The maximal subgroups of the symmetric group

Martino Garonzi

Abstract. In this survey paper I will talk about the classification of the maximal subgroups of the symmetric group of degree n, which can be divided into three main categories: intransitive, imprimitive and primitive maximal subgroups. The O'Nan-Scott theorem and its proof will be discussed. The content of this paper was inspired by two courses I gave, one was a minicourse given in December 2018 in the University of Campinas (state of S.Paulo, Brazil) during the brazilian Escola de Álgebra 2018, the other was an online PhD course given in November 2020 for the University of Padova (Italy). This paper is structured as lecture notes, in particular it contains exercises for the reader.

Contents

Chapter 1

Introduction

The symmetric group of a set Ω is the group $\mathrm{Sym}(\Omega)$ consisting of the bijections $\Omega \to \Omega$. If $\Omega = \{1, \dots, n\}$ for some positive integer n then the group $\mathrm{Sym}(\Omega)$ is commonly denoted by S_n and it is called the symmetric group of degree n. The purpose of this survey paper is to collect the essential information that is known about the maximal subgroups of S_n. A subgroup G of S_n is typically classified according to its action on Ω. Such action can be of three main types: intransitive, meaning that G stabilizes a nonempty proper subset of Ω, imprimitive, meaning that G acts transitively and stabilizes a nontrivial partition of Ω, and primitive, meaning that G acts transitively and does not stabilize any nontrivial partition of Ω. We will discuss the proof of the fact that the maximal intransitive and the maximal imprimitive subgroups of S_n are indeed maximal subgroups of S_n and we will discuss primitive maximal subgroups by stating and proving the O'Nan-Scott theorem. The material is taken from different sources, which are cited throughout the paper and can be found in the bibliography.

Chapter 2

Basic notions about group actions

All group actions we consider are on the right, and this includes our notation for functions, so that the common expression $f(x)$ will rather be denoted by $(x)f$ or xf. G acts on X by the rule $X \times G \to X$, $(x, g) \mapsto xg$ if and only if the following is a group homomorphism:

$$\gamma : G \to \mathrm{Sym}(X), \qquad g \mapsto \gamma_g, \qquad\qquad x\gamma_g := xg \quad \forall x \in X.$$

The kernel of this homomorphism is the *kernel of the action* and the action is called *faithful* if it has trivial kernel. The (*G-*)*orbits* of the action are the sets

$$O_G(x) = \{xg \ : \ g \in G\}, \qquad x \in X.$$

The action is called *transitive* if there is some $x \in X$ such that $O_G(x) = X$ (i.e. there is only one orbit). This is equivalent to saying that, for any $x, y \in X$, there exists $g \in G$ with $xg = y$. The stabilizer of $x \in X$, also called *point stabilizer*, is

$$G_x = \mathrm{Stab}_G(x) = \{g \in G \ : \ xg = x\} \leq G.$$

Clearly, the kernel of an action equals the intersection of the point stabilizers.

We list some relevant group actions.

1. The (transitive) action of right multiplication of G on $X = G$. All the stabilizers, and therefore the kernel, are trivial.

2. The conjugation action of G on a subset X of G closed under conjugation. The stabilizer of $x \in X$ is its centralizer,

$$C_G(x) = \{g \in G \ : \ gx = xg\}.$$

Clearly $x \in C_G(x)$. If this action is transitive, X is called a conjugacy class of G. If $X = G$ then the kernel of this action is the center of G,

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \ : \ xg = gx \ \forall x \in G\}.$$

Also, in this case the image of the homomorphism $G \to \operatorname{Sym}(G)$ lies inside $\operatorname{Aut}(G)$ and therefore, by the isomorphism theorem, $G/Z(G)$ is isomorphic to a subgroup of $\operatorname{Aut}(G)$.

3. The conjugation action of G on the family $\mathscr{H}$ of all subgroups of G (or any family of subgroups of G closed under conjugation). The action is $(H, g) \mapsto H^g := g^{-1}Hg$. The stabilizer of H for this action is denoted by

$$N_G(H) = \{g \in G \ : \ g^{-1}Hg = H\}$$

and it is called the normalizer of H in G. Of course, $H \le N_G(H)$.

4. The (transitive) action by right multiplication of G on $X = \{Hg \ : \ g \in G\}$. The stabilizer of Hg is H^g and the kernel of this action is

$$H_G = \bigcap_{g \in G} H^g.$$

H_G is called the normal core of H in G, hence this action is faithful if and only if $H_G = \{1\}$, which we express by saying that H is "core-free". The isomorphism theorem applied to $G \to \operatorname{Sym}(X)$ implies that G/H_G is isomorphic to a subgroup of S_n, where $n = |X| = |G : H|$. I will refer to this fact as the *generalized Cayley theorem*, because it is a generalization of the classical Cayley theorem saying that any group G is isomorphic to a subgroup of $\operatorname{Sym}(G)$ (choose $H = \{1\}$).

Exercise 2.1. *Let G be a finite group and consider the natural action of $\operatorname{Aut}(G)$ on $G - \{1\}$. Show that this action is transitive if and only if G is an elementary abelian group, that is, a group of the type $C_p{}^n$ for some prime p and some integer $n \ge 1$.*

Assume G acts on X and on Y. These two actions are called equivalent if there exists a bijection $f : X \to Y$ which is compatible with the action of G, in other words $(xg)f = (xf)g$ for every $x \in X$, $g \in G$. Two equivalent actions are essentially "the same action".

Counting principle (Orbit-Stabilizer theorem): if G acts transitively on X and $x \in X$ then $|X| = |G : \operatorname{Stab}_G(x)|$. More precisely, there is a bijection between the set of right cosets of $H = \operatorname{Stab}_G(x)$ and

X sending Hg to xg. This bijection is actually an equivalence of actions. In particular $|X|$ divides $|G|$.

This means in particular that *all the transitive actions of G are "intrinsic": they can be completely recovered from a point stabilizer.* More specifically, if G acts transitively on X and $\alpha \in X$ then the action of G on X is equivalent to the action of right multiplication of G on the set $\{Hg \; : \; g \in G\}$ where $H = \mathrm{Stab}_G(\alpha)$ is the stabilizer of α. So studying the transitive actions of G is equivalent to studying the subgroups of G, and studying the faithful transitive actions of G is equivalent to studying the core-free subgroups of G. For example, the trivial subgroup $\{1\}$ corresponds to the regular action of G on itself.

Another consequence of the counting principle is that every element $x \in G$ has precisely $|G : C_G(x)|$ conjugates in G, and every subgroup $H \leq G$ has precisely $|G : N_G(H)|$ conjugates in G.

The action of G on X is called semiregular if the point stabilizers are trivial, and it is called regular if it is semiregular and transitive. By the counting principle if G acts regularly then $|G| = |X|$. The typical regular action is given by a group acting on itself by right multiplication. Another example of a regular action is that of the Klein 4-group

$$K = \{1, (12)(34), (13)(24), (14)(23)\} < S_4$$

acting naturally on $\{1, 2, 3, 4\}$. More in general if G is a semidirect product $H \ltimes N$ then the action of N of right multiplication on the right cosets of H is regular.

An important example is the following. *If G acts faithfully on X and N is a normal subgroup of G whose induced action on X is transitive then the centralizer $C_G(N)$ acts semiregularly.* Indeed if $g \in C_G(N)$ is such that $xg = x$ for some $x \in X$ then since every element of X has the form xn for some $n \in N$ we have $xn = xgn = xng$ therefore g fixes all the points in X, so $g = 1$ because the action of G is faithful.

Exercise 2.2 (Burnside Lemma)**.** *Let f_g be the number of fixed points of $g \in G$ acting on X. Then the number of orbits of the action is $\frac{1}{|G|} \sum_{g \in G} f_g$. For example, if G acts semiregularly then the number of orbits is $|X|/|G|$, since $f_1 = |X|$ and $f_g = 0$ for every $1 \neq g \in G$. Therefore if the action is regular (semiregular and transitive) then $|G| = |X|$.*

Chapter 3

The symmetric group

Let S_n be the symmetric group on n letters.

It is well-known that if $n \geq 2$ and $n \neq 4$ then the alternating group A_n is a simple group that has index 2 as a subgroup of S_n. Moreover A_n is nonabelian if $n \geq 5$. This easily implies that if $n \neq 4$ the normal subgroups of S_n are $\{1\} < A_n < S_n$ and the normal subgroups of S_4 are $\{1\} < K < A_4 < S_4$ where $K \cong C_2 \times C_2$ is the Klein group.

In particular A_n is the unique subgroup of S_n of index 2, for every $n \geq 3$. Therefore A_n is characteristic in S_n, meaning that $\varphi(A_n) = A_n$ for every $\varphi \in \operatorname{Aut}(S_n)$: this follows from the above since $|S_n : A_n| = |S_n : \varphi(A_n)|$ for every $\varphi \in \operatorname{Aut}(S_n)$.

