Conjugacy classes of $GL_2(\mathbb{F}_p)$ $\quad p(p-1)^2(p+1)$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_p)$

char poly: $x^2 - (a+d)x + (ad-bc) = f(x)$

using rational canonical form let's observe possibilities of factoring $f(x)$

I. $f(x) = (x-\lambda_1)(x-\lambda_2)$ two distinct factors

so canonical form: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ one conjugacy class emerges for each choice of λ_1, λ_2

$\lambda_1, \lambda_2 \in \mathbb{F}_p^\times$ distinct $\Rightarrow \frac{(p-1)(p-2)}{2}$ classes each with cardinality: [see below]

II. $f(x) = (x-\lambda)^2$ one distinct linear factor

so min poly either $\underbrace{(x-\lambda)}$ or $\underbrace{(x-\lambda)^2}$

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \qquad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ ← in $SL_2(\mathbb{F}_p)$ this will split into 2 conj. classes b/c the thing which conjugates one into the other may not have det = 1 (think similar to $S_5 \to A_5$)

rational canonical form so matrices with the same decomp must be similar

why is it necessarily similar to this?

b/c $p-1$ choices for λ

so $p-1$ conj. classes $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ of cardinality: [see below]

and $p-1$ conj. classes $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ of cardinality: [see below]

III. $f(x) = x^2 - (a+d)x + (ad-bc)$ is irreducible over $F = \mathbb{F}_p$

so any matrix with this as their char poly will be similar

$$[T] = \begin{array}{cc} e_1 & Te_1 \\ \end{array}$$
$$[T] = \begin{pmatrix} 0 & -(ad-bc) \\ 1 & a+d \end{pmatrix} = \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$$

representative

$f(T)e = T^2 e - (a+d)Te + (ad-bc)e = 0$

$\Rightarrow T(Te) = (a+d)Te - (ad-bc)e$

How many choices for $f(x)$?

# of classes = # of irred polys of deg 2

b/c if α is a root then so is α^{-1}

$x^2 - tx + d$ irred $\Leftrightarrow$ no roots in $\mathbb{F}_p$

so if α is a root it is in $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^2}$ b/c has p^2 elems (b/c deg 2 extension)

so $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$ can't be in $\mathbb{F}_p$ b/c no roots in $\mathbb{F}_p$ the other root must be $\alpha^{-1} = \bar{\alpha}$

so $x^2 - tx + d = (x-\alpha)(x-\bar{\alpha})$

so $\frac{p^2-p}{2}$ choices for α divide by 2 b/c "2 to 1" map: $\mathbb{F}_{p^2} - \mathbb{F}_p \twoheadrightarrow \{\text{irred poly}\}$

$\alpha \longmapsto (x-\alpha)(x-\bar{\alpha})$

size of each class? Find centralizer of $T \in GL_2(\mathbb{F}_p)$, $T \sim \begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$

ring $\mathbb{F}_p[T] \cong \underbrace{\mathbb{F}_p[x]/(x^2-tx+d)}_{\text{is a field b/c } x^2-tx+d \text{ is irred}} \cong \mathbb{F}_{p^2}$ acts on V, which is dim = 1 over $\mathbb{F}_{p^2}$

so centralizer $= \{A : AT = TA\} = \{A : \underbrace{A \text{ is } \mathbb{F}_{p^2}\text{-linear}}_{\text{aka act on } V \text{ over } \mathbb{F}_{p^2}}\}$

which is one dim so just (a) with $a \in \mathbb{F}_{p^2}^\times$ (scalars) $\Rightarrow p^2-1$ choices

so size of each class is $\frac{p(p-1)^2(p+1)}{p^2-1} = p(p-1)$

In fact for any $T \in GL_2(\mathbb{F}_p)$ we can observe the ring $\mathbb{F}_p[T]$; let $f(x)$ be min poly of T. Then:

I. Split semisimple: $f(x) = (x-\lambda_1)(x-\lambda_2)$

so $\mathbb{F}_p[T] \cong \mathbb{F}_p[x]/(f(x)) = \mathbb{F}_p[x]/(x-\lambda_1) \times \mathbb{F}_p[x]/(x-\lambda_2) = \mathbb{F}_p \times \mathbb{F}_p$ ring with p^2 elems

II. Non semisimple: $f(x) = (x-\lambda)^2$

so $\mathbb{F}_p[T] \cong \mathbb{F}_p[x]/(x-\lambda)^2$

surjection: $\varphi : \mathbb{F}_p[x]/(x-\lambda)^2 \twoheadrightarrow \mathbb{F}_p[x]/(x-\lambda) \cong \mathbb{F}_p$

$\ker(\varphi) = (x-\lambda)$ ideal generated by $x - \lambda = \varepsilon$

$\Rightarrow \mathbb{F}_p[T] \cong \mathbb{F}_p[\varepsilon]$ s.t. $\varepsilon^2 = 0$ adjoin this nilpotent elem

$= \{a + b\varepsilon : a, b \in \mathbb{F}_p\}$ ring with p^2 elem

III. Nonsplit $\Rightarrow$ mod by irred poly gives a field (with p^2 elem)

$\mathbb{F}_p[T] \cong \mathbb{F}_{p^2}$

To find the size of each conj. class:

so $G = C_1 \sqcup \dots \sqcup C_k$ disjoint union of orbits / conj. classes

Recall G acts on itself via conjugation $\Rightarrow$ orbits of this action are conj. classes

$C_1 = \mathrm{orb}_G(x_1)$ where x_1 is the rep for conj. class C_1

orbit-stabilizer: $|G| = \underset{\{gx_1 \cdot g \in G\}}{|\mathrm{orb}_G(x_1)|}\ \underset{\{g\in G : g * x_1 = x_1\} = \{g \in G : gx_1 = x_1 g\}}{|\mathrm{stab}_G(x_1)|} = |C_1|\,|\mathrm{stab}_G(x_1)|$ so $|C_1|$ divides $|G| = p(p+1)(p-1)^2$

b/c action of G is conjugation

*stabilizer = centralizer for action of conjugation

$\Rightarrow |C_1| = |G| / |\mathrm{stab}_G(x_1)|$ so we want to find the size of the stabilizer/centralizer

Recall: central conjugacy classes form the center $Z(G) \le G$ subgroup

I. $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ centralizer?

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} a\lambda & a+b\lambda \\ c\lambda & c+d\lambda \end{pmatrix}$ ← equal $\Rightarrow$ $c=0$, $d=a$, b anything $\Rightarrow \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$ ($y \in \mathbb{F}_p$, $x \in \mathbb{F}_p^\times$) $\Rightarrow p(p-1)$ choices

$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a\lambda + c & \lambda b + d \\ c\lambda & d\lambda \end{pmatrix}$

so this conj. class has centralizer size: $p(p-1)$

Hence each class has cardinality: $(p-1)(p+1)$

II. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_2 b \\ \lambda_1 c & \lambda_2 d \end{pmatrix}$ ← equal $\Rightarrow$ a, d anything, $c = b = 0$ $\Rightarrow \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \Rightarrow (p-1)(p-1)$ choices ($x, y \in \mathbb{F}_p^\times$)

$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda_1 a & \lambda_1 b \\ \lambda_2 c & \lambda_2 d \end{pmatrix}$

so centralizer has size: $(p-1)^2$ $\Rightarrow$ card. of each class: $p(p+1)$

III. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix} = \begin{pmatrix} b & -aa_0 + ba_1 \\ d & -ca_0 + da_1 \end{pmatrix}$

$\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -ca_0 & -da_0 \\ a + ca_1 & b + da_1 \end{pmatrix}$

$b = -ca_0$, $-aa_0 + ba_1 = -da_0$, $d = a + ca_1$, $-ca_0 + \cancel{da_1} = b + \cancel{da_1}$ $\Rightarrow$ $b + ca_0 = 0$, $a_0(d-a) + ba_1 = 0$, $d - a - ca_1 = 0$, $b + ca_0 = 0$ $\Rightarrow \begin{cases} d - a = \frac{-ba_1}{a_0} = ca_1 \\ b + ca_0 = 0 \end{cases}$ (ok b/c $a_0 = \det \neq 0$)

only required to choose d and b and then you can solve for rest

$\Rightarrow \begin{pmatrix} d + \frac{ba_1}{a_0} & b \\ -b/a_0 & d \end{pmatrix}$

$\Rightarrow p^2 - 1$ ← can't both be 0 ($b, d \in \mathbb{F}_p$) so centralizer: $p^2 - 1 = (p-1)(p+1)$

Hence each class has cardinality: $p(p-1)$

so in total we have: conjugacy classes of $GL_2(\mathbb{F}_p)$

	central	non-semisimple	split regular semisimple	anisotropic regular semisimple (or nonsplit)
representative	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$	$\begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$
# of classes	$p-1$ $(\lambda \in \mathbb{F}_p^\times)$	$p-1$ $(\lambda \in \mathbb{F}_p^\times)$	$\frac{(p-1)(p-2)}{2}$ $\lambda_1, \lambda_2 \in \mathbb{F}_p^\times$	$\frac{1}{2}(p^2-p)$ $\in \mathbb{F}_p$
size of each class	1	$(p+1)(p-1)$	$p(p+1)$	$p(p-1)$
char poly	$(x-\lambda)^2$ min poly $(x-\lambda)$	$(x-\lambda)^2$	$(x-\lambda_1)(x-\lambda_2)$	$x^2 - tx + d = (x-\alpha)(x-\bar{\alpha})$ (irreducible) ← $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$

not a direct sum of simple spaces

class equation: $(p-1) + (p-1)(p+1)(p-1) + \frac{1}{2}p(p+1)(p-1)(p-2) + \frac{1}{2}p(p-1)(p^2-p)$

$= (p-1) + (p-1)^2(p+1) + \frac{1}{2}p(p+1)(p-1)(p-2) + \frac{1}{2}p^2(p-1)^2$

$= (p-1)\left[\cancel{1} + p^2 - \cancel{1} + \frac{1}{2}p(p+1)(p-2) + \frac{1}{2}p^2(p-1)\right]$

