An Introduction to Quadratic Forms

Klaas-Tido Rühl

October 30, 2006

1 Quadratic Forms and Quadratic Spaces

We define $\mathbb{N}$ not to contain 0. If we need the natural numbers to include 0, we will use the notation $\mathbb{N}_0$.

Throughout this talk K will always denote the base field.

1.1 Definition. *Let $n \in \mathbb{N}_0$.*

(1) A quadratic form *of dimension n is a homogeneous polynomial $\varphi \in K[X_1, \ldots, X_n]$ of degree 2, where $X_1, \ldots, X_n$ are indeterminates over K. We write* $\dim(\varphi) = n$.

(2) If V is an n-dimensional vector space over K, then $Q : V \to K$ is a quadratic map *on V if*

(i) $Q(av) = a^2 Q(v)$ for all $a \in K$ and $v \in V$, and

(ii) $V \times V \to K$, $(v, w) \mapsto Q(v + w) - Q(v) - Q(w)$, is a symmetric K-bilinear map.

The pair (V, Q) is then called a quadratic space.

1.2 Remark. It is very important to pay attention to the fact, that a quadratic form of dimension n does not have to be a polynomial in all the $X_1, \ldots X_n$. The dimension is a fixed part of the definition of a quadratic form. For example $X_1^2 + X_2^2 \in K[X_1, X_2, X_3]$ is a quadratic form of dimension 3. This implies, that the 0 polynomial can be a quadratic form of any dimension. But it is the only quadratic form of dimension 0. This way of defining quadratic forms is necessary to establish an easy correspondence between quadratic forms and quadratic spaces. △

Henceforth K will be a field with $\operatorname{char}(K) \neq 2$.

For a quadratic map $Q : V \to K$, we define a symmetric K-bilinear map

$$b_Q : \quad V \times V \longrightarrow K, \quad (v, w) \longmapsto \frac{1}{2}\big(Q(v + w) - Q(v) - Q(w)\big). \tag{1.1}$$

We see, that $Q(v) = b_Q(v, v)$ for all $v \in V$. Conversely, if $b : V \times V \to K$ is a symmetric K-bilinear form, then

$$Q_b : \quad V \longrightarrow K, \quad v \longmapsto b(v, v),$$

is a quadratic map on V, and we have $b_{Q_b} = b$. Since b_Q is uniquely determined by Q, and since Q_b is uniquely determined by b, we thus get a bijective correspondence between symmetric K-bilinear forms $V \times V \to K$ and quadratic maps $V \to K$.

1.3 Remark. The bijective correspondence between symmetric bilinear forms and quadratic maps depends heavily on the definition of b_Q in (1.1). If we allowed $\mathrm{char}(K) = 2$, this definition would not be possible. As a consequence there does not exist an analogous bijective correspondence over fields with characteristic 2. △

Now let (V, Q) be a quadratic space of dimension n, and let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a K-basis of V. We obtain a symmetric matrix $A = (b_Q(v_i, v_j))_{i,j=1,\ldots,n}$, and we call A the *matrix associated to Q with respect to $\mathcal{B}$*. With the help of this matrix $A = (a_{ij})_{i,j}$ we obtain the n-dimensional quadratic form $\sum_{i,j=1}^{n} a_{ij} X_i X_j \in K[X_1, \ldots, X_n]$, which we call the *quadratic form associated to Q with respect to $\mathcal{B}$*.

Obviously an n-dimensional quadratic form $\varphi \in K[X_1, \ldots, X_n]$ defines a quadratic map

$$K^n \longrightarrow K, \quad (x_1, \ldots, x_n) \longmapsto \varphi(x_1, \ldots, x_n).$$

We will also denote this map by φ. This makes (K^n, φ) a quadratic space. If A is the matrix associated to φ with respect to the standard basis $\{e_1, \ldots, e_n\}$, then we obviously have $b_\varphi(e_i, e_j) = e_i^t A e_j$, where for any matrix B its transpose is denoted by B^t. Furthermore, if $A = (a_{ij})_{i,j}$, we obtain $\varphi = \sum_{i,j=1}^{n} a_{ij} X_i X_j$. In general we denote by A_φ the matrix associated to a quadratic form φ with respect to the standard basis.

