Semi-linear groups over finite fields

J.W.P. Hirschfeld

June 1999

1 Polarities

The notation of [3, Section 2.1.1] is followed.

A prime $\boldsymbol{\pi}(U)$ is the set of points $\mathbf{P}(X)$ with $X = (x_0, \ldots, x_n)$ satisfying a relation $u_0x_0 + u_1x_1 + \ldots + u_nx_n = 0$. The vector $U = (u_0, \ldots, u_n)$ is a *coordinate vector* of the prime; the u_i are called *prime* or *hyperplane* or *tangential* coordinates.

Let S be a space $PG(n, K)$ and S' its dual space superimposed on S; that is, the points of S' are the primes of S and the primes of S' are the points of S. Consider a function $\mathfrak{T}: S \longrightarrow S'$. If $\mathfrak{T}$ is a collineation, it is called a *reciprocity* of S and induces a collineation, also named $\mathfrak{T}$, of S' to S; that is, if the points of S are transformed to primes, then primes are transformed to points since $\mathfrak{T}$ preserves incidence. If $\mathfrak{T}$ is a projectivity, then it is called a *correlation* of S. In either case, if $\mathfrak{T}$ is involutory, that is $\mathfrak{T}^2 = \mathfrak{I}$, where $\mathfrak{I}$ is the identity, then $\mathfrak{T}$ is called a *polarity* of S. Thus, if P and P' are points and π is a prime such that $P\mathfrak{T} = \pi$ and $\pi\mathfrak{T} = P'$, then, in a polarity, $P = P'$.

Suppose that $\mathfrak{T}$ is a reciprocity; then it is the product of an automorphic collineation σ and a projectivity of S to S' given by the matrix T. Write the image of x under σ as $x\sigma = \tilde{x}$, for any x in K. If $X = (x_0, \ldots, x_n)$, write $\tilde{X} = (\tilde{x}_0, \ldots, \tilde{x}_n)$, and if $T = (t_{ij})$ write $\tilde{T} = (\tilde{t}_{ij})$. Also T^* denotes the transpose of T; that is, $T^* = (t_{ji})$.

Suppose $\mathbf{P}(X)\mathfrak{T} = \boldsymbol{\pi}(V)$ and $\boldsymbol{\pi}(U)\mathfrak{T} = \mathbf{P}(Y)$. Then the first relation is given by $tV = \tilde{X}T$. Now, $\mathbf{P}(X)$ lies in $\boldsymbol{\pi}(U)$ if and only if $\boldsymbol{\pi}(V)$ contains $\mathbf{P}(Y)$; therefore $UX^* = 0 \Longleftrightarrow VY^* = 0$. Hence

$$\tilde{U}\tilde{X}^* = 0 \Longleftrightarrow UX^* = 0 \Longleftrightarrow VY^* = 0 \Longleftrightarrow \tilde{X}TY^* = 0 \Longleftrightarrow YT^*\tilde{X}^* = 0.$$

So $\tilde{U} = sYT^*$ for some s in K and $sY = \tilde{U}T^{*^{-1}}$.

If $\mathfrak{T}$ is a correlation, these equations become $tV = XT$, $sY = UT^{*^{-1}}$. Suppose the reciprocity $\mathfrak{T}$ is a polarity; then

$$\mathbf{P}(X) \longmapsto \boldsymbol{\pi}(\tilde{X}T) \longmapsto \mathbf{P}(\tilde{\tilde{X}}\tilde{T}T^{*^{-1}}) = \mathbf{P}(X).$$

So $tX = \tilde{\tilde{X}}\tilde{T}T^{*^{-1}}$; hence $\tilde{\tilde{X}} = X$ and $\tilde{T}T^{*^{-1}} = tI$. There are two possibilities: either (a) $x\sigma = x$ for all x in K or (b) σ has period two; in case (b), put $x\sigma = \overline{x}$, $\tilde{X} = \overline{X}$, $\tilde{T} = \overline{T}$.

In a polarity $\mathfrak{T}$, if $\mathbf{P}(X)\mathfrak{T} = \boldsymbol{\pi}(V)$ and $\boldsymbol{\pi}(U)\mathfrak{T} = \mathbf{P}(Y)$, then $\boldsymbol{\pi}(V)$ is the *polar* (prime) of $\mathbf{P}(X)$ and $\mathbf{P}(Y)$ is the *pole* of $\boldsymbol{\pi}(U)$. Since $\mathfrak{T}^2 = \mathfrak{I}$, the converse is also true. If $\mathbf{P}(Y)$ lies in $\boldsymbol{\pi}(V)$, the polar of $\mathbf{P}(X)$, then $\mathbf{P}(X)$ lies in $\boldsymbol{\pi}(U)$, the polar of $\mathbf{P}(Y)$. In this case, $\mathbf{P}(X)$ and $\mathbf{P}(Y)$ are *conjugate* points, and $\boldsymbol{\pi}(U)$ and $\boldsymbol{\pi}(V)$ are *conjugate* primes. The point $\mathbf{P}(X)$ is *self-conjugate* if it lies in its own polar prime: the prime $\boldsymbol{\pi}(U)$ is *self-conjugate* if it contains its own pole.

Thus $\mathbf{P}(X)$ and $\mathbf{P}(Y)$ are conjugate if $VY^* = 0$; that is, $\tilde{X}TY^* = 0$. The self-conjugate points $\mathbf{P}(X)$ are given by $\tilde{X}TX^* = 0$.

