absolute values)**.** Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values of a field. Then $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if $|\cdot|_1$ and $|\cdot|_2$ induce the same topology. △

The following proposition gives another characterization of equivalent absolute values.

Proposition 2.4.9. *Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on a field. Then $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there exists a real $c > 0$ such that $|\cdot|_1 = (|\cdot|_2)^c$.*

Proof. See Proposition 1.8 on page 6 of [16]. □

This relation is clearly an equivalence relation, and hence we may consider the equivalence classes.

Definition 2.4.10 (Place)**.** A *place* $\mathfrak{p}$ of a field is the equivalence class of a non-trivial absolute value. A place $\mathfrak{p}$ of a field is called *infinite* if and only if $\mathfrak{p}$ contains an Archimedian absolute value. △

As usual we do not restrict our attention to individual objects, but rather investigate how they interact:

Definition 2.4.11 (Extension of places)**.** Let L/K be an extension of fields, $\mathfrak{p}$ a place of K and $\mathfrak{P}$ a place of L. Then $\mathfrak{P}$ is an *extension* of $\mathfrak{p}$ (notation: $\mathfrak{P}/\mathfrak{p}$) if and only if for all $|\cdot| \in \mathfrak{P}$ the restriction of $|\cdot|$ to K is in $\mathfrak{p}$. △

Later on we will need the following theorem, which is related to the Chinese remainder theorem.

Theorem 2.4.12. *(Approximation theorem) Let $n \geq 1$ be an integer and let $|\cdot|_i$, for $1 \leq i \leq n$, be non-trivial pairwise non-equivalent absolute values on a global field K. Let $x_1, \ldots, x_n \in K$ and $\epsilon > 0$. Then there exists an element $x \in K$ such that $|x - x_i|_i < \epsilon$ for all $1 \leq i \leq n$.*

Proof. See page 35 of Lang [5] or page 48 of [3]. □

This theorem is also called the weak approximation theorem. But since we do not use the strong version (c.f., page 67 of [3]) we suppress 'weak'.

2.5. Valuations

In this section we will prove that the finite places of a given global field K and primes ideals of $\mathcal{O}_K$ are in one-to-one correspondence with each other. This will follow from the fact that both the finite places of K and the prime ideals of $\mathcal{O}_K$ are in bijection with *valuations*.

The consequence of this correspondence is that every notion defined for prime ideals has an immediate generalization to finite places. One can now, for example, define the ramification index of a finite place.

Totally ordered groups. Before we give the definition of a valuation, we first recall the definition of a totally ordered group and maps between them.

Definition 2.5.1 (Totally ordered groups)**.** A *totally ordered group* is an ordered tuple $(\Gamma, \leq, +, 0)$ consisting of a (non-empty) set Γ, a binary relation $\leq$, a binary function $+$ and an element $0 \in \Gamma$ such that

1) $(\Gamma, +, 0)$ is an abelian group;

2) $(\Gamma, \leq)$ is total order;

3) for all $x, y, z \in \Gamma$ we have $x + z \leq y + z$ whenever $x \leq y$. △

Example 2.5.2. The real numbers $\mathbb{R}$ with addition and the usual order is a totally ordered group. ◊

Example 2.5.3 (Hahn product)**.** Let I be an totally ordered index set and $\{\Gamma_i \mid i \in I\}$ a family of totally ordered groups. Then the *Hahn product* or *lexicographic product* is defined by

$$\mathbf{H}_{i\in I}\Gamma_i := \{\alpha \in \textstyle\prod_{i\in I} \Gamma_i \mid \operatorname{supp}(\alpha) \subseteq I \text{ is well-ordered}\},$$

where $\operatorname{supp}(\alpha) = \{i \in I \mid \alpha_i \neq 0\}$ is the *support* of α. Then $\mathbf{H}_{i\in I}\Gamma_i$ is closed under addition, since $\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$ is a well-order: if $I \subseteq \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$, then $\min(I) = \min\{\min(I \cap \operatorname{supp}(\alpha)), \min(I \cap \operatorname{supp}(\beta))\}$. Now define an ordering on $\mathbf{H}_{i\in I}\Gamma_i$ by $\alpha \leq \beta$ if and only if $\alpha_m \leq \beta_m$, with $m = \min(\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta))$. Then $\mathbf{H}_{i\in I}\Gamma_i$ is a totally ordered group. ◊

We conclude this paragraph with the definition of the structure preserving maps between totally ordered groups.

Definition 2.5.4 (Order homomorphisms)**.** Let Γ and Γ' be totally ordered groups. An *order homomorphism* is a order preserving group homomorphism $f : \Gamma \to \Gamma'$. An *order isomorphism* is a order preserving group isomorphism $f : \Gamma \to \Gamma'$. If there exists a order isomorphism $f : \Gamma \to \Gamma'$, then we say that Γ and Γ' are *order isomorphic* (notation: $\Gamma \cong \Gamma'$). △

Valuations. We will now study fields by means of their surjective group homomorphisms form the unit group to a totally ordered group extended with a value ∞ at zero.

Definition 2.5.5 (Valuations)**.** A *valuation* on a field K is a surjective map $v : K \to \Gamma \cup \infty$, with Γ a totally ordered group, such that for all $x, y \in K$

1) $v(x) = \infty$ if and only if $x = 0$;

2) $v(xy) = v(x) + v(y)$;

3) $v(x + y) \geq \min\{v(x), v(y)\}$,

with the convention that $\infty \notin \Gamma$, $\infty \geq x$ and $\infty = x + \infty = \infty + x$ for all $x \in \Gamma \cup \infty$. △

Example 2.5.6 (Order at $\mathfrak{p}$)**.** Let K be a global field and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. Recall from Example 2.4.4 that the order at $\mathfrak{p}$is given by the map $\mathrm{ord}_\mathfrak{p} : K \to \mathbb{Z} \cup \infty$ with $\mathrm{ord}_\mathfrak{p}(0) = \infty$ and $\mathrm{ord}_\mathfrak{p}(x) = n_\mathfrak{p}$, where $n_\mathfrak{p}$ satisfies $x\mathcal{O}_K = \prod_\mathfrak{q} \mathfrak{q}^{n_\mathfrak{q}}$. The map $\mathrm{ord}_\mathfrak{p}$ is a valuation on K. ♢

The first lemma will be useful for determining the value of a sum.

Lemma 2.5.7. *Let v be a valuation on a global field K and let $x, y \in K$. If $v(x) \neq v(y)$ then $v(x + y) = \min\{v(x), v(y)\}$.*

Proof. See page 44 of Cassels and Fröhlich [3]. □

Let us now introduce some notation. Let $v : K \to \Gamma \cup \infty$ be a valuation. Then Γ is called the *value group of* v. The set

$$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$$

is called the *valuation ring of* v. It is easily seen that $\mathcal{O}_v$ is a subring of K. Moreover $\mathcal{O}_v$ is a valuation domain (c.f., Definition 1.9.1), because $v(x) < 0$ implies $v(x^{-1}) > 0$. Proposition 1.9.3 shows that $\mathcal{O}_v$ is a local ring, hence $\mathcal{O}_v$ has a unique maximal ideal. This ideal is given by

$$\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$$

and is called the *valuation ideal of* v. If $x, y \in K$ with $xy = 1$, then $v(x) + v(y) = v(1) = 0$. Hence $x \in \mathcal{O}_v^\times$ if and only if $x \in U_v$, where

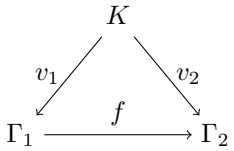
$$U_v := \{x \in K \mid v(x) = 0\}$$

is called the *unit group of* v.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then for notational convenience we will write $\mathcal{O}_\mathfrak{p}$, $\mathfrak{m}_\mathfrak{p}$ and $U_\mathfrak{p}$ for $\mathcal{O}_v$, $\mathfrak{m}_v$ and U_v, whenever $v = \mathrm{ord}_\mathfrak{p}$.

Notice that v and $w = v + v$ both define the same valuation ring and valuation ideal, for every $v : K \to \Gamma$. This comes from the fact that v and w are equivalent, in the following sense:

Definition 2.5.8 (Equivalent valuations)**.** Let $v_i : K \to \Gamma_i$, for $i = 1, 2$, be a valuation on a global field K. Then v_1 and v_2 are equivalent if and only if there exists an order isomorphism $f : \Gamma_1 \to \Gamma_2$ with $v_2 = v_1 \circ f$, i.e., the diagram



commutes. △

Let us now formulate an important property of a valuation.

Definition 2.5.9 (Discrete valuation)**.** A valuation $v : K \to \Gamma \cup \infty$ is called *discrete* if and only if $\Gamma \cong \mathbb{Z}$. △

Recall from Definition 1.9.1, that the valuation ring $\mathcal{O}_v$ is called discrete if and only if $\mathfrak{m}_v$ is principal. The following lemma shows that there is no confusion.

Lemma 2.5.10. *Let $v : K \to \Gamma \cup \infty$ be a valuation. Then v is discrete if and only if $\mathcal{O}_v$ is discrete.*

Proof. Suppose that $\mathcal{O}_v$ is discrete and let π be a generator of $\mathfrak{m}_v$. Then Proposition 1.9.3 shows that $\mathcal{O}_v$ is Noetherian local domain. Let π' be an irreducible element of $\mathcal{O}_v$. Proposition 1.8.2 implies that every non-zero non-unit element is contained in the maximal ideal $\mathfrak{m}_v$. Hence π' is a multiple of π, which shows that π is the unique irreducible element of $\mathcal{O}_v$. Now using Theorem 1.5.5 we see that every $x \in \mathcal{O}_v$ is of the form $u\pi^n$, for some $u \in U_v$ and $n \geq 0$. This implies that Γ is generated by $\pm v(\pi)$ and is isomorphic to $\mathbb{Z}$. Thus v is discrete.

On the other hand, suppose that v is discrete. Let π be an element of $\mathfrak{m}_v$ such that $v(\pi) > 0$ and $\pm v(\pi)$ generate Γ and let $x \in \mathfrak{m}_v$ be arbitrary. Choose $n \geq 0$ such that $v(x) = v(\pi)^n$. Consider x/π^n in K. We have $v(x/\pi^n) = 0$ which shows that $u = x/\pi^n \in U_v$. Thus every $x \in \mathfrak{m}_v$ is a multiple of π. We conclude that π is a generator of $\mathfrak{m}_v$. □

Theorem 2.5.11. *Every valuation on a global field is discrete.*

Proof. Let K be a global field and v a valuation on K with values in Γ. Using Lemma 2.5.10 it suffices to prove that $\mathcal{O}_v$ is discrete an using Proposition 1.9.3 it suffices to prove that $\mathcal{O}_v$ is Noetherian.

Given a chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$ of ideals in $\mathcal{O}_v$. Using Lemma 2.1.4 this gives rise to a decreasing sequence of natural numbers $|\mathcal{O}_K/\mathfrak{a}_0| \geq |\mathcal{O}_K/\mathfrak{a}_1| \geq \cdots$. Since $\leq$ is a well-order of $\mathbb{N}$, this sequence has a least element at which it stabilizes. But $|\mathcal{O}_v/\mathfrak{a}_i| = |\mathcal{O}_v/\mathfrak{a}_j|$ and $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ imply that $\mathfrak{a}_i = \mathfrak{a}_j$, for all $i < j$. Therefore the chain stabilizes and $\mathcal{O}_v$ is Noetherian. Then concludes the proof of the theorem. □

Theorem 2.5.11 implies that every valuation on a global field K is equivalent to a valuation with value group $\mathbb{Z}$.

Primes and finite places. The following proposition shows that the valuations of a global field correspond to the finite places.

Proposition 2.5.12. *Let K be a global field and $0 < c < 1$ a real number. Then there is a one-to-one correspondence*

$$\begin{array}{ccc} \{ \textit{ valuations } v : K \to \mathbb{Z} \cup \infty \ \} & \longleftrightarrow & \{ \textit{ finite places of } K \ \} \\ v & \mapsto & [c^{v(\cdot)}] \\ \log_c(|\cdot|) & \hookleftarrow & \mathfrak{p} \end{array}$$

where $c^\infty = 0$ and $|\cdot|$ is an absolute value in $\mathfrak{p}$ with $\log_c(|K^\times|) = \mathbb{Z}$.

Proof. We first show that both maps are well-defined. Let $v : K \to \mathbb{Z} \cup \infty$ be a valuation. Then $c^{v(\cdot)}$ is a non-Archimedian absolute value on K and $[c^{v(\cdot)/v(\pi)}]$ is a finite place of K. For the other map, let $\mathfrak{p}$ be a finite place of K. Let $||\cdot||$ is an absolute value in $\mathfrak{p}$. Then Proposition 2.4.6 shows that $\log_c(||\cdot||)$ is a valuation on K with value group $\log_c(||K^\times||) \subseteq \mathbb{R}$. Now Theorem 2.5.11 shows that $\log_c(||\cdot||)$ is discrete, which implies that $\log_c(||K^\times||) = \lambda\mathbb{Z}$. Then $|\cdot| = (||\cdot||)^{1/\lambda}$ is an absolute value in $\mathfrak{p}$ such that $\log_c(|\cdot|) = \frac{1}{\lambda}\log_c(||\cdot||) = \mathbb{Z}$. Thus the maps are well-defined.

Finally we show that the maps are each others inverse. Let $\mathfrak{p}$ be a finite place of K. Then $\mathfrak{p}$ is mapped to $v = \log_c(|\cdot|)$, which is mapped back to $\mathfrak{q} = [c^{v(\cdot)}] = [|\cdot|] = \mathfrak{p}$. For the other map, let $v : K \to \mathbb{Z} \cup \infty$ be a valuation. Then v is mapped to $\mathfrak{p} = [c^{v(\cdot)}]$. Now let $|\cdot|$ be an absolute value in $\mathfrak{p}$ with $\log_c(|K^\times|) = \mathbb{Z}$. Then $|\cdot|$ and $c^{v(\cdot)}$ are equivalent absolute values. Thus $|\cdot|_\mathfrak{p} = c^{t\cdot v(\cdot)}$, for some real $t > 0$. Hence $w = \log_c(|\cdot|_\mathfrak{p}) = t \cdot v(\cdot)$. Hence v and w are equivalent valuations, because $f : x \mapsto t \cdot x$ is an order isomorphism from $\mathbb{Z}$ to $\log_c(|K^\times|)$. □

Other authors (e.g., Lang in [5]) define a valuation to be a non-Archimedian absolute value. This proposition shows that our terminology is essentially the same. However others (e.g., Cassels in Chapter II of [3]) use the term valuation for an absolute value, non-Archimedian or not. To distinguish our notion of a valuation with the definition of a valuation as an absolute value we may say that the valuation is additive (see Definition 2.5.5).

The next proposition shows that valuations are essentially the same things as prime ideals in the ring of integers.

Proposition 2.5.13. *Let K be a global field and $\mathcal{O}_K$ the ring of integers of K. Then there is a one-to-one correspondence*

$$\begin{array}{ccc} \{ \text{ valuations } v : K \to \mathbb{Z} \cup \infty \ \} & \longleftrightarrow & \{ \text{ prime ideals of } \mathcal{O}_K \ \} \\ v & \mapsto & \mathfrak{m}_v \cap \mathcal{O}_K \\ \mathrm{ord}_\mathfrak{p} & \hookleftarrow & \mathfrak{p} \end{array}$$

Proof. We first show that the maps are well-defined. It is clear that $\mathfrak{p} \mapsto \mathrm{ord}_\mathfrak{p}$ is well defined. Let v be a valuation of K. Write $\mathfrak{p}_v := \mathfrak{m}_v \cap \mathcal{O}_K$ and let $x, y \in \mathcal{O}_K$ with $xy \in \mathfrak{p}_v$. Then $v(x) + v(y) = v(xy) > 0$, which implies that either $v(x) > 0$ or $v(y) > 0$. Hence we find that either $x \in \mathfrak{p}_v$ or $y \in \mathfrak{p}_v$ which shows that $\mathfrak{p}_v$ is a prime ideal of $\mathcal{O}_K$.

It remains to show that the maps are each others inverse. Let $v : K \to \mathbb{Z} \cup \infty$ be an absolute value. We will prove that $v = \mathrm{ord}_{\mathfrak{p}_v}$. Since K is the field of fractions of $\mathcal{O}_K$, it suffices to show that v and $\mathrm{ord}_{\mathfrak{p}_v}$ coincide on $\mathcal{O}_K$. Since $v(\mathcal{O}_K) = \mathbb{N}$ it suffices to prove that $v(x) = 1$ if and only if $\mathrm{ord}_{\mathfrak{p}_v}(x) = 1$ for all $x \in \mathcal{O}_K$. In other words $x \in \mathfrak{m}_v - \mathfrak{m}_v^2$ if and only if $x \in \mathfrak{p}_v - \mathfrak{p}_v^2$, for all $x \in \mathcal{O}_K$.

Clearly, as $\mathfrak{p}_v := \mathfrak{m}_v \cap \mathcal{O}_K$ we have $x \in \mathfrak{m}_v$ if and only if $x \in \mathfrak{p}_v$. Moreover we have for all $x \in \mathcal{O}_K$ that $x \in \mathfrak{m}_v^2$ if and only if $x \in \mathfrak{p}_v^2$. Indeed, suppose that $x \in \mathfrak{p}_v^2$. Then trivially $x \in \mathfrak{m}_v^2$. On the other hand suppose that $x \in \mathfrak{m}_v^2$. Since $x \in K$, there exists some $a, b \in \mathcal{O}_K$ with $x = (a/b)^2$. Let $\pi \in K$ with $v(\pi) = 1$. Then $x = (a'/b')^2$ with $a' = \pi^n a$, $b' = \pi^n b$ and $n = -v(b)$. Then $v(a') > v(b') = 0$. This shows that $a'/b' \in \mathcal{O}_v$, which implies that $x \in \mathfrak{p}_v^2$. We conclude that $v = \mathrm{ord}_{\mathfrak{p}_v}$.

For the other direction, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ is mapped to $v = \mathrm{ord}_\mathfrak{p}$ and v is mapped to $\mathfrak{m}_v \cap \mathcal{O}_K = \{x \in \mathcal{O}_K \mid \mathrm{ord}_\mathfrak{p}(x) > 0\} = \mathfrak{p}$.

We conclude that the maps are each others inverse, which shows that there is a one-to-one correspondence. □

Let us gather the results from the Proposition 2.5.12 and Proposition 2.5.13 into a single theorem:

Theorem 2.5.14. *Let K be a global field and $\mathcal{O}_K$ the ring of integers of K. Then the maps*

$$\begin{array}{ccccccc} \{ \text{ valuations } \} & \longleftarrow & \{ \text{ prime ideals } \} & \longrightarrow & \{ \text{ finite places } \} \\ \mathrm{ord}_\mathfrak{p} & \hookleftarrow & \mathfrak{p} & \mapsto & |\cdot|_\mathfrak{p} \end{array}$$

are bijections.

We now know how valuations are related to prime ideals of $\mathcal{O}_K$ and finite places of K for any global field K. We will now investigate some properties about the valuations themselves.

Valuation domains. The following result from Krull is fundamental. It gives a characterization of the valuation domains (c.f., Definition 1.9.1).

Theorem 2.5.15 (Krull)**.** *Let R be a domain with field of fractions K. Then R is a valuation domain if and only if $R = \mathcal{O}_v$ for some valuation v on K.*

Proof. If $R = \mathcal{O}_v$ for some valuation v on K, then for all non-zero $x \in K$ we have that $x \notin R$ implies $v(x) < 0$ hence $v(1/x) > 0$ and $1/x \in R$.

On the other hand suppose that R satisfies $x \in R$ or $1/x \in R$ for all nonzero $x \in K$. We now follow the construction on page 65 of [4]. Define $\Gamma = K^\times/R^\times$ and define an ordering on Γ by $aR^\times \leq bR^\times$ for $a, b \in K^\times$ if and only if $b/a \in R$. Using the fact that R is a valuation domain (see Definition 1.9.1), it is straightforward to see that Γ is a totally ordered abelian group. The map $v : K \to \Gamma \cup \infty$ given by $v(a) = aR^\times$ and $v(0) = \infty$ is a valuation on K. It is easy to see that $R = \mathcal{O}_v$. □

Corollary 2.5.16. *Let R be a subring of a global field K. Then R is a valuation domain if and only if $R = \mathcal{O}_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*

Proof. It is clear that $\mathcal{O}_\mathfrak{p}$ is a valuation domain for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Conversely, let R be a valuation domain. Then Theorem 2.5.15 gives a valuation v on K with $R = \mathcal{O}_v$.

Using Proposition 2.5.13 find a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that v corresponds to $\mathfrak{p}$. Hence we have $v = \mathrm{ord}_\mathfrak{p}$ and $R = \mathcal{O}_v = \mathcal{O}_\mathfrak{p}$. □

2.6. Local fields

In this section we will introduce the notion of a *local field*, which is the completion of a global field with respect to a non-trivial absolute value. It turns out that the structure of local fields is easier then that of global field. For example, if L/K is an extension of global fields, then a finite place $\mathfrak{p}$ of K has $[L : K]$ extensions to L. while if L/K is an extension of local fields, a place $\mathfrak{p}$ of K has a unique extension to L.

Completion. Before we dive into the construction of the completion, we start with the definition of valued fields.

Definition 2.6.1 (Valued fields)**.** A *valued field* is a field K together with an absolute value $|\cdot|_k$ of K. △

Example 2.6.2. The rational numbers $\mathbb{Q}$ and real numbers $\mathbb{R}$, with the usual absolute value, is a valued field. The complex numbers $\mathbb{C}$, with the absolute value $|z| = z\overline{z}$, is a valued field. ◊

Now we introduce the structure preserving maps between valued fields.

Definition 2.6.3 (Valued field embedding)**.** Let K and L be valued fields with absolute values $|\cdot|_k$ and $|\cdot|_\ell$ respectively. A map $f : K \to L$ is called a *continuous homomorphism* of valued fields if and only if

1) f is a homomorphism of fields;

2) f is continuous, i.e., there exists a $c > 0$ such that $|f(x)|_\ell = |x|_k^c$ for all $x \in K$.

Let $f : K \to L$ be an embedding. Then f is called an *continuous isomorphism* of valued fields (notation $f : K \cong L$) if and only if there exists an embedding $g : L \to K$ with $g \circ f = \mathrm{id}_K$ and $f \circ g = \mathrm{id}_L$. In this case f is called *invertible*. Let $f : K \to L$ be an continuous isomorphism. Then f is called an *continuous automorphism* of valued fields if and only if $L = K$. △

Before we give some examples, we recall the some definitions from the theory of metric spaces. Let $(x_n)_{n\geq 0}$ be a sequence in a valued field K with absolute value $|\cdot|$. Then $(x_n)_{n\geq 0}$ is called *convergent* with limit $x \in K$ (notation: $\lim_{n\to\infty} x_n = x$) if and only if for all real $\epsilon > 0$ there exists an integer $N \geq 0$ such that $|x - x_n| < \epsilon$ for all $n \geq N$. Furthermore $(x_n)_{n\geq 0}$ is called *Cauchy* if and only if for all real $\epsilon > 0$ there exists an integer $N \geq 0$ such that $|x_m - x_n| < \epsilon$ for all $m, n \geq N$. A subset $A \subseteq K$ is called *dense* if and only if for every $x \in K$ there exists a sequence $(a_n)_{n\geq n}$ in A such that $\lim_{n\to\infty} a_n = x$.

Example 2.6.4 (Automorphisms of $\mathbb{R}$)**.** The identity $\mathrm{id} : \mathbb{R} \to \mathbb{R}$ is the unique continuous automorphism of $\mathbb{R}$. Let K be a valued field with absolute value $|\cdot|_k$ and let $f : \mathbb{R} \to K$ be an continuous homomorphism of valued fields. We will show that f is unique.

Since f is a ring homomorphism, we have that $f(1) = 1$. From $f(-1) + 1 = f(-1) + f(1) = f(0) = 0$ it follows that $f(-1) = -1$. Hence f is completely determined on $\mathbb{Z}$. Moreover since $f(a/b) \cdot f(b) = f(a)$ for all $a, b \in \mathbb{Z}$, we find that f is completely determined on $\mathbb{Q}$. Now let $x \in \mathbb{R}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we find a sequence $(q_n)_{n\geq 0}$ which converges to x. Then we have that

$$\lim_{n\to\infty} |f(q_n) - f(x)|_k = \lim_{n\to\infty} |f(q_n - x)|_k = \lim_{n\to\infty} |q_n - x| = 0,$$

since $|f(\cdot)|_k$ is equivalent to $|\cdot|$ on $\mathbb{R}$. Thus $(f(q_n))_{n\geq 0}$ converges to $f(x)$. Hence, since f is completely determined on $\mathbb{Q}$, we find that f is completely determined on $\mathbb{R}$. Moreover this shows that the identity is the unique continuous automorphism of $\mathbb{R}$. ◊

Example 2.6.5 (Automorphisms of $\mathbb{C}$)**.** Let $f : \mathbb{C} \to \mathbb{C}$ be an continuous automorphism of valued fields. If we apply Example 2.6.4 to the restriction $f_{|\mathbb{R}} : \mathbb{R} \to \mathbb{C}$ of f to $\mathbb{R}$, we find that $f(a) = a$ for all $a \in \mathbb{R}$. Furthermore notice that $f(i^2 + 1) = f(0) = 0$ which implies that $f(i)^2 + 1 = 0$, as f is a homomorphism. In other words, $f(i)$ is a root of $X^2 + 1 = (X + i)(X - i)$. Therefore we have that $f(i) = \pm i$. Hence we conclude from Example 2.6.4 that for all $a, b \in \mathbb{R}$

$$f(a + bi) = f(a) + f(b)f(i) = a \pm bi.$$

This shows that the identity and conjugation are the only continuous automorphisms of $\mathbb{C}$. ◊

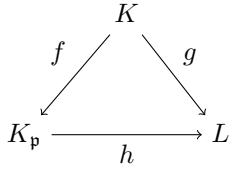
Let us now investigate an important property of a valued field.

Definition 2.6.6 (Completeness)**.** A valued field K is called *complete* if and only if every Cauchy sequence is convergent. △

It turns out that every valued field can be embedded in a complete valued field.

Theorem 2.6.7. *Let K be a valued field with absolute value $|\cdot|$. Then there exists an embedding $f : K \to \hat{K}$ of valued fields such that*

1) *$\hat{K}$ is complete and $f(K)$ is dense in $\hat{K}$;*
2) *for every embedding g from K into a complete valued field L there exists a unique embedding $h : \hat{K} \to L$ such that $h \circ f = g$, i.e., the diagram*



commutes.

Proof. We follow the proof of Theorem 2.1 on page 12 of [16]. Let R be the ring of all Cauchy sequences in K with componentwise addition and multiplication. Then the ideal $\mathfrak{m} = \{(x_n)_{n\geq 0} \in R \mid \lim_{n\to\infty} |x_i|_{\mathfrak{p}} = 0\}$ is a maximal ideal in R. Consider

the field $\hat{K} := R/\mathfrak{m}$ and the ring homomorphism $f : K \to R/\mathfrak{m}$ which maps $x \in K$ to the constant sequence $(x)_{n\geq 0}$. Define the absolute value $||\cdot||$ on $R/\mathfrak{m}$ by

$$||(x_n)_{n\geq 0} + \mathfrak{m}|| := \lim_{n\to\infty} |x_n|.$$

It is easy to see that $||\cdot||$ is indeed a well-defined absolute value with $||f(x)|| = |x|$ and that f is an embedding of valued fields.

Note that $f(K)$ is dense in $\hat{K}$, since every element $(x_n)_{n\geq 0} + \mathfrak{m}$ in $\hat{K}$ is the limit of the sequence $(f(x_n))_{n\geq 0}$ in K. Now, let $(s_n)_{n\geq 0}$ be a Cauchy sequence in $\hat{K}$. Then, since $f(K)$ is dense in $\hat{K}$, there exists a sequence $(s'_n)_{n\geq 0}$ in $f(K)$ with $||s_n - s'_n|| < 1/n$ for all $n \geq 0$. Write $s'_n = f(x_n)$. Then $(s_n)_{n\geq 0}$ converges to $s = (x_n)_{n\geq 0}$. Therefore $\hat{K}$ is complete with respect to $|\cdot|$.

Finally let g be an embedding from K into a complete valued field L. Then the canonical map $h : R \to L$ sending $(x_n)_{n\geq 0}$ to $\lim_{n\to\infty} x_n$ gives rise to an embedding $h : \hat{K} = R/\mathfrak{m} \to L$. As $f(K)$ is dense in $\hat{K}$, this is the unique embedding. It is clear that $h(f(x)) = g(x)$ for all $x \in K$, which implies that the diagram commutes. □

The $\hat{K}$ together with the embedding $f : K \to \hat{K}$ is called a *completion* of K. The second statement in the theorem is called the *universal property* of $f : K \to \hat{K}$.

The universal property implies that the completion $\hat{K}$ is uniquely determined up to a continuous isomorphism.

Lemma 2.6.8. *Let K be a field, K_i a valued field with $|\cdot|_i$ absolute value and base field K and let $f_i : K_i \to \hat{K}_i$ the completion for $i = 1, 2$. Then if $|\cdot|_1$ is equivalent to $|\cdot|_2$, then $\hat{K}_1 \cong \hat{K}_2$.*

Proof. Suppose that $|\cdot|_i$ is equivalent to $|\cdot|_2$. Then $\mathrm{id}_K : K_1 \to K_2$ is an isomorphism of valued fields. Hence we have the following diagram

$$\begin{array}{ccccc} K_i & \xrightarrow{\mathrm{id}_K} & K_j & \xrightarrow{\mathrm{id}_K} & K_i \\ {\scriptstyle f_i}\downarrow & & {\scriptstyle f_j}\downarrow & & {\scriptstyle f_i}\downarrow \\ \hat{K}_i & & \hat{K}_j & & \hat{K}_i \end{array}$$

Then the universal property of $\hat{K}_i$ applied to $f_i \circ \mathrm{id}_K$ gives a map $h_i : \hat{K}_i \to \hat{K}_j$, for $i \neq j$. Hence we find an embedding $h_j \circ h_i : \hat{K}_i \to \hat{K}_i$. Now if we apply the univeral property of $\hat{K}_i$ to $f_i \circ \mathrm{id}_K \circ \mathrm{id}_K$ we conclude that $h_j \circ h_i$ is unique. Trivially we have an embedding $\mathrm{id}_{\hat{K}_i} : \hat{K}_i \to \hat{K}_i$, hence by the uniqueness we find that $h_j \circ h_i = \mathrm{id}_{\hat{K}_i}$. This proves that h_i is an isomorphism and that $\hat{K}_1 \cong \hat{K}_2$. □

Let $\mathfrak{p}$ be a place of a valued field K. Then for any $|\cdot| \in \mathfrak{p}$ we can construct that completion. The above lemma shows that all completions are isomorphic. This enables us to define the *completion at* $\mathfrak{p}$: $K_\mathfrak{p}$.

From the proof of Theorem 2.6.7 we see that the following stronger version of the universal property is also true.

Proposition 2.6.9. *Let K be a valued field and $\mathfrak{p}$ a place of K. Then for every continuous map g from K into a complete valued field L there exists a unique continuous map $h : K_\mathfrak{p} \to L$ such that $h \circ f = g$*

Proof. Substitute 'continuous map' for 'embedding' in the last part of the proof of Theorem 2.6.7. □

This proposition enables us to lift an arbitrary continuous map from a valued field K into a complete valued field to a map defined on the completion of K.

Example 2.6.10 (Local norm map)**.** Let L/K be an extension of global fields and $\mathfrak{p}$ a prime of $\mathfrak{p}$. Then the relative field norm $\mathrm{N}_{L/K} : L \to K$ defines a homomorphism from $L \to K_\mathfrak{p}$, which is continuous by part 1 of Theorem 2.2.5. Proposition 2.6.9 gives us a lift $\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} : L_\mathfrak{P} \to K_\mathfrak{p}$ of $\mathrm{N}_{L/K}$, where $\mathfrak{P}$ is extension of $\mathfrak{p}$ to L. Then $\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}$ is called the *local norm map.* ◊

A useful property of complete valued field is the following.

Theorem 2.6.11. *Let $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ be an extension of local fields. Then $\mathfrak{P}$ is the unique place that extends $\mathfrak{p}$.*

Proof. Since $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ be an extension, $L_{\mathfrak{P}}$ can be viewed as a vector space over $K_{\mathfrak{p}}$. Then any absolute value on $L_{\mathfrak{P}}$ may be regarded as a norm on the $K_{\mathfrak{p}}$-vector space $L_{\mathfrak{P}}$. Proposition 2.2 at page 470 of [6] shows that all norms on $L_{\mathfrak{P}}$ are equivalent, which implies that $\mathfrak{P}$ consists of all non-trivial absolute values. □

The following theorem is very useful for the classification of infinite places.

Theorem 2.6.12 (Ostrowski)**.** *Let K be a field and $\mathfrak{p}$ an infinite place of K. Then $K_{\mathfrak{p}} \cong \mathbb{R}$ or $K_{\mathfrak{p}} \cong \mathbb{C}$ as valued fields.*

Proof. See Theorem 2.2 on page 13 of [16]. □

This leads to the following definition.

Definition 2.6.13. Let K be a field and $\mathfrak{p}$ an infinite place of K. Then $\mathfrak{p}$ is called *real* if and only if $K_{\mathfrak{p}} \cong \mathbb{R}$. Furthermore $\mathfrak{p}$ is called *complex* if and only if $K_{\mathfrak{p}} \cong \mathbb{C}$. △

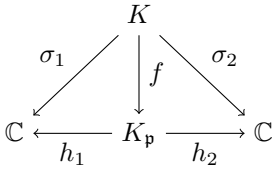
We are now ready to classify the infinite places of any field.

Corollary 2.6.14. *Let K be a field and $|\cdot|$ the standard absolute value on $\mathbb{C}$. Then the map*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{ring homomorphisms} \\ K \to \mathbb{C} \textit{ up to conjugation} \end{array} \right\} & \longrightarrow & \{ \textit{ infinite places of } K \} \\ \sigma & \mapsto & [|\sigma(\cdot)|] \end{array}$$

is a bijection.

Proof. It is clear that $|\sigma(x)|$ is an absolute value on K. Using Ostrowski's theorem we conclude that the map is surjective. We show that the map is injective. Let σ_1 and σ_2 be homomorphisms such that $|\sigma_1(x)|$ and $|\sigma_2(x)|$ are equivalent and let $\mathfrak{p}$ be the place that contains both $|\sigma_1(x)|$ and $|\sigma_2(x)|$. Then $\sigma_i : K \to \mathbb{C}$ is a continuous homomorphism of valued fields. Hence by the second part of Theorem 2.6.7 we find unique continuous homomorphisms f, h_1 and h_2 such that the diagram



commutes. Now Theorem 2.6.12 shows that $K_{\mathfrak{p}} \cong \mathbb{R}$ or $K_{\mathfrak{p}} \cong \mathbb{C}$ as valued fields.

Suppose that $\mathfrak{p}$ is real. Then Example 2.6.4 shows that $h_1 = h_2$, since there is a unique continuous homomorphisms from $\mathbb{R}$ to $\mathbb{C}$. Hence we have that $\sigma_1 = \sigma_2$, as the diagram commutes.

Now suppose that $\mathfrak{p}$ is complex. In that case $\sigma_i : K \to \mathbb{C}$ is also a completion. Hence Theorem 2.6.7 gives unique continuous homomorphisms $h_i' : \mathbb{C} \to K_{\mathfrak{p}}$. Now we find a unique continuous homomorphisms $h_i' \circ h_i : K_{\mathfrak{p}} \to K_{\mathfrak{p}}$ and $h_i \circ h_i' : \mathbb{C} \to \mathbb{C}$. But we also have $\mathrm{id}_{K_{\mathfrak{p}}} : K_{\mathfrak{p}} \to K_{\mathfrak{p}}$ and $\mathrm{id}_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$. Hence from the unicity it follows that $h_i' \circ h_i = \mathrm{id}_{K_{\mathfrak{p}}}$ and $h_i \circ h_i' = \mathrm{id}_{\mathbb{C}}$. Therefore h_1 and h_2 are continuous isomorphisms of valued fields. Now we find that $h_2 \circ h_1' \circ \sigma_1 = \sigma_2$. To conclude the proof notice that $h_2 \circ h_1'$ is an continuous automorphism of $\mathbb{C}$. Hence Example 2.6.5 shows that $h_2 \circ h_1'$ is either the identity or conjugation. Therefore σ_1 and σ_2 are identical up to conjugation. □

Let K be a global field and $\mathfrak{p}$ a finite place. Recall that $\mathcal{O}_K = \{x \in K \mid \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p}\}$. Using Proposition 2.6.9 we find a lift of $\mathrm{ord}_{\mathfrak{p}}$ to $K_{\mathfrak{p}}$. This enables us to define the ring of integers in $K_{\mathfrak{p}}$ by $\mathcal{O}_{K_{\mathfrak{p}}} = \{x \in K_{\mathfrak{p}} \mid \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p}\}$.

Recall that the residue class field of K at a prime ideal $\mathfrak{p}$ is defined by $\overline{K}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{q}$, where $\mathfrak{q} := \{x \in \mathcal{O}_K \mid |x|_\mathfrak{p} < 1\}$ is the prime ideal of $\mathcal{O}_K$ corresponding to the place $\mathfrak{p}$. We can do the same construction in the completion, which leads to the same residue class field: $\overline{K}_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}}/\hat{\mathfrak{q}}$, where $\hat{\mathfrak{q}} := \{x \in \mathcal{O}_{K_\mathfrak{p}} \mid |x|_\mathfrak{p} < 1\}$.

Let f be a polynomial over $\mathcal{O}_{K_\mathfrak{p}}$. Then f is called *primitive* if and only if $f' \not\equiv 0$ modulo $\mathfrak{p}$. The following theorem provides a strong connection between the primitive polynomials over $\mathcal{O}_{K_\mathfrak{p}}$ and the polynomials over $\overline{K}_\mathfrak{p}$.

Theorem 2.6.15 (Hensel's lemma)**.** *Let K be a global field, let $\mathfrak{p}$ be a finite place, let $\mathcal{O}_{K_\mathfrak{p}}$ be the ring of integers of $K_\mathfrak{p}$ and let $\overline{K}_\mathfrak{p}$ the residue class field of K at $\mathfrak{p}$. If a primitive polynomial $f \in \mathcal{O}_{K_\mathfrak{p}}[X]$ admits modulo $\mathfrak{p}$ a factorization*

$$f \equiv \bar{g}\bar{h} \pmod{\mathfrak{p}}$$

into relatively prime polynomials $\bar{g}, \bar{h} \in \overline{K}_\mathfrak{p}[X]$, then f admits a factorization

$$f = gh,$$

with $g, h \in \mathcal{O}_{K_\mathfrak{p}}[X]$ such that $\deg g = \deg \bar{g}$ and

$$g \equiv \bar{g} \pmod{\mathfrak{p}} \qquad h \equiv \bar{h} \pmod{\mathfrak{p}}.$$

Proof. See Theorem 4.6 at page 129 of Neukirch [10]. □

We want to mention one last theorem:

Theorem 2.6.16 (Fundamental formula)**.** *Let L/K be an extension of global fields and $\mathfrak{p}$ a finite place. Then*

$$e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [L_\mathfrak{P} : K_\mathfrak{p}]$$

for all extensions $\mathfrak{P}$ of $\mathfrak{p}$.

Proof. See Theorem 2.5.11 and Proposition 6.8 at page 150 of Neukirch [10]. □

2.7. Ray class groups

In this section we will generalize the class group by considering it as a member of a family of ray class groups. This family is parameterized by a modulus. From now on we will abbreviate 'all but finitely many' by 'almost all'.

Definition 2.7.1 (Moduli)**.** A *modulus* of K is a map $\mathfrak{m} : \{\text{places of } K\} \to \mathbb{N}$, such that $\mathfrak{m}(\mathfrak{p}) = 0$ for almost all places $\mathfrak{p}$ of K. A modulus is denoted as the formal product $\prod_\mathfrak{p} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$. The restriction $\mathfrak{m}_0$ of $\mathfrak{p}$ to the finite places is called the *finite part* of $\mathfrak{m}$. △

The finite places are in one-to-one correspondence with the prime ideals of $\mathcal{O}_K$ and the Archimedian places are in one-to-one correspondence with embeddings $\sigma : K \to \mathbb{C}$. Hence we may factor the modulus $\mathfrak{m}$ as

$$\mathfrak{m} = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \mathfrak{p}^{m(\mathfrak{p})} \prod_{\sigma : K \to \mathbb{C}} \sigma^{m(\sigma)}$$

Let $\mathfrak{p}$ be a finite place of a global field K and let $m \geq 1$ be an integer. Then define the following subset of $K^\times$:

$$V_\mathfrak{p}^m := \{x \in K^\times \mid \operatorname{ord}_\mathfrak{p}(x-1) \geq m\}.$$

Note that $V_\mathfrak{p}^m$ is in fact a subgroup of $K^\times$. Indeed, $1 \in V_\mathfrak{p}^m$, because $\operatorname{ord}_\mathfrak{p}(1-1) = \infty \geq m$. Furthermore for all $x, y \in V_\mathfrak{p}^m$ we have that

$$\operatorname{ord}_\mathfrak{p}(xy-1) = \operatorname{ord}_\mathfrak{p}((x-1)(y-1) + (x-1) + (y-1)) \geq \min\{m^2, m, m\} = m.$$

Finally, for all $x \in V_\mathfrak{p}^m$ we have

$$\operatorname{ord}_\mathfrak{p}(1/x - 1) = \operatorname{ord}_\mathfrak{p}(-(x-1)/x) = \operatorname{ord}_\mathfrak{p}(x-1) - \operatorname{ord}_\mathfrak{p}(x) \geq m - 0,$$

because $\operatorname{ord}_\mathfrak{p}(x-1) \geq m \geq 1$ implies $\mathfrak{p} \mid (x-1)$ and $x - 1 \in \mathfrak{p}$ and $x \notin \mathfrak{p}$ and $\operatorname{ord}_\mathfrak{p}(x) = 0$. Therefore $V_\mathfrak{p}^m$ is a subgroup of $K^\times$. Hence we may define the following:

Definition 2.7.2 (Congruence)**.** Let K be a global field, let x and y in $K^\times$ be units and let $\mathfrak{m}$ be modulus of K. Then x is *(multiplicatively) congruent* to y modulo $\mathfrak{m}$ (notation: $x \equiv y \mod \mathfrak{m}$) if and only if the following two conditions hold:

1) If $\mathfrak{p} \mid \mathfrak{m}$ is a finite place, then $x/y \in V_\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$;

2) If $\mathfrak{p} \mid \mathfrak{m}$ is a real place corresponding to the embedding $\sigma : K \to \mathbb{R}$, then $\sigma(x/y) > 0$. △

Note that $\equiv$ coincides with the usual

With the help of moduli and congruences, we are able to reformulate the approximation theorem.

Theorem 2.7.3 (Chinese remainder theorem for places)**.** *Let $\mathfrak{m}$ be a modulus on a global field K and let $x_\mathfrak{p} \in K$ for all places $\mathfrak{p}$ of K. Then there exists an element $x \in K$ such that for all $\mathfrak{p}$*

$$x \equiv x_\mathfrak{p} \mod \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}.$$

Proof. Use the approximation theorem and the fact that $\mathrm{ord}_\mathfrak{p}(\cdot) = \log_c(|\cdot|_\mathfrak{p})$ with $c = \mathrm{N}_K(\mathfrak{p})^{-1}$. □

Let $K_\mathfrak{m}$ denote the set of $k \in K^\times$ such that $k \equiv 1 \mod \mathfrak{m}$. This is clearly a subgroup of $K^\times$. Now we are ready to define the ray class groups. Let

$$I(\mathfrak{m}) = \{\mathfrak{a} \in I \mid \mathfrak{a} \text{ and } \mathfrak{m}_0 \text{ coprime}\}$$

denote the subgroup of I of fractional ideals of $\mathcal{O}_K$ relatively prime to the finite part of $\mathfrak{m}$. Then the group $I(\mathfrak{m})$ is the free abelian group generated by the prime ideals of $\mathcal{O}_K$ which do not divide the finite part of $\mathfrak{m}$. Furthermore let

$$P_\mathfrak{m} = \{k\mathcal{O}_K \mid k \in K_\mathfrak{m}\}$$

denote the subgroup of $I(\mathfrak{m})$ of principal fractional ideals with generator congruent to 1 modulo the finite part of $\mathfrak{m}$ and positive at the real places occurring in $\mathfrak{m}$. Note that $I(\mathfrak{m})$ is abelian, hence the subgroup $P_\mathfrak{m}$ is normal and we may consider the following definition.

