Quaternion algebras companion

John Voight
jvoight@gmail.com

v0.9.13
June 10, 2018

Preface

This booklet is a supplement to the book *Quaternion algebras*, containing some additional material (statements and proofs, some remarks) and comments on exercises.

Thanks to Joe Quinn for his comments on some of the exercises. Please contact me at `jvoight@gmail.com` if you find mistakes or have other suggestions.

Contents

Part I

Algebra

Chapter 3

Involutions

3.6 Algorithmic aspects

In this section, we exhibit an algorithm to determine if an algebra has a standard involution (and, if so, to give it explicitly as a linear map) [Voi2013, §2]; in the next section we will use this to recognize quaternion algebras. We begin with some basic definitions.

Definition 3.6.1. A field F is **computable** if F comes equipped with a way of encoding elements of F in bits (i.e. the elements of F are recursively enumerable, allowing repetitions) along with deterministic algorithms to perform field operations in F (addition, subtraction, multiplication, and division by a nonzero element) and to test if $x = 0 \in F$; a field is *polynomial-time computable* if these algorithms run in polynomial time (in the bit size of the input).

For precise definitions and a thorough survey of the subject of computable rings we refer to Stoltenberg-Hansen–Tucker [SHT99] and the references contained therein.

Example 3.6.2. A field that is finitely generated over its prime ring is computable by the theory of Gröbner bases [vzGG03]. Any uncountable field is not computable.

Let B be an F-algebra with $\dim_F B = n$ and basis $e_1, e_2, \ldots, e_n$ as an F-vector space. Suppose $e_1 = 1$. A **multiplication table** for B is a system of n^3 elements $(c_{ijk})_{i,j,k=1,\ldots,n}$ of F, called **structure constants**, such that multiplication in B is given by

$$e_i e_j = \sum_{k=1}^{n} c_{ijk} e_k$$

for $i, j \in \{1, \ldots, n\}$.

An F-algebra B is represented in bits by a multiplication table and elements of B are represented in the basis e_i. Basis elements in B can be multiplied directly by the multiplication table but multiplication of arbitrary elements in B requires $O(n^3)$ arithmetic operations (additions and multiplications) in F; in either case, note the output is of polynomial size in the input for fixed B.

We now exhibit an algorithm to test if an F-algebra B (of dimension n) has a standard involution.

First, we note that if B has a standard involution $\bar{\ } : B \to B$, then this involution and hence also the reduced trace and norm can be computed. Let $\{e_i\}_i$ be a basis for B; then $\mathrm{trd}(e_i) \in F$ is simply the coefficient of e_i in e_i^2, and so $\overline{e_i} = \mathrm{trd}(e_i) - e_i$ for each i can be precomputed for B; one recovers the involution on B for an arbitrary element of B by F-linearity. Therefore the involution and the reduced trace can be computed using $O(n)$ arithmetic operations in F and the reduced norm using $O(n^2)$ operations in F.

Algorithm 3.6.3. This algorithm takes as input B, an F-algebra given by a multiplication table in the basis $e_1, \ldots, e_n$ with $e_1 = 1$. It returns as output `true` if and only if B has a standard involution, and if so returns the standard involution as a linear map.

1. For $i = 2, \ldots, n$, let $t_i \in F$ be the coefficient of e_i in e_i^2, and let $n_i = e_i^2 - t_i e_i$. If some $n_i \notin F$, return `false`.
2. For $i = 2, \ldots, n$ and $j = i+1, \ldots, n$, let $n_{ij} = (e_i + e_j)^2 - (t_i + t_j)(e_i + e_j)$. If some $n_{ij} \notin F$, return `false`. Otherwise, return `true`, and the linear map defined by $e_i \mapsto t_i - e_i$.

Proof of correctness. Let $F[x] = F[x_1, \ldots, x_n]$ be the polynomial ring over F in n variables, and let $B_{F[x]} = B \otimes_F F[x]$. Let $\xi = x_1 + x_2 e_2 + \cdots + x_n e_n \in B_{F[x]}$, and define

$$t_\xi = \sum_{i=1}^{n} t_i x_i$$

and

$$n_\xi = \sum_{i=1}^{n} n_i x_i^2 + \sum_{1 \le i < j \le n} (n_{ij} - n_i - n_j) x_i x_j.$$

Let

$$\xi^2 - t_\xi \xi + n_\xi = \sum_{i=1}^{n} c_i(x_1, \ldots, x_n) e_i$$

with $c_i(x) \in F[x]$. Each $c_i(x)$ is a homogeneous polynomial of degree 2. The algorithm then verifies that $c_i(x) = 0$ for $x \in \{e_i\}_i \cup \{e_i + e_j\}_{i,j}$, and this implies that each $c_i(x)$ vanishes identically. Therefore, the specialization of the map $\xi \mapsto \overline{\xi} = t_\xi - \xi$ is the unique standard involution on B. □

3.6.4. Algorithm 3.6.3 requires $O(n)$ arithmetic operations in F, since e_i^2 can be computed directly from the multiplication table and hence

$$(e_i + e_j)^2 = e_i^2 + e_i e_j + e_j e_i + e_j^2$$

can be computed using $O(4n) = O(n)$ operations.

Chapter 4

Quadratic forms

4.6 Algorithmic aspects

We conclude with two comments on algorithms arising naturally from the above; for an overview, see Voight [Voi2013].

First, the proof that a quadratic form can be diagonalized (Lemma 4.3.1) is algorithmic, requiring $O(n^3)$ field operations in F.

Second, Main Theorem 4.4.1 yields the following algorithm for algorithmic recognition of a quaternion algebra.

Algorithm 4.6.1. This algorithm takes as input B, an F-algebra with $\dim_F B = 4$, specified by a multiplication table. It returns as output `true` if and only if B is a quaternion algebra, and if so returns an isomorphism $B \simeq (a, b \mid F)$.

1. Verify that B has a standard involution by calling Algorithm 3.6.3. If not, return `false`.
2. Compute a diagonalized basis $1, i, j, k$ for the quadratic form $\mathrm{nrd}\colon B \to F$.
3. Compute $d := \mathrm{disc}(\mathrm{nrd}) \in F/F^{\times 2}$. If $d \neq 0$, return `true` and the quaternion algebra $(a, b \mid F)$ given by the standard generators i, j. Otherwise, return `false`.

Chapter 5

Ternary quadratic forms and quaternion algebras

5.8 Algorithmic aspects

In this section, we show how the equivalences of Main Theorem 5.4.4 involved in identifying the matrix ring (splitting of a quaternion algebra) can be made algorithmic.

Algorithm 5.8.1. This algorithm takes as input $\alpha \in B$ a zerodivisor and returns as output a nonzero element $\epsilon \in B$ such that $\epsilon^2 = 0$.

1. If $\mathrm{trd}(\alpha) = 0$, return α.
2. Compute $0 \neq \beta \in B$ orthogonal to $1, \alpha$ with respect to the quadratic form nrd. If $\alpha\beta = 0$, return β; otherwise, return $\alpha\beta$.

Proof of correctness. The element $\alpha \neq 0$ is a zerodivisor if and only if $\mathrm{nrd}(\alpha) = \alpha\overline{\alpha} = 0$. Since β is orthogonal to $1, \alpha$ we have $\overline{\beta} = -\beta$ and $\mathrm{trd}(\alpha\beta) = -\mathrm{trd}(\alpha\overline{\beta}) = 0$. If $\alpha\beta = 0$ then β is as desired. If $\alpha\beta \neq 0$ then $\mathrm{nrd}(\alpha\beta) = \mathrm{nrd}(\alpha)\,\mathrm{nrd}(\beta) = 0$, as desired. □

Algorithm 5.8.2. This algorithm takes as input $\epsilon \in B$ satisfying $\epsilon^2 = 0$ and returns as output a standard representation $B \simeq (1, 1 \mid F) \simeq \mathrm{M}_2(F)$.

1. Find $k \in \{i, j, ij\}$ such that $\mathrm{trd}(\epsilon k) = s \neq 0$. Let $t := \mathrm{trd}(k)$ and $n := \mathrm{nrd}(k)$, and let $\epsilon' := (1/s)\epsilon$.
2. Let $j' := k + (-tk + n + 1)\epsilon'$ and let

$$i' := \epsilon' k - (k + t)\epsilon'$$

   Return i', j'.

Proof of correctness. In Step 1, if $\mathrm{trd}(\epsilon k) = 0$ for all such k then $\epsilon \in \mathrm{rad}(\mathrm{nrd})$, contradicting Main Theorem 4.4.1. We have $\mathrm{trd}(\epsilon' k) = \mathrm{trd}(k\epsilon') = 1$ so $\mathrm{trd}(\overline{\epsilon' k}) = -1$.

Consider $I = F\epsilon' + Fk\epsilon'$. Note $\mathrm{trd}(k\epsilon') \neq 0$ implies that $\epsilon', k\epsilon'$ are linearly independent. Let A be the subalgebra of B generated by ϵ' and k. We have $\epsilon' k + k\epsilon' =$

$t\epsilon' + 1$ from (4.2.14) and $k^2 = tk - n$, and thus we compute that left multiplication yields a map

$$A \to \mathrm{End}_F(I) \simeq \mathrm{M}_2(F)$$
$$\epsilon', k \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -n \\ 1 & t \end{pmatrix}.$$

A direct calculation then reveals that $j' \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $i' \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. It follows at once that $A = B$, that $I = B\epsilon'$, and that the map $B \to \mathrm{M}_2(F)$ is an isomorphism. □

In this way, we have seen that in deterministic polynomial time we can convert an isotropic vector (i.e., an F-rational point on the associated conic) or a zerodivisor to an explicit splitting $B \xrightarrow{\sim} \mathrm{M}_2(F)$ for all computable fields F with $\mathrm{char}\, F \neq 2$. On the other hand, the problem of finding such an isotropic vector depends in a serious way on the arithmetic of the field F [Voi2013, §4].

Chapter 8

Simple algebras and involutions

8.6 Algorithmic aspects

In section 4.6, we showed how to recover an isomorphism $B \simeq \mathrm{M}_2(F)$ from a nonzero nilpotent element $\epsilon \in B$ (or more generally, a zerodivisor $\epsilon \in B$). In a similar way, the proof of Proposition 8.2.3 can be made algorithmic: if B_1, B_2 are quaternion algebras over F, then given a nonzero nilpotent element $\epsilon \in B_1 \otimes B_2$, we can exhibit explicitly a common embedded quadratic subfield. By the proof of Proposition 8.2.8, such a nilpotent element is given by a zero of the Albert form $Q(B_1, B_2)$ when $\operatorname{char} F \neq 2$. From Exercise 8.2, we then find an explicit isomorphism $B_1 \otimes B_2 \simeq \mathrm{M}_2(B_3)$. We then have $B_1 \simeq B_2$ if and only if $B_3 \simeq \mathrm{M}_2(F)$, so from this method we have reduced the problem of testing for an isomorphism between quaternion algebras to the problem of splitting a quaternion algebra. For a more general point of view on the algorithmic problem of testing if two central simple algebras over a number field are isomorphic using norm equations, see work by Hanke [Hanke2007].

Part II

Arithmetic

Chapter 9

Lattices and integral quadratic forms

9.9 Algorithmic aspects

We give an algorithmic proof of Proposition 9.8.4.

Algorithm 9.9.1. Let R be a computable ring which is a local PID with (computable) valuation $v : R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

Let $Q\colon M \to R$ be a quadratic form over R and let $e_1, \ldots, e_n$ be a basis for M. This algorithm returns a basis of M in which Q is normalized.

1. If $T(e_i, e_j) = 0$ for all i, j, return $f_i := e_i$. Otherwise, let (i, j) with $1 \leq i \leq j \leq n$ be such that $vT(e_i, e_j)$ is minimal, taking $i = j$ if possible and if not taking i minimal.
2. If $i = j$, let $f_1 := e_i$ and proceed to Step 3. If $i \neq j$ and $2 \in R^\times$, let $f_1 := e_i + e_j$ and proceed to Step 3. Otherwise, proceed to Step 4.
3. Let $e_i := e_1$. For $k = 2, \ldots, n$ let
$$f_k := e_k - \frac{T(f_1, e_k)}{T(f_1, f_1)} f_1.$$
Let $m = 2$ and proceed to Step 5.
4. (We have $2 \notin R^\times$ and $i \neq j$.) Let
$$f_1 := \frac{\pi^{v(T(e_i, e_j))}}{T(e_i, e_j)} e_i,$$
$f_2 := e_j$, $e_i := e_1$ and $e_j := e_2$. Let $d := T(f_1, f_1)T(f_2, f_2) - T(f_1, f_2)^2$. For $k = 3, \ldots, n$, let
$$t_k := T(f_1, f_2)T(f_2, e_k) - T(f_2, f_2)T(f_1, e_k)$$
$$u_k := T(f_1, f_2)T(f_1, e_k) - T(f_1, f_1)T(f_2, e_k)$$
and let
$$f_k := e_k + \frac{t_k}{d} f_1 + \frac{u_k}{d} f_2.$$
Let $m = 3$.

5. Recursively call the algorithm with input $M = Rf_m \oplus \cdots \oplus Rf_n$, and return $f_1, \ldots, f_{m-1}$ concatenated with the output basis.

Given such a basis, one recovers the normalized quadratic form by factoring out in each atomic form the minimal valuation achieved. (One can also keep track of this valuation along the way in the above algorithm, if desired.)

Remark 9.9.2. If $2 \in R^\times$, then a quadratic form Q is atomic if and only if $Q(x) = ax^2$ for $a \in R^\times$, so Algorithm 9.9.1 computes a diagonalization of the form Q, ordering the coefficients by their valuation.

Proof of correctness of Algorithm 9.9.1. In Step 3, we verify that

$$v(T(f_1, f_1)) \leq v(T(f_1, e_k)).$$

Indeed,

$$T(f_1, f_1) = T(e_i, e_i) + 2T(e_i, e_j) + T(e_j, e_j)$$

and so $v(T(f_1, f_1)) = v(T(e_i, e_j))$ by the ultrametric inequality and the hypotheses that $v(T(e_i, e_j)) < v(T(e_i, e_i)), v(T(e_j, e_j))$ and $v(2) = 0$. Therefore Steps 2 and 3 give correct output.

We have left to check Step 4. This is proven by letting $f_k = e_k + t_k f_1 + u_k f_2$ and solving the linear equations $T(f_1, f_k) = T(f_2, f_k) = 0$ for t_k, u_k. The result then follows from a direct calculation, coupled with the fact that $v(d) = 2v(T(f_1, f_2)) \leq v(t_k)$ (and similarly with u_k). This case only arises if (and only if)

$$v(T(f_1, f_2)) < v(T(f_1, f_1)) = v(2Q(f_1)) \leq v(2Q(f_2))$$

so the corresponding block is atomic. □

Algorithm 9.9.1 requires $O(n^2)$ arithmetic operations in R, and can be modified suitably to operate directly on the Gram matrix $(T(e_i, e_j))_{i,j}$ of the quadratic form Q.

Chapter 12

Ternary quadratic forms over local fields

12.6 Algorithmic aspects

In this section, we discuss algorithms for computing the Hilbert symbol. For more details, see Voight [Voi2013, §5].

Let F be a local field and $F \neq \mathbb{C}$. If $F \simeq \mathbb{R}$ is nonarchimedean, let R be the valuation ring, $\mathfrak{p}$ the maximal ideal, π a uniformizer, $k = R/\mathfrak{p}$ the residue field, and $\mathrm{ord}\colon F \to \mathbb{Z} \cup \{\infty\}$ the valuation with $\mathrm{ord}_{\mathfrak{p}}(\pi) = 1$. If F is archimedean, we let $R = F = \mathfrak{p}$ and $\pi = -1$ and let $a = (-1)^{\mathrm{ord}(a)}|a|$ for $a \in F$, so $\mathrm{ord}(a) = 0, 1$ according as $a > 0$ or $a < 0$.

Remark 12.6.1. To be completely precise, a local field F is uncountable, so it is not computable. When we talk about computing in a local field, this can be interpreted either to mean we work in finite precision (and there are several ways to interpret this, giving different models) or we work in the algebraic closure of a global field (see section 14.4) inside its completion at a prime $\mathfrak{p}$.

For $a \in F^\times$, we define the **square symbol**

$$\left\{\frac{a}{F}\right\} := \begin{cases} 1, & \text{if } a \in F^{\times 2}; \\ -1, & \text{if } a \notin F^{\times 2} \text{ and } \mathrm{ord}(a) \text{ is even}; \\ 0, & \text{if } a \notin F^{\times 2} \text{ and } \mathrm{ord}(a) \text{ is odd}. \end{cases}$$

We have $\left\{\frac{a}{F}\right\} = -1$ if and only if $F(\sqrt{a})$ is an unramified field extension of F and $\left\{\frac{a}{F}\right\} = 0$ if and only if $F(\sqrt{a})$ is ramified; when $F \simeq \mathbb{R}$ is real, we follow the convention that $\mathbb{C}$ is considered to be ramified over $\mathbb{R}$. Accordingly, if v is nonarchimedean, then $\left\{\frac{a}{F}\right\} = 0$ if and only if $\mathrm{ord}(a)$ is odd. The square symbol is not multiplicative.

Proposition 12.6.2. *Let $a, b \in F^\times$. Then $(a, b)_F = 1$ if and only if*

$$\left\{\frac{a}{F}\right\} = 1 \text{ or } \left\{\frac{b}{F}\right\} = 1 \text{ or } \left\{\frac{-ab}{F}\right\} = 1 \text{ or } \left\{\frac{a}{F}\right\} = \left\{\frac{b}{F}\right\} = \left\{\frac{-ab}{F}\right\} = -1.$$

Proof. The result is immediately verified if F is archimedean; if F is nonarchimedean, the result follows from (12.5.4). □

To conclude, we discuss the computability of the Hilbert symbol when $\operatorname{char} k \neq 2$ using Proposition 12.6.2. We may suppose F is nonarchimedean. Then we can evaluate $\left\{\frac{a}{F}\right\}$ by simply computing $\operatorname{ord}(a) = e$; if e is odd then $\left\{\frac{a}{F}\right\} = 0$, whereas if e is even then $\left\{\frac{a}{F}\right\} = \left(\frac{a_0}{F}\right)$ where $a_0 = a\pi^{-e} \in R$ and $\left(\frac{a_0}{v}\right) = \left(\frac{a_0}{\mathfrak{p}}\right)$ is the usual Legendre symbol, defined by

$$\left(\frac{a_0}{\mathfrak{p}}\right) := \begin{cases} 0, & \text{if } a_0 \equiv 0 \pmod{\mathfrak{p}}; \\ 1, & \text{if } a_0 \not\equiv 0 \pmod{\mathfrak{p}} \text{ and } a_0 \text{ is a square modulo } \mathfrak{p}; \\ -1, & \text{otherwise.} \end{cases} . \tag{12.6.3}$$

The Legendre symbol can be computed in deterministic polynomial time by Euler's formula

$$\left(\frac{a_0}{\mathfrak{p}}\right) \equiv a_0^{(q-1)/2} \pmod{\mathfrak{p}}$$

using repeated squaring, where $q = \#k$. We find that there exists a deterministic polynomial-time algorithm to evaluate the Hilbert symbol when $\operatorname{char} k \neq 2$.