Now the different types of polarities are examined.

I. *σ is the identity*

Then

$$TT^{*^{-1}} = tI \Longrightarrow T = tT^* \Longrightarrow T^* = tT \Longrightarrow T = t^2T.$$

Since T is non-singular, $t^2 = 1$. Also, $\mathbf{P}(X)$ is conjugate to $\mathbf{P}(Y)$ when $XTY^* = 0$.

(a) K has characteristic $p \neq 2$.

(1) $t = 1,\ T = T^*$.

$$\begin{aligned} XTY^* &= t_{00}x_0y_0 + t_{01}(x_0y_1 + x_1y_0) + \dots\ ; \\ XTX^* &= t_{00}x_0^2 + 2t_{01}x_0x_1 + \dots\ . \end{aligned}$$

In this case, $\mathfrak{T}$ is called an *ordinary polarity* or a *polarity with respect to a quadric.*

(2) $t = -1,\ T = -T^*$: so $t_{ii} = 0,\ t_{ij} = -t_{ji}$.

$$\begin{aligned} XTY^* &= \sum_{i<j} t_{ij}(x_iy_j - x_jy_i) \\ &= t_{01}(x_0y_1 - x_1y_0) + \dots\ ; \\ XTX^* &= 0. \end{aligned}$$

Hence every point $\mathbf{P}(X)$ is self-conjugate. Here, $\mathfrak{T}$ is called a *null polarity* or *symplectic polarity* or a *polarity with respect to a linear complex.* Since T is non-singular and skew-symmetric, n is odd.

(b) K has characteristic $p = 2$.

Now, $t = 1,\ T = T^*,\ t_{ij} = t_{ji}$.

(1) $t_{ii} = 0$, all i. This is similar to the case (a)(2).

$$\begin{aligned} XTY^* &= \sum_{i<j} t_{ij}(x_iy_j + x_jy_i) \\ &= t_{01}(x_0y_1 + x_1y_0) + \dots\ ; \\ XTX^* &= 0. \end{aligned}$$

Every point $\mathbf{P}(X)$ is self-conjugate. As for $p \neq 2$, the correlation $\mathfrak{T}$ is a *null polarity* or *symplectic polarity* or a *polarity with respect to a linear complex.* It only occurs for n odd.

(2) $t_{ii} \neq 0$ for some i.

$$\begin{aligned} XTY^* &= t_{00}x_0y_0 + t_{01}(x_0y_1 + x_1y_0) + \ldots ; \\ XTX^* &= \sum t_{ii}x_i^2 \\ &= \left(\sum \sqrt{t_{ii}}x_i\right)^2 . \end{aligned}$$

The self-conjugate points of $\mathfrak{T}$ therefore comprise a prime. Here, $\mathfrak{T}$ is called a *pseudo-polarity.*

II. *σ has period two*

Let $K' = \{x \in K \mid x\sigma = x\}$; so, for $K = GF(q)$, the field $K' = GF(\sqrt{q})$. In this case,

$$\overline{T}{T^*}^{-1} = tI \Longrightarrow \overline{T} = tT^* \Longrightarrow T = \overline{t}\overline{T}^* \Longrightarrow T = \overline{t}tT.$$

Since T is non-singular, $\overline{t}t = 1$. So, with $K = GF(q)$, it follows from Section 1.5 (iii) that $t = \alpha^{i(\sqrt{q}-1)}$, where α is a primitive element of $\boldsymbol{\gamma}$ and $i \in \overline{\mathbf{N}}_{\sqrt{q}}$. Hence

$$\begin{aligned} t &= \alpha^{i\sqrt{q}}/\alpha^i \\ &= \lambda/\overline{\lambda} \text{ with } \lambda = \alpha^{i\sqrt{q}}. \end{aligned}$$

So $\overline{T} = (\lambda/\overline{\lambda})T^*$, whence $\overline{\lambda T} = (\lambda T)^*$. As λT gives the same polarity as T, it is only necessary to consider the case $t = 1$.

Thus $T^* = \overline{T}$; that is, $t_{ij} = \overline{t_{ji}}$ for all i, j. The points $\mathbf{P}(X)$ and $\mathbf{P}(Y)$ are conjugate when $\overline{X}TY^* = 0$.

$$\begin{aligned} \overline{X}TY^* &= \sum t_{ij}\overline{x_i}y_j \\ &= t_{00}\overline{x_0}y_0 + (t_{01}\overline{x_0}y_1 + \overline{t_{01}}\overline{x_1}y_0) + \ldots ; \\ \overline{X}TX^* &= t_{00}\overline{x_0}x_0 + (t_{01}\overline{x_0}x_1 + \overline{t_{01}}\overline{x_1}x_0) + \ldots . \end{aligned}$$

In this case, $\mathfrak{T}$ is called a *Hermitian* or *unitary polarity.*

To summarize, a polarity of $PG(n, K)$ is a function $\mathfrak{T}$ which transforms points to primes, primes to points, preserves incidence and is involutory. The five types are given in Table 1. For canonical forms for each polarity, see [3, Section 5.3].

