Chapter II

The geometry of classical groups

We denote by V a vector space over the field $\mathbb{F}$. For simplicity we assume that its dimension is finite. Our main references here will be [11], [14], [15] and [21].

1 Sesquilinear forms

Let σ be an automorphism of $\mathbb{F}$ with $\sigma^2 = \mathrm{id}$. Set $\alpha^\sigma := \sigma(\alpha)$ for all $\alpha \in \mathbb{F}$.

(1.1) Definition *A σ-sesquilinear* form *on V is a map* $(\ ,\ ) : V \times V \to \mathbb{F}$ *such that, for every $\lambda, \mu \in \mathbb{F}$ and for every $u, v, w \in V$:*

(1) $(u, v + w) \ = (u, v) + (u, w)$,

(2) $(u + v, w) \ = (u, w) + (v, w)$,

(3) $(\lambda u, \mu v) \ = \lambda \mu^\sigma (u, v)$.

The form is said to be:

i) bilinear symmetric *if $\sigma = \mathrm{id}_{\mathbb{F}}$ and $(v, w) = (w, v)$, $\forall\ v, w \in V$;*

ii) bilinear antisymmetric *if $\sigma = \mathrm{id}_{\mathbb{F}}$ and $(v, v) = 0$, $\forall\ v \in V$;*

iii) hermitian *if $\sigma \neq \mathrm{id}_{\mathbb{F}}$, $\sigma^2 = \mathrm{id}_{\mathbb{F}}$ and $(v, w) = (w, v)^\sigma$, $\forall\ v, w \in V$;*

iv) non singular *if, for every $v \in V \setminus \{0_V\}$, there exists $u \in V$ such that $(u, v) \neq 0_{\mathbb{F}}$.*

(1.2) Definition *V is* non-singular *(or* non-degenerate*) when the form is non-singular.*

(1.3) Lemma *If the form is bilinear antisymmetric, then:*

$$(v, w) = -(w, v), \quad \forall\ v, w \in V.$$

Proof

$0 = (v+w, v+w) = (v, v)+(v, w)+(w, v)+(w, w) = (v, w)+(w, v) \Longrightarrow (v, w) = -(w, v)$.

■

(1.4) Definition *Let V, V' be vector spaces over $\mathbb{F}$, endowed with sesquilinear forms*

$$(\ ,\ ) : V \times V \to \mathbb{F}, \qquad (\ ,\ )' : V' \times V' \to \mathbb{F}.$$

(1) *An* isometry *from V to V' is an invertible element $f \in \mathrm{Hom}_{\mathbb{F}}(V, V')$ such that*

$$(f(v), f(w))' = (v, w), \quad \forall\ v, w \in V.$$

(2) *The spaces $(V, \mathbb{F}, (\ ,\ ))$ and $(V', \mathbb{F}, (\ ,\ )')$ are called* isometric *if there exists an isometry $f : V \to V'$.*

(1.5) Lemma *When $V = V'$, the set of isometries of V is a subgroup of $\mathrm{Aut}_{\mathbb{F}}(V)$, called the* group of isometries *of the form $(\ ,\ )$.*

The proof is left as an exercise.

(1.6) Theorem *(Witt's Extension Lemma) Let V be equipped with a non-degenerate form, either bilinear (symmetric or antisymmetric) or hermitian. Let U and W be subspaces and suppose that*

$$\tau : U \to W$$

is an isometry with respect to the restriction of the form to U and W, Then there exists an isometry $\hat{\tau} : V \to V$ which extends τ, namely such that $\hat{\tau}_U = \tau$.

For the proof of this important result see [1, page 81] or [14, page 367].

2 The matrix approach

Given a σ-sesquilinear form $(\ ,\ )$ on V, let us fix a basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ of V over $\mathbb{F}$.

(2.1) Definition *The* the matrix J *of the above form* with respect to $\mathcal{B}$ *is defined by*

$$J := ((v_i, v_j)), \quad 1 \le i, j \le n.$$

Given $v = \sum_{i=1}^n k_i v_i$, $w = \sum_{i=1}^n h_i v_i$ in V, it follows from the axioms that

$$(v, w) = \sum_{i,j=1}^{n} k_i h_j^\sigma (v_i, v_j) \ = \ v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma, \quad \forall\ v, w \in V. \tag{2.2}$$

(2.3) Lemma *J is* the only *matrix of* $\mathrm{Mat}_n(\mathbb{F})$ *which satisfies* (2.2) *for the given form.*

Proof Let $A = (a_{ij}) \in \mathrm{Mat}_n(\mathbb{F})$ satisfy $(v, w) = v_{\mathcal{B}}^T A w_{\mathcal{B}}^\sigma$ for all v, w in V.
Letting v, w vary in $\mathcal{B}$ and noting that $v_{i\mathcal{B}} = e_i$, $1 \leq i \leq n$ we have:

$$(v_i, v_j) \;=\; {v_{i\mathcal{B}}}^T A {v_{j\mathcal{B}}}^\sigma \;=\; {e_i}^T A e_j = a_{ij}, \quad 1 \leq i, j \leq n.$$

We conclude that $J = A$. ∎

(2.4) Lemma *Let J be the matrix of a σ-sesquilinear form $(\ ,\ )$ on V.*

(1) *If $\sigma = \mathrm{id}_{\mathbb{F}}$, then the form is symmetric if and only if $J^T = J$;*

(2) *if $\sigma = \mathrm{id}_{\mathbb{F}}$, then the form is antisymmetric if and only if $J^T = -J$;*

(3) *if σ has order 2, then the form is hermitian if and only if $J^T = J^\sigma$.*

Moreover the form $(\ ,\ )$ is non-degenerate if and only if $\det J \neq 0$.

