FINITE SIMPLE SUBGROUP OF TRANSITIVE PERMUTATION GROUP OF PRIME DEGREE P

YIXU QIU

1. Introduction

From Last Summer to now, I have done research under the mentorship of Dr. Tucker. Our research started with reading some papers about the Grigorchuk group and group growth, which shows the tree structure and transitive group action.

This special structure raised our interest about the subgroup of the transitive permutation group. Thus, we wanted to find out for which n does $G \leq S_n$ contain two normal subgroups of the same index N_1, N_2 with only N_1 is transitive (acting on [n]). Finally, we proved that group S_{pq} with p, q are prime,$p < q$, contain two normal subgroups of same index N_1, N_2 with only N_1 is transitive if and only if $p|q$.

In our proving process, we have attempted to start our research with simple examples, such as S_5, S_7, S_{11}... This has led us to see some interesting groups, like Mathieu groups. This also allows us to read and cite Jone Gareth's papers related to the subgroup of primitive permutation groups.

This series of research processes has filled me with interest in the subgroups of transitive permutation groups of prime degree. Have we figured out all types of these subgroups? What are their similarities or differences in nature?

To start to discuss the transitive subgroup of S_p, let we review the definition of transitive subgroup:

Definition 1.1. A subgroup G of S_n is called a transitive subgroup of S_n if it acts transitively on the set 1,2,...,n.

For example, Dihedral group D_p is a transitive subgroup of S_p with it have rotation r that act transitively on $p - cycle$. Thus, which groups will have the same properties with the transitive permutation on p elements? And what kind of subgroups they have? In this paper, we will discuss the classification of transitive permutation group of prime degree.

2. Burnside's result

The transitive group of prime degrees has always received a lot of attention. In 1911, Burnside classified transitive groups of prime degree, showing that such groups are doubly transitive or contain a normal regular $p-group$ with p prime[2]. Then, with a well-known Classification of the finite simple groups (CFSG), all doubly transitive groups are known([8], Thm 5.3), which means all doubly transitive groups of prime order are known, so we can easily obtain the Burnside's theorem result:

Theorem 2.1. *Burnside's Result In Doubly Transitive Group A group G which is at least doubly transitive either must be simple or must contain a simple group H as a normal subgroup.*

Let we recall the definition of doubly transitive:

Definition 2.2. A group action of a group G on a set S is said to be **doubly transitive** if given any (x, y) and (x', y') with $x \neq y$, $x' \neq y'$, all elements of S, there exists $g \in G$ such that $gx = x'$ and $gy = y'$.

Here, we only discuss the transitive permutation group of the prime degree case.

Theorem 2.3. *Let G be a transitive permutation, then G is either doubly transitive or solvable.*

Let us prove the theorem 2.3 step by step.[3]

Proposition 2.4. *Let U be a non-empty, proper subset of $\mathbb{F}_p\backslash\{0\}$. Let π be a permutation of $\mathbb{F}_p$ such that $i - j \in U$ for $i, j \in \mathbb{F}_p$ implies $\pi(i) - \pi(j) \in U$. Then there are $a, b \in \mathbb{F}_p$ such that $\pi(i) = ai + b$ for all $i \in \mathbb{F}_p$.*

Proof. By an iterated application of π, since π is in finite order, we can see that $i-j \in U$ if and only if $\pi(i)-\pi(j) \in U$. In particular, replacing U by its complement in $\mathbb{F}_p\backslash\{0\}$ preserves the assumption. Therefore we can assume $|U| \leq \frac{p-1}{2}$.

Let $i \in \mathbb{F}_p$ be fixed. For $u \in U$ we have $(i + u) - i \in U$, hence $\pi(i+u)-\pi(i) \in U$. As π is a permutation, the elements $\pi(i+u)-\pi(i)$ are different for different u. Thus $\{\pi(i+u)-\pi(i) \mid u \in U\} = U$, hence $\{\pi(i + u) \mid u \in U\} = \{\pi(i) + u \mid u \in U\}$. In particular, for all $w \in \mathbb{N}$ we obtain