$= (p-1)\left[p^2 + \frac{1}{2}\left[p^3 - p^2 - 2p + p^3 - p^2\right]\right] = (p-1)(\cancel{p^2} + p^3 - \cancel{p^2} - p) = p(p-1)(p^2-1) = p(p-1)^2(p+1) = |G|$ ✓

Now specify to conjugacy classes of $SL_2(\mathbb{F}_p)$: similarly to how conjugacy class split when going from $S_5 \to A_5$ we see the class $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ splits into two

extra analysis (theoretical); next page calculates (raw)

- claim: $SL_2(\mathbb{F}_p) \trianglelefteq GL_2(\mathbb{F}_p)$ is normal

  b/c $\det : GL_2(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^\times$ group hom

  $\text{kernel}(\det) = SL_2(\mathbb{F}_p)$ and kernel of a group hom is always a normal subgroup

  so $SL_2(\mathbb{F}_p)$ is a union of conj. classes of $GL_2(\mathbb{F}_p)$ only: some of them will split

- Note $GL_2(\mathbb{F}_p)$ acts on $SL_2(\mathbb{F}_p)$ via conjugation: $A * B = ABA^{-1}$ for $A \in GL_2(\mathbb{F}_p)$, $B \in SL_2(\mathbb{F}_p)$

  verify group action.
  - $ABA^{-1} \in SL_2(\mathbb{F}_p)$ b/c det is mult: $\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(AA^{-1})\det B = 1$
  - $A_1 * (A_2 * B) = A_1 * (A_2 B A_2^{-1}) = A_1 A_2 B A_2^{-1} A_1^{-1} = (A_1A_2)B(A_1A_2)^{-1} = A_1A_2 * B$
  - $I * B = B$

  so $\varphi : GL_2(\mathbb{F}_p) \longrightarrow \text{Aut}(SL_2(\mathbb{F}_p))$ group homomorphism

  $A \longmapsto$ conj. by A ← $ABA^{-1} = B \iff AB = BA$ i.e. A commutes with all of $SL_2(\mathbb{F}_p)$

  $\ker(\varphi) = \{\text{scalar matrices in } GL_2(\mathbb{F}_p)\} \cong \mathbb{F}_p^\times$

  so $\text{im}(\varphi) \cong GL_2(\mathbb{F}_p)/\ker(\varphi) = GL_2(\mathbb{F}_p)/\text{scalar} \cong PGL_2(\mathbb{F}_p)$

  so orbits of $PGL_2(\mathbb{F}_p)$ acting on $SL_2(\mathbb{F}_p)$ via conj. are conjugacy classes of $GL_2(\mathbb{F}_p)$ contained in $SL_2(\mathbb{F}_p)$ b/c restrict to $SL_2(\mathbb{F}_p)$

  b/c acting via conj on itself $GL_2(\mathbb{F}_p)$ gives conj. class

  $\varphi : GL_2(\mathbb{F}_p) \longrightarrow \text{Aut}(SL_2(\mathbb{F}_p))$ group hom; acting on $SL_2(\mathbb{F}_p)$

  $SL_2(\mathbb{F}_p) \longmapsto$ conj. by elem $\in SL_2(\mathbb{F}_p)$

  acting on itself; orbits of this action are the conj. classes of $SL_2(\mathbb{F}_p)$

  $\text{im}(SL_2(\mathbb{F}_p)) \le \text{Aut}(SL_2(\mathbb{F}_p))$

  $\text{im}(SL_2(\mathbb{F}_p)) \cong SL_2(\mathbb{F}_p)/\underbrace{\text{kernel}}_{} = SL_2(\mathbb{F}_p)/\{\pm I\} \cong PSL_2(\mathbb{F}_p)$ ← has $\frac{1}{2}$ the cardinality as $SL_2(\mathbb{F}_p)$; we group together / deem equiv if ± 1

  kernel of this restriction map is scalar matrices $\{\pm I\} \le SL_2(\mathbb{F}_p)$

  so conjugacy classes of $SL_2(\mathbb{F}_p)$ are the orbits of $PSL_2(\mathbb{F}_p)$ acting on $SL_2(\mathbb{F}_p)$

  [$\text{im}(\varphi) \cong PGL_2(\mathbb{F}_p) \le \text{Aut}(SL_2(\mathbb{F}_p))$ image of $GL_2(\mathbb{F}_p)$ acting on $SL_2(\mathbb{F}_p)$

  $\text{im}(SL_2(\mathbb{F}_p)) \cong PSL_2(\mathbb{F}_p) \le \text{Aut}(SL_2(\mathbb{F}_p))$ image of $SL_2(\mathbb{F}_p)$ acting on $SL_2(\mathbb{F}_p)$

  ↳ $\text{im}(SL_2(\mathbb{F}_p)) \le \text{im}(\varphi) \implies PSL_2(\mathbb{F}_p) \le PGL_2(\mathbb{F}_p)$ so index is: $\dfrac{p(p+1)(p-1)}{\frac{1}{2}p(p+1)(p-1)} = 2$

  $\#$ $\frac{1}{2}[p(p+1)(p-1)]$; $p(p+1)(p-1)$

what do we have so far:
- $SL_2(\mathbb{F}_p)$ is a union of conj. classes of $GL_2(\mathbb{F}_p)$
  - conj. classes of $GL_2(\mathbb{F}_p)$ which are contained in $SL_2(\mathbb{F}_p)$ are the orbits of $PGL_2(\mathbb{F}_p)$ on $SL_2(\mathbb{F}_p)$
- conj. classes of $SL_2(\mathbb{F}_p)$ are the orbits of $PSL_2(\mathbb{F}_p)$ acting on $SL_2(\mathbb{F}_p)$ via conj.

$\implies$ Any conj. class of $GL_2(\mathbb{F}_p)$ which is also in $SL_2(\mathbb{F}_p)$ is either:

1) remains its own conj. class or 2) splits into two conj. classes

How to tell if conj. class splits? → counting; observe orbit stabilizer

I. central conjugacy classes: $\begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix}$; $\lambda\in F_p^*$

reduces to just: $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ and $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ in $SL_2(F_p)$ b/c we need det = 1

so 2 central conj. classes, each with 1 elem each

II. Non-semisimple in $GL_2(F_p)$: $\begin{pmatrix}\lambda&1\\0&\lambda\end{pmatrix}$ $\lambda\in F_p^*$

Note if $\begin{pmatrix}\lambda&1\\0&\lambda\end{pmatrix}\in SL_2(F_p)$ then $\lambda^2=1$ so $\lambda=\pm1$

case $\lambda=1$ | suppose $A\sim\underbrace{\begin{pmatrix}1&1\\0&1\end{pmatrix}}_{\text{representative for this class}}$ in $GL_2(F_p)$ $(A\in SL_2(F_p))$

then $PAP^{-1}=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ for some $P\in GL_2(F_p)$

if $\det P=1$ then $P\in SL_2(F_p)$ and $A\sim\begin{pmatrix}1&1\\0&1\end{pmatrix}$ remains conj. in $SL_2(F_p)$

if $\det P=a\neq1$ then $P\notin SL_2(F_p)$.

Does A remain conjugate to $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ in $SL_2(F_p)$?

case: $a=b^2$ is a square in F_p, let $Q=b^{-1}P$ (Note $\det Q=(b^{-1})^2a=1$)

Then $QAQ^{-1}=\begin{pmatrix}b^{-1}&0\\0&b^{-1}\end{pmatrix}PA\left[\begin{pmatrix}b^{-1}&0\\0&b^{-1}\end{pmatrix}P\right]^{-1}$

$=\begin{pmatrix}b^{-1}&0\\0&b^{-1}\end{pmatrix}\begin{pmatrix}b^{-1}&0\\0&b^{-1}\end{pmatrix}^{-1}PAP^{-1}=\begin{pmatrix}1&1\\0&1\end{pmatrix}$

remains conjugate in $SL_2(F_p)$

case: $a\neq b^2$ is NOT a square

Then $A\nsim\begin{pmatrix}1&1\\0&1\end{pmatrix}$ is not conjugate in $SL_2(F_p)$

infact instead, $A\sim\begin{pmatrix}1&a^{-1}\\0&1\end{pmatrix}$ in $SL_2(F_p)$

b/c let $Q=\begin{pmatrix}a^{-1}&0\\0&1\end{pmatrix}P$ Note: $\det Q=a^{-1}\det P=1$

$QAQ^{-1}=\begin{pmatrix}a^{-1}&0\\0&1\end{pmatrix}PA\left[\begin{pmatrix}a^{-1}&0\\0&1\end{pmatrix}P\right]^{-1}$

$=\begin{pmatrix}a^{-1}&0\\0&1\end{pmatrix}PAP^{-1}\begin{pmatrix}a&0\\0&1\end{pmatrix}=\begin{pmatrix}a^{-1}&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&0\\0&1\end{pmatrix}$

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

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

if a^{-1} not a square then a is not a square

$\Rightarrow$ conjugate to anything of the form $\begin{pmatrix}1&a\\0&1\end{pmatrix}$ where a is not a square in F_p

so the class $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ in $GL_2(F_p)$ splits into two classes: $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ and $\begin{pmatrix}1&a\\0&1\end{pmatrix}$

representatives in $SL_2(F_p)$

(where a is not a square in F_p)

aka if A has min poly $(x-1)^2=x^2-2x+1$ i.e. $tr=2$ then falls into one of these two classes

case $\lambda=-1$ | A similar analysis gives us that $\begin{pmatrix}-1&1\\0&-1\end{pmatrix}$ in $GL_2(F_p)$

Splits into two conjugacy classes in $SL_2(F_p)$ with representatives:

$\begin{pmatrix}-1&1\\0&-1\end{pmatrix}$ & $\begin{pmatrix}-1&a\\0&-1\end{pmatrix}$ where a is not a square in F_p

so we get 4 non-semisimple classes; what is the size of each class?

centralizer of $\begin{pmatrix}1&1\\0&1\end{pmatrix}$:

$\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}a&a+b\\c&c+d\end{pmatrix}$ ← equal $\Rightarrow$ $c=0$, $a+\cancel{b}=\cancel{b}+d$, $a=d$, b anything $\Rightarrow\begin{pmatrix}x&y\\0&x\end{pmatrix}$ $x\in\{\pm1\}$, $y\in F_p$ so size $=2p$

$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a+c&b+d\\c&d\end{pmatrix}$

so size of the class is $\dfrac{|SL_2F_p|}{2p}=\dfrac{(p+1)(p-1)}{2}$

III. split regular semisimple in $GL_2(\mathbb{F}_p)$: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ $\lambda_1, \lambda_2 \in \mathbb{F}_p^\times$ (distinct)

Note if $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \in SL_2(\mathbb{F}_p)$ then $\lambda_1\lambda_2 = 1$ so it's really just: $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ $\lambda \in \mathbb{F}_p^\times$

Now take $A \in SL_2(\mathbb{F}_p)$ s.t. $\underbrace{A \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \text{ in } GL_2(\mathbb{F}_p)}_{\text{so } PAP^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \text{ for some } P \in GL_2(\mathbb{F}_p)}$; which conj. class of $SL_2(\mathbb{F}_p)$ does it lie in?

centralizer of $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ is: in $SL_2(\mathbb{F}_p)$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} a\lambda & b\lambda^{-1} \\ c\lambda & d\lambda^{-1} \end{pmatrix}$ ← equal ⇒ $c = b = 0$, $a, d \in \mathbb{F}_p^\times$ $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$ so $ad = 1$ ⇒ $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a\lambda & b\lambda \\ c\lambda^{-1} & d\lambda^{-1} \end{pmatrix}$ ← $a \in \mathbb{F}_p^\times$

so centralizer in $SL_2(\mathbb{F}_p)$ has size $p-1$ ⇒ conjugacy class of $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ has size: $\frac{|SL_2(\mathbb{F}_p)|}{p-1} = p(p+1)$

which is the same size as it is in $GL_2(\mathbb{F}_p)$

Hence remains as one conjugacy class in $SL_2(\mathbb{F}_p)$

How many of them? representative $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$; $\lambda \in \mathbb{F}_p^\times$ s.t. λ, λ^{-1} distinct ⇒ $\frac{p-3}{2}$ choices/classes

divide by 2 b/c order doesn't matter

IV. Nonsplit semi-simple $\begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$ in $GL_2(\mathbb{F}_p)$

becomes $\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} \in SL_2(\mathbb{F}_p)$

centralizer of this elem in $SL_2(\mathbb{F}_p)$?

$t = \text{trace} = \alpha + \bar{\alpha}$ where $\alpha, \bar{\alpha} \in \mathbb{F}_{p^2}^\times$ are the roots of $x^2 - tx + d = (x-\alpha)(x-\bar{\alpha})$ so $\det = \alpha\bar{\alpha} = \text{norm}(\alpha) = \alpha^{p+1}$

well $Z_{GL_2}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} \cong \mathbb{F}_{p^2}^\times = H$ we calculated this already in $GL_2(\mathbb{F}_p)$

How many of these are in $SL_2(\mathbb{F}_p)$ as well? ⇒ need $\det = 1$

$N: H \xrightarrow{\det} \mathbb{F}_p^\times$ det map ⇒ $N: \mathbb{F}_{p^2}^\times \twoheadrightarrow \mathbb{F}_p^\times$ is the norm
$\alpha \longmapsto \alpha^{p+1}$

so $Z_{SL_2}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} = \ker(\varphi)$
$= \{\alpha : \alpha^{p+1} = 1\}$

this has at most $p+1$ roots; But also $\mathbb{F}_{p^2}^\times / \ker \cong \mathbb{F}_p^\times$; $|\mathbb{F}_{p^2}^\times| = p^2 - 1$ and $|\mathbb{F}_p^\times| = p-1$

so we must have $p+1$ elems in kernel

so centralizer is size $p+1$ ⇒ size of conj. class is $p(p-1)$

which is the same size as in $GL_2(\mathbb{F}_p)$ so it doesn't split into multiple conj. classes

we just have less of them → How many? ⟺ How many irred polys $x^2 - tx + 1$

root $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$ $(x-\alpha)(x-\bar{\alpha}) = x^2 - tx + 1$ ⇒ $\text{norm}(\alpha) = \alpha^{p+1} = 1$

so $p+1$ choices, but need $\alpha, \bar{\alpha}$ distinct so $\alpha \neq 1, -1$

⇒ $p-1$ choices for α ⇒ $\frac{p-1}{2}$ choices for t = # of classes (2 to 1 map $\alpha \mapsto t$)

norm: $\alpha \longmapsto \alpha\bar{\alpha} = \alpha^{p+1}$

$\alpha, \bar{\alpha}$ roots of $x^2 - tx + 1 = (x-\alpha)(x-\bar{\alpha})$; any $\varphi \in \mathrm{Gal}(f(x))$ takes roots to roots; only 2 roots so $\mathrm{Gal}(f(x))$ is order 2

"conjugation" map $c: \alpha \longmapsto \alpha^p$

claim: c is an automorphism on $\mathbb{F}_{p^2}$ fixing $\mathbb{F}_p$

inverse: $c^{-1}: \alpha \mapsto \alpha^p$ its own inverse

$c^{-1}(c)(\alpha) = c^{-1}(\alpha^p) = (\alpha^p)^p = \alpha^{p^2} = \alpha$ Fermat's little theorem

fixes $\mathbb{F}_p$: if $x \in \mathbb{F}_p$ then $c: x \mapsto x^p = x \in \mathbb{F}_p$

so $c \in \mathrm{Gal}$, which has order 2 so generates ⇒ $\mathrm{Gal} = \{1, c\}$

so $\alpha \longmapsto \bar{\alpha}$ must be $\alpha \mapsto \alpha^p$ (can't be triv b/c $\alpha, \bar{\alpha}$ distinct) so in summary we have: conjugacy classes of $SL_2(\mathbb{F}_p)$

	central	Non-Semisimple		split regular semisimple	Non split
representative	$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$	$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$	$\begin{pmatrix} \pm 1 & a \\ 0 & \pm 1 \end{pmatrix}$ $a \in \mathbb{F}_p^*$ is not a square	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}$
# of classes	2	2	2	$\frac{1}{2}(p-3)$ $\{\lambda \in \mathbb{F}_p^*: \lambda, \lambda^{-1} \text{ distinct}\}$	$\frac{p-1}{2}$
size of each class	1	$\frac{(p+1)(p-1)}{2}$	$\frac{(p+1)(p-1)}{2}$	$p(p+1)$	$p(p-1)$
char poly	$(x \pm 1)^2$ min poly $(x \pm 1)$	$(x \pm 1)^2$ $\lvert\text{centralizer}\rvert = 2p$		$(x-\lambda)(x-\lambda^{-1})$	$x^2 - tx + 1 = (x-\alpha)(x-\bar{\alpha})$ $\alpha \in \mathbb{F}_{p^2} - \mathbb{F}_p$ $\lvert\text{centralizer}\rvert = p+1$

Take $A \in SL_2(\mathbb{F}_p)$ s.t. $A \sim \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ in $GL_2(\mathbb{F}_p)$; Does this conj. class split in $SL_2(\mathbb{F}_p)$?

Let Z be the centralizer of $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ in $GL_2(\mathbb{F}_p)$; $|Z| = p^2 - 1$ $\begin{pmatrix} f(x_{1,1}) & x \\ f(x) & y \end{pmatrix}$

stabilizer b/c we went $|\text{orb}| = |\text{conj. class } \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}|$ which we obtain from orb-stab thm

centralizer of $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ in $SL_2(\mathbb{F}_p)$?

$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix} = \begin{pmatrix} y & ya-x \\ w & wa-z \end{pmatrix}$

$\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} -z & -w \\ x+az & y+aw \end{pmatrix}$

$\begin{cases} y = -z \\ -w = ya - x \\ w = x + az \\ w\cancel{a} - z = y + a\cancel{w} \end{cases} \Rightarrow \begin{cases} y = -z \\ w = \cancel{x} + az = \cancel{x} - ya \end{cases}$ x is free $\Rightarrow \begin{cases} y = -z \\ w = az = -ya \end{cases} \Rightarrow \begin{pmatrix} x & y \\ -y & -ya \end{pmatrix}$

two free variables $x \in \mathbb{F}_p$, $y \in \mathbb{F}_p^* \Rightarrow p(p-1)$

$\begin{pmatrix} x & y \\ -y & -ya \end{pmatrix} \in SL_2(\mathbb{F}_p)$ so $-xya + y^2 = 1$ further constraint

$y(y - xa) = 1$

centralizer of $\begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}$ in $SL_2(\mathbb{F}_p)$

aside:

so in total we have: conjugacy classes of $GL_2(\mathbb{F}_p)$

	central	Non-semisimple	split regular semisimple	anisotropic regular semisimple
representative	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$	$\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix}$
# of classes	$p-1$ $(\lambda \in \mathbb{F}_p^*)$	$p-1$ $(\lambda \in \mathbb{F}_p^*)$	$\frac{(p-1)(p-2)}{2}$ $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$	$\frac{1}{2}(p^2-p)$ $a_0, a_1 \in \mathbb{F}_p$
size of each class	1	$(p+1)(p-1)$	$p(p+1)$	$p(p-1)$
char poly	$(x-\lambda)^2$	$(x-\lambda)^2$	$(x-\lambda_1)(x-\lambda_2)$	$x^2 - a_1 x + a_0$

OTHER METHOD - but not relevant

IV. Anisotropic semisimple in $GL_2(\mathbb{F}_p)$: $\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix}$ (irreducible char poly)