(2.5) Lemma *Let $J \in \mathrm{Mat}_n(\mathbb{F})$ be the matrix of a sesquilinear form on V with respect to a basis $\mathcal{B}$. Then $J' \in \mathrm{Mat}_n(\mathbb{F})$ is the matrix of the same form with respect to a basis $\mathcal{B}'$ if and only if J and J' are cogradient, namely if there exists P non-singular such that:*

$$J' = P^T J P^\sigma. \tag{2.6}$$

Proof Let J' be the matrix of the form with respect to $\mathcal{B}' = \{v_1', \ldots, v_n'\}$. Then:

$$v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = v_{\mathcal{B}'}^T J' w_{\mathcal{B}'}^\sigma, \quad \forall\ v, w \in V. \tag{2.7}$$

Setting $P := \left(\ (v_1')_{\mathcal{B}}\ \middle|\ \ldots\ \middle|\ (v_n')_{\mathcal{B}}\ \right)$, we have $v_{\mathcal{B}} = P v_{\mathcal{B}'}$ for all $v \in V$. It follows:

$$v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = \left(v_{\mathcal{B}'}^T P^T\right) J \left(P^\sigma w_{\mathcal{B}'}^\sigma\right) = v_{\mathcal{B}'}^T \left(P^T J P^\sigma\right) w_{\mathcal{B}'}^\sigma, \quad \forall\ v, w \in V. \tag{2.8}$$

Comparing (2.7) with (2.8) we get $J' = P^T J P^\sigma$.
Vice versa, let $J' = P^T J P^\sigma$, for some non-singular P. Set $\mathcal{B}' = \{v_1', \ldots, v_n'\}$ where $(v_i')_{\mathcal{B}} = Pe_i$. Then $\mathcal{B}'$ is a basis of V and $v_{\mathcal{B}} = P v_{\mathcal{B}'}$ for all $v \in V$. From (2.8) it follows that J' is the matrix of the form with respect to $\mathcal{B}'$. ∎

(2.9) Theorem

(1) *Let J be the matrix of a sesquilinear form on $V = \mathbb{F}^n$ with respect to the canonical basis $\mathcal{B}$. Then its group of isometries is the subgroup:*

$$H := \left\{ h \in \mathrm{GL}_n(\mathbb{F}) \mid h^T J h^\sigma = J \right\}.$$

(2) *Let $\mathcal{B}'$ be another basis of $\mathbb{F}^n$. Then the group of isometries of the same form is:*

$$P^{-1} H P$$

where P is the matrix of the change of basis from $\mathcal{B}$ to $\mathcal{B}'$.

Proof
(1) If $\mathcal{B} = \{e_1, \ldots, e_n\}$ is the canonical basis, we have $v = v_{\mathcal{B}}$ for all $v \in V$. Thus:

$$(v, w) = v^T J w^\sigma, \quad \forall\ v, w \in V.$$

It follows that an element $h \in \mathrm{GL}_n(\mathbb{K})$ is an isometry if and only if:

$$v^T J w^\sigma = (hv)^T J (hw)^\sigma = v^T (h^T J h^\sigma) w^\sigma, \quad \forall\ v, w \in \mathbb{F}^n.$$

Equivalently h is an isometry if and only if

$$e_i^T J e_j = e_i^T (h^T J h^\sigma) e_j, \quad 1 \leq i, j \leq n \quad \Longleftrightarrow \quad J \ = \ h^T J h^\sigma.$$

(2) $J' = P^T J P^\sigma$ is the matrix of the form with respect to $\mathcal{B}'$. For every $h \in H$ we have:

$$(P^{-1} h P)^T J' \left(P^{-1} h P\right)^\sigma = J' \quad \Longleftrightarrow \quad h^T J h^\sigma = J.$$

■

3 Orthogonality

Let $(\ ,\ ) : V \times V \to \mathbb{F}$ be a bilinear (symmetric or antisymmetric) or an hermitian form.

(3.1) Definition *Two vectors $u, w \in V$ are said to be* orthogonal *if $(u, w) = 0_{\mathbb{F}}$.*

(3.2) Lemma *For every $W \subseteq V$ the subset*

$$W^\perp := \{ v \in V \mid (v, w) = 0,\ \forall\ w \in W \}$$

is a subspace, called the subspace orthogonal *to W.*

(3.3) Definition *Let W be a subspace of V. Then W is said to be*

(1) totally isotropic *(or* totally singular*) if* $W \le W^\perp$*;*

(2) non-degenerate *if* $\mathrm{rad}(W) := W \cap W^\perp = \{0_V\}$*.*

Clearly V non singular $\iff$ $\mathrm{rad}(V) = \{0_V\}$.

(3.4) Lemma *If V is non-degenerate then, for every subspace W of V:*

$$\dim W^\perp = \dim V - \dim W.$$

In particular:

(1) $\left(W^\perp\right)^\perp = W$*;*

(2) *the dimension of a totally isotropic space is at most* $\frac{\dim V}{2}$*.*

Proof Let $\mathcal{B}_W = \{w_1, \ \dots, \ w_m\}$ be a basis of W. For every $v \in V$ we have:

$$v \in W^\perp \iff (w_i, v) = 0_{\mathbb{F}}, \ 1 \le i \le m. \tag{3.5}$$

Extend $\mathcal{B}_W$ to a basis $\mathcal{B} = \{w_1, \ \dots, \ w_m, \ w_{m+1}, \dots, \ w_n\}$ of V and let J be the matrix of the form with respect to $\mathcal{B}$. From $(w_i)_{\mathcal{B}} = e_i$, $1 \le i \le m$, it follows:

$$v \in W^\perp \iff {e_i}^T J v^\sigma_{\mathcal{B}} = 0_{\mathbb{F}}, \ 1 \le i \le m. \tag{3.6}$$

Since J is non-degenerate, its rows are independent. Hence the m equations of the linear homogeneous system (3.6) are independent. This system has n indeterminates, so the space of solutions has dimension $n - m$. We conclude that $W^\perp$ has dimension

$$n - m = \dim V - \dim W.$$

(1) $W \le \left(W^\perp\right)^\perp$ and $\dim \left(W^\perp\right)^\perp = \dim \ V - \dim W^\perp = \dim W$.
(2) Let W be totally isotropic, i.e., $W \le W^\perp$. Then:

$$\dim W \le \dim W^\perp = \dim V - \dim W \quad \implies \quad 2 \dim W \le \dim V.$$

■

(3.7) Definition *Let U, W be subspaces of V. We write $V = U \perp W$ and say that V is an* orthogonal sum *of U and W if $V = U \oplus W$ and U is orthogonal to W, namely if:*

(1) $V = U + W$;

(2) $U \cap W = \{0_V\}$;

(3) $U \leq W^{\perp}$.

(3.8) Corollary *If V and W are non-degenerate, then*

$$V = W \perp W^{\perp}.$$

Moreover $W^{\perp}$ is non-degenerate.