A few words about S_4, the symmetric group of degree 4. The normal subgroups of S_4 are $\{1\} < K < A_4 < S_4$ where K is the Klein group, that is, $K = \{1, (12)(34), (13)(24), (14)(23)\}$. The Sylow 2-subgroups of S_4 are dihedral groups of order 8 and they have index 3 in S_4. In particular they are maximal subgroups (any subgroup of prime index is maximal). Considering the natural action of S_4 on $\{1, 2, 3, 4\}$, the point stabilizers $\operatorname{Stab}_{S_4}(i) = \{g \in S_4 \ : \ ig = i\}$, are maximal subgroups of S_4 of index 4, isomorphic to S_3. The only subgroup of S_4 of index 2 is A_4. The maximal subgroups of S_4 are precisely the following: the 3 Sylow 2-subgroups, the point stabilizers and the alternating group A_4.

Proposition 3.1. *Let $n \geq 3$ and let G be S_n or A_n. If $H < G$ and $H \neq A_n$ then $|G : H| \geq n$ unless $n = 4$ and H is a Sylow 2-subgroup of G. In particular the point stabilizers of G acting naturally on $\{1, \ldots, n\}$ are maximal subgroups of G.*

Proof. Let $m = |G : H|$. G acts transitively (hence non-trivially) by right multiplication on $X = \{Hx \ : \ x \in G\}$, which is a set of size m, this gives a homomorphism $\varphi : S_n \to S_m$ whose image is a transitive subgroup of S_m. Let $K = \ker(\varphi)$ and note that $K \leq H$. Since $H \neq A_n$ we have $m \geq 3$

so $|G : K| = |G : H||H : K| \geq |G : H| = m \geq 3$. The case $n \leq 4$ can be done by hand. If $n \geq 5$ the unique proper nontrivial normal subgroup of S_n has index 2, so $K = \{1\}$. It follows that $|S_n| = n!$ divides $|S_m| = m!$ hence $n \leq m$.

   This implies that the point stabilizers are maximal subgroups because they have index n (by the counting principle, since G acts transitively on $\{1, \ldots, n\}$) and if $n = 4$ the point stabilizers have order 6 hence they are not contained in any Sylow 2-subgroup. □

   We will now list some facts about the symmetric group, which are elementary, in the sense that they can be proved in a few lines in a self-contained way. Recall that the *derived subgroup* of a group G is the subgroup generated by the elements of the form $xyx^{-1}y^{-1}$ (commutators) for $x, y \in G$. It is equal to the smallest normal subgroup N of G such that G/N is abelian. The *Frattini subgroup* of a group G is the intersection of the maximal subgroups of G. The *cycle structure* of a permutation $\sigma \in S_n$ is the increasing sequence of the lengths of the disjoint cycles whose product is σ.

1. The center of S_n and the center of A_n are trivial for $n \geq 4$.

2. The derived subgroup of S_n is A_n.

3. The derived subgroup of A_n is $\{1\}$ for $n \in \{2, 3\}$, it is the Klein group if $n = 4$ and it is A_n if $n \geq 5$.

4. The Frattini subgroup of S_n and the Frattini subgroup of A_n are trivial.

5. In the symmetric group S_n two elements are conjugate if and only if they admit the same cycle structure.

Lemma 3.2. *Let $\sigma = (1 \ldots n) \in S_n$. The centralizer of σ in S_n is $\langle \sigma \rangle$.*

Proof. It is clear that $\langle \sigma \rangle \leq C = C_{S_n}(\sigma)$, so to conclude it is enough to show that $|C| = n$. The number of conjugates of σ in S_n is $|S_n : C| = n!/|C|$. On the other hand, the conjugates of σ in S_n are precisely the n-cycles, and their number is $(n-1)!$, since when constructing an n-cycle we may fix the first element and permute the rest in all possible ways (note that for example $(1234) = (2341) = (3412) = (4123)$). We deduce that $n!/|C| = (n-1)!$ hence $|C| = n$. □

Exercise 3.3. *Find $C_{S_n}(x)$ where $x = (1, 2, \ldots, n-1)$ and $x = (1, 2)(3, 4, \ldots, n)$. [Proceed as in the lemma: first, find the order of such centralizer, then deduce its structure.]*

Exercise 3.4. *Let $x \in S_n$ be a product of b disjoint 3-cycles. Prove that*

$$|C_{S_n}(x)| = 3^b \cdot b! \cdot (n - 3b)!.$$

[Count the conjugates of x and apply the counting principle.]

For the record, if x is the element in the above exercise, the structure of $C_{S_n}(x)$ is $(C_3 \wr S_b) \times S_{n-3b}$ (for the definition of wreath product see Section 8). The base C_3^b is generated by the cycles in the decomposition of x, the permutational part S_b permutes the 3-cycles around and S_{n-3b} contains those permutations whose support is disjoint from the support of x. This idea can be generalized to any permutation.

Exercise 3.5. *Using wreath products (see Section 8), describe the structure of the centralizer in S_n of any element of S_n in terms of its cycle structure. More explicitly, prove that, if $x \in S_n$ has in the cycle decomposition k_i cycles of length l_i, $i = 1, \ldots, t$, $n = \sum_{i=1}^{t} k_i l_i$, with $l_1, \ldots, l_t$ pairwise distinct, then*

$$C_{S_n}(x) \cong \prod_{i=1}^{t} C_{l_i} \wr S_{k_i}.$$

Lemma 3.6. *Let $n \geq 5$. The alternating group A_n cannot act nontrivially on less than n points.*

Proof. Assume A_n acts nontrivially on X, and let $m := |X|$. Assume $m < n$ by contradiction, so that $m \leq n - 1$. The action of A_n on X gives a homomorphism $A_n \to \mathrm{Sym}(X) \cong S_m$ with kernel not equal to A_n. Since A_n is a simple group, such homomorphism is injective, therefore $n!/2 = |A_n| \leq |\mathrm{Sym}(X)| = m! \leq (n-1)!$. This implies that $n \leq 2$, a contradiction. $\square$

Exercise 3.7. *Let $n \geq 5$. Prove that if S_n acts nontrivially on m points and $m < n$, then the orbits of this action have size 1 or 2.*

Exercise 3.8. *Prove that if A and B are subgroups of a finite group G then $|AB| = |A| \cdot |B|/|A \cap B|$. Moreover $AB \leq G$ if and only if $AB = BA$. In particular, if $A \leq N_G(B)$ or $B \leq N_G(A)$, then $AB \leq G$.*

We will now discuss the subgroups of S_n of index n. The following proof is inspired by [17, Lemma 2.2].

Theorem 3.9. *If $n \neq 6$ then the unique subgroups of S_n of index n are the point stabilizers. Moreover S_6 has two conjugacy classes of subgroups of index 6.*

Proof. In the case $n \leq 10$ we will skip the proof. Now assume $n \geq 11$. We first prove that the subgroups of A_n of index n are precisely the n point stabilizers.

Let H be a subgroup of A_n of index n, so that $|H| = |A_n|/n = (n-1)!/2$. First observe that $H \cong A_{n-1}$. Indeed A_n acts nontrivially (hence faithfully, since A_n is a simple group) on the set X of the n right cosets of H by right multiplication and this gives an injective homomorphism $\varphi : A_n \to \mathrm{Sym}(X)$, moreover $\varphi(H)$ is contained in the stabilizer in $\mathrm{Sym}(X)$ of H, which is isomorphic to S_{n-1}, however $|\varphi(H)| = |H| = |A_{n-1}|$ hence $\varphi(H)$ has index 2 in the stabilizer of H, which is a symmetric group, hence $H \cong \varphi(H) \cong A_{n-1}$.

Fix an isomorphism $f : A_{n-1} \to H < S_n$.

If x is a 3-cycle in A_{n-1} then $f(x)$ is also a 3-cycle. To prove this, let $K < A_{n-1}$ be the pointwise stabilizer of the set of points moved by x. Then K is isomorphic to A_{n-4} and it is centralized by x, so $f(K) \cong A_{n-4}$ is a subgroup of S_n centralized by the element $y = f(x)$ of order 3. Assume by contradiction that y is not a 3-cycle. Note that y is a product of pairwise disjoint 3-cycles $y = c_1 \ldots c_b$ where $1 < b \leq n/3$. Since $f(K)$ centralizes y, it acts by conjugation on $\{c_1, \ldots, c_b\}$ and this action must be trivial by Lemma 3.6 since $f(K) \cong K \cong A_{n-4}$, $n - 4 \geq 5$ and $b \leq n/3 < n$. It follows that $f(K)$ centralizes all of the elements $c_1, \ldots, c_b$, in particular it centralizes $c_1 c_2$. By counting the conjugates of $c_1 c_2$ in S_n and by applying the counting principle, we see that the centralizer $C_{S_n}(c_1 c_2)$ has order $18(n-6)!$. Since $|f(K)| = (n-4)!/2$ and $f(K) \leq C_{S_n}(c_1 c_2)$, we obtain that $(n-4)!/2 \leq 18(n-6)!$. This is a contradiction since $n \geq 11$.