$$\sum_{u\in U} \pi(i + u)^w = \sum_{u\in U} (\pi(i) + u)^w.$$

Let $f(X) \in \mathbb{F}_p[X]$ be the polynomial of degree $n \leq p-1$ with $f(i) = \pi(i)$ for all $i \in \mathbb{F}_p$ (note that $n \neq 0$). Suppose $wn \leq p-1$. Then $\sum_{u\in U} f(X+u)^w - \sum_{u\in U}(f(X)+u)^w$ is a polynomial of degree $< p$ which vanishes identically on $\mathbb{F}_p$, thus

$$\sum_{u\in U} f(X+u)^w - \sum_{u\in U}(f(X)+u)^w = 0.$$

Setting $S(k) = \sum_{u\in U} u^k$, by the binomial identity we obtain that

$$\sum_{u\in U}(f(X+u)^w - f(X)^w) = \sum_{k\geq 1} \left(\begin{array}{c} w \\ k \end{array} \right) S(k) f(X)^{w-k}.$$

Note that all derivatives of a polynomial $P \in \mathbb{F}_p[X]$ of degree $\leq p-1$ are linearly independent with decreasing degrees, and since $f(X)^w$ is a polynomial of degree nw, X^{nw} is an $\mathbb{F}_p$-linear combination of the derivatives of $f(X)^w$. Thus we can obtain that

$$\sum_{u\in U}((X+u)^{nw} - X^{nw}) = \sum_{k\geq 1} S(k) g_{w-k}(X),$$

where $g_\ell(X)$ is a polynomial of degree at most ℓn.

Let $r \geq 1$ be minimal with $S(r) \neq 0$. Then the degree of the right handside is at most $n(w-r)$.

Suppose that $r \leq nw$. Then the coefficient of X^{nw-r} on the left handside is (up to a nonzero factor) $S(r)$. Since $S(r) \neq 0$, we must have $nw - r \leq n(w-r)$, so $n = 1$, and we are done.

It remains to consider $r - 1 \geq nw$. Suppose we have chosen w maximal with $nw \leq p-1$. Then $p-1 < n(w+1) \leq 2nw \leq 2(r-1)$, so $r > (p+1)/2$.

This shows $S(k) = 0$ for $k = 1, 2, \ldots, (p-1)/2$. Assume that $U = \{u_1, \ldots, u_k\}$. The corresponding Vandermonde matrix $V := \left(u_j^{i-1}\right)_{i,j=1,\ldots,k}$ is invertible. Now let M be the matrix $\left(u_j^i\right)_{i,j=1,\ldots,k}$. Then, by the multilinearity of the determinant, it follows that

$$\det(M) = \det\left(M^T\right) = u_1 \ldots u_k \cdot \det\left(V^T\right) = u_1 \ldots u_k \cdot \det(V) \neq 0$$

since $0 \notin U$ and $\det(V) \neq 0$. Therefore, M is invertible as well. Note that the sum of the entries of each column j of M is equal to $S(j)$. As $k = |U| \leqslant (p-1)/2$ and $S(j) = 0$ for $j = 1, 2, \ldots, (p-1)/2$, we obtain $vM = 0$ for $v = (1, \ldots, 1) \in \mathbb{F}_p^k$, contradicting the fact that M is invertible. Thus, $|U| \geqslant (p+1)/2$, again a contradiction.

□

With the proposition, we can prove Theorem 2.3:

Proof. Let G be a transitive permutation group on p elements. As p divides the order of G, there is an element $\tau \in G$ of order p. Assume that G acts on $\mathbb{F}_p$, with $\tau(i) = i+1$ for all $i \in \mathbb{F}_p$. Suppose that G is not doubly transitive. So G has at least two orbits on the pairs (i, j) with $i \neq j$. On the other hand, τ permutes cyclically the pairs (i, j) with constant difference, so there is a non-empty proper subset U of $\mathbb{F}_p \backslash \{0\}$ such that $\pi(i) - \pi(j) \in U$ for all $\pi \in G$ and i, j with $i - j \in U$. By the proposition, G is a subgroup of the group of permutations $i \mapsto ai + b$ with $a \in \mathbb{F}_p \backslash \{0\}, b \in \mathbb{F}_p$. In particular, G is solvable. □

Now, let we go back to the non-solvable case of Burnside's result. The structure of finite primitive groups is characterized by the famous O'Nan-Scott Theorem(Jordan, [5], 4.1A). Here, we only discuss the almost simple structure.