Definition 2.7.4 (Ray class groups)**.** Let K be a global field and $\mathfrak{m}$ a modulus. Then the *ray class group* $\mathcal{C}l_\mathfrak{m}(K)$ of K modulo $\mathfrak{m}$ is the quotient $I(\mathfrak{m})/P_\mathfrak{m}$. Elements of $\mathcal{C}l_\mathfrak{m}(K)$ are called *ray classes*. The order $h_\mathfrak{m}$ of $\mathcal{C}l_\mathfrak{m}(K)$ is called the *ray class number*. △

The following theorem shows that the ray class group is finite.

Theorem 2.7.5. *The ray class group $\mathcal{C}l_\mathfrak{m}(K)$ is a finite group.*

Proof. In [5, pp. 124-126] it is shown that $h_\mathfrak{m}$ is a (rational) multiple of the order h of $\mathcal{C}l(K)$ and hence finite. □

2.8. Adèles and idèles

In the previous section, we fixed one place $\mathfrak{p}$ of a global field K and investigated the local field $K_\mathfrak{p}$. We will now study all local fields simultaneously by considering the ring of adèles, which is a subspace of $\prod_\mathfrak{p} K_\mathfrak{p}$. The reason we will not consider the whole product space is because is not locally compact, but we will not go into this. We start with a topological construction:

Definition 2.8.1 (Restricted topological product)**.** Let S be a finite subset of an index set I. Let G_i be a locally compact group for all $i \in I$ and for all $i \notin S$ let K_i be a compact subgroup of G_i. Then the group

$$\{\ (g_i)_i \in \textstyle\prod_i G_i \mid g_i \in K_i \text{ for almost all } i \notin S\ \}$$

with topology generated from the open sets $\prod_i U_i$, where $U_i \subseteq G_i$ is open for all $i \in I$ and $U_i = K_i$ for all $i \notin S$, is called the *restricted topological product* of the G_i with respect to the K_i. △

Using this construction, we may define the ring of adèles.

Definition 2.8.2 (Adèle ring)**.** The *adèle ring* $\mathcal{A}_K$ of a global field K is the restricted topological product (over all places $\mathfrak{p}$ of K) of the $K_\mathfrak{p}$ with respect to the $\mathcal{O}_\mathfrak{p}$ with $\mathfrak{p}$ infinite. △

Consider the map $i : K \to \prod_\mathfrak{p} K_\mathfrak{p}$ given by $x \mapsto (f_\mathfrak{p}(x))_\mathfrak{p}$, where $f_\mathfrak{p} : K \to K_\mathfrak{p}$ is the completion. The next lemma shows that this maps induces a map into the adèle ring $\mathcal{A}_K$.

Lemma 2.8.3. *Let K be a global field and $x \in K$. Then $|f_\mathfrak{p}(x)|_\mathfrak{p} \leq 1$ for almost all places $\mathfrak{p}$.*

Proof. See Theorem 3 at page 47 of [17]. □

It is easy to see that i is in fact continuous. Using the map i we can identity K with a subfield of $\mathcal{A}_K$, which is discrete by the following lemma.

Lemma 2.8.4. *Let K be a global field. Then $i(K)$ is discrete in $\mathcal{A}_K$.*

Proof. See chapter 4 of [17]. □

Theorem 2.8.5. *Let K be a function field and let $a \in \mathcal{A}_K$ an adèle of K. Then the subset*

$$D(a) = \{b \in \mathcal{A}_K \mid |b_\mathfrak{p}|_\mathfrak{p} \leq |a_\mathfrak{p}|_\mathfrak{p}\}$$

is a compact neighborhood of a in $\mathcal{A}_K$.

Proof. See chapter 4 of [17] (c.f., the proof of Lemma 4 at page 206 of [14]). □

We will now show that invertible adèles generalize ideals in the ring of integers.

Definition 2.8.6 (Idèle group)**.** The *idèle group* $\mathcal{I}_K$ of a global field K is the restricted topological product (over all places $\mathfrak{p}$ of K) of the $K_\mathfrak{p}^\times$ with respect to the $\mathcal{O}_\mathfrak{p}^\times$ with $\mathfrak{p}$ infinite. △

As a set, we have that $\mathcal{I}_K = \mathcal{A}_K^\times$. However, the topologies are very different.

Proposition 2.8.7. *Let K be a global field. There is a surjective group homomorphism $j : \mathcal{I}_K \to I_K$.*

Proof. Using Proposition 2.6.9, we see that $\mathrm{ord}_\mathfrak{p} : K \to \mathbb{R}$ has a unique lift $g : K_\mathfrak{q} \to \mathbb{R}$ to the completion at any place $\mathfrak{q}$. That means that if $f : K \to K_\mathfrak{q}$ is the completion, then $\mathrm{ord}_\mathfrak{p}(x) = g(f(x))$ for all $x \in K$. Since there is no confusion, we just write $\mathrm{ord}_\mathfrak{p}$ instead of g.

Notice that $\mathrm{ord}_\mathfrak{p}$ is discrete on $K_\mathfrak{p}$, since it is continuous and discrete on the dense subset $K \subseteq K_\mathfrak{p}$. Moreover $\mathrm{ord}_\mathfrak{p}$ maps $K_\mathfrak{p}$ into the integers. Now consider the map $j : \mathcal{I}_K \to I_K$ given by

$$(a_\mathfrak{p})_\mathfrak{p} \mapsto \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a_\mathfrak{p})},$$

where $\mathrm{ord}_\mathfrak{p}$ is the unique extension of $\mathrm{ord}_\mathfrak{p}$ on K to $K_\mathfrak{p}$. Then j is well-defined, since $a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$ except for some finite places $\mathfrak{p}$. It is clear that j is a homomorphism of groups. □

2.9. Idèle class group

In the previous section we have seen how idèles generalize ideals (via the map j) in the ring of integers. We will now generalize the ideal class group. We start by identifying which idèles correspond to principal ideals.

Recall the definition of $i : K \to \prod_\mathfrak{p} K_\mathfrak{p}$. The idèles in the image $i(K^\times)$ are now called principal.

Definition 2.9.1 (Principal idèles)**.** An idèle a of a global field K is called *principal* if and only if there exists some x in $K^\times$ such that $a = i(x)$. △

This definition makes sense: if $(a_\mathfrak{p})_\mathfrak{p}$ is a principal idèle, then we find some $a \in K$ with $(a_\mathfrak{p})_\mathfrak{p} = i(a)$ and

$$j((a_\mathfrak{p})_\mathfrak{p}) = \prod_{\mathfrak{p} \subseteq \mathcal{O}_K} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(f_\mathfrak{p}(a))} = a\mathcal{O}_K,$$

since $\mathrm{ord}_\mathfrak{p}(f_\mathfrak{p}(a)) = \mathrm{ord}_\mathfrak{p}(a)$, where $f_\mathfrak{p} : K \to K_\mathfrak{p}$ is the completion at $\mathfrak{p}$. Thus the principal idèles corresponds with the principal ideals of $\mathcal{O}_K$.

Now that we have generalization of principal ideals, we may consider the generalization of the ideal class group.

Definition 2.9.2 (Idèle class group)**.** The *idèle class group of K* is the group $\mathcal{C}(K) = \mathcal{I}_K / i(K^\times)$. △

It turns out that the idèle class group is related to the ray class group. This theorem will be uses to translate theorems from the idèlic viewpoint to the classical viewpoint (c.f., proof of Theorem 2.10.5 or Proposition 2.12.9)

Theorem 2.9.3. *Let K be a global field and $\mathfrak{m}$ a modulus. Then the ray class group $\mathcal{C}l_\mathfrak{m}(K)$ of K modulo $\mathfrak{m}$ is isomorphic to a factor group of the idèle class group $\mathcal{C}(K)$.*

Proof. See Proposition 4.6 at page 168 of [8] or see page 146 and 147 of Lang [5]. □

2.10. Density of primes

Let K be a global field with modulus $\mathfrak{m}$. The aim of this section is to show that every ray class in $\mathcal{C}l_\mathfrak{m}(K)$ contains infinitely many prime ideals. We will show this with the help of L-series.

Analytic density. Let $f(s)$ and $g(s)$ be complex functions defined in a neighborhood of $s = 1$. For notational convenience we write $f(s) \sim g(s)$ if and only if there exists some complex function $h(s)$, which is analytic at $s = 1$, such that $f(s) - g(s) = h(s)$. It is clear that this defines an equivalence relation.

Definition 2.10.1 (Analytic density)**.** Let M be a set of primes of a global field K. Then δ is the *analytic density of M* if and only if

$$\sum_{\mathfrak{p} \in M} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \delta \log \frac{1}{1-s}.$$ △

It can be shown that the analytic density generalizes the *natural density*

$$\lim_{n \to \infty} \frac{|\{\text{primes } \mathfrak{p} \text{ in } M \text{ with } \mathrm{N}_K(\mathfrak{p}) \leq n\}|}{|\{\text{primes } \mathfrak{p} \text{ of } K \text{ with } \mathrm{N}_K(\mathfrak{p}) \leq n\}|},$$

but we will not prove this.

Clearly $\delta = 0$ whenever M is finite, because $\log \frac{1}{1-s}$ is not analytic at $s = 1$. Thus M is infinite if $\delta \neq 0$. Therefore it suffices to show that the density of the set $\{\mathfrak{p} \in \mathfrak{R}\}$ of prime ideals in a given ray class $\mathfrak{R} \in \mathcal{C}l_\mathfrak{m}(K)$ is non-zero.

L-series. We will now study L-series, as they turn our to be useful for the calculation of the analytic density. The construction L-series requires the definition of characters:

Definition 2.10.2 (Characters)**.** Let G be a finite abelian group. A *(Dirichlet) character* χ of G is a group homomorphism $\chi : G \to \mathbb{C}^\times$. The *character group* $G^\vee$ of G is the group $\hom(G, \mathbb{C}^\times)$ of all group homomorphisms $\chi : G \to \mathbb{C}^\times$. △

There is only one property of characters, which is of major interest for us:

Lemma 2.10.3. *Let G be a finite abelian group and $g \in G$. Then*

$$\sum_{\chi \in G^\vee} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. See the proof of Lemma 4.7 on page 193 of Milne [8]. □

We are now ready to define the L-series.

Definition 2.10.4 (L-series)**.** Let K be a global field with modulus $\mathfrak{m}$ and let χ be a character of the ray class group $\mathcal{C}l_{\mathfrak{m}}(K)$. Then the *L-series of* χ *modulo* $\mathfrak{m}$ is the series

$$L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\,\mathrm{N}(\mathfrak{p})^{-s}}. \qquad \triangle$$

We first discuss some important properties about this function.

Theorem 2.10.5. *Let K be a global field and $\mathfrak{m}$ a modulus. Let χ be a character of $\mathcal{C}l_{\mathfrak{m}}(K)$. Then*

$$\log L_{\mathfrak{m}}(s,\chi) \sim \begin{cases} \log \frac{1}{1-s} & \text{if } \chi \text{ trivial} \\ 0 & \text{if } \chi \text{ non-trivial} \end{cases}$$

Proof. Let $m(\chi)$ be the order of $L_{\mathfrak{m}}(s,\chi)$ at $s=1$. Then there is some function $h(s)$, which is both analytic and non-zero at $s=1$, such that

$$L_{\mathfrak{m}}(s,\chi) = (1-s)^{m(\chi)}h(s).$$

Hence, taking the logarithm, we conclude that

$$\log L_{\mathfrak{m}}(s,\chi) = -m(\chi)\log\frac{1}{1-s} + \log h(s).$$

Since $\log h(s)$ is analytic at $s=1$, we have by definition that

$$\log L_{\mathfrak{m}}(s,\chi) \sim -m(\chi)\log\frac{1}{1-s}.$$

Therefore this theorem just claims that the order of $L_{\mathfrak{m}}(s,\chi)$ at $s=1$ equals -1, whenever χ is trivial and 0 otherwise. This result is proven in Weil [17] for idèle class characters: see corollaries 1 and 2 at page 124, the remark at the bottom of page 125 and Theorem 11 at page 288. Using Theorem 2.9.3, we may translate our L-series into those used by Weil. □

The following theorem shows that the density of primes in a given ray class is non-zero. Moreover it shows that this density is in fact independent of the choice of the ray class $\mathfrak{R}$.

Theorem 2.10.6. *Let $\mathfrak{m}$ be a modulus for a global field K and let $\mathfrak{R} \in \mathcal{C}l_{\mathfrak{m}}(K)$ be a ray class. Then the density δ of the primes in $\mathfrak{R}$ is $1/h_{\mathfrak{m}}$. Moreover $\mathfrak{R}$ contains infinitely many prime ideals.*

Proof. We follow the proof in Lang [5] on page 166. Take the logarithm on the definition of $L_{\mathfrak{m}}(s,\chi)$ and use the Taylor series of $-\log(1-x)$ to find

$$\log L_{\mathfrak{m}}(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}} -\log(1-\chi(\mathfrak{p})\,\mathrm{N}(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{k=1}^{\infty}\frac{\chi(\mathfrak{p})^k}{k\,\mathrm{N}(\mathfrak{p})^{ks}}.$$

Now since the series

$$\sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{k=2}^{\infty}\frac{\chi(\mathfrak{p})^k}{k\,\mathrm{N}(\mathfrak{p})^{ks}}$$

is bounded , hence analytic, in a neighborhood of 1, we conclude that

$$\log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}}\frac{\chi(\mathfrak{p})}{\mathrm{N}(\mathfrak{p})^s}.$$

Next we split the series using ray classes and use that χ is constant on any ray class to find

$$\log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{R}\in\mathcal{C}l_{\mathfrak{m}}(K)}\chi(\mathfrak{R})\sum_{\mathfrak{p}\in\mathfrak{R}}\frac{1}{\mathrm{N}(\mathfrak{p})^s}.$$

Multiply by $\chi(\mathfrak{R}_0^{-1})$, for some fixed ray class $\mathfrak{R}_0$, and sum over all characters χ. Then

$$\sum_{\chi} \chi(\mathfrak{R}_0^{-1}) \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{R} \in Cl_{\mathfrak{m}}(K)} \sum_{\chi} \chi(\mathfrak{R}\mathfrak{R}_0^{-1}) \sum_{\mathfrak{p} \in \mathfrak{R}} \frac{1}{\mathrm{N}(\mathfrak{p})^s}.$$

Using Theorem 2.10.5 for the left hand side and Lemma 2.10.3 for the right hand side we conclude that

$$\log \frac{1}{1-s} \sim h_{\mathfrak{m}} \sum_{\mathfrak{R} \in Cl_{\mathfrak{m}}(K)} \sum_{\mathfrak{p} \in \mathfrak{R}} \frac{1}{\mathrm{N}(\mathfrak{p})^s}.$$

Thus, since $\mathfrak{m}$ is finite, we find that

$$\sum_{\mathfrak{p}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{\mathrm{N}(\mathfrak{p})^s} \sim \frac{1}{h_{\mathfrak{m}}} \log \frac{1}{1-s}.$$

This shows that the density of the primes in $\mathfrak{R}$ is $1/h_{\mathfrak{m}}$. □

2.11. Local norms

In this section we will prove two important theorems about norms in an extension of global fields. The first is the Hasse norm theorem, which states that in any cyclic extension of global fields any element in the base field is a norm precisely whenever it is a local norm at every place. The second theorem describes the local norm group of a cyclic Kummer extension at almost all finite places.

Norm groups. Let L/K be an extension of global fields and consider the relative field norm

$$\mathrm{N}_{L/K} : L^{\times} \to K^{\times}.$$

From Theorem 2.2.5 we see that $\mathrm{N}_{L/K}$ is continuous with respect to $|\cdot|_{\mathfrak{p}}$, for any place $\mathfrak{p}$ of K. Proposition 2.6.9 then shows that this map has a unique extension to a map

$$\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} : L_{\mathfrak{P}}^{\times} \to K_{\mathfrak{p}}^{\times}.$$

This map is called the *local norm map (at $\mathfrak{p}$)*. Elements in the image of the local norm maps are called *local norms at $\mathfrak{p}$*. In view of this new terminology, we may refer to $\mathrm{N}_{L/K}$ as the *global norm map*.

Recall that L/K is cyclic if and only if L/K is Galois with cyclic Galois group. We first investigate the connection between local and global norms in a cyclic extension L/K of global fields. In other words, we seek a connection between elements of the form $\mathrm{N}_{L/K}(a)$ with $a \in L$ and elements of the form $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(a_{\mathfrak{P}})$ for some $\mathfrak{P}$ above $\mathfrak{p}$ and $a_{\mathfrak{P}} \in L_{\mathfrak{P}}$. This connection is made explicit by Hasse:

Theorem 2.11.1 (Hasse norm theorem)**.** *Let L/K be a cyclic extension of global fields and $x \in K$. Then $x \in \mathrm{N}_{L/K}(L)$ if and only if $x \in \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}})$ for all places $\mathfrak{p}$ of K and $\mathfrak{P}/\mathfrak{p}$.*

Proof. For this proof the reader should be familiar with cohomology, which is not part of this thesis. We will provide the argument, bought from theorem on page 195 of Lang [5] and Corollary 4.5 at page 384 of [10], without going into details.

Consider the exact sequence of the idèle class group:

$$1 \longrightarrow L^{\times} \longrightarrow \mathcal{I}_L \longrightarrow \mathcal{C}(L) \longrightarrow 1.$$

Then cohomology gives rise to a long exact sequence:

$$\cdots \longrightarrow H^{-1}(G, \mathcal{C}(L)) \longrightarrow H^0(G, L^{\times}) \longrightarrow H^0(G, \mathcal{I}_L) \longrightarrow \cdots.$$

By definition that $H^0(G, L^{\times}) = K^{\times}/\mathrm{N}_{L/K}(L^{\times})$ and $H^0(G, \mathcal{I}_L) = \mathcal{I}_K/\mathrm{N}_{L/K}(\mathcal{I}_L)$. Now if $x \in K^{\times}$ is a global norm, we conclude that the idèle $(x)_{\mathfrak{p}}$ is a norm: x is a local norm at every place $\mathfrak{p}$. Suppose x is a local norm at every place $\mathfrak{p}$, i.e. $(x)_{\mathfrak{p}}$ is zero in $H^0(G, \mathcal{I}_L)$. By the remark on page 94 of Lang [5], we conclude that $H^{-1}(G, \mathcal{C}(L)) = 1$. Hence the second map is an injection. Therefore x is zero in $H^0(G, L^{\times})$, which means that x is a global norm. □

Recall that $U_{\mathfrak{p}}$ is the set of local units at $\mathfrak{p}$. We will also need the following theorem.

Theorem 2.11.2 (Local Norm Indices)**.** *Let $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ be an abelian extension of local fields. Then*

1. $[K_{\mathfrak{p}}^{\times} : \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}^{\times})] = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ *the degree of the extension,*
2. $[U_{\mathfrak{p}} : \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}})] = e(\mathfrak{P}/\mathfrak{p})$*, the ramification index*

Proof. See page 142 and 143 of [3]. □

As an application of these two theorems we will study extensions of a global field K of the form $K(d^{1/\ell})$, where ℓ is prime and $d \in K$. Such an extension is called a *Kummer extension*. Notice that this Kummer extension is cyclic whenever K contains the ℓth roots of unity. Before we prove our main theorem, we need the following lemma. Recall that $\overline{K}_{\mathfrak{p}}$ is the residue class field of K at $\mathfrak{p}$, which is defined by $\mathcal{O}_K/\mathfrak{p}$, where $\mathcal{O}_K$ is the ring of integers of K.

Lemma 2.11.3. *Let K be a global field, $\mathfrak{p}$ a finite place of K, ℓ a prime number such that $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \neq \ell$ and that K contains the ℓ-th roots of unity and let $L = K(d^{1/\ell})$ with $d \in K$. Then $u \in U_{\mathfrak{p}} - (U_{\mathfrak{p}})^{\ell}$ if and only if $\bar{u} \in \overline{K}_{\mathfrak{p}}^{\times} - (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}$. Moreover if $\mathfrak{p}$ is ramified, then $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}) = (U_{\mathfrak{p}})^{\ell}$.*

Proof. For notational convenience we abbreviate $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ to N. Consider the inclusions

$$(U_{\mathfrak{p}})^{\ell} \subseteq \mathrm{N}(U_{\mathfrak{P}}) \subseteq U_{\mathfrak{p}}.$$

We will show that $[U_{\mathfrak{p}} : (U_{\mathfrak{p}})^{\ell}] = \ell$ and that $[U_{\mathfrak{p}} : \mathrm{N}(U_{\mathfrak{P}})] = \ell$. Then we find that $[\mathrm{N}(U_{\mathfrak{P}}) : (U_{\mathfrak{p}})^{\ell}] = 1$ or equivalently $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}) = (U_{\mathfrak{p}})^{\ell}$. Along the way we prove that $d \in \mathcal{O}_{\mathfrak{p}} - (\mathcal{O}_{\mathfrak{p}})^{\ell}$ if and only if $\bar{d} \in \overline{K}_{\mathfrak{p}}^{\times} - (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}$.

We first show that $[U_{\mathfrak{p}} : (U_{\mathfrak{p}})^{\ell}] = \ell$. Consider the polynomial $f = X^{\ell} - u$, with $u \in U_{\mathfrak{p}}$. Then f is monic and separable with coefficients in $\mathcal{O}_{\mathfrak{p}}$, because $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \neq \ell$ and $u \in U_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}$. Using Hensel's lemma we conclude that f has a solution in $\mathcal{O}_{\mathfrak{p}}$ if and only if $\overline{f}$ has a solution in $\overline{K}_{\mathfrak{p}}^{\times}$. This shows that $u \in U_{\mathfrak{p}} - (U_{\mathfrak{p}})^{\ell}$ if and only if $\bar{u} = u + \mathfrak{p} \in \overline{K}_{\mathfrak{p}}^{\times} - (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}$, because any root of f in $\mathcal{O}_{\mathfrak{p}}$ lies in $U_{\mathfrak{p}}$. Consider the natural map $\pi = \mathcal{O}_{\mathfrak{p}} \to \overline{K}_{\mathfrak{p}}^{\times}$ given by $\pi(x) = x + \mathfrak{p} = \bar{x}$. If $\pi(x) \neq 0$, then $x \notin \mathfrak{p}$ and hence $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ and $x \in U_{\mathfrak{p}}$. Therefore π restricts to a surjection $U_{\mathfrak{p}} \to \overline{K}_{\mathfrak{p}}^{\times}$. Using that $u \in U_{\mathfrak{p}} - (U_{\mathfrak{p}})^{\ell}$ if and only if $\bar{u} \in \overline{K}_{\mathfrak{p}}^{\times} - (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}$ we conclude using the first isomorphism theorem that the surjection $U_{\mathfrak{p}} \to \overline{K}_{\mathfrak{p}}^{\times}$ reduces to an isomorphism

$$U_{\mathfrak{p}}/(U_{\mathfrak{p}})^{\ell} \cong \overline{K}_{\mathfrak{p}}^{\times}/(\overline{K}_{\mathfrak{p}}^{\times})^{\ell}.$$

From this we see that $[U_{\mathfrak{p}} : (U_{\mathfrak{p}})^{\ell}] = [\overline{K}_{\mathfrak{p}}^{\times} : (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}]$. It remains to show that $[\overline{K}_{\mathfrak{p}}^{\times} : (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}] = \ell$. First notice that $\overline{K}_{\mathfrak{p}}^{\times}$ is cyclic by Theorem 1.3.3. Therefore $[\overline{K}_{\mathfrak{p}}^{\times} : (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}] \leq \ell$. Furthermore K contains the ℓ-th roots of unity, i.e., the monic polynomial $X^{\ell} - 1$ splits completely in $\mathcal{O}_{\mathfrak{p}}$. Since $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \neq \ell$ we see that $X^{\ell} - \bar{1}$ is a separable polynomial over $\overline{K}_{\mathfrak{p}}$, i.e., it has distinct roots. Therefore $\overline{K}_{\mathfrak{p}}$ contains all ℓ-th roots of unity, which shows that $[\overline{K}_{\mathfrak{p}}^{\times} : (\overline{K}_{\mathfrak{p}}^{\times})^{\ell}] \geq \ell$ and $[U_{\mathfrak{p}} : (U_{\mathfrak{p}})^{\ell}] = \ell$.

We will now prove that $[U_{\mathfrak{p}} : \mathrm{N}(U_{\mathfrak{P}})] = \ell$, whenever $\mathfrak{p}$ is ramified. From the fundamental equation

$$e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = \ell$$

and the fact that ℓ is prime we conclude that $e(\mathfrak{P}/\mathfrak{p})$ equals 1 or ℓ. As $\mathfrak{p}$ is ramified, we find $e(\mathfrak{P}/\mathfrak{p}) = \ell$. We claim that $L_{\mathfrak{P}} = K_{\mathfrak{p}}(d^{1/\ell})$. Indeed, we have that $L \subseteq K_{\mathfrak{p}}(d^{1/\ell}) \subseteq L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}(d^{1/\ell})$ is complete with respect to $|\cdot|_{\mathfrak{P}}$ because it is a finite dimensional vector space over $K_{\mathfrak{p}}$ which is complete with respect to $|\cdot|_{\mathfrak{p}}$. The claim follows from the fact that $L_{\mathfrak{P}}$ is the smallest complete extension of L. Using $L_{\mathfrak{P}} = K_{\mathfrak{p}}(d^{1/\ell})$ we see that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a cyclic extension of local fields, because K contains the ℓ-th roots of unity. Hence we may apply Theorem 2.11.2 to conclude that $[U_{\mathfrak{p}} : \mathrm{N}(U_{\mathfrak{P}})] = \ell$.

Hence we conclude that $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}) = (U_{\mathfrak{p}})^{\ell}$. □

The following theorem studies the local norm group of a cyclic Kummer extension at a finite place. The importance of this theorem becomes appearent in section 5.3, where it is used to define valuation rings by means of a first-order formula.

Theorem 2.11.4. *Let K be a global field, $\mathfrak{p}$ a finite place of K, ℓ a prime number such that $\mathrm{char}(\overline{K}_\mathfrak{p}) \neq \ell$ and that K contains the 2ℓ-th roots of unity and let $L = K(d^{1/\ell})$ with $d \in K$. Then for all $\mathfrak{P}$ extending $\mathfrak{p}$ we have*

1) If $\mathrm{ord}_\mathfrak{p}(d) \not\equiv 0$ modulo ℓ then $[L_\mathfrak{P} : K_\mathfrak{p}] = e(\mathfrak{P}/\mathfrak{p}) = \ell$ and

$$\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P}^\times) = \langle d, (K_\mathfrak{p}^\times)^\ell \rangle;$$

2) If $\mathrm{ord}_\mathfrak{p}(d) \equiv 0$ modulo ℓ and $d \notin (K_\mathfrak{p}^\times)^\ell$ then $[L_\mathfrak{P} : K_\mathfrak{p}] = f(\mathfrak{P}/\mathfrak{p}) = \ell$ and

$$\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P}^\times) = \{x \in K_\mathfrak{p}^\times \mid \mathrm{ord}_\mathfrak{p}(x) \equiv 0 \pmod{\ell}\};$$

3) If $d \in (K_\mathfrak{p}^\times)^\ell$ then $L_\mathfrak{P}/K_\mathfrak{p}$ is trivial, and

$$\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P}^\times) = K_\mathfrak{p}^\times.$$

Proof. First of all notice that $L_\mathfrak{P} = K_\mathfrak{p}(d^{1/\ell})$. Furthermore we use the fundamental equation

$$e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = [L_\mathfrak{P} : K_\mathfrak{p}] = \ell. \tag{2.2}$$

As a final remark, we will abbriviate $\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}$ to N.

1) Suppose that $\ell \nmid \mathrm{ord}_\mathfrak{p}(d)$. If $d \in (K_\mathfrak{p}^\times)^\ell$, then $\ell \mid \mathrm{ord}_\mathfrak{p}(d)$. Hence $d^{1/\ell}$ is not in $K_\mathfrak{p}^\times$ and $L_\mathfrak{P}/K_\mathfrak{p}$ is non-trivial. As ℓ is prime, we conclude that $[L_\mathfrak{P} : K_\mathfrak{p}] = \ell$. Furthermore we have $\ell \mid e(\mathfrak{P}/\mathfrak{p})$ because

$$\ell \,\mathrm{ord}_\mathfrak{P}(d^{1/\ell}) = \mathrm{ord}_\mathfrak{P}(d) = e(\mathfrak{P}/\mathfrak{p}) \,\mathrm{ord}_\mathfrak{p}(d).$$

From equation (2.2) it follows that $e(\mathfrak{P}/\mathfrak{p}) = \ell$, i.e., L/K is totally ramified.

We will determine the local norm group. Let N denote the subgroup of $K_\mathfrak{p}^\times$ generated by $(K_\mathfrak{p}^\times)^\ell$ and d. First notice that $(K_\mathfrak{p}^\times)^\ell = \mathrm{N}(K_\mathfrak{p})$ and $d = \mathrm{N}(d^{1/\ell})$ are in $\mathrm{N}(L_\mathfrak{P}^\times)$, because K contains the 2ℓ-th roots of unity. Note that we use 2ℓ instead of ℓ because for $\ell = 2$ we need that $\sqrt{-1} \in K$. Thus N is a subgroup of $\mathrm{N}(L_\mathfrak{P}^\times)$. Conversely, let $x \in \mathrm{N}(L_\mathfrak{P}^\times)$ be arbitrary. We have that $\mathrm{ord}_\mathfrak{p}(N) = \mathbb{Z}$, because $\mathrm{ord}_\mathfrak{p}(d)$ and $\ell = \mathrm{ord}_\mathfrak{p}(\pi^\ell)$ are coprime, for $\pi \in K_\mathfrak{p}^\times$ with $\mathrm{ord}_\mathfrak{p}(\pi) = 1$. Therefore there exists some $n \in N$ such that $nx \in U_\mathfrak{p}$. Recall that $\mathrm{N}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$ and that $\mathfrak{P}$ is the unique prime above $\mathfrak{p}$. Then $\mathfrak{p} \mid \mathrm{N}(x)$ is equivalent to $\mathfrak{P} \mid (x)$, which shows that $x \in U_\mathfrak{P}$ if and only if $\mathrm{N}(x) \in U_\mathfrak{p}$. We conclude that $\mathrm{N}(L_\mathfrak{P}^\times) \cap U_\mathfrak{p} = \mathrm{N}(U_\mathfrak{P})$. If we apply Lemma 2.11.3, we find that

$$nx \in \mathrm{N}(L_\mathfrak{P}^\times) \cap U_\mathfrak{p} = \mathrm{N}(U_\mathfrak{P}) = (U_\mathfrak{p})^\ell \subseteq N,$$

which implies that $x \in N$. We conclude that $\mathrm{N}(L_\mathfrak{P}^\times) = N$.

2) Suppose that $\mathrm{ord}_\mathfrak{p}(d) \equiv 0$ modulo ℓ and $d \notin (K_\mathfrak{p}^\times)^\ell$. We can assume, after adjusting by an ℓ-th power if necessary, that $\mathrm{ord}_\mathfrak{p}(d) = 0$. Lemma 2.11.3 shows that the assumption $d \notin (K_\mathfrak{p}^\times)^\ell$ implies that $\bar{d} \notin \overline{K}_\mathfrak{p}^\times - (\overline{K}_\mathfrak{p}^\times)^\ell$. Hence using $L_\mathfrak{P} = K_\mathfrak{p}(d^{1/\ell})$ we see that $\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p}$ is non-trivial. Furthermore using Hensel's lemma we conclude that $X^\ell - d$ is irreducible over $\mathcal{O}_{K_\mathfrak{p}}$ if and only if $X^\ell - \bar{d}$ is irreducible over $\overline{K}_\mathfrak{p}$. Hence we find that

$$f(\mathfrak{P}/\mathfrak{p}) = [\overline{L}_\mathfrak{P} : \overline{K}_\mathfrak{p}] = [\overline{K}_\mathfrak{p}(\bar{d}^{1/\ell}) : \overline{K}_\mathfrak{p}] = \ell.$$

From equation (2.2) it follows that $e(\mathfrak{P}/\mathfrak{p}) = 1$.

We will now determine the norm group. Let N denote the set of all x in $K_\mathfrak{p}^\times$ such that $\mathrm{ord}_\mathfrak{p}(x) \equiv 0$ modulo ℓ. Let $x \in N$ be arbitrary. Find $\pi \in K_\mathfrak{p}^\times$ with $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ and let k be an integer such that $\mathrm{ord}_\mathfrak{p}(x) = k\ell$. Then $\pi^{-k\ell}x \in U_\mathfrak{p}$ and by Theorem 2.11.2 we see that $\pi^{-k\ell}x \in \mathrm{N}(U_\mathfrak{P})$, since $e(\mathfrak{P}/\mathfrak{p}) = 1$. Furthermore $\mathrm{N}(\pi^{-k}) = \pi^{-k\ell}$ as $\pi \in K$, which shows that $x \in \mathrm{N}(L_\mathfrak{P}^\times)$. Hence we have the following inclusions:

$$N \subseteq \mathrm{N}(L_\mathfrak{P}^\times) \subseteq K_\mathfrak{p}^\times.$$

Theorem 2.11.2 shows that $[K_\mathfrak{p}^\times : \mathrm{N}(L_\mathfrak{P}^\times)] = \ell$. The homomorphism $K_\mathfrak{p}^\times \to \mathbb{Z}/\ell\mathbb{Z}$ given by $x \mapsto \mathrm{ord}_\mathfrak{p}(x) + \ell\mathbb{Z}$ has kernel N, which shows that $[K_\mathfrak{p}^\times : N] = \ell$. From this we conclude that $\mathrm{N}(L_\mathfrak{P}^\times) = N$.

3) As $L_\mathfrak{P} = K_\mathfrak{p}(d^{1/\ell})$, we clearly have that $L_\mathfrak{P}/K_\mathfrak{p}$ is trivial, whenever $d \in (K_\mathfrak{p}^\times)^\ell$. Furthermore the norm map is just the identity, which shows $\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P}^\times) = K_\mathfrak{p}^\times$. □

2.12. Artin's reciprocity law

We will now introduce a very important generalization of the quadratic reciprocity law, which was formulated by Artin as follows:

Theorem 2.12.1 (Quadratic reciprocity law)**.** *There exists a group homomorphism*

$$(\mathbb{Z}/4d\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \quad \textit{with} \quad p + 4d\mathbb{Z} \mapsto \left(\frac{d}{p}\right)$$

for all primes p not dividing $4d$.

Proof. See page 47 of [7] for a derivation of this theorem from the classical quadratic reciprocity law. □

We start with the generalization of the Legendre symbol, which is the Artin symbol. Then we will formulate the generalization of the quadratic reciprocity law, without going into details.

Artin symbol. We will define the Artin symbol, which is the lift of the Frobenius automorphism of the residue class field to the Galois group field extension. For better understanding we will start from the classical viewpoint and then generalize to the idelic viewpoint.

Let L/K be a finite abelian extension of global fields, i.e., a finite Galois extension with abelian Galois group G. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ an extension of $\mathfrak{p}$ to L.

First notice that $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Indeed if $x \in \mathcal{O}_L$ satisfies $x^n = \sum_i a_i x^i$, with $a_i \in \mathcal{O}_K$, then $\sigma(x)^n = \sum_i a_i \sigma(x)^i$, since $\sigma(a_i) = a_i$. We conclude that σ restricts to automorphism of $\mathcal{O}_L$.

Furthermore notice that the Galois group G acts naturally on the prime ideals $\mathfrak{P}$ extending $\mathfrak{p}$. Indeed for all $\sigma \in G$ we have that $\sigma(\mathfrak{P}) \subseteq \mathcal{O}_L$ is a prime ideal above $\sigma(\mathfrak{p}) = \mathfrak{p}$, because σ is an automorphism and K is the fixed field of σ. The stabilizer subgroup $G_\mathfrak{P}$ of $\mathfrak{P}$ of this action is called the *decomposition group*. More explicitly, we have

$$G_\mathfrak{P} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

We conclude that any $\sigma \in G_\mathfrak{P}$ restricts to automorphism of $\mathcal{O}_L$ which reduces to an automorphism $\overline{\sigma}$ of $\overline{L}_\mathfrak{P} = \mathcal{O}_L/\mathfrak{P}$, since $\sigma(\mathfrak{P}) = \mathfrak{P}$. Moreover $\overline{\sigma} \in \mathrm{Gal}(\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p})$, since σ fixes K. Hence for all primes $\mathfrak{P}$ above $\mathfrak{p}$ we find a natural map

$$\pi_\mathfrak{P} : G_\mathfrak{P} \longrightarrow \mathrm{Gal}(\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p}) \qquad \sigma \mapsto \overline{\sigma}.$$

The kernel of $\pi_\mathfrak{P}$ is called the *inertia group* $I_\mathfrak{P}$ of $\mathfrak{P}$. That is,

$$I_\mathfrak{P} = \{\sigma \in G \mid \overline{\sigma} = \mathrm{id}\}$$

We are now ready to define the Artin symbol and Artin map.

Definition 2.12.2 (Artin symbol)**.** Let L/K be a finite abelian extension of global fields. Let $\mathfrak{p}$ be an unramified prime of L/K, let $\mathfrak{P}$ be a prime of L extending $\mathfrak{p}$ and let $\mathrm{Fr}_\mathfrak{P}$ be the Frobenius automorphism of $\overline{L}_\mathfrak{P}/\overline{K}_\mathfrak{p}$. Then

$$(\mathfrak{p}, L/K) := \pi_\mathfrak{P}^{-1}(\mathrm{Fr}_\mathfrak{P})$$

is called the *Artin symbol* of $\mathfrak{p}$. Let $\mathfrak{m}$ be a modulus which is divisible by all ramified primes of L/K. Then the homomorphism

$$(\cdot, L/K) : \mathcal{C}l_{\mathfrak{m}}(K) \longrightarrow G, \qquad \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \mapsto \prod_{i=1}^{t} (\mathfrak{p}, L/K)^{n_i}$$

for all integers n_i and places $\mathfrak{p}_i$ not dividing $\mathfrak{m}$, is called the *Artin map* with respect to $\mathfrak{m}$. △

Let L/K be an abelian extension of global fields. For the remainder of this paragraph we will show that the Artin symbol and Artin map are well-defined. Indeed, we need to show that the preimage $\pi_{\mathfrak{P}}^{-1}(\mathrm{Fr}_{\mathfrak{P}})$ is independent of $\mathfrak{P}$ and that this preimage contains exactly one element. Note that the Artin map is only determined on the primes of K relatively prime to $\mathfrak{m}$. It is clear that this extends uniquely to a homomorphism from $\mathcal{C}l_{\mathfrak{m}}(K)$ to G.

We will now investigate the maps $\pi_{\mathfrak{P}}$. The following theorem shows that there is a strong connection between the maps $\pi_{\mathfrak{P}}$ for different primes $\mathfrak{P}$.

Theorem 2.12.3. *The Galois group G acts transitively on the primes $\mathfrak{P}$ of L extending $\mathfrak{p}$.*

Proof. See Proposition 11 at page 12 of Lang [5]. □

Corollary 2.12.4. *The subset $\pi_{\mathfrak{P}}^{-1}(\mathrm{Fr}_{\mathfrak{P}}) \subseteq G$ only depends on the choice $\mathfrak{p}$.*

Proof. Theorem 2.12.3 implies that if $\mathfrak{P}$ and $\mathfrak{Q}$ are primes extending $\mathfrak{p}$, then there exists a $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{Q}$. Hence we have that $\sigma G_{\mathfrak{P}} \sigma^{-1} = G_{\mathfrak{Q}}$ and $G_{\mathfrak{P}} = G_{\mathfrak{Q}}$, because G is assumed to be abelian. Furthermore this σ reduces to a $\overline{K}_{\mathfrak{p}}$-isomorphism $\overline{\sigma} : \overline{L}_{\mathfrak{P}} \to \overline{L}_{\mathfrak{Q}}$ given by $x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{Q}$. Hence conjungation with σ induces an isomorphism from $\mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$ to $\mathrm{Gal}(\overline{L}_{\mathfrak{Q}}/\overline{K}_{\mathfrak{p}})$ which takes $\mathrm{Fr}_{\mathfrak{P}}$ to $\mathrm{Fr}_{\mathfrak{Q}}$. Indeed, let k be the integer

$$|\operatorname{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})| = |\operatorname{Gal}(\overline{L}_{\mathfrak{Q}}/\overline{K}_{\mathfrak{p}})|.$$

Then we have for all x in $\overline{L}_{\mathfrak{Q}}$ that

$$(\overline{\sigma}\,\mathrm{Fr}_{\mathfrak{P}}\,\overline{\sigma}^{-1})(x) = \overline{\sigma}(\overline{\sigma}^{-1}(x))^k = \overline{\sigma}(\overline{\sigma}^{-1}(x^k)) = x^k = \mathrm{Fr}_{\mathfrak{Q}}(x).$$

In other words, we have the following diagram:

$$\begin{array}{ccccc} G_{\mathfrak{P}} & \xrightarrow{\pi_{\mathfrak{P}}} & \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}) & \ni & \mathrm{Fr}_{\mathfrak{P}} \\ \| & & \downarrow \wr & & \downarrow \\ G_{\mathfrak{Q}} & \xrightarrow{\pi_{\mathfrak{Q}}} & \mathrm{Gal}(\overline{L}_{\mathfrak{Q}}/\overline{K}_{\mathfrak{p}}) & \ni & \mathrm{Fr}_{\mathfrak{Q}} \end{array}$$

which is commutative. Indeed for all $\tau \in G_{\mathfrak{P}} = G_{\mathfrak{Q}}$ and all $x + \mathfrak{Q}$ in $\overline{L}_{\mathfrak{Q}}$ we have that $(\pi_{\mathfrak{Q}}(\tau))(x + \mathfrak{Q}) = \tau(x) + \mathfrak{Q}$ and

$$(\overline{\sigma}\pi_{\mathfrak{P}}(\tau)\overline{\sigma}^{-1})(x + \mathfrak{Q}) = (\overline{\sigma}\pi_{\mathfrak{P}}(\tau))(\sigma^{-1}(x) + \mathfrak{P}) = \overline{\sigma}(\tau\sigma^{-1}(x) + \mathfrak{P}) = \sigma\tau\sigma^{-1}(x) + \mathfrak{Q}.$$

Hence we find that $\overline{\sigma}\pi_{\mathfrak{P}}(\tau)\overline{\sigma}^{-1} = \pi_{\mathfrak{Q}}(\tau)$, since G is abelian. We conclude that $\pi_{\mathfrak{P}}^{-1}(\mathrm{Fr}_{\mathfrak{P}}) = \pi_{\mathfrak{Q}}^{-1}(\mathrm{Fr}_{\mathfrak{Q}})$, which proves the corollary. □

We will show that the Artin symbol exists and is unique. Recall from Example 1.12.11 that the Frobenius automorphism of $\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}$ is a generator for $\mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$. Hence the existence of the Artin symbol is equivalent to the surjectivity of $\pi_{\mathfrak{P}}$.

Theorem 2.12.5. *The following sequence is exact:*

$$0 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}) \longrightarrow 0.$$

Proof. Since K and L are global fields, Lemma 2.1.4 tells us that $\overline{K}_{\mathfrak{p}}$ and $\overline{L}_{\mathfrak{P}}$ are both finite fields. By Example 1.12.11 we conclude that $\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}$ is a Galois extension. Then Theorem 1.12.9 implies that $\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}$ is normal. Now apply Proposition 14 at page 15 of Lang [5]. □

For the uniqueness we focus on the injectivety of $\pi_{\mathfrak{P}}$.

Corollary 2.12.6. *The natural map $G_{\mathfrak{P}} \to \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$ is an isomorphism if and only if $\mathfrak{p}$ is unramified.*

Proof. By the fundamental formula for Galois extensions the order of $G_{\mathfrak{P}}$ equals $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ and the order of $\mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$ equals $f(\mathfrak{P}/\mathfrak{p})$. Therefore $I_{\mathfrak{P}}$ is of order $e(\mathfrak{P}/\mathfrak{p})$. Hence from Proposition 2.12.5 we conclude that the natural map $G_{\mathfrak{P}} \to \mathrm{Gal}(\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$ is an isomorphism if and only if $\mathfrak{p}$ is unramified. □

Artin's reciprocity law. We will now further investigate the properties of the Artin map. Without going into details we summarize the most important properties. Notice that the Artin map depends on the choice of a modulus. It turns out that the Artin map has nice properties, whenever this modulus is admissible.

Recall that $\mathrm{ord}_{\mathfrak{p}}$ has a unique extension to the completion $K_{\mathfrak{p}}$, which implies that $x \equiv 1 \mod \mathfrak{m}$ is a relation on $K_{\mathfrak{p}}^*$.

