Chapter III

The finite simple classical groups

Apart from the general reference given in the Introduction, in this Chapter we mainly refer to [5], [11], [15], [22].

1 A criterion of simplicity

(1.1) Definition *A subgroup M of a group $G \neq \{1\}$ is said to be* maximal *if $M \neq G$ and there exists no subgroup $\widehat{M}$ such that $M < \widehat{M} < G$.*

If M is maximal in G, then every conjugate gMg^{-1} of M is maximal in G. Indeed

$$gMg^{-1} < N < G \implies M < g^{-1}Ng < G.$$

Let G be a subgroup of $\mathrm{Sym}(X)$. For any $\alpha \in X$, the set

$$G_\alpha := \{x \in G \mid x(\alpha) = \alpha\}$$

is a subgroup, called the *stabilizer* of α in G. If $\beta = g(\alpha)$ then $G_\beta = gG_\alpha g^{-1}$.

(1.2) Definition *Let $k \in \mathbb{N}$. $G \leq \mathrm{Sym}(X)$ is called:*

- k-transitive *if, for any two k-tuples of pairwise distinct elements in X:*

  $$(\alpha_1, \dots, \alpha_k)\,,\ (\beta_1, \dots, \beta_k)$$

  there exists $g \in G$ such that $g(\alpha_i) = \beta_i$, $1 \leq i \leq k$;

- transitive *if it is 1-transitive;*

- primitive *if it is transitive and G_α is a maximal subgroup of G for (any) $\alpha \in X$.*

To prove that G is transitive on X it is enough to fix $\gamma \in X$ and show that, for any $\alpha \in X$, there exists $g \in G$ such that $g(\gamma) = \alpha$. Actually a more general fact holds:

(1.3) Lemma *Let $G \leq \mathrm{Sym}(X)$ and $(\gamma_1, \ldots, \gamma_k)$ be a fixed k-tuple of distinct elements in X. If, for every k-tuple $(\alpha_1, \ldots, \alpha_k)$ of distinct elements in X there exists $g \in G$ such that $g(\gamma_i) = \alpha_i$, $1 \leq i \leq k$, then G is k-transitive.*

Proof Given $(\alpha_1, \ldots, \alpha_k)$, $(\beta_1, \ldots, \beta_k)$ let $g_1, g_2 \in G$ be such that:

$$g_1(\gamma_i) = \alpha_i, \quad g_2(\gamma_i) = \beta_i, \quad 1 \leq i \leq k.$$

Then $g_2 g_1^{-1}(\alpha_i) = \beta_i$, $1 \leq i \leq k$. ■

(1.4) Lemma *If $G \leq \mathrm{Sym}(X)$ is 2-transitive, then G is primitive.*

Proof Let $G_\alpha < H \leq G$, with $\alpha \in X$. We want to show that $H = G$. To this purpose, choose $h \in H \setminus G_\alpha$ and set $\beta = h(\alpha)$. So $\beta \neq \alpha$. Now take any $g \in G$. If $g(\alpha) = \alpha$, then $g \in H$. Otherwise $g(\alpha) = \gamma \neq \alpha$ and there exists $\overline{h} \in G$ such that $\left(\overline{h}(\alpha), \overline{h}(\beta)\right) = (\alpha, \gamma)$ since G is 2-transitive. In particular $\overline{h} \in G_\alpha < H$. Moreover, from $\overline{h}(\beta) = \gamma$ we get $\overline{h}h(\alpha) = g(\alpha)$. Thus $g^{-1}\overline{h}h \in G_\alpha < H$. From $\overline{h}h \in H$ it follows $g \in H$. So $G = H$. ■

(1.5) Definition *The* derived subgroup *G' of an abstract group G is the subgroup generated by all* commutators $x^{-1}y^{-1}xy := (x, y)$, *i.e.,:*

$$G' := \left\langle x^{-1}y^{-1}xy \mid x, y \in G \right\rangle.$$

If N is a (normal) subgroup of G, then $\frac{G}{N}$ is abelian if and only if $G' \leq N$.

(1.6) Definition *A group $S \neq \{1\}$ is* simple *if its normal subgroups are $\{1\}$ and S.*

The following Theorem provides a fundamental tool by which the simplicity of the classical groups can be proved.

(1.7) Theorem *(Iwasawa's Lemma). A subgroup S of* $\mathrm{Sym}(X)$ *is a simple group whenever the following conditions hold:*

- *S is primitive;*
- *$S = S'$, i.e., S is perfect;*

- *the stabilizer S_α of (any) $\alpha \in X$ contains a normal abelian subgroup A such that S is generated by the conjugates of A, i.e., $S = A^S := \langle A^s \mid s \in S\rangle$.*

Proof $X = \{s(\alpha) \mid s \in S\}$, by the transitivity of S. Let N be a normal subgroup of S. If $N \leq S_\alpha$, every $x = s(\alpha) \in X$ is fixed by $sNs^{-1} = N$, whence $N = \{\mathrm{id}\}$. So assume:

$$N \not\leq S_\alpha. \tag{1.8}$$

Since S_α normalizes N, the product $S_\alpha N = NS_\alpha$ is a subgroup of S. Moreover $S_\alpha \neq NS_\alpha$ in virtue of (1.8). By the maximality of S_α in the primitive group S we get

$$S_\alpha N = S. \tag{1.9}$$

From the assumptions $S = A^S$, A normal in S_α and N normal in S, it follows:

$$S = A^S = A^{S_\alpha N} = A^N \leq NA \leq S.$$

Thus $S = NA$ and

$$\frac{S}{N} = \frac{NA}{N} \cong \frac{A}{A \cap N} \quad \text{abelian} \quad \Longrightarrow \quad S' \leq N.$$

Finally, from $S' = S$ we conclude $S = N$. ∎

2 The projective special linear groups

2.1 The action on the projective space

(2.1) Definition *The group of $n \times n$ invertible matrices, with entries in $\mathbb{F}$, is called the* general linear group *of degree n over $\mathbb{F}$, and indicated by $\mathrm{GL}_n(\mathbb{F})$ or $\mathrm{GL}_n(q)$ if $\mathbb{F} = \mathbb{F}_q$.*

