ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Classification of quaternion algebras over the field of rational numbers

Bachelor Thesis

Nadir Bayo

October 2017

Supervised by Prof. Dr. Richard Pink

Department of Mathematics, ETH Zürich

Rämistrasse 101, 8092 Zürich

Contents

Introduction

All algebras in this bachelor thesis assumed to be associative and unitary. As the title suggests, our goal is to classify the quaternion algebras, i.e. central simple algebras of dimension 4, over the field of rational numbers. To motivate this question we give an example which the reader may already have encountered: the Hamilton quaternions. They are defined as

$$\mathbb{H} \coloneqq \{t + xi + yj + zk \mid t, x, y, z \in \mathbb{R}\},$$

where i, j and k satisfy the relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

Endowed with an associative multiplication having 1 as neutral element and satisfying the above relations they form a quaternion algebra over $\mathbb{R}$. Stating the above relations is equivalent to giving the relations

$$i^2 = -1, \quad j^2 = -1, \quad \text{and} \quad ij = -ji = k.$$

In the first section of this thesis we will generalize the above example. Consider an arbitrary field F with $\operatorname{char}(F) \neq 2$, nonzero elements $a, b \in F^\times$ as well as an F-vector space A with basis elements $1, i, j, k$. We will show that there exists a unique F-bilinear associative multiplication on A having 1 as neutral element and satisfying the relations

$$i^2 = -a \quad j^2 = b, \quad \text{and} \quad ij = -ji = k.$$

This multiplication turns A into an F-algebra, which we denote by $\left(\frac{a,b}{F}\right)$. The algebra $\left(\frac{a,b}{F}\right)$ is in fact a quaternion algebra, and conversely any quaternion algebra over F is isomorphic to one of the form $\left(\frac{a,b}{F}\right)$ for some $a, b \in F$. In this notation the Hamilton quaternions can be written as $\left(\frac{-1,-1}{\mathbb{R}}\right)$. One can also show that the matrix algebra $\operatorname{Mat}_{2\times 2}(F)$ is isomorphic to $\left(\frac{1,1}{F}\right)$.

This characterization allows us to show that every quaternion algebra is either isomorphic to the matrix algebra or it is a division algebra. Furthermore the characterization gives us a very "hands on" feel for quaternion algebras.

Given a quaternion algebra $\left(\frac{a,b}{F}\right)$ we can define the map

$$\operatorname{nrd}\colon A \to F, \quad t + xi + yj + zk \;\mapsto\; t^2 - ax^2 - by^2 + abz^2.$$

This map is called reduced norm of A and it can be seen as a homogeneous polynomial of degree two in four variables. This polynomial yields a quadratic form on A seen as F-vector space. We can also restrict nrd on $A_0 \coloneqq \operatorname{span}\{i, j, k\}$ and get a ternary quadratic form. The reduced norm is a connecting element between the theory of quaternion algebras and the theory of quadratic forms, which constitutes the main topic of section 2.

To each quadratic form Q over an F-vector space V we can associate an F-bilinear form T. We will show that a change of the basis of V affects the determinant of the representation matrix of T rescaling it by squares. Hence we will introduce the discriminant of a quadratic form as the determinant modulo $(F^\times)^2$.

We will define two equivalence relations on the set of quadratic forms: similarity and isometry. Two quadratic forms over two F-vector spaces V and V' are said to be similar if they can be "converted" in one another by a linear isomorphism and a scaling. If there is no scaling (or in other words the scaling factor is 1), one speaks of isometric quadratic forms.

These tools will allow us to prove the two main theorems of section 2. The first one states that there are natural bijections:

$$\left\{\begin{array}{c}\text{Quaternion algebras}\\ \text{over } F \text{ up to}\\ \text{isomorphism}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{Ternary quadratic forms}\\ \text{over } F \text{ with discriminant}\\ 1 \in F^\times/(F^\times)^2 \text{ up to isometry}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{Nondegenerate ternary}\\ \text{quadratic forms over}\\ F \text{ up to similarity}\end{array}\right\},$$

given respectively by $[A] \mapsto [\mathrm{nrd}|_{A_0}]$ and $[Q] \mapsto [Q]$. The second theorem gives six equivalent conditions about a quaternion algebra and the corresponding quadratic form. In particular it states that a quaternion algebra A is a division algebra if and only if the corresponding reduced norm nrd is isotropic if and only if the form $\mathrm{nrd}|_{A_0}$ is anisotropic.

In section 3 we will introduce the reader to the p-adic numbers $\mathbb{Q}_p$ and we will study the theory of quadratic forms over $\mathbb{Q}_p$. We will show that for each prime p and for $p = \infty$ (setting $\mathbb{Q}_p \coloneqq \mathbb{R}$) there is a unique ternary anisotropic quadratic form over $\mathbb{Q}_p$, up to similarity. Combining this with the two main results of section 2 we will get that, up to isomorphy, there is a unique division quaternion algebra over each field $\mathbb{Q}_p$ for p prime or $p = \infty$.

Finally in section 4 we well proceed to classify the quaternion algebras over $\mathbb{Q}$. Consider a quaternion algebra $A \coloneqq \left(\frac{a,b}{\mathbb{Q}}\right)$. For each p prime or $p = \infty$ we consider the scalar extension

$$A \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \left(\frac{a,b}{\mathbb{Q}_p}\right).$$

From section 3 we know that for each p that $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is either isomorphic to the matrix algebra $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ or to a uniquely determined division quaternion algebra. We will introduce two tools from number theory—the Legendre symbol and the Hilbert symbol—to show that the ramification set of A, defined as

$$\mathrm{Ram}(A) \coloneqq \{p \text{ prime or } p = \infty \mid A \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{is a division algebra}\},$$

is finite of even cardinality.

We will formulate (without proof) the Hasse-Minkowski theorem and prove a corollary, which states that two quadratic forms are isometric over $\mathbb{Q}$ if and only if they are isometric over $\mathbb{Q}_p$ for every p, including $p = \infty$. We will also state (without proof) Dirichlet's theorem on primes in arithmetic progression, wich says that for coprime a and $n \in \mathbb{Z}$ with $n \neq 0$ there exist infinitely many prime numbers p satisfying $p \equiv a \pmod{n}$.

These three results, as well as other small ones will allow us to prove the final theorem of this thesis, stating that there are bijections

$$\left\{\begin{array}{c}\text{Isomorphy classes of}\\ \text{quaternion algebras over } \mathbb{Q}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Finite subsets of } P\\ \text{of even cardinality}\end{array}\right\} \longleftrightarrow \left\{D \in \mathbb{Z}^{\geqslant 1} \text{ squarefree}\right\}.$$

given by

$$[A] \mapsto \mathrm{Ram}(A) \quad \text{and} \quad \Sigma \mapsto \prod_{\substack{p\in\Sigma\\ p\neq\infty}} p$$

respectively. This will give us a complete classification of the quaternion algebras over the field of rational numbers.

We will follow closely the book *Quaternion algebras* by John Voight ([Voi17]) for the theory of quaternion algebras, as well as the bachelor thesis *Der Satz von Hasse-Minkowski* by Charlotte Jergitsch ([Jer17]), which was also supervised by Prof. Dr. Richard Pink, and the book *A Course in Arithmetic* by Jean-Pierre Serre ([Ser73]) for the theory of quadratic forms and the results from number theory. Some other auxiliary literature will also be used.

1 General results about algebras over a field

All rings in this thesis are associative and unitary, but not necessarily commutative.

We begin with some very basic general definitions and remarks on algebras. Fix a field F.

Definition 1.1. An F-algebra is an F-vector space $(A, +, 0_A)$ together with an F-bilinear multiplication map

$$\cdot\colon A \times A \to A,$$

and an element 1_A such that $(A, +, \cdot, 0_A, 1_A)$ is a ring.

Proposition 1.2. *The above definition is equivalent to: A is a ring with a ring homomorphism*

$$\varphi\colon F \to Z(A),$$

where $Z(A)$ is the center of A, i.e. the subring $\{x \in A \mid \forall y \in A\colon xy = yx\}$.

Given a nonzero F-algebra A we identify F with its image $\varphi(F) \subset Z(A)$.

Definition 1.3.

i) An *isomorphism* $\varphi\colon A \to B$ of F-algebras is an F-vector space isomorphism with the additional property $\forall x, y \in A\colon \varphi(xy) = \varphi(x)\varphi(y)$. In other words it is an F-vector space isomorphism, which is also a ring isomorphism.

ii) An *anti-isomorphism* $\varphi\colon A \to B$ of F-algebras is an F-vector space isomorphism with the additional property $\forall x, y \in A\colon \varphi(xy) = \varphi(y)\varphi(x)$.

Definition 1.4. Given an F-algebra A we define the *opposite algebra* A^{op} as the algebra with the same underlying set, 0, 1, and addition, as well as with the multiplication $\alpha \cdot_{\mathrm{op}} \beta \coloneqq \beta \cdot \alpha$. An algebra and its opposite algebra are naturally anti-isomorphic.

Definition 1.5. An F-algebra D is called a *division algebra* if:

i) $D \neq 0$,

ii) $\forall a \in D\ \forall b \in D \setminus \{0\}\ \exists x \in D\colon a = xb$, and

iii) $\forall a \in D\ \forall b \in D \setminus \{0\}\ \exists y \in D\colon a = by$.

Remark 1.6. An F-algebra D is a division algebra if and only if it is a division ring, i.e. if $D \neq 0$ and $D^\times = D \setminus \{0\}$.

Proof. First assume that D is a division algebra. Pick an element $a \in D \setminus \{0\}$. By definition of division algebra there exists an element $a' \in D$ with $a'a = 1$. Thus D is a division ring.

Conversely assume that D is a division ring and pick elements $a \in D$ and $b \in D \setminus \{0\}$. By setting $x \coloneqq ab^{-1}$ and $y \coloneqq b^{-1}a$ the conditions in Def. 1.5 ii) and iii) are satisfied. □

Definition 1.7.

i) A nonzero F-algebra A whose only two-sided ideals are (0) and A, is called *simple.*

ii) An F-algebra A is said to be *central* if $Z(A) = F$.

Lemma 1.8. *Let A and B be F-algebras, with A simple, and $\varphi\colon A \to B$ be an F-algebra homomorphism. Then φ is injective or it is the zero map.*

Proof. The claim follows from the fact that $\ker(\varphi)$ is a two-sided ideal of A. □

We are now ready to define the main object of this thesis.

Definition 1.9. A *quaternion algebra* over a field F is a central simple F-algebra of dimension 4.

We now want to characterize quaternion algebras in terms of generators.

Proposition 1.10.

i) Let $\mathrm{char}(F) \neq 2$*, let* $a, b \in F^\times$ *and let* A *be a four-dimensional* F*-vector space with basis elements* $\{1, i, j, k\}$*. Then there exists a unique* F*-bilinear associative multiplication* $A \times A \to A$ *satisfying:*

$$\forall \alpha \in A\colon 1\alpha = \alpha,\ i^2 = a,\ j^2 = b,\ \text{and } ij = -ji = k.$$

Further this multiplication satisfies

$$k^2 = -ab, ik = -ki = aj,\ \text{and } kj = -jk = bi.$$

This multiplication turns A into an F-algebra.

ii) Let $\mathrm{char}(F) = 2$*, let* $a \in F,\ b \in F^\times$ *and let* A *be a four-dimensional* F*-vector space with basis elements* $\{1, i, j, k\}$*. Then there exists a unique* F*-bilinear associative multiplication* $A \times A \to A$ *satisfying:*

$$\forall \alpha \in A\colon 1\alpha = \alpha,\ i^2 + i = a,\ j^2 = b,\ \text{and } ij = j(i+1) = k.$$

Further this multiplication satisfies

$$k^2 = ab,\ ki = (i+1)k = aj,\ \text{and } kj = jk + b = bi.$$

This multiplication turns A into an F-algebra.

Proof. Both statements are proven in the same way, therefore we only prove i). To prove the existence we define a multiplication on A via the relations

$$\forall \alpha \in A\colon 1\alpha \coloneqq \alpha,\ i^2 \coloneqq a,\ j^2 \coloneqq b, ij \coloneqq k \text{ and } ji \coloneqq -k.$$

Since we require associativity we get $k^2 = (ij)^2 = i(ji)j = -i^2j^2 = -ab$. In a similar way we can show $ik = -ki = aj$ and $kj = -jk = bi$. Having defined the relations for the basis elements, the multiplication extends uniquely to an F-bilinear multiplication on A. Since $\forall \alpha \in A\colon 1\alpha = \alpha$, the multiplication defines an F-algebra structure on A. □

Definition 1.11.

i) In the case $\mathrm{char}(F) \neq 2$ we denote the algebra from Prop. 1.10 i) by $\left(\frac{a,b}{F}\right)$.

ii) In the case $\mathrm{char}(F) = 2$ we denote the algebra from Prop. 1.10 ii) by $\left[\frac{a,b}{F}\right)$.

In both cases i and j are called the *standard generators* of the algebra.

Proposition 1.12.

i) Let $\mathrm{char}(F) \neq 2$. *Every algebra of the form* $\left(\frac{a,b}{F}\right)$ *is a quaternion algebra. Conversely for every quaternion algebra* A *there exist* $a, b \in F^\times$ *such that* A *is isomorphic to* $\left(\frac{a,b}{F}\right)$.

ii) Let $\mathrm{char}(F) = 2$. *Every algebra of the form* $\left[\frac{a,b}{F}\right)$ *is a quaternion algebra. Conversely for every quaternion algebra* A *there exist* $a \in F,\ b \in F^\times$ *such that* A *is isomorphic to* $\left[\frac{a,b}{F}\right)$.

Example 1.13. We can use the above notation to describe the classical Hamilton quaternions:

$$\mathbb{H} \coloneqq \{t + xi + yj + zk \mid t, x, y, z \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\} = \left(\frac{-1,-1}{\mathbb{R}}\right).$$

Example 1.14. The matrix algebra $\mathrm{Mat}_{2\times 2}(F)$ for $\mathrm{char}(F) \neq 2$ is isomorphic to $(\frac{1,1}{\mathbb{R}})$ via

$$\left(\frac{1,1}{F}\right) \to \mathrm{Mat}_{2\times 2}(F),\ i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since not all nonzero matrices are invertible, $\mathrm{Mat}_{2\times 2}(F)$ is not a division algebra.

Proof of Prop. 1.12. Since the goal of this thesis is to classify the quaternion algebras over $\mathbb{Q}$, we restrict ourselves to the proof of the case $\mathrm{char}(F) \neq 2$. First we consider the algebra $A \coloneqq \left(\frac{a,b}{F}\right)$. It is clear that $F \subset Z\left(\left(\frac{a,b}{F}\right)\right)$. Let $\alpha \coloneqq t + xi + yj + zk \in Z\left(\left(\frac{a,b}{F}\right)\right)$. Since $2j$ and $2k$ are both invertible we obtain:

$$\begin{aligned} 0 = \alpha i - i\alpha &= 2j(yi - az) \iff yi - az = 0 \iff y = z = 0, \text{ and} \\ 0 = \alpha j - j\alpha &= 2xk \iff x = 0. \end{aligned}$$

Hence we have $\alpha \in F$, which implies that $\left(\frac{a,b}{F}\right)$ is central.