Note: if $\begin{pmatrix} 0 & -a_0 \\ 1 & a_1 \end{pmatrix} \in SL_2(\mathbb{F}_p)$ then $a_0 = 1 \Rightarrow \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ [so already reduces to at most $p-1$ conj. classes $(\alpha \in \mathbb{F}_p^\times)$]

so char poly is $x^2 - \alpha x + 1$ $(\alpha \in \mathbb{F}_p^\times)$ irreducible

take $A \in SL_2(\mathbb{F}_p)$ s.t. $A \sim \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ in $GL_2(\mathbb{F}_p)$ so A has the same char poly (irred)

since char poly irred, A has no eigenvalues in $\mathbb{F}_p$ and thus no $v \in V$ will be an eigenvector

Hence $B = \{v, Av\}$ will be a basis for V for any nonzero $v \in V$ so $[A]_B = \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$

so using change of basis: $[A]_E = P_{B\to E} \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} P_{E \to B}$

and note $P_{B\to E} = \begin{pmatrix} \vec{v} & A\vec{v} \end{pmatrix}$ important: Any nonzero $\vec{v}$ will give a valid P which conjugates

if $\det P = 1$ then $A \sim \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ remains conjugate in $SL_2(\mathbb{F}_p)$; so we WTS always possible to

choose $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{F}_p^2$ s.t. $\det P = \det \begin{pmatrix} \vec{v} & A\vec{v} \end{pmatrix} = 1$ let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p)$

$Av = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$ so $P = \begin{pmatrix} x & ax+by \\ y & cx+dy \end{pmatrix}$; we want integer solutions x, y to this equation

$\det P = x(cx+dy) - y(ax+by) = cx^2 + dxy - axy - by^2 = cx^2 - by^2 + (d-a)xy \equiv 1 \mod p$

$f(x,y) = cx^2 + (d-a)xy - by^2 - 1 = 0$ want integer solutions (x,y) for any given $a,b,c,d \in \mathbb{F}_p$

we also have the constraint that $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - cb = 1$

complete the square: assume $c \neq 0$:

$$x^2 + \frac{d-a}{c}xy - \frac{b}{c}y^2 = \frac{1}{c}$$

$$\underbrace{x^2 + \frac{d-a}{c}xy + \frac{(d-a)^2}{4c^2}y^2}_{} - \frac{(d-a)^2}{4c^2}y^2 - \frac{b}{c}y^2 = \frac{1}{c}$$

$$\underbrace{\left(x + \frac{(d-a)}{2c}y\right)^2}_{z} - \underbrace{\left[\frac{b}{c} + \frac{(d-a)^2}{4c^2}\right]}_{b'/c} y^2 = \frac{1}{c}$$

$$\Rightarrow cz^2 - b'y^2 = 1 \qquad \boxed{z = x + \frac{d-a}{2c}y,\ b' = b + \frac{d-a}{4c}}$$

Pell's equation? I think will have int sol'ns

Are c, b' relatively prime to p?

if $c \not\equiv 0 \mod p$ then p does not divide ✓

$b' = b + \frac{d-a}{4c} = \frac{4bc + d - a}{4c}$ does p divide?

suppose it did, then $4bc + d - a = pq \equiv 0 \mod p$

$4(ad-1) + d - a \equiv 0$

$4ad - 4 + d - a \equiv 0$

Assuming c, b' both not div by p:

Then let $S = \{cz^2 : z \in \mathbb{F}_p\}$, $|S| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$

and $T = \{1 + b'y^2 : y \in \mathbb{F}_p\}$, $|T| = \frac{p+1}{2}$ as well

$|S| + |T| = p + 1 > |\mathbb{F}_p|$ so pigeon hole $\exists x \in S \cap T$

so $\exists x \in \mathbb{F}_p$ s.t. $x = cz^2 = 1 + b'y^2$ for some $z, y \in \mathbb{F}_p \Rightarrow cz^2 - b'y^2 = 1$ sol'n exists ✓

So we have int sol'ns $z, y \in \mathbb{F}_p$

From which $z = x + \frac{d-a}{2c}y \Rightarrow x = z - \frac{d-a}{2c}y \in \mathbb{F}_p$ we can solve for x

So int sol'ns exist if both c, b' are rel prime to p

what if $p \mid b'$? then we have $cz^2 = 1$

so $z^2 = c^{-1}$ so sol'n exists $\Leftrightarrow$ c is a square mod p

But what if it's not a square??

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1$

$p \mid b' = b + \frac{d-a}{4c}$

so $b + \frac{d-a}{4c} = pq$ for some $q \in \mathbb{Z}$

Subgroups of $GL_2(\mathbb{F}_p)$:

- Borel subgroup: $\left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix} : a,b,c \in \mathbb{F}_p,\ ac \neq 0\right\}$
- Split cartan subgroup: $\left\{\begin{pmatrix} a & 0 \\ 0 & c\end{pmatrix} : a,c \in \mathbb{F}_p,\ ac \neq 0\right\}$
- nonsplit cartan subgroup: $\left\{\begin{pmatrix} a & \varepsilon b \\ b & a\end{pmatrix} : a,b \in \mathbb{F}_p,\ a^2 - \varepsilon b^2 \neq 0,\ \varepsilon \in \mathbb{F}_p^\times \text{ nonsquare}\right\}$

all defined up to conjugation

- $Z = \left\{\begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix} : a \neq 0\right\} \leq GL_2(\mathbb{F}_p)$ scalar matrices form a normal subgroup of $GL_2(\mathbb{F}_p)$
- Let $M \in GL_2(\mathbb{F}_p)$ is non-scalar with one distinct eigenvalue, λ and v eigenvector for λ.

Then $M - \lambda I$ has nontrivial kernel: so $0 < \dim(\ker) \leq \dim(V) = 2$

$(M-\lambda I)v = Mv - \lambda v = \lambda v - \lambda v = 0 \Rightarrow v \in \ker(M - \lambda I)$ and $v \neq 0$

can't be 2 b/c not the 0 matrix

and $M - \lambda I$ is not 0 b/c M is not scalar, $\dim(\ker) + \dim(\mathrm{im}) = 2 \Rightarrow \dim(\ker) = \dim(\mathrm{im}) = 1$

$\dim(\mathrm{im}(M - \lambda I)) = 1$ so $\mathrm{im}(M - \lambda I) = \mathrm{span}(x)$ for some $x \neq 0$

claim: $\mathrm{im}(M - \lambda I) = \mathrm{span}(v)$

$\subseteq$) take $w \in \mathrm{im}(M - \lambda I)$ $w \neq 0$

so $w = (M - \lambda I)x$ for some $x \in (\mathbb{F}_p)^2$

$w = Mx - \lambda x$ suppose $x \in \mathrm{span}\, v$

$\Rightarrow w = M(kv) - \lambda(kv) = k(M - \lambda I)v = 0$ ↯ so $x \notin \mathrm{span}(v)$ so $\{v, x\}$ is a basis for $\mathbb{F}_p^2$

suppose $w \notin \mathrm{span}\, x$ then $(M - \lambda I)x = w = kx \Rightarrow M$ scalar matrix but its not $\Rightarrow w \in \mathrm{span}\, v$

so $\mathrm{im}(M - \lambda I) \subseteq \mathrm{span}\, V$ but since 1 dim it must be equal

so $v \in \mathrm{im}(M - \lambda I)$ hence $v = (M - \lambda I)w$ for some w

$\Rightarrow v = Mw - \lambda w$

$v \neq 0$

suppose $w \in \mathrm{span}\, v$ then $w = kv \Rightarrow v = M(kv) - \lambda(kv) = k(M - \lambda I)v = k \cdot 0 = 0$ ↯

so $\{v, w\}$ basis for $V \Rightarrow \mathcal{B} = \{(M - \lambda I)w, w\} = \{v, w\}$

so $M = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ up to conjugation / change of basis

$Mv = \lambda v$ $Mw = v + \lambda w$

so if M is order p then $M = \begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$; contained in a borel subgroup

Might not be relevant - this is $GL_2(\mathbb{F}_p)$ stuff

subgroups of $SL_2(\mathbb{F}_p)$ $\quad |G| = p(p-1)(p+1)$

- if $p = 2$ then $|SL_2(F_2)| = 1\times2\times3 = 6$ (in fact $SL_2(F_2) = GL_2(F_2)$ same group)

$$SL_2(F_2) = \left\{ \underset{id}{\begin{pmatrix}1&0\\0&1\end{pmatrix}}, \underset{2}{\begin{pmatrix}1&1\\0&1\end{pmatrix}}, \underset{2}{\begin{pmatrix}1&0\\1&1\end{pmatrix}}, \underset{3}{\begin{pmatrix}0&1\\1&1\end{pmatrix}}, \underset{3}{\begin{pmatrix}1&1\\1&0\end{pmatrix}}, \underset{2}{\begin{pmatrix}0&1\\1&0\end{pmatrix}} \right\}$$

so sylow 2-subgroup is of cardinality 2: $\{id, \begin{pmatrix}1&0\\1&1\end{pmatrix}\}, \{id, \begin{pmatrix}1&1\\0&1\end{pmatrix}\}, \{id, \begin{pmatrix}0&1\\1&0\end{pmatrix}\}$ 3 of them

all conjugate to eachother

sylow 3-subgroup (unique!): $\{id, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}\}$

$SL_2(F_2) \cong S_3$

- so from now on we will assume p is odd $(p > 2)$
- Let $Z = \{I_2, -I_2\}$ centralizer of $G = SL_2(F_p)$
- Let $B = \left\{ \begin{pmatrix}a&b\\0&a^{-1}\end{pmatrix} : a,b \in F_p \right\}$ upper triangular $\quad |B| = p(p-1)$ $\quad$ "Borel subgroup"
- Let $T = \left\{ \begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix} : a \in F_p \right\}$ diagonal $\quad T \cong F_p^\times \quad |T| = p-1$
- Let $U = \left\{ \begin{pmatrix}1&a\\0&1\end{pmatrix} : a \in F_p \right\}$ unipotent upper triangular $\quad U \cong F_p \quad |U| = p$ $\quad$ sylow p-subgroup

$B, T, U \subseteq SL_2(F_p)$ subgroups

U is a sylow p-subgroup of $SL_2(F_p)$ $\to$ also lower triangular unipotent will be sylow p so we know it's not unique