If $i, j \in \{1, \ldots, n-1\} - \{1, 2\}$ then $f((12i))$, $f((12j))$ are 3-cycles and

$$A_4 \cong \langle (12i), (12j) \rangle \cong f(\langle (12i), (12j) \rangle) = \langle f((12i)), f((12j)) \rangle.$$

We know that $f((12i))$, $f((12j))$ are 3-cycles and they generate a group isomorphic to A_4, therefore there exist $a, b, x_3, \ldots, x_{n-1}$, pairwise distinct elements of $\{1, \ldots, n\}$, such that $f((12i)) = (abx_i)^{\pm 1}$ for $i = 3, \ldots, n-1$. Such elements generate the stabilizer of the one element $j \in \{1, \ldots, n\}$ fixed by all of them, therefore $f(A_{n-1}) = A_n \cap \mathrm{Stab}_{S_n}(j) = \mathrm{Stab}_{A_n}(j) \cong A_{n-1}$.

Now let H be a subgroup of S_n of index n, in other words $|H| = (n-1)!$. If $H \leq A_n$ then $n = |S_n : H| = |S_n : A_n| \cdot |A_n : H| = 2|A_n : H|$, hence $|A_n : H| = n/2$, and this contradicts Lemma 3.6 since A_n would act nontrivially by right multiplication on the $n/2$ right cosets of H. Therefore $H \not\leq A_n$ and, since $|S_n : A_n| = 2$, this implies that $HA_n = S_n$. Therefore $n! = |S_n| = |HA_n| = |H| \cdot |A_n|/|H \cap A_n|$ and, using the fact that $|H| = (n-1)!$, we find that $|A_n : H \cap A_n| = n$. By the previous discussion we deduce that $H \cap A_n$ is a point stabilizer in A_n, say $H \cap A_n = S \cap A_n$ where $S = \mathrm{Stab}_{S_n}(j)$. Let $L = \langle H, S \rangle$ be the group generated by H and S. Since L contains S and S is a maximal subgroup of S_n, either $L = S$ or

$L = S_n$. If $L = S$ then $H \leq S$ hence $H = S$ since H and S have the same order. We are left to show that $L \neq S_n$. This follows from the fact that the intersection $H \cap A_n = S \cap A_n$ has index 2 in both H and S, therefore it is a normal subgroup of L.

The group S_5 acts by conjugation on the set of its 6 Sylow 5-subgroups and this action is faithful. This gives an injective homomorphism $\varphi : S_5 \to S_6$ with transitive image $H = \varphi(S_5)$. It follows that $H \cong S_5$ has index $6!/5! = 6$ in S_6 and it is not a point stabilizer because it is transitive. It is possible to show that apart from point stabilizers this is indeed the only other class of subgroups of index 6. $\qquad \square$

Observe that if G is any group then the set $\mathrm{Aut}(G)$ of automorphisms of G is a group with composition. We have a natural homomorphism $\varphi : G \to \mathrm{Aut}(G)$ given by $g \mapsto \gamma_g$ where γ_g takes x to $x^g = g^{-1}xg$. The image $\varphi(G)$ is a normal subgroup of $\mathrm{Aut}(G)$ and it is usually denoted by $\mathrm{Inn}(G)$: it is the group of inner automorphisms of G. The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is denoted by $\mathrm{Out}(G)$ and it is called the group of outer automorphisms of G. Clearly, $\ker(\varphi) = Z(G)$ is the center of G, therefore $\varphi(G) \cong G/Z(G)$ embeds into $\mathrm{Aut}(G)$. In particular, if $Z(G) = \{1\}$, then G embeds into $\mathrm{Aut}(G)$; in this particular case we will often think of G as a subgroup of $\mathrm{Aut}(G)$. For instance, the symmetric group S_n of degree $n \geq 3$ embeds into $\mathrm{Aut}(S_n)$.

Theorem 3.10. *If $n \geq 3$ and $n \neq 6$ then $\mathrm{Aut}(S_n) \cong S_n \cong \mathrm{Aut}(A_n)$. More specifically, every automorphism of A_n or S_n is given by conjugation by an element of S_n. Moreover A_6 has index 4 in $\mathrm{Aut}(A_6)$.*

Proof. In this proof we assume $n \geq 5$, so that A_n is simple. The smaller cases can be done by hand.

The group $\mathrm{Aut}(S_n)$ acts naturally on the set of subgroups of S_n of index n, which, being $n \neq 6$, are all the n point stabilizers. Since an automorphism that fixes all point stabilizers must be the identity, this action is faithful, hence we obtain an injective homomorphism $\varphi : \mathrm{Aut}(S_n) \to S_n$. On the other hand, being $Z(S_n) = \{1\}$, the canonical conjugation homomorphism $S_n \to \mathrm{Aut}(S_n)$ is injective, and this implies that $|S_n| \leq |\mathrm{Aut}(S_n)|$, therefore φ is a group isomorphism. In other words every isomorphism $S_n \to S_n$ is given by the conjugation by an element of S_n.

Using the isomorphism $A_6 \cong \mathrm{PSL}(2,9)$, it is possible to find the structure of $\mathrm{Aut}(S_6)$.

$$\text{Aut}(A_6)$$

$$M_{10} \qquad S_6 \qquad \text{PGL}(2,9)$$

$$A_6$$
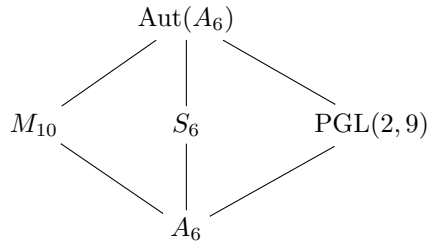
$$\text{Out}(A_6) = \text{Aut}(A_6)/\text{Inn}(A_6) \cong C_2 \times C_2. \qquad \qquad \square$$

Exercise 3.11. *Prove that A_n is the unique subgroup of S_n of index 2 without using the fact that A_n is a simple group for $n \geq 5$. [If N is a subgroup of S_n of index 2 then it must contain $Q = \{x^2 \ : \ x \in S_n\}$.]*

Exercise 3.12. *Let $O \subseteq \Omega = \{1, \ldots, n\}$ and let $G := \text{Stab}(O) = \{g \in S_n \ : \ Og = O\}$. Prove that $G \cong \text{Sym}(O) \times \text{Sym}(\Omega - O)$.*

Exercise 3.13. *Prove that, if S is a nonabelian simple group, then $\text{Aut}(\text{Aut}(S)) \cong \text{Aut}(S)$. Deduce the structure of $\text{Aut}(A_n)$. [Let N be the image of S inside $G = \text{Aut}(S)$; prove that $C_G(N) = \{1\}$.]*

Chapter 4

The maximal subgroups of S_5

If P is a property of a group action (for example transitive, semiregular, regular), a subgroup H of $G = S_n$ is called P if its natural action on $\Omega = \{1, \dots, n\}$ is P. We will use the word "intransitive" to mean "not transitive". Observe that if $H \leq S_n$ is intransitive then it has more than one orbit on Ω, and letting O be one of them, H is clearly contained in $\mathrm{Stab}(O) = \{g \in G \ : \ Og = O\} \cong \mathrm{Sym}(O) \times \mathrm{Sym}(\Omega - O)$. This is called a "maximal intransitive subgroup" of S_n. Note that a maximal intransitive subgroup is maximal among the intransitive subgroups. We are not saying that it is maximal in S_n. As we will see, such a subgroup is indeed maximal unless $|O| = |\Omega - O|$.

Let $G = S_5$. We want to determine the maximal subgroups of G. Observe first that the only normal subgroups of G are $\{1\}$, A_5 and G (as is the case for all symmetric groups of degree at least 5) and A_5 is the only subgroup of G of index 2. We claim that the only maximal subgroups of G are A_5, the point stabilizers, the intransitive subgroups of type $S_3 \times S_2$ and the normalizers of the Sylow 5-subgroups.

Let M be a maximal subgroup of G. Suppose first that 5 does not divide $|M|$. Then M acts intransitively hence it is one of S_4, $S_3 \times S_2$. We may now assume that 5 divides $|M|$. M contains a Sylow 5-subgroup P of G. Suppose 3 divides $|M|$. Then $|G : M|$ divides 8 hence $|G : M| \in \{2, 4, 8\}$. If $|G : M| = 4$ then the natural action of G on the 4 cosets of M implies that G is isomorphic to a subgroup of S_4, a contradiction, since $|S_4| < |G|$. If $|G : M| = 8$ then $|M| = 15$ and M is cyclic (every group of order 15 is cyclic), but S_5 has no elements of order 15. We deduce that $|G : M| = 2$ hence $M = A_5$. Now assume 3 does not divide $|M|$. Then $|M| = 5 \cdot 2^n$ with $n \in \{0, 1, 2, 3\}$, now by Sylow theorem $P \trianglelefteq M$ so $M \leq N_G(P)$ hence $M = N_G(P)$.