Now let $I \neq (0)$ be a two-sided ideal of $\left(\frac{a,b}{F}\right)$. In order to show that I is equal to $\left(\frac{a,b}{F}\right)$ it suffices to show that I contains an element of $F^\times$. So let $0 \neq \alpha \coloneqq t + xi + yj + zk \in I$. If $x = y = z = 0$ then $t \in F^\times \cap I$ and we are done, so assume that one of x, y, z is nonzero. By multiplying α with i, j or k we can assume that $t \neq 0$. Using the invertibility of $-2i, -2j$, and $-2k$ we obtain:

$$\begin{aligned} \alpha i - i\alpha = -2i(yj + zk) \in I \Rightarrow yj + zk \in I \Rightarrow t + xi &= \alpha - (yj + zk) \in I, \\ \alpha j - j\alpha = -2j(xi + zk) \in I \Rightarrow xi + zk \in I \Rightarrow t + yj &= \alpha - (xi + zk) \in I, \\ \alpha k - k\alpha = -2k(xi + yj) \in I \Rightarrow xi + yj \in I \Rightarrow t + zk &= \alpha - (xi + yj) \in I. \end{aligned}$$

So $-2t = \alpha - (t + xi) - (t + yj) - (t + zk) \in F^\times \cap I$ and we are done.

Conversely let A be a quaternion algebra, i.e. a central simple F-algebra of dimension 4. First we assume that A is a division algebra. We take an $i \in A \setminus F$ and consider the ring $F[i]$. This is a commutative subring of the division ring A. The ring $F[i]$ has finite dimension as F-vector space and therefore it is a field. Since $F[i]$ is commutative whereas A is not we have $F \subsetneq F[i] \subsetneq A$, and from the multiplicativity of the degree of an extension of division rings it follows that $[F[i]/F] = 2$. Moreover $F[i]$ is its own centralizer in A. Since $\mathrm{char}(F) \neq 2$ after replacing i by another element of $F[i] \setminus F$ we can assume without loss of generality that $a \coloneqq i^2 \in F$. Consider the $F[i]$-linear map

$$\varphi\colon A \to A,\ \alpha \mapsto i\alpha i^{-1}$$

(the conjugation with i). This is an endomorphism of the two-dimensional left $F[i]$-vector space A. One can check by computation that $\varphi^2 = \mathrm{id}$, which implies that φ has two eigenvalues 1 and -1 and therefore it is diagonalizable. From

$$\varphi(\alpha) = i\alpha i^{-1} = \alpha \iff i\alpha = \alpha i \iff \alpha \in F[i]$$

it follows that $F[i]$ is the eigenspace associated to 1. We take now a $j \in A \setminus F[i]$. In particular j lies in the eigenspace associated to -1 and hence $iji^{-1} = -j \Rightarrow ij = -ji$. From $ij^2 = j^2 i$ it follows that $j^2 \in F[i]$, i.e. $\exists b, c \in F\colon j^2 = b + ic$. If $c \neq 0$, so $i = \frac{1}{c}j^2 - \frac{b}{c} \in F[j]$ and thus $F[i] \subsetneq F[j]$, implying that $F[j] = A$, which is a contradiction by the noncommutativity of A. So $c = 0$ and $j^2 = b \in F$. We claim that $\{1, i, j, ij\}$ is a basis of A over F. Indeed, let $t, x, y, z \in F$ such that $t + xi + yj + zij = 0$. By computing and using $i^2 = a,\ j^2 = b$ and $ij = -ji$ we obtain:

$$\begin{aligned} 0 &= i(\alpha i + i\alpha) = 2a(t + xi) \Rightarrow t + xi = 0, \\ 0 &= j(\alpha j + j\alpha) = 2b(t + yj) \Rightarrow t + yj = 0, \\ 0 &= ij(\alpha ij + ij\alpha) = -2ab(t + zij) \Rightarrow t + zij = 0. \end{aligned}$$

Hence

$$-2t = (t + xi + yj + zij) - (t + xi) - (t + yj) - (t + zij) = 0,$$

which implies $t = 0$, hence $xi = yj = zij = 0$. Since i, j and ij are all nonzero, we have $x = y = z = 0$, which implies the linear independence of $1, i, j$ and ij.

If A is not a division algebra, it has a nonzero proper left ideal, because by Rem. 1.6 we can choose a nonunit $\alpha \in A$, then the left ideal generated by α is a nontrivial left ideal of A. Let I be a nonzero proper left ideal of A and let $m \coloneqq \dim_F(I)$. The operation of A on I corresponds to an F-algebra homomorphism $A \to \mathrm{End}_F(I)$, which is injective since A is simple. We know from linear algebra that $\mathrm{End}_F(I)$ is isomorphic to $\mathrm{Mat}_{m\times m}(F)$ as F-vector space, and from the injectivity it follows that $m^2 = \dim_F(\mathrm{Mat}_{m\times m}(F)) \geqslant \dim_F(A) = 4$, and so $m \geqslant 2$. By arguing in the same fashion with the quotient algebra A/I, which has dimension $4 - m$ over F, we obtain $m \leqslant 2$, hence $m = 2$. Thus A is isomorphic to $\mathrm{Mat}_{2\times 2}(F) \cong \left(\frac{1,1}{F}\right)$. □

The proof of Prop. 1.12 yields the following proposition.

Proposition 1.15. *For a quaternion algebra A over F the following are equivalent:*

i) $A \cong \left(\frac{1,1}{F}\right) \cong \mathrm{Mat}_{2\times 2}(F)$.

ii) A is not a division algebra.

Proof. The implication "i) ⇒ ii)" follows directly from Rem. 1.6. The converse was shown in the proof of Prop. 1.12. □

Let A be an F-algebra.

Definition 1.16. For a finite dimensional F-algebra A we define the *algebra norm* and the *algebra trace* as

$$\begin{aligned} \mathrm{Nm}_{A/F}\colon A \to F,\ \alpha \mapsto \det(T_\alpha), \text{ respectively} \\ \mathrm{Tr}_{A/F}\colon A \to F,\ \alpha \mapsto \mathrm{tr}(T_\alpha), \end{aligned}$$

where T_α is the F-vector space endomorphism of A given by $\beta \mapsto \alpha\beta$.

Definition 1.17. An *involution* on A is an F-linear map

$$\bar{\cdot}\colon A \to A,\ \alpha \mapsto \overline{\alpha}$$

with

i) $\overline{1} = 1$,

ii) $\forall \alpha \in A\colon \overline{\overline{\alpha}} = \alpha$,

iii) $\forall \alpha, \beta \in A\colon \overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$.

The involution $\bar{\cdot}$ is called *standard* if also

iv) $\forall \alpha \in A\colon \alpha\overline{\alpha} \in F$.

Proposition 1.18. *Any F-algebra with an involution is isomorphic to its opposite algebra.*

Proof. By linearity and property iii) of Def. 1.17 an involution defines a homomorphism $A \to A^{\mathrm{op}},\ \alpha \to \overline{\alpha}$, and by ii) it is bijective. □

Lemma 1.19. *Given a standard involution on A we have $\forall \alpha \in A\colon \alpha + \overline{\alpha} \in F$.*

Proof. For any $\alpha \in A$ we have $\alpha + \overline{\alpha} = (\alpha + 1)\overline{(\alpha + 1)} - \alpha\overline{\alpha} - 1 \in F$. □

Definition 1.20. Given a standard involution on A the *reduced norm of α* is the map

$$\mathrm{nrd}\colon A \to F,\ \alpha \mapsto \alpha\overline{\alpha},$$

and the *reduced trace of α* is the map

$$\mathrm{trd}\colon A \to F,\ \alpha \mapsto \alpha + \overline{\alpha}.$$

For $\alpha \in A$ we call the polynomial

$$X^2 - \mathrm{trd}(\alpha)X + \mathrm{nrd}(\alpha) \in F[X]$$

the *reduced characteristic polynomial of α*.

Lemma 1.21. *Given any standard involution on A (which induces a reduced norm and a reduced trace), any $\alpha \in A$ is a root of its reduced characteristic polynomial.*

Proof. For any $\alpha \in A$ we have:

$$\alpha^2 - \mathrm{trd}(\alpha)\alpha + \mathrm{nrd}(\alpha) = \alpha^2 - \alpha\alpha - \overline{\alpha}\alpha + \alpha\overline{\alpha} = -\overline{\alpha}\alpha + \overline{\overline{\alpha}\alpha} = -\overline{\alpha}\alpha + \overline{\alpha}\alpha = 0.$$

□

Proposition 1.22. *Let K be a quadratic F-algebra (i.e. an F-algebra with $\dim_F(K) = 2$). Then K is commutative and has a unique standard involution.*

Proof. Let $\alpha \in K \setminus F$. Since $\dim_F(K) = 2$ we can write $K = F[\alpha]$ and hence K is commutative. Since 1 and α build a basis of K over F we can write $\alpha^2 = t\alpha - n$ for unique $t, n \in F$.

Assume that there is a standard involution on K and let $\tilde{\cdot}$ be any such. Then by Lemma 1.21 we have $\alpha^2 = \mathrm{trd}(\alpha)\alpha - \mathrm{nrd}(\alpha)$ and by uniqueness $t = \mathrm{trd}(\alpha) = \alpha + \tilde{\alpha}$ and $n = \mathrm{nrd}(\alpha)$ and hence every standard involution must satisfy $\tilde{\alpha} = t - \alpha$.

We can extend $\alpha \mapsto t - \alpha$ on K using F-linearity and get the map

$$\bar{\cdot}\colon K \to K,\ x + y\alpha \mapsto x + y(t - \alpha),$$

for any $x, y \in F$. By computing one can check that $\bar{\cdot}$ satisfies the conditions in Def. 1.17 and hence it defines the unique standard involution on K. □

Corollary 1.23. *If A possesses a standard involution, then it is unique.*

Proof. Let $\bar{\cdot}$ be a standard involution on A and pick an arbitrary $\alpha \in A \setminus F$. By Lemma 1.21 we have $\alpha^2 - trd(\alpha)\alpha + \mathrm{nrd}(\alpha)$ and hence $\dim_F F[\alpha] = 2$. By the previous proposition the restriction of $\bar{\cdot}$ to $F[\alpha]$ is unique and since α is arbitrary the standard involution is unique on A as well. □

Corollary 1.24. *Let* $\mathrm{char}(F) \neq 2$. *Any quaternion algebra* $A = \left(\frac{a,b}{F}\right)$ *possesses a unique standard involution. It is given by*

$$\alpha = t + xi + yj + zk \mapsto \overline{\alpha} = t - xi - yj - zk,$$

and hence $\mathrm{trd}(\alpha) = 2t$ *and* $\mathrm{nrd}(\alpha) = t^2 - ax^2 - by^2 + abz^2$.

Proof. By checking that the above defined map satisfies the axioms of a standard involution one proves the existence; the uniqueness is given by Cor. 1.23. □

Proposition 1.25. *Let A be a nontrivial F-algebra with a standard involution and $\alpha \in A \setminus \{0\}$. Then the following are equivalent:*

i) α *is not a left zero divisor.*

ii) α *is not a right zero divisor.*

iii) $\mathrm{nrd}(\alpha) \neq 0$.

iv) $\alpha \in A^\times$.

Proof. Suppose $\mathrm{nrd}(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha \neq 0$ and pick $\beta \in A$ with $\alpha\beta = 0$. Then $\mathrm{nrd}(\alpha)\beta = \overline{\alpha}\alpha\beta = 0$ and since $\mathrm{nrd}(\alpha) \in F^\times$ we have $\beta = 0$. Conversely if α is not a left zero divisor we have $\mathrm{nrd}(\alpha) = \alpha\overline{\alpha} \neq 0$. This proves "i) $\iff$ iii)"; the equivalence "ii) $\iff$ iii)" can be proven analogously.

Once again suppose that $\mathrm{nrd}(\alpha) \neq 0$. We have $\alpha\frac{\overline{\alpha}}{\mathrm{nrd}(\alpha)} = 1$ and hence $\alpha \in A^\times$. Finally suppose that $\alpha \in A^\times$ and pick $\beta \in A$ with $\alpha\beta = 0$. Then $\beta = 1\beta = \alpha^{-1}\alpha\beta = 0$ and hence α is not a left zero divisor. □

2 Quadratic forms and quadratic spaces

We introduce the reader to some basic theory of quadratic forms, which shall serve as foundation for our further discussion of quaternion algebras.

Definition 2.1. A *quadratic form* on an F-vector space V is a map $Q\colon V \to F$ with

i) $\forall \lambda \in F\ \forall x \in V\colon Q(\lambda x) = \lambda^2 Q(x)$, and

ii) the map $T\colon V \times V \to F,\ (x,y) \mapsto Q(x+y) - Q(x) - Q(y)$ is bilinear.

The pair (V,Q) is called *quadratic space* and T the *(symmetric) bilinear form associated to* Q.

Remark 2.2. Since for a quadratic form Q on V we have $\forall x \in V\colon T(x,x) = 2Q(x)$, if $\mathrm{char}(F) \neq 2$ we can uniquely determine Q by knowing T.

Let us assume that $\mathrm{char}(F) \neq 2$ and $n \coloneqq \dim_F(V) < \infty$ and let $B \coloneqq (b_i)_{1 \leqslant i \leqslant n}$ be a basis of V over F.

Definition 2.3. The symmetric $n \times n$-matrix

$$M_B(T) = (T(b_i, b_j))_{i,j} =: (m_{ij})_{i,j}$$

is called the *Gram matrix of* Q *in the basis* B.

By identifying V with F^n (endowed with the standard basis $(e_i)_{1 \leqslant i \leqslant n}$) via the isomorphism $\varphi\colon V \to F^n,\ b_i \mapsto e_i$ we get:

$$\forall x, y \in V\colon T(x,y) = \varphi(x)^T M_B(T) \varphi(y)$$

as well as

$$\forall x = \sum_{i=1}^{n} x_i b_i \in V\colon Q(x) = \frac{1}{2}\varphi(x)^T M_B(T)\varphi(x) = \frac{1}{2}\sum_{i,j=1}^{n} m_{ij} x_i x_j.$$

This yields a homogeneous polynomial of degree 2:

$$f_{Q,B}(X_1, \ldots, X_n) = \frac{1}{2}\sum_{i,j=1}^{n} m_{ij} X_i X_j \in F[X_1 \ldots X_n].$$

Definition 2.4. The polynomial $f_{Q,B}$ is called *polynomial representation of* Q *in the basis* B.

