Universiteit
Antwerpen

Masterproef scriptie

Diophantine definability in number fields and their rings of integers

Auteur: *Nicolas Daans*

Promotor: *Prof. Dr. Karim Johannes Becher*

Datum: 24 mei 2018
Academiejaar 2017-2018

Contents

Introduction

In 1900, David Hilbert formulated the following problem, now known as Hilbert's 10th problem [Hil00].

> Eine Diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Or in English [Hil02]:

> Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Presumably, Hilbert asked for a decision algorithm which has a polynomial $f \in \mathbb{Z}[X_1, X_2, \ldots]$ as input and outputs 1 if the polynomial has a root over $\mathbb{Z}$ and 0 otherwise. In principle his formulation still allows this algorithm to depend on f, for example on the number of variables occurring in f or the total degree of f. In 1970, Yuri Matiyasevich - building on work by Martin Davis, Hilary Putnam and Julia Robinson - showed that such an algorithm cannot exist, not even when fixing the degree and number of variables of f. [Mat70]

We can generalise this problem to an arbitrary commutative ring R.

Question (Hilbert's 10th problem for R)**.** *Can we find a decision algorithm which receives as input a polynomial $f \in \mathbb{Z}[X_1, X_2, \ldots]$ and outputs 1 if the polynomial has a root in $R^{\mathbb{N}}$ and 0 otherwise?*

To tackle this problem, definable sets often play a crucial role. Given a ring R and a subset S, we can ask whether there is a first-order formula in the language of rings such that the elements of S are precisely the elements of R satisfying this formula. By such a formula we mean a meaningful finite combination of the logical symbols $\forall, \exists, \neg, \wedge, \vee, (,), =, \leftrightarrow, \rightarrow$, variable symbols $t, x_1, x_2, x_3, \ldots$ and the algebraic symbols $+, -, \cdot, 0, 1$ with their usual interpretation. For example, the elements of $\mathbb{R}$ lying in $[0, \sqrt{2}]$ are given as the set of $t \in \mathbb{R}$ for which the following formula holds:

$$\exists x_1, x_2 (t = x_1 \cdot x_1 \wedge (1 + 1) - (t \cdot t) = x_2 \cdot x_2).$$

We say that the set $[0, \sqrt{2}]$ is *definable* in $\mathbb{R}$ and that the formula above *defines* $[0, \sqrt{2}]$ in $\mathbb{R}$.

Instead of just any definition, we may ask for a definition of S in R of least logical complexity. Formulas without the quantifiers $\forall$ and $\exists$ will usually not define interesting sets (e.g. if R is a domain, only finite and cofinite sets can possibly have a quantifier-free definition). The next best thing is an *existential* or a *universal* formula, this is a formula which starts with a number of existential (respectively universal) quantifiers and is then followed by a quantifier-free formula. The given definition of $[0, \sqrt{2}]$ is existential. Finally, a subclass of the class of existential formulas is that of the *diophantine* formulas; these are formulas of the type

$$\exists x_1, \ldots, x_n (f(t, x_1, \ldots, x_n) = 0)$$

for some $n \in \mathbb{N}$ and a polynomial $f \in \mathbb{Z}[T, X_1, \ldots, X_n]$.

If a ring is has a definition within a larger ring, then this definition can help relate the complexity of the first-order theories of the two rings. We give an example of how a definability result can lead to a decidability result; the relationship between decidability and definability will be made more precise in Section 2.4.

Observation. *Let R be a commutative ring, suppose that $\mathbb{Z}$ has a diophantine definition in R. Then there is no decision algorithm for systems of diophantine equations over R. If additionally every system of diophantine equations is effectively equivalent over R to a single diophantine equation, it follows that Hilbert's 10th problem for R is unsolvable.*

Definable subsets show up all over model theory, but observations like the one above have been one of the motivations to search for diophantine definitions of subrings and have led to the unsolvability of Hilbert's 10th problem for many rings. We mention $\mathbb{R}(t)$, $\mathbb{C}(t_1, t_2)$ and $\mathbb{C}[t]$ and refer to [Koe14, Chapter 5] for an overview on Hilbert's 10th problem for other rings.

The definability of other sets has proven to be more elusive. A longstanding open question is whether $\mathbb{Z}$ has a diophantine definition in $\mathbb{Q}$. There is no known standard way to decide whether a given subset of $\mathbb{Q}$ is diophantine, and an answer to the above question still seems out of reach. As there are countably many polynomials over $\mathbb{Q}$ and uncountably many subsets of $\mathbb{Q}$, one sees immediately that 'most' subsets of $\mathbb{Q}$ will not be diophantine (or even definable, by the same argument), although even giving one concrete example of such a non-diophantine subset is not entirely trivial. At the end of Section 4.6 we will briefly explain a construction of a non-diophantine subset of $\mathbb{Q}$.

Nevertheless, some surprising new diophantine definitions of subsets of $\mathbb{Q}$ have been discovered recently. The goal of this thesis is to discuss some of these results; this we will do in the third and fourth chapter, after having gone through the necessary prerequisites in the first two chapters. Most of the results will hold for general number fields (finite extensions of $\mathbb{Q}$) and even more generally for so-called global fields.

A solid understanding of central simple algebras over local and global fields is essential for the definability results which are to follow. A local field is a field on which an absolute value function can be defined such that the induced topology is locally compact. Examples of such fields are the fields of real, complex, and p-adic numbers. Global fields are a class of fields for which the theory of central simple

algebras can be understood through a certain set of local extension fields. Examples of global fields are number fields. Because central simple algebras over local fields are relatively easy to describe compared to those over global fields, local fields will play a crucial role in the derivation of definability results later on. Hence, in the first chapter, we will indicate the necessary results on local and global fields. We will assume that the reader is somewhat familiar with the basic concepts of algebraic number theory, valuation theory, topology and the theory of central simple algebras. We shall omit the proof of some of the more technical or deep results we need on local and global fields.

In the second chapter we will discuss the notions of diophantine and definable sets more rigorously and thoroughly. For example, we explain why - at least in number fields and their rings of integers - one can equivalently define diophantine subsets to be projections of sets of the form

$$\bigcup_{i\in I}\bigcap_{j\in J} U_{i,j}$$

where I and J are finite sets and each $U_{i,j}$ is either the zero set of a polynomial or the complement of such a set. This shows that the class of diophantine subsets is larger than one might have guessed at first. We also illustrate the intimate interplay between definability results on the one hand and model-theoretic results on the other hand.

The third chapter focusses on a technique pioneered by Bjorn Poonen and further developed by Philip Dittmann. [Poo09] [Dit18] If A is a central simple algebra over a field K, we consider the set

$$S(A) = \{\mathrm{Trd}(x) \mid x \in A, \mathrm{Nrd}(x) = 1\}$$

where Trd denotes the reduced trace and Nrd the reduced norm. We will show that this set has a diophantine definition depending only on a collection of structure constants of A. We establish a local-global principle for these sets $S(A)$, yielding us powerful tools to define subrings of global fields. For example, if A is a central simple algebra over $\mathbb{Q}$ which splits over $\mathbb{R}$, then denoting by Δ the set of prime numbers p for which A does not split over the field of p-adic numbers $\mathbb{Q}_p$, we will show that

$$S(A) + S(A) = \bigcap_{p\in\Delta} \mathbb{Z}_{(p)}.$$

Here, the left hand side is to be interpreted as the set of sums of two elements of $S(A)$, and $\mathbb{Z}_{(p)}$ is the set of rational numbers with denominator not divisible by p. Noting that the set on the left is diophantine with structure constants of A as parameters, this gives us a way to define many semilocal subrings of $\mathbb{Q}$. We will use these facts to derive a first-order formula which defines the ring of integers in any number field. In particular, this formula defines $\mathbb{Z}$ in $\mathbb{Q}$, but it is not diophantine.

In the final chapter of this thesis, we show that $\mathbb{Q} \setminus \mathbb{Z}$ is a diophantine subset of $\mathbb{Q}$, in other words, $\mathbb{Z}$ is a universal subset of $\mathbb{Q}$. More generally, we prove that in any global field K and for any finite set S of prime ideals the ring of S-integers is universal; in particular if K is a number field, its ring of integers is universal. These results were proven recently by Jochen Koenigsmann for $\mathbb{Q}$ [Koe16], Jennifer Park for

general number fields [Par13] and Kirsten Eisenträger and Travis Morrison for global fields of odd characteristic [EM18], but we will present a new approach. Like these authors we use a trick to show that the Jacobson radical of some semilocal subrings of the global field is diophantine, but we then combine these subsets differently to obtain the ring of integers. Our approach has a number of advantages. We present a unified and arguably simpler proof which relies solely on the classification of quaternion algebras over global fields, and yields a diophantine definition with significantly less quantifiers than the ones found in the literature. Furthermore, our proof can be modified to include global fields of characteristic 2, a case which had not been covered before.

Acknowledgements

This thesis would not have been what it is without the help of my supervisor Karim Johannes Becher. Our interests, backgrounds and preferred approaches - even if not always aligned at first - proved to be complementary in finding the solutions we were after. He always readily made time for me and the many hours spent discussing the topic with him were informative and pleasant, for which I am thankful.

As I was working my way through the main articles which inspired this thesis I have had contact with several of their authors, all of whom were happy to answer any questions I had. I would like to thank Jochen Koenigsmann in particular, whom I never met in person, but who went out of his way to comment on parts of his work and also pointed me towards other interesting articles. When it comes to understanding the current state of the art in the broader topic of definability in rings, I got a lot out of the conversations I had with Arno Fehm and Jan Van Geel, for which I wish to express my gratitude too.

Last but not least I am grateful to my parents for their support and their unrelenting belief that I was doing something meaningful, even if I was never able to explain what exactly that was.

Chapter 1

Local and global fields

We denote by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ the sets of natural, integer, rational, real and complex numbers respectively. We consider 0 to be a natural number.

Let K always be a field.

1.1 Absolute values and valuations

1.1.1 Definition. An *absolute value* on K is a map

$$|.| : K \to \mathbb{R}^+$$

satisfying

(i) for all $x \in K$, $|x| = 0$ if and only if $x = 0$,

(ii) for all $x, y \in K$, $|xy| = |x| \cdot |y|$,

(iii) for all $x, y \in K$, $|x + y| \leq |x| + |y|$.

If $|.|$ even satisfies

(iii') for all $x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$

then we call $|.|$ a *non-archimedean* absolute value, otherwise $|.|$ is called an *archimedean* absolute value. An absolute value naturally makes K into a topological field via the metric $d(x, y) = |x - y|$.

We will mostly implicitly disregard the *trivial absolute value*, given by $|x| = 1$ for all $x \in K^\times$.

1.1.2 Proposition. *Let $|.|_1$ and $|.|_2$ be two absolute values on K. The following are equivalent:*

1. *$|.|_1$ and $|.|_2$ induce the same topology.*
2. *$|.|_1$ and $|.|_2$ have the same open unit ball.*
3. *$|.|_1$ and $|.|_2$ have the same closed unit ball.*

4. There exists an $\alpha \in \mathbb{R}^+$ such that $|.|_1 = |.|_2^\alpha$.

Proof. [OMe00, 11:4]. □

1.1.3 Definition. We call two absolute values on K *equivalent* if they satisfy the equivalent properties from the proposition. An equivalence class of non-trivial absolute values on K is called a *spot* on K.

1.1.4 Remark. A non-archimedean and an archimedean absolute value can not be equivalent (for example because (iii') still holds when replacing $|.|$ by $|.|^\alpha$ for some $\alpha \in \mathbb{R}^+$), whereby we can also apply the terms non-archimedean and archimedean to the spots belonging to non-archimedean and archimedean absolute values respectively. One also calls archimedean spots *infinite* and non-archimedean spots *finite*.

Non-archimedean absolute values can be studied via valuations, as a simple observation will make clear in the following proposition. Recall that a *valuation* on K is a map $v : K \to G \cup \{\infty\}$ where G is a totally ordered abelian group and $\infty \notin G$, and such that for all $x, y \in K$

(i) $v(x) = \infty$ if and only if $x = 0$.

(ii) $v(x \cdot y) = v(x) + v(y)$.

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

The set of elements with non-negative value form a local ring $\mathcal{O}$ called the *valuation ring* of v; its maximal ideal $\mathfrak{m}$ is given by the set of elements with strictly positive value. The field $\mathcal{O}/\mathfrak{m}$ is called the *residue field* of the valuation. There is a surjective homomorphism

$$\mathsf{red}_v : \mathcal{O} \to \mathcal{O}/\mathfrak{m} : x \mapsto x + \mathfrak{m}$$

called the *residue homomorphism*. If no confusion is possible about which valuation is referred to, we might write $\overline{x}$ instead of $\mathsf{red}_v(x)$ for an $x \in \mathcal{O}$. Similarly if $F \in \mathcal{O}[X]$ is a polynomial, $\mathsf{red}_v(F)$ or $\overline{F}$ refers to the polynomial in $(\mathcal{O}/\mathfrak{m})[X]$ obtained by applying red_v to the coefficients of F.

If, after fixing an element $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$, every element of K has a unique representation of the form $a\pi^n$ for $n \in \mathbb{Z}$ and $a \in K$ with $v(a) = 0$, we call the valuation and its valuation ring *discrete*. The element π is called a *uniformiser* or *uniformising element*. The valuation ring determines the valuation up to multiplication by a constant. There is a unique discrete valuation v corresponding to a given discrete valuation ring such that $v(a\pi^n) = n$; this we call the *normalised* valuation.

1.1.5 Proposition. *There is a correspondence between the non-archimedean absolute values and the $\mathbb{R}$-valued valuations on K: for a non-archimedean absolute value $|.|$ on K,*

$$v : K \to \mathbb{R} \cup \{\infty\} : x \mapsto -\ln|x|$$

is a valuation on K, if we take the convention that $-\ln 0 = \infty$. Conversely, for a real-valued valuation v on K,

$$|.| : K \to \mathbb{R}_+ : x \mapsto e^{-v(x)}$$

is a non-archimedean absolute value on K, taking the convention that $e^{-\infty} = 0$. The closed unit ball for the absolute value becomes the valuation ring for the valuation and the open unit ball for the absolute value becomes the maximal ideal for the valuation.

Proof. Easy verification. □

1.1.6 Proposition (Principle of Domination)**.** *Let K be a field with valuation v. Let $a, b \in K$ with $v(a) \neq v(b)$. Then*

$$v(a+b) = \min\{v(a), v(b)\}$$

Proof. Suppose without loss of generality $v(a) = \min\{v(a), v(b)\}$; we need to show $v(a+b) = v(a)$. The inequality $\geq$ is condition (iii) on valuations. On the other hand,

$$v(a) = v(a+b-b) \geq \min\{v(a+b), v(b)\}$$

whereby $v(a) \geq v(a+b)$, as $v(b) > v(a)$. □

1.2 Complete and local fields

1.2.1 Definition. If K has an absolute value $|.|$, we call a field $\widehat{K}$ together with an embedding $\sigma : K \to \widehat{K}$ and an absolute value $\widehat{|.|}$ a *completion* of $(K, |.|)$ if it satisfies:

(i) $\widehat{|\sigma(a)|} = |a|$ for $a \in K$ (i.e. $\widehat{|.|}$ extends $|.|$).

(ii) $\sigma(K)$ is dense in $\widehat{K}$.

(iii) $\widehat{K}$ is complete with respect to the metric induced by $\widehat{|.|}$.

The embedding σ is called a *place* of K. If $(K, |.|)$ is its own completion, we call K *complete*.

1.2.2 Theorem. *There always exists a completion of K. This completion and the embedding are unique up to canonical isomorphism and only depend on the spot of $|.|$. Hence also the place σ only depends on the spot.*

Proof. [OMe00, 11:13, 11:15]. □

1.2.3 Theorem. *Up to topological isomorphism, $\mathbb{R}$ and $\mathbb{C}$ with their usual absolute values are the only complete fields with archimedean absolute value. The unit ball with respect to this absolute values is compact.*

Proof. [OMe00, 12:4]. □

1.2.4 Definition. A place $\sigma : K \to \mathbb{R}$ and its corresponding spot on K are called *real*, a place $\sigma : K \to \mathbb{C}$ and its corresponding spot are called *complex*.

1.2.5 Definition. If $|.|$ is an absolute value on K such that the closed unit ball is compact, then we call $(K, |.|)$ a *local field*.

1.2.6 Remark. Since the unit ball and its compactness are preserved under equivalence of absolute values, it is immediately clear that we need only specify the spot of a field when referring to it as a local field, not the specific absolute value. It is true that there can in fact be only one spot making a given field into a local field, whereby we can just call a field local without having to refer to any spot. We will neither prove nor need this last fact, but will sometimes not explicitly mention the spot if it is clear from the context.

By Theorem 1.2.3 the archimedean local fields are well-understood. We now take a closer look at non-archimedean local fields.

1.2.7 Lemma. *Let $\mathcal{O}$ be a discrete valuation ring, $\mathfrak{m}$ its maximal ideal. $\mathcal{O}/\mathfrak{m}$ is finite if and only if $\mathcal{O}$ is totally bounded with respect to the spot induced by the valuation.*

Proof. Let $|.|$ be an absolute value on $\mathrm{Frac}(\mathcal{O})$ having $\mathcal{O}$ as unit ball. Suppose that $\mathcal{O}/\mathfrak{m}$ is finite. For a given $\varepsilon > 0$, take an $N \in \mathbb{N}$ such that $|x| < \epsilon$ whenever $x \in \mathfrak{m}^N$. Letting X be a set of representatives of $\mathcal{O}/\mathfrak{m}^N$, then X contains $|\mathcal{O}/\mathfrak{m}|^N < \infty$ elements, whereby $\{x + \mathfrak{m}^N \mid x \in X\}$ is a finite open cover of $\mathcal{O}$ of which the elements have diameter less than ε.

Conversely if $\mathcal{O}$ is totally bounded, we obtain a finite set X such that $\{x + \mathfrak{m} \mid x \in X\}$ covers $\mathcal{O}$. But then $X \to \mathcal{O}/\mathfrak{m} : x \mapsto x + \mathfrak{m}$ is surjective, whereby $\mathcal{O}/\mathfrak{m}$ is finite. □

1.2.8 Proposition. *Let $(K, |.|)$ be a non-archimedean absolute valued field, v the valuation associated to $|.|$, $\mathcal{O}$ the valuation ring, $\mathfrak{m}$ its maximal ideal. The following are equivalent:*

(1) $(K, |.|)$ is a local field.

(2) $\mathcal{O}$ is a complete discrete valuation ring and the residue field $\mathcal{O}/\mathfrak{m}$ is finite.

Proof. By definition of a local field, we need to show that condition 2 is equivalent to $\mathcal{O}$ being compact. From the theory of metric spaces we know that a metric space is compact if and only if it is complete and totally bounded. With the above lemma in mind, the only thing that is left to show is that $\mathcal{O}$ is discrete when it is compact.

So suppose that $\mathcal{O}$ is compact. Then the function

$$v : \mathfrak{m} \to [0, +\infty] : x \mapsto v(x)$$

is continuous and has a compact domain, $\mathfrak{m}$ being a closed subset of the compact space $\mathcal{O}$ ($\mathcal{O} \setminus \mathfrak{m} = \mathcal{O}^\times = \mathcal{O}^\times + \mathfrak{m}$ is open). By the extreme value theorem, this function attains its minimum in an element $\pi \in \mathfrak{m}$, whereby

$$\mathfrak{m} = \{x \in K \mid v(x) \geq v(\pi)\}.$$

It now follows readily that π is a uniformising element, whereby $\mathcal{O}$ is a discrete valuation ring. □

1.2.9 Proposition. *Let L/K be an extension of fields, v a valuation on K, extending to a valuation w on L. Let κ and λ be the respective residue fields of v and w. The map*

$$\kappa \to \lambda : \mathsf{red}_v(x) \mapsto \mathsf{red}_w(x)$$

is a well-defined embedding of fields. Let now G_v and G_w be the value groups of v and w. After restricting them to their image under the valuation we can define an embedding of groups

$$G_v \to G_w : v(x) \mapsto w(x).$$

If K is dense in L, both maps are surjective.

Proof. The map $v(x) \mapsto w(x)$ is a well-defined embedding, as w extends v.

Let $\mathcal{O}_v$ and $\mathcal{O}_w$ be the respective valuation rings of v and w. As w extends v we have $\mathcal{O}_v \subseteq \mathcal{O}_w$. As both are local rings, the unique maximal ideal $\mathfrak{m}_w$ of $\mathcal{O}_w$ lies over the unique maximal ideal $\mathfrak{m}_v$ of $\mathcal{O}_v$, whereby $\mathfrak{m}_v \subseteq \mathfrak{m}_w$. This implies that we indeed have a natural homomorphism from $\kappa = \mathcal{O}_v/\mathfrak{m}_v$ to $\lambda = \mathcal{O}_w/\mathfrak{m}_w$ and as both are fields, this is necessarily an embedding.

Suppose now that K is dense in L. Then to any $x \in \mathcal{O}_w$ there exists an $x' \in K$ such that $w(x' - x) > w(x')$. Then by the Principle of Domination

$$v(x') = w(x') = w(x' - x + x) = \min\{w(x' - x), w(x)\} = w(x) \geq 0$$

whereby $x' \in K \cap \mathcal{O}_w = \mathcal{O}_v$. We have $x \in x' + \mathfrak{m}_w$ and $v(x') = w(x)$. As this works for general x, we have shown the surjectivity of the two embeddings. □

1.2.10 Corollary. *Let $(K, |.|)$ be a non-archimedean absolute valued field; denote by $\widehat{K}$ its completion with respect to $|.|$. Denote by v the associated valuation on K. The following are equivalent:*

(1) $\widehat{K}$ is a local field.

(2) v is a discrete valuation with finite residue field.

If π is a uniformiser for v, then also for the completion.

Proof. By Proposition 1.2.9 the second statement is equivalent to the extension of v to $\widehat{K}$ being a discrete valuation with finite residue field. As $\widehat{K}$ is complete by definition, Proposition 1.2.8 yields the equivalence of the two statements.

The last part follows from the second isomorphism in Proposition 1.2.9. □

1.2.11 Example. To any prime number p, we can associate a unique discrete valuation v_p on $\mathbb{Q}$ such that for $x \in \mathbb{Z}$, $v_p(x)$ is the number of times p divides x. The residue field is $\mathbb{Z}/p\mathbb{Z}$, so the completion of $\mathbb{Q}$ with respect to this prime number is a local field with residue field isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We will denote this local field by $\mathbb{Q}_p$ and call it *the field of p-adic numbers*. The element p is a uniformiser for the valuation on $\mathbb{Q}_p$. The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and we set $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.

1.2.12 Proposition (Hensel's Lemma)**.** *Let $\mathcal{O}$ be a complete, discrete valuation ring with maximal ideal $\mathfrak{m}$. Let $f \in \mathcal{O}[X]$ and let $\alpha \in \mathcal{O}/\mathfrak{m}$ be a simple root of f. Then there exists a unique $a \in \alpha$ such that $f(a) = 0$ in $\mathcal{O}$.*

Proof. [EP05, Corollary 1.3.2.] □

1.3 Extensions of local fields

Recall that if A is a Dedekind domain and $K = \mathrm{Frac}(A)$, then every finitely generated non-zero A-submodule of K can be written as a finite product of maximal ideals of A in a unique way. For a maximal ideal $\mathfrak{p}$ of A, the map sending an element $x \in K^\times$ to the number of times $\mathfrak{p}$ appears as a factor in the decomposition of Ax defines a normalised discrete valuation on A, which we will denote by $v_\mathfrak{p}$. These are

up to multiplication by a constant the only valuations on K of which the valuation ring contains A.

Let now L/K be a finite extension of fields, v a normalised discrete valuation on K with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m}$. Then the integral closure B of $\mathcal{O}$ in L is a Dedekind domain. Fix a maximal ideal $\mathfrak{p}$ of B and denote by $v_\mathfrak{p}$ the induced normalised discrete valuation. By definition every element x of K has a unique representation of the form $u\pi^{v(x)}$ where π is a uniformiser for v and $u \in \mathcal{O}^\times$. As the valuation ring of $v_\mathfrak{p}$ contains B and hence $\mathcal{O}$ we find for $x = u\pi^{v(x)} \in K$:

$$v_\mathfrak{p}(x) = v_\mathfrak{p}(u) + v(x)v_\mathfrak{p}(\pi) = v(x)v_\mathfrak{p}(\pi),$$

i.e. $v_\mathfrak{p}|_K = v_\mathfrak{p}(\pi)v$. We call the constant $v_\mathfrak{p}(\pi)$ the *ramification index* of $v_\mathfrak{p}$ over v and say that $v_\mathfrak{p}$ is *unramified* over v if the ramification index is 1. Otherwise, we call $v_\mathfrak{p}$ *ramified* over v. The valuation $v_\mathfrak{p}/v_\mathfrak{p}(\pi)$ is an extension of v; it is always a discrete valuation and it is normalised if and only if $v_\mathfrak{p}$ is unramified over v.

It follows from the above considerations that discrete valuations can be easily extended over finite extensions. Our aim now is to show that this extension is unique in the case of complete discrete valuations.

1.3.1 Definition. Let $|.|$ be an absolute value on K and V be a finite-dimensional K-vector space. A *K-norm* on V is a function $\|.\| : V \to [0, +\infty[$ satisfying for $x, y \in V$ and $a \in k$:

(i) $x = 0$ if and only if $\|x\| = 0$.

(ii) $\|x + y\| \leq \|x\| + \|y\|$. *(triangle inequality)*

(iii) $\|ax\| = |a|\|x\|$.

Such a norm naturally induces a metric and hence a topology on V.

1.3.2 Proposition. *Let $(K, |.|)$ be a complete field, V a finite-dimensional K-vector space. All K-norms on V induce the same topology and V is complete with respect to these norms. If $(K, |.|)$ is local, then the unit ball in V is compact.*

Proof. This is a standard analysis result if $K = \mathbb{R}$ and the same proof works when $(K, |.|)$ is a local field. See [OMe00, 11:17] for a fully worked out explanation. □

1.3.3 Proposition. *Let K be a complete field with respect to the absolute value $|.|$. For any finite extension L/K there is a unique extension of $|.|$ to L and this extension makes L into a complete field. Furthermore, if L/K is separable, then the extension is given by*

$$|y| = |N_{L/K}(y)|^{1/n}$$

for $y \in L$, $n = [L : K]$, where $N_{L/K}$ is the norm of the extension. Finally, if K is local with respect to $|.|$, then L is local with respect to the extension of $|.|$.

Proof. As an absolute value on L extending $|.|$ would in particular be a K-norm on L, the uniqueness, completeness and - in case K is local - localness follow by Proposition 1.3.2. If $K \in \{\mathbb{R}, \mathbb{C}\}$ then also $L \in \{\mathbb{R}, \mathbb{C}\}$ and it is known that the

given formula defines an extension of the absolute value. Otherwise, K is non-archimedean and to show the existence of an extension of $|.|$ it suffices to extend the corresponding valuation, which we know is possible by previous considerations.

We now consider the case where K is non-archimedean and L/K is separable; denote by v the valuation on K corresponding to $|.|$ and w the necessarily unique extension of v to L. Translating the formula for the absolute values to the language of valuations as in Proposition 1.1.5, what we must show is that for $x \in L$

$$w(x) = \frac{v(N_{L/K}(x))}{n}.$$

First, suppose L/K is Galois and let $\sigma_1, \ldots, \sigma_n$ be the K-automorphisms of L. Then indeed

$$v(N_{L/K}(x)) = w\left(\prod_{i=1}^{n} \sigma_i(x)\right) = \sum_{i=1}^{n} (w \circ \sigma_i)(x) = \sum_{i=1}^{n} w(x) = nw(x).$$

as $w \circ \sigma_i$ defines a valuation on L extending v, which must by uniqueness equal w. In the general case, let N/K be the normal closure of L/K. Denote $m = [N : L]$ and let w' be the extension of w to N, then by the Galois case

$$\begin{aligned} mnw(x) = mnw'(x) &= v(N_{N/K}(x)) = v(N_{L/K} \circ N_{N/L}(x)) \\ &= v(N_{L/K}(x^m)) = v(N_{L/K}(x)^m) = mv(N_{L/K}(x)) \end{aligned}$$

which shows the formula in the general case. □

Let now L/K be a degree n separable extension of non-archimedean local fields, let v be the normalised valuation on L. Letting π be a uniformiser for the restriction of the valuation to K, we defined $v(\pi)$ to be the ramification index of the extension of valuations. Since the extension of valuations is unique when K is complete, we can also use the terms ramification index, ramified and unramified for the field extension.

Let κ and κ' be the respective residue fields of K and L with respect to v; by Proposition 1.2.9 we have that κ' is naturally a κ-vector space. Call $\dim_\kappa(\kappa')$ the *inertia degree* of the extension.

1.3.4 Proposition (Fundamental equality)**.** *Consider the setting above. Then n is the product of the inertia degree and the ramification index.*

Proof. [OMe00, 16:4] □

1.3.5 Proposition. *Suppose K is a non-archimedean local field with discrete valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m}$. Let $n \in \mathbb{N}^+$ and $F \in \mathcal{O}[X]$ a monic degree n polynomial such that $\overline{F}$ is irreducible. Let L be the root field of F over K.*

1. *Up to K-isomorphism, L is the unique degree n unramified separable extension of K.*
2. *The norm $N_{L/K}$ only represents elements of value a multiple of n.*
3. *For any separable finite extension M/K with inertia degree a multiple of n, there is a K-embedding of L into M.*

Proof. As $\overline{F}$ is irreducible, F must be irreducible over $\mathcal{O}$ and hence over K (by Gauss' Lemma), whereby L/K is indeed a degree n extension. Similarly, as $\mathcal{O}/\mathfrak{m}$ is a finite and hence perfect field, $\overline{F}$ is separable, whereby the same holds for F. Hence, L/K is separable.