We recall that, over the field $\mathbb{F}$, a matrix is invertible if and only if it has non-zero determinant. By the Theorem of Binet, the map

$$\delta : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^* \quad \text{such that} \quad A \mapsto \det A \tag{2.2}$$

is a homomorphism of groups. Clearly δ is surjective. Its kernel, consisting of the matrices of determinant 1, is called the *special linear group* of degree n over $\mathbb{F}$ and is indicated by $\mathrm{SL}_n(\mathbb{F})$ or $\mathrm{SL}_n(q)$ if $\mathbb{F} = \mathbb{F}_q$. It follows $\frac{\mathrm{GL}_n(\mathbb{F})}{\mathrm{SL}_n(\mathbb{F})} \sim \mathbb{F}^*$. In particular:

$$\frac{|\mathrm{GL}_n(q)|}{|\mathrm{SL}_n(q)|} = q - 1. \tag{2.3}$$

The center Z of $\mathrm{GL}_n(\mathbb{F})$ is defined as

$$Z := \{z \in \mathrm{GL}_n(\mathbb{F}) \mid zg = gz, \forall\ g \in \mathrm{GL}_n(\mathbb{F})\}\,.$$

Z consists of the scalar matrices. Via the homomorphism $g \mapsto Zg$ we have:

$$\begin{tikzcd}
\mathrm{GL}_n(\mathbb{F}) \arrow[r] \arrow[d, dash] & \frac{\mathrm{GL}_n(\mathbb{F})}{Z} := \mathrm{PGL}_n(\mathbb{F}) \arrow[d, dash] & \text{(projective general linear group)} \\
\mathrm{SL}_n(\mathbb{F}) \arrow[r] & \frac{\mathrm{SL}_n(\mathbb{Z})Z}{Z} := \mathrm{PSL}_n(\mathbb{F}) & \text{(projective special linear group).}
\end{tikzcd}$$

Note that:

$$\frac{\mathrm{SL}_n(\mathbb{Z})Z}{Z} \cong \frac{\mathrm{SL}_n(\mathbb{F})}{Z \cap \mathrm{SL}_n(\mathbb{F})}.$$

From the above considerations:

$$|\mathrm{PGL}_n(q)| = \frac{|\mathrm{GL}_n(q)|}{q-1} = |\mathrm{SL}_n(q)|\,, \quad |\mathrm{PSL}_n(q)| = \frac{|\mathrm{SL}_n(q)|}{(n, q-1)}. \tag{2.4}$$

Consider the projective space $X := \mathcal{P}\left(\mathbb{F}^n\right)$, namely the set of 1-dimensional subspaces of $\mathbb{F}^n$. The group $\mathrm{PGL}_n(\mathbb{F})$ acts on X in a natural way. Indeed, the map

$$\begin{array}{rcl}\varphi : \mathrm{GL}_n(\mathbb{F}) & \longrightarrow & \mathrm{Sym}(X) \\ g & \mapsto & \begin{pmatrix} \langle v \rangle \\ \langle gv \rangle \end{pmatrix}\end{array}$$

is a homomorphism with Kernel $Z = \{\lambda I_n \mid \lambda \in \mathbb{F}^*\}$. It follows that

$$\mathrm{PGL}_n(\mathbb{F}) = \frac{\mathrm{GL}_n(\mathbb{F})}{Z} \ \cong\ \mathrm{Im}\varphi\ \leq\ \mathrm{Sym}(X).$$

So, up to the isomorphism induced by φ:

$$\mathrm{PSL}_n(\mathbb{F}) \leq \mathrm{PGL}_n(\mathbb{F}) \leq \mathrm{Sym}(X).$$

(2.5) Lemma *For $n \geq 2$ the group $\mathrm{PSL}_n(\mathbb{F})$ is a 2-transitive subgroup of $\mathrm{Sym}(X)$.*

Proof Let $\{e_1,\ \ldots,\ e_n\}$ be the canonical basis. Given a pair (v_1, v_2) of linearly independent vectors, there exist $s \in \mathrm{SL}_n(\mathbb{F})$ and $\lambda \in \mathbb{F}$ such that $(se_1, se_2) = (\lambda v_1, v_2)$. Indeed, we may extend $\{v_1, v_2\}$ to a basis $\{v_1, v_2, \ldots, v_n\}$ of $\mathbb{F}^n$ and consider the matrices:

$$b = \left(\ v_1 \mid v_2 \mid \ldots \mid v_n\ \right), \quad s = \left(\ \det\ b^{-1} v_1 \mid v_2 \mid \ldots \mid v_n\ \right).$$

Then $s \in \mathrm{SL}_n(\mathbb{F})$ and $se_1 = \lambda v_1$, with $\lambda = \det\ b^{-1}$, $se_2 = v_2$. It follows

$$(\langle se_1 \rangle\,,\ \langle se_2 \rangle) = (\langle v_1 \rangle\,, \langle v_2 \rangle).$$

By Lemma 1.3 the group $\mathrm{PSL}_2(\mathbb{F})$ is 2-transitive on X. ■

2.2 Root subgroups and the monomial subgroup

(2.6) Lemma *Each of the maps from* $(\mathbb{F},+)$ *to* $(\mathrm{SL}_2(\mathbb{F}),\cdot)$ *defined by*

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

is a group monomorphism.

Proof Straightforward calculation. ■

We interpret and generalize this Lemma. As usual we denote by $e_{i,j}$ the $n\times n$ matrix whose entries are all 0, except the entry (i,j) which is 1. Note that $e_{i,i}^2 = e_{ii}$ and $e_{i,j}^2 = 0$ for $i \neq j$. It follows that the map $f_{ij} : (\mathbb{F},+) \to (\mathrm{SL}_n(\mathbb{F}),\cdot)$ such that, for all $t \in \mathbb{F}$:

$$t \mapsto \exp\left(te_{ij}\right) = I + te_{i,j},$$

is a group monomorphism for all $i \neq j$.

