Last time: If $G \subseteq S_n$ 4-sharp + nontriv $\Longrightarrow n = 11$.

Thm: Let ~~the~~ $G \subseteq S_{n+1}$ be trans, and $H = G_{n+1}$ = stab. of $n+1$. Let $k \geq 1$.

(1) Then G is $k+1$ trans $\iff$ H is k trans on $\{1, \dots, n\}$

(2) . . . . . sharp . . . sharp

Pf (1) $\Rightarrow$ Given $a_1 - a_k, b_1 - b_k \in \{1, \dots, n\}$

$\exists\, g \in G$ such $a_1 - a_k, n+1 \xrightarrow{g} b_1 - b_k\ n+1$

Note $g \in H$.

$\Leftarrow$ Given $a_1 - a_{k+1}, b_1 - b_{k+1} \subseteq \{1 - n+1\}$

G tran $\Rightarrow$ $(a_1, \dots a_{k+1}) \xrightarrow{g_1} (c_1, \dots c_k, n+1)$

$(b_1 \dots b_{k+1}) \xrightarrow{g_2} (d_1 \dots d_k, n+1)$

$\exists\, g_3 \in H: (c_1 \dots c_k) \to (d_1 - d_k)$ $\boxed{g_2^{-1} g_3 g_1}$ $\square$

Fact (exercise). If $G \subseteq S_{n+1}$ is transitive. Then G is trivial iff G_{n+1} trivial.

Prop: Let $G \subseteq S_n$, sharp 5, nontriv. Then $n = 12$.

Pf $G_n \subseteq S_{n-1}$ is sharp 4 by Thm. nontriv by fact. $\Rightarrow$ $n-1 = 11 \Rightarrow n = 12$. $\square$

Prop: $G \subseteq S_n$, k-sharp $k \geq 6$, nontriv cannot happen.

Pf $k = 6$. $G_n \subseteq S_{n-1}$ 5 trans., nontriv $\Rightarrow n-1 = 12 \Rightarrow n = 13$. $\Rightarrow$ This contradicts earlier result.

If $k \geq 7$, $G \subseteq S_n$, sharp k, nontriv., then G_n is $k-1$ sharp nontriv

$\square$

Before proving $\exists\ M_{11} \subseteq S_{11}$ sharp 4 nontri

and $\cdots M_{12} \subseteq S_{12}$ -- 5, non

Sharp 3 transitive

Thm: q

(1) For p prime, $q = p^k$, $\exists$ a sharp 3 trans. sg $L(q) \subseteq S_{q+1}$

(2) For p prime, $\neq 2$, k even, $\exists$ a sharp 3 trans. s.g. $M(q) \subseteq S_{q+1}$.

(3) $M(q) \not\cong L(q)$ (stronger than not conj in S_{q+1})

(4) nothing else.

Remark $L(q)$

1. (1) more natural.
2. (2) $M(q)$ is needed for construct M_{11}.
3. $q = 9$ only.

(4) don't do

Going to happen

$$(M_{11})_{11} = M(9)$$

$$(M_{12})_{12} = M_{11}$$

$|L(q)| = (q+1)q(q-1) = M(q)$

sharp 3

$M(9) = 10 \cdot 9 \cdot 8 = 720$

$\Rightarrow M_{11} = 11 \cdot 720 = \ldots$

Quick review of finite fields.

(1) F finite field $\Rightarrow |F| = p^k$ p prime

(2) $\forall p\ \forall k$ p prime, $\exists$ F a f.f. such $|F| = p^k = q$ and all iso.

(3) F is the splitting fields of $x^{p^k-1}-1$ over $\mathbb{Z}/p$

(4) $(F^*, \times)$ ~~cydic~~ cyclic.

(5) $p=2 \Rightarrow$ all elements of F^* are squares. (Pf) $x \to x^2$

$p \neq 2 \Rightarrow$ ½ the elements of F^* are squares $\Rightarrow \ker = \{1,-1\}$

(6) -1 a square $\Leftrightarrow 4 \mid |F^*|$ exercise

(7) $\mathrm{Aut}_{\text{field}}(F_q) \cong \mathbb{Z}/k$ $(q = p^k)$

A generator is $x \longrightarrow x^p$ (Frobenius automorphism).

$L(q)$. $\quad X = F_q \cup \{\infty\} \Rightarrow |X| = q+1 = p^k+1$

Def

$L(q) \subseteq S_{q+1}$ are the perm.'s of ~~$\{1 \ldots q+1\}$~~ X of the form

$$x \longrightarrow \frac{ax+b}{cx+d} \qquad a,b,c,d \in F \qquad ad-bc \neq 0$$

$$\infty \longrightarrow a/c \qquad -d/c \longrightarrow \infty$$

---

mapping not determine a,b,c,d

Prop: Closed under composition

$f_{a'b'c'd'} \circ f_{abcd} = f_{a^*b^*c^*d^*}$ where

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$$

Pf Exercise. $\square$

$\Rightarrow$ inverses, i.e. bij. $\quad a = d,\ b = 0 = c \Rightarrow x \to x$ identity

---

$\Rightarrow$ $L(q)$ is sharp 3 trans.