We consider another basis $B' \coloneqq (b'_i)_{1 \leqslant i \leqslant n}$ with basis change matrix $M_{BB'}$. Then the Gram matrix of Q with respect to B' is given by $M_{B'}(T) = M_{BB'}^T M_B(T) M_{BB'}$. Since $\det(M_{B'}(T)) = \det(M_{BB'})^2 \det(M_B(T))$ we notice that the determinant of the Gram matrix of Q is uniquely determined up to squares.

Definition 2.5. The *discriminant of* Q is defined as

$$\mathrm{disc}(Q) \coloneqq \det(M)\ (\mathrm{mod}(F^\times)^2) \in F/(F^\times)^2,$$

and is independent of the choice of the basis.

Remark 2.6. For a given homogeneous polynomial f of degree two in n variables and any given basis B of V there exists precisely one quadratic form Q on V such that $f = f_{Q,B}$. More explicitly, given $f = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ (without loss of generality $\forall i, j\colon a_{ij} = a_{ji}$) and a basis $B \coloneqq (b_i)_{1 \leqslant i \leqslant n}$ of V the form

$$Q\Big(\sum_{i=1}^{n} x_i b_i\Big) \coloneqq \frac{1}{2} f(x_1, \ldots, x_n)$$

satisfies $f_{Q,B} = f$.

Definition 2.7.

i) Two quadratic spaces (V, Q) and (V', Q') are said to be *similar* if there exists a pair (f, u), where $f\colon V \to V'$ is an F-vector space isomorphism and $u \in F^\times$ satisfying

$$\forall v \in V\colon Q'(f(x)) = uQ(x).$$

We denote the similarity by $Q \sim Q'$.

ii) Two quadratic forms $Q : V \to F$ and $Q'\colon V' \to F$ are said to be *isometric* if they are similar with similarity factor $u = 1$. We denote the isometry by $Q \cong Q'$. We call the isomorphism f an *isometry.*

iii) In the special case $(V, Q) = (V', Q')$ the isometry is called an *autometry.* The set $O(V)$ of all autometries of V is a subgroup of $\mathrm{Aut}_F(V)$.

If the underlying spaces are understood we speak simply of similar, respectively isometric quadratic forms. From the definition it follows directly that both similarity and isometry of quadratic forms are equivalence relations.

Proposition 2.8. *Let (V, Q) and (V', Q') be similar quadratic spaces, (f, u) as in Def. 2.7, and B, B' two bases of V and V' respectively. Then* $\mathrm{disc}(Q') = u^n \mathrm{disc}(Q) \in F/(F^\times)^2$.

Proof. The proof can be done with similar matrix manipulations as in Def. 2.3 – 2.5. □

Definition 2.9.

i) We say that $x, y \in V$ are *orthogonal* with respect to the quadratic form Q if $T(x, y) = 0$.

ii) For a subset $S \subset V$ the set $S^\perp \coloneqq \{x \in V \mid \forall y \in S\colon T(x, y) = 0\}$ is a subspace of V called the *orthogonal complement of S.*

iii) A basis of the quadratic space (V, Q) is said to be *orthogonal*, if the basis elements are pairwise orthogonal with respect to Q.

Definition 2.10.

i) The *orthogonal sum* of two quadratic spaces (V', Q') and (V'', Q'') is the quadratic space (V, Q), where

$$Q\colon V \coloneqq V' \oplus V'' \to F,\ x' + x'' \mapsto Q(x) + Q(x').$$

We denote the quadratic form Q by $Q' \perp Q''$ and the *orthogonal* direct sum of the two subspaces V' and V' by $V' \oplus V''$.

ii) For $a \in F$ we write $\langle a \rangle$ for the quadratic form $Q(x) = ax^2$ on F.

iii) More generally for $a_1, \ldots, a_n \in F$ we define $\langle a_1, \ldots, a_n \rangle \coloneqq \langle a_1 \rangle \perp \ldots \perp \langle a_n \rangle$.

Remark 2.11. In the notation from Def. 2.10 iii) we have:

i) $\forall c \in F\colon \langle a_1, \ldots, a_n \rangle \sim c\langle a_1, \ldots, a_n \rangle = \langle ca_1, \ldots, ca_n \rangle$.

ii) $\forall c \in F,\ \forall 1 \leqslant i \leqslant n\colon \langle a_1, \ldots, c^2 a_i, \ldots, a_n \rangle \cong \langle a_1, \ldots, a_n \rangle$.

iii) $\forall \sigma \in S_n\colon \langle a_1, \ldots, a_n \rangle \cong \langle a_{\sigma 1}, \ldots, a_{\sigma n} \rangle$.

Definition 2.12.

i) The subspace $\mathrm{rad}(V) \coloneqq V^\perp$ is called the *radical of* V. By choosing a subspace W complementary to $\mathrm{rad}(V)$ we obtain a (non unique) orthogonal decomposition

$$V = \mathrm{rad}(V) \oplus W,\ Q = 0 \perp Q|_W.$$

ii) The *rank* of the quadratic form Q, denoted by $\mathrm{rank}(Q)$, is defined as the codimension of $\mathrm{rad}(V)$.

Proposition 2.13. *Let A be an F-algebra with a standard involution. Then:*

i) The reduced norm nrd *defines a quadratic form on A and the associated bilinear form is given by $T(\alpha, \beta) = \mathrm{trd}(\alpha\overline{\beta})$.*

ii) Two elements α and β of A are orthogonal if and only if $\mathrm{trd}(\alpha\overline{\beta}) = \alpha\overline{\beta} + \overline{\alpha}\beta = 0$.

iii) If $1, \alpha, \beta \in A$ are linearly independent, then they are pairwise orthogonal if and only if $\alpha\beta = -\beta\alpha$.

Proof.

i) We check the axioms of a quadratic form. In the first place for any $\alpha \in A$ and for any $\lambda \in F$ we have $\mathrm{nrd}(\lambda\alpha) = \lambda\alpha\overline{\lambda\alpha} = \lambda^2\alpha\overline{\alpha} = \lambda^2\mathrm{nrd}(\alpha)$. For any $\alpha, \beta \in A$ we define $T(\alpha, \beta) \coloneqq \mathrm{nrd}(\alpha + \beta) - \mathrm{nrd}(\alpha) - \mathrm{nrd}(\beta)$. This is clearly symmetric. By computing we obtain:

$$\begin{aligned} T(\alpha, \beta) &= (\alpha + \beta)\overline{(\alpha + \beta)} - \alpha\overline{\alpha} - \beta\overline{\beta} \\ &= \alpha\overline{\alpha} + \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta} - \alpha\overline{\alpha} - \beta\overline{\beta} \\ &= \alpha\overline{\beta} + \overline{\alpha\overline{\beta}} = \mathrm{trd}(\alpha\overline{\beta}) \end{aligned}$$

By symmetry it suffices to prove the linearity of T only in the first component. For any $\alpha, \beta, \gamma \in A$ and for any $\lambda, \mu \in F$ we have:

$$\begin{aligned} T(\lambda\alpha + \mu\beta, \gamma) &= (\lambda\alpha + \mu\beta)\overline{\gamma} + \gamma\overline{(\lambda\alpha + \mu\beta)} \\ &= \lambda\alpha\overline{\gamma} + \lambda\gamma\overline{\alpha} + \mu\beta\overline{\gamma} + \mu\gamma\overline{\beta} \\ &= \lambda T(\alpha, \gamma) + \mu T(\beta, \gamma), \end{aligned}$$

which proves the bilinearity.

ii) follows directly from i).

iii) Using the computations from i) we obtain:

$$\begin{aligned}\alpha\beta + \beta\alpha &= \alpha(\beta + \overline{\beta}) + \beta(\alpha + \overline{\alpha}) - \alpha\overline{\beta} - \beta\overline{\alpha} \\ &= \alpha \operatorname{trd}(\beta) + \beta \operatorname{trd}(\alpha) - \operatorname{trd}(\alpha\overline{\beta}) \\ &= \alpha \operatorname{trd}(\beta\overline{1}) + \beta \operatorname{trd}(\alpha\overline{1}) - \operatorname{trd}(\alpha\overline{\beta}).\end{aligned}$$

Assume that $1, \alpha, \beta$ are linearly independent. If they are pairwise orthogonal then $\alpha\beta + \beta\alpha = 0$. Conversely, if $\alpha\beta + \beta\alpha = 0$ by linear independence we obtain $\operatorname{trd}(\alpha) = \operatorname{trd}(\beta) = \operatorname{trd}(\alpha\overline{\beta}) = 0$ and hence $1, \alpha, \beta$ are pairwise orthogonal. □

Definition 2.14. A quadratic form $Q\colon V \to F$ is called *nondegenerate* if for all $x \in V \setminus \{0\}$ the homomorphism $T_x\colon V \to F,\ y \mapsto T(x, y)$ is nonzero, or equivalently if the homomorphism $V \to V^*,\ x \mapsto T_x$ is injective. Otherwise Q is called *degenerate*.

Proposition 2.15. *Let Q be a quadratic form on an n-dimensional space V. The following are equivalent:*

i) Q *is nondegenerate.*

ii) $\operatorname{rad}(V) = 0$.

iii) $\operatorname{rank}(Q) = n$.

iv) $\operatorname{disc}(V) \neq 0$.

Proof. The equivalence of the first three statements follows directly from the definitions, hence we prove only "i) $\iff$ iv)". Choose a basis B of V and identify V with F^n endowed with the standard basis. Let $M_B(T)$ be the Gram matrix of Q in the basis B. Then:

$$\begin{aligned}Q \text{ is nondegenerate} &\iff \forall x \in V\colon (\forall y \in V\colon T(x, y) = 0 \Rightarrow x = 0) \\ &\iff \forall x \in F^n\colon (\forall y \in F^n\colon x^T M_B(T) y = 0 \Rightarrow x = 0) \\ &\iff \det(M_B(T)) \neq 0 \\ &\iff \operatorname{disc}(Q) \neq 0.\end{aligned}$$

□

Example 2.16. The reduced norm of a quaternion algebra $\left(\frac{a,b}{F}\right)$ with $\operatorname{char}(F) \neq 2$, as seen in Cor. 1.24, defines a nondegenerate quadratic form of rank 4, which is isometric to the form $\langle 1, -a, -b, ab\rangle$ on F^4.

Proposition 2.17. *Let (V, Q) be a quadratic space and let $v \in V$ with $Q(v) \neq 0$. Then we get an orthogonal decomposition $V = \operatorname{span}\{v\} \oplus \operatorname{span}\{v\}^\perp,\ Q = Q|_{\operatorname{span}\{v\}} \perp Q|_{\operatorname{span}\{v\}^\perp}$.*

Proof. For every $x \in V$ we consider the decomposition

$$x = \frac{T(v, x)}{T(v, v)} v + \left(x - \frac{T(v, x)}{T(v, v)} v\right).$$

Then we have $T\big(v, x - \frac{T(v,x)}{T(v,v)} v\big) = 0$ and hence $x - \frac{T(v,x)}{T(v,v)} v \in \operatorname{span}\{v\}^\perp$. Geometrically we can interpret the second summand as the projection of x to $\operatorname{span}\{v\}$. Since $Q(v) \neq 0$ we have $\operatorname{span}\{v\} \cap \operatorname{span}\{v\}^\perp = \{0\}$, which implies $V = \operatorname{span}\{v\} \oplus \operatorname{span}\{v\}^\perp$ and by definition of the orthogonal complement we have $V = \operatorname{span}\{v\} \oplus \operatorname{span}\{v\}^\perp$. □

Proposition 2.18. *Every quadratic space (V, Q) possesses an orthogonal basis. This implies that every quadratic form Q has a representation of the type $f_{Q,B}(X_1, \dots, X_n) = a_1X_1^2 + \cdots a_nX_n^2$ with $a_i \in F$ for some basis B, or in other words for every quadratic form Q there exist $a_1, \dots, a_n \in F$ such that Q is isometric to the form $\langle a_1, \dots, a_n \rangle$.*

Proof. The claim follows from Prop. 2.17 by induction over $\dim_F(V)$ and by taking into account that every basis of a degenerate quadratic space is orthogonal. □

Definition 2.19. Let $Q\colon V \to F$ be a quadratic form.

i) We say that Q *represents* an element $a \in F$ if there exists a $x \in V$ such that $Q(x) = a$.

ii) The quadratic form Q (or the quadratic space (V, Q)) is said to be *isotropic* if it represents $0 \in F$ nontrivially, i.e. if there exists a $x \in V \setminus \{0\}$ such that $Q(x) = 0$.

iii) The quadratic form Q (or the quadratic space (V, Q)) is said to be *universal* if it represents every element of F.

Remark 2.20.

i) A degenerate quadratic form is always isotropic.

ii) If Q and Q' are two similar quadratic forms, then Q is isotropic if and only if Q' is.

iii) Two isometric quadratic forms represent the same elements of F, so if Q and Q' are two isometric quadratic forms, then Q is universal if and only if Q' is.

Example 2.21. Given a two-dimensional F-vector space V and a basis (e_1, e_2) the quadratic form given by $f(X, Y) = XY$ (as explained in Rem. 2.6) is called *hyperbolic plane.* It is clearly universal, and the Gram matrix of the quadratic form with respect to the basis (e_1, e_2) is given by

$$M \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Equivalently a quadratic form Q on V is a hyperbolic plane if there exists a basis (e_1, e_2) of V with $T(e_1, e_1) = T(e_2, e_2) = 0$ and $T(e_1, e_2) = 1$.

Proposition 2.22. *A nondegenerate quadratic form Q is isotropic if and only if it is the orthogonal sum of a hyperbolic plane H and a nondegenerate quadratic form Q'.*

Proof. We follow the proof from Ch. 2, Lemma 2.1 of [Cas08].

"⇐" Clear since the hyperbolic plane is isotropic.

"⇒" Since Q is isotropic there exists an element $e_1 \in V$ with $Q(e_1) = 0$ (and hence $T(e_1, e_1) = 0$). Since Q is nondegenerate, there exists $x \in V$ with $T(e_1, x) \neq 0$. By rescaling x we can assume that $T(e_1, x) = 1$. By putting $e_2 \coloneqq x - Q(x)(e_1)$ we get:

$$\begin{aligned} &T(e_2, e_2) = T(x, x) - 2Q(x)T(x, e_1) + Q(x)^2T(e_1, e_1) = 0 \text{ and} \\ &T(e_1, e_2) = T(e_1, x) - Q(x)T(e_1, e_1) = 1. \end{aligned}$$

$H \coloneqq Q|_{\operatorname{span}\{e_1, e_2\}}$ and $Q' \coloneqq Q|_{\{e_1, e_2\}^\perp}$ do the job. □

Corollary 2.23. *Nondegenerate isotropic quadratic forms are universal.*

Proof. A nondegenerate isotropic quadratic form contains a hyperbolic plane, which is universal. □

Corollary 2.24. *Let $Q\colon V \to F$ be an n-dimensional nondegenerate quadratic form, let $a \in F^\times$. Then the following are equivalent:*

i) Q represents a.

ii) Q is isometric to $Q' \perp \langle a\rangle$ for some $n-1$-dimensional nondegenerate quadratic form Q'.

iii) The quadratic form $Q \perp \langle -a\rangle$ represents 0 nontrivially.

