Quadratic Forms[1]

Martin Ziegler

Barcelona 2019

[1] v0.9, Sat Dec 14 20:22:56 2019 +0100

Contents

Chapter 1

Witt's Theorems

§1 Quadratic forms and spaces

We fix a field F of characteristic $\neq 2$.

Definition. A n n-ary quadratic form is a homogeneous polynomial of degree 2 in n-variables with coefficients in F.

So this is how a ternary quadratic form looks like:

$$f(x_1, x_2, x_3) = a_{1,1}x_1^2 + a_{2,2}x_2^2 + a_{3,3}x_3^2 + a_{1,2}x_1x_2 + a_{1,3}x_1x_3 + a_{2,3}x_2x_3.$$

There are two extreme cases: Unary forms ax^2 and the constant 0-form with no variables. We denote these forms by $\langle a \rangle$ and $\langle\ \rangle$.

Definition. Two quadratic forms f and f' are equivalent, $f \cong f'$, if they differ by an invertible linear transformation of the variables. If $\bar{x}$ is a column vector, this means

$$f(\bar{x}) = f'(S\bar{x}),$$

where S is a matrix in $\mathrm{GL}_n(F)$.

Two unary forms $\langle a \rangle$ and $\langle a' \rangle$ are equivalent iff there $a = s^2a'$ for some $s \in \dot{F}$.

As an example look at the two forms $h = x_1^2 - x_2^2$ and $h' = x_1x_2$. They are equivalent via the matrix

$$S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which is regular in characteristic $\neq 2$.

Lemma 1.1. *A quadratic form can be written as $f(\bar{x}) = B(\bar{x}, \bar{x})$ for a symmetric bilinear form B, which is uniquely determined by f, it is the* polar form *of f.*

Proof. The polar form of $a_{1,1}x_1^2 + a_{2,2}x_2^2 + a_{1,2}x_1x_2$ for example is

$$a_{1,1}x_1y_1 + a_{2,2}x_2y_2 + + \frac{1}{2}a_{1,2}x_1y_2 + \frac{1}{2}a_{1,2}x_2y_1.$$

□

Excursion: Polars in the projective plane
If f is a ternary quadratic form, the equation $f(x_1, x_2, x_3) = 0$ defines a conic Q in the projective plane over F. The polar form B defines the associated *polarity* which correlates a point p with the line defined by $B(p, y) = 0$, the *polar* of p. This can be interpreted in geometrically:

Let a_1 and a_2 be the two points of Q where the lines $\overline{a_1 p}$ and $\overline{a_2 p}$ are tangent to Q. Then the polar of p is the line through a_1 and a_2.

The polar form of a quadratic form f is given by a symmetric matrix M as

$$B(x, y) = x^\top M x.$$

Definition. A quadratic form f is regular, or non-degenerate, if M is regular. The determinant of M is the determinant $\det(f)$ of f.

Lemma 1.2. *If f and f' are equivalent, they have the same determinant* up to a square. *This means $\det(f) = s^2 \det(f')$ for some $s \in \dot{F}$.*

Proof. That $f(\bar{x}) = f'(S\bar{x})$ for a regular matrix S means that

$$\bar{x}^\top M \bar{x} = \bar{x}^\top S^\top M' S \bar{x},$$

and so $M = S^\top M' S$ and $\det(M) = \det(S)^2 \det(M')$. □

We say also that $\det(f)$ and $\det(f')$ have the same *square class.*.

Remark 1.3. *If f is reducible in $F[x_1, \ldots, x_n]$ and $n \geq 3$, then f is degenerate.*

Proof. If f is the product of two linear forms λ_1 and λ_2, write $\lambda_i = \bar{a}_i^\top \bar{x}$ for vectors $\bar{a}_i$. We have then $f(\bar{x}) = \bar{x}^\top \bar{a}_1 \bar{a}_2^\top \bar{x}$. So the matrix M of f is $\frac{1}{2}(\bar{a}_1 \bar{a}_2^\top + \bar{a}_2 \bar{a}_1^\top)$, which has rank ≤ 2. □

Definition. A quadratic space is a finite dimensional F-vector space V with a *quadratic map* $q : V \to F$, which (for a basis $v_1, \ldots, v_n$) is given by a quadratic form

$$f(x_1, \ldots, x_n) = q(x_1 v_1 + \cdots + x_n v_n). \tag{1.1}$$

Since an n-ary quadratic form f is determined[1] by the the function it defines on F^n, we can identify it with the quadratic space (F^n, f).

Definition. An isometry between two quadratic spaces (V, q) and (V', q') is an isomorphism $\varphi : V \to V'$ of vector spaces which preserves q, i.e. $q'(\varphi(v)) = q(v)$. For V and V' being isometric, we write

$$(V, q) \cong (V', q').$$

We will often write simply $V \cong V'$, or $q \cong q'$. It is clear that there is a canonical bijection

$$\frac{n\text{-ary quadratic forms}}{\text{equivalence}} \quad \longleftrightarrow \quad \frac{n\text{-dimensional quadratic spaces}}{\text{isometry}}.$$

[1] remarkably, this is also true in characteristic 2

The polar form B_f of f in (1.1) defines a symmetric bilinear form on V

$$B(\sum_{i=1}^{n} x_i v_i, \sum_{i=1}^{n} y_i v_i) = B_f(\bar{x}, \bar{y}).$$

It is easy to see that this does not depend on the choice of the basis. This follows also from the fact that $q(v) = B(v, v)$ as in the proof of the following lemma.

Lemma 1.4. *Let (V, q) a quadratic space and B the associated polar form on V. Then*

$$B(v, w) = \frac{q(v + w) - q(v) - q(w)}{2}.$$

Proof.

$$\begin{aligned} q(v + w) - q(v) - q(w) &= B(v + w, v + w) - B(v, v) - B(w, w) \\ &= B(v, w) + B(w, v) \\ &= 2B(v, w) \end{aligned}$$

□

We define the determinant $\mathrm{d}(q)$ of a quadratic map as the square class of the determinant of its quadratic form

$$\mathrm{d}(q) = \det(f) \cdot \dot{F}^2.$$

This is well-defined by Lemma 1.2. The quadratic map q is *regular* (or non-degenerate) if f is regular. Clearly q is regular if $\mathrm{d}(q) \neq 0$.

Definition. Two elements x, y of a quadratic space are orthogonal, or $x \perp y$, if $B(x, y) = 0$. Two subsets X and Y of a quadratic space (U, p) are orthogonal if $x \perp y$ for all $x \in X$ and $y \in Y$. We write $X \perp Y$ for this.

The radical of a quadratic space is the set of all vectors which are orthogonal to V:

$$\mathrm{rad}(V, q) = \{v \in V \mid v \perp V\}$$

Lemma 1.5. *A quadratic space is regular iff its radical is* 0.

Proof. Consider the quadratic space space (F^n, f) and M being the matrix of the polar form of f. Then $\mathrm{rad}(F^n, f) = \{\bar{x} \mid \bar{x}^\top M = 0\}$. So M is regular iff $\mathrm{rad}(F^n, f) = 0$. □

Definition. The orthogonal sum $(V \perp W, q \perp r)$ of two quadratic spaces (V, q) and (W, r) is the direct sum $V \perp W = V \oplus W$ with the quadratic form

$$(q \perp r)(v + w) = q(v) + r(w).$$

It follows from Lemma 1.4 that polar form of $q \perp r$ is given by

$$B_{q \perp r}(v + v', w + w') = B_q(v, w) + B_r(v', w').$$

If we fix a basis of $V \perp W$ which consists of a basis of V followed by a basis of W, the matrix of $B_{q \perp r}$ is the block matrix

$$M_{q \perp r} = \left(\begin{array}{c|c} M_q & 0 \\ \hline 0 & M_r \end{array}\right).$$

Whence $\mathrm{d}(q \perp r) = \mathrm{d}(q) \cdot \mathrm{d}(r)$.

The orthogonal sum of V and W can also be described as a quadratic space (U, p) which is the direct sum of two orthogonal subspaces V' and W' such that $(V', p \restriction V') \cong (V, q)$ and $(W', p \restriction W') \cong (W, r)$.

Definition. A form which is identically zero is called totally isotropic.

Lemma 1.6. *Every quadratic form can be uniquely decomposed as $q \cong q_{\mathrm{t}} \perp q_{\mathrm{r}}$, where q_{t} is totally isotropic and q_{r} is regular.*

Proof. If V is a quadratic space, write V as the direct sum of $V_{\mathrm{t}} = \mathrm{rad}(V)$ and any complement V_{r}. This sum is orthogonal. V_{t} is totally isotropic and V_{r} is regular. V_{r} is canonically isomorphic with the quotient $V/\mathrm{rad}(V)$, on which q is well-defined by $q(v + \mathrm{rad}(V)) = q(v)$. □

Proposition 1.7. *Let (U, p) be a quadratic space and V a regular subspace. Then V is the orthogonal sum of V and its* orthogonal complement

$$V^{\perp} = \{u \in U \mid u \perp V\}.$$

Proof. Since V is regular, we have $V \cap V^{\perp} = \mathrm{rad}(V) = 0$. On the other hand, we have always $\dim(V^{\perp}) \geq \dim(U) - \dim(V)$, by Linear Algebra. So U is the direct, and orthogonal, sum of V and $V^{\perp}$. □

Remark 1.8. *If U is regular, we have always* $\dim(V^{\perp}) \geq \dim(U) - \dim(V)$.

Proof. Linear Algebra. □

§2 Diagonalisation

Theorem 2.1. *Every quadratic form is equivalent to a* diagonal *form*

$$\langle a_1, \ldots, a_n \rangle = a_1 x_1^2 + \cdots + a_n x_n^2.$$

Clearly the forms $\langle a_1, \ldots, a_n \rangle$ are the quadratic forms with diagonal matrix

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}.$$

Proof. We have to show that every quadratic space (V, q) has an orthogonal basis $v_1, \ldots, v_n$. We do this by induction on the dimension of V. If $q = 0$, every basis is orthogonal. Otherwise, there choose a vector v_1 with $q(v_1) \neq 0$. Split V as the orthogonal sum of Fv_1 and $V' = {v_1}^{\perp}$. By induction V' has an orthogonal basis $v_2, \ldots, v_n$. Then $v_1, v_2, \ldots, v_n$ is an orthogonal basis of V. □

Note that in an orthogonal basis $v_1, v_2, \ldots, v_n$ the quadratic map q has the form $\langle q(v_1), \ldots, q(v_n) \rangle$.

Definition. Let (V, q) be a quadratic space. We say that a field element a is represented by q if a is non-zero and $q(v) = a$ for some $v \in$V. We denote by D(q) the set of elements represented by q.

