Subgroup of $GL_2(\mathbb{F}_\ell)$

We have $GL_2(\mathbb{F}_2) \cong S_3$ so we will assume $\ell > 2$; ℓ is a prime number.

Denote: $\mathbb{F}_{\ell^2}$ field with ℓ^2 element (unique upto isomorphism by Galois theory)

$V = \mathbb{F}_\ell^2$ $\quad k = \mathbb{F}_\ell$ $\quad$; ~~$V \cong L$ (any homomorphism~~)

$V' = \mathbb{F}_{\ell^2}^2$ $\quad L = \mathbb{F}_{\ell^2}$

$x \to \bar{x} = x^\ell$: Frobenious automorphism on $\mathbb{F}_{\ell^2}$

D is a line in V (subspace with dimension 1)

D': line in V'

an eigenline is vector subspace generated by an eigenvector

+) G. $B = \mathrm{Stab}_{GL_2(\mathbb{F}_\ell)} D$ called Borel subgroup defined by L

Remark: If $D = ke$ then choose f that

$$V = ke \oplus kf$$

then in basis $\{e, f\}$, every element of $\mathrm{Stab}_{GL_2(\mathbb{F}_\ell)} D$

has the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

+) For pair (D_1, D_2) $(D_1 \neq D_2)$ line in V

Set of all $g \in GL_2(\mathbb{F}_\ell)$ that $gD_1 = D_1$, $gD_2 = D_2$

form a group called split Cartan subgroup (defined by D_1, D_2)

Split Cartan subgroup usually denote by T

Remark: If H is normalizer of T

$$T = \left\{ g \in GL_2(\mathbb{F}_\ell) \;\middle|\; \begin{matrix} gD_1 = D_1 \\ gD_2 = D_2 \end{matrix} \right\}$$

$h \in H$ then $hTh^{-1} = \left\{ g \in GL_2(\mathbb{F}_\ell) \;\middle|\; \begin{matrix} ghke_1 = khe_1 \\ ghke_2 = khe_2 \end{matrix} \right\}$

and since any $g \in GL_2(\mathbb{F}_\ell)$ cannot preserve 3 distinct lines
g not homothety (which correspond to 3 independent eigenvector)

So $\{ke_1, ke_2\} = \{khe_1, khe_2\}$

So $h \in T$ or h exchange 2 lines

(For example $h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ exchange $k(0,1)$ and $k(1,0)$)

so $\# \, Norm_{GL_2(\mathbb{F}_\ell)} T / T = 2$

Also for $v_1 \in L_1$, $v_2 \in L_2$ we can see that in this basis v_1, v_2

g has form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $\quad ab \neq 0$

so every split Cartan subgroup isomorphic to $\mathbb{F}_\ell^\times \times \mathbb{F}_\ell^\times$

+) D' line in V' called non-defined over k if $D' \cap V = \{0\}$ and called defined over k if $D' \cap V \neq \{0\}$

we have few properties

~~Prop) $D' \neq \overline{D'}$ iff D' non defined over k~~

~~Proof) if $D' = \overline{D'}$ then $v \in D' \cap V$ $v \neq$ then $\overline{v}$~~

Proposition:) $D' = \overline{D'}$ iff $D' \cap V$ is line in V

"$\Leftarrow$" $D' \cap V = kv$ $\quad v \in V$

$D' = Lv \Rightarrow \overline{D'} = \overline{L}\overline{v} = Lv$

"$\Rightarrow$" $D' = Lv$

$v \neq 0 \quad \overline{v} = \lambda v \quad \lambda \in L^*$

so $\overline{\overline{v}} = v = \overline{\lambda}\,\overline{v} = \overline{\lambda}\lambda v$

$\Rightarrow \overline{\lambda}\lambda = 1$

hence $\lambda = \alpha^{\ell-1}$ $(\alpha \in \mathbb{F}_{\ell^2}^\times)$

$= \dfrac{\overline{\alpha}}{\alpha}$

$w = \overline{\alpha} v$ so $D' = Lw$

$\overline{w} = \alpha \overline{v} = \alpha . \lambda . v$

$= \overline{\alpha} . v = w$

So $w \in V \cap D'$

$D' \cap V$ is line in V $(= kw)$

View $GL_2(\mathbb{F}_\ell) \subset GL_2(\mathbb{F}_{\ell^2})$

Definition)