(2.7) Definition *For* $i \neq j$ *the image of* f_{ij}*, namely the subgroup* $\{I + te_{i,j} \mid t \in \mathbb{F}\}$ *is called a* root subgroup*. Its elements* $I + te_{i,j}$ *are called* elementary transvections*.*

More generally, each of the maps $(\mathbb{F}^{n-1},+,0) \to (\mathrm{SL}_n(\mathbb{F}),\cdot,I_n)$ defined by:

$$v \mapsto \begin{pmatrix} 1 & v^T \\ 0 & I_{n-1} \end{pmatrix}, \quad v \mapsto \begin{pmatrix} 1 & 0 \\ v & I_{n-1} \end{pmatrix}, \quad \forall\, v \in \mathbb{F}^{n-1} \tag{2.8}$$

is a group homomorphism. Since the additive group $\mathbb{F}^{n-1}$ is generated by the subgroups $\mathbb{F}e_i$, $1 \leq i \leq n-1$, the images of the maps in (2.8) are generated by elementary transvections.

For $n \geq 3$, every elementary transvection is a commutator. Indeed:

$$(e_{i,j}, e_{j,k}) = e_{i,k} \quad \text{whenever} \quad |\{i,j,k\}| = 3. \tag{2.9}$$

Any matrix whose columns are the vectors of the canonical basis (in some order) is called a *permutation matrix*. The map $\mathrm{Sym}(n) \to \mathrm{GL}_n(\mathbb{F})$ such that

$$\sigma \mapsto \pi_\sigma := \left(\ e_{\sigma(1)}\ \middle|\ \dots\ \middle|\ e_{\sigma(n)}\ \right)$$

is a monomorphism whose image is the group S_n of permutation matrices. For $n \geq 2$, the determinant map $\delta : S_n \to \langle -1 \rangle$ is an epimorphism with kernel $S_n \cap \mathrm{SL}_n(\mathbb{F})$.
If char $\mathbb{F} \neq 2$, then Ker $\delta \cong \mathrm{Alt}(n)$ has index 2 in S_n. If char $\mathbb{F} = 2$, then Ker $\delta = S_n$.
S_n normalizes the group of diagonal matrices $D \simeq (\mathbb{F}^*)^n$. In fact, for all i,j:

$$\pi_\sigma\, e_{i,j}\, \pi_\sigma^{-1} \ = \ e_{\sigma(i),\sigma(j)}. \tag{2.10}$$

(2.11) Definition *The product $M := DS_n$ of the diagonal and permutation subgroups is called the standard* monomial group.

The monomial subgroup M consists of the matrices whose columns are non-zero multiples of the vectors of the canonical basis (in some order). Clearly

$$\frac{M}{D} \cong \mathrm{Sym}(n).$$

(2.12) Lemma *$M \cap \mathrm{SL}_n(\mathbb{F})$ is generated by elementary transvections.*

Proof Suppose first $n = 2$. Then $M = DS_2 = D\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$. By the modular identity:

$$M \cap \mathrm{SL}_2(\mathbb{F}) = (D \cap \mathrm{SL}_2(\mathbb{F}))\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \mid \alpha \in \mathbb{F}^* \right\} \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

So the claim is true by the following identities:

(1) $\begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha^{-1} - 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix}$;

(2) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.

Then, for $n \geq 2$, the result follows easily. In fact $\mathrm{Sym}(n)$ is generated by transpositions and each matrix $\mathrm{diag}\left(\alpha_1, \ldots, \alpha_{n-1}, \prod_{i=1}^{n-1} \alpha_i^{-1}\right)$ in $D \cap \mathrm{SL}_n(\mathbb{F})$ can be written as

$$\left(\alpha_1, \ldots, 1, \alpha_1^{-1}\right) \ldots \left(1, \ldots, \alpha_{n-1}, \alpha_{n-1}^{-1}\right).$$

■

(2.13) Lemma *The group $\mathrm{SL}_n(\mathbb{F})$ is generated by the* elementary transvections.

Proof Fix $A = (a_{i,j}) \in \mathrm{SL}_n(\mathbb{F})$. We have to show that A is a product of elementary transvections. There exists an entry $a_{h,k} \neq 0$. Let $d = \mathrm{diag}(-1, 1, \ldots, 1)$ and note that, if $h \neq 1$, then $d\pi_{1h} \in M \cap \mathrm{SL}_n(\mathbb{F})$. Similarly, if $k \neq 1$, then $d\pi_{1k} \in M \cap \mathrm{SL}_n(\mathbb{F})$. If $a_{h,k} \neq a_{1,1}$, by Lemma 2.12 we may substitute A with $A' = \pi_{1h} A \pi_{k1}$, or $A' = A d\pi_{k1}$ or $A' = d\pi_{1h} A$ according to $h \neq 1, k \neq 1$, or $h = 1, k \neq 1$ or $h \neq 1$, $k = 1$. Thus:

$$A' = \begin{pmatrix} \alpha & * \\ * & * \end{pmatrix}, \ \alpha = \pm a_{h,k} \neq 0.$$

Again by Lemma 2.12 we may substitute A' with:

$$A'' = \mathrm{diag}\left(\alpha^{-1}, \alpha, 1, \ldots, 1\right) A' = \begin{pmatrix} 1 & v^T \\ w & B \end{pmatrix}$$

where $v, w \in \mathbb{F}^{n-1}$, $B \in \mathrm{SL}_{n-1}(\mathbb{F})$. By (2.8), we may substitute A'' with:

$$\begin{pmatrix} 1 & 0 \\ -w & 1 \end{pmatrix} A'' \begin{pmatrix} 1 & -v^T \\ 0 & I \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}, \quad B' \in \mathrm{SL}_{n-1}(\mathbb{F}).$$

The claim now follows by induction on n. ■

2.3 Simplicity and order

(2.14) Theorem $\mathrm{PSL}_n(\mathbb{F})$ *is simple, except when* $n = 2$ *and* $\mathbb{F} = \mathbb{F}_2$ *or* $\mathbb{F} = \mathbb{F}_3$.