1.4 Definition. *Let $n \in \mathbb{N}_0$.*

(1) Let (V_1, Q_1) and (V_2, Q_2) be two quadratic spaces over K. A homomorphism $f : V_1 \to V_2$ of K-vector spaces is called metric*, if $Q_1(v) = Q_2(f(v))$ for all $v \in V_1$.*

(2) The spaces (V_1, Q_1) and (V_2, Q_2) are called equivalent *or* isometric*, if there exists a metric isomorphism $V_1 \to V_2$. We then write $(V_1, Q_1) \cong (V_2, Q_2)$.*

(3) Two n-dimensional quadratic forms φ and ψ are equivalent *or* isometric*, if there exists an invertible matrix $T \in \mathrm{GL}_n(K)$ such, that $A_\varphi = T A_\psi T^t$. We write $\varphi \cong \psi$.*

It is easy to check, that equivalence of quadratic spaces and quadratic forms is indeed an equivalence relation. Furthermore it is obvious, that φ and ψ are equivalent if and only if (K^n, φ) and (K^n, ψ) are equivalent.

1.5 Remark. Now we have established a correspondence between quadratic forms, quadratic spaces (with a fixed basis) and symmetric matrices. We can assign to every quadratic space with a fixed basis a unique symmetric matrix, which in addition defines a unique quadratic form. Conversely for every quadratic form we obtain a unique quadratic space and a unique symmetric matrix. Furthermore we have seen, that this correspondence is compatible with equivalence. In the following sections this will enable us to switch between these three classes of objects, which will be of great help during many of the following proofs. △

1.6 Definition. *We say, that a quadratic map $Q : V \to K$* represents *an element $a \in K$ if there exists $v \in V \setminus \{0\}$ with $Q(v) = a$. Analogously an n-dimensional quadratic form φ is said to* represent *a if there exists $w \in K^n \setminus \{0\}$ such that $\varphi(w) = a$.*

2 Orthogonality

2.1 Definition. *Let (V, Q) be a quadratic space of dimension n over K.*

(1) Two vectors $v, w \in V$ are called orthogonal, *if $b_Q(v,w) = 0$. We use the notation $v \perp w$.*

(2) A basis $\{v_1, \ldots, v_n\}$ of V is an orthogonal basis *of (V,Q) if $b_Q(v_i, v_j) = 0$ for all $i \neq j$.*

(3) Two subspaces $U_1, U_2 \subset V$ are orthogonal, *if we have $v \perp w$ for all $v \in U_1$ and $w \in U_2$.*

(4) For a subspace $U \subset V$ we define

$$U^\perp \;:=\; \{v \in V \mid v \perp u \;\forall\, u \in U\}\,.$$

If $U \cap U^\perp = \{0\}$, we call $U^\perp$ the orthogonal complement *of U in V.*

(5) The Radical *of (V,Q) is defined as* $\mathrm{Rad}(V) = \mathrm{Rad}(V,Q) := V^\perp \subset V$.

(6) The space (V,Q) is called nondegenerate *or* regular, *if* $\mathrm{Rad}(V) = \{0\}$. *Otherwise (V,Q) is called* degenerate.

(7) An n-dimensional quadratic form φ over K is called nondegenerate *or* regular, *if (K^n, φ) is nondegenerate. Accordingly the form φ is called* degenerate, *if (K^n, φ) is degenerate.*

From the fact that b_Q is a bilinear form it follows, that $U^\perp$ is a subvector space of V for every subspace $U \subset V$. In particular this implies, that $\mathrm{Rad}(V)$ is a subspace of V. Observe, that the 0-dimensional quadratic space $(\{0\}, 0)$ is nondegenerate by definition.

Let (V,Q) be a quadratic space over K, and let $U \subset V$ be a subspace of V. Denote by $U^* = \{f : U \to K \mid f \text{ is } K\text{-linear}\}$ the dual of U. Then we obtain a K-linear map

$$q_U :\; V \longrightarrow U^*, \quad v \longmapsto \big(U \to K, u \mapsto b_Q(v,u)\big).$$

Since $q_U(v) = 0$ if and only if $b_Q(v,u) = 0$ for all $u \in U$, it becomes apparent that $\ker(q_U) = U^\perp$. In particular if follows, that (V,Q) is nondegenerate if and only of $q_V : V \to V^*$ is an isomorphism.

2.2 Definition. *(1) Let (U_1, Q_1) and (U_2, Q_2) be quadratic spaces over K. We define the* orthogonal sum *of these two spaces to be $(U_1 \oplus U_2, Q_1 + Q_2)$, where simply*

$$Q_1 + Q_2 :\quad U_1 \oplus U_2 \longrightarrow K, \quad v_1 + v_2 \longmapsto Q_1(v_1) + Q_2(v_2).$$

We also use the notation $(U_1, Q_1) \perp (U_2, Q_2) := (U_1 \oplus U_2, Q_1 + Q_2)$.