Definition 2.5. A finite group G is **almost simple** if there exists a non-abelian simple group S such that $S \subset G \subset Aut(S)$.

G embeds into $Aut(S)$ in a way that contain S. Note that S embeds into S by conjugation. All the associations with automorphisms are by using conjugation.

Definition 2.6. a **characteristic subgroup** is a subgroup that is mapped to itself by every automorphism of the parent group.

Definition 2.7. A group is said to be **characteristically simple** if it has no proper nontrivial characteristic subgroups

Definition 2.8. A nontrivial subgroup H of a group G is termed a **minimal normal subgroup** if it is normal and for any normal subgroup K of G such that $K \leq H$, either $K = H$ or K is trivial.

Theorem 2.9. *Let G be a finite group and let N be a minimal normal subgroup of G. Then N is characteristically simple*

Lemma 2.10. *A finite group is characteristically simple if and only if it is the direct product of isomorphic simple groups*

Theorem 2.11. *Doubly transitive groups are primitive*

Proof. To prove this, we need to show every block is trivial block. Take a block Y with two distinct elements y_1, y_2. Given an arbitrary $x \in X$, since G is doubly transitive, we can choose $\tau \in G$ such that $\tau(y_1, y_2) = (y_1, x)$. But then $\tau Y \cap Y \neq \emptyset$, since y_1 is in both. Thus $\tau Y = Y$, so $x \in Y$ as well. Thus, $Y = X$. □

Thus, we can start our prove the theorem 2.1: let G be a doubly transitive permutation group of prime degree p on a finite set Ω, and

let $N \neq id_G$ be a minimal normal subgroup of G. We wanted to show that $N \subset G \subset Aut(N)$.

Proof. With theorem 2.9, G is primitive on p elements, thus, N is transitive on Ω and N is characteristically simple. Which means there exist simple group $S_1, S_2, ..., S_K$ such that$N \cong S_1 \times S_2 \times ...S_k$ and $S_1 \cong S_k$ for all $1 \leq i \leq k$. If N is solvable, then $|N| = p$ and $Nisregular$, implying $N = S_1 = C_p$. Thus, N is the unique minimal normal subgroup, so N is the unique Sylow $p - subgroup$ of G so that G is solvable. Thus, it is a contradiction, so N is not solvable, and so is S_1. Thus, S_1 is non-abeliean. As N is transitive on Ω, we have $p||N|$; in particular, $p||S_1|$. If $k > 2$, then p^k is a factor of $|N|$, a contradiction to $N \subset G \subset S_p$. Therefore $k = 1$ and $N = S_1$. Hence G contains a non-abelian simple minimal normal subgroup N. □

So we prove $N \leq G$ and we need to show $G \leq Aut(N)$

Definition 2.12. the centralizer of a subset S in a group G is the set $C_G(S)$ of elements of G that commute with every element of S, or equivalently, such that conjugation by g leaves each element of S fixed.

Lemma 2.13. *Let G be a transitive permutation group of prime degree p and let S be a minimal normal subgroup of G such that S is non-abelian and simple. Then $C_G(S) = id_G$.*

Proof. Let $s \in C_G(S) \cap S$ and $g \in G$, then, we have $g^{-1}sg = g^{-1}gs = s$. Thus, $C_G(S) \cap S$ is a normal subgroup of S. As S is simple, we should have either $C_G(S) \cap S = id_G$ or $C_G(S) \cap S = S$. For the first case, S is a subgroup of $C_G(S)$; thus, S is abelian, a contradiction. Thus, $C_G(S) = id_G$. □

With Lemma 2.13, we have $Aut(N) = id_G$.

Theorem 2.14. *(N/C Theorem) For a subgroup H of group G, the N/C Theorem states that the factor group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$, the group of automorphisms of H.*

By N/C Theorem, thus we have $G = G/id_G = N_G(N)/C_G(N) \leq Aut(N)$ Thus, G is almost simple.

3. Classification of the finite simple groups

Back to the history of Classification of the finite simple groups, in 1983, Guralnick studied primitive simple groups of prime power degree:

Theorem 3.1. *(Guralnick,[4]) Let S be a non-abelian simple group with $H < S$ and $|S : H| = p^a, p$ prime. (S is acting on the cosets of H. And given any embedding of S into the permutation group, we can take H to be the point stabilizer of a point.) Then one of the following statements holds:*

(1) $S = A_n$ and $H = A_{n-1}$ with $n = p^a$.

