EXERCISE SHEET 4

(E83) Let $a, b \in k^*$. For all $c \in k$, there exist $x, y \in k$ with $ax^2 + by^2 = c$.

Answer. Remark. This question is asked in lectures at a point where k is assumed to be finite, so we prove the result in this case. (It should be clear that the result is not clear in general: take $(k, a, b, c) = (\mathbb{R}, 1, 1, -1)$.)

The result is trivial if $\mathrm{char}(k) = 2$, since all elements of k are squares. Assume, then, that $\mathrm{char}(k) \neq 2$. Define two sets:

$$Y = \{c - by^2 \mid y \in k\}$$
$$X = \{ax^2 \mid x \in k\}$$

Both of these sets have size $\frac{q+1}{2}$ hence they must overlap. The result follows.

(E84) Prove Lemma 38 of lectures for $\dim(V) = 2 = \mathrm{char}(k)$.

Answer. Let V be an anisotropic space of dimension 2 over $k = \mathbb{F}_q$ where q is a power of 2. Let $\{v, w\}$ be a basis for V with $w \notin v^\perp$, and observe that

$$Q(xv + yw) = ax^2 + bxy + cy^2$$

for some $a, b, c \in k^*$. Replacing x and y by scalar multiples we can ensure that

$$Q(xv + yw) = x^2 + xy + cy^2$$

and the polynomial $x^2 + x + c \in k[x]$ is irreducible since V is anisotropic. Write $\mathbb{F}_{q^2}$ for the splitting field of this polynomial, i.e. $\mathbb{F}_{q^2} = k(\alpha)$ where $\alpha^2 + \alpha + c = 0$ and the two roots of the polynomial in $\mathbb{F}_{q^2}$ are α and $-1 - \alpha$. Thus $\alpha^\sigma = -1 - \alpha$.

Now identify V with $\mathbb{F}_{q^2}$ via the bijection

$$xv + yw \mapsto x - y\alpha,$$

where $x, y \in \mathbb{F}_q$. Now observe that Q is equal to the norm map:

$$\begin{aligned} N : k(\alpha) \to Fq, xv + yw \mapsto N(x - y\alpha) &= (x - y\alpha)(x - y\alpha)^\sigma \\ &= x^2 + xy + y^2 c. \end{aligned}$$

The result follows.

(E86) Prove Theorem 39 of lectures.

Answer. POL1 and POL2 simply follow from the fact that a subspace of a t.i/ t.s subspace is also a t.i/ t.s subspace.

For POL3, set $p = \langle y \rangle$, a point of the polar space not in the maximal flat U. Consider the linear map

$$U \to k, x \mapsto \beta(x, y)$$

which has kernel K, a hyperplane of U. Then a line of $\langle U, y\rangle$ containing p is a flat if and only if $q \in K$, thus the set of all such lines is the t.i. space $W = \langle K, y\rangle$ which has the same dimension as U and so is maximal. Clearly $W \cap U = K$, a hyperplane of both U and W.

To complete the proof of POL3 I should also deal with the situation when the formed space is orthogonal and $k = \mathbb{F}_q$ with q even. I leave this as (another) exercise.

For POL4, w construct a maximal flat by considering a basis $\{v_1, w_2, \ldots, v_r, w_r, x_1, \ldots, x_s\}$ where (v_i, w_i) are mutually orthgonal hyperbolic pairs and $\langle x_1, \ldots, x_s\rangle$ is an anisotropic subspace. Then $\langle v_1, \ldots, v_r\rangle$ and $\langle w_1, \ldots, w_r\rangle$ are disjoint maximal flats and we are done.

(E88) Let β_1 and β_2 be non-degenerate alternating bilinear forms defined on a $2r$-dimensional vector space V over a field k. Then $\mathrm{Isom}(\beta_1)$ and $\mathrm{Isom}(\beta_2)$ (resp. $\mathrm{Sim}(\beta_1)$ and $\mathrm{Sim}(\beta_2)$) are conjugate subgroups of $\mathrm{GL}_{2r}(k)$. What is more $\mathrm{SemiSim}(\beta_1)$ and $\mathrm{SemiSim}(\beta_2)$ are conjugate subgroups of $\Gamma\mathrm{L}_{2r}(k)$.

