universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

"The Hasse-Minkowski Theorem for global fields"

verfasst von / submitted by

Giancarlo Castellano, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2017 / Vienna, 2017

Studienkennzahl lt. Studienblatt: / degree programme code as it appears on the student record sheet:	A 066 821
Studienrichtung lt. Studienblatt: / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Leonhard Summerer

"... is a bacterial complex, one of the universe's greatest mathematicians, yet immediately ***lethal*** *to the majority of life-forms it encounters."*
Neil Gaiman, J H Williams III, Dave Stewart, *The Sandman: Overture*, issue 6

„Es ist in der Regel ein Fehler, beim Kennenlernen zu erzählen, dass man MathematikerIn ist, weil das meist negative Reaktionen hervorruft. Besser ist es zu sagen, man ist Künstler. Das reicht meist, und wenn das Gegenüber nachfragt, welche Art Kunst man betreibt, sollte man antworten: Abstrakte Kunst. Dann hinterlässt man einen positiven Eindruck, und man hat nicht gelogen, denn Mathematik ist unbestreitbar die abstrakteste Form von Kunst.“
Hermann Schichl

"All art is quite useless."
Oscar Wilde, *Preface* to *The Picture of Dorian Grey*

Abstract

The main goal of this thesis is to present the proof of the Hasse-Minkowski Theorem, a celebrated result in number theory which allows one to fully classify quadratic forms over so-called global fields, in particular over algebraic number fields. The concepts and results relevant to the proof, both from valuation theory and the theory of quadratic forms, are discussed in detail and in a virtually self-contained fashion, with particular emphasis on fundamental invariants of quadratic spaces; the results are then specialized to local fields, and one is finally in a position to prove that quadratic spaces over global fields are completely characterized by their "local behaviour", which is essentially the content of the Hasse-Minkowski Theorem.

Zusammenfassung

Das Hauptziel der vorliegenden Arbeit ist es, den Beweis des Satzes von Hasse-Minkowski zu präsentieren: Dabei handelt es sich um ein berühmtes Resultat aus der Zahlentheorie, das es einem ermöglicht, quadratische Formen über sogenannten globalen Körpern, also insbesondere über algebraischen Zahlkörpern, vollständig zu klassifizieren. Die zum Beweis relevanten Begriffe und Resultate, sowohl aus der Bewertungstheorie als auch aus der Theorie der quadratischen Formen, werden ausführlich behandelt mit speziellem Augenmerk auf fundamentalen Invarianten quadratischer Räume; es wird dabei meist kein spezielles Vorwissen seitens des Lesers vorausgesetzt. Die besprochenen Theoreme werden anschließend auf lokale Körper angewandt; dies ermöglicht zu zeigen, dass quadratische Räume über globalen Körpern vollständig durch ihr "lokales Verhalten" charakterisiert sind, was ja im Wesentlichen dem Inhalt des Satzes von Hasse-Minkowski entspricht.

Contents

Acknowledgements

As anyone who has some experience with writing will likely confirm, no thesis, paper or book can ever be completed without the infinite patience and continued support of one's superiors, colleagues and loved ones. This is where I get a chance to express my gratitude.

The first person I would like to thank is my advisor Leo Summerer: I thank him for being there every step of the way, not only to give useful advice whenever a problem arose, but also to make valuable suggestions and bring new ideas to the table, while never failing to listen to and respect my opinions. In such stressful times as the past few months, his patience and willingness to help have meant a lot to me, and I consider myself lucky to have had him as my advisor.

I also owe a big *grazie* to Herwig Hauser, thanks to whom I have had many more opportunities as a bachelor's and master's student than most could hope to have; *grazie* for many fruitful conversations, and especially *grazie* for the financial support received while writing this thesis.

Further, I would like to extend my gratitude to those who, beside Leo, generously shared their knowledge with me and helped me see the "greater picture" in which to contextualize the Hasse-Minkowski Theorem: Prof. Joachim Schwermer, who I feel honoured to have had a chance to learn from, and Harald Grobner, who I look forward to learning more from in the future.

A special thank-you goes to Hermann Schichl for his many words of advice, encouragement and appreciation throughout the years, and most recently for allowing me to use a quote of him in the epigraph to this thesis.

Thanks also to my colleagues Hana Kováčová, Paola Lopez, Christopher Chiu and Stefan Perlega for their willingness to help whenever I was in doubt, be it mathematical or "philosophical" in nature, and for the insightful conversations we shared.

This is as good a point as any to thank (and apologize to) anyone who has had to put up with my stressed-out self over the past few months, especially my dear friend Salvo who has heroically done so on a daily basis.

Finally, the biggest and most heartfelt "thanks" goes out to my family, especially my mother, father, brother and sister-in-law. If it hadn't been for your foresight, planning, sacrifices and unlimited support, I wouldn't be here writing this to begin with, and I'm

at a loss for words to properly express how thankful I am to each of you. But I fear that, even if I were somehow able to find the right words, this thesis would, as Pierre Fermat would put it, be too short to contain them all.

Introduction

In 1899, Kurt Hensel wrote a paper called *„Über eine neue Begründung der Theorie der algebraischen Zahlen“*, or, *“On a new foundation of the theory of algebraic numbers”*, whose incipit is as follows:

Die Analogie zwischen den Resultaten der Theorie der algebraischen Functionen einer Variabeln und der der algebraischen Zahlen hat mir schon seit mehreren Jahren den Gedanken nahe gelegt, die Zerlegung der algebraischen Zahlen mit Hülfe der idealen Primfactoren durch eine einfachere Behandlungsweise zu ersetzen, welche der Entwickelung der algebraischen Functionen in Potenzreihen für die Umgebung einer beliebigen Stelle völlig entspricht.

The analogy between the results of the theory of algebraic functions of one variable and of algebraic numbers has struck me for several years, and could suggest replacing the decomposition of algebraic numbers into ideal prime factors with a simpler way of treatment, which is completely equivalent to the expansion of algebraic functions into power series in the neighbourhood of a point.

The analogy described by Hensel, which in modern terms may be described as the (formal) analogy between algebraic number fields and function fields, led to the introduction of *local fields* as well as *global fields*, the latter being a collective term for algebraic number fields and fields of rational functions over finite fields. In a 1945 paper, Emil Artin and George Whaples provided an axiomatization of global fields and showed how classical results of algebraic number theory can be recovered directly from the axioms, making the machinery involved in the traditional proofs *“unnecessary for class field theory”*. In the spirit of this paper, Artin's student O. T. O'Meara wrote a book named *Introduction to Quadratic Forms* which contains the classical results from the theory of quadratic forms over algebraic number fields (or their rings of integers), proved now for general global fields (or their rings of integers) via the unified approach of Artin and Whaples' paper. Among the results proved in O'Meara's book is the celebrated Hasse-Minkowski Theorem, a powerful local-global principle which settles the questions of isotropy, representability and isometry for arbitrary regular (finite-dimensional) quadratic spaces over K, where K is classically $\mathbb{Q}$ or an algebraic number field.

The goal of this thesis is to give a more or less self-contained proof of the Hasse-Minkowski Theorem over general global fields (of characteristic $\neq 2$), mostly following O'Meara's book. The addendum "more or less" is explained by the vastness of the subject together with the desire to not wander too far afield, which has meant that some results have been given without proofs and some arguments have only been sketched. The results whose proofs were omitted are for the most part classification results (e.g., the classification theorem for archimedean local fields, or Wedderburn's Theorem on central simple algebras over fields), and the arguments which were only sketched are as a general rule technical in nature.

The outline of the thesis is as follows. Chapter I is devoted to so-called "valuation theory", or more precisely to the theory of absolute values on fields. While there are many, sometimes widely different ways to approach the subject, we have opted to put emphasis on places, rather than absolute values, right from the start. Accordingly, it seemed most natural, albeit perhaps less intuitive, to introduce valued fields as special topological fields whose topology is induced by a metric with additional properties (§1), while an alternative definition which does not rely on metrics is also mentioned. Starting in §2, we specialize to non-archimedean places, which exhibit a direct connection to some types of rings we discuss in §3. Our digression in ring theory naturally leads us to results about Dedekind domains (§4) and thus yields the most important examples of non-archimedean places. Finally we introduce the two classes of valued fields which are relevant to this thesis: on the one hand, we review complete metric spaces (§5) in order to properly cover the theory of local fields in §6 and §7; on the other hand, global fields and the main results about them are dealt with in sections §8 and §9.

In Chapter II, the basic concepts and results from the theory of quadratic forms are presented. First, the theory of symmetric bilinear forms is introduced in great generality in §1; this is needed in §2 to define quadratic forms. §2 also deals with questions of representability, while §3 is devoted to introducing the concept of isometries and proving Witt's fundamental results on quadratic spaces over fields. Finally, in §4 the ground field is assumed to be a local field and a few results are proved in this special case, including the classification of quadratic spaces over $\mathbb{R}$ and $\mathbb{C}$.

Chapter III introduces the use of algebras in the theory of quadratic forms: after a very general introduction of central simple algebras and the Brauer group in §1, quaternion algebras are discussed in detail in §2, and finally linked to (binary) quadratic spaces in §3. It is then possible to define the Hasse invariant (§4) and illustrate its importance already over general fields. The last two sections conclude the study of quadratic forms over local fields: by the previous sections, it is essential to first investigate quaternion algebras over local fields, which is done in §5, and then one quickly derives a classification result for the non-archimedean case (§6).

Finally, Chapter IV is devoted to the formulation and proof of the Hasse-Minkowski Theorem. The statement is given in the preamble, which also features a historical digression explaining the various conventions for naming both the theorem and related results. In §1, we present the classical proof in the special case $K = \mathbb{Q}$; then in §2 we analyze the argument and outline how to adjust it for global fields. §3 follows Artin and Whaples' unified approach in deriving Dirichlet's Unit Theorem for global fields, a result essential to the proof of the Global Square Theorem in §4. Some estimates from these sections are then refined in order to prove a special case of the Hasse Norm Theorem (§5) which is key to the proof of the Hasse-Minkowski Theorem, presented in full generality in §6. To conclude the thesis, we conclude the classification of quadratic spaces over global fields and spend a few words on related results and attempts at generalization.

Throughout this thesis, we shall resort to a handful of common abbreviations, namely: "TFAE" for "the following are equivalent", "w.r.t." for "with respect to" and "iff" in place of "if and only if". We use the standard notations $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ for the sets (equipped each time with the appropriate algebraic structure) of natural numbers (including 0), integers, rationals, reals and complex numbers respectively. Unless explicitly stated, under a "ring" we always understand a commutative ring with unity, and a "field" shall always mean a commutative field, while non-commutative fields are called "skew fields". If R is a ring, then $R^\times$ denotes the set of units, i.e. elements which possess a multiplicative inverse; thus, if $R = K$ is a field, then $K^\times = K \setminus \{0\}$. The set $R^\times$, or $K^\times$, is usually considered with the additional structure of a multiplicative group. Finally, we use $\subseteq$ as a general symbol for inclusion (not necessarily strict); if we *require* an inclusion to be strict, then we shall use $\subsetneq$, while $\subset$ will sometimes be used for inclusions which are evidently strict, i.e. $\mathbb{Q} \subset \mathbb{R}$.

I. Valuation theory

In this chapter we explore some aspects of valuation theory, which provides the appropriate framework for studying the fields of number theory.

§1. Valued fields

In this section we shall introduce valued fields, which are the main object of study of valuation theory. Informally, a valued field is a field K equipped with a metric $d : K \times K \to \mathbb{R}_{\geq 0}$ which is compatible with the field operations in the following sense:
(C1) $d(x+z, y+z) = d(x,y)$ for all $x, y, z \in K$;
(C2) $d(xz, yz) = d(z,0) \cdot d(x,y)$ for all $x, y, z \in K$.
A more rigorous definition requires a bit of preparation. First, recall that given a metric d on a space X, the open balls of the form $B_r(x) := \{y \in X : d(x,y) < r\}$ for $x \in X$ and $r \in \mathbb{R}_{>0}$ form the basis for a topology, the *topology induced by d*. A topology v on a field K is called a *place* of K if it is induced by a metric d which satisfies (C1)-(C2). Finally, a *valued field* is a pair (K, v) where K is a field and v is a place of K.

Example. (1) Let $K = \mathbb{R}$, v be the standard Euclidean topology. Then (K, v) is a valued field.

(2) If (K, v) is a valued field and F is a subfield of K, then F equipped with the subspace topology is again a valued field. In particular, $\mathbb{Q}$ has a "Euclidean place" as a subfield of $\mathbb{R}$, see (1).

(3) Let $K = \mathbb{Q}$, $p \in \mathbb{Z}_{\geq 0}$ a prime number. There is precisely one topology v_p on $\mathbb{Q}$ in which the sets $\{x + p^n\mathbb{Z} : n \in \mathbb{Z}\}$ form a neighbourhood basis for each point $x \in \mathbb{Q}$; it is called the *p-adic topology* on $\mathbb{Q}$ (see also §4). One routinely checks that v_p is a place of $\mathbb{Q}$. Thus, there are infinitely many distinct (!) places on $\mathbb{Q}$.

(4) Let K be any field, v be the *discrete topology* on K, i.e. the one where every subset is open. Then v is a place of K, the so-called *trivial place*, as it is induced by the metric:

$$d(x,y) = \begin{cases} 1 & \text{if } x \neq y; \\ 0 & \text{if } x = y \end{cases}$$

which evidently satisfies (C1)-(C2). ◇

It is often advantageous to describe valued fields via absolute values, whose definition encodes properties (C1)-(C2) in a natural way. Recall that an *absolute value* on a field K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that:

(i) for $x \in K, |x| = 0$ if and only if $x = 0$; *(positive-definiteness)*

(ii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$; *(triangle inequality)*

(iii) $|xy| = |x| \cdot |y|$ for all $x, y \in K$. *(multiplicativity)*

Since the absolute values $|\cdot|$ on K and the metrics d on K which satisfy (C1)-(C2) are in 1-1 correspondence via $d(x, y) := |x - y|$ and $|x| := d(x, 0)$, respectively, we can say that an absolute value *induces* a topology v if the corresponding metric induces v, and in this case v is a place of K by definition.

EXAMPLE. (5) The map which sends $x \in \mathbb{R}$ to its modulus $|x| := \max\{x, -x\}$ is clearly an absolute value on $\mathbb{R}$; it induces the Euclidean topology from (1).

(6) Let $K = \mathbb{Q}$, $p \in \mathbb{Z}_{\geq 0}$ a prime. Define $|\cdot|_p$ as follows: for $x = p^k a/b$, where a and b are nonzero integers coprime to p and k is in $\mathbb{Z}$, set $|x|_p := p^{-k}$. Clearly $|\cdot|_p$ is an absolute value on $\mathbb{Q}$ which induces the p-adic topology on $\mathbb{Q}$, see (3).

(7) Let F be a finite field, $|\cdot|$ an absolute value on F. Then $\left|F^\times\right| := \{|x| : x \in F^\times\}$ is a finite multiplicative subgroup of $\mathbb{R}_{>0}$. But then necessarily $\left|F^\times\right| = \{1\}$, and the place $|\cdot|$ induces is the trivial place of F, see (4).

(8) Consider the field $K = F(t)$ of rational functions in one variable t over a field F, and define $|\cdot|$ as follows: if $0 \neq r(t) \in F(t)$, $r(t) = f(t)/g(t)$ for polynomials f, g over F, set $|r| := 2^{\deg f - \deg g}$. It is an easy exercise to show that $|\cdot|$ yields an absolute value on K; we denote the place of K it induces by $v_{\deg}$. $\diamond$

To wrap up this section, we wish to mention that it is possible to redefine valued fields so as to eliminate the dependency on a concrete metric (or absolute value) on the field. First, a valued field (K, v) is easily shown[1] to be a *topological field*, i.e., the maps

(i) $K \times K \to K$, $\quad (x, y) \mapsto x + y$,

(ii) $K \to K$, $\quad x \mapsto -x$,

(iii) $K \times K \to K$, $\quad (x, y) \mapsto x \cdot y$,

(iv) $K^\times \to K^\times$, $\quad x \mapsto x^{-1}$

are continuous in the topology v.[2] Given a topological field (K, v), let

$$\mathfrak{m} = \mathfrak{m}(v) := \{x \in K : x^n \to 0 \text{ for } n \to \infty\};$$
$$\mathfrak{u} = \mathfrak{u}(v) := \{x \in K^\times : x \notin \mathfrak{m} \text{ and } x^{-1} \notin \mathfrak{m}\};$$
$$\mathfrak{o} = \mathfrak{o}(v) := \mathfrak{m} \cup \mathfrak{u}.$$

[1] Once one picks an absolute value $|\cdot|$ which induces v, the proofs of (i)-(iv) mirror the standard proofs of the same statements over the reals; for instance, to prove (iii) we pick convergent sequences $(x_n), (y_n)$ in K with limits $x, y \in K$ respectively and show that $(x_n y_n)$ converges to xy by verifying that $|x_n y_n - xy| = \left|x_n(y_n - y) + y(x_n - x)\right| \leq \sup\{|x_n| : n \in \mathbb{N}\} \cdot |y_n - y| + |y| \cdot |x_n - x| \xrightarrow{n \to \infty} 0$.

[2] Of course $K \times K$ and $K^\times$ are endowed with the product and subspace topology respectively.

We can now use conditions on these subsets to characterize valued fields amongst all topological fields.

Proposition I.§1. *A topological field (K, v) is a valued field if and only if*

(i) $\mathfrak{m}$ *is open in the topology* v*;*

(ii) $\mathfrak{o}$ *is* bounded*, i.e., for each neighbourhood* U *of* 0 *there exists a neighbourhood* W *of* 0 *such that* $\mathfrak{o} \cdot W \subseteq U$ *(which means:* $xy \in U$ *whenever* $x \in \mathfrak{o}$ *and* $y \in W$*).*

Proof. We only prove necessity; the proof of sufficiency can be found in [Rib99], 1.7.

Let (K, v) be a valued field, d be a metric which induces v and satisfies (C1)-(C2). An element $x \in K$ is in $\mathfrak{m}(v)$ if and only if $d(x^n, 0) = d(x, 0)^n \to 0$ in $\mathbb{R}$, hence $\mathfrak{m}$ is precisely the open unit ball $B_1(0)$ around zero. It follows that $\mathfrak{o}(v) = \{x \in K : d(x, 0) \leq 1\}$ is the closed unit ball.

Now, condition (i) is obviously met; as for (ii), any neighbourhood U of 0 necessarily contains some open ball $B_r(0)$, $r > 0$ and one can put $W := B_r(0)$, for if $x \in \mathfrak{o}$ and $y \in W$, then $d(xy, 0) = d(x, 0) \cdot d(y, 0) < 1 \cdot r = r$, hence $xy \in W \subseteq U$. □

§2. The Archimedean property

In this section we continue our investigation of places of a field. As the title suggests, our focus shall be on the so-called *Archimedean property*, which for an absolute value $|\cdot|$ on a field K reads:

$$\text{for all } x, y \in K \text{ with } 0 < |x| \leq |y| \text{ there exists an } n \in \mathbb{N} \text{ such that } |nx| > |y|\,, \quad (\dagger)$$

where nx denotes the n-fold sum $x+...+x$. While being a cornerstone of real analysis, this property does not hold over general valued fields. In fact, we now proceed to characterize the valued fields where it is violated.

Proposition I.§2. *Let (K, v) be a valued field, $|\cdot|$ an absolute value on K which induces v. The following are equivalent:*

(i) $|\cdot|$ *satisfies the* strong triangle inequality*, i.e.*

$$|x + y| \leq \max\{|x|, |y|\} \text{ for all } x, y \in K;$$

(i') $d : K \times K \to \mathbb{R}_{\geq 0}, (x, y) \mapsto |x - y|$ *is an* ultrametric*, i.e.,*

$$d(x, z) \leq \max\{d(x, y), d(y, z)\} \text{ for all } x, y, z \in K;$$

(ii) $\mathfrak{o} = \mathfrak{o}(v)$ *is a ring;*

(iii) If $x \in K$ *lies in* $\mathfrak{o}$*, then so does* $1 + x$*;*

(iv) $2 = 1 + 1 \in \mathfrak{o}$*;*

(v) $n \in \mathfrak{o}$ *for all* $n \in \mathbb{Z}$*.*

(v') $|\cdot|$ *does* not *satisfy the Archimedean property.*

Proof. The equivalence of (i) and (i') is clear, whereas the implications (ii)⇒(iii)⇒ (iv) both follow from $1 \in \mathfrak{o}$. Using the equality $\mathfrak{o} = \{x \in K : |x| \leq 1\}$ from §1, the implication (i)⇒(ii) also becomes trivial. We now show (iv)⇒(v)⇔(v') and (v)⇒(i).

(iv)⇒(v): Let $n \in \mathbb{Z}$; we show $|n| \leq 1$. Since $|n| = |-n|$, we can suppose $n \geq 1$. Now, the binary expansion of n tells us that n can be written as a sum of terms of the form $a_i 2^i$, which by assumption all have absolute value ≤ 1. Since there are at most $s+1$ such terms, where $s = s(n) := \lfloor \log_2 n \rfloor$, we obtain $|n| \leq s + 1$ by the triangle inequality. For every $k \geq 1$ we have $\left|n^k\right| \leq s(n^k) + 1 \leq k\left(s(n) + 1\right)$, hence $|n| \leq \liminf \sqrt[k]{k(s+1)} = 1$.

(v)⇔(v'): If $|\cdot|$ satisfies (†), then by substituting $x = y = 1$ we obtain that there exists an $n \in \mathbb{N}$ with $|n| = |n1| > 1$. Conversely, if there exists an m with $|m| > 1$, then for given x, y with $0 < |x| \leq |y|$ one can find k with $\left|m^k\right| = |m|^k > \left|y/x\right|$.

(v)⇒(i): Let $x, y \in K$, $m \geq 0$. By the binomial theorem, $(x + y)^m$ equals a $\mathbb{Z}$-linear combination of terms $x^k y^{m-k}$ where $0 \leq k \leq m$. Clearly $\left|x^k y^{m-k}\right| \leq \max\{|x|, |y|\}^m$, so by the triangle inequality, together with the assumption, it follows that $|x + y| \leq \sqrt[m]{m+1} \max\{|x|, |y|\}$, whence the claim. □

Remark. Let $K, v, |\cdot|$ as in the statement of Prop. I.§2.

(1) If $\mathfrak{o}(v) = \{x : |x| \leq 1\}$ is a ring, then one directly computes that $\mathfrak{m}(v) = \{x : |x| < 1\}$ is an ideal of $\mathfrak{o}(v)$. In particular, $x \sim y :\Leftrightarrow x - y \in \mathfrak{m}$ is an equivalence relation (on K !), so we can write $\mathfrak{m} = K \setminus \bigcup_{y \notin \mathfrak{m}} (y + \mathfrak{m})$. By Prop. I.§1, $\mathfrak{m}$ is open; thus, the union of translates of $\mathfrak{m}$ is again open and hence $\mathfrak{m}$ is also closed in (K, v).

(2) Let F be a subfield of K. Then $|\cdot|$ satisfies the strong triangle inequality if and only if its restriction to F does. In particular, if F is finite, we see with the help of Ex. §1.(7) that all places of K must satisfy the equivalent conditions from Prop. I.§2.

(3) Recall that for any field K we have a ring homomorphism $\kappa : \mathbb{Z} \to K$ determined by $1 \mapsto 1$; the unique non-negative integer n with $\ker \kappa = n\mathbb{Z}$ is called the *characteristic* of K and denoted $\chi(K)$. If $\chi(K) > 0$, one readily checks that $\chi(K)$ must be a prime p, so the image of $\mathbb{Z}$ in K is a copy of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus, (2) tells us that if K has a place v which does *not* satisfy the equivalent conditions of Prop. I.§2, then $\chi(K) = 0$ and K contains a copy of $\mathbb{Q}$, namely the field of fractions of $\kappa(\mathbb{Z})$. ⋄

A non-trivial[3] place v is called *non-archimedean*, or sometimes *ultrametric*, if it satisfies the equivalent properties from Prop. I.§2, otherwise it is called *archimedean*. An absolute value is (non-)archimedean if the place it induces is.

[3]Technically, the trivial place also satisfies (i)-(v'), but we choose not to include it because most results only apply to non-trivial places.

EXAMPLE. (1) Consider the absolute value $|\cdot|$ on $K = F(t)$ that we introduced in Ex. §1.(8). For all constant polynomials $c \in F$, we have $|c| = 2^0 = 1$; in particular, condition (v) from the above theorem is met and the place induced by $|\cdot|$ is non-archimedean. The ring $\mathfrak{o}(v)$ contains precisely those $r(t) = f(t)/g(t)$ with $\deg f(t) \leq \deg g(t)$ or $f(t) = 0$.

(2) For every prime integer p, the absolute value $|\cdot|_p$ on $\mathbb{Q}$ from Ex. §1.(6) satisfies the strong triangle inequality; in fact, we shall see in §4 that every non-archimedean place of $\mathbb{Q}$ is induced by some $|\cdot|_p$. On the other hand, the Euclidean place of $\mathbb{Q}$ can be shown to be the *unique* archimedean place of $\mathbb{Q}$. Combining these facts one obtains a complete classification of the non-trivial places of $\mathbb{Q}$, known as **Ostrowski's theorem**. $\diamond$

§3. Valuation rings

In the last section, we have seen that there is a subring of K associated to every non-archimedean place v of K, namely $\mathfrak{o}(v)$. This motivates us to digress into the realm of ring theory, from which we shall ultimately gain much insight into valuation theory.

First, we observe that if A is an integral domain with field of fractions K, then the quotient group $\Gamma = K^\times/A^\times$ can be equipped with a partial ordering[4] $\leq$ as follows:

$$\alpha \leq \beta \text{ iff } Ax \supseteq Ay, \text{ where } \alpha = xA^\times, \beta = yA^\times \in \Gamma.$$

It is easy to verify that Γ together with $\leq$ is a *partially ordered group*, i.e., if $\alpha, \beta, \gamma \in \Gamma$ with $\alpha \leq \beta$, then $\gamma\alpha \leq \gamma\beta$ and $\alpha\gamma \leq \beta\gamma$. We call A a *valuation ring* if $\leq$ is a total ordering on Γ, i.e. if for any two $\alpha, \beta \in \Gamma$ either $\alpha \leq \beta$ or $\beta \leq \alpha$ (or both) holds. The map $\nu = \nu_A : K^\times \to \Gamma$, $x \mapsto xA^\times$ is then called the *Krull valuation* associated to A; it is easy to check that $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ when $x, y, x + y \in K^\times$.

REMARK. An element $z \neq 0$ of a domain A is a non-unit iff $zA^\times > 1A^\times$ in Γ. If A is a valuation ring, the above inequality $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ implies that the non-units of A form an ideal $A \setminus A^\times =: \mathfrak{m}(A)$; in other words, A is a *local* ring. In particular, $\mathfrak{m}(A)$ is the unique maximal[5] ideal of A. By elementary algebra, the quotient ring $A/\mathfrak{m}(A)$ is a field, called the *residue field* of A. $\diamond$

EXAMPLE. (1) Let $|\cdot|$ be a non-archimedean absolute value on a field K, v the place it induces. Since $\mathfrak{o}(v) = \{x \in K : |x| \leq 1\}$, we see that for each $x \in K^\times$ at least one of x and x^{-1} lies in $\mathfrak{o}$; it easily follows that $\mathfrak{o}$ is a valuation ring with field of fractions K. Its unique maximal ideal is precisely $\mathfrak{m}(v)$ and its residue field $\mathfrak{o}/\mathfrak{m}$ is denoted $k(v)$.

[4] The verification that $\leq$ is well-defined and indeed a partial ordering is left to the reader.

[5] Recall that a proper ideal I in a ring R is called *maximal* if it is not strictly contained in any other proper ideal of R.

(2) Let F be a field, $A = F[[t]]$ be the domain of formal power series in one variable t over F. Since $a(t) \in A$ is invertible if and only if its constant term is, the field of fractions of A is precisely $F((t)) := \{a(t)/t^n : a(t) \in F[[t]], n \geq 0\}$, the field of *Laurent series* in t over F, and A is a valuation ring since $\Gamma = \{t^n A^\times : n \in \mathbb{Z}\}$ is totally ordered. $\diamond$

If A is a valuation ring, then the sets $\widetilde{B}_s(x) = \{x\} \cup \{y \in K : \nu(x-y) > s\}$ where $x \in K$, $s \in \Gamma$ form a basis for a topology v on K. If Γ can be identified with an additive (!) subgroup of the reals, then $|x| := C^{-\nu(x)}$ is an absolute value which induces v for any $C > 1$. The inequality $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ translates into the strong triangle inequality for $|\cdot|$, therefore v is non-archimedean.

It can be shown that Γ is isomorphic to a subgroup of the reals if and only if A is a valuation ring of *Krull dimension one*, which in turn amounts to saying that an ideal of A is maximal if and only if it is prime and nonzero[6]. For the remainder of this section, however, our focus shall be on a different condition which plays an important role in many areas of algebra and reads as follows: a ring R is called *Noetherian* if every non-empty set of ideals of R has (at least) one maximal element with respect to inclusion. We shall now see what this condition implies for valuation rings.

Theorem I.§3. *Let A be a domain, $K \supsetneq A$ its field of fractions, $\Gamma = K^\times/A^\times$. TFAE:*

(i) A is a Noetherian ring and a valuation ring;

(ii) A is a Noetherian local ring whose unique maximal ideal $\mathfrak{m}(A)$ is principal;

(iii) A has a uniformizer*, i.e. a non-unit π such that every $0 \neq x \in K$ can be written as $x = u\pi^n$ for a unit $u \in A^\times$ and some $n \in \mathbb{Z}$;*

(iv) There is an order-preserving group isomorphism $\varphi : \mathbb{Z} \to \Gamma = K^\times/A^\times$.

Proof. (i)⇒(ii): We have already shown in the above remark that A is local. To see that $\mathfrak{m}(A) = A \setminus A^\times$ is a principal ideal, let $\{x_j : j \in J\}$ be a set of generators of $\mathfrak{m}(A)$. Since A is Noetherian, there is an x_k such that Ax_k is maximal among the Ax_j's. By the valuation ring property, $Ax_k \supseteq Ax_j$ for all j, which readily implies $\mathfrak{m}(A) = Ax_k$.

(ii)⇒(iii): Let π be a generator of $\mathfrak{m}(A)$; since A is not a field, $\pi \neq 0$. We show that for any $0 \neq a \in A$ there is a largest $n \geq 0$ such that $a \in A\pi^n$. For if this holds, then $a = u\pi^n$ for $u \notin A\pi$, i.e. $u \in A^\times$, and (iii) is proved.
Suppose $a \in A\pi^n$ for all $n \geq 0$, i.e. for each $n \geq 0$ there exists x_n such that $a = x_n\pi^n$. It follows that $x_n = \pi x_{n+1}$ for all n, so we obtain an ascending chain of ideals $Ax_1 \subseteq Ax_2 \subseteq ....$ Since A is Noetherian, this chain has a maximal element, i.e., there exists an x_m such that Ax_m contains all the other Ax_n; but then in particular $x_{m+1} = tx_m$ for some $t \in A$ and thus $(1-\pi t)x_{m+1} = 0$. Since π is not a unit, $1 - \pi t$ is nonzero, hence $x_{m+1} = 0$ and $a = \pi_{m+1}x_{m+1} = 0$.

[6]Recall that a proper ideal I of a ring R is called *prime* if the set-theoretic complement $R \setminus I$ of I in R is closed under multiplication.

(iii)⇒(iv): By assumption, for every $x \in K^\times$ we have $xA^\times = \pi^n A^\times$ for some n, hence $\varphi : \mathbb{Z} \to \Gamma$, $n \mapsto \pi^n A^\times$ has the desired properties.

(iv)⇒(i): Since Γ is isomorphic to $\mathbb{Z}$, it is totally ordered, so A is a valuation ring. To show that A is Noetherian, consider a non-empty set of ideals I of A. For each I, we define $n(I) := \min\{\varphi^{-1}(xA^\times) : 0 \neq x \in I\}$; clearly, two ideals I, J of A satisfy $I \subseteq J$ if and only if $n(I) \geq n(J)$. The claim now follows from the well-known fact that every non-empty subset of $\mathbb{N}$ has a minimal element. □

A domain A which satisfies the equivalent properties from Thm. I.§3 is called a *discrete valuation ring* (*DVR*); the map $\nu_A : K^\times \to \Gamma$, viewed as a $\mathbb{Z}$-valued map, is then called the *normalized valuation* of A. The proof of Thm. I.§3 shows that an element $\pi \in A$ is a uniformizer iff it generates the maximal ideal, which is the case iff $\nu_A(\pi) = 1$.

Note that a DVR can equivalently be defined as a local PID (= *principal ideal domain*) which is not a field. Indeed, the condition that A be a local PID is clearly necessary for (i) (see the proof of the implication (i)⇒(ii)) and sufficient for (ii).

Finally, a (non-archimedean) place v on a field K is called *discrete* if $\mathfrak{o}(v)$ is a DVR. It is not hard to verify that if $|\cdot|$ is an absolute value which induces a discrete place v, then $\left|K^\times\right| = \{|x| : x \in K^\times\}$ is a discrete (multiplicative) subgroup of $\mathbb{R}_{>0}$.

§4. Dedekind domains

In this section we conclude our excursion into ring theory by investigating Dedekind domains, which we will use to construct many examples of discrete places on fields. Recall that a domain A is called *Dedekind* if it is Noetherian of Krull dimension one (see §3) as well as *integrally closed*, i.e. if an element x in the field of fractions K of A satisfies a polynomial relation of the form

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0 \qquad (\ddagger)$$

for some coefficients $a_i \in A$, then x already lies in A. If a principal ideal domain is not a field, then it is easily shown to be Dedekind; in particular, DVRs are local Dedekind domains (one may also check this directly).

Conversely, we shall now show that if A is a local Dedekind domain with unique maximal ideal $\mathfrak{m} = \mathfrak{m}(A)$, then there is an $x \in K$ such that $\mathfrak{m} \cdot x = A$; this immediately implies that $\mathfrak{m} = Ax^{-1}$ is principal, which by Thm. I.§3.(ii) is enough to conclude that A is a DVR.

To construct such an x, we first pick $b \in A$ arbitrary. For $y \in A$, $y \notin Ab$, the set $\{z \in A : yz \in Ab\}$ is a proper ideal of A, denoted by $(Ab : Ay)$. Since A is Noetherian, there is an $a \in A$, $a \notin Ab$ such that $(Ab : Aa)$ is maximal among all $(Ab : Ay)$ with

$y \in A, y \notin Ab$. Set $x = a/b$. By definition, $(Ab : Aa) \cdot x \subseteq A$; we claim that $(Ab : Aa) = \mathfrak{m}$. Since A has Krull dimension one and $(Ab : Aa)$ is clearly nonzero, it suffices to show that $(Ab : Aa)$ is prime; this is a routine check of the definition.

It remains to show that equality holds in the inclusion $\mathfrak{m} \cdot x \subseteq A$. We argue by contradiction: suppose $\mathfrak{m} \cdot x \subsetneq A$, i.e. $\mathfrak{m} \cdot x \subseteq \mathfrak{m}$. By assumption[7] there is a finite system of generators $z_1, ..., z_n$ for $\mathfrak{m}$, so for all i we can write $z_i x = \sum_j a_{ij} z_j$ for $a_{ij} \in A$. Consider the $n \times n$-matrix whose i, j-entry is given by $-a_{ij}$ for $i \neq j$ and $x - a_{ii}$ otherwise; by construction, the column vector $(z_1, ..., z_n)^T$ lies in its kernel, so its determinant vanishes. But its determinant is a polynomial in x as in (‡) and A is integrally closed, so $x \in A$, contradicting $a \notin Ab$.