(2) Let $\psi \in K[X_1, \ldots, X_n]$ and $\chi \in K[Y_1, \ldots, Y_m]$ be quadratic forms over K. The orthogonal sum *$\psi \perp \chi$ is the quadratic form $\psi + \chi \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.*

(3) If φ and ψ are quadratic forms over K such that there exists a quadratic form χ over K with $\varphi \cong \psi \perp \chi$, then ψ is a subform *of φ.*

Obviously the subspaces U_1 and U_2 of $U_1 \oplus U_2$ are orthogonal, hence the term "orthogonal sum". This fact carries over to quadratic forms. More specifically $(K^{n+m}, \psi \perp \chi) \cong (K^n, \psi) \perp (K^m, \chi)$. We immediately see, that

$$A_{\psi \perp \chi} \;=\; \begin{pmatrix} A_\psi & 0 \\ 0 & A_\chi \end{pmatrix}.$$

2.3 Proposition. *Let (V,Q) be a nondegenerate quadratic space over K, and let $U \subset V$ be a subspace of V.*

(1) All metric homomorphisms $f : (V,Q) \to (V',Q')$ are injective

(2) For all subvector spaces $U \subset V$ we have

(i) $(U^\perp)^\perp = U$,

(ii) $\dim_K(U) + \dim_K(U^\perp) = \dim_K(V)$, *and*

(iii) $\mathrm{Rad}(U) = \mathrm{Rad}(U^\perp) = U \cap U^\perp$.

The quadratic space $(U, Q|_U)$ is nondegenerate iff $(U^\perp, Q|_{U^\perp})$ is nondegenerate, and in this case we have $(V, Q) = (U, Q|_U) \perp (U^\perp, Q|_{U^\perp})$.

(3) If V is the orthogonal direct sum of two subspaces, those are nondegenerate and orthogonal to each other.

[Ser73, Proposition 2, page 28]

Proof. (1): If $f(v) = 0$ for some $v \in V_1$, then we have $b_Q(v, w) = b_{Q'}(f(v), f(w)) = 0$ for all $w \in V$. Thus $v \in \mathrm{Rad}(V)$, and as we assumed (V, Q) to be nondegenerate we must have $v = 0$.

(2): Since (V, Q) is nondegenerate, the homomorphism $q_V : V \to V^*$ is an isomorphism. Hence $q_U : V \to U^*$ is surjective, since it is the composition of q_V with the canonical surjection $V^* \to U^*$. As a result we get the exact sequence

$$0 \longrightarrow U^\perp \longrightarrow V \longrightarrow U^* \longrightarrow 0,$$

which implies $\dim_K(V) = \dim_K(U^*) + \dim_K(U^\perp) = \dim_K(U) + \dim_K(U^\perp)$.

Applying, what we have just proven, to $U^\perp$ instead of U, implies $\dim(U) = \dim((U^\perp)^\perp)$. Since obviously $U \subset (U^\perp)^\perp$, we obtain $U = (U^\perp)^\perp$.

Now the equation $\mathrm{Rad}(U) = U \cap U^\perp$ is clear. Replacing U by $U^\perp$ and taking into account that $U = (U^\perp)^\perp$ implies $\mathrm{Rad}(U) = U \cap U^\perp = \mathrm{Rad}(U^\perp)$. The last statement of (2) immediately follows.

(3): If $(V, Q) = (U_1, Q|_{U_1}) \perp (U_2, Q|_{U_2})$, then U_1 and U_2 are obviously orthogonal to each other. Since $U_2 \subset U_1^\perp$ and also $\dim(U_1^\perp) = \dim_K(V) - \dim(U_1) = \dim(U_2)$, it follows that $U_2 = U_1^\perp$. As $\mathrm{Rad}(U_1) = U_1 \cap U_2 = \{0\}$ we see, that U_1 is nondegenerate. By (2) the same is true for $U_2 = U_1^\perp$. □