The Hilbert symbol when $\operatorname{char} k = 2$ is somewhat more complicated; we follow Voight [Voi2013, §6].

Algorithm 12.6.4. Let $\mathfrak{p}$ an even prime with ramification index $e = \operatorname{ord}_{\mathfrak{p}}(2)$, and let $a, b \in F$ be such that $\operatorname{ord}_{\mathfrak{p}}(a) = 0$ and $\operatorname{ord}_{\mathfrak{p}}(b) = 1$. This algorithm outputs a solution to the congruence

$$1 - ay^2 - bz^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

with $y, z \in \mathbb{Z}_F/\mathfrak{p}^{2e}$ and $y \in (\mathbb{Z}_F/\mathfrak{p})^\times$.

1. Let $f \in \mathbb{Z}_{\geq 1}$ be the residue class degree of $\mathfrak{p}$ (so that $\#(\mathbb{Z}_F/\mathfrak{p}) = 2^f$) and let $q = 2^f$. Let π be a uniformizer at $\mathfrak{p}$.
2. Initialize $(y, z) := (1/\sqrt{a}, 0)$.
3. Let $N := 1 - ay^2 - bz^2 \in \mathbb{Z}_F/4\mathbb{Z}_F$ and let $t := \operatorname{ord}_{\mathfrak{p}}(N)$. If $t \geq 2e$, return y, z. Otherwise, if t is even, let

$$y := y + \sqrt{\frac{N}{a\pi^t}}\pi^{t/2}$$

and if t is odd, let

$$z := z + \sqrt{\frac{N}{b\pi^{t-1}}}\pi^{\lfloor t/2 \rfloor}.$$

Return to Step 3.

In this algorithm, when we write $\sqrt{u}$ for $u \in (\mathbb{Z}_F/\mathfrak{p}^{2e})^\times$ we mean a choice of a lift of $\sqrt{u} \in (\mathbb{Z}_F/\mathfrak{p})^\times$ to $\mathbb{Z}_F/\mathfrak{p}^{2e}$. We reduce to the above Hensel lift by the following algorithm.

Algorithm 12.6.5. Let $\mathfrak{p}$ an even prime with ramification index $e = \operatorname{ord}_{\mathfrak{p}} 2$ and let $a, b \in F^\times$ be such that $v(a) = 0$ and $v(b) \in \{0, 1\}$. This algorithm outputs $y, z, w \in \mathbb{Z}_F/\mathfrak{p}^{2e}$ such that

$$1 - ay^2 - bz^2 + abw^2 \equiv 0 \pmod{\mathfrak{p}^{2e}}$$

and $y \in (\mathbb{Z}_F/\mathfrak{p})^\times$. Let π be a uniformizer for $\mathfrak{p}$.

1. If $v(b) = 1$, return the output $(y, z, 0)$ of Algorithm 12.6.4 with input a, b.
2. Suppose $a \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$ and $b \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$. Let $(a_0)^2 a \equiv 1 \pmod{\mathfrak{p}^e}$ and $(b_0)^2 b \equiv 1 \pmod{\mathfrak{p}^e}$. Return
$$y := a_0,\ z := b_0,\ w := a_0 b_0.$$
3. Swap a, b if necessary so that $a \in (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^\times \setminus (\mathbb{Z}_F/\mathfrak{p}^e\mathbb{Z}_F)^{\times 2}$. Let t be the largest integer such that $a \in (\mathbb{Z}_F/\mathfrak{p}^t)^{\times 2}$ but $a \notin (\mathbb{Z}_F/\mathfrak{p}^e)^{\times 2}$. Then t is odd; write $a = a_0^2 + \pi^t a_t$ with $a_0, a_t \in \mathbb{Z}_F$. Let y, z be the output of Algorithm 12.6.4 with input $a' := a$, $b' := -\pi a_t/b$. Return
$$y' := \frac{1}{a_0},\ z' := \frac{\pi^{\lfloor t/2 \rfloor}}{a_0 z},\ w' := \frac{y\pi^{\lfloor t/2 \rfloor}}{a_0 z}$$
(reswapping if necessary).

For a proof of correctness of these two algorithms, see Voight [Voi2013, Algorithms 6.2, 6.5].

Definition 12.6.6. We say that $\pi^{-1} \in F^\times$ is an **inverse uniformizer** for the prime $\mathfrak{p} \subseteq R$ if $\operatorname{ord}_{\mathfrak{p}}(\pi^{-1}) = -1$ and $\operatorname{ord}_{\mathfrak{q}}(\pi^{-1}) \geq 0$ for all $\mathfrak{q} \neq \mathfrak{p}$.

We are now prepared to evaluate the even Hilbert symbol.

Algorithm 12.6.7. Let $B = \left(\frac{a, b}{F}\right)$ be a quaternion algebra with $a, b \in F^\times$, and let $\mathfrak{p}$ be an even prime of F. This algorithm returns the value of the Hilbert symbol $(a, b)_{\mathfrak{p}}$.

1. Scale a, b if necessary by an element of $\mathbb{Q}^{\times 2}$ so that $a, b \in \mathbb{Z}_F$.
2. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$. Let
$$a := (\pi^{-1})^{2\lfloor \operatorname{ord}_{\mathfrak{p}}(a)/2 \rfloor} a \quad \text{and} \quad b := (\pi^{-1})^{2\lfloor \operatorname{ord}_{\mathfrak{p}}(b)/2 \rfloor} b.$$
If $\operatorname{ord}_{\mathfrak{p}} a = \operatorname{ord}_{\mathfrak{p}} b = 1$, let $a := (\pi^{-1})^2(-ab)$. Swap if necessary so that $\operatorname{ord}_{\mathfrak{p}} a = 0$.
3. Call Algorithm 12.6.5, and let $i' := (1 + yi + zj + wij)/2$. Let $f(T) = T^2 - T + \operatorname{nrd}(i')$ be the minimal polynomial of i'. If f has a root modulo $\mathfrak{p}$, return 1.
4. Let $j' := (zb)i - (ya)j$ and let $b' := (j')^2$. If $\operatorname{ord}_v b'$ is even, return 1, otherwise return -1.

Proof of correctness. If in Step 2 we have a root modulo $\mathfrak{p}$, then by Hensel's lemma, f has a root $t \in F_{\mathfrak{p}}$, hence $t - i'$ is a zerodivisor and we return 1 correctly. Otherwise, $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i']$ is the unramified field extension of $F_{\mathfrak{p}}$. We compute that $\operatorname{trd}(j') = \operatorname{trd}(i'j') = 0$, so $B_{\mathfrak{p}} \simeq (K_{\mathfrak{p}}, b' \mid F_{\mathfrak{p}})$ and $B_{\mathfrak{p}}$ is split if and only if $\operatorname{ord}_{\mathfrak{p}} b'$ is even. □

Chapter 14

Quaternion algebras over global fields

14.8 Algorithmic aspects

In this seciton, we show how to make the classification of quaternion algebras (Main Theorem 14.1.3, and more generally Main Theorem 14.6.1) algorithmic, giving a computable bijection between quaternion algebras and ramification sets.

First, we showed in Proposition 14.2.7 how to exhibit explicitly a quaternion algebra B over $\mathbb{Q}$ with a given ramification set $\operatorname{Ram} B = \Sigma$. In general, we need to be able to find a prime q satisfying certain congruence conditions (14.2.11)–(14.2.12), and this may be done with a probabilistic algorithm. The generalization of this algorithm to number fields is as follows [GV2011, Algorithm 4.1].

Algorithm 14.8.1. This algorithm takes as input a finite set $\Sigma \subset \operatorname{Pl}(F)$ of noncomplex places of a number field F of even cardinality, and returns as output $a, b \in \mathbb{Z}_F$ such that the quaternion algebra $B = \left(\frac{a,b}{F}\right)$ has $\operatorname{Ram} B = \Sigma$.

1. Let $\mathfrak{D} := \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}$ be the product of the (finite) primes in Σ. Find $a \in \mathfrak{D}$ such that for all real places v we have $v(a) < 0$ for all $v \in \operatorname{Ram} B$ and such that $a\mathbb{Z}_F = \mathfrak{D}\mathfrak{b}$ with $\mathfrak{D} + \mathfrak{b} = \mathbb{Z}_F$ and $\mathfrak{b}$ odd.
2. Factor the ideal $\mathfrak{b}$ into primes. Find $t \in \mathbb{Z}_F/8a\mathbb{Z}_F$ such that the following hold:
   a) For all primes $\mathfrak{p} \mid \mathfrak{D}$, we have $\left(\frac{t}{\mathfrak{p}}\right) = -1$;
   b) For all primes $\mathfrak{q} \mid \mathfrak{b}$, we have $\left(\frac{t}{\mathfrak{q}}\right) = 1$; and
   c) For all prime powers $\mathfrak{r}^e \parallel 8\mathbb{Z}_F$ with $\mathfrak{r} \nmid \mathfrak{D}$, we have $t \equiv 1 \pmod{\mathfrak{r}^e}$.
3. Find $m \in \mathbb{Z}_F$ such that $b := t + 8am \in \mathbb{Z}_F$ satisfies the following conditions:
   a) b is prime (i.e., (b) is a prime ideal);
   b) $v(b) < 0$ for all real places $v \in \operatorname{Ram} B$; and
   c) $v(b) > 0$ for all real places $v \notin \operatorname{Ram} B$ such that $v(a) < 0$.

It can be verified in a manner similar to the proof over $\mathbb{Q}$ that the algebra $B = \left(\frac{a,b}{F}\right)$ output by Algorithm 14.8.1 has the correct set of ramified places.

The steps in Algorithm 14.8.1 for working with elements in F and ideals in the ring of integers $\mathbb{Z}_F$ are standard, and they are described in the books on computational algebraic number theory by Cohen [Coh93, Coh2000].

Remark 14.8.2. When possible, it is often helpful in practice to take $a\mathbb{Z}_F = \mathfrak{D}$ in Algorithm 14.8.1: for example, if $\mathfrak{D} = \mathbb{Z}_F$ and there exists a unit $u \in \mathbb{Z}_F^\times$ with the right real signs as in Step 3 and such that $u \equiv 1 \pmod 8$, then we may simply take $B = \left(\frac{-1, u}{F}\right)$. In any event, in Step 2, one may find the element t by deterministic or probabilistic means; moreover, one may wish to be alternate between Steps 2 and 3 in searching for b.

14.8.3. Algorithm 14.8.1 may be generalized to the case where F is a global function field is analogous, but at the present time the literature is much less complete in describing a suite of algorithms for computing with integral structures in such fields analogous to those mentioned in section 9.8—particularly in the situation where one works in a relative extension of such fields. (See Hess [Hess2002] for a start.) Therefore, in this book we will often consider just the case of number fields and content ourselves to notice that the algorithms we provide will generalize with appropriate modifications to the global function field setting.

14.8.4. Next, the converse: given a quaternion algebra $B = (a, b \mid F)$ over a number field F, we compute the ramification set $\operatorname{Ram} B$. For this, we simply factor 2 and (the numerator and denominator of) a and b, and for each prime $\mathfrak{p}$ occuring in these factorizations and each real place v of F, we compute the corresponding Hilbert symbol as described in section 12.6.

In the special case where this computation reveals that $\operatorname{Ram} B = \emptyset$, we may ask further for an explicit isomorphism $B \xrightarrow{\sim} \mathrm{M}_2(F)$. (See Voight [Voi2013, Section 7] for discussion of the algorithmic problem of "recognizing the matrix ring".) There are several points of view on this problem, relating it to important algorithmic problems in algorithmic number theory. First, as discussed in 4.6, it is equivalent to compute a zerodivisor in B. One method to find such a zerodivisor is to seek appropriate "small" integral elements. Second, as explained in section 5.5, one can equivalently find a rational point on a conic over F; in the case $F = \mathbb{Q}$, algorithms for this problem are due to Cremona–Rusin [CR2003] and Simon [Sim2005], and they run in probabilistic polynomial time given the factorization of $a, b \in \mathbb{Z}$ (probabilism only occurs in the need to compute square roots modulo p). Aspects of these approaches have been extended to number fields, but there is no as yet definitive reference. Third and finally, by Main Theorem 5.4.4, one can also equivalently solve a norm equation in a relative quadratic extension $K \supseteq F$; there are a number of approaches to this problem (see Simon [Sim2002] and the references therein, and Bartels [Bar80] for more on the theory). Unfortunately, the running time for these algorithms is often poor (as they involve the computation of an S-unit and S-class group). Nevertheless, this point of view generalizes cleanly to splitting central simple algebras over number fields (see work of Hanke [Hanke2007]).

Chapter 15

Discriminants

15.6 Algorithmic aspects

Let F be a number field and $\mathbb{Z}_F$ its ring of integers. Let $B = (a, b \mid F)$ be a quaternion algebra over F, and let $O \subset B$ be a $\mathbb{Z}_F$-order. Recall we represent O by a pseudobasis (9.3.6)

$$O = \mathbb{Z}_F \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k$$

as in section 9.8.

15.6.1. The reduced discriminant $\mathrm{discrd}(O)$ can be computed using 15.2.8 and Lemma 15.4.8, without taking a square root:

$$\mathrm{discrd}(O) = \mathfrak{a}\mathfrak{b}\mathfrak{c}\, m(i, j, k).$$

We now discuss some algorithmic aspects of computing maximal orders in this setting, following Voight [Voi2013, §7]. We say an order $O \subset B$ is $\mathfrak{p}$**-maximal** for a prime $\mathfrak{p}$ of $\mathbb{Z}_F$ if $O_\mathfrak{p} = O \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}}$ is maximal. We begin with an order to start with: rescaling we may suppose $a, b \in \mathbb{Z}_F$, and then we may take $O = \mathbb{Z}_F\langle i, j\rangle$ where i, j are standard generators.

Given an order O, to compute a maximal order $O' \supseteq O$ we compute the reduced discriminant $\mathrm{discrd}(O)$, factor this ideal, and recursively compute a $\mathfrak{p}$-maximal order for every prime $\mathfrak{p} \mid \mathrm{discrd}(O)$, proceeding in two steps.

Definition 15.6.2. An order O is $\mathfrak{p}$**-saturated** if $\mathrm{nrd}|_{O_\mathfrak{p}}$ has a normalized basis $1, i, j, k$ (see Proposition 9.8.4) such that each atomic block has valuation at most 1; we then say that $1, i, j, k$ is a $\mathfrak{p}$**-saturated** basis for O.

We compute a $\mathfrak{p}$-saturated order in the following straightforward way.

Algorithm 15.6.3. Let $O = \mathbb{Z}_F \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k \subset B$ be an order and let $\mathfrak{p}$ be prime. This algorithm computes a $\mathfrak{p}$-saturated order $O' \supseteq O$ and a $\mathfrak{p}$-saturated basis for O'.

1. Choose $d \in \mathfrak{a}$ such that $\mathrm{ord}_\mathfrak{p}(d) = \mathrm{ord}_\mathfrak{p}(\mathfrak{a})$ and let $i := di$; compute similarly with j, k. Let $O' := O$.

2. Run Algorithm 9.9.1 over the localization $\mathbb{Z}_{F,(\mathfrak{p})}$ with the quadratic form nrd on the basis $1, i, j, k$; let $1, i^*, j^*, k^*$ be the output. Let $c \in \mathbb{Z}_F$ be such that $\mathrm{ord}_{\mathfrak{p}}\, c = 0$ and such that $ci^* \in O$, and let $i := ci^*$; compute similarly with j, k.
3. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$. For each atomic form Q in nrd_O, let e be the valuation of Q, and multiply each basis element in Q by $(\pi^{-1})^{\lfloor e/2 \rfloor}$. Return $O' := O + (\mathbb{Z}_F i \oplus \mathbb{Z}_F j \oplus \mathbb{Z}_F k)$ and the basis $1, i, j, k$.

Proof of correctness. In Step 3, we verify that the output of Algorithm 9.9.1 leaves 1 as the first basis element. We note that $\mathrm{ord}_{\mathfrak{p}}\,\mathrm{trd}(j) \leq \mathrm{ord}_{\mathfrak{p}}\,\mathrm{trd}(i(ij))$ since $\mathrm{trd}(i(ij)) = \mathrm{trd}(i)^2 - \mathrm{trd}(j)\,\mathrm{nrd}(i)$ and similarly $\mathrm{ord}_{\mathfrak{p}}\,\mathrm{trd}(i) \leq \mathrm{ord}_{\mathfrak{p}}\,\mathrm{trd}((ij)j)$.

Let $1, i, j, k$ be the basis computed in Step 3. By definition, this basis is $\mathfrak{p}$-saturated; we need to show that O is an order. But O is an order if and only if $O_{\mathfrak{q}}$ is an order for all primes $\mathfrak{q}$, and $O_{\mathfrak{q}} = \Lambda_{\mathfrak{q}}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$. For all $\alpha, \beta \in B$ we have $\alpha\beta + \beta\alpha = \mathrm{trd}(\beta)\alpha + \mathrm{trd}(\alpha)\beta - T(\alpha, \beta)$, so if O is an order then $O + \mathbb{Z}_F\alpha$ is multiplicatively closed if and only if $T(\alpha, \beta) \in \mathbb{Z}_F$ for all $\beta \in O$. We have $T(\alpha, \beta) = 0$ if α, β are orthogonal, and if α, β are a basis for an atomic block Q then by definition the valuation of $T(\alpha, \beta)$ is at least the valuation of Q and we can multiply each by $(\pi^{-1})^{\lfloor e/2 \rfloor}$, preserving integrality. □

One can compute a $\mathfrak{p}$-maximal order as follows.