The main result concerning Dedekind domains in the context of valuation theory is the following:

Theorem I.§4. *Let A be a Dedekind domain, K its field of fractions. Then the (A-)*finite *places of K, i.e. the non-archimedean places v with $A \subseteq \mathfrak{o}(v)$, are all discrete and are in bijection with the nonzero prime ideals $\mathfrak{p}$ of A.*

Before setting out to prove the theorem, we present the following lemma.

Lemma I.§4. *Two places v, v' on a field K coincide if $\mathfrak{m}(v) = \mathfrak{m}(v')$.*

Proof. Let $|\cdot|, |\cdot|'$ be absolute values which induce v, v' respectively. Pick $0 \neq z \in \mathfrak{m}(v) = \mathfrak{m}(v')$ and choose $\rho > 0$ so that $|z|' = |z|^\rho$. If there were an x with $|x|' \neq |x|^\rho$, then we could find a rational number m/n with $n > 0$ such that $(|z|')^{m/n}$ lies between $|x|'$ and $|x|^\rho$, i.e. such that 1 lies between $\left|x^n/z^m\right|'$ and $\left|x^n/z^m\right|^\rho$, contradicting the assumption $\mathfrak{m}(v) = \mathfrak{m}(v')$. Thus, $|x|' = |x|^\rho$ for all $x \in K$ and $|\cdot|, |\cdot|'$ induce the same place of K. □

Proof of the theorem. Let us first suppose that A is local. Then A has precisely one nonzero prime ideal $\mathfrak{m}(A)$ and is a DVR by our earlier remarks. In §3 we saw that the normalized valuation $\nu_A : K^\times \to \mathbb{Z}$ induces a place v' on K with $\mathfrak{m}(A) = \mathfrak{m}(v')$. We shall now show that, if v is a finite place of K, then $\mathfrak{m}(v) = \mathfrak{m}(A)$; we will then be done by Lemma I.§4. *A priori* it holds that $\mathfrak{m}(A) = A \cap \mathfrak{m}(v)$, so it suffices to show $A = \mathfrak{o}(v)$. Suppose there is an $x \in \mathfrak{o}(v)$ such that $x \notin A$. Then, since A is a DVR, $x^{-1} \in A$, so $x = a/b$ with $a \in A \setminus \mathfrak{m}(A)$, $b \in A$. But b cannot be in $A^\times$, otherwise we would have $x \in A$; therefore, $b \in \mathfrak{m}(A)$. But then $a = bx \in \mathfrak{m}(A) \cdot \mathfrak{o}(v) \subseteq \mathfrak{m}(v)$, a contradiction.

Let us return to the general case. For finite v, $\mathfrak{p}_v = \mathfrak{m}(v) \cap A$ is a nonzero prime ideal of A. Conversely, for given $\mathfrak{p}$ consider the domain $A_\mathfrak{p} := \{x = r/s \in K : r, s \in A, s \notin \mathfrak{p}\}$, the *localization* of A at $\mathfrak{p}$. Its ideals are of the form $IA_\mathfrak{p} = \{rx : r \in I, x \in A_\mathfrak{p}\}$ for

[7] It is a well-known fact that a ring is Noetherian if and only if all its ideals are finitely generated.

$I \subseteq \mathfrak{p}$, and $IA_\mathfrak{p}$ is prime if and only if I is; in particular, $A_\mathfrak{p}$ is again Noetherian of Krull dimension one and local with unique maximal ideal $\mathfrak{p}A_\mathfrak{p}$. We now set out to show that $A_\mathfrak{p}$ is also integrally closed. For let $x \in K$ such that there exist $a_i \in A_\mathfrak{p}$ with $x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$. Multiplying this equation by d^n, where d is a common denominator of the a_i's, we obtain a similar polynomial relation for dx with coefficients in A; since A is integrally closed, $dx \in A$, whence $x \in A_\mathfrak{p}$.

We have thus shown that $A_\mathfrak{p}$ is a local Dedekind domain for every $\mathfrak{p}$. By the special case we proved above, there is a unique place $v_\mathfrak{p}$ with $A_\mathfrak{p} \subseteq \mathfrak{o}(v_\mathfrak{p})$; it is a discrete place. Precisely because of the uniqueness of $v_\mathfrak{p}$, we have $v = v_{\mathfrak{p}_v}$ for every v. Conversely, it is clear that $\mathfrak{p} = \mathfrak{p}A_\mathfrak{p} \cap A = \mathfrak{m}(v_\mathfrak{p}) \cap A = \mathfrak{p}_{v_\mathfrak{p}}$ for all $\mathfrak{p}$. In summary, the "maps" $v \mapsto \mathfrak{p}_v$ and $\mathfrak{p} \mapsto v_\mathfrak{p}$ are inverse to each other and the theorem is proved. □

EXAMPLE. (1) By Prop. I.§2.(v), every non-archimedean place v on $\mathbb{Q}$ already satisfies $\mathbb{Z} \subseteq \mathfrak{o}(v)$; since the nonzero prime ideals of $\mathbb{Z}$ are precisely those of the form $p\mathbb{Z}$ for p prime, Thm. I.§4 tells us that the non-archimedean places of $\mathbb{Q}$ are precisely the p-adic places, see Ex. §1.(3).

(2) Let $A = F[t]$ for a field F, $K = F(t)$. We have the following analogue of prime numbers: a polynomial $p(t) \in F[t]$ is called *irreducible* if it cannot be written non-trivially as a product of smaller-degree polynomials. Since A is a PID and in particular Dedekind, it follows similarly to (1) that the finite places of K are in bijection with the irreducible monic polynomials over F.

(3) Let K be an algebraic number field, i.e. a finite extension of the rational field $\mathbb{Q}$. It is a well-known fact that K is the field of fractions of a Dedekind domain $\mathcal{O}_K \supset \mathbb{Z}$, the so-called *ring of integers* of K, see also §§8-9. The exact relationship between the (finite) places of K and those of $\mathbb{Q}$ will be studied in detail in the next sections. ◇

§5. Completeness

Now that we have made ourselves acquainted with several examples of valued fields, we return to the general theory from a more topological viewpoint. We start by reviewing some facts about metric spaces; a more detailed treatment can be found in the literature.

First of all, recall that a sequence (x_n) in a metric space $X = (X, d)$ is called *Cauchy* (with respect to the metric d) if $d(x_n, x_m) \xrightarrow{n,m\to\infty} 0$. We shall denote the set of these sequences by $\mathcal{CS}(X, d)$.

Consider the map $\widetilde{d}\big((x_n), (y_n)\big) := \lim_{n\to\infty} d(x_n, y_n)$ on $\mathcal{CS}(X, d)$; it is not a metric

in general.[8] We can, however, define an equivalence relation $\sim$ on $\mathcal{CS}(X,d)$ via:

$$(x_n) \sim (y_n) \text{ if and only if } \widetilde{d}\big((x_n),(y_n)\big) = 0$$

and form the quotient space $\widehat{X} = \mathcal{CS}(X,d)/\!\sim$. Now the map $\widehat{d}$ given by $\widehat{d}([x_n],[y_n]) := \widetilde{d}\big((x_n),(y_n)\big)$, where $[x_n]$ denotes the equivalence class of (x_n), is well-defined and yields an honest metric on $\widehat{X}$.

Clearly there is an injection $\iota : X \hookrightarrow \widehat{X}$ sending each element $x \in X$ to the equivalence class of the constant sequence $(x)_n$, i.e. to the set of Cauchy sequences in X which converge to x. This injection is often denoted as an inclusion $X \subseteq \widehat{X}$. If equality holds, i.e., if every Cauchy sequence in X converges to some element in X, the space X is called *complete* (with respect to the metric d).

For any space X, the space $\widehat{X}$ constructed above can be shown to satisfy the following:

(i) $\widehat{X}$ is complete with respect to $\widehat{d}$.

(ii) X is *(everywhere) dense* in $\widehat{X}$, i.e., the closure of X in $\widehat{X}$ is all of $\widehat{X}$.

(iii) The restriction of $\widehat{d}$ to X is precisely d.

These properties characterize the pair $(\widehat{X},\widehat{d})$ up to a certain precise notion of isomorphism; one can thus call $\widehat{X}$ *the completion* of X with respect to d.

Example. (1) The real field $\mathbb{R}$ is a complete metric space w.r.t. the Euclidean metric. Indeed, $\mathbb{R}$ is commonly introduced axiomatically as the unique ordered field which satisfies the least upper-bound property, and this property is equivalent to completeness.

(2) The rational field $\mathbb{Q}$ is *not* complete w.r.t. the Euclidean metric; for instance, one can construct a sequence of rational numbers which converges to $\sqrt{2}$ in the larger field $\mathbb{R}$, but $\sqrt{2} \notin \mathbb{Q}$. One easily verifies that the completion of $\mathbb{Q}$ is precisely $\mathbb{R}$.[9] $\diamond$

In the next proposition, we specialize the above notions and results to valued fields.

Proposition I.§5. *Let (K,v) be a valued field. Then:*

(i) if $|\cdot|$, $|\cdot|'$ are two absolute values which induce v, and d, d' are the corresponding metrics, then the completions of K w.r.t. d and d' yield the same space $\widehat{K}$;

(ii) $\widehat{K}$ is again a field;

(iii) v extends uniquely to a place $\widehat{v}$ of $\widehat{K}$.

Proof. (i) By the proof of Lemma I.§4, there exists a $\rho > 0$ such that $|x|' = |x|^\rho$ for all $x \in K$, i.e. $d'(x,y) = d(x,y)^\rho$ for all x, y. Therefore, $\mathcal{CS}(K,d) = \mathcal{CS}(K,d')$; moreover, $\lim\limits_{n\to\infty} d(x_n,y_n) = 0$ if and only if $\lim\limits_{n\to\infty} d'(x_n,y_n) = 0$, and the claim is proved.

[8] The reader may recognize $\widetilde{d}$ as a *pseudometric*.

[9] However, the above construction of $\widehat{X}$ from $\mathcal{CS}(X,d)$ already uses the completeness of the reals, so it is logically inadmissible to *define* $\mathbb{R}$ as $\widehat{\mathbb{Q}}$.

(ii) Since K is a field, the set of Cauchy sequences $\mathcal{CS}$ can be made into a ring with component-wise addition and multiplication. Forming the quotient space with respect to $\sim$ (see above) amounts to factoring out the ideal $\mathfrak{n} := \{(x_n) \in \mathcal{CS} : x_n \xrightarrow{n\to\infty} 0\}$. It remains to show that for $(x_n) \notin \mathfrak{n}$ there exists $(a_n) \in \mathcal{CS}$ with $(a_n)\cdot(x_n) \in 1+\mathfrak{n}$; this is achieved by setting $a_n := 1/x_n$ for $x_n \neq 0$ and $a_n := 1$ otherwise.

(iii) If d is a metric as in (i), then $\widehat{d}([x_n],[y_n]) = \lim d(x_n, y_n)$ again satisfies (C1)-(C2) by continuity of the field operations, so it induces a place $\widehat{v}$ on $\widehat{K}$. If d' is another metric on $\widehat{K}$ whose restriction $d'|_K$ satisfies (C1)-(C2) and induces v, then (cf. (i)) there exists a ρ such that $d'(x,y) = d(x,y)^\rho$ for all $x, y \in K$; passing to the limit, we get $d'([x_n],[y_n]) = \widehat{d}([x_n],[y_n])^\rho$ for all $[x_n],[y_n] \in \widehat{K}$, thus d' induces $\widehat{v}$ as well. □

By Prop. I.§5.(i), it makes sense to speak of the completion of a field K *at a place* v, which is again a valued field and indeed an *extension* of (K, v), see also §7.

We will regularly denote $\widehat{K}$, $\widehat{v}$, $\mathfrak{o}(\widehat{v})$, $\mathfrak{m}(\widehat{v})$, $\mathfrak{u}(\widehat{v})$, $k(\widehat{v}) = \mathfrak{o}(\widehat{v})/\mathfrak{m}(\widehat{v})$ as K_v, v, $\mathfrak{o}_v$, $\mathfrak{m}_v$, $\mathfrak{u}_v$, k_v respectively. If v is of the form $v_\mathfrak{p}$ (see §4), then it is customary to write $K_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{p}\mathfrak{o}_\mathfrak{p}$, $\mathfrak{u}_\mathfrak{p}$, $k_\mathfrak{p}$; if $K = \mathbb{Q}$, the common notations are $\mathbb{Q}_p$, $\mathbb{Z}_p$, $p\mathbb{Z}_p$, $\mathbb{Z}_p^\times$ and $\mathbb{F}_p$ respectively, where p is the (positive) prime integer with $\mathfrak{p} = p\mathbb{Z}$. The elements of $K_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}$, $\mathfrak{u}_\mathfrak{p}$ are commonly referred to as $\mathfrak{p}$-*adic* (or p-*adic* if $K = \mathbb{Q}$) *numbers*, *integers* and *units* respectively.

§6. Local fields

In this section we introduce the first of two classes of fields which are of special interest in number theory. To that end, we are going to use the concept of compactness: a metric space is *(sequentially) compact* if and only if, given a sequence (x_n) in X, there exist a point $x \in X$ and a subsequence (x_{n_k}) with $x_{n_k} \xrightarrow{k\to\infty} x$.

Example. (1) By the Heine-Borel theorem, a subspace of $\mathbb{R}^n$ or $\mathbb{C}^n$, $n \geq 1$, is compact if and only if it is closed and bounded.

(2) The following properties are well-known: a closed subset of a compact space is again compact; the continuous image of a compact set is again compact; products[10] of compact spaces are again compact. ◇

Let K be a field, v be a nontrivial place of K. Then (K, v) is called a *local field* if $\mathfrak{o} = \mathfrak{o}(v)$ is compact. Since multiplication is continuous (cf. §1), this is the case if and only if $z\mathfrak{o} = \{x \in K : |x| \leq |z|\}$ is compact for some (and hence every) $z \in K^\times$.

We mention a few immediate consequences. Let (x_n) be a sequence in the local field (K, v) and suppose the absolute values of the x_n's do not grow arbitrarily large. Since v is nontrivial, $\left|K^\times\right| = \{|x| : x \in K^\times\}$ is unbounded, so there is a z such that $x_n \in z\mathfrak{o}$ for

[10] The proof is straightforward for finite products; the general case is a theorem of Tychonoff.

all n. But then (x_n) has a convergent subsequence by compactness of $z\mathfrak{o}$. In particular, if (x_n) is Cauchy, then it readily follows that (x_n) itself converges to a point of $z\mathfrak{o}$; in other words, (K, v) is a complete valued field in the sense of §5.

One can show (see e.g. [O'M73] or [Rib99]) that any complete archimedean valued field is isomorphic in a suitable sense to either $\mathbb{R}$ or $\mathbb{C}$ with the Euclidean topology. Since $\mathfrak{o}$ is obviously compact in both fields, we obtain a classification of archimedean local fields.

Now let (K, v) be a non-archimedean local field. By Rmk. §2.(1), $\mathfrak{m} = \mathfrak{m}(v)$ is a closed subset of $\mathfrak{o}$ and hence compact. Thus[11], if $|\cdot|$ is any absolute value which induces v, it attains a maximum $\gamma < 1$ on $\mathfrak{m}$. It is not hard to check that any $\pi \in K$ with $|\pi| = \gamma$ is a uniformizer of $\mathfrak{o}$, i.e., v is a discrete place of K.

Next, consider the residue field $k(v) := \mathfrak{o}/\mathfrak{m}$ of $\mathfrak{o}$. If we endow $k(v)$ with the quotient topology, we see that it is both compact and *discrete* in that every point is an open subset (cf. Ex. §1.(4)). But then $k(v)$ can only have finitely many elements.

The following result completes the characterization of non-archimedean local fields:

Proposition I.§6. *Let (K, v) be a complete non-archimedean field.*

(i) Suppose that there exist a finite set $\mathcal{R} \subset \mathfrak{o}(v)$ and an element $\rho \in \mathfrak{m}(v)$ so that every $a \in \mathfrak{o}(v)$ can be written uniquely as an infinite sum $\sum_{i=0}^{\infty} a_i \rho^i$ where $a_i \in \mathcal{R}$ for all i. Then (K, v) is a local field.

(ii) If v is a discrete place and $k(v)$ is a finite field, then (K, v) is local.

Proof. (i) Let (x_n) be a sequence in $\mathfrak{o}$, $x_n = \sum_{i=0}^{\infty} a_{in}\rho^i$ for $a_{in} \in \mathcal{R} = \{r_1, ..., r_q\}$.

We construct a sequence (c_i) in $\mathcal{R}$ inductively so that the set $S_k := \{n : a_{in} = c_i \ \forall i \leq k\}$ is infinite for all $k \geq 0$. Given $c_0, ..., c_{k-1}$, partition S_{k-1} into subsets $S_{k-1,j} := \{n \in S_{k-1} : a_{kn} = r_j\}$, where $j = 1, ..., q$. By the pigeonhole principle, one of these, say S_{k-1,j_0}, must be infinite; set $c_k = r_{j_0}$. We claim that the infinite sum $\sum_i c_i\rho^i$ converges to a point $x \in \mathfrak{o}$; it is then a straightforward task to extract a subsequence of (x_n) which converges to x, and we are through.

To prove the claim, it remains to show that the sequence $(s_k)_{k\geq 0}$, where $s_k = c_0 + c_1\rho + ... + c_k\rho^k$, is Cauchy. If $|\cdot|$ is any absolute value which induces v, then by the strong triangle inequality we obtain

$$|s_n - s_m| = \left|c_{m+1}\rho^{m+1} + ... + c_n\rho^n\right| \leq \max_{m<i\leq n} |c_i||\rho|^i \leq \max_{m<i\leq n} |\rho|^i = |\rho|^{m+1}$$

whenever $n \geq m$, and the right-hand side becomes arbitrarily small for $n, m \to \infty$.

(ii) Let $\mathcal{R}$ be a set of representatives of $\mathfrak{o}(v)$ modulo $\mathfrak{m}(v)$, $0 \in \mathcal{R}$, and let $\rho = \pi$ be

[11] Here we use the fact that $|\cdot|$ is continuous (indeed, the triangle inequality implies $\big||x| - |y|\big| \leq |x - y|$ for all $x, y \in K$) and that continuous real-valued maps on a compact space attain a maximum.

a uniformizer of $\mathfrak{o}(v)$. We show that the assumption of (i) is verified. Indeed, let $a \in \mathfrak{o}$; we have to prove existence and uniqueness of the a_i's. As for existence, we define the a_i's inductively so that, for all $n \geq 0$, $d_{n-1} = a - \sum_{i=0}^{n-1} a_i \pi^i$ is a multiple of π^n: given $a_0, ..., a_{n-1}$, we take a_n to be the unique element of $\mathcal{R}$ with $a_n - d_{n-1}/\pi^n \in \mathfrak{m}$. By construction, $d_n \to 0$, whence $\sum_{i=0}^{n} a_i \pi^i \to a$.

As for uniqueness, suppose that $0 = \sum_i a_i \pi^i$ where $a_i \neq 0$ for some i. If n is the smallest such i, then $-a_n = \sum_{i=n+1}^{\infty} a_i \pi^{i-n}$, therefore $a_n \in \mathfrak{m}$. But the only element in $\mathcal{R} \cap \mathfrak{m}$ is 0, contradicting the assumption $a_n \neq 0$. □

Corollary I.§6. *Let A be a Dedekind domain, K its field of fractions, $\mathfrak{p}$ a nonzero prime ideal of A. If $\#A/\mathfrak{p} = q < \infty$, then $(K_\mathfrak{p}, v_\mathfrak{p})$ is a local field and $\#k_\mathfrak{p} = q$.*

Proof. Since A has Krull dimension one, $\mathfrak{p} \subset A$ is maximal, thus $A/\mathfrak{p}$ is a field. On the other hand, the residue field $k(v_\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ (see the proof of Thm. I.§4) is the field of fractions of $A/\mathfrak{p}$ by elementary algebra. Thus, we obtain $k(v_\mathfrak{p}) = A/\mathfrak{p}$. Now since $\mathfrak{o}(v_\mathfrak{p}) \subseteq \mathfrak{o}_\mathfrak{p}$, $\mathfrak{m}(v_\mathfrak{p}) = \mathfrak{o}(v_\mathfrak{p}) \cap \mathfrak{p}\mathfrak{o}_\mathfrak{p}$, we have $k(v_\mathfrak{p}) \subseteq k_\mathfrak{p}$. To see that equality holds, note that if $a \in \mathfrak{o}_\mathfrak{p}$, then there exists an $a' \in \mathfrak{o}(v_\mathfrak{p})$ with $a - a' \in \mathfrak{m}_\mathfrak{p}$. Indeed, by the properties of the completion there exists a sequence (x_n) in K with $x_n \to a$ for $n \to \infty$; by getting rid of at most finitely many terms, we obtain $x_n - a \in \mathfrak{m}_\mathfrak{p}$ for all n. But then, by Prop. I.§2, we have $x_n \in \mathfrak{o}_\mathfrak{p}$ and hence $x_n \in \mathfrak{o}(v_\mathfrak{p})$ for all n; thus, a' can be taken to be any x_n.

To prove that $(K_\mathfrak{p}, v_\mathfrak{p})$ is local, we show that the assumption of Prop. I.§6.(i) holds. So let $a \in \mathfrak{o}_\mathfrak{p}$. By the above argument, there exists a sequence (x_n) in $\mathfrak{o}(v_\mathfrak{p})$ which converges to a. Further let π be a uniformizer of $\mathfrak{o}(v_\mathfrak{p})$ and let $\mathcal{R}$ be a set of representatives of $\mathfrak{o}(v_\mathfrak{p})$ modulo $\mathfrak{m}(v_\mathfrak{p})$ with $0 \in \mathcal{R}$; we have $\#\mathcal{R} = q$. Arguing similarly as in Prop. I.§6.(ii), we obtain a unique representation $x_n = \sum_{i=0}^{\infty} a_{in} \pi^i$, $a_{in} \in \mathcal{R}$ for each n. Since (x_n) is Cauchy, for each i there must exist an N_i with $a_{in} - a_{i,N_i} \in \mathfrak{m}$, i.e. $a_{in} = a_{i,N_i}$, for all $n \geq N_i$. Then $a - \sum_{i=0}^{k} a_{i,N_i} \pi^i \to 0$ for $k \to \infty$, whence $a = \sum_{i=0}^{\infty} a_{i,N_i} \pi^i$. □

Example. (3) Let F be a finite field, $K = F((t))$, v the place of K induced by $A = F[[t]]$, see Ex. §3.(2). Then the assumptions of Prop. I.§6.(i) are trivially satisfied, so (K, v) is local.

(4) Let $p \in \mathbb{Z}_{\geq 0}$ be a prime. Then $(\mathbb{Q}_p, v_p)$ is local by Cor. I.§6.

(5) Let F be a finite field, $A = F[t]$, $K = F(t)$, $p(t) \in A$ an irreducible polynomial, $\mathfrak{p} = Ap(t)$. Then $\#A/\mathfrak{p} = (\#F)^{\deg p} < \infty$, so $(K_\mathfrak{p}, v_\mathfrak{p})$ is local again by Cor. I.§6. ◇

Remark. If (K, v) is a local field, then there is a canonical choice for an absolute value $|\cdot|$ on K which induces v. Indeed, in the archimedean case one picks $|x| = \max\{x, -x\}$ if $K = \mathbb{R}$ and $|x| := \sqrt{(\Re x)^2 + (\Im x)^2}$ if $K = \mathbb{C}$; if (K, v) is non-archimedean, then for $x \in K^\times$ one defines $|x| := q^{-\nu(x)}$, where $q = \#k(v)$ and ν is the normalized valuation of $\mathfrak{o}(v)$, cf. §3. In each case, $|\cdot|$ is called the *normalized* absolute value on (K, v). ◇

§7. Extensions of local fields

In this section we deal with extensions of valued fields, in particular local fields. First, recall that a *field extension* L/K is a pair of fields K, L with $K \subseteq L$. If a place v of K is the "restriction" of a place w of L as in Ex. §1.(2), we say that w *divides* v, in symbols $w|v$, and that (L, w) is an extension of (K, v).

EXAMPLE. (1) The completion (K_v, v) of a valued field (K, v) is an extension of (K, v).

(2) Let $A = F[t]$, $K = F(t)$ as in Ex. §4.(2). Then every A-finite place of K divides the trivial place on F. ◇

We now proceed to review some aspects of field theory which will allow us to formulate and prove the main result of this section. Recall that the *degree* of an extension L/K, denoted $[L : K]$, is the dimension of L as a vector space over K.

Suppose that $[L : K] = n < \infty$, and for $\alpha \in L$ consider the set $\{1, \alpha, \alpha^2, ...\} \subset L$. By assumption there must be a $d = d(\alpha) \leq n$ so that $1, ..., \alpha^{d-1}$ are linearly independent over K and $\alpha^d = \sum_{i=0}^{d-1} f_i \alpha^i$ for some $f_i \in K$. The polynomial $f(t) = f_{K,\alpha}(t) := t^d - \sum_{i=0}^{d-1} f_i t^i$ is then called the *minimal polynomial* of α over K, as every polynomial g over K with $g(\alpha) = 0$ necessarily has degree $\geq d$. In particular, $f(t)$ is irreducible in $K[t]$.

Now let $K(\alpha)$ denote the linear span of $\{1, ..., \alpha^{d-1}\}$. Then both $\mu_\alpha = \mu_\alpha^{L/K} : L \to L$, $x \mapsto \alpha x$ and its restriction $\bar{\mu}_\alpha : K(\alpha) \to K(\alpha)$ are K-linear maps. Consider the *characteristic polynomial* of $\bar{\mu}_\alpha$, defined as $c(t) = c_\alpha(t) = \det\left(t \cdot \mathrm{Id}_{K(\alpha)} - \bar{\mu}_\alpha\right)$. For $t \in K(\alpha)$ we have $t \cdot \mathrm{Id} - \bar{\mu}_\alpha = t\bar{\mu}_1 - \bar{\mu}_\alpha = \bar{\mu}_{t-\alpha}$, so $c(\alpha) = 0$. But then $c(t) - f(t)$ is a polynomial of degree $< d$ over K which vanishes in α, so necessarily $c(t) = f(t)$.

Finally, consider the characteristic polynomial $C(t) = C_{L/K;\alpha}(t) = \det(t \cdot \mathrm{Id}_L - \mu_\alpha)$ of μ_α. It is easily seen that $K(\alpha)$ is a subfield of L, so L has a basis $\beta_1, ..., \beta_r$ as a vector space over $K(\alpha)$. Then $\{\beta_1, \beta_1\alpha, ..., \beta_1\alpha^{d-1}, \beta_2, ..., \beta_r\alpha^{d-1}\}$ is a K-basis for L, so $n = dr$. The matrix representation of μ_α with respect to this basis is a block matrix, where every block represents $\bar{\mu}_\alpha$, so $C(t) = c(t)^r = f(t)^r$ for all t. The map $N_{L/K} : L \to K$, $\alpha \mapsto \det \mu_\alpha = (-1)^{[L:K]} C_{L/K;\alpha}(0)$ is called the *norm* of the extension L/K.

We are now ready to formulate the main theorem of this section.

Theorem I.§7. *Let (K, v) be a local field with normalized absolute value $|\cdot|$, L/K an extension, $[L : K] = n$. Then*

$$\alpha \mapsto |N_{L/K}(\alpha)|^{1/n}$$

defines an absolute value $\|\cdot\| : L \to \mathbb{R}_{\geq 0}$ on L. The place w it induces is the unique place of L with $w|v$, and (L, w) is again a local field.

Proof. We prove that $\|\cdot\|$ is an absolute value. If (K, v) is archimedean, then by §6 we can assume $K = \mathbb{R}$ or $K = \mathbb{C}$. By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically

closed; it follows that the only finite-degree extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$. Hence, either $L = K$, in which case $\|\cdot\| = |\cdot|$, or $K = \mathbb{R}$ and $L = \mathbb{C}$, in which case one directly computes $N_{L/K}(\alpha) = (\Re\alpha)^2 + (\Im\alpha)^2$, so $\|\cdot\|$ is the ordinary absolute value on $\mathbb{C}$.

Suppose now that (K, v) is non-archimedean. Clearly $\|\cdot\|$ is positive definite and multiplicative, so by Prop. I.§2.(iii) it suffices to show that $\|1 + \alpha\| \leq 1$ if $\|\alpha\| \leq 1$. So fix $\alpha \in L$ with $\|\alpha\| \leq 1$. Then, keeping the notations from above, we have that $\left|f(0)\right| \leq 1$, i.e. $f(0) \in \mathfrak{o}(v)$. Thus, $f \in K[t]$ is irreducible, monic and its constant term lies in $\mathfrak{o}(v)$. We claim that this is enough to show that *all* coefficients of f lie in $\mathfrak{o}(v)$; we shall prove this in III.§5 using **Hensel's Lemma** from II.§4. In particular, it follows that $f(-1) \in \mathfrak{o}(v)$, and we are done since $N_{L/K}(1 + \alpha) = (-1)^n C_{L/K;\alpha}(-1) = (-1)^n f(-1)^{n/d(\alpha)}$.

Now, a direct computation shows $\|x\| = |x|$ for all $x \in K$, hence $w|v$. As for the uniqueness of w, we now prove the following: if w is any topology on L which makes the maps

(i) $L \times L \to L, \quad (\alpha, \beta) \mapsto \alpha + \beta,$

(ii) $K \times L \to L, \quad (x, \alpha) \mapsto x\alpha.$

continuous, and $\varphi : K^n \to L$ is a K-linear isomorphism, then φ is a homoeomorphism between K^n with the product topology and (L, w).

First, φ is continuous: indeed, there exist $\alpha_1, ..., \alpha_n \in L$ so that $\varphi(x) = \sum_{i=1}^n x_i\alpha_i$ for all $x = (x_1, ..., x_n) \in K^n$, thus φ is obtained composing maps as in (i)-(ii). It remains to show that φ sends open sets to open sets. But every open set containing $0 \in K^n$ contains a set of the form $Q_r^n(0) = \{(x_1, ..., x_n) : |x_i| \leq r \ \forall i\}$ for some $r \in \left|K^\times\right|$, so it suffices to show that the image of every such set contains an open neighbourhood V of $0 \in L$.

Let $S = \{(x_1, ..., x_n) : \max_i |x_i| = 1\}$. One readily sees that S is closed; as a subset of the compact set $Q_1^n(0) = \mathfrak{o} \times ... \times \mathfrak{o}$, it is compact. It follows that $\varphi(S) \subset L$ is again compact, and since $0 \notin \varphi(S)$, by continuity of (ii) there exist an open neighbourhood U of $0 \in K$ and an $\varepsilon \in \left|K^\times\right|$ so that $yU \cap \varphi(S) = \emptyset$ whenever $|y| \leq \varepsilon$.

Now let $r \in \left|K^\times\right|$ and let $z \in K$ with $0 < |z| \leq r\varepsilon$. Then $V = zU \subseteq \varphi\left(Q_r^n(0)\right)$; for let $0 \neq \xi \in zU$, $\xi = \varphi(x_1, ..., x_n)$, and choose j so that $\left|x_j\right| = \max_i |x_i|$. Then $x_j^{-1}\xi$ lies in $\varphi(S)$ as well as in $x_j^{-1}zU$, so necessarily $|x_j^{-1}z| > \varepsilon$, whence $\xi \in \varphi\left(Q_r^n(0)\right)$.

Finally, we show that (K, v) is local. We have seen above that $0 \in L$ has a compact neighbourhood Q, e.g. $Q = \varphi\left(\mathfrak{o}(v) \times ... \times \mathfrak{o}(v)\right)$ where φ is a linear isomorphism $K^n \to L$. By the definition of a neighbourhood, one can find a $z \in L^\times$ so that the closed ball $z\mathfrak{o}(w) = \{\alpha \in L : \|\alpha\| \leq \|z\|\}$ is completely contained in Q. But $z\mathfrak{o}(w)$ is closed, hence compact, and Theorem I.§7 is proved. □

Let (K, v) be a non-archimedean local field, (L, w) an extension of (K, v) of finite degree n. Then, by Thm. I.§7 and the results of §6, $\mathfrak{o}(w)$ is a DVR and $k(w) = \mathfrak{o}(w)/\mathfrak{m}(w)$

is a finite field. Since $\mathfrak{o}(v) \subseteq \mathfrak{o}(w)$, $\mathfrak{m}(v) = \mathfrak{o}(v) \cap \mathfrak{m}(w)$, we have $k(v) \subseteq k(w)$. The positive integer $[k(w) : k(v)] = \log \#k(w) / \log \#k(v)$ is called the *ramification index* of L/K and denoted $f = f(w|v)$.

Next, let π denote a uniformizer of $\mathfrak{o}(w)$. The unique $e = e(w|v) \in \mathbb{Z}_{>0}$ such that π^e is a uniformizer of $\mathfrak{o}(v)$ is called the *inertia degree* of L/K. We have $ef = n$; in fact, if $\alpha_1, ..., \alpha_f \in \mathfrak{o}(w)$ are chosen so that the cosets of the α_j's in $k(w) = \mathfrak{o}(w)/\mathfrak{m}(w)$ form a basis for $k(w)$ over $k(v)$, then $\{\alpha_j \pi^\ell : 1 \leq j \leq f, 0 \leq \ell < e\}$ is a basis for L over K.

To see this, recall the representation $a = \sum_{i=0}^{\infty} a_i \pi^i$ from Prop. I.§6, where the a_i's lie in a set of representatives of $\mathfrak{o}(w)$ modulo $\mathfrak{m}(w)$, denoted by $\mathcal{R}$. If we choose $\mathcal{R}$ so that each element of $\mathcal{R}$ is an $\mathfrak{o}(v)$-linear combination of the α_j's, in particular $a_i = \sum_j b_{ij} \alpha_j$ for all i, then $a = \sum_{j,\ell} c_{j\ell} \alpha_j \pi^\ell$ where[12] $c_{j\ell} = \sum_{k=0}^{\infty} b_{ke+\ell,j} \pi^{ke} \in \mathfrak{o}(v)$, and we are through.

Now, if $|\cdot| = |\cdot|_v, |\cdot|_w$ denote the normalized absolute values on (K, v) and (L, w) respectively (see §6), then by definition $|x|_w = |x|_v^{ef} = |x|_v^n$ for all $x \in K$. Let $\|\cdot\|$ be defined as in Thm. I.§7; then $|\cdot|_w$ and $\|\cdot\|$ both induce w, so by the proof of Lemma I.§4 there exists a ρ with $|\alpha|_w = \|\alpha\|^\rho$ for all $\alpha \in L$. If we plug in $\alpha = x \in K$, we see that ρ must be equal to n, whence $|\alpha|_w = |N_{L/K}(\alpha)|_v$ for all $\alpha \in L$.

§8. Global fields

Having introduced local fields in §6, we now proceed to investigate the other class of "fields of number theory", namely that of global fields. Several characterizations of global fields are known; we loosely follow the axiomatization given in [ArWh45].