(2) $S = \mathrm{PSL}(n, q)$ and H is the stabilizer of a point or a hyperplane of $\mathbb{F}_q^n$. Then $|S : H| = (q^n - 1)/(q - 1) = p^a$. (Note that n also is prime.)

(3) $S = \mathrm{PSL}(2, 11)$ and $H = A_5$.

(4) $S = M_{23}$ and $H = M_{22}$ or $S = M_{11}$ and $H = M_{10}$.

(5) $S = \mathrm{PSU}(4, 2) \cong \mathrm{PSp}(4, 3)$ and H is a parabolic subgroup of S of index 27.

We will define the $\mathrm{PSL}(n, q), M_{23}$, and so on later.

G.Jones's PhD thesis in 1975, investigated primitive permutation groups of prime power degree, but at that time, an explicit description on such groups was not available. But he points out that

Lemma 3.2. *Every finite simple group is either A_n, $PSL_n(F_q)$, one of sporadic groups, or some other things like $PSL_n(F_q)$. That classification says all the prime degree permutation groups that are primitive are:*

(1)Generalized dihedral.

(2)A_n or S_n.

(3)Weird ones for 11 which is $G = PSL_2(11), M_{11}, and M_{23}$ with $q = 11, 11$ and 23, which have the permutation group of the form $(11^3 - 11)/2$ with $PSL_2(11)$ is not isomorphic to A_{11}.

(4)General simple semilinear groups over finite fields, which are simple extensions of $PSL_n(F_q)$, which acts on a set of size $q^{n-1} + q^{n-2} + ... + 1$

With Considering $a = 1$ in Guralnick's theorem we obtain the desired groups.

Corollary 3.3. *Let G be an almost simple transitive permutation group of prime degree p, in particular, $S \leqslant G \leqslant \mathrm{Aut}(S)$ for some non-abelian simple group S. Then S is one of the following groups:*

(1) $S = A_p$

(2) $S = \mathrm{PSL}(n, q)$ with $p = (q^n - 1)/(q - 1)$, where n is prime;

(3) $S = \mathrm{PSL}(2, 11)$ with $p = 11$

(4) $S = M_{11}$ with $p = 11$ or $S = M_{23}$ with $p = 23$.

Proof. Let G be almost simple and let S be non-abelian and simple such that $S \leqslant G \leqslant \mathrm{Aut}(S)$. Moreover, let G be a transitive permutation

group of prime degree p on Ω. Let $\omega \in \Omega$ be fixed. We set $H := G_\omega$. Then, by the orbit stabilizer theorem, we have $|G : H| = p$, and H is a maximal subgroup of G. Hence $HS = H$ or $HS = G$. Since S is a subgroup of G, the action of S on Ω is faithful. If $HS = H$ then $S \leqslant H = G_\omega$ and thus every element of S stabilizes ω, a contradiction to S being transitive on Ω, since $\omega^S = \Omega$ by the definition of transitivity. Hence $HS = G$ and the second isomorphism theorem implies

$$p = |G : H| = |HS : H| = |S : S \cap H|$$

The claim follows by applying Theorem 3.1 to S.

□

4. Classification applied

Now, let we discuss the four cases in Corollary 2.9. For case 1, Jordan[5] has proven the Jordan's theorem

Theorem 4.1. *(Jordan,[5],3.3E) let G be a primitive permutation group on Ω of degree n that contains a cycle of prime length p fixing $k \geq 3$ points, so that $G \leq Sym(\Omega)$. Then, $A_n \leq G$.*

Proof. We will skip $p = 2$ or 3 cases here. Thus, suppose $p \geq 5$ andΩ is finite of size n, assume $n \geq p + 3$. We wanted to show that $G \geq A_\omega$. First of all, we wanted to show G is doubly transitive and for each $\alpha \in \Omega$, $_\alpha$ acts primitively on Ω/α.
Now, let consider the set $\mathcal{S}$ consisting of all $\Gamma \subseteq \Omega$ such that $\Gamma \neq \Omega$ and $G_{(\Omega\backslash\Gamma)}$ acts primitively on Γ. Then $\mathcal{S} \neq \emptyset$ because $\text{supp}(x) \in \mathcal{S}$.