Corollary 2.2. *An element $a \in \dot{F}$ is represented by q iff q is equivalent to a diagonal form $\langle a, \ldots \rangle$.*

Proof. By the proof of 2.1. □

Here are some rules about diagonal forms:

1. $\langle a_1, \ldots, a_n \rangle$ is regular iff all a_i are non-zero.
2. $\det\langle a_1, \ldots, a_n \rangle = a_1 \cdot \cdots \cdot a_n$
3. $\langle a_1, \ldots, a_m \rangle \perp \langle b_1, \ldots, b_n \rangle \cong \langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle$

§3 Binary quadratic forms

Lemma 1.6 implies

Remark 3.1. *A degenerate binary quadratic form is equivalent to $\langle 0, b\rangle$, where b is unique up to a square.*

Proposition 3.2. *A regular binary form q is equivalent to $\langle a, b\rangle$ iff q represents a and $\mathrm{d}(q) = ab$.*

Proof. If q represents a, it is equivalent to some $\langle a, b'\rangle$ for some b' by Corollary 2.2. If $\mathrm{d}(q) = ab$, we $b' = b$ up to a square. So $\langle a, b'\rangle \cong \langle a, b\rangle$ □

Definition. Let (V, q) be a quadratic space. A vector $v \in V$ is isotropic if $q(v) = 0$. The space V is isotropic if it contains a non-zero isotropic vector.

So a quadratic space is totally isotropic iff all vectors are isotropic.

Definition. The hyperbolic plane $\mathbb{H}$ is the space which belongs to the form $\langle 1, -1\rangle$.

Theorem 3.3. *Let (V, q) be a regular form of dimension 2. Then the following are equivalent:*

a) $V \cong \mathbb{H}$.

b) $\det(q) = -1 \pmod{\dot{F}^2}$

c) V *is isotropic.*

Proof. a)→b) $\det(\mathbb{H}) = -1$

b)→c) The hypothesis implies that q is equivalent to a form $\langle a, -s^2 a\rangle$. This form has the isotropic vector $\begin{pmatrix} s \\ 1 \end{pmatrix}$.

c)→a) Let v_1 be an non-zero isotropic vector. Since q is regular, there is a w such that $b = B(v_1, w) \neq 0$. So for some choice of ϵ and $v_2' = w + \epsilon v_1$ we have

$$q(v_2') = 2\epsilon b + q(w) = 0.$$

If we set $v_2 = \frac{1}{2b} v_2'$, we have $q(v_1) = q(v_2) = 0$ and $B(v_1, v_2) = \frac{1}{2}$. So, in this basis, q is given by the form $x_1 x_2$, and we see that V is a hyperbolic plane. □

Exercise 3.1. *Let $q(x_1, x_2)$ be a binary quadratic form. Then*

1. *q is anisotropic iff q is irreducible.*
2. *q is degenerate if q is a square, up to a unit of F.*

Definition. An orthogonal sum of finitely many hyperbolic planes is called a hyperbolic space.

Corollary 3.4. *Every regular quadratic form q decomposes as*

$$q \cong q_{\mathrm{h}} \perp q_{\mathrm{a}},$$

where q_{h} is the quadratic form of a hyperbolic space and q_{a} is anisotropic.

The form q_{a} is called the *anisotropic part* of q.

Proof. It is enough to show that a regular space V has a hyperbolic plane as an orthogonal direct summand if it is isotropic. Let $v_1 \in V \backslash 0$ be isotropic. Chose w with $B(v_1, w) \neq 0$. The proof of b)→c) of Theorem 3.3 shows that $Fv_1 + Fw$ is a hyperbolic plane. Being regular it is an orthogonal direct summand of V. □

Theorem 3.5 (Witt Decomposition Theorem)**.** *Every quadratic form q decomposes uniquely as*

$$q \cong q_{\mathrm{t}} \perp q_{\mathrm{h}} \perp q_{\mathrm{a}}$$

where q_{t} is totally isotropic, q_{h} is the quadratic form of a hyperbolic space and q_{a} is anisotropic.

Proof. The existence follows immediately from Lemma 1.6 and Corollary 3.4. Uniqueness follows from the Witt Cancellation Theorem of the next section. □

Definition. The Witt-index of q is $\frac{1}{2}\dim(q_h)$, i.e. the number of copies of $\mathbb{H}$ from which q_h is built.

Remark 3.6. *The Witt-index of a regular quadratic space is the dimension of a maximal totally isotropic subspace.*

So all maximal totally isotropic subspaces have the same dimension.

Proof. Let T be a maximal totally isotropic subspace of V. We proceed by induction on $\dim(T)$. If the dimension is 0, we have $V = V_a$ and the Witt-index is 0. Otherwise decompose T as $T = Fv_1 \perp T'$, for some non-zero v_1. Since V is regular and v_1 is not in T', there is a w which is orthogonal to T' but not orthogonal to v_1. Then v_1 and w generate a hyperbolic plane $\mathbb{H}$. Since $\mathbb{H}$ is regular, we have $V = \mathbb{H} \perp V'$ for $V' = \mathbb{H}^{\perp}$. Since T' is a maximal totally isotropic subspace of V', we can apply the induction hypothesis. □

§4 The Witt Cancellation Theorem

Definition. Let V be a quadratic space. A decomposition $V = U \perp W$ gives rise to an automorphism φ of V by $\varphi(u+w) = u - w$. We call φ a generalised reflection.

Lemma 4.1. *Let v and v' be two vectors in V with $q(v) = q(v') \neq 0$. Then there is a generalised reflection of V which maps v to v'.*

Proof. We show first that there is a decomposition $V = U \perp W$ such that, $v + v' \in U$ and $v - v' \in W$. Indeed, $v + v'$ and $v - v'$ are orthogonal since $B(v+v', v-v') = q(v) - q(v') = 0$. So, if for example $q(v+v') \neq 0$, we can take $U = F(v+v')$ and $W = (v+v')^\perp$. It is not possible that both $q(v+v')$ and $q(v-v')$ are zero by the parallelogram identity

$$q(v+v') + q(v-v') = 2q(v) + 2q(v').$$

Let φ be the reflection defined by the decomposition. Then

$$\varphi(v) = \varphi\Big(\frac{(v+v')}{2} + \frac{(v-v')}{2}\Big) = \frac{(v+v')}{2} - \frac{(v-v')}{2} = v'.$$

□

Theorem 4.2 (Witt Cancellation Theorem)**.** *If $q \perp r$ and $q \perp r'$ are equivalent, then so are r and r'.*

Proof. Since q is a sum of 1-dimensional forms, we may assume that $q = \langle a \rangle$. The case $a = 0$ is easy: write $r = r_{\mathrm{t}} \perp r_{\mathrm{r}}$ and $r' = r'_{\mathrm{t}} \perp r'_{\mathrm{r}}$ as in Lemma 1.6. Then $\big(\langle 0 \rangle \perp r_{\mathrm{t}}\big) \perp r_{\mathrm{r}} \cong \big(\langle 0 \rangle \perp r'_{\mathrm{t}}\big) \perp r'_{\mathrm{r}}$ implies $r_{\mathrm{t}} \cong r'_{\mathrm{t}}$ and $r_{\mathrm{r}} \cong r'_{\mathrm{r}}$ by the uniqueness part of Lemma 1.6.

Now assume that $a \neq 0$. The hypotheses means that in a quadratic space V there are two vectors v and v' with $q(v) = q(v') = a$, and the forms r and r' live on the complements $v^\perp$ and $v'^\perp$. By the lemma there is a reflection φ of V which maps v onto v'. Then φ maps $v^\perp$ to $v'^\perp$, and r and r' are equivalent. □

Exercise 4.1. *Let w be an anisotropic vector and ρ_w the reflection which belongs to the decomposition $V = w^\perp Fw$. Show that*

$$\rho_w(v) = v - \frac{2w}{q(w)} B(w, v).$$

Exercise 4.2. *If V is regular, then every isomorphism between two subspaces U and U' extends to an automorphism of V.*

Note that for regular U this follows from the theorem. A special case is that two non-zero v and v' with $q(v) = q(v') = 0$ are conjugate by an automorphism of V.

§5 The Chain Equivalence Theorem

Theorem 5.1 (Witt Chain Equivalence Theorem)**.** *Two diagonal forms are equivalent iff the can be connected by a chain of diagonal forms such that any two subsequent links,* $\langle a_1, \ldots, a_n\rangle$ *and* $\langle a'_1, \ldots, a'_n\rangle$*, are the same, except that the may differ for some index* i *where* $\langle a_i\rangle \cong \langle a'_i\rangle$*, or for some pair of distinct indices* i *and* j *where* $\langle a_i, a_j\rangle \cong \langle a'_i, a'_j\rangle$

Proof. All forms occurring in this proof are now meant to be diagonal. We call two forms *chain-equivalent* if they can be connected by a chain as in the theorem.
Claim: *A form which represents* b *is chain-equivalent to form* $\langle b\rangle + s'$.
Proof of the claim: Assume that $q = \langle a\rangle + q'$ represents b. There are two cases.
Case 1. $\langle a\rangle$ represents b, Then $\langle a\rangle$ and $\langle b\rangle$ are equivalent and so q and $\langle b\rangle + q'$ are chain-equivalent.
Case 2. $\langle a\rangle$ does not represent b. Then $b = ax^2 + a'$, where a' is represented by q'. Induction on the dimension yields that q' is chain-equivalent to a form $\langle a'\rangle + q''$, and so q is chain-equivalent to $\langle a, a'\rangle + q''$. By Proposition 3.2 the forms $\langle a, a'\rangle$ and $\langle b, aa'b\rangle$ are equivalent and so $\langle a, a'\rangle + q''$ is chain-equivalent to $\langle b, aa'b\rangle + q''$. It follows that q is chain-equivalent to $\langle b\rangle + \langle aa'b\rangle + q''$.
Proof of the theorem: Assume that $q \cong r$. If $r = 0$, then also $q = 0$ and q and r are chain-equivalent. If r is not 0, using $\langle 0, b\rangle \cong \langle b, 0\rangle$, we see that r is chain-equivalent to a form $\langle b\rangle + r'$ for some non-zero b. Now q represents b. So q is chain-equivalent to a form $\langle b\rangle + q'$. It follows from Cancellation that $q' \cong r'$ and by induction, that q' and r' are chain-equivalent, which implies that q and r are chain-equivalent. □

Chapter 2

The Witt ring of F

§6 The Witt-Grothendieck ring

Definition. Let (V, q) and (W, r) be two quadratic spaces with polar forms B_q and B_r. Then $V \otimes_F W$ carries a quadratic form $q \otimes r$ with polar form defined by

$$(B_q \otimes B_r)(v \otimes w, v' \otimes w') = B_q(v, v') \cdot B_r(w, w').$$

$B_q \otimes B_r$ is a well-defined bilinear form, since $B_q(v, v') \cdot B_r(w, w')$ is a multilinear function of v, v', w, w'. It is symmetrical on pure tensors $v \otimes w$ and therefore symmetrical on $V \otimes_F W$.

Exercise 6.1. *Let $m = \dim(n)$ and $n = \dim(r)$. If the determinants of q and r are computed for the bases (v_i) and (w_j), and the determinant of $q \otimes r$ for the basis $(v_i \otimes w_j)$, then* $\det(q \otimes r) = \det(q)^n \cdot \det(r)^m$.