Note that what we proved is that if M is a maximal subgroup of S_5 then one of the following occurs: $M = A_5$, M is maximal intransitive, or M is the normalizer of a Sylow 5-subgroup. Since there are no containments between any two of these groups, they are precisely all the maximal subgroups of S_5.

The normalizer $N_G(P)$ is a semidirect product $C_5 \rtimes C_4$ and it is isomorphic to $\mathrm{AGL}(1,5) = \mathbb{F}_5 \rtimes \mathrm{GL}(\mathbb{F}_5^1)$, the *affine group* of dimension 1 over $\mathbb{F}_5$. Observe that $\mathrm{Aut}(\mathbb{F}_5) \cong U(\mathbb{F}_5) \cong C_4$.

Exercise 4.1. *Find all the maximal subgroups of S_4 and of A_5.*

Chapter 5

Imprimitivity blocks

Let G be a subgroup of S_n acting on $\Omega = \{1, \ldots, n\}$. The number n will also be called the degree of G. As we have seen, it may happen that G stabilizes a non-empty proper subset of Ω, in which case G is called intransitive. But there are other relevant things that G can stabilize, namely *partitions*. A partition of Ω is a family $\mathcal{P} = \{B_1, \ldots, B_k\}$ of non-empty proper subsets of Ω such that $B_1 \cup \ldots \cup B_k = \Omega$ and $B_i \cap B_j = \emptyset$ whenever $i \neq j$. We say that G stabilizes the partition $\mathcal{P}$ if $B_i g \in \mathcal{P}$ for every $g \in G$ and for every $i \in \{1, \ldots, k\}$. An example of stabilized partition is given by the G-orbits, and such partition is not $\{\Omega\}$ if G is intransitive, however we already know this kind of partition. Assume now that G is transitive and that it stabilizes a partition $\mathcal{P} = \{B_1, \ldots, B_k\}$. Then it is clear that G *acts* on $\mathcal{P}$, by $(B_i, g) \mapsto B_i g$, and this action is *transitive*: if $B_i, B_j \in \mathcal{P}$ and $x \in B_i$, $y \in B_j$ then there exists $g \in G$ such that $xg = y$, so $y \in B_i g \cap B_j$. But $B_i g$ and B_j are members of the partition $\mathcal{P}$, so the fact that $B_i g \cap B_j \neq \varnothing$ implies that $B_i g = B_j$. Since the right multiplication by $g \in G$ is a bijection $B_i \to B_i g$, we deduce that all of the members of $\mathcal{P}$ have the same size. Moreover, if B is one of them, then either $B \cap Bg = \emptyset$ or $B = Bg$, for every $g \in G$.

An *imprimitivity block*, or simply block, for the action of G is a non-empty subset B of Ω with the property that $Bg = B$ or $Bg \cap B = \emptyset$ whenever $g \in G$. In particular any orbit of G is a block. Observe that Ω is a block, and $\{\omega\}$ is a block for every $\omega \in \Omega$. The blocks Ω, $\{\omega\}$ are called trivial blocks. Also, $\{\omega\}$ is an example of block that, in general, is not an orbit. It is easy to show that if B is a block then Bg is a block for all $g \in G$. Assume now G acts transitively on Ω. If B is a block for G then $\mathcal{P} = \{Bg \mid g \in G\}$ is a partition of Ω, moreover $|B| = |Bg|$ for all $g \in G$ hence $a = |B|$ divides $|\Omega|$ and the partition $\mathcal{P}$ consists of $b = |\Omega|/|B|$ blocks. In particular $n = |\Omega| = ab$, so if the block B is nontrivial then n cannot be a prime number (see for example our discussion of S_5 above).

The set of translates $\{Bg \; : \; g \in G\}$ is called a block system of G.

The transitive group G is said to be *primitive* if it does not admit any nontrivial block, and *imprimitive* otherwise.

Since the orbits are in particular blocks, in the definition of primitive group the assumption that G is transitive is not needed unless $n = 2$, in which case the trivial group inside S_2 does not have any nontrivial blocks on $\{1, 2\}$.

One easy fact we have just proved is that every transitive group of prime degree is primitive. An easy example of primitive group of prime degree p is given by $\langle(1\ldots p)\rangle$ acting on $\{1,\ldots,p\}$. The dihedral group of degree p is also primitive (this will be an easy consequence of Proposition 5.2).

Easy example: consider $\sigma = (123456)$ and $G = \langle\sigma\rangle < S_6$, as a permutation group of degree 6. Since $\sigma^2 = (135)(246)$ and $\sigma^3 = (14)(25)(36)$, it is clear that G admits precisely two nontrivial block systems, namely $\{\{1,3,5\},\{2,4,6\}\}$ and $\{\{1,4\},\{2,5\},\{3,6\}\}$. As the following picture shows, the cycle (123456) acts as a 2-cycle on the first block system and as a 3-cycle on the second.
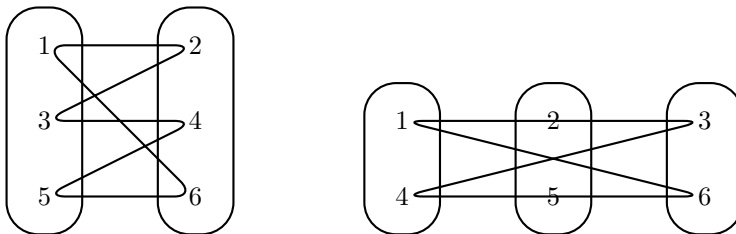
Exercise 5.1. *Using this idea, observe that the cyclic group $\langle(1\ldots n)\rangle$ acting on $\{1,\ldots,n\}$ is primitive if and only if n is a prime number.*

Note that the maximal imprimitive subgroups of S_n are precisely the stabilizers of the partitions of $\{1,\ldots,n\}$ such that all the parts have the same size. Indeed, every imprimitive group is contained in the stabilizer of the associated block system.

The following proposition shows that whether a group $G \leq \mathrm{Sym}(\Omega)$ does or does not stabilize a nontrivial partition of Ω can be detected looking at the subgroups of G containing a point stabilizer.

Proposition 5.2. *Suppose $n > 2$ and $G \leq S_n$ acts transitively on $\Omega = \{1,\ldots,n\}$. G is primitive if and only if the point stabilizer $M = G_\alpha$ (for any $\alpha \in \Omega$) is a maximal subgroup of G.*

In particular, S_n and A_n in their natural actions are primitive groups.

Using the orbit-stabilizer theorem, this implies that studying the (faithful) primitive actions of a group G is equivalent to studying its (core-free) maximal subgroups. This allows to give an abstract definition of primitive group: see section 9.2.

Proof of Proposition 5.2. Assume that $n > 2$ and $G \leq S_n$ acts transitively on Ω. If B is a block for G then the setwise stabilizer of B,

$$G_{\{B\}} := \{g \in G \ : \ Bg = B\},$$

acts transitively on B. Indeed if α, β are elements of B then, since G acts transitively on Ω, there exists $g \in G$ such that $\alpha g = \beta$. In particular $\alpha g \in B \cap Bg$. Since B is a block, this implies that $Bg = B$, which means that $g \in G_{\{B\}}$.

Observe that if B is a block containing α then $G_{\{B\}}$ contains G_α. Indeed if $g \in G_\alpha$ then $\alpha \in B \cap Bg$ hence $B = Bg$ since B is a block.

Assume that $M = G_\alpha$ is maximal in G. Since $M = G_\alpha \leq G_{\{B\}}$, either $G_{\{B\}} = M$ or $G_{\{B\}} = G$. If $G_{\{B\}} = M = G_\alpha$ then, since $G_{\{B\}}$ acts transitively on B, we deduce that $B = \{\alpha\}$. If $G_{\{B\}} = G$ then, since G acts transitively on Ω, we deduce that $B = \Omega$. This proves that G acts primitively.

Conversely, assume that $M = G_\alpha$ is not maximal in G. We prove that G is not primitive. Since M is not maximal in G, there exists K with $M < K < G$. The set

$$B = \{\alpha k \ : \ k \in K\}$$

is a nontrivial block for G. First, note that if $k \in K - M$ then $\alpha \neq \alpha k \in B$ hence $|B| > 1$, and if $g \in G - K$ then $\alpha g \notin B$ since otherwise we could write $\alpha g = \alpha k$ for some $k \in K$, equivalently $gk^{-1} \in G_\alpha = M < K$ and this would imply $g \in K$. Now we prove that B is a block. If $g \in G$ and $\alpha k \in B \cap Bg$, for some $k \in K$, then there is some $t \in K$ with $\alpha k = \alpha tg$ so $tgk^{-1} \in G_\alpha = M$, this implies that $g \in t^{-1}Mk \subseteq K$ and therefore $Bg = B$. □

We also record an important property of the normal subgroups of a primitive group.

