Quadratic Forms over Fields - Notes and Exercises

Jonathan Komada Eriksen

Contents

1 Foundations

Notes on the most important definitions and results from Chp. 1.

1.1 Quadratic forms and spaces

Throughout the book, F is assumed to be a field of characteristic $\neq 2$.

Definition 1.1.1: Quadratic form

An n-ary quadratic form over F is a homogenous polynomial f of degree 2 in n variables.

Closely related to a quadratic form f is the matrix M_f consisting of the (normalized wrt. symmetry) coefficients of f, i.e. such that

$$f(X) = [X_1, \ldots, X_n] M_f [X_1, \ldots, X_n]^t.$$

Definition 1.1.2: Equivalence of forms

We say that two n-ary quadratic forms f, g are **equivalent**, denoted $f \simeq g$, if there exists an invertible matrix $C \in \mathbf{M}_n(F)$ such that $f(X) = g(C \cdot X)$. Equivalently, so that

$$M_f = C^t \cdot M_f \cdot C,$$

i.e. the associated matrices are congruent.

For working out the theory, we usually prefer the "coordinate-free" version.

Definition 1.1.3: Quadratic space

Let V be a finite-dimensional F-vector space, and let

$$B : V \times V \to F$$

be a symmetric bilinear pairing on V. We call the pair (V, B) a **quadratic space**. Associated to this quadratic space is the **quadratic map**

$$\begin{aligned} q_B &: V \to F \\ q_B(x) &= B(x, x) \end{aligned}$$

The quadratic map, and the bilinear pairing determine each other. Of course, q_B satisfies

$$q_B(ax) = B(ax, ax) = a^2 q_B(x),$$

but indeed also

$$\begin{aligned} q(x+y) - q(x) - q(y) &= B(x+y, x+y) - B(x,x) - B(y,y) \\ &= B(x,y) + B(y,x) \\ &= 2B(x,y). \end{aligned}$$

To see the relation back with quadratic forms, notice that if we give V a basis $e_1, \ldots, e_n$, then the form

$$f(X) = \sum_{i,j} B(e_i, e_j) X_i X_j$$

corresponds exactly to q_B (under the given basis of course). Different choice of bases now correspond exactly to different equivalent forms.

We also have a notion of equivalence of quadratic spaces.

Definition 1.1.4: Isometries

Let $(V, B), (V', B')$ be quadratic spaces. An **isometry** is a linear map $\tau : V \to V'$ so that

$$B(x, y) = B'(\tau(x), \tau(y)).$$

For a subspace $S \subseteq V$, recall that the orthogonal compliment is defined as

$$S^\perp := \{x \in V \mid B(x, y) = 0, \forall y \in S\}$$

Definition 1.1.5: Radical

The **radical** $\operatorname{rad} V$ is defined as the orthogonal complement $V^\perp$ of V itself.

The fact that the following conditions are actually equivalent is easy linear algebra.

Definition 1.1.6: Regular space

We say that the quadratic space (V, B) is **regular** if one (and hence all) of the following conditions are met:

- $\operatorname{rad} V = 0$.
- M is nonsingular, where M is the matrix associated to B (and any choice of basis).
- $x \to B(x, -)$ defines an isomorphism $V \to V^*$.
- For $x \in V$, $B(x, y) = 0$ for all y implies that $x = 0$.

The first result is the easy dimension formula.

Proposition 1.1.7

Let (V, B) be a regular quadratic space, and let $S \subseteq V$ be a subspace. Then

a) $\dim V = \dim S + \dim S^\perp$,

b) $(S^\perp)^\perp = S$.

Proof. This is all pretty direct from $x \to B(x, -)$ being an isomorphism of V to its dual. □

We need to establish some notation. First of all, given two spaces $(V_1, B_1), (V_2, B_2)$ we denote the **orthogonal sum** $V_1 \perp V_2$ by the space $(V_1 \oplus V_2, B)$, where B is given by

$$B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2).$$

Its easy to see that orthogonal sums of two quadratic forms should then also simply be taken to be their sums (in independent variables).

Second, for a $d \in F^\times$, we write $\langle d \rangle$ for the isometry class of the quadratic space corresponding to the form dX^2.

Third, we denote by $D(f)$ the set of values in $F^\times$ represented by a quadratic form f (or correspondingly, $D(V)$ for the values represented by q_B for a quadratic space (V, B)). Note that $D(V)$ actually defines a union of cosets of $F^\times/(F^\times)^2$.