Let α be a root of F in L, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a K-basis of L. Denoting by C_F the companion matrix corresponding to F, the norm form is given by

$$N_{L/K}(X_1, \ldots, X_n) = \det(X_1 I_n + X_2 C_F + \ldots + X_n C_F^{n-1}) \in \mathcal{O}[X_1, \ldots, X_n].$$

The reduction of this form modulo $\mathfrak{m}$ is also the norm form of the root field of $\overline{F}$ over $\mathcal{O}/\mathfrak{m}$. This reduced norm form is anisotropic over $\mathcal{O}/\mathfrak{m}$, whereby $N_{L/K}$ can only represent elements of K of value a multiple of n. This shows 2.

That L/K is unramified now follows from the formula in Proposition 1.3.3: if $N_{L/K}$ only represents elements of value a multiple of n, then the extension of a normalised valuation remains normalised, which we know happens only in an unramified extension. We conclude that indeed L/K is a degree n, unramified, separable extension.

Let now M/K be an arbitrary finite separable extension with inertia degree a multiple of n, i.e. the residue field μ of M is an extension of $\mathcal{O}/\mathfrak{m}$ of degree a multiple of n. Note that, by Proposition 1.3.3, M is local. By the Galois Theory of finite fields, $\overline{F}$ has a root in μ, which by Hensel's lemma lifts to a root of F in M. This implies that L embeds into M. We have proven 3.

Finally, the uniqueness in 1 is a special case of 3: if L' is another degree n unramified separable extension, then L embeds into L', but by comparing K-dimensions, this embedding must be an isomorphism. □

1.4 Local squares

We follow [OMe00, Section 63].

1.4.1 Proposition. *Let $\mathcal{O}$ be a complete discrete valuation ring. Let $x \in \mathcal{O}^\times$ and π a uniformiser. Then x is a square in $\mathcal{O}$ if and only if x is a square modulo $4\pi\mathcal{O}$.*

Proof. Suppose that x is a square modulo $4\pi\mathcal{O}$, i.e. $x = a^2 + 4\pi b$ for some $a, b \in \mathcal{O}$. Note that $v(a) = 0$, so we can apply Hensel's lemma to the polynomial $\pi T^2 + aT - b$ to find a $t \in \mathcal{O}$ with $\pi t^2 + at = b$. But then $(a+2\pi t)^2 = a^2 + 4\pi(at + \pi t^2) = a^2 + 4\pi b = x$, whereby indeed x is a square in $\mathcal{O}$. The other implication is trivial. □

1.4.2 Remark. If 2 is a unit in $\mathcal{O}/\pi\mathcal{O}$, then it follows that x is a square in $\mathcal{O}$ if and only if x is a square modulo $\pi\mathcal{O}$.

1.4.3 Corollary. *Let K be a non-archimedean local field of characteristic different from 2. The set of nonzero squares $K^{\times 2}$ is an open subset of K.*

Proof. Let v be the normalised valuation on K, π a uniformiser, $\mathcal{O}$ the valuation ring. Let $a \in K^\times$ be a square, set $m = v(a)$. We will show that $a + 4\pi^{m+1}\mathcal{O} \subseteq K^{\times 2}$. Take $a' \in a + 4\pi^{m+1}\mathcal{O} \subseteq K^{\times 2}$, then $v(a') = v(a) = m$. Furthermore, $\frac{a'}{a} \equiv 1 \bmod 4\pi\mathcal{O}$, so by Proposition 1.4.1 $\frac{a'}{a}$ is a square in K, whereby a' is a square in K. □

1.4.4 Definition. We call a non-archimedean local field *dyadic* if the field has characteristic zero, but the residue field has characteristic two. We call a spot on a field dyadic if the completion with respect to this spot is a dyadic local field.

1.4.5 Proposition. *Let K be a non-archimedean local field with valuation v, valuation ring $\mathcal{O}$ and finite residue field κ. Suppose that* $\mathrm{char}(\kappa) \neq 2$. *Furthermore, let π be a uniformiser and $u \in \mathcal{O}$ such that $\overline{u}$ is not a square in κ. Then $\{1, u, \pi, u\pi\}$ forms a full set of representatives for the square classes of K.*

Proof. Clearly $1, u, \pi, u\pi$ lie in different square classes. Let $x \in K$ be arbitrary, write $x = v\pi^n$ for $v \in \mathcal{O}^\times$, $n \in \mathbb{Z}$. After multiplying x by an appropriate power of π^2 we may assume $n \in \{0, 1\}$. By Proposition 1.4.1 we have that v lies either in the square class of 1 or in that of u, since there are only two square classes in κ. □

1.4.6 Proposition. *Let K be a non-archimedean local field of characteristic different from 2 and with valuation ring $\mathcal{O}$ and uniformiser π. There exists a $u \in \mathcal{O}^\times$ such that $\Delta = 1 + 4u^2$ is not a square.*

Proof. Suppose first that K is non-dyadic. By Proposition 1.4.1 and the finiteness of κ, take an element u in $\mathcal{O}^\times$ which is not a square in K. Then using Hensel's lemma and the fact that every element of κ is a sum of two squares in κ, $u = \alpha^2 + \beta^2$ for some $\alpha \in \mathcal{O}^\times, \beta \in \mathcal{O}$. Then $\Delta = 1 + \frac{\beta^2}{\alpha^2}$ is as required, since $4 \in \mathcal{O}^\times$.

Now suppose K is dyadic. Let $\kappa = \mathcal{O}/\pi\mathcal{O}$ be the finite residue field. Choose a $d \in \mathcal{O}^\times$ such that $X^2 + X - d$ is irreducible modulo $\pi\mathcal{O}$, this is possible by the perfectness of the finite field κ. Then

$$1 - 4d - (2d)^2 \equiv (1 + 2d)^2 \bmod 4\pi\mathcal{O}$$

so by Proposition 1.4.1, $1 - 4d = 4d^2 + u^2$ for some $u \in \mathcal{O}^\times$, whereby $\Delta = 1 + 4\frac{d^2}{u^2}$ does the job, as the discriminant $1 + 4d$ of $X^2 + X - d$ is not a square in K. □

For the rest of this section, let K be a non-archimedean local field of characteristic different from 2 with valuation ring $\mathcal{O}$ and uniformising parameter π, and let $\Delta \in \mathcal{O}$ be a non-square of the form $1 + 4u^2$ for $u \in \mathcal{O}^\times$.

1.4.7 Proposition. *The extension $K(\sqrt{\Delta})/K$ is a separable, unramified quadratic extension.*

Proof. The extension is quadratic as Δ is not a square in K. Furthermore, $d = \frac{1}{4}(\Delta - 1) \in \mathcal{O}^\times$ and $X^2 + X - d$ has Δ as its discriminant, whereby $K(\sqrt{\Delta})$ is the root field of $X^2 + X - d$. But by Hensel's Lemma $X^2 + X - d$ is also irreducible modulo $\pi\mathcal{O}$. We now conclude with Proposition 1.3.5. □

1.4.8 Corollary. *If Δ' is another element of K satisfying the same properties, then $\Delta/\Delta' \in K^{\times 2}$.*

Proof. By previous proposition and Proposition 1.3.5 we have $K(\sqrt{\Delta}) = K(\sqrt{\Delta'})$, whereby $\Delta' \in \Delta K^{\times 2}$. □

1.5 Quaternion algebras over local fields

We briefly recall some results from the abstract theory of quaternion algebras and will assume some familiarity with basic concepts from the theory of central simple algebras; see [Pie82, Chapters 12 and 13] for more about central simple algebras.

Let $a, b \in K$ be such that $b(1+4a) \neq 0$. The K-algebra $K \oplus Ku \oplus Kv \oplus Kuv$ with $u^2 - u = a$, $v^2 = b$ and $uv + vu = v$ is a K-quaternion algebra (a central simple K-algebra of degree 2), which we will denote by $[a, b)_K$. If the field K is clear from the context, we might just write $[a, b)$. It is clear that this algebra is 4-dimensional over K. One way to see that it is central simple is by first considering the case where K contains elements α, β such that $\alpha^2 - \alpha = a$ and $\beta^2 = b$. In this case one can verify that the matrices

$$u = \begin{bmatrix} \alpha & 0 \\ 0 & 1-\alpha \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix}$$

satisfy the relations $u^2 - u = a$, $v^2 = b$ and $uv + vu = v$, whereby we must have that $[a, b)_K \cong \mathbb{M}_2(K)$. This representation also gives us a formula for the reduced trace and norm of an element $x = x_1 + x_2u + x_3v + x_4uv \in [a, b)_K$ with $x_1, x_2, x_3, x_4 \in K$:

$$\begin{aligned} \mathrm{Trd}(x) &= \mathrm{Tr}\left(\begin{bmatrix} x_1 + x_2\alpha & x_3\beta + x_4\alpha\beta \\ x_3\beta + x_4(1-\alpha)\beta & x_1 + x_2(1-\alpha) \end{bmatrix}\right) = 2x_1 + x_2 \\ \mathrm{Nrd}(x) &= \det\left(\begin{bmatrix} x_1 + x_2\alpha & x_3\beta + x_4\alpha\beta \\ x_3\beta + x_4(1-\alpha)\beta & x_1 + x_2(1-\alpha) \end{bmatrix}\right) \\ &= x_1^2 + x_1x_2 - ax_2^2 - b(x_3^2 + x_3x_4 - ax_4^2). \end{aligned}$$

In case K is a general field, there exists a finite extension L/K such that L contains the required elements α, β. So $[a, b)_L = [a, b)_K \otimes L \cong \mathbb{M}_2(L)$ is a central simple L-algebra. It follows from this that $[a, b)_K$ is a central simple K-algebra (see for example [Pie82, Section 12.4]) and that the same formulas for the reduced trace and norm hold [Pie82, Section 16.1].

If $\mathrm{char}(K) \neq 2$ and $a, b \in K^\times$, the K-algebra $K \oplus Ki \oplus Kj \oplus Kij$ with $i^2 = a$, $j^2 = b$ and $ij = -ji$ is a K-quaternion algebra, which we will denote by $(a, b)_K$. If the field K is clear from the context, we might just write (a, b). The argument for the fact that $(a, b)_K$ is a quaternion algebra is similar to what we had for $[a, b)_K$. We find the following formula for trace and norm of $x = x_1 + x_2i + x_3j + x_4ij$ for $x_1, x_2, x_3, x_4 \in K$:

$$\mathrm{Trd}(x) = 2x_1 \quad \text{and} \quad \mathrm{Nrd}(x) = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2.$$

Furthermore if $\mathrm{char}(K) \neq 2$, $a, b \in K$ with $b(1+4a) \neq 0$, one verifies that we have an isomorphism $[a, b)_K \to (1+4a, b)_K$ defined by mapping v to j and u to $\frac{i+1}{2}$. Note thatin any quaternion algebra Q one always has $\mathrm{Nrd}(x) = \mathrm{Nrd}(\mathrm{Trd}(x) - x)$ for all $x \in Q$. This is because x and $\mathrm{Trd}(x) - x$ are both roots of $X^2 - \mathrm{Trd}(x)X + \mathrm{Nrd}(x)$.

It can be shown that if $\mathrm{char}(K) \neq 2$, then every quaternion algebra over K is isomorphic to some algebra of the form $(a, b)_K$. [Pie82, Section 13.1] Then by the isomorphism above, we also obtain that all quaternion algebras over K are isomorphic to some algebra of the form $[a, b)_K$. If $\mathrm{char}(K) = 2$, then by [Sch85,

Section 8.11] also every quaternion algebra over K is isomorphic to some algebra of the form $[a, b)_K$.

A quaternion algebra Q is either a division algebra or split. It is a division algebra if and only if its norm form is anisotropic, i.e. there exist no $x \in Q \setminus \{0\}$ with $\mathrm{Nrd}(x) = 0$. If there exists an $x \in Q$ with $\mathrm{Nrd}(x) = 0$, then there also exists an $x \in Q \setminus \{0\}$ with $\mathrm{Nrd}(x) = 0 = \mathrm{Trd}(x)$. Indeed, suppose $\mathrm{Nrd}(x) = 0$ but $\mathrm{Trd}(x) \neq 0$ for some $x \in Q$. Take a $y \in Q \setminus \{0\}$ such that $\mathrm{Trd}(xy) = \mathrm{Trd}(y) = 0$, this is possible as Trd is linear. We have $\mathrm{Nrd}(xy) = \mathrm{Nrd}(x)\,\mathrm{Nrd}(y) = 0$, so if $xy \neq 0$ we are done. If $xy = 0$, then $0 \neq \mathrm{Trd}(x)y = (\mathrm{Trd}(x) - x)y$, $\mathrm{Trd}(\mathrm{Trd}(x)y) = \mathrm{Trd}(x)\,\mathrm{Trd}(y) = 0$ and $\mathrm{Nrd}(\mathrm{Trd}(x)y) = \mathrm{Nrd}((\mathrm{Trd}(x) - x)y) = \mathrm{Nrd}(x)\,\mathrm{Nrd}(y) = 0$ whereby we are also done.

We conclude that if $a, b \in K$ are such that $b(1 + 4a) \neq 0$, the algebra $[a, b)_K$ is a division algebra if and only if

$$(1 + 4a)X^2 + b(Y^2 + YZ - aZ^2)$$

is anisotropic over K. When $\mathrm{char}(K) \neq 2$ and $a, b \in K^\times$, the algebra $(a, b)_K$ is a division algebra if and only if

$$aX^2 + bY^2 - Z^2$$

is anisotropic over K. We remark that this is equivalent to the quadratic form $X^2 - aY^2$ not representing b. Clearly $X^2 - aY^2$ represents b if and only if $aX^2 + bY^2 - Z^2$ has a zero (x, y, z) with $y \neq 0$. Suppose that $aX^2 + bY^2 - Z^2$ is isotropic and has a non-trivial zero $(x, 0, z)$. Then we must have that a is a square, say $a = u^2$ for $u \in K$. But then also $(\frac{b-1}{2u}, 1, \frac{b+1}{2})$ is a zero of the quadratic form, whereby $X^2 - aY^2$ represents b.

Finally, denoting Brauer equivalence by $\sim$, one has that

$$[a, b)_K \otimes [a, b')_K \sim [a, bb')_K$$

and hence if $\mathrm{char}(K) \neq 2$ also

$$(a, b)_K \otimes (a, b')_K \sim (a, bb')_K.$$

This follows from the discussion in [Sch85, Section 8.12].

1.5.1 Proposition. *Let $a, b \in \mathbb{R}^\times$. $(a, b)_\mathbb{R}$ is non-split if and only if both a and b are negative. Up to isomorphism, $(-1, -1)_\mathbb{R}$ is the only non-split quaternion algebra over $\mathbb{R}$.*

Proof. Clearly if a or b is positive, it is a square in $\mathbb{R}$, whereby $(a, b)_\mathbb{R}$ is split. If a and b are negative, there exist no $x, y \in \mathbb{R}$ with $b = x^2 - ay^2$, whereby (a, b) is non-split. It is clear that then $(a, b)_\mathbb{R} \cong (-1, -1)_\mathbb{R}$. □

For the rest of this section, let K be a non-archimedean local field, $\mathcal{O}$ its valuation ring, $\mathbb{F}_q$ its finite residue field with q elements, π a uniformiser, v the normalised valuation. If $\mathrm{char}(K) \neq 2$, let $\Delta \in \mathcal{O}$ be a non-square of the form $1 + 4u^2$ with $u \in \mathcal{O}^\times$.

1.5.2 Proposition. *Suppose K is non-dyadic and* $\mathrm{char}(K) \neq 2$. *For $a, b \in K$ we have that (a, b) is a division algebra if and only if one of the following holds:*

(a) $v(a)$ is odd, $v(b)$ is even and $b\pi^{-v(b)}$ is not a square modulo $\pi\mathcal{O}$.

(b) $v(b)$ is odd, $v(a)$ is even and $a\pi^{-v(a)}$ is not a square modulo $\pi\mathcal{O}$.

(c) $v(a)$ and $v(b)$ are odd and $-ab\pi^{-v(ab)}$ is not a square modulo $\pi\mathcal{O}$.

Proof. Multiplying one of the slots in (a, b) by π^2 or π^{-2} does not change the isomorphism class of the quaternion algebra, neither does it affect whether one of (a), (b) or (c) holds. Hence we may assume $v(a), v(b) \in \{0, 1\}$. Similarly, we may switch the roles of a and b to assume without loss of generality that $v(a) \geq v(b)$.

We use that for a quaternion algebra (a, b), this algebra being a division algebra is equivalent to the quadratic form $X^2 - aY^2$ not representing b. We now make a case distinction.

- $v(b) = 0 = v(a)$. Then $\overline{a} \neq 0$ and the quadratic form $\overline{a}X^2 + \overline{b}Y^2 - Z^2$ - being a ternary quadratic form - is isotropic over the finite residue field by Chevalley's Theorem. We saw previously that this is equivalent (over a field of characteristic $\neq 2$) to the quadratic form $X^2 - \overline{a}Y^2$ representing $\overline{b}$. And by Hensel's Lemma, we obtain from this that $X^2 - aY^2$ represents b over K.

- $v(b) = 0$ and $v(a) = 1$. By comparing values, we can only have $b = x^2 - ay^2$ for some $x, y \in K$ if $x \in \mathcal{O}$ and $b - x^2 \in \pi\mathcal{O}$. So it is a necessary condition for (a, b) to be split, that b is a square modulo $\pi\mathcal{O}$. Conversely, if b is a square modulo $\pi\mathcal{O}$, then by Hensel's Lemma it is also a square in K, whereby $X^2 - aY^2$ represents b.

- $v(a) = v(b) = 1$. Write $a = \pi u$, $b = \pi v$ for $u, v \in K$ with $v(u) = v(v) = 0$. Then $X^2 - aY^2$ represents b if and only if $\pi(v + uy^2) = x^2$ for some $x, y \in K$, which (by comparing values) is only possible if $v + uy^2 \in \pi\mathcal{O}$, i.e. $-\frac{v}{u}$ is a square modulo $\pi\mathcal{O}$. This is equivalent to $-uv = -ab\pi^{-v(ab)}$ being a square modulo $\pi\mathcal{O}$. On the other hand, if $-ab\pi^{-v(ab)}$ and hence $-\frac{v}{u}$ is a square modulo $\pi\mathcal{O}$, then by Proposition 1.4.1 $-\frac{v}{u} = y^2$ for some $y \in K$, whereby $\pi(v + uy^2) = 0 = 0^2$.

□

1.5.3 Proposition. *Let $a, b \in K$ be such that $b(1 + 4a) \neq 0$, suppose that $[a, b)_K$ is a division algebra. Then $v(a) \leq 0$. If $v(a) = 0$, then either $v(1 + 4a)$ is odd or $v(b)$ is odd.*

Proof. If the characteristic of the residue field is not 2, then also $\mathrm{char}(K) \neq 2$, $[a, b)_K \cong (1 + 4a, b)_K$ and the statement follows from Proposition 1.5.2 and Proposition 1.4.1. Assume for the rest of the proof that the characteristic of the residue field is 2. Note that in this case, $v(a) = 0$ automatically implies $v(1 + 4a) = 0$.

We may multply b by a square and assume without loss of generality that $v(b) \in \{0, 1\}$. If either $v(a) > 0$ or $v(a) = 0$ and $v(b) = 0$, then by the perfectness of the residue field we can find a $y \in \mathcal{O}$ such that $a - \frac{b(1+4a)}{y^2} \equiv 0 \bmod \pi$. Then the

polynomial $X^2 - X - a + \frac{b(1+4a)}{y^2}$ has a root modulo π; by Hensel's Lemma it then has a root in K, i.e. there exists an $x \in K$ with $0 = x^2 - x - a + \frac{b(1+4a)}{y^2}$. It follows that the quadratic form

$$(1+4a)X^2 + b(Y^2 + YZ - aZ^2)$$

has a non-trivial zero $(b, -xy, y)$, whereby $[a, b)_K$ is split. □

1.5.4 Proposition. *Let $d \in \mathcal{O}^\times$ be such that $X^2 - X - d$ is irreducible modulo π. Then $K[X]/(X^2 - X - d)$ is an unramified quadratic extension of K and for all $b \in K^\times$ we have that $[d, b)_K$ is split if and only if $v(b)$ is even.*

Proof. The part about the unramified quadratic extension follows from Proposition 1.3.5. Note that $v(1+4d) = 0$, otherwise $X^2 - X - d$ would be a square modulo π. Hence, if $v(b)$ is even, it follows from previous proposition that $[d, b)$ is split.

By Proposition 1.3.5, the norm form $X^2 - XY - Y^2 d$ of the quadratic extension only represents elements of even value. Hence if $v(b)$ is odd the quadratic form

$$(1+4a)X^2 + b(Y^2 + YZ - aZ^2)$$

must be anisotropic, whereby $[d, b)_K$ is non-split. □

1.5.5 Proposition. *Suppose* $\mathrm{char}(K) \neq 2$. *Let $b \in K$. The quaternion algebra $(\Delta, b)_K$ is split if and only if $v(b)$ is even.*

Proof. Write $\Delta = 1 + 4u^2$ for $u \in \mathcal{O}^\times$. As in the proof of Proposition 1.4.7, $X^2 - X - u^2$ is irreducible mod $\pi\mathcal{O}$. The statement follows from the previous proposition and the fact that $(\Delta, b)_K \cong [u^2, b)_K$. □

1.5.6 Lemma. *Let $aX^2 + bY^2$ be a quadratic form over K, suppose that it represents $c = ax^2 + by^2 \neq 0$ for certain $a, b, x, y \in K$. Then $aX^2 + bY^2$ represents the same elements of K as $cX^2 + abcY^2$.*

Proof. Follows by observing that

$$a(xX + byY)^2 + b(yX - axY)^2 = cX^2 + abcY^2.$$

□

1.5.7 Lemma ([OMe00, 63:11])**.** *Suppose* $\mathrm{char}(K) \neq 2$. *Let $a, b \in \mathcal{O}^\times$. The quadratic form $aX^2 + b\pi Y^2$ either represents 1 or Δ over K.*

Proof. If K is non-dyadic, then depending on whether the residue of a is a square or a non-square in the finite residue field, a will be either a square in K or Δ times a square by Corollary 1.4.8. We can thus focus on the dyadic case.

Lemma 1.5.6 implies that we may without loss of generality replace a by any unit represented by $aX^2 + b\pi Y^2$. If $aX^2 + b\pi Y^2$ represents 1 we are done, otherwise $v(a-1) \leq v(4)$ by Proposition 1.4.1. If $v(a-1) = v(4)$ then by Corollary 1.4.8 $a \in \Delta K^2$ and thus $aX^2 + b\pi Y^2$ represents Δ, whereby we are also done. If $v(a-1) < v(4)$, we will explain how one can find a unit a' represented by $aX^2 + b\pi Y^2$ with $v(a-1) < v(a'-1)$; applying this result and Lemma 1.5.6 inductively will eventually

yield an element a represented by the form with $v(a-1) \geq v(4)$, thereby concluding the proof. Write $a - 1 = \beta\pi^k$ for some $\beta \in \mathcal{O}^\times$, $k = v(a-1)$.

First, suppose that k is even. Then choose a $\lambda \in \mathcal{O}^\times$ with $\lambda^2 \equiv \beta \bmod \pi\mathcal{O}$ (possible by the perfectness of the residue field). Using that $2\lambda\pi^{\frac{k}{2}} \equiv 0 \bmod \pi^{k+1}\mathcal{O}$ because $v(2) = \frac{v(4)}{2} > \frac{k}{2}$ we observe that

$$a = 1 + \beta\pi^k \equiv 1 + \lambda^2\pi^k \equiv (1 + \lambda\pi^{k/2})^2 \bmod \pi^{k+1}\mathcal{O}.$$

Then $a' = a/(1 + \lambda\pi^{k/2})^2$ is represented by $aX^2 + b\pi Y^2$ and $v(a' - 1) \geq k + 1$.

Now suppose that k is odd. This time choose $\lambda \in \mathcal{O}^\times$ with $\lambda^2 b \equiv -\beta \bmod \pi\mathcal{O}$. Then $aX^2 + b\pi Y^2$ represents

$$a' = a + b\pi(\lambda\pi^{\frac{k-1}{2}})^2 = 1 + \beta\pi^k + \lambda^2 b\pi^k \equiv 1 \bmod \pi^{k+1}\mathcal{O}$$

by the fact that k is odd. □

1.5.8 Proposition. *Suppose* $\mathrm{char}(K) \neq 2$. *Up to K-isomorphism, there is a unique non-split quaternion algebra over K.*

Proof. By Proposition 1.5.5, (Δ, π) is non-split if $v(\pi) = 1$. This shows the existence.

We now show that every non-split quaternion algebra is isomoprhic to this (Δ, π). For this, it suffices to show this for a set of quaternion algebras generating the quaternion part of the Brauer group of K. Such a set is given by the quaternions of the form $(a, b\pi)$ for with $a, b \in \mathcal{O}^\times$. So suppose that $a, b \in \mathcal{O}^\times$ are such that $(a, b\pi)$ is non-split.

Even when we only assume $a, b \in \mathcal{O}^\times$, we have by Proposition 1.5.5 that (a, Δ) and $(\Delta, b\Delta)$ are split. If $(a, b\pi)$ is non-split, then $aX^2 + b\pi Y^2$ does not represent 1. By Lemma 1.5.7 it must then represent Δ, whereby $a\Delta X^2 + b\pi\Delta Y^2$ represents 1, hence $(a\Delta, b\pi\Delta)$ is split. Denoting Brauer equivalence by $\sim$, we can now compute:

$$\begin{aligned}(a, b\pi) &\sim (a, b\pi) \otimes (a, \Delta) \otimes (a\Delta, b\pi\Delta) \otimes (\Delta, b\Delta) \sim (a, b\pi\Delta) \otimes (a\Delta, b\pi\Delta) \otimes (\Delta, b\Delta) \\ &\sim (\Delta, b\pi\Delta) \otimes (\Delta, b\Delta) \sim (\Delta, \pi)\end{aligned}$$

whereby indeed $(a, b\pi)$ is isomorphic to (Δ, π). □

For a central simple algebra A over K and a field extension L/K, denote by A_L the central simple algebra $A \otimes_K L$ over L.

1.5.9 Proposition. *Suppose* $\mathrm{char}(K) \neq 2$. *Let Q be a quaternion algebra over K, L/K a quadratic extension. Then Q_L is split.*

Proof. Note that, as we excluded the case $\mathrm{char}(K) = 2$, the extension is always separable. We will make a case distinction on whether L/K is unramified or ramified. Split quaternion algebras over K remain split over L; what we have to show by Proposition 1.5.8 is that $(\Delta, \pi)_L$ is split.

If L/K is unramified, then by Proposition 1.4.7 we have $L = K(\sqrt{\Delta})$. Then the first slot in (Δ, π) becomes a square, whereby $(\Delta, \pi)_L$ is trivially split.

Suppose now that L/K is ramified. Then π has value 2 in the normalised valuation on L, whereby $(\Delta, \pi)_L \cong (\Delta, u)_L$ for some $u \in L$ of value 0. Now apply Proposition 1.5.5 to the field L. □

We state the more general classification theorem for central simple algebras over local fields without proof. Note how the previous two propositions can be reobtained from it.

1.5.10 Theorem. *[Classification of central simple algebras over local fields] Let K be a non-archimedean local field. There is a canonical isomorphism $\mathcal{B}_K : \mathbf{B}(K) \to \mathbb{Q}/\mathbb{Z}$, where $\mathbf{B}(K)$ is the Brauer group of K. If L/K is a finite field extension of degree m and A a central simple algebra over K, then $\mathcal{B}_L(A_L) = m\mathcal{B}_K(A)$.*

Proof. See [Pie82, Section 17.10]. □

1.5.11 Proposition. *A set of representatives of the square classes of $\mathbb{Q}_2$ is given by $\{\pm 1, \pm 3, \pm 2, \pm 6\}$. There is a unique non-split quaternion algebra over $\mathbb{Q}_2$ up to isomorphism. The following table indicates for which values of a and b the quaternion algebra $(a, b)_2$ is split (1) or non-split (-1).*

a/b	*1*	*-1*	*2*	*-2*	*3*	*-3*	*6*	*-6*
1	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*
-1	*1*	*-1*	*1*	*-1*	*-1*	*1*	*-1*	*1*
2	*1*	*1*	*1*	*1*	*-1*	*-1*	*-1*	*-1*
-2	*1*	*-1*	*1*	*-1*	*1*	*-1*	*1*	*-1*
3	*1*	*-1*	*-1*	*1*	*-1*	*1*	*1*	*-1*
-3	*1*	*1*	*-1*	*-1*	*1*	*1*	*-1*	*-1*
6	*1*	*-1*	*-1*	*1*	*1*	*-1*	*-1*	*1*
-6	*1*	*1*	*-1*	*-1*	*-1*	*-1*	*1*	*1*

Proof. The fact that $\{\pm 1, \pm 3, \pm 2, \pm 6\}$ is a full set of representatives for the square classes of $\mathbb{Q}_2$ follows from Proposition 1.4.1: any element of $\mathbb{Q}_2$ is up to a square either in $\mathbb{Z}_2^\times$ or $2\mathbb{Z}_2^\times$, and elements of $\mathbb{Z}_2^\times$ are squares if and only if their residue is a square in $\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$. We first show that the following table is correct.

a/b	-1	-3	2
-1	-1	1	1
-3	1	1	-1
2	1	-1	1

Recall that $(a, b) \cong (b, a)$ is split over a field K if and only if the quadratic form $X^2 - aY^2$ represents b over K. Thus to explain the 1's in the above table, it suffices to observe the equalities below.

$$1^2 - (-1) \cdot 2^2 = 5 \equiv -3 \equiv 13 = 1^2 - (-3) \cdot 2^2 \mod 8$$
$$1^2 - (-1)^2 \cdot 1^2 = 2 = 2^2 - 2 \cdot 1^2$$

For the -1's, we have to show that the quadratic form $X^2 - aY^2 - bZ^2$ has a non-trivial solution $(x, y, z) \in \mathbb{Q}_2^3$. By homogeneity and using that $\mathbb{Q}_2$ is the fraction field of $\mathbb{Z}_2$, we may assume without loss of generality that such a solution lies in $\mathbb{Z}_2^3$, and that x, y and z are not all divisible by 2. Now one easily checks that for each of the quadratic forms $X^2 + Y^2 + Z^2$ and $X^2 - 2Y^2 + 3Z^2$ this cannot happen: for the first it suffices to note that $X^2 + Y^2 + Z^2$ is anisotropic over $\mathbb{Z}_2/4\mathbb{Z}_2 \cong \mathbb{Z}/4\mathbb{Z}$, for the second one observes that $X^2 - 2Y^2 + 3Z^2$ cannot have a root (x, y, z) modulo 8 if at least one of x, y, z is odd.