# of sylow p-subgroups? divides p^2-1 and is $\equiv 1 \mod p$

either 1 or $p+1$

- I think its $p+1$ of them because otherwise U is normal in $SL_2(F_p)$ and I don't think it is

normal: invariant under conj. i.e. $gUg^{-1} = U \quad \forall g \in G$

- Normal subgroup is a union of conjugacy classes

wait... is U a union of all the non-semisimple conj. classes though

claim: $B = \underset{\underset{F_p^\times}{\cong}}{T} \ltimes \underset{\underset{F_p}{\cong}}{U}$ $\quad$ (U acting on T)

$\Rightarrow U \trianglelefteq B$ is normal and $B/U \cong T$ is the quotient group

$d: F_p^\times \xrightarrow{\cong} T$ and $u: F_p \xrightarrow{\cong} U$

$a \longmapsto \begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix} \qquad x \mapsto \begin{pmatrix}1&x\\0&1\end{pmatrix}$

Further: U, T are abelian $\quad \begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}\begin{pmatrix}b&0\\0&b^{-1}\end{pmatrix} = \begin{pmatrix}ab&0\\0&a^{-1}b^{-1}\end{pmatrix} = \begin{pmatrix}b&0\\0&b^{-1}\end{pmatrix}\begin{pmatrix}a&0\\0&a^{-1}\end{pmatrix}$ ✓

also abelian b/c $\cong F_p, F_p^\times$ respectively

Hence: $1 \trianglelefteq U \trianglelefteq B$ with $B/U \cong T$ abelian ; U abelian $\Rightarrow B$ is solvable!

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

$\Rightarrow d(a)u(x)d(a)^{-1} = u(a^2x)$

B has index $p+1$ in $SL_2(F_p)$ $\nearrow$ relatively small so we can look at perm reps + induced (nontrivial 1D reps of B)

Notation: let $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

so $s^2 = -I_2$ and $s\,d(a)\,s^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}$

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

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

$$= d(a^{-1})$$

claim: s normalizes T i.e. $sTs^{-1} = T$

b/c $s\,d(a)\,s^{-1} = d(a^{-1}) \in T$

Bruhat decomp of G:

$SL_2(\mathbb{F}_p) = B \sqcup BsB = B \sqcup UsB$

Take $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G = SL_2(\mathbb{F}_p) = G \setminus B \sqcup B$

if $g \in G\setminus B$ then $c \neq 0$ WTS $g \in UsB$ i.e. $g = usb$ for some $u \in U$, $b \in B$

let $b = s^{-1}u(-a/c)\,g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -a/c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & b - \frac{a}{c}d \\ c & d \end{pmatrix}$$

$$= \begin{pmatrix} c & d \\ 0 & \frac{a}{c}d - b \end{pmatrix} \in B$$

so $g = \underbrace{[u(-a/c)]^{-1}}_{\in U}\, s\, \underbrace{b}_{\in b} = u(-a/c)^{-1}s(s^{-1}u(-a/c)\,g) = g = usb$ so $g \in UsB$

Bruhat decomp $\to$ double coset space $B \setminus \underbrace{SL_2(\mathbb{F}_p)/B}_{X}$

$|G| = p(p+1)(p-1)$; $|B| = p(p-1)$

so G acts transitively on $G/B = X$, $|X| = p+1$ X = lines in $\mathbb{F}_p^2 \cong P_1(\mathbb{F}_p)$

$\hookrightarrow$ understanding this action: $V = (\mathbb{F}_p)^2$

G acts on V via left mult. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$

so using the frobenius automorphism, we see:

$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto x/y \in \mathbb{F}_p \cup \{\infty\} = P_1(\mathbb{F}_p)$

(convention: $\begin{pmatrix} a \\ 0 \end{pmatrix} \mapsto a/0 = \infty$)

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \dfrac{ar+b}{cr+d} \in P_1(\mathbb{F}_p)$

G acts on $P_1(\mathbb{F}_p)$ with the convention $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\infty) = \frac{a}{c}$

transitively and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(-d/c) = \infty$

Note: $B \leq G$; $B = \mathrm{Stab}_X(\infty)$

because: $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}$ A preserves this line; $\mathrm{span}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \infty$

so $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}(\infty) = \frac{a}{0} = \infty$ ✓

$SL_2(\mathbb{F}_p)/B = P_1(\mathbb{F}_p)$

$B \leq G \Rightarrow B$ acts on $SL_2(\mathbb{F}_p)/B = P_1(\mathbb{F}_p)$ on the left as well: $B \setminus \underline{SL_2(\mathbb{F}_p)/B} = B \setminus \underline{P_1(\mathbb{F}_p)}$

so to understand the coset space we'll look at orbits

↳ Observe the orbits: $\{\infty\}$ is its own orbit under B b/c $B = \mathrm{Stab}_X(\infty)$

$\{0, 1, \dots, p-1\}$ all in the same orbit under B

because: $\mathrm{orb}_B(0) = \{ \underline{g\binom{0}{1}} : g \in B \}$

$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\binom{0}{1} = \binom{b}{a^{-1}} = b/a^{-1}$ and $b \in \mathbb{F}_p$ is free

$\Rightarrow \mathrm{orb}_B(0) = \mathbb{F}_p$

so we get the following decomp:

$B \backslash G / B = \{ \{\infty\}, \{0, 1, \dots, p-1\} \}$

↑ ↑ orbits of B acting on $G/B = P_1(\mathbb{F}_p)$

↑ Has only two cosets so decomp G into cosets only two:

$\Rightarrow G = B \sqcup BsB \overset{\text{shown above}}{=} B \sqcup UsB$

↑ just choose an $s \notin B$; $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ makes a nice choice

so $\{\infty\}$ = orbit of B and $\{0, 1, \dots, p-1\}$ = orbit of $G/B = BsB$

Representations of $SL_2(\mathbb{F}_p)$: $p+4$ conjugacy classes $\Leftrightarrow$ $p+4$ representations (irred)

- trivial rep ✓ $\chi(g) = 1 \;\; \forall g \in G$
- "Steinberg permutation representation"
  - $[G:B] = p+1$ index is relatively low; let $X = G/B \cong P_1(\mathbb{F}_p)$

$V = \mathbb{C}[G/B] = \mathbb{C}[X]$ $p+1$ dimensional; basis $\{v_\infty, v_0, v_1, \dots, v_{p-1}\}$

G acts on this space by permuting the basis vectors

Bruhat decomp of G tells us that B fixes $\mathrm{span}(v_\infty)$ and permutes the remaining p elements (transitively).

fixed pts of $g \in G - B$??

permrep: $\chi_V(g) = $ # fixed pts of g in $P_1(\mathbb{F}_p)$

	central	non-semisimple	split semisimple	nonsplit
χ_V	$p+1$	1	2	0
	fixes all	fixes ∞	fixes $0, \infty$	fixes none

I. $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} r = \dfrac{-1(r)+0}{0-1} = r$ fixes everything

II. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} r = \dfrac{r+1}{1} = r+1$ no FP in $\mathbb{F}_p$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \infty = 1/0 = \infty$ fixes ∞ $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in B$ so makes sense

(non semisimple) $\in B$ so all of them will have 1 FP

III. $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} r = \dfrac{\lambda r + 0}{0 + \lambda^{-1}} = \left(\dfrac{\lambda}{\lambda^{-1}}\right) r$ if $r = 0 \in \mathbb{F}_p$ then fixed

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \infty = \dfrac{\lambda}{0} = \infty$ fixes ∞ $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in B$ so makes sense

$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} r = \left(\dfrac{\lambda}{\lambda^{-1}}\right) r = r$ iff $\dfrac{\lambda}{\lambda^{-1}} = 1 \Leftrightarrow \lambda = \lambda^{-1}$ ← but this class requires them unique

$\Rightarrow$ split semi simple 2 FP...?

Ex. $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} r = \dfrac{2r}{3} = 2r \cdot 3^{-1} = 2 \cdot 2 \cdot r = 4r$

$1 \mapsto \dfrac{2r}{3} = 2 \times 3^{-1} = 2 \times 2 = 4$

$2 \mapsto 2 \cdot 2 \times 3^{-1} = 2 \cdot 2 \cdot 2 = 8 = 3$

$4 \mapsto \dfrac{2 \cdot 4}{3} = 8 \times 3^{-1} = 8 \cdot 2 = 16 = 1$

$3 \mapsto 2 \cdot 3 \times 2 = 12 = 2$

more formal proof: $\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix} = \left(\frac{\lambda}{\lambda^{-1}}\right) r = \lambda \times (\lambda^{-1})^{-1} \times r = \lambda^2 r$ where $\lambda \in \mathbb{F}_p^\times - \{\pm 1\}$

so fixes $0, \infty$ and permutes the rest

IV. $\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} r = \frac{0 - 1}{r + t} = \frac{-1}{r+t} = -(r+t)^{-1}$

Ex. $\mathbb{F}_5$ so $t \in \mathbb{F}_p$, $t = \alpha + \bar{\alpha}$ s.t. $\alpha\bar{\alpha} = \alpha^{p+1} = 1$ so $\alpha \in \mu_{p+1} - \{\pm 1\}$

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} 0 = -(t^{-1}) \neq 0$ not fixed

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} 1 = -\underline{(1+t)^{-1}}$ not fixed

$-1 = x^{-1}$

so $1 + t = -1$

$\Rightarrow t = -2$

but then $x^2 + 2x + 1 = (x+1)(x+1)$ would not be in nonsplit

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} 2 = -(2+t)^{-1}$ fixed $\Leftrightarrow$ $(2+t)^{-1} = -2$ $\Leftrightarrow$ $x^{-1} = -2 = 3$ $\Leftrightarrow$ $x = 2$ $\Leftrightarrow$ $2 + t = 2 \Leftrightarrow t = 0$

so 2 fixed iff $t = 0$: $x^2 + 1$ is non split in $\mathbb{F}_5$

but $5 \equiv 1 \mod 4$ so -1 is QR $\Rightarrow$ $x^2 + 1 = (x+2)(x+3)$

would not be nonsplit so not fixed

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} 3 = -(3+t)^{-1}$ fixed $\Leftrightarrow$ $t = 0$ but x^2+1 is split so 3 not fixed

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} 4 = -(4+t)^{-1}$ fixed $\Leftrightarrow$ $x^{-1} = -4 = 1$ so $x = 1$ $\Leftrightarrow$ $4 + t = 1$ $\Rightarrow t = -3 = 2$

but $x^2 + 2x + 1 = (x+1)^2$ splits so 4 not fixed

$\begin{pmatrix}0 & -1\\ 1 & t\end{pmatrix} \infty = 0$ not fixed

0 fixed points

More formal proof?