Proof $S = \mathrm{PSL}_n(\mathbb{F})$ is a 2-transitive subgroup of $\mathrm{Sym}(X)$ by Lemma 2.5, where $X = \mathcal{P}(\mathbb{F}^n)$ is the projective space. Hence S is a primitive subgroup of $\mathrm{Sym}(X)$ by Lemma 1.4. The preimage in $\mathrm{SL}_n(\mathbb{F})$ of the stabilizer $S_{\langle e_1 \rangle}$, namely the group

$$\left\{ \begin{pmatrix} \det a^{-1} & v^T \\ 0_{\mathbb{F}^{n-1}} & a \end{pmatrix} \mid a \in \mathrm{GL}_{n-1}(\mathbb{F}),\ v \in \mathbb{F}^{n-1} \right\}$$

contains the normal abelian subgroup

$$A := \left\{ \begin{pmatrix} 1 & v^T \\ 0 & I \end{pmatrix} \mid v \in \mathbb{F}^{n-1} \right\}.$$

It follows that the projective image of A is abelian and normal in $S_{\langle e_1 \rangle}$.
The group A is generated by the elementary transvections

$$\{I + tE_{12} \mid t \in \mathbb{F}\}, \ \ldots, \ \{I + tE_{1n} \mid t \in \mathbb{F}\}.$$

By (2.10), every elementary transvection $I + te_{i,j}$ is conjugate to $I + tE_{1,2}$ under $DS_n \cap \mathrm{SL}_n(\mathbb{F})$. Thus the conjugates of A generate $\mathrm{SL}_n(\mathbb{F})$ by Lemma 2.13. Hence the conjugates of the projective image of A generate $\mathrm{PSL}_n(\mathbb{F}) = S$.
Finally suppose $|\mathbb{F}| \neq 2, 3$ if $n = 2$. Then $\mathrm{SL}_n(\mathbb{F}) = \mathrm{SL}_n(\mathbb{F})'$, whence $S = S'$: this fact follows from (2.9) for $n \geq 3$, from Lemma 2.12 for $n = 2$.
Our claim is proved in virtue of Iwasawa's Lemma (Theorem 1.7 of this Chapter).
For $|\mathbb{F}| = 2$ and $|\mathbb{F}| = 3$ we have, respectively, $|X| = 3$ and $|X| = 4$. Thus $\mathrm{PSL}_2(2) \leq \mathrm{Sym}(3)$ and $\mathrm{PSL}_2(3) \leq \mathrm{Sym}(4)$ cannot be simple. ■

(2.15) Theorem *When* $\mathbb{F} = \mathbb{F}_q$ *is finite, we have:*

$$|\mathrm{PSL}_n(q)| = \frac{1}{(n, q-1)} q^{\frac{n(n-1)}{2}} (q^2 - 1) \cdots (q^n - 1).$$

Proof The columns of every matrix $\left(v_1 \mid \ldots \mid v_n \right)$ of $\mathrm{GL}_n(\mathbb{F})$ are a basis of $\mathbb{F}^n$ and, vice versa, the vectors of every basis $\{v_1, \ldots, v_n\}$ can be taken as columns of a matrix in $\mathrm{GL}_n(\mathbb{F})$. So $|\mathrm{PSL}_n(q)|$ equals the number of basis of $V = \mathbb{F}_q^n$.
For v_1 one can choose any vector in $V \setminus \{0\}$: here there are $q^n - 1$ choices.
Once v_1 is fixed, v_2 must be chosen in $V \setminus \langle v_1 \rangle$: hence there are $q^n - q$ choices.
Then v_3 must be chosen in $V \setminus \langle v_1, v_2 \rangle$: this gives $q^n - q^2$ choices. And so on... Thus:

$$|\mathrm{GL}_n(q)| = (q^n - 1)(q^n - q)\left(q^n - q^2\right) \ldots \left(q^n - q^{n-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \left(q^i - 1\right).$$

The claim follows from (2.4). ∎

3 The symplectic groups

By Theorem 4.2 of Chapter II, up to conjugation under $\mathrm{GL}_{2m}(\mathbb{F})$, we may define the *symplectic group* $\mathrm{Sp}_{2m}(\mathbb{F})$ as

$$\mathrm{Sp}_{2m}(\mathbb{F}) = \left\{ g \in \mathrm{GL}_{2m}(\mathbb{F}) \mid g^T \begin{pmatrix} \mathbf{0} & I_m \\ -I_m & \mathbf{0} \end{pmatrix} g = \begin{pmatrix} \mathbf{0} & I_m \\ -I_m & \mathbf{0} \end{pmatrix} \right\}.$$

Direct calculation shows that $\mathrm{Sp}_2(\mathbb{F}) = \mathrm{SL}_2(\mathbb{F})$.

(3.1) Theorem *Let $m \geq 2$. Then:*

(1) $\mathrm{Sp}_{2m}(\mathbb{F})$ *is generated by the following matrices and their transposes:*

$$\begin{pmatrix} I_m + te_{i,j} & 0 \\ 0 & I_m - te_{j,i} \end{pmatrix} \begin{matrix} 1 \leq i < j \leq m \\ t \in \mathbb{F} \end{matrix} \quad , \quad \begin{pmatrix} I_m & te_{i,i} \\ 0 & I_m \end{pmatrix} \begin{matrix} 1 \leq i \leq m \\ t \in \mathbb{F} \end{matrix} \quad ;$$

(2) $\mathrm{Sp}_{2m}(\mathbb{F})' = \mathrm{Sp}_{2m}(\mathbb{F})$ *is perfect, except* $\mathrm{Sp}_4(\mathbb{F}_2) \cong \mathrm{Sym}(6)$*;*

(3) *the center of* $\mathrm{Sp}_{2m}(\mathbb{F})$ *is the subgroup generated by* $-I$.

In particular $\mathrm{Sp}_{2m}(\mathbb{F}) \leq \mathrm{SL}_{2m}(\mathbb{F})$ by (1).
For the original proof of (1) see [18]. The rest can be proved by direct calculation.

(3.2) Definition *The projective image of* $\mathrm{Sp}_{2m}(\mathbb{F})$*, namely the group*

$$\frac{\mathrm{Sp}_{2m}(\mathbb{F})Z}{Z} \cong \frac{\mathrm{Sp}_{2m}(\mathbb{F})}{\mathrm{Sp}_{2m} \cap Z} = \frac{\mathrm{Sp}_{2m}(\mathbb{F})}{\langle -I \rangle}$$

is called the projective symplectic group *and indicated by* $\mathrm{PSp}_{2m}(\mathbb{F})$.