Let A be a Dedekind domain, K its field of fractions, and let $\mathcal{F}$ denote the set of A-finite places of K (see also §4). Further, let $\mathfrak{M} \supset \mathcal{F}$ be a set of non-trivial places of K so that $\mathfrak{M} \setminus \mathcal{F}$ is finite and non-empty. We call $(K, A, \mathfrak{M})$ a *global field* if

(G1) for each $v \in \mathfrak{M}$, the completion (K_v, v) of K at v is a local field;

(G2) for $v \in \mathfrak{M}$, let $|\cdot|_v$ denote the normalized absolute value of (K_v, v), and let $\rho_v = 2$ if $K_v = \mathbb{C}$ and $\rho_v = 1$ otherwise. Then, for each $x \in K^\times$, $\{v \in \mathfrak{M} : x \notin \mathfrak{u}(v)\}$ is a finite set and

$$\prod_{v \in \mathfrak{M}} |x|_v^{\rho_v} = 1.$$

Note that (G1) partly explains the use of the terms "global" and "local" for these types of fields: indeed, they hint at the fact that, passing to the completion, one "zooms in" on one particular place. The *product formula* (G2) implies that $\mathfrak{M}$ consists of the "right" places of K.

The domain A is called the *ring of integers* of K and mostly denoted $\mathcal{O}_K$. Places

[12] To see that this series converges, use a similar argument as the one in the proof of Prop. I.§6.(ii).

contained in $\mathcal{F}$ and $S_\infty := \mathfrak{M} \setminus \mathcal{F}$ are simply called *finite* and *infinite* places of K respectively. If $v \in \mathfrak{M}$ is usually denoted by $v_\mathfrak{s}$, we shall regularly write $\mathfrak{o}(\mathfrak{s})$, $\mathfrak{m}(\mathfrak{s})$, $k(\mathfrak{s})$, $|\cdot|_\mathfrak{s}$ and so on instead of $\mathfrak{o}(v_\mathfrak{s})$, $\mathfrak{m}(v_\mathfrak{s})$, $k(v_\mathfrak{s})$, $|\cdot|_{v_\mathfrak{s}}$, and write $\nu_\mathfrak{s}$ for the normalized valuation of $\mathfrak{o}(\mathfrak{s})$ if $v_\mathfrak{s}$ is discrete, see §3.

EXAMPLE. (1) Let $A = \mathbb{Z}$, $K = \mathbb{Q}$. By Ex. §4.(1), the A-finite places of K are precisely the p-adic topologies v_p for $p \in \mathbb{Z}_{\geq 0}$; moreover, let v_∞ be the Euclidean place of $\mathbb{Q}$ as in Ex. §1.(2). Now set[13] $\mathfrak{M} := \{v_p : p \leq \infty\}$. Then $(K, A, \mathfrak{M})$ is a global field. Indeed, (G1) was shown in §6. By Cor. I.§6, $|\cdot|_p = p^{-\nu_p(\cdot)}$, see also Ex. §1.(6). So let $x \in K^\times$; by the fundamental theorem of arithmetic, $\nu_p(x) = 0$ for all but finitely many p and $x = \pm \prod_p p^{\nu_p(x)}$, therefore $|x|_\infty = \prod_p |p^{\nu_p(x)}|_\infty = \prod_p |x|_p^{-1}$, and (G2) follows.

(2) Let F be a finite field, $A = F[t]$, $K = F(t)$, $q = \#F$. If $v = v_\mathfrak{p}$ is an A-finite place of K, then $(K_\mathfrak{p}, v_\mathfrak{p})$ is local by Ex. §4.(2) and Cor. I.§6. The normalized absolute value is then given by $|\cdot|_\mathfrak{p} = (q^{\deg p})^{-\nu_\mathfrak{p}(\cdot)}$, where $p(t) \in A$ generates $\mathfrak{p} \subset A$.

Now let v be a nontrivial place of K which is not A-finite, $|\cdot|$ an absolute value which induces v. By Ex. §1.(7) and Rmk. §2.(2), v is non-archimedean and $\left|F^\times\right| = \{1\}$. Consider $f(t) = \sum_{i=0}^d f_d t^d \in A$ with $f_d \neq 0$. Since by assumption $t \notin \mathfrak{o}(v)$, the strong triangle inequality implies $|f(t)| \leq |f_d t^d| = |t|^d$; in fact, equality must hold since otherwise $|t|^d \leq \max\{|f(t)|, |f(t) - f_d t^d|\} < |t|^d$, which is absurd. But then $v = v_{\deg}$, see Ex. §1.(8).

Let $\mathfrak{M}$ denote the set of all nontrivial places of K. We now show that $(K, A, \mathfrak{M})$ is a global field. To prove (G1), it remains to show that $(K_{\deg}, v_{\deg})$ is local. But $v_{\deg}$ is $F[1/t]$-finite, so this follows from Cor. I.§6. Note that $\left|f(t)/g(t)\right|_{\deg} = q^{\deg f - \deg g}$. To prove (G2), recall that, because of polynomial division, every $f(t) \in F[t]$ can be written as a finite product of irreducible polynomials (and these factors are unique up to permutation and multiplication with constants), and argue similarly as for $\mathbb{Q}$. $\diamond$

The rational field $\mathbb{Q}$ and the function fields $F(t)$ with $\#F < \infty$ are, in a way, the most important examples of global fields, as every global field $(K, \mathcal{O}_K, \mathfrak{M})$ contains a copy of one of them. Indeed, if $\mathfrak{M}$ contains some archimedean place, then $K \supseteq \mathbb{Q}$ by Rmk. §2.(3). If not, then $\mathfrak{o}(\mathfrak{M}) := \bigcap_{v \in \mathfrak{M}} \mathfrak{o}(v)$ is a ring. But (G2) can only hold for $0 \neq x \in \mathfrak{o}(\mathfrak{M})$ if $|x|_v = 1$ for all v, and then $x^{-1} \in \mathfrak{o}(\mathfrak{M})$ as well; in other words, $\mathfrak{o}(\mathfrak{M})$ is a field F. It is finite since it embeds into each $k(v)$ by the familiar argument $F \subseteq \mathfrak{o}(v)$, $\{0\} = F \cap \mathfrak{m}(v)$.

It remains to show that there exists an element $t \in K$ which is *transcendental* over F, i.e. such that $1, t, t^2, \ldots$ are linearly independent over F, for then $F(t) \subseteq K$. So suppose for the sake of contradiction that for each $x \in K^\times$, the elements $1, x, x^2, \ldots$ are linearly dependent over F. Then their linear span $F(x)$ is a finite extension of F (cf. §7) and hence a finite field. Thus, by Ex. §1.(7), $x \in \mathfrak{u}(v)$ for all $v \in \mathfrak{M}$; in other words, all places of $\mathfrak{M}$ are trivial, which is absurd.

[13] By Ostrowski's theorem, see Ex. §2.(2), $\mathfrak{M}$ already contains all non-trivial places of $\mathbb{Q}$.

REMARK. A more conceptual approach to (G2) is the following: suppose that K is a field with a set $\mathfrak{M}$ of non-trivial places so that (G1) holds. Then there is a certain subring of the product $\prod_{v\in\mathfrak{M}} K_v$ which, when endowed with a suitable topology, can be made into a *locally compact topological ring*, the so-called *ring of adèles* $\mathbb{A}_K$. By local compactness, there exists a *Haar measure* μ for the additive group of $\mathbb{A}_K$. Then there exists a unique map[14] $|\cdot| : \mathbb{A}_K \to \mathbb{R}_{\geq 0}$ with $\mu(\mathfrak{a}S) = |\mathfrak{a}|\,\mu(S)$ for all $\mathfrak{a} \in \mathbb{A}_K$, $S \subseteq \mathbb{A}_K$ with $\mu(S) < \infty$.

Suppose now that there is an inclusion $K \hookrightarrow \mathbb{A}_K$ so that the image of K is discrete in $\mathbb{A}_K$ and the quotient of additive groups $\mathbb{A}_K/K$ is compact in the quotient topology. Then, by the properties of the Haar measure, $0 < \mu(\mathbb{A}_K/K) < \infty$; on the other hand, by construction one obtains $|x| = \prod_{v\in\mathfrak{M}} |x|_v^{\rho_v}$ for $x \in K$, where ρ_v is defined as above. Finally, $\mu(\mathbb{A}_K/K) = \mu(x\mathbb{A}_K/K) = \prod_v |x|_v^{\rho_v} \cdot \mu(\mathbb{A}_K/K)$ for $x \in K^\times$, and (G2) follows. $\diamond$

§9. Extensions of global fields

In this final section, we prove that finite-degree extensions of global fields are, under certain additional assumptions, again global fields. In particular, it will follow that the Hasse-Minkowski theorem, see Chapter IV, holds over all algebraic number fields.

The additional assumption mentioned above is that of *separability*, which we now define. Since we shall always be concerned with an extension L/K of finite degree n such that $L = K(\delta)$ for some $\delta \in L$ (see §7), we only give the definition in this special case.[15] First, consider a polynomial f over a field K. It is not hard to show (see e.g. [Isa94], 17.21) that there exists a field $L' \supseteq K$ such that $[L' : K] < \infty$ and f *splits* over L', which means that f can be written as a product of degree-one polynomials with coefficients in L'. If L' is chosen so that $[L' : K]$ is minimal, then it is called a *splitting field* of f over K. All splitting fields of f over K are isomorphic, so we shall speak of *the* splitting field $Z(f, K)$ of f over K.

Now let K, L, δ as above. If f denotes the minimal polynomial $f_{K,\delta}$ of δ over K, then $Z = Z(f, K) \supseteq L$. We say that L/K is a *separable* extension if f has $n = [L : K] = \deg f$ distinct roots in Z. We can now formulate the main theorem of this section:

Theorem I.§9. *Let $(K, \mathcal{O}_K, \mathfrak{M})$ be a global field, and let L/K be a separable extension, $[L : K] = n < \infty$, $L = K(\delta)$ for some $\delta \in L$. Then $(L, \mathcal{O}_L, \mathfrak{N})$, where $\mathcal{O}_L := \{\alpha \in L : f_{K,\alpha}(t) \in \mathcal{O}_K[t]\}$ denotes the* integral closure *of $\mathcal{O}_K$ in L and $\mathfrak{N}$ denotes the set of places w of L which divide some $v \in \mathfrak{M}$, is again a global field.*

[14] Incidentally, the same construction can be carried out for a locally compact topological field (K, v); the resulting map $|\cdot|$ is then "almost" an absolute value (in general, only a weaker version of the triangle inequality holds) which induces v and $\mathfrak{o}(v) = \{x : |x| \leq 1\}$ is compact, so (K, v) is a local field. If $K \neq \mathbb{C}$, then $|\cdot|$ is precisely the normalized absolute value $|\cdot|_v$ of (K, v) as defined in §6, otherwise $|\cdot| = |\cdot|_v^2$.

[15] As it turns out, such a δ always exists if L/K is a finite-degree separable extension; this result is known as the *primitive element theorem*.

Proof. It is a fundamental result of algebraic number theory, see e.g. [Ser79], that $\mathcal{O}_L$ is Dedekind with field of fractions L. Let $\mathcal{F}'$ denote the set of places $w \in \mathfrak{N}$ which are $\mathcal{O}_L$-finite. The following lemma shows that $w \in \mathcal{F}'$ iff w divides $v \in \mathcal{F}$, see §8.

Lemma I.§9. *Let v be a place of K, w be a place of L with $w|v$, $\alpha \in L$. If v (or equivalently w) is non-archimedean and $f_{K,\alpha}(t) \in \mathfrak{o}(v)[t]$, i.e. if $f_{K,\alpha}(t)$ has all coefficients in $\mathfrak{o}(v)$, then $\alpha \in \mathfrak{o}(w)$.*

Proof. Write $f_{K,\alpha}(t) = t^d + \sum_{i=0}^{d-1} f_i t^i$, and let $|\cdot|$ be an absolute value which induces w on L. By §2, $|\cdot|$ must satisfy the strong triangle inequality, so if α did not lie in $\mathfrak{o}(w)$, then we would have that $|\alpha|^d > |\alpha|^{d-1} \geq |\sum_{i=0}^{d-1} f_i \alpha^i| = |-\alpha^d|$, which is absurd. □

Next, we show that $\mathfrak{N} \setminus \mathcal{F}'$ is non-empty and finite. Since $\#(\mathfrak{M} \setminus \mathcal{F}) < \infty$ (see §8), this will follow from Prop. I.§9.(iii) below.

Proposition I.§9. *Let $f = f_{K,\delta}$, $Z = Z(f, K) \supseteq L$. Then:*

*(i) The set $\mathfrak{S}$ of K-*homomorphisms[16] *$\sigma : L \to Z$ has precisely n elements.*

(ii) For each $\alpha \in L$, the product $\prod_{\sigma \in \mathfrak{S}} \sigma(\alpha)$ equals $N_{L/K}(\alpha)$ (see §7).

(iii) For each $v \in \mathfrak{M}$, there is a surjection $\mathfrak{S} \twoheadrightarrow \{w \in \mathfrak{N} : w|v\}$. The preimage of $w|v$ is precisely $\mathfrak{S}_w := \{\sigma \in \mathfrak{S} : \sigma(L) \subseteq L_w\}$.

Proof. (i) Since $1, \delta, ..., \delta^{n-1}$ form a basis for L over K, for each root β of f in Z there is a unique K-homomorphism $\sigma : L \to Z$ which sends δ to β. Conversely, if $\sigma : L \to Z$ is a K-homomorphism, then $f\big(\sigma(\delta)\big) = \sigma\big(f(\delta)\big) = 0$, i.e., $\sigma(\delta)$ is a root of f.

(ii) By a similar argument as before, each $\sigma(\alpha)$ is a root of $f_{K,\alpha}(t)$ in Z; it is then not hard to show that $\prod_{\sigma \in \mathfrak{S}} \big(t - \sigma(\alpha)\big) = C_{L/K;\alpha}(t)$ as defined in §7, and so $\prod_{\sigma \in \mathfrak{S}} \sigma(\alpha) = (-1)^n C_{L/K;\alpha}(0) = N_{L/K}(\alpha)$ as claimed.

(iii) Let $Z' = Z(f, K_v) \supseteq K_v$. By (G1) and Thm. I.§7, Z' has a unique place $u|v$ and (Z', u) is local; let $|\cdot|_u$ denote its normalized absolute value. For $\sigma \in \mathfrak{S}$, $\sigma : L \to Z \subseteq Z'$, one readily checks that $|\cdot|_u \circ \sigma$ is an absolute value on L; let w_σ denote the place of L it induces. We show that $\sigma \mapsto w_\sigma$ is surjective. For let $w|v$, then the inclusion $\iota = \iota_w : L \hookrightarrow L_w$ (see §5) is a K-homomorphism; clearly L_w must contain both K_v and $\iota(\delta)$, hence $L_w \supseteq K_v\big(\iota(\delta)\big)$. On the other hand, $K_v\big(\iota(\delta)\big) \subseteq Z'$ with the restriction of u is a local field, again by (G1) and Thm. I.§7. In particular, it is complete; since it contains $\iota(L)$, it must contain its completion L_w. Thus, we obtain that ι is a map $L \to Z$, $w = w_\iota$, $L_w = K_v\big(\iota(\delta)\big)$, and for $\sigma \in \mathfrak{S}$ we have $w_\sigma = w_\iota$ iff $\sigma(L) \subseteq L_{w_\iota}$. □

It remains to show that (G1) and (G2) hold for $(L, \mathcal{O}_L, \mathfrak{N})$. In fact, (G1) follows from the proof of Prop. I.§9.(iii).

[16] Recall that a K-homomorphism (of fields containing K) is a field homomorphism which is K-linear.

As for (G2), we must first prove that for each $\alpha \in L^\times$ there are at most finitely many $w \in \mathfrak{N}$ such that $\alpha \notin \mathfrak{u}(w)$. To this end, let f and g denote the minimal polynomial of α and $1/\alpha$ respectively over K. Since (G2) holds for K, there are at most finitely many $v_1, ..., v_s \in \mathfrak{M}$ such that not all coefficients of f and g lie in $\mathfrak{o}(v_j)$. By Prop. I.§9.(iii), there are at most finitely many $w_1, ..., w_t \in \mathfrak{N}$ which divide some v_j; if $w \in \mathfrak{N}$, $w \neq w_j$, is non-archimedean, then by Lemma I.§9 both α and $1/\alpha$ lie in $\mathfrak{o}(w)$, in other words $\alpha \in \mathfrak{u}(w)$. As for the archimedean places, note that, by Prop. I.§2.(iv), $v \in \mathfrak{M}$ is archimedean if and only if $2 \notin \mathfrak{o}(v)$, and so $\mathfrak{M}$ only contains finitely many archimedean places by (G2). But then by Prop. I.§9.(iii) and Rmk. §2.(2) the same holds for $\mathfrak{N}$, and we are through.

Finally, we set out to prove the product formula. For $w \in \mathfrak{N}$, let $|\cdot|_w$ denote the normalized absolute value on (L_w, w), and $|\cdot|_v$ denote the normalized absolute value on (K_v, v) where $w|v$; further, let ρ_w and ρ_v be defined analogously as in §8. We know from §7 that $|\alpha|_w^{\rho_w} = |N_{L_w/K_v}\big(\iota_w(\alpha)\big)|_v^{\rho_v}$, where ι_w is as in the proof of Prop. I.§9.(iii), for all $\alpha \in L$. Prop. I.§9.(ii) allows us to write $N_{L_w/K_v}\big(\iota_w(\alpha)\big) = \prod_{\tau \in \mathfrak{S}'_w} \tau\big(\iota_w(\alpha)\big)$, where $\mathfrak{S}'_w = \{\tau : L_w \to Z' : \tau \text{ is a } K_v\text{-homomorphism}\}$, for all $\alpha \in L$.

We now give an alternative description of $\mathfrak{S}'_w$. For $\sigma \in \mathfrak{S}_w$, defined as in Prop. I.§9.(iii), define $\widehat{\sigma} : L_w \to Z'$ via $\widehat{\sigma}(\widehat{x}) = \lim \sigma(x_n)$ where $\widehat{x} \in L_w$ and $\iota(x_n)$ converges to $\widehat{x}$ in L_w. One quickly checks that $\widehat{\sigma}$ is well-defined and that it is the unique extension of σ to L_w. Thus, $\sigma \mapsto \widehat{\sigma}\widehat{\iota_w}^{-1}$ yields an injection $\mathfrak{S}_w \hookrightarrow \mathfrak{S}'_w$. But, by Prop. I.§9.(i), $\mathfrak{S}'_w$ has precisely as many elements as there are roots of $f_{K_v,\iota(\delta)}$ in Z', and one readily checks that this is also the cardinality of $\mathfrak{S}_w$, so the above map is even bijective. Accordingly, for all $\alpha \in L$ we can write $N_{L_w/K_v}(\alpha) = \prod_{\sigma \in \mathfrak{S}_w} \widehat{\sigma}(\alpha) = \prod_{\sigma \in \mathfrak{S}_w} \sigma(\alpha)$.

Finally, let $\alpha \in L^\times$. It remains to show that the product $\prod_{w \in \mathfrak{N}} |\alpha|_w^{\rho_w}$ is equal to 1. But

$$\begin{aligned}
\prod_{w \in \mathfrak{N}} |\alpha|_w^{\rho_w} &= \prod_{v \in \mathfrak{M}} \prod_{w|v} \Big| N_{L_w/K_v}\big(\iota_w(\alpha)\big) \Big|_v^{\rho_v} \\
&= \prod_{v \in \mathfrak{M}} \prod_{w|v} \prod_{\sigma \in \mathfrak{S}_w} |\sigma(\alpha)|_v^{\rho_v} \\
&= \prod_{v \in \mathfrak{M}} \prod_{\sigma \in \mathfrak{S}} |\sigma(\alpha)|_v^{\rho_v} \\
&= \prod_{v \in \mathfrak{M}} \Big| N_{L/K}(\alpha) \Big|_v^{\rho_v} = 1,
\end{aligned}$$

where in the penultimate step we have used Prop. I.§9.(ii) and in the last step we have used the product formula for $(K, \mathcal{O}_K, \mathfrak{M})$ with $x = N_{L/K}(\alpha) \in K^\times$. □

II. Quadratic forms

This chapter is devoted mostly to the basic theory of quadratic forms over general fields (of characteristic $\neq 2$). In the last section, we further specialize to local fields, while quadratic forms over global fields are studied in Chapter IV.

§1. Bilinear forms

In this section we review some well-known facts about bilinear forms in a quite general setting. Let R be a ring, and M be an *R-module*[1], i.e. an abelian group (with respect to an operation denoted as $+$) equipped with a scalar multiplication $R \times M \to M$, denoted as $\cdot$, which is compatible with the ring operations on R in the obvious way:

$r \cdot (x+y) = r \cdot x + r \cdot y$ for all $r \in R$, $x, y \in M$;
$(r+s) \cdot x = r \cdot x + s \cdot x$ for all $r, s \in R$, $x \in M$;
$r \cdot (s \cdot x) = (r \cdot s) \cdot x$ for all $r, s \in R$, $x \in M$;
$1 \cdot x = x$ for all $x \in M$.

A map $b : M \times M \to R$ is called *(R-)bilinear*, or a *bilinear form* on M, if the maps $y \mapsto b(x,y)$ and $x \mapsto b(x,y)$) are R-linear for each fixed $x \in M$ and $y \in M$ respectively. Moreover, b is called *symmetric* if $b(x,y) = b(y,x)$ for all $x, y \in M$.

Example. (1) Consider R as an R-module in the trivial way. Then $(x,y) \mapsto rxy$ defines a symmetric R-bilinear form on R for each $r \in R$.

(2) Let $M = R^n$ with component-wise addition and scalar multiplication. Then $b : \big((x_1,...,x_n),(y_1,...,y_n)\big) \mapsto \sum_{i=1}^n x_i y_i$ defines a symmetric bilinear form on M. Note that if $R = \mathbb{R}$ is the field of real numbers, then b is the standard scalar product on $\mathbb{R}^n$, commonly denoted $\langle\ ,\ \rangle$. ◇

Thanks to Ex.(2) we can carry over some notation and terminology from linear algebra to general symmetric bilinear forms b. For instance, for a submodule $N \subseteq M$ we denote

$$N^\perp = \{y \in M : b(x,y) = 0 \text{ for all } x \in N\}$$

[1]Note that if R is a field F, then an R-module is simply a vector space over F.

and say that a submodule $N' \subseteq M$ is *orthogonal* to N if $N' \subseteq N^\perp$. (By symmetry of b, this is the case if and only if N is orthogonal to N'.) Two elements $x, y \in M$ are said to be orthogonal to each other if their R-linear spans Rx, $Ry \subseteq M$ are orthogonal submodules; an element $0 \neq x \in M$ is called *isotropic* if it is orthogonal to itself, otherwise *anisotropic*. Finally, we introduce the notation $M = N \perp N'$ as a shortcut for: $M = N \oplus N'$ and $N' \subseteq N^\perp$.

EXAMPLE. (3) Consider $M = R^n$, b as in (2), and let $e_j = \big(\delta_{ij}\big)_{i=1,\dots,n} \in M$, where δ_{ij} denotes the Kronecker symbol. Then $M = Re_1 \perp ... \perp Re_n$.

(4) If $R = \mathbb{R}$, $M = V$ has finite dimension over $\mathbb{R}$ and b is positive definite, then it is well-known that $V = W \perp W^\perp$ for any subspace $W \subseteq V$.

(4') On the other hand, consider $V = \mathbb{R}^2$ and $b : \big((x_1, x_2), (y_1, y_2)\big) \mapsto x_1y_1 - x_2y_2$. Then b is clearly indefinite, $x = (1, 1) \in V$ is isotropic and $V \neq \mathbb{R}x \oplus (\mathbb{R}x)^\perp = \mathbb{R}x$. $\diamond$

The difference between examples (4) and (4') can be explained by making use of the concept of a *regular* (sub-)space. If $R = F$ is a field and $M = V$ is a finite-dimensional vector space over F, then regularity of V (more accurately, of the pair (V, b)) means precisely that, for any basis $v_1, ..., v_n$ of V over F, the *Gram matrix*

$$\big(b(v_i, v_j)\big)_{1 \leq i,j \leq n}$$

of b with respect to $v_1, ..., v_n$ is invertible. Thus, in this setting regularity is equivalent to the (in general weaker) condition that (V, b) be *nondegenerate*, i.e. $V^\perp = \{0\}$.

REMARK. In order to check regularity, it suffices to check invertibility of $\big(b(v_i, v_j)\big)$ for *one* basis $v_1, ..., v_n$ of V. Indeed, if $v_1', ..., v_n'$ is a basis of V, $v_j' = \sum_i c_{ij} v_i$, then $C = (c_{ij})$ is invertible by elementary linear algebra, so:

$$\big(b(v_i, v_j)\big) \text{ is invertible iff } \Big(b(v_i', v_j')\Big) = C^T \big(b(v_i, v_j)\big)\, C \text{ is invertible.}$$

Incidentally, this equation shows that, if (V, b) is regular, then $\det\big(b(v_i, v_j)\big) \in F^\times$ is uniquely determined up to multiplication by the square of a nonzero element; in other words, its coset in the quotient group $F^\times / F^{\times 2}$ is well-defined. This coset is called the *determinant* of the pair (V, b) and denoted $\det(V, b)$ or $\det V$. If V is not regular one sets $\det V = 0$. $\diamond$

The next proposition shows that, under the assumption of regularity, it is possible to generalize some basic properties of the standard scalar product in Euclidean space.

Proposition II.§1. *Let $R = F$ be a field, $M = V$ be of finite dimension over F. Then:*

(i) For every regular subspace $W \subseteq V$, $W^\perp$ is the unique subspace U of V with $V = W \perp U$;

(ii) If V is regular and $W \subseteq V$ is any subspace, then

$$\dim W + \dim W^\perp = \dim V; \qquad W^{\perp\perp} = W.$$

Proof. Throughout this proof, for $W \subseteq V$ let W^* denote the space of linear functionals on W and let $\varphi_W : V \to W^*$, $x \mapsto \big(y \mapsto b(x,y)\big)$. By definition, $(W, b|_W)$ is nondegenerate, i.e., $W \cap W^\perp = \{0\}$, if and only if φ_W is bijective.

(i) Since W is regular, it is nondegenerate, hence $W \cap W^\perp = \{0\}$. We now show $V = W + W^\perp$. Consider the inclusions $\varphi_W(W) \subseteq \varphi_W(V) \subseteq W^*$; by bijectivity of φ_W, we have $\dim \varphi_W(W) = \dim W = \dim W^*$, hence $\varphi_W(W) = \varphi_W(V)$. But then for each $x \in V$ there is a $y \in W$ with $x - y \in \ker \varphi_W = W^\perp$, thus $V = W + W^\perp$ as claimed.

Now let $U \subseteq V$ be another subspace with $V = W \perp U$. Clearly U and $W^\perp$ must have the same dimension. But U is orthogonal to W, so $U \subseteq W^\perp$, therefore equality holds.

(ii) Since V is regular, $\varphi_V : V \to V^*$ is bijective, so its restriction $\varphi_W : V \to W^*$ is surjective; the first claim now follows from the rank-nullity theorem since $\ker \varphi_W = W^\perp$.

As for the second claim, note that the first implies $\dim W^\perp + \dim W^{\perp\perp} = \dim V$, hence $\dim W = \dim W^{\perp\perp}$. But then we are done since clearly $W \subseteq W^{\perp\perp}$. □

§2. Quadratic forms and representations

In this section, we finally introduce the main subject of this chapter, namely quadratic forms. Classically, a quadratic form over a ring R is simply a *homogeneous quadratic polynomial* over R, i.e. an expression of the form

$$q(x_1, ..., x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

for some $a_{ij} \in R$ and some $n \in \mathbb{N}$. More geometrically, a *quadratic form* on an R-module M is a map $q : M \to R$ with the following properties:

(i) $q(ax) = a^2 q(x)$ for all $a \in R$, $x \in M$;

(ii) the map $\beta = \beta_q : M \times M \to R$, $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is bilinear.

The pair (M, q) is called a *quadratic module* over R. If $R = F$ is a field, then $M = V$ is a vector space over F and (V, q) is called a *quadratic space* over F. An *n-ary quadratic space* is a quadratic space (V, q) with $\dim V = n < \infty$; moreover, we use the traditional terms *binary*, *ternary*, *quaternary* and *quinary* for $n = 2$, 3, 4 and 5 respectively.

If b is a symmetric bilinear form on M, then $q_b : x \mapsto b(x, x)$ is a quadratic form on M; one readily checks that $\beta_{q_b} = 2b$. Thus, if 2 is invertible in R, we obtain a bijection

between quadratic forms and symmetric bilinear forms on M via $b \mapsto q_b$, $q \mapsto \frac{1}{2}\beta_q$; this allows us to unambiguously consider a quadratic module (M, q) as a module with a symmetric bilinear form $b_q := \frac{1}{2}\beta_q$ and accordingly use all the terms and notations from §1. For this reason, we shall henceforth **restrict to the case** $2 \in R^\times$. Whenever the ring R at hand is a field F, we equivalently assume that $\chi(F) \neq 2$, cf. Rmk. I.§2.(3).

The following proposition is a fundamental result on quadratic forms over fields.

Proposition II.§2. *Let (V, q) be a finite-dimensional quadratic space over a field F. Then V has an* orthogonal basis*, i.e. a basis $v_1, ..., v_n$ with $V = Fv_1 \perp ... \perp Fv_n$.*

Proof. We proceed by induction on $n = \dim V$. If q is identically zero, then any basis is orthogonal and we are done. Otherwise, let $v_1 \in V$ such that $q(v_1) \neq 0$, and expand v_1 to a basis $v_1, u_2, ..., u_n$ of V. For $i = 2, ..., n$ let $w_i := u_i - \frac{b(v_1,u_i)}{q(v_1)}v_1$; we check that the subspace W spanned by $w_2, ..., w_n$ satisfies $V = Fv_1 \perp W$. Now we can use the induction hypothesis on W since $\dim W = n - 1$. □

Remark. (1) If $v_1, ..., v_n$ is an orthogonal basis of V, then the matrix $\big(b(v_i, v_j)\big)_{i,j}$, cf. Rmk. §1, has diagonal form with entries $q(v_i) =: a_i$ on the diagonal. In particular, (V, q) is regular if and only if $a_i \neq 0$ for all i, in which case $\det V = a_1 \cdots a_n F^{\times 2}$. We also say that q has "diagonal form" with respect to $v_1, ..., v_n$ since $q(x) = \sum a_i x_i^2$ for all $x = \sum x_i v_i \in V$.

(2) There is also a concept of "diagonalization" for quadratic forms q in the classical sense: the mixed terms can be eliminated by successively replacing each variable x_i by an appropriate linear combination of $x_i, ..., x_n$ which "completes the square", and we are left with $q(x_1, ..., x_n) = \sum a_i x_i^2$. The number of variables which appear in this diagonal form, i.e. the number of i such that $a_i \neq 0$, is called the *rank* of q. Comparing with (1), we obtain that V is regular if and only if q has "full rank" in the classical sense. ◇

A classical problem pertaining to quadratic forms (in the classical sense) is the solvability of equations of the form $q(x_1, ..., x_n) = a$ for a given q and a given $a \in R$: one says that q *represents* a if the equation has a (nontrivial)[2] solution. In our geometric setting, this translates as follows: (M, q) *represents* $a \in R$ if there exists some $0 \neq x \in M$ with $q(x) = a$. If $R = F$ is a field, $M = V$, then (V, q) is called *isotropic* if it represents 0, i.e. if it contains an isotropic vector, and *universal* if it represents every $a \in F^\times$.

Example. Let $R = F$ be a finite field of characteristic $\chi(F) = p \neq 2$ and consider $\omega : F \to F$, $c \mapsto c^2$; since $\omega(F) = \{0\} \cup F^{\times 2}$, we have[3] $\#\omega(F) = 1 + \#F^{\times 2} = 1 + \frac{\#F^\times}{2}$.

[2] If $a = 0 \in R$, then $x_1 = ... = x_n = 0$ is regarded as a *trivial* solution to the equation $q(x_1, ..., x_n) = a$.

[3] For the second equality, we use some elementary group theory. Indeed, $\omega|_{F^\times} : F^\times \to F^\times$ is a group homomorphism with kernel $\{1, -1\}$ and image $F^{\times 2}$.

Now let $M = V$ have finite dimension $n \geq 2$ over F, and let $q(x) = \sum a_i x_i^2$ be a "diagonalization" of q as in Rmk. §2.(1). Suppose further that V is regular, in particular $a_1 \neq 0 \neq a_2$, and let $a \in F^\times$. From our earlier observations regarding ω, we infer that the image of $(x_1, x_2) \mapsto a_1 x_1^2$ and the image of $(x_1, x_2) \mapsto a - a_2 x_2^2$ both have $1 + \frac{\#F^\times}{2} > \frac{\#F}{2}$ elements. But then they have non-empty intersection, thus there exists a pair (x_1, x_2) with $q(x_1 v_1 + x_2 v_2) = a$. This proves that every regular space of finite dimension $n \geq 2$ over F is universal. $\diamond$

We conclude this section with the following fundamental result on representability and some easy applications.

Theorem II.§2. *Let (V, q) be a finite-dimensional quadratic space over a field F. If V is regular and isotropic, then it is universal.*

Proof. Let $v \in V$ be an isotropic vector. Since V is regular, v does not lie in $V^\perp = \{0\}$, so there exists some $w' \in V$ with $b(v, w') \neq 0$, where $b = b_q$; we can assume $b(v, w') = 1$. It is now a straightforward computation that $w = w' - \frac{q(w')}{2} v$ is again isotropic, $b(v, w) = 1$ and $q\left(v + \frac{a}{2} w\right) = a$ for all $a \in F$. $\square$

Corollary II.§2. *Let V, q, F be as in Thm. II.§2, $b = b_q$, and suppose that V is regular. Then:*

(i) Let $a \in F^\times$, and consider $V' = V \times F$ equipped with $q' : V' \to F$, $(x, y) \mapsto q(x) - ay^2$. Then V represents a if and only if V' represents 0;

(ii) if $\dim V = 2$, then V represents 0 if and only if $\det V = -1 \cdot F^{\times 2}$;

(iii) if $\dim V = 4$, $\det V = 1 \cdot F^{\times 2}$, and $W \subseteq V$ is a regular ternary subspace, then V represents 0 if and only if W does.

Proof. (i) Necessity is clear: if $x \in V$ satisfies $q(x) = a$, then $q'\big((x, 1)\big) = 0$. Conversely, suppose that V' represents 0. If V represents 0, we are done by Thm. II.§2; otherwise, there exist $0 \neq c \in F$ and $x \in V$ with $0 = q'\big((x, c)\big) = q(x) - ac^2$. But then $q\left(\frac{1}{c} x\right) = a$.

(ii) Suppose that V contains an isotropic vector v, and let $w \in V$ be as in the proof of Thm. II.§2. The vectors v and w are linearly independent (for otherwise we would have $b(v, w) = 0$), so they form a basis for V; the Gram matrix (see Rmk. §1) of b with respect to v, w is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, hence $\det V = -1 \cdot F^{\times 2}$.

Conversely, let $\det V = -1 \cdot F^{\times 2}$. Since V is regular, it has an orthogonal basis v_1, v_2 by Prop. II.§2; we have $q(v_1) q(v_2) \in -1 \cdot F^{\times 2}$, i.e. $-q(v_1) q(v_2) = a^2$ for some $a \in F^\times$. But then $x = v_2 + \frac{q(v_2)}{a} v_1$ is isotropic.

(iii) We only need to prove necessity. By Prop. II.§1, we have $\dim W^\perp = 1$, i.e. $W^\perp = Fx$ for some $x \in V$, and $V = W \perp Fx$; in particular, since (V, q) is regular, $q(x) \neq 0$, cf. Rmk.(1). Now W represents $-q(x)$ by part (i), so there exist $w \in W$, $U \subseteq V$

with $W = U \perp Fw$ and accordingly $V = U \perp Fw \perp Fx$. Using Rmk.(1), we obtain that $\det V = q(x)q(w)\det U = -q(x)^2 \det U = -\det U \in F^\times/F^{\times 2}$, i.e., $\det U = -1 \cdot F^{\times 2}$. Now U (and hence also $W \supseteq U$) contains an isotropic vector by part (ii). $\square$

§3. Isometries and Witt's Theorem

In this section, we prove that any quadratic space can be decomposed into an orthogonal sum of subspaces and that this decomposition is unique up to a precise notion of isomorphism. The following conventions are in force throughout this section, unless stated otherwise: whenever we work over a ring R or a field F, we assume that 2 is invertible there; moreover, all quadratic spaces over fields are assumed to be finite-dimensional.