Lemma 4.2. *(Jordan, [5], 3.3.16) Let H and K be subgroups of* $\text{Sym}(\Omega)$ *with supports Δ and Γ respectively. If each of H and K acts primitively on its support, and $\Delta \cap \Gamma \neq \emptyset$, then $\langle H, K\rangle$ acts primitively on $\Delta \cup \Gamma$.*

Thus, with lemma 4.2, we have if $\Delta, \Gamma \in \mathcal{S}$ with $\Delta \cap \Gamma \neq \emptyset$ and $\Delta \cup \Gamma \neq \Omega$, then $\Delta \cup \Gamma \in \mathcal{S}$. Now, Let Δ be a maximal element of $\mathcal{S}$ containing $\text{supp}(x)$, we claim that $|\Delta| = n - 1$. With G is primitive, there exists $y \in G$ such that $\Delta^y \cap \Delta \neq \emptyset$ or Δ. And it is clearly that $\Delta^y \in \mathcal{S}$, so by the maximality of Δ, we can get that $\Delta^y \cup \Delta = \Omega$. Thus, we have $n < 2|\Delta|$.
Now, suppose that $\delta \in \Omega\backslash\Delta$. Since we have $2|\Delta| > n$, for all $z \in G_\delta, \Delta \cap \Delta^z \neq \emptyset$, and we have $\delta \notin \Delta \cup \Delta^z$. Thus, $\Delta \cup \Delta^z \in \mathcal{S}$. So by the maximality of Δ, $\Delta = \Delta^z$ for all $z \in G_\delta$. Since G is primitive, G_δ is a maximal subgroup of G, and so $G_\delta = G_{\{\Delta\}}$. Since this is true for all points $\delta \in \Omega\backslash\Delta$, and the point stabilizers of G are distinct maximal subgroups since G is not regular, therefore $\Omega\backslash\Delta = \{\delta\}$ as claimed.

From the result above, we get that G is doubly transitive, and G_δ acts primitively on its support and G_δ contain a 3-cycle.
Then, we can use induction for $n \geq p+4$ to show G_δ still contains a 3-cycle.

Theorem 4.3. *(Jordan, [5], 3.3A(i)) Let G be a primitive subgroup of $Sym(\Omega)$, if G contains a 3-cycle, then $G \leq A_n$*

Thus, with Theorem 4.3, done. □

Gareth Jones's 2014 paper[6] gives a more general theorem that also deals with the case $k = 0, 1, 2$.

And let us skip cases 2 and 3 and talk about case 4 first. In 1986, Mathieu discover some multiply transitive permutation groups, including two sporadic simple groups $M_{11} and M_{23}$

Definition 4.4. (Mathieu Group) Mathieu groups are the five sporadic simple groups $M_{11}, M_{12}, M_{22}, M_{23} and M_{24}$ introduced by Mathieu. These five groups are multiply transitive permutation groups on 11, 12, 22, 23, or 24 objects.

Bertram Huppert and Norman Blackburn showed that the automorphism groups reveal no other almost simple groups with socle M11 respectively M23.[7]

Definition 4.5. Scole is the subgroups generated by the minimal normal subgroups of G

Theorem 4.6. *(Huppert and Blackburn, [7], Chapter XII) For $i = 11, 23, 24$, we have $\mathrm{Aut}(M_i) \cong M_i$ and for $i = 12, 22$, we have $|\mathrm{Aut}(M_i) : \mathrm{Inn}(M_i)| = 2$.*

As $\mathrm{Aut}(M_{11}) \cong M_{11}$ and $\mathrm{Aut}(M_{23}) \cong M_{23}$, the only almost simple transitive permutation group of degree 11 respectively degree 23 with socle M_{11} respectively M_{23} is the Mathieu group of each degree itself.

Both Mathieu groups are full automorphism groups of t - (v, k, λ)-designs containing 11 respectively 23 points.

Theorem 4.7. *(Huppert and Blackburn, [7], Chapter XII (1) The Mathieu group M_{11} is the automorphism group of a 4-(11,5,1) design.*

(2) The Mathieu group M_{23} is the automorphism group of a 4-(23,7,1) design.