Algorithm 15.6.4. Let O be an order and let $\mathfrak{p}$ be prime. This algorithm computes a $\mathfrak{p}$-maximal order $O' \supseteq O$.

1. Compute a $\mathfrak{p}$-saturated order $O' \supseteq O$ and let $1, i, j, k$ be a $\mathfrak{p}$-saturated basis for O'. Let π^{-1} be an inverse uniformizer for $\mathfrak{p}$.
2. Suppose $\mathfrak{p}$ is odd. Swap i for j or k if necessary so that $a := i^2$ has $\mathrm{ord}_{\mathfrak{p}}(a) = 0$. Let $b := j^2$. If $\mathrm{ord}_{\mathfrak{p}}\, b = 0$, return O'. Otherwise, if $\mathrm{ord}_{\mathfrak{p}}\, b = 1$ and $\left(\frac{a}{\mathfrak{p}}\right) = 1$, solve
$$x^2 \equiv a \pmod{\mathfrak{p}}$$
for $x \in \mathbb{Z}_F/\mathfrak{p}$. Adjoin the element $\pi^{-1}(x - i)j$ to O', and return O'.
3. Otherwise, $\mathfrak{p}$ is even. Let $t := \mathrm{trd}(i)$, let $a := -\mathrm{nrd}(i)$, and let $b := j^2$.
   a. Suppose $\mathrm{ord}_{\mathfrak{p}}\, t = 0$. If $\mathrm{ord}_{\mathfrak{p}}\, b = 0$, return O'. If $\mathrm{ord}_{\mathfrak{p}}\, b = 1$ and there is a solution $x \in \mathbb{Z}_F$ to $x^2 - tx + a \equiv 0 \pmod{\mathfrak{p}}$, and return $O + \mathbb{Z}_F\pi^{-1}(x - i)j$.
   b. Suppose $\mathrm{ord}_{\mathfrak{p}}\,\mathrm{trd}(i) > 0$. Let y, z, w be the output of Algorithm 12.6.5 with input a, b. Let
$$i' := (\pi^{-1})^e(1 + yi + zj + wij).$$
   Adjoin i' to O, and return to Step 1.

Proof of correctness. At every step in the algorithm, for each prime $\mathfrak{q} \neq \mathfrak{p}$ the order $O_{\mathfrak{q}}$ does not change, so we need only verify that $O_{\mathfrak{p}}$ is a maximal order.

In Step 2, b is a uniformizer for $\mathfrak{p}$ and $\mathrm{discrd}(O_{\mathfrak{p}}) = 4ab\mathbb{Z}_{F,\mathfrak{p}}$. If $\mathrm{ord}_{\mathfrak{p}}(b) = 0$ then $\mathrm{ord}_{\mathfrak{p}}\,\mathrm{discrd}(O_{\mathfrak{p}}) = 0$ so O is maximal. Otherwise, $\mathrm{discrd}(O_{\mathfrak{p}}) = \mathfrak{p}$ and $B_{\mathfrak{p}} \simeq (K_{\mathfrak{p}}, b \mid F_{\mathfrak{p}})$ where $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i]$. We conclude that $B_{\mathfrak{p}}$ is a division ring (and hence $O_{\mathfrak{p}}$ is maximal) if and only if $(a/\mathfrak{p}) = -1$. If $(a/\mathfrak{p}) = 1$ and $j' = \pi^{-1}(x - i)j$, then $1, i, j', ij'$

form the $\mathbb{Z}_{F,\mathfrak{p}}$-basis for a maximal order, since $(j')^2 = (\pi^{-1})^2(x^2 - a)b \in \mathbb{Z}_{F,\mathfrak{p}}$ and $j'i = -ij'$.

In Step 3, first note that ij is also orthogonal to $1, i$: since i is orthogonal to j we get $\mathrm{trd}(ij) = 0$, so ij is orthogonal to 1, and similarly $\mathrm{trd}(iji\bar{i}) = \mathrm{trd}(\mathrm{nrd}(i)j) = 0$. In particular, $B_{\mathfrak{p}} = (K_{\mathfrak{p}}, b \mid F_{\mathfrak{p}})$ where $K_{\mathfrak{p}} = F_{\mathfrak{p}}[i]$. By a comparison of discriminants, using the fact that the basis is normalized, we see that $1, i, j, ij$ is a $\mathfrak{p}$-saturated basis for O as well, so without loss of generality we may take $k = ij$.

Suppose first that $\mathrm{ord}_{\mathfrak{p}} \mathrm{trd}(i) = 0$, so we are in Step 3a. If $\mathrm{ord}_{\mathfrak{p}} b = 0$, then $\mathrm{ord}_{\mathfrak{p}} \mathrm{discrd}(O_{\mathfrak{p}}) = 0$ so $O_{\mathfrak{p}}$ is maximal. If $\mathrm{ord}_{\mathfrak{p}} b > 0$, then since the basis is $\mathfrak{p}$-saturated, $\mathrm{ord}_{\mathfrak{p}} b = 1$. Thus as in the case for $\mathfrak{p}$ odd, $B_{\mathfrak{p}}$ is a division ring if and only if $K_{\mathfrak{p}}$ is not a field, and as above the adjoining the element $\pi^{-1}(x - i)j$ yields a maximal order.

So suppose we are in Step 3b, so $\mathrm{ord}_{\mathfrak{p}} \mathrm{trd}(i) > 0$. Since $1, i, j, k$ is normalized, $\mathrm{ord}_{\mathfrak{p}} \mathrm{trd}(i) = \mathrm{ord}_{\mathfrak{p}} T(1, i) \leq \mathrm{ord}_{\mathfrak{p}} T(j, k)$. Adjoining i' to O gives a $\mathbb{Z}_{F,\mathfrak{p}}$-module with basis $1, i', j, i'j$ since $y \in (\mathbb{Z}_F/\mathfrak{p})^\times$; adjoining j' gives a module with basis $1, i', j', i'j'$ for the same reason. We verify that $O_{\mathfrak{p}}$ after these steps is an order: $\mathrm{trd}(i') = 2(\pi^{-1})^e \in \mathbb{Z}_{F,\mathfrak{p}}$ and $\mathrm{nrd}(i') = (\pi^{-1})^{2e}(1 - ay^2 - bz^2 + abw^2) \in \mathbb{Z}_{F,\mathfrak{p}}$ by construction, so at least $\mathbb{Z}_{F,\mathfrak{p}}[i] = \mathbb{Z}_{F,\mathfrak{p}} \oplus \mathbb{Z}_{F,\mathfrak{p}} i$ is a ring. Similarly $(j')^2 = b' \in \mathbb{Z}_{F,\mathfrak{p}}$. Finally, $\mathrm{trd}(i'i) = 2(\pi^{-1})^e ya$ and $\mathrm{trd}(i'j) = 2(\pi^{-1})^e zb$; it follows that $\mathrm{trd}(i'j') = 0$, and hence $j'i' = -\overline{i'}j' = -i'j' - \mathrm{trd}(i')j'$, so we have an order. □

Remark 15.6.5. In the proof of correctness for Algorithm 15.6.4, in each case where $\mathfrak{p}$ is ramified in B we have in fact written $B_{\mathfrak{p}} \simeq (K_{\mathfrak{p}}, \pi \mid F_{\mathfrak{p}})$ where $K_{\mathfrak{p}}$ is the unramified extension of $F_{\mathfrak{p}}$. The reader will note the similarity between this algorithm and the algorithm to compute the Hilbert symbol: the former extends the latter by taking a witness for the fact that the algebra is split, namely a zerodivisor modulo $\mathfrak{p}$, and uses this to compute a larger order (giving rise therefore to the matrix ring).

15.6.6. Combining Algorithm 15.6.3 and 15.6.4, we have the following immediate consequence: if $O \subset B$ is an order in a quaternion algebra B over a number field F and $\mathfrak{p}$ is prime of $\mathbb{Z}_F$ which is unramified in B, then there exists an algorithm to compute an explicit embedding $O \hookrightarrow \mathrm{M}_2(O_{\mathfrak{p}})$. Such an algorithm is sometimes called an algorithm to *recognize the p-matrix ring*.

The algorithmic complexity in factoring cannot be avoided in this context, according to the following theorem.

Theorem 15.6.7. *For a fixed number field F, the problem of computing maximal orders in quaternion algebras over F is probabilistic polynomial-time equivalent to the problem of factoring integers.*

For a proof, see Voight [Voi2013, Theorem 7.15] (following a hint of Ronyai [Ron92, §6]).

Remark 15.6.8. More generally, there are algorithms to compute maximal orders in semisimple algebras over number fields that run in deterministic polynomial time given oracles for the problems of factoring integers and factoring polynomials over finite fields: see Ivanyos–Rónyai [IR93, Theorem 5.3], Nebe–Steel [NS2009], and Friedrichs [Fri2000].

Chapter 17

Classes of quaternion ideals

17.8 Algorithmic aspects

In this section, we exhibit an algorithm to compute the size of the class set of an order in a totally definite quaternion algebra. A more sophisticated algorithm, inspired by the notion of Hecke operators acting on modular forms, will be discussed in Chapter 41; our goal in this section is just to try to convince the reader that computations can be carried out easily in practice.

Let F be a number field with ring of integers R, let B be a division quaternion algebra over F, and let $O \subset B$ be an R-order. Then by Main Theorem 17.7.1, there is an effective constant $C > 0$ such that

$$\mathrm{Cls}_{\mathsf{R}}\, O = \{[I]_{\mathsf{R}} : I \subseteq O \text{ invertible and } \mathsf{N}(I) \leq C\}.$$

We compute $\mathrm{Cls}\, O$ in two steps: first, we compute the set of invertible integral O-ideals $I \subseteq O$ with bounded absolute norm, and second we sort them according to their right class.

For the first step, we first note that $\mathsf{N}(I) = \mathsf{N}(\mathrm{nrd}(I))^2$; we can loop over those ideals $\mathfrak{a} \subseteq R$ with bounded $\mathsf{N}(\mathfrak{a})$ by factoring in R, and so it suffices to enumerate all invertible $I \subseteq O$ with $\mathrm{nrd}(I) = \mathfrak{a}$. In general, we appeal to a slight modification of Exercise 16.5: every such ideal is represented as $I = \mathfrak{a}O + \beta O$ with $\beta \in O$, and conversely the R-lattice $\mathfrak{a}O + \beta O$ is locally principal if $\mathrm{nrd}(\beta)R + \mathfrak{a} = \mathrm{nrd}(\beta)$. Since β is well-defined as an element of $O/\mathfrak{a}O$, we can simply enumerate representatives of the finite quotient.

We can stay more organized in our task by factoring. If $I \subseteq O$ and $I' \subseteq O$ are invertible integral O-ideals with reduced norms $\mathrm{nrd}(I) = \mathfrak{a}$ and $\mathrm{nrd}(I') = \mathfrak{a}'$ such that $\mathfrak{a} + \mathfrak{a}' = R$, then $I \cap I'$ is an invertible integral O-ideal with reduced norm $\mathfrak{a}\mathfrak{a}'$: this follows by looking locally. Conversely, if J has reduced norm $\mathfrak{a}\mathfrak{a}'$ with $\mathfrak{a} + \mathfrak{a}' = R$, then $I = \mathfrak{a}O + J$ has reduced norm $\mathfrak{a}$. So it suffices to compute the set of ideals whose reduced norm is a power of a prime $\mathfrak{p}$. When $\mathfrak{p}$ is unramified in B and O is $\mathfrak{p}$-maximal for all primes $\mathfrak{p} \mid \mathfrak{a}$, we have more direct control over the set of right ideals as follows.

To compute the set of right O-ideals of reduced norm $\mathfrak{p}^e$ with $\mathfrak{p}$ unramified, using 15.6.6 we compute an embedding $\iota_{\mathfrak{p}} : O \hookrightarrow \mathrm{M}_2(R_{\mathfrak{p}})$, and then we take the set of ideals $I = \mathfrak{p}^e O + \alpha O$ where $\iota_{\mathfrak{p}}(\alpha)$ is congruent to an element in the set (17.6.2) modulo $\mathfrak{p}^e$.

Now we turn to the second step: given invertible right O-ideals I, J, we need to check if $[I] = [J] \in \operatorname{Cls} O$. We first appeal to (17.3.3): we see it is algorithmically equivalent to check if $(J : I)_{\mathsf{L}}$ is principal. The colon ideal itself can be computed using standard methods for pseudobases. To check for principality, we follow Kirschmer–Voight [KV2010, Algorithm 4.10] and employ tactics from lattice reduction.

Algorithm 17.8.1. Let I be an integral R-lattice and suppose that I is principal. Then this algorithm exhibits a generator for I.

1. Compute $\operatorname{nrd}(I) \subset R$ and let $c \in R$ be such that $\operatorname{nrd}(I) = cR$. Initialize $\alpha := 1$. If $c \in R^\times$, return α.
2. View I as a lattice equipped with the absolute reduced norm Q (17.7.11). Reduce I using the LLL algorithm [LLL82]. By exhaustively enumerating short elements in I, find $\gamma \in I$ such that $\operatorname{nrd}(\gamma) = cd$ with $\mathsf{N}(d) < \mathsf{N}(c)$. Let $\alpha := \gamma\alpha/d$, let $I := d\gamma^{-1}I$, and let $c := d$, and return to Step 2.

Proof. In Step 2 we have $\operatorname{nrd}(d\gamma^{-1}I) = d^2/(cd)\operatorname{nrd}(I) = dR$, and so if the algorithm terminates then it gives correct output by Lemma 16.3.8 since $d\gamma^{-1}I = \alpha O$ if and only if $I = (\gamma\alpha/d)O$. The algorithm terminates because at each stage in Step 2, $\mathsf{N}(d) < \mathsf{N}(c)$ a decreasing sequence of positive integers so this is executed only finitely many times, and if I is principal a generator will be found eventually by exhaustive enumeration. □

In practice, Algorithm 17.8.1 runs better than naive enumeration; however, we are unable to prove a rigorous runtime bound. With that proviso, given the generator c as in Step 1, we can measure the value of the LLL-step as follows [KV2010, Lemma 4.11].

Lemma 17.8.2. *There exists $C \in \mathbb{R}_{>0}$ such that for every invertible R-lattice I, the first basis element γ in the LLL-reduced basis in Step 2 of Algorithm 17.8.1 satisfies*

$$|\operatorname{Nm}_{B/\mathbb{Q}}(\operatorname{nrd}(\gamma))|^2 \leq C\mathsf{N}(\operatorname{discrd}(O_{\mathsf{R}}(I))) \cdot \mathsf{N}(I).$$

Proof. The output of the LLL algorithm [LLL82, Proposition 1.9] is an element $\gamma \in I$ which satisfies

$$Q(\gamma) \leq 2^{(4n-1)/2} \operatorname{covol}(I)^{1/(2n)}.$$

We argue as in Proposition 17.7.19:

$$\operatorname{covol}(I) = \mathsf{N}(I) \operatorname{covol}(O)$$

so by (17.7.18)

$$|\operatorname{Nm}_{F/\mathbb{Q}}(\operatorname{nrd}(\gamma))|^2 \leq \frac{1}{n^{2n}} Q(\gamma)^{2n} \leq \frac{2^{(4n-1)n}}{n^{2n}} \mathsf{N}(I) \operatorname{covol}(O)$$

so the result follows taking

$$C = \frac{2^{(4n-1)n}}{n^{2n}} \frac{\operatorname{covol}(O)}{\mathsf{N}(\operatorname{discrd}(O))}.$$

□

Lemma 17.8.2 indicates that, up to a constant depending on the quaternion algebra (choice of a, b), Algorithm 17.8.1 examines elements that are close to being generators.

Now suppose that B is totally definite, so in particular F is totally real. Then we can improve on Algorithm 17.8.1 to provide a rigorous algorithm with an estimate on the running time, as follows [KV2010, Algorithm 6.3]. In this case, we defined the absolute reduced norm Q (17.7.11) independently of choices. For $c \in F^\times$, we define $Q_c(\alpha) := Q(c^{-1}\alpha)$ for $\alpha \in B$.

Algorithm 17.8.3. Let B be a totally definite quaternion algebra. Let $I \subset O$ be an invertible R-lattice. This algorithm determines if I is principal and, if so, returns a generator for I.

1. Compute $\mathrm{nrd}(I) \subseteq R$ and test if $\mathrm{nrd}(I)$ is principal; if not, then return `false`. Otherwise, let $c \in R$ be such that $\mathrm{nrd}(I) = cR$. Initialize $\alpha := 1$.
2. Determine if there exists a unit $u \in \mathbb{Z}_F^\times$ such that $v(uc) > 0$ for all real places v. If so, let $c := uc$; if not, return `false`.
3. For each totally positive unit $z \in R_{>0}^\times / R^{\times 2}$:
   a. Let α be a shortest vector of the lattice I with respect to the rational quadratic form Q_{ucz}.
   b. If $\varphi_{ucz}(\alpha) = n$ then return `true` and the element α.
4. Return `false`.

Remark 17.8.4. Note that if $F = \mathbb{Q}$ then in Steps 3, 4 we have $z = u = 1$. Hence the algorithm simply looks for a shortest vector in the lattice I (with respect to the reduced norm form).

Proof of correctness of Algorithm 17.8.3. In Step 1, if I is principal, then $\mathrm{nrd}(I)$ is generated by a totally positive element uc where $u \in R^\times$. Then Lemma (16.3.8) implies that $\alpha \in I$ generates I if and only if $\mathrm{nrd}\,\alpha = ucz$ for some $z \in R_{>0}^\times$. To find such an element α, we only need to search for elements of norm ucz where z runs through some arbitrary transversal of $R_{>0}^\times / R^{\times 2}$.

Let $z \in R_{>0}^\times$ and $\alpha \in I$. Then $\mathrm{nrd}\,\alpha \in \mathrm{nrd}\,I = (ucz)R$, so $m = (ucz)^{-1}(\mathrm{nrd}\,\alpha) \in R$ is totally positive. The arithmetic-geometric mean inequality implies

$$n \leq n\,\mathrm{Nm}_{F/\mathbb{Q}}(m)^{1/n} \leq \mathrm{Tr}_{F/\mathbb{Q}}\, m = Q_{ucz}(\alpha).$$

Moreover, equality holds throughout if and only if $1 = \mathrm{Nm}_{F/Q}\, m$ and $v(m) = v'(m)$ for all real places v, v', so equality holds if and only if $m = 1$. Hence $\mathrm{nrd}(\alpha) = ucz$ if and only if $\alpha \in I$ satisfies $Q_{ucz}(\alpha) = n$ is a shortest vector. □

Algorithm 17.8.3 runs in deterministic polynomial time in the size of the input for a fixed totally real field F [KV2010, Proposition 6.9]: Steps 1,2 involve some precomputation which can be done in constant time for fixed F, and the shortest vector computation can be performed in constant time for a fixed dimensional lattice by employing the LLL-algorithm [LLL82] (see e.g., Kannan [Kan87, Section 3]).