Proposition 5.3. *Let $G \leq S_n$ whose natural action on $\Omega = \{1, \ldots, n\}$ is primitive. Let $\{1\} \neq N \trianglelefteq G$. Then the natural action of N on Ω is transitive.*

Proof. Let $O = \alpha N \subseteq \Omega$ be the N-orbit of $\alpha \in \Omega$. We need to show that $O = \Omega$. We claim that O is a block for the action of G on Ω. If $g \in G$ and $\beta \in O \cap Og$ then there exist $n_1, n_2 \in N$ such that $\beta = \alpha n_1 = \alpha n_2 g$. If $\alpha n \in O$ then

$$\alpha n = \alpha n_2 g n_1^{-1} n = \alpha n_2 \cdot g n_1^{-1} n g^{-1} \cdot g \in \alpha N g = Og,$$

this proves that $O \subseteq Og$ hence $O = Og$. So O is a block for G. Since G acts primitively, either $|O| = 1$ or $O = \Omega$. Since N is nontrivial and G acts faithfully, $O = \alpha N$ contains at least two elements, so $O = \Omega$. □

Exercise 5.4. *If G acts transitively on Ω with point stabilizer A and B is a subgroup of G then B acts transitively if and only if $AB = G$.*

Chapter 6

Multiple transitivity and Jordan's theorem

The material of this section is taken from Wielandt's book [16].

Let G act faithfully on a set Ω, in other words $G \leq \mathrm{Sym}(\Omega)$. Set $n := |\Omega|$.

Let $1 \leq k \leq n$. We say that the action of G on Ω (or G itself) is k-transitive if the natural action of G on the set

$$O_k(\Omega) := \{(x_1, \ldots, x_k) \in \Omega^k \ : \ x_i \neq x_j \ \forall i \neq j\}$$

is transitive. G is called sharply k-transitive if the natural action on $O_k(\Omega)$ is regular. For example S_n in its natural action of degree n is sharply n-transitive and sharply $(n-1)$-transitive.

Since $|\Omega_k| = n(n-1)\cdots(n-k+1)$, if G is k-transitive then $|G|$ is divisible by $n(n-1)\cdots(n-k+1)$, and it equals such number if G is sharply k-transitive. In particular the only n-transitive permutation group of degree n is S_n, the only $(n-1)$-transitive permutation group of degree n is S_n and the only $(n-2)$-transitive permutation groups of degree n are A_n and S_n.

Example: the normalizer in S_5 of a Sylow 5-subgroup of S_5 is sharply 2-transitive of degree 5.

Clearly, if G is k-transitive for some $k \geq 2$ then it is also $(k-1)$-transitive.

Lemma 6.1. *If $2 \leq k \leq n$ and G is k-transitive then it is primitive.*

Proof. By the above remark it is enough to prove this for $k = 2$. Assume that G is 2-transitive and let B be a block for the action of G such that $2 \leq |B| < |\Omega|$. Let $\alpha, \beta \in B$ be distinct. Since $B \neq \Omega$ there exists $\gamma \in \Omega - B$. Since G is 2-transitive there exists $g \in G$ taking the pair (α, β) to (α, γ), in other words $\alpha g = \alpha$, $\beta g = \gamma$. Therefore $\alpha \in B \cap Bg$, however $B \neq Bg$ being $\gamma \in Bg - B$. This contradicts the fact that B is a block. $\square$

Exercise 6.2. *There exist several primitive groups that are not 2-transitive. [Consider groups of prime degree.]*

Assume G is transitive and let $1 \le k \le n$. Then G is k-transitive if and only if there exists $\alpha \in \Omega$ such that the stabilizer $\mathrm{Stab}_G(\alpha)$ is $(k-1)$-transitive on $\Omega - \{\alpha\}$, and in this case this holds for every $\alpha \in \Omega$ by the transitivity of G.

Lemma 6.3. *Assume G is transitive on Ω, $U \le G$ and $\Delta \subseteq \Omega$ is an U-orbit. Denote by U^Δ the image of the natural homomorphism $U \to \mathrm{Sym}(\Delta)$. If U^Δ is primitive on Δ and $|\Omega| < 2|\Delta|$ then G is primitive on Ω.*

Proof. Let $\alpha \in \Delta$. Let B be a block for G. We will show that either $|B| = 1$ or $B = \Omega$. Since G is transitive, if $x \in B$ there exists $g \in G$ with $xg = \alpha$, therefore $\alpha \in Bg$. Now Bg is a block for G, and if we show that either $|Bg| = 1$ or $Bg = \Omega$ then we would have that either $|B| = 1$ or $B = \Omega$, which is what we want, so we may assume $\alpha \in B$.

We claim that $\Delta \cap B$ is a block for U. If $u \in U$ and $\beta \in (\Delta \cap B) \cap (\Delta \cap B)u$, then $\beta \in B \cap Bu$ so, being B a block for G, $B = Bu$. It follows that $(\Delta \cap B)u = \Delta u \cap Bu = \Delta \cap B$ being Δ a U-orbit.

We deduce that $\Delta \cap B$ is a block for U^Δ as well, being contained in Δ. Moreover $\alpha \in \Delta \cap B$. Since U^Δ is primitive on Δ, either $\Delta \cap B = \Delta$ or $\Delta \cap B = \{\alpha\}$. If $\Delta \cap B = \Delta$ then $\Delta \subseteq B$, in particular $|B| \ge |\Delta| > n/2$, but $|B|$ divides $|\Omega| = n$ and this implies that $|B| = n$, in other words $B = \Omega$.

Assume now that $\Delta \cap B = \{\alpha\}$. If $g \in G$ then $\Delta \cap Bg$ is either empty or it is a block for U^Δ. This is proved exactly as in the above proof that $\Delta \cap B$ is a block for U. By the primitivity of U^Δ on Δ, either $|\Delta \cap Bg| \le 1$ or $\Delta \cap Bg = \Delta$. In the second case the same argument as before proves that $Bg = \Omega = B$, so we may assume that $|\Delta \cap Bg| \le 1$ for every $g \in G$. Since $\bigcup_{g \in G} Bg = \Omega$, this implies that there are at least $|\Delta|$ sets of the form Bg, however the number of such blocks is a divisor of n and $|\Delta| > n/2$, hence there are precisely n such blocks, and this can only happen if $|B| = 1$. $\square$

If $\Delta \subseteq \Omega$ and $H \le G$ then we will denote by H_Δ the intersection $\bigcap_{x \in \Delta} \mathrm{Stab}_H(x)$, that is, the pointwise stabilizer of Δ in H.

Corollary 6.4. *Assume G is transitive on Ω and let Δ, Γ be subsets of Ω. Assume $G = \langle C, D \rangle$ where $C \le G_{\Omega - \Gamma}$ acts primitively on Γ, $D \le G_{\Omega - \Delta}$ acts primitively on Δ. Then G is primitive on Ω.*

Proof. Since $G = \langle C, D \rangle$ is transitive and C, D do not move anything outside $\Gamma \cup \Delta$, we deduce that $\Gamma \cup \Delta = \Omega$. Similarly, since C stabilizes Γ and D stabilizes Δ, the fact that $G = \langle C, D \rangle$ is transitive implies that $\Gamma \cap \Delta \ne \varnothing$. These two facts imply that either $|\Delta| > n/2$ or $|\Gamma| > n/2$.

Since C acts primitively on Γ, we have that Γ is a C-orbit, similarly Δ is a D-orbit. Therefore G is primitive by Lemma 6.3. $\qquad\square$

Note that if Δ is a proper subset of Ω and $\alpha \in \Delta$ then $\bigcap_{\alpha \in \Delta g} \Delta g$ is a block for G. Therefore, if G is primitive, then

$$\bigcap_{\Delta g \ni \alpha} \Delta g = \{\alpha\}.$$

This can be phrased by saying that if $\alpha, \beta \in \Delta$ are distinct then there exists $g \in G$ such that $\alpha g \in \Delta$, $\beta g \notin \Delta$.

A group G acting primitively on Ω is called 2-primitive if the stabilizer G_α acts primitively on $\Omega - \{\alpha\}$ for every $\alpha \in \Omega$.

Also, note that if $H \leq G \leq S_n$ and H is primitive, then G is primitive as well.

Proposition 6.5. *Assume G is primitive on Ω and $\Omega = \Gamma \cup \Delta$ where $\Gamma \cap \Delta = \varnothing$, $1 < |\Gamma| < |\Omega|$, $1 \leq |\Delta| < |\Omega|$. If G_Δ is transitive on Γ, then G is 2-transitive on Ω. Moreover, if G_Δ is primitive on Γ, then G is 2-primitive on Ω.*

Proof. Induction on $|\Delta|$. The case $|\Delta| = 1$ is trivial, since by assumption G is transitive on Ω and G_Δ is transitive on Γ. Now assume $|\Delta| > 1$.