Lemma 6.1.

$$\langle a_1, \ldots, a_m \rangle \otimes \langle b_1, \ldots, b_n \rangle \cong \langle a_1 b_1, \ldots, a_i b_j, \ldots, a_m b_n \rangle$$

Proof. If (v_i) is an orthogonal basis of V and (w_j) an orthogonal basis of W, then $(v_i \otimes w_j)$ is an orthogonal basis of $V \otimes_F W$. If $q(v_i) = a_i$ and $r(w_j) = b_j$, we have $(q \otimes r)(v_i \otimes w_j) = B_q(v_i, v_i) \cdot B_r(w_j, w_j) = a_i b_j$. □

Corollary 6.2. $\mathrm{d}(q \otimes r) = \mathrm{d}(q)^{\dim(r)} \cdot \mathrm{d}(r)^{\dim(q)}$

This follows of course also from Exercise 6.1.

Definition. A half-ring is a structure $(R, +, \cdot, 0, 1)$ where $(R, +, 0)$ and $(R, \cdot, 1)$ are commutative monoids, satisfying $(x + y) \cdot z = x \cdot z + y \cdot z$ and $0 \cdot x = 0$.

If $(R, +, 0)$ is a *cancellation* semi-group, i.e. $x + y = x' + y \Rightarrow x = y'$, then $0 \cdot x = 0$ follows from the other axioms since $(0 \cdot x) + (0 \cdot x) = (0 + 0) \cdot x = 0 \cdot x = 0 + (0 \cdot x)$.

The free half-ring generated by $a_1, \ldots, a_n$ is $\mathbb{N}[a_1, \ldots, a_n]$, i.e. the set of all polynomials in $\mathbb{Z}[a_1, \ldots, a_n]$ without negative coefficients.

Proposition 6.3. *The set of equivalence classes of quadratic forms over F are a half-ring under the operations $q + r = q \perp r$ and $q \cdot r = q \otimes r$. The additive semi-group has cancellation.*

Proof. This can easily be checked using diagonal forms, see page 6 and Lemma 6.1. Note that $0 = \langle\rangle$ and $1 = \langle 1\rangle$. Actually the equations to be verified come from natural isomorphisms. For example the natural vector space isomorphism between $(U \oplus V) \otimes_F W$ and $(U \otimes_F W) \oplus (V \otimes_F W)$ yields an isometry between $(p \perp q) \otimes r$ and $(p \otimes r) \perp (q \otimes r)$. That the additive semi-group has cancellation is the Witt Cancellation Theorem 4.2. □

Lemma 6.4. *Let $(R, +, \cdot, 0, 1)$ be any structure with two operations and two constants. Then there is unique homomorphism γ from R into a commutative ring*[1] *$G(R)$ such that every homomorphism from R into a ring S is the composition of γ and a unique homomorphism $G(R) \to S$. The ring $G(R)$ is called the* Grothendieck ring *of R.*

The *Grothendieck group* of a structure $(R, +, 0)$ is defined similarly.

Proof. Let $\mathcal{R} = \mathbb{Z}[g(r)]_{r \in R}$ be the free commutative ring generated by symbols $g(r)$, for $r \in R$. Let I be the ideal generated by all the elements $g(r+s) - g(r) - g(s)$, $g(rs) - g(r)g(s)$, $g(0)$, $g(1) - 1$. Set $G(R) = \mathcal{R}/I$ and $\gamma(r) = g(r) + I$. □

Note that $G(R)$ is generated by the $\gamma(r)$ as a ring.

Lemma 6.5. 1. *A cancellation monoid $(R, +, 0)$ is embedded in its Grothendieck group.*

2. *Let $(R, +, \cdot, 0, 1)$ be a half-ring and $(G(R), +, \cdot, 0, 1)$ its Grothendieck ring. Then $(G(R), +, 0)$ is the Grothendieck group of $(R, +, 0)$.*

Proof. 1. The Grothendieck group of a cancellation monoid $(R, +, 0)$. consists of equivalence classes of pairs (r, s), where $(r, s) \sim (r', s')$ if $r + s' = r' + s$. The embedding is given by $\gamma(r) = (r, 0)/\sim$.

2. We start with the Grothendieck group $\gamma : R \to G$ of $(R, +, 0)$ and show that G carries a unique ring structure for which γ is a ring homomorphism. This must then be the Grothendieck ring of R.

For this note that G is the set of all differences $\gamma(r) - \gamma(s)$. So we have to show that

$$\big(\gamma(r) - \gamma(s)\big) \bullet \big(\gamma(r') - \gamma(s')\big) = \gamma(r \cdot r' + s \cdot s') - \gamma(r \cdot s' + s \cdot r') \tag{6.1}$$

defines a ring multiplication on G. For every r the map $x \mapsto \gamma(r \cdot x)$ is a homomorphism from R to G. So there is an endomorphism $\lambda_r : G \to G$ with $\gamma(r \cdot x) = \lambda_r(\gamma(x))$. Then the right hand side of (6.1) equals $(\lambda_r - \lambda_s)\big(\gamma(r') - \gamma(s')\big)$, which shows that $\bullet$ is well-defined by (6.1). The rest is easy to check.[2] □

Definition. The Witt-Grothendieck ring $\widehat{\mathrm{W}}(F)$ is the Grothendieck ring of the half-ring of equivalence classes of *regular* quadratic forms over F.

[1] All rings considered (also non-commutative ones) have an identity 1, and all ring homomorphism considered preserve the identity.

[2] The axiom $0 \cdot x = 0$ is not used in the proof.

Corollary 6.6. *1. Every element of $\widehat{\mathrm{W}}(F)$ has the form $q - r$ for regular forms q and r.*

2. $q - r = q' - r' \;\Leftrightarrow\; q \perp r' \cong r \perp q'$.

Lemma 6.7. *The ideal generated by $\mathbb{H}$ is $\mathbb{Z}\cdot\mathbb{H}$, i.e. the additive group generated by $\mathbb{H}$.*

Proof. From $\langle a\rangle \otimes \mathbb{H} \cong \langle a, -a\rangle \cong \mathbb{H}$ follows that $q \cdot \mathbb{H} \cong \dim(q) \cdot \mathbb{H}$. So in $\widehat{\mathrm{W}}(F)$ we have $(q - r) \cdot \mathbb{H} = (\dim(q) - \dim(r)) \cdot \mathbb{H}$. □

Definition. The Witt ring of F is the quotient

$$\mathrm{W}(F) = \widehat{\mathrm{W}}(F)/(\mathbb{Z} \cdot \mathbb{H}).$$

Lemma 6.8. *Every element of $\mathrm{W}(F)$ is of the form $q + \mathbb{Z} \cdot \mathbb{H}$ for a unique anisotropic form q.*

So the Witt ring is in bijection with the set of equivalence classes of anisotropic forms.

Proof. We have to show that in $W(F)$ every $q - r$ equals a unique anisotropic form. Indeed, since$-\langle 1\rangle = \langle -1\rangle$ modulo $\mathbb{Z} \cdot \mathbb{H}$, we have $q - r = q + \langle -1\rangle \cdot r$ in $\mathrm{W}(F)$. Decompose $s = q + \langle -1\rangle \cdot r$ as $s_\mathrm{h} + s_\mathrm{a}$. Then $q - r = s_\mathrm{a}$ in $\mathrm{W}(F)$. If two anisotropic forms s_1 and s_2 are equal in $\mathrm{W}(F)$, then $s_1 = n \cdot \mathbb{H} + s_2$ or $s_2 = n \cdot \mathbb{H} + s_2$ for some $n \in \mathbb{N}$. This is only possible if $n = 0$. □

We call two quadratic forms q and r *Witt equivalent* if they are equal in $\mathrm{W}(F)$, and denote this by $q \sim r$. Then we have

Corollary 6.9. *1. Two regular forms are Witt equivalent iff their anisotropic parts are isomorphic.*

2. Two regular forms of the same dimension are Witt equivalent iff they are equivalent.

Proof. 1. A regular form is Witt equivalent to its anisotropic part.

2. Decompose $q^i = q^i_\mathrm{h} + q^i_\mathrm{a}$. Then $q^1 \cong q^2$ iff $\dim(q^1_\mathrm{h}) = \dim(q^2_\mathrm{h})$ and $q^1_\mathrm{a} \cong q^2_\mathrm{a}$ iff $\dim(q^1) = \dim(q^2)$ and $q^1 \sim q^2$. □

§7 Presentation by generators and relations

Proposition 7.1. *The additive group of $\widehat{\mathrm{W}}(F)$ is presented as an abelian group by*

generators: a symbol $[a]$ for each $a \in \dot{F}$

(7.2) *relations:* $[ab^2] = [a]$

(7.3) $[a] + [b] = [a+b] + [(a+b)ab]$, *if* $a + b \neq 0$

Proof. Let A be the abelian group presented by the generators and relations. Since the relations are true for the generators $\langle a\rangle$ of $\widehat{\mathrm{W}}(F)$, the assignment $[a] \mapsto \langle a\rangle$ defines an epimorphism $A \to \widehat{\mathrm{W}}(F)$. We show that the kernel is trivial. So let $[a_1] + \cdots + [a_m] - [b_1] - \cdots - [b_n]$ be mapped to 0. Then $\langle a_1, \ldots, a_m\rangle$ and $\langle b_1, \ldots, b_n\rangle$ are isomorphic. It follows that $m = n$. By the Witt Chain Equivalence Theorem 5.1 we have only to consider the cases $n = 1$ and $n = 2$. If $\langle a_1\rangle \cong \langle b_1\rangle$, we have $a_1 = s^2 b_1$, so $[a_1] - [b_1] = 0$ in A by (7.2). If $\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle$, we have $b_1 = a_1 x_1^2 + b_2 x_2^2$ and $a_1 a_2 = b_1 b_2 \pmod{\dot{F}^2}$. Using (7.2) and (7.3) this gives

$$[a_1] + [a_2] = [a_1 x_1^2] + [a_2 x_2^2] = [b_1] + [b_1(a_1 x_1^2 a_2 x_2^2)] = [b_1] + [b_2].$$

□

Corollary 7.2. *The additive group of $\mathrm{W}(F)$ is presented as an abelian group by the same generators and relations as $\widehat{\mathrm{W}}(F)$ plus the relation*

$$[-1] = -[1].$$

Proof. This is clear since $\mathrm{W}(F)$ is $\widehat{\mathrm{W}}(F)$ modulo the additive subgroup generated by $\langle 1\rangle + \langle -1\rangle$. □

Proposition 7.3. *The ring $\widehat{\mathrm{W}}(F)$ is a presented as a commutative ring by*

generators: a symbol $[a]$ for each $a \in \dot{F}$

(7.3) *relations:* $[a] + [b] = [a+b] + [(a+b)ab]$, *if* $a + b \neq 0$

(7.4) $[ab] = [a][b]$

(7.5) $[1] = 1$

Proof. We prove first that the relations (7.2), or $[b^2] = 1$, hold in the commutative ring R presented by the generators and relations. For this we compute $[b] + [b]$ in two ways. First we have

$$[b] + [b] = [b+b] + [(b+b)bb] = [2b] + [2b^3].$$

For $b = 1$ this yields $2 = 2[2]$, which implies

$$[b] + [b] = 2[b] = 2[2][b] = 2[2b].$$

So we have $[2b] = [2b^3]$ and multiplication with $[\frac{1}{2b}]$ yields $1 = [1] = [b^2]$.