17.8.5. By the surjective map $\mathrm{Cls}_{\mathsf{R}} O \to \mathrm{Typ}\, O$ in (17.4.13), these algorithms also give representatives for $\mathrm{Typ}\, O$: they are the set of orders $\{O_{\mathsf{L}}(I) : [I] \in \mathrm{Cls}_{\mathsf{R}} O\}$, since $O_{\mathsf{L}}(I) \simeq O_{\mathsf{L}}(I')$ for I, I' invertible right O-ideals if and only if $O_{\mathsf{L}}(I) = \alpha^{-1} O_{\mathsf{L}}(I')\alpha = O_{\mathsf{L}}(\alpha^{-1} I')$ if and only if $[I] = [I']$. In other words, we need only check equality of the left orders.

Chapter 20

Integral representation theory

20.5 Local Jacobson radical

Theorem 20.5.1. *Let $\phi\colon O \to O/\mathfrak{p}O$ be reduction modulo $\mathfrak{p}$. Then*

$$\operatorname{rad} O = \phi^{-1}(\operatorname{rad} O/\mathfrak{p}O) \supseteq \mathfrak{p}O,$$

and $(\operatorname{rad} O)^r \subseteq \mathfrak{p}O$ for some $r > 0$.

Proof. We follow Reiner [Rei2003, Theorem 6.15]. We first show $\operatorname{rad} O \supseteq \mathfrak{p}O$. Let $M = Ox$ be a simple left O-module 20.4.2; then either $\mathfrak{p}M = M$ or $\mathfrak{p}M = \{0\}$. The former implies the latter by Nakayama's lemma. Thus by definition, we conclude

$$\mathfrak{p}O \subseteq \operatorname{rad} O. \tag{20.5.2}$$

Next, we have a surjective homomorphism $\phi\colon O \to O/\mathfrak{p}O$. By Corollary 20.4.10, we have $\phi(\operatorname{rad} O) \subseteq \operatorname{rad}(O/\mathfrak{p}O)$ and an induced map

$$\phi\colon O/\operatorname{rad} O \to (O/\mathfrak{p}O)/(\operatorname{rad} O/\mathfrak{p}O).$$

At the same time, we have an surjective map $\psi\colon O/\mathfrak{p}O \to O/\operatorname{rad} O$ by (20.5.2). By Lemma 20.4.7, $O/\operatorname{rad} O$ is Jacobson semisimple, so by Corollary 20.4.10 again, $\psi(\operatorname{rad}(O/\mathfrak{p}O)) = \{0\}$. Thus ψ factors through a surjective map

$$\psi\colon (O/\mathfrak{p}O)/\operatorname{rad}(O/\mathfrak{p}O) \to O/\operatorname{rad} O.$$

Putting ϕ and ψ together as surjective homomorphisms between finite-dimensional k-vector spaces, we conclude that both are isomorphisms, and $\operatorname{rad} O = \phi^{-1}(\operatorname{rad} O/\mathfrak{p}O)$.

Finally, $\operatorname{rad} O/\mathfrak{p}O$ is a nilpotent ideal by Lemma 7.4.8, so $(\operatorname{rad} O/\mathfrak{p}O)^r = \{0\}$ for some $r > 0$. Thus $\phi((\operatorname{rad} O)^r) = \{0\}$, and $(\operatorname{rad} O)^r \subseteq \mathfrak{p}O$. □

Corollary 20.5.5. *Let $I \subseteq O$ be a two-sided ideal. Then the following are equivalent:*

(a) $I \subseteq \operatorname{rad} O$*;*
(b) $I^r \subseteq \operatorname{rad} O$ *for some $r > 0$; and*

(c) *I is topologically nilpotent.*

Proof. We follow Reiner [Rei2003, Exercise 39.1, Exercise 6.3]. The implication (i) $\Rightarrow$ (ii) is immediate. For (ii) $\Rightarrow$ (iii), by Theorem 20.5.1, we have $(\operatorname{rad} O)^s \subseteq \mathfrak{p}O$ for some $s > 0$. Therefore if $I^r \subseteq \operatorname{rad} O$ then $I^{rs} \subseteq (\operatorname{rad} O)^s \subseteq \mathfrak{p}O$. Finally (iii) $\Rightarrow$ (i), suppose $I^r \subseteq \mathfrak{p}O$ for some $r > 0$. Let $\phi\colon O \to O/\mathfrak{p}O$ be the reduction map. Then $\phi(I)$ is a nilpotent ideal in $O/\mathfrak{p}O$, so $\phi(I) \subseteq \operatorname{rad}(O/\mathfrak{p}O)$; by Theorem 20.5.1, $I \subseteq \phi^{-1}(\operatorname{rad} O/\mathfrak{p}O) = \operatorname{rad} O$. □

20.7 Local integral representation theory

Let $J = \operatorname{rad} O$; then O/J is a semisimple k-algebra, by Corollary 20.5.2. We now follow Hijikata–Nishida [HN94, §1].

Lemma 20.7.10. *Let $I \subseteq B$ be a left O-submodule.*

(a) *I has a unique maximal O-submodule $I' \subseteq I$ if and only if I/JI is simple as a O/J-module. In this situation, I is indecomposable and $I' = JI$.*
(b) *If I is projective, then it has a unique maximal O-submodule if and only if it is indecomposable.*

Proof. Statement (a) follows since O/J is semisimple. Statement (b) follows from Lemma 20.6.8. □

Corollary 20.7.11. *Let M be a left O-module with a unique maximal O-submodule, and let $V := M \otimes_R F$. Suppose that $\ell(V) \geq \ell(Be)$ for all primitive idempotents e of O. Then M is projective and indecomposable.*

Proof. By Lemma 20.7.10(a), M/JM is simple and therefore $M/JM \simeq I/JI$ for some projective indecomposable I by Lemma 20.6.8. Write $I = Oe$ where e is a primitive idempotent, so we have a O-module homomorphism $Oe \to I/JI \simeq M/JM$. Choosing a lift of the image of e, we get a map $\phi\colon Oe \to M$. By Nakayama's lemma, ϕ is surjective. Therefore induced map $\phi_F\colon Be \to V$ is a surjective F-algebra homomorphism. But by hypothesis $\ell(Be) \geq \ell(V)$, so ϕ_F is injective. Thus ϕ is injective and thus gives an isomorphism of M with a projective indecomposable module. □

Corollary 20.7.12. *Let M be a finitely generated left O-module. The following are equivalent:*

(a) *M has a unique composition series;*
(b) *$M \supseteq JM \supseteq J^2M \supseteq \dots$ is a composition series; and*
(c) *$J^iM/J^{i+1}M$ is simple for all $i \geq 0$.*

If these equivalent conditions hold, then $V := M \otimes_R F$ is simple as a B-module.

Proof. The equivalences are immediate from Lemma 20.7.10. For the second statement, suppose V is not simple, with $V \supsetneq W \supsetneq \{0\}$. We consider the O-submodule $M \cap W \subseteq M$; since $\bigcap_{i=1}^{\infty} J^i M = \{0\}$ and nontriviality, there exists $r \geq 0$ such that $M \cap W \subseteq J^r M$ but $M \cap W \nsubseteq J^{r+1} M$. Now consider the inclusion

$$J^{r+1} M \subsetneq J^{r+1} M + (M \cap W) \subsetneq J^r M, \tag{20.7.13}$$

the strictness of inclusions following the hypotheses. This contradicts uniqueness of the composition series. □

20.7.14. Suppose that M has a unique composition series. Then $\mathfrak{p}M \subseteq M$ is a submodule, so by uniqueness $\mathfrak{p}M = J^t M$ for some $t \geq 1$. We call t the **period** of the composition series.

20.7.15. Let $I \subseteq B$ be a left O-module. Suppose that I/JI is simple. Let $I' \supseteq I$ be a minimal O-supermodule.

We claim that if I is the minimal O-supermodule of JI, then I is the maximal O-submodule of I'. Indeed, $JI' \subsetneq I'$ so by minimality, $JI' \subseteq I$; since I/JI is simple, we have either $JI' = I$ or $JI' = JI$. We rule out the former because then $I'/JI' = I'/JI \simeq I'/I \oplus I/JI$ is decomposable, so I is not the minimal O-supermodule.

Chapter 21

Hereditary and extremal orders

21.5 Classification of local hereditary orders

We provide a proof of the following result.

Theorem 21.5.1. *Let R be a complete DVR with $F = \operatorname{Frac} R$. Let B be a finite-dimensional F-algebra, and let $O \subseteq B$ be an R-order. Let $J = \operatorname{rad} O$. Then the following are equivalent, along with the conditions′ where 'left' is replaced by 'right':*

(i) *O is extremal;*
(ii) *Every projective indecomposable left O-submodule $P \subseteq B$ is the minimum O-supermodule of JP;*
(iii) *Every projective indecomposable left O-module P has a unique composition series;*
(iv) *Every projective indecomposable left O-module P has a unique composition series consisting of projectives;*
(v) *O is hereditary;*
(vi) *J is projective as a left O-module;*
(vii) *If P is a projective indecomposable left O-module, then JP is also projective indecomposable; and*
(viii) *J is invertible as a (sated) two-sided O-ideal.*

Proof. We follow Hijikata–Nishida [HN94, §1].

(i) $\Rightarrow$ (ii). Let $P = Oe \subseteq O \subseteq B$ (see 20.6.4) and suppose that (ii) does not hold for P. Then there is a minimal O-supermodule $M \supsetneq JP = Je$ such that $M \neq P$. We cannot have $M \subseteq P = Oe$ by minimality, so $M \not\subseteq O$ by projection onto Be. Now $M + J \supsetneq J$ is a minimal O-supermodule because $(M + J)/J \simeq M/Je$ and $M \supseteq Je$ is minimal. Therefore by 20.6.12, we have $J(M + J) \subseteq J$, i.e., $M + J \subseteq O_{\mathsf{R}}(J)$. But $M + J \not\subseteq O$, so $O_{\mathsf{R}}(J) \neq O$, contradicting Proposition 21.2.3.

(ii) $\Rightarrow$ (iii). Among the projective indecomposables $P = Oe$, we choose P so that $\ell(V)$ is maximal, where $V = FP$. By (ii), there exists $P \supsetneq P_1$ a minimal O-supermodule. Then $P = JP_1$ is the maximum O-submodule of P_1. By Corollary 20.7.11, P_1 is projective indecomposable since $\ell(V)$ is maximal, and repeating the process we get a period $P \subseteq P_1 \subseteq \cdots \subseteq P_r$ where $P_r \subseteq P$ as left O-modules,

and $P_{r-1} = JP_r$, and P has a unique composition series. Therefore V is a simple B-module, and $\ell(V) = 1$. Since $\ell(V) \geq \ell(Be)$ for all e, we conclude $\ell(Be) = 1$ for all idempotents e.

Now let P be a projective indecomposable. But we just showed that $\ell(FP) \geq \ell(Be) = 1$ for all idempotents e, so the same argument applying Corollary 20.7.11 in the previous paragraph works for P.

(iii) $\Rightarrow$ (iv). The same argument as in the previous implication applies.

(iv) $\Rightarrow$ (v). Let I be an indecomposable left O-ideal; writing I as a direct sum of indecomposables, we may suppose I is indecomposable. The B-module FI has a simple quotient. By (iv), I has unique composition series, so $FI = Be$ is simple. We therefore have an exact sequence of B-modules

$$0 \to \ker \phi \to FI \xrightarrow{\phi} Be \to 0$$

which intersectiong with O gives an exact sequence of O-modules

$$0 \to I \cap \ker \phi \to I \xrightarrow{\phi|_I} \phi(I) \to 0.$$

We have $\phi(I) \subseteq I$; by (iv), iterating, we conclude $\phi(I)$ is projective and so is a direct summand. But I is indecomposable, so $I \simeq \phi(I)$ and I is projective.

(v) $\Rightarrow$ (vi). Immediate.

(vi) $\Rightarrow$ (iv). Let $P \simeq Oe$ be a projective indecomposable; then $JP = Je$ is the maximum O-submodule. By (vi), JP is also projective; so we can iterate to a unique composition series.

(vi) $\Rightarrow$ (vii). We have $P = Oe$ for an idempotent e, so $JP = Je$ and $J = Je \oplus J(1-e)$.

(vii) $\Rightarrow$ (vi). Write $O \simeq \bigoplus_i P_i^{\oplus n_i}$ as a finite direct sum of indecomposable left O-ideals P_i. Then $J \simeq \bigoplus (JP_i)^{\oplus n_i}$. By (vi), each JP_i is projective indecomposable, so isomorphic to $P_{\tau(i)}$ for some $\tau(i)$. Thus J is projective.

(vii) $\Rightarrow$ (i). We continue with the previous paragraph, so we know (vi) and hence (iv). Therefore $JP_i \subseteq P_i$ is the unique projective indecomposable, and so τ must be a permutation of the indices. Therefore by 20.6.6, $O_{\mathsf{L}}(J) = O$. It follows that O is extremal, by Proposition 21.2.3.

For the left-right symmetry in (i)–(vii), we note that extremal (i) is left-right symmetric, and we can repeat all of the above arguments on the right instead.

(i) + (vi) + (vi′) $\Leftrightarrow$ (viii): by Theorem 20.3.2, we have $O_{\mathsf{L}}(J) = O_{\mathsf{R}}(J) = O$ and O projective as a two-sided O-ideal if and only if J is invertible as a (sated) two-sided O-ideal. □

Chapter 24

Quaternion orders and ternary quadratic forms

24.6 Twisting and final bijection

Remark 24.6.1. When $2 \in R^\times$ (and more generally for certain schemes with 2 invertible), Balmer–Calmès [BC2012] develop a categorical theory of *lax-similitude* that coincides with our notion of twisting.

Part III

Analysis

Chapter 26

Classical zeta functions

26.2 Analytic class number formula

We provide a proof of the following technical result.

Theorem 26.2.19. *Let $X \subseteq \mathbb{R}^n$ be a cone. Let $N : X \to \mathbb{R}_{>0}$ be a function satisfying*

$$N(tx) = t^n N(x) \quad \text{for all } x \in X,\ t \in \mathbb{R}_{>0}.$$

Suppose that

$$X_{\leq 1} := \{x \in X : N(x) \leq 1\} \subseteq \mathbb{R}^n \tag{26.2.20}$$

is a bounded subset with volume $\mathrm{vol}(X_{\leq 1})$*. Let $\Lambda \subseteq \mathbb{R}^n$ be a (full) $\mathbb{Z}$-lattice in $\mathbb{R}^n$, and let*

$$\zeta_{\Lambda,X}(s) := \sum_{\lambda \in X \cap \Lambda} \frac{1}{N(\lambda)^s}.$$

Then $\zeta_{\Lambda,X}(s)$ converges for $\mathrm{Re}\, s > 1$ *and has a simple pole at $s = 1$ with residue*

$$\zeta^*_{\Lambda,X}(1) = \lim_{s \searrow 1} (s-1)\zeta_{\Lambda,X}(s) = \frac{\mathrm{vol}(X_{\leq 1})}{\mathrm{covol}(\Lambda)}.$$

Proof. We have

$$\mathrm{vol}(X_{\leq 1}) = \lim_{t\to\infty} \frac{\mathrm{vol}(\Lambda)}{t^n} \#(\tfrac{1}{t}\Lambda \cap X_{\leq 1}) = \mathrm{vol}(\Lambda) \lim_{t\to\infty} \frac{\#(\frac{1}{t}\Lambda \cap X_{\leq 1})}{t^n}.$$

By the homogeneity condition on N,

$$\#(\tfrac{1}{t}L \cap X_{\leq 1}) = \#(L \cap X_{\leq t^n}).$$

Label the points of $\Lambda \cap X = \{\lambda_1, \lambda_2, \ldots\}$ so that $N(\lambda_1) \leq N(\lambda_2) \leq \ldots$; we claim that

$$\lim_{k\to\infty} \frac{k}{N(\lambda_k)} = \frac{\mathrm{vol}(X_{\leq 1})}{\mathrm{covol}(\Lambda)} = v.$$

To prove this claim, write $b(x) = \#(\Lambda \cap X_{\leq x^n})$ for $x > 0$. From the previous paragraph, $b(x)/x^n \to v$. Let $x_k^n = N(\lambda_k)$ for $k \geq 1$. Then for all $\epsilon > 0$, we have $b(x_k - \epsilon) < k \leq b(x_k)$. So

$$\frac{b(x_k - \epsilon)}{(x_k - \epsilon)^n}\left(1 - \frac{\epsilon}{x_k^n}\right) < \frac{k}{N(\lambda_k)} \leq \frac{b(x_k)}{x_k^n}.$$

Taking the limit as $k \to \infty$, since $x_k^n \to \infty$ we have $\lim_{k\to\infty} k/N(\lambda_k) = v$ by the sandwich theorem, proving the claim.

Now, for all $\epsilon > 0$, there exists K such that for $k \geq K$ we have

$$(v - \epsilon)^s \frac{1}{k^s} < \frac{1}{N(\lambda_k)^s} < (v + \epsilon)^s \frac{1}{k^s};$$

summing over $k \geq K$, we multiply by $(s - 1)$ and let $s \to 1^+$ to get

$$(v - \epsilon)\zeta_{\mathbb{Q}}^*(1) \leq \zeta_{\Lambda,X}^*(1) \leq (v + \epsilon)\zeta_{\mathbb{Q}}^*(1)$$

where $\zeta_{\mathbb{Q}}^*(1) = 1$ is the residue of the Riemann zeta function (25.2.4). Now letting $\epsilon \to 0$,

$$\zeta_{\Lambda,X}^*(1) = v = \frac{\mathrm{vol}(X_{\leq 1})}{\mathrm{covol}(\Lambda)}.$$ □

Chapter 30

Optimal embeddings

30.10 Algorithmic aspects

In Lemma 30.6.17, we computed local embedding numbers for Eichler orders when the residue field has odd cardinality. Suppose now that R is local, with residue field of *even* cardinality. Then the calculation of the local embedding number is quite painful and as such is not conducive to a formula that is both compact and intelligible; nevertheless, the representation in Proposition 30.6.12(c) shows that the local embedding number is effectively computable.