Table 1: **Polarities in** $PG(n, K)$

Number	Name and which n	Characteristic p of K	Equations	Conditions on T	Locus of self-conjugate points
Ia(1)	Ordinary all n	$p \neq 2$	$tV = XT$ $sY = UT^{*-1}$	$t_{ij} = t_{ji}$	$XTX^* = 0$
Ia(2)	Null odd n	$p \neq 2$	$tV = XT$ $sY = UT^{*-1}$	$t_{ij} = -t_{ji}$ $t_{ii} = 0$	$PG(n, K)$
Ib(1)	Null odd n	$p = 2$	$tV = XT$ $sY = UT^{*-1}$	$t_{ij} = t_{ji}$ $t_{ii} = 0$	$PG(n, K)$
Ib(2)	Pseudo- all n	$p = 2$	$tV = XT$ $sY = UT^{*-1}$	$t_{ij} = t_{ji}$ $t_{kk} \neq 0$, some k	$\sum \sqrt{t_{ii}} x_i = 0$
II	Hermitian all n	p arbitrary $[K : K'] = 2$	$tV = \overline{X}T$ $sY = \overline{U}T^{*-1}$	$t_{ij} = \overline{t_{ji}}$ $t_{ii} \in K'$	$\overline{X}TX^* = 0$

2 Groups on the line

2.1 Quadrics and Hermitian varieties

The notation of [3, Section 2.7] is followed for a variety.

Let $Q(1,q)$ be the set of quadrics in $PG(1,q)$. Then

$$Q(1,q) = \{\mathbf{v}(a_0X_0^2 + a_{01}X_0X_1 + a_1X_1^2) \mid a_0, a_{01}, a_1 \in \boldsymbol{\gamma}\}.$$

So $|Q(1,q)| = q^2 + q + 1$. Then, under the action of $PGL(2,q)$ on $Q(1,q)$, there are three orbits:

(i) $q+1$ repeated points $\mathbf{v}((X_0 + tX_1)^2)$, $t \in \boldsymbol{\gamma}^+$;

(ii) $q(q+1)/2$ point pairs $\mathbf{v}((X_0 + sX_1)(X_0 + tX_1))$, $s,t \in \boldsymbol{\gamma}^+$, $s \neq t$; that is, hyperbolic quadrics $\mathcal{H}_1$;

(iii) $q(q-1)/2$ elliptic quadrics $\mathcal{E}_1$ containing no points and given by $\mathbf{v}(f)$, where $f(X_0, X_1)$ is monic and irreducible over $\mathbf{F}_q$.

The group of projectivities fixing $\mathcal{H}_1$ is $PGO_+(2,q)$ and the group of projectivities fixing $\mathcal{E}_1$ is $PGO_-(2,q)$. Hence

$$\begin{aligned} |PGO_+(2,q)| &= |PGL(2,q)|/[q(q+1)/2] = 2(q-1); \\ |PGO_-(2,q)| &= |PGL(2,q)|/[q(q-1)/2] = 2(q+1). \end{aligned}$$

In fact, if $\mathcal{H}_1 = \mathbf{v}(X_0X_1)$, its group of projectivities is

$$G(\mathcal{H}_1) = \left\{ \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & t \\ 1 & 0 \end{bmatrix} \,\middle|\, t \in \gamma_0 \right\}.$$

When q is odd and $\mathcal{E}_1 = \mathbf{v}(X_0^2 - \nu X_1^2)$ with ν a non-square, the group is

$$G(\mathcal{E}_1) = \left\{ \begin{bmatrix} 1 & t \\ \nu t & 1 \end{bmatrix}, \begin{bmatrix} 1 & t \\ -\nu t & -1 \end{bmatrix} \,\middle|\, t \in \boldsymbol{\gamma}^+ \right\}.$$

When q is even and $\mathcal{E}_1 = \mathbf{v}(X_0^2 + X_0X_1 + \delta X_1^2)$ with δ of trace one, the group is

$$G(\mathcal{E}_1) = \left\{ \begin{bmatrix} 1 & t \\ \delta t & t+1 \end{bmatrix}, \begin{bmatrix} 1 & t \\ 1+\delta t & 1 \end{bmatrix} \,\middle|\, t \in \boldsymbol{\gamma}^+ \right\}.$$

An elliptic quadric may be considered as comprising a pair of points of $PG(1,q^2)$ conjugate over $GF(q)$. So, with $f = a_0X_0^2 + a_{01}X_0X_1 + a_1X_1^2$, if $\mathcal{E}_1 = \mathbf{v}(f)$, then $f = a_0(X_0 - \alpha X_1)(X_0 - \alpha^q X_1)$ where $\alpha \in \mathbf{F}_{q^2} \backslash \mathbf{F}_q$.

The q^2+1 points of $PG(1,q^2)$ fall into two sets:

(i) $q+1$ in a subgeometry $PG(1,q)$;

(ii) $q^2 - q$ in a $PG(1,q^2)\backslash PG(1,q)$ comprising $q(q-1)/2$ conjugate pairs.

With q a square, let $U(1,q)$ be the set of Hermitian varieties in $PG(1,q)$. Then

$$U(1,q) = \{\mathbf{v}(a_0\overline{X}_0X_0 + b\overline{X}_0X_1 + \overline{b}X_0\overline{X}_1 + a_1\overline{X}_1X_1) \,|\, a_0, a_1 \in \mathbf{F}_{\sqrt{q}},\ b \in \mathbf{F}_q\},$$

where $\overline{x} = x^{\sqrt{q}}$. So $|U(1,q)| = (q+1)(\sqrt{q}+1)$. By [3, Lemma 5.2], if $\mathcal{F} \in U(1,q)$, then $\mathcal{F} \sim \mathcal{V} = \mathbf{v}(\overline{X}_0X_0 + e\overline{X}_1X_1)$, where $e = 0$ or 1. When $e = 0$, then $\mathcal{V}$ comprises the single point $\mathbf{U}_1$. When $e = 1$, then the non-singular $\mathcal{V} = \mathcal{U}_1 = \mathbf{v}(\overline{X}_0X_0 + \overline{X}_1X_1)$. By [3, Section 1.5(v)], the equation $x^{\sqrt{q}+1} = -1$ has $\sqrt{q}+1$ solutions in $\mathbf{F}_q$. So $\mathcal{U}_1$ comprises $\sqrt{q}+1$ points. Thus, under the action of $PGL(2,q)$, the set $U(1,q)$ has two orbits:

(i) $q+1$ points, each counted $\sqrt{q}+1$ times;

(ii) $\sqrt{q}(q+1)$ varieties $\mathcal{U}_1$, each comprising $\sqrt{q}+1$ points.

Hence

$$|PGU(2,q)| = |PGL(2,q)|/[\sqrt{q}(q+1)] = \sqrt{q}(q-1).$$

It should be noted that in both $Q(1,q)$ and $U(1,q)$, the variety $\mathbf{v}(0)$, that is, the whole line $PG(1,q)$, has not been included.

Lemma 2.1 *The rational points of a Hermitian variety $\mathcal{U}_{1,q}$ form a subline $PG(1,\sqrt{q})$ and conversely.*

Proof: By [3, Section 1.5(v)], there exists α in $\mathbf{F}_q$, q square, such that $\alpha^{\sqrt{q}-1} = -1$, that is, $\overline{\alpha} = -\alpha$. Again from [3], by Theorem 5.7 and Corollary 5.4,

$$\begin{aligned} \mathcal{U}_1 &= \mathbf{v}(\overline{X}_0X_0 + \overline{X}_1X_1) \\ &\sim \mathbf{v}(\alpha\overline{X}_0X_1 + \overline{\alpha}X_0\overline{X}_1) \\ &= \mathbf{v}(X_0X_1(X_0^{\sqrt{q}-1} - X_1^{\sqrt{q}-1}) \\ &= \{\mathbf{U}_0, \mathbf{U}_1\} \cup \{\mathbf{P}(t,1) \,|\, t \in GF(\sqrt{q})\backslash\{0\}\} \\ &= PG(1,\sqrt{q}). \end{aligned}$$

□

Corollary 2.2 *For q square,*

(i) $PGU(2,q) \cong PGL(2,\sqrt{q})$;

(ii) $PSU(2,q) \cong PSL(2,\sqrt{q})$.

Corresponding to $\mathcal{U}_1$, for q square, and to $\mathcal{H}_1$ and $\mathcal{E}_1$, for q odd, are the respective polarities. In the Hermitian case, the polar pairs of points of $PG(1,q)\backslash\mathcal{U}_1$ are the conjugate pairs when $\mathcal{U}_1$ is considered as $PG(1,q)$. The polarities for $\mathcal{H}_1$ and $\mathcal{E}_1$ are discussed below.

It remains to consider a null polarity for any q and a pseudo-polarity for q even. A null polarity has bilinear form $X_0Y_1 - X_1Y_0$, and is therefore the identity mapping. For a pseudo-polarity, $X_0Y_0 + X_0Y_1 + X_1Y_0$ is the canonical form. It has the one self-polar point $\mathbf{P}(0,1)$.

Lemma 2.3 (i) $PGSp(2,q) = PGL(2,q)$;

(ii) $PGPs^*(2,q) \cong (\mathbf{Z}_2)^h$, *where* $q = 2^h$.

Proof: (i) Since the only null polarity is the identity, every projectivity fixes it.

(ii) The projectivities commuting with the canonical pseudo-polarity are those with matrix $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$, $t \in \boldsymbol{\gamma}$. Hence they form a group isomorphic to the additive group of $\boldsymbol{\gamma}$. □

Corollary 2.4 *There are* $q^2 - 1$ *pseudo-polarities on* $PG(1,q)$.

2.2 The projective group

From [3, Section 6.1], $PGL(2,q)$ acts sharply triply transitively on $PG(1,q)$, and has order $q(q^2-1)$. The number $e(2,q)$ of conjugacy classes of $PGL(2,q)$ will now be calculated; this is the number of distinct projectivities of $PG(1,q)$ independently of the coordinate system.

Firstly, the number $E(2,q)$ of conjugacy classes of $GL(2,q)$ is calculated. In Table 2, for each canonical matrix T with a distinct symbol as in [3, Section 2.4], the elementary divisors of $XI - T$, each of which is the power of an irreducible polynomial, are listed with any special conditions and the number of distinct forms with this symbol. So

$$\begin{aligned} E(2,q) &= 2(q-1) + \mathbf{c}(q-1,2) + N(2,q) \\ &= 2(q-1) + (q-1)(q-2)/2 + q(q-1)/2 \\ &= q^2 - 1, \end{aligned}$$

where $N(2,q)$ is the number of monic, binary irreducible quadratics over $\mathbf{F}_q$.

The elementary divisors for projectivities can now be listed as in Table 3. To count the number of distinct types, it should be noted that the set of elementary divisors $F_1(X), \ldots, F_r(X)$ gives the same projectivity as $F_1(X/t), \ldots, F_r(X/t)$ for t in $\boldsymbol{\gamma}_0$. The cases of q even (Table 4) and q odd (Table 5) need to be distinguished. Here $o(t)$ is the order of the element t. So, for q even,

$$e(2,q) = 1 + (q-1)/2 + 1 + N(2,q)/(q-1) = 1 + (q-2)/2 + 1 + q/2 = q+1.$$

In this case, $e(2,q) = E(2,q)/(q-1)$.