Proof. It is clear that ii) implies both i) and iii). If Q represents a, so there exists $x \in V$ with $Q(x) = a$. Define $Q' \coloneqq Q|_{\operatorname{span}\{x\}^\perp}$. Since $Q|_{\operatorname{span}\{x\}}$ is isometric to $\langle a\rangle$ we get the isometry $Q \cong Q' \perp \langle a\rangle$. Thus i) implies ii). Finally we prove "iii) $\Rightarrow$ ii)". Let $Q \perp \langle -a\rangle$ represent 0 nontrivially. Then there exist $x \in V$ and $y \in F$ with $Q(x) - ay^2 = 0$. If $y = 0$, then $x \neq 0$ and hence Q is isotropic, thus by Cor. 2.23 Q represents a. If $y \neq 0$ we have $Q(\frac{x}{y}) = a$ and we are done. □

Now, similarly as in Prop. 2.17, for any $v \in V$ with $Q(v) \neq 0$ we consider the endomorphism

$$\tau_v\colon V \to V,\ x \mapsto x - \frac{2T(v,x)}{T(v,v)}v.$$

Lemma 2.25. *The endomorphism τ_v satisfies the following properties:*

i) $\forall x \in V\colon Q(\tau_v(x)) = Q(x)$.

ii) $\forall x \in V\colon \tau_v(\tau_v(x)) = x$.

iii) $\forall x \in \operatorname{span}\{v\}\colon \tau_v(x) = -x$.

iv) $\forall x \in \operatorname{span}\{v\}^\perp\colon \tau_v(x) = x$.

In particular the first two statements imply that τ_v is an autometry of V.

Proof. The proof can be done by simple calculation. □

Lemma 2.26. *For any $x, y \in V$ with $Q(x) = Q(y) \neq 0$ there exists an autometry τ of V with $\tau(x) = y$.*

Proof. Since $Q(x) = Q(y)$ implies $T(x,x) = T(y,y)$ we have

$$\begin{aligned} Q(x-y) + Q(x+y) &= Q(x-y+x+y) - Q(x-y+x+y) + Q(x-y) + Q(x+y) \\ &= Q(2x) - T(x-y, x+y) \\ &= 4Q(x) - T(x,x) + T(y,y) \\ &= 4Q(x) \neq 0, \end{aligned}$$

which implies that $Q(x-y)$ and $Q(x+y)$ cannot be both equal zero. If $Q(x-y) \neq 0$ then

$$\tau_{x-y}(x) = x - \frac{2T(x,x-y)}{T(x-y,x-y)}(x-y) = x - \frac{2T(x,x-y)}{2T(x,x-y)}(x-y) = y$$

and by setting $\tau \coloneqq \tau_{x-y}$ we are done. Otherwise we have $Q(x+y) \neq 0$ and

$$\tau_{x+y}(x) = x - \frac{2T(x, x+y)}{T(x+y, x+y)}(x+y) = x - \frac{2T(x, x+y)}{2T(x, x+y)}(x+y) = -y.$$

By the previous lemma $\tau_y \tau_{x+y}(x) = \tau_y(-y) = y$ and we conclude by setting $\tau \coloneqq \tau_y \tau_{x+y}$. □

Remark 2.27. We can interpret τ_v geometrically as the reflection with respect to the hyperplane orthogonal to v. In the special case $V = \mathbb{R}^n$ and $Q(x) = \frac{1}{2}||x||^2$ it is called *Householder reflection*; the reader may have encountered it in linear algebra or numerical analysis.

With these both lemmas we can prove the following important theorem of the theory of quadratic forms.

Theorem 2.28 (Witt)**.** *Let (V, Q) and (V', Q') be two isometric quadratic spaces with orthogonal decompositions $W_1 \oplus W_2$ and $W_1' \oplus W_2'$, with nondegenerate subspaces W_1 and W_1'. Then the following two equivalent statements hold:*

i) (Witt cancellation) If W_1 and W_1' are isometric, then W_2 and W_2' are isometric as well.

ii) (Witt extension) If $g\colon W_1 \to W_1'$ is an isometry, then there exists an isometry $f\colon V \to V'$ with $f|_{W_1} = g$ and $f(W_2) = W_2'$.

Proof. We follow the proof of Satz 3.1 of [Kne02]. In the first place let us prove the equivalence of the two statements.

"⇒" Let $g\colon W_1 \to W_1'$ be an isometry. By i) there is an isometry $h\colon W_2 \to W_2'$. Then the isometry $f \coloneqq g \oplus h\colon W_1 \oplus W_2 \to W_1' \oplus W_2'$ is an extension of g.

"⇐" Let $g\colon W_1 \to W_1'$ be an isometry. By ii) there is an extension f of g with $f(W_2) = W_2'$. Then $h \coloneqq f|_{W_2}$ is an isometry $W_2 \to W_2'$.

We prove ii) using induction on $m \coloneqq \dim_F(W_1) = \dim_F(W_1')$. For $m = 0$ there is nothing to show. If $m > 0$ chose an orthogonal basis $(b_i)_{1 \leqslant i \leqslant m}$ for W_1. Thus we can write

$$V = W_1 \oplus W_2 = \bigoplus_{i=1}^{m-1} Fb_i \oplus Fb_m \oplus W_2.$$

By induction hypothesis there exists an isometry $\tilde{f}\colon V \to V'$ satisfying $\forall 1 \leqslant i \leqslant m-1\colon \tilde{f}(b_i) = g(b_i)$. We define $\tilde{b}_m \coloneqq \tilde{f}^{-1}\big(g(b_m)\big)$. Since $f^{-1} \circ g$ is an autometry of V it preserves orthogonality, which implies that $\tilde{b}_m$ is orthogonal to b_i for all $i < m$. Moreover we have $Q(\tilde{b}_m) = Q\big(f^{-1}\big(g(b_m)\big)\big) = Q(b_m) \neq 0$ since $\operatorname{span}\{b_m\}$ is a regular subspace of V. By Lemma 2.26 there is a $\tau \in \{\tau_{b_m - \tilde{b}_m}, \tau_{\tilde{b}_m} \tau_{b_m + \tilde{b}_m}\}$ sending b_m to $\tilde{b}_m$. By orthogonality τ fixes b_i for any $i < m$. We conclude by setting $f \coloneqq \tilde{f} \circ \tau$. This is in fact an isometry $V \to V'$ and its restriction on W_1 is by construction equal to g. □

Now we can apply the theory of quadratic forms which we developed in this section to prove three theorems which build the first step towards the classification of the rational quaternion algebras.

Let A be a quaternion algebra over F. Then we define the subspace of *pure quaternions* $A_0 \coloneqq \{\alpha \in A \mid \operatorname{trd}(A) = 0\} = \{1\}^\perp$. By Ex. 2.16 and Thm. 2.28 i) the restriction of the reduced norm on A_0 defines a quadratic form in three variables, which is isometric to $\langle -a, -b, ab\rangle$ for a and b in $F^\times$ such that $A \cong \left(\frac{a,b}{F}\right)$.

Theorem 2.29. *Let A and A' be two quaternion algebras over F. According to Cor. 1.24 and Prop. 2.13 both algebras with their respective reduced norms are quadratic spaces. Then the following are equivalent:*

i) A and A' are isomorphic as F-algebras.

ii) A and A'^{op} are isomorphic as F-algebras.

iii) A and A' are isometric as quadratic spaces.

iv) A_0 and A'_0 are isometric as quadratic spaces.

If $f\colon A_0 \to A'_0$ is an isometry, then f extends uniquely to either an isomorphism $f\colon A \to A'$ or to an isomorphism $f\colon A \to A'^{\mathrm{op}}$ of F-algebras.

Proof. The equivalence between i) and ii) follows from the fact that any any algebra with a standard involution is isomorphic to its opposite algebra. The equivalence between iii) and iv) follows directly from Thm. 2.28.

We prove "i) $\Rightarrow$ iii)". Let $f\colon A \to A'$ be an F-algebra isomorphism. From Cor. 1.23 we know that the standard involutions (and hence the reduced norms) on A and on A' are unique. Let us denote both standard involutions by $\bar{\cdot}$ and both reduced norms by nrd. Since $\alpha' \mapsto f\big(\overline{f^{-1}(\alpha')}\big)$ defines a standard involution on A' as well, we have $\forall \alpha' \in A'\colon \overline{\alpha'} = f\big(\overline{f^{-1}(\alpha')}\big)$. So we have

$$\forall \alpha \in A\colon \mathrm{nrd}(f(\alpha)) = f(\alpha)\overline{f(\alpha)} = f(\alpha)f(\overline{\alpha}) = f(\alpha\overline{\alpha}) = f(\mathrm{nrd}(\alpha)) = \mathrm{nrd}(\alpha),$$

where the last equality follows from the fact that $\mathrm{nrd}(\alpha) \in F$. So f is an isometry of quadratic spaces.

Finally we prove "iv) $\Rightarrow$ i)". Let $f\colon A_0 \to A'_0$ be an isometry. Write $A = \left(\frac{a,b}{F}\right)$ with $a, b \in F^\times$ and standard generators i, j, as in Def. 1.11. Since $f(i) \in A'_0$, we have $\overline{f(i)} = -f(i)$ and hence

$$f(i)^2 = -f(i)\overline{f(i)} = -\mathrm{nrd}(f(i)) = -\mathrm{nrd}(i) = a.$$

Analogously we have $f(j)^2 = b$. Since i, j and ij are pairwise orthogonal and isometries preserve orthogonality, $f(i), f(j)$ and $f(ij)$ are pairwise orthogonal as well. In particular by Prop. 2.13 iii) we get $f(i)f(j) = -f(j)f(i)$. Moreover from $\mathrm{trd}\big(f(i)f(j)\overline{f(i)}\big) = a\ \mathrm{trd}(f(j)) = 0$ and $\mathrm{trd}\big(f(i)f(j)\overline{f(j)}\big) = -b\ \mathrm{trd}(f(i)) = 0$ it follows that $f(i)f(j)$ is orthogonal to both $f(i)$ and $f(j)$. Since $\dim_F(A'_0) = 3$ there exists an $u \in F^\times$ with $f(ij) = uf(i)f(j)$. By taking reduced norms we get

$$\begin{aligned}\mathrm{nrd}(i)\mathrm{nrd}(j) = \mathrm{nrd}(ij) &= \mathrm{nrd}(f(ij)) = \mathrm{nrd}(uf(i)f(j)) \\ &= u^2\mathrm{nrd}(f(i))\mathrm{nrd}(f(j)) = u^2\mathrm{nrd}(i)\mathrm{nrd}(j),\end{aligned}$$

which implies that $u = \pm 1$. If $u = 1$ we have $f(ij) = f(i)f(j)$ and f extends to an algebra isomorphism $A \to A'$ via $1 \mapsto 1$. Otherwise $f(ij) = -f(i)f(j)$ and f extends to an algebra isomorphism $A \to A'^{\mathrm{op}}$ via $1 \mapsto 1$. By postcomposing it with the standard involution $A'^{\mathrm{op}} \to A'$ we get an F-algebra isomorphism $A \to A'$. □

Theorem 2.30. *There is a bijection:*

$$\left\{\begin{array}{c}\textit{Quaternion algebras}\\ \textit{over } F \textit{ up to}\\ \textit{isomorphism}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{Ternary quadratic forms}\\ \textit{over } F \textit{ with discriminant}\\ 1 \in F^\times/(F^\times)^2 \textit{ up to isometry}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{Nondegenerate ternary}\\ \textit{quadratic forms over}\\ F \textit{ up to similarity}\end{array}\right\}$$

Proof. We begin with the proof of the first bijection. From the equivalence "i) $\iff$ iv)" of Thm. 2.29 the map $A \mapsto \operatorname{nrd}|_{A_0}$ yields a well-defined injective map $[A] \mapsto [\operatorname{nrd}|_{A_0}]$ between isomorphy and isometry classes. In order to prove the surjectivity of this map we consider a quadratic space (Q, V) with $\operatorname{disc}(Q) = 1 \in F^\times/(F^\times)^2$. By choosing an orthogonal basis according to Prop. 2.18 we obtain an isometry $Q \cong \langle -a, -b, c\rangle$ for some $a, b, c \in F$ with $abc \in (F^\times)^2$ (and following $\frac{c}{ab} \in (F^\times)^2$). Rescaling the third basis vector with Rem. 2.11 ii) yields

$$Q \cong \langle -a, -b, c\rangle = \left\langle -a, -b, ab\ \frac{c}{ab}\right\rangle \cong \langle -a, -b, ab\rangle \cong \operatorname{nrd}|_{A_0},$$

with $A = \left(\frac{a,b}{F}\right)$, so the map is surjective.

Next we prove the second bijection. The natural map sending the isometry class of a quadratic form to the similarity class of the quadratic form is clearly well-defined. To prove the surjectivity we need to prove that every nondegenerate ternary quadratic form is similar to some form with discriminant 1. Let Q be a nondegenerate ternary quadratic form. By choosing an orthogonal basis and using Rem. 2.11 we obtain

$$Q \cong \langle a, b, c\rangle \sim abc\langle a, b, c\rangle = \langle a^2bc, ab^2c, abc^2\rangle \cong \langle bc, ac, ab\rangle,$$

with the last quadratic form having discriminant $1 \in F^\times/(F^\times)^2$. This proves the surjectivity.

In order to prove the injectivity we consider two quadratic spaces (Q, V) and (Q', V') with discriminant $1 \in F^\times/(F^\times)^2$ whose isometry classes map to the same similarity class (hence Q and Q' are similar). We want to prove that they are in fact isometric. By the definition of similarity there exists a $u \in F^\times$ and an isomorphism $f\colon V \to V'$ with $\forall x \in V\colon Q'(f(x)) = uQ(x)$. By Prop. 2.8 we have $1 = \operatorname{disc}(Q') = u^3 \operatorname{disc}(Q) = u \operatorname{disc}(Q) \in F^\times/(F^\times)^2$ and following $u \in (F^\times)^2$. We write $u = c^2$ for a $c \in F^\times$ and obtain

$$Q'(c^{-1}f(x)) = c^{-2}Q'(f(x)) = u^{-1}uQ(x) = Q(x).$$

So Q and Q' are isometric via $c^{-1}f$ and hence the map is injective (and bijective). □

Lemma 2.31. *Let $a \in F^\times$ and let $i \notin F$ with $i^2 = a$ and consider the F-algebra $K := F[i]$, which is isomorphic to $F[X]/(X^2 - a)$ as a ring.*

i) If a is a square in F then K is isomorphic to $F \times F$ as a ring, thus it is not a field.

ii) If a is not a square in F then K is a quadratic field extension of F and is therefore equal to its own fraction field $F(i)$.