$\mathrm{PSp}_{2m}(\mathbb{F})$, being a subgroup of $\mathrm{PSL}_n(\mathbb{F})$, acts on the projective space $X = \mathcal{P}(\mathbb{F}^n)$. Since all vectors are isotropic, all 1-dimensional subspaces $\langle v \rangle$ and $\langle w \rangle$ are isometric. By Witt's extension Lemma there exists $g \in Sp_{2m}(\mathbb{F})$ such that $\langle gv \rangle = \langle w \rangle$. So $\mathrm{PSp}_{2m}(\mathbb{F})$ is transitive on X. Again by Witt's Lemma , the stabilizer of $\langle v \rangle$ in $\mathrm{PSp}_{2m}(\mathbb{F})$ has 3 orbits on X, namely:

$$\{\langle v \rangle\}, \quad \{\langle w \rangle \mid (v,w) = 0\}, \quad \{\langle w \rangle \mid (v,w) \neq 0\}.$$

Using this information, one can prove the following

(3.3) Lemma $\mathrm{PSp}_{2m}(\mathbb{F})$ *is a primitive subgroup of* $\mathrm{Sym}(X)$, *where* $X = \mathcal{P}(\mathbb{F}^n)$.

(3.4) Theorem *Assume* $m \geq 2$ *and* $\mathbb{F} \neq \mathbb{F}_2$ *when* $m = 2$. *Then* $\mathrm{PSp}_{2m}(\mathbb{F})$ *is simple.*

Proof (sketch) Under our assumptions, the group $S = \mathrm{PSp}_{2m}(\mathbb{F})$ is perfect, by point (2) of Theorem 3.1, and acts primitively on the projective space $X = \mathcal{P}(\mathbb{F}^n)$ by the previous Lemma. In order to apply Iwasawa's Lemma to S, it is convenient to suppose that $Sp_{2m}(\mathbb{F})$ is the group of isometries of

$$J' = \begin{pmatrix} J_1 & \\ & J_2 \end{pmatrix}, \quad \text{where} \quad J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J_2 = \begin{pmatrix} \mathbf{0} & I_{m-1} \\ -I_{m-1} & \mathbf{0} \end{pmatrix}$$

The linear preimage of the stabilizer $S_{\langle e_1 \rangle}$ of $\langle e_1 \rangle$ fixes $\langle e_1 \rangle^\perp = \langle e_1, e_3, \dots e_{2m} \rangle$ and induces the group $\mathrm{Sp}_{2(m-1)}(\mathbb{F})$ on $\frac{\langle e_1 \rangle^\perp}{\langle e_1 \rangle}$. So it consists of the matrices:

$$\left\{ \begin{pmatrix} \alpha & \beta & \alpha u^T J_2 c \\ 0 & \alpha^{-1} & \mathbf{0}^T \\ \mathbf{0} & u & c \end{pmatrix} \mid 0 \neq \alpha,\ \beta \in \mathbb{F},\ u \in \mathbb{F}^{2m-2},\ c \in \mathrm{Sp}_{2m-2}(\mathbb{F}) \right\}. \tag{3.5}$$

Noting that

$$\begin{pmatrix} \alpha & \beta & \alpha u^T J_2 c \\ 0 & \alpha^{-1} & \mathbf{0}^T \\ \mathbf{0} & u & c \end{pmatrix}^{-1} = \begin{pmatrix} \alpha^{-1} & -\beta & -u^T J_2 \\ 0 & \alpha & \mathbf{0}^T \\ \mathbf{0} & -\alpha c^{-1} u & c^{-1} \end{pmatrix}$$

it is not difficult to check that the abelian group :

$$A = \left\{ \begin{pmatrix} 1 & \gamma & \mathbf{0}^T \\ 0 & 1 & \mathbf{0}^T \\ \mathbf{0} & \mathbf{0} & I_{2m-2} \end{pmatrix} \mid \gamma \in \mathbb{F} \right\}$$

is normal in the preimage of $S_{\langle e_1 \rangle}$ described by (3.5). One can also show that the conjugates of A generate $\mathrm{Sp}_{2m}(\mathbb{F})$. So the projective image of A is an abelian, normal subgroup of $S_{\langle e_1 \rangle}$, whose conjugates generate S. Our claim follows from Theorem 1.7. ■

(3.6) Theorem $|\mathrm{PSp}_{2m}(q)| \;=\; \frac{1}{(2,q-1)}\; q^{m^2}(q^2-1)(q^4-1)\cdots(q^{2m}-1)$.

Proof Each matrix of $Sp_{2m}(q)$ is a basis $\{v_1,\ldots,v_m,v_{-1},\ldots,v_{-m}\}$ of $\mathbb{F}^{2m}$ such that

$$(v_i,v_{-i}) = v_i^T J v_{-i} = 1, \quad (v_i,v_j) = v_i^T J v_j = 0 \quad j \neq -i.$$

$0 \neq v_1$ can be chosen in $(q^{2m}-1)$ ways (as $(v,v)=0$ for all v.
For any fixed v_1, the vector v_{-1} can be chosen in q^{2m-1} ways. Indeed it must satisfy

$$(v_1,v_{-1}) = v_1^T J v_{-1} = 1. \tag{3.7}$$

The space of solutions of the homogeneous equation in $2m$ indeterminates

$$v_1^T J v_{-1} = 0$$

has dimension $2m-1$. Hence the system (3.7) has q^{2m-1} solutions.

$$\mathbb{F}^n = \langle v_1, v_2\rangle \perp \langle v_2,\ldots,v_m,v_{-2},\ldots,v_{-m}\rangle .$$

Applying induction to the number of symplectic basis of $\langle v_2,\ldots,v_{-m}\rangle$ we get

$$|Sp_{2m}(q)| \;=\; (q^{2m}-1)q^{2m-1}\;\left(q^{(m-1)^2}(q^2-1)(q^4-1)\cdots(q^{2(m-1)}-1)\right).$$