Definition 2.12.7. Let L/K be an extension of global fields. A modulus $\mathfrak{m}$ of K is called *admissible* if and only if

$$W_{\mathfrak{m}}(\mathfrak{p}) := \{x \in K_{\mathfrak{p}}^* \mid x \equiv 1 \mod \mathfrak{m}\} \subseteq \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^{\times})$$

for every place $\mathfrak{p}$ of K and $\mathfrak{P}/\mathfrak{p}$ of L. △

Let L/K be an extension of global fields. If $\mathfrak{n}$ is a modulus of L and $\mathfrak{m}$ is a modulus of K, then we say that $\mathfrak{n}$ *extends* $\mathfrak{m}$ if and only if $\mathfrak{p} \mid \mathfrak{m}$ implies $\mathfrak{P} \mid \mathfrak{n}$ for all extensions $\mathfrak{P}/\mathfrak{p}$ of places.

The following theorem from Artin is of fundamental importance:

Theorem 2.12.8 (Artin's reciprocity law)**.** *Let L/K be an abelian extension of global fields, let $\mathfrak{m}$ be an admissible modulus of K which is divisible by all ramified places and $\mathfrak{n}$ be the modulus of L extending $\mathfrak{m}$. Then the Artin map $\mathfrak{a} \mapsto (\mathfrak{a}, L/K)$ on ideals induces an isomorphism*

$$\mathcal{C}l_{\mathfrak{m}}(K)/\,\mathrm{N}(\mathcal{C}l_{\mathfrak{n}}(L)) \longrightarrow G.$$

Proof. This is the combination of Theorem 1 and the remark below at page 199, Theorem 2 at page 204 and Theorem 3 at page 205 of [5]. Notice that Proposition 2.2.3 shows that $\mathrm{N} : I_L \to I_K$ factors through a map $\mathcal{C}l_{\mathfrak{n}}(L) \to \mathcal{C}l_{\mathfrak{m}}(K)$. □

Remark. Artin's reciprocity law does not exhibit any symmetry that would justify the term "reciprocity". The name derives from the fact that it extends the quadratic reciprocity law. See for example [7] for an introduction.

Now we will translate this theorem to the language of idèles which allows us to decompose the Artin map into local Artin maps.

Recall the definition of $j : \mathcal{I}_K \to I_K$ from the proof of Proposition 2.8.7.

Proposition 2.12.9. *Let L/K be an abelian extension of global fields, let $\mathfrak{m}$ be an admissible modulus of K and $\mathfrak{n}$ be the modulus of L above $\mathfrak{m}$. Then $j : \mathcal{I}_K \to I_K$ induces an isomorphism*

$$\mathcal{C}(K)/\,\mathrm{N}(\mathcal{C}(L)) \longrightarrow \mathcal{C}l_{\mathfrak{m}}(K)/\,\mathrm{N}(\mathcal{C}l_{\mathfrak{n}}(L)).$$

Proof. See Theorem 8 (and below) at page 150 of Lang [5]. □

Using j, we may consider the Artin map *on idèles*:

$$\mathcal{I}_K \longrightarrow G, \qquad a \mapsto (a, L/K) := \textstyle\prod_{\mathfrak{p}} (\mathfrak{p}, L/K)^{\mathrm{ord}_{\mathfrak{p}}(a_{\mathfrak{p}})}.$$

If we apply Proposition 2.12.9 to Theorem 2.12.8, we are able to determine the kernel of the Artin map on idèles.

Theorem 2.12.10 (Global Artin's reciprocity law)**.** *Let L/K be an abelian extension of global fields. The Artin map on idèles induces the isomorphism*

$$\mathcal{C}(K)/\,\mathrm{N}(\mathcal{C}(L)) \longrightarrow G, \qquad a \mapsto (a, L/K)$$

The global reciprocity law may be reformulated into a local theorem.

Theorem 2.12.11 (Local Artin's reciprocity law)**.** *For every place* $\mathfrak{p}$ *of* K *an isomorphism*

$$(\cdot, L/K)_{\mathfrak{p}} : K_{\mathfrak{p}}/\operatorname{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}) \longrightarrow G_{\mathfrak{P}},$$

such that for all $x \in K^{\times}$ *we have*

$$\textstyle\prod_{\mathfrak{p}}(x, L/K)_{\mathfrak{p}} = 1.$$

Proof. If we precompose $(\cdot, L/K)$ with the map $x \mapsto x_{\mathfrak{p}} = (\ldots, 1, x, 1, \ldots)$ from $K_{\mathfrak{p}}$ to $\mathcal{I}_K$, we find the isomorphism $(\cdot, L/K)_{\mathfrak{p}}$. Moreover for any $x \in K^{\times}$ we have in $\mathcal{C}(K)$ that $1 = (\ldots, x, x, x, \ldots) = \prod_{\mathfrak{p}} x_{\mathfrak{p}}$. Therefore in G we find

$$1 = (1, L/K) = (\textstyle\prod_{\mathfrak{p}} x_{\mathfrak{p}}, L/K) = \prod_{\mathfrak{p}}(x_{\mathfrak{p}}, L/K) = \prod_{\mathfrak{p}}(x, L/K)_{\mathfrak{p}}.$$

This proves the corollary. □

Remark. Notice that the local and global version of the reciprocity law are equivalent. Indeed suppose that for every place $\mathfrak{p}$ of K we are given an isomorphism

$$(\cdot, L/K)_{\mathfrak{p}} : K_{\mathfrak{p}}/\operatorname{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}) \longrightarrow G_{\mathfrak{P}},$$

such that for all $x \in K^{\times}$ we have $\prod_{\mathfrak{p}}(x, L/K)_{\mathfrak{p}} = 1$. Then we define a global map by

$$(\cdot, L/K) : \mathcal{I}_K \longrightarrow G, \qquad a \mapsto \prod_{\mathfrak{p}}(a_{\mathfrak{p}}, L/K)_{\mathfrak{p}}.$$

Since $\prod_{\mathfrak{p}}(x, L/K)_{\mathfrak{p}} = 1$, this map factors through a map $\mathcal{C}(K) \to G$. By the Hasse norm theorem we see that its kernel is $\operatorname{N}(\mathcal{C}(L))$. Hence we found the global Artin map on idèles: $\mathcal{C}(K)/\operatorname{N}(\mathcal{C}(L)) \to G$.

Chapter 3

First-Order Logic

In this chapter we will reformulate the questions from the introduction into precise questions. To be able to do this we need to provide precise definitions of what is meant by a statements and an objects. These will be introduced in section 3.1 and 3.2, where we will define statements to be $\mathcal{L}$-sentences and objects to be $\mathcal{L}$-structures. Then in section 3.3 we will define the concept of proofs and in section 3.4 we define when a map $f : \mathbb{N} \to \mathbb{N}$ is considered to be computable. In section 3.5 we will introduce Gödel numberings, which allows us to view computable maps as algorithms on the set of all $\mathcal{L}$-sentences and $\mathcal{L}$-formulas. Hence we able to define decidability. In section 3.6 we will discuss some properties of sets of $\mathcal{L}$-sentences. Then we have developed enough terminology to reformulate the questions form the introduction and we will do this in section 3.7.

The final goal of this chapter is to prepare for Chapter 5. There we will show that the theory of a global field is undecidable. This will be done by showing that the theory of of natural numbers is undecidable and that this theory can be interpreted in the theory of a global field. We will make this precise in section 3.8, 3.9 and 3.10.

3.1. Syntax

The syntax of first-order logic defines what a language is, i.e. it determines which expressions are valid. The goal of this section is to define this syntax.

Let us start with the most elementary object in the syntax: a *symbol*. It should be clear what a symbol is, and hence our definition will be a bit informal. A *k-ary function/relation symbol* is character c together with the following data: an integer $k \geq 0$ indicating the *arity* and a boolean value indicating whether c is a function or not. A nullary function symbol is called a *constant* and a nullary relation symbol is either a *tautology* ($\top$) or *falsum* ($\bot$).

Having settled this notion, we now turn to the definition of a language.

Definition 3.1.1 (Language)**.** A *language* $\mathcal{L}$ is a collection of k-ary function and relation symbols which contains a binary relation symbol $=$ and a nullary relation symbol $\bot$. △

The main examples of languages of this thesis are the following:

Example 3.1.2 (Language of rings)**.** The language $\mathcal{L}_{\text{ring}}$ of *rings* consist of two binary function symbols $+$ and $\times$, a binary relation symbol $<$ and two constants 0 and 1 together with the auxiliary symbols $=$ and $\bot$. In general this auxiliary symbols are left unmentioned. ◊

Example 3.1.3 (Language of arithmetic)**.** The language $\mathcal{L}_{\text{arith}}$ of *arithmetic* is the expansion of the language of rings with a binary relation symbol $<$. ◊

Definition 3.1.4 (Strings)**.** Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-string* of length $k \geq 0$ is a sequence "$c_1c_2c_3 \cdots c_k$", of *characters* from the *alphabet*

$$\mathcal{L} \cup \{\vee, \neg, \exists\} \cup \{v_i \mid i \in \mathbb{N}\} \cup \{), ,, (\}.$$

Here $\vee$, $\neg$ and $\exists$ are called the *logical connectives* and the v_i are called *variables*. If r, s and t are $\mathcal{L}$-strings or symbols then rs is the $\mathcal{L}$-string which concatenates r

with s and $r[s/t]$ is the $\mathcal{L}$-string in which every occurrence of t in r is replaced by s. △

The quotation marks may be dropped if there is no risk of confusion.

Definition 3.1.5 (Terms)**.** Let $\mathcal{L}$ be a language. A string t is an *$\mathcal{L}$-term* if and only if either

1) t equals v_i for some $i \in \mathbb{N}$, or

2) t equals $F(t_1, \ldots, t_k)$, where $t_1, \ldots, t_k$, $k \geq 0$, are $\mathcal{L}$-terms and F is a k-ary function symbol of $\mathcal{L}$.

An $\mathcal{L}$-term t is called *closed* if and only if v_i does not occur t for all $i \in \mathbb{N}$. △

We use the convention that the list $t_1, \ldots, t_k$ is empty for $k = 0$, hence the second property implies for $k = 0$ that the constants are terms. Furthermore note that this definition is not completely self-referential, because of the first case and the second case for $k = 0$. This definition is therefore an inductive definition.

In practice we will often write $t_1 \, F \, t_2$ instead of $F(t_1, t_2)$ and $t_1 \, R \, t_2$ instead of $R(t_1, t_2)$, for all $\mathcal{L}$-terms t_1 and t_2 and binary function symbols f and binary relation symbols R of $\mathcal{L}$.

We will also use symbols like x, y and z to denote variables, instead of restricting ourselves to use only the symbols v_i. This however should not lead to confusion as long as the variables are not denoted by a symbol of the language, i.e. a function or relation symbol.

Before we define which $\mathcal{L}$-strings are $\mathcal{L}$-formulas, we need the following definition.

Definition 3.1.6 (Free variables)**.** Let $\mathcal{L}$ be a language and ϕ an $\mathcal{L}$-string. A variable v_i is called *bound* in ϕ if and only if $\exists v_i$ occurs in ϕ and v_i is called *free* in ϕ otherwise. △

Note that in the above definition, v_i does not need to occur in ϕ. We will now define the $\mathcal{L}$-formulas.

Definition 3.1.7 (Formulas)**.** Let $\mathcal{L}$ be a language. A $\mathcal{L}$-string ϕ is called an *$\mathcal{L}$-formula* if and only if either

1) ϕ is *atomic*, i.e., ϕ equals $R(t_1, \ldots, t_k)$, $k \geq 0$, where $t_1, \ldots, t_k$ are $\mathcal{L}$-terms and R is a k-ary relation symbol of $\mathcal{L}$, or

2) ϕ equals $\psi_0 \vee \psi_1$, where ψ_0 and ψ_1 are $\mathcal{L}$-formulas such that if v_i occurs in ψ_j then v_i is free in ψ_{1-j} for all $i \in \mathbb{N}$ and $j \in \{0, 1\}$, or

3) ϕ equals $\neg\psi$, where ψ is an $\mathcal{L}$-formula, or

4) ϕ equals $\exists v_i \psi$, where $i \in \mathbb{N}$, ψ an $\mathcal{L}$-formula and v_i free in ψ.

The set of all $\mathcal{L}$-formulas variables is denoted by $\mathcal{F}_\mathcal{L}$. Let ϕ an $\mathcal{L}$-formula. The set of all $\mathcal{L}$-formulas ϕ with at most n free variables occurring in ϕ, is denoted by $\mathcal{F}^n_\mathcal{L}$. A formula ϕ is called a *sentence* if and only if $\phi \in \mathcal{F}^0_\mathcal{L}$. A formula ϕ is called *quantifier-free* if and only if $\exists$ and $\forall$ do not occur in ϕ. If ϕ is a formula, then we write $\phi(v_{i_1}, \ldots, v_{i_n})$, $n \geq 1$, or just $\phi(\vec{v})$ to mean that the free variables of ϕ are $v_{i_1}, \ldots, v_{i_n}$. △

Example 3.1.8. The $\mathcal{L}_{\text{ring}}$-string $\exists v_1(v_1 = 0 \vee \exists v_2(v_1 \times v_2 = 1))$ is an example of an $\mathcal{L}_{\text{ring}}$-sentence, as it can be build from the atomic $\mathcal{L}_{\text{ring}}$-formulas $v_1 = 0$ and $v_1 \times v_2 = 1$. ◊

Note that there is an important condition in the second item. The $\mathcal{L}_{\text{ring}}$-string

$$s = v_2 = 0 \vee \exists v_2(v_2 = v_1 + 1)$$

is not considered to be an $\mathcal{L}_{\text{ring}}$-formula, because v_2 occurs in $v_2 = 0$ while $\exists v_2$ occurs in $\exists v_2(v_2 = v_1 + 1)$. In other words, v_2 occurs both free (in a subformula) and bound in this formula.

Although s has a uniquely defined interpretation (in the sense of Definition 3.2.7), we will exclude it from the set of formulas. The reason is that there are problems with substitution. For example, the substitution

$$(v_2 = 0 \vee \exists v_2(v_2 = v_1 + 1))[t/v_2] \;=\; (t = 1 \vee \exists t(t = v_1 + 1))$$

makes no sense for any term t other then a variable v_i. However, we have the following:

Lemma 3.1.9. *Let $\mathcal{L}$ be a language, ϕ an $\mathcal{L}$-formula and v_k a free variable of ϕ. Let t be an $\mathcal{L}$-term such that v_i occurs in t implies v_i is free in ϕ for all $i \in \mathbb{N}$. Then the substitution $\phi[t/v_k]$ is an $\mathcal{L}$-formula.*

Proof. If v_i does not occur in ϕ, then $\phi[t/v_k]$ is trivially an $\mathcal{L}$-formula. Suppose that v_i occurs in ϕ. We show that $\phi[t/v_k]$ is an $\mathcal{L}$-formula, by *induction on formulas*.

atomic formula: Suppose that ϕ is atomic. Then $\phi[t/v_k]$ is clearly an atomic $\mathcal{L}$-formula.

disjuction: Suppose that ϕ equals $\psi_0 \vee \psi_1$, where ψ_0 and ψ_1 are $\mathcal{L}$-formulas such that if v_i occurs in ψ_j then v_i is free in ψ_{1-j} for all $i \in \mathbb{N}$ and $j \in \{0, 1\}$. Using the induction hypothesis, we find that both $\psi_0[t/v_k]$ and $\psi_1[t/v_k]$ are $\mathcal{L}$-formulas. Since $\phi[t/v_k]$ equals $\psi_0[t/v_k] \vee \psi_1[t/v_k]$, it remains to check whether the $\psi_j[t/v_k]$ satisfy the additional property on the variables. Suppose that v_i occurs in $\psi_j[t/v_k]$. Then v_i occurs in ψ_j or v_i occurs in t. If v_i occurs in ψ_j, then v_i is free in ψ_{1-j}. If v_i occurs in t, then v_i is free in ϕ, hence v_i is free in ψ_{1-j}. We find that v_i is free in ψ_{1-j} in both cases. Now since v_i is free in ψ_{1-j} if and only if v_i is free in $\psi_{1-j}[t/v_k]$, we conclude that $\phi[t/v_k]$ is an $\mathcal{L}$-formula.

negation: Suppose that ϕ equals $\neg\psi$, where ψ is an $\mathcal{L}$-formula. Then $\phi[t/v_k]$ is clearly an $\mathcal{L}$-formula.

existential quantifier: Suppose that ϕ equals $\exists v_i\psi$, with v_i free in ψ.

We conclude that $\phi[t/v_k]$ is an $\mathcal{L}$-formula. □

At first sight it seems that the symbols $\neq$, $\wedge$, $\rightarrow$, $\leftrightarrow$ and $\forall$ are missing from this definition. However this is not a problem since these symbols are definable using only symbols from Definition 3.1.7. Indeed, let ϕ and ψ be $\mathcal{L}$-formulas and $i \in \mathbb{N}$ an integer, we define the following abbreviations:

1) $t_1 \neq t_2$ for $\neg(t_1 = t_2)$;
2) $\phi \wedge \psi$ for $\neg(\neg\phi \vee \neg\psi)$;
3) $\phi \rightarrow \psi$ for $\neg\phi \vee \psi$;
4) $\phi \leftrightarrow \psi$ for $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$;
5) $\forall v_i\phi$ for $\neg\exists v_i\neg\phi$;
6) $\exists! v_i\phi$ for $\exists v_i\phi \wedge \forall v_j(\phi \rightarrow v_i = v_j)$.

3.2. Semantics

In the previous section we introduced the notion of $\mathcal{L}$-sentence ϕ. This ϕ can be viewed as property. In this section we will define the object of which ϕ is a property and also how one should interpret ϕ in a given object.

Structures and substructures. We will now introduce the objects.

Definition 3.2.1 (Structures)**.** Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-structure* consists of

1) a set M such that $M \neq \emptyset$ and $M \cap \mathcal{L} = \emptyset$;
2) a function $F^M : M^k \rightarrow M$ for each k-ary, $k \geq 0$, function symbol F of $\mathcal{L}$;
3) a subset $R^M \subseteq M^k$ for each k-ary, $k \geq 0$, relation symbol R of $\mathcal{L}$, such that
   a) $=^M$ equals $\{(m, m) \mid m \in M\}$;

b) $\bot^M$ equals $\emptyset$.

The function F^M and relation R^M are called the *interpretation* of f respectively R in M. △

In the above definition we use the convention that M^0 is a singleton set $\{*\}$. Therefore a nullary function (i.e., a constant) defines an element $F^M(*)$ of M.

First we list some examples of structures.

Example 3.2.2. If R is a ring then R is an $\mathcal{L}_{\text{ring}}$-structure, where $\mathcal{L}_{\text{ring}}$ is the language of rings. The converse is not always true, since we want some axioms to be true. ◊

Example 3.2.3. The set $\mathbb{N}$ of natural numbers with usual ordering, addition and multiplication and interpretation of 0 and 1 is an $\mathcal{L}_{\text{arith}}$-structure. ◊

In Example 3.2.2 we see that $\mathcal{L}_{\text{ring}}$-structures generalize the concept of a ring. We will now generalize the concept of a subring.

Definition 3.2.4 (Substructures)**.** Let $\mathcal{L}$ be a language an let M and N be $\mathcal{L}$-structures. Then N is a substructure of M if and only if for all $k \geq 0$, $\vec{n} \in N^k$, k-ary function symbol F and k-ary relation symbol R we have

1) $N \subseteq M$;

2) $F^N(\vec{n}) = F^M(\vec{n})$;

3) $R^N = R^k \cap M^k$. △

Truth. Consider an $\mathcal{L}$-structure M. In the previous section we defined syntactically the notion of formulas and sentences. These notions are useful because they are connected with "reality" by means of interpretations. Such an interpretation allow us to assign truth to each sentence. It turns out that we will need to define an interpretation of sentences in a larger (generally much larger) language in order to define truth.

Definition 3.2.5 (Language of a structure)**.** Let M be an $\mathcal{L}$-structure. Then the *language of* M (notation: $\mathcal{L}_M$) is the language $\mathcal{L}$ together with a constant m for all $m \in M$. △

The definition of a structure gives us the interpretation of constants and function symbols. We now inductively define the interpretation of closed terms.

Definition 3.2.6 (Interpretation of terms)**.** Let $\mathcal{L}$ be a language and M an $\mathcal{L}$-structure and t a closed $\mathcal{L}_M$-term. Then $t = F(t_1, \ldots, t_k)$ where $t_1, \ldots, t_k$, $k \geq 0$, are $\mathcal{L}_M$-terms and F is a k-ary function symbol of $\mathcal{L}$. Expand M to an $\mathcal{L}_M$-structure by defining $m^M = m$ for all $m \in M$. The *interpretation* t^M of t is defined by $F^M(t_1^M, \ldots, t_k^M)$, where $t_1^M, \ldots, t_k^M$ are the interpretations of $t_1, \ldots, t_k$. △

For $k = 0$ this definition coincides with the interpretation of a constant $m \in M$ in the $\mathcal{L}_M$-structure m. This provides the base of the inductive definition.

Finally we define the notion of truth of closed $\mathcal{L}$-formulas using *reverse induction*.

Definition 3.2.7 (Truth)**.** Let $\mathcal{L}$ be a language and M an $\mathcal{L}$-structure and ϕ an $\mathcal{L}_M$-sentence. Then ϕ is *true* for M or M *satisfies* ϕ (notation: $M \models \phi$) if and only if either

1) ϕ equals $R(t_1, \ldots, t_k)$ for some closed $\mathcal{L}_M$-terms $t_1, \ldots, t_k$, $k \geq 0$, and a k-ary relation symbol R of $\mathcal{L}$ such that $(t_1^M, \ldots, t_k^M) \in R^M$, or

2) ϕ equals $\psi_0 \vee \psi_1$ where ψ_0 and ψ_1 are $\mathcal{L}_M$-formulas such that $M \models \psi_0$ or $M \models \psi_1$, or

3) ϕ equals $\neg\psi$ where ψ is an $\mathcal{L}_M$-formula such that not $M \models \psi$ (notation: $M \not\models \psi$), or

4) ϕ equals $\exists v_i \psi$ where ψ is an $\mathcal{L}_M$-formula and $i \in \mathbb{N}$ such that there exists a $m \in M$ with $M \models \psi[m/v_i]$.

If $\Gamma \subseteq \mathcal{F}_\mathcal{L}$ is a set of $\mathcal{L}$-sentences, then M is a *model* of Γ (notation: $M \models \Gamma$) if and only if $M \models \phi$, for all $\phi \in \Gamma$. △

Note that property 4) of this definition forced us to use the extended language $\mathcal{L}_M$.

Structure homomorphisms. As seen in Example 3.2.2, an $\mathcal{L}_{\text{ring}}$-structure is a generalization of a ring. It is not a surprise that we can also generalize the notion of a ring homomorphism. We will do this for an arbitrary language.

Definition 3.2.8 (Homomorphisms)**.** Let $\mathcal{L}$ be a language and let M and N be $\mathcal{L}$-structures. A map $j : M \to N$ is called an *$\mathcal{L}$-homomorphism* if and only if

1) $j(c^M) = c^M$, for every constant c in $\mathcal{L}$.

2) $j(F^M(\vec{m})) = F^N(j\vec{m})$, for each function symbol F of $\mathcal{L}$;

3) if $\vec{m} \in R^M$ then $j(\vec{m}) \in R^N$, for each relation symbol R of $\mathcal{L}$.

An $\mathcal{L}$-homomorphism $j : M \to N$ is called an *$\mathcal{L}$-isomorphism* if and only if there exist a $j' : N \to M$ with $j' \circ j = \text{id}_M$ and $j \circ j' = \text{id}_N$. △

If N is an $\mathcal{L}$-substructure of a $\mathcal{L}$-structure M, then the inclusion map induces an $\mathcal{L}$-homomorphism. The converse is not true: if $j : N \to M$ is an $\mathcal{L}$-homomorphism, then $j(N)$ need not be an $\mathcal{L}$-substructure of M, as we only have that $R^N \subseteq R^k \cap M^k$. This motivates the definition of $\mathcal{L}$-embeddings.

Definition 3.2.9 (Embeddings)**.** Let $\mathcal{L}$ be a language and let M and N be $\mathcal{L}$-structures. A map $j : M \to N$ is called an *$\mathcal{L}$-embedding* if and only if j is an $\mathcal{L}$-homomorphism with $j(R^M) = R^N$, for each relation symbol R of $\mathcal{L}$. △

Notice that an $\mathcal{L}$-embedding is injective, as $j(m_1) = j(m_2)$ implies $m_1 = m_2$. This justifies the term embedding.

If j is an $\mathcal{L}$-isomorphism, then it is easy to see that j is an $\mathcal{L}$-embedding.

The following theorem gives another characterization of $\mathcal{L}$-homomorphisms and $\mathcal{L}$-embeddings and a useful property of $\mathcal{L}$-isomorphisms.

Theorem 3.2.10. *Let $\mathcal{L}$ be a language and M and $j : M \to N$ a map of $\mathcal{L}$-structures.*

1) If j is an $\mathcal{L}$-homomorphism, then $M \models \phi(\vec{m})$ implies $N \models \phi(j\vec{m})$ for all atomic $\mathcal{L}$-formulas $\phi(\vec{x})$ and all $\vec{m}$ in M.

2) If j is an $\mathcal{L}$-embedding, then $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$ for all quantifier-free $\mathcal{L}$-formulas $\phi(\vec{x})$ and all $\vec{m}$ in M.

3) If j is an $\mathcal{L}$-isomorphism, then $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$ for all $\mathcal{L}$-formulas $\phi(\vec{x})$ and all $\vec{m}$ in M.

Proof. We first prove a preliminary result. Suppose that j is an $\mathcal{L}$-homomorphism. Let t be an $\mathcal{L}$-term with free variables among $x_1, \ldots, x_n$, $\vec{m} \in M^n$ and $n \in M$. We will show with induction on terms that $j(t^M(\vec{m})) = t^N(j\vec{m})$.

If t is a variable, then we trivially have that $j(t^M(\vec{m})) = t^N(j\vec{m})$.

If t equals $F(t_1, \ldots, t_k)$, with f a k-ary, $k \geq 0$, function symbol of $\mathcal{L}$ and t_i an $\mathcal{L}$-term with free variables among $x_1, \ldots, x_n$, then

$$j(t^M(\vec{m})) = j(F^M(t_1(\vec{m}), \ldots, t_k(\vec{m}))).$$

Now since j is an $\mathcal{L}$-homomorphism we see that

$$j(t^M(\vec{m})) = F^N(j(t_1(\vec{m})), \ldots, j(t_k(\vec{m})))$$

and with the induction hypothesis we find that $j(t^M(\vec{m})) = t^N(j\vec{m})$.

We conclude that $j(t^M(\vec{m})) = t^N(j\vec{m})$ for all $\mathcal{L}$-terms $t(\vec{x})$, $\vec{m} \in M^n$ and $n \in M$.

1) Suppose that j is an $\mathcal{L}$-homomorphism and let ϕ be an atomic formula with free variables among $x_1, \ldots, x_n$ and $\vec{m} \in M^n$. We show that $M \models \phi(\vec{m})$ implies $N \models \phi(j\vec{m})$. Suppose that $M \models \phi(\vec{m})$. As ϕ is atomic, ϕ equals $R(t_1(\vec{x}), \ldots, t_k(\vec{x}))$, with R a k-ary relation symbol and $t_i(\vec{x})$ an $\mathcal{L}$-term. Then this is equivalent to

$$(t_1(\vec{m}), \ldots, t_k(\vec{m})) \in R^M.$$

This implies that

$$(j(t_1(\vec{m})), \ldots, j(t_k(\vec{m}))) \in R^N,$$

since j is an $\mathcal{L}$-homomorphism. Note that this would be an equivalence, whenever j was an $\mathcal{L}$-embedding. We conclude from the preliminary result that $(t_i(j\vec{m}))_{i=1}^k \in R^N$ and $N \models \phi(j\vec{m})$.

2) Suppose that j is an $\mathcal{L}$-embedding and let ϕ be a quantifier-free $\mathcal{L}$-formula with free variables among $x_1, \ldots, x_n$ and $\vec{m} \in M^n$. We will show with induction on formulas that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ is atomic, we conclude from the proof of the first item that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\psi_0 \vee \psi_1$, then the induction hypothesis implies that $M \models \psi_i(\vec{m})$ if and only if $N \models \psi_i(j\vec{m})$ for both i. Hence $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\neg\psi$, then the induction hypothesis implies that $M \models \psi(\vec{m})$ if and only if $N \models \psi(j\vec{m})$. With contraposition we find that $M \not\models \psi(\vec{m})$ if and only if $N \not\models \psi(j\vec{m})$. This shows that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\exists x\psi$, then ϕ is not quantifier-free, which contradicts the assumption.

We conclude that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$ for all quantifier-free $\mathcal{L}$-formulas $\phi(\vec{x})$ and all $\vec{m}$ in M.

3) Suppose that j is an $\mathcal{L}$-isomorphism. Let ϕ be an $\mathcal{L}$-formula with free variables among $x_1, \ldots, x_n$ and $\vec{m} \in M^n$. We will show with induction on formulas that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ is atomic, then the fact that j is an $\mathcal{L}$-embedding shows that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\psi_0 \vee \psi_1$, then the induction hypothesis implies that $M \models \psi_i(\vec{m})$ if and only if $N \models \psi_i(j\vec{m})$ for both i. Hence $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\neg\psi$, then the induction hypothesis implies that $M \models \psi(\vec{m})$ if and only if $N \models \psi(j\vec{m})$. With contraposition we find that $M \not\models \psi(\vec{m})$ if and only if $N \not\models \psi(j\vec{m})$. This shows that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

If ϕ equals $\exists x\psi$, then $M \models \psi(\vec{m})$ is equivalent to $M \models \psi(a, \vec{m})$ for some $a \in M$. Hence with the induction hypothesis and the fact the j is surjective, we find that this is equivalent to $N \models \psi(j(a), j\vec{m})$, which shows that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$.

We conclude that $M \models \phi(\vec{m})$ if and only if $N \models \phi(j\vec{m})$ for all $\mathcal{L}$-formulas $\phi(\vec{x})$ and all $\vec{m}$ in M. □

Elementary equivalence. As we now have a good notion of truth, we also have a good notion of whether two structures have the same properties:

Definition 3.2.11 (Elementary equivalence)**.** Let M and N be $\mathcal{L}$-structures. Then M is *elementary equivalent* to N (notation $M \equiv N$) if and only if $M \models \phi$ if and only if $N \models \phi$, for all $\mathcal{L}$-sentences ϕ. △

An example of elementary equivalent structures are isomorphic structures. Indeed, if $j : M \to N$ an $\mathcal{L}$-isomorphism between $\mathcal{L}$-structures, then application of Theorem 3.2.10 shows that M and N are elementary equivalent. In the following chapters we will determine whether the converse is true for some specific $\mathcal{L}_{\text{ring}}$-structures.

Formulas and properties. Let $\mathcal{L}$ be a language and M an $\mathcal{L}$-structure. Then an $\mathcal{L}$-sentence can be seen as a property of M. Two $\mathcal{L}$-sentences ϕ and ψ may define the same property in every $\mathcal{L}$-structure; $M \models \phi \leftrightarrow \psi$, for every $\mathcal{L}$-structure M. In this case ϕ and ψ are called *equivalent*.

If $\phi(\vec{v})$ is an $\mathcal{L}$-formula with free variables among $v_1, \ldots, v_n$ for some integer $n \geq 0$, then $\phi(\vec{v})$ can be seen as a property of an n-tuple $\vec{m} \in M^n$. Two $\mathcal{L}$-formulas $\phi(\vec{v})$ and $\psi(\vec{v})$ may define the same property in every $\mathcal{L}$-structure; $M \models \forall \vec{v}(\phi(\vec{v}) \leftrightarrow \psi(\vec{v}))$, for every $\mathcal{L}$-structure M. In this case $\phi(\vec{v})$ and $\psi(\vec{v})$ are called *equivalent*.

In general we will only be interested in whether two formulas define the same property in a special kind of $\mathcal{L}$-structure, namely an $\mathcal{L}$-structure M with $M \models \phi$ for every ϕ in a given set Γ of $\mathcal{L}$-sentences. In order to make this generalization, we define the following:

Definition 3.2.12 (Semantical consequence)**.** Let $\mathcal{L}$ be a language, Γ a set of $\mathcal{L}$-sentences and ϕ an $\mathcal{L}$-sentence. Then ϕ is a *(semantical) consequence* of Γ (notation: $\Gamma \models \phi$) if and only if $M \models \Gamma$ implies $M \models \phi$ for every $\mathcal{L}$-structure M. △

Using this definition we generalize the above definition of equivalent formulas.

Definition 3.2.13 (Equivalent formulas)**.** Let $\mathcal{L}$ be a language, Γ a set of $\mathcal{L}$-sentences and ϕ and ψ two $\mathcal{L}$-formulas with free variables among $x_1, \ldots, x_n$. Then ϕ and ψ are called Γ-*equivalent* if and only if $\Gamma \models \forall \vec{x}(\phi \leftrightarrow \psi)$. Moreover ϕ and ψ are called *equivalent* if and only if $\Gamma = \emptyset$. △

It is easy to see that this relation is an equivalence relation on the set of $\mathcal{L}$-formulas and its equivalence classes are called *properties*.

For notational convenience in the following theorem we will say that an $\mathcal{L}$-formula λ is an $\mathcal{L}$-*literal* if and only if either $\lambda = \alpha$ or $\lambda = \neg\alpha$ for some atomic $\mathcal{L}$-formula α.

Theorem 3.2.14 (Disjunctive normal form)**.** *Let $\mathcal{L}$ be a language. Every quantifier-free $\mathcal{L}$-formula is equivalent to an $\mathcal{L}$-formula of the form*

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \lambda_{ij},$$

where $m, n \geq 1$ are integers and λ_{ij} are $\mathcal{L}$-literals, i.e., either $\lambda_{ij} = \alpha$ or $\lambda_{ij} = \neg\alpha$ for some atomic $\mathcal{L}$-formula α.

Proof. Let ϕ be a quantifier-free $\mathcal{L}$-formula. We will show by induction on the formulas that ϕ is equivalent to an $\mathcal{L}$-formula of the form $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \lambda_{ij}$, where $m, n \geq 1$ are integers and λ_{ij} are $\mathcal{L}$-literals.

If ϕ is atomic, then this is trivial.

If ϕ equals $\psi_0 \vee \psi_1$, then it follows trivially from the induction hypothesis on ψ_i.

If ϕ equals $\neg\psi$, then with the induction hypothesis we find that ψ is equivalent to an $\mathcal{L}$-formula of the form $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \lambda_{ij}$. Now ψ states the following: there is an $i \in \{1, \ldots, n\}$ such that for all $j \in \{1, \ldots, m\}$ we have that λ_{ij} is true. Now ψ states: for all $i \in \{1, \ldots, n\}$ there is an $j \in \{1, \ldots, m\}$ such that that λ_{ij} is false. This can be rewritten as: there is a map $f : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that for all $i \in \{1, \ldots, n\}$ we have that $\lambda_{if(i)}$ is false. The above discussion shows that we have proved the following equivalences:

$$\neg \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \lambda_{ij} \quad \leftrightarrow \quad \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m} \neg\lambda_{ij} \quad \leftrightarrow \quad \bigvee_{f} \bigwedge_{i=1}^{n} \neg\lambda_{if(i)}.$$

Hence ϕ is of the correct form.

If ϕ equals $\exists x\psi$, then ϕ is not quantifier-free which contradicts the assumption.

We conclude that for all quantifier-free $\mathcal{L}$-formulas ϕ are equivalent to an $\mathcal{L}$-formula of the form $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \lambda_{ij}$, where $m, n \geq 1$ are integers and λ_{ij} are $\mathcal{L}$-literals. □

3.3. Proofs

Definition 3.3.1 (Labelled trees)**.** Let $\mathcal{L}$ be a language. An $\mathcal{L}$-labelled tree T is a finite set T together with a partial order $\leq$, a function $f : T \to \mathcal{F}_{\mathcal{L}}$ and a set $M \subseteq T$ such that

1) T has a least element;

2) the set $\{x \in T \mid x \leq y\}$ is totally ordered for all $y \in T$;

3) every $x \in M$ is maximal in T

The function f is called the *labelling function* of T and the set M is called the set of *marked leaves* of T. The least element of T is called the *root* of T. Any maximal element of T is called a *leaf* of T. If r is the root of T, then $f(r)$ is called the *conclusion* of T. If a is a (marked) leaf of T, then $f(a)$ is called an (*marked*) *assumption* of T. △

We will not care about the specific elements of a tree, but we will only be interested in the labels of that elements. Therefore we will consider two labelled trees to be identical whenever they are isomorphic as a partially ordered set and the labels are fixed under the isomorphism.

Example 3.3.2 (Assumption tree)**.** Let T be a singleton set (i.e., T consist of one element r) and let ϕ be an $\mathcal{L}$-formula, for some language $\mathcal{L}$. Then T together with partial order $=$, the function $f(r) = \phi$ and the empty set $\emptyset$, is called the *assumption tree* with conclusion ϕ (notation: $\mathrm{ass}(\phi)$). ◊

Example 3.3.3 (Joining trees)**.** Let k be a positive integer, $\mathcal{L}$ a language, T_i be an $\mathcal{L}$-labelled tree with labelling function f_i and marked leaves M_i for $i = 1, \ldots, k$. For any element r, let T_r be the disjoint union $\{r\} \sqcup T_1 \sqcup \cdots \sqcup T_k$, together with the partial order $\leq$ defined by $x \leq y$ if and only if $x = r$ or $x \leq_i y$ for some i, the labelling function f given by

$$f(x) := \begin{cases} \phi & \text{if } x = r \\ f_i(x) & \text{if } x \in T_i \end{cases},$$

and the marked leaves given by the disjoint union $M_1 \sqcup \cdots \sqcup M_k$. Then T_r is the tree which *joins* $T_1, \ldots, T_k$ by adding the conclusion ϕ (notation: $(T_1, \ldots, T_k)_\phi$). Note that we do not care about the specific element r, which implies that this tree is well defined. ◊

Example 3.3.4 (Marking trees)**.** Let $\mathcal{L}$ be a language, T an $\mathcal{L}$-labelled tree with labelling function f and marked leaves M, and ϕ an $\mathcal{L}$-formula. Then the $\mathcal{L}$-labelled tree T with marked leaves $M \cup f^{-1}(\phi)$ is the tree which marks all assumptions ϕ in T (notation: T^ϕ). ◊

Definition 3.3.5 (Proof trees)**.** Let $\mathcal{L}$ be a language. An $\mathcal{L}$-labelled tree T is called a *proof tree* if and only if either

1) $T = \mathrm{ass}(\phi)$, where ϕ is an $\mathcal{L}$-formula (*assumption*);

2) $T = (T_0, T_1)_{\psi_0 \vee \psi_1}$, where ψ_i is an $\mathcal{L}$-formula and T_i a proof tree with conclusion ψ_i ($\vee$-*introduction*), or

3) $T = (S, T_0^{\psi_0}, T_1^{\psi_1})_\chi$, where χ and ψ_i are $\mathcal{L}$-formulas, S a proof tree with conclusion $\psi_0 \vee \psi_1$ and T_i a proof tree with conclusion χ ($\vee$-*elimination*), or

4) $T = (T^\psi)_{\neg\psi}$, where ψ is an $\mathcal{L}$-formula and T a proof tree with conclusion $\bot$ ($\neg$-*introduction*), or

5) $T = (S, T)_\bot$, where ψ is an $\mathcal{L}$-formula, S a proof tree with conclusion ψ and T a proof tree with conclusion $\neg\psi$ ($\neg$-*elimination*), or

6) $T = (T^{\neg\psi})_\psi$, where ψ is an $\mathcal{L}$-formula and T a proof tree with conclusion $\bot$ ($\bot$-*elimination*), or

7) $T = (T)_{\exists v_i \psi}$, where $\exists v_i \psi$ and $\phi[t/v_i]$ are $\mathcal{L}$-formulas and T a proof tree with conclusion $\phi[t/v_i]$ ($\exists$-*introduction*), or

8) $T = (T, S^{\phi[v_j/v_i]})_\chi$, with T and S a proof trees with conclusions $\exists v_i \phi$ and χ respectively, and v_j is a variable such that v_j does not occur in ϕ, in χ or in any unmarked assumptions of $S^{\phi[v_j/v_i]}$ ($\exists$-*elimination*), or

9) $T = (T, S)_{\phi[s/v_i]}$, with t and s an $\mathcal{L}$-terms, T and S proof trees with conclusions $\phi[t/v_i]$ and $s = t$ respectively, and $\phi[s/v_i]$ an $\mathcal{L}$-formula (*substitution*). △

Note that, since an $\mathcal{L}$-labelled tree is finite, every proof tree can be constructed from finitely many assumption trees.

Definition 3.3.6 (Provability)**.** Let $\mathcal{L}$ be a language, $\Gamma \subseteq \mathcal{F}_\mathcal{L}$ a set of $\mathcal{L}$-formulas and ϕ an $\mathcal{L}$-formula. Then ϕ is provable from Γ (notation: $\Gamma \vdash \phi$) if and only if there exists a proof tree T with unmarked assumptions among $\Gamma \cup \{\forall v_i(v_i = v_i) \mid i \in \mathbb{N}\}$. △

We will abbreviate $\{\phi\} \vdash \psi$ as $\phi \vdash \psi$ and abbreviate $\emptyset \vdash \psi$ as $\vdash \psi$. In view of Definition 3.2.12, our definition of provability is sound in the following sense:

Theorem 3.3.7 (Soundness)**.** *Let $\mathcal{L}$ be a language, Γ a set of $\mathcal{L}$-formulas and ϕ an $\mathcal{L}$-formula. If $\Gamma \vdash \phi$ then $\Gamma \models \phi$.*

Proof. See Theorem 3.2.1 on page 87 of [9]. □

Gödel proved, using the axiom of choice, that the converse of this theorem is also true. This is very useful as we shall see.

Theorem 3.3.8 (Completeness)**.** *Let $\mathcal{L}$ be a language, Γ a set of $\mathcal{L}$-formulas and ϕ an $\mathcal{L}$-formula. If $\Gamma \models \phi$ then $\Gamma \vdash \phi$.*

Proof. See Theorem 3.2.2 on page 87 of [9]. □

3.4. Computable functions

In this section we will define when an arithmetic function is computable. The following definition does this in an inductive way.

Definition 3.4.1 (Computable functions)**.** A partial function $f : \mathbb{N}^k \to \mathbb{N}$, $k \geq 1$, is called *computable* or *recursive* if and only if either

1) f is the *zero function*, i.e., $k = 1$ and $f(x) = 0$ for all $x \in \mathbb{N}$, or

2) f is the *successor function*, i.e., $k = 1$ and $f(x) = x + 1$ for all $x \in \mathbb{N}$;

3) f is a *projection function*, i.e., $f(\vec{x}) = x_i$ for some $1 \leq i \leq k$ and all $\vec{x} = (x_1, \ldots, x_k) \in \mathbb{N}^k$, or

4) f is obtained by *composition*, i.e., $f(\vec{x}) = g(h_1(\vec{x}), \ldots, h_\ell(\vec{x}))$ for all $\vec{x} \in \mathbb{N}^k$, where $g : \mathbb{N}^\ell \to \mathbb{N}$ and $h_j : \mathbb{N}^k \to \mathbb{N}$ for all $1 \leq j \leq \ell$ are partial recursive functions, or

5) f is obtained by *recursion*, i.e., $k = 2$ and $f(x, 0) = g(x)$ and $f(x, y + 1) = h(x, y, f(x, y))$ for all $x, y \in \mathbb{N}$, where $g : \mathbb{N} \to \mathbb{N}$ and $h : \mathbb{N}^3 \to \mathbb{N}$ are partial recursive functions, or

6) f is obtained by *minimization*, i.e., $f(\vec{x}) = \min\{y \in \mathbb{N} \mid g(\vec{x}, y) = 0\}$ for all $\vec{x} \in \mathbb{N}^k$, where $g : \mathbb{N}^{k+1} \to \mathbb{N}$ is a partial recursive function. △

Any property of a partial function may be translated to subsets $A \subseteq \mathbb{N}$ of the domain by means of its *characteristic function* χ_A defined by

$$\chi_A : x \mapsto \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Definition 3.4.2 (Decidable subsets)**.** A subset $A \subseteq \mathbb{N}$ is called *computable* or *decidable* if and only if its characteristic function is computable. △

Example 3.4.3. The following functions/relations are computable

1) $\{(n, m) \mid n = m\}$ (see Example 7.1 in [2]);

2) $\{(n,m) \mid n \leq m\}$ (see Example 7.1 in [2]);

3) $(n,m) \mapsto n+m$ (see Example 6.2 in [2]);

4) $(n,m) \mapsto n \cdot m$ (see Example 6.3 in [2]);

5) The $(n+1)$-th prime number $\pi(n)$ (see Example 7.12 in [2]);

6) The order of n at m:

$$\operatorname{ord}(n,m) = \begin{cases} \max\{k \mid m^k \text{ divides } n\} & \text{if } n,m \geq 2 \\ 0 & \text{otherwise} \end{cases}$$

(see Example 7.11 in [2]);

7) The remainder of n up to division by m: $\operatorname{rem}(n,m)$ (see Example 7.7 in [2]).