Proof Since V is non-degenerate, Lemma 3.4 gives $\dim V = \dim\ W + \dim\ W^{\perp}$. Since W is non-degenerate, we have $W \cap W^{\perp} = \{0\}$. It follows $V = W \oplus W^{\perp}$. Finally $W^{\perp}$ is non-degenerate as $W^{\perp} \cap \left(W^{\perp}\right)^{\perp} = W^{\perp} \cap W = \{0\}$. ■

As a consequence of Witt's Lemma, we have the following:

(3.9) Corollary *Let V be endowed with a non-degenerate, either bilinear (symmetric or antisymmetric) or hermitian form. Then all the maximal totally isotropic subspaces have the same dimension, which is at most $\frac{\dim V}{2}$.*

Proof Let M be a totally isotropic subspace of largest possible dimension m. Clearly M is a maximal totally isotropic subspace. Take any totally isotropic subspace U. Since $\dim U \leq m$, there exists an injective $\mathbb{F}$-linear map $\tau : U \to M$. Now $\tau : U \to \tau(U)$ is an isometry, as the restriction of the form to U and to $\tau(U)$ is the zero-form. By theorem 1.6, there exists an isometry $\hat{\tau} : V \to V$ which extends τ. Thus $U \leq \hat{\tau}^{-1}(M)$ with $\hat{\tau}^{-1}(M)$ totally isotropic as $\hat{\tau}^{-1}$ is an isometry of V. If U is a maximal totally isotropic subspace, then $U = \hat{\tau}^{-1}(M)$ has dimension m. By Lemma 3.4 we have $m \leq \frac{\dim V}{2}$. ■

4 Symplectic spaces

(4.1) Definition *A vector space V over $\mathbb{F}$, endowed with a non-degenerate antisymmetric bilinear form is called* symplectic.

(4.2) Theorem *Let V be a symplectic space over $\mathbb{F}$, of dimension n. Then:*

(1) $n = 2m$ *is even;*

(2) *there exists a basis $\mathcal{B}$ of V with respect to which the matrix of the form is:*

$$J = \begin{pmatrix} \boldsymbol{0} & I_m \\ -I_m & \boldsymbol{0} \end{pmatrix}. \tag{4.3}$$

Proof Induction on n.

Suppose $n = 1$, $V = \mathbb{F}v$, $0 \neq v \in V$. For every $\lambda, \mu \in \mathbb{F}$: $(\lambda v, \mu v) = \lambda\mu(v, v) = 0_{\mathbb{F}}$, in contrast with the assumption that V is non degenerate. Hence $n \geq 2$.

Fix a non-zero vector $v_1 \in V$. There exists $w \in V$ such that $(v_1, w) \neq 0_{\mathbb{F}}$. In particular v_1 e w are linearly independent. Setting $w_1 := \lambda^{-1}w$, we have:

$$(v_1, w_1) = \left(v_1, \lambda^{-1}w\right) = \lambda^{-1}(v_1, w) = 1_{\mathbb{F}}.$$

If $n = 2$ our claim is proved since the matrix of the form w. r. to $\mathcal{B} = \{v_1,\ w_1\}$ is

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

If $n > 2$ we note that the subspace $W := \langle v_1, w_1 \rangle$ is non-singular. Thus:

$$V = W \ \perp \ W^{\perp}.$$

$W^{\perp}$ is non-degenerate, hence it is a symplectic space of dimension $n - 2$. By induction on n we have that $n - 2 = 2(m - 1)$ whence $n = 2m$, and moreover that $W^{\perp}$ admits a basis $\{v_2,\ \dots,\ v_m,\ w_2,\ \dots,\ w_m\}$ with respect to which the matrix of the form is

$$J_{W^{\perp}} = \begin{pmatrix} \mathbf{0} & I_{m-1} \\ -I_{m-1} & \mathbf{0} \end{pmatrix}.$$

Choosing $\mathcal{B} = \{v_1,\ v_2,\ \dots,\ v_m,\ w_1,\ w_2,\ \dots,\ w_m\}$ we obtain our claim. ■

(4.4) Definition *The group of isometries of a symplectic space V over $\mathbb{F}$ of dimension $2m$ is called the* symplectic group *of dimension $2m$ over $\mathbb{F}$ and indicated by* $\mathrm{Sp}_{2m}(\mathbb{F})$.

By the previous considerations, up to conjugation we may assume:

$$\mathrm{Sp}_{2m}(\mathbb{F}) = \left\{g \in \mathrm{GL}_{2m}(\mathbb{F}) \mid g^T J g = J\right\}.$$

where J is as in (4.3). The subspace $\langle e_1, \dots, e_m \rangle$, is a maximal totally isotropic space.

5 Some properties of finite fields

In contrast with the symplectic case, the classification of the non-singular, bilinear symmetric or hermitian forms, depends on the field $\mathbb{F}$ and may become very complicated. Thus our treatment will need further assumptions on $\mathbb{F}$. Since our interest is focused on finite fields, we will recall here a few specific facts, needed later, assuming the basic properties. As usual $\mathbb{F}_q$ denotes the finite field of order q, a prime power.

Consider the homomorphism $f : \mathbb{F}_q^* \to \mathbb{F}_q^*$ defined by $f(\alpha) := \alpha^2$. Clearly $\mathrm{Ker} f = \langle -1 \rangle$. If q is odd, $\mathrm{Ker} f$ has order 2. In this case $\mathrm{Im} f$, the set of non-zero squares in $\mathbb{F}_q$, has order $\frac{q-1}{2}$. Moreover, for any $\epsilon \in \mathbb{F}_q^* \setminus \mathrm{Im} f$, the coset $(\mathrm{Im} f)\,\epsilon = \left\{\alpha^2\epsilon \mid \alpha \in \mathbb{F}_q^*\right\}$ is the set of *non-squares.*
If q is even, $\mathrm{Ker} f$ has order 1. So f is surjective, i.e., every element of $\mathbb{F}_q$ is a square.