Answer. We can choose a basis $\mathcal{B}$ for β_1 so that $\beta_1(x, y) = x^T Ay$ where

e: matrix

$$A = \begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix} \tag{1}$$

Then

$$\mathrm{Isom}(\beta_1) = \{X \in \mathrm{GL}_{2r}(k) \mid X^T AX = A\}.$$

Since there is also a basis so that $\beta_2(x, y) = x^T Ay$, we conclude that there exists $C \in \mathrm{GL}_{2r}(k)$ such that, with respect to the basis $\mathcal{B}$,

$$\begin{aligned} \mathrm{Isom}(\beta_2) &= \{X \in \mathrm{GL}_{2r}(k) \mid (C^{-1}XC)^T A(C^{-1}XC) = A\} \\ &= \{CYC^{-1} \in \mathrm{GL}_{2r}(k) \mid Y^T AY = A\} = \mathrm{Isom}(\beta_1)^{C^{-1}}. \end{aligned}$$

(E91) Let G act on a set Ω. Prove that the permutation rank is 2 if and only if G acts 2-transitively on Ω.

Answer. The permutation rank is equal to the number of orbits of G on Ω^2. Clearly G must have at least two such orbits as an element of G cannot map a pair of distinct points to a pair of non-distinct points. Thus G has permutation rank 2 if and only if the two orbits are the set of pairs of distinct points and the set of pairs of non-distinct points. Thus G is transitive on the set of pairs of distinct points, i.e. G is 2-transitive.

Conversely if G is 2-transitive, then it is transitive on the set of pairs of distinct points and therefore transitive on the set of pairs of non-distinct points, and therefore has permutation rank 2.

(E93) Prove that if $\beta(x, y) = 0$, then there exists z with $\beta(x, z), \beta(y, z) \neq 0$.

Answer. The spaces $\langle x\rangle^\perp$ and $\langle y\rangle^\perp$ are subspaces of V of dimension $2r-1$. Clearly their union is not the full vector space V, thus we can take z to be any non-zero element outside their union.

(E94) Prove that if $\beta(x, y) \neq 0$, then there exists z with $\beta(x, z) = \beta(y, z) = 0$.

Answer. Observe that both $\langle x\rangle^\perp$ and $\langle y\rangle^\perp$ are subspaces of dimension $2r-1$. Since $2r > 3$, they must intersect non-trivially and we can take z to be any element in their intersection.

(E96) Given a transvection t, there exists $f \in V^*$ and $a \in \ker(f)$ such that

$$vT = v + (vf)a \text{ for all } v \in V.$$

Answer. Not first that $t - I$ has rank 1. Thus we can choose a basis for V whose first $n-1$ elements, $v_1, \dots, v_{n-1}$ are in $\ker(t-I)$ and whose last element is some vector x. Write $y = x(t-I)$ and note that y is non-zero. Then define the linear functional

$$f : V \to k, c_1v_1 + \cdots c_{n-1}v_{n-1} + cx \mapsto c$$

and observe that, if $v = c_1v_1 + \cdots c_{n-1}v_{n-1} + cx$, then

$$(v)(t-I) = f(v)y.$$

Now, since $(t-I)^2 = 0$ we observe that $y \in \ker(t-I)$ and we are done.

(E97) Prove that symplectic transvections in $\mathrm{Sp}_6(2)$ and $\mathrm{Sp}_4(3)$ are commutators.

Answer. Now let t be a symplectic transvection and write

$$t : V \to V, v \mapsto v + \lambda\beta(v, a)a$$

where $\lambda \in k^*$ and $a \in V$. Let $w \in V$ be such that (w, a) is a hyperbolic pair. Now extending this to a symplectic basis (with w as the first element of the basis and a the last) and invoking Witt's lemma, we know that we can conjugate by an element of $\mathrm{Sp}_{2r}(k)$ so that t is equal to the matrix

$$t = \begin{pmatrix} 1 & 0 & \cdots & 0 & \lambda\beta(v,a) \\ 0 & 1 & & & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Thus, given two conjugacy classes of symplectic transvections in $\mathrm{Sp}_{2r}(k)$ one can find representatives t_1 and t_2 such that $t_1 - I$ is a scalar multiple of $t_2 - I$.

Now let us consider $\mathrm{Sp}_{2r}(k)$ defined with respect to the matrix (1). Then both

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & A^t \end{pmatrix} \text{ and } \begin{pmatrix} I & B \\ 0 & I \end{pmatrix}$$

where A is any invertible $r \times r$ matrix, and B is any symmetric $r \times r$ matrix. Then the commutator of these two matrices is equal to

$$\begin{pmatrix} I & B - ABA^T \\ 0 & I \end{pmatrix}.$$

One can easily check that, for the following choices this commutator has rank 1 and so is a transvection t:

(1) $r = 2$, $|k| = 3$, $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;

(2) $r = 3$, $|k| = 2$, $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$.

What is more if one takes a scalar multiple γB rather than B, then one obtains the transvection t_2 such that $t_2 - I = \gamma(t - I)$. Thus all conjugacy classes of transvections are represented as required.