+) Non split Cartan subgroup defined by line D_1' non-defined over $\mathbb{F}_\ell$ / k is set of all $g \in GL_2(\mathbb{F}_\ell)$ that preserve D_1' (view action in V')

(usually denote by A)

Proposition) $D' \subset V'$ line

If $g \in GL_2(\mathbb{F}_\ell)$ that $g(D') = D'$

then $g(\overline{D'}) = \overline{D'}$

Proof) Consider $v \neq 0$; $v \in D'$ then

$g(v) = \lambda v$

so $\overline{g}(\overline{v}) = \overline{\lambda}\,\overline{v}$

but $g \in GL_2(\mathbb{F}_\ell)$ so $g = \overline{g}$ so $g(\overline{v}) = \overline{\lambda}\,\overline{v}$

so $g(\overline{D'}) = \overline{D'}$

Consider $D' \subset V'$ is a line non-defined over $\mathbb{F}_\ell$ / k

$A_{D'} = \mathrm{Stab}_{GL_2(k)}(D')$. ~~Ch~~ Fix some $v \neq 0$ $v \in D'$ then if $g \in A_{D'}$ then $gv = \lambda_g v$ for $\lambda_g \in L^\times$

Consider group homomorphism

$$F : A_D \to L^\times$$
$$g \to \lambda_g$$

Proposition) F is an isomorphism

+) We prove F is injective:

If $\lambda_g = 1$ then

$g(v) = v \quad \forall v \in D'$

$g(\overline{v}) = \overline{v} \quad \forall v \in D'$ so $g(u) = u \quad \forall u \in \overline{D'}$

D' non defined over $\mathbb{F}_\ell$ / k so $D' \neq \overline{D'}$ so $D' \oplus \overline{D'} = V$

So g is identity map

F is surjective) Let $\lambda \in L^\times$

we prove that exist g that $F(g) = \lambda$

D' non defined over h so $D' = \mathrm{Span}_L(1, u)$ with $u \in F_{\ell^2} \setminus F_\ell$

$(D' \cap V = \phi)$

so $\{1, u\}$ is basis of F_{ℓ^2} over F_ℓ

we choose $a, b, c, d \in F_\ell$ that

$a + bu = \lambda$

$c + du = \lambda u$

$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$ (since if not then $\lambda u = x\lambda$ for some $x \in h^\times$ but this cannot happen since $\lambda \neq 0$, $u \notin h^\times$)

So $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ map D' to D' and

$F(g) = \lambda$

So F is a group ~~m~~ isomorphism

From the above proposition we see ~~any~~ that every non-split Cartan subgroup is isomorphic to $F_{\ell^2}^\times$ (cyclic order $\ell^2 - 1$)

Remark) If H is normalizer of A

$A = \{ g \in GL_2(F_\ell) \mid g D' = D',\ D' \text{ non defined over } h \}$

$h \in H$ then $hAh^{-1} = \{ g \in GL_2(F_\ell) \mid g\, hD' = hD',\ D' \text{ non defined over } h \}$

Because $hD' \cap V = hD' \cap hV = h(D' \cap V) = \phi$ (since $h \in GL_2(F_\ell)$)

So hD' a line that non defined over h

So from the proposition) and $g \in GL_2(F_\ell)$ not homothety can not preserve 3 distinct eigenvalue

we have $hD' = D'$ or $hD' = \overline{D'}$

so $h \in A$ or h exchang D' and $\overline{D'}$

So ~~a~~ $\# \mathrm{Norm}_{GL_2(F_\ell)} A / A = 2$

In above notation if $\overline{u} = x + uy$ $(x, y \in F_\ell)$

$y \neq 0$ so element

$\begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix}$ swap D' and $\overline{D'}$

We propose our main theorem>

<u>Theorem></u> G is subgroup of $GL_2(F_\ell)$

If $\ell \mid \# G$ then either

a) G contained in a Borel subgroup

•) G contained in $SL_2(F_\ell)$

If $\ell \nmid \# G$ H be image of G in $PGL_2(F_\ell)$

then either:

(1) H cyclic, G contained in a Cartan subgroup

(2) H dihedral, G contained in normalizer of a Cartan subgroup

but not Cartan subgroup itself

(3) H is isomorphic to A_4, S_4, A_5

In case (2) ℓ must be odd.