$\Diamond$

3.5. Gödel numberings

In this section we will show that in some languages the set of all formulas may be identified in a nice way with a subset of the natural numbers.

Definition 3.5.1 (Code of a sequence)**.** Let n be a non-negative integer and $(a_i)_{i=1}^n$ a finite sequence in $\mathbb{N}$. Then $x \in \mathbb{N}$ is called the *code of* $(a_i)_{i=1}^n$ (notation: $\langle a_1, \ldots, a_n \rangle$) if and only if

$$x = 2^n 3^{a_1} 5^{a_2} \cdots \pi(n)^{a_n},$$

where $\pi(i)$ is the $(i+1)$-th prime number (i.e, $\pi(0) = 2$). $\triangle$

Since every non-zero natural number admits a factorization into prime numbers, we see that every non-zero natural number encodes some sequence.

Let x and y in $\mathbb{N}$ be the codes of the sequences $(a_i)_{i=1}^n$ and $(b_i)_{i=1}^m$ respectively. Then define $\operatorname{lh}(x) := n$,

$$x_i := \begin{cases} a_i & \text{if } 1 \leq i \leq \operatorname{lh}(x) \\ 0 & \text{otherwise} \end{cases}$$

and $x * y = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$. The maps lh, $(\cdot)_i$ and $*$ are in fact computable by Example 3.4.3.

Definition 3.5.2 (Gödel Numbering)**.** Let $\mathcal{L}$ be a language, $\ulcorner \cdot \urcorner$ be a map from the set of $\mathcal{L}$-strings to $\mathbb{N}$ and let $g : \mathbb{N} \to \mathbb{N}$ be the partial map given by

$$\begin{aligned} \langle 1, \ulcorner v_i \urcorner \rangle &\mapsto \langle 1, i \rangle, \\ \langle 2, \ulcorner f_i(t_1, \ldots, t_k) \urcorner \rangle &\mapsto \langle 2, i, \ulcorner t_1 \urcorner, \ldots, \ulcorner t_k \urcorner \rangle, \\ \langle 3, \ulcorner R_i(t_1, \ldots, t_k) \urcorner \rangle &\mapsto \langle 3, i, \ulcorner t_1 \urcorner, \ldots, \ulcorner t_k \urcorner \rangle, \\ \langle 4, \ulcorner \phi_0 \vee \phi_1 \urcorner \rangle &\mapsto \langle 4, \ulcorner \phi_0 \urcorner, \ulcorner \phi_1 \urcorner \rangle, \\ \langle 5, \ulcorner \neg \phi \urcorner \rangle &\mapsto \ulcorner 5, \phi \urcorner, \\ \langle 6, \ulcorner \exists v_i \phi \urcorner \rangle &\mapsto \langle 6, \ulcorner v_i \urcorner, \ulcorner \phi \urcorner \rangle. \end{aligned}$$

Then $\ulcorner \cdot \urcorner$ is called a *Gödel numbering* of $\mathcal{L}$ if and only if g is injective, both g and g^{-1} are computable and both the domain and the image of g are decidable. $\triangle$

Example 3.5.3. Let $A \subseteq \mathbb{N}$ be a undecidable subset. Consider the language $\mathcal{L}_A$ which has an a-ary relation symbol R_a for all $a \in A$. Then $\mathcal{L}_A$ does not admit any Gödel numbering. Indeed, suppose that $\ulcorner \cdot \urcorner$ is a Gödel numbering and let $a \in \mathbb{N}$ be given. Then since the image of f is decidable, we have an algorithm that checks whether $\langle 3, a, \ulcorner v_1 \urcorner, \ldots, \ulcorner v_a \urcorner \rangle \in \mathbb{N}$ is in the image of f. Hence we find an algorithm which checks whether $a \in A$, which is a contradiction. $\Diamond$

We will now focus on the language of arithmetic. Recall that this language has two binary function symbols $+$ and $\times$ a binary relation symbol $<$ and two constants $0, 1$.

Theorem 3.5.4. *Every finite language admits a Gödel numbering.*

Proof. Suppose that $\mathcal{L}$-consist of a k_i-ary function symbol f_i for $1 \leq i \leq r$ and an ℓ_j-ary relation symbol R_j for $1 \leq j \leq s$. Then define

$$\begin{aligned}
\ulcorner v_i \urcorner &:= \langle 1, i \rangle \\
\ulcorner f_i(t_1, \ldots, t_{k_i}) \urcorner &:= \langle 2, i, \ulcorner t_1 \urcorner, \ldots, \ulcorner t_{k_i} \urcorner \rangle \\
\ulcorner R_j(t_1, \ldots, t_{\ell_j}) \urcorner &:= \langle 3, j, \ulcorner t_1 \urcorner, \ldots, \ulcorner t_{\ell_j} \urcorner \rangle \\
\ulcorner \psi_0 \vee \psi_1 \urcorner &:= \langle 4, \ulcorner \psi_0 \urcorner, \ulcorner \psi_1 \urcorner \rangle \\
\ulcorner \neg \psi \urcorner &:= \langle 5, \ulcorner \psi \urcorner \rangle \\
\ulcorner \exists v_i \psi \urcorner &:= \langle 6, \ulcorner \psi \urcorner, \ulcorner v_i \urcorner \rangle
\end{aligned}$$

We will show that there exists a partial map g which satisfies the conditions in the definition of the Gödel numbering. Take g by $\langle i, x \rangle \mapsto x$ and g^{-1} is given by $x \mapsto \langle x_1, x \rangle$. These functions are computable. Moreover the domain of g is computable, since $\mathrm{dom}(g) = \{x \in \mathbb{N} \mid x_1 = (x_2)_1\}$. The image of g is computable, since $\mathrm{im}(g) = \{x \in \mathbb{N} \mid f^{-1}(x) \in \mathrm{dom}(g)\}$. We conclude that $\ulcorner \cdot \urcorner$ is a Gödel numbering. □

Theorem 3.5.4 applies to the languages of our interest.

Corollary 3.5.5. *The language of arithmetic $\mathcal{L}_{\mathrm{arith}}$ and the language of rings $\mathcal{L}_{\mathrm{ring}}$ admit a Gödel numbering.*

3.6. Theories

In this section we study properties of collections of sentences, which we will call theories.

Definition 3.6.1 (Theories)**.** Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-theory* is a set T of $\mathcal{L}$-sentences. An element of T is called a *theorem* of T. △

We now list some theories which are important for us.

Example 3.6.2 (Theory of a structure)**.** Let $\mathcal{L}$ be a language and M an $\mathcal{L}$-structure. Then $\mathrm{Th}(M) := \{\phi \in \mathcal{F}^0_{\mathcal{L}} \mid M \models \phi\}$ is called the *theory of M*. ◊

Example 3.6.3 (Elementary diagram)**.** Let $\mathcal{L}$ be a language and M an $\mathcal{L}$-structure. Then the set $\mathrm{diag}(M)$ of all quantifier-free $\mathcal{L}_M$-sentences ϕ with $M \models \phi$ is called the *elementary diagram of M*.

Let M be an $\mathcal{L}$-structure and let N be a model of $\mathrm{diag}(M)$. Then the map $j : M \to N$ given by $m \mapsto m^N$ is a $\mathcal{L}_M$-embedding. We first show that j is a $\mathcal{L}$-homomorphism. If c is a constant in $\mathcal{L}$. Then $c^M = m$ for some $m \in M$ and $c = m \in \mathrm{diag}(M)$ and $m^N = c^N$ and $j(c^M) = j(m) = m^N = c^N$. If f is a function symbol of $\mathcal{L}$ and $f^M(\vec{m}) = n$ for some $\vec{m}, n$ in M, then $f(\vec{m}) = n \in \mathrm{diag}(M)$ and hence $f^N(j\vec{m}) = j(n)$. If R is a relation symbol of $\mathcal{L}$ and $\vec{m} \in R^M$ for some $\vec{m}$ in M, then $R(\vec{m}) \in \mathrm{diag}(M)$ and hence $\vec{m} \in R^N$. We conclude that j is an $\mathcal{L}$-homomorphism. It remains to show that $j(R^M) = R^N$. We have $\vec{m} \in R^M$ if and only if $M \models R(\vec{m})$. Since $N \models \mathrm{diag}(M)$ we see that $M \models R(\vec{m})$ if and only if $N \models R(j\vec{m})$ or equivalently $j\vec{m} \in R^n$. This shows that $j(R^M) = R^N$ ◊

Example 3.6.4 (Theory of fields)**.** The theory T_{ring} of rings is the following set of sentences in the language of rings:

$$\forall x, y, z(x + (y + z) = (x + y) + z)$$
$$\forall x(x + 0 = x)$$
$$\forall x \exists y(x + y = 0)$$
$$\forall x, y(x + y = y + x)$$

which encode that any model of T_{ring} is a commutative group. Furthermore T_{ring} contains the additional senctences:

$$\forall x, y, z(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$$
$$\forall x, y, z(x \cdot (y + z) = x \cdot y + x \cdot z)$$
$$\forall x(x \cdot 1 = x)$$
$$\forall x, y(x \cdot y = y \cdot x).$$

Clearly R is a model of T_{ring} if and only if R is a ring. Similarly we are able to define the theory of fields T_{field}, which has the additional sentences

$$0 \neq 1$$
$$\forall x \exists y(x = 0 \vee xy = 1).$$

We clearly have $T_{\text{field}} \models T_{\text{ring}}$ ◊

Let us now examine two important properties of theories, namely consistency and decidability.

Consistency. A general theory T may consist of contradictory sentences, i.e., $T \vdash \bot$. In this case T does not have a model. On the other hand, if T does not have a model, then trivially $T \models \bot$. By the completeness theorem, we conclude that $T \vdash \bot$. This leads to the following definition.

Definition 3.6.5 (Consistency)**.** A theory T in a language $\mathcal{L}$ is called *consistent* if and only if T has a model. △

If T is an infinite theory it is hard to see whether T is consistent. However the compactness theorem gives a solution to this.

Theorem 3.6.6 (Compactness theorem)**.** *Let $\mathcal{L}$ be a language. An $\mathcal{L}$-theory is consistent if and only every finite subtheory is consistent.*

Proof. Let Γ be an $\mathcal{L}$-theory. If Γ is consistent, then it has a model. Hence every finite subtheory has a model and is consistent. Conversely suppose that Γ is not consistent. Then trivially $\Gamma \models \bot$, since there are no $\mathcal{L}$-structures with $M \models \Gamma$ (c.f., Definition 3.2.12). By the completeness theorem we find that $\Gamma \vdash \bot$. Hence there exists a proof tree T with unmarked assumptions among $\Gamma \cup \{\forall v_i(v_i = v_i) \mid i \in \mathbb{N}\}$. Let Γ_0 be the set of unmarked assumptions of T. Since T is finite, we see that Γ_0 is finite. Moreover, $\Gamma_0 \vdash \bot$. By the soundness theorem, we conclude that $\Gamma_0 \models \bot$. Hence we found a finite subtheory Γ_0 of Γ which is not consistent. This proves the theorem. □

Decidability. Using the Gödel numbering we find a correspondence of theories and of subsets of $\mathbb{N}$. Properties of subsets of $\mathbb{N}$ translate to properties of theories:

Definition 3.6.7 (Decidability)**.** Let $\mathcal{L}$ be a language with Gödel numbering $\ulcorner \cdot \urcorner$ and T a set of $\mathcal{L}$-sentences. Then T is called *decidable* if and only if the image $\ulcorner T \urcorner \subseteq \mathbb{N}$ is decidable. △

The following lemma shows that decidability is independent of the Gödel numbering.

Lemma 3.6.8. *Let $\mathcal{L}$ be a language and T a set of $\mathcal{L}$-sentences. If T is decidable with respect to one Gödel numbering of $\mathcal{L}$ then decidable with respect to any Gödel numbering of $\mathcal{L}$.*

Proof. Suppose that T is decidable with respect to a Gödel numbering $\ulcorner \cdot \urcorner$ and let $\ulcorner \cdot \urcorner'$ be an arbitrary Gödel numbering. We will show with induction on the formulas that the partial map $f : \ulcorner \phi \urcorner' \mapsto \ulcorner \phi \urcorner$ is computable. Then T is decidable with respect to $\ulcorner \cdot \urcorner'$, because the image $x \in \ulcorner T \urcorner'$ if and only if $f(x) \in \ulcorner T \urcorner$.

Then Algorithm 1 on page 71 shows that the partial map $\ulcorner \phi \urcorner' \mapsto \ulcorner \phi \urcorner$ is computable. Hence the image $\ulcorner T \urcorner' \subseteq \mathbb{N}$ is decidable. □

Algorithm 1: Transition function from $\lceil\cdot\rceil_0$ to $\lceil\cdot\rceil_1$

Function `Trans`$(n) : \mathbb{N} \to \mathbb{N}$ **is**
  if $n = \lceil t \rceil_0$ *for some* $\mathcal{L}$*-term* t **then**
    if $n = \lceil f_i(t_1, \ldots, t_k) \rceil_0$ *for some* $\mathcal{L}$*-formula* $f_i(t_1, \ldots, t_k)$ **then**
      compute $(i, \lceil t_1 \rceil_0, \ldots, \lceil t_k \rceil_0) \leftarrow n$
      compute $\lceil t_j \rceil_1 \leftarrow$ `Trans`$(\lceil t_j \rceil_0)$ for all j
      return $\lceil f_i(t_1, \ldots, t_k) \rceil_1 \leftarrow (i, \lceil t_1 \rceil_1, \ldots, \lceil t_k \rceil_1)$
    else if $n = \lceil v_i \rceil_0$ *for some variable* v_i **then**
      compute $i \leftarrow n$
      return $\lceil v_i \rceil_1 \leftarrow i$
  else if $n = \lceil \phi \rceil_0$ *for some* $\mathcal{L}$*-formula* ϕ **then**
    if $n = \lceil \psi_0 \vee \psi_1 \rceil_0$ *for some* ϕ_i **then**
      compute $\lceil \psi_i \rceil_0 \leftarrow n$ and $\lceil \psi_i \rceil_1 \leftarrow$ `Trans`$(\lceil \psi_i \rceil_0)$
      return $\lceil \psi_0 \vee \psi_1 \rceil_1 \leftarrow (\lceil \psi_0 \rceil_1, \lceil \psi_1 \rceil_1)$
    else if $n = \lceil \exists v_i \psi \rceil_0$ *for some* $\mathcal{L}$*-formula* ψ *and variable* v_i **then**
      compute $\lceil v_i \rceil_0 \leftarrow n$ and $\lceil v_i \rceil_1 \leftarrow$ `Trans`$(\lceil v_i \rceil_0)$
      compute $\lceil \psi \rceil_0 \leftarrow n$ and $\lceil \psi \rceil_1 \leftarrow$ `Trans`$(\lceil \psi \rceil_0)$
      return $\lceil \exists v_i \psi \rceil_1 \leftarrow (\lceil v_i \rceil_1, \lceil \psi \rceil_1)$
    else if $n = \lceil \neg \psi \rceil_0$ *for some* $\mathcal{L}$*-formula* ψ **then**
      compute $\lceil \psi \rceil_0 \leftarrow n$ and $\lceil \psi \rceil_1 \leftarrow$ `Trans`$(\lceil \psi \rceil_0)$
      return $\lceil \neg \psi \rceil_1 \leftarrow \lceil \psi \rceil_1$
    else if $n = \lceil R_i(t_1, \ldots, t_k) \rceil_0$ *for some* $\mathcal{L}$*-formula* $R_i(t_1, \ldots, t_k)$ **then**
      compute $(i, \lceil t_1 \rceil_0, \ldots, \lceil t_k \rceil_0) \leftarrow n$
      compute $\lceil t_j \rceil_1 \leftarrow$ `Trans`$(\lceil t_j \rceil_0)$ for all j
      return $\lceil R_i(t_1, \ldots, t_k) \rceil_1 \leftarrow (i, \lceil t_1 \rceil_1, \ldots, \lceil t_k \rceil_1)$
  else
    return 0

Definition 3.6.9 (Axiomatizable)**.** A theory T in a language $\mathcal{L}$ is called *axiomatizable* if and only if there exists a decidable subtheory $A \subseteq T$ with $A \models T$. △

Clearly the assumption that A is decidable makes this definition non-trivial. Otherwise $A = T$ would work.

If M is a model of a theory T in a language $\mathcal{L}$, then every $\mathcal{L}$-sentence ϕ is either true or false in M. This means that either $\mathrm{Th}(M) \models \phi$ or $\mathrm{Th}(M) \models \neg\phi$, since ϕ or $\neg\phi$ is in $\mathrm{Th}(M)$. This need not be true for $T \subseteq \mathrm{Th}(M)$, since there may exists an $\mathcal{L}$-sentence with $M \models \phi$ and $N \models \neg\phi$ for some models M and N of T.

Definition 3.6.10 (Completeness)**.** A theory T in a language $\mathcal{L}$ is called *complete* if and only if either $T \models \phi$ or $T \models \neg\phi$. △

Theorem 3.6.11. *If T is axiomatizable and complete, then T is decidable.*

Proof. Our aim is to find an algorithm which decides whether $T \models \phi$ is true or not. Since T is complete, this reduces to deciding whether $T \models \phi$ or $T \models \neg\phi$ holds. Using the completeness theorem, we see that we have to find an algorithm which decides whether $T \vdash \phi$ or $T \vdash \neg\phi$ is true. We will construct an algorithm which simultaneously seeks a proof for both ϕ and $\neg\phi$. This algorithm will terminate after finitely many steps, because either ϕ or $\neg\phi$ has a proof.

A first step in constructing this algorithm is to encode proof trees, so that finding a proof reduces to finding a natural number which corresponds to that proof. We will define the code $\lceil T \rceil \in \mathbb{N}$ of a proof tree T by induction on proof trees. This code will determine the code of its conclusion, the code of the sequence of all unmarked assumptions and the codes of the proof trees from which it is constructed. To be

precise, we define

$$\begin{aligned}
\ulcorner \mathrm{ass}(\phi) \urcorner &:= \langle 1, \ulcorner \phi \urcorner \rangle \\
\ulcorner (T_0, T_1)_{\psi_0 \vee \psi_1} \urcorner &:= \langle 2, \ulcorner \psi_0 \vee \psi_1 \urcorner, a_0 * a_1, \ulcorner T_0 \urcorner, \ulcorner T_1 \urcorner \rangle \\
\ulcorner (T_0^{\psi_0}, T_1^{\psi_1}, T_2)_{\chi} \urcorner &:= \langle 3, \ulcorner \chi \urcorner, (a_0 \setminus \ulcorner \psi_0 \urcorner) * (a_1 \setminus \ulcorner \psi_1 \urcorner) * a_2, \ulcorner T_0 \urcorner, \ulcorner T_1 \urcorner, \ulcorner T_2 \urcorner \rangle \\
\ulcorner (T_0^{\psi})_{\neg \psi} \urcorner &:= \langle 4, \ulcorner \neg \psi \urcorner, a_0 \setminus \ulcorner \psi \urcorner, \ulcorner T \urcorner \rangle \\
\ulcorner (T_0, T_1)_{\bot} \urcorner &:= \langle 5, \ulcorner \bot \urcorner, a_0 * a_1, \ulcorner T_0 \urcorner, \ulcorner T_1 \urcorner \rangle \\
\ulcorner (T_0^{\neg \psi})_{\psi} \urcorner &:= \langle 6, \ulcorner \psi \urcorner, a_0 \setminus \ulcorner \neg \psi \urcorner, \ulcorner T \urcorner \rangle \\
\ulcorner (T_0)_{\exists v_i \psi} \urcorner &:= \langle 7, \ulcorner \exists v_i \psi \urcorner, a_0, \ulcorner T \urcorner \rangle \\
\ulcorner (T_0, T_1^{\phi[v_j/v_i]})_{\chi} \urcorner &:= \langle 8, \ulcorner \chi \urcorner, a_0 * (a_1 \setminus \ulcorner \phi[v_j/v_i] \urcorner), \ulcorner T_0 \urcorner, \ulcorner T_1 \urcorner \rangle \\
\ulcorner (T_0, T_1)_{\phi[s/v_i]} \urcorner &:= \langle 9, \ulcorner \phi[s/v_i] \urcorner, a_0 * a_1, \ulcorner T_0 \urcorner, \ulcorner T_1 \urcorner \rangle
\end{aligned}$$

where a_i is the second entry of sequence encoded by $\ulcorner T_1 \urcorner$. Here $\setminus$ is defined as follows: if a and b are the codes of sequences (a_i) and (b_j), then $a \setminus b$ is the code of the sequence (a_i), where a_i is left out whenever $a_i \in (b_j)$. This is a computable function.

We will now sketch an algorithm which determines whether n is the code of a proof tree. Let $n \in \mathbb{N}$ be given. Compute the first entry n_0 of the sequence encoded by n. Then check if the rest of the sequence is consistent with this first entry. That is, we check if n_1 is the code of a formula and if n_3, n_4 and n_5 (if applicable) are the codes of proof trees. Note that this is a recursive algorithm. We come back to this later. Then we check whether the conclusion n_1 is correct in view of the conclusion and unmarked assumptions of the subtrees. Note that is most cases we just need to compute the conclusion of the subtrees. However, if $n_0 = 8$, then we need to check that v_j does not occur in ϕ, χ and the unmarked assumptions of $T_1^{\phi[v_j/v_i]}$. This is why we need to be able to compute the unmarked assumptions from a proof tree *without* recursion.

There is also a recursive algorithm $\mathcal{A}$ which decides whether $x \in \mathbb{N}$ is the code of a proof three with unmarked assumptions in a decidable decidable subset $A \subseteq \mathbb{N}$ and with conclusion equal to $y \in \mathbb{N}$.

Using $\mathcal{A}$ we construct an algorithm $\mathcal{B}$ which, given the code $\ulcorner \phi \urcorner$ of an $\mathcal{L}$-formula ϕ and the set of codes $\ulcorner A \urcorner \subseteq \mathbb{N}$ of an axiomatization A of a complete theory T, determines whether $T \models \phi$. For all $n \in \mathbb{N}$, $\mathcal{B}$ checks, using $\mathcal{A}$ whether $n \in \mathbb{N}$ is the code of a proof three with unmarked assumptions in a decidable decidable subset $A \subseteq \mathbb{N}$ and with conclusion equal to $\ulcorner \phi \urcorner \in \mathbb{N}$ or $\ulcorner \neg \phi \urcorner$. Then using the remarks at the beginning of the proof, $\mathcal{B}$ decides whether $T \models \phi$. This shows that T is decidable. □

3.7. Reformulating the goal

In the preceding sections we have introduced the very basic notions of formal logic. In this section we will prepare for the final three chapters by formulating the three questions from the introduction into our developed mathematical language.

We first clarify what the objects and the statements from the introduction are. The set of objects is a family of isomorphism classes of $\mathcal{L}_{\mathrm{ring}}$-structures. The statements about these objects are $\mathcal{L}_{\mathrm{ring}}$-formulas.

Before we reformulate the questions, we first introduce some notation. Let E be a family of isomorphism classes $\mathcal{L}_{\mathrm{ring}}$-structures (e.g., E consists of all algebraically closed fields) and let e be an isomorphism class in E. Then Theorem 3.2.10 shows that for all fields K and L in e we have that $\mathrm{Th}(K) = \mathrm{Th}(L)$. Hence we may just write $\mathrm{Th}(e)$ instead of $\mathrm{Th}(K)$ or $\mathrm{Th}(L)$.

Now we will reformulate the first question. This question ask if it is decidable whether a given statement is true for a given object. In other words it asks:

Question 1. *Is* $\mathrm{Th}(e)$ *decidable, for all* $e \in E$*?*

In order to reformulate the second question, we will need a good definition of what is meant by a distinguished class.

Definition 3.7.1 (Definable subset of E)**.** A subset $S \subseteq E$ is called *definable* if and only if there exists an $\mathcal{L}_{\text{ring}}$-sentence ϕ such that for all $e \in E$

$$e \in S \quad \text{if and only if} \quad \phi \in \text{Th}(e).$$

An isomorphism class $e \in E$ is definable if and only if the subset $\{e\} \subseteq E$ is definable. △

Now the second question may be reformulated as follows.

Question 2. *What are the definable subsets of E?*

The third question asks if it is true that objects with the same properties are equal. Thus, in terms of isomorphism classes of $\mathcal{L}_{\text{ring}}$-structures and $\mathcal{L}_{\text{ring}}$-formulas, this question asks:

Question 3. *Is $e = f$ whenever $\text{Th}(e) = \text{Th}(f)$, for all $e, f \in E$?*

If this question has a positive answer, then the terms 'isomorphic' and 'elementary equivalent' are interchangeable.

If every isomorphism class is definable, then Question 3 has a positive answer. Indeed if $\text{Th}(e) = \text{Th}(f)$, then f satisfies the defining formula of e, hence $e = f$.

3.8. Representability

In the remaining sections of this chapter we will make preparations for chapter 4. There we will show that the theory of a global field is not decidable. The proof of this fact can be divided into two steps. We first show that the theory of natural number in the language of arithmetic is not decidable by proving that it is not definable. Then we show how to interpret the theory of natural numbers in the theory of a global field and prove that de undecidability is preserved under this interpretation.

In this section we will introduce the notion of definability and representability. The former is used in the next section and the latter is used in the last section.

Definition 3.8.1 (Representable functions)**.** Let M be an $\mathcal{L}$-structure. A partial k-ary function $F : M^k \to M$, $k \geq 0$, is called *$\mathcal{L}$-representable* if and only if there exists an $\mathcal{L}$-formula $\phi(y, \vec{x})$ such that for all $m \in M$ and $\vec{n} \in \text{dom}(F)$ we have

$$M \models \phi(m, \vec{n}) \quad \text{if and only if} \quad m = F(\vec{n}).$$

In this case we say that $\phi(y, \vec{x})$ *represents* F. △

If $\mathcal{L}$ is understood, then we may write just representable. Notice that the property of representability translates to relations by means of the characteristic function.

Definition 3.8.2 (Representable relations)**.** Let M be an $\mathcal{L}$-structure, $k \geq 0$ an integer and R a k-ary relation in $\mathcal{L}$. Then R is called *$\mathcal{L}$-representable* if and only if the characteristic function $\chi_R : M^k \to \{0, 1\}$ is $\mathcal{L}$-representable. △

If R is nullary, then $A = R^M$ is just a subset of M. We call a subset A an *$\mathcal{L}$-definable* if and only if A is $\mathcal{L}$-representable as a relation. Suppose that the characteristic function χ_A of $A \subseteq M$ is $\mathcal{L}$-representable. Then we find a formula $\phi(y, x)$ which represents χ_A. Now we have that

$$A = \{x \in M \mid M \models \chi_A(1, x)\},$$

which explains why A is called $\mathcal{L}$-definable.

We will now study the intersection of two $\mathcal{L}$-definable sets.

Lemma 3.8.3. *Let M be an $\mathcal{L}$-structure and A and B be $\mathcal{L}$-definable sets in M. Then $A \cap B$ is an $\mathcal{L}$-definable subset of M.*

Proof. Let $\phi(x)$ and $\psi(x)$ be the defining formulas for A and B respectively. Then $\phi(x) \wedge \psi(x)$ is the defining formula for the intersection. □

It turns out that some $\mathcal{L}$-definable subsets are related, that is, they are a member of the same family.

Definition 3.8.4 (Definable families)**.** Let M be an $\mathcal{L}$-structure. An *$\mathcal{L}$-definable family* in M is a collection $\mathscr{F}$ of subsets *parametrized* by an $\mathcal{L}$-formula $\phi(x;\vec{y})$ with n parameters satisfying $\psi(\vec{y})$, that is,

$$\mathscr{F} = \{A_{\vec{c}} \mid \vec{c} \in M^n, M \models \psi(\vec{c})\}, \quad \text{with} \quad A_{\vec{c}} = \{m \in M \mid M \models \phi(m;\vec{c})\}. \qquad \triangle$$

Note that members of a $\mathcal{L}$-definable family in M are in fact $\mathcal{L}_M$-definable

Lemma 3.8.5. *Let M be an $\mathcal{L}$-structure and $\mathscr{F}$ a $\mathcal{L}$-definable family in M. Then $\bigcap_{S\in\mathscr{F}} S$ is a $\mathcal{L}$-definable set.*

Proof. Let $\phi(x,\vec{y})$ be the formula which parametrizes $\mathscr{F}$ and let $\psi(\vec{y})$ determine the parameters. Then it is clear that $\forall\vec{y}(\psi(\vec{y}) \wedge \phi(x,\vec{y}))$ defines the intersection. □

3.9. Theory of natural numbers

In this section we will show that the set of Gödel numbers $\ulcorner \mathrm{Th}(\mathbb{N}) \urcorner \subseteq \mathbb{N}$ of the theory of natural numbers in the language of arithmetic is not $\mathcal{L}_{\mathrm{arith}}$-definable. This will imply that the theory of natural numbers is not decidable. Furthermore we will show that some specific arithmetic function are representable in $\mathcal{L}_{\mathrm{ring}}$.

Gödels bèta function. In this paragraph we will show that certain arithmetic functions are representable. Gödel realized that there is a strong connection between computable arithmetic maps and $\mathcal{L}_{\mathrm{arith}}$-representable arithmetic maps. This connection simplifies our task, when we need to show that a function is $\mathcal{L}_{\mathrm{arith}}$-representable.

Theorem 3.9.1 (Gödel)**.** *If a partial arithmetic function f is computable then f is $\mathcal{L}_{\mathrm{arith}}$-representable.*

Proof. See Theorem 16.16 and the remark below it on page 212 in [2]. □

A direct consequence of Theorem 3.9.1 is the following:

Corollary 3.9.2. *If a subset $A \subseteq \mathbb{N}$ is decidable then A is $\mathcal{L}_{\mathrm{arith}}$-definable.*

We start with the definition of one of the most useful arithmetic function: the bèta function. This function encodes all finite sequences.

Theorem 3.9.3. *There exists an $\mathcal{L}_{\mathrm{arith}}$-representable function $\beta : \mathbb{N}^3 \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ and $k_1, \ldots, k_n \in \mathbb{N}$ there exists $\vec{x} \in \mathbb{N}^2$ with $\beta(\vec{x}, 0) = n$ and $\beta(\vec{x}, i) = k_i$ for all $1 \leq i \leq n$.*

Proof. Take $\beta(m,k,i) = \mathrm{rem}(k, mi+1)$. Then β is computable (see Example 3.4.3), hence $\mathcal{L}_{\mathrm{arith}}$-representable. We now show that β satisfies the condition. Let $n \in \mathbb{N}$ and $k_1, \ldots, k_n \in \mathbb{N}$. Choose $m = (\max\{n, k_1, \ldots, k_n\})!$ and choose with the Chinese remainder theorem $k \in \mathbb{N}$ with $k \equiv k_i$ modulo $mi+1$ for all $1 \leq i \leq n$. This is possible, because $mi+1$ and $mj+1$ are coprime for $1 \leq i < j \leq n$. Indeed, let p be a common prime divisor. Then $p \mid (mj+1) - (mi+1)$, hence $p \mid m(j-i)$ and $p \mid m$ or $p \mid j-i$ as p is prime. Now since $j - i < n$, we have that $j - i \mid m$. Therefore we find that $p \mid m$ in both cases and since $p \mid mi+1$ we conclude that $p \mid 1$. Thus $mi+1$ and $mj+1$ are coprime. □

The Gödel bèta function can be used to make inductive definitions, like finite sums, finite products or powers.

Corollary 3.9.4. *There exists an $\mathcal{L}_{\mathrm{arith}}$-formula $\phi(y,x,i)$ such that ϕ represents the function $(x,i) \mapsto x^i$.*

Proof. Consider the $\mathcal{L}_{\mathrm{arith}}$-formula

$$\begin{aligned}\phi(y,x,i) := \exists\vec{a}(\beta(\vec{a},1) = 1 \wedge \beta(\vec{a},i+1) = y \\ \wedge \forall k(1 < k \leq i+1 \to \beta(\vec{a},k) = x \cdot \beta(\vec{a},k-1)))\end{aligned}$$

It is clear that ϕ represents $(x,i) \mapsto x^i$. □

We are now able to represent the order at a prime.

Corollary 3.9.5. *There exists an $\mathcal{L}_{\text{arith}}$-formula $\phi(n, x; p)$ such that ϕ represents the function* $\text{ord}_p : \mathbb{N} \to \mathbb{N}$.

Proof. Using Corollary 3.9.4, we may consider the $\mathcal{L}_{\text{arith}}$-formula

$$\phi(y, x; p) := p^n \mid x \wedge p^{n+1} \nmid x.$$

It is clear that ϕ represents ord_p. □

Undefinability of natural numbers. In this paragraph we will establish a result which shows that the theory of the natural numbers has self reference. This is done via Gödel numbering.

Lemma 3.9.6 (Diagonal lemma)**.** *Let $\ulcorner \cdot \urcorner$ be a Gödel numbering of the language $\mathcal{L}_{\text{arith}}$ of arithmetic. For every $\mathcal{L}_{\text{arith}}$-formula $\phi(x)$ with one free variable x there exists an $\mathcal{L}_{\text{arith}}$-sentence ψ such that*

$$\mathbb{N} \models \psi \leftrightarrow \phi(\ulcorner \psi \urcorner)$$

Proof. Let $\Delta : \mathbb{N} \to \mathbb{N}$ be the partial mapping defined by $\ulcorner \theta \urcorner \mapsto \ulcorner \theta(\ulcorner \theta \urcorner) \urcorner$ for all $\mathcal{L}_{\text{arith}}$-formulas $\theta(x)$ with at most one free variable x. This mapping is well-defined and computable by Definition 3.5.2 and is called the *diagonalization mapping*. In fact, this map corresponds under the Gödel numbering by the substitution $\theta \mapsto \theta[\ulcorner \theta \urcorner / x]$. By Theorem 3.9.1 we conclude that Δ is $\mathcal{L}_{\text{arith}}$-definable: there exists an $\mathcal{L}_{\text{arith}}$-formula $\delta(z, y)$ such that

$$\mathbb{N} \models \forall y(\delta(\ulcorner \theta \urcorner, y) \leftrightarrow y = \ulcorner \theta(\ulcorner \theta \urcorner) \urcorner)$$

Let $\beta(z)$ be the formula defined by $\beta(z) := \forall y(\delta(z, y) \to \phi(y))$. Then by substitution of $\ulcorner \beta \urcorner$ we have

$$\mathbb{N} \models \beta(\ulcorner \beta \urcorner) \leftrightarrow \forall y(\delta(\ulcorner \beta \urcorner, y) \to \phi(y)).$$

Using the definition of δ gives

$$\mathbb{N} \models \beta(\ulcorner \beta \urcorner) \leftrightarrow \forall y(y = \ulcorner \beta(\ulcorner \beta \urcorner) \urcorner \to \phi(y))$$

Hence we conclude by substitution of $y = \ulcorner \beta(\ulcorner \beta \urcorner) \urcorner$ that

$$\mathbb{N} \models \beta(\ulcorner \beta \urcorner) \leftrightarrow \phi(\ulcorner \beta(\ulcorner \beta \urcorner) \urcorner)$$

Now the conclusion follows for $\psi := \beta(\ulcorner \beta \urcorner)$ □

We now turn our attention to Tarski's undefinability theorem:

Theorem 3.9.7 (Tarski's undefinability theorem)**.** *Let $\ulcorner \cdot \urcorner$ be a Gödel numbering of the language $\mathcal{L}_{\text{arith}}$ of arithmetic. Then set $\ulcorner \text{Th}(\mathbb{N}) \urcorner \subseteq \mathbb{N}$ of all Gödel numbers of true $\mathcal{L}_{\text{arith}}$-sentences is not $\mathcal{L}_{\text{arith}}$-definable.*

Proof. Suppose that $\ulcorner \text{Th}(\mathbb{N}) \urcorner$ is definable by an $\mathcal{L}_{\text{arith}}$-formula $\text{True}(x)$, i.e., we have $\mathbb{N} \models \text{True}(x)$ if and only if $x \in \ulcorner \text{Th}(\mathbb{N}) \urcorner$. By the diagonal lemma there exists a formula ψ such that $\mathbb{N} \models \psi \leftrightarrow \neg\text{True}(\ulcorner \psi \urcorner)$. Now we have that $\mathbb{N} \models \psi$ if and only if $\mathbb{N} \models \neg\text{True}(\ulcorner \psi \urcorner)$. Hence by the completeness of $\text{Th}(\mathbb{N})$ we find $\mathbb{N} \models \psi$ if and only if $\mathbb{N} \not\models \text{True}(\ulcorner \psi \urcorner)$. By the definition of True we conclude $\mathbb{N} \models \psi$ if and only if $\mathbb{N} \not\models \psi$, which gives a contradiction. Therefore $\ulcorner \text{Th}(\mathbb{N}) \urcorner$ is not $\mathcal{L}_{\text{arith}}$-definable. □

Corollary 3.9.8. *The $\mathcal{L}_{\text{arith}}$-theory* $\text{Th}(\mathbb{N})$ *is not decidable.*

Proof. If we apply the theorem of Tarski to Corollary 3.9.2, the set $\ulcorner \text{Th}(\mathbb{N}) \urcorner \subseteq \mathbb{N}$ of all Gödel numbers of true $\mathcal{L}_{\text{arith}}$-sentences is not decidable. □

3.10. Interpretations

In this section we investigate the second step of in proving that the theory of a global fields is undecidable by showing how one interprets the theory of the natural numbers in this theory. We will study two types of interpretations: interpretations of theories and interpretations of models.

Interpretations of theories. The most natural way to interpret a given theory in another one is as follows:

Definition 3.10.1 (Interpretation of theories)**.** Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be languages. Let T_1 be an $\mathcal{L}_1$-theory and T_2 an $\mathcal{L}_2$-theory. An *interpretation* λ of T_1 in T_2 (notation: $\lambda : T_1 \rightsquigarrow T_2$) is a map $\lambda : \mathcal{F}^0_{\mathcal{L}_1} \to \mathcal{F}^0_{\mathcal{L}_2}$ such that for all $\mathcal{L}_1$-sentences ϕ

$$\phi \in T_1 \quad \text{if and only if} \quad \lambda(\phi) \in T_2$$

We say that T_1 is *interpretable* in T_2 if there exists an interpretation $\lambda : T_1 \rightsquigarrow T_2$. △

Let us now examine whether decidability is preserved under interpretations.

Proposition 3.10.2. *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be languages which admit a Gödel numbering $\lceil\cdot\rceil_1$ and $\lceil\cdot\rceil_2$ respectively. Let T_i be an $\mathcal{L}_i$-theory for $i = 1, 2$. Let $\lambda : T_1 \rightsquigarrow T_2$ be an interpretation such that the partial map $\lceil\phi\rceil_1 \mapsto \lceil\lambda\phi\rceil_2$ is computable. If T_2 is decidable then T_1 is decidable.*

Proof. Assume that $\lceil T_2\rceil_2 \subseteq \mathbb{N}$ is decidable. Hence, the characteristic function $\chi_2 : \mathbb{N} \to \{0, 1\}$ with $\chi_2(x) = 1$ if and only if $x \in \lceil T_2\rceil_2$ is then a computable function. If we compose χ_2 with the computable partial map $\lceil\phi\rceil_1 \mapsto \lceil\lambda\phi\rceil_2$, we conclude that the characteristic function of $\lceil T_1\rceil_1 \subseteq \mathbb{N}$ is computable, which shows that T_1 is decidable. □

If we apply Proposition 3.10.2 to Corollary 3.9.8 we find:

Corollary 3.10.3. *Let $\mathrm{Th}(\mathbb{N})$ be the theory of $\mathbb{N}$ in language of arithmetic and T be an $\mathcal{L}$-theory. If there exists an interpretation $\lambda : \mathrm{Th}(\mathbb{N}) \to T$, then T is undecidable.*

Interpretations of models. The definition of an interpretation is a rather abstract: it just uses the syntax. We will now give a connection to models. We place ourselves in the following setting: consider that we are given an $\mathcal{L}_1$-structure M_1 and an $\mathcal{L}_2$-structure M_2. We will investigate which connection between M_1 and M_2 is sufficient for the existence of an interpretation of $\mathrm{Th}(M_1)$ in $\mathrm{Th}(M_2)$. It turn out that is suffices to assume the existence of an injective map $f : M_1 \to M_2$ such that the image $f(M_1)$ is an $\mathcal{L}_2$-definable and the push forwards along f of the interpretations of the function and relation symbols of $\mathcal{L}_1$ are $\mathcal{L}_2$-representable on $f(M_1)$.

Let us first make precise what is meant by a push forward of a function.

Definition 3.10.4 (Push forward of functions)**.** Let $f : M_1 \to M_2$ be an injective map of an $\mathcal{L}_1$-structure M_1 to an $\mathcal{L}_2$-structure M_2 and let F be a k-ary function symbol of $\mathcal{L}_1$. Then the *push forward of F^{M_1} along f* is the partial function

$$f_*F^{M_1} : f(M_1) \longrightarrow f(M_1), \qquad \vec{x} \mapsto f(F^{M_1}(f^{-1}\vec{x})). \qquad \triangle$$

We can define the same for relations:

Definition 3.10.5 (Push forward of relations)**.** Let $f : M_1 \to M_2$ be an injective map of an $\mathcal{L}_1$-structure M_1 to an $\mathcal{L}_2$-structure M_2 and let R be a k-ary relation symbol of $\mathcal{L}_1$. Then the *push forward of R^{M_1} along f* is the partial relation

$$f_*R^{M_1} := f(R^{M_1}) \subseteq f(M_1)^k. \qquad \triangle$$

Notice that the push forward is well-defined as f is injective. Furthermore the function $F^{f(M_1)}$ is clearly an interpretation of F on the image $f(M_1)$.

Definition 3.10.6 (Interpretation of models)**.** Given an $\mathcal{L}_1$-structure M_1 and an $\mathcal{L}_2$-structure M_2. An *interpretation* f of M_1 in M_2 is an injective map $f : M_1 \to M_2$ such that for all function symbols F and relation symbols R in $\mathcal{L}_1$:

1) the image $f(M_1)$ is $\mathcal{L}_2$-definable in M_2;

2) the push forward $f_*F^{M_1}$ is $\mathcal{L}_2$-representable on $f(M_1)$;

3) the push forward $f_*R^{M_1}$ is $\mathcal{L}_2$-representable on $f(M_1)$.

We say that M_1 is *interpretable* in M_2 if and only if there exists an interpretation $f : M_1 \to M_2$. △

A map $\mu : \mathcal{F}_{\mathcal{L}_1} \to \mathcal{F}_{\mathcal{L}_2}$ is called *graded* if and only if $\mu\mathcal{F}^n_{\mathcal{L}_1} \subseteq \mathcal{F}^n_{\mathcal{L}_2}$, for all $n \in \mathbb{N}$. Now the following theorem shows that an interpretation of models induces an interpretation of theories.

Theorem 3.10.7. *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be languages. Let $f : M_1 \to M_2$ be an interpretation of an $\mathcal{L}_1$-structure M_1 in an $\mathcal{L}_2$-structure M_2. Then there exists a graded map $\mu : \mathcal{F}_{\mathcal{L}_1} \to \mathcal{F}_{\mathcal{L}_2}$ such that for all $n \in \mathbb{N}$ and for all $\phi \in \mathcal{F}^n_{\mathcal{L}_1}$ and all $\vec{m} \in M_1^n$*

$$M_1 \models \phi(\vec{m}) \quad \textit{if and only if} \quad M_2 \models (\mu\phi)(f\vec{m})$$

Moreover there exists an interpretation $\lambda : \mathrm{Th}(M_1) \rightsquigarrow \mathrm{Th}(M_2)$.

Proof. We construct by induction on the formulas a graded map $\mu : \mathcal{F}_{\mathcal{L}_1} \to \mathcal{F}_{\mathcal{L}_2}$. As a preliminary result, we show that the $\mathcal{L}_1$-terms are $\mathcal{L}_2$-definable. To be more precise, we construct for all $\mathcal{L}_1$-terms $t(x_1, \ldots, x_\ell)$ an $\mathcal{L}_2$-formula $\chi_t(x_0, \vec{x})$ with the following condition: for all $m_0 \in M_1$ and $\vec{m} \in M_1^\ell$ we have

$$m_0 = t(\vec{m}) \quad \text{if and only if} \quad M_2 \models \chi_t(fm_0, f\vec{m}). \tag{3.1}$$

Here $(fm_0, f\vec{m})$ is shorthand for $(f(m_0), f(m_1), \ldots, f(m_\ell))$. We now construct the $\mathcal{L}_2$-formula $\chi_t(y, \vec{x})$ is constructed by induction on the number of function symbols occurring in $t(\vec{x})$. Let $t(\vec{x})$ be a $\mathcal{L}_1$-term and N the number of function symbols occurring in t.