(5.1) Lemma *Every element of* $\mathbb{F}_q$ *is the sum of two squares.*

Proof By what observed above we may suppose q odd. Consider the set

$$X := \left\{\alpha^2 + \beta^2 \mid \alpha, \beta \in \mathbb{F}_q\right\}.$$

Note that $|X|$ does not divide $q = |\mathbb{F}_q|$, since:

$$|X| \geq \frac{q-1}{2} + 1 = \frac{q+1}{2} > \frac{q}{2}.$$

If every element of X were a square, X would be an additive subgroup of $\mathbb{F}_q$, in contrast with Lagrange's Theorem. So there exists a non-square $\epsilon \in X$. Write $\epsilon = \gamma^2 + \delta^2$. It follows that every non-square is in X. Indeed a non-square has shape $\alpha^2\epsilon = (\alpha\gamma)^2 + (\alpha\delta)^2$. ■

$\mathrm{Aut}\left(\mathbb{F}_{p^a}\right) = \mathrm{Gal}_{\mathbb{F}_p}\left(\mathbb{F}_{p^a}\right)$ has order a. So $\mathrm{Aut}\left(\mathbb{F}_{p^a}\right)$ is generated by the Frobenius automorphism $\alpha \mapsto \alpha^p$, which has has order a. It follows that $\mathbb{F}_{p^a}$ has an automorphism σ of order 2 if and only if $a = 2b$ is even. In this case, we set $q = p^b$, so that $\mathbb{F}_{p^a} = \mathbb{F}_{q^2}$. The automorphism $\sigma : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ of order 2 is the map: $\alpha \mapsto \alpha^q$. Moreover $\alpha\alpha^q \in \mathbb{F}_q$ for all $\alpha \in \mathbb{F}_{q^2}$, since $(\alpha\alpha^q)^q = \alpha\alpha^q$.

(5.2) Theorem *The* Norm *map* $N : \mathbb{F}_{q^2} \to \mathbb{F}_q$ *defined by* $N(\alpha) := \alpha\alpha^q$*, is surjective.*

Proof The restriction of N to $\mathbb{F}_{q^2}^*$ is a group homomorphism into $\mathbb{F}_q^*$. Its kernel consists of the roots of $x^{q+1} - 1$, hence has order $\leq q + 1$. Thus its image has order $q - 1$. ■

6 Unitary and orthogonal spaces

We recall that σ denotes an automorphism of the field $\mathbb{F}$ such that $\sigma^2 = \mathrm{id}$. More precisely, $\sigma = \mathrm{id}$ in the orthogonal case, $\sigma \neq \mathrm{id}$ in the hermitian case.

(6.1) Lemma *Consider a non-degenerate, bilinear symmetric or hermitian form* $(\ ,\ ) : V \times V \to \mathbb{F}$. *If* $\mathrm{char}\,\mathbb{F} = 2$ *assume that the form is hermitian. Then* V *admits an orthogonal basis, i.e., a basis with respect to which the matrix of the form is diagonal.*

Proof We first show that there exists v such that $(v, v) \neq 0$. This is clear when $\dim V = 1$, since the form is non-degenerate. So suppose $\dim V > 1$.
For a fixed non-zero $u \in V$, there exists $w \in V$ such that $(u, w) \neq 0_{\mathbb{F}}$. Clearly we may assume $(u, u) = (w, w) = 0$. If $\mathrm{char}\,\mathbb{F} \neq 2$, setting $\lambda = (u, w)$, $\quad v = \lambda^{-1}u + w$ we have:

$$(v, v) = \lambda^{-1}(u, w) + \left(\lambda^{-1}\right)^{\sigma}(w, u) = \lambda^{-1}\lambda + (\lambda^{\sigma})^{-1}\lambda^{\sigma} = 2 \cdot 1_{\mathbb{F}} \neq 0_{\mathbb{F}}.$$

If $\mathrm{char}\,\mathbb{F} = 2$, the form is hermitian by assumption. So there exists $\alpha \in \mathbb{F}$ such that $\alpha^{\sigma} \neq \alpha$. In this case, setting $v = \lambda^{-1}\alpha u + w$ we have $(v, v) = \alpha + \alpha^{\sigma} = \alpha - \alpha^{\sigma} \neq 0_{\mathbb{F}}$.
Induction on $\dim V$, applied to $\langle v \rangle^{\perp}$, gives the existence of an orthogonal basis of V. ■

(6.2) Remark *The hypothesis char* $\mathbb{F} \neq 2$ *when the form is bilinear symmetric, is necessary. Indeed the matrix* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *defines a non-degenerate symmetric form on* $V = \mathbb{F}_2^2$. *Since* $(v, v) = 0$ *for all* v, *no orthogonal basis can exist.*

Even the existence of an orthogonal basis is far from a complete classification as shown, for example, by a Theorem of Sylvester ([14, Theorem 6.7 page 359]).

(6.3) Example *By the previous theorem, the symmetric matrices*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

are pairwise not cogradient in $\mathrm{Mat}_3(\mathbb{R})$.

6.1 Unitary spaces

(6.4) Definition *A space* V, *with a non-degenerate hermitian form, is called* unitary.

(6.5) Theorem *Let* V *be a unitary space. Suppose that, for all* $v \in V$, *there exists* $\mu \in \mathbb{F}$ *such that* $N(\mu) := \mu\mu^{\sigma} = (v, v)$. *Then there exists an orthonormal basis of* V, *i.e., a basis with respect to which the matrix of the hermitian form is the identity.*

In particular such basis exists for $\mathbb{F} = \mathbb{C}$, σ the complex conjugation, and for $\mathbb{F} = \mathbb{F}_{q^2}$.

Proof By Lemma 6.1 there exists $v \in V$ with $(v, v) \neq 0$. Under our assumptions there exists $\mu \in \mathbb{F}$ such that $\mu\mu^\sigma = (v, v)$. Substituting v with $\mu^{-1}v$ we get $(v, v) = 1$. For $n = 1$ the claim is proved. So suppose $n > 1$. The subspace $\langle v \rangle$ is non-degenerate. It follows that $V = \langle v \rangle \perp \langle v \rangle^\perp$. As $\langle v \rangle^\perp$ is non-degenerate of dimension $n-1$, our claim follows by induction. ∎

(6.6) Definition *The group of isometries of a unitary space V over $\mathbb{F}$ of dimension n, called the* unitary group *of dimension n over $\mathbb{F}$, is indicated by $\mathrm{GU}_n(\mathbb{F})$.*

By Theorem 6.5, if $\mathbb{F} = \mathbb{C}$ and σ is the complex conjugation or $\mathbb{F} = \mathbb{F}_{q^2}$, we may assume:

$$\mathrm{GU}_n(\mathbb{F}) = \left\{ g \in \mathrm{GL}_n(\mathbb{F}) \mid g^T g^\sigma = I_n \right\}.$$

(6.7) Remark *There are fields which do not admit any automorphism of order 2: so there are no unitary groups over such fields. To the already mentioned examples of $\mathbb{R}$ and $\mathbb{F}_{p^{2b+1}}$, we add the algebraic closure $\overline{F}_p$ of $\mathbb{F}_p$, as shown below.*