For q odd, $e(2,q) = 1 + 1 + (q-3)/2 + 1 + 1 + (q-1)/2 = q+2$.

Theorem 2.5 (i) $E(2,q) = q^2 - 1$; (ii) $e(2,q) = q + (q-1,2)$.

Let $\mathfrak{T} = \mathbf{M}(T)$ be a projectivity given by $Y = XT$ with $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. In non-homogeneous coordinates $s = y_0/y_1$ and $t = x_0/x_1$, this becomes

$$bst + ds - at - c = 0, \tag{2.1}$$

with $ad - bc \neq 0$. When $a + d = 0$, so that (2.1) becomes

$$bst + d(s + t) - c = 0, \tag{2.2}$$

then $\mathfrak{T}$ is called an *involution*. So an involution has order one or two, and is accordingly called *improper* or *proper*.

A proper involution has two, one, or no fixed points as

$$bt^2 + 2dt - c = 0, \tag{2.3}$$

has two, one, or no solutions in $\mathbf{F}_q$; it is respectively called *hyperbolic*, *parabolic*, or *elliptic*. Since, on a line, a prime is the same thing as a point, each proper involution must be a polarity and, conversely, each polarity must be an involution, not necessarily proper. From (2.2), a proper involution is determined by two pairs of corresponding points.

For q odd, there are two types of proper involution; the corresponding matrices are

$$T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ \nu & 0 \end{bmatrix}.$$

In non-homogeneous coordinates, the equations are

$$s = -t, \quad s = \nu/t.$$

The involution $s = -t$ has fixed points $t = 0$ and $t = \infty$, and is therefore hyperbolic. Since, for any pair of corresponding points, the coordinates s and t satisfy $s + t = 0$, the pair is harmonically separated by the fixed points, [3, Section 6.1]. The involution $s = \nu/t$ has no fixed points and is therefore elliptic. These hyperbolic and elliptic involutions are nothing other than the polarities determined by the respective hyperbolic and elliptic quadrics; namely, $\mathcal{H}_1 = \mathbf{v}(X_0X_1)$ and $\mathcal{E}_1 = \mathbf{v}(X_0^2 - \nu X_1^2)$.

Table 2: **Conjugacy classes of** $GL(2, q)$

Symbol	Elementary divisors	Conditions	Number
$[(1,1)1]$	$X - t,\ X - t$	$t \in \boldsymbol{\gamma}_0$	$q - 1$
$[(1)1, (1)1]$	$X - t_0,\ X - t_1$	$t_i \in \boldsymbol{\gamma}_0,\ t_0 \neq t_1$	$\mathbf{c}(q - 1, 2)$
$[(2)1]$	$(X - t)^2$	$t \in \boldsymbol{\gamma}_0$	$q - 1$
$[(1)2]$	$X^2 - a_1X - a_0$		$N(2, q)$

Table 3: **Conjugacy classes of** $PGL(2,q)$

Symbol	Elementary divisors	Conditions
$[(1,1)1]$	$X-1,\ X-1$	
$[(1)1,(1)1]$	$X-1,\ X-t$	$t \in \boldsymbol{\gamma},\ t \neq 0,1$
$[(2)1]$	$(X-1)^2$	
$[(1)2]$	$X^2-a_1X-a_0$	$a_1=0$ or $a_0=1$

Table 4: **Conjugacy classes of** $PGL(2,q)$, q **even**

Symbol	Elementary divisors	Conditions	Order of projectivity	Number of non-conjugate projectivities
$[(1,1)1]$	$X+1,\ X+1$		1	1
$[(1)1,(1)1]$	$X+1,\ X+t$	$t \in \boldsymbol{\gamma}\backslash\{0,1\}$	$o(t)$	$(q-2)/2$
$[(2)1]$	$(X+1)^2$		2	1
$[(1)2]$	X^2+a_1X+1	root α in $\mathbf{F}_{q^2}$ with subexponent m	m	$N(2,q)/(q-1)$

Table 5: **Conjugacy classes of** $PGL(2,q)$, q **odd**

Symbol	Elementary divisors	Conditions	Order of projectivity	Number of non-conjugate projectivities
$[(1,1)1]$	$X-1,\ X-1$		1	1
$[(1)1,(1)1]$	$X-1,\ X+1$		2	1
$[(1)1,(1)1]$	$X-1,\ X-t$	$t^3 \neq t$	$o(t)$	$(q-3)/2$
$[(2)1]$	$(X-1)^2$		p	1
$[(1)2]$	$X^2-\nu$	ν non-square	2	1
$[(1)2]$	X^2-X-a_0	root α in $\mathbf{F}_{q^2}$ with subexponent $m>2$	m	$(q-1)/2$

For q even, there is just one type of proper involution. It has the symbol $[(2)1]$ and matrix

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

In non-homogeneous coordinates, its equation is

$$s = t + 1.$$

There is just the one fixed point $t = \infty$, and the involution is therefore parabolic. It is, in fact, a pseudo-polarity with bilinear form $X_1Y_1 + X_0Y_1 + X_1Y_0$.