($N = 0$): Suppose $t(\vec{x})$ does not contain a function symbol. Then $t(\vec{x})$ is a variable x_i for some i. Now define $\chi_t(y, \vec{x})$ by $y = x_i$. It is clear that χ_t satisfies (3.1).

($N \implies N + 1$): Suppose $t(\vec{x})$ contains $N + 1$ function symbols and assume that $\chi_t(y, \vec{x})$ is constructed whenever $t(\vec{x})$ contains at most N function symbols. Since $N + 1 \neq 0$, we find using Definition 3.1.5 that $t(\vec{x})$ equals $F(t_1, \ldots, t_k)$ where $k \geq 0$, F is a k-ary function symbol of $\mathcal{L}_1$ and $t_i(\vec{x})$ us ab $\mathcal{L}_1$-term for all i. By the hypotheses $\chi_{t_i}(y_i, \vec{x})$ is defined for all i, since $t_i(\vec{x})$ has at most N function symbols occurring in it. Hence we may define

$$\chi_t(y, \vec{x}) := \exists \vec{y} \left(\phi_F(y, \vec{y}) \wedge \bigwedge_{i=1}^{k} \chi(y_i) \wedge \chi_{t_i}(y_i, \vec{x}) \right),$$

where $\chi(x)$ is a $\mathcal{L}_2$-formula that defines the inclusion $f(M_1) \subset M_2$ and $\phi_F(y, \vec{y})$ represents $F^{f(M_1)}$: the push forward along f of the interpretation F^{M_1} of F in M_1. Notice that for $k = 0$, $\chi_t(y, \vec{x})$ reduces to just $\phi_F(y)$ which defines the constant $f(t)$ in $f(M_1)$. It is clear that χ_t satisfies (3.1). We conclude that for all $\mathcal{L}_1$-terms $t(\vec{x})$ there exists an $\mathcal{L}_2$-formula $\chi_t(y, \vec{x})$ such that (3.1) holds.

Now we are ready to define μ. Let ϕ be an $\mathcal{L}_1$-formula and N denote the number of occurrences of $\exists$, $\neg$ and $\vee$.

($N = 0$): Suppose ϕ does not contain $\exists$, $\neg$ and $\vee$. Then ϕ equals $R(t_1, \ldots, t_k)$, $k \geq 0$, where $t_1, \ldots, t_k$ are $\mathcal{L}$-terms and R is a k-ary relation symbol of $\mathcal{L}$. Define $\lambda\phi$ to be the $\mathcal{L}_2$-formula

$$\chi_t(y, \vec{x}) := \exists \vec{y} \left(\phi_R(\vec{y}) \wedge \bigwedge_{i=1}^{k} \chi(y_i) \wedge \chi_{t_i}(y_i, \vec{x}) \right),$$

where $\phi_R(\vec{y})$ represents the k-ary relation symbol R of $\mathcal{L}_1$.

($N \implies N + 1$): Suppose ϕ contains $N + 1$ occurrences of $\exists$, $\neg$ and $\vee$. Since $N + 1 \neq 0$, we find using Definition 3.1.7 that ϕ equals either $\psi_0 \vee \psi_1$, $\neg\psi$ or $\exists x\psi$ for some $\mathcal{L}_1$-formulas ψ, ψ_0 and ψ_1. We define $\mu\phi$ to be $\mu(\psi_0) \vee \mu(\psi_1)$, $\neg\mu(\psi)$ and $\exists x(\chi(x) \wedge \mu(\psi))$ respectively, where χ defines the image of f.

We now constructed μ by induction on the formulas. It is clear that μ satisfies the conditions in the theorem.

If we restrict the graded map μ to a map $\lambda : \mathcal{F}^0_{\mathcal{L}_1} \to \mathcal{F}^0_{\mathcal{L}_2}$, we find an interpretation of $\mathrm{Th}(M_1) \rightsquigarrow \mathrm{Th}(M_2)$. □

If we apply Theorem 3.10.7 to the theory $\mathrm{Th}(\mathbb{N})$ we find, using Corollary 3.9.8, that:

Corollary 3.10.8. *Let $\mathbb{N}$ be the structure of the natural numbers in language of arithmetic and K be a ring. If there exists an interpretation $f : \mathbb{N} \to K$ then the theory $\mathrm{Th}(K)$ in the language of rings is undecidable.*

Chapter 4

Algebraically Closed Fields

A field K is called *algebraically closed* precisely whenever every algebraic extension L/K is trivial. In this chapter we will study the family of countable algebraically closed fields E_{cacf} in order to answer the three questions from the introduction, which were reformulated in section 3.7. We restrict ourselves to algebraically closed fields which are countable, since then E_{cacf} is a set and the transcendence degree over the prime subfield is at most countably infinite. This will be used to completely describe the family E_{cacf}.

It turns out that the questions about E_{cacf} are rather easy, when one knows that the theory of an algebraically closed field admits quantifier elimination. This will be shown in the first section. In the second section, we will then answer the three questions from the introduction.

4.1. Quantifier elimination

An important tool in the study of algebraically closed fields is quantifier elimination. In view of Definition 3.2.13 we define the following:

Definition 4.1.1 (Quantifier elimination)**.** A theory T in a language $\mathcal{L}$ admits *quantifier elimination* if and only if every $\mathcal{L}$-formula is T-equivalent to a quantifier-free $\mathcal{L}$-formula. △

Example 4.1.2. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\phi(\vec{x}) := \exists \vec{y}(x_1y_1 + x_2y_3 = 1 \wedge x_1y_2 + x_2y_4 = 0 \wedge x_3y_1 + x_4y_3 = 0 \wedge x_3y_2 + x_4y_4 = 1)$$

Then $\phi(\vec{x})$ asserts that the matrix $\left(\begin{smallmatrix} x_1 & x_2 \\ x_3 & x_4 \end{smallmatrix}\right)$ is invertible. Hence the determinant test shows that ϕ is T_{field}-equivalent to a quantifier-free formula

$$T_{\text{field}} \models \forall \vec{x}(\phi \leftrightarrow x_1x_4 - x_2x_3 \neq 0). \qquad \Diamond$$

To prove that a theory admits quantifier elimination we have to show something about a general $\mathcal{L}$-formula. Recall that an $\mathcal{L}$-formula λ is a literal if and only if $\lambda = \alpha$ or $\lambda = \neg\alpha$, where α is an atomic $\mathcal{L}$-formula. The next theorem reduces the complexity of formulas we have to check.

Theorem 4.1.3. *Let $\mathcal{L}$ be a language, T an $\mathcal{L}$-theory. Then the following are equivalent:*

1) *T admits quantifier elimination.*

2) *$\exists x(\bigwedge_{i=1}^{n} \lambda_i)$ is T-equivalent to a quantifier-free $\mathcal{L}$-formula, for all integers $n \geq 1$ and all $\mathcal{L}$-literals λ_i.*

Proof. 1) ⇒ 2). Trivial.

2) ⇒ 1). We show that T admits quantifier elimination with induction on formulas. Let ϕ be an $\mathcal{L}$-formula. If ϕ equals $R(t_1, \ldots, t_k)$, $\psi_0 \vee \psi_1$ or $\neg\psi$, then ϕ is quantifier-free by the induction hypothesis. If ϕ equals $\exists x\psi$, then using the induction hypothesis we find a quantifier-free $\mathcal{L}$-formula θ which is T-equivalent to ψ. Using the disjunctive normal form (Theorem 3.2.14) we find $\mathcal{L}$-literals λ_{ij} such that $\bigvee_{j=1}^{m} \bigwedge_{i=1}^{n} \lambda_{ij}$ is equivalent to θ. Hence ϕ is equivalent to $\exists x \bigvee_{j=1}^{m} \bigwedge_{i=1}^{n} \lambda_{ij}$

or equivalently $\bigvee_{j=1}^{m} \exists x \bigwedge_{i=1}^{n} \lambda_{ij}$. Using the assumption we see that $\exists x \bigwedge_{i=1}^{n} \lambda_{ij}$ is equivalent to a quantifier free $\mathcal{L}$-formula ψ_j, for all j. We find that ϕ is T-equivalent to $\bigvee_{j=1}^{m} \psi_j$, which is quantifier-free. We conclude that every $\mathcal{L}$-formula ϕ is T-equivalent to a quantifier-free $\mathcal{L}$-formula. □

Although we simplified the complexity of the formula which we want to free from quantifiers, this is still not at all easy to accomplish. However the following theorem will give an equivalent condition for a formula to be T-equivalent to a quantifier-free formula. Before we continue to that theorem, let us prove a clever standard trick to get rid of the universal quantifier in the definition of quantifier elimination.

Lemma 4.1.4. *Let T be a theory in a language $\mathcal{L}$, let ϕ be an $\mathcal{L}$-formula with free variables $x_1, \ldots, x_k$, for some $k \geq 0$, and let $c_1, \ldots, c_k$ be constant symbols of $\mathcal{L}$. If no c_i occurs in T or ϕ, then*

$$T \models \forall \vec{x} \phi(\vec{x}) \quad \text{if and only if} \quad T \models \phi(\vec{c}).$$

Proof. If $T \models \forall \vec{x} \phi(\vec{x})$ then trivially $T \models \phi(\vec{c})$. On the other hand, suppose that $T \models \phi(\vec{c})$. Define $\mathcal{L}'$ to be the language $\mathcal{L}$ without the c_i. We will show that $T \models \forall \vec{x} \phi(\vec{x})$. In other words, we show that for every $\mathcal{L}$-structure M with $M \models T$ we have $M \models \forall \vec{x} \phi(\vec{x})$. Notice that, since no c_i occurs in T or ϕ, it suffices to show that for every $\mathcal{L}'$-structure N with $N \models T$ we have $N \models \forall \vec{x} \phi(\vec{x})$. Hence let N be an $\mathcal{L}'$-structure and $\vec{n} \in N^k$. Then expand N to an $\mathcal{L}$-structure M by defining $c_i^M = n_i$ for $1 \leq i \leq k$. Then we still have that $M \models T$ and from the assumption $T \models \phi(\vec{c})$ we see that $M \models \phi(\vec{n})$. Hence we conclude that $T \models \forall \vec{x} \phi(\vec{x})$, which proves the lemma. □

The following theorem gives a model-theoretic interpretation of being equivalent to a quantifier-free formula.

Theorem 4.1.5. *Let T a theory in a language $\mathcal{L}$ and ϕ an $\mathcal{L}$-formula with free variables $x_1, \ldots, x_k$, for some $k \geq 0$. Then the following are equivalent:*

1) *ϕ is T-equivalent to a quantifier-free $\mathcal{L}$-formula.*

2) *If M and N are models of T and A is an $\mathcal{L}$-structure contained in $M \cap N$ then for all $\vec{a} \in A^k$ we have that $M \models \phi(\vec{a})$ whenever $N \models \phi(\vec{a})$.*

Proof. 1) ⇒ 2). Let M and N be models of T and A an $\mathcal{L}$-structure contained in $M \cap N$. Suppose that there exists a quantifier-free $\mathcal{L}$-formula $\psi(\vec{x})$ which is T-equivalent to ϕ. Then $M, N \models \phi(\vec{a})$ if and only if $M, N \models \psi(\vec{a})$ for all $\vec{a} \in A^n$. Applying Theorem 3.2.10 to the inclusions $A \to M$ and $A \to N$, we find that $M, N \models \psi(\vec{a})$ if and only if $A \models \psi(\vec{a})$, which proves the second statement.

2) ⇒ 1). Suppose that for every model M and N of T and every $\mathcal{L}$-structure $A \subseteq M \cap N$ we have $M \models \phi(\vec{a})$ if and only if $N \models \phi(\vec{a})$ for all $\vec{a} \in A^k$. Let $c_1, \ldots, c_k$ be constant symbols which do not occur in $\mathcal{L}$, and consider the language $\mathcal{L}_c = \mathcal{L} \cup \{c_1, \ldots, c_k\}$. We will show that there is a quantifier-free $\mathcal{L}$-formula $\psi(\vec{x})$ such that $T \models \forall \vec{x}(\phi \leftrightarrow \psi)$, i.e., for all $\mathcal{L}$-structures M with $M \models T$ we have $M \models \forall \vec{x}(\phi \leftrightarrow \psi)$.

Notice that the map $\psi(\vec{x}) \to \psi(\vec{c})$ from the set of quantifier-free $\mathcal{L}$-formulas with free variables among $x_1, \ldots, x_k$ to the set of quantifier-free $\mathcal{L}_c$-formulas is a bijection, because it is invertible. Using this and Lemma 4.1.4 it suffices to show that there is a quantifier-free $\mathcal{L}_c$-sentence ψ such that for all $\mathcal{L}_c$-structures M with $M \models T$ we have $M \models \phi(\vec{c}) \leftrightarrow \psi$. In other words, it suffices to show that there is a quantifier-free $\mathcal{L}_c$-sentence ψ such that $T \models \phi(\vec{c}) \leftrightarrow \psi$.

Now let Γ be the set of all quantifier-free $\mathcal{L}_c$-formulas ψ with $T \models \phi(\vec{c}) \to \psi$. Thus Γ is the set of all quantifier-free consequences of $\phi(\vec{c})$. We claim that $T \cup \Gamma \models \phi(\vec{c})$. The compactness theorem then shows that there are $\psi_1, \ldots, \psi_n \in \Gamma$ with $T \models \bigwedge_{i=1}^{n} \psi_i \to \phi(\vec{c})$, and by construction of Γ we also have $T \models \phi(\vec{c}) \to \bigwedge_{i=1}^{n} \psi_i$. Thus $\psi := \bigwedge_{i=1}^{n} \psi_i$ is a quantifier-free $\mathcal{L}_c$-sentence such that $T \models \phi(\vec{c}) \leftrightarrow \psi$. We conclude that ϕ is T-equivalent to the quantifier-free $\mathcal{L}$-formula corresponding with the $\mathcal{L}_c$-sentence ψ.

It remains to prove the claim: $T \cup \Gamma \models \phi(\vec{c})$. Suppose that the claim is false. Let M be an $\mathcal{L}_c$-structure such that $M \models T \cup \Gamma \cup \{\neg\phi(\vec{c})\}$. Let A be the *prime $\mathcal{L}_c$-substructure of M*: $A := \{t^M \mid t \text{ is an } \mathcal{L}_c\text{-term}\}$.

Let $n \geq 0$ and let $\theta_1, \ldots, \theta_n \in \text{diag}(A)$ be be arbitrary. Then the construction of A shows that each $\mathcal{L}_A$-sentence θ_i is equivalent to an $\mathcal{L}_c$-sentence $\hat{\theta}_i$. If $T \cup \{\hat{\theta}_1, \ldots, \hat{\theta}_n\} \cup \{\phi(\vec{c})\}$ is inconsistent, then $T \models \phi(\vec{c}) \to \neg \bigwedge_{i=1}^n \hat{\theta}_i$. Thus $\neg \bigwedge_{i=1}^n \hat{\theta}_i$ is an element of Γ, which implies that $M \models \neg \bigwedge_{i=1}^n \hat{\theta}_i$. But this contradicts the fact that $M \models \hat{\theta}_i$ for all i, because $\theta_i \in \text{diag}(A)$ and $A \subseteq M$. The compactness theorem shows that there exists an $\mathcal{L}_c$-structure with $N \models T \cup \text{diag}(A) \cup \{\phi(\vec{c})\}$.

Now M, N and A violate the assumption, since $M \models \neg\phi(\vec{a})$ and $N \models \phi(\vec{a})$ for $\vec{a} := \vec{c}^M = \vec{c}^N \in A^k$. This contradiction proves the claim. □

4.2. Richness of algebraically closed fields

In this section we will provide an answer to the questions from section 3.7 for E equal to the set of isomorphism classes of countable algebraically closed fields E_{cacf}.

We start with the definition of an algebraically closed field:

Definition 4.2.1 (Algebraically closed fields)**.** A field K is called *algebraically closed* if and only if every algebraic extension L/K is trivial. △

Now let E_{cacf} denote the set of isomorphism classes of countable algebraically closed fields.

The following theorem provides a classification of the isomorphism classes in E_{cacf}.

Theorem 4.2.2. *Let K and L be countable algebraically closed fields. Then K and L are isomorphic if and only if* $\text{char}(K) = \text{char}(L)$ *and* $\text{trdeg}(K) = \text{trdeg}(L)$.

Proof. If K and L are isomorphic then clearly $\text{char}(K) = \text{char}(L)$ and $\text{trdeg}(K) = \text{trdeg}(L)$. Suppose that $\text{char}(K) = \text{char}(L)$ and $\text{trdeg}(K) = t = \text{trdeg}(L)$ and let K_0 and L_0 be the prime subfield of K and L respectively. Then K_0 and L_0 are isomorphic, because $\text{char}(K) = \text{char}(L)$. Hence we find an isomorphism $f_0 : K_0 \to L_0$. Let $X = \{x_i \mid 0 \leq i < t\}$ and $Y = \{y_i \mid 0 \leq i < t\}$ be trancendence bases of K/K_0 and L/L_0 (note that t may be infinite). Define $K_1 = K_0(X)$ and $L_1 = L_0(Y)$. Clearly f_0 can be extended to an isomorphism $f_1 : K_1 \to L_1$, by declaring $f_1(x_i) = y_i$, for all $0 \leq i < t$. We will now construct the following diagram

$$\begin{array}{ccccccc} K_0 & \longrightarrow & K_1 & \longrightarrow & K_2 & \cdots\cdots\cdots\cdots\cdots\cdots & K \\ \Big\downarrow{\scriptstyle f_0} & & \Big\downarrow{\scriptstyle f_1} & & \Big\downarrow{\scriptstyle f_2} & & \Big\downarrow{\scriptstyle f} \\ L_0 & \longrightarrow & L_1 & \longrightarrow & L_2 & \cdots\cdots\cdots\cdots\cdots\cdots & L \end{array}$$

where the horizontal maps are inclusions and all vertical maps are isomorphisms.

Let $k_2, k_3, \ldots$ be an enumeration of K, which is possible since K is countable. Define $K_n = K_{n-1}(k_n)$ for all integers $n \geq 2$. Furthermore define $L_n = L_{n-1}(l_n)$ for all integers $n \geq 2$, where l_n is chosen as follows: Notice that k_n is algebraic over K_{n-1}, since $X \cup \{k_n\}$ is algebraically dependent. Let $\sum_{i=1}^d a_i T^i$ be the minimal polynomial of k_n over K_{n-1}. Then choose l_n to be a root in K of the polynomial $\sum_{i=1}^d f_{n-1}(a_i) T^i$, which is irreducible over K_{n-1}, since $f_{n-1} : K_{n-1} \to L_{n-1}$ is an isomorphism. Note that this is possible, since L is algebraically closed.

Now define $f_n(k_n) = l_n$. Notice that $f_n : K_{n-1}(k_n) \to L_n$ is completely determined by the value of $f_n(k_n)$. Indeed $1, k_n, \ldots, k_n^{d-1}$ is a basis of K_n over K_{n-1}, where d is the degree of the minimal polynomial of k_n.

We inductively defined f_n for all $n \in \mathbb{N}$. Now, let f be the union of all f_n (formally, f is the union of all graphs $f_n \subseteq K \times L$). Then f is an injective ring homomorphism from K to L, since all f_n are injective ring homomorphisms. Furthermore note that $f(K)$ is algebraically closed, since K is algebraically closed and f is injective. Hence $L/f(K)$ is either trivial, or transcendental. Now $L/f(K)$ is not transcendental, since this implies an extension of the trancendence basis Y of

L/L_0. Hence $L/f(K)$ is trivial, which means that f is surjective and hence an isomorphism.

We conclude that K and L are isomorphic. □

Decidability of $\mathrm{Th}(K)$**.** We will now provide an answer to the first question from in introduction: is $\mathrm{Th}(K)$ decidable, where K is an algebraically closed field. We will apply Theorem 3.6.11 to find an answer.

First notice that $\mathrm{Th}(K)$ is complete, for every $\mathcal{L}_{\mathrm{ring}}$-structure K. Hence it suffices to find an axiomatization A of $\mathrm{Th}(K)$ for every algebraically closed field K. Recall that $A \subseteq \mathrm{Th}(K)$ is called an axiomatization if and only if A is decidable and $A \models \mathrm{Th}(K)$. The difficult task is to prove that $A \models \mathrm{Th}(K)$. In other words: $A \models \phi$ for all $\phi \in \mathrm{Th}(K)$.

Notice that for all $n \geq 2$ we have that $\phi_n \in \mathrm{Th}(K)$, where

$$\phi_n := \forall a_0 \cdots \forall a_n((a_n \neq 0 \vee \cdots \vee a_1 \neq 0 \vee a_0 = 0) \leftrightarrow \exists x(a_n x^n + \cdots + a_0 = 0)).$$

Furthermore we have either $p = 0 \in \mathrm{Th}(K)$ or $p \neq 0 \in \mathrm{Th}(K)$, for all primes p. It turns out that these $\mathcal{L}_{\mathrm{ring}}$-sentences completely determine $\mathrm{Th}(K)$.

Let T_{acf} be the *theory of algebraically closed fields* is the theory of rings T_{field} together with the axiom ϕ_n for all integers $n \geq 2$. It is easy (but tedious) to prove that T_{acf} is decidable. Using the Theorems from the previous section, we are able to show that T_{acf} admits quantifier elimination.

Theorem 4.2.3. *The $\mathcal{L}_{\mathrm{ring}}$-theory T_{acf} admits quantifier elimination.*

Proof. With induction on formulas, one can show that every atomic $\mathcal{L}_{\mathrm{ring}}$-formula free variables among $x_1, \ldots, x_k$ is T_{ring}-equivalent to an atomic $\mathcal{L}_{\mathrm{ring}}$-formula of the form

$$\sum c_{i_1,\ldots,i_k} x_1^{i_1} \cdots x_k^{i_k} = 0$$

with $c_{i_1,\ldots,i_k} := \pm(1 + \cdots + 1)$ and $x_j^{i_j} := x_j \cdots x_j$. Hence every $\mathcal{L}_{\mathrm{ring}}$-literal is T_{ring}-equivalent to an $\mathcal{L}_{\mathrm{ring}}$-literal of the form $P = 0$ or $P \neq 0$ for some $P \in \mathbb{Z}[x_1, \ldots, x_k]$. Now notice that $\bigwedge_{i=1}^n P_i \neq 0$ is T_{field}-equivalent to $P_1 \cdots P_n \neq 0$. Hence, Theorem 4.1.3 shows that it suffices to show that

$$\phi := \exists x(P_0 \neq 0 \wedge P_1 = 0 \wedge \cdots \wedge P_n = 0)$$

is T_{acf}-equivalent to a quantifier free $\mathcal{L}_{\mathrm{ring}}$-formula, where each P_i has free variables among $x_1, \ldots, x_k$. Without loss of generality we may assume that $x_1 = x$.

We will apply Theorem 4.1.5. Let K and L be algebraically closed fields, let R be a subring of $K \cap L$, let $\vec{a} \in R^k$ and suppose that $L \models \phi(\vec{a})$.

If $n = 0$, then ϕ says that $P_0(\vec{a}, x) \in R[X]$ is not identically zero. Thus not all coefficients of $P_0(\vec{a}, x)$ are zero in R. Hence $P_0(\vec{a}, x)$ has only finitely many zeros in $K \supseteq R$, Since K is infinite (no finite field is algebraically closed) we conclude that $K \models \exists x P_0(\vec{a}, x)$.

If $n > 0$, then there exists an $b \in L$ with $L \models P_0(\vec{a}, b) \neq 0$ and $L \models P_i(\vec{a}, b) = 0$ for all $0 < i \leq n$. Then b is algebraic over R and since the algebraic closure embeds into K, we find some $c \in K$ with $K \models P_0(\vec{a}, c) \neq 0$ and $K \models P_i(\vec{a}, c) = 0$ for all $0 < i \leq n$.

Now Theorem 4.1.5 applies and we conclude that T_{acf} admits quantifier elimination. □

Let us expand T_{acf} a little more. For each $p \in \mathbb{N}$, which is either prime or zero, define the theory

$$T_{\mathrm{acf}}^p := \begin{cases} T_{\mathrm{acf}} \cup \{p = 0\} & \text{if } p > 0 \\ T_{\mathrm{acf}} \cup \{q \neq 0 \mid q \text{ prime}\} & \text{if } p = 0 \end{cases}$$

It is easy (but tedious) to prove that T_{acf}^p is decidable. Moreover, T_{acf}^p is a complete theory.

Corollary 4.2.4. *Let ϕ be an $\mathcal{L}_{\mathrm{ring}}$-sentence and let $p \geq 0$ be either zero or prime. Then ϕ is T_{acf}-equivalent to an $\mathcal{L}_{\mathrm{ring}}$-sentence of the form $\bigvee_{i=1}^n t_i = 0$ or $\neg \bigvee_{i=1}^n t_i = 0$, with $t_i = 1 + \cdots + 1$ for all i. Thus we have either $T_{\mathrm{acf}}^p \models \phi$ or $T_{\mathrm{acf}}^p \models \neg\phi$.*

Proof. Let ϕ be an $\mathcal{L}_{\text{ring}}$-sentence. Since T_{acf} admits quantifier elimination, we find a T_{acf}-equivalent quantifier-free $\mathcal{L}_{\text{ring}}$-formula ψ. Using the disjunctive normal form we find λ_{ij} such that ϕ is T_{acf}-equivalent to $\bigvee_i \bigwedge_j \lambda_{ij}$. Now notice that λ_{ij} is $\mathcal{L}_{\text{ring}}$-equivalent to either $t_{ij} = 0$ or $t_{ij} \neq 0$ for some closed $\mathcal{L}_{\text{ring}}$-term t_{ij} (i.e., $t_{ij} = 1 + \cdots + 1$). Let $\mu_{ij}(t)$ be either $t_{ij} = t$ or $t_{ij} \neq t$, depending on λ_{ij}. Then the set $S_i := \{t \in \mathbb{N} \mid \bigwedge_j \mu_{ij}(t)\}$ is either finite or cofinite. Hence

$$S := \{t \in \mathbb{N} \mid \bigvee_i \bigwedge_j \mu_{ij}(t)\} = \bigcup_i S_i$$

is also either finite or cofinite. Hence we find closed $\mathcal{L}_{\text{ring}}$-terms $t_1, \ldots, t_n$ such that $S = \{t \in \mathbb{N} \mid \bigvee_{i=1}^n t_i = 0\}$ or $S = \{t \in \mathbb{N} \mid \neg \bigvee_{i=1}^n t_i = 0\}$. This shows that ϕ is T_{acf}-equivalent to an $\mathcal{L}_{\text{ring}}$-sentence of the form $\bigvee_{i=1}^n t_i = 0$ or $\neg \bigvee_{i=1}^n t_i = 0$.

The second part of the corollary follows immediately. □

From this corollary we know that T_{acf}^p is a complete axiomatization of $\text{Th}(K)$. If we apply Theorem 3.6.11, we find a positive answer to the Question 1:

Theorem 4.2.5. *The theory* $\text{Th}(e)$ *is decidable for every* $e \in E_{\text{cacf}}$.

Definable subsets of E_{cacf}. We will now turn our attention to the description of all definable subsets of E_{cacf}. The following theorem provides an answer to the Question 2, as it completely describes the definable subsets of E_{cacf}.

Theorem 4.2.6. *Let* $S \subseteq E_{\text{cacf}}$ *be a subset. Then* S *is definable if and only if there exists primes* $p_1, \ldots, p_n$ *in* $\mathbb{N}$*, such that* S *or* $E_{\text{cacf}} - S$ *equals* $\{[K] \in E_{\text{cacf}} \mid \text{char}(K) = p_i$ *for some* $i\}$.

Proof. Let $S \subseteq E_{\text{cacf}}$ be a definable subfamily and ϕ be the defining formula of S. Then by Corollary 4.2.4 we find closed $\mathcal{L}_{\text{ring}}$-terms t_i such that ϕ is T_{acf}-equivalent to $\bigvee_{i=1}^n t_i = 0$ or $\neg \bigvee_{i=1}^n t_i = 0$. Notice that the closed $\mathcal{L}_{\text{ring}}$-terms correspond with the natural numbers and that the $\mathcal{L}_{\text{ring}}$-sentence $m \cdot n = 0$ is T_{field}-equivalent to $m = 0 \vee n = 0$. This implies that t_i we may assume without loss of generality that the t_i correspond with prime numbers. This proves the theorem. □

From Theorem 4.2.6 we see that Question 3 has a negative answer:

Corollary 4.2.7. *There is no* $\mathcal{L}_{\text{ring}}$*-sentence* ϕ *such that* $K \models \phi$ *if and only if* $\text{char}(K) = 0$ *for all algebraically closed fields* K.

Theorem 4.2.6 also shows that the transcendence degree is not definable. Moreover, no isomorphism class in E_{cacf} can be defined.

Corollary 4.2.8. *There is no* $\mathcal{L}_{\text{ring}}$*-sentence* ϕ_n *such that* $K \models \phi_n$ *if and only if* $\text{trdeg}(K) = n$ *for all algebraically closed fields* K.

Proof. Suppose that ϕ_n exists. Let K be an algebraically closed field with $K \models \phi_n$. Consider $L = \overline{K(X)}$, i.e., L is the algebraic closure of the quotient field of the polynomial ring over K. Then $\text{trdeg}(L) = n + 1$ and $\phi_n \not\models L$. Moreover we have $\text{char}(L) = \text{char}(K)$. Hence Theorem 4.2.6 implies that $\phi_n \in \text{Th}(K) = \text{Th}(L)$, which gives a contradiction. □

If we restrict ourselves to some fixed transcendence degree, then almost all isomorphism classes are definable, except for characteristic zero. But it is clear that the theory of characteristic zero is distinct from the theory of positive characteristic. Hence isomorphism classes are determined by its theory.

Chapter 5

Global Fields

In this chapter we will study the isomorphism classes of global fields E_{gf} by answering the questions from section 3.7.

In order to answer Question 1, we will apply the results from the final sections of Chapter 3 and show how to interpret the theory of natural numbers inside the theory $\text{Th}(K)$ of a global field K. We will follow [14] and define an interpretation $I : \mathbb{N} \to K$, which implies a negative answer to the first question.

Then we focus on the Question 2 and 3. We will show that the definable subsets of E_{gf} are in one-to-one correspondence with the $\mathcal{L}_{\text{arith}}$-definable subsets of $\mathbb{N}$. This will imply a positive answer to Question 3.

The structure of this chapter is as follows. From section 5.1 up to section 5.5 we will prove that there exists an interpretation $I : \mathbb{N} \to K$. It is quite easy to define such a map, but it is a bit harder to show that the image is an $\mathcal{L}_{\text{arith}}$-structure with $\mathcal{L}_{\text{ring}}$-representable functions and relations. We will deal with this in section 5.5. By far the hardest part is to show that the image is $\mathcal{L}_{\text{ring}}$-definable. We will prove this by showing in section 5.1 and 5.2 that the valuation domains $\mathcal{O}_{\mathfrak{p}}$, with $\mathfrak{p}$ finite place, are $\mathcal{L}_{\text{ring}}$-definable. Then, using Proposition 1.9.4, we will derive in section 5.3 that the ring of integers $\mathcal{O}_K$ is an $\mathcal{L}_{\text{ring}}$-definable subset. This will allow us to introduce divisibility in $\mathcal{O}_K$, which will be used in section 5.4 to show that the family of all finite subsets is $\mathcal{L}_{\text{ring}}$-definable. Then in section 5.5 we will see that this implies that the image of I is definable, which proves that I is an interpretation.

Then we will turn our attention to Question 2 and 3. In section 5.6 we prove that the Gödel function is $\mathcal{L}_{\text{ring}}$-representable, which enables us to make make inductive definitions. We will apply this to polynomials over the prime subfield in section 5.7, where we will give a one-to-one correspondence between $\mathbb{N}$ and the polynomials in $\mathbb{K}[X]$. This enables us to show in section 5.8 that the definable subsets of E_{gf} are in one-to-one correspondence with the $\mathcal{L}_{\text{arith}}$-definable subsets of $\mathbb{N}$.

5.1. Reduction to local norms

The first goal of this section is to show that for every global field K there is a definable family $\mathscr{F}$, which consists of almost all valuation rings $\mathcal{O}_{\mathfrak{p}}$, with $\mathfrak{p}$ an finite place K. To be more explicit, we will define $\mathcal{L}_{\text{ring}}$-formulas $\phi(x;\vec{y})$ and $\chi(\vec{y})$ with free variables x and $y_1, \ldots, y_n$, $n \geq 1$, such that $\phi(x;\vec{y})$ defines valuation ring $\mathcal{O}_{\mathfrak{p}}$ at some finite place $\mathfrak{p}$ whenever $\chi(\vec{y})$ holds. Almost all valuation rings should occur in this way.

The first step is to define an individual valuation ring $\mathcal{O}_{\mathfrak{p}}$ for some finite place $\mathfrak{p}$, by providing an $\mathcal{L}_K$-formula (the coefficients from M will eventually be replaces by parameters). In this section we will reduce the definability of $\mathcal{O}_{\mathfrak{p}}$ to finding a first-order definition of local norms.

Let ℓ be some prime number. Let $N_{\mathfrak{p}}^{\ell}$ denote the set of all non-zero elements of K such that $\text{ord}_{\mathfrak{p}}(x) \equiv 0$ modulo ℓ, i.e.

$$N_{\mathfrak{p}}^{\ell} := \{x \in K^{\times} \mid \text{ord}_{\mathfrak{p}}(x) \equiv 0 \mod \ell\}.$$

The following lemma simplifies our task of defining $\mathcal{O}_{\mathfrak{p}}$:

Lemma 5.1.1. *Let $\mathfrak{p}$ be a finite place of a global field K, $\ell \geq 2$ a prime number and $\mathcal{L}_{\text{ring}}$ the language of rings. If $N_{\mathfrak{p}}^{\ell}$ is defined by an $\mathcal{L}_{\text{ring}}$-formula $\phi(x)$, then $\mathcal{O}_{\mathfrak{p}}$ is defined by the $\mathcal{L}_{\text{ring}}$-formula*

$$\psi(x) := \exists z(\phi(z) \wedge 1 + \pi x^{\ell} = z),$$

with $\pi \in K^{\times}$ such that $\text{ord}_{\mathfrak{p}}(\pi) = 1$.

Proof. Let x be an element of K. If $x \neq 0$ then $\text{ord}_{\mathfrak{p}}(\pi x^{\ell}) = 1 + \ell \,\text{ord}_{\mathfrak{p}}(x) \equiv 1$ modulo ℓ and $\text{ord}_{\mathfrak{p}}(\pi x^{\ell}) = \infty$ whenever $x = 0$. Therefore $\text{ord}_{\mathfrak{p}}(1) = 0 \neq \text{ord}_{\mathfrak{p}}(\pi x^{\ell})$ and hence by Lemma 2.5.7 we have

$$\text{ord}_{\mathfrak{p}}(1 + \pi x^{\ell}) = \min\{0, \text{ord}_{\mathfrak{p}}(\pi x^{\ell})\} = \min\{0, 1 + \ell \,\text{ord}_{\mathfrak{p}}(x)\}.$$

We find that $\text{ord}_{\mathfrak{p}}(1 + \pi x^{\ell}) \equiv 0$ modulo ℓ if and only if $\text{ord}_{\mathfrak{p}}(x) \geq 0$.

Using the assumption on $\phi(x)$ and definition of $\psi(x)$ we find that the conditions $K \models \psi(x)$, $K \models \phi(1 + \pi x^{\ell})$ and $\text{ord}_{\mathfrak{p}}(1 + \pi x^{\ell}) \equiv 0$ modulo ℓ are equivalent. Therefore $K \models \psi(x)$ if and only if $\text{ord}_{\mathfrak{p}}(x) \geq 0$, i.e., $x \in \mathcal{O}_{\mathfrak{p}}$. □

The above lemma remains true if $\ell \geq 1$ is an integer, but we do not need this.

This lemma reduced the problem to finding an $\mathcal{L}_{\text{ring}}$-formula $\phi(x)$ that defines $N_{\mathfrak{p}}^{\ell}$. We will now apply the class field theory in order to define $N_{\mathfrak{p}}^{\ell}$. Following Rumely [14], we conclude from the second part of Theorem 2.11.4 that $N_{\mathfrak{p}}^{\ell}$ equals the intersection of K with the local norm group at $\mathfrak{p}$ of the cyclic Kummer extension $K(d^{1/\ell})$ of K, for some d and ℓ.

Theorem 5.1.2. *Let $\mathfrak{p}$ be a finite place of a global field K. Suppose that $\ell \neq \text{char}(\overline{K}_{\mathfrak{p}})$ is a prime number such that K contains the 2ℓ-th roots of unity. Let $L^d = K(d^{1/\ell})$ be an extension of K and $\mathfrak{P}$ an extension of $\mathfrak{p}$. Let $\Delta_{\mathfrak{p}}$ the set of all $d \in K$ such that L^d/K is non-trivial and unramified at $\mathfrak{p}$. Then for all $d \in \Delta_{\mathfrak{p}}$ we have that*

$$N_{\mathfrak{p}}^{\ell} = K \cap \text{N}_{L_{\mathfrak{P}}^d/K_{\mathfrak{p}}}((L_{\mathfrak{P}}^d)^{\times}).$$

Proof. This is the second item of Theorem 2.11.4. □

In view of this theorem we call $N_{\mathfrak{p}}^{\ell}$ the *local norm group* at $\mathfrak{p}$.

For general K such prime ℓ which satisfies the conditions of Theorem 5.1.2 does not exist. However the next lemma, which will be is slightly more general then needed, shows that we are able to reduce to this case. This generality is needed when we turn our attention to $\mathcal{L}_{\text{ring}}$-definable families.

Lemma 5.1.3. *Let L/K be a non-trivial finite separable extension of global fields of degree m and let*

$$\mathscr{F}_L \subseteq \{\mathcal{O}_{\mathfrak{P}} \mid \mathfrak{P} \text{ finite place of } L\}$$

an $\mathcal{L}_{\text{ring}}$-definable family of valuation rings of L, parametrized by $\phi(x; \vec{y})$ with n parameters satisfying $\chi(\vec{y})$. Then

$$\mathscr{F}_K = \{\mathcal{O}_{\mathfrak{P}} \cap K \mid \mathcal{O}_{\mathfrak{P}} \in \mathscr{F}_L\}$$

is an $\mathcal{L}_{\text{ring}}$-definable family of valuation rings of K, parametrized by $\phi^m(x; \vec{y})$ with $m(n+1) - 1$ parameters satisfying $\chi^m(\vec{y})$.

Proof. First notice that $\mathcal{O}_{\mathfrak{P}} \cap K = \mathcal{O}_{\mathfrak{p}}$, with $\mathfrak{p} = \mathfrak{P} \cap K$, because

$$\mathcal{O}_{\mathfrak{p}} = \{x \in K \mid \text{ord}_{\mathfrak{p}}(x) \geq 0\} = \{x \in L \cap K \mid \text{ord}_{\mathfrak{P}}(x)/e(\mathfrak{P}/\mathfrak{p}) \geq 0\} = \mathcal{O}_{\mathfrak{P}} \cap K.$$

Therefore $\mathscr{F}_K$ is a family of valuation rings of K. It remains to show that $\mathscr{F}_K$ is $\mathcal{L}_{\text{ring}}$-definable, whenever $\mathscr{F}_L$ is $\mathcal{L}_{\text{ring}}$-definable. This is done via an explicit construction of ϕ^m and χ^m from ϕ and χ. Notice that by the primitive element theorem we have $L = K(\alpha)$, since L/K is a finite separable extension. The idea is to regard L as a vector space over K with basis $1, \alpha, \ldots, \alpha^{m-1}$. Then every element of L may be viewed as an m-tuple of elements of K. Replace every occurrence of a variable u in both ϕ and χ with $(u_1, \ldots, u_m)$, every occurrence of 0 with $(0, \ldots, 0)$ and every occurrence of 1 with $(1, 0, \ldots, 0)$. Then replace every substring of ϕ

of the form $(u_1, \ldots, u_m) + (v_1, \ldots, v_m)$ with $(u_1 + v_1, \ldots, u_n + v_m)$ and replace every substring of ϕ of the form $(u_1, \ldots, u_m) \times (v_1, \ldots, v_m)$ with $(w_1, \ldots, w_m)$, with $w_i = \sum_{k=0}^{i} u_k v_{i-k}$. Finally replace every substring of ϕ of the form $(u_1, \ldots, u_m) = (v_1, \ldots, v_m)$ with $(u_1 = v_1 \wedge \cdots \wedge u_m = v_m)$. Now we obtained $\mathcal{L}_{\text{ring}}$-formulas

$$\tilde{\psi}^m(x_1, \ldots, x_m; y_{11}, \ldots, y_{1m}, \ldots, y_{n1}, \ldots, y_{nm})$$
$$\tilde{\chi}^m(y_{11}, \ldots, y_{1m}, \ldots, y_{n1}, \ldots, y_{nm}).$$

Rename the variable x_1 to x, x_{i+1} to y_i for $1 \leq i < n$ and y_{ij} to y_{im+j-1} for $1 \leq i \leq n$ and $1 \leq j \leq m$. Then it is clear that $\mathscr{F}_K$ is parametrized by $\psi^m(x; \vec{y})$ with $m(n+1) - 1$ parameters satisfying

$$\chi^m(\vec{y}) := y_1 = 0 \wedge \cdots \wedge y_{m-1} = 0 \wedge \tilde{\chi}^m(y_m, \ldots, y_{m(n+1)-1}).$$

This proves the lemma. □

Let L be the extension of K obtained by adjoining the 2ℓ-th roots of unity. Then L/K is a finite separable extension, since every 2ℓ-th root of unity is separable over K. Application of Lemma 5.1.3 shows that $\mathcal{O}_\mathfrak{p}$ is $\mathcal{L}_{\text{ring}}$-definable in K whenever $\mathcal{O}_\mathfrak{P}$ is $\mathcal{L}_{\text{ring}}$-definable in L. Therefore we may assume without loss of generality that K contains the 2ℓ-th roots of unity.

Furthermore we may always choose ℓ such that $\ell \neq \text{char}(\overline{K}_\mathfrak{p})$. Indeed, either $\ell = 2$ or $\ell = 3$ will suffice. This shows that we are able to apply Theorem 5.1.2 for general K.

5.2. Construction of local norms

Let K be a global field, $\mathfrak{p}$ a finite prime of K and ℓ a prime number with $\ell \neq \text{char}(\overline{K}_\mathfrak{p})$. In this section we will prove that $N_\mathfrak{p}^\ell$ is $\mathcal{L}_{\text{ring}}$-definable. Then Lemma 5.1.1 shows that $\mathcal{O}_\mathfrak{p}$ is definable.

In view of Theorem 5.1.2, we will abbreviate $K(d^{1/\ell})$ to L^d and we will write $\Delta_\mathfrak{p}$ for the set of all $d \in K$ such that L^d/K is non-trivial and unramified at $\mathfrak{p}$. Since every global norm is a local norm, we know that

$$\text{N}_{L^d/K}((L^d)^\times) \subseteq K \cap \text{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}((L^d_\mathfrak{P})^\times) = N_\mathfrak{p}^\ell$$

Lemma 5.2.1 will show that the global norms from L^d are $\mathcal{L}_{\text{ring}}$-definable. The aim of this section is to 'construct' the local norms $N_\mathfrak{p}^\ell$ from the global norms $\text{N}_{L^d/K}(L^\times)$. If this construction is 'nice enough', then the $\mathcal{L}_{\text{ring}}$-definability of $N_\mathfrak{p}^\ell$ will follow from the $\mathcal{L}_{\text{ring}}$-definability of the global norms from L^d.

The construction will be as follows: if $D \subseteq K$ is an $\mathcal{L}_{\text{ring}}$-definable subset with $D \subseteq \Delta_\mathfrak{p}$, then it follows from Lemma 5.2.1 that

$$N_D = \bigcup_{d \in D} \text{N}_{L^d/K}((L^d)^\times)$$

is an $\mathcal{L}_{\text{ring}}$-definable subset of $N_\mathfrak{p}^\ell$. Then, using Proposition 5.2.2 and Theorem 5.2.6, we will show that there exists $\mathcal{L}_{\text{ring}}$-definable subsets $D_1, D_2 \subseteq K$ such that $D_1, D_2 \subseteq \Delta_\mathfrak{p}$ and

$$N_\mathfrak{p}^\ell = N_{D_1} N_{D_2},$$

which implies that $N_\mathfrak{p}^\ell$ is $\mathcal{L}_{\text{ring}}$-definable.

The first step is to show that, using norm forms, the global norms of L^d are $\mathcal{L}_{\text{ring}}$-definable.