By contradiction suppose there exists an automorphism σ of order 2 of $\mathbb{F} := \overline{F}_p$.
Let $\alpha \in \mathbb{F}$ be such that $\sigma(\alpha) \neq \alpha$. Since α is algebraic over $\mathbb{F}_p$, we have that $\mathbb{K} = \mathbb{F}_p(\alpha)$ is finite of order p^n for some n. Thus $\mathbb{K}$ is the splitting field of $x^{p^n} - x$. It follows that $\mathbb{K}$ is fixed by σ and $\sigma_{|\mathbb{K}}$ has order 2. Thus $n = 2m$, $|\mathbb{K}| = q^2$ with $q = p^m$ and $\sigma(\alpha) = \alpha^q$. Now consider the subfield $\mathbb{L}$ of $\mathbb{F}$ of order q^4. Again $\mathbb{L}$ is fixed by σ and $\sigma(\beta) = \beta^{q^2}$ for all β in $\mathbb{L}$. From $\mathbb{K} \leq \mathbb{L}$ we get the contradiction $\alpha \neq \sigma(\alpha) = \alpha^{q^2} = \alpha$.

6.2 Quadratic Forms

(6.8) Definition *A* quadratic form *on V is a map $Q : V \to \mathbb{F}$ such that:*

(1) *$Q(\lambda v) = \lambda^2 Q(v)$ for all $\lambda \in \mathbb{F}$, $v \in V$;*

(2) *the* polar *form $(v, w) := Q(v + w) - Q(v) - Q(w)$, $\forall\ v, w \in V$, is bilinear.*

Q is non-degenerate *if its polar form is non-degenerate.*

Note that:

$$Q(0_V) = Q(0_{\mathbb{F}} 0_V) = (0_{\mathbb{F}})^2 Q(0_V) = 0_{\mathbb{F}}. \tag{6.9}$$

Q uniquely determines its polar form (,) which is clearly symmetric. Moreover

$$2Q(v) = (v, v), \quad \forall\ v \in V. \tag{6.10}$$

Indeed: $Q(2v) = Q(v + v) = Q(v) + Q(v) + (v, v)$ gives $4Q(v) = 2Q(v) + (v, v)$.
It follows from (6.10) that, if char $(\mathbb{F}) = 2$, the polar form (,) is antisymmetric.
On the other hand, if car $\mathbb{F} \neq 2$, every symmetric bilinear form (,) is the polar form of the quadratic form Q defined by:

$$Q(v) := \frac{1}{2}(v, v), \quad \forall\ v \in V.$$

Direct calculation shows that Q is quadratic and that

$$Q(v + w, v + w) - Q(v) - Q(w) = (v, w).$$

By the above considerations, in characteristic $\neq 2$, the study of quadratic forms is equivalent to the study of symmetric bilinear forms. But, for a unified treatment, we study the orthogonal spaces via quadratic forms.

6.3 Orthogonal spaces

(6.11) Definition *Let (V, Q) and (V', Q') be vector spaces over $\mathbb{F}$, endowed with quadratic forms Q and Q' respectively. An* isometry *from V to V' is an invertible element $f \in \mathrm{Hom}_{\mathbb{F}}(V, V')$ such that*

$$Q'(f(v)) = Q(v), \quad \forall\ v \in V.$$

The spaces (V, Q) and (V', Q') are isometric *if there exists an isometry $f : V \to V'$.*

Clearly, when $V = V'$, $Q = Q'$, the isometries of V form a subgroup of $\mathrm{Aut}_{\mathbb{F}}(V)$.

(6.12) Definition *Let Q be a non degenerate quadratic form on V.*

(1) *(V, Q) is called an* orthogonal space*;*

(2) *the group of isometries of (V, Q), called the* orthogonal group *relative to Q, is denoted by $O_n(\mathbb{F}, Q)$, where $n = \dim V$.*

Note that, in an orthogonal space, we may consider orthogonality with respect to the polar form, which is non-singular by definition of orthogonal space.

(6.13) Lemma *Suppose char* $\mathbb{F} = 2$.

(1) *any orthogonal space* (V, Q) *over* $\mathbb{F}$ *has even dimension;*

(2) *the orthogonal group* $O_{2m}(\mathbb{F}, Q)$ *is a subgroup of the symplectic group* $\mathrm{Sp}_{2m}(\mathbb{F})$.

Proof
(1) The polar form of any quadratic form is antisymmetric by (6.10), hence degenerate in odd dimension.
(2) The polar form associated to Q is non-degenerate, antisymmetric and it is preserved by every $f \in O_{2m}(\mathbb{F}, Q)$. Indeed:

$$(v, w) := Q(v + w) - Q(v) - Q(w) = Q(f(v + w)) - Q(f(v)) - Q(f(w)) =$$

$$Q(f(v) + f(w)) - Q(f(v)) - Q(f(w)) = (f(v), f(w)), \quad \forall\, v, w \in V.$$

■

(6.14) Lemma *Let* (V, Q) *be an orthogonal space of dimension* ≥ 2. *If* $Q(v_1) = 0$ *for some non-zero vector* $v_1 \in V$, *then there exists* $v_{-1} \in V \setminus \langle v_1 \rangle$ *such that:*

$$Q\left(x_1 v_1 + x_{-1} v_{-1}\right) = x_1 x_{-1}, \quad \forall\, x_1, x_{-1} \in \mathbb{F}. \tag{6.15}$$

The subspace $\langle v_1, v_{-1} \rangle$ *is non-singular.*

Proof $Q(v_1) = 0$ gives $(v_1, v_1) = 2Q(v_1) = 0$. As the polar form of Q is non-degenerate, there exists $u \in V$ with $(v_1, u) \neq 0$. In particular v_1 and u are linearly independent. Set

$$v_{-1} := (v_1, u)^{-1} u - (v_1, u)^{-2} Q(u) v_1.$$

Then $v_{-1} \notin \langle v_1 \rangle$ and:

$$(v_1, v_{-1}) = 1, \quad Q\left(v_{-1}\right) = (v_1, u)^{-2} Q(u) - (v_1, u)^{-2} Q(u) = 0.$$

Using the assumption $Q(v_1) = 0$ we get (6.15). The subspace is non-singular as the matrix of the polar form with respect to $\{v_1, v_{-1}\}$ is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ■

(6.16) Definition *An orthogonal space* (V, Q) *is called* anisotropic *if* $Q(v) \neq 0$ *for all non-zero vectors* $v \in V$.