Proof. If a is a square in F we choose a square root of a in F and denote it by $\sqrt{a}$. We consider the ring homomorphism $\varphi\colon F[X] \to F \times F,\ f \mapsto \big(f(\sqrt{a}), f(-\sqrt{a})\big)$. It is surjective as for any $(b_1, b_2) \in F \times F$ the polynomial $f(X) = \frac{1}{2\sqrt{a}}(b_1 - b_2)X + \frac{1}{2}(b_1 + b_2)$ is a preimage of (b_1, b_2) under φ. The ideal $(X^2 - a)$ is contained in the kernel of φ and by the universal property of the factor rings there exists a well-defined surjective homomorphism $\overline{\varphi}\colon F[X]/(X^2 - a) \to F \times F$, which is also an F-linear map between two-dimensional F-vector spaces. Dimensions being the reason for it, $\overline{\varphi}$ is bijective and hence a ring isomorphism, which proves i).

If a is not a square in F, the polynomial $X^2 - a$ is irreducible in $F[X]$ and hence $K \cong F[X]/(X^2 - 1)$ is a field, which proves ii). □

Lemma 2.32. *Let K be as in the previous lemma. Then for any $\alpha = x + iy \in K$ we have:*

$$\mathrm{Nm}_{K/F}(x + iy) = x^2 - ay^2.$$

Proof. K is a two dimensional vector space with basis $B \coloneqq (1, i)$. Since $(x + iy)1 = x + iy$ and $(x + iy)i = ay + ix$ the transformation matrix of $T_\alpha \colon K \to K,\ \beta \mapsto \alpha\beta$ in the basis B is given by

$$M_{BB}(T_\alpha) = \begin{pmatrix} x & ay \\ y & x \end{pmatrix}.$$

So $\mathrm{Nm}_{K/F}(x + iy) = \det(M_{BB}(T_\alpha)) = x^2 - ay^2$. □

Theorem 2.33. *Let $A = \left(\frac{a,b}{F}\right)$ be a quaternion algebra over F with standard generators i and j. Then the following are equivalent:*

i) $A \cong \left(\frac{1,1}{F}\right) \cong \mathrm{Mat}_{2\times 2}(F)$.

ii) A is not a division algebra.

iii) The quadratic form $\mathrm{nrd} \cong \langle 1, -a, -b, ab\rangle$ *is isotropic.*

iv) The quadratic form $\mathrm{nrd}|_{A_0} \cong \langle -a, -b, ab\rangle$ *is isotropic.*

v) The binary form $\langle a, b\rangle$ represents 1.

vi) $b \in \mathrm{Nm}_{K/F}(K^\times)$, *where* $K \coloneqq F[i]$.

Proof. The equivalence between i) and ii) is the statement of Prop. 1.15. The equivalence between ii) and iii) follows from Rem. 1.6 and Prop. 1.25.

We prove "iii) ⇒ iv)". Choose $\alpha \in A \smallsetminus \{0\}$ with $\mathrm{nrd}(\alpha) = 0$. If $\mathrm{trd}(\alpha) = 0$ we are done. Otherwise chose $\beta \in A \smallsetminus \{0\}$ orthogonal to 1 and α, satisfying $\mathrm{trd}(\alpha\beta) = 0$. The last condition tells us that $\alpha\beta$ lies in A_0. Since $\alpha\beta + \overline{\alpha}\beta = (\alpha + \overline{\alpha})\beta \neq 0$ we get that $\alpha\beta$ and $\overline{\alpha}\beta$ cannot be both zero. If $\alpha\beta \neq 0$ we are done, since $\mathrm{nrd}(\alpha\beta) = \mathrm{nrd}(\alpha)\ \mathrm{nrd}(\beta) = 0$. Otherwise we observe that $\mathrm{trd}(\overline{\alpha}\beta) = \mathrm{trd}\big(\overline{\overline{\alpha}\beta}\big) = \mathrm{trd}(\overline{\beta}\alpha) = 0$ and hence $\overline{\alpha}\beta$ lies in A_0, too. Then, just as above, we conclude by saying that $\mathrm{nrd}(\overline{\alpha}\beta) = 0$.

Next we prove "iv) ⇒ v)". Let $\alpha = xi + yj + zk \in A_0$ with $\mathrm{nrd}(\alpha) = -ax^2 - by^2 + abz^2 = 0$. If $z = 0$, the form $\langle a, b\rangle$ is isotropic and hence universal by Cor. 2.23, so it represents 1. Otherwise we have $a(\frac{y}{az})^2 + b(\frac{x}{bz})^2 = 1$ and we are done.

Now we prove "v) ⇒ vi)". Assume that the form $\langle a, b\rangle$ represents 1. So there exist x and y in F with $ax^2 + by^2 = 1$. If $y \neq 0$, then $b = (\frac{1}{y})^2 - a(\frac{x}{y})^2 = \mathrm{Nm}_{K/F}(\frac{1}{y} - i\frac{x}{y}) \in \mathrm{Nm}_{K/F}(K^\times)$. If $y = 0$, then $a = \left(\frac{1}{x}\right)^2$ a square in F. We fix a square root $\sqrt{a} \in F$. Then $\mathrm{Nm}_{K/F}\left((1 + \frac{b}{4}) - \frac{i}{\sqrt{a}}(1 - \frac{b}{4})\right) = b$ and we are done. (In fact in the case that a is a square in F the map $\mathrm{Nm}_{K/F}$ is surjective.)

Finally we prove "vi) ⇒ iii)". If $b \in \mathrm{Nm}_{K/F}(K^\times)$, there exist x and y in F with $b = x^2 - ay^2$. Then $\mathrm{nrd}(x + iy + j) = x^2 - ay^2 - b = 0$ and hence nrd is isotropic. □

Definition 2.34. A quaternion algebra which satisfies these equivalent conditions is said to be *split.*

3 Quaternion algebras over the fields $\mathbb{R}$ and $\mathbb{Q}_p$

The reader may already be familiar with the p-adic numbers $\mathbb{Q}_p$ and the p-adic integers $\mathbb{Z}_p$. Before we apply the theory of the p-adic numbers to rational quaternion algebras we want to give a very quick recap of the basic definitions and some basic results. For a more detailed introduction to the p-adic numbers we refer the reader to Ch. II of [Ser73] or to Section 2 of [Jer17].

Given a prime number p, we consider the so-called p-adic valuation

$$v_p \colon \mathbb{Q} \to \mathbb{R},\ x \mapsto v_p(x) \coloneqq \begin{cases} \infty & \text{if } x = 0, \\ n & \text{for } x = p^n \frac{a}{b},\ \text{with } a, b, n \in \mathbb{Z}, ab \neq 0,\ \text{and } p \nmid ab \end{cases}.$$

The *p-adic valuation* yields an absolute value, called the *p-adic absolute value*, denoted by $|\cdot|_p$ on $\mathbb{Q}$ and given by $|x|_p \coloneqq p^{-v_p(x)}$, with the convention $p^{-\infty} \coloneqq 0$. The *p-adic numbers* $\mathbb{Q}_p$ arise as a completion of $\mathbb{Q}$, seen as a metric space, with respect to the p-adic absolute value.

It is conventional to allow p to be not only a prime number, but also ∞. In the above notation we denote the usual absolute value on $\mathbb{Q}$ by $|\cdot|_\infty$. The field of the real numbers $\mathbb{R}$ can be seen as a completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ and therefore it is sometimes denoted by $\mathbb{Q}_\infty$. In both cases the absolute value $|\cdot|_p$ on $\mathbb{Q}$ extends isometrically to an absolute value on $\mathbb{Q}_p$, which we denote in the same way.

Finally, there is the trivial absolute value on $\mathbb{Q}$: it is given by $|0|_{\mathrm{tr}} = 0$ and $|x|_{\mathrm{tr}} = 1$ for $x \neq 0$. The field of rational numbers is a complete metric space with respect to the metric induced by this absolute value and is therefore its own completion.

According to Ostrowski's theorem, any nontrivial absolute value on $\mathbb{Q}$ is equivalent to precisely one of the absolute values $|\cdot|_p$ for p a prime number or $p = \infty$, thus the only nontrivial completions of $\mathbb{Q}$ are given by $\mathbb{Q}_p$ for p a prime number or $p = \infty$. Since the proof of this theorem would lead us too far away from the actual goal of this thesis, we refer the interested reader to the proof of Thm. 3.1.3 of [Gou97].

Throughout this section we will assume $p \neq \infty$, unless stated otherwise. For prime p we define the *p-adic integers* $\mathbb{Z}_p$ as the closed unit ball in $\mathbb{Q}_p$. i.e.

$$\mathbb{Z}_p \coloneqq \{x \in \mathbb{Q}_p \mid\ |x|_p \leqslant 1\} = \{x \in \mathbb{Q}_p \mid\ v_p(x) \geqslant 0\}$$

One can show that $\mathbb{Z}_p$ is a subring of the field $\mathbb{Q}_p$ and that

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p \mid\ |x|_p = 1\} = \{x \in \mathbb{Q}_p \mid\ v_p(x) = 0\}.$$

We call $\mathbb{Z}_p^\times$ the *group of p-adic units.* It will be useful to know that for a prime p every element x of $\mathbb{Q}_p^\times$ can be written uniquely as $x = up^n$ for an integer $n \in \mathbb{Z}$ and a p-adic unit u. The exponent n is given by the extension of the p-adic valuation to $\mathbb{Q}_p$, so $n = v_p(x)$.

Furthermore $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$ and the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (one shows this applying the homomorphism theorem to the composition $\mathbb{Z} \hookrightarrow \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p/p\mathbb{Z}_p$).

The goal of this section is to prove that over any field $\mathbb{Q}_p$ (whereby we allow the possibility $p = \infty$) there exist, up to isomorphy, only two quaternion algebras: $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ and a uniquely determined division algebra. Before we can prove this theorem we need some preparatory results about quadratic forms over finite fields and over the p-adic integers.

Proposition 3.1. *Let k be a finite field of odd cardinality and let Q be a quadratic form over a k-vector space V.*

i) If $\operatorname{rank}(Q) \geqslant 2$ *then Q represents all elements of $k^\times$.*

ii) If $\operatorname{rank}(Q) \geqslant 3$ *then Q represents all elements of k (i.e. it is universal).*

Proof. We follow the proof of Prop. 4, Ch. IV of [Ser73]. We denote by q the cardinality of k. The subgroup $(k^\times)^2$ of nonzero squares has index 2 in $k^\times$ (this can be easily proven applying the homomorphism theorem to $k^\times \to k^\times,\ x \mapsto x^2$), hence $|(k^\times)^2| = \frac{q-1}{2}$ and $|k^2| = \frac{q+1}{2}$.

Let $a, b, c \in k^\times$. We show that the equation $ax^2 + by^2 = c$ has a solution $(x, y) \neq (0, 0)$. We define the sets $A \coloneqq \{ax^2 \mid x \in k\}$ and $B \coloneqq \{c - by^2 \mid y \in k\}$. Since they both have cardinality $\frac{q+1}{2}$ they have a nonempty intersection. Let $z \coloneqq ax^2 = c - by^2 \in A \cap B$ for some $x, y \in k$. Then (x, y) is a nonzero solution of the above equation.

i) If $Q\colon V \to k$ is a quadratic form of rank $n \geqslant 2$ there exists an isometry $Q \cong \langle a, b\rangle \perp Q'$ for some $a, b \in k^\times$ and some quadratic form $Q'\colon k^{n-2} \to k$. For any $c \in k^\times$ by the above argument we can find $x, y \in k^\times$ with $ax^2 + by^2 = c$. Thus $(\langle a, b\rangle \perp Q')(x, y, 0, \ldots, 0) = c$, hence Q represents c.

ii) If $Q\colon V \to k$ is a quadratic form of rank $n \geqslant 3$ we can write $Q \cong \langle a, b, -c\rangle \perp Q'$ for some $a, b, c \in k^\times$ and some quadratic form $Q'\colon k^{n-3} \to k$. By the above argument we can find $x, y \in k^\times$ with $ax^2 + by^2 = c$. Thus $\langle a, b, -c\rangle(x, y, 1)$ is isotropic and by Cor. 2.23 universal. Hence $Q \cong \langle a, b, -c\rangle \perp Q'$ is universal, too. □

Corollary 3.2. *Every nondegenerate quadratic form Q of rank $n > 0$ over a finite field k is isometric to one of the form $\langle 1, \ldots, 1, d\rangle$ on k^n, where $d = \operatorname{disc}(Q) \in k^\times/(k^\times)^2$.*

Proof. We prove the statement per induction over n. For $n = 1$ there is nothing to show. Now let $n > 1$. By the previous lemma Q represents 1 and therefore by Cor. 2.24 it is isometric to $\langle 1\rangle \perp Q'$ for some nondegenerate form Q' of rank $n - 1$ and $\operatorname{disc}(Q') = \operatorname{disc}(Q)$. The claim follows directly from the induction hypothesis. □

At this point we want to make a generalization of the content of Section 2 and define a quadratic form not only over a field but also over the ring of the p-adic integers $\mathbb{Z}_p$. We give here only the basic results which we want to apply to our discussion of quaternion algebras and refer the reader to Ch. 1, §6 of [Sch85] or Ch. I and V of [Kne02] for a more detailed discussion of quadratic form over rings.

Definition 3.3. Given a free $\mathbb{Z}_p$-module M we define a *quadratic form* on M as a map $Q\colon M \to \mathbb{Z}_p$ with

i) $\forall \lambda \in \mathbb{Z}_p\ \forall x \in M\colon Q(\lambda x) = \lambda^2 Q(x)$, and

ii) the map $T\colon M \times M \to \mathbb{Z}_p,\ (x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is $\mathbb{Z}_p$-bilinear.

The pair (M, Q) is called *quadratic module* and T the *symmetric bilinear form associated to Q*. If $p \neq 2$, then $2 \in \mathbb{Z}_p^\times$ and as in section 2 we can uniquely determine Q by knowing T, as in Rem. 2.2.

Let us assume that M is free of finite rank n. Since M is free we can carry over many concepts from the theory of quadratic forms over fields from Section 2, such as similarity, isometry and orthogonality, defining them in the same way over $\mathbb{Z}_p$. Nondegeneracy is defined in a similar way as over a field.

Definition 3.4. Denote by $M^* \coloneqq \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ the dual module of M. A quadratic form $Q\colon M \to \mathbb{Z}_p$ is called *nondegenerate* if the homomorphism $M \to M^*,\ x \mapsto (T_x\colon y \mapsto T(x,y))$ is an *isomorphism* (and not only injective as in Def. 2.14). Otherwise Q is called *degenerate.*

In the case $p \neq 2$ (since we need 2 to be a unit) we can represent the quadratic form via its Gram matrix, as done with quadratic forms over fields in section 2. Moreover we can diagonalize the quadratic form, as shown in the next proposition.