Since the relations are true for the generators $\langle a\rangle$ of $\widehat{\mathrm{W}}(F)$, the assignment $[a] \mapsto \langle a\rangle$ defines a surjective ring epimorphism $R \to \widehat{\mathrm{W}}(F)$. By the above the map $A \to \widehat{\mathrm{W}}(F)$ (see the proof of 7.1) factors through the map $R \to \widehat{\mathrm{W}}(F)$, which is therefore injective. □

Corollary 7.4. *The ring* $\mathrm{W}(F)$ *is presented as a commutative ring by the same generators and relations as* $\widehat{\mathrm{W}}(F)$ *plus the relation*

$$[-1] = -[1].$$

□

§8 The fundamental ideal

Dimension is a homomorphism from the half-ring of regular quadratic forms to $\mathbb{Z}$. So, the formula

$$\dim(q - r) = \dim(q) - \dim(r),$$

extends it to a ring homomorphism $\dim : \widehat{\mathrm{W}}(F) \to \mathbb{Z}$.

Definition. The fundamental ideal $\widehat{\mathrm{I}}F$ of $\widehat{\mathrm{W}}(F)$ is the kernel of dim.

Lemma 8.1. *$\widehat{\mathrm{I}}F$ is additively generated by the expressions $\langle 1\rangle - \langle a\rangle$, where $a \in \dot{F}$.*

Proof. $\langle a_1, \dots, a_n\rangle - \langle b_1, \dots, b_n\rangle = \sum_{i=1}^{n}(\langle 1\rangle - \langle a_i\rangle) - \sum_{i=1}^{n}(\langle 1\rangle - \langle b_i\rangle)$. □

The determinant d being a homomorphism from the semigroup of regular quadratic forms to $\dot{F}/\dot{F}^2$ extends to an additive[3] homomorphism

$$\mathrm{d} : \widehat{\mathrm{W}}(F) \to \dot{F}/\dot{F}^2$$

If we give the additive group $\mathbb{Z} \times \dot{F}/\dot{F}^2$ a ring structure[4] by using the trivial multiplication on $\dot{F}/\dot{F}^2$,

$$(z, \epsilon) \cdot (z', \epsilon') = \big(zz', \epsilon^{z'}(\epsilon')^{z}\big),$$

we have a ring homomorphism

$$(\dim, \mathrm{d}) : \widehat{\mathrm{W}}(F) \to \mathbb{Z} \times \dot{F}/\dot{F}^2$$

by Corollary 6.2. [5]

Proposition 8.2. *The homomorphism* $(\dim, \mathrm{d})$ *induces an isomorphism*

$$\widehat{\mathrm{W}}(F)/\widehat{\mathrm{I}}^2F \to \mathbb{Z} \times \dot{F}/\dot{F}^2.$$

Proof. The map $(\dim, \mathrm{d})$ is sujective since $(\dim, \mathrm{d})\big((z-1)\cdot\langle 1\rangle + \langle a\rangle\big) = (z, a)$. So it remains to show that $\widehat{\mathrm{I}}^2F$ is the kernel. One inclusion is clear: $\widehat{\mathrm{I}}^2F$ is additively generated by the products

$$\big(\langle 1\rangle - \langle a\rangle\big)\cdot\big(\langle 1\rangle - \langle b\rangle\big) = \langle 1, ab\rangle - \langle a, b\rangle. \tag{8.6}$$

$\langle 1, ab\rangle$ and $\langle a, b\rangle$ have the same dimension and determinant. So $\widehat{\mathrm{I}}^2F$ is contained in the kernel.

Claim: *Every element of $\widehat{\mathrm{W}}(F)$ is modulo $\widehat{\mathrm{I}}^2F$ equivalent to an element of the form $(z-1)\cdot\langle 1\rangle + \langle a\rangle$.* Proof: Modulo $\widehat{\mathrm{I}}^2F$ we have $\langle a\rangle + \langle b\rangle \equiv \langle 1\rangle + \langle ab\rangle$ and $\langle a\rangle - \langle b\rangle \equiv -\langle 1\rangle + \langle ab\rangle$.

Now let s be in the kernel. By the claim we may assume that $s = (z-1)\langle 1\rangle + \langle a\rangle$. Then $z = 0$ and $a \equiv 1 \pmod{\dot{F}}$ and $s = 0$ is in $\widehat{\mathrm{I}}^2F$. □

[3] i.e. $\mathrm{d}(q + r) = \mathrm{d}(q)\,\mathrm{d}(r)$

[4] Let R be a commutative ring and A be an R-module. The set of all formal sums $r + a$ is a ring with the obvious addition and the multiplication $(r + a)\cdot(r' + a') = rr' + (r'a + ra')$.

[5] That this is a well definined homomorphism follows also from Proposition 7.3. Simply check that elements $(\dim, \mathrm{d})(\langle a\rangle)$ satisfy the relations. The relation (7.4) for example is true since $(\dim, \mathrm{d})(\langle ab\rangle) = (1, ab) = (1, a)\cdot(1, b) = (\dim, \mathrm{d})(\langle a\rangle)\cdot(\dim, \mathrm{d})(\langle a\rangle)$.

Since $\dim(\mathbb{H}) = 2$, the dimension function descends to a ring homomorphism $\dim_0 : \mathrm{W}(F) \to \mathbb{Z}/2\mathbb{Z}$.

Definition. The fundamental ideal $\mathrm{I}F$ of $\mathrm{W}(F)$ the kernel of $\dim_0$.

Lemma 8.3. *In the diagram*

$$\begin{array}{ccccc} \widehat{\mathrm{I}}F & \to & \widehat{\mathrm{W}}(F) & \to & \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{I}F & \to & \mathrm{W}(F) & \to & \mathbb{Z}/2\mathbb{Z} \end{array}$$

the map $\widehat{\mathrm{I}}F \to \mathrm{I}F$ is a bijection.

Proof. The ideals $\mathbb{Z} \cdot \mathbb{H}$ and $\widehat{\mathrm{I}}F$ intersect trivially, so the map is injective. The ideal $\mathrm{I}F$ consists of the classes of even dimensional forms q. Write $q = p + r$, where p and r are forms of the same dimension. Then in $\mathrm{W}(F)$ we have $q = p - \langle -1 \rangle \cdot r$, and $p - \langle -1 \rangle \cdot r \in \widehat{\mathrm{I}}F$. □

Corollary 8.4. $\mathrm{I}F$ *is additively generated by forms* $\langle 1, a \rangle$.

Proof. This follow from Lemma 8.1, since in $\mathrm{W}(F)$ we have $\langle 1 \rangle - \langle a \rangle = \langle 1, -a \rangle$. □

Corollary 8.5. $\mathrm{I}^n F$, *the n-th power of* $\mathrm{I}F$, *is additively generated by n-fold* Pfister forms

$$\langle\langle a_1, \ldots, a_n \rangle\rangle = \langle 1, a_1 \rangle \cdot \cdots \cdot \langle 1, a_n \rangle.$$

□

By convention $\langle\langle\ \rangle\rangle = \langle 1 \rangle$.

The determinant d is not well defined on $\mathrm{W}(F)$ since $\dot{(}\mathbb{H}) = -1$. So we define for any $s \in \widehat{\mathrm{W}}(F)$

$$\mathrm{d}_\pm(s) = (-1)^{\frac{n(n-1)}{2}} \mathrm{d}(s).$$

Lemma 8.6. $\mathrm{d}_\pm(s)$ *depends only on the class of s in* $\mathrm{W}(F)$.

Proof. We have to show that $\mathrm{d}_\pm(s) = \mathrm{d}_\pm(s + \mathbb{H})$. This means that $(-1)^{\frac{n(n-1)}{2}}$ changes its sign, or $\frac{n(n-1)}{2}$ changes its parity, if n is increased by 2. This follows from the table

$n \pmod 4$	0	1	2	3
$\frac{n(n-1)}{2} \pmod 2$	0	0	1	1

or, for positive n, from the formula $\frac{n(n-1)}{2} = \sum_{i=1}^{n-1} i$. □

Note that $\mathrm{d}_\pm$ does not define a homomorphism from the additive group of $\mathrm{W}(F)$ to $\dot{F}/\dot{F}^2$, since $\frac{n(n-1)}{2}$ is not a homomorphism from $\mathbb{Z}$ to $\{1, -1\}$.

Let K be the additive subgroup of $\mathbb{Z} \times \dot{F}/\dot{F}^2$ which is generated by $(2, -1)$. This is actually an ideal since $(z, \epsilon) \cdot (2, -1) = \big(2z, (-1)^z\big) \in K$ for all z and ϵ. Let Q be the quotient $(\mathbb{Z} \times \dot{F}/\dot{F}^2)/K$. We have with this notation.

Proposition 8.7. *The homomorphism* $(\dim, \mathrm{d})$ *induces an isomorphism* $\mathrm{W}(F)/\mathrm{I}^2 F \to \mathrm{Q}$.

Proof. This follows from Proposition 8.2 as follows. The homomorphism $(\dim, \mathrm{d})$ maps $\mathbb{H}$ to $(2,-1)$. This implies that the inverse image of K is $\widehat{\mathrm{I}}^2F + \mathbb{Z}\mathbb{H}$. On the other hand $\widehat{\mathrm{W}}(F) \to \mathrm{W}(F)$ maps $\widehat{\mathrm{I}}^2F$ onto I^2F. so we have $\mathrm{W}(F)/\mathrm{I}^2F \cong \widehat{\mathrm{W}}(F)/\big(\widehat{\mathrm{I}}^2F + \mathbb{Z}\mathbb{H}\big) \cong \big(\mathbb{Z} \times \dot{F}/\dot{F}^2\big)/K \cong \mathrm{Q}$. □

The embedding $\dot{F}/\dot{F}^2 \to (\mathbb{Z}\times\dot{F}/\dot{F}^2)$ and the projection $(\mathbb{Z}\times\dot{F}/\dot{F}^2) \to \mathbb{Z}/2\mathbb{Z}$ induce a short exact sequence

$$\dot{F}/\dot{F}^2 \to \mathrm{Q} \to \mathbb{Z}/2\mathbb{Z}.$$

Remark 8.8. *The sequence splits iff* $-1 \in \dot{F}^2$.

We will describe the structure of Q in Exercise 9.3, depending on wether the sequence splits or not.