In case (3) ℓ must be prime to $6, 6, 30$ respectively.

~~(1) H cyclic, G contained in a Cartan subgroup~~

~~(2) H dihedral, G contained in normalizer of a Cartan subgroup but not Cartan subgroup itself~~

~~(3) H isomorphic to A_4, S_4, A_5.~~

~~In case (2) l must be odd. In case (3) l must prime to 6, 6, 30 respectively.~~

We propose a lemma:

<u>Lemma1)</u> $g \in GL_2(\mathbb{F}_l)$ order prime to l.
Then g is diagonalizable in $GL_2(\mathbb{F}_{l^2})$

<u>Proof)</u> order of g is a then $g^a = I$

also characteristic polynomial of g is: $x^2 - tr(g)x + det(g) = 0$

$x^a - 1$ is separable polynomial in $\mathbb{F}_l$

consider ~~$gcd(x^a-1)$~~ $gcd(x^a - 1, x^2 - tr(g)x + det(g)) = q(x)$

$q(x)$ is separable polynomial (since it divides $x^a - 1$)

$deg\ q \le 2$

so q has all roots in $\mathbb{F}_{l^2}$ ($\mathbb{F}_{l^2}$ is unique quadratic extension of $\mathbb{F}_l$)

$q(g) = 0$ in $M_{2\times 2}(\mathbb{F}_l)$. All roots of q in $\mathbb{F}_{l^2}$
and they are pairwise distinct.

this show that g can be diagonalizable in $\mathbb{F}_{l^2}$.

~~Also, g has two eigenvector with distinct eigenvalue over $\mathbb{F}_{l^2}$~~

Lemma 2) if $\ell \mid |G|$ then either G contained in a Borel subgroup of $GL_2(\mathbb{F}_\ell)$ or G contains $SL_2(\mathbb{F}_\ell)$

Proof) choose $\sigma \in G$ with order G.

$$\sigma^\ell = I \quad \text{so} \quad (\sigma - I)^\ell = 0$$

so $(\sigma - I)^2 = 0$

So exist v that $(\sigma - I)v = 0$

Consider line $D = kv$. If every element of G fix D then G contained in Borel subgroup associated to D.

If not then $\sigma_1 \in G$ map D to D_1

$\sigma_1 \sigma \sigma_1^{-1}$ order ℓ

take $v_1 \in D_1$ then v and v_1 make σ and $\sigma_1 \sigma \sigma_1^{-1}$ has form

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \sigma_1 \sigma \sigma_1^{-1} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

($bc \neq 0$ since σ and $\sigma_1 \sigma \sigma_1^{-1}$ order ℓ)

So exist a power of σ and $\sigma_1 \sigma \sigma_1^{-1}$ has form

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

We have lemma

Lemma) $s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $u = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate $SL_2(\mathbb{F}_\ell)$ (can omit proved)

Proof) $T = s^{-1} u s^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

We know that s, T generate $SL_2(\mathbb{Z})$

$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL_2(\mathbb{F}_\ell)$ so $\bar{a}\bar{d} - \bar{b}\bar{c} = 1 \pmod{p}$

either $\bar{a}$ or $\bar{b}$ not equal to 0

assume $\bar{a} \neq 0$, choose lift a, c, d of $\bar{a}, \bar{c}, \bar{d}$

choose b lift of $\bar{b}$ that $\bar{b} \equiv b \pmod p$ (chinese remainder theorem)
$b \equiv 1 \pmod a$

Consider $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Put $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1+pe \ (e \in \mathbb{Z})$

$(a, b) = 1$ so choose m, n that $am - bn = 1$ (Bezout)

Consider $\begin{pmatrix} a & b \\ c-epn & d-epm \end{pmatrix}$

$$\det \begin{pmatrix} a & b \\ c-epn & d-epm \end{pmatrix} = a(d-epm) - b(c-epn)$$
$$= (ad-bc) - pe(am-bn) = \underline{1}$$

and $\begin{pmatrix} a & b \\ c-epn & d-epn \end{pmatrix}$ map to $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$

So by lemma 3 G contain $SL_2(\mathbb{F}_\ell)$

+) Remark> $GL_2(\mathbb{F}_\ell) / SL_2(\mathbb{F}_\ell) \cong \mathbb{F}_\ell^\times$ (via det map)

cyclic group order $\ell - 1$

So we can determine all such group in this case.