We now look at R-linear maps $f : M \to M'$ between quadratic modules (M, q), (M', q') which "preserve" their structure in the sense that $q' \circ f = q$. An injective map with this property is called a *metric morphism*, and an *isometry* if it is even bijective. Finally, (M, q), (M', q') are called *isometric* or *isomorphic*, in symbols $(M, q) \cong (M', q')$, if there exists an isometry $f : M \to M'$; in this case, q and q' assume the same values, i.e. $q(M) = q'(M') \subseteq F$, and $b_q(x, y) = b_{q'}\big(f(x), f(y)\big)$ for all $x, y \in M$.

Given quadratic spaces over a field F, we can investigate if they are isomorphic using Gram matrices only, cf. Rmk. §1. Indeed, let (V, q) be a quadratic space over F, and let B be the Gram matrix of $b = b_q$ with respect to some basis $v_1, ..., v_n$ of V. If (V', q') is isomorphic to (V, q) via the isometry $f : V \to V'$, then V' has a basis such that the Gram matrix of $b' = b_{q'}$ with respect to this basis equals B, namely $f(v_1), ..., f(v_n)$. Conversely, if (V', q') has a basis $v_1', ..., v_n'$ such that the Gram matrix of b' with respect to $v_1', ..., v_n'$ equals B, then $f : V \to V'$, $v_i \mapsto v_i'$ is an isometry. For this reason, it is customary to use $\langle B \rangle$ to denote *any* quadratic space isomorphic to (V, q), i.e. any quadratic space whose Gram matrix with respect to some basis equals B.

Note the special case $n = 1$, where B is just a scalar $a \in F$; in this case, $\langle a \rangle$ can be used to denote any one-dimensional quadratic (sub-)space (W, q) spanned by a vector x with $q(x) = a$. Following the literature, we shall sometimes denote orthogonal sums $\langle a_1 \rangle \perp \langle a_2 \rangle \perp ... \perp \langle a_n \rangle$ of one-dimensional subspaces simply by $\langle a_1, a_2, ..., a_n \rangle$.

REMARK. (1) Let $a \in F^\times$. By definition, V represents a if and only if V contains a subspace of the form $\langle a \rangle$. If this is the case, then this subspace is regular since $a \neq 0$, so with the help of Prop. II.§1.(i) we obtain: V represents a if and only if $V = \langle a \rangle \perp U$ for some subspace $U \subseteq V$ (in which case necessarily $U = \langle a \rangle^\perp$).

(2) Again let $a \in F^\times$. The space (V', q') defined as in Cor. II.§2.(i) can be written as $V \perp \langle -a \rangle$. The *ad hoc* procedure used to construct V' can be generalized as follows: given spaces (V_1, q_1), (V_2, q_2), equip the cartesian product $V = V_1 \times V_2$ with the quadratic

form $q : V_1 \times V_2 \to F$, $(x_1, x_2) \mapsto q_1(x_1) + q_2(x_2)$; after the obvious identifications, we obtain $V = V_1 \perp V_2$. We may refer to V as the "outer orthogonal sum" of V_1 and V_2.

(3) Consider $V = F \times F$ together with the quadratic form $q : V \to F$, $(x_1, x_2) \mapsto x_1 x_2$ (note that this definition makes sense over any ring R). The Gram matrix of b_q with respect to the standard basis $e_1 = (1, 0)$, $e_2 = (0, 1)$ is precisely $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; on the other hand, by denoting $v_1 = (1, 1)$, $v_2 = (1, -1)$ we obtain $V = Fv_1 \perp Fv_2 = \langle 1 \rangle \perp \langle -1 \rangle$.

Any quadratic space isomorphic to (V, q) is called a *hyperbolic*[4] *plane* over F. Since $\det V = -1 \cdot F^{\times 2}$, any hyperbolic plane is regular and must represent 0 by Cor. II.§2.(ii). Conversely, upon taking a closer look at the proofs of Thm. II.§2 and Cor. II.§2.(ii) one sees that any regular space (V', q') which represents 0 contains a two-dimensional subspace $\mathbb{H}$ of the form $\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$, i.e. a hyperbolic plane; by Prop. II.§1.(i), $V = \mathbb{H} \perp \mathbb{H}^{\perp}$. $\diamond$

Now that we are more familiar with isometries of quadratic spaces, we set out to prove the result mentioned at the beginning of this section (Thm. II.§3 below).

Throughout the sequel, we fix a field F and a quadratic space (V, q) over F of dimension n and denote $b = b_q$. We shall be interested in the isometries $f : V \to V$; together with function composition, these form a group, the so-called *orthogonal group* of (V, q), denoted $\mathrm{O}(V, q)$ or $\mathrm{O}(V)$. The first useful observation is that, if $z \in V$ is anisotropic, i.e. $q(z) \neq 0$, then there exists an element $\tau_z \in \mathrm{O}(V)$ which fixes $(Fz)^{\perp}$ point-wise and sends z to $-z$; this isometry can be thought of as a "reflection" across the "hyperplane" normal to z. Explicitly, τ_z is given by

$$x \mapsto x - \frac{2b(x, z)}{q(z)} z;$$

it is routine to check that all the properties stated above are satisfied.

Lemma II.§3. *Suppose $x, y \in V$ satisfy $q(x) = q(y) \neq 0$. Then there exists some $\sigma \in \mathrm{O}(V)$ such that $\sigma(x) = y$. Moreover, one can achieve that σ is the identity on $(Fx)^{\perp} \cap (Fy)^{\perp}$.*

Proof. If $z = x - y$ is anisotropic, i.e. if $0 \neq q(x-y) = q(x) + q(y) - 2b(x, y) = 2b(x, x-y)$, then we can set $\sigma = \tau_z$ since

$$\tau_z(x) = x - \frac{2b(x, x-y)}{q(x-y)}(x-y) = x - (x-y) = y.$$

If $q(x - y) = 0$, we use the identity $q(x - y) + q(x + y) = 2q(x) + 2q(y) = 4q(x) \neq 0$ to infer that $q(x + y) \neq 0$ and accordingly set $\sigma = \tau_y \circ \tau_{x+y}$ since then $\sigma(x) = \tau_y(-y) = y$. In either case, it is easy to check that σ also satisfies the additional property. $\square$

[4] It is likely that the term originates from the fact that, for $a \in F^{\times}$, the solution set of the equation $xy = a$ in the plane F^2 is a hyperbola.

Proposition II.§3 (Witt's Theorem)**.** *Let W, W' be regular subspaces of V of the same dimension m, and suppose there is an isometry $f : W \to W'$. Then*

(i) there exists $\sigma \in \mathrm{O}(V)$ with $\sigma|_W = f$, and

(ii) $W^\perp \cong (W')^\perp$.

Proof. (i) We use induction on the dimension. If $m = 1$, then we are done by the lemma.

If $m > 1$, pick $x \in W$ anisotropic and write $W = U \perp Fx$ (cf. Prop. II.§1.(i)). By the induction hypothesis, there exists some $\sigma' \in \mathrm{O}(V)$ with $\sigma'|_U = f|_U$. Set $y = (\sigma')^{-1}\big(f(x)\big)$; by construction we have $q(y) = q(x) \neq 0$, so by the lemma there is some $\tau \in \mathrm{O}(V)$ with $\tau(x) = y$ and such that $\tau(u) = u$ whenever $b(x, u) = b(y, u) = 0$.

Now set $\sigma = \sigma' \circ \tau$. Clearly $\sigma(x) = \sigma'(y) = f(x)$; moreover, for any $u \in U$, we have $b(y, u) = b\big(f(x), \sigma'(u)\big) = b\big(f(x), f(u)\big) = b(x, u) = 0$, hence τ is the identity on U and $\sigma = f \circ \mathrm{Id} = f$ on U.

(ii) If σ is as in part (i), then it follows from $W' = \sigma(W)$ that $(W')^\perp = \sigma(W^\perp)$. Thus, $g = \sigma|_{W^\perp} : W^\perp \to (W')^\perp$ is the sought-after isometry. □

Corollary II.§3 (Witt's Cancellation Theorem)**.** *If V is regular and V_1, V_2 are arbitrary quadratic spaces with $V \perp V_1 \cong V \perp V_2$ (cf. Rmk.(2)), then $V_1 \cong V_2$.*

Proof. Let $f : V \perp V_1 \to V \perp V_2$ be an isometry; clearly, $V \perp V_2 = f(V) \perp f(V_1)$. If we now consider V as a subspace of $V \perp V_2$, then $f|_V : V \to f(V)$ is an isometry of regular subspaces of $V \perp V_2$ and, by Prop. II.§3.(ii), we have $V_2 = V^\perp \cong f(V)^\perp = f(V_1)$. But then we are done since $f(V_1) \cong V_1$. □

Finally, we present and prove the much-anticipated result concerning the decomposition of quadratic spaces:

Theorem II.§3 (Witt's Decomposition Theorem)**.** *There are subspaces V_0, $V_a \subseteq V$, unique up to isometry, and a unique natural number $m \geq 0$ such that:*

(i) each nonzero element of V_0 is isotropic;

(ii) each nonzero element of V_a is anisotropic;

(iii) $V = V_0 \perp \mathbb{H}_1 \perp ... \perp \mathbb{H}_m \perp V_a$, where each $\mathbb{H}_i$ is a hyperbolic plane, see Rmk.(3).

Proof. For the existence part, set $V_0 = V^\perp$ and let $W \subseteq V$ be any subspace such that $V = V^\perp \oplus W$; then we automatically have $V = V^\perp \perp W$. Now, W is necessarily regular since $W \cap W^\perp \subseteq W \cap V^\perp = \{0\}$. If W contains an isotropic vector, then by Rmk.(3) it contains a hyperbolic plane $\mathbb{H}_1$ and $W = \mathbb{H}_1 \perp W'$ for a subspace $W' \subseteq W$; applying the same procedure to W' and iterating, we can write $W = \mathbb{H}_1 \perp ... \perp \mathbb{H}_m \perp U$ where U does not contain isotropic vectors, so we set $V_a = U$.

As for uniqueness, suppose that $V = V_0' \perp \mathbb{H}_1' \perp ... \perp \mathbb{H}_r' \perp V_a'$ is another decomposition as above. The subspace V_a' is regular (cf. Rmk. §2.(1)), so $W' := \mathbb{H}_1' \perp ... \perp \mathbb{H}_r' \perp V_a'$ is regular as well. But then $V^\perp$ must be equal to V_0', hence $V_0 = V_0'$.

We now show[5] $W \cong W'$. Consider any isometry $\sigma \in \mathrm{O}(V)$,

$$\sigma : V^\perp \perp \mathbb{H}_1 \perp ... \perp \mathbb{H}_m \perp V_a \to V^\perp \perp \mathbb{H}'_1 \perp ... \perp \mathbb{H}'_r \perp V'_a;$$

it must hold that $\sigma(V^\perp) = V^\perp$, and so necessarily $\sigma(W) = W'$, i.e., $\mathbb{H}_1 \perp ... \perp \mathbb{H}_m \perp V_a \cong \mathbb{H}'_1 \perp ... \perp \mathbb{H}'_r \perp V'_a$.

Since all hyperbolic planes are isomorphic to each other by definition, we can use Witt's Cancellation Theorem to cancel $\min\{m, r\}$ of them. If $r \neq m$, we are left with isometric spaces where only one of them represents 0, which is absurd; thus, m and r must be equal. But then we have $V_a \cong V'_a$, which concludes the proof. □

Remark. (4) The number m is called the *Witt index* of (V, q). For a regular quadratic space (V, q), it can be shown that, if $W \subseteq V$ is a subspace such that each nonzero element of W is isotropic, then $\dim W \leq m$, and equality is in fact attained.

(5) Given a field F, consider the set of isometry classes of (finite-dimensional) regular quadratic spaces over F (the *isometry class* of (V, q) contains precisely those quadratic spaces isometric to (V, q)). The outer orthogonal sum $\perp$ from (2) is an operation on this set which makes it into a commutative monoid M; Witt's Cancellation Theorem states precisely that this monoid is *cancellative* (cf. $\mathbb{N}$, which is a cancellative monoid with respect to $+$). By a standard procedure (essentially the same one can use to obtain $\mathbb{Z}$ from $\mathbb{N}$, or $\mathbb{Q}$ from $\mathbb{Z}$), we can endow $M \times M$ with an equivalence relation $\sim$ such that the quotient set is a group which contains a copy of M, the *Grothendieck group* of M.

As it turns out, cf. Rmk. III.§1.(4), the monoid M is equipped with an additional operation $\otimes$; one checks that $\otimes$ distributes over $\perp$, so it is interpreted as multiplication. But this operation naturally extends to a multiplication on the Grothendieck group of M, which thus becomes a ring, the so-called *Witt-Grothendieck ring* $\widehat{W}(F)$ of F. Moreover, one can define the *Witt ring* $W(F)$ of F as the ring obtained from $\widehat{W}(F)$ by factoring out the ideal $\mathbb{Z} \cdot \mathbb{H}$ generated by the isometry class of hyperbolic planes; this ring turns out to be key to some aspects of the theory of quadratic forms, see e.g. [Lam04].

(6) Suppose that V is regular. If we rephrase Rmk. §2.(1) with the notation $\langle \cdot \rangle$ introduced in this section, we have that $V = \perp_{i=1}^n \langle a_i \rangle$ where $a_i \in F^\times$. Clearly, $\langle a \rangle \cong \langle a' \rangle$ if and only if $aF^{\times 2} = a'F^{\times 2}$; thus, upon fixing a system of representatives $\mathcal{R}$ for $F^\times / F^{\times 2}$, one finds that every n-ary regular quadratic space over F is isometric to $\langle r_1, ..., r_n \rangle$ for some $r_1, ..., r_n \in \mathcal{R}$. Note, however, that the r_i's are not uniquely determined (not even up to a permutation); for instance, $\mathbb{H} = \langle 1, -1 \rangle = \langle a, -a \rangle$ for any $a \in F^\times$, cf. (3). ⋄

[5] Caution is advised here: the conclusion $W \cong W'$ does *not* follow directly from Prop. II.§3.(ii) since $V_0 = V^\perp$ is not regular.

§4. Local fields

As announced at the beginning of this chapter, this section is devoted to the study of quadratic forms over local fields, which were introduced in I.§6. While this topic will be discussed more thoroughly in Chapter III, the tools already at our disposal – particularly Rmk. §3.(6) – together with Thm. II.§4 below enable us to derive a few useful results.

Throughout the section, (K, v) is used to denote a fixed local field of characteristic $\chi(K) \neq 2$. Whenever we assume K to be non-archimedean, the usual notations $\mathfrak{o} = \mathfrak{o}(v)$, $\mathfrak{m} = \mathfrak{m}(v)$, $\mathfrak{u} = \mathfrak{u}(v)$ from Chapter I, as well as $k = k(v) = \mathfrak{o}/\mathfrak{m}$ and $q = \#k$, are in force; moreover, in this case we denote the normalized valuation of $\mathfrak{o}$ (see I.§3) with ν and fix a uniformizer π of $\mathfrak{o}$.

Theorem II.§4. *Let $G = K^\times/K^{\times 2}$.*

(i) If $K = \mathbb{C}$, then G is the trivial group $\{1\}$.

(ii) If $K = \mathbb{R}$, then $G = \{1 \cdot \mathbb{R}^{\times 2}, -1 \cdot \mathbb{R}^{\times 2}\} \cong \mathbb{Z}/2\mathbb{Z}$.

(iii) If (K, v) is non-archimedean, then the cardinality $\left[K^\times : K^{\times 2}\right]$ of G equals $4q^{\nu(2)}$.

Remark. We specialize the observations made in Rmk. §3.(6).

(1) Part (i) of Thm. II.§4 tells us that any regular finite-dimensional quadratic space (V, q) over $\mathbb{C}$ is isomorphic to $\langle 1\rangle \perp ... \perp \langle 1\rangle$, hence *all regular spaces of the same dimension $n < \infty$ over $\mathbb{C}$ are isomorphic to each other.*

(2) From part (ii) of Thm. II.§4 we retrieve **Sylvester's law of inertia**: if (V, q) is a regular finite-dimensional quadratic space over $\mathbb{R}$, then there exist nonnegative integers r, s with

$$V \cong \underbrace{\langle 1\rangle \perp ... \perp \langle 1\rangle}_{r \text{ times}} \perp \underbrace{\langle -1\rangle \perp ... \perp \langle -1\rangle}_{s \text{ times}}.$$

Note that, if (V, q) has another decomposition with a different pair (r', s'), then using Witt's Cancellation Theorem we obtain an isometry between a space of the form $\langle 1, ..., 1\rangle$ and a space of the form $\langle -1, ..., -1\rangle$, which is absurd since the former represents 1 while the latter does not. This shows that the pair (r, s) is uniquely determined; it is called the *signature* of (V, q). It also follows immediately that two quadratic spaces over $\mathbb{R}$ are isomorphic if and only if they have the same signature. ◇

Parts (i) and (ii) of the theorem are clear. We have opted to defer the proof of (iii) to the end of this section; this is because some of the auxiliary results which we use in the proof are needed again later on and thus best presented individually.

We henceforth suppose that (K, v) is non-archimedean, unless stated otherwise. The first result we need is *Hensel's Lemma*, which allows one to find roots of polynomials over $\mathfrak{o}$ by "lifting" roots over $k = \mathfrak{o}/\mathfrak{m}$. We introduce the following notation: for $a \in \mathfrak{o}$,

we use $\overline{a}$ to denote the image of a under the canonical quotient map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$. For $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathfrak{o}[t]$ we write accordingly $\overline{f}(t) = \sum_{i=0}^{d} \overline{a_i} t^i \in k[t]$.

Proposition II.§4 (Hensel's Lemma)**.** *Let $f(t) = \sum_{i=0}^{d} a_i t^i \in \mathfrak{o}[t]$.*

(i) If $\overline{f}$ factors over k, $\overline{f} = gh$ with $g, h \in k[t]$ relatively prime[6]*, then $f = GH$ for polynomials $G, H \in \mathfrak{o}[t]$ with $\overline{G} = g$, $\overline{H} = h$ and $\deg G = \deg g$.*

(ii) If $\overline{f}$ has a simple root $a \in k$, then f has a root $c \in \mathfrak{o}$ with $\overline{c} = a$.

Proof. (i) We construct sequences $(g_k)_{k\geq 0}$, $(h_k)_{k\geq 0}$, $(r_k)_{k\geq 0}$, $(s_k)_{k\geq 0}$ of polynomials over $\mathfrak{o}$ with the property that, for all k:

$f - g_k h_k \in \pi^{k+1}\mathfrak{o}[t]$;
$g_k r_k + h_k s_k \in 1 + \pi\mathfrak{o}[t]$;
$g_{k+1} - g_k$, $h_{k+1} - h_k \in \pi^{k+1}\mathfrak{o}[t]$;
$\deg g_k = \deg g_0$.

For $k = 0$, choose $g_0, h_0, r_0, s_0 \in \mathfrak{o}[t]$ so that $\overline{g_0} = g$, $\overline{h_0} = h$ and $g\overline{r_0} + h\overline{s_0} = 1$ in $k[t]$ (this is possible by assumption); then the above properties are clearly satisfied.

We now proceed to define g_{k+1}, h_{k+1}, r_{k+1}, s_{k+1} from given g_k, h_k, r_k, s_k. Set $u = (f - g_k h_k)/\pi^{k+1}$; then u lies in $\mathfrak{o}[t]$ by assumption. If we perform polynomial division of $r_k u$ by g_k, we obtain $r_k u = g_k q + r$ for some $q, r \in \mathfrak{o}[t]$ such that $\deg r < \deg g_k$. Now set $r_{k+1} := r$, $s_{k+1} := s_k u + q h_k$, $g_{k+1} := g_k + \pi^k r_{k+1}$, $h_{k+1} := h_k + \pi^k s_{k+1}$. Note that $\deg g_{k+1} = \deg g_k = \deg g_0$; the other properties are verified just as easily.

Let b_{ki} denote the coefficient of t^i in g_k. For each i, the sequence $(b_{ki})_{k\geq 0}$ is Cauchy since $g_n - g_m \in \pi^{m+1}\mathfrak{o}[t]$ whenever $n \geq m$; set $G(t) = \sum_{i=0}^{\deg g_0} (\lim_{k\to\infty} b_{ki})\, t^i$. One now constructs $H(t)$ analogously and easily verifies the required properties.

(ii) By assumption, we can write $\overline{f} = gh$ where $g(t) = t - a$; since a is a simple root, $g(t)$ and $h(t)$ are relatively prime. Now proceed as in the proof of (i); note that all the g_k's have the same leading coefficient, so if $g_0(t)$ is chosen monic, then G will necessarily be of the form $G(t) = t - c$ for some $c \in \mathfrak{o}$ with $\overline{c} = a$. □

Using Hensel's Lemma, we can prove the following result. In order to state it, we introduce the notation $U_r := 1 + \mathfrak{m}^r$ for $r \geq 1$. Note that U_r is an open ball around 1 for all r and that $\mathfrak{u} \supseteq U_1 \supseteq U_2 \supseteq \ldots$.

Corollary II.§4 (Local Square Theorem)**.** *Let $s = \nu(2)$. Then $U_{s+1}^2 = U_{2s+1}$.*

Proof. We write $U_{s+1} = 1 + \mathfrak{m}^{\nu(2)} \cdot \mathfrak{m} = 1 + (2\mathfrak{o}) \cdot \mathfrak{m}$ simply as $1 + 2\mathfrak{m}$, and analogously $U_{2s+1} = 1 + 4\mathfrak{m}$. Since $(1 + 2\mathfrak{m})^2 \subseteq 1 + 4\mathfrak{m} + 4\mathfrak{m}^2 = 1 + 4\mathfrak{m}$, it remains to show that for every $a \in \mathfrak{o}$ there exists $b \in \mathfrak{o}$ with $1 + 4\pi a = (1 + 2\pi b)^2$, i.e., b is a root of

[6] Recall that two polynomials g, h are *relatively prime* if there exist polynomials r, s with $gr + hs = 1$. Over fields, this is equivalent to g, h having no common factor of degree greater than zero.

$f(t) = \pi t^2 + t - a \in \mathfrak{o}[t]$. But $\overline{f}(t) = t - \overline{a} \in k[t]$ has a simple root over k, so f has a root $b \in \mathfrak{o}$ by Hensel's Lemma. $\square$

REMARK. (3) If (K, v) is an *arbitrary* local field, then $K^{\times 2}$ is open in K. Indeed, this is obvious if (K, v) is archimedean. Otherwise, let $x = y^2 \in K^{\times 2}$. Then $K^{\times 2}$ contains the open ball $xU_{2s+1} = (yU_{s+1})^2$ around x by the Local Square Theorem. $\diamond$

We now present the proof of Thm. II.§4.(iii), as anticipated earlier.

Proof of Thm. II.§4.(iii). We start with the following elementary result from group theory: if A, B are groups, $\varphi : A \to B$ is a group homomorphism and $H \subseteq A$ is a subgroup, then the index $[A : H]$ of H in A equals $[\ker\varphi : \ker\varphi|_H][\varphi(A) : \varphi(H)]$. Indeed, by the isomorphism theorems we have $[\ker\varphi : \ker\varphi|_H] = [\ker\varphi : \ker\varphi \cap H] = [H \ker\varphi : H]$ as well as $[\varphi(A) : \varphi(H)] = [\varphi(A) : \varphi(H \ker\varphi)] = [A : H \ker\varphi]$.

Now let $A = K^\times$, $B = \mathbb{R}_{\geq 0}$, $\varphi : A \to B$, $x \mapsto |x|$, where $|\cdot|$ is the normalized absolute value of (K, v), and $H = K^{\times 2}$. We obtain

$$\begin{aligned}\left[K^\times : K^{\times 2}\right] &= \left[\left|K^\times\right| : \left|K^{\times 2}\right|\right]\left[\mathfrak{u} : \mathfrak{u}^2\right] \\ &= 2\left[\mathfrak{u} : \mathfrak{u}^2\right]\end{aligned}$$

since $\left|K^\times\right| / \left|K^{\times 2}\right| \cong \mathbb{Z}/2\mathbb{Z}$; thus, it suffices to show that $\left[\mathfrak{u} : \mathfrak{u}^2\right] = 2q^{\nu(2)}$.

To that end, we again use the above group-theoretic result with $A = B = \mathfrak{u}$, $\varphi : A \to B$, $x \mapsto x^2$ and $H = U_{s+1}$ where $s = \nu(2)$. Note that $\ker\varphi = \{1, -1\}$ but $\ker\varphi|_H = \{1\}$, for if -1 lay in H then we would have $2 \in 2\mathfrak{m}$, i.e. $1 \in \mathfrak{m}$, which is absurd. Thus,

$$[\mathfrak{u} : U_{s+1}] = 2\left[\mathfrak{u}^2 : U_{s+1}^2\right] = 2\left[\mathfrak{u}^2 : U_{2s+1}\right]$$

by the Local Square Theorem. Multiplying the leftmost and rightmost side by $\left[\mathfrak{u} : \mathfrak{u}^2\right]$ and then dividing by $[\mathfrak{u} : U_{s+1}]$, we obtain $\left[\mathfrak{u} : \mathfrak{u}^2\right] = 2\left[U_{s+1} : U_{2s+1}\right]$ by the isomorphism theorems.

Finally, we compute the index on the right-hand side. For $r = s+1, ..., 2s$ consider the group homomorphism from U_r to the additive group k^+ of k which sends x to $\overline{(x-1)/\pi^r}$ (note that the quantity under the horizontal bar lies in $\mathfrak{o}$ by definition of U_r). This homomorphism is onto and has kernel U_{r+1} for each r, hence

$$[U_{s+1} : U_{2s+1}] = [U_{s+1} : U_{s+2}] \cdots [U_{2s} : U_{2s+1}] = \underbrace{\#k \cdots \#k}_{s=\nu(2) \text{ times}}$$

and the proof is completed. $\square$

REMARK. (4) Suppose that $1 = u_0, u_1, ..., u_{l-1} \in \mathfrak{u}$ form a set of representatives for $\mathfrak{u}/\mathfrak{u}^2$. We saw in the proof of Thm. II.§4.(iii) that $\left[K^\times : K^{\times 2}\right] = 2\left[\mathfrak{u} : \mathfrak{u}^2\right]$; we claim that $1, u_1, ..., u_{l-1}, \pi, \pi u_1, ..., \pi u_{l-1} \in \mathfrak{o}$ form a set of representatives for $K^\times/K^{\times 2}$.

Indeed, suppose that $\pi u_i K^{\times 2} = u_j K^{\times 2}$ for some i, j. Then $\pi u_i/u_j$ is the square of some $x \in K^\times$. But then $2\nu(x) = \nu(x^2) = \nu(\pi u_j/u_j) = 1$ which is absurd. On the other hand, if $\pi u_i K^{\times 2} = \pi u_j K^{\times 2}$ then $u_i K^{\times 2} = u_j K^{\times 2}$ and hence $i = j$ by assumption. $\diamond$

EXAMPLE. Let $K = \mathbb{Q}_2$ be the field of 2-adic numbers introduced in I.§5. In this case, the residue field $k = \mathbb{F}_2$ has characteristic 2, and so $\nu(2) > 0$; in fact, $\nu(2) = 1$. Note that, since k has precisely one nonzero element, $\mathfrak{u}$ coincides with $1 + \mathfrak{m} = U_1$. Now each $x \in \mathfrak{u}$ lies either in U_2 or in $-1 \cdot U_2$, thus $\mathfrak{u}^2 = U_2^2$. The Local Square Theorem then yields $\mathfrak{u}^2 = U_3$, i.e., $x \in \mathbb{Z}_2^\times$ *is a square if and only if* $x \equiv 1 \mod 8$.[7]

We now compute a set of representatives for $\mathfrak{u}/\mathfrak{u}^2 = U_1/U_3$. We already know a set of representatives for U_1/U_2, namely $1, -1$; moreover, we see that $U_2 = U_3 \cup 5 \cdot U_3$, hence $\pm 1, \pm 5$ is a set of representatives for U_1/U_3. By Rmk.(4), $\pm 1, \pm 2, \pm 5, \pm 10$ is a set of representatives for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. $\diamond$

The non-archimedean local field (K, v) is called *dyadic* if $\nu(2) > 0$, or equivalently if $\chi(k) = 2$, and *nondyadic* otherwise. In the nondyadic case, we know from Ex. §2 that $k^{\times 2} \subsetneq k^\times$, so there exists some element $u \in \mathfrak{u}$ with $\overline{u} \notin K^{\times 2}$. Then the proof of Thm. II.§4.(iii) tells us that $\mathfrak{u}/\mathfrak{u}^2$ consists precisely of the two classes $1 \cdot \mathfrak{u}^2$, $u \cdot \mathfrak{u}^2$.

We conclude this chapter by proving that the binary quadratic space $\langle u, u\rangle$ over (K, v) represents 1, a result which will be needed later on. The key observation is that the binary space $\langle \overline{u}, \overline{u}\rangle$ over the residue field k represents 1, as shown in Ex. §2, so there exist $x, y \in \mathfrak{o}$ with $\overline{u}\,\overline{x}^2 + \overline{u}\,\overline{y}^2 = 1$. Now we find that $x \in \mathfrak{u}$, for if x lay in $\mathfrak{m}$, then $\overline{u} = 1/\overline{y}^2$ would be a square in k, contradicting our choice of u. Thus, if we write $ux^2 + uy^2 - 1 = \pi z \in \mathfrak{m}$ for some $z \in \mathfrak{o}$, then $ux^2(1 + z'\pi) + uy^2 = 1$, where $z' = -\frac{z}{ux^2} \in \mathfrak{o}$. Since $\nu(2) = 0$, the Local Square Theorem shows that $1 + z'\pi \in K^{\times 2}$, so $1 + z'\pi = t^2$ for some $t \in K^\times$. But then $u(xt)^2 + uy^2 = 1$, so $\langle u, u\rangle$ represents 1 as claimed.

[7]For a more thorough explanation of the notation $x \equiv 1 \mod 8$, see footnote 2 in Chapter IV.

III. Invariants of quadratic spaces

In this chapter, we continue our study of quadratic spaces by associating certain algebras to them. The investigation of these algebras will lead us to define *(isometry) invariants* of quadratic spaces, i.e. quantities which do not depend on the diagonalization (cf. Rmk. II.§2.(1), Rmk. II.§3.(6)) of the space in question.

§1. The Brauer group

The chief purpose of the present section is to introduce the Brauer group, which will be key in the definition of the Hasse invariant in §4. In order to do so, we shall first need a few facts about central simple algebras over fields.

Recall that an *algebra* over a field F is a vector space A over F equipped with a product $\cdot : A \times A \to A$ which is F-bilinear (cf. II.§1). We shall mostly be concerned with *associative* algebras A, where the aforementioned product satisfies the associativity law; such an algebra is then automatically a ring[1]. The algebra A is called *commutative* if the bilinear product $\cdot$ is symmetric, and *unital* if it has a multiplicative identity 1.

Finally, an *algebra homomorphism* $\varphi : A \to B$ between F-algebras A and B is an F-linear map with $\varphi(xy) = \varphi(x)\varphi(y)$ for $x, y \in A$; two algebras are isomorphic if there exists an *algebra isomorphism*, i.e. a bijective algebra homomorphism, between them.

Example. (1) Let $F \subseteq E$ be a field extension. Then E is an algebra over F; it is unital, associative and commutative.

(1') If E is a skew field containing F, then everything holds as in (1) except for commutativity. In order to treat the commutative and noncommutative case jointly, one defines a *division algebra* over F to be a unital associative[2] algebra D over F such that for each $0 \neq x \in D$ there exists $x^{-1} \in D$ with $xx^{-1} = x^{-1}x = 1_D$.

(2) The ring $M_n(F)$ of $n \times n$-matrices over a field F is a unital associative algebra over F, but it is not commutative except for $n = 1$.

(2') Let V be a vector space over a field F, and let $\mathrm{End}(V) = \mathrm{End}_F(V)$ denote the space of F-linear maps from V to V. Then composition of maps makes $\mathrm{End}(V)$ into a

[1] In contrast to our usual convention, this ring need not be commutative or unitary.

[2] There is also a concept of non-associative division algebras, but we will not go into that here.

unital associative algebra over F; if V has finite dimension n over F, then $\dim \mathrm{End}(V) = n^2$. Upon choosing a basis for V we obtain an algebra isomorphism $\mathrm{End}(V) \cong M_n(F)$ by elementary linear algebra.

(3) Euclidean space $\mathbb{R}^3$ with the cross product $\times$ is an algebra over $\mathbb{R}$. Note that $\times$ is not associative; instead, it satisfies the so-called *Jacobi identity*

$$u \times (v \times w) = (u \times v) \times w + v \times (u \times w).$$

(Real) algebras whose multiplication satisfies this equality are known as *Lie algebras*. $\diamond$

For the rest of this section, let the ground field F be fixed. All algebras over F are assumed to be associative, unital and finite-dimensional (as vector spaces over F) unless explicitly stated otherwise. Under these assumptions, we are able to identify F with the subspace $F1_A \subseteq A$ and will tacitly do so throughout.

Given an algebra A over F, the *centre* of A, denoted $Z(A)$, is the set of elements of A which commute with every other element of A, i.e., $Z(A) = \{x \in A : xy = yx \text{ for all } y \in A\}$. Clearly, $F = F1_A \subseteq Z(A)$; we call A *central* if equality holds.

Next, a subspace of A is called a *left ideal* if it is a left ideal of the underlying ring, and analogously for right ideals; a subspace which is both a left ideal and a right ideal is a *two-sided ideal*. The algebra A is *simple* if its only two-sided ideals are the trivial ones, namely $\{0\}$ and A itself.

Finally, an algebra over F which is both central and simple is called a central simple algebra (CSA) over F.

Example. (4) Any division algebra D over a field F, see (1'), is trivially simple. Its centre is automatically a field containing F.

(5) Consider $A = M_n(F)$ as in (2). It is a well-known fact that the only elements in $Z(A)$ are the scalar multiples of 1_A, thus A is central.

We now prove that A is simple. Indeed, let $I \subseteq A$ be a two-sided ideal. We show that, if I contains a nonzero matrix $M = (m_{ij})_{1 \leq i,j \leq n}$, then $I = A$. Indeed, for $1 \leq i, j \leq n$ let E_{ij} denote the matrix which has a 1 in the j-th slot of its i-th row and 0's everywhere else. If, say, $m_{ij} \neq 0$, one readily computes that $E_{ll} = (m_{ij}^{-1} E_{li}) M E_{jl} \in I$ for any $1 \leq l \leq n$, thus $1_A = E_{11} + ... + E_{nn} \in I$. $\diamond$

The next step towards the construction of the Brauer group is to define an equivalence relation on the set of CSAs over F. In preparation for that, we briefly review some basic facts regarding tensor products of vector spaces.

Recall that, given vector spaces V, W over F, there exist an F-vector space $V \otimes_F W$ and a bilinear map $\beta : V \times W \to V \otimes_F W$, $(v, w) \mapsto v \otimes w$ with the following universal property: for every bilinear map $\varphi : V \times W \to U$, where U is any F-vector space, there

exists a unique linear map $\overline{\varphi} : V \otimes_F W \to U$ with $\varphi = \overline{\varphi} \circ \beta$. As with all objects defined via a universal property, $V \otimes_F W$ is unique up to a (linear) isomorphism; it is called the *tensor product* of V and W (over F).