Case 1. $2|\Delta| < |\Omega|$. Since $|\Delta| > 1$, there exist $\alpha, \beta \in \Delta$ with $\alpha \neq \beta$. Since G is primitive, there exists $g \in G$ such that $\alpha \in \Delta g$, $\beta \notin \Delta g$. Since $2|\Delta| < |\Omega| = n$, we deduce that $|\Gamma| > n/2$ hence $\Gamma \cap \Gamma g \neq \varnothing$. Since G_Δ is transitive (resp. primitive) on Γ and $g^{-1}G_\Delta g$ is transitive (resp. primitive) on Γg, the group $H := \langle G_\Delta, g^{-1}G_\Delta g \rangle$ is transitive (resp. primitive, by Corollary 6.4, being $g^{-1}G_\Delta g = G_{\Delta g}$) on $\Gamma \cup \Gamma g$. Let $\overline{\Delta} := \Delta \cap \Delta g$, the set of elements of Δ fixed by H, in particular $H \leq G_{\overline{\Delta}}$, so $G_{\overline{\Delta}}$ is transitive (resp. primitive) on $\Gamma \cup \Gamma g = \Omega - \overline{\Delta}$. We have $1 \leq |\overline{\Delta}| < |\Delta|$ being $\alpha \in \overline{\Delta}$ and $\beta \notin \overline{\Delta}$. We may therefore apply induction and deduce that G is 2-transitive (resp. 2-primitive).

Case 2. $2|\Delta| \geq |\Omega|$. Since $|\Gamma| > 1$, there exist $\alpha, \beta \in \Gamma$ with $\alpha \neq \beta$. Since G is primitive, there exists $g \in G$ such that $\alpha \in \Gamma g$, $\beta \notin \Gamma g$. Then $\Gamma \cap \Gamma g$ is non-empty (it contains α) and again the group $H := \langle G_\Delta, g^{-1}G_\Delta g \rangle$ is transitive (resp. primitive) on $\Gamma \cup \Gamma g$. Since $2|\Delta| \geq |\Omega|$, we have $2|\Gamma| \leq |\Omega|$ and this implies that $\Gamma \cup \Gamma g \neq \Omega$. Moreover, since $\Gamma \neq \Gamma g$, the set Γ is properly contained in $\Gamma \cup \Gamma g$. Setting $\overline{\Delta} := \Delta \cap \Delta g$, we find that $\Omega - \overline{\Delta} = \Gamma \cup \Gamma g$ and $0 < |\overline{\Delta}| < |\Delta|$. We may therefore apply induction and deduce that G is 2-transitive (resp. 2-primitive). $\qquad\square$

Theorem 6.6 (Jordan)**.** *Assume G is primitive on Ω, G_Δ is primitive on $\Omega - \Delta = \Gamma$ and $1 < |\Gamma| = m < n = |\Omega|$. Then G is $(n - m + 1)$-transitive.*

Proof. Induction on $|\Delta| = n - m$. The case $|\Delta| = 1$ is trivial since by assumption G_Δ is primitive on Γ. Now assume $|\Delta| > 1$. Proposition 6.5 implies that G is 2-primitive, hence if $\delta \in \Delta$ then $\text{Stab}_G(\delta)$ acts primitively on $\Omega - \{\delta\}$. Since $\Omega - \{\delta\}$ equals the disjoint union $\Gamma \cup (\Delta - \{\delta\})$ we may apply induction and deduce that $\text{Stab}_G(\delta)$ is $(n - m)$-transitive on $\Omega - \{\delta\}$. Since this holds for every $\delta \in \Delta$, we deduce that G is $(n - m + 1)$-transitive. $\qquad\square$

Corollary 6.7. *Let $G \leq S_n$ act primitively on $\Omega = \{1, \ldots, n\}$. If G contains a transposition then $G = S_n$. If G contains a 3-cycle then $G = A_n$ or $G = S_n$.*

Proof. Let g be a 2-cycle or a 3-cycle in S_n and assume $g \in G$. Let Γ be the set of points moved by g and $\Delta = \Omega - \Gamma$. Clearly, $|\Gamma| \in \{2, 3\}$ and G_Δ acts primitively on Γ, since $g \in G_\Delta$ and $\langle g \rangle$ acts primitively on Γ since $|\Gamma|$ is a prime number. Theorem 6.6 implies that G is $(n - 1)$-transitive if $|\Gamma| = 2$, and G is $(n - 2)$-transitive if $|\Gamma| = 3$. In the first case $|G|$ is divisible by $n!$, hence $G = S_n$, in the second case $|G|$ is divisible by $n!/2$, hence $G = A_n$ or $G = S_n$. $\qquad\square$

This easily implies that the maximal imprimitive subgroups of S_n are maximal subgroups of S_n. Indeed a proper subgroup properly containing them would be primitive and would contain a 2-cycle (moving two elements of a block).

A similar argument can be used for A_n using 3-cycles (being the 2-cycles odd permutations) but it is more tricky since there could be blocks of size 2. Actually, in the case of the alternating group A_n, the maximality of the maximal imprimitive subgroups holds for $n \neq 8$. The imprimitive subgroup $A_8 \cap (S_2 \wr S_4)$ is properly contained in the affine group $\text{AGL}_3(2)$: see [10].

More in general, it is possible to prove the following.

Theorem 6.8. *Let $G \leq S_n$ act primitively on $\Omega = \{1, \ldots, n\}$ and assume G contains a p-cycle for some prime p such that $p \leq n - 3$. Then $G = A_n$ or $G = S_n$.*

Exercise 6.9. *If G is a solvable 4-transitive permutation group then $G \cong S_4$. Hint: show that any minimal normal subgroup N is regular and study the conjugation action of a point stabilizer on N (N is a vector space over a field with p elements, p prime, and the conjugation action of the point stabilizer on $N - \{1\}$ is 3-transitive and linear).*

Chapter 7

Maximal intransitive subgroups

A subgroup of S_n is called maximal intransitive if it is maximal among the intransitive subgroups of S_n. We saw that the maximal intransitive subgroups of S_n are of type $G = \mathrm{Stab}(O)$ where O is a non-empty proper subset of $\Omega = \{1, \ldots, n\}$. Such subgroups are of type $S_a \times S_b$ where $0 < a = |O| < n$, $b = n - a = |\Omega - O|$, $a + b = n$. We study the maximality of G inside S_n. If G is not maximal then it is properly contained in $K \leq S_n$ which therefore is transitive on Ω. If K is primitive then it contains a 2-cycle, moving 2 elements of O or of $\overline{O} := \Omega - O$, and Jordan's theorem implies that $K = S_n$.

Suppose now that K is imprimitive, let B be a nontrivial block for K. Then B is a nontrivial block for G, therefore $B \cap O$ is either empty or a block for G^O and $B \cap \overline{O}$ is either empty or a block for $G^{\overline{O}}$. Since $G^O \cong \mathrm{Sym}(O)$ is primitive on O and $G^{\overline{O}} \cong \mathrm{Sym}(\overline{O})$ is primitive on $\overline{O}$, we deduce that either $|B \cap O| \leq 1$ or $B \cap O = O$, furthermore either $|B \cap \overline{O}| \leq 1$ or $B \cap \overline{O} = \overline{O}$.

Assume $B \cap O = \{\alpha\}$, $B \cap \overline{O} = \{\beta\}$, then $B = \{\alpha, \beta\}$. If there exists $\gamma \in O - B$ then $g = (\alpha\gamma) \in G$ and $Bg = \{\beta, \gamma\}$, a contradiction, and similarly $\overline{O} - B = \varnothing$, so $\Omega = B$ and $n = 2$, this contradicts the fact that B is nontrivial.

Assume $B \cap O = \{\alpha\}$, $B \supseteq \overline{O}$. Then $B = \{\alpha\} \cup \overline{O}$, however this is a contradiction because, since B is a nontrivial block, there exists $\beta \in O - B$, hence there exists $g \in G$ such that $\alpha g = \beta$ (being $G^O = \mathrm{Sym}(O)$) so $Bg = \{\beta\} \cup \overline{O}$ is not disjoint from B and not equal to B.

We are left with the case in which one of $B \cap O$ and $B \cap \overline{O}$ is empty, say $B \cap O = \varnothing$. Then $B = \overline{O}$. Since K is transitive, there exists $k \in K$ that takes an element of $\overline{O}$ to an element of O, hence $Bk \subseteq O$. But then

$Bk = Bk \cap O$ is a block for $G^O = \mathrm{Sym}(O)$, of size at least 2, hence $Bk = O$.

This proves that if O is a proper subset of Ω and $G = \mathrm{Stab}(O) < \mathrm{Sym}(\Omega)$ is not a maximal subgroup then $|\Omega| > 2$ and $|O| = |\overline{O}|$. In other words G has type $S_a \times S_a$ with $2a = n$. Indeed, such subgroup is not maximal if $n > 2$: it is contained in an imprimitive wreath product $S_a \wr S_2$, the stabilizer of a partition with two parts of size a, which, as we will see in the next section, is a maximal subgroup of S_{2a}.