In case $\ell \nmid |G|$ view $H \in PGL_2(\mathbb{F}_{\ell^2})$

so $\ell \nmid |H|$

Order of H prime to ℓ

let $h \in H$ so order of h prime to ℓ, using lemma 1

every element of H is diagonalizable and has two distinct eigenvalue over $\mathbb{F}_{\ell^2}$

View $GL_2(\mathbb{F}_\ell) \subset GL_2(\mathbb{F}_{\ell^2})$

We propose a lemma:

Lemma 4) If $\sigma_1 \neq \sigma_2 \in H$ preserve an eigenline D_1'

then exist $D_2' \neq D_1'$ that $\sigma_1 D_2' = \sigma_2 D_2' = D_2'$

Proof) If σ_1, σ_2 has only D_1' is line stable under action of σ_1 / σ_2

Choose other eigenline D_3' of σ_1

then take $v_1 \in D_1$, $v_3 \in D_3'$

In basis $\{v_1, v_3\}$ we have

$$\sigma_1 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} c & b \\ 0 & e \end{pmatrix}$$

a, d, c, b, e nonzero (b non zero since $\sigma_2 D_3' \neq D_3'$)

then $\sigma_1^{-1} \sigma_2^{-1} \sigma_1 \sigma_2 = \begin{pmatrix} 1 & c^{-1} b(1 - a^{-1} d) \\ 0 & 1 \end{pmatrix}$

not identity since $a \neq d$ and this above element has order ℓ

(absurd)

$PGL_2(\mathbb{F}_\ell)$ act on set $\mathbb{P}(V) = \mathbb{P}^1(k)$ (set of lines in V)

so does H.

define $S = \{ D' \in \mathbb{P}(V)$ that exist h nontrivial, $h \in H$ that $h(D') = D' \}$

~~$d_1 \dots d_v$ representative of orbits under~~

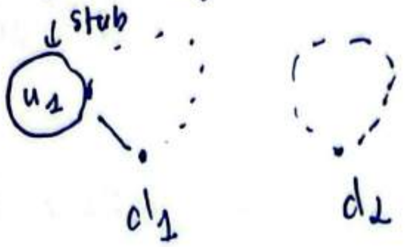
H act on S (~~via~~ because: if $h(D) = D$ then $(\ell h \ell^{-1})(\ell(D)) = \ell(D) \quad \forall \ell \neq h \in H$)

~~d_1~~ $H \longrightarrow \mathrm{Per}(S)$

$h \to (D \to h(D))$

S is finite. $d_1 \dots, d_v$ representative of orbits under action of H.

u_i is the number of elements of H fix d_i ($u_i > 1$ $\forall i$)
so if h is order of H then
orbit of d_i contain h/u_i elements.



Count the number of pair (ℓ, D)
where ℓ a non trivial element of H and $\ell(D) = D$.

We have
$$2h - 2 = (u_1 - 1)\frac{h}{u_1} \qquad + (u_v - 1)\frac{h}{u_v}$$

or $$2\left(1 - \frac{1}{h}\right) = \left(1 - \frac{1}{u_1}\right) + \dots + \left(1 - \frac{1}{u_v}\right)$$

We have $2 > \text{LHS} = \text{RHS} \geq \frac{1}{2} v$ so $v \leq 3$
If $v = 1$ $1 > \text{RHS} = \text{LHS} \geq 2\left(1 - \frac{1}{2}\right) = 1$ so $v > 1$
So $v = 2$ or $v = 3$.
We have 5 cases
(1) $v = 2$, $u_1 = u_2 = h$
(2) $v = 3$, $2 | h$, $u_1 = u_2 = 2$, $u_3 = \frac{h}{2}$
(3) $v = 3$, $h = 12$, $u_1 = 2$, $u_2 = u_3 = 3$
(4) $v = 3$, $h = 24$, $u_1 = 2$, $u_2 = 3$, $u_3 = 4$
(5) $v = 3$, $h = 60$, $u_1 = 2$, $u_2 = 3$, $u_3 = 5$

in Case (1) all element of H have same eigvalue (using Lemma 4)
so all element of G have same eigenvalue
so they lie on associated Cartan subgroup
(split or nonsplit depend on eigvalue
defined over F_ℓ or not)
H is Cyclic since D_1, D_2 two eigvalue (here we view in F_{ℓ^2})