Lemma 2.6 *On $PG(1,q)$ the number of involutions is q^2 :*

(i) *when q is even, q^2-1 are parabolic and one is the identity, the only improper involution;*

(ii) *when q is odd, $q(q+1)/2$ are hyperbolic and $q(q-1)/2$ are elliptic.*

Proof: The possible types for q odd and even follow from the above analysis of canonical forms or, equally well, from (2.3). For q even, all points are fixed when $b = c = 0$, and so by (2.2) the involution is the identity; otherwise, there is just the one fixed point $t = \sqrt{c/b}$. For q odd, the involution is hyperbolic or elliptic as $\Delta = d^2 + bc$ is a square or not; the discriminant Δ cannot be zero as otherwise Δ would not be bijective.

The number of involutions is

$$|\{\mathbf{P}(b,d,c) \mid d^2 + bc \neq 0\}| = |PG(2,q)\backslash\mathcal{P}_2|,$$

the number of points in the plane off the conic, which is $(q^2 + q + 1) - (q + 1) = q^2$.

For q even, the only improper involution is the identity. The other $q^2 - 1$ involutions are parabolic; alternatively, each is a pseudo-polarity.

For q odd, there are as many hyperbolic and elliptic involutions as corresponding quadrics. □

Lemma 2.7 *In $PG(2,q)$, q even and $q \geq 4$, each of the three proper involutions determined by a tetrad P_1, P_2, P_3, P_4 of points has the same fixed point P.*

Proof: If $P_1\mathfrak{T} = P_2$ and $P_3\mathfrak{T} = P_4$ in an involution $\mathfrak{T}$ given by (6.8), then, if P_i has coordinate t_i,

$$\begin{aligned} bt_1t_2 + d(t_1 + t_2) + c &= 0, \\ bt_3t_4 + d(t_3 + t_4) + c &= 0, \end{aligned}$$

whence

$$\lambda b = t_1 + t_2 + t_3 + t_4,\ \ \lambda d = t_1t_2 + t_3t_4,\ \ \lambda c = t_1t_2t_3 + t_1t_2t_4 + t_1t_3t_4 + t_2t_3t_4.$$

The fixed point P has parameter $t = \sqrt{c/b}$. As this is invariant under any permutation of the t_i, the lemma is proved. □

In this lemma, P is called the *associated* point of the tetrad $\{P_1, P_2, P_3, P_4\}$.

Corollary 2.8 *The coordinate α of the associated point of the tetrad $\mathcal{T}$ is as follows:*

(i) *when* $\mathcal{T} = \{t_1, t_2, t_3, t_4\}$,

$$\alpha^2 = (t_1 + t_2 + t_3 + t_4)/(t_1t_2t_3 + t_1t_2t_4 + t_1t_3t_4 + t_2t_3t_4);$$

(ii) *when* $\mathcal{T} = \{\infty, 0, 1, r\}$, *then* $\alpha = \sqrt{r}$.

Lemma 2.9 *If* $\mathbf{h}(P_1, P_2; P_3, P_4)$, *then the involution* $\mathfrak{T}$ *with pairs* $\{P_1, P_2\}$ *and* $\{P_3, P_4\}$ *is hyperbolic or elliptic as* $q \equiv 1$ *or* $q \equiv -1 \pmod 4$.

Proof: If P_1, P_2, P_3, P_4 have respective coordinates $\infty,\ 0,\ 1,\ -1$, then $\mathfrak{T}$ is given by $st+1 = 0$. So the fixed points are given by $t^2+1 = 0$. Hence $\mathfrak{T}$ is hyperbolic or elliptic as -1 is a square or not; so the result follows. □

3 Orders of and isomorphisms among the semi-linear groups

3.1 Definitions

(i) The groups $DX(n,q)$ are defined for $n \geq 2$, where

$$\begin{aligned} D &= I,\ S,\ G,\ \Gamma,\ \Gamma S,\ P,\ PS,\ PG,\ P\Gamma,\ P\Gamma S; \\ X &= L,\ O,\ O_+,\ O_-,\ U,\ Sp,\ Ps,\ Ps^*. \end{aligned}$$

For $D = I, S, G, \Gamma, \Gamma S$, the group $DX(n,q)$ is a group of semi-linear transformations in $V(n,q)$. For $D = P, PS, PG, P\Gamma, P\Gamma S$, the group $DX(n,q)$ is a group of collineations in $PG(n-1,q)$. The symbol X refers to the form (quadratic, Hermitian, or bilinear) involved. In particular, the full linear and semi-linear groups of varieties and polarities in $V(n,q)$ are given by the respective rows $GX(n,q)$ and $\Gamma X(n,q)$ in Table 6. The full projective and collineation groups of varieties or polarities in $PG(n-1,q)$ are given by the respective rows $PGX(n,q)$ and $P\Gamma X(n,q)$.

(ii) $IX(n,q) = X(n,q)$.

$X(n,q)$ = group of linear transformations leaving invariant the canonical form specified in the table.

$SX(n,q)$ = subgroup of $X(n,q)$ of linear transformations with determinant one.

$S'X(n,q) = SX(n,q)'$ = commutator subgroup of $SX(n,q)$.

$GX(n,q)$ = group of linear transformations leaving invariant the canonical form up to a scalar multiple.

$\Gamma X(n,q)$ = group of semi-linear transformations leaving invariant the canonical form up to an automorphism of $\boldsymbol{\gamma} = \mathbf{F}_q$ and a scalar multiple.

$\Gamma SX(n,q)$ = group of semi-linear transformations that are a product of an element of $SX(n,q)$ and an automorphism of $\boldsymbol{\gamma}$.