We conclude that the small table correctly shows which quaternion algebras are split. By Proposition 1.5.8, all non-split ones are isomorphic, and the set $\{-1,-3,2\}$ generates the square classes of $\mathbb{Q}_2$. Hence one obtains the large table from the small one by applying the bilinearity of the quaternion algebra symbol. □

1.5.12 Proposition. *Suppose* $\mathrm{char}(K) \neq 2$. *The set of* $(a,b) \in K^2$ *for which the quaternion algebra* $(a,b)_K$ *splits, is both open and closed.*

Proof. This follows from Corollary 1.4.3 and the fact that for any $a,b,c \in K^\times$, $(ac^2,b) \cong (a,b) \cong (a,bc^2)$. □

1.6 Approximation

1.6.1 Proposition (Continuous dependence of polynomial roots on coefficients)**.** *Let* $|.|$ *be an absolute value on* K *and*

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

a polynomial with roots $x_1,\ldots,x_m \in K$. *For all* $\varepsilon > 0$ *there exists a* $\delta > 0$ *such that whenever* $y_1,\ldots,y_n \in K$,

$$g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0 = \prod_{i=1}^{n}(X - y_i)$$

and $|a_i - b_i| < \delta$ *for all* $i \in \{0,\ldots,n-1\}$, *then to every* x_i *there exists at least one* y_j *with* $|x_i - y_j| < \varepsilon$.

Proof. Let x be a root of f, set

$$M = \max\{|a_i - b_i| \mid i = 0,\ldots,n-1\} \quad \text{and} \quad m = \min\{|x - y_i| \mid i = 1,\ldots,n\}.$$

Our aim is to show that, if δ is sufficiently small, $M < \delta$ implies $m < \varepsilon$. We would then have solved the problem for a fixed root x of f, but since there are only finitely many roots of f, we can calculate δ for each of them individually, then take the minimum of all these δ to solve the problem for all roots of f at once.

Observe that

$$m^n \leq \prod_{i=1}^{n}|x - y_i| = |g(x)| = |g(x) - f(x)| \leq \sum_{i=1}^{n}|a_i - b_i||x|^i \leq M\sum_{i=1}^{n}|x|^i.$$

If we take δ small enough, the right hand side can be made smaller than ε^n, implying that $m < \varepsilon$. □

1.6.2 Proposition (Krasner's Lemma)**.** *Let* $\mathcal{O}$ *be the valuation ring of a non-archimedean complete field* K, $f \in K[X]$ *an irreducible polynomial,* N/K *a finite extension splitting* f *and* v *a valuation on* N. *Take* $x = x_1 \in N$ *with* f *as minimal polynomial over* K. *Write* $f = \prod_{i=1}^{n}(X - x_i)$ *for some* $n \in \mathbb{N}, x_i \in N$. *If a* $y \in N$ *satisfies*

$$v(y - x) > \max\{v(x_i - x) \mid x_i \neq x\}$$

then $K(x,y)$ *is purely inseparable over* $K(y)$. *In particular, if* x *is separable over* K, *then* $x \in K(y)$.

Proof. We follow the proof of [EP05, Theorem 4.1.7.]. To show that $K(x,y)$ is purely inseparable over $K(y)$ is equivalent to showing that $\sigma(x) = x$ for every $K(y)$-automorphism σ of N. Suppose for the sake of a contradiction that $\sigma(x) \neq x$ for some $K(y)$-automorphism σ of N. We may replace N by a finite normal extension of $K(y)$ containing $K(x,y)$. As $\sigma(x)$ is a root of f different from x, we have

$$\delta = \max\{v(x_i - x) \mid x_i \neq x\} \geq v(\sigma(x) - x).$$

Since $N/K(y)$ is a finite extension, Proposition 1.3.3 implies that $v \circ \sigma = v$, as $v \circ \sigma$ is a valuation on N with the same restriction to $K(y)$ as v. We obtain

$$\begin{aligned} v(\sigma(x) - x) &= v((y - x) - (y - \sigma(x)) \geq \min\{v(y - x), v(y - \sigma(x))\} \\ &= \min\{v(y - x), v(\sigma(y - x)) = v(y - x) > \delta \geq v(\sigma(x) - x)\}, \end{aligned}$$

a contradiction. □

1.6.3 Corollary. *Let v be the normalised valuation on a non-archimedean local field K, $f \in K[X]$ an irreducible, monic and separable polynomial. If $g \in K[X]$ is another monic polynomial of the same degree such that f and g are sufficiently close (i.e. the maximum of the values of the coefficients of $f - g$ is sufficiently high), then g is also irreducible.*

Proof. Let N be the splitting field of f and extend v to N. Let x be a root of f in N. Since the coefficients of a polynomial depend continuously on the roots of the polynomial by Proposition 1.6.1, by choosing g close enough to f we can make g have a root $x' \in N$ such that $v(x - x')$ is bigger than $v(x - x_i)$ and $v(x' - x_i')$ for all Galois conjugates $x_2, \ldots, x_n$ of x and $x_2', \ldots, x_m'$ of x'. Krasner's lemma then yields that $K(x) = K(x')$. As x' is a root of g, g has the same degree as f and $K(x)$ has the same K-dimension as $K(x')$, we must have that g is the minimal polynomial of x'; in particular g is irreducible. □

1.6.4 Theorem (Artin-Whaples, Weak Approximation Theorem)**.** *Let $|.|_1, \ldots, |.|_n$ be pairwise non-equivalent absolute values on K. Then to any $x_1, \ldots, x_n \in K$ and $0 < \varepsilon \in \mathbb{R}$, there exists an $x \in K$ such that $|x - x_i|_i < \varepsilon$ for all i.*

Proof. See [EP05, Theorem 1.1.3]. □

1.7 Global fields

1.7.1 Definition. A *number field* is a finite extension of $\mathbb{Q}$, the field of rational numbers. An *algebraic function field* is a finite extension of $\mathbb{F}_p(T)$, where p is a prime number and $\mathbb{F}_p$ is the finite field with p elements. We call a field a *global field* if it is either a number field or an algebraic function field.

The reader might find it peculiar that an umbrella term is introduced for these two seemingly unrelated classes of fields. It will become clear throughout this section that both classes of fields have the property that their Brauer group is in a certain sense determined by the Brauer groups of their completions. Global fields are thus

fields which can be studied via their completions, which will turn out to always be local fields.

For the rest of the section, let K be a global field. We introduce some notation which we will use for global fields throughout this thesis. Denote by $\mathbb{P}'$ the collection of non-complex spots on K, let $\mathbb{P}$ be the subset of finite spots. For a spot $\mathfrak{p}$ of K we write $K_\mathfrak{p}$ for the completion of K with respect to this spot. We write $\mathcal{O}_\mathfrak{p}$ for the valuation ring of $K_\mathfrak{p}$ and $\mathcal{O}_{(\mathfrak{p})} = K \cap \mathcal{O}_\mathfrak{p}$. If $K = \mathbb{Q}$, we might instead write $\mathbb{Z}_p$ for the valuation ring of $\mathbb{Q}_p$ and $\mathbb{Z}_{(p)}$ for $\mathbb{Q} \cap \mathbb{Z}_{(p)}$. If K is a number field, $\mathcal{O}_K$ will denote its ring of integers, i.e. the integral closure of $\mathbb{Z}$ in K.

1.7.2 Theorem. *The completion with respect to any spot of K is a local field.*

Proof. By Theorem 1.2.3 we need only consider non-archimedean spots.

For $K = \mathbb{Q}$, the non-archimedean spots can be interpreted as prime numbers p and the corresponding completions are the local fields $\mathbb{Q}_p$. For $K = \mathbb{F}_p(T)$, the valuations are given by the (discrete) degree valuation and the (discrete) valuations at irreducible polynomials in $\mathbb{F}_p[T]$. In either case, the residue fields are finite-dimensional $\mathbb{F}_p$-vector spaces, hence finite. By Corollary 1.2.10 all completions are local fields.

Now let K be an arbitrary global field. Let F be equal to $\mathbb{Q}$ if K is a number field or $F = \mathbb{F}_p(T)$ if K is an algebraic function field of characteristic p. Set $n = [K : F]$ and let $\mathfrak{p}$ be a non-archimedean spot on K. Set $K_\mathfrak{p}$ for the completion of K with respect to the spot $\mathfrak{p}$ and let $F_\mathfrak{p}$ be the topological closure of F in $F_\mathfrak{p}$. Then $F_\mathfrak{p}$ is a complete field in which F is dense, and since we know that completions of F are local fields, $F_\mathfrak{p}$ is local. The subfield $KF_\mathfrak{p}$ of $K_\mathfrak{p}$ is a finite extension of $F_\mathfrak{p}$ of degree at most n, so by Proposition 1.3.3 it is again a local field. But $K \subseteq KF_\mathfrak{p} \subseteq K_\mathfrak{p}$, whereby we must have $K_\mathfrak{p} = KF_\mathfrak{p}$. In particular, $K_\mathfrak{p}$ is indeed a finite extension of $F_\mathfrak{p}$ and hence local. □

1.7.3 Proposition. *All spots on an algebraic function field are non-archimedean. If K is a number field and $n = [K : \mathbb{Q}]$, then there are precisely n archimedean spots on K.*

Proof. The place corresponding to an archimedean spot is an embedding into $\mathbb{C}$ by Theorem 1.2.3. An algebraic function field cannot embed into $\mathbb{C}$ and a number field of degree n over $\mathbb{Q}$ has precisely n embeddings into $\mathbb{C}$. □

Let A/K be a central simple algebra. We write $A_\mathfrak{p}$ for the central simple $K_\mathfrak{p}$-algebra $A \otimes_K K_\mathfrak{p}$. Finally, we denote $\Delta(A)$ for the set of all spots $\mathfrak{p}$ of K for which $A_\mathfrak{p}$ is not split.

We will now describe the Brauer group $\mathbf{B}(K)$ of a global field K. For a spot $\mathfrak{p}$ of K, we have a homomorphism of groups

$$\mathbf{B}(K) \to \mathbf{B}(K_\mathfrak{p}) : \overline{A} \mapsto \overline{A_\mathfrak{p}}$$

where $\overline{A}$ denotes the equivalence class of a central simple algebra. The fact that this map is well-defined follows from the fact that Brauer equivalence is preserved under field extensions. If we would know that for every central simple algebra A over K

there are only finitely many spots $\mathfrak{p}$ for which $A_\mathfrak{p}$ is non-split (i.e. $\Delta(A)$ is finite) then we could glue the above homomorphisms into a homomorphism of groups

$$\varphi : \mathbf{B}(K) \to \bigoplus_{\mathfrak{p}\in\mathbb{P}'} \mathbf{B}(K_\mathfrak{p}).$$

Recall from Theorem 1.5.10 that for a finite spot $\mathfrak{p}$ there is a canonical isomorphism

$$\mathcal{B}_\mathfrak{p} : \mathbf{B}(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z}.$$

By a theorem of Frobenius $\mathbf{B}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$; for a real spot $\mathfrak{p}$ on K, define the homomorphism

$$\mathcal{B}_\mathfrak{p} : \mathbf{B}(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z} : \overline{A} \mapsto \begin{cases} 0 & \text{if } A \text{ is split} \\ \frac{1}{2} & \text{if } A \text{ is non-split.} \end{cases}$$

Taking the sum over all $\mathfrak{p}$ yields a homomorphism of groups

$$\Sigma : \bigoplus_{\mathfrak{p}\in\mathbb{P}'} \mathbf{B}(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z} : (\overline{A_\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}'} \mapsto \sum_{\mathfrak{p}\in\mathbb{P}'} \mathcal{B}_\mathfrak{p}(\overline{A_\mathfrak{p}}).$$

Note that the sum always contains only finitely many non-zero terms, so this is well-defined. We are now ready to state the main result on central simple algebras over global fields.

1.7.4 Theorem. *Let K be a global field. For any central simple algebra A over K, $\Delta(A)$ is finite. With the above notations, we have an exact sequence of group homomorphisms*

$$0 \longrightarrow \mathbf{B}(K) \xrightarrow{\varphi} \bigoplus_{\mathfrak{p}\in\mathbb{P}'} \mathbf{B}(K_\mathfrak{p}) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Proof. See [NSW15, Theorem 8.1.17]. □

Note how much non-trivial information is contained in this sequence: it is not a priori clear that φ is injective or even that it is well-defined (i.e. that $\Delta(A)$ is always finite), or that $\operatorname{Ker}\Sigma \subseteq \operatorname{Im}\varphi$, or that $\operatorname{Ker}\Sigma \supseteq \operatorname{Im}\varphi$. We will state some corollaries of this sequence.

1.7.5 Theorem (Albert-Hasse-Brauer-Noether)**.** *Let A/K be a central simple algebra over a number field K. If $A_\mathfrak{p}$ splits for every spot $\mathfrak{p}$ of K, then A is already split over K.*

Proof. This is the injectivity of φ, so this is part of the exactness of the sequence. □

For a rational prime p and a number $a \in \mathbb{Z}_{(p)}$, we define the Legendre symbol:

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } a \in p\mathbb{Z}_{(p)} \\ 1 & \text{if } a \in \mathbb{Z}_{(p)}^{\times 2} \\ -1 & \text{if } a \in \mathbb{Z}_{(p)}^{\times} \setminus \mathbb{Z}_{(p)}^{\times 2} \end{cases}.$$

1.7.6 Proposition. *Let $a, b \in \mathbb{Q}^\times$ and p a rational prime different from 2. Then $p \in \Delta((a,b))$ if and only if one of the following holds:*

(a) $v_p(a)$ *is odd,* $v_p(b)$ *is even and* $\left(\frac{bp^{-v(b)}}{p}\right) = -1$.

(b) $v_p(b)$ *is odd,* $v_p(a)$ *is even and* $\left(\frac{ap^{-v(a)}}{p}\right) = -1$..

(c) $v_p(a)$ *and* $v_p(b)$ *are odd and* $\left(\frac{-abp^{-v(ab)}}{p}\right) = -1$.

Proof. Direct application of Proposition 1.5.2. □

1.7.7 Theorem (Hilbert reciprocity)**.** *Let Q be a quaternion algebra over a global field K. The set of spots of K over which Q is non-split contains a finite, even number of elements.*

Proof. If Q is a quaternion algebra, so is $Q_\mathfrak{p}$ for a spot $\mathfrak{p}$ on K. Denoting by $\mathbf{B}_2(K_\mathfrak{p})$ the subgroup of $\mathbf{B}(K_\mathfrak{p})$ generated by quaternion algebras, φ maps Q to an element of $\bigoplus_{\mathfrak{p}\in\mathbb{P}'} \mathbf{B}_2(K_\mathfrak{p})$. By Proposition 1.5.8 (or the well-known Brauer group of $\mathbb{R}$) we have that $\mathbf{B}_2(K_\mathfrak{p}) \cong \mathbb{Z}/2\mathbb{Z}$, whereby we can see $\varphi(Q)$ as en element of $(\mathbb{Z}/2\mathbb{Z})^{(\mathbb{P}')}$. Theorem 1.7.4 implies that $\Sigma \circ \varphi = 0$, meaning that an even number of components of $\varphi(Q)$ is equal to 1, which is precisely what we needed to prove.

We give an elementary proof of the fact that $\Sigma \circ \varphi|_{\mathbf{B}_2(K)} = 0$ for $K = \mathbb{Q}$ as a corollary of the quadratic reciprocity law.

Consider $\mathbb{P}$ as the set of prime numbers and $\mathbb{P}'$ as $\mathbb{P} \cup \{\infty\}$. It follows from Proposition 1.5.2 that for any $p \in \mathbb{P}\setminus\{2\}$ we have $p \notin \Delta((a,b))$ when $v_p(a)$ and $v_p(b)$ are even. In particular, $\Delta((a,b))$ is always finite, so indeed $\varphi((a,b)) \in (\mathbb{Z}/2\mathbb{Z})^{(\mathbb{P}')}$ and $\Sigma \circ \varphi|_{\mathbf{B}_2(\mathbb{Q})}$ is well-defined.

To show that $\Sigma \circ \varphi|_{\mathbf{B}_2(\mathbb{Q})} = 0$, it suffices to show that $\Sigma \circ \varphi|_{\mathbf{B}_2(\mathbb{Q})}$ is zero on a generating set of $\mathbf{B}_2(\mathbb{Q})$. Such a generating set is given, for example, by the quaternion algebras of the form $(p,q), (p,-1)$ and $(-1,-1)$ where $p, q \in \mathbb{P}$.

We know that $\Delta((-1,-1)) = \{\infty, 2\}$. For $p \in \mathbb{P}$, by our previous remark the only candidates for spots which might be contained in $\Delta((p,-1))$ are p and 2; we need to show that either both or neither of them are contained in $\Delta((p,-1))$. Indeed we have $\Delta((2,-1)) = \emptyset$ and for p odd:

$$2 \in \Delta((p,-1)) \Leftrightarrow p \equiv 3 \bmod 4 \Leftrightarrow \left(\frac{-1}{p}\right) = -1 \Leftrightarrow p \in \Delta((p,-1)).$$

Now let $p, q \in \mathbb{P}$; we aim to show that $\Delta((p,q))$ contains either zero or two elements. Again there are only three candidates for primes which might be contained in $\Delta((p,q))$: p, q and 2.

If $p = q = 2$, it follows from Proposition 1.5.11 that $(2,2)_2$ is split, whereby $\Delta((2,2))$ is empty. If $p = 2$ and q is some odd prime, we have by Proposition 1.7.6

$$q \in \Delta((2,q)) \Leftrightarrow \left(\frac{2}{q}\right) = -1 \Leftrightarrow q \equiv \pm 3 \bmod 8,$$

which, by Proposition 1.5.11, is equivalent to $2 \in \Delta((2,q))$.

Now suppose that p and q are both odd. We have by Proposition 1.5.11 that $2 \in \Delta((p,q))$ if and only if $p \equiv q \equiv 3 \bmod 4$. On the other hand, by Proposition 1.7.6

and quadratic reciprocity,

$$p \in \Delta((p,q)) \Leftrightarrow \left(\frac{q}{p}\right) = -1 \Leftrightarrow \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)(q-1)}{4}} = -1$$
$$\Leftrightarrow \begin{cases} \left(\frac{p}{q}\right) = 1 & \text{if } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right) = -1 & \text{otherwise} \end{cases}$$
$$\Leftrightarrow \begin{cases} q \notin \Delta((p,q)) & \text{if } p \equiv q \equiv 3 \bmod 4 \\ q \in \Delta((p,q)) & \text{otherwise} \end{cases}.$$

All this together yields that, indeed, $\Delta((p,q))$ contains either zero or two elements. □

The fact that $\operatorname{Ker}\Sigma \subseteq \operatorname{Im}\varphi$ in the exact sequence in Theorem 1.7.4 implies that for any set $S \subseteq \mathbb{P}'$ with an even number of elements, there exists a quaternion algebra Q over K such that $\Delta(Q) = S$. The rest of the section will be about deriving a more concrete form of this result. We first state and prove a statement in the case $K = \mathbb{Q}$ based on Dirichlet's Theorem on arithmetic prime progressions, then derive the theorem for general K by invoking a result from class field theory.

1.7.8 Theorem. *Let S be a set consisting of a finite, even number of spots of $\mathbb{Q}$. To any $a \in \mathbb{Q}^\times$ such that for all $\mathfrak{p} \in S$, a is not a square in $\mathbb{Q}_\mathfrak{p}$, there exists a $b \in \mathbb{Q}^\times$ such that one can take $\Delta((a,b)) = S$.*

Proof. Again denote by $\mathbb{P}$ the set of prime numbers and interpret $\mathbb{P}' = \mathbb{P} \cup \{\infty\}$ as the set of spots. Let $a \in K^\times$ be as in the statement; define T to be the finite set of prime numbers p for which $v_p(a)$ is odd. Let b' be - up to a minus sign - the product of the prime numbers in $S \setminus T$ and let b' be negative if and only if $\infty \in S$. By Dirichlet's Theorem on arithmetic prime progressions, pick a positive prime number $q \notin S \cup T$ satisfying the following congruences:

(i) For all $p \in S \cap T \setminus \{2\}$, qb' is a non-square modulo p.

(ii) For all $p \in T \setminus S$, $qb' \equiv 1 \bmod p$.

(iii) The residue of $qb' \bmod 8$ is such that $2 \in \Delta((a, qb'))$ if and only if $2 \in S$. Such a residue exists by Proposition 1.5.11.

Set $b = qb'$. By Proposition 1.7.6 these conditions and the fact that q is a prime number guarantee that

$$\Delta((a,b)) \cap T \subseteq S \subseteq \Delta((a,b)) \subseteq S \cup \{q\}.$$

So $\Delta((a,b))$ is either S or $S \cup \{q\}$; by Hilbert reciprocity we must in fact have $S = \Delta((a,b))$. □

We introduce some concepts from global class field theory. The *idele group* J_K of K is the subgroup of $\prod_{\mathfrak{p}\in\mathbb{P}'} K_\mathfrak{p}^\times$ consisting of elements $(i_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}'}$ such that $|i_\mathfrak{p}|_\mathfrak{p} = 1$ for all but finitely many $\mathfrak{p} \in \mathbb{P}'$. Here $|.|_\mathfrak{p}$ is a absolute value on $K_\mathfrak{p}$ extending an absolute value in $\mathfrak{p}$; by Proposition 1.1.2 the definition of J_K does not depend on

the choice of $|.|_\mathfrak{p}$. The elements of J_K are called *ideles* of K. The image of the embedding $K^\times \to J_K : a \mapsto (a)_{\mathfrak{p}\in\mathbb{P}'}$ is denoted by P_K and called the subgroup of *principal ideles*.

Let L/K be a separable finite extension of global fields. For a spot $\mathfrak{q}$ of L lying over a spot $\mathfrak{p}$ of K, the topological closure of K in $L_\mathfrak{q}$ is isomorphic to $K_\mathfrak{p}$ (by the proof of Theorem 1.7.2) whereby we can consider $K_\mathfrak{p}$ as a subfield of $L_\mathfrak{q}$. We also have just like in the proof of Theorem 1.7.2 that $L_\mathfrak{q} = LK_\mathfrak{p}$, whereby $[L_\mathfrak{q} : K_\mathfrak{p}] \leq [L : K]$. We define the *idele norm map* $N_{L/K} : J_L \to J_K$ by $N_{L/K}((b_\mathfrak{q})_\mathfrak{q}) = (a_\mathfrak{p})_\mathfrak{p}$ where

$$a_\mathfrak{p} = \prod_\mathfrak{q} N_{L_\mathfrak{q}/K_\mathfrak{p}}(b_\mathfrak{q})$$

and $\mathfrak{q}$ runs over all (finitely many) spots lying over $\mathfrak{p}$. Denote the image of this map by $N_{L/K}J_L$.

1.7.9 Lemma. *Let L/K be a separable quadratic extension of global fields. Then*

$$[J_K : P_K N_{L/K} J_L] = 2.$$

Proof. This is a special case of a much more general theorem from global class field theory called the Artin Reciprocity Law; see [Tat67, Section 5] for details. □

1.7.10 Theorem. *Let K be a global field,* $\mathrm{char}(K) \neq 2$. *Let S be a set consisting of a finite, even number of non-complex spots of K. Let $a \in K^\times$, set $L = K[\sqrt{a}]$ and suppose that for all $\mathfrak{p} \in S$, the extension $L_\mathfrak{p}/K_\mathfrak{p}$ is unramified and quadratic. Then there exists a $b \in K^\times$ such that $\Delta((a,b)_K) = S$.*

Proof. We follow the approach of [OMe00, 71:19]. If $S = \emptyset$ we can just set $b = 1$; suppose from now on that $S \neq \emptyset$. Consider the homomorphism of groups

$$\varphi : J_K \to (\mathbb{Z}/2\mathbb{Z})^{(\mathbb{P}')} : (i_\mathfrak{p})_\mathfrak{p} \mapsto ((a, i_\mathfrak{p})_\mathfrak{p})_\mathfrak{p}$$

where we identify $(a, i_\mathfrak{p})_\mathfrak{p}$ with 0 if it is split and 1 if it is non-split. We observe that $N_{L/K}J_L \subseteq \operatorname{Ker}\varphi$. Indeed, if $i_\mathfrak{p} = N_{L_\mathfrak{q}/K_\mathfrak{p}}(j_\mathfrak{q})$, then using the fact that $L_\mathfrak{q} = LK_\mathfrak{p} = K_\mathfrak{p}\sqrt{a}]$, $i_\mathfrak{p}$ is represented over $K_\mathfrak{p}$ by the form $X^2 - aY^2$. This implies that $(a, i_\mathfrak{p})_\mathfrak{p}$ is split. The same holds when $i_\mathfrak{p}$ is a finite product of elements of the form $N_{L_\mathfrak{q}/K_\mathfrak{p}}(j_\mathfrak{q})$.

Let $\Sigma : (\mathbb{Z}/2\mathbb{Z})^{(\mathbb{P}')} \to \mathbb{Z}/2\mathbb{Z}$ the summation mapping and set $\Psi = \Sigma \circ \varphi$. As $N_{L/K}J_L \subseteq \operatorname{Ker}\varphi$ we definitely also have $N_{L/K}J_L \subseteq \operatorname{Ker}\Psi$. Hilbert Reciprocity says precisely that $P_K \subseteq \operatorname{Ker}\Psi$, whereby $P_K N_{L/K}J_L \subseteq \operatorname{Ker}\Psi$. But by the lemma $[J_K : P_K N_{L/K}J_L] = 2$ and clearly Ψ is surjective as S is non-empty, whereby we must have $\operatorname{Ker}\Psi = P_K N_{L/K}J_L$, i.e. we have an exact sequence

$$0 \longrightarrow P_K N_{L/K} J_L \longrightarrow J_K \xrightarrow{\Psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Using that for all $\mathfrak{p} \in S$ the extension $K_\mathfrak{p}[\sqrt{a}]/K_\mathfrak{p}$ is quadratic and unramified, there exists a $b_\mathfrak{p} \in K_\mathfrak{p}$ such that $(a, b_\mathfrak{p})_\mathfrak{p}$ is non-split; in fact just take any $b_\mathfrak{p}$ with odd value by Proposition 1.5.5. It follows that we can find an idele $(b_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}'} \in J_K$ such that $(a, b_\mathfrak{p})_\mathfrak{p}$ is non-split precisely for $\mathfrak{p} \in S$: if $\mathfrak{p} \notin S$, just set $b_\mathfrak{p} = 1$. As $\Psi((b_\mathfrak{p})_\mathfrak{p}) = 0$, by the exact sequence we have $(b_\mathfrak{p})_\mathfrak{p} \in P_K N_{L/K}J_L$. And since $N_{L/K}J_L \subseteq \operatorname{Ker}\varphi$, it follows that there is a $b \in K^\times$ such that $\varphi((b)_\mathfrak{p}) = \varphi((b_\mathfrak{p})_\mathfrak{p}) = ((a, b_\mathfrak{p})_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}'}$. This b does the job. □

1.7.11 Theorem. *Let K be a global field. Let S be a set consisting of a finite, even number of non-complex spots of K. Let $d \in K$ be such that $1 + 4d \neq 0$, set $L = K[X]/(X^2 - X - d)$ and suppose that for all $\mathfrak{p} \in S$, the extension $L_\mathfrak{p}/K_\mathfrak{p}$ is unramified and quadratic. Then there exists a $b \in K^\times$ such that $\Delta([d, b)_K) = S$.*

Proof. If $\mathrm{char}(K) \neq 2$ this is an immediate consequence of the previous theorem, as in this case $X^2 - X - d = (X - \frac{1}{2})^2 - (\frac{1}{4} + d)$, whereby $L = K[\sqrt{1 + 4d}]$, and furthermore $(1 + 4d, b)_K \cong [d, b)_K$.