REMARK. (1) The map β from above is not surjective in general; however, each element of $V \otimes_F W$ is a finite linear combination of so-called "pure tensors" $v \otimes w$. Thus, choosing a basis $\{b_j\}$ of W we obtain a unique representation of each $t \in V \otimes_F W$ as $t = \sum_j v_j \otimes b_j$ where $v_j \in V$ for all j. If we choose a basis $\{a_i\}$ of V, then t has a unique representation $t = \sum_{i,j} c_{ij} a_i \otimes b_j$ for $c_{ij} \in F$. In particular, $\dim(V \otimes_F W) = \dim V \cdot \dim W$.

(2) For arbitrary vector spaces V, W, U over F, there are canonical linear isomorphisms $V \otimes_F W \cong W \otimes_F V$ and $(V \otimes_F W) \otimes_F U \cong V \otimes_F (W \otimes_F U)$, which we shall henceforth treat as identifications.

(3) For given V, define $T^0 V := F$ and $T^n V := T^{n-1} V \otimes_F V$ for $n \geq 1$. Consider now the infinite direct sum $TV := \bigoplus_{n \geq 0} T^n V$. The assignment $(v_1 \otimes ... \otimes v_k) \cdot (u_1 \otimes ... \otimes u_l) := v_1 \otimes ... \otimes v_k \otimes u_1 \otimes ... \otimes u_l$ can be extended uniquely to a bilinear product on TV which makes TV into a unital associative (infinite-dimensional) algebra over F, the so-called *tensor algebra* of V.

(4) If (V, q), (V', q') are quadratic spaces over F, then the assignment $v \otimes v' \mapsto q(v) \cdot q'(v')$ can be extended to a map $q \otimes q' : V \otimes_F V' \to F$ which is easily checked to be a quadratic form on $V \otimes_F V'$.

(5) If A, B are (unital associative) algebras over F, then $(a \otimes b)(a' \otimes b') := aa' \otimes bb'$ induces a product which makes $A \otimes_F B$ into a (unital associative) algebra over F. $\diamond$

Two CSAs A, B over F are said to be *similar*, in symbols $A \sim B$, if there exist positive integers r, n such that $A \otimes_F M_r(F)$ and $B \otimes_F M_n(F)$ are isomorphic as F-algebras, cf. Ex.(2) for the notation. This is indeed an equivalence relation: to check transitivity, note that $M_r(F) \otimes_F M_n(F) \cong M_{rn}(F)$ for all $n, r \geq 1$.

We use $[A]$ to denote the equivalence class of A with respect to $\sim$ and $B(F)$ to denote the set of equivalence classes. The following lemma shows that $[A] \cdot [B] := [A \otimes_F B]$ yields a well-defined operation on $B(F)$, cf. also Rmk.(5); by Rmk.(2), this operation is associative and commutative. The element $[F]$ ($= [M_n(F)]$ for any $n \geq 1$) serves as a multiplicative unit, so $B(F)$ is a monoid. Proposition III.§1 below shows that $B(F)$ is even a group, the so-called *Brauer group* of F.

We now proceed to prove both the lemma and the proposition.

Lemma III.§1. *Let A, B be CSAs over F. Then $A \otimes_F B$ is again a CSA over F.*

Proof. We first show that $A \otimes_F B$ is central. For let $z \in Z(A \otimes_F B)$, $z = \sum_j v_j \otimes b_j$ where b_j form a basis of B and $v_j \in A$, cf. Rmk.(1). For any $a \in A$ we have $z(a \otimes 1_B) = (a \otimes 1_B) z$, which translates into $a v_j = v_j a$ for all j, hence $v_j \in Z(A) = F$ for all j. By linearity and

distributivity, we can now write $z = 1_A \otimes b$ for some $b \in B$. Applying a similar procedure as above, we find that $b \in Z(B)$, hence $z \in F = F(1_A \otimes 1_B)$.

Now let I be a nonzero two-sided ideal of $A \otimes_F B$, and again let $\{b_j : j = 1, ..., m\}$ be a basis of B. Let $x = \sum_j v_j \otimes b_j$ be a nonzero element of I, where $v_j \in A$ for all j; if, say, $v_1 \neq 0$, then 1_A lies in the two-sided ideal generated by v_1 in A by simplicity of A, hence we can find some nonzero element $y \in I$ of the form $y = 1 \otimes b_1 + \sum_{j=2}^m v'_j \otimes b_j$ for some v'_j. Pick $a \in A$; then $z = (a \otimes 1_B)y - y(a \otimes 1_B)$ is again an element of I, and $z = \sum_{j=2}^m u_j \otimes b_j$ for appropriate u_j's. Iterating, we find that I must contain an element of the form $1_A \otimes b$ for some $0 \neq b \in B$. But then we obtain $1_A \otimes 1_B \in I$ by simplicity of B, hence $I = A$ and $A \otimes_F B$ is simple. □

Proposition III.§1. *The monoid $B(F)$ defined above is a group.*

Proof. Let A be a CSA over F, and set $n = \dim_F A$. It suffices to show that there exists some CSA B over F with $A \otimes_F B \cong M_r(F)$ for some r.

Consider now the *opposite algebra* A^{op} of A. Intuitively, this is the algebra obtained by equipping the underlying set of A with the "reversed multiplication" $x \odot y := y \cdot x$; formally, we define $A^{\mathrm{op}} := \{a^{\mathrm{op}} : a \in A\}$ and $a^{\mathrm{op}} \cdot b^{\mathrm{op}} := (b \cdot a)^{\mathrm{op}}$. Clearly, the centre of A^{op} is just $\{a^{\mathrm{op}} : a \in Z(A)\}$, and each two-sided ideal of A^{op} must be of the form $I^{\mathrm{op}} = \{a^{\mathrm{op}} : a \in I\}$ for some two-sided ideal I of A; thus, A^{op} is again a CSA over F.

Let $T := A \otimes_F A^{\mathrm{op}}$. For $a, b \in A$ we can define $\psi(a \otimes b^{\mathrm{op}})$ to be the map $x \mapsto axb$ in $\mathrm{End}(A)$ and then extend ψ to an algebra homomorphism $\psi : T \to \mathrm{End}(A)$. The kernel of ψ is necessarily a proper ideal of T; but T is simple by the above lemma, so ψ is injective. From $\dim_F T = n^2 = \dim_F \mathrm{End}(A)$ we deduce that ψ is an isomorphism. Finally, we use the isomorphism $\mathrm{End}(A) \cong M_n(F)$ from Ex.(2') to verify that $[A] \cdot [A^{\mathrm{op}}] = [M_n(F)] = 1 \in B(F)$, as claimed. □

We conclude this section with a fundamental structure theorem for (finite-dimensional) CSAs over fields, which incidentally yields an alternative description of the Brauer group.

Theorem III.§1 (Wedderburn's Theorem)**.** *Let A be a CSA over F. Then there exist a positive integer n and a central division algebra D over F such that $A \cong M_n(F) \otimes_F D$. Moreover, n is uniquely determined and D is unique up to algebra isomorphism.*

Proof. See e.g. [GiSz06]. □

Corollary III.§1. *Let A be a CSA over F. Then:*

(i) The class $[A] \in B(F)$ contains, up to isomorphism, exactly one division algebra.

(ii) If B is another CSA over F with $\dim_F A = \dim_F B$, then $A \sim B$ iff $A \cong B$.

(iii) If $\dim_F A \leq 4$, then A is either isomorphic to $M_2(F)$ or a division algebra.

Proof. By Wedderburn's Theorem, we can write $A \cong M_n(D)$ for some $n \geq 1$ and some division algebra D over F; let D be fixed for the rest of this proof.

(i) It is clear that $D \in [A]$. If D' is a division algebra with $D' \in [A]$, then $M_r(F) \otimes_F D' \cong M_k(F) \otimes_F A \cong M_{nk}(F) \otimes_F D$ for some $r, k \geq 1$, and by the uniqueness part of Wedderburn's Theorem we obtain $nk = r$ and $D' \cong D$.

(ii) Clearly, isomorphic algebras are always similar. As for the converse, note that by part (i), there exists some $m \geq 1$ with $B \cong M_m(D)$. Comparing dimensions over F, one sees that m must be equal to n, thus $B \cong A$ as claimed.

(iii) One has $4 \geq \dim_F A = n^2 \dim_F D$, cf. Rmk.(1), thus either $n = 2$ (in which case $\dim_F D = 1$, i.e. $D = F$) or $n = 1$ and accordingly $A \cong D$. □

In particular, Cor. III.§1.(i) shows that the elements of $B(F)$ are in 1-1 correspondence with the isomorphism classes of central division algebras over F.

§2. Quaternion algebras

In this section, we specialize to quaternion algebras. As in the preceding section, the ground field F is fixed and all algebras over F are assumed to be unital, associative and finite-dimensional unless explicitly stated otherwise.

We define a *quaternion algebra* over F to be a central simple algebra of dimension 4 over F. By Cor. III.§1.(iii), a quaternion algebra is either isomorphic to $M_2(F)$ or a central division algebra, and by Cor. III.§1.(iii) two quaternion algebras are similar if and only if they are isomorphic.

The following result yields a useful characterization of quaternion algebras in characteristic $\neq 2$, cf. Rmk. I.§2.(3).

Proposition III.§2. *Let F be a field of characteristic $\neq 2$, and let A be an algebra of dimension 4 over F. Then A is a quaternion algebra over F if and only if it has a* quaternion basis *over F, i.e. a basis $1 = 1_A, i, j, k$ with $i^2, j^2 \in F^\times 1$ and $k = ij = -ji$.*

Proof. ($\Leftarrow$) Let $1, i, j, k$ be a quaternion basis of A. We first show that A is simple. Let $I \subset A$ be a two-sided ideal which contains some $x \neq 0$; we have to show $1 \in I$. This is trivial if $x \in F^\times$, so suppose that $x = \alpha + \beta i + \gamma j + \delta k$ with, say, $\beta \neq 0$. Then $y := \frac{1}{2ab}(kx - xk)k = \beta i + \gamma j$ lies in I, where we have set $a = i^2$, $b = j^2$; accordingly, $\frac{1}{2a\beta}(yi + iy) = 1 \in I$.

Next, we show that A is central. Indeed, if $x = \alpha + \beta i + \gamma j + \delta k$ commutes with k, then $\beta i + \gamma j = 0$ by the above computation, hence by linear independence of i, j we obtain $\beta = \gamma = 0$. A similar argument with j in place of k yields: if $x \in Z(A)$, then $x \in F$.

($\Rightarrow$) If $A = M_2(F)$, then $1_A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $j = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right)$ and $k = \left(\begin{smallmatrix} 0 & -b \\ 1 & 0 \end{smallmatrix}\right)$ form a basis for A over F for any $b \in F^\times$; they satisfy $i^2 = 1_A$, $j^2 = b1_A$ and $k = ij = -ji$ as

required. Thus, we henceforth suppose that A is not isomorphic to $M_2(F)$. But then A is a division algebra D by the above observations.

For each $x \in D$, the subspace $F(x)$ spanned by $1, x, x^2, ...$ is a subfield of D, cf. I.§7, and $\dim_F D = \dim_F F(x) \cdot \dim_{F(x)} D$. Necessarily $\dim_F F(x) \neq 4$, for otherwise $D = F(x)$ would be commutative, but $Z(D) \subsetneq D$. Thus, if $\alpha \notin F$ then $F(\alpha)$ has degree 2 over F. If $f(t) = t^2 + pt + q$ is the minimal polynomial of α over F, then $i = 2\alpha + p$ is an element of $F(\alpha) \setminus F$ whose square equals the discriminant $\Delta \in F^\times$ of $f(t)$.

We define $\varphi : A \to A$, $x \mapsto \frac{1}{\Delta} ixi$; since $\varphi \circ \varphi = \mathrm{Id}_D$, each eigenvalue of φ is either $+1$ or -1. The eigenspace E_1 corresponding to 1 is precisely the set of $y \in A$ which commute with i; we can argue as above that its dimension must be precisely 2, hence $E_1 = F(i)$. It follows that the other eigenspace E_{-1} is non-empty, i.e., there exists $0 \neq j \in A$ with $ij = -ji$. Since $ij^2 = -jij = j^2 i$, we have $j^2 \in E_1 = F(i)$. On the other hand, $F(j)/F$ is necessarily again an extension of degree 2, so $j^2 + cj - b = 0$ for some $b, c \in F$. But then $cj = b - j^2 \in F(i)$, which implies $c = 0$ and thus $j^2 = b \in F^\times$. Since $k = ij \in E_{-1}$, the elements j, k form a basis for E_{-1}, hence $1, i, j, k$ form a basis for $E_1 \oplus E_{-1} = D$. □

For the remainder of this section, we **assume that F has characteristic $\neq 2$.**

Example. (1) Let $A = F^4$ with the standard basis[3] e_0, e_1, e_2, e_3. Note that a bilinear product $\cdot$ on A is uniquely determined by the values of $e_l \cdot e_m$ for all $0 \leq l, m \leq 3$; conversely, *any* choice of these sixteen values yields a bilinear operation $\cdot$ on A.

Now let $a, b \in F^\times$, and consider the following equations: $e_0 \cdot e_l = e_l \cdot e_0 = e_l$ for all l, $e_1^2 = ae_0$, $e_2^2 = be_0$ and $e_1 e_2 = -e_2 e_1 = e_3$. If we demand that $\cdot$ be associative, then the value of $e_l \cdot e_m$ is uniquely determined for all l, m, hence $\cdot$ makes A into a quaternion algebra over F by Prop. III.§2. This quaternion algebra is commonly denoted $\left(\frac{a,\ b}{F}\right)$ or $\big(a, b \mid F\big)$, or even (a, b) when there is no risk of confusion.

(1') The real algebra $\big(-1, -1 \mid \mathbb{R}\big)$ is denoted $\mathbb{H}$ after the Irish mathematician William Rowan Hamilton, who famously carved the equation $i^2 = j^2 = k^2 = ijk = -1$ on a stone of Broom Bridge on the day it occurred to him, 16 October 1843; the elements of $\mathbb{H}$ are known as *(Hamilton's) quaternions*. Note that, if we identify the subspace spanned by $e_1 = i, e_2 = j, e_3 = k$ with Euclidean space $\mathbb{R}^3$, then $e_l \cdot e_m = e_l \times e_m$ for $l \neq m$, where $\times$ denotes the cross product from Ex. §1.(3). ◇

Remark. We make a few observations regarding algebras of the form $\left(\frac{a,\ b}{F}\right)$, cf. Ex.(1).

(1) Let A be a quaternion algebra over F, and let $1, i, j, k$ be a quaternion basis for A. Set $a = i^2$, $b = j^2 \in F^\times$. Then there is an algebra isomorphism $A \to \big(a, b \mid F\big)$ given by sending $1, i, j, k$ to the standard basis vectors e_0, e_1, e_2, e_3 of F^4 respectively.

[3]The vector e_l has a 1 in its $(l+1)$-th component and 0's everywhere else.

(1') We saw in the proof of Prop. III.§2 that $A \cong M_2(F)$ if and only if $A \cong \big(1, b \mid F\big)$ for some $b \in F^\times$.

(2) Let $a, b \in F^\times$, $A = \big(a, b \mid F\big)$, and denote the standard basis vectors e_0, e_1, e_2, e_3 by $1, i, j, k$ respectively. Then an algebra homomorphism $A \to A'$ is uniquely determined by the images of i and j. For instance, the permutation $i \mapsto j$, $j \mapsto i$ (as a map $F^4 \to F^4$) yields $A \xrightarrow{\cong} \big(b, a \mid F\big)$. Similarly, $A \cong \big(a, -ab \mid F\big)$ via $i \mapsto i$, $j \mapsto k$. Finally, for $c, d \in F^\times$ one finds $A \cong \big(ac^2, bd^2 \mid F\big)$ via $i \mapsto ci$, $j \mapsto dj$. ◇

We now introduce the concept of a composition algebra over F. Let A be a unital (not necessarily associative) algebra over F, and suppose that A has an *involution (of the first kind)*, i.e. an F-linear map $A \to A$, $x \mapsto \overline{x}$ which satisfies $\overline{\overline{x}} = x$ and $\overline{x \cdot y} = \overline{y} \cdot \overline{x}$ for all $x, y \in A$. (Note that F-linearity also implies $\overline{a} = a$ for all $a \in F$.) Suppose further that, for each $x \in A$, the element $x + \overline{x}$ lies in $F = F1_A$, and denote $\mathrm{T} : A \to F$, $x \mapsto x + \overline{x}$. Then T is again F-linear; we call it the *trace form* of A.

Consider the map $A \times A \to F$, $(x, y) \mapsto \frac{1}{2}\mathrm{T}(x\overline{y})$. This is a symmetric bilinear form on A, cf. II.§1, and its associated quadratic form, cf. II.§2, is precisely $x \mapsto x\overline{x}$, which we call the *norm form* of A and denote N. We call A (more precisely, the triple $(A, {}^-, \mathrm{N})$) a *composition algebra* if the space (A, N) is nondegenerate, cf. II.§1, and if N additionally satisfies $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ for all $x, y \in A$.

Remark. (3) The term *composition algebra* is derived from the classical problem of "composing" quadratic forms, which in modern terms reads as follows: given quadratic spaces (V, q) and (U, q'), does there exist a bilinear pairing $U \times V \to V$, denoted by $(x, y) \mapsto x \cdot y$, such that $q(x \cdot y) = q'(x)q(y)$ for all $x \in U$, $y \in V$?

In the special case where the ground field is $\mathbb{R}$ and $(V, q) \cong (U, q') \cong \langle 1, ..., 1\rangle$, Adolf Hurwitz (1859-1919) was able to show that the aforementioned bilinear pairing exists if and only if $n = 1, 2, 4$ or 8. Note that the case $n = 1$ is trivial, $n = 2$ corresponds to the *two-square identity* known from antiquity, and $n = 4$ corresponds to the *four-square identity* discovered by Euler.

(4) Let A be a composition algebra over F. By multiplicativity of the norm form, an element $0 \neq x \in A$ is invertible only if $\mathrm{N}(x) \neq 0$; conversely, if $\mathrm{N}(x) \in F^\times$ then $y = \frac{1}{\mathrm{N}(x)}\overline{x}$ satisfies $xy = yx = 1$, hence $y = x^{-1}$. It immediately follows that A is a division algebra if and only if (A, N) does not represent 0; if, instead, (A, N) is isotropic, one says that A is *split* over F, or that A *splits* over F. ◇

Example. (2) Let $A = F$ and $\overline{x} := x$ for all $x \in F$. Then we have $\mathrm{N}(x) = x^2$ for all x, so (A, N) is trivially nondegenerate and N is multiplicative.

(3) Let E be an extension of F of degree $[E : F] = 2$, and let $\alpha \in E$. If $\alpha \in F$, define $\overline{\alpha} := \alpha$, otherwise let $\overline{\alpha}$ be the other root of the minimal polynomial $f_\alpha(t)$ of α over F,

i.e., $f_\alpha(t) = t^2 - (\alpha + \overline{\alpha})t + \alpha\overline{\alpha}$. We check directly that $\alpha\overline{\alpha} = N_{E/F}(\alpha)$ for all $\alpha \in E$, where $N_{E/F}$ is the norm from I.§7.

Suppose now that E is the splitting field (cf. I.§9) of a polynomial $g(t) = t^2 - b$ over F for some $b \in F^\times$. Then E contains two roots δ and $-\delta$ of $g(t)$, and by comparing dimensions we see that $F(\delta)$ is all of E, so every element $\alpha \in E$ can be written as $\alpha = c_0 + c_1\delta$ for some $c_0, c_1 \in F$. With this notation, $N_{E/F}(\alpha) = (c_0 + c_1\delta)(c_0 - c_1\delta) = c_0^2 - bc_1^2$; hence, $(E, N_{E/F})$ is a quadratic space isometric to $\langle 1\rangle \perp \langle -b\rangle$. We check that $(E, N_{E/F})$ is regular and not isotropic; moreover $N_{E/F}$ is multiplicative, as seen in I.§7, hence E is a composition algebra. $\diamond$

For a quaternion algebra A over F, set $A^\circ := \{x \in A : x^2 \in F,\ x \notin F^\times\}$. Note that, if $1, i, j, k$ is any quaternion basis of A, cf. Prop. III.§2, then A° equals precisely $Fi \oplus Fj \oplus Fk$: indeed, the right-to-left inclusion is straightforward; conversely, if $x = \alpha + \beta i + \gamma j + \delta k \in A^\circ$ with $\alpha \neq 0$ and, say, $\beta \neq 0$, then the coefficient of i in the basis representation of x^2 is $2\alpha\beta \neq 0$.

Note that there is a decomposition of A as a direct sum $A = Z(A) \oplus A^\circ$. By linear algebra, there exists a unique surjective map $P : A \to A^\circ$ with $P \circ P = P$ and $\ker P = Z(A) = F$. Then the F-linear map $A \to A$, $x \mapsto \overline{x} := x - 2P(x)$ is an involution; it is called the *canonical involution* of A, or simply *conjugation*. Note that $A^\circ = \{x \in A : \overline{x} = -x\}$ and $F = \{x \in A : \overline{x} = x\}$.

For the norm form $\mathrm{N} : A \to F$, $x \mapsto x\overline{x}$, we have $\mathrm{N}(x) = x^2$ for $x \in F$ and $\mathrm{N}(x) = -x^2$ for $x \in A^\circ$. If $1, i, j, k$ is any quaternion basis for A, then $(A, \mathrm{N}) = F1 \perp Fi \perp Fj \perp Fk$; in particular, we immediately compute $\det A = (i^2)^2(j^2)^2 \cdot F^{\times 2} = 1 \cdot F^{\times 2}$, so (A, N) is regular. Finally, an easy computation shows that N is multiplicative. We conclude that *every quaternion algebra over F is a composition algebra over F*. By Cor. III.§1.(iii), A splits, see Rmk.(4), if and only if $A \cong M_2(F)$.

Remark. (5) The above discussion shows that, if $1, i, j, k$ is a quaternion basis of A, then $A^\circ = Fi \perp Fj \perp Fk$; similarly as above, we compute $\det(A^\circ, \mathrm{N}|_{A^\circ}) = 1 \cdot F^{\times 2}$. By Cor. II.§2.(iii), we conclude that A is isotropic if and only if A° is.

(6) Let $a, b \in F^\times$, and let $A = \big(a, b \mid F\big)$. Then $(A, \mathrm{N}) \cong \langle 1, -a, -b, ab\rangle$. In particular, (A, N) is isometric to $\langle 1, -a\rangle \otimes_F \langle 1, -b\rangle$, cf. Rmk. §1.(4).

(7) Let A, A' be quaternion algebras. If $\varphi : A \to A'$ is an algebra isomorphism, then φ must carry $Z(A)$ to $Z(A')$ and A° to $(A')^\circ$ by the respective definitions; in particular, $\varphi(\overline{x}) = \overline{\varphi(x)}$ for all $x \in A$. Thus, if N' denotes the norm form of A', then one computes $\mathrm{N}'(\varphi(x)) = \varphi(\mathrm{N}(x)) = \mathrm{N}(x)$, that is to say, φ is an isometry between (A, N) and (A', N').

Conversely, suppose that there is an isometry $(A, \mathrm{N}) \to (A', \mathrm{N}')$. Then, by (6) together with Witt's Cancellation Theorem, we obtain an isometry f from A° to $(A')^\circ$. Then $f(i), f(j), f(k)$ necessarily form an orthogonal basis for $(A')^\circ$, and one verifies that

$1_{A'}, f(i), f(j), f(k)$ form a quaternion basis for A'. Thus, *two quaternion algebras are isomorphic if and only if they are isometric.* $\diamond$

§3. Clifford algebras

In the present section, we briefly review Clifford algebras of quadratic spaces; as it turns out, these are invariant under isometry, cf. the preamble of this chapter. We shall focus especially on the Clifford algebras of regular binary quadratic spaces. As in the preceding section, the ground field F is fixed and all algebras over F are assumed to be unital, associative and finite-dimensional unless explicitly stated otherwise. Moreover, we shall use the conventions, terminology and results from Chapter II rather freely; accordingly, the ground field is additionally required to have characteristic $\neq 2$, cf. Rmk. I.§2.(3), and all quadratic spaces over F are tacitly assumed to be finite-dimensional.

We start with the following definition. Given a quadratic space (V, q) over F, we say that the algebra A over F is *compatible* with (V, q) if $A \supseteq V$ and $x^2 = q(x)1_A$ for all $x \in V$. A *Clifford algebra* of (V, q) is an algebra C compatible with (V, q) which satisfies the following universal property: for every algebra C' compatible with (V, q), there exists an algebra homomorphism $\varphi : C \to C'$ which is the identity on V. If C exists, then it is unique up to isomorphism (of algebras) by the universal property and is thus referred to as "the" Clifford algebra of (V, q).

If (V, q) is regular, then it has a Clifford algebra: for let $A = TV$ denote the tensor algebra of V from Rmk. §1.(3), and let I denote the two-sided ideal of A generated by all elements of the form $x \otimes x - q(x)1_A$ for some $x \in V$. Then the quotient space $A/I =: C(V)$ is again an algebra over F; we denote its product simply by $\cdot$. The property $x^2 = x \cdot x = q(x)1_{C(V)}$ is immediate by definition of I, while the sought-after inclusion $V \subset C(V)$ comes from the map $V \overset{\cong}{\to} T^1V \subset A$.

It remains to show that $C(V)$ has the universal property of the Clifford algebra. To that end, we fix an orthogonal basis $v_1, ..., v_n$ for V and establish the following claim: any algebra homomorphism $\varphi : C(V) \to B$ to any F-algebra B is uniquely determined by the values $\varphi(v_i)$ for $i = 1, ..., n$. This claim also implies that an isometry $f : (V, q) \to (V', q')$ of quadratic spaces induces an algebra isomorphism $C(V) \overset{\cong}{\to} C(V')$; hence, *the Clifford algebra is invariant under isometry.*

We first observe that the "words" $v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_k}$ in the v_i's of arbitrary length $k \geq 0$ form a basis for TV. In $C(V)$, however, we have $v_i^2 = q(v_i)1_{C(V)} \in F^\times 1_{C(V)}$ for all i by regularity of (V, q); moreover, we readily compute that $b_q(x, y)1_{C(V)} = \frac{1}{2}(xy + yx)$ for all $x, y \in V$, and hence $v_iv_j = -v_jv_i$ whenever $i \neq j$. Using these computation rules, it is now easy to see that an F-basis for $C(V)$ is given by the products $v_{i_1}v_{i_2} \cdots v_{i_k}$ for $0 \leq k \leq n$, $1 \leq i_1 < i_2 < ... < i_k \leq n$ and the claim follows at once.

Now let (V,q) be a regular binary quadratic space over F. Then the Clifford algebra $C(V)$ of (V,q) is a quaternion algebra: indeed, if v_1, v_2 is an orthogonal basis of (V,q), then the above observations tell us precisely that $1, v_1, v_2, v_1v_2$ form a quaternion basis for $C(V)$. If $V = \langle a,b\rangle$ for $a,b \in F^\times$, then one can identify $C(V)$ with $\left(\frac{a,\ b}{F}\right)$, cf. Ex. §2.(1) as well as Rmk. §2.(1), via $v_1 \mapsto i$, $v_2 \mapsto j$.

The next theorem illustrates how some useful information about a regular binary quadratic space is already encoded in its Clifford algebra.

Theorem III.§3. *Let (V,q) be a regular binary quadratic space over F, and let $C = C(V,q)$ be its Clifford algebra. Further, let $a,b \in F^\times$ with $V = \langle a,b\rangle$, let E be a splitting field (cf. I.§9) of $f(t) = t^2 - b$ over F, and let $N_{E/F}$ be the norm of the field extension E/F, see I.§7. The following are equivalent:*

(i) (V,q) represents 1;

(i') the equation $ax_1^2 + bx_2^2 = 1$ has a solution $(x_1,x_2) \in F^2$;

(ii) C splits as a composition algebra, see Rmk. §2.(4);

(iii) There exists $\alpha \in E^\times$ with $a = N_{E/F}(\alpha)$.

Proof. Let v_1, v_2 denote an orthogonal basis of V with $q(v_1) = a$, $q(v_2) = b$. The equivalence of (i) and (i') is clear since $q(x_1v_1 + x_2v_2) = ax_1^2 + bx_2^2$ for all $x_1, x_2 \in F$. We go on to show the equivalences (i)⇔(ii) and (i)⇔(iii). Throughout the proof, we identify C with $\left(\frac{a,\ b}{F}\right)$ and use $1, i, j, k$ to denote the standard quaternion basis e_0, e_1, e_2, e_3 of C.

(i)⇒(ii): Pick an element $x \in V$ with $q(x) = 1$. Further, pick $0 \neq y \in V$ orthogonal to x and set $b' = q(y)$; since V is regular, $b' \neq 0$. Now $(V,q) \cong \langle 1, b'\rangle$; by the invariance of the Clifford algebra, $C \cong \left(1, b' \mid F\right)$. But then $C \cong M_2(F)$ by Ex. §2.(1'), and the claim follows from the observations made in §2.

(ii)⇒(i): By assumption, (C, N) is isotropic, where N denotes the norm form of C. We know from Rmk. §2.(5) that this is the case if and only if $(C^\circ, \mathrm{N}|_{C^\circ})$ is isotropic. Define $Q : C^\circ \to F$, $x \mapsto -ab\mathrm{N}(x)$; then (C°, Q) is of course again isotropic. But $(C^\circ, Q) = Fi \perp Fj \perp Fk = \langle a^2b\rangle \perp \langle ab^2\rangle \perp \langle -a^2b^2\rangle = \langle b\rangle \perp \langle a\rangle \perp \langle -1\rangle$, cf. Rmk. II.§3.(6); thus, the claim follows from Cor. II.§2.(i).

(i)⇔(iii): If $b \in F^{\times 2}$, then $E = F$, thus $N_{E/F} = \mathrm{Id}_F$, and both claims are trivially true (note that $q(x) = 1$ with $x = \frac{1}{b}v_2$). Thus, suppose that $b \notin F^{\times 2}$; then $[E:F] = 2$, so we are in the situation of Ex. §2.(3). In particular, (E,Q), where $Q : \alpha \mapsto -N_{E/F}(\alpha)$, is a quadratic space over F with $(E,Q) \cong \langle b\rangle \perp \langle -1\rangle$, and condition (iii) can be rephrased as: (E,Q) represents $-a$. But then, by Cor. II.§2.(i), both (iii) and (i) are equivalent to $\langle a\rangle \perp \langle b\rangle \perp \langle -1\rangle$ being isotropic. □

Using Cor. III.§1.(ii)-(iii), we infer that the equivalent conditions of Thm. III.§3 are satisfied if and only if $C \sim M_2(F)$, cf. §1, i.e. if and only if $[C] = 1$ in the Brauer group $B(F)$ of F. Thus, we can note a few consequences of Thm. III.§3 in terms of

computation rules for the Brauer group. For $a, b \in F^\times$, we agree to denote the similarity class of $\left(\frac{a,\ b}{F}\right)$ in $B(F)$ again by $\left(\frac{a,\ b}{F}\right)$.

Corollary III.§3. *Let $a, a', b \in F^\times$. Then:*
(i) $\left(\frac{a,\ -a}{F}\right) = 1$ *in* $B(F)$, *and if* $a \neq 1$, *then* $\left(\frac{a,\ 1-a}{F}\right) = 1$;
(ii) $\left(\frac{a,\ b}{F}\right)\left(\frac{a',\ b}{F}\right) = \left(\frac{aa',\ b}{F}\right)$ *in* $B(F)$.

Proof. (i) First, note that $\langle a, -a\rangle$ is isotropic and regular, hence universal by Thm. II.§2. Moreover, if $(V, q) = Fv_1 \perp Fv_2$ with $q(v_1) = a = 1 - q(v_2)$, then $q(v_1 + v_2) = 1$, hence V represents 1. We are now done by the equivalence (i)⇔(ii) of Thm. III.§3.

(ii) Let $A = \left(\frac{a,\ b}{F}\right)$ and $A' = \left(\frac{a',\ b}{F}\right)$. By the definition of the product in $B(F)$, we have to show that $B = A \otimes_F A'$ is similar to $\big(aa', b \mid F\big)$.

Let $e_0, ..., e_3$ and $e'_0, ..., e'_3$ denote the standard (quaternion) bases of A and A', and denote $e_{lm} := e_l \otimes e'_m$ for all l, m. By definition of the product in B, cf. Rmk. §1.(5), we immediately find $e_{00} = 1_B$, $e_{10}^2 = e_1^2 \otimes (e'_0)^2 = a$ and so on. Now let B_1 denote the subalgebra spanned by $1_B, e_{11}, e_{20}, e_{31}$. It is a matter of computation to show that these elements form a quaternion basis for B_1; by Rmk. §2.(1) we obtain an isomorphism $B_1 \xrightarrow{\cong} \big(aa', b \mid F\big)$. Analogously, the elements $1_B, e_{01}, e_{23}, -a'e_{22}$ form a quaternion basis for the subalgebra B_2 which they span, thus $B_2 \cong \big(a', -a'b^2 \mid F\big)$.

Next, we claim that $B \cong B_1 \otimes_F B_2$. Observe that each of e_{11} and e_{20} commutes with each of e_{01} and e_{23}, so the algebras B_1, B_2 commute element-wise. Moreover, an easy, if tedious, computation shows that each e_{lm} can be obtained as a scalar multiple of the product of some basis element of B_1 with some basis element of B_2.

Consider the bilinear map $B_1 \times B_2 \to B$, $(b_1, b_2) \mapsto b_1 b_2$. By the universal property of tensor products, we obtain a corresponding linear map $B_1 \otimes_F B_2 \to B$. By Lemma III.§1, $B_1 \otimes_F B_2$ is simple, so this linear map must be injective. By comparing dimensions, we infer that it is an isomorphism.

In the Brauer group $B(F)$, our observations so far read $(a, b)(a', b) = (aa', b)(a', -a'b^2)$, where we have omitted the field F for brevity. But, by one of the isomorphisms of Rmk. §2.(2), we then have $(a', -a'b^2) \cong (a', -a')$, so we are done by part (i). □

§4. The Hasse invariant

In this section, we introduce the Hasse invariant associated to quadratic spaces. This invariant will turn out to be among the fundamental invariants of quadratic spaces, see Thm. III.§4 and its corollary below. We again fix a ground field F of characteristic $\neq 2$ and make the same assumptions as in §3 regarding quadratic spaces over F and algebras over F for the entire section.

Let (V,q) be a regular n-ary quadratic space over F, and let $(V,q) \cong \langle a_1,...,a_n\rangle$ be a diagonalization of V, where $a_i \in F^\times$ for all i. Define $s(V) = s(V,q)$ to be the element

$$s(V,q) = \prod_{1\le i<j\le n} \left(\frac{a_i,\ a_j}{F}\right)$$

in the Brauer group $B(F)$ of F, cf. §1, where $\left(a_i, a_j \mid F\right)$ denotes the quaternion algebra defined as in Ex. §2.(1), or more precisely its similarity class in $B(F)$.

We now claim that $\prod_{1\le i<j\le n} \left(b_i, b_j \mid F\right) = s(V)$ for any diagonalization $(V,q) \cong \langle b_1,...,b_n\rangle$, $b_i \in F^\times$. Thus, $s(V) \in B(F)$ is well-defined and invariant under isometry; it is named the *Hasse invariant* of (V,q).