■

4 The orthogonal groups

Given an orthogonal space (V,Q), with $V=\mathbb{F}^n$, we consider its group of isometries:

$$O_n(\mathbb{F},Q) := \{h \in \mathrm{GL}_n(\mathbb{F}) \mid Q(v) = Q(hv), \quad \forall\, v \in \mathbb{F}^n\}. \tag{4.1}$$

Any $h \in O_n(\mathbb{F},Q)$ preserves the non-degenerate symmetric bilinear form

$$(v,w) := Q(v+w) - Q(v) - Q(w), \quad \forall\, v,w \in \mathbb{F}^n. \tag{4.2}$$

Thus, if J denotes the matrix of (4.2) with respect to the canonical basis, we have:

$$h^T J h = J, \quad \forall\, h \in O_n(\mathbb{F},Q). \tag{4.3}$$

It follows, in particular, $(\det h)^2 = 1$, i.e., $\det h = \pm 1$ for all $h \in O_n(\mathbb{F},Q)$.

Suppose first char $\mathbb{F} \neq 2$. By the considerations at the beginning of Section 6.2, the isometries of J are precisely the isometries of Q. So we have the alternative definition:

$$O_n(\mathbb{F}, Q) := \left\{h \in \mathrm{GL}_n(\mathbb{F}) \mid h^T J h = J\right\}, \quad \text{char } \mathbb{F} \neq 2. \tag{4.4}$$

In $O_n(\mathbb{F}, Q)$ there are matrices of determinant -1, as the reflections defined below. So the group of orthogonal transformations of determinant 1, namely the group

$$SO_n(\mathbb{F}, Q) := O_n(\mathbb{F}, Q) \cap \mathrm{SL}_n(\mathbb{F})$$

has index 2 in $O_n(\mathbb{F}, Q)$.
Now suppose char $\mathbb{F} = 2$. By Lemma 6.13 of Chapter II, we have $n = 2m$ and

$$O_{2m}(\mathbb{F}, Q) = SO_{2m}(\mathbb{F}, Q) \leq \mathrm{Sp}_{2m}(\mathbb{F}). \tag{4.5}$$

(4.6) Definition *For each $w \in \mathbb{F}^n$ with $Q(w) \neq 0$, the* reflection *r_w is the map*

$$v \mapsto v - \frac{(v, w)}{Q(w)} w, \quad \forall\, v \in \mathbb{F}^n.$$

It is immediate to see that $r_w \in O_n(\mathbb{F}, Q)$. Moreover:

(4.7) Theorem

(1) *the orthogonal group $O_n(\mathbb{F}, Q)$ is generated by the reflections;*

(2) *the center of $O_n(\mathbb{F}, Q)$ is generated by $-I$.*

But we are more interested in generators of the derived subgroup of $O_n(\mathbb{F}, Q)$, since this is the group whose projective image is generally simple.

(4.8) Definition *$\Omega_n(\mathbb{F}, Q)$ denotes the derived subgroup of $O_n(\mathbb{F}, Q)$ and $P\Omega_n(\mathbb{F}, Q)$ its projective image in $\mathrm{PGL}_n(\mathbb{F})$.*

Clearly $\Omega_n(\mathbb{F}, Q) \leq \mathrm{SO}_n(\mathbb{F}, Q)$. It can also be shown that:

$$|\mathrm{SO}_n(\mathbb{F}, Q) : \Omega_n(\mathbb{F}, Q)| \leq 2.$$

(4.9) Theorem *Let $m \geq 2$. Write $v = \sum_{i=1}^{m} (x_i e_i + x_{-i} e_{-i})$ if $v \in \mathbb{F}^{2m}$, $v = x_0 e_0 + \sum_{i=1}^{m} (x_i e_i + x_{-i} e_{-i})$ if $v \in \mathbb{F}^{2m+1}$.*

- *If $Q(v) = \sum_{i1}^{m} x_i x_{-i}$, then $\Omega_n(\mathbb{F}, Q) := \Omega_n^+(\mathbb{F})$ is generated by the following matrices and their transposes:*

$$\begin{pmatrix} I_m + t e_{i,j} & 0 \\ 0 & I_m - t e_{j,i} \end{pmatrix}, \quad \begin{pmatrix} I_m & t\,(e_{i,j} - e_{j,i}) \\ 0 & I_m \end{pmatrix}, \quad t \in \mathbb{F},\ i < j \leq m.$$

- *If $Q(v) = x_0^2 + \sum_{i_1}^m x_i x_{-i}$ and char $\mathbb{F} \neq 2$, then $\Omega_n(\mathbb{F}, Q)$ is generated by the following matrices and their transposes:*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & I_m + te_{j,i} & 0 \\ 0 & 0 & I_m - te_{i,j} \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -te_i^T \\ 2e_i & I_m & -t^2 e_{i,i} \\ 0 & 0 & I_m \end{pmatrix}, \quad t \in \mathbb{F},\ j < i \leq m.$$

Note that the matrices of the corresponding polar forms are respectively

$$J_{2m} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}, \quad J_{2m+1} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & I_m \\ 0 & I_m & 0 \end{pmatrix}.$$

In what follows, let $t^2 + t + \zeta$ be an irreducible polynomial in $\mathbb{F}[t]$, with roots $\alpha \neq \overline{\alpha}$ in

$$\mathbb{K} := \mathbb{F}(\alpha).$$

(4.10) Lemma *Consider the space $(\mathbb{F}^2, Q_\zeta)$ with $Q_\zeta(v) = x_1^2 + x_1 x_{-1} + \zeta x_{-1}^2$ for each $v = \begin{pmatrix} x_1 \\ x_{-1} \end{pmatrix}$. Set $P = \begin{pmatrix} 1 & -\alpha \\ 1 & -\overline{\alpha} \end{pmatrix}$. Then*

$$\mathrm{O}_2(\mathbb{F}, Q_\zeta) = P^{-1}\mathrm{O}_2^+(\mathbb{K})P \cap \mathrm{SL}_2(\mathbb{F})$$

where $\mathrm{O}_2^+(\mathbb{K})$ is the group of isometries of Q, with $Q(v) = x_1 x_{-1}$.
In particular, up to conjugation:

- *$O_2^+(q) = \left\langle \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ with β of order $q-1$;*
- *$O_2^-(q) = \left\langle \begin{pmatrix} \frac{-\overline{\alpha}\gamma + \alpha\gamma^{-1}}{\alpha - \overline{\alpha}} & \frac{\zeta(\gamma - \gamma^{-1})}{\alpha - \overline{\alpha}} \\ \frac{-\gamma + \gamma^{-1}}{\alpha - \overline{\alpha}} & \frac{\alpha\gamma - \overline{\alpha}\gamma^{-1}}{\alpha - \overline{\alpha}} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\rangle$ with $\gamma \in \mathbb{F}_{q^2}$ of order $q+1$.*

Proof We pass from the canonical basis $\{e_1, e_2\}$ of $\mathbb{K}^2$ to the basis $\mathcal{B} = \{P^{-1}e_1, P^{-1}e_2\}$. For any v as in the statement, its coordinate vector $v_\mathcal{B}$ with respect to $\mathcal{B}$ becomes:

$$v_\mathcal{B} = Pv = \begin{pmatrix} x_1 - \alpha x_{-1} \\ x_1 - \overline{\alpha} x_{-1} \end{pmatrix}.$$

With this change of coordinates, the form Q such that $Q(v) = x_1 x_{-1}$ becomes Q_ζ, as:

$$Q(Pv) = (x_1 - \alpha x_{-1})(x_1 - \overline{\alpha} x_{-1}) = x_1^2 + x_1 x_{-1} + \zeta x_{-1}^2 = Q_\zeta(v).$$

Since $\mathrm{O}_2^+(\mathbb{K})$ preserves the quadratic form Q, its conjugate $P^{-1}\mathrm{O}_2^+(\mathbb{K})P$ preserves Q_ζ. Indeed, let $A \in \mathrm{O}_2^+(\mathbb{K})$. Then, for all $v \in \mathbb{K}^2$:

$$Q_\zeta(v) = Q(Pv) = Q(APv) = Q\left(PP^{-1}APv\right) = Q_\zeta\left((P^{-1}AP)v\right).$$

The rest follows by calculation. ■

(4.11) Remark *The space* $(\mathbb{F}^2, Q_\zeta)$ *is anisotropic, but* $(\mathbb{K}^2, Q_\zeta)$ *is not, since* $t^2+t+\zeta$ *is reducible over* $\mathbb{K}$*. In fact, by the previous Lemma,* $(\mathbb{K}^2, Q_\zeta)$ *is isometric to* $(\mathbb{K}^2, Q)$*.*

When $n = 2m$, let $t^2+t+\zeta = (t-\alpha)(t-\overline{\alpha})$ be as in the Lemma 4.10 and set

$$Q_\zeta = \sum_{i=1}^{m} x_i x_{-i} + x_m^2 + \zeta x_{-m}^2.$$

$\Omega_n(\mathbb{F}, Q_\zeta)$ is a subgroup of a conjugate of $\Omega_n^+(\mathbb{K})$. Indeed, let $S = \operatorname{diag}(I_{n-2}, P)$ with P as in Lemma 4.10. then:

$$\Omega_n(\mathbb{F}, Q_\zeta) = S^{-1}\Omega_n^+(\mathbb{K})S \cap \mathrm{SL}_n(\mathbb{F}).$$

Recall that, when $\mathbb{F} = \mathbb{F}_q$ then, up to conjugation:

$$\Omega_n(\mathbb{F}_q, Q_\zeta) = \Omega_n^-(q).$$

For $n \geq 3$ the center of $\Omega_n(\mathbb{F}, Q)$ is $\Omega_n(\mathbb{F}, Q) \cap \langle -I \rangle$. Thus the projective image

$$P\Omega_{2m}^+(\mathbb{F}, Q) := \frac{\Omega_n(\mathbb{F}, Q)}{\Omega_n(\mathbb{F}, Q) \cap \langle -I \rangle}.$$

(4.12) Theorem *The groups* $P\Omega_{2m}^+(q)$*,* $P\Omega_{2m}^-(q)$*, for all* q *and* $m \geq 3$*, are simple. The groups* $P\Omega_{2m+1}(q)$*, for* q *odd and* $m \geq 2$*, are simple.*

The proof is based on Iwasawa's Lemma, since $P\Omega_{2m}^+(\mathbb{F}, Q)$ is perfect and acts as a primitive group on the set of isotropic 1-dimensional subspaces.

$$\begin{aligned}
|P\Omega_{2m+1}(q)| &= \tfrac{1}{(2,q-1)}\, q^{m^2}(q^2-1)(q^4-1)\cdots(q^{2m}-1)\\
\left|P\Omega_{2m}^+(q)\right| &= \tfrac{1}{(4,q^m-1)}\, q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m-1)\\
\left|P\Omega_{2m}^-(q)\right| &= \tfrac{1}{(4,q^m+1)}\, q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m+1).
\end{aligned}$$

5 The unitary groups

Let $\mathbb{F}$ have an automorphism σ of order 2 and f be a non-singular hermitian form on $\mathbb{F}^n$ with matrix J with respect to the canonical basis. The unitary group is defined as:

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

In particular, when $\mathbb{F} = \mathbb{F}_{q^2}$ or $\mathbb{F} = \mathbb{C}$ and σ is the complex conjugation, we may assume $J = I$ by the classification of hermitian form over these fields.
The center Z of $\mathrm{GU}_n(\mathbb{F}, f)$ consists of the scalar matrices αI such that

$$\alpha\alpha^\sigma = 1.$$

In particular the center of $\mathrm{GU}_n(q^2)$ has order $q+1$. (Exercise).

$$\mathrm{SU}_n(\mathbb{F}, f) := \mathrm{GU}_n(\mathbb{F}, f) \cap \mathrm{SL}_n(\mathbb{F}).$$

The projective image of $\mathrm{SU}_n(\mathbb{F}, f)$ in $\mathrm{PGL}_n(\mathbb{F})$, namely the group

$$\mathrm{PSU}_n(\mathbb{F}, f) := \frac{\mathrm{SU}_n(\mathbb{F}, f)Z}{Z} \cong \frac{\mathrm{SU}_n(\mathbb{F}, f)}{\mathrm{SU}_n(\mathbb{F}, f) \cap Z}$$

is called the *projective special unitary group*.