2.4 Corollary. *Every subform of a nondegenerate quadratic form φ over K is nondegenerate.*

3 Diagonal Forms

Consider an n-dimensional quadratic form φ over K such that the standard basis $\{e_1, \ldots, e_n\}$ is also an orthogonal basis of (K^n, φ). In this case A_φ is a diagonal matrix with entries say $a_1, \ldots, a_n \in K$, and we use the notation

$$\langle a_1, \ldots, a_n \rangle \;:=\; \varphi \;=\; a_1 X_1^2 + \cdots + a_n X_n^2 \;\in\; K[X_1, \ldots, X_n]$$

and call φ a *diagonal (quadratic) form* with entries $a_1, \ldots, a_n$. Now assume $\mathrm{Rad}(K^n, \varphi) \neq \{0\}$. Then there exists some $0 \neq v = \lambda_1 e_1 + \cdots + \lambda_n e_n$ with $\lambda_i \in K$ such that

$$b_\varphi(v, e_i) \;=\; \lambda_i b_\varphi(e_i, e_i) \;=\; \lambda_i a_i \;=\; 0 \qquad \forall\, i = 1, \ldots, n.$$

Since $v \neq 0$, there must exist at least one $j \in \{1, \ldots, n\}$ such that $a_j = 0$. Conversely every nondegenerate form can only have nonzero entries.

3.1 Lemma. *Every quadratic space (V, Q) can be written as an orthogonal sum $(V, Q) = (\mathrm{Rad}(V), 0) \perp (U, Q|_U)$ with some subvector space $U \subset V$.*

Proof. Choose any basis $\{v_1, \ldots, v_r\}$ for $\mathrm{Rad}(V)$ and complete it to a basis $\{v_1, \ldots, v_n\}$ of V. Let U be the subspace of V generated by $v_{r+1}, \ldots, v_n$. Then $V = \mathrm{Rad}(V) \oplus U$, and by the definition of $\mathrm{Rad}(V)$ we have $b_Q(v, w) = 0$ for all $v \in \mathrm{Rad}(V)$ and all $w \in U$. This shows, that $\mathrm{Rad}(V)$ and U are orthogonal, which completes the proof. □

3.2 Theorem. *Every n-dimensional quadratic space (V, Q) has an orthogonal basis $\{v_1, \ldots, v_n\}$. In particular, if there exists an $a \in \mathrm{im}(Q) \setminus \{0\}$, then we can choose v_1 such that $Q(v_1) = a$.*

[Ser73, Theorem 1, page 30]

Proof. If $\mathrm{Rad}(V) = V$, then $Q = 0$ and any basis of V is an orthogonal basis. By the previous lemma it therefore only remains to show the theorem for the case, that $\dim_K(V) \geq 1$ and (Q, V) is nondegenerate.

Let $a \in K^*$ such that there exists a $v \in V \setminus \{0\}$ with $Q(v) = a$. Such an a must exists, since we excluded the case $Q = 0$. We will proceed by induction on n. For the case $n = 1$ the vector v trivially defines an orthogonal basis.

Now let $n > 1$. The subspace $Kv \subset V$ generated by v is trivially nondegenerate. By Proposition 2.3 (2) $U := (Kv)^\perp$ is nondegenerate as well and $(V, Q) = (Kv, Q|_{Kv}) \perp (U, Q|_U)$. By the induction hypothesis we can find an orthogonal basis $\{v_2, \ldots, v_n\}$ for U. If we set $v_1 := v$, then $\{v_1, \ldots, v_n\}$ is the desired orthogonal basis. □

3.3 Corollary. *Every quadratic form φ of dimension n over K is equivalent to a diagonal form $\langle a_1, \ldots, a_n \rangle$. If $\varphi \neq 0$, then a_1 can be chosen to be any element of $a \in \mathrm{im}(\varphi) \setminus \{0\}$.*

Proof. By the previous theorem we can find an orthogonal basis $\{v_1, \ldots, v_n\}$ of K^n such that $\varphi(v_1) = a$ if $\varphi \neq 0$. Consider the isomorphism $f : K^n \to K^n$ given by $e_i \mapsto v_i$, where $\{e_1, \ldots, e_n\}$ is the standard basis of K^n. Then $(K^n, \varphi \circ f)$ is a quadratic space with the standard basis as an orthogonal basis. Let ψ be the associated quadratic form to $\varphi \circ f$ with respect to the standard basis, then $\psi \cong \varphi$ and $\psi = \langle a_1, \ldots, a_n \rangle$. Furthermore $a_1 = a$ if $\varphi \neq 0$. □

Before closing this section we introduce the discriminant of a quadratic form and prove a useful lemma, that is indispensable for the work with quadratic forms.