Non-singular anisotropic spaces exist.

(6.17) Example *Let V be a separable, quadratic field extension of $\mathbb{F}$. Then*

$$|\mathrm{Gal}_{\mathbb{F}}(V)| = \dim_{\mathbb{F}} V = 2 \quad \Longrightarrow \quad \mathrm{Gal}_{\mathbb{F}}(V) = \langle \sigma \rangle, \quad \mathbb{F} = V_{\langle \sigma \rangle}.$$

The Norm *map* $N_{\mathbb{F}}^{V} : V \to \mathbb{F}$ *defined by:*

$$N_{\mathbb{F}}^{V}(v) := vv^{\sigma}, \quad \forall\, v \in V$$

is a non-degenerate anisotropic quadratic form on V.

More details are given in the next Lemma.

(6.18) Lemma *Let $f(t) = t^2 + at + b \in \mathbb{F}[t]$ be separable, irreducible and consider*

$$V = \frac{\mathbb{F}[t]}{\langle t^2 + at + b \rangle} = \{x_1 + x_{-1}t \mid x_1,\ x_{-1} \in \mathbb{F}\}$$

with respect to the usual sum of polynomials and product modulo $f(t)$. Then :

$$N_{\mathbb{F}}^{V}(x_1 + x_{-1}t) = x_1^2 - ax_1x_{-1} + bx_{-1}^2, \quad \forall\, x_1, x_{-1} \in \mathbb{F}. \tag{6.19}$$

With respect to the basis $\{1, t\}$, the polar form of $N_{\mathbb{F}}^{V}$ is the non-singular matrix

$$J = \begin{pmatrix} 2 & -a \\ -a & 2b \end{pmatrix}.$$

Proof Let $\mathrm{Gal}_{\mathbb{F}}(V) = \langle \sigma \rangle$. Then t and t^{σ} are the roots of $f(t)$ in V. Thus

$$t + t^{\sigma} = -a, \quad tt^{\sigma} = b, \quad x^{\sigma} = x,\ \forall\, x \in \mathbb{F}.$$

It follows:

$$N_{\mathbb{F}}^{V}(x_1 + x_{-1}t) = (x_1 + x_{-1}t)(x_1 + x_{-1}t^{\sigma}) = -ax_1x_{-1} + x_1^2 + bx_{-1}^2.$$

J is non-degenerate since $\mathrm{Det}\,(J) = 4b - a^2 \neq 0$ by the irreducibility of $t^2 + at + b$ (and its separability when char $\mathbb{F} = 2$). ■

(6.20) Remark *If $\mathbb{F} = \mathbb{F}_q$ then $V = \mathbb{F}_{q^2}$ and the map $N_{\mathbb{F}}^{V} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ coincides with $v \mapsto vv^q = v^{q+1}$. As shown in Section 5 it is surjective. It follows that the map $\begin{pmatrix} x_1 \\ x_{-1} \end{pmatrix} \mapsto x_1^2 - ax_1x_{-1} + bx_{-1}^2$ from $\mathbb{F}_q^2$ to $\mathbb{F}_q$ is surjective.*

The anisotropic orthogonal spaces are only those of Example 6.17. We first show:

(6.21) Theorem *Let (W, Q) be an anisotropic orthogonal space of dimension 2.*

(1) *For each non-zero vector $v_1 \in W$ there exists $v_{-1} \in W \setminus \{v_1\}$ such that*

(6.22) $$Q(x_1 v_1 + x_{-1} v_{-1}) = Q(v_1)\left(x_1^2 + \zeta x_{-1}^2 + x_1 x_{-1}\right) \quad \forall\, x_1,\ x_{-1} \in \mathbb{F}$$

where $t^2 - t + \zeta$ is irreducible in $\mathbb{F}[t]$.

(2) *If the map $\mathbb{F}^2 \to \mathbb{F}$ defined by $\begin{pmatrix} x_1 \\ x_{-1} \end{pmatrix} \mapsto x_1^2 + \zeta x_{-1}^2 + x_1 x_{-1}$ is onto, the space (W, Q) is isometric to $(V, N_{\mathbb{F}}^V)$, where $V = \frac{\mathbb{F}[t]}{\langle t^2 - t + \zeta\rangle}$.*

In particular:

- *if $\mathbb{F}$ is algebraically closed, no such W exists;*
- *if $\mathbb{F} = \mathbb{F}_q$, all orthogonal anisotropic 2-dimensional spaces are isometric.*

Proof
(1) We first show that there exists $w \in W \setminus \langle v_1 \rangle$ such that $(v_1, w) \neq 0$. Indeed, if $(v_1, v_1) \neq 0$, then $W = \langle v_1 \rangle \oplus \langle v_1 \rangle^\perp$ and we take $w = v_1 + u$ with $u \in \langle v_1 \rangle^\perp$. If $(v_1, v_1) = 0$, then $\langle v_1 \rangle \leq \langle v_1 \rangle^\perp \neq W$ and we take $w \in W \setminus \langle v_1 \rangle^\perp$.
Now set:
$$v_{-1} := Q(v_1)(v_1, w)^{-1} w, \quad \zeta = \frac{Q(v_{-1})}{Q(v_1)}.$$
It follows $(v_1, v_{-1}) = Q(v_1)$ and, for all $x_1, x_{-1} \in \mathbb{F}$:

$$Q(x_1 v_1 + x_{-1} v_{-1}) = x_1^2 Q(v_1) + x_{-1}^2 Q(v_{-1}) + x_1 x_{-1} Q(v_1) = Q(v_1)\left(x_1^2 + \zeta x_{-1}^2 + x_1 x_{-1}\right).$$

In particular, for $x_{-1} = 1$, we get $x_1 v_1 + v_{-1} \neq 0$, whence:

$$0 \neq Q(x_1 v_1 + v_{-1}) = Q(v_1)\left(x_1^2 + x_1 + \zeta\right), \quad \forall\, x_1 \in \mathbb{F}.$$

Thus $t^2 + t + \zeta$ is irreducible in $\mathbb{F}[t]$, since it has no roots in $\mathbb{F}$. It follows that $t^2 - t + \zeta$ is also irreducible.
(2) There exists $\begin{pmatrix} \lambda \\ \mu \end{pmatrix} \in \mathbb{F}^2$ such that $\lambda^2 + \zeta\mu^2 + \lambda\mu = Q(v_1)^{-1}$. Substituting v_1 with $\lambda v_1 + \mu v_{-1}$ in point (1), we may suppose $Q(v_1) = 1$. Then (6.22) gives $Q(x_1 v_1 + x_{-1} v_{-1}) = x_1^2 + \zeta x_{-1}^2 + x_1 x_{-1}$. We conclude that the map $f = W \to \frac{\mathbb{F}[t]}{\langle t^2 - t + \zeta\rangle}$ defined by:

(6.23) $$x_1 v_1 + x_{-1} v_{-1} \mapsto x_1 + x_{-1} t$$

is an isometry in virtue of (6.19).