First thm of day

(need $L(q)$ trans. ✓)

Thm $L(q) \leq S_{q+1}$ sharp 3 trans.

Pf Let $H = L(q)_\infty$ = stab. of ∞. $\leq S_q$

Note $\infty \to \infty \Leftrightarrow c = 0$

$H(q) = \{x \to ax+b,\ a,b \in F,\ a \neq 0\}$.

(note $c = 0 \Rightarrow d \neq 0$)

a,b determine the mapping Ex.

$|H(q)| = q(q-1)$. ✓

subclaim: $H(q) \leq S_q = S_F$ sharp 2 trans.

Pf $(x,y) \in F_q \times F_q$ $x \neq y$,
$(x',y') \in F_q \times F_q$ $x' \neq y'$

NTS $\exists!$ (a,b) $a \neq 0$ s.t. $(x,y) \to (x',y')$

i.e. $ax+b = x'$, $ay+b = y'$ $\Leftrightarrow \begin{bmatrix} x & 1 \\ y & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix}$

$x \neq y \Rightarrow \exists!$ sol $\square$

Another view of $L(q)$

$GL(2, \mathbb{F}_q)$ acts on $\mathbb{F}_q^2$

trans. + faithful but not primitive.

The 1-d ss. $\setminus (0)$ are blocks

Here we can consider $\mathbb{P}^1$ P_1, projective line i.e. the set of 1-d. sspaces

$$|P_1| = \frac{q^2-1}{q-1} = q+1$$

Think of $GL(2, \mathbb{F}_q)$ acting on P_1

Lost faithfulness: So mod out by Kernel of action and get a s.g. of S_{q+1}

Fact: Kernel $= (cI)_{c \neq 0}$.

Hence we get $\frac{GL(n,q)}{(cI)_{c \neq 0}} \leq S_{q+1}$

$PL(n,q)$ ''

Exercise $PL(n,q) \leq S_{q+1} \Longleftrightarrow$

'' $L(q) \leq S_{q+1}$

Identify $\mathbb{P}^1 \longleftrightarrow F \cup \infty$

$(a,1) \quad a$

$\square$

2nd construct $M(q)$ $q = p^k$

proof $k = 2m$

Note the l^{th} power of the Frob. auto $(x \to x^p)$ is $x \to x^{p^l}$

Let $\sigma(x) = x^{p^m} = m^{\text{th}}$ power of F.A

$\sigma(x)$ has order 2 Exercise

$X = F_q \cup (\infty)$ $|X| = q+1$

$M(q) \in S_X$ is the set of bij. of X follow

$$\begin{cases} x \longrightarrow \dfrac{ax+b}{cx+d}, & ad-bc \neq 0 \\ & ad-bc = \square \\ x \longrightarrow \dfrac{a\sigma(x)+b}{c\sigma(x)+d} & ad-bc \neq 0 \\ & ad-bc \neq \square \end{cases}$$

Rem. $p=2$ $M(q) = L(q)$

$\infty \to \frac{a}{c}$

$-\frac{d}{c} \to \infty$ if $ad-bc = \square$

$\sigma\left(-\frac{d}{c}\right) \to \infty$ if $ad-bc \neq \square$

Prop: $M(q)$ is a s.g.

pf (Exercise)

use (1) $\begin{vmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & \sigma(d) \end{vmatrix} = \sigma \begin{vmatrix} a & b \\ c & d \end{vmatrix}$

(2) σ preserves $\square$'s

(3) product of 2 non $\square$'s is a $\square$

$\square$

Prop. $M(q)$ is sharp 3 on $\{k - q+1\}$

"pf" $S(q) = M(q)|_{\infty}$ $(\Leftarrow c=0)$

$$= \begin{cases} x \longrightarrow ax+b & a \neq 0 \\ & a = \square \\ x \longrightarrow a\,\sigma(x)+b & a \neq \square \end{cases}$$

map determines a, b

Key step! (Exercise)

$S(q)$ is sharp 2 trans. on $\{1 - q\}$

$\Rightarrow M(q)$ is sharp 3 $\square$

$|L(q)| = |M(q)| = (q+1)q(q-1)$

Thm $L(q) \not\cong M(q)$ $q = p^k$

$p \neq 2$ $k = 2m$

Pf. Proof if $q = 9$

$|L(q)| = |M(q)| = 10 \cdot 9 \cdot 8 = 720.$

$720 = \cancel{5\,3}\ 5\,3^2\,2^4$

Proof is done by showing the Sylow 2-SG. are non iso.