We have

$$\Delta = \mathrm{Stab}_{GL_2(\mathbb{F}_{\ell^2})} D_1 \cap \mathrm{Stab}_{GL_2(\mathbb{F}_{\ell^2})} D_2 \cong \mathbb{F}_{\ell^2}^\times \times \mathbb{F}_{\ell^2}^\times$$

So H is subgroup of Δ / Δ_1 ← cyclic group since $\mathbb{F}_{\ell^2}^\times$ cyclic

$\left(\Delta_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{F}_{\ell^2} \right\}\right)$ so H is cyclic

(2) $v=3$, h even, $u_1 = u_2 = 2$, $u_3 = \frac{h}{2}$

we have a lemma

Lemma 3) If O is an orbit of action of H on S then $\overline{O}$ is also an orbit.

Proof) Pick $d_i \in O$ so O is set of all distinct eigenline among $h(d_i)$ for all $h \in H$.

we have $\overline{h(d_i)} = \overline{h}(\overline{d_i}) = h(\overline{d_i})$ for all $h \in H$

so $\overline{O}$ is an orbit that contains $\overline{d_i}$

We have 3 cases:

(2.1) $h = 2$ so ~~H is cyclic ($H \cong \mathbb{Z}/2\mathbb{Z}$)~~
~~we have 2 orbit with 1 elements and 1 orbit with 2 elements~~

~~so G~~ $u_3 = 1$ (absurd since all $u_i > 1$)

(2.2) $h=4$ so we have H has 4 elements

3 orbits with size 2.

Using the lemma 3 above we have at least 1 orbit called O that $O = \overline{O}$

assume $O = \{d_1, d_2\}$

so we have either $\overline{d_1} = d_1$, $\overline{d_2} = d_2$

or $\overline{d_1} = d_2$, $\overline{d_2} = d_1$

If $\bar{d}_1 = d_1$, $\bar{d}_2 = d_2$ so two eigenline $d_1\, d_2$ is defined over k

and $\mathrm{Stab}_H d_1 = H_0$ is cyclic group order 2 of H so normal in H

$h \notin H_0$ must interchange d_1 and d_2 so

inverse image of H_0 in G in split cartan subgroup of GL_2

the remaining elements of G interchange d_1, d_2 so

G lies in normalizer of ~~Car~~ split cartan subgroup but not

in Cartan subgroup itself

If $\bar{d}_1 = d_2$, $\bar{d}_2 = d_1$ So two eigenline d_1, d_2 non-defined over k

Similar as above for $H_0 = \mathrm{Stab}_H d_1$ cyclic order 2, normal in H.

inverse image of H_0 in G in non split Cartan subgroup of GL_2.

So G lies in normalizer of non-split Cartan subgroup but not

in Cartan subgroup itself

(2.3) if $h > 4$ so orbit of d_3 is only orbit with 2 elements (called O)

using lemma 6 we must have $O = \bar{O}$

~~so $O = \{d_3, d_4\}$~~ Assume $O = \{d_3, d_3'\}$

so $\mathrm{stab}_H (d_3) = H_0$ has index 2. by lemma 4, every element

of H_0 have same two eigenline so H_0 cyclic (like Case (1))

H_0 normal in H

inverse image of H_0 in G must be in Cartan subgroup of GL_2

(split or nonsplit depend on d_3 defined

or non-defined over k)

the other element of ~~H_0~~ G interchange d_3 and d_3'

So G lies in normalizer of a Cartan subgroup but not in

Cartan subgroup itself

(* Remark if $O = \{d_1, d_2\}$ is an orbit then d_1, d_2 are two eigenline

of all $g \in \mathrm{Stab}(d_1)$)

(3) $v = 3$, $h = 12$, $u_1 = 2$, $u_2 = u_3 = 3$

orbit of cl_3 has 4 element that permuted by H.

induced represent of H is faithful

$(H \hookrightarrow S_4)$

cl_3

Since there are 4 elements and no nontrivial element of H has more than two ~~eigenline~~. distinct eigenline.