Is V irred? No!

$$\langle \chi_V, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)^2 = \frac{1}{p(p+1)(p-1)} \left[2(p+1)^2 + \frac{4(p+1)(p-1)}{2} + \frac{p(p-3)(p+1)}{2}(4) \right]$$

$$= \frac{1}{p(p+1)(p-1)} \left[2(p+1)^2 + 2(p+1)(p-1) + 2p(p-3)(p+1) \right]$$

$$= \frac{2\cancel{(p+1)}\left[p+\cancel{1} + p - \cancel{1} + p^2 - 3p\right]}{p\cancel{(p+1)}(p-1)} = \frac{2(p^2 - p)}{p(p-1)} \neq 1$$

Must subtract off trivial rep!! so now we get:

	central	non-semi simple	split semi simple	nonsplit
$\chi_{st.}$	p	0	1	-1

$\frac{1}{2}\left(p^3 - 2p^2 - 3p\right) + \frac{1}{2}\left[p(p^2 - 2p + 1)\right]$

$p(p^2 - 3p + p - 3)$

sanity check: $\langle \chi_{st.}, \chi_{st.} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{st}(g)^2 = \frac{1}{p(p+1)(p-1)} \left[2p^2 + 0 + \frac{1}{2} p(p-3)(p+1) + \frac{1}{2} p(p-1)^2 \right]$

$$= \frac{1}{p(p+1)(p-1)} \left[2p^2 + \frac{1}{2}\left[p^3 - 2p^2 - 3p + p^3 - 2p^2 + p \right] \right]$$

$$= \frac{1}{p(p+1)(p-1)} \left[\cancel{2p^2} + p^3 - \cancel{2p^2} - p \right]$$

$$= \frac{p(p^2-1)}{p(p^2-1)} = 1 \quad \checkmark \text{ irred.}$$

Now induced representations: $B \leq G$ with $[G:B] = p+1$

so d dimensional representations of B will yield $d(p+1)$ reps of G

Let's find the representations of B:

luckily $U \trianglelefteq B$ gives us an abelian quotient: $B/U = T \cong \mathbb{F}_p^\times$

Fact: if H is a quotient of G then any rep of H gives us a rep of G by composing with the quotient map

$\mathbb{F}_p^\times$ is abelian, size $p-1$ $\Rightarrow$ $p-1$ one dim reps of T

$\mathbb{F}_p^\times \cong \mathbb{Z}/_{p-1}\mathbb{Z}$ so let g be generator and fix ζ a primitive $p-1^{st}$ root of unity

Any character χ suffices to be defined on g

so for $i \in \{1, .., p-2\}$ we'll get $p-2$ (nontrivial) characters

$\chi_i : g \mapsto \zeta^i$

kinda like χ_i where $i = p-1$ b/c then $g \mapsto \zeta^{p-1} = 1$

(and ofc the trivial char $\chi_{triv} : g \mapsto 1$ for a total of $p-1$ reps)

Note if $i = \frac{p-1}{2}$ then $\chi_i^2(g) = g^{p-1} = 1$ has trivial square

so we get $\chi_{p-1/2} : \begin{matrix} \text{squares} \mapsto 1 \\ \text{nonsquares} \mapsto -1 \end{matrix}$; the remaining all take on various powers of ζ

Hence we get $p-2$ nontrivial one dim reps of B → trivial one gives us steinbergs perm rep

$\psi_i : \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi_i(a)$ $\quad i \in \{1, .., p-2\} - \{\frac{p-1}{2}\}$

from composing with the quotient map

$$B \longrightarrow B/U = T \cong \mathbb{F}_p^\times$$

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \overset{\sim}{\longmapsto} a$$

$$\psi_{\frac{p-1}{2}} : \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi_{\frac{p-1}{2}}(a) = \begin{cases} 1 & a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & a \text{ is a nonsquare} \end{cases}$$

Each ψ_i is a one dim rep of B; Fix one of them, call it ψ defined as $\psi : \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi(a)$ for some fixed char χ of $\mathbb{F}_p^\times$

so $\chi : g \mapsto \zeta$ is rep of $\mathbb{F}_p^\times$ which gives us

$\psi : \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi(a) = \chi(g^{d_a}) = \zeta^{d_a}$ for some d_a

(b/c $a \in \mathbb{F}_p^\times$ so $a = g^{d_a}$ for some d_a; $\mathbb{F}_p^\times = \langle g \rangle$)

ψ has nontrivial square

Now let $V_\psi = \{ f : G \to \mathbb{C} : f(xb) = \overline{\psi(b)} f(x) \ \forall b \in B \}$

this is the induced rep of G; $|V_\psi| = |G/B| = p+1$

$$\chi_{V_\psi}(g) = \sum_{\substack{aB \in G/B \\ \text{s.t. } gaB = aB}} \overset{\psi \text{ is only defined on } B}{\psi(a^{-1}ga)} = \sum_{\substack{x \in \mathbb{P}_1(\mathbb{F}_p) \\ \text{s.t. } gx = x}} \psi($$

sum over the cosets fixed by g

ψ is defined on B and g might not be in B so we need to conjugate it into B

	central	non-semi simple	split semi simple	nonsplit
χ_{V_ψ}	$\pm(p+1)$	± 1	$\chi(\lambda) + \chi(\lambda^{-1})$	0

fixes none so remains as 0

I. central fixes all of $\mathbb{P}_1(\mathbb{F}_p)$ so $p+1$ nonzero terms

$$\chi_{V_\psi}(I_2) = \sum_{aB \in G/B} \overset{\text{each term is } 1}{\psi(I)} = p+1$$

claim: $sBs^{-1} \cap B = T$

observe $s\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}s^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$

$= \begin{pmatrix} 0 & -a^{-1} \\ a & b\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$

$= \begin{pmatrix} a^{-1} & 0 \\ -b & a\end{pmatrix}$

so intersection is just diagonal matrices

ψ is rep of $B \supseteq T$

so $\psi\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix} = \psi\left(s\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda\end{pmatrix}s^{-1}\right) = \chi(\lambda^{-1}) = \chi(\lambda)^{-1}$ [i.e. $\psi(d(a)) = \chi(a)^{-1}$]

so $\chi_{V_\psi}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix} = \sum\limits_{\substack{aB \in G/B \\ \text{s.t. } \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{smallmatrix}\right)aB = aB}} \psi\left(a^{-1}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}a\right)$

only defined on B but $T \subseteq B$ so ok

sum over those that are fixed

I. central: fixes all cosets / fixes all of $P_1(\mathbb{F}_p)$

so $\chi_{V_\psi}\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} = \sum\limits_{\substack{aB \in G/B \\ p+1 \text{ cosets}}} \psi\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} = (p+1)\chi(1)^{-1} = p+1$

b/c $\chi(-1) = -1$ b/c -1 is order 2 in $\mathbb{F}_p^*$ so we need order 2 elem in $\mathbb{C}^\times$

$\chi_{V_\psi}\begin{pmatrix} -1 & 0 \\ 0 & -1\end{pmatrix} = (p+1)\chi(-1)^{-1} = (p+1)(-1) = -(p+1)$

II. split semisimple $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}$ $\lambda \neq \pm 1$ has two fixed points in $P_1(\mathbb{F}_p)$ so 2 terms in the sum

0 and ∞

$\chi_{V_\psi}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix} = \underbrace{\psi\left(a_0^{-1}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}a_0\right)}_{a_0B \text{ is the coset corresponding to } 0} + \underbrace{\psi\left(a_1^{-1}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}a_1\right)}_{a_1B \text{ corresponds to } \infty}$

some conjugate of $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix}$ so must remain diagonal and with same eigenvalues, but are not the same b/c correspond to two diff fixed pts

$= \psi\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{pmatrix} + \psi\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda\end{pmatrix}$

$= \chi(\lambda)^{-1} + \chi(\lambda^{-1})^{-1} = \chi(\lambda) + \chi(\lambda^{-1})$

III. Non split no fixed points $\Rightarrow$ just 0

IV. Non semisimple has 1 fixed point in $P_1(\mathbb{F}_p)$ so only one term in the sum

it's ∞

$\chi_{V_\psi}\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix} = \psi\left(a^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}a\right) = \psi\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix} = \chi(1) = 1$

aB is the coset fixed by $\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$

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

$\chi_{V_\psi}\begin{pmatrix} -1 & 1 \\ 0 & -1\end{pmatrix} = \dots = \chi(-1) = -1$

i.e. $a^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}a \in B$

fixed by $\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$ so $a^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}a = \begin{pmatrix} 1 & 1 \\ 0 & 1\end{pmatrix}$

$B \backslash G / B = \{\{\infty\}, \{0, 1, \dots, p-1\}\}$

$G = B \sqcup BsB$

irreducible? $\langle \chi_{V_\psi}, \chi_{V_\psi}\rangle = \frac{1}{|G|}\sum\limits_{g \in G} \chi(g)^2 = \frac{1}{p\cancel{(p+1)}(p-1)}\left[2(p+1)^2 + 4\left(\frac{1}{2}\cancel{(p+1)}(p-1)\right) + \frac{1}{2}p(p-3)\cancel{(p+1)}\left[\chi(\lambda) + \chi(\lambda^{-1})\right]^2\right]$

$p(p^2 - 3p + p - 3$

$= \frac{1}{\cancel{p}(p-1)}\left[2p + \cancel{2} + 2p - \cancel{2} + \frac{1}{2}\cancel{p}(p-3)\left[\chi(\lambda) + \chi(\lambda^{-1})\right]^2\right]$

doesn't seem to be irred?