Suppose now that $\mathrm{char}(K) = 2$. We may again assume that $S \neq \emptyset$ and set

$$\varphi : J_K \to (\mathbb{Z}/2\mathbb{Z})^{(\mathbb{P}')} : (i_\mathfrak{p})_\mathfrak{p} \mapsto ([d, i_\mathfrak{p})_\mathfrak{p})_\mathfrak{p}$$

where we identify $[d, i_\mathfrak{p})_\mathfrak{p}$ with 0 if it is split and 1 if it is non-split. We observe that $N_{L/K} J_L \subseteq \mathrm{Ker}\, \varphi$. Indeed, if $i_\mathfrak{p} = N_{L_\mathfrak{q}/K_\mathfrak{p}}(j_\mathfrak{q})$, then using the fact that $L_\mathfrak{q} = LK_\mathfrak{p} = K[X]/(X^2 - X - d)$, $j_\mathfrak{q}$ is represented over $K_\mathfrak{p}$ by the form $X^2 - XY - dY^2$. Because $\mathrm{char}(K) = 2$ this implies that the quadratic form

$$(1 + 4d)X^2 + i_\mathfrak{p}(Y^2 + YZ - dZ^2)$$

is isotropic over $K_\mathfrak{p}$, whereby $[d, i_\mathfrak{p})_\mathfrak{p}$ is split. The same holds when $i_\mathfrak{p}$ is a finite product of elements of the form $N_{L_\mathfrak{q}/K_\mathfrak{p}}(j_\mathfrak{q})$.

The rest of the proof is almost identical to that of the previous theorem, so we leave it out. □

Chapter 2

Logic, decidability and model theory

2.1 The language of rings

We work with the language of rings $\mathcal{L}_{\text{ring}} = (+, -, \cdot, 0, 1)$. This consists of all syntactically correct (see next paragraph) finite sequences one can build using these symbols together with the logical symbols $\forall, \exists, \neg, \wedge, \vee, (,), \doteq, \leftrightarrow, \rightarrow$ and a countable number of *variable symbols* $x_1, x_2, x_3, \ldots$. For the latter we might use other symbols (like $y_1, y_2, y_3, \ldots$ or $a, b, c, \ldots$) instead for convenience. The symbols $\forall, \exists$ are called *quantifiers*, whereas $\neg, \vee, \wedge, \leftrightarrow$ and $\rightarrow$ are called *connectives*. We call $\doteq$ the *equality symbol*.

The dot in $\doteq$ is used to stress that this symbol is used in the formal language: it is a purely syntactic entity which does not a priori imply the equality of any two mathematical objects. We therefore reserve the symbol $=$ to denote actual equality of mathematical objects.

Sequences in correct syntax will be called *formulas*. Some authors specifically call them 'syntactically correct formulas' or 'well-formed formulas'. When we speak about formulas, we automatically assume correct syntax. They can be defined by a two-step inductive definition.

1. We define what a *term* is:

   (a) A variable symbol x_i is a term. The constant symbols 0 or 1 are terms.

   (b) If t_1 and t_2 are terms, then so are $(t_1 + t_2)$, $(t_1 \cdot t_2)$ and $(t_1 - t_2)$.

2. We define what a *formula* is and what its *subformulas* are:

   (a) If t_1 and t_2 are terms, then $(t_1 \doteq t_2)$ is a formula. It has no subformulas.

   (b) If φ_1 and φ_2 are formulas and x_i is a variable, then $\forall x_i \varphi_1, \exists x_i \varphi_1, (\varphi_1 \vee \varphi_2), (\varphi_1 \wedge \varphi_2), (\varphi_1 \rightarrow \varphi_2), (\varphi_1 \leftrightarrow \varphi_2)$ and $\neg\varphi_1$ are formulas. The subformulas of $\forall x_i \varphi_1, \exists x_i \varphi_1$ and $\neg\varphi_1$ are exactly φ_1 and all of its subformulas. Similarly φ_1, φ_2 and all of their respective subformulas are by definition the subformulas of $(\varphi_1 \vee \varphi_2), (\varphi_1 \wedge \varphi_2), (\varphi_1 \rightarrow \varphi_2)$ and $(\varphi_1 \leftrightarrow \varphi_2)$

Examples of formulas are $((x \cdot y \doteq x+y) \to (x \doteq 0-1))$ and $(((1+1 \doteq 1) \wedge (x \doteq 1)) \vee \forall y(x \doteq 0))$. The subformulas of the first formula are $(x \cdot y \doteq x+y)$ and $(x \doteq 0-1)$. To increase readability, we will often suppress brackets when no confusion is possible; we would instead write the previous two formulas as $x \cdot y \doteq x+y \to x \doteq 0-1$ and $(1+1 \doteq 1 \wedge x \doteq 1) \vee \forall y(x \doteq 0)$. An example of a finite sequence of symbols which is not a formula: $1+1 \doteq +\forall(($.

To each formula φ we can assign a finite set of variable symbols, called its set of *free variables*. We denote this set as $\mathrm{Fr_v}(\varphi)$. It can again be defined inductively: if $\varphi = `t_1 \doteq t_2`$ (note that $=$ is used to indicate equality of two formulas, whereas $\doteq$ is still just a meaningless symbol), then $\mathrm{Fr_v}(\varphi)$ is defined to be the finite set of variables occurring in φ. If φ_1 and φ_2 are formulas of which the set of free variables is known, then we define:

- $\mathrm{Fr_v}(\varphi_1 \vee \varphi_2)$, $\mathrm{Fr_v}(\varphi_1 \wedge \varphi_2)$, $\mathrm{Fr_v}(\varphi_1 \to \varphi_2)$ and $\mathrm{Fr_v}(\varphi_1 \leftrightarrow \varphi_2)$ to be equal to $\mathrm{Fr_v}(\varphi_1) \cup \mathrm{Fr_v}(\varphi_2)$.
- $\mathrm{Fr_v}(\neg\varphi_1)$ to equal $\mathrm{Fr_v}(\varphi_1)$.
- $\mathrm{Fr_v}(\forall x_i \varphi_1)$ and $\mathrm{Fr_v}(\exists x_i \varphi_1)$ to equal $\mathrm{Fr_v}(\varphi_1) \setminus \{x_i\}$.

We say a formula is a *statement* if its set of free variables is empty. Furthermore, given an instance of a variable x in a formula φ, we say it *occurs freely* in φ if it is a free variable of both φ and all subformulas of φ containing this instance of x. For example in the formula $x \doteq 0 \to \forall x(x \doteq 1)$ the first variable symbol x occurs freely, but the last one does not.

A set R together with functions $+_R, -_R, \cdot_R : R \times R \to R$ and constants $0_R, 1_R \in R$ is called an $\mathcal{L}_{\mathrm{ring}}$-*structure*. Note that we do not impose any conditions on these functions and constants, in particular we do not require that R be a ring.

We want to be able to interpret statements in structures, e.g. we want to read a statement like

$$\forall x \exists y(x \cdot y \doteq 1)$$

as: "For all elements $x \in R$, there exists an element $y \in R$ with the property that $x \cdot_R y = 1_R$." The above statement is then said to be true in structures where every element has a 'right inverse' (for lack of a better word in structures which might not be rings), and false in structures where this is not the case. Formally defining truth of statements via induction is a bit trickier, since, even though the formula given above is a statement, some of its subformulas (like $\exists y(x \cdot y \doteq 1)$) are not; they are just formulas. To tackle this problem, we need to add additional symbols to the language $\mathcal{L}_{\mathrm{ring}}$.

We extend the language $\mathcal{L}_{\mathrm{ring}}$ to the language $\mathcal{L}_{\mathrm{ring}+R}$ for a ring R, which contains the formulas made with the symbols of $\mathcal{L}_{\mathrm{ring}}$, as well as a new constant symbol $\tilde{r}$ for every element $r \in R$. These constant symbols have the same syntactical roles as the constants 0 and 1 in $\mathcal{L}_{\mathrm{ring}}$. An $\mathcal{L}_{\mathrm{ring}}$-structure R can naturally be considered an $\mathcal{L}_{\mathrm{ring}+R}$-structure by interpreting $\tilde{r}$ as r for each $r \in R$, i.e., $\tilde{r}_R = r$. Finally, given an $\mathcal{L}_{\mathrm{ring}+R}$-formula φ and $r_1, \ldots, r_n \in R$, we denote $\varphi(x_1/\tilde{r_1}, \ldots, x_r/\tilde{r_n})$ for the $\mathcal{L}_{\mathrm{ring}+R}$-formula obtained by replacing every freely occurring instance of x_i in φ by $\tilde{r_i}$.

We can now define inductively when an $\mathcal{L}_{\mathrm{ring}+R}$-statement is *true* in R (or *holds in* R). For a statement φ we denote $R \models \varphi$ if φ holds in R and $R \not\models \varphi$ otherwise.

1. If $\varphi = t_1 \doteq t_2$ for some terms t_1 and t_2, then we say $R \models \varphi$ if and only if $t_1^R = t_2^R$, where t_1^R (respectively t_2^R) is obtained from t_1 (resp. t_2) by replacing all instances of $+$ by $+_R$, $-$ by $-_R$, $\cdot$ by $\cdot_R$, 0 by 0_R, 1 by 1_R and $\tilde{r}$ by $\tilde{r}_R = r$.

2. If φ_1 and φ_2 are $\mathcal{L}_{\mathrm{ring}+R}$-statements, then $R \models \varphi_1 \wedge \varphi_2$ if and only if $R \models \varphi_1$ and $R \models \varphi_2$. Similarly, we interpret $\vee$ as 'or', $\neg$ as 'not', $\rightarrow$ as 'implies' and $\leftrightarrow$ as 'is equivalent to'.

3. $R \models \forall x \varphi$ (respectively $R \models \exists x \varphi$) if and only if $R \models \varphi(x/\tilde{r})$ for all $r \in R$ (respectively for some $r \in R$).

When φ is a formula with $\mathrm{Fr_v}(\varphi) \subseteq \{x_1, \ldots, x_n\}$, we will often simply denote $\varphi(r_1, \ldots, r_n)$ instead of $\varphi(x_1/\tilde{r_1}, \ldots, x_n/\tilde{r_n})$ if no confusion is possible.

Let $\mathcal{R}$ be a class of $\mathcal{L}_{\mathrm{ring}}$-structures. We say that two formulas $\varphi_1(x_1, \ldots, x_m)$ and $\varphi_2(x_1, \ldots, x_m)$ with $\mathrm{Fr_v}(\varphi_1) \cup \mathrm{Fr_v}(\varphi_2) = \{x_1, \ldots, x_m\}$ are *equivalent in* $\mathcal{R}$ if for all $R \in \mathcal{R}$ and for all $(r_1, \ldots, r_m) \in R^m$ we have $R \models \varphi_1(r_1, \ldots, r_m)$ if and only if $R \models \varphi_2(r_1, \ldots, r_m)$.

It is a tautology from propositional logic that the formula $\varphi_1 \wedge \varphi_2$ is equivalent in the class of $\mathcal{L}_{\mathrm{ring}}$-structures to $\neg(\neg\varphi_1 \vee \neg\varphi_2)$. Similarly, $\varphi_1 \rightarrow \varphi_2$ is the same as $\neg\varphi_1 \vee \varphi_2$, $\varphi_1 \leftrightarrow \varphi_2$ is the same as $(\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1)$ and $\forall x \varphi$ is the same as $\neg\exists x \neg\varphi$. When we prove the truth of a certain set of formulas in a certain class of structures by induction on the length of the formula, it often suffices to consider the connectives $\neg$ and $\wedge$ and the quantifier $\exists$ in the induction step, since we may assume that any formula has been replaced by an equivalent formula using only those connectives and quantifier.

Finally, we will call an injective map $\sigma : R \rightarrow R'$ between $\mathcal{L}_{\mathrm{ring}}$-structures R and R' an *embedding* of $\mathcal{L}_{\mathrm{ring}}$-structures if it respects all functions and constants, i.e. one has $\sigma(0_R) = 0_{R'}$, $\sigma(x +_R y) = \sigma(x) +_{R'} \sigma(y)$ for all $x, y \in R$, and similarly for 1, $-$ and $\cdot$. If additionally σ is surjective, we call σ an *isomorphism* of $\mathcal{L}_{\mathrm{ring}}$-structures; one easily verifies that in this case, σ^{-1} is also an isomorphism. If $R \subseteq R'$ are $\mathcal{L}_{\mathrm{ring}}$-structures and the inclusion map $R \rightarrow R'$ is an embedding, we call R an $\mathcal{L}_{\mathrm{ring}}$-*substructure* of R'. If R' and R are rings this coincides with the notion of a subring.

2.2 Definability and existential definability

2.2.1 Definition. Let φ be a formula in $\mathcal{L}_{\mathrm{ring}}$ (respectively $\mathcal{L}_{\mathrm{ring}+R}$) with an arbitrary number of free variables. We call φ:

1. *quantifier-free* if no quantifiers occur in φ.

2. *positive* if φ is quantifier-free and the only logical connectives occurring in φ are $\wedge$ and $\vee$.

3. *elementary* if $\varphi = f(y_1, \ldots, y_m) \doteq 0$ for some $m \in \mathbb{N}$, free variables $y_1, \ldots, y_m$ and a polynomial $f \in \mathbb{Z}[Y_1, \ldots, Y_m]$ (respectively $f \in R[Y_1, \ldots, Y_m]$).

4. *existential* (respectively *positive-existential*) if $\varphi = \exists x_1, \ldots, x_n \psi$ where $n \in \mathbb{N}$ and ψ is quantifier-free (respectively positive).

5. *diophantine* if $\varphi = \exists x_1, \ldots, x_n \psi$ where $n \in \mathbb{N}$ and ψ is elementary.

2.2.2 Definition. Let R be a ring, $n \in \mathbb{N}$. A subset A of R^n is called *definable* if there exists a formula φ in $\mathcal{L}_{\text{ring}}$ with $\text{Fr}_{\text{v}}(\varphi) \subseteq \{t_1, \ldots, t_n\}$ as free variables and such that $A = \{(t_1, \ldots, t_n) \in R^n \mid R \models \varphi(t_1, \ldots, t_n)\}$. We say that φ *defines* A in R^n. Furthermore, if φ can be chosen to be quantifier-free (respectively elementary, positive, existential, positive-existential or diophantine), then we also use the same term for A.

2.2.3 Examples.

1. The set of primes in $\mathbb{Z}$ is defined by

$$\varphi(t) = \neg(t \doteq 0 \vee t \doteq 1) \wedge \forall x, y(x \cdot x \doteq 1 \vee y \cdot y \doteq 1 \vee \neg(x \cdot y \doteq t)).$$

2. The set $\mathbb{N}$ is diophantine in $\mathbb{Z}$ and defined by

$$\varphi(t) = \exists x_1, x_2, x_3, x_4(t \doteq x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

   by the Four-Square Theorem. The same definition defines the set of non-negative numbers in $\mathbb{Q}$.

3. If R is a domain, then its positive and elementary subsets are precisely R itself and all finite sets, as any non-zero polynomial has only finitely many zeroes in R. Its quantifier-free subsets are precisely all finite and cofinite sets.

4. If K is a field and $n \in \mathbb{N}$, then the positive subsets of K^n are the algebraic varieties in K^n. The positive-existential subsets are the projections of algebraic varieties from higher-dimensional K-spaces to K^n.

5. The closed unit ball in $\mathbb{R}^n$ is diophantine and defined by

$$\varphi(x_1, \ldots, x_n) = \exists y \left(1 - \sum_{i=1}^{n} x_i^2 \doteq y^2\right)$$

2.2.4 Proposition. *Let R be a ring, A and B subsets. If A and B are both definable (respectively quantifier-free, positive, existential, positive-existential), then so are their union and intersection. If A is definable (respectively quantifier-free), then so is $R \setminus A$.*

Proof. Combine the following observations for general formulas φ_1 and φ_2:

$$\{\underline{t} \in R \mid R \models \varphi_1(\underline{t})\} \cup \{\underline{t} \in R \mid R \models \varphi_2(\underline{t})\} = \{\underline{t} \in R \mid R \models \varphi_1(\underline{t}) \vee \varphi_2(\underline{t})\}$$
$$\{\underline{t} \in R \mid R \models \varphi_1(\underline{t})\} \cap \{\underline{t} \in R \mid R \models \varphi_2(\underline{t})\} = \{\underline{t} \in R \mid R \models \varphi_1(\underline{t}) \wedge \varphi_2(\underline{t})\}$$
$$R \setminus \{\underline{t} \in R \mid R \models \varphi_1(\underline{t})\} = \{\underline{t} \in R \mid R \models \neg\varphi_1(\underline{t})\}$$
$$R \models \exists x_1, \ldots x_n \varphi_1 \vee \exists y_1, \ldots, y_m \varphi_2 \Leftrightarrow R \models \exists x_1, \ldots, x_n, y_1, \ldots, y_m(\varphi_1 \vee \varphi_2)$$
$$R \models \exists x_1, \ldots x_n \varphi_1 \wedge \exists y_1, \ldots, y_m \varphi_2 \Leftrightarrow R \models \exists x_1, \ldots, x_n, y_1, \ldots, y_m(\varphi_1 \wedge \varphi_2)$$

where in the last line one should take care that the symbols x_i and y_j are pairwise different. In the second to last line this is not needed; we can reformulate the definition with $\max\{n, m\}$ quantifiers instead of $n + m$. □

We now briefly focus our attention on the relation between the concepts of existential, positive-existential and diophantine sets. In general, we have that diophantine sets are positive-existential and positive-existential sets are existential, but none of these concepts coincide.

2.2.5 Proposition. *Let R be a domain with fraction field K, $n \in \mathbb{N}$ and A and B be diophantine (respectively elementary) subsets of R^n. Then $A \cup B$ is diophantine (respectively elementary). If the fraction field of R does not contain the algebraic closure of its prime field, then also $A \cap B$ is diophantine (respectively elementary). In particular, in the latter case, all positive-existential sets are diophantine (respectively all positive sets elementary).*

Proof. We will focus on the statements about diophantine sets; the statements about elementary sets follow by observing that no quantifiers are introduced in the proof. Let $A = \{\underline{t} \in R^n \mid R \models \exists x_1, \ldots, x_m(f(\underline{t}, x_1, \ldots, x_m) \doteq 0)\}$ and $B = \{\underline{t} \in R^n \mid R \models \exists y_1, \ldots, y_p(g(\underline{t}, y_1, \ldots, y_p) \doteq 0)\}$ for some $m, p \in \mathbb{N}$ and $f \in \mathbb{Z}[T_1, \ldots, T_n, X_1, \ldots, X_m], g \in \mathbb{Z}[T_1, \ldots, T_n, Y_1, \ldots, Y_p]$.

The first statement is immediate, since

$$A \cup B = \{\underline{t} \in R^n \mid \exists x_1, \ldots, x_m, y_1, \ldots, y_p(f(\underline{t}, x_1, \ldots, x_m)g(\underline{t}, y_1, \ldots, y_p) \doteq 0)\}$$

holds when R is a domain (otherwise, only the inclusion from left to right holds).

For the second statement, fix a non-constant polynomial $F \in \mathbb{Z}[X]$ without roots in $\mathrm{Frac}(R)$. Homogenizing yields a form $F^* \in \mathbb{Z}[X, Y]$ which is anisotropic over R. We now have

$$A \cap B = \left\{ \underline{t} \in R^n \,\middle|\, \begin{array}{l} \exists x_1, \ldots, x_m, y_1, \ldots, y_m \\ (F^*((\underline{t}, x_1, \ldots, x_m), g(\underline{t}, y_1, \ldots, y_p)) \doteq 0) \end{array} \right\}.$$

From combining the last two statements it is clear that all positive-existential sets are diophantine. □

2.2.6 Example. Let R be any commutative ring. One easily verifies that the diophantine subsets of the product ring $R \times R$ are precisely the sets of the form $A \times A$ where A is a diophantine subset of the ring R. This makes it easy to construct examples of situations where the union of diophantine sets need no longer be diophantine. For example, if R is a field, then

$$R^\times = \{x \in R \mid R \models \exists y(x \cdot y \doteq 1)\}$$

is diophantine and so is $\{0\} = \{x \in R \mid R \models x \doteq 0\}$, implying that $R^\times \times R^\times$ and $\{(0, 0)\}$ are diophantine subsets of the product ring $R \times R$, defined by the same formulae. Their union $(R^\times \times R^\times) \cup \{(0, 0)\}$ is not of the form $A \times A$ for $A \subseteq R$ and hence not diophantine.

2.2.7 Example. Let R be an algebraically closed field. The subset

$$\{(0, 0)\} = \{(x, y) \in R^2 \mid R \models x \doteq 0\} \cap \{(x, y) \in R^2 \mid R \models y \doteq 0\}$$

of R^2 (now considered as an affine space over R, not as the product ring) is an intersection of two diophantine sets, but it is not diophantine itself. Indeed, suppose we would have

$$\{(0, 0)\} = \{(x, y) \in R^2 \mid R \models \exists x_1, \ldots, x_n(f(x, y, x_1, \ldots, x_n) \doteq 0)\}$$

for some polynomial $f \in \mathbb{Z}[X, Y, X_1, \ldots, X_n]$. Then there exist $c_1, \ldots, c_n \in R$ such that $f(0, 0, c_1, \ldots, c_n) = 0$. But then there are infinitely many $(x, y) \in R^2$ for which $f(x, y, c_1, \ldots, c_n) = 0$ by the fact that R is algebraically closed, and all these (x, y) also lie in

$$\{(x, y) \in R^2 \mid R \models \exists x_1, \ldots, x_n (f(x, y, x_1, \ldots, x_n) \doteq 0)\},$$

contradicting the assumption that this set is equal to $\{(0, 0)\}$.

One has the following condition for the equality of existential and positive-existential sets:

2.2.8 Proposition. *Let R be a ring. Then the following are equivalent:*

(1) For all $n \in \mathbb{N}$, all existential subsets of R^n are positive-existential.

(2) $R \setminus \{0\}$ is positive-existential.

Proof. Since $R \setminus \{0\} = \{t \in R \mid t \neq 0\}$ is existential (even quantifier-free), the implication from (1) to (2) is clear. Suppose conversely that $R \setminus \{0\}$ is given by some positive-existential formula ψ.

By elementary logic, every quantifier-free formula in $\mathcal{L}_{\text{ring}}$ is equivalent (in the ring R) to a formula of the form

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \varphi_{i,j}$$

where $\varphi_{i,j}$ is either an elementary formula or the negation of an elementary formula. This can be seen by first translating formulas with the logical connectives $\rightarrow$ and $\leftrightarrow$ into equivalent formulas which only use $\wedge, \vee$ and $\neg$, then using De Morgan's laws to make sure $\neg$ is only found in front of elementary formulas, and finally using associativity and distributivity laws for $\wedge$ and $\vee$.

Using the two last formulas from the proof of Proposition 2.2.4, we conclude that all existential sets are finite unions of finite intersections of elementary sets and complements of elementary sets. Elementary sets are trivially positive-existential. If we can show that the complement of an elementary set is positive-existential, than we can use the result of Proposition 2.2.4 to conclude the proof.

So consider an elementary set $A = \{\underline{t} \in R^n \mid R \models f(\underline{t}) \doteq 0\}$. Then indeed:

$$R \setminus A = \{\underline{t} \in R^n \mid R \models \neg(f(\underline{t}) \doteq 0)\} = \{\underline{t} \in R^n \mid R \models \psi(f(\underline{t}))\}$$

□

2.2.9 Example. Let R be an infinite, compact Hausdorff topological ring (e.g. one can take $\mathbb{Z}_p$ - the ring of p-adic integers - which is also a noetherian domain). Let $n \in \mathbb{N}^+$. By definition, an elementary subset of R^n is given as the zero set of a polynomial $f \in R[X_1, \ldots, X_n]$. As polynomials are continuous functions, this zero set is a closed subset of R^n. Positive subsets of R^n are obtained by taking finite unions and intersections of elementary subsets of R^n, so they are again closed subsets of R^n. As R^n is compact, we even have that positive subsets are compact.

Now positive-existential subsets of R^n are obtained by projecting positive subsets of R^{n+m} for some $m \in \mathbb{N}$ onto R^n. In particular, as projections are continuous functions, we obtain that positive-existential subsets of R^n are always compact. And because R is infinite and compact, $R \setminus \{0\}$ is not closed, hence not compact, hence not positive-existential.

If R is a field, then finding an existential definition for $R \setminus \{0\}$ is not hard:

$$R \setminus \{0\} = \{t \in R \mid R \models \exists x(t \cdot x \doteq 1)\}.$$

The following proposition also gives a positive answer for some Dedekind domains, including the ring of integers of a number field. It is an adaptation of [Koe14, exercise 3.3.].

2.2.10 Proposition. *Let R be a Dedekind domain, $p, q \in \mathbb{Z}$ two different primes which are not invertible in R. For $t \in R$ we have that $t \neq 0$ if and only if there exists a $y \in R$ with $t \mid (py-1)(qy-1)$. Thus:*

$$R \setminus \{0\} = \{t \in R \mid R \models \exists x \exists y(t \cdot x \doteq (p \cdot y - 1) \cdot (q \cdot y - 1))\}.$$

Proof. As $(py-1)(qy-1)$ is never zero for $y \in R$, the direction from right to left is trivial. Conversely, take $t \in R \setminus \{0\}$. We have to show that $(pY-1)(qY-1)$ has a zero in R/tR. Remember that, in a Dedekind domain, every non-zero ideal is a product of maximal ideals. By the Chinese remainder theorem, we may therefore assume $tR = \mathfrak{p}^n$ for some maximal ideal $\mathfrak{p}$ of R. Since p and q cannot both lie in $\mathfrak{p}$ (as $ap + bq = 1$ for some $a, b \in \mathbb{Z}$), one of them must be invertible in $R/\mathfrak{p}^n$. But then this inverse is a root of $(pY-1)(qY-1)$ in $R/\mathfrak{p}^n$. □

2.2.11 Remark. In $\mathbb{Z}$, one could alternatively use the Four-Square Theorem to write $t - 1 \geq 0 \vee -t - 1 \geq 0$ into a diophantine formula, but this formula would introduce four extra quantifiers instead of two and similarly use a polynomial of degree four instead of two.

By combining the previous results with Proposition 2.2.5, we obtain the following.

2.2.12 Corollary. *Let R be either a global field or the ring of integers of a number field, $n \in \mathbb{N}$. Then the diophantine subsets of R^n, the positive-existential subsets of R^n and the existential subsets of R^n coincide.*

For later use, we spell out an important result on the first-order theory of algebraically closed fields

2.2.13 Proposition (Quantifier elimination in algebraically closed fields)**.** *Let $\mathcal{C}$ be the class of algebraically closed fields. In $\mathcal{C}$, every $\mathcal{L}_{ring}$-formula is equivalent to a quantifier-free formula.*

Proof. [PD11, Theorem 3.4.4] □

This also implies that the definable subsets of an algebraically closed field are the same as the quantifier-free sets, whereby only finite and cofinite sets can possibly be definable in an algebraically closed field.

2.3 Extended language of rings

In the language of rings, we can only make use of the constants 0 and 1 in our formulas. Through combination of these constants with the functions $+$ and $-$ we can also use integers as constants. This implies that we can de facto use any element of $\mathbb{Q}$ (respectively $\mathbb{F}_p$) as a constant when defining a subset of $\mathbb{Q}$ (respectively $\mathbb{F}_p$), as any equality of polynomials with coefficients in $\mathbb{Q}$ can be translated into an equality of polynomials over $\mathbb{Z}$ by multiplying out the denominators. In this sense, every formula in $\mathcal{L}_{\mathrm{ring}+\mathbb{Q}}$ is equivalent to a formula in $\mathcal{L}_{\mathrm{ring}}$.

In a ring R larger than $\mathbb{Q}$ or $\mathbb{F}_p$, allowing elements of R as constants will in general allow for more definable subsets.

2.3.1 Lemma. *Let R, R' be $\mathcal{L}_{ring}$-structures, $\sigma : R \to R'$ an isomorphism of $\mathcal{L}_{ring}$-structures. If $\psi(x_1, \ldots, x_m)$ is an $\mathcal{L}_{ring}$-formula with $\mathrm{Fr_v}(\psi) \subseteq \{x_1, \ldots, x_m\}$, then for $(r_1, \ldots, r_m) \in R^m$ we have*

$$R \models \psi(r_1, \ldots, r_m) \Leftrightarrow R' \models \psi(\sigma(r_1), \ldots, \sigma(r_m)).$$

Proof. We will show the statement by induction on the length of the formula ψ. In each step we need only prove the implication from left to right; the other follows by applying the same argument to σ^{-1}.

1. If $\psi(x_1, \ldots, x_m)$ is of the form $t_1(x_1, \ldots, x_m) \doteq t_2(x_1, \ldots, x_m)$ for some terms t_1 and t_2, then the implication follows from the fact that σ respects constants and all operations (i.e. $t_1^{R'}(\sigma(r_1), \ldots, \sigma(r_m)) = \sigma(t_1^R(r_1, \ldots, r_m))$ and similarly for t_2).

2. Clearly if the statement is true for ψ_1 and ψ_2, then it is true if ψ is equal to $\psi_1 \wedge \psi_2$.

3. Assume $\psi = \neg\psi_1$. Suppose $(r_1, \ldots, r_m) \in R^m$ is such that $R \models \psi(r_1, \ldots, r_m)$, i.e. $R \not\models \psi_1(r_1, \ldots, r_m)$. Then by induction hypothesis (direction right to left), $R' \not\models \psi_1(\sigma(r_1), \ldots, \sigma(r_m))$, whereby indeed $R' \models \psi(\sigma(r_1), \ldots, \sigma(r_m))$.

4. Suppose now that $\psi = \exists x_{m+1}\psi_1(x_1, \ldots, x_m, x_{m+1})$. If $R \models \psi(r_1, \ldots, r_m)$, then $R \models \psi_1(r_1, \ldots, r_m, r)$ for some $r \in R$. But then by induction hypothesis $R' \models \psi_1(\sigma(r_1), \ldots, \sigma(r_m), \sigma(r))$, whereby also $R' \models \psi(\sigma(r_1), \ldots, \sigma(r_m))$.