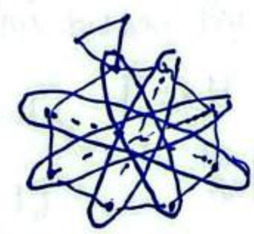
So H isomorphic to subgroup of S_4 with order 12

so $H \cong A_4$

(4) $v = 3$, $h = 24$, $u_1 = 2$, $u_2 = 3$, $u_3 = 4$

orbit of u_2 has 8 eigenline.

each eigenline has a stabilizer group with 3 elements.



Image

By sylow theorem. the number n_3 of 3-subgroups has property: $n_3 \equiv 1 \pmod 3$, $n_3 \mid 8$

so $n_3 \in \{1, 4\}$

we see that among list of 8 stabilizer groups corresponding to 8 eigenlines, no 3 groups can be equal since $h \in H$ cannot have 3 eigenline.

So in list of 8 stabilizer groups we have at least 4 ~~of~~ 3-groups that pairwise distinct

So $n_3 = 4$ and hence 8 eigenlines ~~che~~ are divide in 4 pairs

(each pairs are two eigenlines of an element with order 3

Also, each element of order 3 generate a 3-subgroups.

So ~~above~~ ~~4s~~ 8 eigenlines above is all eigenlines correspond to a elements of H of order 3.

if $h_0 \in H$ fixed each pairs. then because each pair has two elements
$h_0 \neq id$

order of h_0 is 2. So h_0 not fixed any eigenlines among 8 eigenlines (Since if not $h_0 \in$ Stab (lines among 8 lines) so h_0 order 3 absurd)

So h_0 interchange elements of each pairs $(*)$ If there is another h' that h' exchange elements of each pair then $h' h_0^{-1}$ preserve 8 lines so must the trivial

This mean that h_0 is unique with property $(*)$

Consider $l \in H$ then $(l h_0 l^{-1})^2 = id$

if $l h_0 l^{-1}$ order 2 then similar above

$l h_0 l^{-1}$ has property $(*)$ so $l h_0 l^{-1} = h_0$

so $l h_0 = h_0 l$

if $l h_0 l^{-1}$ order 1 then $h_0 = id$ (absurb)

So h_0 in centre of H. then consider $v \in Stab(d_2)$ nontrivial

$h_0 v$ has order 6. (condictiction since every $h_1 \in H$ has $h_1(D) = D$ so $h_1 \in Stab\, D$ but the latter group only has order among 2, 3, 9 by (3))

So $H \longrightarrow Per(4 \text{ pairs})$

is injective so $H \cong S_4$

Case (5)) $v=3,\ h=60,\ u_1=2,\ u_2=3,\ u_3=5$
each u_i prime

every element of H has prime order

($\forall h \neq 0\ h(D)=D$ so $h \in Stab(D) \leftarrow$ order prime)

if σ_1, σ_2 has same order ~~then~~ ($\sigma_1, \sigma_2 \in H$)

then ~~σ_1~~ choose D_1, D_2 that $\sigma_1(D_1)=D_1$
$\sigma_2(D_2)=D_2$

then $\langle\sigma_1\rangle = Stab(D_1)$
$\langle\sigma_2\rangle = Stab(D_2)$

but among 3 different orbits, 2 stabilizer group have same element must correspond to 2 elements of same orbits

this mean they are conjugate.

~~So σ_1, σ_2 conjugate~~ So two cyclic subgroups of same order are conjugate (*)

So any normal subgroup of H contain all or none of elements of any given order

H has 15 elements order 2 $\quad \frac{(2-1)}{2}\cdot\frac{60}{2} = 15$

20 elements order 3 $\quad \left(\frac{3-1}{2}\right)\cdot\frac{60}{3} = 20$

24 element order 5 $\quad \left(\frac{5-1}{2}\right)\cdot\frac{60}{5} = 24$

(divide by 2 since 2 eigenline of the element in same orbits by (*))

this mean H has only $H, \{1\}$ is normal subgroup

only simple group order 60 is A_5

so $H \cong A_5$

End the proof.

determinant induced a group homomorphism

$$\mathrm{mdet} : PGL_2(\mathbb{F}_\ell) \to \mathbb{F}_\ell^* / (\mathbb{F}_\ell^*)^2$$
$$g \to \det g$$

$\ell > 2$ we have $\mathbb{F}_\ell^* / (\mathbb{F}_\ell^*)^2 \cong \mathbb{Z}/2\mathbb{Z}$

<u>Corollary)</u> G subgroup of $GL_2(\mathbb{F}_\ell)$

H image of G in $PGL_2(\mathbb{F}_\ell)$

Assume $\# G^{ab} \mid \ell^m(\ell-1)$

$\mathrm{mdet}(H) = \mathbb{Z}/2\mathbb{Z}$

then one of following holds.