If $n = 1$, then there is nothing to prove. Now let $n = 2$. By the results of §3, the Clifford algebra $C(V)$ of (V,q) can be identified with $\left(a, b \mid F\right)$ for any diagonalization $(V,q) \cong \langle a, b\rangle$. Hence, $s(V)$ is precisely the Clifford algebra of (V,q) and thus unique.

Now let $n \ge 3$, and let the a_i's and b_i's be again as above. The claim follows easily if $a_i = b_i$ for all $i \ge 3$, for then $\left(a_1, a_2 \mid F\right) \cong \left(b_1, b_2 \mid F\right)$ by the case $n = 2$, and repeatedly applying Cor. III.§3.(ii) yields the following computation in $B(F)$:

$$\begin{aligned}
\prod_{1\le i<j\le n} \left(\frac{a_i,\ a_j}{F}\right) &= \left(\frac{a_1,\ a_2}{F}\right)\left(\frac{a_1,\ a_3\cdots a_n}{F}\right)\left(\frac{a_2,\ a_3\cdots a_n}{F}\right)\prod_{3\le i<j} \left(\frac{a_i,\ a_j}{F}\right)\\
&= \left(\frac{a_1,\ a_2}{F}\right)\left(\frac{a_1a_2,\ a_3\cdots a_n}{F}\right)\prod_{3\le i<j} \left(\frac{a_i,\ a_j}{F}\right)\\
&= \left(\frac{b_1,\ b_2}{F}\right)\left(\frac{b_1b_2,\ b_3\cdots b_n}{F}\right)\prod_{3\le i<j} \left(\frac{b_i,\ b_j}{F}\right)\\
&= \prod_{1\le i<j\le n} \left(\frac{b_i,\ b_j}{F}\right),
\end{aligned}$$

where we have used $a_1a_2 \cdot F^{\times 2} = \det V = b_1b_2 \cdot F^{\times 2}$ and Rmk. §2.(2).

The above special case motivates the following definition: given regular n-ary quadratic spaces $(V,q) = \langle a_1,...,a_n\rangle$ and $(V',q') = \langle b_1,...,b_n\rangle$, we say that (V,q) and (V',q') are *simply equivalent* if there exist two indices i,j with $\langle a_i\rangle \perp \langle a_j\rangle \cong \langle b_i\rangle \perp \langle b_j\rangle$ and $a_k = b_k$ for all $k \ne i,j$. We call two regular spaces V and V' *chain-equivalent* and write $V \approx V'$ if there exist spaces $V = V^{(0)}, V^{(1)},..., V^{(m)} = V'$ so that each $V^{(i)}$ is simply equivalent to $V^{(i+1)}$ for $0 \le i < m$.

Clearly, simply equivalent spaces are isomorphic, so naturally chain-equivalent spaces are also isomorphic. The following lemma shows that the converse holds; in particular, the special case proved above is already enough to conclude the proof that $s(V)$ is well-defined and invariant as claimed.

Lemma III.§4 (Chain-Equivalence Theorem)**.** *Let (V,q), (V',q') be regular spaces over F. If V, V' are isometric, then they are chain-equivalent.*

Proof. The proof is by induction on $n = \dim V = \dim V'$. For $n = 1, 2$ there is nothing to prove, so we henceforth suppose that $n \geq 3$.

We start by showing that there is a regular space $(V'',q'') \approx (V,q)$ of the form $(V'',q'') = \langle b_1, c_2, ..., c_n\rangle$. In other words: among all regular spaces (V'',q'') which are chain-equivalent to (V,q), pick $(V'',q'') = \langle c_1, ..., c_n\rangle$ such that some $\langle c_1, ..., c_p\rangle$ represents b_1, and p is smallest possible; we claim $p = 1$.

For suppose that $p \geq 2$, and write $b_1 = c_1x_1^2 + ... + c_px_p^2$ for appropriate $x_1, ..., x_p \in F$. We must have $d = c_1x_1^2 + c_2x_2^2 \neq 0$, for otherwise we could find a smaller p with the required properties. Since $\langle c_1, c_2\rangle$ represents d, we find that $\langle c_1, c_2\rangle \cong \langle d, d'\rangle$ for some $d' \in F^\times$. Then we readily check that (V'',q'') (and thus also (V,q)) is chain-equivalent to $\langle d, c_3, ..., c_n, d'\rangle$. But then $\langle d, c_3, ..., c_p\rangle$ already represents $b_1 = d + c_3x_3^2 + ... + c_px_p^2$, contradicting the minimality of p.

Thus, we have found $(V'',q'') \approx (V,q)$ with $(V'',q'') = \langle b_1, c_2, ..., c_n\rangle$, as claimed. We apply Witt's Cancellation Theorem to (V',q') and (V'',q'') and thus obtain $\langle c_2, ..., c_n\rangle \cong \langle b_2, ..., b_n\rangle$. Then, by the induction hypothesis, these two $(n-1)$-dimensional spaces are chain-equivalent, and so finally $(V,q) \approx (V'',q'') \approx (V',q')$. □

At the beginning of this section, we claimed that the Hasse invariant is among the fundamental invariants of quadratic spaces. The following result indeed shows that the Hasse invariant alone is essentially enough to classify quadratic spaces of small dimension.

Theorem III.§4. *Let (V,q), (V',q') be regular quadratic spaces over F of the same dimension $n \leq 3$. Then $(V,q) \cong (V',q')$ if and only if $\det V = \det V'$ and $s(V) = s(V')$.*

Proof. The invariance of $\det V$ and $s(V)$ settles necessity. We proceed to show sufficiency.

For $n = 1$, the statement is clearly true (indeed, equality of the determinants is already sufficient). For $n = 2$, pick $a, b, a', b' \in F^\times$ with $(V,q) \cong \langle a, b\rangle$ and $(V',q') \cong \langle a', b'\rangle$, and let $C = \big(a, b \mid F\big)$ and $C' = \big(a', b' \mid F\big)$ denote the Clifford algebras of V, V' respectively (cf. §3). By our above discussion, the assumption $s(V) = s(V')$ means precisely that $C \sim C'$, cf. §1. But then by the uniqueness part of Wedderburn's Theorem we obtain $C \cong C'$, cf. the discussion at the beginning of §2. By Rmk. §2.(6)-Rmk. III.§2.(7), this is equivalent to $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle$. But $ab \cdot F^{\times 2} = \det V = \det V' = a'b' \cdot F^{\times 2}$, so we can cancel both $\langle 1\rangle$ and $\langle ab\rangle = \langle a'b'\rangle$ by Witt's Cancellation Theorem and obtain $\langle -a, -b\rangle \cong \langle -a', -b'\rangle$, which amounts to $V \cong V'$.

Now let $n = 3$. If $\det V = \det V'$ equals $1 \cdot F^{\times 2}$, then we can proceed similarly as before: indeed, we can write $(V,q) \cong \langle a, b, -ab\rangle$ and $(V',q') \cong \langle a', b', -a'b'\rangle$ for appropriate

$a, b, a', b' \in F^\times$, and then a direct computation shows that $s(V)$ and $s(V')$ are the similarity classes of $\big(a, b \mid F\big)$ and $\big(a', b' \mid F\big)$ respectively in the Brauer group $B(F)$. From the assumption $s(V) = s(V')$ we obtain, as before: $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle$, and Witt's Cancellation Theorem again yields $(V, q) \cong (V', q')$.

For the general case, pick $d \in F^\times$ with $dF^{\times 2} = \det V$, and note that $(V, q) \cong (V', q')$ if and only if $(V, \overline{q}) \cong (V', \overline{q}')$, where $\overline{q}(x) := dq(x)$ for all $x \in V$ and analogously $\overline{q}'(x) := dq'(x)$ for all $x \in V'$. Now a direct computation using Rmk. §2.(2) and Cor. III.§3 shows $s(V, \overline{q}) = s(V, q) = s(V', q') = s(V', \overline{q}')$. But $\det(V, \overline{q}) = \det(V', \overline{q}') = d^4 \cdot F^{\times 2} = 1 \cdot F^{\times 2}$, so we are done by the special case. □

Finally, we derive useful criteria for regular quadratic spaces of small dimension to be isotropic. As in (the proof of) Cor. III.§3, we agree to denote the similarity class of $\big(a, b \mid F\big)$ in $B(F)$ again by $\big(a, b \mid F\big)$ and to omit the field F at times for brevity. Moreover, we shall use Cor. III.§3.(ii) freely throughout the proof.

Corollary III.§4. *Let (V, q) be a regular quadratic space, and let $d \in F^\times$ with $dF^{\times 2} = \det V$.*

(i) If $\dim V = 3$, then (V, q) is isotropic if and only if $s(V) = \big(-1, -d \mid F\big)$.

(ii) If $\dim V = 4$ and $d \in F^{\times 2}$, then (V, q) is isotropic if and only if $s(V) = \left(\frac{-1,\ -1}{F}\right)$.

Proof. (i) By Rmk. II.§3.(3), (V, q) is isotropic if and only if V contains a hyperbolic plane as a regular subspace, $V = \mathbb{H} \perp \mathbb{H}^\perp$. Now $\mathbb{H} \cong \langle 1, -1\rangle$; thus, upon comparing determinants and dimensions we find that V is isotropic if and only if $V \cong \langle 1, -1, -d\rangle =: V'$. But by Thm. III.§4 this is the case if and only if $s(V) = s(V') = (1, -1)(1, -d)(-1, -d) = (-1, -d)$, where we have used that $(1, b)$ splits for any $b \in F^\times$, cf. §§2-3.

(ii) Let $W \subset V$ be a regular ternary subspace of V. Then by Cor. II.§2.(iii), V is isotropic if and only if W is, and by part (i) this is equivalent to $s(W) = (-1, -d')$, where $d'F^{\times 2} = \det W$.

Now pick $a \in F^\times$ with $V = \langle a\rangle \perp W$; note that $ad' \cdot F^{\times 2} = \det V = 1 \cdot F^{\times 2}$. A direct computation shows that $s(V) = (a, d')s(W)$, but the isomorphisms from Rmk. §2.(2) yield $(a, d') = (a, -ad') = (a, -1) = (-1, a)$, so we conclude that V is isotropic if and only if $s(V) = (-1, a)(-1, -d') = (-1, -1)$. □

§5. Quaternion algebras over local fields

In this section, we proceed to provide a concrete classification of quaternion algebras over F in the case that F is a local field (K, v), cf. also I.§6. Our assumption that $\chi(K) \neq 2$, cf. Rmk. I.§2.(3), is still in force; furthermore, we keep the assumptions from §2 regarding algebras over K, unless explicitly stated otherwise.

The key results to classify quaternion algebras over *archimedean* local fields are Thm. II.§4 and the isomorphism $\left(\frac{ac^2,\ bd^2}{F}\right) \cong \left(\frac{a,\ b}{F}\right)$ for $a, b, c, d \in F^\times$ from Rmk. §2.(2). Indeed, let $K = \mathbb{C}$. Then the above facts combined tells us that *every* quaternion algebra over $\mathbb{C}$ is isomorphic to $\left(\frac{1,\ 1}{\mathbb{C}}\right)$, and hence isomorphic to $M_2(\mathbb{C})$ by Rmk. §2.(1').

As for $K = \mathbb{R}$, let $A = \left(a, b \mid \mathbb{R}\right)$ for $a, b \in \mathbb{R}^\times$. If one of a or b is positive, then by the above argument $A \cong M_2(\mathbb{R})$; otherwise, $A \cong \left(\frac{-1,\ -1}{\mathbb{R}}\right) = \mathbb{H}$, see Ex. §2.(1'). Thus, up to isomorphism, *there is precisely one nonsplit quaternion algebra over* $\mathbb{R}$.

We now turn to the non-archimedean case, i.e., suppose that (K, v) is non-archimedean. The classification theorem for quaternion algebras will follow from a strong result (see Prop. III.§5 below) on certain extensions of (K, v), which is essentially derived from Hensel's Lemma. We retain the notations fixed, established or introduced in II.§4; in particular, recall the notation $\overline{a}$ for the image of $a \in \mathfrak{o}(v)$ under the canonical quotient map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m} = k$, and the analogous notation $\overline{f}$ for polynomials $f(t)$ with coefficients in $\mathfrak{o}$.

Before we proceed, we wish to recall a definition which we shall use in the statement of Lemma III.§5 below. Let F be an arbitrary field, and let $f(t) = \sum_{i=0}^{d} a_i t^i \in F[t]$. Then $f'(t) = \sum_{i=0}^{d-1} a_{i+1}(i+1)t^i \in F[t]$ is called the *formal derivative* of f. It is readily checked that f' satisfies the familiar sum and product rules from elementary calculus; in particular, if Z is a splitting field of f over F (cf. I.§9) and $\alpha \in Z$, then an easy application of the product rule yields: *α is a multiple root of f if and only if $f(\alpha) = f'(\alpha) = 0$.*

Remark. (1) Let L/K be an arbitrary finite-degree field extension with $L = K(\delta)$ for some $\delta \in L$. Then the discussion in I.§9 tells us precisely that L/K is separable if and only if $f'(\delta) \neq 0$, where $f = f_{K,\delta}$ denotes the minimal polynomial of δ over K. But f must divide every polynomial which vanishes in δ, and $\deg f' < \deg f$, so we obtain the following: *L/K is separable if and only if f' is not the zero polynomial.* $\diamond$

Our first result comprises two immediate but useful consequences of Hensel's Lemma.

Lemma III.§5. *Let (L, w) be a local field containing (K, v), $[L : K] = n < \infty$. Suppose that $L = K(\alpha)$ for some $\alpha \in L$, and let $f(t)$ be the minimal polynomial of α over K.*

(i) $\alpha \in \mathfrak{o}(w)$ if and only if $f(t)$ has coefficients in $\mathfrak{o}(v)$;

(ii) if $f \in \mathfrak{o}(v)[t]$ and $f'(\alpha) \in \mathfrak{u}(w)$, then $\overline{f}(t) \in k(v)[t]$ is again irreducible.

Proof. (i) Sufficiency is essentially the content of Lemma I.§9. In order to prove necessity, we first prove the following general claim: *if f is an irreducible monic polynomial over K with $f(0) \in \mathfrak{o}(v)$, then f has coefficients in $\mathfrak{o}(v)$.*

Write $f(t) = \sum_{i=0}^{n} a_i t^i$; by assumption, $a_n = 1$. Since $\mathfrak{o}(v)$ is a valuation ring, there exists an l so that $a_i \in a_l \mathfrak{o}$ for all i; let j be the smallest such l. Then $F = f/a_j$ has

coefficients in $\mathfrak{o}(v)$. Since j is minimal, there exists $h(t)$ with $\overline{F}(t) = t^j h(t)$ in $k(v)[t]$. Now $h(0) = 1$, i.e., t^j and $h(t)$ are relatively prime and we can apply Hensel's Lemma to find $G, H \in \mathfrak{o}(v)[t]$ with $F = GH$, $\deg G = j$. But F is irreducible by assumption, so either $j = 0$ or $j = n$. Since $a_0, a_n \in \mathfrak{o}(v)$, it follows that $a_i \in a_j\mathfrak{o} \subseteq \mathfrak{o}$ for all i, and the claim is proved. To conclude the proof of necessity, note that $\alpha \in \mathfrak{o}(w)$ is equivalent to $N_{L/K}(\alpha) \leq 1$ by definition of w, and this in turn is equivalent to $f(0) = a_0 \in \mathfrak{o}(v)$.

(ii) Suppose for the sake of contradiction that the minimal polynomial $g(t)$ of $\overline{\alpha}$ over $k(v)$ is not $\overline{f}(t)$. Then $g(t)$ is a divisor of $\overline{f}(t)$ since $\overline{f}(\overline{\alpha}) = \overline{f(\alpha)} = 0 \in k(w)$. Thus, write $\overline{f} = gh$ for some $h \in k(v)[t]$. By assumption, $\overline{f}'(\overline{\alpha}) \neq 0$ in $k(w)$, hence $\overline{\alpha}$ is not a multiple root of $\overline{f}$. Accordingly, $g(t)$ and $h(t)$ are relatively prime, otherwise f' would be identically zero by Rmk.(1), so by Hensel's Lemma we obtain a factorization $f = GH$ for $G, H \in \mathfrak{o}(v)[t]$ with $\deg G = \deg g > 1$. But f is irreducible, so we have reached the desired contradiction. □

Remark. (2) Note that the auxiliary claim in the proof of Lemma III.§5.(i) was formulated and proved using Hensel's Lemma for K, but not the properties of the local field (L, w). Thus, this claim can be used to close the gap in the proof of Thm. I.§7 without incurring in circular reasoning.

(3) Keep the notations (L, w), n, α, f from Lemma III.§5 above. Further, let $f(w|v) = [k(w) : k(v)]$ and $e(w|v)$ denote the ramification index and inertia degree of L/K respectively, cf. I.§7; we have $e(w|v)f(w|v) = n$. Under the assumption (ii), $\overline{f}$ is the minimal polynomial of $\overline{\alpha}$ over $k(v)$. Then the degree of $k(v)(\overline{\alpha}) \subseteq k(w)$ over $k(v)$ is precisely the degree of $\overline{f}$, which is the same as $\deg f = [K(\alpha) : K] = n$. Thus, $n \geq f(w|v) \geq [k(v)(\overline{\alpha}) : k(v)] = n$, and accordingly $e(w|v) = 1$. An extension with the last property is said to be *unramified*. ◇

Example. (1) Let $q = \#k(v)$, and consider the polynomial $f(t) = t^{q-1} - 1$ over K. Let ζ be a root of f in some splitting field of f over K, and denote $L = K(\zeta)$. Now let $\Phi(t)$ denote the minimal polynomial of ζ over K, and write $f(t) = \Phi(t)h(t)$ for $h(t) \in K[t]$. By the properties of the formal derivative, $f'(\zeta) = \Phi'(\zeta)h(\zeta)$. But[4] $f'(\zeta) = (q-1)\zeta^{q-2}$ lies in $\mathfrak{u}(w)$, so $\Phi'(t) \in \mathfrak{u}(w)$ and we can apply Lemma III.§5.(ii) and Rmk.(3).

Now, by the properties of finite fields, $\overline{f}(t)$ splits into linear factors over $k = k(v)$; in fact, each nonzero element of k is a root of $\overline{f}$. Thus, $\overline{\zeta}$ already lies in $k(v)$. But we saw in Rmk.(3) that $[K(\zeta) : K] = [k(\overline{\zeta}) : k]$, hence ζ lies in K. In other words, *K contains all $(q-1)$-th roots of unity, where $q = \#k(v)$.*

(1') Now let ζ be an element of K with $\zeta^m = 1$ for some $m \geq 1$ which is relatively prime to q. Consider the elements $1, \zeta, \zeta^2, ..., \zeta^{m-1}$; they make up all the roots of $g(t) = t^m - 1$

[4]Since $q = \#k(v)$, the q-fold sum of 1's equals 0 in $k(v)$, so we infer that $q \in \mathfrak{m}(v)$. Thus, $q - 1 \in \mathfrak{u}(v)$, for otherwise $1 = q - (q-1) \in \mathfrak{m}(v)$ which is absurd.

in K. We shall now show that $\overline{1}$, $\overline{\zeta}$, ..., $\overline{\zeta}^{m-1}$ are pairwise distinct in $k(v)$; it will follow that $\overline{\zeta}^m = 1$ in $k(v)$, and so m must divide the order $q-1$ of the multiplicative group $k(v)^\times$, i.e., ζ is a $(q-1)$-th root of unity.

In order to prove the claim, write $g(t) = \prod_{i=0}^{m-1}(t-\zeta^i)$. Then $m\zeta^{m-1} = g'(\zeta) = \prod_{i\neq j}(\zeta^i - \zeta^j)$. But the left-hand side lies in $\mathfrak{u}(v)$ since m is relatively prime to $\#k(v)$; so we finally see that $\overline{\zeta^i} \neq \overline{\zeta^j}$ whenever $i \neq j$ and we are through. $\diamond$

We are now ready to prove:

Proposition III.§5. *Let (L,w) be a local field containing (K,v), $[L:K] < \infty$, and let $q = \#k(v)$, $q' = \#k(w)$.*

(i) If L is a splitting field of $\Phi_n(t) = t^{q^n} - t$ over K for some n, then L/K is unramified*, cf. Rmk.(3), and $[L:K] = n$.*

(ii) Conversely, if L/K is unramified and $[L:K] = n$, then L is a splitting field of $\Phi_n(t)$ over K.

Proof. (i) By directly computing $\Phi_n'(t)$, one checks that Φ_n has no multiple roots in L, cf. Rmk.(1), so L contains $q^n - 1$ pairwise distinct (q^n-1)-th roots of unity. By Ex.(1'), each of these elements must be a $(q'-1)$-th root of unity, hence $q^n \leq q'$.

We now use the following well-known fact: every finite subgroup of the multiplicative group of a field is cyclic. From this, we infer that L contains a *primitive* (q^n-1)-th root of unity ζ; but then $L = K(\zeta)$, and L/K is unramified by Rmk.(3) and Ex.(1).

It remains to show that $n = [L:K]$. One now checks that $x^{q^n} = x$ for all $x \in k(w)$, hence q^n must be a multiple of $q' = \#k(w)$. But $q' = q^{f(w|v)}$, so we obtain $[L:K] = f(w|v) = n$ as claimed.

(ii) By assumption, $q' = q^n$, so L contains all (q^n-1)-th roots of unity by Ex.(1). In particular, L contains a splitting field Z of $\Phi_n(t)$ over K. But then part (i) implies that $[Z:K] = n$, so $Z = L$. $\square$

Remark. (4) Let (L,w) be a *quadratic* extension of (K,v), i.e., $[L:K] = 2$. Then there exists some $\alpha \in L$ whose minimal polynomial $f(t)$ has degree 2 (otherwise, $L = K$). Let $f(t) = t^2 + at + b$, $a, b \in K$. Then[5] $\delta' = 2\alpha + a \in L$ satisfies $(\delta')^2 = \Delta = a^2 - 4b \in K^\times$; note that $\Delta \notin K^{\times 2}$ (for otherwise $f(t)$ would factor nontrivially over K), so $L = K(\delta')$.

Now write $\Delta = \pi^r u$, where $r \in \mathbb{Z}$, $u \in \mathfrak{u}(v)$, cf. I.§3, and suppose that L/K is unramified. Then π is a uniformizer for $\mathfrak{o}(w)$, and so $\Delta = \pi^r u$ is also the unique representation of $\Delta \in L$. But then r must be even, since $\Delta = (\delta')^2$, so u is the square of $\delta = \delta'\pi^{-r/2}$ and $L = K(\delta)$.

(4') We keep the assumption that L/K be unramified, i.e., $[k(w):k(v)] = 2$. The map which sends δ to $-\delta$ can be extended to a K-homomorphism from L to L, cf. I.§9, which

[5] Note that this is the first time we use the assumption $\chi(K) \neq 2$ in this section.

we denote σ. Moreover, we denote by $\overline{N}$ the norm of the extension $k(w)/k(v)$, see also I.§7. This map is surjective by finiteness of $k(v)$; in particular, for each $x \in \mathfrak{u}(v)$ there exists some $b_0 \in \mathfrak{o}(w)$ with $\overline{N}(\overline{b_0}) = \overline{x}$, i.e. with $N_{L/K}(b_0) - x \in \mathfrak{m}(v)$.

As the notation b_0 suggests, it is possible for each $i \geq 0$ to find some $b_i \in \mathfrak{o}(w)$ so that $N_{L/K}(b_0 + b_1\pi + ... + b_k\pi^k) - x \in \mathfrak{m}(v)^{k+1}$ for all k. This is achieved using the equality $N_{L/K}(\alpha) = \alpha\sigma(\alpha)$ for all $\alpha \in L$ as well as the finiteness of $k(v)$, see e.g. [Lam04], Prop. VI.2.9. Then one obtains that $\beta = \sum_{i=0}^{\infty} b_i\pi^i \in \mathfrak{o}(w)$ satisfies $N_{L/K}(\beta) = x$; in other words, $N_{L/K}$ *is onto* $\mathfrak{u}(v)$. On the other hand, note that π does not lie in the image of $N_{L/K}$, for $\nu(\pi) = 1$, but $\nu\left(N_{L/K}(\alpha)\right) = \nu\left(\alpha\sigma(\alpha)\right) = \nu_w(\alpha)\nu_w\left(\sigma(\alpha)\right) = 2\nu_w(\alpha)$ for all $\alpha \in L$, where ν_w denotes the normalized valuation of $\mathfrak{o}(w)$, cf. I.§3. $\diamond$

In light of Prop. III.§5 and Rmk.(4), we henceforth denote by L the essentially unique quadratic unramified extension of K and write $L = K(\delta)$, where $u = \delta^2$ lies in $\mathfrak{u}(v)$.

Theorem III.§5. *Let D be a nonsplit quaternion algebra (thus, a division algebra) over K. Then there exists some $i \in D^\circ$ with $i^2 = u$. Thus, D is isomorphic to $\left(\frac{u,\ \pi}{K}\right)$.*

Proof. For the sake of brevity as well as clarity, we shall only sketch the proof of the first claim; a more complete proof can be found e.g. in [Lam04], Thm. VI.2.10.

Consider the norm form N of D as in §3 and define $\omega := \nu \circ \mathrm{N}|_{D^\times}$, where of course $D^\times = D \setminus \{0\}$ and ν is the normalized valuation of $\mathfrak{o}(v)$. Since (D, N) is not isotropic, ω is a well-defined map $D^\times \to \mathbb{Z}$.

Set $\mathfrak{O} = \{x \in D : \omega(x) \geq 0\}$ as well as $\mathfrak{P} = \{x \in D : \omega(x) > 0\}$. Then $\mathfrak{o}(v) \subseteq \mathfrak{O}$ is a *ring extension*, and $\mathfrak{P} \cap \mathfrak{o}(v) = \mathfrak{m}(v)$. Mirroring well-known proofs from algebraic number theory, one establishes that $\mathfrak{k} = \mathfrak{O}/\mathfrak{P}$ is a finite-dimensional (!) division algebra over $k(v)$; additionally, it turns out that $\dim_{k(v)} \mathfrak{k} > 1$.

Now **Wedderburn's Little Theorem** tells us that $\mathfrak{k}$ is a finite field, and by the theory of finite fields $\mathfrak{k} = k(v)(\overline{s})$ for some $s \in D$, $s \notin K$. The field $K(s) \subset D$ necessarily has degree 2 over K, see also the proof of Prop. III.§2, and one can compute that the degree of its residue field over $k(v)$ equals 2, so $K(s)/K$ is an unramified extension. Thus, one can identify $K(s)$ with L, and $D \supset K(s)$ contains some $i \notin K = Z(D)$ with $i^2 = u$.

The second claim now follows easily: first, as in the proof of Prop. III.§2, one finds some element $j \in D$ so that $1, i, j, ij$ form a quaternion basis for D. Write $j^2 = \pi^m u'$ for some $m \in \mathbb{Z}$, $u' \in \mathfrak{u}(v)$, and note that, in the Brauer group $B(K)$ of K, one has $[D] = (u, \pi^m u') = (u, u')(u, \pi^\varepsilon)$, where $\varepsilon \in \{0, 1\}$. Now u' lies in the image of $N_{L/K}$ by Rmk.(4'), so by Thm. III.§3 we have $(u, u') = 1$ and accordingly $[D] = (u, \pi^\varepsilon)$. If $\varepsilon = 0$, then D splits, contradicting the assumption, thus $D \cong \left(\frac{u,\ \pi}{F}\right)$, where we have used Cor. III.§1.(ii). Note that the latter is indeed a division algebra: this follows again from Thm. III.§3 since π is not in the image of $N_{L/K}$ by Rmk.(4'). $\square$

REMARK. (5) The above argument can be modified and extended so as to classify *arbitrary* central division algebras D over the local field (K, v). In the definition of the "valuation" $\omega = \omega_D$ on D, the norm form N must be replaced by the *reduced norm*, whose definition relies on the fact that there exists a *Galois extension* K'/K with $D \otimes_K K' \cong M_r(K')$ for some $r \geq 1$; the valuation itself now maps to $\frac{1}{d}\mathbb{Z}$, where d is the square root of $\dim_K D$ (this is always an integer).

As above, one shows that $\mathfrak{O}/\mathfrak{P}$ is a finite extension of $k(v)$ generated by a single element and that D contains a local field L'; the group of K-automorphisms of L' is generated by a single element σ. Using a well-known result on CSAs known as the **Skolem-Noether Theorem**, one can then construct a group homomorphism $B(K) \to \mathbb{Q}/\mathbb{Z}$ (it turns out that this is even bijective), and so one can interpret the *Hasse invariant* of a CSA A over K as an element of $\mathbb{Q}/\mathbb{Z}$. $\diamond$

§6. Invariants over local fields

In this final section, we use the results of §5 to define the classical invariants of quadratic spaces over local fields and subsequently employ these invariants to obtain a powerful classification theorem, see Thm. III.§6 below. As in §5, we consider a fixed local field (K, v) of characteristic $\neq 2$ and make the same assumptions as in §§2-3 regarding quadratic spaces over K and algebras over K; moreover, we use the terminology and results from Chapter II quite freely, and retain the notations from II.§4 whenever (K, v) is supposed to be non-archimedean.

Let $B(K)$ denote the Brauer group of the local field K, and let $\mathrm{Quat}(K) \subseteq B(K)$ denote the subgroup generated by all quaternion algebras over K. The results of §5 show us that there is at most one nonsplit quaternion algebra over K; if D is such an algebra, then using Cor. III.§3.(ii) and Rmk. §2.(1') one easily checks that $[D]^2 = 1 \in B(K)$, so $\mathrm{Quat}(K)$ is either trivial (iff $K = \mathbb{C}$) or it has precisely two elements, in which case we identify it with the multiplicative group $\{-1, 1\}$. In particular, for a quadratic space (V, q) over K we can consider its Hasse invariant $s(V)$ from §4 to be an element of $\{\pm 1\}$; then, following tradition, one calls $s(V)$ the *Hasse symbol* of (V, q).

Now consider the map which sends a pair (a, b) of elements of $K^\times$ to the class of $\left(\frac{a,\ b}{K}\right)$ in $\mathrm{Quat}(K)$. By one of the isomorphisms of Rmk. §2.(2), this induces a well-defined map

$$\begin{aligned} K^\times/K^{\times 2} \times K^\times/K^{\times 2} &\to \{\pm 1\} \\ (a \cdot K^{\times 2}, b \cdot K^{\times 2}) &\mapsto (a, b) = (a, b)_K, \end{aligned}$$

called the *Hilbert symbol*. Clearly, if (V, q) is a quadratic space over K with a diagonalization $\langle a_1, ..., a_n \rangle$, then the Hasse symbol $s(V)$ equals precisely $\prod_{i<j}(a_i, a_j)_K$.

EXAMPLE. Suppose that (K, v) is a *nondyadic* (non-archimedean) local field, cf. II.§4. Then $(u_1, u_2)_K = 1$ whenever $u_1, u_2 \in \mathfrak{u}(v)$. Indeed, this is clear if either u_1 or u_2 is a square, and otherwise it follows from the observation at the end of II.§4 together with Thm. III.§3.

Now consider the regular ternary space $(V, q) = \langle u_1, u_2, u_3 \rangle$ over (K, v) where $u_i \in \mathfrak{u}(v)$, and let $d = u_1 u_2 u_3$. Then clearly $-d \in \mathfrak{u}(v)$, and an application of Cor. III.§3 yields $(-1, -d)_K = 1 = s(V)$, so (V, q) is isotropic by Cor. III.§4.

Since a space is isotropic whenever it has an isotropic subspace, we obtain the following result: if (V, q) is a regular n-ary space over (K, v) with $n \geq 3$ and $(V, q) \cong \langle u_1, ..., u_n \rangle$ for some $u_i \in \mathfrak{u}(v)$, then (V, q) is isotropic. $\diamond$

REMARK. (1) If one considers $K^\times / K^{\times 2}$ as a vector space over $\mathbb{F}_2$, then the Hilbert symbol turns out to be a *symmetric bilinear form* on $K^\times / K^{\times 2}$, cf. II.§1; indeed, linearity is precisely Cor. III.§3.(ii). This form can be shown to be nondegenerate: in fact, this is immediate if (K, v) is archimedean, and is easily seen if (K, v) is nondyadic (cf. II.§4) by combining Thm. II.§4, Thm. III.§5 and Thm. III.§3.

Now let $b \in K^\times$, $b \notin K^{\times 2}$, and consider the map $a \mapsto (a, b)_K$. By Thm. III.§3, its kernel is precisely $N_{L/K}(L^\times)$, where L is a splitting field of $g(t) = t^2 - b$ over K, and since the Hilbert symbol is nondegenerate, the kernel is not all of $K^\times$. Thus, the above map descends to a surjective group homomorphism $K^\times / N_{L/K}(L^\times) \to \{\pm 1\}$, and we obtain that the index $[K^\times : N_{L/K}(L^\times)]$ of the subgroup $N_{L/K}(L^\times)$ in $K^\times$ is precisely 2.

(2) For $K = \mathbb{Q}_p$ with $p \in \mathbb{Z}_{>0}$, cf. I.§5, it is possible to compute the Hilbert symbol $(\ ,\ )_p := (\ ,\ )_{\mathbb{Q}_p}$ directly, see e.g. [Ser73]; as it turns out, the explicit form involves the *Legendre symbol*, a function $\mathbb{F}_p^\times \to \{\pm 1\}$ which takes on the value 1 if the argument is a square and -1 otherwise.

Now let $a, b \in \mathbb{Q}$, and consider the Hilbert symbols $(a, b)_p$ for all primes $p \in \mathbb{Z}_{>0}$ and for the "infinite prime" ∞, where $(a, b)_\infty := (a, b)_\mathbb{R} = \max\{\mathrm{sgn}(a), \mathrm{sgn}(b)\}$. One can then use the *quadratic reciprocity law*, a famous result relating Legendre symbols at different primes, to prove that

$$\prod_{p \leq \infty} (a, b)_p = 1,$$

an equation known as **Artin's reciprocity law** which even extends to general global fields, see [O'M73]. $\diamond$

We now turn to the problem of classifying quadratic spaces over (K, v) by means of invariants. The archimedean case was already covered in II.§4: quadratic spaces over $\mathbb{C}$ are classified by their dimension alone, whereas quadratic spaces over $\mathbb{R}$ are classified by their dimension as well as signature.

The non-archimedean case requires, as usual, somewhat more work. Let $D = \left(\frac{u,\,\pi}{F}\right)$, where u is as in §5, and let N denote the norm form of D; since D is a division algebra, $\mathrm{N}(D^\times)$ is a subgroup of $K^\times$. In the proof of Thm. III.§5, we saw that D contains a subfield isomorphic to L, and a closer look at Rmk. §2.(6) and Ex. §2.(3) will show that N agrees with $N_{L/K}$ on this subfield, therefore $\mathrm{N}(D^\times) \supseteq N_{L/K}(L^\times) \supseteq \mathfrak{u}(v)$, where the last inclusion was proved in Rmk. §5.(4'). On the other hand, $\mathrm{N}(D^\times)$ also contains $-\pi$ since $(D, \mathrm{N}) \cong \langle 1, -u, -\pi, u\pi\rangle$ by Rmk. §2.(6). But $-\pi$ and $\mathfrak{u}(v)$ already generate $K^\times$, so *the quadratic space* (D, N) *is universal.*

Moreover, we observe that, if (V, q) is a quaternary space over (K, v) with $\det V = 1 \cdot F^{\times 2}$ and if (V, q) represents 1 but not 0, then (V, q) is already isometric to (D, N). Indeed, by these assumptions we can write $(V, q) \cong \langle 1, -x, -y, xy\rangle$ for some $x, y \in K^\times$, and thus (V, q) is isomorphic to a quaternion algebra (A, N') with its norm form by Rmk. §2.(6)-(7). Since (V, q) does not represent 0, we find that (A, N') is not split; but then $(A, \mathrm{N}') \cong (D, \mathrm{N})$ by Thm. III.§5, and we are through.