Proposition 1.1.8: Representation Criterion

A quadratic space (V, B) represents a value $d \in F^\times$ if and only if there exists another quadratic space (V', B'), and an isometry

$$V \cong \langle d \rangle \perp V'.$$

Proof. The if part is obvious. For the other way, first show that we can assume that V is regular (because we always have $V \cong \operatorname{rad} V \perp W$ for some regular space W, which satisfies $D(W) = D(V)$). Then, the proof is just showing that

$$V \cong F \cdot v \perp (F \cdot v)^\perp$$

for $v \in V$ satisfying $q_B(v) = d$. □

Applying the above many times shows that any quadratic form over a field is diagonalizable, or equivalently, has an orthogonal basis. For more notation, we abbreviate $\langle d_1\rangle\perp\ldots\perp\langle d_n\rangle$ by $\langle d_1,\ldots,d_n\rangle$.

1.2 Hyperbolic plane and hyperbolic subspaces

First another couple of words:

Definition 1.2.1: Isotropic space

Let $v \in V$ be a non-zero vector in a quadratic space (V, B). If $q_B(v) = 0$, v is said to be **isotropic**; Otherwise it is **anisotropic**. This extends to the whole space (V, B), which is said to be isotropic if it contains a non-zero isotropic vector, and anisotropic otherwise.

And some more notation: For a quadratic form f, we define the **determinant** $d(f) := \det(M_f)\cdot(F^\times)^2$. Of course, an equivalent form has a determinant that differs by a square, so this is really a well defined element of $F/(F^\times)^2$ on equivalence classes of forms.

Theorem 1.2.2

Let (V, B) be a 2-dimensional quadratic space. TFAE:

1) V is regular and isotropic.
2) V is regular and $d(V) = -1 \cdot F^2$.
3) $V \cong \langle 1, -1\rangle$.
4) V corresponds to the (equivalence class of the) quadratic form X_1X_2.

Proof. 3) $\Leftrightarrow$ 4) is just a change of variables relating the quadratic forms $X_1^2 - X_2^2$ and X_1X_2.

For 1) $\Rightarrow$ 2), write $ax_1 + bx_2$ for some isotropic vector in V, where x_1, x_2 is an orthogonal basis. Then $d(V) = q(x_1)q(x_2)\cdot(F^\times)^2$, but we also have $q(x_1) = -(b/a)^{-2}q(x_2)$.

For 2) $\Rightarrow$ 3), notice that by the representation criterion and the discriminant, it is enough to show that 1 is represented, which is what the proof does. Finally 3) $\Rightarrow$ 1) is trivial. $\square$

The quadratic space corresponding to $\langle 1, -1\rangle$ is called the hyperbolic plane. This is extended to any even dimension, by taking orthogonal sums of the hyperbolic plane. Such a space is called a hyperbolic space.

Definition 1.2.3: Universal form

A quadratic form q (or quadratic space (V, B)) is called universal if it represents all of $F^\times$.

Of course, the hyperbolic plane is clearly universal.

A useful theorem is

Theorem 1.2.4

Let (V, B) be a regular quadratic space. Then:

a) V Every totally isotropic subspace $U \subseteq V$ of dimension r is contained in a hyperbolic subspace $T \subseteq V$ of dimension $2r$.

b) V is isotropic if and only if V contains a hyperbolic plane (necessarily as a direct summand)

c) V is isotropic $\Rightarrow$ V is universal

Proof. It is easy to see that a) implies b), which in turn implies c). Now proving a) can be done in the following way: Take a basis $x_1, \ldots x_r$ of U. Then look at the subspace $S \subset U$ spanned by $x_n2, \ldots, x_r$. Now (since V is regular), we get that

$$\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp$$

by one of the earlier propositions. Thus, we can take $y_1 \in U^\perp \setminus S^\perp$, and consider the space generated by x_1, y_1. Explicitly computing the determinant of this space shows that it is hyperbolic. The proof of 1) now follows by induction on r. □

Corollary 1.2.5: First representation theorem

Let q be a regular quadratic form. Then $d \in D(q)$ if and only if $q \perp \langle -d \rangle$ is isotropic.

Proof. If $d = q([x_1, \ldots, x_n])$, then $q \perp \langle -d \rangle([x_1, \ldots, x_n, 1]) = 0$. Conversely, if $q \perp \langle -d \rangle([x_1, \ldots, x_n, x_{n+1}]) = 0$, then there are two cases to consider: If $x_{n+1} \neq 0$, then $q([x_1/x_{n+1}, \ldots x_n/x_{n+1}]) = d$, otherwise q was already isotropic, and hence universal. □

1.3 Witt's theorem's

We start with a theorem, which (looking ahead) will say that the monoid of quadratic forms over a field is cancellable.