30.10.1. We can improve upon the brute force method of calculating $m(S, O)$ by calculating $M(s)$ more directly as follows. The map $S/2S \to S/2S$ given by $x \mapsto x^2 - tx$ is $\mathbb{F}_2$-linear, and therefore by linear algebra over $\mathbb{F}_2$ one can compute all solutions to $f(x) = x^2 - tx + n \equiv 0 \pmod{\mathfrak{p}^f}$ if $f \leq \mathrm{ord}_{\mathfrak{p}}(2)$. For each of these solutions, one can then use Hensel lifting to test which among them give rise to solutions modulo $\mathfrak{p}^f$ for $f \leq \mathrm{ord}_{\mathfrak{p}}(4)$; and then Hensel's lemma implies that each such solution lifts to a unique solution modulo $\mathfrak{p}^f$ whenever $f > \mathrm{ord}_{\mathfrak{p}}(4)$.

Part IV

Geometry and topology

Chapter 33

Hyperbolic plane

33.3 Upper half-plane

We provide a further elaboration of the proof of the following theorem.

Theorem 33.3.14. *The group* $\mathrm{PSL}_2(\mathbb{R})$ *acts on* H^2 *via orientation-preserving isometries, i.e.,* $\mathrm{PSL}_2(\mathbb{R}) \hookrightarrow \mathrm{Isom}^+(\mathsf{H}^2)$.

Proof elaboration. Let υ be a (piecewise continuously differentiable) path in H^2 given by $z(t)$ for $t \in [0,1]$; then by definition

$$\ell(\upsilon) = \int_0^1 \left|\frac{\mathrm{d}z}{\mathrm{d}t}\right| \frac{\mathrm{d}t}{\operatorname{Im} z(t)}.$$

The path $g\upsilon$ is given by $z'(t) = g(z(t))$, and by the chain rule

$$\begin{aligned}\ell(g(\upsilon)) &= \int_0^1 \left|\frac{\mathrm{d}z'(t)}{\mathrm{d}t}\right| \frac{\mathrm{d}t}{\operatorname{Im} z'(t)} \\ &= \int_0^1 \left|\frac{\mathrm{d}g(z(t))}{\mathrm{d}z}\frac{\mathrm{d}z(t)}{\mathrm{d}t}\right| \frac{\mathrm{d}t}{\operatorname{Im} g(z(t))} \\ &= \int_0^1 \left|\frac{\mathrm{d}z(t)}{\mathrm{d}t}\right| \frac{\mathrm{d}t}{\operatorname{Im} z(t)},\end{aligned}$$

the latter equality from (33.3.14). The fact that lengths are preserved immediately implies the invariance of the hyperbolic metric. □

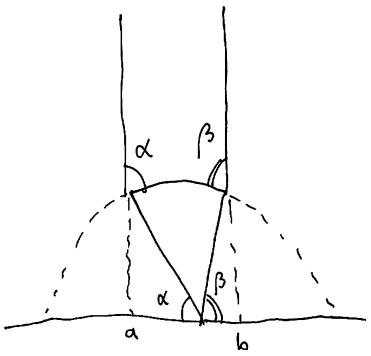
33.6 Hyperbolic area and the Gauss–Bonnet formula

We prove the Gauss–Bonnet formula.

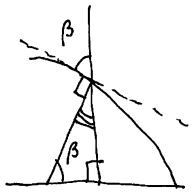
Theorem 33.6.1 (Gauss–Bonnet formula)**.** *Let T be a hyperbolic triangle with angles α, β, γ. Then*

$$\mu(T) = \pi - (\alpha + \beta + \gamma).$$

Proof. We first consider the case where T has at least one vertex in $\operatorname{bd}\mathbf{H}^2$. Since the group $\mathrm{PSL}_2(\mathbb{R})$ acts transitively on the boundary $\operatorname{bd}\mathbf{H}^2$, by applying an element of $\mathrm{PSL}_2(\mathbb{R})$, we may suppose this vertex is ∞ (without changing the area). Then there is a diagram as follows:



The fact that the angles are duplicated along the real axis is explained by the following diagram:



The semicircular segment lies along a circle with some radius c; applying the isometry

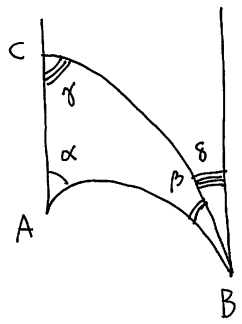
$$g = \begin{pmatrix} 1/\sqrt{c} & 0 \\ 0 & \sqrt{c} \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R})$$

with the effect $g(z) = z/c$, and then translating, we may suppose that this segment lies along the unit circle. Then

$$\begin{aligned} \iint_T \frac{\mathrm{d}x\mathrm{d}y}{y^2} &= \int_a^b \int_{\sqrt{1-x^2}}^{\infty} \frac{\mathrm{d}y}{y^2}\mathrm{d}x = \int_a^b \frac{-1}{y}\Big|_{\sqrt{1-x^2}}^{\infty}\mathrm{d}x \\ &= \int_a^b \frac{\mathrm{d}x}{\sqrt{1-x^2}} = \int_{\pi-\alpha}^{\beta} -\mathrm{d}\theta = \pi - (\alpha+\beta) \end{aligned}$$

where we make the substitution $x = \cos\theta$. If T has two or three vertices in $\operatorname{bd}\mathbf{H}^2$, the same argument applies, but with possibly $\alpha = 0$ (and $a = -1$) or $\beta = 0$ (and $b = 1$).

So we are left with the case where T has all vertices in $\mathbf{H}^2$. We then consider the following diagram:



The triangle with vertices B, C, ∞ has area $\pi - (\delta + (\pi - \gamma)) = \gamma - \delta$, and the triangle with vertices A, B, ∞ has area $\pi - \alpha - \beta - \delta$, so our triangle with vertices A, B, C has area equal the difference,

$$\pi - (\alpha + \beta + \delta) - (\gamma - \delta) = \pi - (\alpha + \beta + \gamma). \qquad \square$$

Part V

Arithmetic geometry

Chapter 40

Classical modular curves and modular forms

40.3 Classical modular forms

We prove (most of) the following proposition.

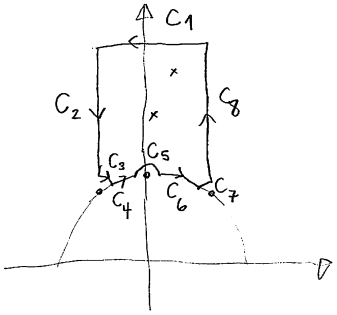
Proposition 40.3.4. *Let $f : \mathsf{H}^2 \to \mathbb{C}$ be a meromorphic modular form of weight k, not identically zero. Then*

$$\operatorname{ord}_\infty(f) + \sum_{\Gamma z \in \Gamma\backslash \mathsf{H}^2} \frac{1}{e_z} \operatorname{ord}_z(f) = \frac{k}{12} \tag{40.3.5}$$

where $e_z = \#\operatorname{Stab}_\Gamma(z)$.

The sum (40.3.5) has only finitely many terms, by 40.3.1, and the stabilizers are given in 40.3.2.

Proof. See Serre [Ser73, §3, Theorem 3]. To prove this theorem, we perform a contour integration $\dfrac{1}{2\pi i}\dfrac{\mathrm{d}f}{f}$ on the boundary of ⌑. More precisely, first suppose that f has neither zero nor pole on the boundary of ⌑ except possibly at $i, \omega, -\omega^2$. We consider the contour C containing all zeros or poles of f in int(⌑).



By the argument principle,

$$\frac{1}{2\pi i}\int_C \frac{\mathrm{d}f}{f} = \sum_{z\in \mathrm{int}(\square)} \mathrm{ord}_z(f). \tag{40.3.6}$$

We write C as the sum of several contours as indicated. In the change of variable $z \mapsto q = e^{2\pi i z}$, the contour C_1 transforms into a circle centered at $q = 0$ with negative orientation whose only enclosed zero or pole is ∞. Thus

$$\frac{1}{2\pi i}\int_{C_1} \frac{\mathrm{d}f}{f} = -\mathrm{ord}_\infty(f). \tag{40.3.7}$$

We have $T^{-1}(C_8) = C_2$ with opposite orientation; since $f(z+1) = f(z)$, these contributions cancel. On C_3, as the radius of this arc of a circle tends to 0,

$$\frac{1}{2\pi i}\int_{C_3} \frac{\mathrm{d}f}{f} \to \frac{1}{2\pi i}\left(\frac{-\pi i}{3}\right)\mathrm{ord}_\omega(f) = -\frac{1}{6}\mathrm{ord}_\omega(f) \tag{40.3.8}$$

as the angle formed with ω by the endpoints of C_2 is $\pi/3$ (Exercise 40.1). Similarly,

$$\frac{1}{2\pi i}\int_{C_5} \frac{\mathrm{d}f}{f} \to -\frac{1}{2}\mathrm{ord}_i(f) \quad \text{and} \quad \frac{1}{2\pi i}\int_{C_7} \frac{\mathrm{d}f}{f} \to -\frac{1}{6}\mathrm{ord}_{-\omega^2}(f). \tag{40.3.9}$$

Finally, $S(C_6) = C_4$ with *opposite* orientation; but now $f(Sz) = z^k f(z)$ so

$$\frac{\mathrm{d}f(Sz)}{\mathrm{d}z} = kz^{k-1}f(z) + z^k\frac{\mathrm{d}f(z)}{\mathrm{d}z}$$

and hence

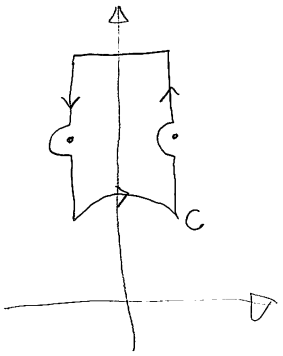
$$\frac{\mathrm{d}f(Sz)}{f(Sz)} = k\frac{\mathrm{d}z}{z} + \frac{\mathrm{d}f(z)}{f(z)},$$

so

$$\begin{aligned}\frac{1}{2\pi i}\int_{C_4\cup C_6}\frac{\mathrm{d}f}{f} &= \frac{1}{2\pi i}\int_{C_4}\frac{\mathrm{d}f}{f} - \frac{1}{2\pi i}\int_{C_4}\left(k\frac{\mathrm{d}z}{z} + \frac{\mathrm{d}f}{f}\right)\\ &= \frac{1}{2\pi i}\int_{C_4} -k\frac{\mathrm{d}z}{z} \to \frac{-k}{2\pi i}\left(\frac{-\pi i}{6}\right) = \frac{k}{12}\end{aligned} \tag{40.3.10}$$

as the angle formed with 0 is $\pi/6$. Summing, we obtain the result.

If f has a zero or pole on the boundary of $\square$, we repeat the same argument with a contour modified as follows:



The details are omitted. □

Appendix A

Hints and comments on exercises

1.2. For part (a), see May [May66, p. 290].

1.3(b). The minimal polynomial is irreducible, because D is a division algebra. The minimal polynomial divides the characteristic polynomial of degree 3 which factors over $\mathbb{R}$, so the minimal polynomial has degree at most 2. If the minimal polynomial has degree 2 (irreducible), then since every irreducible factor of the characteristic polynomial is a factor of the minimal polynomial, we conclude that the characteristic polynomial has even degree, a contradiction. So the minimal polynomial has degree 1, and this implies that $\alpha \in \mathbb{R}$ for all $\alpha \in D$, contradicting $D \neq \mathbb{R}$.

2.3. For such a map, we must have $ij \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Check that the four matrices are linearly independent, so the map is an F-linear isomorphism. Then, using the universal property of algebras given by generators and relations, show that the given matrices satisfy the relations in B, so the map is an F-algebra homomorphism.

2.5. Try $j' = i'j - ji'$, and show that $j'i' + i'j' = 0$. If $(j')^2 = 0$, consider instead $j' = i'k - ki'$.

2.6. Use Exercise 2.4.

2.8. Use Exercise 2.4(c) and show that the center over $\overline{F}$ has dimension 1 or compute directly with $\alpha i - i\alpha = \alpha j - j\alpha = 0$ for $\alpha = t + xi + yj + zk \in B$.

2.12. B acts on itself by left multiplication, which in the standard basis gives a map

$$B \hookrightarrow \mathrm{M}_4(F)$$
$$t + xi + yj + zk \mapsto \begin{pmatrix} t & ax & by & -abz \\ x & t & -bz & by \\ y & az & t & -ax \\ z & y & -x & t \end{pmatrix}.$$

2.19. Use the left regular representation either to F or a subfield K, and use the block matrix determinant. See also Aslaksen [Asl96].

3.3. The standard involution on $F \times F$ is given by $(x, y) \mapsto (y, x)$. (Note that F embeds diagonally in $F \times F$, so $a \mapsto (a, a)$, and so F is indeed fixed under this map.)

3.6. $g \mapsto g^{-1}$ is a standard involution if and only if G has exponent 2 and char $F = 2$ (so the standard involution is the identity and $F[G]$ is commutative).

3.8. Let $i, j \in K \setminus F$. Then $i + j$ satisfies a quadratic polynomial, but $ji = ij$, so we have $(i + j)^2 = i^2 + 2ij + j^2 \in F(i + j) + F$ hence $2ij = c(i + j) + d$ with $c, d \in F$: but then since $2 \neq 0$, we have $2i \neq c \in F$ so $j = (ci + d)/(2i - c) \in K$.

3.9. For part (a), Suppose B has degree 2. Choose a basis $1, x_2, \ldots, x_m$. For each i, the quadratic F-algebras $F[x_i]$ have a standard involution, and so extending by F-linearity we obtain a map $\bar{}: B \to B$. For $x \in B$, let $t(x) = x + \overline{x}$ and $n(x) = x\overline{x}$.

By induction and F-linearity, we may suppose $1, x, y$ are F-linearly independent. Suppose $(x+y)^2 - s(x+y) + m = 0$ with $s, m \in F$. We show that $s = t(x) + t(y)$. We have

$$\begin{aligned}(x - y)^2 &= x^2 - (xy + yx) + y^2 = 2(x^2 + y^2) - s(x + y) + m \\ &= (2t(x) - s)x + (2t(y) - s)y + (m - 2n(x) - 2n(y))\end{aligned}$$

But $(x - y)^2 \in F(x - y) + F$ so $2t(x) - s = s - 2t(y)$, i.e. $2s = 2t(x) + 2t(y)$. Since char $F \neq 2$, we have $s = t(x) + t(y)$ as desired.

To conclude, we show $\overline{xy} = \overline{y}\,\overline{x}$. We may suppose $xy \notin F$. We verify that both $(xy)^2 - (xy + \overline{y}\,\overline{x})xy + (\overline{y}\,\overline{x})(xy) = 0$ and $(xy)^2 - (xy + \overline{xy})xy + \overline{xy}(xy) = 0$, so the result follows by uniqueness of the minimal polynomial.

For part (b), by the uniqueness of the standard involution, we have $\overline{x} = x + 1$ if $x \notin F$. But then if $1, x, y$ are F-linearly independent we have $x + y + 1 = \overline{x + y} = \overline{x} + \overline{y} = (x + 1) + (y + 1) = x + y$, a contradiction. So $\dim_{\mathbb{F}_2} B \leq 2$. Since a Boolean ring consists of idempotents, we have $B = \mathbb{F}_2$ or $B \cong \mathbb{F}_2^2$.

3.10. Under right multiplication by $B = \mathrm{M}_n(F)$, a matrix is nothing other than the direct sum of its rows, so in particular, the characteristic polynomial of right multiplication by $A \in \mathrm{M}_n(F)$ acting on $\mathrm{M}_n(F)$ will be the nth power of the usual characteristic polynomial of A acting on row vectors $V \cong F^n$. (In the language of Chapter 7, $B = \mathrm{M}_n(F)$ as a right B-module is $B \cong V^n$ where $V \cong F^n$ is the unique simple right B-module.)

3.12. By F-linearity, it suffices to verify these statements on a basis for B.

3.13. The class equation reads

$$q^4 - 1 = (q - 1) + m(q^2 + 1)$$

for some $m \in \mathbb{Z}_{\geq 0}$. Thus $(q^2 + 1) \mid (q - 1)$, a contradiction.

This argument can be generalized in a natural way to prove Wedderburn's theorem in full: see Schue [Schu88], for example.

3.15. See van Praag [vPr68, vPr02].

4.6. For part (c), by the transitivity of trace, we may assume K/F is purely inseparable and $[K : F]$ is a multiple of p. But then all roots of the minimal polynomial of $x \in K$ over F are equal, so the characteristic polynomial of multiplication by $x \in K$ has all roots equal and there are a multiple of p of them and thus the trace is zero.

For part (d), $\mathrm{tr}((a + b\sqrt{5})^2) = 2(a^2 + 5b^2)$ and

$$\mathrm{tr}((a + b\alpha + c\alpha^2)^2) = 2(a^2 - 2ab + 10ac + 5b^2 - 8bc + 13c^2).$$

4.7. Choosing bases for V, V' and writing f as a matrix $A \in \mathrm{GL}_n(F)$ in these bases, we find that $ux^t[T]x = x^t(A^t[T']A)x$ for all $x \in V \simeq F^n$, so $u[T] = A^t[T']A$. Taking determinants, we find $\det T' = u^n \det T \in F/F^{\times 2}$.

4.8. See Lam [Lam2005, Chapter X] for more on Pfister forms; in particular, for (c) see Lam [Lam2005, Theorem X.1.7].

5.3. The implication (vi) $\Rightarrow$ (v) follows similarly: if $a \in F^{\times 2}$ then already $\langle a \rangle$ represents 1; if $a \notin F^{\times 2}$ and we have $x^2 - ay^2 = b$ then either $x = 0$, in which case $\langle a, b \rangle$ is isotropic and thus represents 1, or $x \neq 0$ and then $a(y/x)^2 + b(1/x)^2 = 1$ as desired.

5.4. If $B = \left(\frac{a,b}{\mathbb{F}_q}\right)$ then $K = \mathbb{F}_q(i) \cong \mathbb{F}_{q^2}$ and $\mathrm{Nm} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ is surjective so $b \in \mathrm{Nm}_{K/F}(K^\times)$.