□

2.3.2 Proposition. *Let R be an $\mathcal{L}_{ring}$-structure, σ an automorphism of R, $m \in \mathbb{N}$. If $S \subseteq R^m$ is definable in $\mathcal{L}_{ring}$, then $S = \sigma(S)$ where we define*

$$\sigma(S) = \{(\sigma(x_1), \ldots, \sigma(x_m)) \mid (x_1, \ldots, x_m) \in S\}.$$

Proof. Apply Lemma 2.3.1 to the definition of S. □

It follows in particular that in a number field K, only sets which are invariant under conjugation can be defined in $\mathcal{L}_{\mathrm{ring}}$, whereas in $\mathcal{L}_{\mathrm{ring}+K}$, also other sets (e.g. sets of the form $\{x\}$ for $x \in K \setminus \mathbb{Q}$) can be defined. We will show that this is the only thing we gain when passing from $\mathcal{L}_{\mathrm{ring}}$ to $\mathcal{L}_{\mathrm{ring}+K}$.

2.3.3 Proposition. *Let L/K be a simple, finite field extension, $m \in \mathbb{N}$, $S \subseteq K^m$ a subset which is definable in $\mathcal{L}_{ring+L}$ and such that $S = \sigma(S)$ for all K-automorphisms of L. Then S is definable in $\mathcal{L}_{ring+K}$ with one additional existential quantifier. In particular, if S is positive-existential in $\mathcal{L}_{ring+L}$, then also in $\mathcal{L}_{ring+K}$.*

Proof. Fix a primitve element p of L/K. By writing out all constants in the $\mathcal{L}_{\text{ring}+K}$-definition of S as a K-linear combination of powers of p, we may assume there exists an $\mathcal{L}_{\text{ring}+K}$-formula $\varphi(x_1, \ldots, x_m, c)$ such that

$$S = \{(x_1, \ldots, x_m) \in L^m \mid L \models \varphi(x_1, \ldots, x_m, p)\}.$$

Let $f \in K[T]$ be the minimal polynomial of p over K. We are done if we can show that

$$S = \{(x_1, \ldots, x_m) \in L^m \mid L \models \exists c(f(c) \doteq 0 \wedge \varphi(x_1, \ldots, x_m, c))\}$$

since then S would be definable in $\mathcal{L}_{\text{ring}+K}$ with a definition with one additional existential quantifier, and if φ is positive-existential in $\mathcal{L}_{\text{ring}+K}$, then so is $\exists c(f(c) \doteq 0 \wedge \varphi(x_1, \ldots, x_m, c))$.

The inclusion from left to right is trivial (take $c = p$). Conversely, suppose $L \models \exists c(f(c) \doteq 0 \wedge \varphi(x_1, \ldots, x_m, c))$ for some $(x_1, \ldots, x_m) \in L^m$. As $f(c) = 0$, $c = \sigma(p)$ for some K-automorphism σ of L. We thus have $L \models \varphi(x_1, \ldots, x_m, \sigma(p))$. By Lemma 2.3.1 this implies $L \models \varphi(\sigma^{-1}(x_1), \ldots, \sigma^{-1}(x_m), p)$, whereby we have $(\sigma^{-1}(x_1), \ldots, \sigma^{-1}(x_m)) \in S$. But then by hypothesis also $(x_1, \ldots, x_m) \in S$. □

2.3.4 Corollary. *Let K be a number field, $m \in \mathbb{N}$, $S \subset K^m$ a subset which is definable in $\mathcal{L}_{ring+K}$ and such that $S = \sigma(S)$ for all automorphisms σ of K. Then S is definable in $\mathcal{L}_{ring}$ with one additional existential quantifier. In particular, if S is positive-existential in $\mathcal{L}_{ring+K}$, then also in $\mathcal{L}_{ring}$.*

Proof. This follows by the Primitive Element Theorem, previous proposition and the transformation from $\mathcal{L}_{\text{ring}+\mathbb{Q}}$-formulas to $\mathcal{L}_{\text{ring}}$ formulas in the beginning of this section. □

This result means that, if we are looking for a (positive-existential, existential) first-order definition in $\mathcal{L}_{\text{ring}}$ of a subset of a number field K which is closed under automorphisms - like the ring of integers $\mathcal{O}_K$ - we are done when we find a (positive-existential, existential) definition of the set in $\mathcal{L}_{\text{ring}+K}$.

2.3.5 Remark. The number field K in the corollary can be replaced by any algebraic extension of $\mathbb{Q}$. Indeed, only finitely many elements of K appear in any $\mathcal{L}_{\text{ring}+K}$-formula and we only needed a primitive element for the subfield of K generated by all those constants in the proof of the proposition.

2.3.6 Remark. For algebraic function fields, some complications arise when trying to formulate an analogon to Corollary 2.3.4. First of all, even in the base case of $K = \mathbb{F}_p(T)$, having a constant symbol for T in the language is desirable, given that for any $a, b, c, d \in \mathbb{F}_p$ with $ad \neq bc$, there is an automorphism sending T to $(aT + b)/(cT + d)$, severely limiting the amount of $\mathcal{L}_{\text{ring}}$-definable sets by Proposition 2.3.2. Furthermore, as one can not expect a general finite extension over $\mathbb{F}_p(T)$ to have a primitive element, more than one existential quantifier might need to be introduced when applying Proposition 2.3.3.

2.4 Decidability and Hilbert's 10th problem

We only briefly mention the relation between existential definability and decidability; see [Koe14] for a more in-depth discussion and sources for all statements in this section.

For this, we need the notion of a decision algorithm. An *algorithm* can be thought of as a computer program given by a finite list of instructions, taking a certain integer as input, performing a finite (but not a priori bounded) number of calculations, then giving another integer as output. After fixing a bijection to $\mathbb{Z}$, one can consider algorithms which take any element of a countable set as input. A *decision algorithm* is an algorithm which outputs either 0 or 1.

To make the notion of an algorithm rigorous, one can use Turing machines. Since we will only use decidability results as a motivation and not in formal proofs (except for one inconsequential proposition at the end of Section 4.6), we see no reason to discuss the formalities of Turing machines here.

In 1900, David Hilbert formulated the following problem, now known as Hilbert's 10th problem: "*Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.* " [Hil02] Presumably, Hilbert asked for a decision algorithm which has a polynomial $f \in \mathbb{Z}[X_1, X_2, \ldots]$ as input and outputs 1 if the polynomial has a root in $\mathbb{Z}^{\mathbb{N}}$ and 0 otherwise, although in principle his formulation still allows this algorithm to depend on f, for example on the number of variables occurring in f or the total degree of f. In our modern language, we are looking for a decision algorithm which has a diophantine statement φ in $\mathcal{L}_{\text{ring}}$ as input and 1 as output if and only if $\mathbb{Z} \models \varphi$. Note that Hilbert's formulation suggests that he did not question the existence of such an algorithm; at the time, it was still unheard of that a mathematical problem might not have a solution, and Hilbert was a notorious optimist when it came to the power of mathematics.

In 1970, Yuri Matiyasevich - building on work by Martin David, Hilary Putnam and Julia Robinson - proved a theorem which characterises the diophantine subsets of $\mathbb{Z}$ in terms of the existence of an algorithm which prints the elements of these subsets. Again, we refer the interested reader to [Koe14] for the precise statement of this result and only mention the following corollary.

2.4.1 Theorem. *There is an $n \in \mathbb{N}$, a polynomial $U \in \mathbb{Z}[T, X_1, \ldots, X_n]$ and an algorithm producing, for each algorithm $\mathcal{A}$, some $t_{\mathcal{A}} \in \mathbb{Z}$ such that $\mathcal{A}$ fails to answer correctly whether there is some $\underline{x} \in \mathbb{Z}^n$ with $U(t, \underline{x}) = 0$.*

In particular, this implies that the algorithm Hilbert asked for cannot exist, not even when allowed to depend on the degree or the number of variables.

There is a natural extension of Hilbert's 10th problem: given a ring R, does there exist a decision algorithm which can have any diophantine statement φ in $\mathcal{L}_{\text{ring}}$ as input and has 1 as output if and only if $R \models \varphi$? This question is open for many rings, in particular for all number fields K (including $\mathbb{Q}$) and many - but not all - of their rings of integers $\mathcal{O}_K$.

We now establish a link with the study of diophantine subsets of rings. Suppose R is a number field or the ring of integers in a number field. Let us assume that $\mathbb{Z}$

is an existential subset of R, i.e. there exists an existential formula φ in $\mathcal{L}_{\text{ring}}$ such that $\mathbb{Z} = \{t \in R \mid R \models \varphi(t)\}$. We can now consider the formula

$$\psi(t) = \exists x_1, \ldots, x_n (U(t, x_1, \ldots, x_n) \doteq 0 \wedge \varphi(x_1) \wedge \varphi(x_2) \wedge \ldots \wedge \varphi(x_n))$$

and we have that for $t \in R$, $R \models \psi(t)$ if and only if there exist $x_1, \ldots, x_n \in \mathbb{Z}$ such that $U(t, x_1, \ldots, x_n) = 0$. It follows from the techniques in the proof of Proposition 2.2.4 that ψ is again existential. By Corollary 2.2.12, ψ can even be rewritten as a diophantine formula. But there can not exist a decision algorithm which has a $t \in R$ as its input and outputs 1 if and only if $R \models \psi(t)$, for this would in particular be an algorithm which - on inputting $t \in \mathbb{Z}$ - outputs 1 if and only if $U(t, x_1, \ldots, x_n) = 0$ for some $x_1, \ldots, x_n \in \mathbb{Z}$ and this is impossible by Theorem 2.4.1. Thus we have proven:

2.4.2 Theorem. *Let R be either a number field or the ring of integers in a number field. Suppose $\mathbb{Z}$ has an existential definition in R. Then there exists $m \in \mathbb{N}$, a polynomial $V \in \mathbb{Z}[T, X_1, \ldots, X_m]$ and an algorithm producing, for each algorithm $\mathcal{A}$, some $t_{\mathcal{A}} \in \mathbb{Z}$ such that $\mathcal{A}$ fails to answer correctly whether there is some $\underline{x} \in R^m$ with $V(t, \underline{x}) = 0$. In particular, the aforementioned generalization of Hilbert's 10th problem to R has a negative answer.*

2.4.3 Remark. Let l be the number of quantifiers appearing in φ, then the number of quantifiers appearing in ψ is $n(l+1)$. Suppose the formula φ defining $\mathbb{Z}$ in R is positive-existential (recall from Corollary 2.2.12 that we can convert existential formulas to positive-existential formulas, but this increases the number of quantifiers). Then also the formula ψ is positive-existential. As explained in the proof of Proposition 2.2.5, no additional quantifiers are introduced when passing from a positive-existential formula to an equivalent diophantine formula, so ψ is equivalent to a diophantine formula with $n(l+1)$ quantifiers. It follows that we can pick $m = n(l+1)$ in the above theorem.

2.5 Model-theoretic aspects

When Σ is a set of $\mathcal{L}_{\text{ring}}$-statements, we denote $\text{Mod}(\Sigma)$ for the class of all $\mathcal{L}_{\text{ring}}$-structures R for which $R \models \varphi$ for all $\varphi \in \Sigma$. We call the elements of $\text{Mod}(\Sigma)$ the *models* of Σ. For example, one could set Σ to be the set of all ring axioms (like $\forall x(x \cdot 1 \doteq x)$ and $\forall x \forall y(x + y \doteq y + x)$) and then $\text{Mod}(\Sigma)$ would be the class of rings. $\text{Mod}(\Sigma \cup \{1 + 1 + 1 \doteq 0, \neg(1 \doteq 0)\})$ would be the class of rings of characteristic 3.

Conversely, if R is a fixed $\mathcal{L}_{\text{ring}}$-structure, then we denote $\text{Th}(R)$ for the set of all statements φ for which $R \models \varphi$. We call $\text{Th}(R)$ *the theory of* R.

Finally, by combining the above two, we can consider $\text{Mod}(\text{Th}(R))$. This is the class of all $\mathcal{L}_{\text{ring}}$-structures in which all statements, which hold in R, also hold. It follows from Lemma 2.3.1 that this class contains all $\mathcal{L}_{\text{ring}}$-structures which are isomorphic to R. If R is finite one can show that $\text{Mod}(\text{Th}(R))$ is exactly the class of structures which are isomorphic to R, but if R is infinite, then $\text{Mod}(\text{Th}(R))$ contains structures of arbitrarily large cardinality, so it contains many non-isomorphic structures. See for example [PD11, Theorem 2.4.3.] for more details.

Let $R' \in \mathrm{Mod}(\mathrm{Th}(R))$. When $A \subseteq R^n$ is defined by a formula $\varphi(\underline{x})$, then it makes sense to use this formula to define a set $A' = \{\underline{x} \in R'^n \mid R' \models \varphi(\underline{x})\}$, its *transfer* to R'. Note that passing from A to A' does not depend on the used definition of A: if $\psi(\underline{x})$ is another formula also defining A in R^n, then

$$\forall x_1, \ldots, x_n(\varphi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)) \in \mathrm{Th}(R),$$

whereby the two formulas also define the same set in any model of $\mathrm{Th}(R)$.

Studying transfers of definable subsets is of interest when studying existential subsets because of the following remarkable model-theoretic result:

2.5.1 Proposition (Łoś-Tarski Preservation Theorem)**.** *Let A be a definable subset of an $\mathcal{L}_{ring}$-structure R. Then A is existential if and only if for any $R', R'' \in \mathrm{Mod}(\mathrm{Th}(R))$ with respective transfers A' and A'' of A and such that R' is an $\mathcal{L}_{ring}$-substructure of R'', we have $A' \subseteq A''$.*

Proof. One direction is elementary: if an existential statement is satisfied in a substructure, then also in the larger structure. Hence, if A and thereby A' are existential, then all elements of A' still satisfy the existential definition of A when evaluated in the larger structure R'', whereby they also lie in A''.

For a proof of the other implication, see [PD11, Theorem 3.1.7.]. The proposition depends on a weak version of the Axiom of Choice and the proof is therefore non-constructive. □

We will give an application of this proposition. We first state the main result of [Dit18].

2.5.2 Theorem. *Let K be a global field, n be a positive natural number. There exists an existential first-order formula $\varphi_{K,n}(x_0, \ldots, x_{n-1})$ in $\mathcal{L}_{ring}$ such that $K \models \varphi_{K,n}(a_0, \ldots, a_{n-1})$ if and only if the polynomial $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ has no root in K.*

The theorem says that the set

$$\{(a_0, \ldots, a_{n-1}) \in K^n \mid X^n + a_{n-1}X^{n-1} + \ldots + a_0 \text{ has no root in } K\}$$

is existential. Note that it is trivially universal: it is equal to

$$\{(a_0, \ldots, a_{n-1}) \in K^n \mid \forall x \in K : x^n + a_{n-1}x^{n-1} + \ldots + a_0 \neq 0\}.$$

We will not prove this theorem nor rely on it after this section, but focus now on some corollaries, illustrating the interplay between model theory and definability.

2.5.3 Proposition. *Let K be a global field, $K', K'' \in \mathrm{Mod}(\mathrm{Th}(K))$ and K' a subfield of K''. Then K' is relatively algebraically closed in K''.*

Proof. Define the formula

$$\gamma_{K,n}(a_0, \ldots, a_{n-1}) = \forall x(\neg(x^n + a_{n-1}x^{n-1} + \ldots + a_0 \doteq 0)).$$

Theorem 2.5.2 can then be rewritten as

$$K \models \forall a_0, \ldots, a_{n-1}(\varphi_{K,n}(a_0, \ldots, a_{n-1}) \leftrightarrow \gamma_{K,n}(a_0, \ldots, a_{n-1})).$$

It follows that Theorem 2.5.2 also holds, with the same formula $\varphi_{K,n}$, in the fields K' and K''. Let $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K'[X]$ be a polynomial without a root in K'. Then $K' \models \varphi_{K,n}(a_0, \ldots, a_{n-1})$, whereby also $K'' \models \varphi_{K,n}(a_0, \ldots, a_{n-1})$ by the fact that $\varphi_{K,n}$ is an existential formula. Hence f does not have a root in K'' either. This shows that K' is relatively algebraically closed in K''. □

2.5.4 Proposition. *Let L/K be a purely transcendental extension of fields, $n \in \mathbb{N}$. A polynomial $f \in K[X_1, \ldots, X_n]$ which is irreducible over K remains irreducible over L.*

Proof. We first consider the special case where K and L are algebraically closed. There is clearly a (universal) first-order $\mathcal{L}_{\mathrm{ring}+K}$-statement describing that f is irreducible: it suffices to formulate that for all $k \in \{1, \ldots, \lfloor \frac{n}{2} \rfloor\}$, f is not the product of a degree k and a degree $n-k$ polynomial. Thus by Proposition 2.2.13, there is actually a *quantifier-free* formula describing that f is irreducible. When a quantifier-free statement is true in a smaller field, it is also true in a larger field. Hence if f is irreducible over K, then also over L.

Alternatively, if one wishes to avoid the use of quantifier elimination, the above special case can also be derived from the weak version of Hilbert's Nullstellensatz.

Consider now the general case. After a change of coordinates we may assume f has a non-zero constant coefficient, and by rescaling we may then assume this coefficient is 1. Let $\overline{L}$ be an algebraic closure of L and $\overline{K}$ the algebraic closure of K in $\overline{L}$. There is a unique way (up to permutation) to factor f over $\overline{K}$ as a product of irreducible polynomials $f_1, \ldots, f_n \in \overline{K}[X_1, \ldots, X_n]$ with constant coefficient 1. As $\overline{K}$ is algebraically closed, these $f_1, \ldots, f_n$ remain irreducible over $\overline{L}$ by the special case. Now assume for the sake of a contradiction that f factors non-trivially as $g \cdot h$ over L, where again we may assume that g and h have constant coefficient 1. Then by unique factorisation in $\overline{L}[X_1, \ldots, X_n]$, g and h each are a product of some of the f_i. Then the coefficients of g and h lie in $\overline{K} \cap L$. But $\overline{K} \cap L = K$ by the assumption on L/K. This contradicts f being irreducible over K. □

2.5.5 Proposition. *Let n be a positive natural number, $I \subseteq \mathbb{N}^n$ a finite set, K a global field. There exists an existential formula $\iota_{K,I}((x_i)_{i \in I})$ such that $K \models \iota_{K,I}((a_i)_{i \in I})$ if and only if*

$$f = \sum_{i=(i_1,\ldots,i_n) \in I} a_i X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

is irreducible in K.

Proof. By Proposition 2.5.3 and Proposition 2.5.4 we have for $K', K'' \in \mathrm{Mod}(\mathrm{Th}(K))$ with K' a subfield of K'' that every irreducible polynomial over K' remains irreducible over K''. As we already know that there is a first-order formula describing that f is irreducible, the result now follows by applying Proposition 2.5.1. □

Chapter 3

Traces of norm-1 elements as building blocks

3.1 A local-global result

First, we recall a few results from the theory of central simple algebras. Let K always be a field.

3.1.1 Proposition. *Let $n \in \mathbb{N}$, D a central simple division algebra of degree n over K and let L be a field of degree n over K. Then L splits D if and only if L can be embedded into D over K.*

Proof. See [Pie82, Corollary 13.3]. □

We denote Nrd and Trd for the reduced norm and trace respectively (see [Pie82, Chapter 16] for a definition).

3.1.2 Proposition. *Let A/K be a central simple algebra of degree $n \in \mathbb{N}$ and $x \in A$. If $L \subseteq A$ is a degree n field extension of K containing x, then $\mathrm{Nrd}(x) = N_{L/K}(x)$ and $\mathrm{Trd}(x) = \mathrm{Tr}_{L/K}(x)$.*

Proof. Explained in [Pie82, Section 16.1]. □

In this section we follow Philip Dittmann [Dit18], who generalised methods first established for quaternion algebras by Bjorn Poonen in [Poo09].

Let A be a central simple algebra over K and let $l \in \mathbb{N}, l \geq 2$. Define

$$S(A) = \{\mathrm{Trd}(x) \mid x \in A, \mathrm{Nrd}(x) = 1\}$$
$$U_l(K) = \left\{ a_{l-1} \in K \;\middle|\; \begin{array}{l} \exists a_1, \ldots, a_{l-2} \in K : \\ X^l - \sum_{i=1}^{l-1} a_i X^i + (-1)^l \text{ is irreducible over } K \end{array} \right\}.$$

Note that the latter consists of those elements of K which are the trace of an element of norm 1 in some degree l field extension of K. From this we directly infer that $U_l(\mathbb{C}) = \emptyset$ for all l, that $U_2(\mathbb{R}) =]-2, 2[$ and that $U_l(\mathbb{R}) = \emptyset$ if $l > 2$.

If K is a non-archimedean local field, denote $\mathcal{O}_K$ for its valuation ring, red for the residue homomorphism from K to its residue field. Set $\mathcal{O}_{\mathbb{R}} = [-4, 4]$.

3.1.3 Proposition. *Let A be a central simple algebra over K and assume that $l = \deg(A)$ is prime.*

1. *If A is split, then $S(A) = K$.*
2. *If A is a division algebra, then*

$$\{x \in K^\times \mid x^l = l^l\} \subseteq S(A) \subseteq U_l(K) \cup \{x \in K^\times \mid x^l = l^l\}.$$

Furthermore if K is a local field, then the second inclusion becomes an equality and $U_l(K)$ is open with respect to the metric topology. Moreover, $S(A) \subseteq \mathcal{O}_K$.

Proof. If A is split, then Trd and Nrd are just the trace and norm of matrices over K. We know that all monic polynomials over K appear as characteristic polynomials of matrices over K, so indeed we have $S(A) = K$.

From now on, suppose A is a division algebra. Assume $x \in K^\times$ is such that $x^l = l^l$. Note that this is only possible if $\mathrm{char}(K) \neq l$. Considering $\frac{x}{l}$ as an element of A, we then have $\mathrm{Trd}\left(\frac{x}{l}\right) = x$ and $\mathrm{Nrd}\left(\frac{x}{l}\right) = 1$, whereby $x \in S(A)$. This shows the first inclusion.

Now take $q \in A \setminus K$ with $\mathrm{Nrd}(q) = 1$. Then its minimal polynomial over K is a degree l monic, irreducible polynomial with X^{l-1}-coefficient $-\mathrm{Trd}(q)$ and constant coefficient $(-1)^l$. Hence, $\mathrm{Trd}(q) \in U_l(k)$. This proves the second inclusion.

If $K = \mathbb{C}$, A cannot be a division algebra. If $K = \mathbb{R}$, then indeed $U_2(\mathbb{R}) =]-2, 2[$ is open and $U_2(\mathbb{R}) \cup \{x \in \mathbb{R} \mid x^2 = 2^2\} =]-2, 2[\cup \{-2, 2\} = [-2, 2]$. Suppose that K is a non-archimedean complete field; let v be the normalised valuation on K. The openness of $U_l(K)$ follows from Corollary 1.6.3 (note that $X^l - \sum_{i=1}^{l-1} a_i X^i + (-1)^l$ is always separable if it is irreducible). Take $x \in A$ with $\mathrm{Nrd}(x) = 1$. By Proposition 1.3.3 v extends uniquely to a valuation on the complete field $K(x)$ and we have $v(x) = v(N_{K(x)/K}(x))/[K(x) : K] = 0$, whereby x lies in the valuation ring $\mathcal{O}_{K(x)}$. It is a known corollary of Chevalley's theorem that this implies that x is integral over $\mathcal{O}_K$ (see e.g. [EP05, Theorem 3.1.3]), in particular the trace of x lies in $\mathcal{O}_K$. This proves $S(A) \subseteq \mathcal{O}_K$.

Remains to show that $U_l(K) \subseteq S(A)$ for local fields. Take $a_{l-1} \in U_l(K)$, consider a polynomial $F = X^l - \sum_{i=1}^{l-1} a^i X^i + (-1)^l$ for some $a_1, \ldots, a_{l-2} \in K$ such that F is irreducible. Let L be the root field of F over K. As $[L : K] = l = \deg(A)$, it follows from Theorem 1.5.10 (or the fact that $L \cong \mathbb{C}$ if $K = \mathbb{R}$) that L splits A and thus by Proposition 3.1.1 embeds into A. This means a does occur as the reduced trace of an element of reduced norm 1.

□

3.1.4 Proposition. *Let K be a global field and A a central simple algebra over K of prime degree l, $\mathbb{P}'$ the set of non-complex spots of K. Then*

$$S(A) = \bigcap_{\mathfrak{p} \in \mathbb{P}'} S(A_\mathfrak{p}) \cap K.$$

Proof. The inclusion $\subseteq$ is clear: if $a \in S(A)$, then there exists an $x \in A$ with $\mathrm{Nrd}(x) = 1$ and $\mathrm{Trd}(x) = a$ and one can take the same x in $A_\mathfrak{p}$ (we identify x with $x \otimes 1$) to obtain $a \in S(A_\mathfrak{p})$. Furthermore, if A is split, then by the first part of Proposition 3.1.3 the set on the left (and hence also the set on the right) equals K.

So assume that A is a division algebra instead. Consider $a \in \bigcap_{\mathfrak{p}\in\mathbb{P}'} S(A_\mathfrak{p}) \cap K$. We want to show that there exists an $x \in A$ with $\mathrm{Nrd}(x) = 1$ and $\mathrm{Trd}(x) = a$.

Let $\Delta(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ for pairwise different spots $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of K (there are only finitely many by Theorem 1.7.4). By hypothesis we can pick an $x_i \in A \otimes K_{\mathfrak{p}_i}$ with $\mathrm{Nrd}(x_i) = 1$ and $\mathrm{Trd}(x_i) = a$. If $x_i \in K_{\mathfrak{p}_i}$, then $a = \mathrm{Trd}(x_i) = lx_i$, whereby $x_i \in A$ and we are done globally. So assume that $a \in U_l(K_{\mathfrak{p}_i})$ for all i.

Let $f_i \in K_\mathfrak{p}[X]$ be an irreducible degree l polynomial with constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$. If $l = 2$ the polynomial f_i is completely determined as $X^2 - aX + 1$. Otherwise we must have that all $K_{\mathfrak{p}_i}$ are non-archimedean. Hence we can use weak approximation and the fact that K is dense in $K_\mathfrak{p}$ to find a monic degree l polynomial $f \in K[X]$ which is arbitrarily close in the $\mathfrak{p}_i$-adic topology to f_i, which has constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$. Let x be a root of f, then $K_\mathfrak{p}(x)$ is a degree l extension of $K_\mathfrak{p}$ for all $\mathfrak{p} \in \Delta(A)$. Furthermore, $\mathrm{Tr}_{K(x)/K}(x) = a$ and $N_{K(x)/K}(x) = 1$.

By Theorem 1.5.10 (and, if necessary, a seperate consideration when $K = \mathbb{R}$) the field $K(x)$ splits $A_\mathfrak{p}$ for all spots $\mathfrak{p}$ of K. By the Albert-Hasse-Brauer-Noether Theorem (Theorem 1.7.5) we get that $K(x)$ splits A. By Proposition 3.1.2 we then have that $K(x)$ can be embedded into A over K. The image of x under this embedding has the same minimal polynomial over K as x, whereby it has trace a and norm 1. □

3.2 Quaternion algebras and a $\forall\exists$-definition of the ring of integers

We apply the results of the previous section to quaternion algebras over local fields and global fields. In the local case, we want to show the following:

3.2.1 Proposition. *Let K be a non-archimedean local field. Then $\mathcal{O}_K = U_2(K) + U_2(K)$.*

For this, it appears to be useful to consider $U_2(\mathbb{F}_q)$ for the finite field with q elements. Note that

$$U_2(\mathbb{F}_q) = \{\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) \mid x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q, N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = 1\}.$$

As the norm function in the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$ is given by taking the $(q+1)$-th power, each value in $\mathbb{F}_q^\times$ is the norm of exactly $q+1$ elements of $\mathbb{F}_{q^2}$. In particular, there are $q+1$ elements with norm 1. Of these, 1 and -1 are the only elements of $\mathbb{F}_q$, and the remaining elements come in conjugate pairs, meaning that they have the same trace. We conclude that $U_2(\mathbb{F}_q)$ contains $\frac{q-1}{2}$ elements if q is odd, or $\frac{q}{2}$ if q is even.

Proof of Proposition 3.2.1. The inclusion from right to left is known from Proposition 3.1.3 already; we show the other inclusion. Let $\mathbb{F}_q$ be the residue field of $\mathcal{O}_K$, $\mathsf{red} : \mathcal{O}_K \to \mathbb{F}_q$ the residue map. It is clear that $U_2(\mathbb{F}_q) \subseteq \mathsf{red}(U_2(K))$. If we can show that $\mathsf{red}(U_2(K))$ contains at least one (if q is even) or two (if q is odd) elements not contained in $U_2(\mathbb{F}_q)$, then by the discussion above and the Pidgeon Hole Principle $\mathbb{F}_q = U_2(\mathbb{F}_q) + \mathsf{red}(U_2(K))$. So for $x \in \mathcal{O}_K$, there exists a $y \in U_2(K)$ such

that $\mathsf{red}(x-y) \in U_2(\mathbb{F}_q)$. Then $x - y \in \mathsf{red}^{-1}(U_2(\mathbb{F}_q)) \subseteq U_2(K)$. As this holds for general x, we can indeed conclude that $\mathcal{O}_K \subseteq U_2(K) + U_2(K)$.

We claim that $\pm 2 \in \mathsf{red}(U_2(K)) \setminus U_2(\mathbb{F}_q)$, which gives the required two elements if q is odd and the required one element if q is even. As $X^2 \pm 2X + 1 = (X \pm 1)^2$ we see that $\pm 2 \notin U_2(\mathbb{F}_q)$.