A t - (v, k, λ)-design with $\lambda = 1$ as in Theorem 4.5 is called a Steiner system. Both Steiner systems are not symmetric, as the 4 -(11,5,1)-design has 66 blocks and the 4-(23, 7, 1)-design has 253 blocks. This leads to the fact that both Mathieu groups each only have a single permutation representation.

5. Group $PSL_2 11$

Now, let talked about the case 2: $PSL_2 11$.
Let $\Delta := \{\alpha, \beta, \gamma, \delta, \epsilon\}$ and consider the action of $A := A_\Delta$ on $\Omega := \Delta^2$. We label the ten elements of Ω as follows

0	1	2	3	4	5	6	7	8	9
$\delta\epsilon$	$\alpha\epsilon$	$\alpha\beta$	$\beta\gamma$	$\gamma\delta$	$\alpha\gamma$	$\beta\delta$	$\gamma\epsilon$	$\delta\alpha$	$\beta\epsilon$

and calculate the images of some particular elements of A under this action:

$$\begin{aligned}
(\alpha\beta\gamma) &\mapsto a = (197)(235)(486)\\
(\beta\gamma)(\epsilon\delta) &\mapsto b = (18)(25)(49)(67)\\
(\alpha\beta)(\epsilon\delta) &\mapsto c = (16)(35)(47)(89)\\
(\alpha\delta)(\beta\gamma) &\mapsto y_1 = (01)(24)(56)(79)\\
(\alpha\delta)(\beta\epsilon) &\mapsto y_2 = (02)(16)(37)(45)
\end{aligned}$$

Then $H := \langle b, y_1\rangle \cong A$ and $H_0 = \langle a, b\rangle \cong S_3$. The orbits of H_0 are $\{0\}, \{1, 4, 6, 7, 8, 9\}$ and $\{2, 3, 5\}$, and so $1, y_1$ and y_2 form a set of representatives for the (H_0, H_0)-double cosets in H. Let ∞ be a point not in Ω, and define $x := (\infty 0)(35)(48)(79)$.

To prove G is doubly transitive, we need go through the Theorem 5.1:

Theorem 5.1. *(Jordan, [5], 7.5A) Let $H \leq \mathrm{Sym}(\Omega)$ be a transitive group of rank r. Fix $\alpha \in \Omega$ and let $y_0 = 1, y_1, \ldots, y_{r-1}$ be a set of representatives for the (H_α, H_α)-double cosets in H. Now choose a point ω not in Ω and put $\Omega^* := \Omega \cup \{\omega\}$, and let $x \in \mathrm{Sym}(\Omega^*)$ with $\omega \in \mathrm{supp}(x)$. Then $G := \langle H, x\rangle$ is a transitive extension of H whenever the following conditions hold:*
(i) $x^2 \in H$;
(ii) $xy_i x \in HxH$ for $i = 1, \ldots, r-1$; and
(iii) $xH_\alpha x = H_\alpha$.

Proof. Put $K := H \cup HxH$. We shall first show that K is a subgroup of $\mathrm{Sym}(\Omega^*)$. Indeed, (i) shows that K is closed under taking inverses, so it is enough to show that $KK \subseteq K$. However, from (iii) and (ii) we have $x^{-1}H_\alpha y_i H_\alpha x^{-1} = H_\alpha x y_i x H_\alpha \subseteq HxH$ for each $i \geq 1$, and so by (i) and (iii):
$xHx = x^{-1}Hx^{-1} = x^{-1}H_\alpha x^{-1} \cup \bigcup_{i\geq 1} x^{-1}H_\alpha y_i H_\alpha x^{-1} \subseteq H \cup HxH = K$

Hence $KK \subseteq H \cup HxHxH \subseteq HKH = K$ as required. Thus K is a subgroup and so $G = \langle H, x\rangle = H \cup HxH$

Finally, $G_\omega = H$ since ω is fixed by H but not by any element in HxH. Thus G is a transitive extension of H □

Thus, observe that $(xy_1)^3 = 1$ and $(xy_2)^3 = c$, $G := \langle H, x\rangle$ are satisfied the (i)-(iii) condition of Theorem 5.1. Thus G is a 2-transitive group of degree 11 and order $11 \cdot 10 \cdot 6$.