(iii) The groups $DX(n,q)$ beginning with the symbol P are the corresponding projective groups.

The centre of $\Gamma L(n,q)$ is $Z = \{\lambda I \mid \lambda \in \gamma_0\}$, where I is the identity of $\Gamma L(n,q)$. Then $PX, PSX, PGX, P\Gamma X, P\Gamma SX$ are the respective canonical images of $X, SX, GX, \Gamma X, \Gamma SX$ under $\Gamma L(n,q) \longrightarrow \Gamma L(n,q)/Z$.
(iv) Elsewhere, the following notation is used:

$$\begin{array}{rclcrcl} \Gamma SX &=& \Sigma X, && P\Gamma SX &=& P\Sigma X, \\ S'O &=& \Omega, && PS'O &=& P\Omega, \\ S'O_+ &=& \Omega_+, && PS'O_+ &=& P\Omega_+, \\ S'O_- &=& \Omega_-, && PS'O_- &=& P\Omega_-, \end{array}$$

with the lower indices + and − often written as upper indices.
(v) Commonly, but not here, when q is even, the orthogonal groups $SO_+(n,q)$ and $SO_-(n,q)$ are the kernels not of the determinant map, but taken with respect to the Dickson or Arf invariant. In that case, $|SO_\pm(n,q)| = \frac{1}{2}|O_\pm(n,q)|$.

3.2 Isomorphisms proved in the text

$\mathbf{S}_3 \cong PGL(2,2) \cong PSL(2,2)$	Section 6.4(i)
$\mathbf{A}_4 \cong PSL(2,3)$	Section 6.4(ii)
$\mathbf{S}_4 \cong PGL(2,3)$	Section 6.4(ii)
$\mathbf{A}_5 \cong PGL(2,4) \cong PSL(2,4)$	Section 6.4(iii)
$\mathbf{A}_5 \cong PSL(2,5)$	Section 6.4(iv)
$\mathbf{S}_5 \cong P\Gamma L(2,4)$	Section 6.4(iii)
$\mathbf{S}_5 \cong PGL(2,5)$	Section 6.4(iv)
$\mathbf{A}_6 \cong PSL(2,9)$	Section 6.4(vii)
$\mathbf{S}_6 \cong P\Gamma SL(2,9)$	Section 6.4(vii)
$PGL(3,2) \cong PSL(3,2) \cong PSL(2,7)$	Section 6.4(v)
$PGL(2,q) \cong PGSp(2,q)$	Lemma 6.4(i)
$PGL(2,\sqrt{q}) \cong PGU(2,q)$	Corollary 6.3(i)
$PSL(2,\sqrt{q}) \cong PSU(2,q)$	Corollary 6.3(i)
$PGPs^*(2,2^h) \cong (\mathbf{Z}_2)^h$	Lemma 6.4(ii)
$PGL(2,q) \cong PGO(3,q)$	Corollary 7.14
$PGL(2,q) \cong PGPs(3,q)$	Lemma 8.20

3.3 Table of group orders

In Tables 6a and 6b, the orders of all the groups $DX(n,q)$ are given for $q = p^h$ and $n \geq 2$. The orders are the table entries multiplied by the factor F given for each column, except where $|\,n,q\,|$ gives the specific order of $DX(n,q)$ for certain small n and q. Also, (n_1,n_2) is the greatest common divisor of n_1 and n_2. With $\epsilon = 1$ or -1,

$$\lambda_\epsilon(m,r) = r^{m(m-1)/2} \prod_{i=1}^{m} (r^i - \epsilon^i).$$

Table 6a: **Orders of the semi-linear groups**

	$X:$	L	O	O_+	O_-
	$F:$	$(q-1)^{-1}\times$	$q^{(n-1)/2}\times$	$q^{n-2}(q^{n/2}-1)\times$	$q^{n-2}(q^{n/2}+1)\times$
		$\lambda_1(n,q)$	$\lambda_1((n-1)/2,q^2)$	$\lambda_1((n-2)/2,q^2)$	$\lambda_1((n-2)/2,q^2)$
D					
I		$q-1$	$(q-1,2)$	2	2
S		1	1	$(q,2)$	$(q,2)$
S'		1	$(q-1,2)^{-1}$	$(q-1,2)^{-1}$	$(q-1,2)^{-1}$
		$\vert 2,2\vert=3$	$\vert 3,2\vert=3$	$\vert 4,2\vert=18$	
		$\vert 2,3\vert=8$	$\vert 5,2\vert=360$	$\vert 2,q\vert=1(q\text{odd})$	
G		$q-1$	$q-1$	$2(q-1)$	$2(q-1)$
Γ		$h(q-1)$	$h(q-1)$	$2h(q-1)$	$2h(q-1)$
ΓS		h	h	$h(q,2)$	$h(q,2)$
P		1	1	$(q,2)$	$(q,2)$
PS		$(n,q-1)^{-1}$	1	$2^{(-1)^q}$	$2^{(-1)^q}$
PS'		$(n,q-1)^{-1}$	$(q-1,2)^{-1}$	$(q^{n/2}-1,4)^{-1}$	$(q^{n/2}+1,4)^{-1}$
		$\vert 2,2\vert=3$	$\vert 3,2\vert=3$	$\vert 4,2\vert=18$	
		$\vert 2,3\vert=4$	$\vert 5,2\vert=360$	$\vert 2,q\vert=1(q\text{odd})$	
PG		1	1	2	2
$P\Gamma$		h	h	$2h$	$2h$
$P\Gamma S$		$h(n,q-1)^{-1}$	h	$2^{(-1)^q}h$	$2^{(-1)^q}h$
n		all	odd	even	even
q		all	all	all	all
Invariant		$PG(n-1,q)$	$\mathcal{P}_{n-1}$	$\mathcal{H}_{n-1}$	$\mathcal{E}_{n-1}$