Proposition 3.5. *For $p \neq 2$ any nondegenerate quadratic module (M, Q) over $\mathbb{Z}_p$ possesses an orthogonal basis.*

Proof. We follow the proof of Thm. 6.4 from Ch. 1 of [Sch85]. We first prove that there exists $v \in M$ with $Q(v) \in \mathbb{Z}_p^\times$. Fix a basis $B \coloneqq (b_i)_{1\leqslant i\leqslant n}$ of M. Since Q is nondegenerate, the determinant of the Gram matrix $M_B(T)$ lies in $\mathbb{Z}_p^\times$. In particular, expanding along the first row we get $\det(M_B(T)) = \sum_{i=1}^n d_i T(b_1, b_i) \in \mathbb{Z}_p^\times$ with $d_i \in \mathbb{Z}_p$, hence there must exist a $1 \leqslant j \leqslant n$ with $T(b_1, b_j) \in \mathbb{Z}_p^\times$. Since $T(b_1, b_j) = Q(b_1 + b_j) - Q(b_1) - Q(b_j)$, one of $Q(b_1 + b_j)$, $Q(b_1)$ and $Q(b_j)$ must be a unit. Set v equal to $b_1 + b_j$, b_1 or b_j, accordingly and consider the decomposition

$$x = \frac{T(v,x)}{T(v,v)} v + \left(x - \frac{T(v,x)}{T(v,v)} v \right),$$

which is well-defined since $T(v,v) = 2Q(v) \in \mathbb{Z}_p^\times$. The proof is concluded in the same way as the proofs of Prop. 2.17 and 2.18. □

An important theorem of the theory of the p-adic integers is Hensel's lemma. Its inductive proof can be seen as an analog of Newton's method for finding roots of a polynomial over the p-adics.

Theorem 3.6 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[X_1, \dots X_m]$ and let $\frac{\partial f}{\partial X_i}$ be the formal partial derivative of f with respect to X_i, for every $1 \leqslant i \leqslant n$. Suppose that there exist integers j, k and n with $1 \leqslant j \leqslant n$ and $0 \leqslant 2k < n$, as well as $x = (x_i)_{1\leqslant i\leqslant m} \in \mathbb{Z}_p^m$ with*

$$f(x) \equiv 0 \pmod{p^n} \text{ and } v_p\left(\frac{\partial f}{\partial X_j}(x) \right) = k.$$

Then there exists a root y of f in $\mathbb{Z}_p^m$ with $y \equiv x \pmod{p^{n-k}}$.

Proof. For this proof we refer the reader to Ch. II, Thm. 1 of [Ser73]. □

Corollary 3.7. *Let $p \neq 2$ and let $x, z \in \mathbb{Z}_p$ with $p \nmid x$ and $z \equiv x^2 \pmod{p}$. Then z is a square in $\mathbb{Z}_p$.*

Proof. Let $f \coloneqq X^2 - z$. We have $f(x) \equiv 0 \pmod{p}$ and $v_p\big(f'(x)\big) = v_p(2x) = 0$. Applying Hensel's lemma we get a root $y \in \mathbb{Z}_p$ of f, which is a square root of z. □

Corollary 3.8. *Let $x \in \mathbb{Q}_2^\times$ and write $x = u2^n$ for unique $u \in \mathbb{Z}_2^\times$ and $n \geqslant 0$. Then $x \in (\mathbb{Q}_2^\times)^2$ if and only if n is even and $u \equiv 1 \pmod 8$.*

Proof. We follow the proof from Satz. 2.36 from [Jer17]. If x is a square, say $x = y^2$ for some $y \in \mathbb{Q}_2^\times$, then $n = v_2(x) = v_2(y^2) = 2v_2(y)$, hence n is even. Write $y = v2^{\frac{n}{2}}$ with uniquely determined $v \in \mathbb{Z}_2^\times$. By assumption we have $u = v^2$. Since $2 \nmid u$ and $2 \nmid v$ we can write $u = 2s+1$ and $v = 2t+1$ with $s, t \in \mathbb{Z}_2$. Then we have $2s+1 = (2t+1)^2 = 4t^2+2t+1$, hence $s = 2t(t+1)$. Since either $2 \mid t$ or $2 \mid (t+1)$ we get $4 \mid s$, thus $u \equiv 1 \pmod 8$.

Conversely, assume that n is even and $u \equiv 1 \pmod 8$. Let $f \coloneqq X^2 - u \in \mathbb{Z}_2[X]$. We have $f(3) \equiv 0 \pmod{2^3}$ and $v_2\big(f'(3)\big) = 1$. By Hensel's Lemma there exists an element $v \in \mathbb{Z}_2$ with $v^2 = u$. Thus $x = (v2^{\frac{n}{2}})^2$ is a square. □

Let $Q\colon M \to \mathbb{Z}_p$ be a quadratic form on a free $\mathbb{Z}_p$-module M. Consider the reduction $\bar{\cdot}\colon \mathbb{Z}_p \to \mathbb{F}_p$. This yields a well-defined reduction map $\bar{\cdot}\colon M \to \overline{M} \coloneqq M/pM$. Furthermore $\overline{M}$ is in a natural way an $\mathbb{F}_p$-vector space. Let y and y' in M with $\overline{y} = \overline{y}'$, i.e. there exists an element $z \in M$ with $y' = y + pz$. Then we have:

$$\overline{Q(y')} = \overline{Q(y+pz)} = \overline{T(y,pz)} + \overline{Q(y)} + \overline{Q(pz)} = \overline{p}\ \overline{T(y,z)} + \overline{Q(y)} + \overline{p}^2\ \overline{Q(z)} = \overline{Q(y)}.$$

Definition 3.9. The *reduction of Q modulo p* is the quadratic form

$$\overline{Q} \coloneqq Q \pmod p\colon \overline{M} \to \mathbb{F}_p, \quad x \mapsto \overline{Q}(x) \coloneqq \overline{Q(y)},$$

where $y \in M$ is an arbitrary element satisfying $\overline{y} = x$. By the above computation this is well-defined.

Having defined the reduction of a quadratic form we can prove another corollary of Hensel's lemma.

Corollary 3.10. *Let $p \neq 2$ and $Q\colon M \to \mathbb{Z}_p$ be a quadratic form over $\mathbb{Z}_p$.*

i) Q is nondegenerate if and only the reduction $\overline{Q}$ is.

ii) If Q is nondegenerate, then Q is isotropic if and only if $\overline{Q}$ is.

Proof. Let m be the rank of M. By Prop. 3.5 we can restrict ourselves to the case $M = \mathbb{Z}_p^m$ and $Q = \langle a_1, \dots, a_m \rangle$ for some $a_i \in \mathbb{Z}_p$.

i) We have:
$$\begin{aligned} Q \text{ is nondegenerate} &\iff a_1 \cdots a_m \in \mathbb{Z}_p^\times \\ &\iff \forall 1 \leqslant i \leqslant m\colon a_i \in \mathbb{Z}_p^\times \\ &\iff \forall 1 \leqslant i \leqslant m\colon \overline{a}_i \neq \overline{0} \\ &\iff \overline{Q} = \langle \overline{a}_1, \dots, \overline{a}_m \rangle \text{ is nondegenerate.} \end{aligned}$$

ii) Note that showing that Q is isotropic is equivalent to finding a nontrivial zero of the polynomial $f = \sum_{i=1}^m a_i X_i^2$. Similarly, showing that $\overline{Q}$ is isotropic is equivalent to finding a nontrivial zero in $(\mathbb{F}_p)^m$ of the reduced polynomial $\overline{f}$.

Assume that Q is isotropic. Then there exists $x = (x_i)_{1 \leqslant i \leqslant m} \in \mathbb{Z}_p^m$ with $f(x) = 0$. Multiplying x by $\max_{1 \leqslant i \leqslant m} |x_i|_p$ we can assume that $\overline{x} \neq 0$. So we have found a notrivial zero of $\overline{f}$, namely $\overline{x}$, hence $\overline{Q}$ is isotropic.

Conversely, assume that there exists $0 \neq \overline{x} = (\overline{x}_i)_{1 \leqslant i \leqslant m} \in (\mathbb{F}_p)^m$ with $\overline{f}(\overline{x}) = 0$. We can lift $\overline{x}$ to an element $x = (x_i)_{1 \leqslant i \leqslant m}$ of $\mathbb{Z}_p^m$ satisfying $f(x) \equiv 0 \pmod{p}$. Since $\overline{x} \neq 0$ there exists $1 \leqslant j \leqslant m$ with $p \nmid x_j$. Since $\overline{Q}$ is nondegenerate we have $\forall\ 1 \leqslant i \leqslant m \colon p \nmid a_i$. Then

$$v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = v_p(2a_j x_j) = 0,$$

and applying Hensel's lemma we find $y \in (\mathbb{Z}_p)^m$ with $f(y) = 0$, satisfying $y \equiv x \pmod{p}$. In particular $y \neq 0$ and thus Q is isotropic. □

Proposition 3.11. *Let $p \neq 2$. Two nondegenerate quadratic forms $Q \colon M \to \mathbb{Z}_p$ and $Q' \colon M' \to \mathbb{Z}_p$ over $\mathbb{Z}_p$ are isometric if and only if they reductions modulo p are.*

Proof. Assume that Q and Q' are isometric. Then there exists an isomorphism $f \colon M \to M'$ satisfying $\forall x \in M \colon Q'(f(x)) = Q(x)$. The isomorphism f reduces to an isomorphism $\overline{f} \colon \overline{M} \to \overline{M'}$, which satisfies

$$\forall x \in \overline{M} \colon \overline{Q'}\big(\overline{f}(x)\big) = \overline{Q'}\big(\overline{f(y)}\big) = \overline{Q'(f(y))} = \overline{Q(y)} = \overline{Q}(\overline{y}) = \overline{Q}(x),$$

where $y \in M$ is an arbitrary element with $\overline{y} = x$.

Conversely, assume that $\overline{Q}$ and $\overline{Q'}$ are isometric. Choose bases B of M and B' of M'. We denote the respective Gram matrices by C and C'. By isometry modulo p there exists a matrix $U \in \mathrm{GL}_n(\mathbb{Z}_p)$ with $U^T C' U \equiv C \pmod{p}$.

Claim. There exists a sequence of matrices $(U_k)_{k \geqslant 1}$ in $\mathrm{GL}_n(\mathbb{Z}_p)$ satisfying:

i) $U_k^T C' U_k \equiv C \pmod{p^{2^{k-1}}}$, and

ii) $U_{k+1} \equiv U_k \pmod{p^{2^{k-1}}}$.

Proof of Claim. We set $U_1 \coloneqq U$, which by definition satisfies i). Assume that U_k is constructed for some $k \geqslant 1$ and set $r \coloneqq 2^{k-1}$. By i) there exists a matrix $B \in \mathrm{Mat}_{n \times n}$ with $U_k^T C' U_k - C = p^r B$. Since C and C' are symmetric, B is symmetric as well. We set $U_{k+1} \coloneqq U_k + p^r A$ for some matrix $A \in \mathrm{Mat}_{n \times n}(\mathbb{Z}_p)$. This matrix satisfies ii). Computing and using the symmetry of C' we obtain:

$$\begin{aligned} U_{k+1}^T C' U_{k+1} - C &= (U_k + p^r A)^T C' (U_k + p^r A) - C \\ &= U_k^T C' U_k - C + U_k^T C' p^r A + p^r A^T C' U_k + p^{2r} A^2 \\ &= p^r (B + (U_k^T C' A) + (U_k^T C' A)^T) + p^{2r} A^2. \end{aligned}$$

Setting $A \coloneqq -\frac{1}{2}(U_k^T C')^{-1} B$ we get $U_{k+1}^T C' U_{k+1} - C \equiv 0 \pmod{p^{2r}}$, which proves i). ■

By ii) and completeness of $\mathbb{Z}_p$ the sequence $(U_k)_{k \geqslant 1}$ converges to a matrix $\hat{U} \in \mathrm{Mat}_{n \times n}(\mathbb{Z}_p)$. Furthermore, from ii) and $\det(U_1) \in \mathbb{Z}_p^\times$ it follows that for all $k \geqslant 1 \colon \det(U_k) \in \mathbb{Z}_p^\times$, hence $\hat{U} \in \mathrm{GL}_n(\mathbb{Z}_p)$. Finally from i) it follows that $\hat{U}^T C' \hat{U} = C$, thus Q and Q' are isometric. □

Proposition 3.12. *Let $p \neq 2$. Then the quotient group $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ has order 4 and is represented by the classes of $1, e, p$ and ep, where $e \in \mathbb{Z}_p^\times$ is any element which reduces to a nonsquare modulo p.*

Proof. Any element $x \in \mathbb{Q}_p^\times$ can be written uniquely as $x = up^{2k+l}$ with integers $k \in \mathbb{Z}$ and $l \in \{0,1\}$ and $u \in \mathbb{Z}_p^\times$. Then clearly $x \equiv up^l \pmod{(\mathbb{Q}_p^\times)^2}$. Fix an element $e \in \mathbb{Z}_p^\times \smallsetminus (\mathbb{Z}_p^\times)^2$. We want to show that u is congruent to either 1 or $e \pmod{(\mathbb{Q}_p^\times)^2}$.

Once more we denote by $\bar{\cdot}$ the reduction $\mathbb{Z}_p \to \mathbb{F}_p$. Since $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$ we can write $\mathbb{F}_p^\times$ as a disjoint union of $(\mathbb{F}_p^\times)^2$ and $\overline{e}(\mathbb{F}_p^\times)^2$. Thus $\overline{u}(\mathbb{F}_p^\times)^2 = \overline{e}^\varepsilon(\mathbb{F}_p^\times)^2$ for some $\varepsilon \in \{0,1\}$. That is, there exists $y \in \mathbb{Z}_p^\times$ such that $\overline{u} = \overline{e}^\varepsilon \overline{y}^2$, or in other words $u \equiv e^\varepsilon y^2 \pmod{p}$. So $ue^{-\varepsilon} \equiv y^2 \pmod{p}$ and by Cor. 3.7 $ue^{-\varepsilon}$ is a square in $\mathbb{Z}_p$. Thus u is congruent to $e^\varepsilon \pmod{(\mathbb{Q}_p^\times)^2}$. □

Proposition 3.13. *For every p, including $p = \infty$, there exists precisely one anisotropic ternary quadratic form over $\mathbb{Q}_p$, up to similarity.*

Proof. We first prove the proposition for odd p. We show that the form $\langle 1, -e, -p\rangle$ is anisotropic. Suppose that there exist $x, y, z \in \mathbb{Q}_p$ not all equal zero with $x^2 - ey^2 - pz^2 = 0$. Multiplying x, y and z by $\max\{|x|_p, |y|_p, |z|_p\}$ we may assume that they all lie in $\mathbb{Z}_p$ and of least one of them lies in $\mathbb{Z}_p^\times$. Reducing modulo p we obtain $x^2 \equiv ey^2 \pmod{p}$. If $p \nmid y$, then $y \in \mathbb{Z}_p^\times$ and $e \equiv (\frac{x}{y})^2 \pmod{p}$ which is a contradiction to the definition of e. So $p \mid y$, which implies $p \mid x$ and $z \in \mathbb{Z}_p^\times$. Then we have $1 = v_p(pz^2) = v_p(x^2 - ey^2) \geqslant 2$, which is a contradiction. Thus $\langle 1, -e, -p\rangle$ is anisotropic.