And $PSL_2(11)$ is a group with a doubly transitive representation of degree 12 that is isomorphic to G

6. Simplicity of $PSL(n, p)$

$PSL(n, p)$ is not naturally a subgroup of S_p but of S_{p+1}. And a very interesting point about $PSL(n, p)$ is that it is not known if there are infinitely primes that can be written as $(q^n - 1)(q - 1)$ for some prime power q. In this section, we wanted to show the simplicity of $PSL(n, p)$.

Definition 6.1. The **special linear group** $SL_n(F)$ of degree n over a field F is the set of n × n matrices with determinant 1, with the group operations of ordinary matrix multiplication and matrix inversion.

For a field F and integer $n \geq 2$, the projective special linear group is the quotient group of $\mathrm{SL}_n(F)$ by its center:

$$\mathrm{PSL}_n(F) = SL_n(F)/Z\left(\mathrm{SL}_n(F)\right)$$

In 1831, Galois claimed that $\mathrm{PSL}_2\left(\mathbb{F}_p\right)$ is a simple group for all primes $p > 3$ without proof. This turns out to be the case for all fields and all n with two exceptions:

$$\mathrm{PSL}_2\left(\mathbb{F}_2\right) \cong S_3$$
$$\mathrm{PSL}_2\left(\mathbb{F}_3\right) \cong A_4$$

To prove $\mathrm{PSL}_n(F)$ is simple for all F when $n > 2$, we will study the action of $\mathrm{SL}_n(F)$ on linear subspaces of F^n, which is the projective space $\mathbf{P}^{n-1}(F)$ and show it satisfies lwasawa's criterion.

Theorem 6.2. *(lwasawa's criterion) Let G act doubly transitively on a set X. Assume the following:*

(1) For some $x \in X$ the group S_{tab} has an abelian normal subgroup whose conjugate subgroups generate G.

(2) $[G, G] = G$.

Then G/K is a simple group, where K is the kernel of the action of G on X.

Note: the kernel of an action is the kernel of the homomorphism $G \longrightarrow \mathrm{Sym}(X)$

For nonzero $v \in F^n$, write the linear subspace F_v as $[v]$. Pick $[v_1] \neq [v_2]$ and $[w_1] \neq [w_2]$ in $\mathbf{P}^{n-1}(F)$. We seek an $A \in \mathrm{SL}_n(F)$ such that $A[v_1] = [w_1]$ and $A[v_2] = [w_2]$. Extend $\{v_1, v_2\}$ and $\{w_1, w_2\}$ a bases of $F^n, \{v_1, v_2, \ldots, v_n\}$ and $\{w_1, w_2, \ldots, w_n\}$ respectively. Let $L : F^n \longrightarrow F^n$ be the linear map where $v_i \mapsto w_i$. The determinant of this map is non-zero and thus we can scale the n-th coordinate projection map by a suitable scalar to construct a new linear map of determinant 1 which satisfies double transitivity for (v_1, v_2) and (w_1, w_2). Thus, $\mathrm{PSL}_n(F)$ acts doubly transitively.

If $A \in \mathrm{SL}_n(F)$ is in the kernel of this action the $A[v] = [v]$ for all nonzero $v \in F^n$, and so $Av = \lambda_v v$ where $\lambda_v \in F^\times$. Thus all vectors are eigenvectors, and the only such matrices with this property are scalar diagonal matrices which is exactly the center of $SL_n(F)$.

Consider the stabilizer of the point

$$\begin{bmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{bmatrix} \in \mathbf{P}^{n-1}(F)$$

which is the group of $n \times n$ determinant 1 matrices

$$\begin{bmatrix} a & * \\ 0 & M \end{bmatrix}$$

where $a \in F^\times, M \in \mathrm{GL}_{n-1}(F)$, and $*$ is a row vector of length $n-1$. For this to be in $SL_n(F)$ we must have $a = \frac{1}{\det M}$.

The group

$$U := \left\{ \begin{pmatrix} 1 & * \\ 0 & I_{n-1} \end{pmatrix} \right\} \cong F^{n-1}$$

is abelian and normal as it is the kernel of the projection of $H \to GL_{n-1}(F)$.

The elementary matrices $I_n + \lambda E_{ij}$ have 1 's on the main diagonal and a λ in the (i, j) position. Therefore its determinant is 1 , so such matrices are in $\mathrm{SL}_n(F)$.