Lemma 5.2.1. *There is an $\mathcal{L}_{\text{ring}}$-term $\text{N}_\ell(x; \vec{y})$ such that for every non-ℓth power d in K we have that $\exists \vec{a}(x = \text{N}_\ell(d; \vec{a}))$ defines $\text{N}_{L^d/K}((L^d)^\times)$.*

Proof. The extension L^d/K is non-trivial, because d is not an ℓ-th power. The powers of $d^{1/\ell}$ form a basis of L^d as a vector space over K. Thus the norm map $\text{N}_{L^d/K} : L^d \to K$ defines a *norm form*

$$\text{N}_\ell(d, \vec{a}) = \text{N}_{L^d/K}(a_0 + a_1 d^{1/\ell} + \cdots + a_{\ell-1} d^{(\ell-1)/\ell}).$$

Now it suffices to show that $\mathrm{N}_\ell(d,\vec{a})$ is a polynomial in d and $\vec{a}$ with integer coefficients, since $\mathrm{N}_\ell(d,\vec{a})$ is then an $\mathcal{L}_{\mathrm{ring}}$-term which satisfies the condition.

We calculate the norm using Theorem 2.2.5. For any $\alpha \in K$, let M_α denote the $\ell \times \ell$ matrix representing the linear map $x \mapsto \alpha x$ from L^d to L^d, with respect to the power basis $1, d^{1/\ell}, \ldots, d^{(\ell-1)/\ell}$. Write $\alpha = a_0 + a_1 d^{1/\ell} + \cdots + a_{\ell-1} d^{(\ell-1)/\ell}$. Then it is easily seen that

$$M_\alpha = a_0 M_1 + a_1 M_{d^{1/\ell}} + \cdots + a_{\ell-1} M_{d^{(\ell-1)/\ell}}.$$

Now since for all i, every entry of $M_{d^{i/\ell}}$ is either 0, 1 or d, we conclude that the entries of M_α consist of polynomials in d and $\vec{a}$ with integer coefficients. The same hold for the determinant of M_α, hence also for $\mathrm{N}_\ell(d,\vec{a})$. □

To be more explicit; the $\mathcal{L}_{\mathrm{ring}}$-term $\mathrm{N}_\ell(x; y_1, \ldots, y_\ell)$ equals $\mathrm{N}_2 = y_1^2 - y_2^2 x$ for $\ell = 2$ and for $\ell = 3$ we find $\mathrm{N}_3 = y_1^3 + y_2^3 x + y_3^3 x^2 - 3y_1 y_2 y_3 x$.

It follows from Lemma 5.2.1 that N_D is $\mathcal{L}_{\mathrm{ring}}$-definable. Indeed, N_D is defined by

$$\psi_\ell(x) := \exists \vec{a} \exists d \ (\delta(d) \wedge x = \mathrm{N}_\ell(d,\vec{a})), \tag{5.1}$$

whenever D is defined by $\delta(x)$.

Proposition 5.2.2. *Consider the $\mathcal{L}_{\mathrm{ring}}$-formula*

$$\delta_\ell(x; y_1, y_2) = \exists \vec{a}_1 \exists \vec{a}_2 (d = \mathrm{N}_\ell(y_1, \vec{a}_1) \wedge x y_2 = \mathrm{N}_\ell(y_1 y_2, \vec{a}_2)) \tag{5.2}$$

If $\delta_\ell(x; u, \pi)$, then $x \in \Delta_\mathfrak{p}$, for all $x, u, \pi \in K$ with $u \in U_\mathfrak{p} - U_\mathfrak{p}^\ell$ and $\mathrm{ord}_\mathfrak{p}(\pi) = 1$.

Proof. Suppose that d satisfies $\delta(x; u, \pi)$. Note that $\mathrm{ord}_\mathfrak{p}(u) = 0$ with $u \notin (K_\mathfrak{p}^\times)^\ell$ and that $\mathrm{ord}_\mathfrak{p}(\pi) = 1 \neq 0$ modulo ℓ. Hence by Theorem 2.11.4 we find that $K_\mathfrak{p}(u^{1/\ell})/K_\mathfrak{p}$ is unramified of degree ℓ and $K_\mathfrak{p}((u\pi)^{1/\ell})/K_\mathfrak{p}$ is totally ramified. Furthemore d is a norm local norm of $K_\mathfrak{p}(u^{1/\ell})/K_\mathfrak{p}$ at $\mathfrak{p}$ and $d\pi$ is a local norm of $K_\mathfrak{p}((u\pi)^{1/\ell})/K_\mathfrak{p}$ at $\mathfrak{p}$. From the description of the norm groups in Theorem 2.11.4 and the fact that $\mathrm{ord}_\mathfrak{p}(\pi) = 1$ we conclude that for some $m, n \in \mathbb{N}$ and $v, w \in U_\mathfrak{p}$

$$d = v\pi^{n\ell}, \qquad d\pi = w^\ell (u\pi)^m.$$

If we multiply the first by π we find $v\pi^{n\ell+1} = w^\ell (u\pi)^m$. Hence

$$n\ell + 1 = \mathrm{ord}_\mathfrak{p}(v\pi^{n\ell+1}) = \mathrm{ord}_\mathfrak{p}(w^\ell (u\pi)^m) = m,$$

because the order of u, v and w at $\mathfrak{p}$ are all zero. We now find that $d = u(wu^n\pi^n)^\ell$ and hence $K_\mathfrak{p}(d^{1/\ell})/K_\mathfrak{p} = K_\mathfrak{p}(u^{1/\ell})/K_\mathfrak{p}$ is unramified of degree ℓ. Again by Theorem 2.11.4 we find that $\mathrm{ord}_\mathfrak{p}(x) \equiv 0$ modulo ℓ, as x is a local norm at $\mathfrak{p}$. □

We will now construct u and π, such that N_D, with $D \subseteq \Delta_\mathfrak{p}$ the subset of K defined by $\delta_\ell(x, u, \pi)$, is a large subgroup of $N_\mathfrak{p}^\ell$. For this construction, we need some preliminary lemmas.

Lemma 5.2.3. *Let K be a global field and $n \in \mathbb{N}$ an integer. For all elements $a_1, \ldots, a_n \in K$ and all pairwise distinct places $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ there exists an $x \in \mathcal{O}_K$ such that (x) is a prime ideal and $x \equiv a_i$ modulo $\mathfrak{p}_i$ for all i.*

Proof. By the approximation theorem we find an $x_0 \in K$ such that $x_0 \equiv a_i$ modulo $\mathfrak{p}_i$ for all i. Now consider the ray class of (x_0) modulo $\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ (i.e., $[(x_0)] \in Cl_\mathfrak{m}(K)$). By Theorem 2.10.6, $[(x_0)]$ contains infinitely many prime ideals. Furthermore notice that every ideal in $[(x_0)]$ is principal. Hence we find some x such that (x) is a prime ideal of $\mathcal{O}_K$ and that $(x/x_0) \in P_\mathfrak{m}$, i.e., $x/x_0 \equiv 1$ modulo $\mathfrak{p}_i$ for all i. Therefore we find that $x \equiv a_i$ modulo $\mathfrak{p}_i$ for all i. Notice that $x \in \mathcal{O}_K$, since (x) is a prime ideal. This completes the proof. □

Lemma 5.2.4. *Let $L^d = K(d^{1/\ell})$ be an extension of a global field K and let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct totally ramified places of K. Then there exists $\xi_\mathfrak{p}, \xi_\mathfrak{q} \in K$ such that $\xi_\mathfrak{p} \in U_\mathfrak{p} - U_\mathfrak{p}^\ell$ and $\xi_\mathfrak{q} \in U_\mathfrak{q} - U_\mathfrak{q}^\ell$ and $(\xi_\mathfrak{p}, L^d/K)_\mathfrak{p} \cdot (\xi_\mathfrak{q}, L^d/K)_\mathfrak{q} = 1$.*

Proof. As L^d/K is totally ramified above $\mathfrak{p}$ and $\mathfrak{q}$ we find that $G_\mathfrak{p} = G_\mathfrak{q} = \mathrm{Gal}(L^d/K)$. Therefore $(\cdot, L^d/K)_\mathfrak{p} : K_\mathfrak{p} \to \mathrm{Gal}(L^d/K)$ and $(\cdot, L^d/K)_\mathfrak{q} : K_\mathfrak{q} \to \mathrm{Gal}(L^d/K)$ are both surjective. Now notice that Theorem 2.11.4 implies that $\mathrm{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}((L^d_\mathfrak{P})^\times) = \langle d, (K^\times_\mathfrak{p})^\ell \rangle$ and that $\ell \nmid \mathrm{ord}_\mathfrak{p}(d)$, because $\mathfrak{p}$ is totally ramified. Hence we have that $\mathrm{ord}_\mathfrak{P}$ is surjective on $\mathrm{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}((L^d_\mathfrak{P})^\times))$. Since norms are in the kernel of the Artin map, we see that $(\cdot, L^d/K)_\mathfrak{p} : U_\mathfrak{p} \to \mathrm{Gal}(L^d/K)$ is still surjective. The same argument shows that $(\cdot, L^d/K)_\mathfrak{q} : U_\mathfrak{q} \to \mathrm{Gal}(L^d/K)$ is surjective.

Pick $\sigma \in \mathrm{Gal}(L^d/K)$ with $\sigma \neq 1$. Then by the surjectivity there exists $\xi_\mathfrak{p}$ and $\xi_\mathfrak{q}$ with $(\xi_\mathfrak{p}, L^d/K)_\mathfrak{p} = \sigma$ and $(\xi_\mathfrak{q}, L^d/K)_\mathfrak{q} = \sigma^{-1}$. Furthermore Lemma 2.11.3 implies that $\mathrm{N}_{L^d/K}(U_\mathfrak{P}) = U^\ell_\mathfrak{p}$ and $\mathrm{N}_{L^d/K}(U_\mathfrak{Q}) = U^\ell_\mathfrak{q}$, hence $\sigma, \sigma^{-1} \neq 1$ implies $\xi_\mathfrak{p} \in U_\mathfrak{p} - U^\ell_\mathfrak{p}$ and $\xi_\mathfrak{q} \in U_\mathfrak{q} - U^\ell_\mathfrak{q}$. □

Lemma 5.2.5. *Let $\mathfrak{p}$ be a finite place of a global field K, let $\ell \neq \mathrm{char}(\overline{K}_\mathfrak{p})$ be a prime number and $x, y \in \mathcal{O}_K$ with $x \equiv y$ modulo $\mathfrak{p}$. Then $y \in (K^\times_\mathfrak{p})^\ell$ implies that*

$$x \in (K^\times_\mathfrak{p})^\ell \subseteq \mathrm{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}((L^d_\mathfrak{P})^\times),$$

where $L^d = K(d^{1/\ell})$ is an extension of K and $\mathfrak{P}$ a place of L^d above $\mathfrak{p}$.

Proof. If $x \equiv y$ modulo $\mathfrak{p}$, with $x, y \in \mathcal{O}_K$, then $X = 1$ is a solution of the primitive polynomial $yX^\ell - x$ over $K_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. Using Hensel's lemma we conclude that x/y is an ℓ-th power in $K^\times_\mathfrak{p}$, i.e., $x/y \in (K^\times_\mathfrak{p})^\ell$. Hence if $y \in (K^\times_\mathfrak{p})^\ell$, then $x \in (K^\times_\mathfrak{p})^\ell$. Furthermore since $\mathrm{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}(x) = x^\ell$ for all $x \in K^\times_\mathfrak{p}$ we see that x is a local norm at $\mathfrak{p}$. □

Recall the definition of δ_ℓ from (5.2). We are now ready to prove the following theorem:

Theorem 5.2.6. *Let $\mathfrak{p}$ be a finite place of a global field K. Suppose that $\ell \neq \mathrm{char}(\overline{K}_\mathfrak{p})$ is a prime number such that K contains the 2ℓ-th roots of unity. Then there are infinitely many places $\mathfrak{q} \neq \mathfrak{p}$ for which there exist $u, \pi \in K$ such that $\delta_\ell(x; u, \pi)$ defines a subset $D \subseteq \Delta_\mathfrak{p}$ with*

$$N_D \;=\; N^\ell_\mathfrak{p} \cap N^\ell_\mathfrak{q} \;=\; \{x \in N^\ell_\mathfrak{p} \mid \mathrm{ord}_\mathfrak{q}(x) \equiv 0 \mod \ell\}.$$

Proof. For notational convenience we will write $\mathfrak{p}_0$ and $\mathfrak{q}_0$ for $\mathfrak{p}$ and $\mathfrak{q}$ emphasize that $\mathfrak{p}$ and $\mathfrak{q}$ are fixed. The proof consists of three steps.

The first step is to construct $\mathfrak{q}_0$, u and π. Let $m \in \mathbb{N}$ be an integer so large that for all $\mathfrak{p} \mid \ell$ and $x \in K$ such that $x \equiv 1$ modulo $\mathfrak{p}^m$ we have $x \in (K^\times_\mathfrak{p})^\ell$. I do not know how to prove the existence of m. Consider the ray class group $\mathcal{C}l_\mathfrak{m}(K)$ modulo

$$\mathfrak{m} = \left(\prod_{\mathfrak{p}\mid\infty} \mathfrak{p}\right)\left(\prod_{\mathfrak{p}\mid\ell} \mathfrak{p}^m\right).$$

Then let $\mathfrak{q}_0$ be any prime in the inverse class of $\mathfrak{p}_0$, distinct from $\mathfrak{p}_0$ (equality only occurs when $[\mathfrak{p}_0]^{-1} = [\mathfrak{p}_0]$ in $\mathcal{C}l_\mathfrak{m}(K)$). By Theorem 2.10.6 there are infinitely many choices for $\mathfrak{q}_0$. By construction we find an element π in $\mathcal{O}_K$ such that

$$(\pi) = \mathfrak{p}_0\mathfrak{q}_0, \qquad \pi \equiv 1 \mod \mathfrak{m}.$$

Now consider the extension $L^\pi = K(\pi^{1/\ell})$ of K. By Theorem 2.11.4 the extension L^π/K is totally ramified above $\mathfrak{p}_0$ and $\mathfrak{q}_0$, since $\mathrm{ord}_{\mathfrak{p}_0}(\pi) = \mathrm{ord}_{\mathfrak{q}_0}(\pi) = 1$. Hence using Lemma 5.2.3 and Lemma 5.2.4 we find some $u \in \mathcal{O}_K$ such that (u) is prime prime ideal of $\mathcal{O}_K$ and

$$\begin{aligned} u &\equiv 1 \mod \mathfrak{m} \\ u &\equiv \xi_{\mathfrak{p}_0} \mod \mathfrak{p}_0 \\ u &\equiv \xi_{\mathfrak{q}_0} \mod \mathfrak{q}_0, \end{aligned}$$

where $\xi_{\mathfrak{p}_0} \in U_{\mathfrak{p}_0} - U^\ell_{\mathfrak{p}_0}$ and $\xi_{\mathfrak{q}_0} \in U_{\mathfrak{q}_0} - U^\ell_{\mathfrak{q}_0}$ and $(\xi_{\mathfrak{p}_0}, L^\pi/K)_{\mathfrak{p}_0} \cdot (\xi_{\mathfrak{q}_0}, L^\pi/K)_{\mathfrak{q}_0} = 1$. This completes the construction of $\mathfrak{q}_0$, u and π.

The second step is to show that $D \subseteq \Delta_{\mathfrak{p}_0} \cap \Delta_{\mathfrak{q}_0}$, where D is the subset of K which is defined by $\delta_\ell(x; u, \pi)$. This follows form Proposition 5.2.2 applied to both

$\mathfrak{p}_0$ and $\mathfrak{q}_0$ and hence it suffices to show that $u \in U_{\mathfrak{p}_0} - U_{\mathfrak{p}_0}^{\ell}$, $u \in U_{\mathfrak{q}_0} - U_{\mathfrak{q}_0}^{\ell}$ and $\mathrm{ord}_{\mathfrak{p}_0}(\pi) = \mathrm{ord}_{\mathfrak{q}_0}(\pi) = 1$. The first condition follows from $u \equiv \xi_{\mathfrak{p}_0}$ modulo $\mathfrak{p}_0$ and $u \equiv \xi_{\mathfrak{q}_0}$ modulo $\mathfrak{q}_0$ applied to Lemma 5.2.5. The latter condition is a trivial consequence from $(\pi) = \mathfrak{p}_0\mathfrak{q}_0$.

The final step is to show that $N_D = N_{\mathfrak{p}_0}^{\ell} \cap N_{\mathfrak{q}_0}^{\ell}$, which is done the standard way by proving the two inclusions.

Let $x \in N_D$ be arbitrary. Then there exists some $d \in D$ such that $x \in \mathrm{N}_{L^d/K}((L^d)^{\times})$. As every global norm is a local norm we find that $x \in K$ satisfies $x \in \mathrm{N}_{L^d_{\mathfrak{P}_0}/K_{\mathfrak{p}_0}}((L^d_{\mathfrak{P}_0})^{\times})$ and $x \in \mathrm{N}_{L^d_{\mathfrak{Q}_0}/K_{\mathfrak{q}_0}}((L^d_{\mathfrak{Q}_0})^{\times})$. Now since $D \subseteq \Delta_{\mathfrak{p}_0} \cap \Delta_{\mathfrak{q}_0}$ we may apply Theorem 5.1.2 for $\mathfrak{p}_0$ and $\mathfrak{q}_0$ and conclude that $x \in N_{\mathfrak{p}_0}^{\ell}$ and $x \in N_{\mathfrak{q}_0}^{\ell}$. We conclude that $N_D \subseteq N_{\mathfrak{p}_0}^{\ell} \cap N_{\mathfrak{q}_0}^{\ell}$.

Conversely let $x_0 \in N_{\mathfrak{p}_0}^{\ell} \cap N_{\mathfrak{q}_0}^{\ell}$ be arbitrary. We will prove that $x_0 \in N_D$. Write

$$(x_0) = \mathfrak{p}_0^{p\ell}\mathfrak{q}_0^{q\ell}\mathfrak{q}_1^{k_1}\cdots\mathfrak{q}_s^{k_s},$$

for some integer $s \geq 1$ and integers $p, q, k_1, \ldots, k_s \in \mathbb{Z}$. It suffices to find some $d \in D$ such that $x_0 \in \mathrm{N}_{L^d/K}((L^d)^{\times})$. We choose d as follows: by Lemma 5.2.3 there exists some $d \in \mathcal{O}_K$ such that (d) is a prime ideal of $\mathcal{O}_K$ and

$$\begin{aligned}
&d \equiv 1 \mod \mathfrak{m}\\
&d \equiv \xi_{\mathfrak{p}_0} \mod \mathfrak{p}_0\\
&d \equiv \xi_{\mathfrak{q}_0} \mod \mathfrak{q}_0\\
&d \equiv 1 \mod (u)\\
&d \equiv 1 \mod \mathfrak{q}_i, \qquad i = 1, \ldots, s.
\end{aligned}$$

The remainder of the proof consists of checking that $d \in D$ and $x_0 \in \mathrm{N}_{L^d/K}((L^d)^{\times})$.

We prove that d satisfies

$$\delta_{\ell}(x; u, \pi) = \exists\vec{a}_1 \exists\vec{a}_2 (x = \mathrm{N}_{\ell}(u, \vec{a}_1) \wedge x\pi = \mathrm{N}_{\ell}(u\pi, \vec{a}_2)),$$

which means that $d \in D$. In other words, we show that d is a global norm from L^u and that $d\pi$ is a global norm from $L^{u\pi}$.

We show that d is a global norm from $L^u = K(u^{1/\ell})$. By the Hasse norm theorem applied to the cyclic Kummer extension L^u/K we conclude that it suffices to prove that d is a local norm of L^u/K at every prime. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ in L^u.

- If $\mathfrak{p}$ is an infinite place then Ostrowski's theorem implies $K_{\mathfrak{p}} \cong \mathbb{C}$, since K contains the $s\ell$-th roots of unity. Thus $L^u_{\mathfrak{P}}/K_{\mathfrak{p}}$ is trivial and d is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p} \mid \ell$ then $L^u_{\mathfrak{P}}/K_{\mathfrak{p}}$ is trivial, because $u \equiv 1$ modulo $\mathfrak{m}$ implies $u \equiv 1$ modulo $\mathfrak{p}^m$ and by construction of m we find that $u \in (K_{\mathfrak{p}}^{\times})^{\ell}$. Thus $\mathrm{N}_{L^u_{\mathfrak{P}}/K_{\mathfrak{p}}}(x) = x$ for all $x \in K_{\mathfrak{p}}^{\times}$ and hence d is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p} = (u)$ then $d \equiv 1$ modulo $\mathfrak{p}$ and $d \in \mathcal{O}_K$, since (d) is a prime ideal. Now Lemma 5.2.5 shows that d is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p}$ is a finite prime with $\mathfrak{p} \nmid \ell$, $\mathfrak{p} \neq (u)$ and $\mathfrak{p} \neq (d)$ then $\mathrm{ord}_{\mathfrak{p}}(u) = 0$ and $\mathrm{ord}_{\mathfrak{p}}(d) = 0$. Hence Theorem 2.11.4 shows that L^u is unramified at $\mathfrak{p}$ (either trivial or non-trivial). Therefore d is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p} = (d)$ then we find by Artin's reciprocity law that

  $$1 = \textstyle\prod_{\mathfrak{q}}(d, L^u/K)_{\mathfrak{q}} = (d, L^u/K)_{\mathfrak{p}},$$

  because the previous items show that $(d, L^u/K)_{\mathfrak{q}} = 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. Therefore d is a local norm at $\mathfrak{p}$.

We conclude that d is a global norm form L^u.

Next we show that $d\pi$ is a global norm from $L^{u\pi} = K((u\pi)^{1/\ell})$. By the Hasse norm theorem applied to the cyclic Kummer extension $L^{u\pi}/K$ we conclude that it suffices to prove that $d\pi$ is a local norm of $L^{u\pi}/K$ at every prime. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ in $L^{u\pi}$.

- If $\mathfrak{p}$ is an infinite place then Ostrowski's theorem implies $K_\mathfrak{p} \cong \mathbb{C}$, since K contains the $s\ell$-th roots of unity. Thus $L^{u\pi}_\mathfrak{P}/K_\mathfrak{p}$ is trivial and $d\pi$ is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p} \mid \ell$ then $L^{u\pi}_\mathfrak{P}/K_\mathfrak{p}$ is trivial, because $u, \pi \equiv 1$ modulo $\mathfrak{m}$ implies $u\pi \equiv 1$ modulo $\mathfrak{p}^m$ and by construction of m we find that $u\pi \in (K_\mathfrak{p}^\times)^\ell$. Thus $\mathrm{N}_{L^{u\pi}_\mathfrak{P}/K_\mathfrak{p}}(x) = x$ for all $x \in K_\mathfrak{p}^\times$ and hence $d\pi$ is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p}$ equals $\mathfrak{p}_0$ or $\mathfrak{q}_0$ then $d \equiv \zeta_\mathfrak{p} \equiv u$ modulo $\mathfrak{p}$ and $d/u \equiv 1$ modulo $\mathfrak{p}$. Now Lemma 5.2.5 shows that d/u is a local norm at $\mathfrak{p}$. But Theorem 2.11.4 shows that $u\pi$ is also a norm from $L^{u\pi}/K$, hence $d\pi = (d/u)(u\pi)$ is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p} = (u)$ then $d, \pi \equiv 1$ modulo $\mathfrak{p}$ and $d \in \mathcal{O}_K$, since (d) is a prime ideal. Now Lemma 5.2.5 shows that d is a local norm at $\mathfrak{p}$. We claim that π is also a local norm at $\mathfrak{p}$. Then it follows that $d\pi$ is a local norm at $\mathfrak{p}$.

  We prove the claim. Notice that $(u, L/K)_\mathfrak{q}$ is different from 1 only if $\mathfrak{q}$ is $\mathfrak{p}_0$, $\mathfrak{q}_0$ or $\mathfrak{p}$: at infinite places $(u, L/K)_\mathfrak{q} = 1$ because $u \equiv 1$ modulo $\mathfrak{m}$; at $\mathfrak{q} \mid \ell$, $(u, L/K)_\mathfrak{q}$ because $u \in (K_\mathfrak{q}^\times)^\ell$; and for all other finite places other then $\mathfrak{p}_0$, $\mathfrak{q}_0$ or $\mathfrak{p}$, $(u, L/K)_\mathfrak{q} = 1$ because $L_\mathfrak{Q}/K_\mathfrak{q}$ is unramified and $\mathrm{ord}_\mathfrak{q}(u) = 0$. Furthermore u differs from $\xi_{\mathfrak{p}_0}$ by an ℓ-th power in $K_{\mathfrak{p}_0}$, since $\mathfrak{p}_0 \nmid \ell$ and similarly for $\xi_{\mathfrak{q}_0}$. Therefore

  $$(u, L/K)_{\mathfrak{p}_0} = (\xi_{\mathfrak{p}_0}, L/K)_{\mathfrak{p}_0} = (\xi_{\mathfrak{q}_0}, L/K)^{-1}_{\mathfrak{q}_0} = (u, L/K)_{\mathfrak{q}_0}.$$

  By Artin's reciprocity law and we have

  $$1 = \prod_\mathfrak{q} (u, L/K)_\mathfrak{q} = (u, L/K)_{\mathfrak{p}_0} \cdot (u, L/K)_{\mathfrak{q}_0} \cdot (u, L/K)_\mathfrak{p} = (u, L/K)_\mathfrak{p}$$

  which means that u is a local norm from $L^u_\mathfrak{P}/K_\mathfrak{p}$. But L/K is unramified at $\mathfrak{p}$ and $\mathrm{ord}_\mathfrak{p}(u) = 1$, hence $L^u_\mathfrak{P}/K_\mathfrak{p}$ must be trivial. This means that $u \in K_\mathfrak{p}^\ell$ and that u is a local norm at $\mathfrak{p} = (u)$.

- If $\mathfrak{p}$ is a finite prime with $\mathfrak{p} \nmid \ell$, $\mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{q}_0, (u), (d)$ then $\mathrm{ord}_\mathfrak{p}(d) = 0$ and Theorem 2.11.4 shows that $L^{u\pi}$ is unramified at $\mathfrak{p}$ (either trivial or non-trivial). Therefore we find that d is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p} = (d)$ then we find by Artin's reciprocity law that

  $$1 = \textstyle\prod_\mathfrak{q} (d, L^{u\pi}/K)_\mathfrak{q} = (d, L^{u\pi}/K)_\mathfrak{p},$$

  because the previous items show that $(d, L^{u\pi}/K)_\mathfrak{q} = 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. Therefore d is a local norm at $\mathfrak{p}$.

We conclude that $d\pi$ is a norm from $L^{u\pi}$. Furthermore we have that $d \in D$. In other words: d satisfies $\delta_\ell(x; u, \pi)$.

Finally we show that $x_0 \in \mathrm{N}_{L^d/K}((L^d)^\times)$. By the Hasse norm theorem applied to the cyclic Kummer extension L^d/K we conclude that it suffices to prove that x_0 is a local norm of L^d/K at every prime. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ in L^d.

- If $\mathfrak{p}$ is an infinite place then Ostrowski's theorem implies $K_\mathfrak{p} \cong \mathbb{C}$, since K contains the $s\ell$-th roots of unity. Thus $L^d_\mathfrak{P}/K_\mathfrak{p}$ is trivial and x_0 is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p} \mid \ell$ then $L^d_\mathfrak{P}/K_\mathfrak{p}$ is trivial, because $d \equiv 1$ modulo $\mathfrak{m}$ implies $d \equiv 1$ modulo $\mathfrak{p}^m$ and by construction of m we find that $d \in (K_\mathfrak{p}^\times)^\ell$. Thus $\mathrm{N}_{L^d_\mathfrak{P}/K_\mathfrak{p}}(x) = x$ for all $x \in K_\mathfrak{p}^\times$ and hence x_0 is a local norm at $\mathfrak{p}$.

- If $\mathfrak{p}$ equals $\mathfrak{p}_0$ or $\mathfrak{q}_0$ then $d \equiv \zeta_\mathfrak{p}$ modulo $\mathfrak{p}$. So Lemma 5.2.5 shows that d is a non-ℓ-th power unit in $K_\mathfrak{p}$ and $L^d_\mathfrak{P}/K_\mathfrak{p}$ is unramified of degree ℓ. Theorem 2.11.4 now shows that x_0 is a local norm at $\mathfrak{p}$ because $x_0 \in N^\ell_{\mathfrak{p}_0} \cap N^\ell_{\mathfrak{q}_0}$.

- If $\mathfrak{p} \nmid \ell$ and $\mathfrak{p} = \mathfrak{q}_i$ with $1 \leq i \leq s$ then $d \equiv 1$ modulo $\mathfrak{p}$. Hence since $d \in \mathcal{O}_K$ and $\mathfrak{p} \nmid \ell$ we conclude from Lemma 5.2.5 that $d \in (K_{\mathfrak{p}}^{\times})^{\ell}$. Therefore $L_{\mathfrak{P}}^{d}/K_{\mathfrak{p}}$ is trivial and that x_0 is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p}$ is a finite prime with $\mathfrak{p} \nmid \ell$, $\mathfrak{p} \neq (d)$, $\mathfrak{p} \neq \mathfrak{p}_0$ and $\mathfrak{p} \neq \mathfrak{q}_i$ for all $0 \leq i \leq s$, then $\mathrm{ord}_{\mathfrak{p}}(x_0) = 0$ and Theorem 2.11.4 shows that L^d is unramified at $\mathfrak{p}$ (either trivial or non-trivial). Therefore we find that x_0 is a local norm at $\mathfrak{p}$.
- If $\mathfrak{p} = (d)$ then we find by Artin's reciprocity law that

  $$1 = \textstyle\prod_{\mathfrak{q}}(d, L^d/K)_{\mathfrak{q}} = (d, L^d/K)_{\mathfrak{p}},$$

  because the previous items show that $(d, L^d/K)_{\mathfrak{q}} = 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. Therefore d is a local norm at $\mathfrak{p}$.

We conclude that $x \in \mathrm{N}_{L^d/K}((L^d)^{\times})$.

We now have shown that $x_0 \in N_D$, which finishes the proof of the equality $N_D = N_{\mathfrak{p}_0}^{\ell} \cap N_{\mathfrak{q}_0}^{\ell}$. □

Recall the definition of ψ_ℓ from (5.1) and δ_ℓ from (5.2) at page 88. We now show that we can find $\mathcal{L}_{\mathrm{ring}}$-definable subsets $D_1, D_2 \subseteq \Delta_{\mathfrak{p}}$ such that $N_{\mathfrak{p}}^{\ell} = N_{D_1} N_{D_2}$ and conclude that $\mathcal{O}_{\mathfrak{p}}$ is $\mathcal{L}_{\mathrm{ring}}$-definable.

Corollary 5.2.7. *Let K be a global field and suppose that ℓ is a prime number such that K contains the 2ℓth roots of unity. Consider the $\mathcal{L}_{\mathrm{ring}}$-formula*

$$\phi_\ell(x; \vec{y}) := \exists x_1 \exists x_2 (x = x_1 x_2 \wedge \psi_\ell(x_1; y_1, y_2) \wedge \psi_\ell(x_2; y_3, y_4)). \tag{5.3}$$

For all finite places $\mathfrak{p}$ of K with $\ell \neq \mathrm{char}(\overline{K}_{\mathfrak{p}})$ there exists some $\vec{c} \in K^4$ such that $\phi_\ell(x; \vec{c})$ defines the valuation ring $\mathcal{O}_{\mathfrak{p}}$ in K.

Proof. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be two distinct primes as in Theorem 5.2.6, i.e., the subsets D_i, for $i = 1, 2$, satisfy $N_{D_i} = N_{\mathfrak{p}}^{\ell} \cap N_{\mathfrak{q}_i}^{\ell}$ are defined by $\delta(x; u_i, \pi_i)$ for some $u_i, \pi_i \in K$. We claim that $N_{D_1} N_{D_2} = N_{\mathfrak{p}}^{\ell}$. In this case every $x \in N_{\mathfrak{p}}^{\ell}$ is a product of an $x_1 \in N_{D_1}$ and some $x_2 \in N_{D_2}$. Furthermore N_{D_i} is defined by

$$\psi_\ell(x; u_i, \pi_i) := \exists \vec{a}, d(\delta(d; u_i, \pi_i) \wedge x = \mathrm{N}_\ell(d, \vec{a})).$$

Hence $\phi_\ell(x; u_1, \pi_1, u_2, \pi_2)$ defines $N_{\mathfrak{p}}^{\ell}$. Using Lemma 5.1.1 we conclude that $\mathcal{O}_{\mathfrak{p}}$ is $\mathcal{L}_{\mathrm{ring}}$-definable.

It remains to show that $N_{D_1} N_{D_2} = N_{\mathfrak{p}}^{\ell}$. Observe that N_{D_1}, N_{D_2}, $N_{D_1} N_{D_2}$ and $N_{\mathfrak{p}}^{\ell}$ are all subgroups of $K^{\times}$ as they contain 1 and are closed under multiplication. Since N_{D_1} is a subgroup of the product $N_{D_1} N_{D_2}$ we find a tower of groups

$$N_{D_1} \subsetneq N_{D_1} N_{D_2} \subseteq N_{\mathfrak{p}}^{\ell},$$

where the proper inclusion follows form the fact that $N_{D_1} \neq N_{D_2}$. Since this index of N_{D_1} in $N_{\mathfrak{p}}^{\ell}$ equals ℓ we conclude that the index of $N_{D_1} N_{D_2}$ in $N_{\mathfrak{p}}^{\ell}$ divides ℓ. But since ℓ is prime and the first inclusion is proper, we find that this index equals 1. This proves the claim. □

5.3. Definability of valuation domains

Corollary 5.2.7 and Lemma 5.1.3 provide a huge step towards defining a large family of valuation rings. But there is still one thing missing, namely the formula which determines the parameters (c.f., Definition 3.8.4). This problem is solved in the following lemma.

Lemma 5.3.1. *Let $\mathfrak{p}$ be a finite place of a global field K. Suppose that $\ell \neq \mathrm{char}(\overline{K}_{\mathfrak{p}})$ is a prime number such that K contains the 2ℓ-th roots of unity. Then there exists $\mathcal{L}_{\mathrm{ring}}$-formulas $\phi_\ell(x; \vec{y})$ and $\chi_\ell(\vec{y})$ such that*

$$\mathscr{F} = \begin{cases} \{\mathcal{O}_{\mathfrak{p}} \mid \mathfrak{p} \text{ finite}\} & \text{if } \mathrm{char}(K) > 0 \\ \{\mathcal{O}_{\mathfrak{p}} \mid \mathfrak{p} \text{ finite and } \mathfrak{p} \nmid \ell\} & \text{if } \mathrm{char}(K) = 0 \end{cases}$$

is parametrized by ϕ_ℓ with parameters satisfying χ_ℓ.

Proof. Recall the definition of ϕ_ℓ from (5.3). Consider the $\mathcal{L}_{\text{ring}}$-formulas

$$\begin{aligned}\theta_\ell(\vec{y}) &= \forall x_1 \forall x_2((\phi_\ell(x_1;\vec{y}) \wedge \phi_\ell(x_2;\vec{y})) \to (\phi_\ell(x_1 - x_2;\vec{y}) \wedge \phi_\ell(x_1x_2;\vec{y})))\\ \rho_\ell(\vec{y}) &= \forall x(x \neq 0 \to (\phi_\ell(x;\vec{y}) \wedge \phi_\ell(1/x;\vec{y})))\\ \chi_\ell(\vec{y}) &= \theta_\ell(\vec{y}) \wedge \rho_\ell(\vec{y}).\end{aligned}$$

Suppose that $\vec{c} \in K^4$ satisfies $\chi_\ell(\vec{y})$. Then $\phi_\ell(x;\vec{c})$ defines a valuation domain in L (c.f., Definition 1.9.1). Hence by Corollary 2.5.16 we conclude that $\phi_\ell(x;\vec{c})$ defines $\mathcal{O}_\mathfrak{p}$ for some finite place $\mathfrak{p}$ of L. On the other hand, Corollary 5.2.7 implies that for every $\mathfrak{p}$ with $\text{char}(\overline{K}_\mathfrak{p}) \neq \ell$ there exists some $\vec{c} \in K^4$ such that $\phi_\ell(x;\vec{c})$ defines the valuation ring $\mathcal{O}_\mathfrak{p}$ in K. It is clear that $\vec{c} \in K^4$ satisfies $\chi_\ell(\vec{y})$.

Let $\mathscr{F}$ be the family parametrized by $\phi_\ell(x;\vec{y})$ with parameters satisfying $\chi_\ell(\vec{y})$. If $\text{char}(K) > 0$, then $\ell \neq \text{char}(K) = \text{char}(\overline{K}_\mathfrak{p})$ and we find by the above discussion that $\mathscr{F} = \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \text{ finite}\}$. If $\text{char}(K) = 0$, then the above discussion implies that $\mathscr{F} = \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \text{ finite and } \mathfrak{p} \nmid \ell\}$. This concludes the proof. □

Notice that the $\mathcal{L}_{\text{ring}}$-formulas ϕ_ℓ and χ_ℓ depend on specific properties of K. Thus we did not found a uniform definition of the family of valuation rings. This will be solved in the following theorem, which is a reformulation of the results of paragraph 3 of [14].

Theorem 5.3.2. *There exists $\mathcal{L}_{\text{ring}}$-formulas and* $\text{val}(x; y_1, \ldots, y_9)$ *and* $\text{isval}(\vec{y})$ *such that if K is a global field, then* val *and* isval *parametrize the family*

$$\mathscr{F} = \begin{cases} \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \textit{ finite and } \mathfrak{p} \nmid 2\} & \textit{if } \text{char}(K) = 0 \\ \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \textit{ finite}\} & \textit{if } \text{char}(K) > 0 \end{cases}$$

Proof. Recall the definition of ϕ_ℓ from (5.3) and the construction of ϕ_ℓ^m from the proof of Lemma 5.1.3. Then Lemma 5.1.3 and Lemma 5.3.1 show that the $\mathcal{L}_{\text{ring}}$-formula

$$\text{val}(x, y_1, \ldots, y_9) := \begin{cases} \phi_3(x; y_1, \ldots, y_4) & \text{if } 2 = 0 \wedge \exists x(x^2 + x + 1 = 0) \\ \phi_3^2(x; y_1, \ldots, y_9) & \text{if } 2 = 0 \wedge \neg\exists x(x^2 + x + 1 = 0) \\ \phi_2(x; y_1, \ldots, y_4) & \text{if } 2 \neq 0 \wedge \exists x(x^2 + 1 = 0) \\ \phi_2^2(x; y_1, \ldots, y_9) & \text{if } 2 \neq 0 \wedge \neg\exists x(x^2 + 1 = 0) \end{cases}$$

with parameters satisfying

$$\text{isval}(y_1, \ldots, y_9) := \begin{cases} \chi_3(y_1, \ldots, y_4) & \text{if } 2 = 0 \wedge \exists x(x^2 + x + 1 = 0) \\ \chi_3^2(y_1, \ldots, y_9) & \text{if } 2 = 0 \wedge \neg\exists x(x^2 + x + 1 = 0) \\ \chi_2(y_1, \ldots, y_4) & \text{if } 2 \neq 0 \wedge \exists x(x^2 + 1 = 0) \\ \chi_2^2(y_1, \ldots, y_9) & \text{if } 2 \neq 0 \wedge \neg\exists x(x^2 + 1 = 0) \end{cases}$$

defines the family $\mathscr{F}$. □

Let $\mathbb{F}$ be the prime subfield of K. Then $k \subseteq K$ is called the *field of constants* of K if and only if k is the relative algebraic closure of the $\mathbb{F}$ in K. The following corollary shows that k is definable in positive characteristic.

Corollary 5.3.3. *There exists an $\mathcal{L}_{\text{ring}}$-formula* $\text{int}(x)$ *such that*

$$\{x \in K \mid K \models \text{int}(x)\} = \begin{cases} \mathcal{O}_K & \textit{if } \text{char}(K) = 0 \\ k & \textit{if } \text{char}(K) > 0 \end{cases}$$

for every global field K.

Proof. Note that the choice of 2 was not necessary and 3 also leads to an $\mathcal{L}_{\text{ring}}$-formulas and $\text{val}'(x; y_1, \ldots, y_9)$ and $\text{isval}'(\vec{y})$ that defines the family

$$\mathscr{F} = \begin{cases} \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \text{ finite and } \mathfrak{p} \nmid 3\} & \text{if } \text{char}(K) = 0 \\ \{\mathcal{O}_\mathfrak{p} \mid \mathfrak{p} \text{ finite}\} & \text{if } \text{char}(K) > 0 \end{cases}$$

Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\text{int}(x) := \forall \vec{y}(\text{isval}(\vec{y}) \to \text{val}(x;\vec{y})) \wedge \forall \vec{y}(\text{isval}'(\vec{y}) \to \text{val}'(x;\vec{y})).$$

Then $\text{int}(x)$ defines $\bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over all finite places of K. Proposition 1.9.4 shows that this is equal to the integral closure of R in K, where R is the prime subring of K (i.e., R is the intersection of all subrings of K). If $\text{char}(K) = 0$, then $R = \mathbb{Z} = \mathcal{O}_{\mathbb{K}}$ and $\text{int}(x)$ defines $\mathcal{O}_K$. If $\text{char}(K) = p > 0$, then $R = \mathbb{F}_p$ and $\text{int}(x)$ defines the integral closure of $\mathbb{F}_p$. As $\mathbb{F}_p$ is a field, the integral closure of $\mathbb{F}_p$ equals the algebraic closure of $\mathbb{F}_p$. Thus $\text{int}(x)$ defines the field of constants k of K. □

Corollary 5.3.3 allows us to choose uniformy a non-integral t in K. Furthermore this allows us to define the notion of divisibility in the ring of integers in characteristic zero. If K is a number field, then we define

$$y \mid x := \exists z(\text{int}(z;t) \wedge x = yz). \tag{5.4}$$

The following corollary is very interesting as it allows us to distinguish number fields from function fields. This will be very important in defining a model of the natural numbers in a general global field, as we may treat the number field case and the function field case separately.

Corollary 5.3.4. *There exists an $\mathcal{L}_{\text{ring}}$-sentence χ_0 such that $K \models \chi_0$ if and only if $\text{char}(K) = 0$ for all global fields K.*

Proof. Consider the sentence

$$\chi_0 := \forall x(\text{int}(x) \wedge 2 \neq 0 \wedge 2 \cdot x \neq 1).$$

If $\text{char}(K) = 0$, then $\text{int}(x)$ defines $\mathcal{O}_K$. Thus χ_0 is true, since 2 is not invertible in $\mathcal{O}_K$. If $\text{char}(K) = p > 0$ with $p \neq 2$, then 2 is invertible in $\mathbb{F}_p$ and χ_0 is false. □

This corollary can be used to find a uniform definition of the ring of integers.

Corollary 5.3.5. *There exists an $\mathcal{L}_{\text{ring}}$-formula $\text{rin}(x;t)$ such that if K is a global field and $t \in K$ non-integral, then* rin *defines $\mathcal{O}_K$.*

Proof. Define the $\mathcal{L}_{\text{ring}}$-formula

$$\text{rin}(x;t) := \begin{cases} \text{int}(x) & \text{if } \chi_0 \\ \forall \vec{y}(\text{isval}(\vec{y}) \to (\text{val}(x;\vec{y}) \to \phi(t;\vec{y}))) & \text{otherwise} \end{cases}$$

If $\text{char}(K) = 0$, then $\text{rin}(x;t)$ defines $\mathcal{O}_K$ by Corollary 5.3.3. If $\text{char}(K) = p > 0$, then $\text{rin}(x;t)$ defines $\bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over the finite places $\mathfrak{p}$ of K with $t \in \mathcal{O}_{\mathfrak{p}}$. Then Proposition 1.9.4 shows that $\text{rin}(x;t)$ defines the integral closure of $\mathbb{F}_p[t]$. Then, by definition, $\text{rin}(x;t)$ defines $\mathcal{O}_K$. □

This corollary allows us to define the notion of divisibility in the ring of integers. If K is a global field and $t \in K$ is non-integral, then we define

$$y \mid_t x := \exists z(\text{rin}(z;t) \wedge x = yz). \tag{5.5}$$

This clearly generalizes the notion of divisibility defined by (5.4) to arbitrary characteristic. Notice that x and y need not lie in $\mathcal{O}_K$. However if $y \mid_t x$ and either x or y is in $\mathcal{O}_K$, then both are in $\mathcal{O}_K$.

5.4. Definability of finite subsets

Our next step in defining a model of the natural numbers is to find a predicate which enables us to quantify over all finite subsets of K. In other words we will show that the family of all finite subsets of K is an $\mathcal{L}_{\text{ring}}$-definable family $\mathscr{F}$.

