

PART I. $SL_2(\mathbb{F}_q)$

Reference.
My book on $SL_2(\mathbb{F}_q)$

Chapter 1. Structure

Chapter 2. Harish-Chandra theory

Chapter 3. Introduction to ℓ -adic cohomology

Chapter 4. Deligne-Lusztig theory for $SL_2(\mathbb{F}_q)$: study of Drinfeld curve $x y^q - y x^q = 1$.

- p prime number $\mathbb{F}_p \subset \mathbb{F}$ alg. closed
- q a power of p $\mathbb{F}_q \subset \mathbb{F}$
- $F: \mathbb{F} \rightarrow \mathbb{F}$
 $x \mapsto x^q$ Frobenius auto.
(trivial on $\mathbb{F}_q$)

$$\tilde{G} = GL_2(\mathbb{F}_q) = \{ g \in Mat_2(\mathbb{F}_q) \mid \det(g) \neq 0 \}$$

$\cup$

$$G = SL_2(\mathbb{F}_q) = \{ g \in Mat_2(\mathbb{F}_q) \mid \det(g) = 1 \}$$

$$G \triangleleft \tilde{G}$$

Chapter 1. Structure

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\tilde{Z} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^\times \right\} \subset \tilde{G}$$

$$Z = \tilde{Z} \cap G$$

$$= \{ \pm I_2 \}$$

$$|Z| = \begin{cases} 2 & \text{if } p \text{ is odd} \\ 1 & \text{if } p = 2 \end{cases}$$

1. A. Natural action.

Let $V = \mathbb{F}_q \times \mathbb{F}_q$ as an $\mathbb{F}_q$ -vector space

$$\mathbb{P}^1(\mathbb{F}_q) = \{ \text{lines in } V \}$$
$$= \{ [x; y] \mid x, y \in \mathbb{F}_q, (x, y) \neq (0, 0) \}$$

$\nearrow$

$\searrow$

$\mathbb{F}_q \cup \{ \infty \}$

$\cup$

$0 \mapsto [1; 0]$

$\frac{y}{x}$

$\infty \mapsto [0; 1]$

line $\mathbb{F}_q \cdot (x, y)$

$\tilde{G}$ acts linearly on V
so it acts on $\mathbb{P}^1(\mathbb{F}_q)$

Proposition 1.0. $\tilde{G}$ acts faithfully
on V , and $\tilde{Z}$ is the kernel of the
action on $\mathbb{P}^1(\mathbb{F}_q)$

Proposition 1.1. G acts transitively
on $V \setminus \{(0,0)\}$; so it acts
transitively on $\mathbb{P}^1(\mathbb{F}_q)$.

Proof. Let $(x, y) \in V \setminus \{(0,0)\}$

• If $y = 0$, then $x \neq 0$ and
 $(x, 0) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} (1, 0)$

• If $y \neq 0$, then $(x, y) = \begin{pmatrix} x & -y^{-1} \\ y & 0 \end{pmatrix} (1, 0)$ ■

1.3. Natural subgroups.

$$B = \text{Stab}_G([1; 0]) \quad \text{Borel subgroup}$$

$$= \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}$$

$$U = \text{Stab}_G(1, 0) \quad \text{Unipotent radical}$$

$$= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_q \right\} \triangleleft B$$

$$T = \text{Stab}_G(\underbrace{[1; 0]}_{\text{"0"}}) \cap \text{Stab}_G(\underbrace{[0; 1]}_{\text{"0"}})$$

$$= \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^\times \right\}$$

split torus

$$B = T \ltimes U$$

$$\begin{aligned} \bullet u: \mathbb{F}_q^\times &\xrightarrow{\sim} U \\ b &\longmapsto \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = u(b) \end{aligned}$$

$$\begin{aligned} \bullet d: \mathbb{F}_q^\times &\xrightarrow{\sim} T \\ a &\longmapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \end{aligned}$$

$$d(a) u(b) d(a)^{-1} = u(a^2 b)$$

$$(1.2) \quad |U| = q \quad ; \quad |T| = q-1$$

$$|B| = q(q-1)$$

$$|G| = q(q-1)(q+1)$$

$$|G| = |\mathbb{P}^1(\mathbb{F}_q)| \cdot |B|$$

$$\cdot s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} ; N = \langle T, s \rangle$$