Finally, suppose $\mathbb{F} = \mathbb{F}_q$ and let $\left(V, N_{\mathbb{F}_q}^{V}\right)$ $\left(V', N_{\mathbb{F}_q}^{V'}\right)$ be 2-dimensional anisotropic orthogonal spaces. Since V and V' are finite fields of the same order, there exists a field automorphism $f : V \to V'$ such that $f_{|\mathbb{F}_q} = \mathrm{id}$. From

$$f(v)f(v^q) = f(vv^q) = vv^q, \quad \forall\, v \in V$$

we conclude that f is an isometry. ■

(6.24) Corollary *Let (V, Q) be an orthogonal space, with $V = \mathbb{F}_q^{2m}$.*

(1) *There exists a basis $\mathcal{B} = \{v_1 \ldots, v_m, v_{-1} \ldots, v_{-m},\}$ of V such that either $Q = Q^+$ or $Q = Q^-$ where, for all $v = \sum_{i=1}^{m} x_i v_i + x_{-i} v_{-i} \in V$:*

- *$Q^+(v) = \sum_{i=1}^{m} x_i x_{-i}$;*
- *$Q^-(v) = \sum_{i=1}^{m} x_i x_{-i} + x_m^2 + \zeta x_{-m}^2$, with $t^2 - t + \zeta$ a fixed, separable irreducible polynomial in $\mathbb{F}_q[t]$ (arbitrarily chosen with these properties).*

(2) *Q^+ has polar form $\sum_{i=1}^{m} (x_i y_{-i} + x_{-i} y_i)$, with matrix $J_1 = \begin{pmatrix} \mathbf{0} & I_m \\ I_m & \mathbf{0} \end{pmatrix}$;*

Q^- has polar form $\sum_{i=1}^{m} (x_i y_{-i} + x_{-i} y_i) + 2\,(x_m y_m + \zeta x_{-m} y_{-m})$, with matrix

$$J_2 = \begin{pmatrix} \mathbf{0} & I_{m-1} & 0 & 0 \\ I_{m-1} & \mathbf{0} & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2\zeta \end{pmatrix}.$$

(3) *(V, Q^+) is not isometric to (V, Q^-).*

The corresponding groups of isometries are indicated by $O_{2m}^+(q)$ and $O_{2m}^-(q)$.

Proof

(1) Let $m = 1$. If V is non-anisotropic, Lemma 6.14 gives $Q = Q^+$. If V is anisotropic, Theorem 6.21 gives $Q = Q^-$. So assume $m > 1$.

Step 1. We claim that there exists a non-zero vector $v_1 \in V$ such that $Q(v_1) = 0$.
By the same argument used in the proof of point (1) of Theorem 6.21, there exists a non-singular 2-dimensional subspace $W = \langle v_m, v_{-m} \rangle$. We may assume that W is anisotropic. Hence (W, Q) is isometric to $\left(\mathbb{F}_{q^2}, N_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}\right)$ and

$$Q\,(x_m v_m + x_{-m} v_{-m}) = x_m x_{-m} + x_m^2 + \zeta x_{-m}^2, \quad \forall\, x_m, x_{-m} \in \mathbb{F}_q$$

for some irreducible polynomial $t^2 - t + \zeta \in \mathbb{F}[t]$.

Take a non-zero vector w in $W^\perp$. By the surjectivity of the norm for finite fields, there exist $u \in W$ such that $Q(u) = -Q(w)$. Then $v_1 = u + w \neq 0$, since $W \cap W^\perp = \{0\}$. Moreover, from $(u, w) = 0$, we get: $Q(v_1) = Q(u + w) = Q(u) + Q(w) = 0$.

Step 2. By Lemma 6.14 there exists a non-singular 2-dimensional subspace $\langle v_1, v_{-1}\rangle$ such that $Q(x_1 v_1 + x_{-1} v_{-1}) = x_1 x_{-1}$. We get:

$$V = \langle v_1, v_{-1}\rangle \oplus \langle v_1, v_{-1}\rangle^\perp .$$

By induction, $\langle v_1, v_{-1}\rangle^\perp$ has a basis $\mathcal{B}' = \{v_2 \ldots, v_m, v_{-2} \ldots, v_{-m},\}$ such that the restriction of Q to $\langle v_1, v_{-1}\rangle^\perp$ is either Q^+ or Q^-. This gives (1).

(2) Routine calculation using (1).

(3) V is a direct sum of mutually orthogonal 2-dimensional spaces:

$$V = \langle v_1, v_{-1}\rangle \perp \cdots \perp \langle v_m, v_{-m}\rangle$$

with the further property $(v_i, v_i) = 0$, $1 \leq i \leq m-1$. For Q^+ we have also $(v_m, v_m) = 0$, so that $\langle v_1, \ldots, v_m\rangle$ is a totally isotropic space of largest possible dimension $m = \frac{n}{2}$ (see Lemma 3.9). For Q^- the space $W = \langle v_1, \ldots, v_{m-1}\rangle$ is totally isotropic. It follows:

$$W \oplus \langle v_m, v_{-m}\rangle = W^\perp.$$

Let $\widehat{W}$ be a totally isotropic space which contains W. Then

$$W = W + \left(\widehat{W} \cap \langle v_m, v_{-m}\rangle\right) = W + \{0\} = W$$

since $\langle v_m, v_{-m}\rangle$ is anisotropic. We conclude that $W = \widehat{W}$, i.e., W is a maximal isotropic space of dimension $m-1$. So Q^+ and Q^- cannot be isometric. ∎

(6.25) Theorem *Let (V, Q) be an orthogonal space, with $V = \mathbb{F}_q^{2m+1}$, q odd. There exists a basis of V such that the matrix of the polar form is one of the following:*

(6.26) $$I_{2m+1} = \begin{pmatrix} 1 & & \\ & \cdots & \\ & & 1 \end{pmatrix}, \quad J = \begin{pmatrix} I_{2m} & \\ & \epsilon \end{pmatrix},$$

where ϵ is a fixed non-square in $\mathbb{F}_q^*$ (arbitrarily chosen with this property). The two polar forms I_{2m+1} and J give rise to non-isometric orthogonal spaces, but their groups of isometries are conjugate, hence isomorphic. Both groups are indicated by $O_{2m+1}(q)$.