We will first show that it suffices to define a *cofinal* subfamily $\mathscr{F}'$ of $\mathscr{F}$ with respect to inclusion, that is, every member of $\mathscr{F}$ is contained in a member of $\mathscr{F}'$. Then $\mathscr{F}$ can be constructed from $\mathscr{F}'$ by shrinking the members of $\mathscr{F}'$.

Finally we will show that such a cofinal subfamily is definable for both zero and positive characteristic.

In order to prove that the definability of the cofinal subfamily is sufficient, we need two preliminary lemmas.

Lemma 5.4.1. *Let K be a global field and n a positive integer. Then for all non-zero $k_1, \ldots, k_n \in K$ there exists only finitely many $x \in \mathbb{K}$ such that $1 + xk_i$ is zero or a unit in $\mathcal{O}_K$ for some i.*

Proof. The idea is to find a non-zero polynomial $P \in \mathbb{K}[X]$ with the following property: for all $x \in \mathbb{K}$ we have that $1 + xk_i$ is zero or a unit in $\mathcal{O}_K$ for some i implies $P(x) = 0$. Consider the function $P : \mathbb{K} \to \mathbb{K}$ given by

$$P(x) = \prod_{i=1}^{n} \left((1 + xk_i) \prod_{c \in \mathcal{O}_{\mathbb{K}}^{\times}} \left(\mathrm{N}_{K/\mathbb{K}}(1 + xk_i) - c \right) \right)$$

Notice that this product is finite, since $\mathcal{O}_{\mathbb{K}}^{\times}$ equals either $\{\pm 1\}$ or $\mathbb{F}_p^{\times}$ whenever $\mathrm{char}(K) = p$.

We first show that P is a non-zero polynomial in x over $\mathbb{K}$. If $k_i \in \mathbb{K}$, then $\mathrm{N}_{\mathbb{K}(k_i)/\mathbb{K}}(1 + xk_i) = 1 + xk_i$ is a non-zero polynomial in x over $\mathbb{K}$, since all $k_i \neq 0$. Hence P is a non-zero polynomial over $\mathbb{K}$. Suppose that $k_i \notin \mathbb{K}$ and let $d = \deg(k_i) \geq 2$ be the degree of k_i over $\mathbb{K}$. Recall that

$$\mathrm{N}_{\mathbb{K}(k_i)/\mathbb{K}}(1 + xk_i) = \det(M_{1+xk_i}),$$

where $M_{1+xk_i} : \mathbb{K}(k_i) \to \mathbb{K}(k_i)$ is the linear map defined by multiplication by $1+xk_i$. Notice that $M_{1+xk_i} = M_1 + M_x M_{k_i} = I + xM_{k_i}$, because $1, x \in \mathbb{K}$. Now find $a_j \in \mathbb{K}$ for $0 \leq j < d$ such that $X^d - a_{d-1}X^{n-1} - \cdots - a_0$ is the minimal polynomial of k_i over $\mathbb{K}$. Then with respect to the power basis $1, k_i, \ldots, k_i^{d-1}$ of $\mathbb{K}(k_i)/\mathbb{K}$, the linear map M_{k_i} is represented by the matrix

$$M_{k_i} = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{d-2} \\ 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix}.$$

Now it is clear that $\det(M_{1+xk_i})$ is a non-zero polynomial in x over $\mathbb{K}$. Hence if $x \in \mathbb{K}$, then $\mathrm{N}_{K/\mathbb{K}(k_i)}(1 + xk_i) = (1 + xk_i)^{[K:\mathbb{K}(k_i)]}$. Using the transitivity of the norm we conclude that

$$\mathrm{N}_{K/\mathbb{K}}(1 + xk_i) = \mathrm{N}_{\mathbb{K}(k_i)/\mathbb{K}}(\mathrm{N}_{K/\mathbb{K}(k_i)}(1 + xk_i)) = \mathrm{N}_{\mathbb{K}(k_i)/\mathbb{K}}(1 + xk_i)^{[K:\mathbb{K}(k_i)]}$$

is a non-zero polynomial in x over $\mathbb{K}$. This implies that P is a non-zero polynomial over $\mathbb{K}$.

Finally we show that P satisfies the desired property. Let $x \in \mathbb{K}$ be arbitrary. If $1 + xk_i = 0$ for some i, then $P(x) = 0$. If $1 + xk_i \in \mathcal{O}_{\mathbb{K}}^{\times}$ for some i, then $\mathrm{N}_{K/\mathbb{K}}(1 + xk_i) \in \mathcal{O}_{\mathbb{K}}^{\times}$, because $\mathrm{N}_{K/\mathbb{K}} : K^{\times} \to \mathbb{K}^{\times}$ is a homomorphism with $\mathrm{N}_{K/\mathbb{K}}(\mathcal{O}_K) \subseteq \mathcal{O}_{\mathbb{K}}$. Hence $P(x) = 0$. We conclude that P satisfies the property.

The lemma follows from the fact that P has only finitely many roots, because P is non-zero. □

Lemma 5.4.2. *Let K be a global field with non-integral $t \in K$ and let n be a positive integer. Then for all non-zero $k_1, \ldots, k_n \in K$ there exists a non-zero ideal $\mathfrak{a} \in \mathcal{O}_K$ such that for all $h \in \mathfrak{a}$*

$$1 + hk_1 \quad \cdots \quad 1 + hk_n$$

are pairwise relatively prime elements of $\mathcal{O}_K$.

Proof. Suppose we are given non-zero $k_1, \ldots, k_n \in K$ for some positive integer n. Consider a ideal non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that for all $\mathfrak{p}$

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq \max_j \mathrm{ord}_{\mathfrak{p}}(k_j^{-1}) \tag{5.6}$$

and for all $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(k_j - k_{j'}) \geq 1$ for some j and j'

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \geq \max_{j,j'} \mathrm{ord}_{\mathfrak{p}}(k_j - k_{j'}). \tag{5.7}$$

Note that $\mathfrak{a}$ is well-defined, because there are only finitely many primes $\mathfrak{p}$ such that we demand $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) > 0$.

We will show that $\mathfrak{a}$ satisfies the conditions. Let $h \in \mathfrak{a}$ be arbitrary. Then we have that $(h) \subseteq \mathfrak{a}$ and hence $\mathfrak{a} \mid (h)$. This implies that $\mathrm{ord}_{\mathfrak{p}}(h) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$. Using equation (5.6) we find for all $\mathfrak{p}$ and j that $\mathrm{ord}_{\mathfrak{p}}(h) \geq \mathrm{ord}_{\mathfrak{p}}(k_j^{-1})$, which means that $\mathrm{ord}_{\mathfrak{p}}(hk_j) \geq 0$ and $1 + hk_j \in \mathcal{O}_K$. Moreover, if there exists a prime $\mathfrak{p}$ and j and j' such that $\mathfrak{p} \mid (1 + hk_j)$ and $\mathfrak{p} \mid (1 + hk_{j'})$, then $\mathfrak{p} \mid hk_j - hk_{j'}$. Hence using (5.7) we have that

$$1 \leq \mathrm{ord}_{\mathfrak{p}}(h(k_j - k_{j'})) = \mathrm{ord}_{\mathfrak{p}}(h) + \mathrm{ord}_{\mathfrak{p}}(k_j - k_{j'}) \leq 2\,\mathrm{ord}_{\mathfrak{p}}(h).$$

This implies that $\mathfrak{p} \mid (h)$. Now, since $\mathfrak{p} \mid (1 + hk_j)$, we have $\mathfrak{p} \mid (1)$. We conclude that

$$1 + hk_1 \quad \cdots \quad 1 + hk_n$$

are pairwise relatively prime elements of $\mathcal{O}_K$. □

We will now show that it suffices to define a cofinal subfamily of $\mathscr{F}$.

Theorem 5.4.3. *Let n be a positive integer and let $\phi(x; \vec{y}; t)$ be an $\mathcal{L}_{\mathrm{ring}}$-formula, with parameters satisfying $\chi(\vec{y})$, such that if K is a global field and $t \in K$ non-integral, then ϕ and χ define a cofinal subfamily of the family $\mathscr{F}$ of all finite subsets of K. Then the $\mathcal{L}_{\mathrm{ring}}$-formula*

$$\psi(x; \vec{y}, \vec{z}; t) := \phi(x; \vec{y}; t) \wedge 1 + (x - z_1)z_2 \mid_t z_3,$$

with parameters satisfying $\chi(\vec{y})$ defines $\mathscr{F}$.

Proof. Suppose that $\phi(x; \vec{y}; t)$ and $\chi(\vec{y})$ define a cofinal subfamily of the family $\mathscr{F}$ of all finite subsets of K. Then it is clear from the definition that $\psi(x; \vec{y}, \vec{z}; t)$ with parameters satisfying $\chi(\vec{y})$ defines a subfamily of $\mathscr{F}$. It remains to show that for all finite subsets S there exists parameters $\vec{y}$ and $\vec{z}$ such that $\chi(\vec{y})$ and $\psi(x; \vec{y}, \vec{z}; t)$ defines S.

Let $S = \{k_1, \ldots, k_m\}$ be a finite subset of K. We construct $\vec{y}$ and $\vec{z}$. By the assumption on $\phi(x; \vec{y}, t)$, we can find $\vec{y}$ such that $\chi(\vec{y})$ and $\phi(x; \vec{y}, t)$ defines $\{k_1, \ldots, k_m, \ldots, k_n\}$, with $n \geq m$. Pick z_1 such that $0 \neq k_i' := k_i - z_1$ for all $1 \leq i \leq n$. Using Lemma 5.4.2 we find a non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that for all $h \in \mathfrak{a}$

$$1 + hk_1' \quad \cdots \quad 1 + hk_m' \quad \cdots \quad 1 + hk_n'$$

are pairwise relatively prime elements of $\mathcal{O}_K$. From Lemma 5.4.1 we know that only finitely many $h \in \mathbb{K}$ for which $1 + xyk_i'$ is zero or a unit in $\mathcal{O}_K$ for some i. As $\mathfrak{a}$ is non-zero, we see that $|\mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}| = |\mathcal{O}_{\mathbb{K}}|$ is infinite. Hence we find some non-zero $h \in \mathfrak{a} \cap \mathcal{O}_{\mathbb{K}}$ such that

$$1 + hk_1' \quad \cdots \quad 1 + hk_m' \quad \cdots \quad 1 + hk_n'$$

are non-zero non-unit pairwise relatively prime elements of $\mathcal{O}_K$. Now define $z_2 := h$ and $z_3 := (1 + hk_1') \cdots (1 + hk_m')$.

We show that $\psi(x; \vec{y}, \vec{z}; t)$ defines S. If k satisfies $\psi(x; \vec{y}, \vec{z}, t)$, then $k = k_r$ for some $1 \leq r \leq n$, since k satisfies $\phi(x; \vec{y}, t)$. Furthermore we have that $1 + hk' \mid (1 + hk_1') \cdots (1 + hk_m')$, with $k' = k - z_1$, because $1 + (k - z_1)z_2$ divides z_3 in $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ dividing the proper principal ideal $(1 + hk')$. Such prime $\mathfrak{p}$ exists, since all $1 + hk_i'$ are non-zero non-unit elements of $\mathcal{O}_K$. Then since $\mathfrak{p}$ is prime we find some $1 \leq s \leq m$ such that $\mathfrak{p} \mid (1 + hk_s')$. Using the fact that all $1 + hk_i'$ are pairwise relatively prime, we find that $1 + hk' = 1 + hk_r' = 1 + hk_s'$. Since h is non-zero we conclude that $k = k_s$ with $1 \leq s \leq m$. Conversely it is easy to see that k_i satisfies $\psi(x; \vec{y}, \vec{z}; t)$ for all $1 \leq i \leq m$, which means that $\psi(x; \vec{y}, \vec{z}; t)$ defines S.

We conclude that $\psi(x; \vec{y}, \vec{z}; t)$, with parameters satisfying $\chi(\vec{y})$ defines the family $\mathscr{F}$ of all finite subsets of K. □

Now we are going to show that such a cofinal subfamily is definable. In view of Corollary 5.3.4, we may treat the number field case and the function field case separately. We start with the number field case, which is proven by Robinson [13]. Recall the definition of divisibility in number fields by formula (5.4).

Theorem 5.4.4 (Robinson)**.** *There exists an $\mathcal{L}_{\text{ring}}$-formula $\phi_N(x; y_1, y_2; y_3)$ with parameters satisfying $\chi_N(\vec{y})$ such that if K is a number field, then ϕ_N and χ_N define a cofinal subfamily of the family $\mathscr{F}$ of all finite subsets of K.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\phi_N(x; y_1, y_2, y_3) := (x - y_1)y_2(1 + (x - y_1)y_2) \mid y_3,$$

with parameters satisfying

$$\chi_N(\vec{y}) := y_2, y_3 \neq 0 \wedge \text{int}((x - y_1)y_2) \wedge \text{int}(y_3).$$

Let K be a number field. We first show that $\phi_N(x; \vec{y})$ defines a finite subset of K, whenever $K \models \chi_N(\vec{y})$. Siegel (page 204 and 205 of [15]) proved that if $t \geq 0$ is real and $f(X) \in \mathcal{O}_K[X]$ with at least two distinct roots, then there are finitely many $a \in \mathcal{O}_K$ such that $N_K(f(a)) \leq t$. Notice that $N_K(f(a)) \leq N_K(b)$ implies $f(a) \mid b$. Take $f(X) = X(X + 1)$ and $a = (x - y_1)y_2$. Then f has two distinct roots, and $a \in \mathcal{O}_K$ since $K \models \chi_N(\vec{y})$. Now apply Siegels result to f and a and conclude that there are only finitely many x that satisfy $a(1 + a) \mid y_3$. Thus ϕ_N defines a finite subset.

Let K be a number field and let S be a finite subset K. Pick y_1 such that $x - y_1$ is non-zero for all $x \in S$ and take y_2 such that $(x - y_1)y_2 \in \mathcal{O}_K$. If we take

$$y_3 = \prod_{x \in S} f((x - y_1)y_2),$$

then is it easy to see that $K \models \phi_N(x; y_1, y_2, y_3)$ for all $x \in S$. □

We now show an analogues result for function fields.

Theorem 5.4.5 (Rumely)**.** *There exists an $\mathcal{L}_{\text{ring}}$-formula $\phi_F(x; y_1, y_2; t)$ with parameters satisfying $\chi_F(\vec{y})$ such that if K is a function field and $t \in K$ non-integral, then ϕ_F and χ_F define a cofinal subfamily of the family $\mathscr{F}$ of all finite subsets of K.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\phi_F(x; y_1, y_2; t) := \forall \vec{z}(\text{isval}(\vec{z}) \to (\text{val}(x/y_1; \vec{z}) \vee \text{val}(x/y_2; \vec{z}))),$$

with parameters satisfying $\chi_F(\vec{y}, t) := y_1, y_2 \neq 0$. Let K be a global field with non-integral $t \in K$ and let $\vec{y} \in K^2$ with $K \models \chi_F(\vec{y}, t)$. Suppose that x satisfies $\phi_F(x; \vec{y}; t)$. Then for all $\mathfrak{p}$ we have either $\text{ord}_\mathfrak{p}(x/y_1) \geq 0$ or $\text{ord}_\mathfrak{p}(x/y_2) \geq 0$. Hence $\text{ord}_\mathfrak{p}(x) \geq \min_i \text{ord}_\mathfrak{p}(y_i)$ for all $\mathfrak{p}$. Now consider the adèle $\mathfrak{a}$ such that $\text{ord}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}) = \min_i \text{ord}_\mathfrak{p}(g_i)$ for all $\mathfrak{p}$. Then $\text{ord}_\mathfrak{p}(x) \geq \text{ord}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$ for all $\mathfrak{p}$ and we have $x \in K \cap D(\mathfrak{a})$. From Theorem 2.8.5 we see that $D(\mathfrak{a})$ is compact and from Lemma 2.8.4 we know that K is discrete in $\mathcal{A}_K$. Hence $K \cap D(\mathfrak{a})$ is finite and we conclude that ϕ_F defines a finite subset.

On the other hand let K be a function field and let S be a finite subset of K. Choose y_1 such that $\text{ord}_\mathfrak{p}(y_1) \leq \min_{x \in S} \text{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p}$ with $\min_{x \in S} \text{ord}_\mathfrak{p}(x) < 0$ and then choose y_2 such that $\text{ord}_\mathfrak{p}(y_2) = 0$ for all $\mathfrak{p}$ with $\text{ord}_\mathfrak{p}(y_1) > 0$. We show that $\phi_F(s; \vec{y}; t)$ for all $x \in S$. Let $x_0 \in S$, $\vec{z} \in K^9$ and suppose that $K \not\models \text{val}(x_0/y_1; \vec{z})$. Then $\text{ord}_\mathfrak{p}(x_0) < \text{ord}_\mathfrak{p}(y_1)$ and from the construction of y_1 it follows that $0 \leq \min_{x \in S} \text{ord}_\mathfrak{p}(x)$. Hence, from $x_0 \in S$ we see that $\text{ord}_\mathfrak{p}(y_1) > \text{ord}_\mathfrak{p}(x_0) \geq 0$. The construction of y_2 shows that $\text{ord}_\mathfrak{p}(y_2) = 0$. This implies that $\text{ord}_\mathfrak{p}(x_0/y_2) = \text{ord}_\mathfrak{p}(x_0) \geq 0$, which means that $K \models \text{val}(x_0/y_2; \vec{z})$. Therefore x_0 satisfies ϕ_F. □

If we apply the above theorems to Theorem 5.4.3, we find a tool to quantify over all finite sets.

Theorem 5.4.6. *There exists an $\mathcal{L}_{\text{ring}}$-formula* $\text{set}(x; y_1, \ldots, y_6; t)$ *with parameters satisfying* $\text{isset}(\vec{y})$*, such that if K is a global field and $t \in K$ non-integral, then* set *and* isset *define the family $\mathscr{F}$ of all finite subsets of K.*

Proof. Let ϕ_N and χ_N be the $\mathcal{L}_{\text{ring}}$-formulas from Theorem 5.4.4, let ϕ_N and χ_N be the $\mathcal{L}_{\text{ring}}$-formulas from Theorem 5.4.5 and let χ_0 be the $\mathcal{L}_{\text{ring}}$-sentence from Corollary 5.3.4. Then for every global field K, the $\mathcal{L}_{\text{ring}}$-formula

$$\phi(x; y_1, y_2, y_3; t) := \begin{cases} \phi_N(x; y_1, y_2, y_3) & \text{if } \chi_0 \\ \phi_F(x; y_1, y_2; t) & \text{otherwise} \end{cases}$$

with parameters satisfying

$$\chi(x; y_1, y_2, y_3) := \begin{cases} \chi_N(y_1, y_2, y_3) & \text{if } \chi_0 \\ \chi_F(y_1, y_2) & \text{otherwise} \end{cases}$$

defines a cofinal subfamily of $\mathscr{F}$, where $\mathscr{F}$ is the family of all finite subsets of K. Then Theorem 5.4.3 gives an $\mathcal{L}_{\text{ring}}$-formula $\text{set}(x; y_1, \ldots, y_6; t)$ with parameters satisfying $\text{isset}(\vec{y})$, which satisfies the conditions of the theorem. □

5.5. Model of the natural numbers

In this section we will prove that for every global field, there exist an interpretation from $\mathbb{N}$ to K. Let us first describe the image of this map. Let K be a global field and $t \in K$ be non-integral. Then we define

$$\mathbb{N}_t := \begin{cases} \{0, 1, 2, \ldots\} & \text{if } \text{char}(K) = 0 \\ \{1, t, t^2, \ldots\} & \text{otherwise} \end{cases}$$

Then consider the natural map

$$I_t : \mathbb{N} \to \mathbb{N}_t \qquad n \mapsto \begin{cases} n & \text{if } \text{char}(K) = 0 \\ t^n & \text{otherwise} \end{cases} \tag{5.8}$$

If t is understood we will abbreviate $I_t(n)$ to $\underline{n}$. In this section we will show that I_t is an interpretation.

We first show that the image of I_t is definable.

Lemma 5.5.1. *There exists an $\mathcal{L}_{\text{ring}}$-formula* $\text{nat}(x; t)$ *such that for all global fields K and non-integral $t \in K$,* nat *defines $\mathbb{N}_t$, with*

Proof. Given a global field K and $t \in K$ non-integral. Consider the $\mathcal{L}_{\text{ring}}$-formulas

$$\text{nat}_N(x; t) := \exists \vec{a}(\text{isset}(\vec{a}) \to (\text{set}(0; \vec{a}, t) \wedge \forall y(\text{set}(y; \vec{a}, t) \to (y = x \vee \text{set}(y+1; \vec{a}, t)))))$$

and

$$\text{nat}_F(x; t) := \exists \vec{a}(\text{isset}(\vec{a}) \to (\text{set}(1; \vec{a}, t) \wedge \forall y(\text{set}(y; \vec{a}, t) \to (y = x \vee \text{set}(ty; \vec{a}, t)))))$$

and let χ_0 be an $\mathcal{L}_{\text{ring}}$-sentence such that $K \models \chi_0$ if and only if $\text{char}(K) = 0$. We will show that the $\mathcal{L}_{\text{ring}}$-formula

$$\text{nat}(x; t) := \begin{cases} \text{nat}_N(x) & \text{if } \chi_0 \\ \text{nat}_F(x; t) & \text{otherwise} \end{cases}$$

defines the set $\mathbb{N}_t$.

Let $x \in K$ be arbitrary. If $x \in \mathbb{N}_t$, then it is clear that $K \models \text{nat}(x; t)$, since we can take $\vec{a}$ such that $\text{set}_N(\vec{a}, y)$ defines $\{0, 1, \ldots, x\}$ or $\text{set}_F(\vec{a}, y; t)$ defines $\{1, t, \ldots, x\}$. Conversely suppose that $K \models \text{nat}(x; t)$. If $x \notin \mathbb{N}_t$, then both $\text{set}_N(\vec{a}, y)$ and $\text{set}_F(\vec{a}, y; t)$ define an infinite set, which is impossible. Hence $x \in \mathbb{N}_t$. □

Consider the maps $\oplus, \otimes : \mathbb{N}_t \times \mathbb{N}_t \to \mathbb{N}_t$ defined by

$$\underline{n} \oplus \underline{m} := \underline{n + m}, \qquad \underline{n} \otimes \underline{m} := \underline{n \times m} \tag{5.9}$$

and the binary relation on $\mathbb{N}_t$ defined by

$$\underline{n} \leq \underline{m} \quad \text{if and only if} \quad n \leq m \tag{5.10}$$

We now show that addition, multiplication and the order relation are uniformly $\mathcal{L}_{\text{ring}}$-representable.

Lemma 5.5.2. *There are $\mathcal{L}_{\text{ring}}$-formulas ϕ_+, $\phi_\times$ and $\phi_\leq$ such that for all global fields K and non-integral $t \in K$, ϕ_+, $\phi_\times$ and $\phi_\leq$ represent $\oplus$, $\times$ and $\leq$ respectively.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$ formula

$$\phi_+(y; x_1, x_2) := \begin{cases} y = x_1 + x_2 & \text{if } \chi_0 \\ y = x_1 \times x_2 & \text{otherwise} \end{cases}$$

Then ϕ_+ represents $\oplus$, since

$$\underline{n} \oplus \underline{m} = \begin{cases} n + m & \text{if } \operatorname{char}(K) = 0 \\ t^{n+m} = t^n \times t^m & \text{otherwise} \end{cases}$$

Using Lemma 5.5.1 we find that

$$\phi_\leq(x_1, x_2; t) := \exists y(\operatorname{nat}(y; t) \wedge x_1 + z = x_2)$$

represents the order relation on $\mathbb{N}_t$. Finally, consider the map $f_t : \mathbb{N}_t \to \mathbb{N}_t$ given by $\underline{n} \otimes \underline{n+1}$. Using the fact that n and $n+1$ are coprime for all $n \in \mathbb{N}$, we see that the $\mathcal{L}_{\text{ring}}$-formula

$$\psi(y; x; t) := \forall z(y \mid_t z \leftrightarrow (x \mid_t z \wedge x + 1 \mid_t z))$$

represents f_t. Then the $\mathcal{L}_{\text{ring}}$-formula

$$\phi_\times(y; x_1, x_2; t) := \begin{cases} y = x_1 x_2 & \text{if } \chi_0 \\ f_t(x_1 \oplus x_2) = f_t(x_1) + f_t(x_2) + y + y & \text{otherwise} \end{cases}$$

represents $\otimes$, which concludes the proof of the lemma. □

From Lemma 5.5.1 and Lemma 5.5.2 we conclude that I_t is an interpretation.

Theorem 5.5.3. *If K is a global field, then the map $I_t : \mathbb{N} \to K$ given by equation (5.8) is an interpretation of models.*

If we apply Theorem 3.10.7 and Corollary 3.10.8 to Theorem 5.5.3 we conclude that Question 1 has a negative answer for E_{gf}.

Corollary 5.5.4. *There exists a graded map $\mu : \mathcal{F}_{\mathcal{L}_{\text{arith}}} \to \mathcal{F}_{\mathcal{L}_{\text{ring}}}$ such that for all global fields K, $n \in \mathbb{N}$ and for all $\phi \in \mathcal{F}^n_{\mathcal{L}_{\text{arith}}}$ and all $\vec{m} \in \mathbb{N}^n$*

$$\mathbb{N} \models \phi(\vec{m}) \quad \textit{if and only if} \quad K \models (\mu\phi)(I_t\vec{m})$$

Moreover the theory $\operatorname{Th}(K)$ of a global field K is undecidable.

5.6. The Gödel function

As we have answered Question 1, we will now focus on Question 2 and 3. In this section we will introduce the Gödel function for global fields and show that it is $\mathcal{L}_{\text{ring}}$-representable. This will allow us to make inductive definitions, such as finite sums and products of variable finite length.

We start with the definition of the Gödel function.

Definition 5.6.1 (Gödel functions)**.** Let K be a global field with non-integral $t \in K$ and $n \geq 1$ an integer. A function $F : K^n \times \mathbb{N}_t \to K$ is called a *Gödel function for* K if and only if

1) $F(\vec{x}, \underline{0}) \in \mathbb{N}_t$ for all $\vec{x} \in K^n$;

2) for all $m \in \mathbb{N}$ and $k_1, \ldots, k_m$ in K there exists some $\vec{x} \in K^n$ such that $F(\vec{x}, \underline{0}) = \underline{m}$ and $F(\vec{x}, \underline{i}) = k_i$ for all $1 \leq i \leq m$. △

Gödel functions allow us to represent all finite sequences in $\mathbb{N}_t$. Indeed, $F(\vec{x}, \underline{0})$ defines the length and $F(\vec{x}, \underline{i})$ returns the i-th entry of the sequence defined by $\vec{x}$.

We will show that every global field K admits a Gödel function. We first prove some preliminary results.

Lemma 5.6.2. *Let p be a prime number. Then for each $f \in \mathbb{F}_p[X]$ there exists infinitely many $m \in \mathbb{N}$ such that $f \mid X^{2m} - X^m$.*

Proof. Let g be an irreducible polynomial in $\mathbb{F}_p[X]$ and let L be the splitting field of g over $\mathbb{F}_p$. Note that $L/\mathbb{F}_p$ is algebraic, hence finite. Then L contains p^d elements, where $d = [L : \mathbb{F}_p]$. Thus $|L^\times| = p^d - 1$ and Lagrange theorem shows that every $x \in L^\times$ satisfies $X^{p^d-1} = 1$. Thus if $x \in L$ and $k \in \mathbb{N}$, then satisfies $X^{k(p^d-1)}(X^{k(p^d-1)} - 1) = X^{2m} - X^m = 0$ for $m = k(p^d - 1)$. Since g is irreducible, f is separable. Hence $f \mid X^{2m} - X^m$.

Let f be a polynomial in $\mathbb{F}_p[X]$. Factor f into irreducibles: $f = f_1 \cdots f_n$ and let d be a common multiple of the degrees of the f_i. Then $f_i \mid X^{2m} - X^m$ with $m = p^d - 1$. Now for all $e \in \mathbb{N}$ with $p^e \geq n$ we have that

$$f \;=\; f_1 \cdots f_n \;\mid\; (X^{2m} - X^m)^n \;\mid\; (X^{2m} - X^m)^{p^e} \;=\; X^{2m'} - X^{m'},$$

with $m' = p^e m$. Since d and e do not have an upper bound in $\mathbb{N}$, we conclude that there are infinitely many $m \in \mathbb{N}$ such that $f \mid X^{2m} - X^m$. □

Lemma 5.6.3. *Let K be a global field with non-integral $t \in K$ and let n be a positive integer. Then for all non-zero $k_1, \ldots, k_n \in K$ there exist $h_1, \ldots, h_n \in \mathcal{O}_\mathbb{K}$ such that*

$$\begin{matrix} 1 + h_1k_1 & \cdots & 1 + h_1k_n \\ \vdots & \ddots & \vdots \\ 1 + h_nk_1 & \cdots & 1 + h_nk_n \end{matrix}$$

is a matrix of non-zero non-unit pairwise relatively prime elements of $\mathcal{O}_K$. Moreover if $\mathrm{char}(K) > 0$ then $h_i = t^{2m_i} + t^{m_i}$ for some $m_i \in \mathbb{N}$.

Proof. We will construct the h_s in $\mathcal{O}_\mathbb{K}$ by induction on s. Given $s \in \mathbb{N}$ with $1 \leq s \leq n$ and suppose we have determined $h_1, \ldots, h_{s-1}$ (for $s = 1$ there is no assumption). The construction of h_s consists of three steps.

Using Lemma 5.4.2 we find some $x \in \mathcal{O}_\mathbb{K}$ such that for all $y \in \mathcal{O}_\mathbb{K}$

$$\begin{matrix} 1 + xyk_1 & \cdots & 1 + xyk_n \end{matrix}$$

are non-zero pairwise relatively prime elements of $\mathcal{O}_K$.

Consider the ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that for all $\mathfrak{p}$ with $\mathfrak{p} \mid 1 + h_ik_j$ for some i and j

$$\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) > \max_{i<s,j,j'} \mathrm{ord}_\mathfrak{p}(h_ik_j/xk_{j'}) \tag{5.11}$$

Note that $\mathfrak{a}$ is well-defined, because there are only finitely many primes $\mathfrak{p}$ such that we demand $\mathrm{ord}_\mathfrak{p}(\mathfrak{a}) > 0$. Choose any $y \in \mathfrak{a} \cap \mathcal{O}_\mathbb{K}$, with $y \neq (xk_j)^{-1}$ for all j. Now if there exists a prime $\mathfrak{p}$ and i, j and j' such that $\mathfrak{p} \mid 1 + xyk_{j'}$ and $\mathfrak{p} \mid 1 + h_ik_j$, then $\mathfrak{p} \mid xyk_{j'} - h_ik_j$. Using Lemma 2.5.7 we see that

$$1 \leq \mathrm{ord}_\mathfrak{p}(xyk_{j'} - h_ik_j) = \min\{\mathrm{ord}_\mathfrak{p}(xyk_{j'}), \mathrm{ord}_\mathfrak{p}(h_ik_j)\} = \mathrm{ord}_\mathfrak{p}(h_ik_j),$$

because $\mathrm{ord}_\mathfrak{p}(xyk_{j'}) > \mathrm{ord}_\mathfrak{p}(h_ik_j)$ by equation (5.11). We conclude that $\mathfrak{p} \mid h_ik_j$ and hence $\mathfrak{p} \mid 1$. Therefore, using the induction hypothesis, the whole matrix

$$\begin{matrix} 1 + h_1k_1 & \cdots & 1 + h_1k_n \\ \vdots & \ddots & \vdots \\ 1 + h_{s-1}k_1 & \cdots & 1 + h_{s-1}k_n \\ 1 + xyk_1 & \cdots & 1 + xyk_n \end{matrix}$$

consists of non-zero pairwise relatively prime elements of $\mathcal{O}_K$.

It remains to find $z \in \mathcal{O}_\mathbb{K}$ such that $1 + xyzk_i$ is a non-zero non-unit element of $\mathcal{O}_K$, for all i. Then for $h_s = xyz$, the matrix $(1 + h_ik_j)_{i,j=1}^n$ consists of non-zero non-unit pairwise relatively prime elements of $\mathcal{O}_K$, because $yz \in \mathfrak{a} \cap \mathcal{O}_\mathbb{K}$ with $yz \neq (xk_j)^{-1}$ for all j. Using Lemma 5.4.1 with $x_j = xyk_j \neq 0$ and $y = z$, we find a non-zero polynomial P over $\mathbb{K}$ such that for all $z \in \mathcal{O}_\mathbb{K}$ we have $P(z) = 0$ if and only if $1 + xyzk_j$ is a unit in $\mathcal{O}_K$ for some j. Since P is non-zero, there are at most $\deg(P) < \infty$ elements $z \in \mathcal{O}_\mathbb{K}$ such that $P(z) = 0$. If $\mathrm{char}(K) = 0$, then choose any

$z \in \mathcal{O}_{\mathbb{K}} = \mathbb{Z}$ with $P(z) \neq 0$. If $\mathrm{char}(K) = p > 0$ then Lemma 5.6.2 shows that there are infinitely many $z \in \mathcal{O}_{\mathbb{K}} = \mathbb{F}_p[t]$ such that $xyz = t^{2m} - t^m$ for some $m \in M$. Hence there exist some $z \in \mathbb{F}_p[t]$ such that $P(z) \neq 0$ and $xyz = t^{2m} - t^m$ for some $m \in M$. Now define $h_s := xyz$. This concludes the proof. □

We are now ready to show that every global field admits a Gödel function.

Theorem 5.6.4. *There exists an $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(k, x_1, \ldots, x_9, i; t)$ such that for all global fields K and non-integral $t \in K$, ϕ represents $F_t : K^9 \times \mathbb{N}_t \to K$ which satisfies*

1) *$F_t(\vec{x}, \underline{0}) \in \mathbb{N}_t$ for all $\vec{x} \in K^9$;*
2) *for all $m \in \mathbb{N}$ and $k_1, \ldots, k_m$ in K there exists some $\vec{x} \in K^9$ such that $F_t(\vec{x}, \underline{0}) = \underline{m}$ and $F_t(\vec{x}, \underline{i}) = k_i$ for all $1 \leq i \leq m$.*

Proof. Let χ_0 be the $\mathcal{L}_{\mathrm{ring}}$-formula with $K \models \chi_0$ if and only if $\mathrm{char}(K) = 0$, and let β_t be the push forward of the Gödel bèta function along I_t. Consider the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\rho(h, \vec{n}, i; t) := \begin{cases} h = \beta_t(\vec{n}, i) & \text{if } \chi_0 \\ h = \beta_t(\vec{n}, i)^2 - \beta_t(\vec{n}, i) & \text{otherwise} \end{cases}$$

and let $h_t(\vec{n}, i) : \mathbb{N}_t^3 \to \mathcal{O}_{\mathbb{K}}$ be the function represented by ρ. Now define the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\psi(k, \vec{x}, i; t) := \mathrm{set}(k; x_1, \ldots, x_6; t) \wedge 1 + h_t(x_7, x_8, i)(k - x_4) \mid x_9.$$

We will show that

$$\phi(k, \vec{x}, i; t) := \begin{cases} k = \beta_t(x_7, x_8, \underline{0}) & \text{if } i = \underline{0} \text{ and } \mathrm{nat}(x_7; t) \wedge \mathrm{nat}(x_8; t) \\ k = 0 & \text{if } i = \underline{0} \text{ and } \neg\, \mathrm{nat}(x_7; t) \vee \neg\, \mathrm{nat}(x_8; t) \\ \psi(k, \vec{x}, i; t) & \text{if } i > \underline{0} \text{ and } \exists! k(\psi(k, \vec{x}, i; t)) \\ k = 0 & \text{otherwise} \end{cases}$$

represents a function F_t which satisfies the desired properties.

First notice that this formula defines a function, because for all $\vec{x}$, i and t there is a unique k with $\phi(k, \vec{x}, i; t)$.

The first property is easy, since for all $\vec{x} \in K^9$ we have $F_t(\vec{x}, \underline{0}) = \beta_t(x_7, x_8, \underline{0}) \in \mathbb{N}_t$ if $\mathrm{nat}_t(x_7)$ and $\mathrm{nat}_t(x_8)$ and $F_t(\vec{x}, \underline{0}) = \underline{0} \in \mathbb{N}_t$ otherwise.

For the second property, suppose we are given $m \in \mathbb{N}$ and $k_1, \ldots, k_m$ in K. In view of the proof of Theorem 5.4.6, we may take $x_1, \ldots, x_6 \in K$ such that $\mathrm{set}_t(k; \vec{x})$ defines the set $\{k_1, \ldots, k_m\}$ and $0 \neq k_i' := k_i - x_4$ for all i. Using Lemma 5.6.3 we find for all $1 \leq i \leq m$ natural numbers $m_i \in \mathbb{N}$ such that $(1 + h_i k_j')_{i,j=1}^n$, with

$$h_i := \begin{cases} m_i & \text{if } \chi_0 \\ t^{2m_i} - t^{m_i} & \text{otherwise} \end{cases},$$

is a matrix of non-zero non-unit pairwise relatively prime elements of $\mathcal{O}_K$.

Pick $x_7, x_8 \in K$ such that $F_t(\vec{x}, \underline{0}) := \beta_t(x_7, x_8, \underline{0}) = \underline{m}$ and $\beta(x_7, x_8, \underline{i}) = \underline{m_i}$ for all $1 \leq i \leq n$. Then $h_i = h_t(x_7, x_8, i)$ for all $1 \leq i \leq n$.

Now comes the main trick. Define $x_8 := \prod_{i=1}^n (1 + h_i k_i')$. Then for all $k \in K$ and all $1 \leq i \leq n$ we have that $K \models \psi(k, \vec{x}, i; t)$ if and only if $k = k_i$. The 'if' part is trivial. For the other direction notice that $k = k_s$ for some s and $k - x_4 = k_s' \neq 0$, because $K \models \mathrm{set}_t(k, x_1, \ldots, x_6)$. Since $1 + h_i k_s'$ is neither a zero nor a unit in $\mathcal{O}_K$, we may consider a prime ideal $\mathfrak{p}$ which divides both $(1 + h_i k_s')$ and (x_9). Thus the product x_9 is in $\mathfrak{p}$ and hence some factor $1 + h_j k_j'$ is in $\mathfrak{p}$ or equivalently $\mathfrak{p} \mid (1 + h_j k_j')$ for some j. Now we have $s = j = i$, since $1 + h_i k_s'$ and $1 + h_j k_j'$ are relatively prime otherwise. We conclude that $k = k_s = k_i$, which shows that $F_t(\vec{x}, \underline{i}) = k_i$ □

Theorem 5.6.4 allows us to make inductive definitions. We will list a few examples, which will be used in the next sections.

Corollary 5.6.5. *There exists an $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(x, \omega, \underline{i}; t)$ such that for all global fields K and all non-integral $t \in K$ and all $\underline{i} \in \mathbb{N}_t$ and all $\omega \in K$, ϕ defines ω^i.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\begin{aligned}\phi(x,\omega,\underline{i};t) := \exists\vec{a}(&F_t(\vec{a},\underline{0}) = 1 \wedge F_t(\vec{a},\underline{i}) = x\\ &\wedge \forall k \in \mathbb{N}_t(\underline{1} \leq k \leq \underline{i} \to F_t(\vec{a},k) = \omega \cdot F_t(\vec{a},k \ominus \underline{1}))).\end{aligned}$$

It it clear that ϕ defines ω^i. □

We have a similar result for sums.

Corollary 5.6.6. *Let $\psi(y,x;t)$ be an $\mathcal{L}_{\text{ring}}$-formula such that for all global fields K and all non-integral $t \in K$, ψ represents a function $f : \mathbb{N}_t \to K$. Then there exists an $\mathcal{L}_{\text{ring}}$-formula $\phi(x,i;t)$ such that for all global fields K and all non-integral $t \in K$ and all $i \in \mathbb{N}_t$, ϕ defines $\sum_{k=0}^{i} f(k)$.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\begin{aligned}\phi(x,i;t) := \exists\vec{a}(&\psi(F_t(\vec{a},\underline{0}),\underline{0};t) \wedge \psi(F_t(\vec{a},i),x;t)\\ &\wedge \forall k \in \mathbb{N}_t(\underline{1} \leq k \leq i \to \exists f(\psi(f,k;t) \wedge F_t(\vec{a},k) = f + F_t(\vec{a},k \ominus \underline{1})))).\end{aligned}$$

It it clear that ϕ defines $\sum_{k=0}^{i} f(k)$. □

Corollary 5.6.7. *There exists an $\mathcal{L}_{\text{ring}}$-formula $\phi(y,x,s,t)$ such that for all global fields K with non-integral $s,t \in K$ we have that ϕ represents $I_{s,t} : \mathbb{N}_s \to \mathbb{N}_t$ which satisfies for all $n \in \mathbb{N}$ and all non-integral $s,t \in K$*

1) $I_{s,t} \circ I_s = I_t$, and

2) $I_{s,t} = I_{u,t} \circ I_{s,u}$.

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\begin{aligned}\phi(y,x,s,t) := \exists c\exists\vec{a}\exists n(&\neg\operatorname{int}(c) \wedge \operatorname{nat}(n;c) \wedge F_c(\vec{a},\underline{0}) = F_c(\vec{a},\underline{1}) = \underline{0}\\ &\wedge F_c(\vec{a},\underline{2n}) = x \wedge F_c(\vec{a},\underline{2n+1}) = y\\ &\wedge \forall i \in \mathbb{N}_c(\underline{2} \leq i \leq \underline{2n+1} \to (\\ &(\underline{2} \mid_c i \wedge F_c(\vec{a},i) = s \cdot F_c(\vec{a},i \ominus \underline{2})) \vee\\ &(\underline{2} \nmid_c i \wedge F_c(\vec{a},i) = t \cdot F_c(\vec{a},i \ominus \underline{2})))))\end{aligned}$$

It is clear that ϕ represents $I_{s,t}$ and that $I_{s,t}$ has the required properties. □

5.7. Polynomials over the prime subfield

In this section we will show that there is a partial map $\mathbb{N}_t \to \mathbb{K}[X]$, with $\mathcal{L}_{\text{ring}}$-definable domain A_t, such that the evaluation P_t at $X = \omega$ is a uniformly $\mathcal{L}_{\text{ring}}$-representable function.

Consider the map $\pi : \mathbb{N} \to \mathbb{N}$ that maps n to the $(n+1)$-th prime number and consider for each prime p the map $\operatorname{ord}_p : \mathbb{N} \to \mathbb{N}$ determined by the formula $n = \prod_{p|n} p^{\operatorname{ord}_p(n)}$. Then using Theorem 5.5.4 and the fact that π and ord_p are $\mathcal{L}_{\text{arith}}$-representable, we conclude that the push forwards π_t and $\operatorname{ord}_{p,t}$ of π and ord_p along I_t are uniformly $\mathcal{L}_{\text{ring}}$-representable. Hence using Corollary 5.6.5 and 5.6.6 we find that there is a uniformly $\mathcal{L}_{\text{ring}}$-representable function $P_t : K \times B_t \to K$ given by

$$P_t(\omega,n) := \sum_{i=0}^{n_0} a_t(n_{i+1})\omega^{\underline{i}}, \qquad n_i = \operatorname{ord}_{\pi_t(\underline{i}),t}(n). \tag{5.12}$$

with $B_t := \{n \in \mathbb{N}_t \mid n_{i+1} \in A_t, i = 0,\ldots,n_0\}$.

Enumeration of $\mathbb{K}$. In this paragraph we show that there is an $\mathcal{L}_{\text{ring}}$-representable partial surjective map $a_t : \mathbb{N}_t \to \mathbb{K}$, with $\mathcal{L}_{\text{ring}}$-definable domain A_t. Recall that $\mathbb{F}$ is the prime subfield of K. Then the following theorem provides a general surjection.

Proposition 5.7.1. *For all $n \geq 0$ there exists an $\mathcal{L}_{\text{ring}}$-formula $\phi_n(y,k;t,x_1,\ldots,x_n)$ such that for all global fields K and all non-integral $t_0 \in K$, ϕ represents a surjection $s_t^{\vec{x}} : \mathbb{N}_t \to \mathbb{F}[x_1,\ldots,x_n]$.*

Proof. We construct s_t^n by induction on n. For $n = 0$, consider the function

$$s_t(k) := \begin{cases} (-1)^{k_2} \otimes k_3 & \text{if } \chi_0 \\ \sum_{i=1}^{k} 1 & \text{otherwise} \end{cases},$$

where $k_p = \mathrm{ord}_{p,t}(k)$. If $\mathrm{char}(K) = 0$ then Corollary 3.9.5 and Corollary 5.6.5 show that the first case is uniformly representable. If $\mathrm{char}(K) > 0$ then Corollary 5.6.6 implies that this case is also uniformly representable. Hence s_t^0 is uniformly representable.