$= \frac{1}{p-1}\left[4 + \frac{1}{2}(p-3)\left[\chi(\lambda) + \chi(\lambda^{-1})\right]^2\right]$

$\uparrow$

$\lambda \in \mathbb{F}_p^\times - \{\pm 1\}$ (λ, λ^{-1} distinct)

so let $\mathbb{F}_p^\times = \langle g \rangle$ generator and ξ prim $p-1^{st}$ root of unity then $\chi(\lambda) = \chi(g^a) = \xi^a$

$\chi(\lambda^{-1}) = \chi(g^{p-1-a}) = \xi^{p-1-a}$

so $[\chi(\lambda) + \chi(\lambda)^{-1}]^2 = (\xi^a)^2 + 2 + (\xi^{p-1-a})^2 = x$

irreducible...?

would require $\frac{1}{p-1}\left[4 + \frac{1}{2}(p-3)x\right] = 1$

$4 + \frac{1}{2}(p-3)x = p-1$

$(p-3)x = 2(p-5)$

$x = \frac{2p-10}{p-3}$ ...? weird

So now we have constructed:

trivial rep, Steinberg rep, $p-3$ nontrivial reps as above

so now let χ be the rep of $\mathbb{F}_p^\times$ which sends squares $\mapsto 1$, nonsquares $\mapsto -1$

and ψ the associated rep of B:

$$\psi_{\frac{p-1}{2}} : \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi_{\frac{p-1}{2}}(a) = \begin{cases} 1 & a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & a \text{ is a nonsquare} \end{cases}$$

so we get V_ψ rep of G of dimension $p+1$

	central	non-semi simple	split semi simple	nonsplit
χ_{V_ψ}	$\pm(p+1)$	1	± 2	0

↖ still no FP

I. central

$\chi_{V_\psi}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (p+1)\,\psi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (p+1)\chi(1) = p+1$

$\chi_{V_\psi}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = (p+1)\chi(-1)^{-1} = -(p+1)$

II. split semisimple: same idea (2 fixed pts)

$\chi_{V_\psi}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \chi(\lambda^{-1}) + \chi(\lambda)$

$= \begin{cases} 2 & \text{if } \lambda \text{ is a square} \\ -2 & \text{nonsquare} \end{cases}$

Note: inverse preserves square/nonsquare mod p

III. nonsemisimple: one fixed pt

$\chi_{V_\psi}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \chi(1) = 1$

issue: this isn't irreducible as we calculated before??

(more precise) representations of $SL_2(F_p)$

Character table:

		$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&a\\0&1\end{pmatrix}$	$\begin{pmatrix}-1&1\\0&-1\end{pmatrix}$	$\begin{pmatrix}-1&a\\0&-1\end{pmatrix}$	$\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&t\end{pmatrix}$	
					$a\in F_p^\times$ non square		$a\in F_p^\times$ non square	$\lambda\in F_p^\times-\{\pm1\}/_{\lambda\neq\lambda^{-1}}$	$t=\alpha+\bar\alpha$, $\alpha\in F_{p^2}-F_p$ s.t. $\alpha\bar\alpha=\alpha^{p+1}=1$	
	# of classes	1	1	1	1	1	1	$\frac{p-3}{2}$	$\frac{p-1}{2}$	
	size	1	1	$\frac{(p+1)(p-1)}{2}$	"	"	"	$p(p+1)$	$p(p-1)$	
	trivial	1	1	1	1	1	1	1	1	1
$\chi: g\mapsto 1$	Steinberg	p	p	0	0	0	0	1	-1	1 suspiciously not irred?
$\chi: g\mapsto \xi$, $\xi\in\mu_{p-1}-\{\pm1\}/\xi\neq\bar\xi$	Non quad.	$p+1$	$\chi(-1)(p+1)$	1	1	$\chi(-1)$	$\chi(-1)$	$\chi(\lambda)+\chi(\lambda^{-1})$	0	$\frac{p-3}{2}$ of these; irred!
$\chi: g\mapsto -1$	Quadratic	$p+1$								1

I. Steinberg perm rep comes from inducing trivial rep of $B\leq G$

$V=\mathbb{C}[G/B]$ has basis $\{v_\infty, v_0, v_1,\dots,v_{p-1}\}$

G acts on V by permuting basis vectors so:

$\chi_V = \#$ FP of $G \curvearrowright P_1(F_p)$ and then -1 to subtract trivial rep

$\chi_V\begin{pmatrix}1&0\\0&1\end{pmatrix}=p+1$ nonsemisimple $\in B$ so fixes ∞ so $\chi_V\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}=2$

$\chi_V\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=p+1$ $\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}r=\left(\frac{\lambda}{\lambda^{-1}}\right)r$ also fixes 0

Nonsplit has no fixed points in $P_1(F_p)$: $\begin{pmatrix}0&-1\\1&t\end{pmatrix}r=\frac{-1}{r+t}$

II. Induced representations of B

$U\trianglelefteq B$ with $B/U=T\cong F_p^\times$; $F_p^\times$ abelian $\Rightarrow$ $p-1$ one dimensional characters of $F_p^\times$

$\mu_{p-1}=\{\xi\in\mathbb{C}:\xi^{p-1}=1\}$ $p-1^{st}$ roots of unity Note $p-1$ is even so $-1\in\mu_{p-1}$

let χ be a character of $F_p^\times$ and g a generator for $F_p^\times$ (each χ suffices to be defined on g)

thus $\underline{\chi: g\mapsto\xi}$ for some $\xi\in\mu_{p-1}$

χ are indexed by $\xi\in\mu_{p-1}$ $\Rightarrow$ $p-1$ of them

order 2; $\chi^2(g)=1$

Among these characters we have: trivial $\chi: g\mapsto 1$ and quadratic $\chi: g\mapsto -1$

so we have $p-3$ "nontrivial square" characters of $F_p^\times$

so fix χ a non quadratic character of $F_p^\times$ so $\chi: g\mapsto\xi$ where $\xi\neq\pm1$ $(\xi\in\mathbb{C})$ i.e. χ has nontrivial square

this induces to a representation of B by composing with the quotient map

$\psi:\begin{pmatrix}a&b\\0&a^{-1}\end{pmatrix}\longmapsto\chi(a)=\xi$

so then we get an induced rep V_ψ of G with the following character:

$$\chi_{V_\psi}(g)=\sum_{\substack{aB \\ \text{s.t. } gaB=aB}}\psi(aga^{-1})$$

terms in sum = # fixed points of $G\curvearrowright P_1(F_p)$

i.e. $a^{-1}ga\in B$ ← a is what conjugates g into B

$\chi_{V_\psi}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \sum_{aB} \psi\left(a\begin{pmatrix}1&0\\0&1\end{pmatrix}a^{-1}\right) = (p+1)\psi(I) = p+1$

every coset is fixed by the id

What is $\chi(-1)$?

$\chi(-1)$ must satisfy $x^2=1$

so $\chi(-1) = \pm 1$

could it be either? I think so - for now I will just write $\chi(-1)$

$\chi_{V_\psi}\begin{pmatrix}-1&0\\0&-1\end{pmatrix} = \sum_{aB} \psi\left(a\begin{pmatrix}-1&0\\0&-1\end{pmatrix}a^{-1}\right) = (p+1)\psi\begin{pmatrix}-1&0\\0&-1\end{pmatrix} = (p+1)\chi(-1)$

$\chi_{V_\psi}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \sum_{\substack{aB \\ \text{s.t. } gaB=a \\ \text{i.e. } \underline{a^{-1}ga \in B}}} \psi\left(a^{-1}\begin{pmatrix}1&1\\0&1\end{pmatrix}a\right)$ ↰ only one term in the sum

Note: nonsemisimple has only one fixed pt in $P_1(\mathbb{F}_p)$: ∞

$\begin{pmatrix}1&1\\0&1\end{pmatrix}r = r+1$ for $r\neq\infty$; $\begin{pmatrix}1&1\\0&1\end{pmatrix}\infty = \infty$

the coset which it fixes is simply B b/c $\begin{pmatrix}1&1\\0&1\end{pmatrix} \in B$ so $a^{-1}\begin{pmatrix}1&1\\0&1\end{pmatrix}a \in B$ for $a=I$

$= \psi\begin{pmatrix}1&1\\0&1\end{pmatrix} = \chi(1) = 1$

$\chi_{V_\psi}\begin{pmatrix}1&a\\0&1\end{pmatrix} = \ldots = \chi(1) = 1$ the same b/c a being square/nonsquare doesn't affect it

$\chi_{V_\psi}\begin{pmatrix}-1&1\\0&-1\end{pmatrix} = \sum_{\substack{aB \\ \text{s.t.} \\ \underline{a^{-1}\begin{pmatrix}-1&1\\0&-1\end{pmatrix}a \in B}}} \psi\left(a^{-1}\begin{pmatrix}-1&1\\0&-1\end{pmatrix}a\right) = \psi\begin{pmatrix}-1&1\\0&-1\end{pmatrix} = \chi(-1) = \chi_{V_\psi}\begin{pmatrix}-1&a\\0&-1\end{pmatrix}$

only for $a=I$; one fixed pt

$\chi_{V_\psi}\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} = \sum_{\substack{aB \\ \text{s.t. } gaB=aB \\ \text{ie } \underline{a^{-1}\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}a\in B}}} \psi\left(a^{-1}\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}a\right)$

Note: 2 fixed pts $(0,\infty)$ so 2 terms in this sum

since $\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} \in B$ already, one coset which is fixed is just B

then note $s\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}s^{-1} = \begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

$= \begin{pmatrix}0&\lambda^{-1}\\-\lambda&0\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

$= \begin{pmatrix}\lambda^{-1}&0\\0&\lambda\end{pmatrix} \in B$ so the other coset which is fixed is sB