Proposition 1.3.

$$(a) G = B \cup B \circ B \quad (\text{Bruhat decomposition})$$

$$(b) G = \langle U, sUs^{-1} \rangle$$

$$sUs^{-1} = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbb{F} \right\}$$

$$(c) s d(a) s^{-1} = d(a^{-1}) \quad \text{and} \quad s^2 = -I_2 \in T.$$

$$\text{so } T \triangleleft N \quad \text{and} \quad N/T \simeq \mathbb{Z}/2\mathbb{Z}$$

(RE. N is not a semidirect product if $p \neq 2$: exercise)

Proof. (a) Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$

$$\cdot \text{ If } c = 0 \text{ then } g \in B$$

$$\cdot \text{ If } c \neq 0, \text{ then}$$

$$s^{-1} \begin{pmatrix} 1 & -\frac{a}{c} \\ 0 & 1 \end{pmatrix} g \in B$$

$$\text{so } g \in U \circ B \subset B \circ B$$

$$(b) \text{ Let } H = \langle U, sUs^{-1} \rangle$$

$Bg(a), G = \langle U, T, s \rangle$
so it is sufficient to prove that

$$T \subset H \quad \text{and} \quad s \in H.$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = s = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \in H$$

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in H.$$

(c) is easy. ■

Corollary 1.4. (a) $Z = Z(G)$

$$(b) \text{ If } q > 3 \text{ then } D(G) = G$$

and G/Z is simple

$$\parallel$$

$$PSL_2(\mathbb{F}_q)$$

Proof. (a) $C_G \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \{ \pm I_2 \} \times U$

$$C_G \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \{ \pm I_2 \} \times sUs^{-1}$$

$$\text{so } Z(G) \subset \{ \pm I_2 \} \subset Z(G)$$

(b) Assume that $q > 3$.

So there exists $a \in \mathbb{F}_q^\times$ s.t. $a^2 \neq 1$.

$$[d(a), u(x)] = u((a^2 - 1)x) = \begin{pmatrix} 1 & (a^2 - 1)x \\ 0 & 1 \end{pmatrix}$$

Since $a^2 \neq 1$, every element of U is a commutator.

Similarly, $uUu^{-1} \subset D(G) \supset U$

By Prop. 1.3 (b), $D(G) = G$.

Let $H \triangleleft G$.

• If $H \subset B$, then $H \subset \bigcap_{g \in G} {}^g B = Z$ exercise

so $H = 1$ or Z .

• If $H \not\subset B$. Let $G_0 = HB$: subgroup of G because $H \triangleleft G$. It contains strictly B .

By Bruhat decomposition, $G = G_0$

Let $\pi: B \longrightarrow G/H$

π is surjective ($BH = G$)

$$\text{Ker } \pi = B \cap H$$

$$\text{We have } G/H \cong B/B \cap H$$

perfect
solvable

$$\Rightarrow G/H = 1; \text{ i.e. } H = G.$$

so G/Z is simple. ■

1.C. Non-split case.

$$d_2: \mathbb{F}_{q^2}^\times \hookrightarrow \tilde{G} = GL_2(\mathbb{F}_q)$$

$\downarrow \psi$
 F

$$\begin{cases} \det d_2(\xi) = \xi^{1+q} \\ \det F = -1 \end{cases} \quad (\text{see lecture 1})$$

Let μ_{q+1} denote the kernel

$$\begin{array}{ccc} \mathbb{F}_{q^2}^\times & \longrightarrow & \mathbb{F}_{q^{q+1}}^\times \\ x & \longmapsto & x_{q+1} \end{array}$$