Now pick a $\pi \in \mathcal{O}_K$ with $v(\pi) = 1$. We claim that $X^2 - (\pm 2 + \pi)X + 1$ is irreducible. Indeed we observe that

$$X^2 - (2+\pi)X + 1 = (X-1)^2 - \pi(X-1) - \pi$$
$$X^2 - (-2+\pi)X + 1 = (X+1)^2 - \pi(X+1) + \pi$$

and by Eisenstein's criterion the polynomials on the right are irreducible. It follows that $\pm 2 + \pi \in U_2(K)$, whereby $\pm 2 \in \mathsf{red}(U_2(K))$. □

3.2.2 Remark. In [Poo09, Lemma 2.3] it is shown that in fact $U_2(\mathbb{F}_q) + U_2(\mathbb{F}_q) = \mathbb{F}_q$ for prime powers $q > 11$, but not for (all) smaller prime powers. Thus the argument with $\pm 2 \in \mathsf{red}(U_2(K)) \setminus U_2(\mathbb{F}_q)$ was needed at least for $q \leq 11$. The idea to use the Pidgeon Hole Principle for this was ours; the use of Eisenstein's criterion to show that $\pm 2 \in \mathsf{red}(U_2(K))$ is due to Dittmann.

3.2.3 Remark. Recall that $U_2(\mathbb{R}) =]-2, 2[$. Hence $U_2(\mathbb{R}) + U_2(\mathbb{R}) =]-4, 4[$.

We apply this result to find a $\forall\exists$-definition of $\mathcal{O}_K$ in K, where K is a number field and $\mathcal{O}_K$ its ring of integers. By this we mean a formula of the form $\forall x_1, \ldots, x_n \exists y_1, \ldots, y_m \psi$ where ψ is quantifier-free. This was first realised in [Poo09], then simplified in [Par13].

Let Q be a quaternion algebra over a field K, then we denote $T(Q) = S(Q) + S(Q)$. Note that for $Q = (a,b)_K$ (if $\mathrm{char}(K) \neq 2$) and $Q = [a,b)_K$ we have by the formulas for trace and norm derived in Section 1.5:

$$S((a,b)_K) = \{t \in K \mid \exists x_2, x_3, x_4 (t^2 - 4ax_2^2 - 4bx_3^2 + 4abx_4^2 = 4)\}$$
$$S([a,b)_K) = \left\{ t \in K \;\middle|\; \begin{array}{l} \exists x_1, x_3, x_4 (x_1^2 + x_1(t - 2x_1) + (t-2x_1)^2 \\ -b(x_3^2 + x_3x_4 - ax_4^2) = 1) \end{array} \right\}$$
$$T(Q) = \{x \in K \mid \exists y (y \in S(Q) \wedge x - y \in S(Q))\}$$

so the sets $S((a,b)_K)$ and $S([a,b)_K)$ are positive-existential in the language $\mathcal{L}_{\mathrm{ring}+\{a,b\}}$ (additional constant symbols for a and b) with 3 quantifiers each; the sets $T((a,b)_K)$ and $T([a,b)_K)$ are positive-existential in $\mathcal{L}_{\mathrm{ring}+\{a,b\}}$ with 7 quantifiers each.

3.2.4 Lemma. *Let Δ be a finite set of spots of a field K and let, for each $\mathfrak{p} \in \Delta$, $A_\mathfrak{p}$ and $B_\mathfrak{p}$ be subsets of $K_\mathfrak{p}$. Then*

$$\bigcap_{\mathfrak{p}\in\Delta} A_\mathfrak{p} \cap K + \bigcap_{\mathfrak{p}\in\Delta} B_\mathfrak{p} \cap K \subseteq \bigcap_{\mathfrak{p}\in\Delta} (A_\mathfrak{p} + B_\mathfrak{p}) \cap K$$

and equality holds when $A_\mathfrak{p}$ and $B_\mathfrak{p}$ are open subsets of $K_\mathfrak{p}$ for each $\mathfrak{p} \in \Delta$.

Proof. The inclusion from left to right is trivial. Suppose now that $A_\mathfrak{p}$ and $B_\mathfrak{p}$ are open and t is an element of the set on the right. Then to each $\mathfrak{p} \in \Delta$, there exists an $x_\mathfrak{p} \in A_\mathfrak{p}$ such that $t - x_\mathfrak{p} \in B_\mathfrak{p}$. As K is dense in $K_\mathfrak{p}$ and by the openness of $A_\mathfrak{p}$ and $B_\mathfrak{p}$, we may assume $x_\mathfrak{p} \in K$. Using Theorem 1.6.4 we find an $x \in K$ such that $x \in A_\mathfrak{p}$ and $t - x \in B_\mathfrak{p}$ for all $\mathfrak{p} \in \Delta$. □

3.2.5 Remark. As the sum of two open subsets of $K_\mathfrak{p}$ is again open, the above lemma can be applied inductively.

Let $\mathfrak{p}$ be a spot of K. If $\mathfrak{p}$ is finite with corresponding valuation $v_\mathfrak{p}$, recall that we wrote $\mathcal{O}_\mathfrak{p}$ for the valuation ring of $v_\mathfrak{p}$ in $K_\mathfrak{p}$ and $\mathcal{O}_{(\mathfrak{p})}$ for $\mathcal{O}_\mathfrak{p} \cap K$. If $\mathfrak{p}$ is infinite, define $\mathcal{O}_{(\mathfrak{p})}$ as the preimage of $\mathcal{O}_\mathbb{R} = [-4, 4]$ under the corresponding place.

3.2.6 Proposition. *Let Q be a quaternion algebra over a global field K. Then*

$$T(Q) = \bigcap_{\mathfrak{p} \in \Delta(Q)} \mathcal{O}_{(\mathfrak{p})}.$$

Proof. We have by Proposition 3.1.4

$$T(Q) = S(Q) + S(Q) = \bigcap_{\mathfrak{p} \in \Delta} S(Q_\mathfrak{p}) \cap K + \bigcap_{\mathfrak{p} \in \Delta} S(Q_\mathfrak{p}) \cap K.$$

It thus follows immediately from Proposition 3.1.3 and Lemma 3.2.4 that $T(Q) \subseteq \bigcap_{\mathfrak{p} \in \Delta(Q)} \mathcal{O}_{(\mathfrak{p})}$. For the other inclusion, note that

$$\begin{aligned}
T(Q) &= \bigcap_{\mathfrak{p} \in \Delta} S(Q_\mathfrak{p}) \cap K + \bigcap_{\mathfrak{p} \in \Delta} S(Q_\mathfrak{p}) \cap K \\
&\supseteq \{\pm 4\} \cup \left(\bigcap_{\mathfrak{p} \in \Delta} U_2(K_\mathfrak{p}) \cap K + \bigcap_{\mathfrak{p} \in \Delta} U_2(K_\mathfrak{p}) \cap K \right) && \text{(Proposition 3.1.3)} \\
&= \{\pm 4\} \cup \bigcap_{\mathfrak{p} \in \Delta} (U_2(K_\mathfrak{p}) + U_2(K_\mathfrak{p})) \cap K && \text{(Lemma 3.2.4)} \\
&= \bigcap_{\mathfrak{p} \in \Delta(Q)} \mathcal{O}_{(\mathfrak{p})}. && \text{(Proposition 3.2.1)}
\end{aligned}$$

□

We are now close to finding a $\forall\exists$-definition for $\mathcal{O}_K$ in a number field K. Suppose that $\mathfrak{Q}$ is a set of quaternion algebras over K such that

(i) all $Q \in \mathfrak{Q}$ split over all real infinite spots $\mathfrak{p}$ of K.

(ii) for every finite spot $\mathfrak{p}$ of K there exists some $Q \in \mathfrak{Q}$ such that $Q_\mathfrak{p}$ is split.

Then it follows from the proposition that

$$\mathcal{O}_K = \bigcap_{\mathfrak{p} \in \mathbb{P}} \mathcal{O}_{(\mathfrak{p})} = \bigcap_{Q \in \mathfrak{Q}} T(Q),$$

i.e. for $t \in K$ we have that $t \in \mathcal{O}_K$ if and only if

$$\forall Q \in \mathfrak{Q} : t \in T(Q).$$

We know already that $T((a, b)_K)$ has an existential definition in terms of a and b. If we can make a good choice for $\mathfrak{Q}$, we can hope to find a definition for $\mathcal{O}_K$ which uses at most two universal quantifiers for the a and b and some existential quantifiers. For this, we take a look at a corollary of Proposition 1.5.5:

3.2.7 Proposition. *Let K be a global field,* $\mathrm{char}(K) \neq 2$. *For any $a, b \in K$ with $(1+a^2)b \neq 0$, the quaternion algebra $(1+a^2, b)_{\mathfrak{p}}$ is split for all real archimedean spots $\mathfrak{p}$ of K. For every non-archimedean place $\mathfrak{p}$ of K, there exist $a, b \in K$ such that $(1+a^2, b)_{\mathfrak{p}}$ is not split.*

Proof. The first part is clear, as $1 + a^2$ becomes positive in every embedding into $\mathbb{R}$. The second part follows by combining Proposition 1.4.6 and Proposition 1.5.5 with the density of K in $K_{\mathfrak{p}}$ and the fact that being non-split is an open property (Proposition 1.5.12). □

Hence we can take

$$\mathcal{O}_K = \bigcap_{\substack{a,b \in K \\ (1+a^2)b \neq 0}} T((1+a^2, b)_K)$$

whereby we have for $t \in K$ that

$$\begin{aligned} & \forall a, b \exists x_1, x_2, x_3, x_4, y_2, y_3, y_4 \\ t \in \mathcal{O}_K \Leftrightarrow\ & ((1+a^2)b = 0 \vee (x_1^2 - (1+a^2)x_2^2 - bx_3^2 + (1+a^2)bx_4^2 - 1 = 0 \\ & \wedge\ (t - 2x_1)^2 - 4(1+a^2)y_2^2 - 4by_3^2 + 4(1+a^2)by_4^2 - 4 = 0)). \end{aligned}$$

Note that this definition does not depend on the number field K. If we fix K, we can use the techniques from Proposition 2.2.5 to convert this into a formula of the form $\forall a, b \exists x_1, x_2, x_3, x_4, y_1, y_2, y_3\ f(a, b, x_1, \ldots, y_3, t) = 0$ for some polynomial $f \in \mathbb{Z}[A, B, X_1, \ldots, Y_3, T]$ of total degree 13. For example, if K is a real number field like $\mathbb{Q}$, a possible choice for this polynomial would be

$$\begin{aligned} f = \ & B(1+A^2)((X_1^2 - (1+A^2)X_2^2 - BX_3^2 + (1+A^2)X_4^2 - 1)^2 \\ & + ((T - 2X_1)^2 - 4(1+A^2)Y_2^2 - 4BY_3^2 + 4(1+A^2)BY_4^2 - 4)^2). \end{aligned}$$

We conclude with a diophantine definability result for valuation rings in global fields.

3.2.8 Proposition. *Let K be a global field, Q, Q' quaternion algebras over K such that $\Delta(Q) \cap \Delta(Q')$ contains only finite places of K. Then*

$$T(Q) + T(Q') = \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \Delta(Q')} \mathcal{O}_{(\mathfrak{p})}$$

Proof. Combine Proposition 3.2.6 and Lemma 3.2.4. □

3.2.9 Proposition. *Let K be a global field. For any finite spot $\mathfrak{p}$ of K, the ring $\mathcal{O}_{(\mathfrak{p})}$ is an existential subset of K in the extended language $\mathcal{L}_{ring+K}$; there exists an existential definition with 15 quantifiers.*

Proof. By Theorem 1.7.10, take quaternion algebras Q, Q' such that $\Delta(Q) \cap \Delta(Q') = \{\mathfrak{p}\}$. Then by Proposition 3.2.8, $T(Q) + T(Q') = \mathcal{O}_{(\mathfrak{p})}$, and just as $T(Q)$ and $T(Q')$ are existential because they are the sum of two existential sets, $T(Q) + T(Q')$ is existential. $T(Q)$ and $T(Q')$ each require at most $3 + 3 + 1 = 7$ quantifiers, so their sum requires at most $7 + 7 + 1 = 15$. □

3.2.10 Proposition. *Let S be a set of prime ideals of K, $|S| \geq 2$. Then the set $\bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition in K in $\mathcal{L}_{ring+K}$ with 14 quantifiers. If $|S|$ is even, then the number of quantifiers can be reduced to 7.*

Proof. Suppose first that $|S|$ is even. By Theorem 1.7.10 we can pick a quaternion algebra Q over K with $\Delta(Q) = S$. Then $T(Q) = \bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}$ (by Proposition 3.2.6) has a positive-existential definition with 7 quantifiers. If S contains an odd number of elements but $|S| \geq 2$, we can write S as the union of two sets S' and S'', each with an even number of elements. Find quaternion algebras Q' and Q'' such that $\Delta(Q') = S'$ and $\Delta(Q'') = S''$. Now

$$\bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})} = \bigcap_{\mathfrak{p}\in S'} \mathcal{O}_{(\mathfrak{p})} \cap \bigcap_{\mathfrak{p}\in S''} \mathcal{O}_{(\mathfrak{p})} = T(Q') \cap T(Q'')$$

has a positive-existential definition with $7 + 7 = 14$ quantifiers. □

3.3 Generalisations to higher dimensions

We now discuss how the traces of norm-1 elements still have the desired existential definability properties in higher-dimensional central simple algebras.

3.3.1 Lemma. *Let K be a field and $l \in \mathbb{N}$, let $(e_i)_{i=1}^{l^2}$ be a K-basis for $\mathbb{M}_l(K)$. Furthermore, suppose $a_{i,j,m} \in K$ are such that $e_i \cdot e_j = \sum_{i=1}^{l^2} a_{i,j,m} e_m$ for every $i, j \in \{1, \ldots, l^2\}$. Given $c_1, \ldots, c_{l^2} \in K$, the characteristic polynomial of $\sum_{i=1}^{l^2} c_i e_i$ is the unique monic polynomial $\chi(T)$ over K for which*

$$\chi(T)^l = \det\left(TI_{l^2} - \left[\sum_{i=1}^{l^2} c_i a_{i,m,j}\right]_{j,m}\right).$$

Proof. Let $B = [b_{j,m}]_{j,m} = \sum_{i=1}^{l^2} c_i e_i$ and consider the K-linear map

$$\psi : \mathbb{M}_l(K) \to \mathbb{M}_l(K) : A \mapsto B \cdot A.$$

We calculate the characteristic polynomial of this map with respect to two bases of $\mathbb{M}_l(K)$. First, consider the canonical basis $(M^{i,j})_{i,j}$, where $M^{i,j}$ has a 1 at the intersection of the i-th row and the j-th column and a 0 everywhere else. One has $\psi(M^{i,j}) = \sum_{m=1}^{l} b_{m,i} M^{m,j}$, so with respect to this basis, the matrix representing ψ is a block diagonal matrix consisting of l blocks each containing the matrix B. It follows that its characteristic polynomial is given by $\det(TI_l - B)^l = \chi(T)^l$.

By definition of the $a_{i,j,m}$ and the fact that $B = \sum_{i=1}^{l^2} c_i e_i$, the matrix representing ψ with respect to the basis $(e_i)_{i=1}^{l^2}$ is $\left[\sum_{i=1}^{l^2} c_i a_{i,m,j}\right]_{j,m}$. Recalling that the characteristic polynomial of a linear map does not depend on the choice of basis, the desired equality follows. □

3.3.2 Remark. The lemma gives a direct proof of the fact that the structure constants of a basis of $\mathbb{M}_l(K)$ completely determine the characteristic polynomial of a given linear combination of these basis elements. In fact, they even completely determine the conjugacy class of this linear combination in $\mathbb{M}_l(K)$: this is a direct application of the Skolem-Noether Theorem [Pie82, Section 12.6].

3.3.3 Proposition. *Let K be a field, A a central simple algebra over K of degree l. Fix a K-basis $(e_i)_{i=1,\dots,l^2}$ of A and set $e_i \cdot e_j = \sum_{m=1}^{l^2} a_{i,j,m} e_m$ for some $a_{i,j,m} \in K$. Then the sets*

$$\mathfrak{T} = \left\{ (x_1, \dots, x_{l^2}, y) \in K^{l^2+1} \middle| \operatorname{Trd}\left(\sum_{m=1}^{l^2} x_m e_m\right) = y \right\}$$
$$\mathfrak{N} = \left\{ (x_1, \dots, x_{l^2}, y) \in K^{l^2+1} \middle| \operatorname{Nrd}\left(\sum_{m=1}^{l^2} x_m e_m\right) = y \right\}$$

are subsets of K which have a quantifier-free definition in $\mathcal{L}_{ring+(a_{i,j,m})_{i,j,m}}$, i.e. the language of rings with an additional constant symbol $\widetilde{a_{i,j,m}}$ for every $a_{i,j,m}$.

Proof. Let K' be an algebraically closed field containing K. A splits over K', i.e. there is a K-embedding $\phi : A \to M_l(K')$. By basic properties of reduced norm and trace (see for example [Pie82, Section 16.1]) we have that

$$\mathfrak{T} = \left\{ (x_1, \dots, x_{l^2}, y) \in K^{l^2+1} \middle| \operatorname{Tr}\left(\sum_{m=1}^{l^2} x_m \phi(e_m)\right) = y \right\} \text{ and}$$
$$\mathfrak{N} = \left\{ (x_1, \dots, x_{l^2}, y) \in K^{l^2+1} \middle| \det\left(\sum_{m=1}^{l^2} x_m \phi(e_m)\right) = y \right\}.$$

The above lemma tells us that we can find $\mathcal{L}_{\text{ring}+a_{i,j,m}}$-formulas $\psi_{\text{Tr}}, \psi_{\det}$ with free variables $x_1, \dots, x_{l^2}, y$ such that $\psi_{\text{Tr}}(x_1, \dots, x_{l^2}, y)$ holds for $x_1, \dots, x_{l^2}, y \in K'$ if and only if y is the trace of $\sum_{i=1}^{l^2} x_m \phi(e_m)$, and similarly for $\psi_{\det}$ and the determinant. By quantifier elimination in algebraically closed fields (Proposition 2.2.13), we may assume that both ψ_{Tr} and $\psi_{\det}$ are quantifier-free. But then ψ_{Tr} and $\psi_{\det}$ give the required quantifier-free definitions of $\mathfrak{T}$ and $\mathfrak{N}$ in K. □

3.3.4 Corollary. *Given the conditions as in the proposition, the set $S(A)$ can be defined via an existential formula in the language $\mathcal{L}_{ring+(a_{i,j,k})_{i,j,k}}$ with l^2 existential quantifiers.*

Proof. With the notation for $\mathfrak{T}$ and $\mathfrak{N}$ from above we have

$$S(A) = \{y \in K \mid \exists x_1, \dots, x_{l^2} \in K : (x_1, \dots, x_{l^2}, y) \in \mathfrak{T} \wedge (x_1, \dots, x_{l2}, 1) \in \mathfrak{N}\}$$

where $(x_1, \dots, x_{l^2}, y) \in \mathfrak{T}$ and $(x_1, \dots, x_{l2}, 1) \in \mathfrak{N}$ can be expressed through a quantifier-free expression by the proposition. □

We conclude by stating higher-dimensional analogues of Proposition 3.2.1 and Proposition 3.2.6. Surprisingly, both the local and the global result become easier.

3.3.5 Lemma. *Let F be a finite field, $l > 2$ a prime number. Then $F = U_l(F)$.*

Proof. See [Dit18, Lemma 2.7]. For $l = 3$ there is a simple counting argument: we need to show that to every $a \in F$ there exists a b such that $f_b(X) = X^3 - aX^2 + bX - 1$ is irreducible. If a given $f_b(X)$ is reducible, then there exists a $c \in F^\times$ such that $X - c$ divides $f_b(X)$. But for each such c, there can be at most one b such that $X - c$ divides $f_b(X)$. By counting, there must be an irreducible $f_b(X)$. □

3.3.6 Proposition. *Let K be a local field. Then for any prime number $l > 2$, $\mathcal{O}_K = U_l(K)$.*

Proof. If K is a local field, denote F for its finite residue field and red for the residue map $K \to F$. By previous lemma we have that

$$\mathcal{O}_K = \mathsf{red}^{-1}(F) = \mathsf{red}^{-1}(U_l(F)) \subseteq U_l(K) \subseteq \mathcal{O}_K$$

where the first inclusion is trivial from the definition of $U_l(K)$ and the second inclusion is given by Proposition 3.1.3. □

3.3.7 Proposition. *Let $l > 2$ be a prime number, A a central simple algebra of degree l over a global field K. Then*

$$S(A) = \bigcap_{\mathfrak{p} \in \Delta(A)} \mathcal{O}_{(\mathfrak{p})}.$$

Proof. Note that $\Delta(A)$ consists only of finite spots; as a central simple algebra of odd degree, $A_\mathfrak{p}$ is split for all infinite places $\mathfrak{p}$. The statement now follows through combination of Proposition 3.1.3, Proposition 3.1.4 and Proposition 3.3.6 □

3.3.8 Remark. The above gives rise to more definitions of subrings of global fields by methods similar to those in Section 3.2. For example, if K is a number field containing a third root of unity ζ, then it is known that all degree 3 central simple algebras are of the form $(a, b)^{[3]}$, i.e. generated over K by elements x, y such that $x^3 = a$, $y^3 = b$ and $yx = \zeta xy$. We find that

$$\mathcal{O}_K = \bigcap_{a,b \in K^\times} S((a, b)^{[3]}).$$

By Corollary 3.3.4, this translates to a $\forall\exists$-formula with two universal and nine existential quantifiers, defining $\mathcal{O}_K$ in K in any number field containing the third roots of unity.

Chapter 4

Universally defining rings of integers

Throughout this chapter we let K be a global field. We denote by $\mathbb{P}$ the set of finite spots (prime ideals) of K and by $\mathbb{P}'$ the set of all non-complex spots. For a spot $\mathfrak{p} \in \mathbb{P}'$ and a quaternion algebra Q over K, denote by $Q_\mathfrak{p}$ the quaternion algebra over the completion K_p.

4.1 From existential to universal

In Section 3.2 we showed how the ring of integers of a number field could be defined in this field through a $\forall\exists$-formula. Koenigsmann went further and found a way to define $\mathbb{Z}$ in $\mathbb{Q}$ via a universal formula. That is, he found an existential definition of $\mathbb{Q} \setminus \mathbb{Z}$ in $\mathbb{Q}$. [Koe16] This was later generalised to arbitrary number fields by Park in [Par13]. Kirsten Eisenträger and Travis Morrison then found a universal definition of the set of S-integers in an algebraic function field of odd characteristic, using a slightly different generalisation of Koenigsmann's argument. [EM18] For a finite set S of non-archimedean spots of a global field K, the *ring of S-integers* is defined to be

$$\mathcal{O}_S = \{x \in K \mid \forall \mathfrak{p} \in \mathbb{P} \setminus S : v_\mathfrak{p}(x) \geq 0\} = \bigcap_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathcal{O}_{(\mathfrak{p})}.$$

Note that when K is a number field and $S = \emptyset$ we recover the classical ring of integers. We will use some of the existentially definable sets introduced by Koenigsmann, but will then take a new approach to defining $\mathcal{O}_S$ in K, relying more heavily on Hilbert reciprocity than was done by Koenigsmann, but requiring no additional class field theory, unlike Park's approach. Furthermore, our approach should work in all global fields, including those of characteristic 2.

4.1.1 Proposition. *Let $S \subseteq \mathbb{P}$ be a non-empty set of prime ideals. Suppose that*

$$\bigcup_{\mathfrak{p} \in S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$$

has a positive-existential definition in K with n quantifiers. Then

$$\bigcap_{\mathfrak{p} \in S} \mathcal{O}_{(\mathfrak{p})}$$

has a universal definition in K with $n+1$ quantifiers.

Proof. Let $\varphi(t)$ be a positive-existential formula defining $\bigcup_{\mathfrak{p}\in S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ in K. We will show that

$$\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})} = \{x\in K \mid K\models \forall u(\neg(x\cdot u \doteq 1)\vee\neg\varphi(u)))\}$$

whereby we will have the required definition for $\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}$. Take $x\in K$, then indeed we have

$$\begin{aligned} x\in\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})} &\Leftrightarrow \forall\mathfrak{p}\in S: x\in\mathcal{O}_{(\mathfrak{p})} \Leftrightarrow \forall\mathfrak{p}\in S: v_{\mathfrak{p}}(x)\geq 0\\ &\Leftrightarrow x=0 \text{ or } \nexists\mathfrak{p}\in S: v_{\mathfrak{p}}(x^{-1})>0 \Leftrightarrow x=0 \text{ or } \nexists\mathfrak{p}\in S: x^{-1}\in\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}\\ &\Leftrightarrow x=0 \text{ or } x^{-1}\notin\bigcup_{\mathfrak{p}\in S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})} \Leftrightarrow K\models\neg(\exists u(x\cdot u\doteq 1\wedge\varphi(u)))\\ &\Leftrightarrow K\models\forall u(\neg(x\cdot u\doteq 1)\vee\neg\varphi(u))). \end{aligned}$$

□

4.1.2 Remark. The above proposition could be formulated more abstractly as follows: if the Jacobson radical of a subring of K containing $\mathcal{O}_K$ has an existential definition in K, then the ring itself has a universal definition.

4.1.3 Corollary. *Let $S\subseteq\mathbb{P}$ be a finite, non-empty set of prime ideals. Then $\bigcup_{\mathfrak{p}\in S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition with 15 quantifiers and $\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}$ has a universal definition with 16 quantifiers in $\mathcal{L}_{ring+K}$.*

Proof. The second statement follows from the first by Proposition 4.1.1. By Proposition 3.2.9 $\mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition with 15 quantifiers. Then the same holds for $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$: pick an element $\pi\in\mathfrak{p}\setminus\mathfrak{p}^2$, then $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}=\pi\mathcal{O}_{(\mathfrak{p})}$, whereby one can formalise the statement $x\in\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ by writing out the formula for $\frac{x}{\pi}\in\mathcal{O}_{(\mathfrak{p})}$, then clearing out denominators.

If every $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition with 15 quantifiers, then so does a finite union of such sets by (the proof of) Proposition 2.2.4. □

By the previous proposition it might feel like we are very close to an existential definition of $\bigcup_{\mathfrak{p}\in\mathbb{P}}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ in K, yielding the required universal definition of $\mathcal{O}_K$ by Proposition 4.1.1. However, in first-order formulas we can only quantify over the elements of K and not over, for example, the elements of $\mathbb{P}$. Thus even describing this union would require an appropriate definition of $\mathbb{P}$, which is probably harder than describing $\mathcal{O}_K$ in K. In the next proposition we outline the strategy which we will use to find existential definitions of $\bigcup_{\mathfrak{p}\in S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ for some infinite sets S.

4.1.4 Proposition. *Let $S\subseteq\mathbb{P}$ be a non-empty set of prime ideals. If there exists a set $\Phi\subseteq K^m$ for some $m\in\mathbb{N}$ and a family $(A_{\vec{x}})_{\vec{x}\in\Phi}$ of subsets of K such that*

- *Φ is a positive-existential subset of K^m with n_1 quantifiers.*
- *there is a positive-existential formula $\psi(t,\vec{u})$ with $m+1$ free variables and n_2 quantifiers such that $A_{\vec{x}}=\{y\in K\mid K\models\psi(y,\vec{x})\}$.*

- *each* $A_{\vec{x}}$ *with* $\vec{x} \in \Phi$ *is contained in some* $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ *for* $\mathfrak{p} \in S$.
- *each* $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ *with* $\mathfrak{p} \in S$ *is contained in some* $A_{\vec{x}}$ *with* $\vec{x} \in \Phi$.

Then we have

$$\bigcup_{\mathfrak{p}\in S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})} = \bigcup_{\vec{x}\in\Phi} A_{\vec{x}},$$

a positive-existential definition for $\bigcup_{\mathfrak{p}\in S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ *with* $n_1 + n_2 + m$ *quantifiers and a universal definition for* $\bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}$ *with* $n_1 + n_2 + m + 1$ *quantifiers.*

Proof. For the equality of sets, the inclusions $\supseteq$ and $\subseteq$ are enforced by the third and fourth hypotheses respectively. This leads to a positive-existential definition with $n_1 + n_2 + m$ quantifiers since for $y \in K$ we have that

$$y \in \bigcup_{\vec{x}\in\Phi} A_{\vec{x}} \Leftrightarrow \exists \vec{x} \in K^m : (\vec{x} \in \Phi \wedge y \in A_{\vec{x}}).$$

The last part follows from Proposition 4.1.1. □

4.2 Jacobson radical of semilocal subrings

For a quaternion algebra Q over K and a $c \in K^\times$ we define the following sets

$$\begin{aligned} T(Q)^\times &= \{u \in T(Q) \mid \exists v \in T(Q) \text{ with } uv = 1\} \\ I^c(Q) &= c \cdot K^2 T(Q)^\times \cap (1 - K^2 \cdot T(Q)^\times) \\ J^c(Q) &= I^c(Q) + I^c(Q) \\ H^c(Q) &= (c^{-1}T(Q) + cT(Q)^{-1})^{-1} \cup \{0\} \end{aligned}$$

where for a set $A \subseteq K$ we define $A^{-1} = \{x \in K^\times \mid x^{-1} \in A\}$. If $T(Q)$ is a ring, then $T(Q)^\times$ is the set of units of $T(Q)$, so this notation is consistent. For $c \in K^\times$, set

$$\begin{aligned} \mathbb{P}(c) &= \{\mathfrak{p} \in \mathbb{P} \mid v_\mathfrak{p}(c) \text{ is odd}\} \\ \mathbb{P}[c] &= \{\mathfrak{p} \in \mathbb{P} \mid v_\mathfrak{p}(c) < 0\} \end{aligned}$$

4.2.1 Proposition. *Let* $c \in K^\times$, Q *a quaternion algebra over* K.

1. *We have*

$$T(Q)^\times = \bigcap_{\mathfrak{p}\in\Delta(Q)} \mathcal{O}_{(\mathfrak{p})}^\times$$

whereby for an infinite spot $\mathfrak{p}$ *with corresponding place* $\sigma_\mathfrak{p}$,

$$\mathcal{O}_{(\mathfrak{p})}^\times = \sigma_\mathfrak{p}^{-1}(\mathcal{O}_{K_\mathfrak{p}}^\times) = \sigma_\mathfrak{p}^{-1}([-4, -\frac{1}{4}] \cup [\frac{1}{4}, 4]).$$

2. *Denoting by* $v_\mathfrak{p}$ *the normalised valuation at a finite spot* $\mathfrak{p} \in \mathbb{P}$ *we have*

$$K^2 \cdot T(Q)^\times = \{0\} \cup \bigcap_{\mathfrak{p}\in\Delta(Q)\cap\mathbb{P}} v_\mathfrak{p}^{-1}(2\mathbb{Z})$$

3. *For $y \in K^\times$, we have $y \in I^c(Q)$ if and only if both of the following hold:*

   (i) For all $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)$, $v_\mathfrak{p}(y)$ is odd and positive.