Elementary matrices have two key properties:

(1)For $n > 2$ each $I_n + \lambda E_{ik}$ is conjugate in $SL_n(F)$

(2)These matrices generate $\mathrm{SL}_n(F)$

$I_n + E_{12} \in U$ so we have that subgroups of $SL_n(F)$ which are conjugate to U generate.

Finally, we wanted to show that $[\mathrm{SL}_n(F), \mathrm{SL}_n(F)] = \mathrm{SL}_n(F)$.

All we need is to show that $I_n + E_{12}$ is a commutator in $\mathrm{SL}_n(F)$ since our facts about elementary matrices give that the commutator (which is normal) contains all elementary matrices, and thus generates all of $\mathrm{SL}_n(F)$.

Let

$$g = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

then

$$ghg^{-1}h^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = l_3 + E_{12}$$

This extends to $I_n + E_{12}$ via

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & I_{n-3} \end{pmatrix}$$

$$= \begin{pmatrix} g & 0 \\ 0 & I_{n-3} \end{pmatrix} \begin{pmatrix} h & 0 \\ 0 & I_{n-3} \end{pmatrix} \begin{pmatrix} g & 0 \\ 0 & I_{n-3} \end{pmatrix}^{-1} \begin{pmatrix} h & 0 \\ 0 & I_{n-3} \end{pmatrix}^{-1}$$

Thus, by lwasawa's criterion we have prove the simplicity of $PSL(n, p)$

7. ACKNOWLEDGMENTS

I want to thank Professor Thomas Tucker for his mentorship in past whole year. He gave me great encouragement and support, providing valuable guidance and advice. He can always provide immediate answers and guidance when I encounter difficulties, allowing me to overcome difficulties and keep moving forward. At the same time, he also provided important ideas and guidance for my research, allowing me to gain a deeper understanding of relevant research in group action and gain a deeper understanding. Moreover, I would like to thank

the members of my review committee(Professor Thomas Tucker, Professor Juan Rivera-Letelier, and Professor Jonathan Pakianathan) for taking the time out of your busy schedule to review my paper and providing valuable opinions and suggestions to me. Thank you for your support and affirmation, which will be the driving force for me to continue my research and learning. I also wanted to thank Professor Arda Demirhan, My collaborator Jacob Miller and Zhu Zheng. Last year, we collaborated on a research about group S_{pq} with p, q are prime,$p < q$, contain two normal subgroups of same index N_1, N_2 with only N_1 is transitive. This research is the source of inspiration for my honor thesis and has also made me more clear about my ideas for continuing on the path of mathematical research in the future. And I also want to thank the professor of Math 236h and Math 436, Professor Jonathan Pakianathan and Professor Naomi Jochnowitz, Your course has sparked my interest in the field of Algebra. I am sincerely grateful to the professors who have provided me with a lot of help in my university studies, especially Professor Alex Iosevich, Professor Dinesh Thukur, and Professor Xuwen Chen. Without your teaching and assistance, I may not continue my studies in mathematics.

Finally, I would like to express my gratitude to my family and friends who have always supported and encouraged me on my academic journey. It is their support and companionship that have allowed me to continuously grow and progress. Here, I express my deepest gratitude to all of you for your tremendous help in my academic journey.

References

[1] Qian Cai, Hua Zhang, "A Note on Primitive Permutation Groups of Prime Power Degree", Journal of Discrete Mathematics, vol. 2015, Article ID 194741, 4 pages, 2015. https://doi.org/10.1155/2015/194741

[2] W. Burnside, Theory of Groups of Finite Order, Cambridge Univ. Press, 2nd edn. (1911)

[3] Müller, Peter. "Permutation groups of prime degree, a quick proof of Burnside's theorem." Archiv der Mathematik 85 (2005): 15-17.

[4] R. M. Guralnick, Subgroups of prime power index in a simple group, J. Algebra 81 (1983), 304311.

[5] John D. Dixon and Brian Mortimer, Permutation Groups, Springer-Verlag, New York - Heidelberg - Berlin, 1996.

[6] Jones, Gareth A. "Primitive permutation groups containing a cycle." Bulletin of the Australian Mathematical Society 89.1 (2014): 159-165.

[7] B. Huppert, N. Blackburn, Finite groups III, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[8] P. J. Cameron, "Finite permutation groups and finite simple groups," Bulletin of the London Mathematical Society, vol. 13, no. 1, pp. 1–22, 1981.