Proof. The sequence splits iff there is a section $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Q}$, which means that $1+2\mathbb{Z}$ can be lifted to an element $(2n+1,\epsilon)$ which has order 2 in Q, or $(2(2n+1),1) \in K$. This is equivalent to $1 = -1$ in $\dot{F}/\dot{F}^2$. □

Let Q' the cartesian product $\mathbb{Z}/2\mathbb{Z} \times \dot{F}/\dot{F}^2$. Define a bijection $\mathrm{Q}' \to \mathrm{Q}$ by

$$(\bar{n},\epsilon) \mapsto (n,\epsilon)\cdot K, \qquad \text{for } n = 0,1 \text{ and } \bar{n} = n + 2\mathbb{Z}$$

and pull back the operations from Q. This yields, for $e, e' \in \mathbb{Z}/2\mathbb{Z}$,

$$\begin{aligned}(e,\epsilon) + (e',\epsilon') &= \big(e+e', (-1)^{ee'}\epsilon\epsilon'\big)\\ (e,\epsilon)\cdot(e',\epsilon') &= \big(ee', \epsilon^{e'}(\epsilon')^{e}\big).\end{aligned}$$

The n-fold sum of $(\bar{1},1)$ computed with the addition formula is

$$(\bar{n}, (-1)^1(-1)^2\cdots(-1)^{n-1}) = \big(\bar{n}, (-1)^{\frac{n(n-1)}{2}}\big).$$

So, the inverse map $\mathrm{Q} \to \mathrm{Q}'$ is given by $(n,\epsilon)\cdot K \mapsto \big(\bar{n}, (-1)^{\frac{n(n-1)}{2}}\epsilon\big)$.

Corollary 8.9. *The pair* $(\dim_0, \mathrm{d}_\pm)$ *defines an isomorphism* $\mathrm{W}(F)/\mathrm{I}^2F \to \mathrm{Q}'$.

Corollary 8.10. *A regular form* q *of dimension* n *is in* I^2F *iff* n *is even and* $\mathrm{d}(q) = (-1)^{\frac{n(n-1)}{2}}$.

Corollary 8.11.

$$\mathrm{I}F/\mathrm{I}^2F \cong \dot{F}/\dot{F}^2$$

Proof. The ideal $\mathrm{I}F$ is the kernel of the composite map $W(F) \to \mathrm{Q} \to \mathbb{Z}/2\mathbb{Z}$ and therefore the inverse image of the kernel of $\mathrm{Q} \to \mathbb{Z}/2\mathbb{Z}$, which is $\dot{F}/\dot{F}^2$. □

Corollary 8.12. *For a field* F *the following are equivalent:*

a) $\widehat{\mathrm{W}}(F)$ *is noetherian.*

b) $\mathrm{W}(F)$ *is noetherian.*

c) $\dot{F}/\dot{F}^2$ *is finite.*

Proof. a)→b) Homomorphic images of noetherian rings are noetherian again.

b)→c) $\mathrm{I}F/\mathrm{I}^2F \cong \dot{F}/\dot{F}^2$ is a $\mathrm{W}(F)/\mathrm{I}F \cong \mathbb{Z}/2\mathbb{Z}$-module. If $\mathrm{W}(F)$ is noetherian, this module is finitely generated and therefore finite.

c)→a) If $\dot{F}/\dot{F}^2$ is finite, there are only finitely many 1-dimensional forms. So $\widehat{\mathrm{W}}(F)$ is finitely generated – even as an abelian group. □

§9 Examples

9.1 Quadratically closed fields

Definition. A field F is quadratically closed if every element is a square.

Proposition 9.1. *Let F be a quadratically closed field. Then*

1. *Regular quadratic forms are equivalent iff they have the same dimension.*
2. $\dim : \widehat{\mathrm{W}}(F) \to \mathbb{Z}$ *is a ring isomorphism.*
3. $\dim_0 : \mathrm{W}(F) \to \mathbb{Z}/2\mathbb{Z}$ *is a ring isomorphism.*

Proof. 1. Each regular diagonal form $\langle a_1, \ldots, a_n\rangle$ is equivalent to $\langle \underbrace{1, \ldots, 1}_{n}\rangle$.

2. Consider an element $q - r$ of $\widehat{\mathrm{W}}(F)$. If $\dim(q-r) = 0$, we have $\dim(q) = \dim(r)$ and therefore $q \cong r$, and $q - r = 0$ in $\widehat{\mathrm{W}}(F)$. This shows that the kernel of dim is trivial.

3. The isomorphism in 2. maps $\mathbb{Z} \cdot \mathbb{H}$ to $2\mathbb{Z}$. □

Exercise 9.1. *To be quadratically closed is necessary for each of the three statements of the proposition.*

9.2 Euclidean fields

Definition. A field is formally real if -1 is not a sum of squares. A formally real field is euclidean if every element or its negative is a square.

Formally real fields are fields which have an *ordering*. That is a linear order satisfying $x < y \;\Rightarrow\; x + z < y + z$ and $x < y \wedge 0 < z \;\Rightarrow\; xz < yz$. A Euclidean field F has a unique ordering, given by $x < y \;\Leftrightarrow\; y - x \in \dot{F}^2$.

Proposition 9.2. *Let F be an euclidean field. Then*

1. *For each positive n there are, up to equivalence, exactly two anisotropic forms: $n \cdot \langle 1\rangle = \langle \underbrace{1, \ldots, 1}_{n}\rangle$ and $n \cdot \langle -1\rangle = \langle \underbrace{-1, \ldots, -1}_{n}\rangle$.*
2. *$\widehat{\mathrm{W}}(F)$ is the group ring $\mathbb{Z}[G]$, where $G = \{\langle 1\rangle, \langle -1\rangle\}$.*
3. $\mathrm{W}(F) \cong \mathbb{Z}$. *For regular diagonal forms the isomorphism is given by the* signature

$$\sigma(\langle a_1, \ldots, a_n\rangle) = (\#\ \textit{of positive } a_i\textit{'s}) - (\#\ \textit{of negative } a_i\textit{'s}).$$

For a group G the *group ring* $\mathbb{Z}[G]$ is a ring which contains G as a multiplicative subgroup, with 1 as identity, which is a basis of the ring as a free abelian group. This means that every element can uniquely be written as $\sum_{g \in G} z_g g$, with $z_g \in \mathbb{Z}$. This exists also for non-commutative groups G.

Proof. Since $\dot{F}/\dot{F}^2 = \{1, -1\}$, every regular form is equivalent to a form

$$n_+ \cdot \langle 1\rangle + n_- \cdot \langle -1\rangle =< \langle \underbrace{1, \ldots, 1}_{n_+} \underbrace{-1, \ldots, -1}_{n_-}\rangle. \tag{9.7}$$

Such a form can only be isotropic if $n_+ = 0$ or $n_- = 0$. Since F is formally really, the forms $n_+ \cdot \langle 1\rangle$ and $n_- \cdot \langle -1\rangle$ are anisotropic indeed and non-isomorphic, except of course if $n_+ = n_- = 0$. This proves 1.

It follows now from the Cancellation Theorem (or the Decomposition Theorem 3.5) that in the forms (9.7) the numbers n_+ and n_- are uniquely determined. So the half-ring of equivalence classes of regular forms is $\mathbb{N}[G]$ and 2. follows immediately.

The isomorphism in 2. maps the class of $\mathbb{H}$ to $1 + \langle -1\rangle$. This element generates the kernel of the homomorphism $\widehat{\mathrm{W}}(F) \to \mathbb{Z}$ which maps $\langle -1\rangle$ to -1. □

Sylvester's *Inertia Law* states that in every ordered field equivalent diagonal forms have the same signature. For euclidean fields this is the uniqueness of the numbers n_+ and n_- in (9.7). The general case follows from the fact that every ordered field can be embedded in a euclidean field, with the order preserved.

Exercise 9.2. *To be euclidean is necessary for each of the three statements of the proposition.*

9.3 Fields where every regular binary form is universal

Definition. A quadratic form which represents every non-zero element of F is called universal.

The hyperbolic plane is universal since its quadratic form is equivalent to x_1x_2, see the example on p. 2. Since every regular isotropic form contains a hyperbolic plane (see Theorem 3.5), this implies that every regular isotropic form is universal

Lemma 9.3. *Let $F = \mathbb{F}_q$ be a finite field (of odd characteristic). Then*

1. $|\dot{F}/\dot{F}^2| = 2$
2. -1 *is a square in* F *iff* $q \equiv 1 \pmod 4$.

Proof. Since the characteristic is odd, the element -1 is different from 1 and the only element of order 2. The kernel of the squaring map $\dot{F} \to \dot{F}^2$ is $\{1, -1\}$, so we have $|\dot{F}^2| = \frac{q-1}{2}$. That -1 is a square is equivalent to the existence of an element of order 4. Since $\dot{F}$ is a cyclic group of order $q - 1$, this is means that 4 divides $q - 1$. □

Corollary 9.4. *In a finite field every regular binary quadratic form is universal.*

Proof. Let $\langle a, b\rangle$ be regular and $c \in F = \mathbb{F}_q$. Since both sets aF^2 and $c - bF^2$ have $\frac{q+1}{2}$ elements, they intersect. So there are x and y with $ax^2 = c - by^2$, or $c = ax^2 + by^2$. □

Theorem 9.5. *Let F a field where every regular binary form is universal. Then*

1. *Regular quadratic forms are equivalent iff they have the same dimension and the same determinant up to a square.*

2. $(\dim, \mathrm{d}) : \widehat{\mathrm{W}}(F) \to \mathbb{Z} \times \dot{F}/\dot{F}^2$ *is a ring isomorphism.*

3. $\mathrm{W}(F) \cong \mathrm{Q}$.

Proof. The hypothesis implies, and is actually equivalent to, that a regular form $\langle a, b\rangle$ is equivalent to $\langle 1, ab\rangle$. Then, every regular form is equivalent to a form $(z-1)\cdot\langle 1\rangle + \langle a\rangle$, see the proof of Proposition 8.2. For example

$$\langle a, b, c\rangle \cong \langle 1, ab, c\rangle \cong \langle 1, 1, abc\rangle.$$

Such a form is determined by its dimension z and determinant a. This proves 1. and implies that the homomorphism $\widehat{\mathrm{W}}(F) \to \mathbb{Z} \times \dot{F}/\dot{F}^2$ is injective, which is 2.

We can deduce 2. also from 8.2 since the forms (8.6) are zero. The last assertion follow immediately from 2. as in the proof of 8.2. □

Corollary 9.6. *Let $F = \mathbb{F}_q$ be a field of odd characteristic. Then*

1. *If $q \equiv 1 \pmod 4$, then $\mathrm{W}(F) \cong \mathbb{Z}/2\mathbb{Z}[\dot{F}/\dot{F}^2]$.*

2. *If $q \equiv 3 \pmod 4$, then $\mathrm{W}(F) \cong \mathbb{Z}/4\mathbb{Z}$.*

Proof. Write $(\dot{F}/\dot{F}^2, \cdot)$ additively as $\{0, s\}$. Then $Z/2 \times \dot{F}/\dot{F}^2$ is the the free ring $\mathbb{Z}[s]$ generated by s subjected to the relations $2s = 0$ and $s^2 = 0$. Let s' be the element $-1 \cdot \dot{F}$. Then ideal K is the set of all $2z + zs'$.