(i) G contains $SL_2(\mathbb{F}_\ell)$

(ii) G contained in a Borel subgroup

(iii) G contained in a normalizer of Cartan subgroup C but $G \not\subset C$

(iv) $H \cong S_4$

<u>Proof)</u> Assume that G contained in nonsplit Cartan subgroups C

C cyclic order ℓ^2-1

$G = G^{ab}$ abelian hence order diving $\ell-1$ by assumption

C cyclic order $(\ell-1)(\ell+1)$

G is included in unique subgroup of C order $\ell-1$

but this is subgroup of homothetic $\mathbb{F}_\ell^*$

so we are in case (ii)

$\mathrm{mdet}(G) = \mathrm{mdet}(H)$

H^{ab} has even order then H not isomorphic to A_4 or A_5

$(A_4^{ab} = \mathbb{Z}/3,\ A_5^{ab} = 1)$

Split Cartan subgroups included in some Borel subgroup:

So conclude ~~theorem~~. corollary

Proposition) Assume like in previous corollary.

Assume furthermore that $\text{mdet}\ G \to \mathbb{Z}/2\mathbb{Z}$

is the unique nontrivial morphism $G \to \mathbb{Z}/2\mathbb{Z}$

then

a) in case (ii) exists morphism $c_1, c_2 \ G \to \mathbb{F}_\ell^\times$

such that

$$\forall g \in G \quad tr(g) = c_1(g) + c_2(g)$$
$$det(g) = c_1(g) c_2(g)$$

b) in case (iii) then for all $g \in G$

$$det(g)^{-1}\, tr(g)^2 = 0, 1, 2 \text{ or } 4.$$

Proof) a) Assume we are in case (ii). Up to conjugacy

we may assume G included in group of upper triangular matrices

$g \in G$ then $g = \begin{pmatrix} a(g) & b(g) \\ 0 & d(g) \end{pmatrix}$

$a(g), d(g) \in \mathbb{F}_\ell^\times$. a, d are group morphism $G \to \mathbb{F}_\ell^\times$

set $c_1(g) = a(g)$
$c_2(g) = d(g)$ satisfy the require.

b) If we are in case (iii), mean that

exist 2 distinct line D_1', D_2' in V'

both defined over $\mathbb{F}_\ell$ or both not defined over $\mathbb{F}_\ell$

that G stabilizes $\{D_1', D_2'\}$ but not fix D_1' or D_2'

which $G \to S_2 \cong \mathbb{Z}/2\mathbb{Z}$

permutation the line. So this must coincide with mdet.

If mdet(g) nontrivial then g exchanges D_1' and D_2'

In suitable basis g has form

$$\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \quad \text{so } \operatorname{tr}(g) = 0$$

c) If we in case (iv). Any element of S_4 has order 1, 2, 3 or 4.

It follows that for all g in G there is $n \in \{1, 2, 3, 4\}$ that g^n is homothety

if x, y eigen values of g in $F_{\ell^2}^{\times}$ $\quad x^n = y^n$ so $(x/y)^n = 1$

(i) if $x = y$ $\quad \det(g)^{-1} \operatorname{tr}(g)^2 = \frac{(x+x)^2}{x^2} = 4$

(ii) x/y order 2 then $x = -y$

$$\det(g)^{-1} \operatorname{tr}(g) = 0$$

(iii) x/y order 3 then $x = \zeta y$ $\quad (\zeta^2 + \zeta + 1 = 0)$

$$\frac{\operatorname{tr}(g)^2}{\det(g)} = \frac{(\zeta y + y)^2}{\zeta y^2} = \frac{(\zeta+1)^2}{\zeta} = \zeta^4/\zeta = 1$$

(iv) x/y order 4 then $x = iy$ $\quad i^2 = -1$

$$\frac{\operatorname{tr}(g)^2}{\det(g)} = \frac{(iy + y)^2}{iy^2} = \frac{(i+1)^2}{i} = 2$$

$\square$