To show the uniqueness let Q be an anisotropic (hence nondegenerate) ternary quadratic form over $\mathbb{Q}_p$ and choose a', b', c' such that $Q \cong \langle a', -b', -c'\rangle$. By Rem. 2.11 multiplying a', b' and c' by even powers of p doesn't affect the isometry, so we can assume that $v_p(a'), v_p(b'), v_p(c') \in \{0,1\}$.

Claim. There exist $b, c \in \mathbb{Z}_p^\times$ with $v_p(b) = 0$ and $v_p(c) = 1$ such that $Q \cong \langle a', -b', -c'\rangle \sim \langle 1, -b, -c\rangle$

Proof of Claim.

- If $v_p(a') = v_p(b') = v_p(c')$, we set $b \coloneqq \frac{b'}{a'}$ and $c \coloneqq \frac{c'}{a'}$.
- If two of the valuations are equal 0 and the other one is equal 1 by permuting we can assume that $v_p(a') = v_p(b') = 0$ and $v_p(c') = 1$. Then set $b \coloneqq \frac{b'}{a'}$ and $c \coloneqq \frac{c'}{a'}$.
- If one of the valuations is equal 0 and the other two are equal 1 by permuting we can assume that $v_p(a') = v_p(b') = 1$ and $v_p(c') = 0$. Then set $b \coloneqq \frac{b'}{a'}$ and $c \coloneqq \frac{c'p^2}{a'}$.

In all three cases we get $\langle a', -b', -c'\rangle \sim \langle 1, -b, -c\rangle$ with $v_p(b) = 0$ and $v_p(c) \in \{0,1\}$.

We consider the form $\langle 1, -b, -c\rangle$ as quadratic form $\mathbb{Z}_p^3 \to \mathbb{Z}_p$. If $v_p(c) = 0$ then the form $\langle 1, -b, -c\rangle \pmod{p}\colon \overline{\mathbb{Z}_p^3} \to \mathbb{F}_p$ is nondegenerate. By Prop. 3.1 it is isotropic, and by Cor. 3.10 $\langle 1, -b, -c\rangle$ (and hence Q) is isotropic too, which is a contradiction. So $v_p(c) = 1$. ■

By Prop. 3.12 we can reduce the discussion to the case $b \in \{1, e\}$ and $c \in \{p, ep\}$. If $b = 1$ the form $\langle 1, -b, -c\rangle$ contains a hyperbolic plane and therefore it is isotropic, which is a contradiction. So $b = e$. Since by Rem. 2.11, Cor. 3.2 and Prop. 3.11

$$\langle 1, -e, -ep\rangle \sim \langle e, -e^2, -e^2p\rangle \cong \langle e, -1, -p\rangle \cong \langle 1, -e, -p\rangle,$$

we can assume that $c = p$, and hence we have shown that Q is similar to the form $\langle 1, -e, -p\rangle$.

In the case $p = 2$ one possibility is to argue in a similar fashion as for odd p with the form $\langle 1, -5, -2\rangle$. We refer the reader for this proof to Prop. 1.6 of [Che10]. Alternatively one can use the Hilbert symbol, which we will introduce in section 4, to prove that this form is anisotropic and then show that every anisotropic ternary form over $\mathbb{Q}_2$ is similar to $\langle 1, -5, -2\rangle$. Since $[\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2] = 8$ (see Lemma 3.6 of [Jer17]) this is in fact a finite problem.

Another possibility is to work with the quadratic form given by the polynomial $X^2 + XY + Y^2 + 2Z^2 \in \mathbb{Q}_2[X, Y, Z]$. However this would require some results from the theory of quadratic forms over fields of characteristic 2, since in the proof we need to reduce the form modulo 2, getting a form over $\mathbb{F}_2$. These results were not treated in this thesis, but an overview of the theory can be found in Ch. 6 of [Voi17] or in Sect. 7 of [EKM08]. The proof of the proposition for the form given by $X^2 + XY + Y^2 + 2Z^2$ can be found in Prop. 12.4.2 of [Voi17].

Finally we consider the case $p = \infty$. The form $\langle 1, 1, 1\rangle$ is clearly anisotropic over $\mathbb{R}$. Now let Q be a ternary anisotropic quadratic form over $\mathbb{R}$ and chose $a, b, c \in \mathbb{R}$ with $Q \cong \langle a, b, c\rangle$. Since $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{1, -1\}$ we can assume that $a, b, c \in \{1, -1\}$. Since Q is anisotropic we have $a = b = c$, thus in either case Q is similar to $\langle 1, 1, 1\rangle$. □

Theorem 3.14. *For any p prime number or $p = \infty$ there is a unique division quaternion algebra over $\mathbb{Q}_p$, up to isomorphy.*

i) For prime p it is given by $\left(\frac{e,p}{\mathbb{Q}_p}\right)$, where $e \in \mathbb{Z}_p^\times$ is an arbitrary element that reduces to a nonsquare modulo p.

ii) For $p = 2$ it is given by $\left(\frac{5,2}{\mathbb{Q}_2}\right)$.

iii) For $p = \infty$ it is given by the Hamilton quaternions $\mathbb{H} = \left(\frac{1,1}{\mathbb{R}}\right)$.

Proof. The statement follows directly from Prop. 3.13, Thm. 2.30 and from the equivalence "ii) $\iff$ iv)" of Thm. 2.33. □

4 Quaternion algebras over $\mathbb{Q}$

The goal of this section—and of this thesis—is to classify the rational quaternion algebras up to isomorphism. We need to use some tools from number theory, such as the Legendre symbol, the Hilbert norm residue symbol and the theorems connected with them, Dirichlet's theorem on arithmetic progressions, the Hasse-Minkowski theorem about rational quadratic forms, as well as the main result of the previous section.

Definition 4.1. Given an odd prime p and an integer $a \in \mathbb{Z}$ we define the *Legendre symbol* as

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is congruent to a square } (\mathrm{mod}\, p), \\ 0 & \text{if } p \mid a, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not congruent to a square } (\mathrm{mod}\, p). \end{cases}$$

If $\left(\frac{a}{p}\right) = 1$ we call a a *quadratic residue modulo* p and if $\left(\frac{a}{p}\right) = -1$ we call a a *quadratic nonresidue modulo* p. Clearly if a and b are congruent modulo p, their Legendre symbols will be equal, so we can see the Legendre symbol as a map $\mathbb{F}_p \to \{-1, 0, 1\}$. Since $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ we can extend the Legendre symbol to all p-adic integers $\mathbb{Z}_p$, defining the Legendre symbol of $a \in \mathbb{Z}_p$ via its congruence class modulo p.

Proposition 4.2. *The Legendre symbol is multiplicative, i.e.*

$$\forall p \text{ odd prime},\ \forall a, b \in \mathbb{Z}_p \colon \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. We consider several cases:

- If p divides a or b, then it divides ab as well and the statement follows.
- If both a and b are quadratic residues modulo p, say $a \equiv x^2 \ (\mathrm{mod}\, p)$ and $b \equiv y^2 \ (\mathrm{mod}\, p)$, then $ab \equiv (xy)^2 \ (\mathrm{mod}\, p)$ and therefore it is a quadratic residue as well. So the product of two quadratic residues is again a quadratic residue.
- Conversely assume that both a and ab are quadratic residues, say $a \equiv x^2 \ (\mathrm{mod}\, p)$ and $ab \equiv z^2 \ (\mathrm{mod}\, p)$. Then $b \equiv \left(\frac{z}{x}\right)^2 \ (\mathrm{mod}\, p)$ a quadratic residue. This proves indirectly that the product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.
- Finally we claim that the product of two quadratic nonresidues is a quadratic residue. We argue directly over the finite field $\mathbb{F}_p$. Let $a \in \mathbb{F}_p$ be a nonsquare and consider the unit group
$$\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\} = \{a, 2a, \ldots, (p-1)a\}.$$
By the previous case we know that the product of a and a square is a nonsquare and since p is odd we know that there are exactly $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$. Hence, cardinality being the reason for it, the product of a and any of $\frac{p-1}{2}$ nonsquares is a square, and since a is an arbitrary nonsquare we are done. □

From now on let P be the set $\{p \in \mathbb{Z}^{>0} \mid p \text{ is prime}\} \cup \{\infty\}$.

Definition 4.3. Given $p \in P$ and two elements $a, b \in \mathbb{Q}_p^\times$ we define the *Hilbert norm residue symbol* as

$$(a,b)_p \coloneqq \begin{cases} 1 & \text{if } Z^2 - aX^2 - bY^2 = 0 \text{ possesses a nontrivial solution } (z,x,y) \in \mathbb{Q}_p^3, \\ -1 & \text{otherwise.} \end{cases}$$

Proposition 4.4. *For any $p \in P$ and any $a, b \in \mathbb{Q}_p^\times$ the following are equivalent:*

i) $(a,b)_p = 1$.

ii) The binary form $\langle a, b\rangle$ over $\mathbb{Q}_p$ represents 1.

iii) The quaternion algebra $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is isomorphic to the matrix algebra $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$.

Proof. The equivalence "i) $\iff$ iii)" follows from Cor. 2.24:

$$\begin{aligned} (a,b)_p = 1 &\iff \text{The form } \langle 1, -a, -b\rangle \text{ is isotropic.} \\ &\iff \text{The form } \langle -1, a, b\rangle \cong \langle a, b\rangle \perp \langle -1\rangle \text{ is isotropic.} \\ &\iff \langle a, b\rangle \text{ represents 1.} \end{aligned}$$

The equivalence "ii) $\iff$ iii)" was already stated and proven for an arbitrary field F of characteristic $\neq 2$ in Thm. 2.33. □

Proposition 4.5. *For any $p \in P$ the Hilbert symbol defines a symmetric, bimultiplicative mapping on the equivalence classes modulo $(\mathbb{Q}_p^\times)^2$, i.e. for any $a, b, c \in \mathbb{Q}_p^\times$ we have the following:*

i) $(a,b)_p = (b,a)_p$.

ii) $(a, bc^2)_p = (a,b)_p$.

iii) $(a,bc)_p = (a,b)_p (a,c)_p$.

Using these relations to determine all the values of the Hilbert symbol it suffices to explicitly give only the following values:

iv) In the case $p = \infty$ the values are given by

$$(1,1)_p = (1,-1)_p = (-1,1)_p = 1 \text{ and } (-1,-1)_p = -1.$$

v) For an odd prime p and any p-adic units $u, v \in \mathbb{Z}_p^\times$ we have

$$(p,p)_p = (-1)^{\frac{p-1}{2}}, \quad (p,u)_p = \left(\frac{u}{p}\right), \quad (u,v)_p = 1.$$

vi) For $p = 2$ and any 2-adic units $u, v \in \mathbb{Z}_2^\times$ we have

$$(2,2)_p = 1, \quad (2,u)_p = (-1)^{\frac{u^2-1}{8}}, \quad (u,v)_p = (-1)^{\frac{u-1}{2}\frac{v-1}{2}},$$

where for any $a \in \mathbb{Z}_2$ we define $(-1)^a$ as $(-1)^{a \pmod 2}$.

Proof. We will only give a sketch of the proof of this proposition, referring the reader to Prop. 3.5 and Satz 3.8 of [Jer17] or to Satz 9.6.2, Satz 9.6.3 and Lemma 9.6.5 of [Sch07] for a complete proof.

The statements i) and ii) follow immediately from the definition of the Hilbert symbol. To show the multiplicativity there are various ways, but the most direct one is to compute all the values of the Hilbert symbol. In the case the case $p = \infty$ there are 4 values to compute, in the case that p is an odd prime there are $4^2 = 16$ values to compute (as seen in Prop. 3.12 the factor group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ consists of 4 elements) and in the case $p = 2$ there are $8^2 = 64$ to compute (since the factor group $\mathbb{Q}_2^\times/(\mathbb{Q}_p^\times)^2$ consists of 8 elements, see Lemma 3.6 in [Jer17]). Using the symmetry of the Hilbert symbol one actually has to compute only the half of those values.

After having computed all the values of the Hilbert symbol and having set up the table for all the values the (bi)multiplicativity and the values in iv), v) and vi) follow.

In the case $p = \infty$ it is clear that the values from iv) are sufficient to compute all other values, since a nonzero real number is either a square or the product of -1 with a square.

Given $p \neq \infty$, and $a, b \in \mathbb{Q}_p^\times$ we can write $a = up^m$ and $b = vp^m$ for unique $m, n \in \mathbb{Z}$ and $u, v \in \mathbb{Z}_p^\times$. Since by i) we can rescale a and b by squares, we can assume that $m, n \in \{0, 1\}$. By multiplicativity we have

$$(pu, v) = (p, v)(u, v) \text{ and } (pu, pv) = (p, p)(u, p)(p, v)(u, v),$$

hence the values computed in v) and vi) are sufficient to compute all the values of the Hilbert symbol over $\mathbb{Q}_p$. □

Corollary 4.6. *Let $a, b \in \mathbb{Q}$. Then for all but possibly finitely many $p \in P$ we have $(a, b)_p = 1$.*

Proof. Since we can multiply both a and b by squares, we can assume that $a, b \in \mathbb{Z}$. We know that for all primes p that do not divide $2ab$ we have $(a, b)_p = 1$. Since ab (and hence $2ab$) has only finitely many prime factors we can conclude. □

Proposition 4.7 (Law of quadratic reciprocity)**.**

i) Given two disctinct odd primes p and q we have: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

ii) (First supplement) For any odd prime p we have: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

iii) (Second supplement) For any odd prime p we have: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Proof. There are many different ways to prove this classical proposition from number theory. We refer the reader to the one found in Ch. I, Thm. 4 and 5 of [Ser73]. □

Proposition 4.8 (Law of Hilbert reciprocity)**.** *For any $a, b \in \mathbb{Q}^\times$ we have*

$$\prod_{p \in P}{}' (a, b)_p = 1.$$

Proof. We want to use the the law of quadratic reciprocity to prove Hilbert's reciprocity law. The two laws are actually equivalent, and the proof of the law of quadratic reciprocity follows very easily from Hilbert reciprocity using Prop. 4.5 iv), v) and vi).