If $q \equiv 1 \pmod 4$, then $s' = 0$. So Q is a $\mathbb{Z}/2\mathbb{Z}$-algebra with basis $1, s$ and multiplication defined by $s^2 = 0$. The elements $1, 1+s$ are also a basis and $(1+s)^2 = 1$. So Q is the group-ring $\mathbb{Z}/2\mathbb{Z}[\{1, 1+s\}]$, and $\{1, 1+s\}$ is isomorphic to $\dot{F}/\dot{F}^2$.

If $q \equiv 3 \pmod 4$, then $s' = s$. Then Q is the ring freely generated by s with the relations $2s = 0$, $s^2 = 0$ and $2 + s = 0$. So we can replace s by -2 and get the relations $2(-2) = 0$ and the equivalent $(-2)^2 = 0$. This defines $\mathbb{Z}/4\mathbb{Z}$. □

Exercise 9.3. *Show for arbitrary F that $\mathrm{Q} \cong (\mathbb{Z}/2\mathbb{Z})[\dot{F}/\dot{F}^2]$ if -1 is a square, and $\mathrm{Q} \cong (\mathbb{Z}/4\mathbb{Z})[\dot{F}/\pm\dot{F}^2]$ otherwise.*

Theorem 9.7. *If k is algebraically closed, then in the rational function field $F = k(t)$ every regular binary form is universal.*

For the proof we need some preparations.

Definition. A quadratic form q is a group form if $\mathrm{D}(q)$, the set of elements represented by q, is a subgroup of $\dot{F}$.

Note that $\mathrm{D}(q)$ is closed under multiplication with elements of $\dot{F}^2$. So, if x is in $D(q)$, then $x^{-1} = x\cdot(x^{-1})^2$ is also in $\mathrm{D}(q)$. Note also that group forms represent 1, so are equivalent to forms $\langle 1, a_2, \ldots, a_n\rangle$.

Lemma 9.8. *For arbirary F, The Pfister form $\langle 1, a\rangle$ is a group form.*

This is true for all Pfister forms, see Corollary 10.2.

Proof. If b is represented by $q = \langle 1, a\rangle$, the form q is equivalent to $\langle b, ba\rangle = \langle b\rangle \cdot q$. So $\mathrm{D}(q) = b \cdot \mathrm{D}(q)$. □

Another proof is to represent q as the norm form of a 2-dimensional algebra[6] A over F. Let A have the basis $1, \alpha$ and the multiplication be given by $\alpha \bullet \alpha = -a$. Multiplication with $w = x + y\alpha$ has the matrix $\begin{pmatrix} x & -ya \\ y & x \end{pmatrix}$, which has the determinant $x^2 + y^2 a = q(w)$. That q is a group form follows now from $q(v \bullet w) = q(v)q(w)$.

Lemma 9.9. *Let q be regular and $a \neq 0$. Then q represents a iff $\langle -a\rangle \perp q$ is isotropic.*

Proof. If $q(w) = a$, we have $-a \cdot 1^2 + q(w) = 0$, so $\langle -a\rangle \perp q$ is isotropic. If conversely $-a \cdot x^2 + q(w) = 0$ and not both x and w are zero, we distinguish two cases. It x is not zero, we have $q(x^{-1}w) = a$. If x is zero, q is isotropic and whence universal. So q represents also a. □

Corollary 9.10. $a \in \mathrm{D}\big(\langle -b\rangle \perp q\big)$ *iff* $b \in \mathrm{D}\big(\langle -a\rangle \perp q\big)$.

Proof of Theorem 9.7. Every non-zero element of F is a product of powers of polynomials $(t - \alpha)$, $\alpha \in k$, possibly with negative exponents. So $\dot{F}/\dot{F}^2$ is generated by the $t - \alpha$. We note first that every for all α and β the three polynomials 1, $\alpha - t$ and $\beta - t$ are linearly dependent over k. Since $k = k^2$, this implies that $\langle 1, \alpha - t, \beta - t\rangle$ is isotropic. So $t - \alpha$ belongs to $\mathrm{D}\big(\langle 1, \beta - t\rangle\big)$. By Lemma 9.8 is follows that all all $-f$ belong to $\mathrm{D}\big(\langle 1, \beta - t\rangle\big)$. Whence all $t - \beta$ belong to $\mathrm{D}\big(\langle 1, f\rangle\big)$, which implies that all $\langle 1, f\rangle$ are universal. Since every regular binary form is a multiple of some $\langle 1, f\rangle$, this proves the theorem. □

[6] An F-algebra is an F-vector space A with a bilinear multiplication which turns A into a ring, possibly non-commutative. The map $a \mapsto a \cdot 1$ defines a homomorphism from F to the center (see p. 29) of A. So an F-algebra is a ring with a homomorphism from F to the center of A. If A is not 0, we may consider F as a subring of A. Morphims between F-algebras are F-linear maps which are ring homomorphisms at the same time.

§10 Pfister forms

10.1 Round forms

Definition. An element $a \in \dot{F}$ is a similarity factor of q if $\langle a\rangle \cdot q \cong q$. The set $\mathrm{G}(q)$ of similarity factors of q is group.

It is easy to see that Witt equivalent regular forms have the same similarity factors. Also, by Corollary 6.9 (2), $\langle a\rangle \cdot q$ and q are equivalent iff they are Witt equivalent. So $\mathrm{G}(q)$ can be computed in $\mathrm{W}(F)$.

It is clear that $\dot{F}^2$ is a subgroup of $\mathrm{G}(q)$. The equation $\mathrm{D}(\langle a\rangle \cdot q) = a \cdot \mathrm{D}(q)$ implies that $\mathrm{D}(q)$ is closed under multiplication with similarity factors of q.

Definition. A form is round if $\mathrm{G}(q) = \mathrm{D}(q)$.

Except for totally isotropic forms, where $\mathrm{D}(q)$ is empty and $\mathrm{G}(q) = \dot{F}$, this is equivalent to $\mathrm{D}(q) \subset \mathrm{G}(q)$. Note that the 0-fold Pfister form $\langle 1\rangle$ is round. In the proof of Lemma 9.8 we proved that 1-fold Pfister forms $\langle 1, a\rangle$ are round.

Theorem 10.1. *If q is round, then so is $\langle 1, a\rangle \cdot q$.*

Proof. Assume that c is represented by $q' = \langle 1, a\rangle \cdot q$. Then $c = x + ay$, where x and y are values of q. There care three cases:

Case $y = 0$. Then $c = x$ is a similarity factor of q and therefore of q'.

Case $x = 0$. Then $c = ay$ is a similarity factor of q' since a is a similarity factor of $\langle 1, a\rangle$ and y is a similarity factor of q.

Case $x, y \neq 0$. Then x and y are in $\mathrm{G}(q)$ and we have for all d, e

$$\langle d, e\rangle \cdot q \cong \langle dx, e\rangle \cdot q \cong \langle d, ey\rangle \cdot q. \tag{10.8}$$

Then

$$\begin{aligned} \langle 1, a\rangle \cdot q &\cong \langle x, ay\rangle \cdot q && \text{by (10.8)} \\ &\cong \langle c, caxy\rangle \cdot q \\ &\cong \langle c, ca\rangle \cdot q && \text{by (10.8)} \\ &\cong \langle c\rangle \cdot \langle 1, a\rangle \cdot q \end{aligned}$$

□

Corollary 10.2. *Pfister forms are round, and therefore group forms.*

10.2 2-fold Pfister forms

Pfister forms represent 1 and have therefore the form $q = \langle 1\rangle \perp q_0$. q_0 is uniquely determined and called the *pure part* of q.

Exercise 10.1. *A regular ternary form is the pure part of a Pfister form iff it has determinant* 1. *A regular quaternary form is a Pfister form iff it represents* 1 *and has determinant* 1.

Lemma 10.3. *For a 2-fold Pfister q form the following are equivalent:*

a) q is isotropic

b) q is hyperbolic, i.e. equivalent to $\langle\langle 1,-1\rangle\rangle$.

c) The pure part of q is isotropic

Proof. a)→b): If q is isotropic, it is equivalent to a form $\mathbb{H} \perp s$ for some binary form s. Since q has determinant 1, s has determinant -1 and is therefor again a hyperbolic plane by Theorem 3.3.

b)→c) The pure part of $q = \langle 1,-1,1,-1\rangle$ is $\langle -1,1,-1\rangle$.

c)→a) This is clear. □

Corollary 10.4. *For all $a, b \in \dot{F}$ the following are equivalent:*

a) $\langle\langle a,b\rangle\rangle$ is isotropic

b) $\big(1+\langle a\rangle\big)\big(1+\langle b\rangle\big) = 0$ in $\mathrm{W}(F)$

c) $\langle a,b\rangle$ represents -1.

Proof. b) is a reformulation of $\langle 1,a\rangle\langle 1,b\rangle$ being hyperbolic.

c) is equivalent to $\langle a,b,ab\rangle$ being isotropic, since $\langle 1,a,b\rangle \cong \langle ab\rangle\langle a,b,ab\rangle$ and therefore by Lemma 9.9

$$-1 \in \mathrm{D}(\langle a,b\rangle) \;\Leftrightarrow\; \langle 1,a,b\rangle \text{ isotropic} \;\Leftrightarrow\; \langle a,b,ab\rangle \text{ isotropic.}$$

□

Exercise 10.2. *Prove that $\langle\langle a,b\rangle\rangle$ is isotropic iff $-a$ is a norm in the algebra $F[t]/(t^2+b)$.*

Chapter 3

Central simple algebras

§11 Quaternion algebras

Definition. For elements a, b in $\dot{F}$ the quaternion algebra $\left(\frac{a,b}{F}\right)$ is the F-algebra with generators i and j and defining relations $i^2 = a$, $j^2 = b$ and $ij = -ji$.

Hamilton's quaternions are in this notation $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.

Lemma 11.1. *The elements* $1,i,j,k = ij$ *form a basis of* $\left(\frac{a,b}{F}\right)$

Proof. The the next table shows that the subspace A of $\left(\frac{a,b}{F}\right)$ spanned by $1,i,j$ and k is closed under multiplication.

$\cdot$	i	j	k
i	a	k	aj
j	$-k$	b	$-bi$
k	$-aj$	bi	$-a$

So A equals $\left(\frac{a,b}{F}\right)$. To show that $1,i,j$ and k are linearly independent we start with a vector space B with basis $1,i,j$ and define a bilinear multiplication by the table above and the stipulation that 1 is a neutral element. It is now easy, but tedious, to verify the associative law for the basis elements. □

Another proof of the lemma is as follows: Let K be any extension of F which contains a square root α of a and a square root β of b. By the next corollary the quaternion algebra

$$\left(\frac{a,b}{F}\right) = K \otimes_F \left(\frac{a,b}{F}\right)$$

is isomorphic to $\mathrm{M}_2(F)$, the algebra of all 2×2-matrices over F, which has dimension 4.