3.4 Definition. *Let φ be a quadratic form over K.*

(1) We define the determinant *of φ as* $\det(\varphi) := \det(A_\varphi)$.

(2) The discriminant *of φ is $d(\varphi) := \det(A_\varphi)(K^*)^2 \in {}^{K^*}\!/_{(K^*)^2} \cup \{0\}$, where ${}^{K^*}\!/_{(K^*)^2}$ is the* square class group *of K.*

Let φ and ψ be two quadratic forms over K with $\varphi \cong \psi$, and let $T \in \mathrm{GL}_n(K)$ be the isometry such that $A_\psi = T A_\varphi T^t$. If $\det(T) \neq \pm 1$, then $\det(\varphi) \neq \det(\psi)$. Thus we see, that the determinant of a quadratic form is not well defined on the equivalence class of a quadratic form. But since $\det(\psi) = \det(T)^2 \det(\varphi)$, it follows, that $d(\varphi) = d(\psi)$. Furthermore by corollary 3.3 and the fact that $\det(T) \neq 0$ we have $\det(\varphi) \neq 0$ resp. $d(\varphi) \neq 0$ if and only if φ is nondegenerate.

3.5 Lemma. *If $\varphi = \langle a, b \rangle$ with $a, b \in K^*$ and $c \in \mathrm{im}(\varphi) \setminus \{0\}$, then $\varphi \cong \langle c, abc \rangle$.*

Proof. By corollary 3.3 we have $\varphi \cong \langle c, x\rangle$ with some $x \in K^*$. Since $d(\varphi) = d(\langle c, x\rangle)$, there exists some $z \in K^*$ with $ab = z^2cx$. Therefore $x = \frac{ab}{z^2c}$. Since obviously $\langle c, x\rangle \cong \langle c, z^2c^2x\rangle$, we obtain $\langle a, b\rangle \cong \langle c, abc\rangle$. □

4 Isotropy and Hyperbolic Planes

4.1 Definition. *Let (V, Q) be a quadratic space and φ be a quadratic form over K.*

(1) A vector $v \in V \setminus \{0\}$ is called isotropic*, if $Q(v) = 0$. A subspace $U \subset V$ is called* totally isotropic *or plainly* isotropic*, if $Q|_U = 0$.*

(2) The form φ is called isotropic*, if there exists some $v \in K^n \setminus \{0\}$ with $\varphi(v) = 0$. Otherwise φ is called* anisotropic*.*

Trivially $\mathrm{Rad}(V, Q)$ is a totally isotropic subspace. Accordingly every degenerate form φ is isotropic.

4.2 Definition. *(1) A quadratic space (V, Q) is a* hyperbolic plane*, if V has a basis consisting of two isotropic vectors $v, w \in V$ such that $b_Q(v, w) \neq 0$.*

(2) The quadratic form $\langle 1, -1\rangle$ and every form, that is isometric to it, will be called a hyperbolic plane*. A quadratic form, that is isometric to an orthogonal sum of hyperbolic planes is called* hyperbolic*.*

If $b_Q(v, w) = a \in K^*$, then $b_Q(v, \frac{1}{a}w) = 1$ and $\{\frac{1}{a}v, w\}$ is still a basis consisting of isotropic vectors. Hence we can always assume, that $b_Q(v, w) = 1$. Then the matrix associated to Q with respect to $\{v, w\}$ is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. In particular we see, that (V, Q) is nondegenerate.

If we consider the 2-dimensional quadratic form $\chi = 2X_1X_2 \in K[X_1, X_2]$ over K, then it follows, that (K^2, χ) is a hyperbolic plane. Choosing the basis $\{v + \frac{1}{2}w, v - \frac{1}{2}w\}$ we obtain the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, which shows, that $(K^2, \langle 1, -1\rangle)$ is a hyperbolic plane, too. This explains the double use for the notion "hyperbolic plane". Notably it follows, that $\langle 1, -1\rangle \cong 2X_1X_2$.