We can now prove the following fundamental result about quadratic spaces over (K, v).

Proposition III.§6. *Suppose that (K, v) is non-archimedean, and let (V, q) be an n-ary quadratic space over K with $n \geq 5$. Then (V, q) is isotropic.*

Proof. Since a space with $\det V = 0$ necessarily represents 0, we can assume that (V, q) is regular. Moreover, it suffices to prove the claim for $n = 5$, for a space with an isotropic subspace is itself isotropic. Finally, one can assume that (V, q) represents 1; for if $r \in K^\times$ is any element represented by (V, q), then $(V, \widetilde{q})$, where $\widetilde{q} : V \to K$, $x \mapsto \frac{1}{r}q(x)$, is a quadratic space which represents 1, and which is regular and isotropic if and only if (V, q) is regular and isotropic.

Suppose for the sake of contradiction that (V, q) does not represent 0. By the above assumptions, there exists a diagonalization $(V, q) \cong \langle 1, a, b, c, d\rangle$ for some $a, b, c, d \in K^\times$. Since the subspace $\langle 1, a, b\rangle$ is not isotropic, neither is $\langle 1, a, b, ab\rangle$ (use Cor. II.§2.(iii)), so $\langle 1, a, b, ab\rangle \cong (D, \mathrm{N})$ by the above observation.

We now claim that $\langle 1, -c, -d\rangle$ is isotropic. For if not, then $\langle 1, -c, -d, cd\rangle$ is not isotropic, and the above observation shows that it must be isometric to $\langle 1, a, b, ab\rangle$. But then an easy manipulation yields $\langle a, b, c, d\rangle \cong \langle 1, -1, -ab, cd\rangle$, so (V, q) is isotropic, a contradiction. Hence, $\langle 1, -c, -d\rangle$ is isotropic, i.e., $\langle c, d\rangle$ represents 1 (use Cor. II.§2.(i)), so we can write $\langle c, d\rangle \cong \langle 1, d'\rangle$, and by comparing determinants we can choose $d' = cd$.

Applying the same argument twice more, we obtain

$$(V, q) \cong \langle 1, a, b, 1, cd\rangle \cong \langle 1, 1, ab, 1, cd\rangle \cong \langle 1, 1, 1, 1, abcd\rangle,$$

and $\langle 1, 1, 1, 1\rangle$ is isometric to (D, N) again by the observation preceding the proposition. But then $\langle 1, 1, 1, 1\rangle$ is universal, since (D, N) is; in particular, it represents $-abcd$, so

(V, q) is isotropic by Cor. II.§2.(i). □

We are now able to completely classify quadratic spaces of arbitrary dimension over any non-archimedean local field (K, v).

Theorem III.§6. *Suppose that (K, v) is non-archimedean, and let (V, q), (V', q') be quadratic spaces of the same dimension n over K. Then $(V, q) \cong (V', q')$ if and only if their determinants and their Hasse symbols are equal.*

Proof. Necessity is clear. As for sufficiency, the proof is by induction on n for $n \geq 4$; the "induction basis" $n \leq 3$ was settled in Thm. III.§4 for arbitrary fields F.

Suppose that $n \geq 4$. Both $V \perp \langle -1 \rangle$ and $V' \perp \langle -1 \rangle$ are isotropic by Prop. III.§6, so both (V, q) and (V', q') represent 1; we can thus write $V \cong \langle 1 \rangle \perp U$ and $V' \cong \langle 1 \rangle \perp U'$ for $(n-1)$-ary subspaces $U \subset V$, $U' \subset V'$. It is immediate from the assumptions on V and V' that $(U, q|_U)$ and $(U', q'|_U)$ have the same determinant and the same Hasse symbol, so by induction we conclude that $U \cong U'$, and the claim follows. □

IV. Quadratic forms over global fields

In this chapter, we finally turn to investigating quadratic forms over general global fields (of characteristic $\neq 2$). As we shall see shortly, the global case essentially reduces to the local case covered in III.§§5-6; this is the content of the fundamental result widely known as "Hasse-Minkowski theorem" (see below), whose proof is the core and ultimate aim of this thesis and makes up most of the present chapter.

The following notations are fixed for the entirety of Chapter IV: we shall consider a global field $(K, \mathcal{O}_K, \mathfrak{M})$ of characteristic $\neq 2$, cf. I.§9, and a **regular** quadratic space (V, q) over K of dimension $n \geq 1$, cf. II.§2. For each $v \in \mathfrak{M}$, let $V_v := V \otimes_K K_v$, cf. III.§1; this is a vector space over K_v in an obvious way, and its dimension is again n, for given a basis $v_1, ..., v_n$ for V over K, the vectors $v_i \otimes 1_{K_v}$ for $i = 1, ..., n$ form a basis for V_v over K_v.

Next, we make V_v into a quadratic space over K_v. Let $v_1, ..., v_n$ be an orthogonal basis for (V, q), and let $a_i = q(v_i)$ for each i. By our earlier observation, each $x \in V_v$ can be written as $x = \sum_{i=1}^n x_i(v_i \otimes 1_{K_v})$ for some $x_i \in K_v$. Then the assignment $x \mapsto \sum_{i=1}^n a_i x_i^2$ defines a map $q_v : V_v \to K_v$, and (V_v, q_v) is indeed an n-ary quadratic space over K_v. Clearly, one can again write $(V_v, q_v) \cong \langle a_1, ..., a_n \rangle$; note that the a_i's are now seen as elements of K_v.

We are now in a position to present the statement of the Hasse-Minkowski Theorem.

Hasse-Minkowski Theorem. *In order for (V, q) to be isotropic, it is necessary and sufficient that (V_v, q_v) be isotropic for each $v \in \mathfrak{M}$.*

It should be noted that, in the literature, the name "Hasse-Minkowski Theorem" (or "Theorem of Minkowski and Hasse", cf. [Kne02]) can be used to refer to as many as three different results, one being the one stated above and the other two being Thm. IV.§6 and Cor. IV.§6; some distinguish between a weak and a strong form of the theorem, while others name Thm. IV.§6 and Cor. IV.§6 the "Strong" and "Weak Hasse Principle" respectively. In order to understand this terminology, it is worth spending a few words on the historical development of these results; we refer to [Sch07] for further reading.

Hermann Minkowski (1864-1909) was the first to provide a full classification of arbitrary quadratic forms over $\mathbb{Q}$ by means of certain invariants, which he defined based on his own earlier (and deeper) results of the theory of quadratic forms *over the integers* $\mathbb{Z}$. Helmut Hasse (1908-1979) had the insight to apply p-adic techniques, first introduced by his advisor Kurt Hensel (1861-1941), to the theory of quadratic forms; this allowed him on the one hand to re-obtain Minkowski's classification result, and on the other hand to derive a fundamental theorem which corresponds to Thm. IV.§6 for $\mathbb{Q}$. Hasse's approach proved successful not only because it was better suited for generalization (Hasse himself extended the "Strong Hasse Principle" to arbitrary algebraic number fields), but also because it paved the way for a series of formally analogous "Hasse principles", or *local-global principles*. As an example, we mention a theorem Hasse proved together with Richard Brauer (1901-1977) and Emmy Noether (1882-1935), which states that *a central simple algebra A over an algebraic number field K is isomorphic to $M_n(K)$ for some n if and only if $A \otimes_K K_v \cong M_n(K_v)$ for all $v \in \mathfrak{M}$.*

In light of the historical digression above, we perceive Kneser's choice "Theorem of Minkowski and Hasse" to be the most accurate; in this thesis, however, we adhere to the convention of writing "Hasse-Minkowski". Following [Ser73], we shall reserve this name for the result stated above, but not for its corollaries in §6.

§1. The special case $K = \mathbb{Q}$

Before we proceed to give the full proof of the Hasse-Minkowski theorem in the general case, see §6, it is worthwhile to present its classical proof over the field of rational numbers $K = \mathbb{Q}$, regarded as a global field with $\mathcal{O}_K = \mathbb{Z}$ and $\mathfrak{M}$ as in Ex. I.§8.(1). Indeed, cf. §2 as well as §6, the general structure of this argument can be preserved for the general case, and one only needs to devise new proofs for a few partial results.

The proof is by induction on $n = \dim V$ for $n \geq 5$; the "induction basis" thus consists of the cases $n = 1, 2, 3$ or 4, each of which is treated individually.

For $n = 1$ the claim is vacuously true. Indeed, any regular isotropic quadratic space (V, q) over K must contain a hyperbolic plane and thus have dimension at least 2, cf. Rmk. II.§3.(3).

Now suppose that $n = 2$, and pick $d \in F^\times$ with $\det V = d \cdot F^{\times 2}$. Upon invoking Cor. II.§2.(ii), we see that the claim is equivalent to the following proposition with $x = -d$.

Proposition IV.§1. *Let $x \in \mathbb{Q}^\times$. Then $x \in \mathbb{Q}^{\times 2}$ if and only if $x \in \mathbb{Q}_p^{\times 2}$ for all $p \leq \infty$.*

Proof. Necessity is obvious. To prove sufficiency, use the fundamental theorem of arithmetic (cf. Ex. I.§8.(1)) to write $x = \varepsilon \cdot \prod_{p \text{ prime}} p^{\nu_p(x)}$, where $\varepsilon \in \{\pm 1\}$ and ν_p is the normalized valuation of $\mathbb{Z}_p$. By the assumption $x \in \mathbb{Q}_\infty^{\times 2} = \mathbb{R}_{>0}$, we infer $\varepsilon = 1$. On the

other hand, for all $p < \infty$ we have $x = y_p^2$ for some $y_p \in \mathbb{Q}_p$, hence $\nu_p(x) = 2\nu_p(y_p)$ is an even integer. But then x is a nonzero square in $\mathbb{Q}$, as claimed. $\square$

We now devote ourselves to the case $n = 3$. We sketch an elementary proof which Serre attributes to Legendre, see [Ser73]; for a different elementary proof see e.g. [BoSh86].

Without loss of generality, we can assume that (V, q) represents 1. For if $r \in \mathbb{Q}^\times$ is any element represented by (V, q), then $(V, \widetilde{q})$, where $\widetilde{q} : V \to \mathbb{Q}$, $x \mapsto \frac{1}{r}q(x)$, is a quadratic space which represents 1, and which is regular and isotropic if and only if (V, q) is regular and isotropic.

Then there exists a diagonalization $(V, q) \cong \langle 1, -a, -b\rangle$ with $a, b \in \mathbb{Q}^\times$. Upon multiplying a, b with elements of $\mathbb{Q}^{\times 2}$, we can assume that $\nu_p(a), \nu_p(b) \in \{0, 1\}$ for all $p < \infty$, i.e., a, b are *squarefree integers*. Furthermore, upon permuting a, b we can assume that $|a| \leq |b|$, where $|\cdot|$ denotes the usual (Euclidean) absolute value $|\cdot|_\infty$.

We proceed by induction on $m = |a| + |b|$. The induction basis is $m = 2$, i.e., $|a| = |b| = 1$; in this case, at least one of a, b must equal 1 (for otherwise (V_∞, q_∞) is positive definite, contradicting the assumption that it represents 0), so it is easy to find an isotropic vector over $\mathbb{Q}$.

Now let $m > 2$, i.e. $|b| \geq 2$. Our strategy is to find some squarefree $b' \in \mathbb{Z}$ with $|b'| < |b|$ such that, if K denotes either $\mathbb{Q}$ or $\mathbb{Q}_p$ for some $p < \infty$, then bb' lies in the image of $N_{K(\sqrt{a})/K}$. Indeed, under this assumption and using the multiplicativity of $N_{K(\sqrt{a})/K}$, we obtain that b is a norm if and only if b' is a norm, which by Thm. III.§3 and Cor. II.§2.(i) means that $\langle 1, -a, -b\rangle$ is isotropic over K if and only if $\langle 1, -a, -b'\rangle$ is isotropic over K, and then we are done by the induction hypothesis.

We proceed as follows: let $p \in \mathbb{Z}_{>0}$ be a prime dividing b. Then by assumption, the equation $x^2 - ay^2 - bz^2 = 0$ has a solution $(x, y, z) \in \mathbb{Q}_p^3$. If $a \not\equiv 0 \pmod{p}$, i.e. $a \in \mathbb{Z}_p^\times$, then upon scaling (x, y, z) we can assume that at least one of x, y, z lies in $\mathbb{Z}_p^\times$. Since by assumption $x^2 - ay^2 \equiv 0 \pmod{p}$, one checks that $y \equiv 0 \pmod{p}$ would lead to a contradiction, hence $y \not\equiv 0 \pmod{p}$ and the residue class of a modulo p is a square. Observe that the last statement also trivially holds under the assumption $a \equiv 0 \pmod{p}$.

By the Chinese Remainder Theorem, we conclude that the residue class of a modulo b is a square, i.e., there exist $-b/2 \leq t < b/2$ and $b'' \in \mathbb{Z}$ with $t^2 = a + bb''$. In other words, if K denotes either $\mathbb{Q}$ or $\mathbb{Q}_p$ for any $p < \infty$, then $bb'' = N_{K(\sqrt{a})/K}(t + \sqrt{a})$. Now write $b'' = b'u^2$ for $u \in \mathbb{Z}$ so that b' is a squarefree integer. Then $|b'| \leq |b''| = |(t^2 - a)/b| \leq |b|/4 + 1 < |b|$, as required, and the proof is complete.

To conclude the induction basis, we consider the case $n = 4$. Write $(V, q) = \langle a_1, a_2, a_3, a_4\rangle$ for $a_i \in \mathbb{Q}^\times$. Since (V_∞, q_∞) is isotropic by assumption, we may assume that $a_1 > 0 > a_4$; moreover, we can assume that all the a_i's are integers, cf. the ternary case. We proceed

to construct an integer $a \in \mathbb{Z}$ such that $\langle a_1, a_2\rangle$ represents a and $\langle a_3, a_4\rangle$ represents $-a$; this will clearly imply that (V, q) represents 0.

Let P denote the set of odd primes which divide at least one of the a_i's. By assumption, for each $p \in P$ there exist $x_1, ..., x_4 \in \mathbb{Q}_p$ with $\sum_{i=1}^4 a_i x_i^2 = 0$. Let $b_p = a_1x_1^2 + a_2x_2^2 = -a_3x_3^2 - a_4x_4^2$. If $b_p = 0$, i.e. if both $\langle a_1, a_2\rangle$ and $\langle a_3, a_4\rangle$ are isotropic over $\mathbb{Q}_p$, then they are both universal by Thm. II.§2, so we can pick b_p to be any nonzero element of $\mathbb{Q}_p$ which they both represent. By scaling[1] the x_i's, we can finally assume the following: *for each $p \in P$, we have $b_p \in \mathbb{Z}_p$, $b_p \neq 0$ and $\nu_p(b_p) \leq 1$.*

The proof is complete if we can construct a positive integer $a \in \mathbb{Z}_{>0}$ with:

(i) $a\mathbb{Q}_p^{\times 2} = b_p\mathbb{Q}_p^{\times 2}$ for all $p \in \{2\} \cup P$;

(ii) at most one of the prime factors of a is *not* an element of $\{2\} \cup P$.

For consider the regular ternary spaces $U = \langle a_1, a_2, -a\rangle$ and $W = \langle a, a_3, a_4\rangle$. Since $a_1 > 0 > a_4$, each represents 0 over $\mathbb{Q}_\infty = \mathbb{R}$. For $p \in \{2\} \cup P$, condition (i) tells us that U and W represent 0 over $\mathbb{Q}_p$, for $\langle a_1, a_2, -b_p\rangle$ and $\langle b_p, a_3, a_4\rangle$ are isotropic by definition of b_p. Finally, if p is an odd prime which divides none of $a_1, ..., a_4, a$, then both spaces are isotropic over $\mathbb{Q}_p$ by Ex. III.§6. By condition (ii), there remains at most one prime p' for which U or W may not represent 0.

We now resort to Artin's reciprocity law, cf. Rmk. III.§6.(2). This equation, when combined with Cor. II.§2.(i), tells us that, if $c, d \in \mathbb{Q}^\times$ and $\langle c, d, -1\rangle$ is isotropic over $\mathbb{Q}_p$ for all $p \leq \infty$ *except at most one*, then it is already isotropic over *all* $\mathbb{Q}_p$, $p \leq \infty$. One can now infer that U and W are isotropic over all $\mathbb{Q}_p$, $p \leq \infty$, hence they are isotropic over $\mathbb{Q}$ by the ternary case, and we are indeed done.

It remains to construct $a \in \mathbb{Z}_{>0}$ with the required properties (i)-(ii). In order for (i) to hold, it suffices that $ab_p^{-1} \in 1 + p^{2\nu_p(2)+1}\mathbb{Z}_p$ by Rmk. II.§4.(3). But then we only have to solve the system of congruences[2]

$$\begin{aligned} a &\equiv b_2 \pmod{16}, \\ a &\equiv b_p \pmod{p^2}, \qquad p \in P, \end{aligned}$$

which by the Chinese Remainder Theorem has infinitely many solutions in $\mathbb{Z}_{>0}$. Note that the residue class modulo $m = 16\prod_{p\in P} p^2$ of these solutions is uniquely determined.

Let a' be a solution to the above congruences, and let d denote the greatest common divisor of m and a'. We apply **Dirichlet's theorem** on primes in arithmetic progressions: if $n, l \in \mathbb{Z}$ are relatively prime, then there exists $k \geq 0$ such that $n + kl$ is a prime.

[1] Here we make the implicit assumption that the x_i's can be chosen all different from 0. This is indeed no loss of generality, cf. e.g. [BoSh86], Algebraic Supplement, Theorem 8.

[2] For $p \in P \cup \{2\}$, the element $b_p \in \mathbb{Z}_p$ has a representation $b_p = \sum_{i\geq 0} c_i p^i$ by I.§6. Thus, the congruence $a \equiv b_p \pmod{p^2}$ is to be understood as $a \equiv c_0 + c_1 p \pmod{p^2}$, where the right-hand side is of course in $\mathbb{Z}$.

In our case, $l = m/d$, $n = a'/d$; we obtain that $a'/d + km/d =: p'$ is a prime for some $k \geq 0$. But then $a = a' + km = dp'$ again solves the above system of congruences and additionally satisfies condition (ii), as required, and the quaternary case is proved.

It is now time for the induction step. Thus, we henceforth assume that (V, q) is an n-ary regular quadratic space over $\mathbb{Q}$ with $n \geq 5$. We write $(V, q) \cong \langle a_1, ..., a_n \rangle$, where again we may assume that $a_i \in \mathbb{Z}$; further, let $U = \langle a_1, a_2 \rangle \subseteq V$ and $W = \langle a_3, ..., a_n \rangle = U^\perp \subseteq V$.

Similarly as for $n = 4$, we aim to find some $a \in \mathbb{Q}$ such that a is represented by U and $-a$ is represented by W. First, we repeat the argument made before to see that for each $p \leq \infty$ there exists some $b_p \in \mathbb{Q}_p^\times$ so that U_p represents b_p and W_p represents $-b_p$. Let $S = \{p \text{ odd} : p | a_i \text{ for some } i \geq 3\} \cup \{2, \infty\}$. Again by Rmk. II.§4.(3), we see that it suffices to make $|ab_p^{-1} - 1|_p$ sufficiently small for all $p \in S$; however, we cannot again formulate this in terms of congruences since S contains the infinite place of $\mathbb{Q}$.

Instead, we proceed as follows: for $p \in S$ pick $x_p, y_p \in \mathbb{Q}_p^\times$ with $a_1 x_p^2 + a_2 y_p^2 = b_p$, and find $x, y \in \mathbb{Q}$ so that $a = a_1 x^2 + a_2 y^2$ makes $|ab_p^{-1} - 1|_p$ sufficiently small for all $p \in S$. This is achieved applying the following valuation-theoretical analogue of the Chinese Remainder Theorem, where $x_1, ..., x_r$ are of course to be replaced by $\{x_p, p \in S\}$ and $\{y_p, p \in S\}$ respectively.

Lemma IV.§1 (Artin-Whaples Approximation Theorem)**.** *Let $S = \{v_1, ..., v_r\}$ be a finite set of nontrivial places on a field K, and for each i let $|\cdot|_i$ be an absolute value on K which induces v_i. Then, for any given $x_1, ..., x_r \in K$ and for each $\varepsilon > 0$ there exists some $x \in K$ with $|x - x_i|_i < \varepsilon$ for all i.*

Proof. First, we claim that for each i there exists some $z_i \in K$ with $|z_i|_i > 1, |z_i|_j < 1$ for $j \neq i$. This is proved by induction on $r = \#S$. If $r = 1$, then the claim is equivalent to $|\cdot|_1$ being nontrivial. If $r = 2$, then we can pick $\xi_1, \xi_2 \in K^\times$ with $|\xi_1|_1 < 1 \leq |\xi_1|_2$ and $|\xi_2|_2 < 1 \leq |\xi_2|_1$ and set $z_1 = \xi_1/\xi_2$ as well as $z_2 = \xi_2/\xi_1$.

Now let $r > 2$, and fix $i \in \{1, ..., r\}$. Choose $k \neq i$. By the induction hypothesis, there exists some ξ with $|\xi|_i > 1, |\xi|_j < 1$ for all $j \neq i$, $j \neq k$, and there exists some ζ with $|\zeta|_i > 1, |\zeta|_k < 1$. If $|\xi|_k < 1$, then there is nothing left to prove. If $|\xi|_k = 1$, then we can choose $z_i = \zeta \xi^l$ for sufficiently large $l \in \mathbb{N}$. Finally, if $|\xi|_k > 1$, then we can choose $z_i = \zeta \xi^l / (1 + \xi^l)$ for l sufficiently large, and the claim is proved.

Thus, let $z_i \in K$ be as above, and for $m \in \mathbb{N}$ define $\xi_m = \sum_{i=1}^r \frac{x_i z_i^m}{1 + z_i^m}$. For each i, $|\xi_m - x_i|_i$ becomes arbitrarily small as m goes to infinity, so we can choose $x = \xi_m$ for some sufficiently large m. □

To summarize, the lemma tells us that for ε small enough we can find some a with the required properties. Consider $W' := \langle a, a_3, ..., a_n \rangle$. Then W'_p is isotropic for $p \notin S$ since $W_p \subseteq W'_p$ is isotropic by Ex. III.§6, and it is also isotropic for $p \in S$ by the construction

of a. Hence, W' represents 0 over $\mathbb{Q}$ by the induction hypothesis. But then $V \supseteq W'$ also represents 0, and the proof of the Hasse-Minkowski theorem for the rational field $\mathbb{Q}$ is complete.

§2. Strategy for generalization

In this section, we take a closer look at the argument presented in §1 and discuss how it can be modified so that it carries over to the general case. In doing so, we shall essentially outline the content of the following sections.

First, we observe that, if we are able to generalize Prop. IV.§1 to arbitrary global fields, then the Hasse-Minkowski Theorem for $n = 2$ will also carry over with precisely the same proof. In order to formulate and prove the appropriate generalization, we shall resort to the formalism of idèles, which we now introduce. For the given global field K, consider the multiplicative group $\prod_{v\in\mathfrak{M}} K_v^\times$. An *idèle over* K is an element $(i_v)_v$ of this product with the property that there are at most finitely many $v \in \mathfrak{M}$ with $|i_v|_v \neq 1$; clearly, the idèles over K form a group, denoted J_K. Note that, if $x \in K^\times$, then $(x)_v$ is an idèle by axiom (G2) for global fields; idèles of this form are called *principal idèles*, and form a subgroup of J_K which we identify with $K^\times$.

Remark. (1) The group J_K of idèles is precisely the group of units of the ring of adèles $\mathbb{A}_K$ introduced in Rmk. I.§8. Starting from the topology on $\mathbb{A}_K$, one can make J_K into a topological group (caution: the topology on J_K is *not* the subspace topology!). ⋄

Now let $(L, \mathcal{O}_L, \mathfrak{N})$ be a global field such that L/K is a finite-degree extension, and let $j = (j_w)_{w\in\mathfrak{N}} \in J_L$. For each $v \in \mathfrak{M}$, define $i_v \in K_v$ as $i_v = \prod_{w|v} N_{L_w/K_v}(j_w)$: it is easy to check that $i = (i_v)_{v\in\mathfrak{M}}$ is an idèle over K, so we have defined a map $J_L \to J_K$. Since its restriction to the subgroup $L^\times$ of principal idèles over L is precisely the norm $N_{L/K}$, cf. I.§9, we agree to denote this map again by $N_{L/K}$.

We shall take a closer look at the quadratic case, i.e. $[L : K] = 2$. By Prop. I.§9.(iii), for each $v \in \mathfrak{M}$ there are at most two places in $\mathfrak{N}$ which divide v. If there is a unique place $w \in \mathfrak{N}$ with $w|v$, then repeating the argument in the proof of Prop. I.§9.(iii) one finds that $[L_w : K_v] = 2$; otherwise, there exist two distinct places $w_1, w_2 \in \mathfrak{N}$ which divide v, and $L_{w_1} = K_v = L_{w_2}$. We denote by $\mathfrak{M}' \subset \mathfrak{M}$ the set of places of the first kind, and by $\mathfrak{M}''$ the set of places of the second kind.

Remark. (2) Let L be as above, with the additional assumption $[L : K] = 2$; further let $i = (i_v)_{v\in\mathfrak{M}} \in J_K$, and suppose that i lies in $N_{L/K}(J_L)$. Then clearly $i_v \in N_{L_w/K_v}(L_w)$ whenever $v \in \mathfrak{M}'$ by the definitions.

Conversely, suppose that for each $v \in \mathfrak{M}'$ there exists some $j_w \in L_w$ with $i_v = N_{L_w/K_v}(j_w)$. Then we can choose $j_{w_1} = i_v \in K_v = L_{w_1}$ and $j_{w_2} = 1 \in L_{w_2}$, where w_1, w_2 are the two places which divide v, and then verify directly that $j = (j_w)_{w \in \mathfrak{N}}$ lies in J_L and satisfies $N_{L/K}(j) = i$. $\diamond$

We are now in a position to formulate the sought-after generalization of Prop. IV.§1:

Theorem IV.§2 (Global Square Theorem)**.** *Let $\beta \in K^\times$, and suppose that $\{v \in \mathfrak{M} : \beta \notin K_v^{\times 2}\}$ is a finite set. Then $\beta \in K^{\times 2}$.*

The outline of the proof is as follows. Suppose for the sake of contradiction that β is not a square in K, and let $L \supseteq K$ be a splitting field of $g(t) = t^2 - \beta$ over K. As in Rmk. III.§2.(3), we find that $L = K(\delta)$, where δ is a root of $g(t)$ over L, and clearly $[L : K] = 2$. The above observations apply, so we can define $\mathfrak{M}'$ and $\mathfrak{M}''$ as mentioned in the quadratic case, and it is easy to see that $\mathfrak{M}' = \{v \in \mathfrak{M} : \beta \notin K_v^{\times 2}\}$ and accordingly $\mathfrak{M}'' = \{v \in \mathfrak{M} : \beta \in K_v^{\times 2}\}$.

Now let $S \supseteq \mathfrak{M}'$ denote a finite set containing all places v for which $|\beta|_v \neq 1$. If $i = (i_v)_v \in J_K$ is an arbitrary idèle, then an application of the Artin-Whaples Approximation Theorem, see §1, yields some $x \in K^\times$ such that $xi_v^{-1} \in K_v^{\times 2}$ for all $v \in S$. Then $x^{-1}i$ is in the image of $N_{L/K}$ by Rmk.(2). Thus, we will have achieved the sought-after contradiction (and established the Global Square Theorem) if we can prove that the subgroup $K^\times \cdot N_{L/K}(J_L)$ has index at least 2 in J_K.

In light of the above discussion, we can now establish a programme for the rest of the chapter. In §3, we shall only work with the global field K and consider a fixed set of places $\Omega \subset \mathfrak{M}$ with the following properties:

(a) every $v \in \Omega$ is non-archimedean;

(b) the set-theoretic complement $S = \mathfrak{M} \setminus \Omega$ has a finite number $s \geq 1$ of elements.

For a given Ω as above, we shall look at $U(\Omega) := \bigcap_{v \in \Omega} \mathfrak{u}(v) = \{x \in K : |x|_v = 1 \text{ for all } v \in \Omega\}$. The main result of the section is a structure theorem for $U(\Omega)$ which generalizes Dirichlet's Unit Theorem from algebraic number theory, cf. §3 for more details.

In §4, we shall fix an element $\beta \in K$, $\beta \notin K^{\times 2}$ and again consider $L = K(\delta)$ with $\delta^2 = \beta$ as above. A consequence of Thm. IV.§3 is that one can always find a set Ω as above with certain additional properties; we shall use this fact to establish the inequality $[J_K : K^\times N_{L/K}(J_L)] \geq 2$ from above.

Next, in §5 we shall refine our previous result and show that $[J_K : K^\times N_{L/K}(J_L)] = 2$. In particular, this equality will imply the following local-global principle, which turns out to be essentially equivalent to the Hasse-Minkowski theorem for $n = 3$: in order for $x \in K$ to lie in the image of $N_{L/K}$, it is sufficient that x lie in the image of N_{L_w/K_v} for any pair of places $w \in \mathfrak{N}$, $v \in \mathfrak{M}$ with $w|v$.

Finally, in §6 we shall prove the Hasse-Minkowski theorem as stated in the preamble to the present chapter and thus conclude our study of quadratic forms over global fields.

§3. Dirichlet's Unit Theorem

In this section, we prove a generalized version of Dirichlet's Unit Theorem, following the programme outlined in the previous section. Mind that many notations from previous chapters will be used freely in the sequel, especially the ones from I.§§8-9.

Consider the group J_K of idèles over K, cf. §2. For any $i = (i_v)_v \in J_K$, the product $\prod_{v\in\mathfrak{M}}|i_v|_v$ is defined; it is called the *volume* of i and denoted $\|i\|$. Further, we say that i *bounds* an element $x \in K$ if $|x|_v \leq |i_v|_v$ for all $v \in \mathfrak{M}$, and denote with $M(i)$ the set of elements of K which are bounded by i.

Lemma IV.§3. *Each idèle $i \in J_K$ bounds at most finitely many elements of K. More precisely, there exists a constant $D > 0$ such that $M(i) \leq \max\{1, D\|i\|\}$ for all $i \in J_K$.*

Proof. Fix a non-archimedean place v_0 of K. Upon multiplication with some element $y \in K^\times$, we can assume that $\left|i_{v_0}\right|_{v_0} = 1$; note that this does not affect the situation since $\|yi\| = \|i\|$, and x is bounded by i if and only if yx is bounded by yi.

If i bounds only $0 \in K$, we are trivially done. Otherwise, let X be a finite subset of K such that all elements of X are bounded by i; by our earlier assumption, $X \subseteq \mathfrak{o}(v_0)$. Now let M denote the cardinality of X, and pick $r \geq 0$ so that $q^r < M \leq q^{r+1}$, where $q = \#k(v_0)$ is the cardinality of the residue field of $\mathfrak{o}(v_0)$. Observe that, for all r, q^r is precisely the cardinality of the quotient ring $\mathfrak{o}(v_0)/\mathfrak{m}(v_0)^r$, so by the pigeonhole principle there exist $x_1, x_2 \in X$ with $x_1 - x_2 \in \mathfrak{m}(v_0)^r$. In particular, $|x_1 - x_2|_{v_0} \leq q^{-r} \leq q/M$ by definition of the normalized absolute value $|\cdot|_{v_0}$.

On the other hand, if $v \neq v_0$ is non-archimedean, then $|x_1 - x_2|_v \leq |i_v|_v$ by the strong triangle inequality, and if v is archimedean then $|x_1 - x_2|_v \leq 2|i_v|_v$. Now the product formula yields $1 = \prod_v |x_1 - x_2|_v^{\rho_v} \leq 4^\omega q\|i\|/M$, where ω is the number of archimedean places of K, which is finite by I.§9. In particular, $M = \#X$ is bounded above and the lemma is proved. □

Remark. (1) Let $M > 0$ be a positive constant, and consider elements $x_0, ..., x_M \in K$, where $x_0 = 0$. Then, for all but finitely many $v \in \mathfrak{M}$, we have $\left|x_i - x_j\right|_v = 1$ whenever $i \neq j$ by the product formula; we claim that, for each such v which is non-archimedean, we have $\#k(v) > M$. For suppose the contrary: then an application of the pigeonhole principle shows that there exist $i \neq j$ with $x_i - x_j \in \mathfrak{m}(v)$, contradicting the assumption about v, cf. also the proof of the lemma. In particular, *there are at most finitely many non-archimedean places $v \in \mathfrak{M}$ with $\#k(v) \leq M$.*

(2) Surprisingly, the above lemma is essentially sufficient to derive a classification of global fields. Indeed, we saw in I.§8 that K contains a field K_0 which is isomorphic either to $\mathbb{Q}$ or to $F(t)$ for some finite field F; let $x_1, ..., x_l$ be elements of K which are linearly independent over K_0, let y be some element of $\mathcal{O}_{K_0}$ (i.e. an integer, if K has archimedean places, and a polynomial with coefficients in F otherwise) and consider

$$\mathfrak{S} = \mathfrak{S}(x_1, ..., x_l; y) := \left\{ \sum_{i=1}^{l} a_i x_i : a_i \in \mathcal{O}_{K_0},\ |a_i|_\infty \leq |y|_\infty \ \ \forall i \right\},$$

where v_∞ is the unique infinite place of K_0. Upon distinguishing the cases $K_0 = \mathbb{Q}$, $K_0 = F(t)$, one directly checks that $\#\mathfrak{S} > |y|_\infty^l$, and so the lemma, combined with our results on extensions of valued fields from I.§§7-9, yields

$$|y|_\infty^l \leq D'\|y\| = D' \prod_{v \in S_\infty} |y|_v = D' |y|_\infty^{\sum_{v \in S_\infty} [L_v : K_\infty]}$$

for some positive constant D'. Since $|y|_\infty$ can take arbitrarily large values, we conclude that $l \leq \sum [L_v : K_\infty] < \infty$, and so *the dimension of K over K_0 is finite*, and accordingly *every global field is a finite-degree extension of either $\mathbb{Q}$ or $F(t)$ for a finite field F.* $\diamond$

We now prove that every idèle whose volume is sufficiently large bounds at least one nonzero element of K.

Proposition IV.§3. *There exists some positive constant C such that $M(i) \geq C\|i\|$ for all $i \in J_K$.*

Sketch of proof. The idea of the proof is to find idèles $j, j' \in J_K$ such that $|j_v|_v < |i_v|_v < |j'_v|_v$ for every place v, and subsequently obtain a lower estimate for $M(j) \leq M(i)$; then C can be chosen to be any positive constant less than $M(j)/\|j'\| < M(i)/\|i\|$.

The first step uses the construction and conclusions of Rmk.(2): one picks a basis $x_1, ..., x_l$ for K over K_0 and finds (e.g. using the Artin-Whaples Approximation Theorem) a positive constant B depending only on $x_1, ..., x_l$ such that $\mathfrak{S}(x_1, ..., x_l; y) \leq B|y|_\infty$ for every $y \in \mathcal{O}_K$. Another application of the Approximation Theorem shows that, upon scaling, one can assume that $|i_v|_v \leq 1$ for every finite place v and $|yB^2|_v < |i_v|_v < |yB^4|_v$ if v is infinite, where y is a certain element of $\mathcal{O}_K$. Using these inequalities, it is easy to define j, j' with the required property.