   (ii) For all $\mathfrak{p} \in (\Delta(Q) \cap \mathbb{P}) \setminus \mathbb{P}(c)$, $v_\mathfrak{p}(y)$ and $v_\mathfrak{p}(1-y)$ are even.

4. *One has*
$$J^c(Q) = \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}.$$

5. *For a real spot $\mathfrak{p} \in \mathbb{P}' \setminus \mathbb{P}$, denote by $\sigma_\mathfrak{p}$ the corresponding embedding into $\mathbb{R}$. We have*
$$H^c(Q) \subseteq \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}[c]} \mathfrak{p}^{-v_\mathfrak{p}(c)}\mathcal{O}_{(\mathfrak{p})}$$
and equality holds if $|\sigma_p(c)| \leq 4$ for all $\mathfrak{p} \in \Delta(Q) \setminus \mathbb{P}$.

Proof. The first statement follows immediately from Proposition 3.2.6.

We prove the second statement. The inclusion from left to right is trivial. Conversely, if y is a non-zero element of the right set, then for any $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}$, there exists a $u_\mathfrak{p} \in K^\times$ such that $v_\mathfrak{p}(y) = 2v_\mathfrak{p}(u_\mathfrak{p}) = v_\mathfrak{p}(u_\mathfrak{p}^2)$. Using weak approximation, we find a $u \in K^\times$ such that $v_\mathfrak{p}(y) = 2v_\mathfrak{p}(u) = v_\mathfrak{p}(u^2)$. Finally, using Theorem 1.6.4 once again, we can scale u by an appropriate element of $\bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}} \mathcal{O}^\times_{(\mathfrak{p})}$ to obtain $\frac{x}{u^2} \in T(Q)^\times$. This shows the other inclusion.

For the third statement, let first $y \in I^c(Q) \setminus \{0\}$. Then for $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)$, by definition of $I^c(Q)$ we get that $v_\mathfrak{p}(y)$ is odd and $v_\mathfrak{p}(1-y)$ is even. Then we have $0 = v_\mathfrak{p}(1-y+y) = \min\{v_\mathfrak{p}(1-y), v_\mathfrak{p}(y)\}$, whereby we must actually have $v_\mathfrak{p}(y) > 0$. On the other hand, if $\mathfrak{p} \in (\Delta(Q) \cap \mathbb{P}) \setminus \mathbb{P}(c)$, then $v_\mathfrak{p}(y)$ and $v_\mathfrak{p}(1-y)$ are even. This shows that elements of $I^c(Q) \setminus \{0\}$ satisfy conditions (i) and (ii).

Suppose now that $y \in K^\times$ satisfies (i) and (ii). Then from (i) we get that
$$c^{-1}y \in \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} v_\mathfrak{p}^{-1}(2\mathbb{Z})$$
and as $0 = v_\mathfrak{p}(1-y+y) = \min\{v_\mathfrak{p}(1-y), v_\mathfrak{p}(y)\}$ for $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)$,
$$1 - y \in \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} \mathcal{O}^\times_{(\mathfrak{p})} \subseteq \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} v_\mathfrak{p}^{-1}(2\mathbb{Z}).$$
From (ii) we get that
$$c^{-1}y, 1-y \in \bigcap_{\mathfrak{p} \in (\Delta(Q) \cap \mathbb{P}) \setminus \mathbb{P}(c)} v_\mathfrak{p}^{-1}(2\mathbb{Z}).$$
Hence if both (i) and (ii) hold, then
$$c^{-1}y, 1-y \in \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}} v_\mathfrak{p}^{-1}(2\mathbb{Z}) \subseteq K^2T(Q)^\times.$$

We now prove the equality
$$J^c(Q) = I^c(Q) + I^c(Q) = \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$$

The inclusion from left to right is trivial from condition (i). Let $x \in K^\times$. For each $\mathfrak{p} \in \mathbb{P}$ we can write x as a sum of two elements of $K^\times$ with $\mathfrak{p}$-adic value $v_\mathfrak{p}(x) - 1$. In fact, just pick any $y \in K^\times$ with $v_\mathfrak{p}(y) = v_\mathfrak{p}(x) - 1$, then we know that

$$v_\mathfrak{p}(x) = v_\mathfrak{p}(y + x - y) \geq \min\{v_\mathfrak{p}(y), v_\mathfrak{p}(x - y)\} = \min\{v_\mathfrak{p}(x) - 1, v_\mathfrak{p}(x - y)\}$$

and by the Principle of Domination equality holds unless $v_\mathfrak{p}(x) - 1 = v_\mathfrak{p}(x - y)$. Since equality cannot hold in our case, we must have $v_\mathfrak{p}(x) - 1 = v_\mathfrak{p}(x - y)$. Thus we have written x as a sum of two elements of value $v_\mathfrak{p}(x) - 1$. Note that if $v_\mathfrak{p}(x) \geq 2$, then $v_\mathfrak{p}(x) - 1 > 0$.

We infer from these considerations and by weak approximation that for $x \in \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ we can find y_1, y_2 which satisfy criteria (i) and (ii) and such that $x = y_1 + y_2$. This proves the other inclusion and thus the fourth statement.

Now for the fifth statement. Clearly 0 lies in the sets on both sides of the equation. Take $x \in H^c(Q) \setminus \{0\}$, then $x^{-1} = c^{-1}t' + ct^{-1}$ for some $t' \in T(Q)$, $t \in T(Q) \setminus \{0\}$. Assume that $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}[c]$. Then $v_\mathfrak{p}(c^{-1}t) = -v_\mathfrak{p}(c) + v_\mathfrak{p}(t') > 0$ and $v_\mathfrak{p}(ct^{-1}) = v_\mathfrak{p}(c) - v_\mathfrak{p}(t) < 0$. Thus by the Principle of Domination

$$v_\mathfrak{p}(x^{-1}) = \min\{v_\mathfrak{p}(c^{-1}t'), v_\mathfrak{p}(ct^{-1})\} = v_\mathfrak{p}(c) - v_\mathfrak{p}(t) \leq v_\mathfrak{p}(c)$$

whereby $v_\mathfrak{p}(x) \geq -v_\mathfrak{p}(c)$. This shows that the inclusion from left to right holds.

Suppose now that $|\sigma_p(c)| \leq 4$ for all $\mathfrak{p} \in \Delta(Q) \setminus \mathbb{P}$. Take a non-zero $x \in \bigcap_{\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}[c]} \mathfrak{p}^{-v_\mathfrak{p}(c)}\mathcal{O}_{(\mathfrak{p})}$, then $v_\mathfrak{p}(x) \geq v_\mathfrak{p}(c)$ for all $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}[c]$. We again use a technique based on weak approximation: we will show that for any $\mathfrak{p} \in \Delta(Q)$ we can find a $t_\mathfrak{p} \in T(Q_\mathfrak{p}) \setminus \{0\}$ such that $t'_\mathfrak{p} = cx^{-1} - c^2 t_\mathfrak{p}^{-1} \in T(Q_\mathfrak{p})$, then by weak approximation one can actually find a $t \in T(Q) \setminus \{0\}$ such that $t' = cx^{-1} - c^2 t^{-1} \in T(Q)$, whereby we will have $x^{-1} = c^{-1}t' + ct^{-1} \in H^c(Q)$.

When $\mathfrak{p} \in \Delta(Q) \cap \mathbb{P}$, then $T(Q_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$ by Proposition 3.2.1. Assume first that $v_\mathfrak{p}(x) \geq -v_\mathfrak{p}(c)$. In this case we can set $t_\mathfrak{p} = xc$, as then $v_\mathfrak{p}(xc) = v_\mathfrak{p}(x) + v_\mathfrak{p}(c) \geq 0$ and $t'_\mathfrak{p} = cx^{-1} - c^2 t_\mathfrak{p} = 0 \in T(Q_\mathfrak{p})$. Now suppose that $v_\mathfrak{p}(x) < -v_\mathfrak{p}(c)$. By our assumption on x this is only possible when $v_\mathfrak{p}(c) \geq 0$. In this case we can set $t_\mathfrak{p} = 1 \in T(Q_\mathfrak{p}) \setminus \{0\}$, for then $t'_\mathfrak{p} = cx^{-1} - c^2 t_\mathfrak{p}^{-1}$ has value $v_\mathfrak{p}(c) + v_\mathfrak{p}(x^{-1} - c) = 2v_\mathfrak{p}(c) \geq 0$, whereby $t'_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} = T(Q_\mathfrak{p})$.

Finally we consider a real spot $\mathfrak{p} \in \Delta(Q)$. Then $T(Q_\mathfrak{p}) = [-4, 4]$ and $T(Q_\mathfrak{p})^{-1} =]-\infty, -\frac{1}{4}] \cup [\frac{1}{4}, +\infty[$. It is clear that if $|\sigma_\mathfrak{p}(c)| \leq 4$, then

$$\sigma_\mathfrak{p}(c)^{-1}] - 4, 4[+ \sigma_\mathfrak{p}(c) \left(\right] -\infty, -\frac{1}{4} \left[\cup \right] \frac{1}{4}, +\infty \left[\right) \supseteq \mathbb{R}^\times$$

whereby we will be able to find appropriate $t_\mathfrak{p}$ and $t'_\mathfrak{p}$. □

4.2.2 Corollary. *Let $a, b, c \in K^\times$ and suppose that $\mathrm{char}(K) \neq 2$ and $\mathbb{P}(c)$ contains all dyadic prime ideals. Then*

$$J^a((a,b)) \cap J^b((a,b)) \cap J^c((a,b)) = \bigcap_{\mathfrak{p} \in \Delta((a,b)) \cap \mathbb{P}} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}.$$

Proof. By the fourth part of the proposition we have

$$J^a((a,b)) \cap J^b((a,b)) \cap J^c((a,b)) = \bigcap_{\mathfrak{p} \in \Delta((a,b)) \cap (\mathbb{P}(a) \cup \mathbb{P}(b) \cup \mathbb{P}(c))} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}.$$

Thus we have to argue why $\Delta((a,b)) \cap (\mathbb{P}(a) \cup \mathbb{P}(b) \cup \mathbb{P}(c)) = \Delta((a,b)) \cap \mathbb{P}$, i.e. $\Delta((a,b)) \cap \mathbb{P} \subseteq \mathbb{P}(a) \cup \mathbb{P}(b) \cup \mathbb{P}(c)$. This follows from Proposition 1.5.2. □

4.2.3 Corollary. *Let $a, b \in K^\times$ and suppose that* $\mathrm{char}(K) = 2$. *Then*

$$H^a([a,b)) \cap J^b([a,b)) \subseteq \bigcap_{\mathfrak{p} \in \Delta([a,b))} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$$

and equality holds when $v_\mathfrak{p}(a) \geq -1$ for all $\mathfrak{p} \in \Delta([a,b))$.

Proof. By Proposition 1.5.3 we have $\Delta([a,b)) \subseteq \mathbb{P}[a] \cup \mathbb{P}(b)$. The claim now follows from the fourth and fifth parts of the proposition. □

4.2.4 Remark. This last corollary does not hold if K has any other characteristic than 2, since then we no longer have $\Delta([a,b)) \subseteq \mathbb{P}[a] \cup \mathbb{P}(b)$. Indeed, over $\mathbb{Q}$ we have that $[13,-1)_\mathbb{Q} \cong (3,-1)_\mathbb{Q}$ is non-split over $\mathbb{Q}_3$, but $v_3(13) = v_3(-1) = 0$.

4.2.5 Lemma. *Denote by $Q_{a,b}$ either $(a,b)_K$ (if* $\mathrm{char}(K) \neq 2$*) or $[a,b)_K$. There exists a positive-existential formula $\varphi(a,b,c,d)$ with 3 quantifiers such that for $a, b \in K^\times$ (respectively $b, 1+4a \in K^\times$) and $c, d \in K$*

$$K \models \varphi(a,b,c,d) \Leftrightarrow (c = d = 0 \text{ or } (d \neq 0 \text{ and } \frac{c}{d} \in S(Q_{a,b}))).$$

Similarly, there exists a positive-existential formula $\psi(a,b,c,d)$ with 7 quantifiers such that for $a, b \in K^\times$ (respectively $b, 1+4a \in K^\times$) and $c, d \in K$,

$$K \models \psi(a,b,c,d) \Leftrightarrow (c = d = 0 \text{ or } (d \neq 0 \text{ and } \frac{c}{d} \in T(Q_{a,b})))$$

Proof. We give the proof for $Q_{a,b} = (a,b)_K$; the proof for $[a,b)_K$ is similar. Set

$$\varphi(a,b,c,d) = \exists x_2, x_3, x_4 (c^2 - 4ax_2^2d^2 - 4bx_3^2d^2 + 4abx_4^2d^2 = 4d^2)$$

and always assume $a, b \neq 0$. Then this formula trivially does not hold when $d = 0$ and $c \neq 0$ and it trivially holds when $c = d = 0$. If we assume now that $d \neq 0$, then we can divide the equation by d^2 to obtain the formula saying that $\frac{c}{d} \in S((a,b))$.

Now set

$$\psi(a,b,c,d) = \exists y (\varphi(a,b,y,1) \wedge \varphi(a,b,yd-c,d)).$$

Using the formulae from Proposition 2.2.4 this can be reformulated as a positive-existential formula with 7 quantifiers. Assuming again that $a, b \neq 0$, this formula holds when $c = d = 0$ (choose $y = 2$) and does not hold when $d = 0$ and $c \neq 0$ by the result for φ. If $d \neq 0$, $\varphi(a,b,yd-c,d)$ can be interpreted as $y - \frac{c}{d} = \frac{yd-c}{d} \in S((a,b))$ and we reobtain the definition of $\frac{c}{d} \in T((a,b))$. □

4.2.6 Proposition. *L $Q_{a,b}$ be as above, let $a, b, c \in K^\times$ (respectively $b, c, 1+4a \in K^\times$). There exist positive-existential definitions of $T(Q_{a,b})^\times$, $I^c(Q_{a,b})$, $J^c(Q_{a,b})$ and $H^c(Q_{a,b})$ with* 14, 30, 61 *and* 15 *quantifiers respectively.*

Proof. Reusing the notation of last lemma,

$$T(Q_{a,b})^\times = \{x \in K \mid K \models \psi(a,b,x,1) \wedge \psi(a,b,1,x)\},$$

yielding a definition with $7+7=14$ quantifiers. For $x \in K$ and again $a,b,c \in K^\times$ we have

$$x \in I^c(Q_{a,b}) \Leftrightarrow \exists q, q' \in K : (cxq^2 \in T(Q_{a,b})^\times \text{ and } (1-x)q'^2 \in T(Q_{a,b})^\times).$$

We count $2+14+14=30$ quantifiers. By the trick for 'adding' two sets, we obtain a positive-existential definition of $J^c(Q_{a,b})$ with $2 \cdot 30 + 1 = 61$ quantifiers.

Finally we claim that for $x \in K$ and $c \in K^\times$,

$$x \in H^c(Q_{a,b}) \Leftrightarrow K \models \exists t(\psi(a,b,t,1) \wedge \psi(a,b,ct-c^2x,tx)).$$

This would yield the required positive-existential definition with 15 quantifiers. If $x = 0 \in H^c(Q_{a,b})$, then the formula on the right holds (set $t=0$). On the other hand, if $t=0$, then $K \models \psi(a,b,ct-c^2x,tx)$ implies that $x=0$.

Suppose now that $tx \neq 0$. Then $K \models \psi(a,b,t,1) \wedge \psi(a,b,ct-c^2x,tx)$ is equivalent to $t \in T(Q_{a,b}) \wedge \frac{ct-c^2x}{tx} \in T(Q_{a,b})$. This is true if and only if $t \in T(Q_{a,b})$ and there exists a $t' \in T(Q_{a,b})$ with $x^{-1} = ct^{-1} + c^{-1}t'$.

We conclude that

$$\begin{aligned} x \in H^c(Q_{a,b}) &\Leftrightarrow x = 0 \text{ or } x^{-1} \in c^{-1}T(Q) + cT(Q)^{-1} \\ &\Leftrightarrow x = 0 \text{ or } \exists t \in T(Q) \setminus \{0\} : K \models \psi(a,b,ct-c^2x,tx) \\ &\Leftrightarrow K \models \exists t(\psi(a,b,t,1) \wedge \psi(a,b,ct-c^2x,tx)). \end{aligned}$$

□

4.3 A universal definition of $\mathbb{Z}$ in $\mathbb{Q}$

Let now $K = \mathbb{Q}$; identify $\mathbb{P}$ with the set of rational prime numbers and $\mathbb{P}'$ with $\mathbb{P} \cup \{\infty\}$ with ∞ representing the unique real spot.

In this section we give a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$.

4.3.1 Lemma. *Let l be a positive prime number.*

- *If $l \equiv -1 \bmod 4$, $\Delta((-1,-2l)) = \{l, \infty\}$.*
- *If $l \equiv 3 \bmod 8$ or $l \equiv 5 \bmod 8$, $\Delta((-l,-2)) = \{l,\infty\}$*
- *If $l \equiv 1 \bmod 8$ and p is a positive prime such that $p \equiv 5 \bmod 8$ and $\left(\frac{p}{l}\right) = -1$, then $\Delta((-p,-2l)) = \{l,\infty\}$.*

Proof. If $l \equiv -1 \bmod 4$, -1 is not a square modulo l. It follows by Proposition 1.5.11, Proposition 1.7.6 and Proposition 1.5.1 that $\{l,\infty\} = \Delta((-1,-2l))$.

If $l \equiv 3 \bmod 8$ or $l \equiv 5 \bmod 8$, 2 is not a square modulo l. The statement thus follows again from the same three propositions.

Finally, suppose $l \equiv 1 \bmod 8$, $0 < p \equiv 5 \bmod 8$ and $\left(\frac{p}{l}\right) = -1$. Then again by the same three propositions we have $\{\infty, l\} \subseteq \Delta((-p,-2l)) \subseteq \{\infty, l, p\}$; by Hilbert Reciprocity (Theorem 1.7.7) we must actually have $\Delta((-p,-2l)) = \{l,\infty\}$. □

4.3.2 Lemma. *Let $p, q \in \mathbb{Q}^\times$ be such that $v_2(q)$ is even. Then*

$$J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q)) = \bigcap_{l \in \Delta((-p,-2q)) \setminus \{\infty\}} l\mathbb{Z}_{(l)}$$

Proof. By the third part of Proposition 4.2.1 we have

$$J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q)) = \bigcap_{l \in \Delta} l\mathbb{Z}_{(l)}$$

with $\Delta = \Delta((-p,-2q)) \cap \mathbb{P}(-p) \cap \mathbb{P}(-2q)$. Note that $2 \in \mathbb{P}(-2q)$ as $v_2(q)$ is even by the hypothesis on q. By Proposition 1.7.6 we have $\Delta((-p,-2q)) \setminus \{\infty\} \subseteq \mathbb{P}(-p) \cup \mathbb{P}(-2q) \cup \{2\} = \mathbb{P}(-p) \cup \mathbb{P}(-2q)$. We see that $\Delta = \Delta((-p,-2q)) \setminus \{\infty\}$, concluding the proof. □

4.3.3 Theorem. *We have*

$$\bigcup_{l \in \mathbb{P}} l\mathbb{Z}_{(l)} = \bigcup_{\substack{p,q>0 \\ q \in \mathbb{Q}^2 T((-1,-1))^\times}} J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q)).$$

Hence, there is a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ with 148 quantifiers.

Proof. We apply the strategy outlined in Proposition 4.1.4.

First, recall from the second part of Proposition 4.2.1 that $\mathbb{Q}^2 T((-1,-1))^\times = \{0\} \cup v_2^{-1}(2\mathbb{Z})$, as $\Delta((-1,-1)) = \{2, \infty\}$.

For any $p, q > 0$, $(-p,-2q)_\infty$ is non-split. It follows by Hilbert reciprocity (Theorem 1.7.7) that $(-p,-2q)$ is non-split at some finite prime too. $\Delta = \Delta((-p,-2q)) \setminus \{\infty\}$ is therefore non-empty and by Lemma 4.3.2, $J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q)) = \bigcap_{l \in \Delta} l\mathbb{Z}_{(l)} \subseteq \bigcup_{l \in \mathbb{P}} l\mathbb{Z}_{(l)}$ if additionally $q \in \mathbb{Q}^2 T((-1,-1))^\times = \{0\} \cup v_2^{-1}(2\mathbb{Z})$. This shows the inclusion from right to left.

For the other inclusion we need to show - as explained in Proposition 4.1.4 - that for any prime $l \in \mathbb{P}$ there exist some parameters p and q such that $J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q)) = \mathbb{Z}_{(l)}$, i.e. such that $\Delta((-p,-2q)) \setminus \{\infty\} = \{l\}$. This follows from Lemma 4.3.1:

- If $l = 2$, one can take $p = q = 1$.
- If $l \equiv 3 \bmod 8$ or $l \equiv 7 \bmod 8$ one can take $p = 1$, $q = l$.
- If $l \equiv 3 \bmod 8$ or $l \equiv 5 \bmod 8$, take $p = l$, $q = 1$.
- If $l \equiv 1 \bmod 8$, one can set $q = l$ and let p be a prime such that $p \equiv 5 \bmod 8$ and $\left(\frac{p}{l}\right) = -1$.

This concludes the proof of the equality. To see how this leads to a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ with 148 quantifiers, note that we need $122 = 61 + 61$ quantifiers just for $J^{-p}((-p,-2q)) \cap J^{-2q}((-p,-2q))$ already. Another four quantifiers are needed to express $p > 0$ (using the Four Square Theorem) and same for $q > 0$. Finally, $\mathbb{Q}^2 T((-1,-1))^\times$ needs another 15 quantifiers to define. This brings the total to $122 + 2 + 2 \cdot 4 + 15 = 147$ existential quantifiers for $\bigcup_{l \in \mathbb{P}} l\mathbb{Z}_{(l)}$, or 148 universal quantifiers for $\mathbb{Z}$. □

4.3.4 Remark. The novelty in the above approach is how we obtained the inclusion from right to left: we described a collection of quaternion algebras which were always non-split at ∞ - a spot seemingly unrelated to the set which is to be defined - to ensure that, by Hilbert Reciprocity, every quaternion algebra in the collection would also be non-split at a finite spot. One could say we used the infinite spot as a *pivot* in our definition. In the next section, we will describe how one can also use finite primes as pivots, yielding a technique which - unlike the above - works for general global fields.

4.4 Jacobson radical of rings of integers

In this section, we return to the general setting of a global field K, generalising the result from previous section. For the rest of this section, let K always be a global field. We will show that for any finite set $S \subseteq \mathbb{P}$, there is an existential definition of

$$\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$$

in K in the language $\mathcal{L}_{\text{ring}+K}$, where $\mathcal{O}_{(\mathfrak{p})}$ is the valuation ring with respect to $\mathfrak{p}$. This then implies a universal definition of $\bigcap_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathcal{O}_{(\mathfrak{p})}$ via Proposition 4.1.1. For the rest of the chapter, all definability results are to be interpreted in the extended language $\mathcal{L}_{\text{ring}+K}$ as explained in Section 2.3.

Setting $S = \emptyset$ we find a universal definition of the ring of integers $\mathcal{O}_K$ in a number field K. However, even if one is only interested in the case $S = \emptyset$, it will be crucial in our proof to also allow S to be non-empty.

We recall some of the existential definitions we have used so far and introduce some new ones as well. By Corollary 4.1.3, every $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is existential in K. It follows that we can also describe a statement like $x \equiv y \bmod \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ positive-existentially, with 15 quantifiers. For $a, b, c \in K^\times$, we have a positive-existential definition with 61 quantifiers for the set

$$J^c((a,b)) = \bigcap_{l \in \Delta((a,b)) \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}.$$

Finally, by a theorem of Siegel, the totally positive elements of K (i.e. elements which are squares at each infinite spot) are precisely the sums of four squares in K. [Sie21] Hence the formula

$$\varphi(t) = \exists a_1, a_2, a_3, a_4 (t \cdot (a_1^2 + a_2^2 + a_3^2 + a_4^2) \doteq 1)$$

positive-existentially defines the set of non-zero, totally positive elements in K. If K has no real spots (i.e. all elements are totally positive) then the above formula may be replaced by simply $\exists u(t \cdot u \doteq 1)$. For $x \in K$, we will write $x > 0$ for $K \models \varphi(x)$.

4.4.1 Proposition. *Let $S \subseteq S' \subseteq \mathbb{P}$ and suppose that $S' \setminus S$ is finite. If $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S'} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition with n quantifiers, then the set $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ has a positive-existential definition with $\max\{n, 15\}$ quantifiers.*

Proof. We have

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}=\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S'}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}\cup\bigcup_{\mathfrak{p}\in S'\setminus S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$$

and by Proposition 2.2.4, a finite union of positive-existential sets is again positive-existential. The number of quantifiers can be chosen to be the maximum of the ones needed for the components of the union. □

In particular, to prove that $\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S}\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is positive-existential for all finite sets S, it is sufficient to find a definition for sets S of odd cardinality.

Suppose for the rest of this section that $\mathrm{char}(K)\neq 2$. Let $\mathbb{P}^{[2]}$ be the finite set of dyadic spots. For a finite spot $\mathfrak{p}$ of K and an element $a\in\mathcal{O}_{(\mathfrak{p})}^{\times}$ we introduce the notation $a\not\boxtimes\mathfrak{p}$ to signify:

- if $\mathfrak{p}\notin\mathbb{P}^{[2]}$: a is not a square modulo $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$.
- if $\mathfrak{p}\in\mathbb{P}^{[2]}$: a is not a square modulo $4\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ but a is a square modulo $4\mathcal{O}_{(\mathfrak{p})}$.

This is motivated by the role of the element Δ introduced in Section 1.4. Furthermore, if S is a set of finite spots, denote by $\Xi(S)$ the set of all $a\in K^{\times}$ for which $a\not\boxtimes\mathfrak{p}$ for all $\mathfrak{p}\in S$.

4.4.2 Lemma. *For any finite set of finite spots S, $\Xi(S)$ is non-empty.*

Proof. As $a\not\boxtimes\mathfrak{p}$ is an open condition for every spot $\mathfrak{p}$, by weak approximation (Theorem 1.6.4) it is sufficient to find for each $\mathfrak{p}\in S$ an $a\in K$ such that $a\not\boxtimes\mathfrak{p}$. This is possible by Proposition 1.4.6. □

4.4.3 Lemma. *Let S be a non-empty, finite set of finite spots of K, $u\in\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}^{\times}$. Then the set*

$$\Phi_u^S=\{(a,b)\in K^2\mid a>0,b\in\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}^{\times},a\equiv u \bmod\prod_{\mathfrak{p}\in S}4\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}\}$$

has a positive-existential definition with 49 quantifiers. The number of quantifiers can be reduced by 4 if K is non-real, by 3 when $|S|$ is odd but at least 3 and by 24 if $|S|$ if even.

Proof. By the remark on Siegel's theorem we can describe $a>0$ with four existential quantifiers, but if K is non-real we may as well omit this.

By Proposition 3.2.9 and Proposition 3.2.10 we can describe $\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}$ with $7, 14$ or 15 quantifiers depending on whether $|S|$ is even, odd but greater than 1, or 1. Then by (the technique from) Proposition 4.2.6 we can define $\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}^{\times}$ with double the number of quantifiers (14, 28 or 30). Finally, having fixed an element $\pi\in K^{\times}$ with $\pi\in 4\mathfrak{p}\setminus 4\mathfrak{p}^2$ for all $\mathfrak{p}\in S$ by Weak Approximation, $a\equiv u \bmod\prod_{\mathfrak{p}\in S}4\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ can be rewritten as $\frac{a-u}{\pi}\in\bigcap_{\mathfrak{p}\in S}\mathcal{O}_{(\mathfrak{p})}$, thus requiring an additional 7, 14 or 15 quantifiers. □

4.4.4 Theorem. *Let S be a finite set of finite spots of K of odd cardinality, $\pi\in K^{\times}$ such that $S\subseteq\mathbb{P}(\pi)$. Let $u,c\in K^{\times}$ be such that*

(i) $u\in\Xi(S)$.

(ii) for all $\mathfrak{p} \in S$, $v_\mathfrak{p}(c) = 0$ *and for all* $\mathfrak{p} \in \mathbb{P}^{[2]} \cup \mathbb{P}(\pi) \setminus S$, $v_\mathfrak{p}(c) = 1$.