(group of $(q+1)$ -th roots of unity)

$$d': \mu_{q+1} \hookrightarrow G$$

We denote by $T' = d'(\mu_{q+1})$

Let μ_{q+1} denote the kernel
of $\mathbb{F}_{q^2}^\times \xrightarrow{x} \mathbb{F}_{q^{q+1}}^\times$
(group of $(q+1)$ -th roots of unity)

$$d' : \mu_{q+1} \hookrightarrow G$$

We denote by $T' = d'(\mu_{q+1})$
(non-split torus)

$$\text{Let } \xi_0 \in \mathbb{F}_{q^2}^\times \text{ s.t. } \xi_0^{q+1} = -1$$

$$s' = d_2(\xi_0) F \in G$$

$$s' d'(\xi) s'^{-1} = d'(\xi^q) = d'(\xi^{-1})$$

$$\text{Let } N' = \langle T', s' \rangle$$

$$s'^2 = -I_2 \quad (\text{exercise})$$

$$(1.5) \quad T' \simeq \mathbb{Z}/(q+1)\mathbb{Z}$$

$$N'/T' \simeq \mathbb{Z}/2\mathbb{Z}$$

$$\text{Recall that } s^2 = -I_2$$

$$T \simeq \mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$$

$$N/T \simeq \mathbb{Z}/2\mathbb{Z}$$

$$\text{Summary. } |G| = q(q-1)(q+1)$$

$$Z = Z(G) = \{ \pm I_2 \}$$

$$D(G) = G \quad \text{if } q > 3$$

$$G/2 \text{ is simple if } q > 3$$

$$B = \underset{\substack{\uparrow \\ \text{split} \\ \text{torus}}}{T} \ltimes \underset{\substack{\uparrow \\ \text{unip.} \\ \text{radical}}}{U} \quad \text{Borel subgroup}$$

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in N_G(T)$$

$$N = \langle T, s \rangle \quad N/T \simeq \mathbb{Z}/2\mathbb{Z}$$

$$N' = \langle T', s' \rangle \quad N'/T' \simeq \mathbb{Z}/2\mathbb{Z}$$

$$s^2 = s'^2 = -I_2$$

$$G = B \cup B s B = \langle U, {}^s U \rangle = \langle U, s \rangle$$

Explicit s' ? see exercise 1.4 in my
book : explicit T' .

Exercise. Show $\tilde{G}$ acts triply transitively on $\mathbb{P}^1(\mathbb{F}_q)$

i.e. $\mathbb{P}^1 \ni (p_1, p_2, p_3) \in \mathbb{P}^1(\mathbb{F}_q)$
 $(p'_1, p'_2, p'_3) \in \mathbb{P}^1(\mathbb{F}_q)$
 s.t. $p_i \neq p_j, p'_i \neq p'_j \text{ for } i \neq j$
 then $\exists g \in \tilde{G}$ s.t.
 $(p'_1, p'_2, p'_3) = g \cdot (p_1, p_2, p_3)$

Show that G acts doubly transitively on $\mathbb{P}^1(\mathbb{F}_q)$, but does not act triply transitively (if $p \neq 2$).