Proof We first show that, if an orthogonal space V over $\mathbb{F}_q$, has dimension > 1, then there exists $v_1 \in V$ with $(v_1, v_1) = 1$. By Lemma 6.1, there exists v_1 such that $(v_1, v_1) \neq 0$. Thus $(v_1, v_1) = \rho^2$ or $(v_1, v_1) = \rho^2\epsilon$ for some $\rho \in \mathbb{F}_q^*$. Substituting v_1 with $\rho^{-1}v_1$, if necessary, we have $(v_1, v_1) \in \{1, \epsilon\}$. If $(v_1, v_1) = \epsilon$, set $\lambda^2 + \mu^2 = \epsilon^{-1}$. Again by Lemma 6.1, applied to $\langle v_1\rangle^\perp$, there exists $v_2 \in \langle v_1\rangle^\perp$ such that $(v_2, v_2) \neq 0$. If $(v_2, v_2) = 1$, we substitute v_1 by v_2. If $(v_2, v_2) = \epsilon$, we substitute v_1 by $\lambda v_1 + \mu v_2$.
Now we prove our claim. If $m = 1$ we can take $\mathcal{B} = \{v_1\}$ with $(v_1, v_1) \in \{1, \epsilon\}$. If $m > 1$ we take v_1 with $(v_1, v_1) = 1$. Then $V = \langle v_1\rangle \perp \langle v_1\rangle^\perp$ and our claim follows by induction on $\dim V$ applied to $\langle v_1, v_2\rangle^\perp$.
I_{2m+1} and J define non isometric spaces because the dimension of a maximal isotropic space are, respectively, m and $m-1$. So J is not cogradient to I_{2m+1}. Also ϵI_{2m+1} is not cogredient to I_{2m+1}, otherwise we would have $\epsilon I_{2m+1} = P^T I_{2m+1} P$, a contradiction as $\epsilon^{2m+1} = \det(\epsilon I_{2m+1})$ is not a square. Since, over $\mathbb{F}_q$, there are only 2 non-isometric orthogonal spaces, J is cogredient to ϵI_{2m+1}. Now I_{2m+1} and ϵI_{2m+1} have the same group of isometries, since:

$$h^T(\epsilon I_{2m+1})h = \epsilon I_{2m+1} \iff h^T I_{2m+1} h = I_{2m+1}.$$

We conclude that the groups of isometries of I_{2m+1} and J are conjugate. ∎

7 Exercises

(7.1) Exercise *Show that* $\mathrm{SL}_2(\mathbb{F}) = \mathrm{Sp}_2(\mathbb{F})$ *over any field* $\mathbb{F}$.

(7.2) Exercise *Let* $(V, Q, \mathbb{F})$ *be an orthogonal space. Suppose* $V = V_1 \perp V_2$.
Show that, for each $v = v_1 + v_2$ *with* $v_1 \in V_1$, $v_2 \in V_2$*:*

$$Q(v) = Q(v_1) + Q(v_2).$$

(7.3) Exercise *Let* V *be a quadratic extension of* $\mathbb{F}$ *and* $\langle\sigma\rangle = \mathrm{Gal}_{\mathbb{F}}(V)$.
Show that the map $N_{\mathbb{F}} : V \to \mathbb{F}$, *defined by* $N_{\mathbb{F}}^V(v) := vv^\sigma$ *is a quadratic form on* V.

(7.4) Exercise *In Lemma* 6.18 *show that the quadratic form*

$$N_{\mathbb{F}}^V(x_1 + x_{-1}t) = x_1^2 - ax_1x_{-1} + b$$

has matrix $J = \begin{pmatrix} 2 & -a \\ -a & 2b \end{pmatrix}$ *with respect to the basis* $\{1, t\}$.

(7.5) Exercise *Say whether the matrices*

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad J' = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

are cogredient. In case they are, indicate a non-singular matrix P *such that* $P^T J P = J'$.

(7.6) Exercise *Let* V *be an anisotropic* 2*-dimensional orthogonal space over* $\mathbb{F}_q$, q *odd. Show that there exists a basis for which the polar form has matrix:* $\begin{pmatrix} 1 & 0 \\ 0 & -\epsilon \end{pmatrix}$, *where* ϵ *is a non square in* $\mathbb{F}_q$.

(7.7) Exercise *Let* q *be odd. Show that* -1 *is a square in* $\mathbb{F}_q$ *if and only if*

$$q \equiv 1 \pmod 4.$$

(7.8) Exercise *Let* q *be odd and* $\epsilon \in \mathbb{F}_q$ *be a non-square. Show that the matrices*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}$$

are not cogredient (equivalently define non-isometric orthogonal spaces).

(7.9) Exercise *Let* q *be odd and* $\epsilon \in \mathbb{F}_q$ *be a non-square. Show that the matrix* $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *is respectively cogredient to*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ if } q \equiv 1 \pmod 4, \quad \begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix} \text{ if } q \equiv 3 \pmod 4.$$

(7.10) Exercise *Let* W *be a totally isotropic subspace of an orthogonal space* V. *Suppose*

$$V = W \oplus U$$

with U *anisotropic. Show that* W *is a maximal isotropic subspace of* V.

(7.11) Exercise *Let* q *be odd,* $V = \mathbb{F}_q^n$ *be a quadratic space, with* $n = 2m$. *Using the classification of quadratic spaces given in this Chapter, show that there exists a basis of* V *with respect to which the polar form has matrix* J_1 *or* J_2 *where*

$$J_1 = \begin{pmatrix} \mathbf{0} & I_m \\ I_m & \mathbf{0} \end{pmatrix}, \quad J_2 = \begin{pmatrix} \mathbf{0} & I_{m-1} & & \\ I_{m-1} & \mathbf{0} & & \\ & & 1 & \\ & & & -\epsilon \end{pmatrix}.$$