4.3 Proposition. *For every nondegenerate quadratic space (V, Q) which has an isotropic element $v \in V$, there exists a decomposition $(V, Q) = (U, Q|_U) \perp (V', Q|_{V'})$ such that $(U, Q|_U)$ is a hyperbolic plane.*

[Ser73, Proposition 3, page 29]

Proof. Since (V, Q) is nondegenerate, there exists $w' \in V$ such that $b_Q(v, w') = 1$. We must have v and w' linearly independant since $b_Q(v, v) = 0$. Now $w := 2w' - b_Q(w', w')v$ is isotropic, as can easily be checked. Also $b_Q(v, w) = 2$. Let U be the subspace of V generated by v and w. Since $(U, Q|_U)$ is nondegenerate the same holds for $(V', Q|_{V'})$ where $V' = U^\perp$ by Proposition 2.3 (2). Furthermore we have $(V, Q) = (U, Q|_U) \perp (V', Q|_{V'})$. □

4.4 Corollary. *If (V, Q) is a nondegenerate quadratic space over K possessing an isotropic element, then $Q(V) = K$.*

[Ser73, Corollary, page 29]

Proof. By the previous proposition we can without loss of generality assume, that (V, Q) is a hyperbolic plane. Furthermore we can assume, that we are given a basis $v, w \in V$ such that v and w are isotropic with $b_Q(v, w) = 1$. Let $a \in K$, then

$$Q\Big(v + \frac{a}{2}w\Big) \;=\; Q(v) + 2b_Q\Big(v, \frac{a}{2}w\Big) + Q\Big(\frac{a}{2}w\Big) \;=\; ab_Q(v, w) \;=\; a.$$

□

4.5 Corollary. *Every nondegenerate, isotropic quadratic form φ over K has a decomposition $\varphi \cong \psi \perp \chi$, where ψ is anisotropic and χ is hyperbolic.*

Proof. The statement follows by applying proposition 4.3 inductively. □

4.6 Corollary. *Up to equivalence there exists only one nondegenerate, isotropic quadratic form of dimension 2 over K. It is given by*

$$\langle 1, -1\rangle \;\cong\; \langle a, -a\rangle \qquad \forall\, a \in K^*.$$

Proof. It suffices to apply the last two corollaries and lemma 3.5. □

5 Witt's Cancellation Theorem

The following theorem lays the foundation for the algebraic theory of quadratic forms.

5.1 Theorem. *(Witt's Cancellation Theorem)*
Let φ, φ_1 and φ_2 be quadratic forms over K such that $\varphi \perp \varphi_1 \cong \varphi \perp \varphi_2$, then $\varphi_1 \cong \varphi_2$.

[Pfi95, Theorem 1.1, page 19]

Proof. Let $\dim(\varphi) = m$, and let $n = \dim(\varphi_1) = \dim(\varphi_2)$. Since the statement only deals with the equivalence of quadratic forms, we can by corollary 3.3 without loss of generality assume, that φ, φ_1 and φ_2 are diagonal forms.

As the dimension of the radical of a quadratic space is naturally invariant under isometry, also the dimensions of $\mathrm{Rad}(K^n, \varphi_1)$ and $\mathrm{Rad}(K^n, \varphi_2)$ must be equal. Assume $\varphi_1 = \langle b_1, \ldots, b_n\rangle$ and $\varphi_2 = \langle c_1, \ldots, c_n\rangle$ with $b_1, \ldots, b_s, c_1, \ldots, c_s \in K^*$ and $b_{s+1} = \cdots = b_n = c_{s+1} = \ldots c_n = 0$ for some $s \in \{0, \ldots, n\}$. Then we can replace φ by $\varphi \perp \langle b_{s+1}, \ldots, b_n\rangle = \varphi \perp \langle c_{s+1}, \ldots, c_n\rangle$, and we can replace φ_1 by $\langle b_1, \ldots, b_s\rangle$ and φ_2 by $\langle c_1, \ldots, c_s\rangle$. That means we can assume, that φ_1 and φ_2 are nondegenerate.

Finally by using a simple induction, we can further restrict our proof to the case, that $\dim(\varphi) = 1$, say $\varphi = \langle a\rangle$ for some $a \in K^*$.

The result of all these reductions is a $(n+1) \times (n+1)$-matrix T such that $(\langle a\rangle \perp \varphi_1)(Tv) = (\langle a\rangle \perp \varphi_2)(v)$ for all $v \in K^{n+1}$. Let $v = \binom{x_0}{v'}$ with $x_0 \in K$ and $v' \in K^n$. Similarly let

$$T \;=\; \begin{pmatrix} t & x^t \\ y & U \end{pmatrix}$$

with $t \in K$, $x, y \in K^n$ and $U \in M_n(K)$. Then

$$\begin{aligned}(\langle a\rangle \perp \varphi_1)(Tv) &= (\langle a\rangle \perp \varphi_1)\left(\begin{pmatrix} tx_0 + x^t v' \\ yx_0 + Uv' \end{pmatrix}\right) \\ &= a(tx_0 + x^t v')^2 + \varphi_1(yx_0 + Uv') \\ &= ax_0^2 + \varphi_2(v') \\ &= (\langle a\rangle \perp \varphi_2)(v).\end{aligned}$$