Theorem 1.3.1: Witt's cancellation theorem

For any quadratic forms q, q_1, q_2 we have that

$$q \perp q_1 \cong q \perp q_2 \Rightarrow q_1 \cong q_2.$$

Proof. Quite a lot of stuff goes into it, see Section 1.4 of the book. □

One important ingredient in the proof above (which we did not write) is that of hyperplane reflections. To define this, consider first

Definition 1.3.2: Orthogonal group

Let (V, B, q) be a quadratic space. The **orthogonal group**, denoted $O_q(V)$ (or just $O(V)$ when clear from context) is the group of self-isometries on (V, B).

Now a hyperplane reflection is an element $\tau_y \in O(V)$ associated to any anisotropic vector $y \in V$, defined by

$$\tau_y(x) = x - \frac{2B(x,y)}{q(y)}y$$

Every hyperplane reflection τ_y leaves the subspace $(F \cdot y)^\perp$ fixed (hence the name), and in fact, τ_y generate all of $O(V)$ (not obvious).

Theorem 1.3.3: Witt's decomposition theorem

Any quadratic space (V, q) can be written as a orthogonal sum

$$(V, q) \cong (V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$$

where (V_t, q_t) is totally isotropic, (V_h, q_h) is hyperbolic, and (V_a, q_a) is anisotropic, in a unique way (up to isometry).

Proof. The decomposition first setting $(V_t, q_t) = \operatorname{rad} V$, and then writing $V \cong \operatorname{rad} V \perp V_0$. Then, V_0 is regular, and we can then apply Section 1.2 b) repeatedly to get the hyperbolic space, and being left with an anisotropic part.

Uniqueness then follows from repeated application of the cancellation theorem. □

We now move on to describe the final of Witt's fundamental theorems, namely the chain equivalence theorem.

Definition 1.3.4: Chain equivalence

Let $q = \langle a_1, \ldots, a_n \rangle$ and $q' = \langle b_1, \ldots, b_n \rangle$ be two diagonal quadratic forms. We say that q and q' are **simply equivalent** if there exists indecies i, j such that $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$, and $a_k = b_k$ for all $k \neq i, j$.
More generally, q and q' are said to be **chain equivalent**, denoted $q \simeq q'$, if there exists diagonal forms $f_1, \ldots, f_m$ such that $q, f_1,\ f_m, q'$ and f_i, f_{i+1} are all simply equivalent.

This allows us to state

Theorem 1.3.5

Let $f = \langle a_1, \ldots, a_n \rangle, g = \langle b_1, \ldots, b_m \rangle$ be diagonal quadratic forms. Then $f \cong g$ if and only if $f \simeq g$.

Proof. Obviously $f \simeq g$ implies $f \cong g$ (aside: the fact that this is obvious suggests that the notation is quite bad imo...), so we focus on the other direction.

First, we can clearly assume that f and g have $n = m$, and only non-zero coefficients (i.e., they are regular of the same dimension. Now choose $f' = \langle c_1, \ldots, c_n \rangle$ of all forms chain equivalent to f, such that $\langle c_1, \ldots, c_p \rangle$ already represents b_1 for the smallest p (this requires AoC). We will prove that $p = 1$. Notice that this implies the theorem as it shows that $\langle c_1 \rangle \cong \langle b_1 \rangle \Rightarrow f \simeq \langle b_1, \ldots, c_n \rangle$, which now proves the theorem by using the cancellation theorem and induction.

So assume that $p > 1$, and write $b_1 = c_1 x_1^2 + \cdots + c_p x_p^2$. By minimality, we have $c_1 x_1^2 + c_2 x_2^2 = d \neq 0$. Now $\langle c_1, c_2 \rangle \cong \langle d, c_1 c_2 d \rangle$ (by the representation theorem + looking at the determinant). But now $f' \simeq \langle d, c_3, \ldots, c_n, c_1 c_2 d \rangle$, and $b = d + c_3 x_3^3 + \cdots + c_p x_p^2$ contradicts the minimality of p. □

Finally, we end with a classical result, which we will simply state for now.

Theorem 1.3.6: Cartan-Dieudonné

Let (V, B, q) be a regular quadratic space of dimension n. Then every isometry $\sigma \in O_q(V)$ is a product of at most n hyperplane reflections.

Proof. See [1, Section 1.7]. □

2 Exercise Solutions

Solutions to some chosen exercises

2.1 Chapter 1

Exercise 2.1.A (Ex. 1)**.** Show that the group of self-isometries of the n-dimensional quadratic space $n\langle 1\rangle$ is isomorphic to $O(1)$.