Lemma 11.2. $\left(\frac{-1,1}{F}\right) \cong \mathrm{M}_2(F)$

Proof. We have to find matrices I and J such that $I^2 = 1$, $J^2 = -1$ such that 1,I,J and $K = IJ$ are linearly independent. These are

$$I = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Together with $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $IJ = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ they are a basis of $\mathrm{M}_2(F)$. □

It may be interesting how to find the such matrices. By 11.11 the quaternion algebra $\left(\frac{-1,1}{F}\right)$ is isomorphic to $\mathrm{M}_2(F)$ because it contains non-zero non-units, for example $e_1 = i + j$ (it has norm zero, see Lemma 11.6). Let L be the left ideal generated by e_1. The the following equations show that $e_1 = i + j$ and $e_2 = 1 + k$ are a basis of L:

$$\begin{aligned} ie_1 &= e_2 & \qquad ie_2 &= e_1 \\ je_1 &= -e_2 & \qquad je_2 &= e_1. \end{aligned}$$

With respect to this basis the matrices I and J correspond to left-multiplication by i and j on L.

Definition. For a quaternion algebra A we denote by A_0 the subvector space of pure quaternions $\pi = xi + yj + zk$.

Corollary 11.3. *If a and $-b$ are squares in F, then $\left(\frac{a,b}{F}\right)$ is isomorphic to* $\mathrm{M}_2(F)$.

Proof. If $\alpha^2 = a$ and $\beta^2 = -b$, then $i \mapsto \alpha i$, $j \mapsto \beta j$ defines an isomorphism $\left(\frac{a,b}{F}\right) \to \left(\frac{1,-1}{F}\right)$. □

Lemma 11.4. *The square function $\pi \mapsto \pi^2$ defines a quadratic form on A_0, which is equivalent to $\langle a, b, -ab\rangle$ via the orthogonal basis i, j, k. The associated polar form is $\dfrac{\pi\beta + \rho\pi}{2}$.*

Proof. The first part follow from the formula

$$(xi + yj + zk)^2 = x^2 + y^2 + z^2.$$

The expression $\frac{\pi\rho+\rho\pi}{2}$ is bilinear, symmetric and gives the square of π if $\pi = \rho$. □

Definition. Conjugation of a quaternion algebra is the F-linear map, which maps $\alpha = c + xi + yj + zk$ to $\bar{\alpha} = c - xi - yj - zk$.

Lemma 11.5. *Conjugation is an anti-automorphism, i.e. an automorphism of the vector space A which satisfies $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$.*

Proof. This is true for any linear automorphism f with $f(i)^2 = a$, $f(j)^2 = b$ and $f(ij) = f(j)f(i)$. □

Definition. The norm N of a quaternion algebra is defined by

$$\mathrm{N}(\alpha) = \alpha\bar{\alpha}.$$

Note that on A_0 we have $\mathrm{N}(\pi) = -\pi^2$.

Lemma 11.6. *1. The map* N *is a quadratic form on* A*, which is equivalent to* $\langle 1, -a, -b, ab\rangle = \langle\langle -a, -b\rangle\rangle$ *via the orthogonal basis* $1, i, j, k$*.*

2. N *is multiplicative:* $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$*.*

3. α *is a unit in* A *iff* $\mathrm{N}(\alpha)$ *is not zero.*

Proof. 1. Write $\alpha = c + \pi$ for $c \in F$ and $\pi \in A_0$. Then $\mathrm{N}(\alpha) = (c+\pi)(c-\pi) = c^2 - \pi^2$.

2. $(\alpha\beta)\overline{\alpha\beta} = (\alpha\beta)(\bar\beta\bar\alpha) = \alpha\,\mathrm{N}(\beta)\bar\alpha = \alpha\bar\alpha\,\mathrm{N}(\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.

3. If α is a unit and $\alpha\beta = 1$, then $\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = 1$. So $\mathrm{N}(\alpha)$ is not zero. If conversely $\mathrm{N}(\alpha)$ is not zero, then $\dfrac{\bar\alpha}{\mathrm{N}(\alpha)}$ is an inverse of α. □

This gives another explanation of the roundness of $\langle\langle -a, -b\rangle\rangle$. If c is a norm, i.e if $c = \mathrm{N}(\alpha)$, we have $c\,\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$. So left multiplication with α is an isometry between $(A, c\,\mathrm{N})$ and (A, N).

Exercise 11.1. *In a finite-dimensional algebra an element which has a right inverse or a left inverse is a unit.*

Corollary 11.7. *For a quaternion algebra* $A = \left(\dfrac{a, b}{F}\right)$ *the following are equivalent:*

a) A *is isotropic*

b) A *is hyperbolic*

c) A_0 *is isotropic*

d) $(1 - \langle a\rangle)(1 - \langle b\rangle) = 0$ *in* $\mathrm{W}(F)$*.*

e) $\langle a, b\rangle$ *represents* 1*.*

Proof. This follows from Lemma 10.3 and Corollary 10.4. □

Proposition 11.8. *Let* A *ans* A' *be two quaternion algebras. Then the following are equivalent:*

a) A *and* A' *are isomorphic as* F*-algebras.*

b) A *and* A' *are isomorphic as quadratic spaces.*

c) A_0 *and* A'_0 *are isomorphic as quadratic spaces.*

Proof. b) and c) are equivalent by the Cancellation Theorem since $A = A_0 \perp \langle 1\rangle$.

a)→c) (A_0, N) can be recovered from the algebra structure of A as follows: The pure part A_0 is the set of elements outside $\dot F$ whose squares are in F. The norm is $-\pi^2$ on A_0.

c)→a) We show that if the quadratic space A_0' is isomorphic to $\langle -a, -b, ab\rangle$, then the algebra A' is isomorphic to $\left(\frac{a,b}{F}\right)$: The assumption implies that A_0' contains elements orthogonal I and J with $I^2 = a$ and $J^2 = b$. Being orthogonal means $IJ = -JI$. This implies that $i \mapsto I$, $j \mapsto I$ defines a homomorphism $\varphi : A = \left(\frac{a,b}{F}\right) \to A'$. There are two ways to show that φ is a bijection. First, we can use that A is *simple*, i.e. has no non-trivial two-sided ideals. This is proved in 11.14.[1] Since, by definition, φ maps 1 to 1, the kernel of φ is different from A and therefore 0. Another argument shows that 1, I, J and $K = IJ$ are non-zero (since $K^2 = -ab$) and orthogonal (since e.g. $IK = aJ = -KI$). So these elements are linearly independent and in the image of φ. □

Corollary 11.9.

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{a',b'}{F}\right) \Leftrightarrow \langle\langle -a, -b\rangle\rangle \cong \langle\langle -a', -b'\rangle\rangle$$

Corollary 11.10.

$$\langle a, b\rangle \cong \langle a', b'\rangle \quad \textit{iff} \quad \left(\frac{a,b}{F}\right) \cong \left(\frac{a',b'}{F}\right) \textit{ and } \mathrm{d}(\langle a, b\rangle) = \mathrm{d}(\langle a', b'\rangle)$$

Proof. If $\mathrm{d}(\langle a, b\rangle) = \mathrm{d}(\langle a', b'\rangle$, we have $\langle 1, ab\rangle \cong \langle 1, a'b'\rangle$ and therefore by the Cancellation Theorem

$$\langle a, b\rangle \cong \langle a', b'\rangle \Leftrightarrow \langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle.$$

□

Definition. A quaternion algebra splits if it is isomorphic to $\mathrm{M}_2(F)$, the algebra of all 2×2-matrices over F.

Theorem 11.11. *For a quaternion algebra A the following are equivalent:*

a) A splits

b) A is isotropic

c) A is not a division ring.

Proof. The equivalence of b) and c) follows immediately from Lemma 11.6.3. Clearly $\mathrm{M}_2(F)$ is not a division ring. So we have to prove that A is a matrix ring, if it is isotropic. We know by 11.7 that A is hyperbolic, that is, A is isomorphic to $\langle 1, -1, 1, -1\rangle$ as a quadratic space. So by 11.9 A is isomorphic to $\left(\frac{1,-1}{F}\right)$, which is in turn isomorphic to $\mathrm{M}_2(F)$ by Lemma 11.2. □

Definition. An F-algebra A is central, if its center

$$\mathrm{Z}(A) = \{a \in A \mid ab = ba \text{ for all } b \in A\}$$

equals F. An algebra A is simple if it is simple as a ring, i.e. A is not 0, and there are no other two-sided ideals besides 0 and A.

[1] This can also be verified by a easy calculation. Or, it follows from also from

Lemma 11.12. *The algebra* $\mathrm{M}_n(F)$ *of all* $n \times n$*-matrices over* F *is central simple if* $n > 0$.

Proof. Let $e_{r,s} = (\delta_{i,r}\delta_{s,j})$ be the matrix with 1 in position (r, s) and zeros elsewhere. These matrices form am F-basis of $\mathrm{M}_n(F)$. They satisfy the equations $e_{r,s}e_{i,j} = \delta_{s,i}e_{r,j}$ and $1 = e_{1,1} + e_{2,2} + \cdots + e_{n,n}$.

An element $x = \sum_{i,j} a_{i,j}e_{i,j}$ commutes with $e_{r,s}$ if

$$\sum_j a_{s,j}e_{r,j} = e_{r,s}x = xe_{r,s} = \sum_i a_{i,r}e_{i,s},$$

which happens only if $a_{s,s} = a_{r,r}$ and all other $a_{s,j}$ and $a_{i,r}$ are zero. So x commutes with all $e_{r,s}$ only it it has the form $\sum_i ae_{i,i}$.

For simplicity let I be a two-sided ideal and $x = \sum_{i,j} a_{i,j}e_{i,j}$ a non-zero element of I. Consider some non-zero $a_{i,j}$. Then I contains all $e_{r,s} = a_{i,j}^{-1}(e_{r,i}xe_{j,s})$, and so I equals A. □

Lemma 11.13. *Let* A *be an* F*-algebra and* K *a field extension of* F. *Then* $K \otimes_F A$ *is an* K*-algebra of the same dimension and we have*

1. *If* $K \otimes_F A$ *is central, then* A *is central.*
2. *If* $K \otimes_F A$ *is simple, then* A *is simple.*

Proof. 1. The tensor product $K \otimes \mathrm{Z}(A)$ is contained in the center of $K \otimes_F A$.

2. If $\mathcal{I}$ is a two-sided ideal in A, the tensor product $K \otimes \mathcal{I}$ is a two-sided ideal in $K \otimes_F A$ □

The converse of 1. is also true, see Lemma 13.2. The converse of 2 is true, if A is central, see Lemma 13.3, and also the next exercise.

Exercise 11.2. *Show that* $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$.

Proposition 11.14. *Quaternion algebras are central simple.*

Proof. If we tensor $\left(\frac{a,b}{F}\right)$ with the algebraic closure K of F, we obtain $\left(\frac{a,b}{K}\right)$, which is isomorphic to $\mathrm{M}_n(K)$ by Corollary 11.3. Now the claim follows from the last two lemmas. □

Wedderburn's theorem on simple algebras, Corollary 12.9, states that simple algebras are matrix rings over division algebras. So in dimension 4 this can be only a division ring or a matrix algebra over F (for more detail see the first paragraph of the proof of 12.11.) This is another proof of the c)↔a) part of Theorem 11.11.