1. D. Small values of q .

$$* q = 2: |G| = 1 \cdot 2 \cdot 3 = 6$$

$$Z = 1$$

$G/Z = G$ acts faithfully on $\mathbb{P}^1(\mathbb{F}_2)$

$$|\mathbb{P}^1(\mathbb{F}_2)| = 3$$

$$\hookrightarrow G \hookrightarrow \tilde{G}_3 = S_3$$

$SL_2(\mathbb{F}_2) \simeq \tilde{G}_3 \simeq S_3$ is solvable

$$* q = 3: |G| = 2 \cdot 3 \cdot 4 = 24$$

$$Z = \mathbb{Z}/2\mathbb{Z}$$

G/Z acts faithfully on $\mathbb{P}^1(\mathbb{F}_3)$

$$|\mathbb{P}^1(\mathbb{F}_3)| = 4$$

$$\hookrightarrow \frac{G}{Z} \hookrightarrow S_4$$

order 12

$PSL_2(\mathbb{F}_3) \simeq A_4$ is solvable

$$* q = 4: |G| = 3 \cdot 4 \cdot 5 = 60$$

G acts faithfully on $\mathbb{P}^1(\mathbb{F}_4)$

$$(Z = 1)$$

$$|\mathbb{P}^1(\mathbb{F}_4)| = 5$$

$$\hookrightarrow G \hookrightarrow S_5$$

$SL_2(\mathbb{F}_4) \simeq A_5$ is simple

* $q = 5$. $|G| = 4 \cdot 5 \cdot 6 = 120$

$|Z| = 2$

$\hookrightarrow G/Z \hookrightarrow S_6$ transitive subgroup

Fact. $PSL_2(\mathbb{F}_5) \cong A_5$ (exercise)

Theorem*. Let G be a simple group of order ≤ 1000 then

$G \cong PSL_2(\mathbb{F}_q)$ for $q \in \{4, 5, 7, 8, 9, 11\}$

$\downarrow$ 60 $\downarrow$ 60 $\downarrow$ 504 $\downarrow$ 360 $\downarrow$ 660
 $\downarrow$ 12 $\downarrow$ 12 $\downarrow$ 12 $\downarrow$ 12
 A_5 A_5 A_5 A_6
 $\downarrow$ 168
 $GL_3(\mathbb{F}_2)$

$G/Z \hookrightarrow S_{q+1} \xrightarrow{\text{sgn}} \{\pm 1\}$
 $\downarrow$ D
 A_{q+1} (for $q \geq 3$)

1.E. Conjugacy classes

Hyp. p is odd (i.e. q is odd)

Let $g \in G$

Let $X_g(X) \in \mathbb{F}_q[X]$ denote its characteristic polynomial:

$$X_g(X) = X^2 - \text{Tr}(g)X + 1$$

The "two" eigenvalues of g in $\mathbb{F}$ are of the form ξ, ξ^{-1} .

$\rightarrow$ If $\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, then $\xi^q \neq \xi$ is also an eigenvalue: $\xi^q = \xi^{-1}$, i.e. $\xi^{q+1} = 1$.
 and $g \sim d'(\xi) \sim d'(\xi)^{-1}$
 $\downarrow$ conjugate (not so easy)

$\rightarrow$ If $\xi \in \mathbb{F}_q^\times$ and $\xi \neq \xi^{-1}$ ($\xi \neq \pm 1$) then $g \sim d(\xi) \sim d(\xi)^{-1}$

$\rightarrow$ If $\xi = \pm 1$ then $g = \pm I_2$
 $\text{or } g \sim \begin{pmatrix} \xi & a \\ 0 & \xi \end{pmatrix} \sim \begin{pmatrix} \xi & a^2 \\ 0 & \xi \end{pmatrix} \quad \forall a \in \mathbb{F}_q^\times$

We fix $z_0 \in \mathbb{F}_q^\times$ which is not a square in $\mathbb{F}_q^\times$.

$$\text{Let } u_+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad u_- = \begin{pmatrix} 1 & z_0 \\ 0 & 1 \end{pmatrix}$$

Proposition 1.6. The following is a set of representatives of conjugacy classes of G :

$$2 \hookrightarrow \cdot I_2 \quad ; \quad -I_2$$

$$4 \hookrightarrow \cdot \pm u_{\pm}$$

$$\frac{q-3}{2} \hookrightarrow \cdot d(a), \quad a \in \mathbb{F}_q^\times \setminus \{\pm 1\} / \text{INVERSE}$$

$$\frac{q-1}{2} \cdot d'(\xi), \quad \xi \in \mu_{q+1} \setminus \{\pm 1\} / \text{INVERSE}$$

There are $q+4$ conjugacy classes.

Proof. See my book: have a look at table 1.1 for more informations. ■

Exercise. What happens if $p=2$?