Then

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})} = \bigcup_{(a,b)\in\Phi_u^S} (J^a((a,b\pi)) \cap J^b((a,b\pi)) \cap J^c((a,b\pi))).$$

In particular, the set $\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ *is a positive-existential subset of* K *in* $\mathcal{L}_{ring+K}$.

4.4.5 Remark. Note that the existence of an appropriate u is given by Lemma 4.4.2 and the existence of π and c by weak approximation ($\mathbb{P}^{[2]} \cap \mathbb{P}(\pi)$ is finite).

Proof of Theorem 4.4.4. By Proposition 4.1.4, Proposition 4.2.6 and Lemma 4.4.3, the set on the right of the equality sign has a positive-existential definition; we need only show the equality.

Let $D_{a,b} = \Delta((a,b\pi)) \cap (\mathbb{P}(a) \cup \mathbb{P}(b) \cup \mathbb{P}(c))$. Note that when $a > 0$, $\Delta((a,b\pi))$ contains no infinite places, and when b and a satisfy the given congruences, $(\mathbb{P}(a) \cup \mathbb{P}(b) \cup \mathbb{P}(c)) \cap S = \emptyset$ and $\mathbb{P}(\pi) \setminus S \subseteq \mathbb{P}(c)$. Hence by Proposition 1.5.2, $D_{a,b} = \Delta((a,b\pi)) \setminus S$. Since we know that for $d \in K^\times$, $J^d((a,b)) = \bigcap_{l\in\Delta((a,b))\cap\mathbb{P}(d)} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$, what we have to show is in fact

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})} = \bigcup_{(a,b)\in\Phi_u^S} \left(\bigcap_{\mathfrak{p}\in D_{a,b}} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})} \right).$$

For the inclusion from right to left, we need only show that $D_{a,b}$ always contains an element of $\mathbb{P} \setminus S$. By the choice of a and b and Proposition 1.5.5, we will have $S \subseteq \Delta((a,b\pi))$. As S contains an odd number of elements, Hilbert reciprocity (Theorem 1.7.7) tell us that $\Delta((a,b\pi)) \setminus S = D_{a,b}$ is non-empty.

To show the other inclusion, it is sufficient to prove that for all $\mathfrak{q} \in \mathbb{P} \setminus S$ there exist a and b satisfying the criteria and such that $D_{a,b} = \{\mathfrak{q}\}$. By weak approximation, we can pick an $a > 0$ such that $a \equiv u \bmod \prod_{\mathfrak{p}\in S} 4\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ and $a \not\equiv \mathfrak{q}$. By Theorem 1.7.10 we can find a $b' \neq 0$ such that $\Delta((a,b'\pi)) = S \cup \{\mathfrak{q}\}$. By Proposition 1.5.5 we have that $v_\mathfrak{p}(\pi b') = 1 + v_\mathfrak{p}(b')$ is odd for all $\mathfrak{p} \in S$, whereby $v_\mathfrak{p}(b')$ is even. Hence we can multiply b' by an appropriate square to obtain a $b \in \bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}^\times$. Then the a en b are as desired and by previous considerations, $D_{a,b} = \Delta((a,b\pi)) \setminus S = \Delta((a,b'\pi)) \setminus S = \{\mathfrak{q}\}$. □

4.4.6 Remark. If $\mathbb{P}^{[2]} \cup \mathbb{P}(\pi) \setminus S$ is empty in Theorem 4.4.4 - that is, if $\mathbb{P}^{[2]} \subseteq S = \mathbb{P}(\pi)$ - then there is no need for an element c and one can remove the part $\cap J^c((a,b\pi))$ from the equation. Existence of such an S is guaranteed if the class number of K is 1, as then any finite subset of $\mathbb{P}$ is of the form $\mathbb{P}(a)$ for some $a \in K$.

4.4.7 Remark. The exact number of quantifiers in the obtained definition depends on the field K, the cardinality of $|S|$ and whether we can eliminate the need for the set $J^c_{a,b\pi}$. In the worst case scenario, we need $49 + 2$ quantifiers for Φ_u^S and $3 \cdot 61$ for the set $J^a_{a,b\pi} \cap J^b_{a,b\pi} \cap J^c_{a,b\pi}$, bringing the total to 234.

4.5 The characteristic 2 case

We can modify the approach to work with quaternion algebras of the form $[a,b)_K$ instead of $(a,b)_K$.

Let S be a finite set of finite spots. Define the set

$$\Xi'(S) = \{a \in K^\times \mid \forall \mathfrak{p} \in S : v_\mathfrak{p}(a) = 0 \text{ and } X^2 - X - d \text{ is irreducible modulo } \pi\}.$$

4.5.1 Lemma. *For any finite set of prime ideals S, $\Xi'(S)$ is non-empty.*

Proof. As the conditions on S are open with respect to every $\mathfrak{p} \in S$, by weak approximation it is sufficient to find for each $\mathfrak{p} \in S$ a $d \in K^\times$ with $v_\mathfrak{p}(d) = 0$ and $X^2 - X - d$ irreducible modulo π. This is possible. □

4.5.2 Lemma. *Let S be a non-empty, finite set of finite spots of K, $u \in \bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}^\times$. Then the set*

$$\Psi_u^S = \{(a,b) \in K^2 \mid b \in \bigcap_{\mathfrak{p}\in S} \mathcal{O}_{(\mathfrak{p})}^\times, a \equiv u \bmod \prod_{\mathfrak{p}\in S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}\}$$

has a positive-existential definition in K with 45 quantifiers. The number of quantifiers can be reduced by 3 when $|S|$ is odd but at least 3 and by 24 if $|S|$ is even.

Proof. Very similar to the proof of Lemma 4.4.3. □

4.5.3 Theorem. *Assume K is a global field with $\mathrm{char}(K) = 2$. Let S be a finite set of spots of K of even cardinality, $\pi \in K^\times$ such that $S \subseteq \mathbb{P}(\pi)$. Let $u, c \in K^\times$ be such that*

(i) $u \in \Xi'(S)$

(ii) for all $\mathfrak{p} \in S$, $v_\mathfrak{p}(c) = 0$ and for all $\mathfrak{p} \in \mathbb{P}(\pi) \setminus S$, $v_\mathfrak{p}(c) = 1$.

Then

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})} = \bigcup_{(a,b)\in\Psi_u^S} (H^a([a,b\pi)) \cap J^b([a,b\pi)) \cap J^c([a,b\pi))).$$

In particular, the set $\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is a positive-existential subset of K in $\mathcal{L}_{ring+K}$.

Proof. By Proposition 4.1.4, Proposition 4.2.6 and Lemma 4.4.3, the set on the right of the equality sign has a positive-existential definition; we need only show the equality.

If $(a,b) \in \Psi_u^S$ then for all $\mathfrak{p} \in S$ one has that $v_\mathfrak{p}(a) = 0$, $v_\mathfrak{p}(b\pi) = v_\mathfrak{p}(b) + v_\mathfrak{p}(\pi) = 0+1 = 1$ and $X^2 - X - a$ is irreducible modulo $\mathfrak{p}$. It follows by Proposition 1.5.4 that $S \subseteq \Delta([a,b\pi))$. As $|S|$ is odd, Hilbert Reciprocity then guarantees that there is a $\mathfrak{q} \in \Delta([a,b\pi)) \setminus S$. By Proposition 1.5.3 either $v_\mathfrak{q}(a) < 0$ whereby $H^a([a,b\pi)) \subseteq \mathfrak{q}\mathcal{O}_{(\mathfrak{q})}$, or $v_\mathfrak{q}(b\pi)$ is odd. And it the latter case, either $v_\mathfrak{q}(b)$ is odd and thus $J^b([a,b\pi)) \subseteq \mathfrak{q}\mathcal{O}_{(\mathfrak{q})}$, or $v_\mathfrak{q}(\pi)$ is odd and $J^c([a,b\pi)) \subseteq \mathfrak{q}\mathcal{O}_{(\mathfrak{q})}$. This concludes the proof for the inclusion from right to left.

To show the other inclusion, it suffices to show that for any given $\mathfrak{q} \in \mathbb{P} \setminus S$ there exist $(a,b) \in \Psi_u^S$ such that $v_\mathfrak{q}(a) = 0$ and $\Delta([a,b\pi)) = S \cup \{\mathfrak{q}\}$. Indeed, having found such (a,b) we would have that $H^a([a,b\pi)) \cap J^b([a,b\pi)) \cap J^c([a,b\pi)) = \mathfrak{q}\mathcal{O}_{(\mathfrak{q})}$.

Given a $\mathfrak{q} \in \mathbb{P} \setminus S$, by weak approximation there exists an $a \in K^\times$ such that $a \equiv u \bmod \prod_{\mathfrak{p}\in S} \mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$, $v_\mathfrak{q}(a) = 0$ and $X^2 - X - a$ is irreducible modulo $\mathfrak{q}$. By Theorem 1.7.11 we can find a $b' \in K^\times$ such that $\Delta([a, b'\pi)_K) = S \cup \{\mathfrak{q}\}$. Proposition 1.5.4 tells us that $v_\mathfrak{p}(b'\pi) = 1 + \mathfrak{p}(\pi)$ is odd for all $\mathfrak{p} \in S$, whereby $v_\mathfrak{p}(b')$ is even and we may multiply b' by an appropriate square to obtain $b \in \bigcap_{\mathfrak{p}\in S} \mathcal{O}^\times_{(\mathfrak{p})}$. Then $(a, b) \in \Psi^S_u$ and $\Delta([a, b\pi)_K) = S \cup \{\mathfrak{q}\}$, whereby we are done. □

4.5.4 Remark. The above theorem is never true if one replaces K by a global field of characteristic different from 2, for the same reason that Corollary 4.2.3 no longer holds. If one is not bothered by unnecessarily complex formulas and more quantifiers than needed, then one could make the above theorem work for global fields of all characteristics by replacing the right hand side by

$$\bigcup_{(a,b)\in\Psi^S_u} (H^a([a, b\pi)) \cap J^b([a, b\pi)) \cap J^c([a, b\pi)) \cap J^{1+4a}([a, b\pi))).$$

4.6 Ring of integers and non-standard models

In this short final section, we give some model-theoretic corollaries of the result obtained in previous section, as well as a model-theoretic criterion which could possibly be used to prove whether the ring of integers of a number field is diophantine. This was done in some form in [Koe16].

Throughout this section, let K be a number field with ring of integers $\mathcal{O}_K$. Recall from the last part of Section 2.2 that if $A \subseteq K$ is a definable subset of K and $K' \in \mathrm{Mod}(\mathrm{Th}(K))$, then we can define the transfer A' of A as the subset of K' which is defined by a formula defining A in K. This subset A' does not depend on the choice of formula.

4.6.1 Proposition. *Let $K', K'' \in \mathrm{Mod}(\mathrm{Th}(K))$ with K' a subfield of K''. Let $\mathcal{O}'_K$ and $\mathcal{O}''_K$ be the respective transfers of $\mathcal{O}_K$ in K' and K''. Then*

$$\mathcal{O}''_K \cap K' \subseteq \mathcal{O}'_K.$$

Proof. Fix a universal formula $\varphi(t)$ defining $\mathcal{O}_K$. Let $x \in \mathcal{O}''_K \cap K'$. Then $K'' \models \varphi(x)$. As $\varphi(t)$ is a *universal* formula, when it holds in a larger structure, it must also hold in a smaller structure. Hence $K' \models \varphi(x)$, whereby $x \in \mathcal{O}'_K$. □

4.6.2 Proposition. *The following are equivalent for the number field K:*

(1) $\mathcal{O}_K$ is existential in K.

(2) For all K', $K'' \in \mathrm{Mod}(\mathrm{Th}(K))$ with K' a subfield of K'' and $\mathcal{O}'_K$ and $\mathcal{O}''_K$ the respective transfers of $\mathcal{O}_K$ in K' and K'', we have

$$\mathcal{O}''_K \cap K' = \mathcal{O}'_K.$$

Proof. By Proposition 2.5.1, (1) is equivalent to $\mathcal{O}'_K \subseteq \mathcal{O}''_K$ for all K', K'' as in (2). As $\mathcal{O}'_K \subseteq K'$ by definition, $\mathcal{O}'_K \subseteq \mathcal{O}''_K$ is in turn equivalent to $\mathcal{O}'_K \subseteq \mathcal{O}''_K \cap K'$. And having this for all K', K'' is equivalent to (2), as the other inclusion was shown unconditionally in previous proposition. □

Recall that Theorem 2.5.2, the main result of [Dit18], shows that there is a large class of universal formulas over global fields equivalent to existential formulas. If one could show that *every* universal formula is equivalent to an existential formula over K, it would follows by induction that every first-order formula would be equivalent to an existential formula over K (one says the theory of K would be *model complete*). In particular, this would yield the desired existential definition of $\mathcal{O}_K$ in K, or $\mathbb{Z}$ in $\mathbb{Q}$ in the case $K = \mathbb{Q}$. It turns out that this is more than one can reasonably hope for.

4.6.3 Lemma. *Let R be a finite or countable ring, S a subset. Let $A, B \subseteq R$ satisfy $A \cup B \supseteq S$ and $A \cap B \cap S = \emptyset$. Suppose that there exists a decision algorithm which evaluates the truth of polynomial equalities over R. If both A and B are existential, then there exists an algorithm which, on input an element $x \in S$, decides whether $x \in A$ or $x \notin A$.*

Proof. Note that by assumption, there exists a decision algorithm which evaluates quantifier-free statements over R. Let ψ_1, ψ_2 be quantifier-free formulas with $\mathrm{Fr_v}(\psi_1) \cup \mathrm{Fr_v}(\psi_2) \subseteq \{t, x_1, \ldots, x_n\}$ such that

$$A = \{t \in R \mid R \models \exists x_1, \ldots, x_n \psi_1(t, x_1, \ldots, x_n)\}$$
$$B = \{t \in R \mid R \models \exists x_1, \ldots, x_n \psi_2(t, x_1, \ldots, x_n)\}.$$

Fix a surjection $C : \mathbb{N} \mapsto R^n$. An algorithm for testing whether a given $x \in S$ lies in A is given as follows: evaluate the truth of

$$\psi_1(t, C(0)), \psi_2(t, C(0)), \psi_1(t, C(1)), \psi_2(t, C(1)), \psi_1(t, C(2)), \psi_2(t, C(2)), \ldots$$

in R until 'true' comes out. If $R \models \psi_1(t, C(n))$ for some n, then $t \in A$. If $R \models \psi_2(t, C(n))$ for some n, then $t \in B$ and thus $t \notin A$. Since one of the two must occur eventually, this algorithm always terminates. □

4.6.4 Proposition. *The theory of $\mathbb{Q}$ is not model complete.*

Proof. Suppose that the theory of $\mathbb{Q}$ were model complete, i.e. all first-order formulas were equivalent to an existential formula. Let U be the polynomial from Theorem 2.4.1. Then there is no algorithm which, on receiving as input a $t \in \mathbb{Z}$, can decide on whether t is a member of the set

$$\Omega = \{t \in \mathbb{Z} \mid \exists x_1, \ldots, x_n \in \mathbb{Z} : U(t, x_1, \ldots, x_n) = 0\}.$$

Now Ω (and hence $\mathbb{Z} \setminus \Omega$) is definable in $\mathbb{Z}$. As we know that $\mathbb{Z}$ is definable in $\mathbb{Q}$, both Ω and $\mathbb{Z} \setminus \Omega$ are definable in $\mathbb{Q}$. If $\mathbb{Q}$ were model complete, then Ω and $\mathbb{Z} \setminus \Omega$ would be existential in $\mathbb{Q}$. But by the lemma (with $R = \mathbb{Q}$, $S = \mathbb{Z}$, $A = \Omega$ and $B = \mathbb{Z} \setminus \Omega$) this would imply the existence of an algorithm which checks membership of Ω, contradicting Theorem 2.4.1. □

4.6.5 Proposition. *There exist $\mathbb{Q}', \mathbb{Q}'' \in \mathrm{Mod}(\mathrm{Th}(\mathbb{Q}))$ and a definable subset A of $\mathbb{Q}$ such that $\mathbb{Q}'$ is a subfield of $\mathbb{Q}''$, but $A' \not\subseteq A''$, where A' and A'' are the respective transfers of A.*

Proof. Combine the previous proposition with Proposition 2.5.1. □

Inleiding

In 1900 formuleerde David Hilbert het volgende probleem, vandaag bekend als Hilbert's tiende probleem (Duits origineel: [Hil00]).

> Gegeven een diophantische vergelijking met een willekeurig aantal onbekenden en met gehele rationale coëfficiënten: geef een proces dat na een eindig aantal bewerkingen beslist of de vergelijking een oplossing met gehele rationale getallen heeft.

Vermoedelijk vroeg Hilbert om een beslissingsalgoritme met een polynoom $f \in \mathbb{Z}[X_1, X_2, \ldots]$ als invoer en als uitvoer 1 wanneer het polynoom een nulpunt heeft over $\mathbb{Z}$ en anders uitvoer 0, hoewel zijn formulering in principe toelaat dat dit algoritme afhangt van f, bijvoorbeeld van het aantal variabelen of de totale graad van f. In 1970 toonde Yuri Matiyasevich - voortbouwend op werk van Martin Davis, Hilary Putnam en Julia Robinson - aan dat zo een algoritme niet kan bestaan, zelfs niet wanneer men de graad en het aantal variabelen van f vasthoudt. [Mat70]

We kunnen deze vraagstelling naar een commutatieve ring R veralgemenen.

Vraag (Hilbert's tiende probleem voor R)**.** *Bestaat er een beslissingsalgoritme dat als invoer een polynoom $f \in \mathbb{Z}[X_1, X_2, \ldots]$ heeft en als uitvoer* 1 *indien het polynoom een nulpunt in $R^{\mathbb{N}}$ heeft en* 0 *indien niet?*

Om dit soort problemen aan te pakken, spelen definieerbare verzamelingen dikwijls een belangrijke rol. Gegeven een ring R en een deelverzameling S, kunnen we ons afvragen of er een eerste-orde formule in de taal van de ringen bestaat zodanig dat de elementen van S precies die elementen van R zijn die aan deze formule voldoen. Met een eerste-orde formule bedoelen we een zinvolle eindige opeenvolging van de logische symbolen $\forall, \exists, \neg, \wedge, \vee, (,), =, \leftrightarrow, \rightarrow$, variabelesymbolen $t, x_1, x_2, x_3, \ldots$ en de algebraïsche symbolen $+, -, \cdot, 0, 1$ met hun gebruikelijke interpretatie. De elementen van $\mathbb{R}$ die in $[0, \sqrt{2}]$ liggen, worden bijvoorbeeld gegeven als de verzameling van alle $t \in \mathbb{R}$ waarvoor de volgende formule geldt:

$$\exists x_1, x_2 (t = x_1 \cdot x_1 \wedge (1 + 1) - (t \cdot t) = x_2 \cdot x_2).$$

Men zegt dat de verzameling $[0, \sqrt{2}]$ *definieerbaar* is in $\mathbb{R}$ en dat de bovenstaande formule $[0, \sqrt{2}]$ in $\mathbb{R}$ *definieert*.

We kunnen ook vragen naar een definitie van S in R met een zo laag mogelijke logische complexiteit. Formules zonder de kwantoren $\forall$ and $\exists$ zullen doorgaans geen interessante verzamelingen definiëren (vb. als R een domein is, kunnen enkel eindige en co-eindige verzamelingen een kwantorvrije definitie hebben). Het op een na eenvoudigste is een *existentiële* of *universele* formule; dit is een formule die begint

met een aantal existentiële (respectievelijk universele) kwantoren, gevolgd door een kwantorvrije formule. De gegeven definitie van $[0, \sqrt{2}]$ is existentieel. Tot slot wordt een deelklasse van de existentiële formules gegeven door de *diophantische* formules; dit zijn formules van het type

$$\exists x_1, \ldots, x_n (f(t, x_1, \ldots, x_n) = 0)$$

voor zekere $n \in \mathbb{N}$ en een polynoom $f \in \mathbb{Z}[T, X_1, \ldots, X_n]$.

Indien een deelring van een ring een definitie heeft in de grotere ring, kan deze definitie een verband tussen de complexiteit van de eerste-orde theorieën van deze ringen blootleggen. Zo kan een antwoord op Hilbert 10 voor de deelring een antwoord voor de grotere ring impliceren, of omgekeerd. In paragraaf 2.4 zullen we dieper ingaan op de relatie tussen beslisbaarheid en definieerbaarheid. Definieerbare verzamelingen werden al vaak gebruikt in modeltheorie, maar mede vanwege de verbanden met beslisbaarheid is men gaan zoeken naar diophantische definities van deelringen en heeft men de onoplosbaarheid van Hilbert's tiende probleem voor vele ringen kunnen aantonen. We vermelden $\mathbb{R}(t)$, $\mathbb{C}(t_1, t_2)$ en $\mathbb{C}[t]$ en verwijzen naar [Koe14, Chapter 5] voor een overzicht van Hilbert's tiende probleem voor ringen.

Andere definieerbaarheidsresultaten bleken moeilijker te vinden. De vraag of $\mathbb{Z}$ een diophantische definitie in $\mathbb{Q}$ heeft, is bijvoorbeeld al geruime tijd open. Er bestaat voor zover we weten geen standaardmethode om diophantische definieerbaarheid na te gaan, en een antwoord op deze vraag lijkt dan ook nog ver buiten bereik. Omdat er aftelbaar veel polynomen over $\mathbb{Q}$ en overaftelbaar veel deelverzamelingen van $\mathbb{Q}$ zijn, ziet men direct dat de 'meeste' deelverzamelingen van $\mathbb{Q}$ niet diophantisch zullen zijn (zelfs niet definieerbaar, om dezelfde reden), hoewel het niet triviaal is om een concreet voorbeeld van een niet-diophantische deelverzameling van $\mathbb{Q}$ te geven. Op het einde van paragraaf 4.6 zullen we hier kort op terugkomen.

Desalniettemin zijn er recentelijk enkele verrassende diophantische definities in $\mathbb{Q}$ gevonden. Het doel van deze thesis is hier enkele van te bespreken; dit doen we in hoofdstukken drie en vier, nadat we de nodige voorkennis hebben opgebouwd in de eerste twee hoofdstukken. De meeste van onze resultaten zullen ook gelden in algemene getallenlichamen (eindige uitbreidingen van $\mathbb{Q}$) en zelfs algemener in zogenaamde globale lichamen.

Een goed begrip van centrale enkelvoudige algebra's over lokale en globale lichamen zal essentieel blijken. Een lokaal lichaam is een lichaam waarop een absolute waarde gedefinieerd kan worden zodanig dat de geïnduceerde topologie lokaal compact is. Voorbeelden van zulke lichamen zijn de reële, complexe en p-adische getallen. Globale lichamen zijn een klasse van lichamen waarover centrale simpele algebra's begrepen kunnen worden via een zekere collectie lokale uitbreidingen. Voorbeelden van globale lichamen zijn getallenlichamen. Het gedrag van centrale enkelvoudige algebra's over lokale lichamen is gemakkelijker te beschrijven dan over globale lichamen, wat lokale lichamen zo nuttig maakt bij het afleiden van definieerbaarheidsresultaten. In het eerste hoofdstuk zullen we de benodigde eigenschappen van lokale en globale lichamen overlopen. We onderstellen dat de lezer vertrouwd is met de basisconcepten van algebraïsche getaltheorie, valuatietheorie, topologie en centrale enkelvoudige algebra's. De bewijzen van enkele van de meer technische of diepe resultaten laten we weg.

In het tweede hoofdstuk bespreken we diophantische en definieerbare verzamelingen meer in detail. Zo leggen we uit waarom - tenminste in getallenlichamen en getallenringen - projecties van verzamelingen van de vorm

$$\bigcup_{i\in I}\bigcap_{j\in J} U_{i,j}$$

met I en J eindig en elke $U_{i,j}$ ofwel een nulverzameling ofwel het complement van een nulverzameling, diophantisch zijn. Dit toont dat de klasse van diophantische verzamelingen groter is dan men misschien aanvankelijk verwachtte. We lichten ook het samenspel tussen definieerbaarheid en modeltheorie toe.

Het derde hoofdstuk behandelt een techniek die bedacht werd door Bjorn Poonen en verfijnd door Philip Dittmann. [Poo09] [Dit18] Als A een centrale enkelvoudige algebra is over een lichaam K, beschouwen we de verzameling

$$S(A) = \{\mathrm{Trd}(x) \mid x \in A, \mathrm{Nrd}(x) = 1\}$$

waar Trd en Nrd het gereduceerde spoor en de gereduceerde norm zijn. We tonen dat deze verzameling een diophantische definitie heeft die enkel van een collectie structuurconstanten van A afhangt. We tonen ook dat $S(A)$ aan een lokaal-globaal principe voldoet, hetgeen ons een krachtig middel geeft om deelverzamelingen van globale lichamen te definiëren. Bijvoorbeeld, stel dat A een centrale enkelvoudige algebra over $\mathbb{Q}$ is die splitst over $\mathbb{R}$. Schrijf Δ voor de verzameling van priemgetallen p waarvoor A niet splitst over de p-adische getallen $\mathbb{Q}_p$. Het blijkt dat

$$S(A) + S(A) = \bigcap_{p\in\Delta} \mathbb{Z}_{(p)}.$$

De linkerkant is de verzameling van sommen van twee elementen uit $S(A)$, $\mathbb{Z}_{(p)}$ is de verzameling rationale getallen met noemer niet deelbaar door p. Aangezien de verzameling links diophantisch is met structuurconstanten van A als parameters, kunnen we hiermee vele semilokale deelringen van $\mathbb{Q}$ definiëren. Dit geeft dan aanleiding tot een eerste-orde formule die de getallenring in elk getallenlichaam definieert. In het bijzonder zal deze formule $\mathbb{Z}$ in $\mathbb{Q}$ definiëren, maar niet diophantisch.

In het laatste hoofdstuk tonen we dat $\mathbb{Q} \setminus \mathbb{Z}$ diophantisch is in $\mathbb{Q}$, of anders gezegd, dat $\mathbb{Z}$ een universele definitie heeft in $\mathbb{Q}$. Daarna tonen we algemener dat in een globaal lichaam K en voor een eindige verzameling van priemidealen S, de ring van S-gehele getallen universeel is. In het bijzonder is de getallenring in een getallenlichaam dus universeel. Deze resultaten zijn recent bewezen door Jochen Koenigsmann voor $\mathbb{Q}$ [Koe16], Jennifer Park voor getallenlichamen [Par13] en Kirsten Eisenträger en Travis Morrison voor globale lichamen van oneven karakteristiek [EM18], maar wij zullen een nieuwe aanpak volgen. Net als deze auteurs gebruiken we een truc om te tonen dat het Jacobsonradicaal van enkele semilocale deelringen van het globale lichaam diophantisch is, maar dan combineren we deze deelverzamelingen op een andere manier om de ring van S-gehele getallen te bekomen. Onze aanpak heeft een aantal voordelen. We geven een eenvoudiger bewijs dat voorgaande resultaten verenigt en enkel steunt op de classificatie van quaternionenalgebra's over globale lichamen. De gevonden definities hebben beduidend minder kwantoren dan die in de bestaande literatuur. Tot slot werkt onze aanpak - na enkele aanpassingen - ook voor globale lichamen van karakteristiek 2, een geval dat niet eerder behandeld werd.

Bibliography

[Dit18] Philip Dittmann. „Irreducibility of polynomials over number fields is diophantine". In: *Composito Mathematica.* (2018). `https://arxiv.org/abs/1601.07829`. Forthcoming.

[EM18] Kirsten Eisenträger and Travis Morrison. „Universally and existentially definable subsets of global fields". In: *Math. Res. Lett.* (2018). `https://arxiv.org/abs/1609.09787`. Forthcoming.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued Fields.* Springer, 2005.

[Hil00] David Hilbert. „Mathematische Probleme." In: *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse* 3 (1900), pp. 253–297.

[Hil02] David Hilbert. „Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900". In: *Bull. Amer. Math. Soc.* 8 (1902), pp. 437–479.

[Koe14] Jochen Koenigsmann. „Undecidability in number theory". In: *Lecture Notes in Mathematics.* 2111 (2014).

[Koe16] Jochen Koenigsmann. „Defining $\mathbb{Z}$ in $\mathbb{Q}$". In: *Annals of Mathematics.* 183 (2016), pp. 73–93.

[Mat70] Yuri V. Matiyasevich. „Diofantovost' perechislimykh mnozhestv [Enumerable sets are Diophantine]". In: *Proc. Dokl. AN SSSR* 191 (1970), pp. 279–282.

[NSW15] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields, Sec. Ed., corr.sec. print.* Springer, 2015.

[OMe00] Timothy O'Meara. *Introduction to Quadratic Forms.* Springer, 2000.

[Par13] Jennifer Park. „A universal first-order formula defining the ring of integers in a number field". In: *Math. Res. Lett.* 20 nr. 5 (2013), pp. 961–980.

[PD11] Alexander Prestel and Charles N. Delzell. *Mathematical Logic and Model Theory.* Springer, 2011.

[Pie82] Richard S. Pierce. *Associative Algebras.* Springer, 1982.

[Poo09] Bjorn Poonen. „Characterizing integers among rational numbers with a universal-existential formula". In: *Amer. J. Math.* 131 (2009), pp. 675–682.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian Forms.* Springer, 1985.

[Sie21] Carl Ludwig Siegel. „Darstellung total positiver Zahlen durch Quadrate". In: *Math. Z.* 11 (1921), pp. 246–275.

[Tat67] John Torrence Tate. „Global Class Field Theory". In: *Algebraic Number Theory*. Thompson Book Company Inc, 1967.