(5.1) Lemma $\mathrm{SL}_2(q) \cong \mathrm{SU}_2(q^2)$.

Proof Let $\gamma \in \mathbb{F}_{q^2}$ be such that $\gamma^{q-1} = -1$. Then $J = \begin{pmatrix} 0 & \gamma \\ -\gamma & 0 \end{pmatrix}$ defines a non-singular hermitian form. Direct calculation shows that, for all $a, b, c, d \in \mathbb{F}_{q^2}$ such that $ad - bc = 1$,

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} J \begin{pmatrix} a^q & b^q \\ c^q & d^q \end{pmatrix} = J \quad \Longleftrightarrow \quad a, b, c, d \in \mathbb{F}_q.$$

■

(5.2) Theorem *For $n \geq 3$ the groups $\mathrm{PSU}_n(\mathbb{F})$ are simple, except when $(n, \mathbb{F}) = (3, \mathbb{F}_4)$.*

Again the proof is based on Iwasawa's Lemma and the primitive action on the set of 1-dimensional isotropic subspaces.
In the finite case:

$$\left|\mathrm{PSU}_n(q^2)\right| = \frac{1}{(n, q+1)}\, q^{\frac{n(n-1)}{2}} (q^2 - 1)(q^3 + 1)(q^4 - 1) \cdots (q^n - (-1)^n).$$

6 The list of finite classical simple groups

Up to isomorphisms, the list is the following:

- $\mathrm{PSL}_n(q) = A_{n-1}(q)$, $n \geq 2$, except $\mathrm{PSL}_2(2) \cong \mathrm{Sym}(3)$, $\mathrm{PSL}_2(3) \cong \mathrm{Alt}(4)$;
- $\mathrm{PSp}_{2m}(q) = C_m(q)$, $m \geq 2$, except $\mathrm{PSp}_4(2) \cong \mathrm{Sym}(6)$;

- $\mathrm{PSp}_4(2)' \cong \mathrm{Alt}(6)$;
- $P\Omega_{2m+1}(q) = B_m(q)$, q odd, $m \geq 2$;
- $P\Omega^+_{2m}(q) = D_m(q)$, $P\Omega^-_{2m}(q) = {}^2D_m(q)$, $m \geq 3$;
- $\mathrm{PSU}_n(q^2) = {}^2A_{n-1}(q)$, $n \geq 3$, except $\mathrm{PSU}_3(4) \cong 3^2.Q_8$.

The lower bounds for n and m above are due to exceptional isomorphisms, such as:

- $\mathrm{SL}_2(q) \cong \mathrm{Sp}_2(q) \cong \mathrm{SU}_2(q^2)$;
- $\Omega^\pm_2(q) \cong C_{\frac{q\mp1}{(2,q-1)}}$ (cyclic group);
- $P\Omega^+_4(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$;
- $P\Omega^-_4(q) \cong \mathrm{PSL}_2(q^2)$;
- $P\Omega^+_6(q) \cong \mathrm{PSL}_4(q)$;
- $P\Omega^-_6(q) \cong \mathrm{PSU}_4(q^2)$;

7 Exercises

(7.1) Exercise *Let G be a subgroup of $\mathrm{Sym}(X)$, $g \in G$ and $\alpha, \beta \in X$. Show that, if $\beta = g(\alpha)$ then $G_\beta = gG_\alpha g^{-1}$.*

(7.2) Exercise

- *Let N be a normal subgroup of G such that the factor group $\frac{G}{N}$ is abelian. Show that $G' \leq N$.*
- *Let N be a subgroup of G such that $G' \leq N$. Show that N is normal and $\frac{G}{N}$ is abelian.*

(7.3) Exercise *Assuming $\alpha\beta\gamma = 1$, write $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ and $\begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & \beta \\ \gamma & 0 & 0 \end{pmatrix}$ as products of elementary transvections.*

(7.4) Exercise *Show that the map $\left(\mathbb{F}^2, +, 0\right) \to (\mathrm{SL}_3(\mathbb{F}), \cdot, I)$ defined by:*

$$\begin{pmatrix} t_1 \\ t_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ t_1 & 1 & 0 \\ t_2 & 0 & 1 \end{pmatrix}$$

is a homomorphism of groups. Write the matrix on the right (and its transpose) as a product of elementary transvections.

(7.5) Exercise *Show that* $\mathrm{SL}_2(\mathbb{F}) = \mathrm{SL}_2(\mathbb{F})'$ *except when* $|\mathbb{F}| = 2, 3$.

(7.6) Exercise *Show that the center* Z *of* $\mathrm{SL}_n(\mathbb{F})$ *consists of scalar matrices.*

(7.7) Exercise *Show that:* $|Z \cap \mathrm{SL}_n(q)| = (n, q-1)$.

(7.8) Exercise *Show that any matrix* $m \in \mathrm{Mat}_n(\mathbb{F})$ *is conjugate to its transpose.* (**Hint**: *start from a companion matrix) and deduce that:*

- *any symplectic transformation* $g \in \mathrm{Sp}_{2m}(\mathbb{F})$ *is conjugate to* g^{-1} *under* $\mathrm{GL}_{2m}(\mathbb{F})$*;*
- *any orthogonal transformation* $g \in O_n(\mathbb{F}, Q)$ *is conjugate to* g^{-1} *under* $\mathrm{GL}_n(\mathbb{F})$.

(7.9) Exercise *Let* $\mathbb{F}^n$ *be an orthogonal space with respect to* Q. *Show that, for every* $0 \neq w \in \mathbb{F}^n$ *the reflection* r_w *is a linear transformation of determinant* -1, *and an isometry of* Q. *Write the matrix of* r_w *with respect to a basis* $w, w_2, \ldots, w_n$ *where* $w_2, \ldots, w_n$ *is a basis of* $\langle w \rangle^{\perp}$.