5.9. See Lam [Lam2005, Examples III.2.12–13]. For the first, exhibit an explicit isometry $\langle 1, 1, 1 \rangle \cong \langle 2, 3, 6 \rangle$. For the second, note that $\langle 2, 5, 10 \rangle$ represents 7 but $\langle 1, 1, 1 \rangle$ does not (by showing $x^2 + y^2 + z^2 + w^2 \not\equiv 0 \pmod 8$ for $x, y, z, w \in \mathbb{Z}$ with $\gcd(x, y, z, w) = 1$); or note that $\langle 1, 1, 1 \rangle$ represents 1 but $\langle 2, 5, 10 \rangle$ (looking modulo 5, and arguing similarly).

5.11. Indeed, for any $x, y, z \in V$, by Clifford multiplication we have

$$\begin{aligned}(x + yz)(\overline{x + yz}) = (x + yz)(x + zy) &= q(x) + yzx + xzy + q(y)q(z) \\ &= q(x) + q(y)q(z) - T(x, y)z + T(x, z)y + T(y, z)x.\end{aligned}$$

Suppose that $\bar{\ }: \mathrm{Clf}(Q) \to \mathrm{Clf}(Q)$ is a standard involution and $\mathrm{rk}(V) \geq 3$. If x, y, z are F-linearly independent, then we must have $T(x, y) = T(x, z) = T(y, z) = 0$. Then the fact that $(x + 1)(x + 1) = Q(x) + 1 + 2x$ for all $x \in V$ implies that $2 = 0 \in F$, a contradiction. A similar argument works for $\mathrm{Clf}^0(Q)$.

5.18. See Auel [Auel2015, Theorem 1.8] for a proof of a more general result.

6.2. Since K is separable, the restriction of the reduced norm to K is nondegenerate. Let $j \in K^\perp \setminus \{0\}$ be a nonzero element in the orthogonal complement of K. Then $B = K + Kj$ since $\dim_F(K + Kj) = 4$. Since $1 \in K$, we have $T(1, j) = \mathrm{trd}(j) = 0$ (recall (4.2.14)) so $\bar{j} = -j$ and $b = j^2 \in F^\times$. By (4.2.15) we have $\mathrm{trd}(\bar{j}\alpha) = 0$ so

$$\bar{j}\alpha + \bar{\alpha}j = \bar{\alpha}j - j\alpha = 0$$

so $j\alpha = \bar{\alpha}j$.

6.12. Let $e_1, \ldots, e_n$ be a normalized basis for V, and let $n = 2m + 1$. By Example 6.3.7, since Q is nondegenerate we may take $a_1 \cdots a_m = 1$ and $c_1 = d$, i.e., $Q \simeq [1, b_1] \perp \cdots \perp [1, b_m] \perp \langle 1 \rangle$. Then

$$e_i e_j - e_j e_i = e_i e_j + e_i e_j = T(e_i, e_j)$$

for all i, j. For $I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, let $e_I = e_{i_1} \cdots e_{i_r}$. By the orthogonal decomposition, e_i centralizes e_I if and only if $i \notin I$ for each $i = 1, \ldots, 2n$, and e_n centralizes $\mathrm{Clf}(Q)$. Therefore $Z(\mathrm{Clf}(Q)) \simeq F[e_n] \simeq F[x]/(x^2 - d)$. If $d = 1$, the unique solution to $\zeta^2 = 1$ in $Z(\mathrm{Clf}(Q)) \cap \mathrm{Clf}^1(Q)$ is e_n.

7.3. The map $a \otimes b \mapsto (x \mapsto ax\bar{b})$ gives an F-algebra homomorphism $B \otimes_F B \to \mathrm{End}_F(B) \cong \mathrm{M}_4(F)$, which is injective since $B \otimes_F B$ is simple and therefore an isomorphism by a dimension count.

7.12. See e.g. Drozd–Kirichenko [DK94, Theorem 6.1.2].

7.13. The augmentation ideal is the kernel of the surjective map $\sum_g a_g g \mapsto \sum_g a_g$, so is nontrivial.

7.14. See Reiner [Rei2003, Exercise 7.8], Lam [Lam2001, Theorem 6.1], etc.

7.19. Lemma 7.4.8 characterizes $\operatorname{rad} B$ as the largest two-sided ideal in which every element is nilpotent, so we show that $\operatorname{rad} \operatorname{nrd}$ has this property. First, $\operatorname{rad} \operatorname{nrd}$ is a two-sided ideal: if $\epsilon \in \operatorname{rad} \operatorname{nrd}$ and $\alpha \in B$, then $\operatorname{trd}(\beta\alpha\epsilon) = 0$ for all $\beta \in B$ so $\alpha\epsilon \in \operatorname{rad} \operatorname{nrd}$ and similarly $\operatorname{trd}(\beta\epsilon\alpha) = \operatorname{trd}(\alpha\beta\epsilon) = 0$ so $\epsilon\alpha \in \operatorname{rad} \operatorname{nrd}$. Next, every $\epsilon \in \operatorname{rad} \operatorname{nrd}$ is nilpotent: we have $\operatorname{trd}(\epsilon) = 0$, so $\epsilon^2 = -\operatorname{nrd}(\epsilon)$ and $\operatorname{trd}(\epsilon^2) = -2\operatorname{nrd}(\epsilon) = 0$ so $\operatorname{nrd}(\epsilon) = 0$ and $\epsilon^2 = 0$.

7.22. This exercise was given in a course by Bjorn Poonen in Spring 2000 at the University of California, Berkeley.

First, parts (a) and (b). Choose $x \in D \setminus F$. Then $K = F(x)$ is a purely inseparable extension of F so the minimal polynomial of x in D (or in $\overline{F}$) is of the form $T^{p^n} - a$. In particular, $p \mid [K : F]$, but D is a left K-vector space and $[D : F] = [D : K][K : F]$ so $p \mid [D : F]$.

For part (c), all roots of the minimal polynomial of x are equal, hence all eigenvalues of $x \otimes 1 \in \mathrm{M}_n(F)$ are equal, and the number of them is divisible by p by (a), so the trace is zero. For part (d), by (c), all elements of $\mathrm{M}_n(\overline{F})$ have trace zero, which is a contradiction.

7.24. Apply the Skolem–Noether theorem to a nontrivial automorphism of K; verify that the conjugating element has trace zero.

Let $j \in B^\times$ satisfy $j\alpha j^{-1} = \overline{\alpha}$. Then $B = K \oplus Kj$, but $j^2\alpha j^{-2} = \alpha$ so $j^2 \in Z(B)$ so $j^2 = b \in F^\times$.

7.27. By Corollary 7.7.9, every maximal subfield K of B has the same dimension, so since F is a finite field they are isomorphic (as abstract fields). But then by the Skolem–Noether theorem, since every element lies in a maximal subfield, we have $B^\times = \bigcup_{\alpha \in B^\times} \alpha^{-1} K^\times \alpha$, which is a contradiction.

One can also proceed without using the maximal subfield dimension theorem. Suppose B is a minimal counterexample (by cardinality); then B is a division ring, but every subalgebra of B is a field. Let $F = Z(B)$. Let $i \in B \setminus F$; then by minimality, the centralizer of i is a maximal subfield K. We may assume $K = F(i)$. If $B = K$, we are done. Otherwise, let i have multiplicative order m. Consider $L : B \to B$ by $L(\alpha) = i\alpha i^{-1}$. Then L is a K-linear map with L^m equal to the identity. We may therefore decompose B into eigenspaces for L. Arguing as in the case of quaternion division rings, we show that each such nonzero eigenspace has dimension 1 as K-vector space. Now consider the normalizer $N = N_B(K)$. Then there is a bijection between the set of cosets of $N/K^\times$ and the eigenspaces of L. But N acts on K as F-linear automorphisms with kernel $K^\times$, so $N/K^\times$ is a subgroup of the Galois group $\mathrm{Gal}(K/F)$. It must be the full Galois group, otherwise $N/K^\times$ fixes some subfield and its centralizer is a noncommutative F-subalgebra, contradicting minimality. Therefore $\dim_K B = \dim_F K$. We now proceed as above.

There are a large number of proofs of Wedderburn's little theorem: see for example Kaczynski [Kacz64].

8.2. If i, j and i', j' are standard generators of B and B', respectively, then consider

the subalgebras generated by the pair $i \otimes 1$ and $j \otimes j'$ and then pair $i \otimes i'$ and $1 \otimes j'$.

8.11. See Weil [Weil60, §7, Propositions 2–3].

9.8. The lattices are free, so by induction we reduce to the one-dimensional case, which is simply the statement that $\widehat{R}_\mathfrak{p} \cap F = R_\mathfrak{p} \subseteq \widehat{F}_\mathfrak{p}$ and follows since $R_\mathfrak{p} = \{x \in F : v(x) \geq 0\}$.

10.6. Using the matrix units, show that if $M = (m_{ij})_{i,j} \in O$ then $m_{ij} \cdot 1 \in O$, but then m_{ij} is integral over R so in fact $m_{ij} \in R$ and hence $M \in \mathrm{M}_n(R)$.

10.8. The converse is true if $\mathrm{char}\, F \neq 2$ and R is integrally closed. It is immediate if $1/2 \in R$ since $\mathrm{trd}(\alpha^2) = \mathrm{trd}(\alpha)^2 - 2\,\mathrm{nrd}(\alpha)$, so $2\,\mathrm{nrd}(\alpha) \in R$. But for the same reason more generally we have $2\,\mathrm{nrd}(\alpha^n) = 2\,\mathrm{nrd}(\alpha)^n \in R$ so $R[\mathrm{nrd}(\alpha)] \subseteq (1/2)R$; so if R is integrally closed we have in fact $\mathrm{nrd}(\alpha) \in R$.
The statement is false if $\mathrm{char}\, F = 2$: take $B = F \times F$ (with $\mathrm{char}\, F = 2$) and $\alpha = (a, a)$ with $a \in F$ not integral over R. Then $\mathrm{trd}(\alpha^n) = 2a^n = 0$ for all n but α is not integral.

12.1. Let $k = \mathbb{F}_q$. If Q is not nondegenerate, then it is isotropic already. Otherwise, choosing a normalized basis for V we may assume the quadratic form Q is of the form $z^2 = f(x, y)$ where $f(x, y)$ is a quadratic form in two variables. If q is even we are now done since every element of k is a square. So suppose q is odd. Then function $f(x, 1)$ takes exactly $(q + 1)/2$ values in k, but there are $(q - 1)/2$ nonsquares in $k^\times$, so at least one of the values must be a square.

12.2. The quadratic form $\langle -1, e, -1\rangle$ is isotropic by a previous exercise, so diagonalizing we have $\langle -1, e\rangle \cong \langle 1, s\rangle$ for some $s \in k^\times$. But $\mathrm{disc}(\langle -1, e\rangle) = -e = s = \mathrm{disc}(\langle 1, s\rangle) \in k^\times/k^{\times 2}$, so $\langle 1, s\rangle \cong \langle 1, -e\rangle$. More generally, this argument shows that two nonsingular binary quadratic forms over a finite field are isometric if and only if they have the same discriminant.

12.7. For (a), under the multiplication map $m : G \times G \to G$, we have $m(1, 1) = 1$; since multiplication is continuous, there exists an open neighborhood $V_1 \times V_2 \ni (1, 1)$ with $V_1 \times V_2 \subseteq m^{-1}(U)$, i.e., $V_1 V_2 \subseteq U$. Letting $V = V_1 \cap V_2 \ni 1$, then $V^2 \subseteq U$. Statement (b) follows similarly, using that inversion is continuous.

12.8. Let $xH, yH \in G/H$ be distinct. Then $yHx^{-1} \subseteq G$ is closed and $1 \notin yHx^{-1}$. By Exercise 12.7, there is an open neighborhood $V \ni 1$ in G such that $V^{-1}V \subseteq G \smallsetminus yHx^{-1}$. So $VxH \ni xH$ and $VyH \ni yH$ are disjoint open neighborhoods as desired.

12.9. Exercise suggested by Grant Molnar.

13.1. Write B in the form $B = \left(\dfrac{K, 2}{\mathbb{Q}_2}\right)$ with $K \supseteq \mathbb{Q}_2$ the unique unramified extension of $\mathbb{Q}_2$.

13.5. The standard involution on B has $\overline{O} = O$ and $\overline{P} = P$ since $\overline{j} = -j$, therefore it induces a standard involution on the quotient O/P. Recall the classification of these algebras (Theorem 3.5.1, extended to Theorem 6.2.8 in all characteristics).

13.15. The proof that addition and multiplication are continuous with respect to the absolute value $|\,|$ induced by w is identical to the commutative case. We have a filtration $O \supset P \supset P^2 \supset \dots$ where P is generated by j and thus to show that B is complete it suffices to note that the limit of the partial sums $x_0 + x_1 j + x_2 j^2 + \cdots = (x_0 + x_2\pi + \dots) + (x_1 + x_3\pi + \dots)j \in K + Kj$ exists since K is complete. The

set O is compact since it is complete and totally bounded. By translating, since O is open we have that B is locally compact. Finally, if $x \notin O$ then $w(x) < 0$ so the ring generated by O and x is equal to B; but B is not compact, since the open cover $\bigcup_i \pi^{-i} O$ has no subcover. See Vignéras [Vig80a, Lemme II.1.6].

13.14 First proof: the symbol is trivial if and only if F is a splitting field for $(-1, -1 \mid \mathbb{Q}_2)$ if and only if $[F : \mathbb{Q}_2]$ is even, by Proposition 13.4.4.
Second, more direct proof: Let e be the ramification degree of F over $\mathbb{Q}_2$ and f the inertial degree, so $[F : \mathbb{Q}_2] = ef$. We need to show $(-1, -1)_F = 1$ if and only if e is even or f is even. By a change of basis, we have $(-1, -1 \mid F) = (-3, -2 \mid F)$, so we need to show $(-3, -2)_F = 1$ if and only if e is even or f is even. The F-algebra $K = F[x]/(x^2 + 3)$ is not a field if and only if f is even, and then the quaternion algebra splits. So suppose f is odd. Then K is a field, the unramified quadratic extension of F, so the algebra is split if and only if -2 is a norm from K to F if and only if $e = \mathrm{ord}_v(2)$ is even.

14.8. Take $t = \pm q \prod_{p \in \Sigma \setminus \{\infty\}} p^{\mathrm{ord}_p(t_p)}$. Select the prime q to satisfy congruences to ensure that the conditions hold. [See also Cassels [Cas78, Corollary to Theorem 6.5.1].]

14.11. There are infinitely many separable quadratic splitting fields of B (by the Hasse–Minkowski theorem), and only finitely many of them can be contained in L. Check that a separable quadratic field $K \supseteq F$ that is not contained in L is linearly disjoint with L over F.

15.19. See Reiner [Rei2003, Theorem 41.3]; the result generalizes to the statement that if $O' \supseteq O$ is a maximal order containing O, then $O' \simeq O'_1 \times \cdots \times O'_r$, and

$$(O' : O)_{\mathsf{L}} = \bigoplus_{i=1}^{r} \frac{n}{n_i} \operatorname{codiff}(O'_i)$$

a result due to Jacobinski [Jaci66]. See also Reiner [Rei2003, Exercises 41.1–41.3].

16.14. See Shimura [Shi71, Proposition 4.11, (5.4.2)].

16.16. This exercise is due to Kaplansky [Kap69]. We compute that

$$O_{\mathsf{L}}(I) = \begin{pmatrix} R & R & (a) \\ (a) & R & (a^2) \\ R & R & R \end{pmatrix} \quad \text{and} \quad O_{\mathsf{R}}(I) = \begin{pmatrix} R & R & R \\ R & R & R \\ (a^2) & (a^2) & R \end{pmatrix}$$

and

$$I^{-1} = \begin{pmatrix} R & R & R \\ R & R & R \\ (a) & R & (a^2) \end{pmatrix}$$

has $I^{-1}I = O_{\mathsf{R}}(I)$ but

$$II^{-1} = \begin{pmatrix} (a) & R & (a) \\ (a) & R & (a^2) \\ R & R & R \end{pmatrix} \neq O_{\mathsf{L}}(I).$$

17.3. Reduce to the local case; the result follows from Paragraph 16.6.9. Or consider the connecting ideal $I = OO'$: clearly $O \subseteq O_{\mathsf{L}}(I)$ so equality holds since O is maximal.

17.7(a). The norm is Euclidean because $B_\infty \simeq \mathbb{H}$ and $\mathbb{H}$ has the standard Euclidean norm. The order $\mathbb{Z}\langle i, j, k\rangle$ is discrete in B_∞ (taking coordinate neighborhoods); it follows that O is discrete in B_∞ as well, since O is commensurable with $\mathbb{Z}\langle i, j, k\rangle$ (a coordinate neighborhood contains only finitely many points).

17.7(b). See also Goren–Lauter [GL2007, Lemma 2.1.1].

17.7(c). See also Goren–Lauter [GL2007, Corollary 2.1.2].

18.2. Suppose that $IJ \subseteq \{0\}$ with I, J two-sided O-ideals. Then $(IF)(JF) = F(IJ) = \{0\}$. If I, J are both nonzero, then by Paragraph 18.2.1, $IF = JF = B$, so $B = \{0\}$, impossible.

18.3. J has the structure of an R-module, since $R \subseteq Z(O)$. Since R is noetherian and O is finitely generated as an R-module, J is finitely generated as an R-module; and $JF \subseteq B$ is a nonzero two-sided ideal of B, so since B is simple, we have $JF = B$.

18.6. See Fröhlich [Frö73], with thanks to Ardakov [Ard-MO].

20.6. We first show the inclusion ($\subseteq$) following (a)–(c). Since $\operatorname{rad} A$ is a two-sided ideal, it suffices to show that $1 - \beta \in A^\times$. Suppose $A(1-\beta) \subsetneq A$, then there is a maximal left ideal $I \subseteq A$ such that $A(1-\beta) \subseteq I$ and so $1 - \beta \in I$; but since $\operatorname{rad} A \subseteq I$, we conclude $1 \in I$, a contraduction. Therefore $A(1-\beta) = A$, so there exists $\alpha \in A$ such that $\alpha(1-\beta) = 1$ and $1 - \beta$ has the left inverse α. Further, $1 - \alpha = -\alpha\beta \in \operatorname{rad} A$. Repeating the argument again, we conclude that $A(1-(1-\alpha)) = A\alpha = A$, so there exists $\gamma \in A$ such that $\gamma\alpha = 1$, and $\gamma = \gamma(\alpha(1-\beta)) = 1-\beta$; thus α is also a right inverse of $1-\beta$. Thus $1-\beta \in A^\times$. Conversely, we show ($\supseteq$) to show (d). Let $\beta \in A$ be such that $1 - \alpha\beta\gamma \in A^\times$ for all $\alpha, \gamma \in A$. Let M be a simple left A-module; we show that $\alpha M = \{0\}$. Let $x \in M$, $x \neq 0$; if $\beta x \neq 0$, then by simplicity $M = A\beta x$ so $\beta = \alpha\beta x$ for some $\alpha \in A$ and $(1 - \alpha\beta)x = 0$; since $1 - \alpha\beta \in A^\times$, we have $x = 0$, a contradiction.