§12 The Wedderburn Theorem

In the following R will be a ring, not necessarily commutative. By *R-module* we mean *left* R-module.

Definition. A non-zero R-module L is minimal,, if it has no submodules other that 0 and L. A direct sum of minimal modules is semi-simple..

Lemma 12.1. *A module is semi-simple iff it is a sum of minimal modules.*

Proof. Let M be the sum of the minimal submodules L_i, $(i \in I)$. Choose a maximal subfamily $(L_i \mid i \in I_0)$ which is independent, i.e. where $M_0 = \sum_{i \in I_0} L_i$ is a direct sum. Consider an element $j \in I$. The maximality of the subfamily implies that L_j and M_0 intersect non-trivially. Since L_j is minimal, it must be contained in M_0. This shows $M_0 = M$. □

Exercise 12.1. *Show that a module is semi-simple iff every submodule is a direct summand.*

Hint: If M is a sum of minimal submodules, N a submodule and K is maximal with $K \cap N = 0$, then $K + N = M$, as in the last Lemma. For the other direction, show first for arbitrary M: *If $a \in M$, and N is maximal with $a \notin N$, then $a + N$ generates a minimal submodule of M/N.*

Exercise 12.2. *Quotients and submodules of semi-simple modules are semi-simple again. If M is the sum of minimal ideals L_i, then every minimal ideal is isomorphic to one of the L_i.*

Hint: A quotient of a minimal L is either zero or isomorphic to L. Also use the last exercise.

Definition. A ring R is semi-simple if it is semi-simple as a left R-module.

Exercise 12.3. *If R is semi-simple, then all R-modules are semi-simple. Each minimal module is isomorphic to a minimal left ideal of R.*

Hint: Every cyclic module Ra is isomorphic to $R/\mathrm{Ann}(a)$, where $\mathrm{Ann} = \{r \mid ra = 0\}$.

Theorem 12.2 (Wedderburn)**.** *A semi-simple ring is a finite direct product of matrix rings $\mathrm{M}_n(D)$, over division rings D.*

We will see (Exercise 12.4, Proposition 12.8, Corollary 12.9) that the converse is also true: Finite direct products of matrix rings over division rings are semi-simple.

Definition. A ring is left artinian artinian if there is no infinite descending sequence of let ideals.

Finite-dimensional algebras are artinian, or more generally, rings which contain a division ring over which they are a finite-dimensional left vector-space. So we have

Corollary 12.3. *Semi-simple rings are artinian.*

Exercise 12.4. *Show, without using Wedderburn's Theorem, that finite direct products of semi-simple (artinian) rings are semi-simple (artinian).*

Wedderburn's theorem will follow from a series of lemmas:

Lemma 12.4. *A non-zero homomorphism between two minimal modules is an isomorphism.*

Proof. If $\varphi : L_1 \to L_2$ is a non-zero, the kernel of φ is zero if L_1 is minimal, and the image is L_2 if L_2 is minimal. □

Corollary 12.5 (Schur's Lemma)**.** *The endomorphism ring* $\mathrm{End}(L)$ *of a minimal module is a division ring.*

Lemma 12.6. *The endomorphism ring of a direct sum* $M = \bigoplus_{i=1}^{n} N_i$ *of* n *copies of* N *is isomorphic to* $\mathrm{M}_n(\mathrm{End}(N))$.

Proof. Let $\epsilon_i : N_i \to M$ and $\pi_i : M \to N_i$ be the embeddings and the projections which come with the direct sum decomposition. Note that we have $\pi_i \epsilon_j = \delta_{ij}$ and $\sum_{i=1}^{n} \epsilon_i \pi_i = 1$. If φ is an endomorphism of M, then $\varphi = \sum_{i,j} \epsilon_i \varphi_{i,j} \pi_j$, where $\varphi_{i,j} = \pi_i \varphi \epsilon_j$ is a homomorphism $N_j \to N_i$, i.e. an endomorphism of N. The map[2] $\varphi \mapsto \sum_{i,j} \varphi_{i,j} e_{i,j}$ defines now an isomorphism $\mathrm{End}(M) \to \mathrm{M}_n(\mathrm{End}(N))$. □

Lemma 12.7. *The endomorphism ring of the left* R*-module* ${}_R R$*, is canonically isomorphic to* R^{op}.

Proof. Right multiplication with an element r is an endomorphism ρ_r of ${}_R R$. This defines a ring homomorphism from R^{op} to $\mathrm{End}({}_R R)$, which is injective because $r = \rho_r(1)$. Every endomorphism φ equals ρ_r for $r = \varphi(1)$, since $\varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1) = \rho_r(x)$. □

Proof of Theorem 12.2. A semi-simple ring R is the direct sum of finitely many minimal left ideals since such a sum equals R if only it contains 1. We group isomorphic left ideals together and write

$$ {}_R R \cong L_1^{n_1} \oplus \cdots \oplus L_k^{n_k}, $$

with pairwise non-isomorphic minimal L_i. Since for different i and j there are no non-zero homomorphisms from $L_i^{n_i}$ to $L_j^{n_j}$, the endomorphism ring of ${}_R R$ is isomorphic to the direct product of the $\mathrm{End}(L_i^{n_i})$. Each of these rings is isomorphic to $\mathrm{M}_{n_i}(\mathrm{End}(L_i^{n_i}))$, and by Schur's Lemma each $D_i = \mathrm{End}(L_i^{n_i})$ is a division ring. So R^{op} is isomorphic to a direct product of the $\mathrm{M}_{n_i}(D_i)$. Now the theorem follows since, by the transposition map, $\mathrm{M}_{n_i}(D_i)^{\mathrm{op}} \cong \mathrm{M}_{n_i}(D_i^{\mathrm{op}})$. □

Proposition 12.8. *A simple artinian ring* R *is semi-simple. All minimal left ideals are isomorphic as* R*-modules.*

Proof. Since R is artinian and non-zero, there is a minimal left ideal L. Then $\sum_{r \in R} Lr$ is a two-sided ideal and so equals R. The Lr are either 0 or isomorphic to L. Now apply Exercise 12.2. □

Corollary 12.9 (Wedderburn Theorem on simple algebras)**.** *A finite-dimensional simple* F*-algebra is a matrix algebra* $\mathrm{M}_n(D)$ *over a division ring* D *which is itself a finite-dimensional* F*-algebra.*

[2] The $e_{i,j}$ are the matrices used in the proof of 11.12.

Proof. A finite-dimensional simple F-algebra A is a direct product of matrix rings over division rings. By simpleness (or since all minimal left ideas are isomorphic) there is only one factor $\mathrm{M}_n(D)$. The proof of Lemma 11.12 shows that the center of $\mathrm{M}_n(D)$ equals the center of D, which must then contain F. (Alternatively one can argue that D is the endomorphism ring of a (minimal) left ideal, and so contains F.) □

Remark 12.10. *If D is a division ring and $n > 0$, $\mathrm{M}_n(D)$ is simple artinian.*

Proof. That $\mathrm{M}_n(D)$ is simple can be seen either by the same proof as 11.12, or by the observation $\mathrm{M}_n(D) = D \otimes_F \mathrm{M}_n(F)$, where F is any field contained in D, and an application of 13.3. □

Proposition 12.11. *A central simple F-algebra of dimension 4 is a quaternion algebra. The dimensions 2 and 3 do not occur.*

Proof. Let A be a central simple F-algebra of dimension 2, 3 or 4. Then A is a $M_n(D)$, for a division ring F, which has F in its center. Since $\dim_F(A) = \dim_F(D) \cdot n^2$, we have either $A = M_2(F)$, which is a quaternion algebra, or $A = D$.

So we may assume that A is a division algebra. Since A is not commutative there are non-commuting elements p and q. The field $F(p)$ lies properly between F and A, and since we have

$$\dim_F(A) = [F(p) : F] \cdot \dim_{F(p)}(A),$$

it follows that $[F(p) : F] = \dim_{F(p)}(A) = 2$ and A has dimension 4 over F. Since F is not of characteristic 2, the two fields $F(p)$ and $F(q)$ can be obtained by adjoining square roots of element of F. So we may assume that p^2 and q^2 are in F. c Since $F(p)$ is commutative, conjugation with p is an non-trivial automorphism of $F(p)$-vector space A. In terms of the basis $1, q$ this automorphism is given by a matrix $\begin{pmatrix} 1 & \delta \\ 0 & \epsilon \end{pmatrix}$, for $\delta, \epsilon \in F(p)$. Conjugation with p^2 is trivial, so the matrix has order 2, which means that $\epsilon^2 = 1$ and $\delta + \delta\epsilon = 0$. If $\epsilon = 1$, it would follow that $\delta = 0$, and conjugation with p would be trivial. So we have $\epsilon = -1$, and it follows that

$$p^{-1}qp = \delta - q.$$

This implies $pq + qp = px \in F(p)$. It follows that on $V = F \cdot p + F \cdot q$ the function $\frac{1}{2}(xy + yx)$ defines a symmetric F-bilinear form with values in F. Chose an orthogonal basis I, J of V. And set $I^2 = a$ and $J^2 = b$. We have $IJ = -JI$. So the $i \mapsto I$ and $j \mapsto J$ defines a homomorphism from $\left(\frac{a,b}{F}\right)$ to A, which is an isomorphism, since $\left(\frac{a,b}{F}\right)$ is simple and A has dimension (at most) 4. □

§13 The Brauer Group

We call a central simple algebra an *CSA*.. Usually this will be an algebra over F.

The *tensor product* $C = A \otimes_F B$ of two F-algebras A and B is the tensor product of the F-vector spaces with the (bilinear) multiplication defined by

$$(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb').$$

This is again an F-algebra. The homomorphisms $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$ embed A and B in C. We will often identify A and B with their images in C. Note that in C the elements of A commute with the elements of B.

Theorem 13.1. *If A and B are CSA, the so is $A \otimes_F B$.*

This follows from the next two Lemmas.

Lemma 13.2. *For two F-algebras A and B we have* $\mathrm{Z}(A \otimes_F B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B)$.

Proof. Let z be in the center of $A \otimes_F B$. If (a_i) is a basis of A. we can write $z = \sum_i a_i \cdot b_i$, for unique $b_i \in B$. An equation $bz = zb$ translates to $\sum_i a_i \cdot bb_i = \sum_i a_i \cdot b_i b$. So, since z commutes with B, all b_i belong to B. It follows that for a basis (b_i') of $C(B)$ we can write $z = \sum_i a_i' \cdot b_i'$, for unique a_i' in A. Since z commutes with A it follows as before that all a_i' belong to $\mathrm{Z}(A)$. □

Lemma 13.3. *If A is CSA and B is simple, then also $A \otimes_F B$ is simple.*

Index