Solution. The space can be represented by the matrix $M_f = I_n$. A self-isometry is a transform $T : \mathbb{F}^n \to \mathbb{F}^n$ such that $B(Tx, Ty) = B(x, y)$. Using the basis $M_B = I_n$ we see that $B(Tx, Ty) = x^t T^t I_n T y = x^t T^t T y^t$, in other words, we want $T^t T = I_n$, which are exactly the orthogonal matrices. □

Exercise 2.1.B (Ex. 8)**.**

1. Show that if $\{F_i : i \in I\}$ is a family of subfields of K, then for $F = \cap_{i \in I} F_i$, the natural map $F^\times/(F^\times)^2 \to \prod_i F_i^\times/(F_i^\times)^2$ is injective.
2. Conclude that if I is finite, and $F_i^\times/(F_i^\times)^2$ is finite for all i, then $F^\times/(F^\times)^2$ is also finite.

Solution. We start with 1). Take $\alpha \in F^\times$, which maps to the trivial class. This means that for all i, there exists $\beta_i \in F_i^\times$ so that $\beta_i^2 = \alpha$. Of course, we may fix $\beta_i = \beta$ for all i, since they are all subfields of K, in which α only has the roots $\pm\beta$. But then β is in the intersection of all F_i, and thus also in F.
2) is obvious from 1). □

Exercise 2.1.C (Ex. 10)**.** Show that the following conditions (on F) are equivalent:

1. Every 4-dimensional form over F of determinant -1 is isotropic.
2. Every even-dimensional form over F of determinant -1 is isotropic.
3. Every 3-dimensional form over F represents its own determinant.
4. Every odd-dimensional form over F represents its own determinant.

Solution. We will show 1) $\Rightarrow$ 3) $\Rightarrow$ 4) $\Rightarrow$ 2) $\Rightarrow$ 1).
1) $\Rightarrow$ 3): Take any 3-dimensional form q. By 1), the form $q \perp \langle -\det(q) \rangle$ is isotropic (compute its determinant), thus q represents $\det(q)$
3) $\Rightarrow$ 4): Hmm I'm stuck, maybe I need a better way later.
4) $\Rightarrow$ 2): Take an even-dimensional form q of determinant -1. Write $q \cong q' \perp \langle a \rangle$. Since $-1 = \det(q')a$, we have $\langle a \rangle \cong \langle -1/\det(q') \rangle \cong \langle -\det(q') \rangle$.. By 4), q' represents $\det(q')$, and thus the form is clearly isotropic.
2) $\Rightarrow$ 1): Obvious. $\square$

Exercise 2.1.D (Ex. 12)**.** In a hyperbolic space V, a maximal totally isotropic subspace is called a **Lagrangian**. Show that V is always the sum of two Lagrangians.

Solution. First, note that the hyperbolic plane has a basis so that it corresponds to the form X_1X_2. In this case, the unit vectors (which we will denote e_1, f_1) generate 1-dimensional Lagrangians, and we have $B(e_1, f_1) = 1$.
Let $\dim V = 2r$, and choose the basis $e_1, \ldots, e_r, f_1, \ldots, f_r$ obtained by taking the direct sum of the basis chosen above. Direct computation shows that $\mathrm{Span}\{e_1, \ldots, e_r\}$ is totally isotropic, and same for f. This already solves the exercise, but we also further note that $B(e_i, f_j) = \delta_{ij}$, i.e. this is a symplectic basis. $\square$

Exercise 2.1.E (Ex.29)**.** For any finite-dimensional F-algebra A, let $\mathrm{tr}_A : A \to F$ denote the algebraic trace on A. Then

$$(x, y) \to \mathrm{tr}_A(xy)$$

defines a symmetric bilinear form on A, denoted by (A, tr_A) (or more precicely, $(A, \mathrm{tr}_{A/F})$). If B is another finite-dimensional F-algebra, show that:

1. $(A \times B, \mathrm{tr}_{A \times B}) \cong (A, \mathrm{tr}_A) \perp (B, \mathrm{tr}_B)$, and
2. $(A \otimes B, \mathrm{tr}_{A \otimes B}) \cong (A, \mathrm{tr}_A) \otimes (B, \mathrm{tr}_B)$.

Solution. Recall that the algebraic trace is defined by chosing any basis of A, and taking $\mathrm{tr}_A(a) := \mathrm{tr}(L_a)$, where $L_a(x) = ax$.
1) For $(a, b) \in A \times B$, we have $L_{(a,b)}((x, y)) = (ax, by) = (L_a \oplus L_b)(a, b)$. The result follows since $\mathrm{tr}(T_1 \oplus T_2) = \mathrm{tr}(T_1) + \mathrm{tr}(T_2)$.
2) Similarily, we have $L_{a \otimes b}(x \otimes y) = ax \otimes by = (L_a \otimes L_b)(x \otimes y)$. The result follows since $\mathrm{tr}(T_1 \otimes T_2) = \mathrm{tr}(T_1)\,\mathrm{tr}(T_2)$. $\square$

References

[1] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*. Vol. 67. American Mathematical Soc., 2005.