21.4. Let I be a two-sided integral O-ideal. Then since O is a finitely generated R-module and R is noetherian, we conclude that I is contained in a proper maximal (integral) O-ideal M. From $I \subseteq M$ we conclude that $IM^{-1} \subseteq O$, so IM^{-1} is integral. But $\operatorname{nrd}(IM^{-1}) = \operatorname{nrd}(I)/\operatorname{nrd}(M) \mid \operatorname{nrd}(I)$. It follows that I can be written as the product of maximal ideals M by induction on the reduced norm.
We will now show that in fact a maximal O-ideal is prime. For suppose that $IJ \subseteq M$ and that $I \nsubseteq M$. Then $I + M$ is a two-sided O-ideal strictly containing M so $I + M = O$. But then $J = IJ + MJ \subseteq M$. Conversely, if P is prime and $P \subseteq I$ where I is a proper two-sided integral O-ideal. Since O is hereditary, I is invertible and $P = I(I^{-1}P)$; but $I^{-1}P \subseteq P$ implies $I^{-1} \subseteq O$ which is impossible so $I \subseteq P$ hence $P = I$.
To conclude, we show that this group is abelian. Let P, Q be prime ideals. Then $PQ \subseteq P$, so as above PQP^{-1} is integral, say $PQP^{-1} = Q'$. If $Q' = O$ then $Q = O$, a contradiction. But then choosing $0 \neq p \in P \cap R$ then $Q = pQp^{-1} \subseteq Q'$, but Q is maximal so $Q = Q'$. Thus $PQ = Q'P$, so the group is abelian.

21.6(a). We follow Reiner [Rei2003, Exercise 39.2]. Let $J = \operatorname{rad} O$. Certainly $O + J'$ is an R-order, since $OJ'O \subseteq O'J'O' \subseteq J'$.

21.6(b). We want to show that $J \subseteq \operatorname{rad}(O + J')$, and for that we can show $J + J' \subseteq$

$\mathrm{rad}(O + J')$. By Corollary 20.5.5, for r large we have $J^r \subseteq \mathfrak{p}O$. Thus

$$(J + J')^r \subseteq J^r + J' \subseteq \mathfrak{p}O + J' \subseteq \mathfrak{p}O' + J';$$

and for r possible larger by Theorem 20.5.1, we have $(J')^r \subseteq \mathfrak{p}O'$ so

$$(\mathfrak{p}O' + J')^r \subseteq \mathfrak{p}O' \subseteq (J')^r \subseteq \mathfrak{p}O'.$$

Combining these, and making r even larger,

$$(J + J')^{r^3} \subseteq (\mathfrak{p}O')^r \subseteq \mathfrak{p}O \subseteq \mathfrak{p}(O + J').$$

Now by Corollary 20.5.5, we have $J + J' \subseteq \mathrm{rad}(O + J')$.

21.6(c). We have shown $(J')^r \subseteq \mathfrak{p}O$; if $J' \subseteq O$, then by Corollary 20.5.5 we conclude $J' \subseteq J$.

21.9. See Small [Sma66].

21.10. See Reiner [Rei2003, Theorem 40.7].

21.13. See [AG60, Theorem 2.3].

22.5(a). See Voight [Voi2011a, Lemma 3.7]. The map s descends first to $(\bigwedge^2 M)^{\otimes 3}$ since

$$s(x \otimes x' \otimes y \otimes y' \otimes z \otimes z') = 0$$

whenever $x = x'$ and

$$s(x \otimes x' \otimes y \otimes y' \otimes z \otimes z') = -s(x' \otimes x \otimes y \otimes y' \otimes z \otimes z'),$$

with similar statements for y, z.

22.5(b). To show that s in fact descends to $\bigwedge^3(\bigwedge^2 M)$, we observe that

$$s(x \wedge x' \otimes y \wedge y' \otimes z \wedge z') = 0$$

whenever $x = y$ and $x' = y'$ (with similar statements for x, z and y, z). To finish, we show that

$$s((x \wedge x') \otimes (y \wedge y') \otimes (z \wedge z')) = -s((y \wedge y') \otimes (x \wedge x') \otimes (z \wedge z')).$$

To prove this, we may do so locally and hence assume that M is free with basis e_1, e_2, e_3; by linearity, it is enough to note that

$$\begin{aligned} s((e_1 \wedge e_2) \otimes (e_2 \wedge e_3) \otimes (e_3 \wedge e_1)) &= (e_1 \wedge e_2 \wedge e_3) \otimes (e_2 \wedge e_3 \wedge e_1) \\ &= (e_2 \wedge e_3 \wedge e_1) \otimes (e_2 \wedge e_3 \wedge e_1) \\ &= -s((e_2 \wedge e_3) \otimes (e_1 \wedge e_2) \otimes (e_3 \wedge e_1)). \end{aligned}$$

22.5(c). It follows then also that s is an isomorphism, since it maps the generator

$$(e_1 \wedge e_2) \wedge (e_2 \wedge e_3) \wedge (e_3 \wedge e_1) \in \bigwedge^3(\bigwedge^2 M)$$

to the generator $(e_1 \wedge e_2 \wedge e_3) \otimes (e_2 \wedge e_3 \wedge e_1) \in (\bigwedge^3 M)^{\otimes 2}$.

22.10. Exercise suggested by Asher Auel.

22.8. We have

$$\psi(\overline{x} \wedge \overline{y}) = 1 \wedge \overline{x} \wedge \overline{y} \wedge \overline{xy} = 1 \wedge (-x) \wedge (-y) \wedge (-xy) = -(1 \wedge x \wedge y \wedge xy)$$

for all $x, y \in O$, with similitude factor $h = -1 : \bigwedge^4 O \xrightarrow{\sim} \bigwedge^4 O$.

23.6. By the computation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mathfrak{p} & R \\ \mathfrak{p}^e & \mathfrak{p} \end{pmatrix} = \begin{pmatrix} a\mathfrak{p} + b\mathfrak{p}^e & aR + b\mathfrak{p} \\ c\mathfrak{p} + d\mathfrak{p}^e & cR + d\mathfrak{p} \end{pmatrix}$$

we see that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_{\mathrm{L}}(J)$ if and only if $a \in R$, $b \in \mathfrak{p}^{-1}$, $c \in \mathfrak{p}^{e-1}$, and $d \in R$. A similar calculation holds on the right.

23.7. Start with any R-basis x_1, x_2 of L; writing a basis of M in terms of x_1, x_2 yields the columns of a matrix in $\mathrm{GL}_2(F)$. If we change the basis of L or of M, we are applying the group $\mathrm{GL}_2(R)$ on the left or right to this matrix, i.e., we can perform integral row and column operations on this matrix. Now by direct manipulation with 2×2-matrices (more abstractly, the theory of elementary divisors), we can transform this matrix into a diagonal matrix of the desired form.

24.2. See Faddeev [Fad65, Proposition 24.2].

25.3. See Weston [Wes, Lemma 1.19].

25.4. We follow Weston [Wes, Proposition 4.5], working through each part. Write

$$\zeta_{K,[\mathfrak{b}]}(s) = \frac{1}{w(\mathrm{Nm}(\mathfrak{b})^s)} \sum_{b=1}^{\infty} \frac{b_n}{n^s}$$

where

$$b_n := \#\{a \in \mathfrak{b}^{-1} : \mathrm{Nm}(a) = n\}.$$

Since $\mathrm{Nm}(a) = |a|^2$, for all $x > 1$

$$\sum_{n \le x} b_n = \#\{a \in \mathfrak{b}^{-1} : 0 < |a| \le \sqrt{x}\};$$

from Lemma 25.2.11, we conclude

$$\left| \sum_{n \le x} b_n - \frac{\pi x}{A} \right| \le C\sqrt{x}$$

where A is the coarea of $\mathfrak{b}^{-1}$ and C is a constant that does not depend on x. We compute that

$$A = \mathrm{Nm}(\mathfrak{b}^{-1}) \frac{\sqrt{|d|}}{2}.$$

This proves (a).

Now consider the Dirichlet series

$$f(s) := \frac{1}{wN(\mathfrak{b})^s} \sum_{n=1}^{\infty} \left(b_n - \frac{\pi}{A} \right) \frac{1}{n^s}.$$

Then the estimate

$$\left|\sum_{n\le x}\left(b_n - \frac{\pi}{A}\right)\right| = \left|\sum_{n\le x} b_n - \frac{\pi x}{A}\right| \le C\sqrt{x}$$

by the comparison test implies that $f(s)$ converges for all $\operatorname{Re} s > 1/2$ and in particular $f(s)$ converges at $s = 1$, proving (b).
For $s > 1$,

$$f(s) = \zeta_{K,[\mathfrak{b}]}(s) - \frac{\pi}{Aw\operatorname{Nm}(\mathfrak{b})^s}\zeta(s)$$

so

$$\zeta_{K,[\mathfrak{b}]}(s) = f(s) + \frac{2\pi}{w\sqrt{|d|}}\operatorname{Nm}(\mathfrak{b})^{1-s}\zeta(s).$$

hence

$$\begin{aligned}\operatorname{res}_{s=1}\zeta_K(s) &= \lim_{s\searrow 1}(s-1)\zeta_{K,[\mathfrak{b}]}(s)\\ &= \lim_{s\searrow 1}(s-1)f(s) + \frac{2\pi}{w\sqrt{|d|}}\lim_{s\searrow 1}(s-1)\operatorname{Nm}(\mathfrak{b})^{1-s}\zeta(s)\\ &= 0 + \frac{2\pi}{w\sqrt{|d|}}\cdot 1 = \frac{2\pi}{w\sqrt{|d|}}.\end{aligned}$$

This proves (c).
Finally, (d): $\zeta_{K,[\mathfrak{b}]}(s)$ has a simple pole at $s = 1$ with residue independent of $[\mathfrak{b}]$. Summing the residues over $[\mathfrak{b}] \in \operatorname{Cl}(K)$, from (25.2.9) we conclude the result.

25.6. For further reading, see Fitzgerald [Fit2011] and Clark–Jagy [CJ2014].

25.7(b). We follow Lenstra [Len79, Lemma 1.5]. Let J be an invertible right O-ideal; without loss of generality, we may suppose $J \subseteq O$ is integral. We argue by induction on $\operatorname{nrd}(J) > 0$. The base case $\operatorname{nrd}(J) = 1$ implies that $J = O$, which is true. Since I, J are invertible, we have $J^{-1}I \neq I$, so there exists $\gamma \in J^{-1}I \setminus I$. Since I is Euclidean, there exists $\mu \in I$ such that $\operatorname{nrd}(\gamma - \mu) < \operatorname{nrd}(I)$. Let $\nu = \gamma - \mu$. Then $\nu \neq 0$, else $\gamma = \mu \in I$. Since $\gamma \in J^{-1}I$ and $\mu \in I$ we have $\nu \in J^{-1}I$, so $J' = \nu I^{-1}J \subseteq O$ is an integral, invertible right O-ideal. We have

$$\operatorname{nrd}(J') = \operatorname{nrd}(\nu)\operatorname{nrd}(I)^{-1}\operatorname{nrd}(J) < \operatorname{nrd}(J).$$

So by induction, for $[J'] \in \operatorname{Cl}(O)$ we have either $[J'] = 1$ or $[J'] = [I]$, and thus $[J] = [I^{-1}] = [I]$ or $[J] = 1$, the latter using the fact that $\operatorname{Pic}(O)$ has exponent dividing 2.

26.2 First (a). Let $V = F_{\mathbb{R}}$ be the ambient space. The group $R^\times$ acts by preserving the norm, so we can write $(V/R^\times)_{\le 1} = V_{\le 1}/R^\times$. Choose a system of fundamental units for $R^\times$ and let $\mathbb{Z}^{r+c-1} \simeq E \le R^\times$ be the group generated by them; then $R^\times = ER^\times_{\mathrm{tors}}$, and so

$$\operatorname{vol}(V_{\le 1}/R^\times) = \frac{1}{w}\operatorname{vol}(V_{\le 1}/E) = \frac{2^c}{w}\int_{V_{\le 1}/E} \mathrm{d}x\,\mathrm{d}z$$

with x_i, z_j standard coordinates on $\mathbb{R}^r \times \mathbb{C}^c$—and we use multi-index notation to simplify.

Now (b). Let ρ_j, θ_j be polar coordinates on $\mathbb{C}^c$, and for symmetry restrict the domain V to the domain V^+ with $x_i > 0$ for all i. Then

$$\int_{V_{\le 1}/E} \mathrm{d}x\,\mathrm{d}z = 2^r \int_{V^+_{\le 1}/E} \mathrm{d}x\,(\rho\,\mathrm{d}\rho\,\mathrm{d}\theta) = 2^r(2\pi)^c \int_{W^{+,\le 1}/E} \rho\,\mathrm{d}x\,\mathrm{d}\rho$$

where W^+ is the projection of V^+ onto the x, ρ-coordinate plane. Now let $x_{r+j} = \rho_j^2$ to get

$$2^r(2\pi^c) \int_{W^+_{\le 1}/E} \rho\,\mathrm{d}x\,\mathrm{d}\rho = 2^r\pi^c \int_{W^{+,\le 1}/E} \mathrm{d}x$$

and the norm is now simply the product of $r + c$ (positive) coordinates.
Next, (c): we apply the change of variables $u_i = \log x_i$; the condition $\prod_i x_i = t \le 1$ becomes $\sum_i u_i = \log t \le 0$, and we obtain

$$\int_{W^{+,\le 1}/E} \mathrm{d}x = \int_{\log(W^{+,\le 1}/E)} e^u\,\mathrm{d}u = \int_{-\infty}^{0} e^t\,\mathrm{d}t \int_P \mathrm{d}u = \int_P \mathrm{d}u$$

where P is the fundamental parallelogram for the additive (logarithmic) action of $R^\times$.
Finally (d): by definition, P has covolume Reg_F, and putting all of these together, we conclude that

$$\mathrm{vol}(V_{\le 1}/R^\times) = \frac{2^c}{w} 2^r\pi^c \mathrm{Reg}_F = \frac{2^r(2\pi)^c \mathrm{Reg}_F}{w_F}$$

as claimed.

28.3(a). See Newman [New72, Theorem II.7].

28.6. We show that $\widehat{\alpha} \notin B^\times \widehat{O}^\times$. Indeed, suppose that $\widehat{\alpha} = \beta\widehat{\mu}$ with $\beta \in B^\times$ and $\widehat{\mu} \in \widehat{O}^\times$. Since $\mathrm{nrd}(O^\times) \cap \mathbb{Q}^\times = \{\pm 1\}$, we may suppose $\beta \in B^1$. Then $\ell\widehat{\alpha}\widehat{\mu}^{-1} = \ell\beta = \gamma \in B \cap \widehat{O} = O$; thus $\mathrm{nrd}(\gamma) = \ell^2$. But $\mathrm{nrd}|_O = \langle 1, -p, -q, pq\rangle$ only represents ℓ^2 by $\pm\ell$, a contradiction.

29.1(a). It suffices to show that H has a compact neighborhood in G/H. Since G is locally compact, there is a compact neighborhood $U \ni 1$ in G. By Exercise 12.7(b), there exists an open neighborhood $V \ni 1$ such that $V^{-1}V \subseteq U$. The projection map $\pi\colon G \to G/H$ is open by definition of the quotient topology, so $\pi(V) \subseteq G/H$ is an open neighborhood of H. The closure $\mathrm{cl}(\pi(V)) \subseteq \pi(U)$ is therefore compact.

29.9. We know that $B\backslash\underline{B}$ is compact, so $\underline{\mu}(B\backslash\underline{B}) < \infty$. Let $\underline{E} \subseteq \underline{B}^\times$ be a compact set with measure $\underline{\mu}(\underline{E}) > \underline{\mu}(B\backslash\underline{B})$. Then (generalizing Minkowski), we claim that the map $\underline{B} \to \overline{B}\backslash\underline{B}$ is not injective on $\underline{E}$: otherwise, integrating the characteristic function Φ of $\underline{E}$ we find $\underline{\mu}(\underline{E}) \le \underline{\mu}(B\backslash\underline{B})$, a contradiction:

$$\begin{aligned}\underline{\mu}(\underline{E}) &= \int_{\underline{B}} \Phi(\underline{\alpha})\,\mathrm{d}\mu(\underline{\alpha}) = \int_{B\backslash\underline{B}} \sum_{\beta\in B} \Phi(\underline{\alpha}+\beta)\,\mathrm{d}\underline{\mu}(\underline{\alpha}) \\ &\le \int_{B\backslash\underline{B}} \mathrm{d}\underline{\mu}(\alpha) = \underline{\mu}(B\backslash\underline{B}).\end{aligned}$$

30.7. If q is odd, then this follows from Lemma 30.6.17. Suppose q is even. The set $M(1)$ still counts the roots of f_γ in the residue field, so $\#M(1) = 1 + \left(\frac{K}{\mathfrak{p}}\right)$. If $d \notin R^\times$, then $K \supseteq F$ is a ramified field extension and we claim that $M(2) = \emptyset$, i.e., there are (still) no solutions to $f_\gamma(x) \equiv 0 \pmod{\mathfrak{p}^2}$: indeed, we have $t \in \mathfrak{p}$, so if $\mathrm{ord}_\mathfrak{p}(x) \geq 1$ then $n \in \mathfrak{p}^2$ contradicting that S is integrally closed, and if $\mathrm{ord}_\mathfrak{p}(x) = 0$ then $n \in R^\times$ so there exists $a \in R$ such that $a^2 \equiv n \pmod{\mathfrak{p}}$, and replacing $x \leftarrow x - a$ we reduce to the previous case.