Chapter 8

Maximal imprimitive subgroups

If H and K are two groups and $K \leq S_n$, then $H wr K = H \wr K$ denotes the wreath product between H and K, i.e., the semidirect product $H^n \rtimes K$, where K acts on H^n by permuting the coordinates. More specifically $\pi \in K$ acts on H^n by

$$(x_1, \ldots, x_n)^\pi = (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}}).$$

This may look strange but it is necessary to have a well-defined action on the right, indeed defining $t_i = x_{i\pi^{-1}}$ we have $t_{i\tau^{-1}} = x_{i\tau^{-1}\pi^{-1}} = x_{i(\pi\tau)^{-1}}$ hence

$$((x_1, \ldots, x_n)^\pi)^\tau = (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}})^\tau = (x_{1\tau^{-1}\pi^{-1}}, \ldots, x_{n\tau^{-1}\pi^{-1}})$$
$$= (x_{1(\pi\tau)^{-1}}, \ldots, x_{n(\pi\tau)^{-1}}) = (x_1, \ldots, x_n)^{\pi\tau}.$$

Recall that exponentiating by π means conjugation $(\pi^{-1}g\pi)$.

Note that if $K \leq S_n$ then $|H \wr K| = |H|^n |K|$, so for example $|S_a \wr S_b| = a!^b b!$.

If $a, b > 1$ and $ab = n$, then the full wreath product $S_a \wr S_b$ embeds into S_n as an imprimitive subgroup. To see this it is enough to check that $S_a \wr S_b$ acts faithfully and imprimitively on the set $\{1, \ldots, a\} \times \{1, \ldots, b\}$, which is a set of size $ab = n$, by the rule

$$(i, j)^{(x_1, \ldots, x_b)\sigma} := (ix_j, j\sigma).$$

This is an action since

$$(i, j)^{(x_1, \ldots, x_b)\sigma \cdot (y_1, \ldots, y_b)\tau} = (i, j)^{(x_1 y_{1\sigma}, \ldots, x_b y_{b\sigma})\sigma\tau} = (ix_j y_{j\sigma}, j\sigma\tau),$$
$$\left((i, j)^{(x_1, \ldots, x_b)\sigma}\right)^{(y_1, \ldots, y_b)\tau} = (ix_j, j\sigma)^{(y_1, \ldots, y_b)\tau} = (ix_j y_{j\sigma}, j\sigma\tau).$$

This action is imprimitive admitting $B_j = \{1, \ldots, a\} \times \{j\}$ as a block system, $j = 1, \ldots, b$. Indeed,

$$B_j^{(x_1, \ldots, x_b)\sigma} = B_j^{\sigma} = B_{j\sigma}.$$

The block system consists of b blocks of size a. Also, it is easy to see that this action is faithful. Therefore $S_a \wr S_b$ embeds into S_{ab} as an imprimitive subgroup.

Actually $S_a \wr S_b$ is a maximal imprimitive subgroup, meaning that it is not properly contained in any imprimitive subgroup of S_n. Moreover, every maximal imprimitive subgroup is of this type. This can be proved using the following result, which is due to Frobenius.

Theorem 8.1 (Embedding Argument). *Let H be a subgroup of the finite group G, let $x_1, \ldots, x_n$ be a right transversal for H in G, and let ξ be any homomorphism with domain H, say $\xi : H \to X$. Then the map*

$$f: \ G \to \xi(H) \wr S_n,$$

$$x \mapsto (\xi(x_1 x x_{1\pi}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1}))\pi,$$

where $\pi \in S_n$ is the unique permutation that satisfies $x_i x \in H x_{i\pi}$ for all $i = 1, \ldots, n$, is a well-defined homomorphism with kernel equal to the normal core of $\ker \xi$ in G, in other words $\ker f = (\ker \xi)_G$.

Proof. Since $x_i \in H x_i$ the permutation corresponding to the identity is 1 hence $f(1) = 1$. Now let $x, y \in G$ and assume $x_i x x_{i\pi}^{-1} \in H$, $x_i y x_{i\tau}^{-1} \in H$ for all $i \in I = \{1, \ldots, n\}$, then applying the second to $i\pi$ we find $x_{i\pi} y x_{i\pi\tau}^{-1} \in H$ for all $i \in I$, so $x_i x y x_{i\pi\tau}^{-1} = (x_i x x_{i\pi}^{-1})(x_{i\pi}^{-1} y x_{i\pi\tau}^{-1}) \in H$. It follows that the permutation corresponding to xy is $\pi\tau$ and

$$f(xy) = (\xi(x_i x y x_{i\pi\tau}^{-1}))_{i \in I} \pi\tau = (\xi(x_i x x_{i\pi}^{-1})\xi(x_{i\pi} y x_{i\pi\tau}^{-1}))_{i \in I} \pi\tau$$

$$= f(x) \cdot \pi^{-1}(\xi(x_{i\pi} y x_{i\pi\tau}^{-1}))_{i \in I} \pi\tau = f(x) \cdot (\xi(x_i y x_{i\tau}^{-1}))_{i \in I} \tau = f(x)f(y).$$

$f(x) = 1$ if and only if the permutation π corresponding to x is the identity and $x_i x x_i^{-1} \in \ker(\xi)$ for all $i \in I$, in other words $x \in x_i^{-1} \ker \xi x_i$ for all $i \in I$. Since $\ker \xi \trianglelefteq H$, the conjugates of $\ker \xi$ in G are precisely the groups $x_i^{-1}(\ker \xi) x_i$ for $i \in I$. This proves that $\ker f = (\ker \xi)_G$. $\qquad\square$

Now assume $G \leq S_n$ acts transitively and imprimitively on $\Omega = \{1, \ldots, n\}$. This means that there is a nontrivial imprimitivity block B for G, let $a = |B|$. Let $H = G_{\{B\}} = \{g \in G : Bg = B\}$, the setwise stabilizer of B. Observe that G acts transitively on the set of blocks $\{Bg : g \in G\}$ with H as point stabilizer, so $|G : H|$ equals the number of translates of B, call it b. Since the translates of B partition Ω we have $ab = n$. Of course we have a homomorphism $\xi : H \to Sym(B) \cong S_a$ induced

by the action of H on B. By Theorem 8.1 we deduce a homomorphism $f : G \to \xi(H) \wr S_b \leq S_a \wr S_b$ with kernel the normal core of $\ker(\xi)$ in G. Observe that if $h \in \ker(\xi)$ then h fixes B pointwise, and if $h \in \ker(\xi)^g$ then $ghg^{-1} \in \ker(\xi)$ so h fixes Bg pointwise. This implies that $(\ker(\xi))_G = \{1\}$ hence f is injective. This means that G embeds in the wreath product $S_a \wr S_b$, on the other hand such wreath product embeds in S_n as an imprimitive subgroup with blocks of size a. This proves that the stabilizers in S_n of the partitions consisting of b blocks of size a (i.e. the maximal imprimitive subgroups of S_n with blocks of size a) are isomorphic to wreath products $S_a \wr S_b$. Similarly, the maximal imprimitive subgroups of A_n with b blocks of size a are isomorphic to the intersection between A_n and the maximal imprimitive subgroups of S_n with b blocks of size a, in other words, with abuse of notation, they are of the form $A_n \cap (S_a \wr S_b)$ (and not $A_a \wr A_b$, careful!).

Also, in the previous argument, we may restrict the codomain of f to $\xi(H) \wr K$ where K is the image of the homomorphism $G \to S_b$ corresponding to the transitive action of G on the b blocks. $\xi(H)$ and K could be called "components" of G. Therefore we can always embed any imprimitive group G into the wreath product of the so-called "primitive components" of G. Specifically, we start with a block B whose setwise stabilizer acts primitively on it (that is, a "minimal block"), meaning that the setwise stabilizer $H := G_{\{B\}}$ acts primitively on B, then we apply the above construction giving $G \leq \xi(H) \wr K$ with $K \leq S_b$ transitive of degree b, and we repeat the process with K if K is imprimitive, otherwise we stop. This gives an embedding fo G in the so-called iterated wreath product

$$G \leq P_1 \wr P_2 \wr P_3 \wr \ldots \wr P_k,$$

where the notation is $X \wr Y \wr Z := X \wr (Y \wr Z)$. The groups $P_1, \ldots, P_k$ are primitive groups which are called the primitive components of G.

For example the dihedral group of order 8 (inside S_4), $D = \langle (1234), (24) \rangle$ acts imprimitively on $\{1, 2, 3, 4\}$ having $B = \{1, 3\}$ as a block. The above argument shows that D embeds into $C_2 \wr C_2$ and this actually shows that D and $C_2 \wr C_2$ are isomorphic (they have the same order).