Suppose that $s_t^{\vec{x}}$ is uniformly representable. Then define

$$s_t^{\vec{x},x_{n+1}}(k) := \sum_{i=0}^{k_0} s_t^{\vec{x}}(k_{i+1}) \cdot x_{n+1}^i, \qquad k_i = \mathrm{ord}_{\pi_t(\underline{i}),t}(k).$$

Corollary 5.6.5 and 5.6.6 show that s_t^{n+1} is uniformly representable, which proves the theorem. □

This proposition show that there exists an $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(x)$ such that for all global fields K, ϕ defines $\mathbb{F}$. Indeed, the $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(x) := \exists t(\neg \mathrm{int}(t) \wedge \exists i \in \mathbb{N}_t(s_t(i) = x))$ defines $\mathbb{F}$.

Corollary 5.7.2. *There exists an $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(x, i; t)$ such that for all global fields K with non-integral t, ϕ represents a surjective map $q_t : \mathbb{N}_t \to \mathcal{O}_{\mathbb{K}}$.*

Proof. Let χ_0 be the $\mathcal{L}_{\mathrm{ring}}$-sentence such that $K \models \chi_0$ if and only if $\mathrm{char}(K) = 0$. Then the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\phi(x, i; t) := \begin{cases} s_t(i) = x & \text{if } \chi_0 \\ s_t^t(i) = x & \text{otherwise} \end{cases}$$

represents a surjection $q_t : \mathbb{N}_t \to \mathcal{O}_{\mathbb{K}}$. □

As $\mathbb{K} = Q(\mathcal{O}_{\mathbb{K}})$, we are now able to prove that the following:

Theorem 5.7.3. *There exists $\mathcal{L}_{\mathrm{ring}}$-formulas $\phi(x, i; t)$ and $\psi(x; t)$ such that for all global fields K with non-integral t, ψ defines $A_t \subseteq K$, with $A_t \subseteq \mathbb{N}_t$, and ϕ represents a surjective map $a_t : A_t \to \mathbb{K}$.*

Proof. Let $q_t : \mathbb{N}_t \to \mathcal{O}_{\mathbb{K}}$ be the surjection from Corollary 5.7.2. Consider the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\psi(x; t) := q_t(\mathrm{ord}_{3,t}(x)) \neq 0.$$

and the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\phi(x, i; t) := q_t(\mathrm{ord}_{3,t}(i)) \cdot x = q_t(\mathrm{ord}_{2,t}(i)).$$

Then Corollary 5.7.2 shows that ϕ represents a surjective map $a_t : A_t \to \mathbb{K}$. □

From A_t one can easily provide an $\mathcal{L}_{\mathrm{ring}}$-formula that defines B_t. Hence Theorem 5.7.3 shows that P_t from equation (5.12) is uniformly $\mathcal{L}_{\mathrm{ring}}$-representable.

Definability of the degree. If K is a global field, then we have a map $\deg_{\mathbb{K}} : K \to \mathbb{N}$ which maps $x \in K$ to the degree $[\mathbb{K}(x) : \mathbb{K}]$ of x over K. If we compose this map with I_t, we find a map $\deg_{\mathbb{K},t} : K \to \mathbb{N}_t$. In this paragraph we will show that this maps is $\mathcal{L}_{\mathrm{ring}}$-representable.

We will need two preliminary lemmas. Recall from Theorem 5.6.4 the definition of the Gödel function $F_t : K^9 \times \mathbb{N}_t \to K$.

Lemma 5.7.4. *There exists an $\mathcal{L}_{\mathrm{ring}}$-formula $\phi(y, \vec{x}, \omega, \underline{m}; t)$ such that for all global fields K and all non-integral $t \in K$ and all $\omega \in K$, ϕ represents that map*

$$P_t(\vec{x}, \omega, \underline{m}) = \sum_{i=0}^{m} F_t(\vec{x}, \underline{i+1})\omega^i.$$

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\phi(y,\vec{x},\omega,\underline{m};t) := \exists\vec{a}(F_t(\vec{a},\underline{0}) = F_t(\vec{x},\underline{0}) \wedge F_t((\vec{a},\underline{m}) = y \\ \wedge \forall k \in \mathbb{N}_t(\underline{1} \leq k \leq \underline{m} \to F_t(\vec{a},k) = F_t(\vec{x},k \oplus \underline{1})\omega^k + F_t(\vec{a},k \ominus \underline{1}))).$$

It is clear that ϕ represents P_t. □

Lemma 5.7.5. *For all $\mathcal{L}_{\text{ring}}$-formulas ψ there exists an $\mathcal{L}_{\text{ring}}$-formulas $\phi_{\leq}(m;t)$ and $\phi_{\geq}(m;t)$ such that for all global fields K and all non-integral $t \in K$, $\phi_{\leq}$ defines $\min\{n \in \mathbb{N}_t \mid \psi(n)\}$ and $\phi_{\geq}$ defines $\max\{n \in \mathbb{N}_t \mid \psi(n)\}$.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula(s) given by

$$\begin{aligned} \phi_{\leq}(m;t) &:= \psi(m) \wedge \forall n \in \mathbb{N}_t(\psi(n) \to m \leq n) \\ \phi_{\geq}(m;t) &:= \psi(m) \wedge \forall n \in \mathbb{N}_t(\psi(n) \to m \geq n) \end{aligned}$$

It is clear that $\phi_{\leq}$ and $\phi_{\geq}$ define the constants $\min\{n \in \mathbb{N}_t \mid \psi(n)\}$ and $\max\{n \in \mathbb{N}_t \mid \psi(n)\}$. □

Now we are ready to show that $\deg_{\mathbb{K},t}$ is $\mathcal{L}_{\text{ring}}$-representable.

Theorem 5.7.6. *There exists an $\mathcal{L}_{\text{ring}}$-formula $\phi(d,\omega;t)$ such that for all global fields K and all non-integral $t \in K$, ϕ defines $\deg_{\mathbb{K},t} : K \to \mathbb{N}_t$.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\phi(d,\omega;t) := d = \min\{n \in \mathbb{N}_t \mid \exists\vec{a}(P_t(\vec{a},\omega,n) = 0)\}.$$

It is clear that ϕ represents $\deg_{\mathbb{K},t}$. □

As we know from Lemma 5.7.5 that the maximum is $\mathcal{L}_{\text{ring}}$-definable, we have the following corollary.

Corollary 5.7.7. *There exists an $\mathcal{L}_{\text{ring}}$-formula $\phi(d;t)$ such that for all global fields K and all non-integral $t \in K$, ϕ defines $[K : \mathbb{K}]_t$.*

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula $\phi(d;t)$ given by

$$\phi(d;t) := d = \max\{n \in \mathbb{N}_t \mid \exists\omega(n = \deg_{\mathbb{K},t}(\omega))\}$$

We will now show that ϕ defines the constant $[K : \mathbb{K}]_t$. Suppose that $K \models \phi(d;t)$. Since $K/\mathbb{K}$ is seperable, we find by the primitive element theorem an $\omega \in K$ with $K = \mathbb{K}(\omega)$ or equivalently $\deg_{\mathbb{K}}(\omega) = [K : \mathbb{K}]$. Moreover we have that $\deg_{\mathbb{K}}(\omega)$ divides $[K : \mathbb{K}]$ for all $\omega \in K$. Hence $[K : \mathbb{K}]$ is the maximum of all $\deg_{\mathbb{K}}(\omega)$ with $\omega \in K$. □

5.8. Richness of global fields

In this section we will apply the results of the previous sections to the family isomorphism classes of global fields E_{gf}.

Just like algebraically closed fields in chapter 4, we will first determine the isomorphism classes.

Theorem 5.8.1. *Let K be a global field. Then $K = \mathbb{K}(\omega)$ with ω algebraic over $\mathbb{K}$.*

Proof. Note that $K/\mathbb{Q}$ is seperable by Theorem 1.11.9 when $\text{char}(K) = 0$. Furthermore, using Lemma 1 at page 48 of Weil [17], we can choose $t \in K$ such that $K/\mathbb{F}_p(t)$ is separable, whenever $\text{char}(K) > 0$. The theorem follows from the primitive element theorem. □

Interpretation of K in $\mathbb{N}$. Let K be a global field, $t \in K$ be non-integral and $\omega \in K$ such that $K = \mathbb{K}(\omega)$. In this paragraph we will construct an injective map $J_{t,\omega} : K \to \mathbb{N}$ and show that it is a *uniform* interpretation, i.e., there are $\mathcal{L}_{\text{arith}}$-formulas ϕ_+, $\phi_\times$, ϕ_0, ϕ_1, $\phi_=$ and ϕ_{im}, with some parameters $\vec{y}$, which make J_t into an interpretation, and these $\mathcal{L}_{\text{ring}}$-formulas do not depend on K. With Theorem 3.10.7 this gives rise to a map $\lambda : \mathcal{F}^0_{\mathcal{L}_{\text{ring}}} \to \mathcal{F}^n_{\mathcal{L}_{\text{arith}}}$ such that for every global field K and every $\mathcal{L}_{\text{ring}}$-sentence ϕ we have

$$K \models \phi \quad \text{if and only if} \quad \mathbb{N} \models (\lambda\phi)(\vec{y}).$$

The map $J_{t,\omega}$ and the related formulas are constructed in several steps.

Lemma 5.8.2. *There are $\mathcal{L}_{\text{arith}}$-formulas $\phi^1_+(z,x,y;\chi)$, $\phi^1_\times(z,x,y;\chi)$, $\phi^1_0(x;\chi)$, $\phi^1_1(x;\chi)$, $\phi^1_=(x,y;\chi)$ and $\phi^1_{\text{im}}(x;\chi)$ such that if K is a global field with prime subring R, then the map $J^1 : R \to \mathbb{N}$ given by*

$$x \mapsto \begin{cases} 2x-1 & \text{if } \operatorname{char}(K) = 0 \text{ and } x > 0 \\ -2x & \text{if } \operatorname{char}(K) = 0 \text{ and } x \leq 0 \\ y & \text{if } 0 \leq y < p := \operatorname{char}(K) \text{ and } p \mid x - y \end{cases}$$

is an interpretation, by these $\mathcal{L}_{\text{ring}}$-formulas with $\chi = \operatorname{char}(K)$.

Proof. Define $\phi^1_+(z,x,y;\chi)$ by the $\mathcal{L}_{\text{ring}}$-formula

$$\phi^1_+ := \begin{cases} z = 2(\frac{x+1}{2} + \frac{y+1}{2}) - 1 & \text{if } \chi = 0,\ 2 \nmid x \text{ and } 2 \nmid y \\ z = -2(\frac{x}{-2} + \frac{y+1}{2}) & \text{if } \chi = 0,\ 2 \mid x \text{ and } 2 \nmid y \text{ and } \frac{x}{-2} + \frac{y+1}{2} \leq 0 \\ z = 2(\frac{x}{-2} + \frac{y+1}{2}) - 1 & \text{if } \chi = 0,\ 2 \mid x \text{ and } 2 \nmid y \text{ and } \frac{x}{-2} + \frac{y+1}{2} > 0 \\ z = -2(\frac{x+1}{2} + \frac{y}{-2}) & \text{if } \chi = 0,\ 2 \nmid x \text{ and } 2 \mid y \text{ and } \frac{x+1}{2} + \frac{y}{-2} \leq 0 \\ z = 2(\frac{x+1}{2} + \frac{y}{-2}) - 1 & \text{if } \chi = 0,\ 2 \nmid x \text{ and } 2 \mid y \text{ and } \frac{x+1}{2} + \frac{y}{-2} > 0 \\ z = -2(\frac{x}{-2} + \frac{y}{-2}) & \text{if } \chi = 0,\ 2 \mid x \text{ and } 2 \mid y \\ z = x + y - k\chi & \text{if } 0 \leq x + y - k\chi < \chi \text{ for some } k \in \{-1,0,1\} \end{cases}$$

Define $\phi^1_\times$ by the $\mathcal{L}_{\text{ring}}$-formula

$$\phi^1_\times(z,x,y;\chi) := \begin{cases} z = 2(\frac{x+1}{2} \times \frac{y+1}{2}) - 1 & \text{if } \chi = 0,\ 2 \nmid x \text{ and } 2 \nmid y \\ z = -2(\frac{x}{-2} \times \frac{y+1}{2}) & \text{if } \chi = 0,\ 2 \mid x \text{ and } 2 \nmid y \\ z = -2(\frac{x+1}{2} \times \frac{y}{-2}) & \text{if } \chi = 0,\ 2 \nmid x \text{ and } 2 \mid y \\ z = 2(\frac{x}{-2} \times \frac{y}{-2}) - 1 & \text{if } \chi = 0,\ 2 \mid x \text{ and } 2 \mid y \\ z = x \times y - k\chi & \text{if } 0 \leq x \times y - k\chi < \chi \text{ for some } k \in \mathbb{N} \end{cases}$$

Furthermore define $\phi^1_0(x) := x = 0$, $\phi^1_1(x) := x = 1$, $\phi^1_=(x,y;\chi) := x = y$ and

$$\phi^1_{\text{im}}(x;\chi) := \chi > 0 \to 0 \leq x < \chi.$$

It is clear that these $\mathcal{L}_{\text{ring}}$-formulas satisfy the desired properties. □

Lemma 5.8.3. *There are $\mathcal{L}_{\text{arith}}$-formulas $\phi^2_+(z,x,y;\chi)$, $\phi^2_\times(z,x,y;\chi)$, $\phi^2_0(x;\chi)$, $\phi^2_1(x;\chi)$, $\phi^2_=(x,y;\chi)$ and $\phi^2_{\text{im}}(x;\chi)$ such that if K is a global field and $t \in K$ is non-integral, then the map $J^2_t : \mathcal{O}_{\mathbb{K}} \to \mathbb{N}$ given by*

$$x \mapsto \begin{cases} J^1(x) & \text{if } \operatorname{char}(K) = 0 \\ \min\{n \in \mathbb{N} \mid x = \sum_{i=0}^{n_0} I^1(n_{i+1})t^i\} & \text{if } \operatorname{char}(K) > 0 \end{cases}$$

where $n_k = \operatorname{ord}_{\pi(k)}(n)$ for all $k \in \mathbb{N}$ and $I^1 = (J^1)^{-1}$, is an interpretation, by these $\mathcal{L}_{\text{ring}}$-formulas with $\chi = \operatorname{char}(K)$.

Proof. Let $f^1_+ : \mathbb{N}^3 \to \mathbb{N}$ be the function represented by $\phi^1_+(z,x,y;\chi)$. Define

$$\phi^2_+ := \begin{cases} z = f^1_+(x,y;0) & \text{if } \chi = 0 \\ z = \min\{n \in \mathbb{N} \mid n_k = f^1_+(x_k,y_k;\chi), 1 \leq k \leq x_0 + y_0\} & \text{if } \chi > 0 \end{cases}$$

Let $f^1_\times : \mathbb{N}^3 \to \mathbb{N}$ be the function represented by $\phi^1_\times(z,x,y;\chi)$. Define

$$\phi^2_\times := \begin{cases} z = f^1_\times(x,y;0) & \text{if } \chi = 0 \\ z = \min\{n \in \mathbb{N} \mid n_k = \sum_{i=0}^k f^1_+(x_{i+1}, y_{k-i+1};\chi), 1 \le k \le x_0 y_0\} & \text{if } \chi > 0 \end{cases}$$

Define ϕ^2_0 by

$$\phi^2_0(x;\chi) := \begin{cases} x = 0 & \text{if } \chi = 0 \\ x = 1 & \text{if } \chi > 0 \end{cases}$$

Define ϕ^2_1 by

$$\phi^2_1(x;\chi) := \begin{cases} x = 1 & \text{if } \chi = 0 \\ x = 6 & \text{if } \chi > 0 \end{cases}$$

Define $\phi^2_=(x,y;\chi) := x = y$. Finally define ϕ^2_{im} by

$$\phi^2_{\text{im}}(x;\chi) := \begin{cases} \phi^1_{\text{im}}(x;0) & \text{if } \chi = 0 \\ \forall k \phi^1_{\text{im}}(x_{k+1};\chi) \wedge \neg\phi^1_0(x_{x_0+1};\chi)) \wedge \forall k > x_0\ \phi^1_0(x_{k+1};\chi) & \text{if } \chi > 0 \end{cases}$$

where $x_k = \text{ord}_{\pi(k)}(x)$ for all $k \in \mathbb{N}$. It is clear that these $\mathcal{L}_{\text{ring}}$-formulas satisfy the desired properties. □

Lemma 5.8.4. *There are $\mathcal{L}_{\text{arith}}$-formulas $\phi^3_+(z,x,y;\chi)$, $\phi^3_\times(z,x,y;\chi)$, $\phi^3_0(x;\chi)$, $\phi^3_1(x;\chi)$, $\phi^3_=(x,y;\chi)$ and $\phi^3_{\text{im}}(x;\chi)$ such that if K is a global field and $t \in K$ is non-integral, then the map $J^3_t : \mathbb{K} \to \mathbb{N}$ given by*

$$x \mapsto \min\{n \in \mathbb{N} \mid x = I^2_t(n_0)/I^2_t(n_1)\}$$

where $n_k = \text{ord}_{\pi(k)}(n)$ for all $k \in \mathbb{N}$ and $I^2_t = (J^2_t)^{-1}$, is an interpretation, by these $\mathcal{L}_{\text{ring}}$-formulas with $\chi = \text{char}(K)$.

Proof. For all $n,k \in \mathbb{N}$, we write $n_k := \text{ord}_{\pi(k)}(n)$. Let $+^2_\chi$ be the relation represented by $\phi^2_+(z,x,y;\chi)$ and $\times^2_\chi$ be the relation represented by $\phi^2_\times(z,x,y;\chi)$. Define for $\square = +, \times$ the $\mathcal{L}_{\text{ring}}$-formula

$$\phi^3_\square := z = \min\{n \in \mathbb{N} \mid \psi_\square(n,x,y;\chi)\},$$

where

$$\psi_+(n,x,y;\chi) := n_0 \times^2_\chi x_1 \times^2_\chi y_1 = n_1 \times^2_\chi (x_0 \times^2_\chi y_1 +^2_\chi x_1 \times^2_\chi y_0)$$

and

$$\psi_\times(n,x,y;\chi) := n_0 \times^2_\chi x_1 \times^2_\chi y_1 = n_1 \times^2_\chi x_0 \times^2_\chi y_0$$

Furthermore define $\phi^3_0(x;\chi) := \phi^2_0(x_0,\chi)$ and $\phi^3_1(x;\chi) := \phi^2_1(x_0,\chi) \wedge \phi^2_1(x_1,\chi)$ and $\phi^3_=(x,y;\chi) := x = y$. Finally we define

$$\phi^3_{\text{im}}(x;\chi) := \phi^2_{\text{im}}(x_0;\chi) \wedge \phi^2_{\text{im}}(x_1;\chi) \wedge \neg\phi^2_0(x_1,\chi) \wedge \theta,$$

with

$$\theta := \forall n(n \le x \wedge n_0 \times^2_\chi x_1 = n_1 \times^2_\chi x_0 \to n = x).$$

It is clear that these $\mathcal{L}_{\text{ring}}$-formulas satisfy the desired properties. □

The following proposition encodes all polynomials over $\mathbb{K}$:

Proposition 5.8.5. *There are $\mathcal{L}_{\text{arith}}$-formulas $\phi^4_+(z,x,y;\chi)$, $\phi^4_\times(z,x,y;\chi)$, $\phi^4_0(x;\chi)$, $\phi^4_1(x;\chi)$, $\phi^4_=(x,y;\chi)$ and $\phi^4_{\text{im}}(x;\chi)$ such that if K is a global field and $t \in K$ is non-integral, then the map $J^4_t : \mathbb{K}[X] \to \mathbb{N}$ given by*

$$x \mapsto \min\{n \in \mathbb{N} \mid x = \sum_{i=0}^{n_0} I^3_t(n_{i+1}) X^i\}$$

with $n_k = \text{ord}_{\pi(k)}(n)$ for all $k \in \mathbb{N}$ and $I^3_t = (J^3_t)^{-1}$, is an interpretation, by these $\mathcal{L}_{\text{ring}}$-formulas with $\chi = \text{char}(K)$.

Proof. For all $n, k \in \mathbb{N}$, we write $n_k := \mathrm{ord}_{\pi(k)}(n)$. Let $+^3_\chi$ be the relation represented by $\phi^3_+(z,x,y;\chi)$ and $\times^3_\chi$ be the relation represented by $\phi^3_\times(z,x,y;\chi)$. Define for $\square = +, \times$ the $\mathcal{L}_{\mathrm{ring}}$-formula where

$$\psi_\square(n,x,y;\chi) := \forall k(1 \leq k \leq x_0 + y_0 \to n_k = x_k +^3_\chi y_k)$$

and

$$\psi_\times(n,x,y;\chi) := \forall k(1 \leq k \leq x_0 y_0 \to n_k = \sum_{i=0}^{k} x_{i+1} \times^3_\chi y_{k-i+1})$$

Furthermore define $\phi^4_0(x;\chi) := \forall k \phi^3_0(x_k,\chi)$, $\phi^4_=(x,y;\chi) := x = y$ and

$$\phi^4_1(x;\chi) := \phi^2_1(x_1,\chi) \wedge \forall k(k \neq 1 \to \phi^3_0(x_k,\chi)).$$

Finally we define

$$\phi^4_{\mathrm{im}}(x;\chi) := \forall k \phi^3_{\mathrm{im}}(x_{k+1};\chi) \wedge \neg\phi^3_0(x_{x_0+1};\chi)) \wedge \forall k > x_0\ \phi^3_0(x_{k+1};\chi).$$

It is clear that these $\mathcal{L}_{\mathrm{ring}}$-formulas satisfy the desired properties. □

Using the encoding of all polynomials over $\mathbb{K}$, we can now construct an encoding of the factor ring $K \cong \mathbb{K}[X]/(f)$, where f is the minimal polynomial of a primitive element $\omega \in K$. But in order to provide an $\mathcal{L}_{\mathrm{ring}}$-representation of the push-forwards of addition and multiplication, we will need to know the code g of f.

Proposition 5.8.6. *There are $\mathcal{L}_{\mathrm{arith}}$-formulas $\phi_+(z,x,y;\chi,g)$, $\phi_\times(z,x,y;\chi,g)$, $\phi_0(x;\chi,g)$, $\phi_1(x;\chi,g)$, $\phi_=(x,y;\chi,g)$ and $\phi_{\mathrm{im}}(x;\chi,g)$ such that if K is a global field, $t \in K$ is non-integral and $\omega \in K$ with $K = \mathbb{K}(\omega)$, then the map $J_{t,\omega} : K \to \mathbb{N}$ given by*

$$x \mapsto \min\{n \in \mathbb{N} \mid x = \sum_{i=0}^{n_0} I^3_t(n_{i+1})\omega^i\}$$

with $n_k = \mathrm{ord}_{\pi(k)}(n)$ for all $k \in \mathbb{N}$ and $I^3_t = (J^3_t)^{-1}$, is an interpretation, with $\chi = \mathrm{char}(K)$ and $g = J^4_t(f^\omega)$.

Proof. For all $n, k \in \mathbb{N}$, we write $n_k := \mathrm{ord}_{\pi(k)}(n)$. Let $+^4_\chi$ be the relation represented by $\phi^4_+(z,x,y;\chi)$ and $\times^4_\chi$ be the relation represented by $\phi^4_\times(z,x,y;\chi)$. Define for $\square = +, \times$ the $\mathcal{L}_{\mathrm{ring}}$-formula

$$\phi^2_\square := z = \min\{n \in \mathbb{N} \mid \psi_\square(n,x,y;\chi,g)\},$$

where

$$\psi_\square(n,x,y;\chi,g) := \exists h(n = x \square^4_\chi x +^4_\chi h \times^4_\chi g).$$

Furthermore define $\phi_0(x;\chi) := \phi^4_0(x,\chi)$ and $\phi_1(x;\chi) := \phi^4_1(x,\chi)$ and $\phi_=(x,y;\chi) := x = y$. Finally we define

$$\phi_{\mathrm{im}}(x;\chi,g) := \forall n(n \leq x \wedge \exists h(n = x +^4_\chi h \times^4_\chi g) \to n = x)$$

It is clear that these $\mathcal{L}_{\mathrm{ring}}$-formulas satisfy the desired properties. □

If we apply Theorem 3.10.7 to Proposition 5.8.6 we conclude the following:

Theorem 5.8.7. *There exists a map $\lambda : \mathcal{F}^0_{\mathcal{L}_{\mathrm{ring}}} \to \mathcal{F}^2_{\mathcal{L}_{\mathrm{arith}}}$ such that for every global field K and every $\mathcal{L}_{\mathrm{ring}}$-sentence ϕ we have*

$$K \models \phi \quad \text{if and only if} \quad \mathbb{N} \models (\lambda\phi)(\chi, g),$$

with $\chi = \mathrm{char}(K)$ and $g = J^4_t(f)$ where $f \in \mathbb{K}[X]$ such that $K \cong \mathbb{K}[X]/(f)$.

Code of a global field. In this paragraph we will assign to every global field K a natural number $\ulcorner K \urcorner \in \mathbb{N}$ with the following properties:

1) there is an $\mathcal{L}_{\text{ring}}$-formula $\text{code}(x;t)$ such that if K is a global field and $t \in K$ non-integral, then $\text{code}(x,t)$ defines $I_t(\ulcorner K \urcorner) \in K$;

2) there is an $\mathcal{L}_{\text{arith}}$-formula $\text{char}(x,y)$ such that if K is a global field, then $\mathbb{N} \models \text{char}(\chi, \ulcorner K \urcorner)$ if and only if K has characteristic χ, for all $\chi \in \mathbb{N}$;

3) there is an $\mathcal{L}_{\text{arith}}$-formula $\text{gen}(x,y;t)$ such that if K is a global field and $t \in K$ is non-integral, then $\mathbb{N} \models \text{gen}(g, \ulcorner K \urcorner; t)$ if and only if $J_t^4(f) = g$, for some $f \in \mathbb{K}[X]$ such that $K \cong \mathbb{K}[X]/(f)$.

We will first define a constant $\text{char}(t) \in \mathbb{N}_t$, such that for all $p \in \mathbb{N}$

$$K \models \exists t(\neg \text{int}(t) \wedge I_t(p) = \text{char}(t))$$

if and only if $\text{char}(K) = p$. It is easy to see that

$$\phi(x,t) := \begin{cases} x = 0 & \text{if } \chi_0 \\ x = \min\{n \in \mathbb{N}_t \mid n = 0\} & \text{otherwise} \end{cases}$$

defines this constant.

Recall that we can enumerate the polynomials over $\mathbb{K}$ using P_t from (5.12). Hence we can define the minimal polynomial over $\mathbb{K}$ of a given $\omega \in K$ by the $\mathcal{L}_{\text{ring}}$-formula

$$\text{minpol}(\omega, n; t) := P_t(\omega, n) = 0 \wedge \text{ord}_{2,t}(n) = \deg_{\mathbb{K},t}(\omega), \tag{5.13}$$

which defines a subset of $K \times B_t$ of pairs (ω, n), such that n is the code of a minimal polynomial of ω. Recall from Corollary 5.6.7 the definition of the map $I_{t,s}$ and consider the $\mathcal{L}_{\text{ring}}$-formula

$$\begin{aligned} \text{genpol}(n;t) := \neg n \in B_t \wedge \exists s \exists \omega(\neg \text{int}(s) \wedge \deg_{\mathbb{K},s}(\omega) = [K:\mathbb{K}]_s \\ \wedge \text{minpol}(\omega, I_{t,s}(n)); s). \end{aligned} \tag{5.14}$$

Then $K \models \text{genpol}(n;t)$ if and only if n encodes the minimal polynomial of a generating (i.e., primitive) element of $K/\mathbb{K}$. Therefore we can define the following:

Definition 5.8.8 (Coding of global fields)**.** The map $\ulcorner \cdot \urcorner : E_{\text{gf}} \to \mathbb{N}$ defined by $\ulcorner e \urcorner = m$ if and only if for all primes p with $p \mid m$ we have $p = 2, 3$ and for some $K \in e$

$$K \models \exists t(\neg \text{int}(t) \wedge I_t(m_0) = \text{char}(t) \wedge I_t(m_1) = \min\{n \in \mathbb{N}_t \mid \text{genpol}(n;t)\})$$

is called the *coding of global fields.* △

For notational convenience we will write $\ulcorner K \urcorner$ instead of $\ulcorner [K] \urcorner$. We now show that $\ulcorner e \urcorner$ is well-defined. First of all, if K and K' are isomorphic, then they are elementary equivalent. Therefore the definition does not depend on the choice of K in e. Furthermore notice that $K \models \text{genpol}(n;t)$ if and only if $\text{genpol}(I_{t,t'}(n); t')$, for all non-integral $t, t' \in K$, because $I_{t,s}(n) = I_{t',s}(I_{t,t'}(n))$ by Corollary 5.6.7. Now using that $I_{t'}(m) = I_{t,t'}(I_t(m))$, we conclude that m does not depend on the choice of t.

The reason that we have defined the coding $\ulcorner \cdot \urcorner$ in this way is because there is now a uniform definition of $\ulcorner K \urcorner$ in a global field K.

Lemma 5.8.9. *There is an $\mathcal{L}_{\text{ring}}$-formula $\text{code}(x;t)$ such that if K is a global field, then*

$$K \models \forall x(\text{code}(x;t) \leftrightarrow x = I_t(\ulcorner K \urcorner)).$$

Proof. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\text{code}(x;t) := x = \min\{n \in \mathbb{N}_t \mid \text{genpol}(n;t)\}.$$

It is clear from the definition that $\phi(x)$ defines $I_t(\ulcorner K \urcorner)$. □

It is easy to see that we have reached the goal of this section, since we can define $\text{char}(x,y) := x = y_0$ and $\text{gen}(x,y;t) := x = y_1$.

Characterization of definable subsets. The following theorem characterizes completely the definable subsets of E_{gf}. This provides an answer to Question 2 in the case of global fields.

Theorem 5.8.10. *Let $S \subseteq E_{\mathrm{gf}}$ be a set of isomorphism classes of global fields. Then there exists an $\mathcal{L}_{\mathrm{ring}}$-sentence ϕ with $S = \{e \in E_{\mathrm{gf}} \mid e \models \phi\}$ if and only if there exists an $\mathcal{L}_{\mathrm{arith}}$-formula $\psi(x)$ with $S = \{e \in E_{\mathrm{gf}} \mid \mathbb{N} \models \psi(\lceil e \rceil)\}$.*

Proof. Let $S \subseteq E_{\mathrm{gf}}$ be a set of isomorphism classes of global fields. Suppose that there exists an $\mathcal{L}_{\mathrm{arith}}$-formula $\psi(x)$ with $S = \{e \in E_{\mathrm{gf}} \mid \mathbb{N} \models \psi(\lceil e \rceil)\}$. Then let μ be the uniform interpretation of $\mathrm{Th}(\mathbb{N})$ in the theory of global fields from Corollary 5.5.4. Then it is clear that

$$\phi := \exists t \exists m(\neg \operatorname{int}(t) \wedge \operatorname{code}(m; t) \wedge (\mu\psi)(m))$$

is an $\mathcal{L}_{\mathrm{ring}}$-sentence such that $S = \{e \in E_{\mathrm{gf}} \mid e \models \phi\}$.

On the other hand, let λ be the map from Theorem 5.8.7. Then

$$\psi(x) := (\lambda\phi)(x_0, x_1)$$

is an $\mathcal{L}_{\mathrm{arith}}$-formula $\psi(x)$ with $S = \{e \in E_{\mathrm{gf}} \mid \mathbb{N} \models \psi(\lceil e \rceil)\}$. □

The strength of Theorem 5.8.10 becomes clear by its corollaries.

Corollary 5.8.11. *For all global fields K there is a sentence ϕ_K which is true in K and false for all global fields L with $L \ncong K$.*

Proof. Let K be a global field and consider the $\mathcal{L}_{\mathrm{arith}}$-formula

$$\psi(x) := x = 1 + \cdots + 1 \qquad (\lceil K \rceil \text{ times}).$$

Then application of Theorem 5.8.10 yields an $\mathcal{L}_{\mathrm{ring}}$-sentence ϕ_K, which is true for K and false for every global fields L with $L \ncong K$. □

Thus Corollary 5.8.11 shows that every global field is definable by a single $\mathcal{L}_{\mathrm{ring}}$-sentence. This implies that two global fields are isomorphic whenever their theories are equal (i.e., whenever they are elementary equivalent). This provides a positive answer to Question 3.

Corollary 5.8.12. *For all global fields K and L we have that $K \equiv L$ if and only if $K \cong L$.*

Proof. Let K and L be global fields. If $K \cong L$ then clearly $K \equiv L$. Conversely suppose that $K \equiv L$ and let ϕ_K be the $\mathcal{L}_{\mathrm{ring}}$-sentence from Corollary 5.8.11. Then $L \models \phi_K$, hence $L \cong K$. □

Chapter 6

Finitely Generated Fields

Let K be a field and $\mathbb{F}$ its prime subfield. If $K/\mathbb{F}$ is finitely generated, then K is called a *finitely generated field*. Let E_{ifgf} denote the set of all isomorphism classes of infinite finitely generated fields. Note that we will consider only finitely generated fields which are infinite, as then we are able to reduce global fields. In this chapter we will provide a negative answer to Question 1 with $E = E_{\text{ifgf}}$.

To achieve this, we show that for every infinite finitely generated field K there exists an interpretation from $\mathbb{N}$ to K. Just as with the interpretation of $\mathbb{N}$ into a global field, the hardest part is to show that the image is definable. We will prove this by reducing to global fields using results from Poonen [11]. These will be discussed in section 6.1. Then in section 6.2 we conclude that Question 1 has a negative answer.

The answer of Question 2 and 3 is not yet known in the case of infinite finitely generated fields.

6.1. Reduction to global fields

In this section we will show that there exists an $\mathcal{L}_{\text{ring}}$-formula that defines a global field inside every infinite finitely generated field K. We will first describe this global field and then show that it is definable, using results of Poonen [11].

We first extend our notations about global fields from section 2.1. Let K be a infinite finitely generated field. Then $t \in K$ is called *integral* if and only if t is integral over the prime subring of K. For every non-integral $t \in K$ define

$$\mathcal{O}_{\mathbb{K}} := \begin{cases} \mathbb{Z} & \text{if } \operatorname{char}(K) = 0 \\ \mathbb{F}_p[t] & \text{if } \operatorname{char}(K) = p > 0 \end{cases} \tag{6.1}$$

Then define K_t to be the algebraic closure $\mathbb{K} = Q(\mathcal{O}_{\mathbb{K}})$ in K. It is clear that K_t is a global field, as it is finitely generated over the prime subfield and has Kronecker dimension one. We will provide a first order definition of K_t in K.

Characteristic zero. If K is an infinite finitely generated field, then the algebraic closure k of $\mathbb{F}$ in K is called the *field of constants*. Notice that if $\operatorname{char}(K) = 0$, then $\mathbb{F} = \mathbb{K}$ and $k = K_t$ is a global field. Hence the following theorem allows us to define K_t in characteristic zero.

Theorem 6.1.1 (Poonen)**.** *There exists a $\mathcal{L}_{\text{ring}}$-formula $\phi(x)$ such that for all finitely generated fields K with field of constants k we have*

$$\{x \in K \mid K \models \phi(x)\} \;=\; \begin{cases} k & \text{if } \operatorname{char}(K) = 0 \\ \emptyset & \text{otherwise} \end{cases}$$

Proof. See Lemma 3.7 of [11]. □

Poonen proved (proof of Theorem 1.1 on page 15 of [11]), using the theory from Chapter 5, that the above theorems implies that characteristic zero is definable. However, the proof could be much easier.

Corollary 6.1.2. *There exists an $\mathcal{L}_{\text{ring}}$-sentence χ_0 such that $K \models \chi_0$ if and only if $\text{char}(K) = 0$ for all infinite finitely generated fields.*

Proof. Let $\phi(x)$ be the $\mathcal{L}_{\text{ring}}$-formula from Theorem 6.1.1 and consider the $\mathcal{L}_{\text{ring}}$-sentence $\chi_0 := \exists x \phi(x)$. It is clear that $K \models \chi_0$ if and only if $\text{char}(K) = 0$. □

This corollary generalizes Corollary 5.3.4. Hence we are now able to separate positive characteristic from characteristic zero.

Positive characteristic. Let K be an infinite finitely generate field. We will now show that K_t is definable in positive characteristic. It clearly suffices to show that the family

$$\mathscr{F}_K := \{K_t \mid t \text{ non-integral}\} \tag{6.2}$$

is $\mathcal{L}_{\text{ring}}$-definable, whenever $\text{char}(K) > 0$.

We first investigate some basic properties of $\mathscr{F}$.

Lemma 6.1.3. *Let K be an infinite finitely generate field with $\text{char}(K) > 0$ and let $s, t \in K$ be non-integral. If $t \in K_s$, then $K_s = K_t$.*

Proof. Suppose that $t \in K_s$. Then we have $K_s \cap K_t \neq k$, where k is the field of constants of K. Since K_s and K_t are algebraically closed in K we find that $k \subseteq K_s \cap K_t$. Thus there exists some non-integral $x \in K$ with $x \in K_s \cap K_t$. This implies that $\mathbb{F}[x] \subseteq K_s \cap K_t$ and since K_s and K_t are algebraically closed in K we find that K_s and K_t both equal the relative integral closure of $\mathbb{F}[x]$ in K. Hence $K_s = K_x = K_t$. □

Theorem 6.1.4 (Poonen)**.** *There exists $\mathcal{L}_{\text{ring}}$-formulas $\phi(x; \vec{y})$ and $\chi(\vec{y})$ such that if K is an infinite finitely generated field with $\text{char}(K) > 0$, then ϕ and χ define $\mathscr{F}_K$.*

Proof. We claim that $F \in \mathscr{F}_K$ if and only if F is algebraically closed in K and $\text{trdeg}(F/k) = 1$. Then Proposition 4.10 of [11] proves the theorem.

If $F = K_t$, for some non-integral $t \in K$, then by definition F is algebraically closed and $\text{trdeg}(F/k) = 1$. Conversely suppose that $F \subseteq K$ is a subfield such that F is algebraically closed in K and $\text{trdeg}(F/k) = 1$. Pick $t \in K - k$ non-integral. Then from the uniqueness of the relative algebraic closure it follows that F equals the relative algebraic closure of $\mathbb{F}_p[t]$, where $p = \text{char}(K) > 0$. Hence $F = K_t$. □

We are now ready to show that K_t is $\mathcal{L}_{\text{ring}}$-definable.

Corollary 6.1.5. *There exists an $\mathcal{L}_{\text{ring}}$-formula $\text{gf}(x; t)$ such that if K is an infinite finitely generated field and $t \in K$ is non-integral, then* gf *defines K_t.*

Proof. Let $\phi(x)$ be the $\mathcal{L}_{\text{ring}}$-formula from Theorem 6.1.1, χ_0 the $\mathcal{L}_{\text{ring}}$-sentence from Corollary 6.1.2, $\psi(x; \vec{y})$ and $\chi(\vec{y})$ the $\mathcal{L}_{\text{ring}}$-formulas from Theorem 6.1.4. Consider the $\mathcal{L}_{\text{ring}}$-formula

$$\text{gf}(x; t) := \begin{cases} \phi(x) & \text{if } \chi_0 \\ \forall \vec{y}(\chi(\vec{y}) \to (\psi(x; \vec{y}) \to \psi(t; \vec{y}))) & \text{otherwise} \end{cases}$$

If $\text{char}(K) = 0$, then Theorem 6.1.1 shows that gf defines K_t. If $\text{char}(K) > 0$, then Theorem 6.1.4 shows that gf defines $\bigcup\{K_s \mid t \in K_s\}$. Then Lemma 6.1.3 shows that gf defines K_t. □

6.2. Richness of finitely generated fields

Let us first describe the image of this map. Let K be an infinite finitely generated field and $t \in K$ be non-constant. Then we define the map

$$I_t : \mathbb{N} \to K \qquad n \mapsto \begin{cases} n & \text{if } \text{char}(K) = 0 \\ t^n & \text{otherwise} \end{cases} \tag{6.3}$$

We will prove that I_t is an interpretation.

Lemma 6.2.1. *Let K be an infinite finitely generated field and $t \in K$ be non-integral. Then there exists a graded map $\mu : \mathcal{F}_{\mathcal{L}_{\text{ring}}} \to \mathcal{F}_{\mathcal{L}_{\text{ring}}}$ such that for all $n \in \mathbb{N}$ and for all $\phi \in \mathcal{F}^n_{\mathcal{L}_{\text{ring}}}$ and all $\vec{m} \in K_t^n$*

$$K_t \models \phi(\vec{m}) \quad \textit{if and only if} \quad K \models (\mu\phi)(\vec{m})$$

Proof. Let $\iota : K_t \to K$ be the inclusion of K_t in K. Then Corollary 6.1.5 shows that the image of ι is definable. Hence $\iota : K_t \to K$ is an interpretation of models, since addition and multiplication are trivially $\mathcal{L}_{\text{ring}}$-representable. The lemma now follows from Theorem 3.10.7. □

Theorem 6.2.2. *Let K be an infinite finitely generated field and $t \in K$ be non-integral. Then the map $I_t : \mathbb{N} \to K$ given by equation (6.3) is an interpretation of models.*

Proof. Notice that I_t factors through a map $I'_t : \mathbb{N} \to K_t$ and the inclusion $\iota : K_t \subseteq K$. Now let $\mu : \mathcal{F}_{\mathcal{L}_{\text{ring}}} \to \mathcal{F}_{\mathcal{L}_{\text{ring}}}$ be the map from Lemma 6.2.1. Then $\mu\,\text{nat}(x;t)$ defines the image of J_t in K. Using $\mu\,\text{rin}(x;t)$ instead of $\text{rin}(x;t)$ shows that divisibility $|_t$ is $\mathcal{L}_{\text{ring}}$-representable in K. Hence the proof of Lemma 5.5.2 also applies to infinite finitely generated fields. Thus I_t is an interpretation. □

If we apply Theorem 3.10.7 and Corollary 3.10.8 to Theorem 6.2.2 we conclude that Question 1 has a negative answer for E_{ifgf}.

Corollary 6.2.3. *The theory* $\text{Th}(K)$ *of an infinite finitely generated field K is undecidable.*

Question 2 and 3 will remain unanswered in this thesis. At the time of writing, they are open questions in this field of mathematics.

Pop showed some strong evidence that Question 3 should have a positive answer. He showed in [12] that if K and L are finitely generated fields with $\text{Th}(K) = \text{Th}(L)$ and K is a function field of general type then K is isomorphic to L. He furthermore shows that the set of isomorphism classes of global fields is a definable subset of E_{ifgf}.

Bibliography

[1] F. Beukers. Rings and galois theory, 2012. Available at `http://www.staff.science.uu.nl/~beuke106/ringengalois/dic.pdf`.

[2] George S. Boolos, John P. Burgess, and Richard C. Jeffrey. *Computability and logic*. Cambridge University Press, Cambridge, fifth edition, 2007.

[3] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, 1969.

[4] László Fuchs and Luigi Salce. *Modules over non-Noetherian domains*, volume 84 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2001. Available at `books.google.nl/books?isbn=0821819631`.

[5] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[6] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[7] H. W. Lenstra, Jr. and P. Stevenhagen. Artin reciprocity and Mersenne primes. *Nieuw Arch. Wiskd. (5)*, 1(1):44–54, 2000.

[8] J.S. Milne. Class field theory (v4.02), 2013. Available at `http://www.jmilne.org/math/`.

[9] I. Moerdijk and J. van Oosten. Sets, models and proofs, 2011. Available at `http://www.staff.science.uu.nl/~ooste110/syllabi/setsproofs09.pdf`.

[10] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[11] Bjorn Poonen. Uniform first-order definitions in finitely generated fields. *Duke Math. J.*, 138(1):1–22, 2007.

[12] Florian Pop. Elementary equivalence versus isomorphism. *Invent. Math.*, 150(2):385–408, 2002.

[13] Julia Robinson. On the decision problem for algebraic rings. In *Studies in mathematical analysis and related topics*, pages 297–304. Stanford Univ. Press, Stanford, Calif, 1962.

[14] R. S. Rumely. Undecidability and definability for the theory of global fields. *Trans. Amer. Math. Soc.*, 262(1):195–217, 1980.

[15] Carl Siegel. Approximation algebraischer Zahlen. *Math. Z.*, 10(3-4):173–213, 1921.

[16] P. Stevenhagen. Voortgezette getaltheorie, 2002. Available at `http://websites.math.leidenuniv.nl/algebra/localfields.pdf`.

[17] André Weil. *Basic number theory*. Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

List of Symbols

Index