$= \psi\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} + \psi\left(s\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}s^{-1}\right)$ ↶ $\lambda \in \mathbb{F}_p^\times - \{\pm1\}$

$= \psi\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} + \psi\begin{pmatrix}\lambda^{-1}&0\\0&\lambda\end{pmatrix} = \chi(\lambda) + \chi(\lambda^{-1})$

How many of these induced reps do we actually get?

well there are $p-3$ nonquadratic reps of $\mathbb{F}_p^\times$ b/c $\chi: g \mapsto \xi$ for $\xi \in \mathbb{F}_p^\times - \{\pm1\}$

but note that $\chi_1: g \mapsto \xi$ then $\chi_1(\lambda^{-1}) = \chi_1(\lambda)^{-1} = \chi_1(g^a)^{-1} = (\xi^a)^{-1} = (\bar{\xi})^a = \chi_2(\lambda)$

$\chi_2: g \mapsto \bar{\xi}$ ← complex conj. (if $\xi \in \mu_{p-1}$ then $\bar\xi \in \mu_{p-1}$ so this is valid rep)

$\chi_{V_{\psi_1}}: \begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} \mapsto \chi_1(\lambda) + \chi_1(\lambda^{-1}) = \chi_2(\lambda^{-1}) + \chi_2(\lambda) = \chi_2(\lambda) + \chi_2(\lambda^{-1})$

$\chi_{V_{\psi_2}}: \begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix} \mapsto \chi_2(\lambda) + \chi_2(\lambda^{-1})$ ← the same value

and $\chi_1(-1) = \chi_2((-1)^{-1}) = \chi_2(-1) \Rightarrow \chi_1, \chi_2$ give isomorphic reps of G

NO?

Hence we have $\frac{p-3}{2}$ "non quadratic" reps coming from $\chi: g \mapsto \xi$ for $\xi \in \mu_{p-1} - \{\pm1\}/_{\xi \neq \bar\xi}$

irreducible: $\langle \chi_{V_\psi}, \chi_{V_\psi}\rangle = \frac{1}{p\cancel{(p+1)}(p-1)}\left[(p+1)^{\cancel{2}} + (p+1)^{\cancel{2}} + 2\frac{\cancel{(p+1)}(p-1)}{2} + 2\frac{\cancel{(p+1)}(p-1)}{2} + \sum_{\lambda\in\mathbb{F}_p^\times-\{\pm1\}/\lambda\neq\lambda^{-1}} p\cancel{(p+1)}[\chi(\lambda)+\chi(\lambda^{-1})]^2\right]$

$= \frac{1}{p(p-1)}\left[2p+\cancel{2} + p\cancel{-1} + p\cancel{-1} + p\underline{\sum_\lambda[\chi(\lambda)^2+\chi(\lambda^{-1})^2+2]}\right] = \frac{1}{p(p-1)}[4p + 2p(p-3)]$

$= \frac{2p^2-6p+4p}{p(p-1)} = \frac{2p^2-2p}{p(p-1)} = 2$

suspiciously not irred...

$p\Big[\underbrace{\xi+\xi^2+\ldots+\xi^{p-2}}_{=0} + (p-3)2\Big]$

$\langle \chi_{V_{\psi_1}}, \chi_{triv}\rangle = \frac{1}{p\cancel{(p+1)}(p-1)}\left[\cancel{(p+1)} + \chi(-1)\cancel{(p+1)} + 2\frac{\cancel{(p+1)}(p-1)}{2} + 2\frac{\cancel{(p+1)}(p-1)}{2}\chi(-1) + p\cancel{(p+1)}\sum_{\lambda\in\mathbb{F}_p^\times-\{\pm1\}/\lambda\neq\lambda^{-1}}\chi(\lambda)+\chi(\lambda^{-1})\right]$

$= \frac{1}{p(p-1)}\left[\cancel{1} + \chi(\cancel{-1}) + p\cancel{-1} + \chi(-1)(p\cancel{-1}) + p\underbrace{\sum_{\xi\in\mu_{p-1}-\{\pm1\}}\xi}_{=0}\right]$

$= \frac{1}{p(p-1)}[p + \chi(-1)p]$

also: $0 = \xi^{p-1} - 1 = (\xi-1)(\xi^{p-2}+\xi^{p-3}+\ldots+\xi+1)$

so $\xi^{p-2}+\ldots+\xi+1 = 0$

so $\sum_{\xi\in\mu_{p-1}-\{1\}}\xi = -1$

$\Rightarrow -1 + \sum_{\xi\in\mu_{p-1}-\{\pm1\}}\xi = -1$

so $\sum_{\xi\in\mu_{p-1}-\{\pm1\}}\xi = 0$

irred $\Leftrightarrow \chi(-1) = -1$ suspicious b/c it doesn't have to be

Now fix $\chi: g \mapsto -1$ quadratic rep of $\mathbb{F}_p^\times$ $(\chi^2 = 1)$

this will send $\chi: \begin{matrix} \text{squares} \mapsto 1 \\ \text{nonsq} \mapsto -1 \end{matrix}$ i.e. $\chi: x \mapsto \left(\frac{x}{p}\right)$ gives us $\psi: \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto \chi(a)$ rep of B

which again induces to a rep of G : V_ψ

$\chi_{V_\psi}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \sum_{aB} \psi\left(a^{-1}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} a\right) = (p+1)\psi(I) = p+1$

$\chi_{V_\psi}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \ldots = \chi(-1)(p+1)$

I think this will not be irred; I think it splits into 2 irred characters of dim $\frac{p+1}{2}$ each

character on the rest should stay the same

example: $SL_2(\mathbb{F}_5)$ $|G| = 4 \times 5 \times 6 = 120$ -1 is a square mod 5 $\mathbb{F}_5^\times = \langle 3 \rangle$ ($\{1,2,3,4\}$)

squares: $\{1,4\}$ nonsquares: $\{2,3\}$ $M_4 = \{1,-1,i,-i\}$

									x^2-4x+1	x^2-x+1	
	size	1	1	12	12	12	12	30	20	20	
		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & a \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	
	trivial	1	1	1	1	1	1	1	1	1	
$\chi: 3 \mapsto 1$	steinberg	5	5	0	0	0	0	1	-1	-1	
$\chi: 3 \mapsto i$	Non quad. $\cong \chi: 3 \mapsto -i$	6	-6	1	1	-1	-1	$\chi(2)+\chi(3) = 0$	0	0	$\chi(-1) = \chi(4) = \chi(3^2) = i^2 = -1$
$\chi: 3 \mapsto -1$	Quadratic	6	6	1	1	1	1	-2	0	0	Not irred!
$\chi: 3 \mapsto -1$	Q_1	3	3	$\sqrt{2}$	$-\sqrt{2}$	1	1	-1	0	0	
	Q_2	3	3	$1-\sqrt{2}$	$1+\sqrt{2}$	0	0	-1	0	0	
$\frac{p-1}{2} = 2$	1	4 $\leftarrow p-1$									$\frac{p+3}{2} = 4$ remaining
	2	4									
$2 = 2$	3	2									
	4	2									

$\uparrow \frac{p-1}{2}$

or maybe there is an i in there? like $\sqrt{-2}, -\sqrt{-2}$, $1-\sqrt{-2}, 1+\sqrt{-2}$ ...?

$V_Q = V_{Q_1} \oplus V_{Q_2}$ so $\chi_{V_Q} = \chi_{V_{Q_1}} + \chi_{V_{Q_2}}$

$\frac{p-1}{2} + 2 = \frac{p-1+4}{2} = \frac{p+3}{2}$

Prop: trivial dim 1

steinberg dim p

$\frac{p-3}{2}$ non quadratic dim $p+1$

2 quadratic dim $\frac{p+1}{2}$

$\frac{p-1}{2}$ of dimension $p-1$

2 remaining of dim $\frac{p-1}{2}$

$\frac{p-3+p-1}{2} + 4 + 2$

$= p+4$ total reps

Centralizer of U? Normalizer of U?

$C_G(U) \subseteq N_G(U) \subseteq G$

$C_G(U) = \{\text{commute with } U\}$

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in U$ $\quad a \in F_p$ fixed

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & ax+y \\ z & az+w \end{pmatrix}$$

$\leftarrow$ want equal $\Rightarrow \begin{cases} x = x + az \\ ax + y = y + aw \\ z = z \\ az + w = w \end{cases} \Rightarrow \begin{cases} z = 0 \\ x = w \\ y \text{ is free} \end{cases} \Rightarrow \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \in C_G(U)$

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x+az & y+aw \\ z & w \end{pmatrix}$$

but since $x^2 = 1 \Rightarrow x = \pm 1$

so $\boxed{C_G(U) = \left\{\begin{pmatrix} \pm 1 & x \\ 0 & \pm 1 \end{pmatrix} : x \in F_p\right\} = ZU}$

$N_G(U) = \{g \in G \text{ s.t. } gU = Ug\}$ fixes U under conj.

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in U$ $\quad a \in F_p$ fixed

b/c det $= 1$ so inverse is just adj

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}^{-1} = \begin{pmatrix} x & ax+y \\ z & az+w \end{pmatrix}\begin{pmatrix} w & -y \\ -z & x \end{pmatrix} = \begin{pmatrix} xw - z(ax+y) & -xy + x(ax+y) \\ zw - z(az+w) & -zy + x(az+w) \end{pmatrix} \in U$$

so $\begin{cases} xw - \cancel{z}xa - \cancel{zy} = -\cancel{zy} + x\cancel{z}a + xw = 1 \\ z\cancel{w} - z^2a - \cancel{zw} = 0 \\ -xy + x^2a + xy \in F_p \text{ free} \end{cases} \Rightarrow \begin{cases} xw = 1 \\ -z^2a = 0 \\ x^2a \in F_p \text{ free} \end{cases}$ y is free $\Rightarrow \begin{matrix} w = x^{-1} \\ z = 0 \end{matrix} \Rightarrow \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \in N_G(U)$

$\boxed{\text{so } N_G(U) = B = \{\text{upper } \Delta \text{ matrices}\}}$