To obtain the required estimate for $M(j)$, one defines an ideal I of $\mathcal{O}_K$ with the property that $\#(\mathcal{O}_K/I) = \prod_{v \text{ finite}} |i_v|_v^{-1}$, and uses the pigeonhole principle, together with the inequality $\#\mathfrak{S}(x_1, ..., x_l; y) > |y|_\infty^l$ from Rmk.(2), to obtain that $M(j) > |y|_\infty^l \#(\mathcal{O}_K/I)$. A direct computation shows $M(j)/\|j'\| > \prod_{v \text{ infinite}} |B^4|_v^{-1}$, so C can be taken to be the constant on the right-hand side. $\square$

Having derived the necessary results about idèles, we return to the situation addressed in the previous section; in particular, we freely use the notations Ω, S, s, $U(\Omega)$ as defined in §2.

Theorem IV.§3. *Suppose that $s \geq 2$. Then:*

(i) Let $v \in S$. Then there exists some $\varepsilon_v \in U(\Omega)$ such that $|\varepsilon_v|_v < 1$ and $|\varepsilon_v|_w > 1$ for all $w \in S$ with $w \neq v$.

(ii) Let ε_v as in part (i) be given for each $v \in S$. Then for $v_0 \in S$, the $s-1$ elements ε_v with $v \in S$, $v \neq v_0$ are multiplicatively independent and generate a subgroup $H \subseteq U(\Omega)$ of finite index.

Proof. (i) Let $q = \#k(v)$ if v is non-archimedean; otherwise, set $q = 1$. Let C denote the constant from Prop. IV.§3 and consider the set $T = \{w \in \Omega : \#k(w) \leq q/C\} \subset \Omega$; then T is finite by Rmk.(1), and upon taking a smaller C we can assume that T is non-empty.

Now let $X = \{x \in K : C/q \leq |x|_w \leq 1 \text{ for all } w \in \Omega\}$. If $x \in X$ and $w \in \Omega$, $w \notin T$, then we find that $1/\#k(w) < |x|_w \leq 1$; but then necessarily $|x|_w = 1$ since $|\cdot|_w$ is itself a power of $\#k(w)$. On the other hand, if $w \in T$ then the image of X under $|\cdot|_w$ is a finite set, therefore we can find $x_1, ..., x_r \in X$ with $X = \bigcup_{i=1}^r x_i U(\Omega)$.

We claim that there exists some $i \in J_K$ with the following properties:

1. $|i_w|_w = 1$ for all $w \in \Omega$;
2. $|i_w|_w < |x_i|_w$ for all $1 \leq i \leq r$ and all $w \in S$, $w \neq v$;
3. $1 \leq C\|i\| \leq q$.

In fact, suppose that i_w is already chosen for every $w \in \Omega$, $w \neq v$. If v is archimedean then $|\cdot|_v$ takes on any real positive value, so we can choose i_v as we wish; otherwise, let m be an integer with $q^m \leq C \prod_{w \neq v} |i_w|_w \leq q^{m+1}$ and choose $i_v \in K_v$ so that $|i_v|_v = q^{-m}$.

Now, since $C\|i\| \geq 1$, there is at least one nonzero element $x \in K$ which is bounded by i by Prop. IV.§3; in particular, $\prod_{w \in S} |x|_w \leq q/C$. But then one readily checks that $x \in X$, so $x = \varepsilon_v x_i$ for some $\varepsilon_v \in U(\Omega)$ and some $1 \leq i \leq r$. An easy computation, together with the product formula, shows that ε_v satisfies the required properties.

(ii) Let $T = S \setminus \{v_0\}$. Then the first claim reads: if $\prod_{v \in T} \varepsilon_v^{l_v} = 1$ for integers l_v, then $l_v = 0$ for all v. Suppose that such a formula holds and for some l_v not all zero; we can assume that $P = \{v \in T : l_v > 0\}$ is non-empty. Then direct inspection shows that $\alpha = \prod_{v \in P} \varepsilon_v^{l_v} = \prod_{v \in T \setminus P} \varepsilon_v^{-l_v}$ satisfies $|\alpha|_v \leq 1$ for all $v \in \mathfrak{M}$ and $|\alpha|_{v_0} < 1$, contradicting the product formula.

As for the second claim, we show that, for each $x \in U(\Omega)$, there exists some $u \in H$ so that xu^{-1} is bounded by the idèle $i \in J_K$ whose components are given by $i_v = \varepsilon_v$ for $v \in T$ and $i_v = 1$ otherwise. The claim will then follow using Lemma IV.§3.

First, note that there exists some $u_0 \in H$ which is bounded by i and which satisfies $|u_0|_{v_0} < 1$ and $|u_0|_v > 1$ for all $v \in T$. Indeed, the finite set $\{y \in H : y \text{ is bounded by}$

$i\}$ is non-empty (it contains 1), so it contains an element u_0 for which $|u_0|_{v_0}$ is minimal, and if $|u_0|_v$ were greater than or equal to 1 for some $v \in T$, then $\varepsilon_v u_0 \in H$ would be bounded by i and satisfy $|\varepsilon_v u_0|_{v_0} < |u_0|_{v_0}$, contradicting our choice of u_0.

Now consider the set $\{u \in H : xu^{-1} \leq |\varepsilon_v|_v \text{ for all } v \in S\}$. Again, it is non-empty (e.g., it contains u_0^m for m sufficiently large), and an argument analogous to the above one yields some element u of this set so that $z = xu^{-1}$ satisfies $|z|_{v_0} < 1$ and $|z|_v > 1$ for all $v \in T$, i.e., z is bounded by i. □

We immediately obtain the following corollary:

Corollary IV.§3 (Dirichlet's Unit Theorem)**.** *The abelian group $U(\Omega)$ is finitely generated of rank $s-1$, and its torsion subgroup equals the group of roots of unity in K.*

Proof. First suppose that $s = 1$. If $x \in U(\Omega)$, i.e., $|x|_v = 1$ for all $v \in \mathfrak{M}$ except for the single element v_0 of S, then the product formula forces $|x|_v = 1$ for *all* v, i.e., x is an element of $\mu := \bigcap_{v\in\mathfrak{M}} \mathfrak{u}(v)$. Clearly, every root of unity in K is contained in μ; conversely, note that all elements of μ are bounded by the idèle $(1)_{v\in\mathfrak{M}}$, so μ is a finite group by Lemma IV.§3 and accordingly each of its elements is a root of unity.

If, instead, $s > 1$, then Thm. IV.§3 yields a subgroup H of rank $s-1$ which has finite index in $U(\Omega)$, so $U(\Omega)$ is indeed finitely generated. Since there are no relations between the generators of H, we have that H is free abelian of rank $s-1$, so the rank of $U(\Omega)$ is again $s-1$. As for the torsion subgroup of $U(\Omega)$, clearly all its elements must be roots of unity; conversely, every root of unity is contained in $\mu \subseteq U(\Omega)$. □

Remark. (3) Let $J(\Omega) := \{i = (i_v)_v \in J_K : |i_v|_v = 1 \text{ for all } v \in \Omega\}$. An argument similar to the one in the proof of Thm. IV.§3.(i) shows that, for any $i' = (i'_v)_v \in J_K$, there exists some $x \in K^\times$ such that $\left|xi'_v\right|_v = 1$ for all but finitely many $v \in \mathfrak{M}$, and for $v \in \Omega$ there are only a finite number of possibilities for $\left|xi'_v\right|_v$.

Accordingly, one can find a finite set I of idèles such that, for any $i' \in J_K$, there exists some $i = (i_v)_v \in I$ with $\left|xi'_v\right|_v = |i_v|_v$ for all $v \in \Omega$. But this means precisely that $xi' = i \cdot i_0$, where $i_0 \in J(\Omega)$. In other words, *the subgroup $K^\times \cdot J(\Omega)$ of J_K is of finite index*: this can be seen as a generalization of the classical result that *the ideal class number is finite* for an algebraic number field, see [O'M73], §33.

(3') Let $\widetilde{\Omega} \subseteq \Omega$ be a subset satisfying (a)-(b) from §2 and such that $|i_v|_v = 1$ for all $i \in I$ and $v \in \Omega$; by definition of idèles, it is always possible to find such a set $\widetilde{\Omega}$, e.g. by removing from Ω all the (finitely many) places v such that $|i_v|_v \neq 1$ for some $i \in I$. Then the index of $K^\times \cdot J(\widetilde{\Omega})$ in J_K is necessarily 1, i.e. $J_K = K^\times \cdot J(\widetilde{\Omega})$. ◇

§4. The Global Square Theorem

This section is devoted to completing the proof of the Global Square Theorem, see §2. Thus, throughout the section we consider a fixed $\beta \in K$ and we suppose that $\beta \notin K^{\times 2}$. The notations $\mathfrak{M}'$, $\mathfrak{M}''$, $L = K(\delta)$ and $N_{L/K} : J_L \to J_K$ shall be used freely.

As we saw in §2, the missing piece to prove the Global Square Theorem is the inequality $[J_K : K^\times N_{L/K}(J_L)] \geq 2$. The key observation is that, by discarding finitely many places and working with a subset $\Omega \subset \mathfrak{M}$ as in §2, some index computations becomes easier. The set Ω will be chosen so that it satisfies properties (a)-(b) from §2 as well as:

(c) for each $v \in \Omega, |\beta|_v = 1$;
(d) for each $v \in \Omega$ the local field (K_v, v) is nondyadic, cf. II.§4;
(e) $J_K = K^\times \cdot J(\Omega)$;
(f) $J_L = L^\times \cdot J(\Omega')$, where $\Omega' = \{w \in \mathfrak{N} : w|v \text{ for some } v \in \Omega\}$.

To see that such an Ω exists, first note that, if Ω has property (a) or (c), then so does each of its subsets; moreover, if Ω has property (b), (e) or (f), and if $\widetilde{\Omega} \subseteq \Omega$ is a subset such that $\Omega \setminus \widetilde{\Omega}$ is finite, then by Rmk. §3.(3') we see that $\widetilde{\Omega}$ again satisfies (b), (e) or (f)). Now the product formula tells us that there are at most finitely many places in $\mathfrak{M}$ which violate (c); similarly, since (K_v, v) is dyadic if and only if $|2|_v < 1$, there are at most finitely many places in $\mathfrak{M}$ which violate (d), and the existence of Ω with (a)-(f) follows.

For the sake of brevity, we make the following convention: we shall henceforth denote $N_{L/K}$ simply as N and $J(\Omega)$, $J(\Omega')$, $U(\Omega)$, $U(\Omega')$ simply by J, J', U and U' respectively. Moreover, we set $m := [J_K : K^\times N(J_L)]$.

The first observation is that, if Ω satisfies properties (a)-(e), then $N(U') \subseteq U$. Indeed, for every $v \in \Omega$ and every $w|v$ we have $N_{L_w/K_v}(\mathfrak{u}(w)) = \mathfrak{u}(v)$ by (c), cf. Rmk. III.§5.(4'). Moreover, combining this with Rmk. §2.(2), one readily obtains a description of $N(J')$; indeed, this is the set of idèles $i = (i_v)_v \in J$ such that $i_v \in N_{L_w/K_v}(L_w)$ whenever $v \in \mathfrak{M}' \cap S$ and $w|v$. In particular, $N(J') \subseteq J$.

Now, by properties (e)-(f), we can write $m = [K^\times J : K^\times N(L^\times J')]$. But $N(L^\times) \subseteq K^\times$, and $K^\times J = JK^\times N(J')$, so $m = [J : K^\times N(J') \cap J]$ by the isomorphism theorems of group theory. Clearly the intersection right of the colon is just $UN(J')$, so, again by the isomorphism theorems, we obtain

$$m = \frac{[J : N(J')][U \cap N(J') : N(U')]}{[U : N(U')]}. \qquad (*)$$

In the remainder of this section, we shall compute $[J : N(J')]$ and $[U : N(U')]$ and show that their ratio equals 2; since the remaining index is necessarily a positive integer, the claim will follow.

The index $[J : N(J')]$ is easy to compute; indeed, let Ω satisfy properties (a)-(e) and consider the group homomorphism $J \to \prod_{v \in S} K_v^\times$ which sends $i = (i_v)_v$ to $(i_v)_{v \in S}$. By our above characterization of $N(J')$, the image of $N(J')$ under this homomorphism is

$$\prod_{v \in S \cap \mathfrak{M}''} K_v^\times \times \prod_{\substack{v \in S \cap \mathfrak{M}' \\ w|v}} N_{L_w/K_v}(L_w^\times),$$

and so $[J : N(J')] = \prod_{v,w} [K_v^\times : N_{L_w/K_v}(L_w^\times)]$, where the product ranges over $v \in S \cap \mathfrak{M}'$ and $w|v$. But for each $v \in \mathfrak{M}'$ there is precisely one place $w|v$, and by Rmk. III.§6.(1) each index on the right-hand side equals 2, so $[J : N(J')] = 2^b$, where $b = \#(S \cap \mathfrak{M}')$.

As for $[U : N(U')]$, we again only assume that Ω satisfies (a)-(e). We shall need the following lemma, which is often introduced in the context of class field theory; it is called the **Q-machine** in [Lan94]. In this formulation, it can easily be proved by twofold application of the group-theoretic result used in the proof of Thm. II.§4.(iii) together with the isomorphism theorems.

Lemma IV.§4. *Let $G = (G, \cdot)$ be an abelian group, and suppose that there are group endomorphisms $N, T : G \to G$ such that $N \circ T = T \circ N$ sends all of G to 1. If H is a subgroup such that both $N(H) \subseteq H$ and $T(H) \subseteq H$, let $Q(H)$ denote the* ***Herbrand quotient***

$$Q(H) := \frac{[\ker T \cap H : N(H)]}{[\ker N \cap H : T(H)]},$$

provided that both indices on the right-hand side are finite. If H is of finite index in G and if $Q(H)$ is defined, then $Q(G) = Q(H)$.

We now sketch how the lemma can be used to derive the desired result. In our case, the group G will be U', and, as the notation suggests, the map N will of course be the norm $N_{L/K}$, restricted to $U' \subset L^\times$. Recall that, for $\alpha = c_0 + c_1\delta \in L$, we can write $N(\alpha) = \alpha\sigma(\alpha)$, where $\sigma(\alpha) = c_0 - c_1\delta$, cf. Rmk. III.§5.(4'). We define $T(\alpha) := \alpha/\sigma(\alpha)$ for $\alpha \in U'$. As for the subgroup H, we use Dirichlet's Unit Theorem, combined with the structure theorem for finitely generated abelian groups, to write U as a product of its torsion subgroup with a free subgroup $\widetilde{H}$ of rank $s - 1$, and define $H = \widetilde{H} \cdot T(U')$.

One now verifies that the assumptions of the lemma are all satisfied, and so

$$\frac{[\ker T : N(U')]}{[\ker N : T(U')]} = \frac{[\ker T \cap H : N(H)]}{[\ker N \cap H : T(H)]}.$$

Note that the numerator on the left-hand side is precisely the required index $[U : N(U')]$, for $\ker T = \{\alpha \in U' : \alpha = \sigma(\alpha)\} = U' \cap K = U$. Thus, it suffices to compute the remaining indices.

The numerator on the right-hand side is readily computed once we see that $N(H) = N(\widetilde{H}) = \widetilde{H}^2$ and $\ker T \cap H = \{\pm 1\} \cdot \widetilde{H}$; indeed, by the structure theorem for finitely generated abelian groups and the isomorphism theorems we can write the index $[\ker T \cap H : N(H)] = [\ker T \cap H : (\ker T \cap H)^2]$ as a product of indices $[G : G^2]$, where G is either a finite group or a copy of the additive integers, and we obtain $[\ker T \cap H : N(H)] = 2^s$ since $\widetilde{H}$ has rank $s-1$. Similarly, one checks that $\ker N \cap H = T(U')$ and $T(H) = T(U')^2$ and computes that the denominator on the right-hand side equals 2^{s+1-b}.

It remains to compute $[\ker N : T(U')]$; this is slightly more technical, and one needs property (e) of Ω as well as the fact that L_w/K_v is unramified, cf. III.§5, at every place $v \in \Omega$; a complete proof can be found in [O'M73], 65:10, step 4). As it turns out, we have equality $T(U') = \ker N$. Putting together all these computations, we obtain

$$[U : N(U')] = 2^s/2^{s+1-b} = 2^{b-1} = [J : N(J')]/2,$$

as claimed, and the proof of the Global Square Theorem is finally complete.

Remark. (1) Since 2^{b-1} equals the index of a subgroup, which is a positive integer by definition, we obtain that $b \geq 1$. In other words, if $\beta \in U(\Omega)$ and $\beta \notin K^{\times 2}$, then there exists at least one place $v \in S$ such that $\beta \notin K_v^{\times 2}$.

(1') Let $J^2(\Omega) := \{i = (i_v)_v \in J(\Omega) : i_v \in K_v^{\times 2} \text{ for all } v \in S\}$. Then $J^2(\Omega) \cap U(\Omega) = U(\Omega)^2$.

(2) Consider the index $[J_K : K^\times J^2(\Omega)]$, where $J^2(\Omega)$ is as in (1'). A computation very similar to the one made at the beginning of this chapter yields that this index equals

$$\frac{[J(\Omega) : J^2(\Omega)]}{[U(\Omega) : U(\Omega) \cap J^2(\Omega)]}.$$

By (1'), the denominator equals $[U(\Omega) : U(\Omega)^2]$, and we can rewrite this as a product of indices as in the above proof using the structure theorem for finitely generated abelian groups. By Dirichlet's Unit Theorem, we know that $U(\Omega)$ has rank $s-1$, and a direct computation yields $[U : U^2] = 2^s$.

As for the numerator, we can again use the homomorphism $J(\Omega) \to \prod_{v \in S} K_v^\times$ and the isomorphism theorems to write $[J(\Omega) : J^2(\Omega)]$ as $\prod_{v \in S} [K_v^\times : K_v^{\times 2}]$. Now we are (almost) done by Thm. II.§4.(i)-(iii): the product formula for $2 \in K^\times$ shows that

$$\prod_{v:\ \nu_v(2)>0} \big(\#k(v)\big)^{\nu_v(2)} = \prod_{v:\ |2|_v<1} |2|_v^{-1} = \prod_{v \text{ archimedean}} |2|_v^{\rho_v},$$

so the value of $[J(\Omega : J^2(\Omega)]$ simplifies to 4^s and the sought-after index $[J_K : K^\times J^2(\Omega)]$ equals precisely 2^s. This will be needed in the next section. $\diamond$

§5. The Hasse Norm Theorem

In this section, we continue the programme presented in §2 and prove that the index $[J_K : K^\times N(J_L)]$ estimated in §4 is indeed *equal* to 2, where the notations are as in the previous sections. As a corollary, we shall obtain the result given immediately below, which is a special case of the celebrated Hasse Norm Theorem, see also Rmk.(1). Given the prominence of this result in the proof of the Hasse-Minkowski Theorem, we have opted to use "The Hasse Norm Theorem" as the title for the entire section.

Theorem IV.§5. *In order for $x \in K$ to lie in the image of $N_{L/K}$, it is necessary and sufficient that x lie in the image of N_{L_w/K_v} whenever $v \in \mathfrak{M}$ and $w|v$.*

Remark. (1) The above statement is usually formulated and proved for general *cyclic* extensions of global fields; in this more general context, it is widely known as the **Hasse Norm Theorem**.

(1') In the language of Galois cohomology, the Hasse Norm Theorem translates into the claim that the map $H^0(G, L^\times) \to H^0(G, J_L)$ associated to the inclusion $L^\times \hookrightarrow J_L$ is injective, where G denotes the *Galois group* of the extension L/K. Owing to the long exact sequence of cohomology, this claim follows from $H^{-1}(G, J_L/L^\times) = \{1\}$, which is in turn a reformulation of a result from class field theory. ◇

We proceed to sketch the proof of the inequality $[J_K : K^\times N(J_L)] \leq 2$. To this end, choose a set $\Omega \subset \mathfrak{M}$ with properties (a)-(e) as in §4; all the notations and abbreviations introduced in §4 are still in force.

In Rmk. §4.(2), we showed, using the structure theorem for finitely generated abelian groups, that $[U : U^2] = 2^s$; a closer look at this argument will show that there exist elements $\varepsilon_1, ..., \varepsilon_s \in U$ with the following property: *the elements $\prod_{j\in T} \varepsilon_j$, where T ranges over all subsets of $\{1, ..., s\}$, form a system of representatives for U/U^2.*

Without loss of generality, we can take $\varepsilon_1 = \beta$. Indeed, upon rearranging the ε_j's and multiplying them with elements of U^2, we can assume that $\beta = \varepsilon_1 \cdots \varepsilon_l$ for some $l \leq s$, and so the elements $\beta, \varepsilon_2, ..., \varepsilon_s$ again have the above property.

We now claim that we can find places $v_1, ..., v_s \in \Omega$ such that $\varepsilon_j \in K_{v_j}^{\times 2}$ for all j and $\varepsilon_j \notin K_{v_l}^{\times 2}$ whenever $j \neq l$. If $s = 1$, then this is clear (in fact, there are infinitely many possibilities for v_1 by the Global Square Theorem); for $s > 1$, one applies the Global Square Theorem to a larger global field obtained by adjoining to K the square roots of $\varepsilon_2, ..., \varepsilon_s$.

Given $v_1, ..., v_s \in \Omega$ as in the above claim, one defines subgroups $H_1 \subseteq H_2 \subseteq ... \subseteq H_s$ of $K^\times N(J_L)$ as follows. For each $j > 1$, consider the injection $\iota_j : K_{v_j}^\times \to J_K$ which sends x to $i = (i_v)_v$ with $i_{v_j} = x$ and $i_v = 1$ for every $v \neq v_j$. Since $\varepsilon_1 = \beta$ is a square in K_{v_j} for

each $j > 1$, Rmk. §2.(2) shows that every idèle i in the image of ι_j is automatically in the image of $N(J_L)$. Thus, take $H_1 = K^\times J^2(\Omega)$, where $J^2(\Omega)$ is defined as in Rmk. §4.(1'); an application of Rmk. §2.(2) will show that H_1 is indeed contained in $K^\times N(J_L)$. Next, set $H_j = H_{j-1} \cdot \iota_j(K_{v_j})$ for each $j > 1$.

The next step is to prove that all inclusions are strict; this is proved by showing that the assumption $\iota_j(K_{v_j}) \subseteq H_{j-1}$ for some $j > 1$ leads to a contradiction. As a result, we obtain that the index $[H_s : H_1]$ is at least 2^{s-1}, and so the same holds for the index $[K^\times N(J_L) : K^\times J^2(\Omega)]$. But then, using Rmk. §4.(2), we have

$$\begin{aligned}[J_K : K^\times N(J_L) &= [J_K : K^\times J^2(\Omega)]/[K^\times N(J_L) : K^\times J^2(\Omega)] \\ &\leq 2^s/2^{s-1} = 2,\end{aligned}$$

and the main claim of this section is proved.

Proof of Thm. IV.§5. Necessity is clear, so we proceed to prove sufficiency. Thus, suppose that $x \in K^\times$ (the case $x = 0$ is trivial) and that $x \in N_{L_w/K_v}(L_w^\times)$ whenever $v \in \mathfrak{M}$ and $w|v$.

Pick a set $\Omega \subset \mathfrak{M}$ such that properties (a)-(f) from §4 hold. By the product formula, $|x|_v \neq 1$ for at most finitely many $v \in \Omega$; upon discarding these, we can assume that additionally $x \in U(\Omega)$. An application of Rmk. §2.(2) shows that x must also be in $N(J')$. But, since $[J_K : K^\times N(J_L)] = 2$, the equation (*) from §4 implies that

$$U(\Omega) \cap N(J') = N(U'),$$

so $x \in N(U') \subseteq N(L^\times)$ as claimed. □

§6. The Hasse-Minkowski Theorem

We conclude this chapter with the proof of the Hasse-Minkowski Theorem as stated at the beginning of this chapter. Since necessity is obvious, we shall only prove sufficiency.

Similarly as in §1, the proof is by induction for $n \geq 5$. In fact, the same argument can be used, provided that the theorem has already been proved for $n \leq 4$: first, one diagonalizes $(V, q) \cong \langle a_1, ..., a_n \rangle$ and looks at the regular subspace $W = \langle a_3, ..., a_n \rangle \subset V$. By Ex. III.§6, if v is a non-archimedean place such that (K_v, v) is nondyadic and $\left|a_j\right|_v = 1$ for all $j \geq 3$, then W_v is isotropic; the product formula shows that there are at most finitely many "exceptional places" v for which W_v is not isotropic.

Next, one uses the Artin-Whaples Approximation Theorem at the set of "exceptional places" to construct an element $a \in K^\times$ such that the regular subspace $W' = \langle a \rangle \perp W$

of V is isotropic at *all* places of K. One is now able to apply the induction hypothesis to W', and the proof is complete.

We now proceed to establish the theorem for $n \leq 4$. The claim is vacuous for $n = 1$; as for $n = 2$, we can use precisely the same argument as in §1 upon replacing Prop. IV.§1 by the Global Square Theorem. Thus, it merely remains to modify our arguments for $n = 3$ and $n = 4$.

Suppose that $n = 3$. Since scaling the quadratic form q does not affect isotropy, we can assume without loss of generality that (V, q) represents 1, hence $(V, q) \cong \langle 1, -a, -b\rangle$ for $a, b \in K^\times$.

Let L be a splitting field of $g(t) = t^2 - b$ over K; then $[L : K] = 2$ and $L = K(\delta)$ for some δ with $\delta^2 = b$. Note that, whenever $v \in \mathfrak{M}$ and $w|v$, we have $L_w = K_v(\delta)$ by the proof of Prop. I.§9.(iii).

Now the assumption that (V_v, q_v) is isotropic for all $v \in \mathfrak{M}$, together with Thm. III.§3, shows that $a \in N_{L_w/K_v}(L_w)$ whenever $v \in \mathfrak{M}$ and $w|v$. But then the Hasse Norm Theorem tells us that $a \in N_{L/K}(K)$, so, again by Thm. III.§3, (V, q) is isotropic over K.

Finally, suppose that $n = 4$. If $\det V = 1 \cdot K^{\times 2}$, we can immediately apply the ternary case proved above. Indeed, pick a regular ternary subspace $W \subset V$; by Cor. II.§2.(iii), V is isotropic if and only if W is. But for each $v \in \mathfrak{M}$ we have $\det V_v = 1 \cdot K_v^{\times 2}$, and W_v is a regular ternary subspace of V_v, so W_v is isotropic for all v again by Cor. II.§2.(iii), and W is isotropic by the case $n = 3$.

We can reduce the general situation to the above special case by the following lemma.

Lemma IV.§6. *Let (V, q) be a regular quaternary space over a field F of characteristic $\neq 2$, and let $d \in F^\times$ such that $d \cdot F^{\times 2} = \det V$. Let $E \supseteq F$ be a splitting field, cf. I.§9, of $g(t) = t^2 - d$ over F. Then V is isotropic if $V \otimes_F E$ is.*

Proof. Let $V_E := V \otimes_F E$ and let q_E be the quadratic form on V_E defined as in the preamble of this chapter. If $d \in F^{\times 2}$, then $E = F$ and there is nothing to prove. Otherwise, the extension E/F has degree 2; by assumption, it contains a square root δ of d, and every element $z \in V_E$ can be written as $z = x + y\delta$ for $x, y \in V$ (e.g. one can choose a representation of z with respect to some basis and apply Ex. III.§2.(3) to the coefficients).

Suppose for the sake of contradiction that (V, q) is not isotropic. By isotropy of V_E, there exists some $z = x+y\delta \in V_E$ with $q_E(z) = 0$, i.e. with $q(x)+dq(y)+2\delta b_q(x, y)$, where b_q is the symmetric bilinear form associated to q as in II.§2. This implies $b_q(x, y) = 0$, i.e., x and y are orthogonal, as well as $q(x) = -dq(y)$. If $q(x)$ or $q(y)$ were equal to zero, then necessarily $x = y = 0$ and hence $z = 0$, a contradiction; we infer that $q(x)$ and $q(y)$

are nonzero.

By the results of Chapter II, we can write $V \cong \langle q(x)\rangle \perp \langle -dq(x)\rangle \perp U$ for some binary subspace U. But then comparing determinants yields $\det U = -1 \cdot F^{\times 2}$; thus, U is isotropic by Cor. II.§2.(ii), and so is $V \supset U$. □

The argument goes as follows: suppose that (V, q) is a quaternary regular space, and pick $d \in K^\times$ with $dK^{\times 2} = \det V$. Then $V_L := V \otimes_K L$, where L is a splitting field of $t^2 - d$ over K, has determinant equal to $1 \cdot L^{\times 2}$ since d is a square in L. Now L is again a global field, and since all V_v are isotropic it is easy to check that $(V_L)_w$ is isotropic for all $w \in \mathfrak{N}$. By the above special case, V_L is isotropic, and the lemma allows us to conclude that V is itself isotropic.

The proof of the Hasse-Minkowski Theorem for global fields is now complete. Let us record a few consequences.

Theorem IV.§6. *Let (V', q') be a regular n-ary quadratic space over K. Then (V, q) and (V', q') are isometric if and only if $(V_v, q_v) \cong (V'_v, q'_v)$ for all $v \in \mathfrak{M}$.*

Proof. Necessity is clear. As for sufficiency, we proceed by induction on the common dimension n, where the induction basis consists of the vacuous case $n = 0$.

Suppose now that $n \geq 1$, and let $a \in K^\times$ be some element represented by V. Then clearly each V_v represents a, and so every V'_v represents a since they are isometric by assumption. By Cor. II.§2.(i), this means precisely that for each $v \in \mathfrak{M}$, the space $V'_v \perp \langle -a\rangle$ is isotropic. But then $V' \perp \langle -a\rangle$ is isotropic by the Hasse-Minkowski theorem, and so V' represents a.

We can thus write $V = \langle a\rangle \perp W$ and $V' = \langle a\rangle \perp W'$ for $(n-1)$-ary subspaces $W \subset V$ and $W' \subset V'$. Applying Witt's Cancellation Theorem at each $v \in \mathfrak{M}$, we find that W_v and W'_v are isometric for each v, hence $W \cong W'$ by the induction hypothesis. But then $V \cong V'$ as claimed. □

Remark. In the course of the above proof, we have also shown that *V represents a if and only if V_v represents a for all v.* ◇

Combining the above theorem with the classification of quadratic forms over local fields from III.§6, we obtain:

Corollary IV.§6. *Let (V', q') be a regular quadratic space over K. Then (V, q) and (V', q') are isometric if and only if all of the following hold:*

(i) $\dim V' = \dim V$*;*

(ii) $\det V' = \det V$*;*

(iii) for every non-archimedean $v \in \mathfrak{M}$, the Hasse invariants $s(V'_v)$ and $s(V_v)$ are equal;

(iv) for every $v \in \mathfrak{M}$ with $K_v = \mathbb{R}$, the signature (r, s) of V_v equals the signature (r', s') of V'_v.

We wish to conclude this thesis by noting how the Hasse-Minkowski Theorem is unique amongst local-global principles in that most natural attempts at generalization fail, even over $\mathbb{Q}$. The most famous example of this is the fact that *there is no general local-global principle for cubic forms*, i.e. homogeneous polynomials of degree 3; indeed, Ernst Selmer showed hat the equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has nontrivial solutions in $\mathbb{Q}_p$ for each $p \leq \infty$, but no nontrivial solution over $\mathbb{Q}$, see also [Conrad]. Nonetheless, there are partial positive results, recorded e.g. in [Lan97], Chapter X: for instance, a *nonsingular* cubic form f *in at least* 9 *variables* over $\mathbb{Q}$ which has a nontrivial zero over every $\mathbb{Q}_p$ also has a nontrivial zero over $\mathbb{Q}$, where "nonsingular" simply means that the only common zero of all partial derivatives of f is the origin. Moreover, it is known that every cubic form in 10 variables over some $\mathbb{Q}_p$ has a nontrivial zero, and that every nonsingular cubic form in 10 variables over $\mathbb{Q}$ has a nontrivial zero. More generally, Bryan Birch proved that for each odd d there exists some $n = n(d)$ such that every homogeneous polynomial of degree d over $\mathbb{Q}$ in at least n variables has a nontrivial zero.

Another natural generalization of the Hasse-Minkowski theorem would be a local-global principle for quadratic modules over *rings of integers* $\mathcal{O}_K$ of global fields, the classical case being $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$. We restrict ourselves to a special class of quadratic modules, namely *lattices* over $\mathcal{O}_K$; again, there is a natural way to "localize" a lattice at each (finite) place v of K, obtaining a lattice over the ring of integers $\mathfrak{o}_v$ of K_v, and we say that two lattices over $\mathcal{O}_K$ are *in the same genus* if all their localizations are isometric. The general result is then stated as follows: *the genus of any lattice over $\mathcal{O}_K$ contains only finitely many isometry classes.* Over $\mathcal{O}_K = \mathbb{Z}$, one can find an effective upper bound for the number of classes in a genus, which is less than 2 e.g. when $q(x_1, ..., x_n) = x_1^2 + ... + x_n^2$ for $n \leq 4$. This can be used to retrieve classical results on the representability of a positive integer as a sum of two, three or four squares, as well as a famous result of Gauss which states that every positive integer is the sum of three triangular numbers, see [Ser73] and [Kne02].

Bibliography

[ArWh45] Emil Artin, George Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. 51, pp. 469–492, 1945.

[BoSh86] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Academic Press, 1986.

[CaFr67] J.W. Cassels, Albrecht Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[Coh07] Henri Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Springer New York, 2007.

[Conrad] Keith Conrad, *Selmer's Example*, electronic, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/selmerexample.pdf.

[GiSz06] Philippe Gille, Tamás Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, 2006.

[Has31] Helmut Hasse, *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol* (German), Nachr. Ges. Wiss. Göttingen, pp. 64–69, 1931.

[Isa94] I. Martin Isaacs, *Algebra: A Graduate Course*, American Mathematical Society, 1994.

[Kne02] Martin Kneser, *Quadratische Formen* (German), Springer-Verlag Berlin Heidelberg New York, 2002.

[Lam04] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, American Mathematical Society, Providence, Rhode Island, 2004.

[Lan94] Serge Lang, *Algebraic Number Theory*, Springer-Verlag New York, Second Edition, 1994.

[Lan97] Serge Lang, *Survey of Diophantine Geometry*, Springer-Verlag, 1997.

[Lan02] Serge Lang, *Algebra*, Springer-Verlag New York, 2002.

[Neu15] Jürgen Neukirch, *Klassenkörpertheorie* (German), electronic, https://www.mathi.uni-heidelberg.de/∼schmidt/Neukirch/

[O'M73] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag Berlin Heidelberg GmbH, Third Corrected Printing, 1973.

[Par14] R. Parimala, *A Hasse Principle for quadratic forms over function fields*, Bull. Amer. Math. Soc., 2014.

[RV99] Dinakar Ramakrishnan, Robert J. Valenza, *Fourier Analysis on Number Fields*, Springer New York, 1999.

[Rib99] Paulo Ribenboim, *The Theory of Classical Valuations*, Springer-Verlag New York Berlin Heidelberg, 1999.

[Sch07] Joachim Schwermer, *Minkowski, Hensel, and Hasse: On The Beginnings of the Local-Global Principle*, Chapter 7 in *Episodes in the History of Modern Algebra (1800-1950)*, edited by Jeremy Gray and Karen Hunger Parshall, American Mathematical Society, 2007.

[Ser73] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, 1973.

[Ser79] Jean-Pierre Serre, *Local Fields*, Springer-Verlag New York, 1979.

[War89] Seth Warner, *Topological Fields*, North-Holland, 1989.