Since $\mathrm{char}(K) \neq 2$ we have $t + 1 \neq 0$ or $t - 1 \neq 0$. This means that one of the equations

$$x_0 = tx_0 + x^t v' \qquad \text{or} \qquad -x_0 = tx_0 + x^t v' \tag{5.1}$$

has a solution, namely $x_0 = \frac{x^t}{1-t} v'$ or $x_0 = \frac{x^t}{-t-1} v'$. Without loss of generality we can assume, that $x_0 = \frac{x^t}{t-1} v'$ is a solution of the first equation in (5.1). Put $w := \frac{1}{1-t} x \in K^n$. Then $a(tx_0 + x^t v')^2 = ax_0^2$ and we must have

$$\varphi_1((yw^t + U)v') \;=\; \varphi_2(v).$$

Since $v \in K^{n+1}$ and therefore $v' \in K^n$ are arbitrary elements, and since by our assumption φ_1 and φ_2 are nondegenerate, we must have $(yw^t + U) \in \mathrm{GL}_n(K)$. Thus $\varphi_1 \cong \varphi_2$. □

As an application we prove Witt's chain equivalence theorem, which will be needed to show, among other things, that the *Hasse invariant* is well-defined.

5.2 Definition. *Let $\varphi = \langle a_1, \ldots, a_n\rangle$ and $\psi = \langle b_1, \ldots, b_n\rangle$ be two quadratic forms over K.*

(1) The forms φ and ψ are simply-equivalent*, if there exist two indices i and j (we do not require $i \neq j$) such that $\langle a_i, a_j\rangle \cong \langle b_i, b_j\rangle$ and $a_k = b_k$ for all $k \in \{1, \ldots, n\}$ with $k \neq i, j$.*

(2) The forms φ and ψ are called chain-equivalent*, if there exists a sequence of diagonal forms $\varphi_0, \ldots, \varphi_k$ such that $\varphi = \varphi_0$, $\psi = \varphi_k$ and φ_i and φ_{i-1} are simply-equivalent for $i = 1, \ldots, k$. We write $\varphi \approx \psi$.*

It is obvious, that chain-equivalence of two quadratic forms implies, that those forms are equivalent in the usual sense. The following theorem takes care of the opposite direction.

5.3 Lemma. *If $\varphi = \langle a_1, \ldots, a_n\rangle$ and ψ are two n-dimensional diagonal forms over K, such that there exists a permutation $\sigma \in S_n$ with $\psi = \langle a_{\sigma(1)}, \ldots, a_{\sigma(n)}\rangle$, then φ and ψ are chain-equivalent.*

Proof. The lemma follows from the fact, that S_n is generated by transpositions. □

5.4 Theorem. *(Witt's Chain Equivalence Theorem)*
If φ and ψ are equivalent diagonal forms over K, then they are also chain-equivalent.

[Lam05, Theorem 5.2, page 16]

Proof. let $\varphi = \langle a_1, \ldots, a_n\rangle$ and $\psi = \langle b_1, \ldots, b_n\rangle$. Since $\varphi \cong \psi$ the K-vector spaces $\mathrm{Rad}(K^n, \varphi)$ and $\mathrm{Rad}(K^n, \psi)$ must have the same dimension. This means, that φ and ψ must have the same number of zero entries. From the previous lemma it follows, that it suffices to show the theorem only for the subforms of φ and ψ that consist only of the non-zero entries of φ resp. ψ. So we can without loss of generality assume, that φ and ψ are nondegenerate. We proceed by induction on n. The cases $n = 1, 2$ are trivial.

Assume $n \geq 3$. Since chain-equivalence implies equivalence, every form, that is chain-equivalent to φ, will represent b_1. We choose a diagonal form $\varphi' = \langle c_1, \ldots, c_n \rangle$ that is chain-equivalent to φ with $b_1 = c_1\lambda_1^2 + \cdots + c_p\lambda_p^2$, $\lambda_i \in K$, such that p is minimal for all forms chain-equivalent to φ. We want to show, that $p = 1$.