Table 6b: **Orders of the semi-linear groups**

U	Sp	Ps	Ps^*	$:X$	
$(\sqrt{q}+1)^{-1}\times$	$q^{n/2}\times$	$q^{(n-1)/2}\times$	$q^{(3n-4)/2}\times$	$:F$	
$\lambda_{-1}(n,\sqrt{q})$	$\lambda_1(n/2,q^2)$	$\lambda_1((n-1)/2,q^2)$	$\lambda_1((n-2)/2,q^2)$		
					D
$\sqrt{q}+1$	1	1	1		I
1	1	1	1		S
1	1	1	1		S'
$\|2,4\|=3$	$\|2,2\|=3$	$\|3,2\|=3$	$\|2,q\|=1$		
$\|2,9\|=8$	$\|2,3\|=8$	$\|5,2\|=360$	$\|4,2\|=12$		
$\|3,4\|=54$	$\|4,2\|=360$		$\|6,2\|=11520$		
$q-1$	$q-1$	$q-1$	$q-1$		G
$h(q-1)$	$h(q-1)$	$h(q-1)$	$h(q-1)$		Γ
h	h	h	h		ΓS
1	$(q-1,2)^{-1}$	1	1		P
$(n,\sqrt{q}+1)^{-1}$	$(q-1,2)^{-1}$	1	1		PS
$(n,\sqrt{q}+1)^{-1}$	$(q-1,2)^{-1}$	1	1		PS'
$\|2,4\|=3$	$\|2,2\|=3$	$\|3,2\|=18$	$\|2,q\|=1$		
$\|2,9\|=4$	$\|2,3\|=4$	$\|5,2\|=360$	$\|4,2\|=12$		
$\|3,4\|=54$	$\|4,2\|=360$		$\|6,2\|=11520$		
1	1	1	1		PG
h	h	h	h		$P\Gamma$
$h(n,\sqrt{q}+1)^{-1}$	$h(q-1,2)^{-1}$	h	h		$P\Gamma S$
all	even	odd	even		n
square	all	even	even		q
$\mathcal{U}_{n-1}$	null polarity	pseudo-polarity	pseudo-polarity		Invariant

As an illustration, let q be odd and $n = 2$. Take $\mathcal{H}_1 = \mathbf{v}(X_0X_1)$. Then the orders of some of the groups are as in the following table:

G	$O_+(2,q)$	$SO_+(2,q)$	$GO_+(2,q)$	$PO_+(2,q)$	$PSO_+(2,q)$	$PGO_+(2,q)$
$\mid G \mid$	$2(q-1)$	$q-1$	$2(q-1)^2$	$q-1$	$\frac{1}{2}(q-1)$	$2(q-1)$

The groups are as follows, where $t \sim -t$ indicates that these give equivalent group elements:

$$
\begin{array}{rcl}
O_+(2,q) & = & \left\{ \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \begin{bmatrix} 0 & t \\ t^{-1} & 0 \end{bmatrix} \middle| t \in \mathbf{F}_q \backslash \{0\} \right\}, \\
SO_+(2,q) & = & \left\{ \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \middle| t \in \mathbf{F}_q \backslash \{0\} \right\}, \\
GO_+(2,q) & = & \left\{ \begin{bmatrix} s & 0 \\ 0 & t \end{bmatrix}, \begin{bmatrix} 0 & s \\ t & 0 \end{bmatrix} \middle| s, t \in \mathbf{F}_q \backslash \{0\} \right\}, \\
PO_+(2,q) & = & \left\{ \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \begin{bmatrix} 0 & t \\ t^{-1} & 0 \end{bmatrix} \middle| t \in \mathbf{F}_q \backslash \{0\},\ t \sim -t \right\}, \\
PSO_+(2,q) & = & \left\{ \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \middle| t \in \mathbf{F}_q \backslash \{0\},\ t \sim -t \right\}, \\
PGO_+(2,q) & = & \left\{ \begin{bmatrix} 1 & 0 \\ 0 & t \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ t & 0 \end{bmatrix} \middle| s, t \in \mathbf{F}_q \backslash \{0\} \right\}.
\end{array}
$$

References

[1] P. J. Cameron. *Projective and Polar Spaces*, volume 13 of *QMW Maths Notes*. University of London, London, 1991, 147 pp.

[2] J. A. Dieudonné. *La Géometrie des Groupes Classiques*. Springer, Berlin, third edition, 1971, 129 pp.

[3] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second edition, Oxford University Press, Oxford, 1998.

[4] J. W. P. Hirschfeld. *Finite Projective Spaces of Three Dimensions*. Oxford University Press, Oxford, 1985, 316 pp.

[5] J. W. P. Hirschfeld and J. A. Thas. *General Galois Geometries*. Oxford University Press, Oxford, 1991, 407 pp.

[6] D. E. Taylor. *The Geometry of the Classical Groups*. Heldermann, Berlin, 1992, 229 pp.

[7] B. L. van der Waerden. *Gruppen von Linearen Transformationen*. Springer, Berlin, 1935, 91 pp. (Chelsea, 1948).