32.2. First compute all elements in O of norm 2, then show the product of any two of these elements belongs to $2O$.

32.4. Write $j^{-1}\gamma j = a\overline{\gamma}/\operatorname{nrd}(\gamma)$ with $a \in F^\times$, and taking reduced norms we get $\operatorname{nrd}(\gamma) = a^2/\operatorname{nrd}(\gamma)$, so $\operatorname{nrd}(\gamma) = \pm a$ and $j^{-1}\gamma j = \pm\overline{\gamma}$; then taking reduced trace to get $\operatorname{trd}(\gamma) = \pm\operatorname{trd}(\gamma)$; if $\operatorname{trd}(\gamma) \neq 0$ then we are done, otherwise $\operatorname{trd}(\gamma) = 0$ so $\overline{\gamma} = -\gamma$ and the result is true anyway.

32.5. See Chinburg–Friedman [CF2000, Lemma 2.8].

32.7. See Hallouin–Maire [HM2006, Proposition 5].

33.1. For (a), estimate the integral defining the length above and below.

33.5. We refer to the method of proof in the Iwasawa decomposition (Proposition 33.4.2). First, we translate by $-\operatorname{Re} z$ to assume that $z = yi$ and then stretch to obtain $z = i$. To conclude, we rotate (fixing z) to obtain z' purely imaginary; that this is possible is easiest to see in $\mathbf{D}^2$, or it can be verified directly.
Alternatively, if z, z' are on a vertical line we can translate; otherwise there is a unique circle through z, z' that is orthogonal to the real axis, having center c, and the matrix $\begin{pmatrix} 0 & -1 \\ 1 & -c \end{pmatrix}$ acting by $z \mapsto -1/(z-c)$ maps this circle to a vertical line, so we reduce to the previous case.

33.6. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the image of $g^{-1}(\mathbb{R}_{>0}i)$ is equal to

$$\operatorname{Re}\left(\frac{az+b}{cz+d}\right) = 0$$

so by (33.3.7) is given by $ac|z|^2 + (1+2bc)\operatorname{Re} z + bd = 0$, and this is a circle whose center is on the real axis if $ac \neq 0$ and a vertical line if $ac = 0$.

33.8. By Exercise 33.5, we may assume that the points lie on the imaginary axis. We then move to the unit disc, taking the center to be the unique midpoint of the geodesic between these two points; then the points are $-t, t \in \mathbf{D}^2$ with $t \in \mathbb{R}_{>0}$. We then compute using the formula (33.7.5) for distance that the line L is described by $|w-t|^2 = |w+t|^2$, and expanding this consists of the set of points $\operatorname{Re} w = 0$. This set is geodesic and is the perpendicular bisector of the geodesic segment $[-t, t]$. It follows that $H(\gamma; z_0)$ is geodesic, because for two distinct points w, w' in the right half-plane $\operatorname{Re}(w), \operatorname{Re}(w') \geq 0$, say, the geodesic between them is an arc of a circle also in the right half-plane.

33.10. Checking this on the generators in Lemma 33.4.4 make the result almost imme-

diate. Alternatively, note that if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z, z' \in \mathbf{H}^2$ then

$$gz - gz' = \frac{z - z'}{(cz + d)(cz' + d)}$$

so plugging in recovers the result.

33.11. We have $2\cosh(\log(x)) = \exp(\log(x)) + \exp(-\log(x)) = x + 1/x$ for $x \in \mathbb{R}_{>0}$, and

$$\frac{x + y}{x - y} + \frac{x - y}{x + y} = 2\left(1 + \frac{2y^2}{x^2 - y^2}\right)$$

for $x, y \in \mathbb{R}$ with $x \neq \pm y$. Now simplify, and enjoy the magical cancellation.

33.12. We have

$$1 - |\phi(z)|^2 = \frac{4\operatorname{Im}(z)}{|z + i|^2}$$

and $\phi'(z) = (2i)/(z + i)^2$, so

$$\frac{2|\phi'(z)|}{1 - |\phi(z)|^2} = \frac{1}{\operatorname{Im} z}.$$

Part (b) follows from plugging in $\mathrm{d}w = \phi'(z)\mathrm{d}z$ into part (a).

33.15. Let $w = u + iv$, so the map has $(u, v) = (x/(1 + t), y/(1 + t))$. By the chain rule, we have

$$\mathrm{d}u = -\frac{x}{(1 + t)^2}\mathrm{d}t + \frac{1}{1 + t}\mathrm{d}x$$
$$\mathrm{d}v = -\frac{y}{(1 + t)^2}\mathrm{d}t + \frac{1}{(1 + t)^2}\mathrm{d}t$$

Now square; and then substitute $-t\mathrm{d}t + x\mathrm{d}x + y\mathrm{d}y = 0$ from differentiating $-t^2 + x^2 + y^2 = -1$, get

$$\mathrm{d}u^2 + \mathrm{d}v^2 = \frac{x^2 + y^2 - 2t(1 + t)}{(1 + t)^4}\mathrm{d}t^2 + \frac{\mathrm{d}x^2 + \mathrm{d}y^2}{(1 + t)^2}.$$

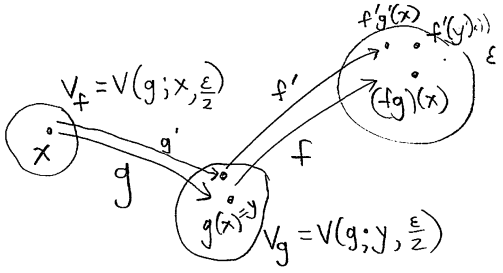
Finally, from $-t^2 + x^2 + y^2 = -1$ show that $1 - u^2 - v^2 = 2/(1 + t)$, and substitute to get the result.

33.16. Or work directly, with $p = (t, x, y)$ show we may assume $v = (1, a, b)$, in which case $t - ax - by = 0$, and given that $t^2 - x^2 - y^2 = 1$, then show $a^2 + b^2 - 1 > 0$ by the Cauchy–Schwarz inequality.

34.4. We check that multiplication is continuous. Let $U = V(h; x, \epsilon) \subseteq \mathrm{Isom}(X)$ be an open ball. Suppose $fg = h \in U$. Let $g(x) = y$ and let

$$V_f = V(f; y, \epsilon/2) \ni f \quad \text{and} \quad V_g = V(g; x, \epsilon/2) \ni g.$$

We claim that $V_f V_g \subseteq U$, so that $(V_f, V_g) \ni (f, g)$ is an open neighborhood, and thus the inverse image of U is open as desired. So let $f' \in V_f$ and $g' \in V_g$.



Then by the triangle inequality, we have

$$\begin{aligned}\rho(f'g'(x), h(x)) &\le \rho(f'g'(x), f'(y)) + \rho(f'(y), h(x)) \\ &= \rho(g'(x), g(x)) + \rho(f'(y), f(y)) < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.\end{aligned}$$

34.6. See Shimura [Shi71, Theorem 1.1, Lemma 1.2].

34.7. To show that it is a local homeomorphism, let $x \in X$. By definition, we find an open neighborhood $U \ni x$ such that $gU \cap U \neq \emptyset$ if and only if $g \in \mathrm{Stab}_G(x)$; since G acts freely, we have $\mathrm{Stab}_G(x) = \{1\}$, so in fact $gU \cap U = \emptyset$ for all $g \neq 1$. Therefore U maps injectively into $G\backslash X$: if $\pi(y) = \pi(y')$ for $y, y' \in U$ then $y' = gy \in U \cap gU$ for some $g \in G$, so $g = 1$ and $y = y'$. To conclude, we need to show that this injection is continuous, and for that it suffices to show that if $V \subseteq U$ then $\pi(V)$ is open; and indeed, $\pi(V)$ is open if and only if $\pi^{-1}(\pi(V)) = \bigcup_{g \in G} gV$ is open by definition of the quotient topology, and the latter is open as each gV is open (G acts continuously).
(Indeed, one can show that the quotient topology is the unique topology on $G\backslash X$ such that the quotient map is continuous and a local homeomorphism.)

34.8. Let $V \ni x$ be an open neighborhood with $\mathrm{cl}(V)$ compact; replacing U by $U \cap V$, we may suppose U has $\mathrm{cl}(U)$ compact. The boundary $\mathrm{bd}(U) \subseteq \mathrm{cl}(U)$ is closed so compact. Now there exists an open neighborhood $V \ni x$ and an open set $W \supseteq \mathrm{bd}(U)$ such that $V \cap W = \emptyset$. (Since X is Hausdorff, the compact set $\mathrm{bd}(U)$ is covered by finitely many separating open sets, so we can take an intersection.) In particular, $\mathrm{cl}(V) \cap \mathrm{bd}(U) = \emptyset$. Let $V' = U \cap V$. Then

$$\mathrm{cl}(V') = \mathrm{cl}(U) \cap \mathrm{cl}(V) = (U \cup \mathrm{bd}(U)) \cap \mathrm{cl}(V) = U \cap \mathrm{cl}(V) \subseteq U.$$

34.14. Let $x = (1, 0, \ldots, 0) \in \mathbb{R}^{n+1}$. We have $\mathrm{SO}(n) \simeq \mathrm{Stab}_x(\mathrm{SO}(n+1)) \le \mathrm{SO}(n+1)$. Gram–Schmidt orthogonalization implies that $\mathrm{SO}(n+1)$ acts transitively on $\mathbf{S}^n$. Next, $\mathrm{SO}(n+1)$ is compact, because it is closed (defined by polynomial equations) and bounded; thus $\mathrm{SO}(n+1)$ acts properly on $\mathbf{S}^n$ (Proposition 34.4.9). The result follows then from 34.4.11.

34.16. See Lee [Lee2011, Proposition 12.25].

34.17. From the formula (33.5.3) for distance, we have:

$$\begin{aligned} 2\cosh\rho(i,gi) &= 2+\frac{|i-gi|^2}{\operatorname{Im} gi} = 2+\frac{\left|i-\dfrac{ai+b}{ci+d}\right|^2}{\dfrac{1}{|ci+d|^2}} \\ &= 2+|(ci+d)i-(ai+b)|^2 = 2+(b+c)^2+(d-a)^2 \\ &= a^2+b^2+c^2+d^2-2ad+2bc+2 = \|g\|^2. \end{aligned}$$

35.1. We have

$$\begin{aligned} \int_{\square} \frac{\mathrm{d}x\mathrm{d}y}{y^2} &= \int_{-1/2}^{1/2}\int_{\sqrt{1-x^2}}^{\infty} \frac{\mathrm{d}y\mathrm{d}x}{y^2} = \int_{-1/2}^{1/2} \frac{\mathrm{d}x}{\sqrt{1-x^2}} \\ &= \sin^{-1}(1/2)-\sin^{-1}(-1/2) = \frac{\pi}{3}. \end{aligned}$$

36.3. Compute

$$(aw+b)(cw+d)^{-1} = (aw+b)(\overline{cw+d})\,\mathrm{nrd}(cw+d) = aw\overline{cw}+b\overline{cw}+aw\overline{d}+b\overline{d}$$

and continue.

36.4. To show that g is a hyperbolic isometry, compute the Jacobian.

37.6. We have

$$z' = gz \in I(g^{-1}) \Leftrightarrow \rho(g^{-1}z',0) = \rho(z',0) \Leftrightarrow \rho(z,0) = \rho(gz,0) \Leftrightarrow z \in I(g)$$

and the result follows.

Bibliography

[Ard-MO] Konstantin Ardakov, Noncommutative group of invertible ideals of a ring, URL (version: 2015-09-24): `http://mathoverflow.net/q/219093`.

[Asl96] Helmer Aslaksen, *Quaternionic determinants*, Math. Intelligencer **18** (1996), no. 3, Summer 1996, 57–65.

[AG60] Maurice Auslander and Oscar Goldman, *Maximal orders*, Trans. Amer. Math. Soc. **97** (1960), 1–24.

[Auel2015] Asher Auel, *Surjectivity of the total Clifford invariant and Brauer dimension*, J. Algebra, **443** (2015), 395–421.

[BC2012] Paul Balmer and Baptiste Calmès, *Bases of total Witt groups and lax-similitude*, J. Algebra Appl. **11** (2012), no. 3, 1250045, 24 pp.

[Bar80] Hans-Jochen Bartels, *Über Normen algebraischer Zahlen*, Math. Ann. **251** (1980), 191–212.

[Cas78] J.W.S. Cassels, *Rational quadratic forms*, Academic Press, London, 1978.

[CF2000] Ted Chinburg and Eduardo Friedman, *The finite subgroups of maximal arithmetic Kleinian groups*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 6, 1765–1798.

[CJ2014] Pete L. Clark and William C. Jagy, *Euclidean quadratic forms and ADC forms II: integral forms*, Acta Arith. **164** (2014), 265–308.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math., vol. 138, Springer-Verlag, Berlin, 1993.

[Coh2000] Henri Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math., vol. 193, Springer-Verlag, New York, 2000.

[CR2003] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441.

[DK94] Yurij A. Drozd and Vladimir V. Kirichenko, *Finite dimensional algebras*, with an appendix by Vlastimil Dlab, translated by Vlastimil Dlab, Springer-Verlag, Berlin, 1994.

[Fad65] D.K. Faddeev, *Introduction to multiplicative theory of modules of integral representations*, Algebraic number theory and representations, Proc. Steklov Institute of Math., vol. 80 (1965), American Math. Soc., Providence, 1968, 164–210.

[Fit2011] Robert W. Fitzgerald, *Norm Euclidean quaternionic orders*, INTEGERS **11** (2011), no. A58.

[Fri2000] Carsten Friedrichs, *Berechnung von Maximalordnungen uber Dedekindringen*, Ph. D. dissertation, Technischen Universität Berlin, 2000.

[Frö73] A. Fröhlich, *The Picard group of noncommutative rings, in particular of orders*, Trans. Amer. Math. Soc. **180** (1973), 1–45.

[FRU74] A. Fröhlich, I. Reiner and S. Ullom, *Class groups and Picard groups of orders*, Proc. London Math. Soc. (3) **29** (1974), 405–434.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 2nd edition, Cambridge University Press, Cambridge, 2003.

[GL2007] Eyal Z. Goren, Kristen E. Lauter, *Class invariants for quartic CM fields*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 2, 457–480.

[GV2011] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **80** (2011), 1071–1092.

[HM2006] Emmanuel Hallouin and Christian Maire, *Cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **595** (2006), 189–213.

[Hanke2007] Timo Hanke, *The isomorphism problem for cyclic algebras and an application*, ISSAC '07: Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery, New York, 2007, 181–186.

[Hess2002] Florian Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445.

[HN94] H. Hijikata and K. Nishida, *Bass orders in non semisimple algebras*, J. Math. Kyoto Univ. **34** (1994), no. 4, 797–837.

[IR93] Gábor Ivanyos and Lajos Rónyai, *Finding maximal orders in semisimple algebras over* $\mathbb{Q}$, Comput. Complexity **3** (1993), no. 3, 245–261.

[Jaci66] H. Jacobinski, *On extensions of lattices*, Michigan Math. J. **13** (1966), 471–475.

[Kacz64] T. J. Kaczynski, *Another proof of Wedderburn's theorem*, Amer. Math. Monthly **71** (1964), 652–653.

[Kan87] R. Kannan, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res. **12** (1987), no. 3, 415–440.

[Kap69] Irving Kaplansky, *Submodules of quaternion algebras*, Proc. London Math. Soc. (3) **19** (1969), 219–232

[KV2010] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **39** (2010), no. 5, 1714–1747; *Corrigendum: Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput. (SICOMP) **41** (2012), no. 3, 714.

[Lam2001] Tsit-Yuen Lam, *A first course in noncommutative rings*, 2nd. ed., Grad. Texts in Math., vol. 131, Springer-Verlag, New York, 2001.

[Lam2005] Tsit-Yuen Lam, *Introduction to quadratic forms over fields*, Grad. Studies in Math., vol. 67, Amer. Math. Soc., Providence, 2005.

[Lee2011] John M. Lee, *Introduction to topological manifolds*, 2nd ed., Grad. Texts in Math., vol 202, Springer-Verlag, New York, 2011.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 513–534.

[Len79] H.W. Lenstra, jr., *Euclidean ideal classes*, Astérisque **61** (1979), 121–131.

[May66] Kenneth O. May, *The impossibility of a division algebra of vectors in three dimensional space*, Amer. Math. Monthly **73** (1966), no. 3, 289–291.

[NS2009] Gabriele Nebe and Allan Steel, *Recognition of division algebras*, J. Algebra **322** (2009), no. 3, 903–909.

[New72] Morris Newman, *Integral matrices*, Pure Appl. Math., vol. 45, Academic Press, New York, 1972.

[Rei2003] Irving Reiner, *Maximal orders*, London Math. Soc. Monogr. (N.S.), vol. 28, Clarendon Press, Oxford University Press, Oxford, 2003.

[Ron92] Lajos Rónyai, *Algorithmic properties of maximal orders in simple algebras over* $\mathbb{Q}$, Comput. Complexity **2** (1992), no. 3, 225–243.

[Schu88] John Schue, *The Wedderburn theorem of finite division rings*, American Math. Monthly **95** (1988), no. 5, 436–437.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Grad. Texts in Math., vol. 7, Springer-Verlag, New York, 1973.

[Shi71] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lectures, no. 1, Publications of the Mathematical Society of Japan, no. 11, Iwanami Shoten, Tokyo, Princeton University Press, Princeton, 1971.

[Sim2002] Dénis Simon, *Solving norm equations in relative number fields using S-units*, Math. Comp. **71** (2002), no. 239, 1287–1305.

[Sim2005] Dénis Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp. **74** (2005), no. 251, 1531–1543.

[Sma66] L. Small, *Hereditary rings*, Proc. Nat. Acad. Sci. USA **55** (1966), 25–27.

[SHT99] Viggo Stoltenberg-Hansen and John V. Tucker, Computable rings and fields, *Handbook of computability theory*, ed. Edward R. Griffor, North-Holland, Amsterdam, 1999, 336–447.

[vPr68] Paul van Praag, *Une caractérisation des corps de quaternions*, Bull. Soc. Math. Belgique **10** (1968), 283–285.

[vPr02] Paul van Praag, *Quaternions as reflexive skew fields*, Adv. Appl. Clifford Algebr. **12** (2002), no. 2, 235–249.

[Vig80a] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., vol. 800, Springer, Berlin, 1980.

[Voi2011a] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134.

[Voi2013] John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and higher degree forms, Developments in Math., vol. 31, Springer, New York, 2013, 255–298.

[Weil60] André Weil, *Algebras with involution and the classical groups*, J. Indian Math. Soc. **24** (1960) 589–623.

[Wes] Tom Weston, *Lectures on the Dirichlet class number formula for imaginary quadratic fields*.