Assume, that $p \geq 2$. Since p is minimal no subsum of $c_1\lambda_1^2 + \cdots + c_p\lambda_p^2$ can be equal to zero. In particular $d = c_1\lambda_1^2 + c_2\lambda_2^2 \neq 0$. By lemma 3.5 we have $\langle c_1, c_2 \rangle \cong \langle d, c_1c_2d \rangle$. Thus

$$\begin{aligned} \varphi \approx \varphi' &= \langle c_1, c_2, c_3, \ldots, c_n \rangle \\ &\approx \langle d, c_1c_2d, c_3, \ldots, c_n \rangle \\ &\approx \langle d, c_3, \ldots, c_n, c_1c_2d \rangle, \end{aligned}$$

and $b_1 = d + c_3^2 + \ldots c_n^2$. This contradicts the minimality of p. Hence we must have $p = 1$ and $\varphi \approx \varphi' = \langle b_1, c_2, \ldots, c_n \rangle$. Since $\varphi \cong \varphi'$ by Witt's cancellation theorem 5.1 it follows from $\langle b_1, c_2, \ldots, c_n \rangle \cong \langle b_1, \ldots, b_n \rangle$, that $\langle c_2, \ldots, c_n \rangle \cong \langle b_2, \ldots, b_n \rangle$. By the induction hypothesis $\langle c_2, \ldots, c_n \rangle \approx \langle b_2, \ldots, b_n \rangle$. Altogether we obtain

$$\varphi \approx \langle b_1, c_2, \ldots, c_n \rangle \approx \langle b_1, \ldots, b_n \rangle = \psi.$$

□

6 Application: Quadratic Forms over Finite Fields

Let $p \neq 2$ be a prime number, and let $q = p^r$ be a power of p. In this section we will give a complete classification of quadratic forms over the finite field $\mathbb{F}_q$ with q elements. In the following results we will only consider nondegenerate forms. By lemma 3.1 this does not siginify a restriction, since the radical of a quadratic space is invariant under equivalence.

6.1 Proposition. *If φ is a nondegenerate quadratic form over $\mathbb{F}_q$ with $\dim(\varphi) \geq 2$, then $\mathrm{im}(\varphi) \supset \mathbb{F}_q^*$. In the case $\dim(\varphi) \geq 3$ we even have $\mathrm{im}(\varphi) = \mathbb{F}_q$.*

[Ser73, Proposition 4, page 34]

Proof. By corollary 3.3 it suffices to consider an arbitrary 2-dimension diagonal form $\langle a, b \rangle$. If $\langle a, b \rangle$ is already isotropic, then we have $\mathrm{im}(\langle a, b \rangle) = \mathbb{F}_q$ and there is nothing to show. So assume, that $\langle a, b \rangle$ is anisotropic. The statement will be proven, if we can show for any $x \in \mathbb{F}_q^*$, that $\langle a, b, x \rangle$ is isotropic. But this is a consequence of the Chevalley theorem. □

We know, that $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ has exactly two elements, since $p \neq 2$. Let a denote an element of $\mathbb{F}_q^*$ which is not a square.

6.2 Proposition. *Every nondegenerate quadratic form φ of dimension n over $\mathbb{F}_q$ is equivalent to either*

$$\langle 1, \ldots, 1, 1 \rangle \qquad \text{or} \qquad \langle 1, \ldots, 1, a \rangle$$

depending on whether its discriminant is the unit element of $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ or not.

[Ser73, Proposition 5, page 34]

Proof. The statement is trivial if $n = 1$. Now if $n \geq 2$, then the previous proposition shows, that φ represents 1. By lemma 3.5 we have $\varphi \cong \langle 1 \rangle \perp \psi$ with $\dim(\psi) = n - 1$. The statement now follows by simple induction. □

6.3 Corollary. *Two nondegenerate forms over $\mathbb{F}_q$ are equivalent if and only if they have the same dimension and the same discriminant.*

[Ser73, Corollary, page 35]

References

[Lam05] Lam, Tsit-Yuen: *Introduction to Quadratic Forms over Fields*. American Mathematical Society, 2005

[Pfi95] Pfister, Albrecht: *London Math. Soc. Lecture Note Series*. Bd. 217: *Quadratic Forms with Applications to Algebraic Geometry and Topology*. Cambridge University Press, 1995

[Ser73] Serre, Jean-Pierre: *Graduate Texts in Mathematics*. Bd. 7: *A Course in Arithmetic*. Springer-Verlag New York, Heidelberg, Berlin, 1973