So we assume the law of quadratic reciprocity. Let $a, b \in \mathbb{Q}^\times$. Multiplying a and b by squares without loss of generality we can assume that a and b lie in $\mathbb{Z}$. The product $\prod'_{p\in P}(a,b)_p$ is well-defined since all but possibly finitely many factors are equal 1, by Cor. 4.6.

Writing $a = q_0 \cdots q_m$ and $b = r_0 \cdots r_n$ with $q_0, r_0 \in \{+1, -1\}$, primes q_i and r_i for $i \geqslant 1$ and using the bimultiplicativity of the Hilbert symbol we obtain

$$\prod_{p\in P}{}'(a,b)_p = \prod_{i=0}^{m}\prod_{j=0}^{n}\prod_{p\in P}{}'(q_i, r_j)_p,$$

so it suffices to prove the proposition only for the case that a and b are primes or -1 (since if a or b is equal 1, then all the Hilbert symbols are equal 1, too). By symmetry we can restrict ourselves to the following 7 different cases:

- $a = b = -1$,
- $a = -1,\ b = q$ for an odd prime q,
- $a = -1,\ b = 2$,
- $a = 2,\ b = q$ for an odd prime q.
- $a = b = 2$
- $a = b = q$ for an odd prime q, and
- $a = q,\ b = r$ for distinct odd primes q and r.

We show only the last case, the one where the law of quadratic reciprocity is required. All other cases follow in an analogous way directly from Prop. 4.5. If q and r are distinct odd primes we have:

$$(q,r)_p = \begin{cases} 1 & \text{if } p \neq 2, q, r \\ \left(\frac{r}{q}\right) & \text{if } p = q \\ \left(\frac{q}{r}\right) & \text{if } p = r \\ (-1)^{\frac{q-1}{2}\frac{r-1}{2}} & \text{if } p = 2 \end{cases}.$$

Then $\prod'_{p\in P}(q,r)_p = 1$ follows directly from the law of quadratic reciprocity. □

Theorem 4.9 (Dirichlet's theorem on arithmetic progressions)**.** *Given $a, n \in \mathbb{Z}$ coprime with $n \neq 0$ there are infinitely many primes p with $p \equiv a \pmod{n}$.*

Proof. For its long proof, which would lead us too far away from the goal of this bachelor's thesis, we refer the reader to Ch. VI of [Ser73]. □

Dirichlet's theorem is needed as an intermediate step in the proof of the Hasse-Minkowski theorem, which we will state below, as well as in the proof of our main theorem, as we will see.

Let V be a finitely dimensional $\mathbb{Q}$-vector space, $n := \dim_{\mathbb{Q}}(V)$, and $p \in P$. Consider the scalar extension $V_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} V$. This is in a natural way an n-dimensional $\mathbb{Q}_p$-vector space. Every basis $B := (b_i)_{1\leqslant i\leqslant n}$ of V over $\mathbb{Q}$ yields a basis $B_p := (b_{p,i})_{1\leqslant i\leqslant n} := (1 \otimes b_i)_{1\leqslant i\leqslant n}$ of V_p over $\mathbb{Q}_p$.

Definition 4.10. For V, n, p, B and B' as above consider a quadratic form $Q\colon V \to \mathbb{Q}$ and the polynomial representation $f_{Q,B} \in \mathbb{Q}[X_1, \ldots, X_n] \subset \mathbb{Q}_p[X_1, \ldots, X_n]$ of Q in the basis B (see Def. 2.4). We define the *extension of Q on V_p* as the unique quadratic form $Q_p\colon V_p \to \mathbb{Q}_p$ satisfying $f_{Q_p,B_p} = f_{Q,B}$. This is well-defined by Rem. 2.6.

Theorem 4.11 (Hasse-Minkowski)**.** *Let Q be a rational quadratic form. Then Q is isotropic if and only if the extensions Q_p are isotropic for every $p \in P$.*

Proof. This theorem is the main goal of [Jer17]; we therefore refer the reader to its proof in this thesis (see Satz 5.1). □

Corollary 4.12. *Let Q and Q' be two rational nondegenerate quadratic forms of the same rank. Then they are isometric if and only for every $p \in P$ their extensions Q_p and Q'_p are.*

Proof. If Q and Q' are isometric we can extend the isometry over $\mathbb{Q}$ to an isometry over $\mathbb{Q}_p$ and so Q_p and Q'_p are isometric for every $p \in P$, which proves one direction. We prove the converse by induction on $n \coloneqq \operatorname{rank}(Q) = \operatorname{rank}(Q')$. If $n = 0$, there is nothing to show, so assume $n \geqslant 1$.

Assume that the extensions Q_p and Q'_p are isometric for every $p \in P$. Since Q is nonzero we can choose an element $a \in \mathbb{Q}^\times$ represented by Q. Then a is represented by Q_p for all p and by isometry also by Q'_p for all p. From Cor. 2.24 it follows that for every p the form $\langle -a\rangle \perp Q'_p \cong \big(\langle -a\rangle \perp Q'\big)_p$ is isotropic. Applying the Hasse-Minkowski theorem and Cor. 2.24 we get that Q' represents a.

Applying one last time Cor. 2.24 we can write $Q \cong \langle a\rangle \perp \hat{Q}$ and $Q' \cong \langle a\rangle \perp \hat{Q}'$ for some forms $\hat{Q}$ and $\hat{Q}'$ of rank $n-1$. By assumption the forms

$$Q_p \cong \big(\langle a\rangle \perp \hat{Q}\big)_p \cong \langle a\rangle \perp \hat{Q}_p \text{ and } Q'_p \cong \big(\langle a\rangle \perp \hat{Q}'\big)_p \cong \langle a\rangle \perp \hat{Q}'_p$$

are isometric, and from Witt's theorem (Thm. 2.28) it follows that $\hat{Q}_p$ and $\hat{Q}'_p$ are isometric. By the induction hypothesis $\hat{Q}$ and $\hat{Q}'$ are isometric, which implies that Q and Q' are isometric, concluding the proof. □

We are now ready to state and prove our main theorem. Let $A = (\frac{a,b}{\mathbb{Q}})$ be a rational quaternion algebra. For all $p \in P$ we consider the scalar extension

$$A \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \Big(\frac{a, b}{\mathbb{Q}_p}\Big).$$

As seen in the previous section for each p there are only two possibilities, up to isomorphy, for the quaternion algebra $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$, namely $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ or a uniquely determined division algebra. If the first case occurs we say that A is *split* at p, otherwise we say that A is *nonsplit* or *ramified* at p. We denote the set of all p's at which A ramifies—the so-called *ramification set*—by

$$\operatorname{Ram}(A) \coloneqq \{p \text{ prime or } p = \infty \mid A \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{ is a division algebra}\}.$$

Theorem 4.13. *There is a bijection:*

$$\left\{ \begin{array}{c} \textit{Isomorphy classes of} \\ \textit{quaternion algebras over } \mathbb{Q} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{Finite subsets of } P \\ \textit{of even cardinality} \end{array} \right\} \longleftrightarrow \Big\{ D \in \mathbb{Z}^{\geqslant 1} \textit{ squarefree} \Big\}.$$

The maps are given by

$$f\colon [A] \mapsto \mathrm{Ram}(A) \quad \textit{and} \quad g\colon \Sigma \mapsto \prod_{\substack{p\in\Sigma \\ p\neq\infty}} p$$

respectively.

Proof. The well-definedness and the injectivity of g are immediate. For any squarefree integer $a \geqslant 1$ with prime factorization $a = p_1 \cdots p_n$ for $n \geqslant 0$ and distinct prime numbers p_i we define

$$\Sigma_a \coloneqq \begin{cases} \{p_1, \ldots, p_n\}, & \text{if } n \text{ is even} \\ \{p_1, \ldots, p_n, \infty\}, & \text{if } n \text{ is odd} \end{cases}.$$

Clearly $g(\Sigma_a) = a$, thus g is bijective.

The well-definedness of f follows directly from Cor. 4.6 and Prop. 4.8. We prove the injectivity, which is a consequence of Cor. 4.12. Let A and A' are two quaternion algebras with $\mathrm{Ram}(A) = \mathrm{Ram}(A')$ and denote by nrd and nrd$'$ the reduced norms on A and A', respectively. We observe that for every $p \in P$ the extension of nrd to $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ (which we denote by nrd_p according to Def. 4.10) is equal to the reduced norm on $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$; the same holds for nrd$'$. Using the fact that for every p there is (up to isomorphy) a unique division quaternion algebra over $\mathbb{Q}_p$ (Thm. 3.14), and that two quaternion algebras algebras are isomorphic if and only if they are isometric as quadratic spaces (endowed with the respective reduced norm, Thm. 2.29), as well as the Hasse-Minkowski theorem (Thm. 4.11) we get:

$$\begin{aligned} \mathrm{Ram}(A) = \mathrm{Ram}(A') &\iff \forall p \in P\colon A \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{ is a division algebra if and only if } A' \otimes_{\mathbb{Q}} \mathbb{Q}_p \text{ is} \\ &\iff \forall p \in P\colon A \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong A' \otimes_{\mathbb{Q}} \mathbb{Q}_p \\ &\iff \forall p \in P\colon \mathrm{nrd}_p \cong \mathrm{nrd}'_p \\ &\iff \mathrm{nrd} \cong \mathrm{nrd}' \\ &\iff A \cong A'. \end{aligned}$$

Finally we prove the surjectivity of f. Let $\Sigma \subset P$ be a subset of even cardinality and define

$$D = g(\Sigma) \coloneqq \prod_{\substack{p\in\Sigma \\ p\neq\infty}} p, \quad u \coloneqq \begin{cases} -1, & \text{if } \infty \in \Sigma \\ 1, & \text{if } \infty \notin \Sigma \end{cases}, \quad D^* \coloneqq uD.$$

Claim. There exists a prime q such that $q^* \coloneqq uq$ satisfies the following:

$$\forall p \text{ odd with } p \mid D\colon \left(\frac{q^*}{p}\right) = -1, \quad \text{and} \quad q^* \equiv \begin{cases} 1 \pmod 8, & \text{if } 2 \nmid D \\ 5 \pmod 8, & \text{if } 2 \mid D \end{cases}.$$

Proof of Claim. We prove the case $u = 1$ and $2 \nmid D$, since the other three cases are analogous. Let $p_1, \ldots, p_n$ be the odd prime factors of D and choose integers $a_1, \ldots, a_n$ with $\forall 1 \leqslant i \leqslant n\colon \left(\frac{a_i}{p_i}\right) = -1$. From the Chinese remainder theorem it follows that the system of congruences

$$\begin{cases} r \equiv a_1 \pmod{p_1} \\ \quad \vdots \\ r \equiv a_n \pmod{p_n} \\ r \equiv 1 \pmod 8 \end{cases}$$

has a solution a modulo $8p_1 \cdots p_n$, thus we can write $r \equiv a \pmod{8p_1 \cdots p_n}$. We know that a and $8p_1 \cdots p_n$ are coprime, since if there exists an i with $p_i \mid a$, then $a_i \equiv 0 \pmod{p_i}$, which is a contradiction; and if $2 \mid a$, then $a \not\equiv 1 \pmod 8$, which is a contradiction as well. Using Dirichlet's theorem on arithmetic progressions (Thm. 4.9) we can conclude that there exists a prime q with

$$q \equiv a \equiv r \pmod{8p_1 \cdots p_n}.$$

Thus q satisfies the required congruence relations, which proves the claim. ■

Now we consider the quaternion algebra $A = \left(\frac{D^*, q^*}{\mathbb{Q}}\right)$ and compute the Legendre symbols $(D^*, q^*)_p$ for all $p \in P \setminus \{q\}$ using Prop. 4.5.

- $(D^*, q^*)_\infty = u$,
- $\forall p \nmid 2Dq \colon (D^*, q^*)_p = 1$,
- $\forall p$ odd with $p \mid D \colon (D^*, q^*)_p = \left(\frac{q^*}{p}\right) = -1$, and
- $(D^*, q^*)_2 = \begin{cases} (-1)^{\frac{D^*-1}{2}\frac{q^*-1}{2}} = 1, & \text{if } 2 \nmid D \\ (-1)^{\frac{q^{*2}-1}{8}} \cdot (-1)^{\frac{D^*/2-1}{2}\frac{q^*-1}{2}} = -1, & \text{if } 2 \mid D \end{cases}$.

So we have $\Sigma \subset \operatorname{Ram}(A) \subset \Sigma \cup \{q\}$. The Hilbert reciprocity law Prop. 4.8 implies

$$1 = \prod_{p \in P}{}' (D^*, q^*)_p = (D^*, q^*)_q \prod_{p \in \Sigma \cup \{2, \infty\}} (D^*, q^*)_p.$$

If $2 \notin \Sigma$, then $(D^*, q^*)_2 = 1$, similarly if $\infty \notin \Sigma$, then $(D^*, q^*)_\infty = 1$. Knowing that Σ is of even cardinality and that $\forall p \in \Sigma \colon (D^*, q^*)_p = -1$ we can conclude that the product on the right hand side of the equality is equal to 1. This implies that $(D^*, q^*)_q$ is also equal to 1 and hence $q \notin \operatorname{Ram}(A)$. So $\operatorname{Ram}(A) = \Sigma$ which proves the bijectivity of f. □

Definition 4.14. The integer D^* defined in the proof of Thm. 4.13 is called the *discriminant* of A and denoted by $\operatorname{disc}(A)$.

References

[Cas08] J. W. S. Cassels. *Rational Quadratic Forms*. Dover, 2008.

[Che10] G. Chenevier. *The infinite fern and families of quaternionic modular forms. Lect. 6: Definite quaternion algebras and their modular forms*. 2010. URL: `http://gaetan.chenevier.perso.math.cnrs.fr/coursihp.html`.

[EKM08] R. Elman, N. Karpenko, and A. Merkurjev. *The Algebraic and Geometric Theory of Quadratic Forms*. Vol. 56. Colloquium Publications. American Mathematical Society, 2008.

[Gou97] F. Q. Gouvêa. *p-adic numbers. An introduction*. Springer, 1997.

[Jer17] C. Jergitsch. *Der Satz von Hasse-Minkowski*. BA thesis, ETH Zürich, 2017. URL: `https://people.math.ethz.ch/~pink/Theses/Bachelor.html`.

[Kne02] M. Kneser. *Quadratische Formen*. Springer, 2002.

[Sch07] A. Schmidt. *Einführung in die algebraische Zahlentheorie*. Springer, 2007.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms*. Springer, 1985.

[Ser73] J.-P. Serre. *A Course in Arithmetic*. Springer, 1973.

[Voi17] J. Voight. *Quaternion algebras*. Current draft version v0.9.2, April 18, 2017. URL: `https://math.dartmouth.edu/~jvoight/quat.html`.