We will see that if $a \geq 5$ then $S_a \wr S_b$ is also a primitive group (abstractly) with the so-called product action (see section 9.3) but the degree of primitivity is much larger: a^b. This falls into a broader concept which is the following: the primitive groups of degree n, other than A_n and S_n, are "small": their order is less than 4^n, as proved by Praeger and Saxl in 1980 building up on results of Wielandt [12]. More work in this direction was done by several authors in [5, 8, 13, 11]. The first result of this type was proved by Bochert in [3].

Note that we are in the position to clearly understand the maximal subgroups of S_6. We have the alternating group A_6, the maximal intransitive subgroups $S_1 \times S_5$, $S_2 \times S_4$ and the maximal imprimitive

subgroups $S_2 \wr S_3$, $S_3 \wr S_2$. We have seen that S_5 acts on its 6 Sylow 5-subgroups and this action is primitive because, as we have seen, the normalizer of a Sylow 5-subgroup of S_5 is maximal in S_5. Therefore S_5 embeds in S_6 as a primitive subgroup, which is maximal in S_6 because it has index 6. So S_6 has one class of primitive maximal subgroups isomorphic to S_5. This is the list of all the maximal subgroups of S_6.

Exercise 8.2. *Let $n = p^k$ be a prime power. The iterated wreath product $P = C_p \wr C_p \wr \ldots \wr C_p$ of k copies of C_p is isomorphic to the Sylow p-subgroups of S_n.*

Exercise 8.3. *Let $n = mp^k$ with m not divisible by p. Let $\Omega = \{1, \ldots, n\}$ and let P be a Sylow p-subgroup of S_n. Show that*

- *The action of P on Ω is transitive if and only if $m = 1$.*

- *The action of P on Ω is primitive if and only if $m = k = 1$.*

Chapter 9

Primitive maximal subgroups

9.1 Characteristically simple groups

Recall that if G is a group then a subgroup N of G is called characteristic if $N^\varphi = N$ for every $\varphi \in \operatorname{Aut}(G)$ and in this case the notation is $N \trianglelefteq_c G$. For every $g \in G$, the map $\gamma_g : G \to G$, $x^{\gamma_g} := x^g = g^{-1}xg$ is an automorphism of G, therefore if $N \trianglelefteq_c G$ then $N \trianglelefteq G$.

Note that if $A \trianglelefteq_c B \trianglelefteq G$ then $A \trianglelefteq G$ because $\gamma_g|_B \in \operatorname{Aut}(B)$ for every $g \in G$.

G is called *characteristically simple* if its only characteristic subgroups are $\{1\}$ and G. Obviously, every simple group is characteristically simple.

A subgroup N of a group G is called a minimal normal subgroup of G if $N \neq \{1\}$ and whenever $L \leq N$, $L \trianglelefteq G$, either $L = \{1\}$ or $L = N$. Note that every minimal normal subgroup of G is characteristically simple. Indeed, if $L \trianglelefteq_c N$ then, since $N \trianglelefteq G$, L is normal in G, hence $L = \{1\}$ or $L = N$ by minimality of N.

Proposition 9.1. *If S is a nonabelian simple group the normal subgroups of $S^n = S \times \cdots \times S$ are its subproducts, in other words, the subgroups $T_1 \times \cdots \times T_n$ where T_i is either $\{1\}$ or S, for every $i \in \{1, \ldots, n\}$. In particular, the minimal normal subgroups of S^n are its factors.*

Proof. Let N be a normal subgroup of S^n with a nontrivial element $g = (s_1, \ldots, s_n)$ and suppose $s_1 \neq 1$. Then conjugating with $(x, 1, 1, \ldots, 1)$ we find that N contains all the elements $g_x = (s_1^x, s_2, \ldots, s_n)$, so that $N \ni g_x g^{-1} = (t_x, 1, 1, \ldots, 1)$ where $t_x = [x^{-1}, s_1] = x^{-1}s_1 x s_1^{-1}$. Since S is a nonabelian simple group, its center is trivial, in particular $s_1 \notin Z(S)$, hence there exists $x \in S$ such that $t_x \neq 1$. The conjugacy class of an

element always generates a normal subgroup, so since S is a nonabelian simple group and $t_x \neq 1$, the conjugates of t_x in S generate S. Since N is normal in S^n, this implies that N contains $S \times \{1\} \times \ldots \times \{1\}$. The same argument shows that N contains the i-th factor of S^n whenever $s_i \neq 1$, and proves the claim. $\square$

Proposition 9.2. *Let G be a finite group. G is characteristically simple if and only if there exist a (possibly abelian) simple group S and a natural number n such that $G \cong S^n$.*

Proof. If S is a simple group and n is a natural number then $G = S^n$ is characteristically simple. To see this, note that if S is abelian then $S \cong C_p$ for some prime p and $\mathrm{Aut}(G) \cong \mathrm{GL}(n, p)$, the group of invertible $n \times n$ matrices with coefficients in $\mathbb{F}_p$, where we may see C_p as the additive group of the field with p elements $\mathbb{F}_p$, being $\mathbb{F}_p$-linearity automatic from additivity. Since $\mathrm{GL}(n, p)$ acts transitively on the nonzero vectors, $C_p{}^n$ is characteristically simple. If S is nonabelian, the fact that S^n is characteristically simple follows from Proposition 9.1 and the fact the symmetric group of degree n acts as a group of automorphisms of S^n by permuting the coordinates, so the subproducts are permuted around. See the exercises.

Now assume G is characteristically simple. If N is a minimal normal subgroup of G then N^f is a minimal normal subgroup of G for every $f \in \mathrm{Aut}(G)$. Since G is characteristically simple,

$$\langle N^f \; : \; f \in \mathrm{Aut}(G) \rangle = G.$$

We claim that any subgroup of G which is generated by some number m of subgroups of type N^f is a direct product of some of them. We proceed by induction on m. Assume that $H \leq G$ is generated by $m > 1$ subgroups of type N^f, say $N^{f_1}, \ldots, N^{f_m}$, where $f_1, \ldots, f_m \in \mathrm{Aut}(G)$. Let $K := \langle N^{f_i} \; : \; i \geq 2 \rangle$. By induction K is a direct product of some N^{f_i}. Since $K \trianglelefteq G$ and N^{f_1} is a minimal normal subgroup of G, if $N^{f_1} \cap K \neq \{1\}$ then $N^{f_1} \leq K$ hence $H = K$ and the result follows. If instead $N^{f_1} \cap K = \{1\}$ then $H = N^{f_1} \times K$ and we are done.

We deduce that G is a direct product of some of the N^{f_i}. Since each N^{f_i} is a minimal normal subgroup of G, they are all simple. Setting $S = N^{f_1}$ we have $N^{f_i} = S^{f_1^{-1} f_i} \cong S$ for all i. $\square$

Exercise 9.3. *Let M be a maximal subgroup of a finite solvable group. Prove that M has prime power index (Hint: by induction on $|G|$; let N be a minimal normal subgroup of G, if $M \geq N$ then work in G/N and use induction, otherwise observe that N is characteristically simple).*

Exercise 9.4. *Let G be a finite group. If $|G| \geq 3$ then $\mathrm{Aut}(G) \neq \{1\}$.*

Exercise 9.5. *Let G be a finite group. Then G is elementary abelian if and only if the natural action of $\mathrm{Aut}(G)$ on $G - \{1\}$ is transitive.*

Exercise 9.6. *Let T be a nonabelian simple group. Prove that*

$$\mathrm{Aut}(T^n) \cong \mathrm{Aut}(T) \wr S_n.$$

[Use the embedding argument with $H = N_{\mathrm{Aut}(T^n)}(R)$ and $\xi : H \to \mathrm{Aut}(R)$ the homomorphism induced by the natural action of H on R, where $R = T \times \{1\} \times \cdots \times \{1\}$. Note that $|G : H| = n$, where $G = \mathrm{Aut}(T^n)$, since G acts transitively on the n factors of T^n and H is the stabilizer of one of the factors.]

9.2   Primitive groups: structure

When studying the structure of primitive groups it is useful to give a "permutation-free" definition, using Proposition 5.2.

Definition 9.7 (Primitive group - abstract definition). *We say that a finite group G is primitive of degree n if it admits a maximal subgroup M of index n whose normal core is trivial, i.e. $M_G = \{1\}$. In other words, M is a core-free maximal subgroup.*

Such a group G can be seen as a permutation group of degree n by means of its right multiplication action on $\Omega = \{Mx : x \in G\}$. The corresponding homomorphism $\gamma : G \to \mathrm{Sym}(\Omega)$ is injective because its kernel is $M_G = \{1\}$, and the permutation group $\gamma(G) \cong G$ on Ω is primitive in the sense that it has no nontrivial blocks. Note that this is precisely the situation we are in when we consider a group $G \leq \mathrm{Sym}(\Omega)$ (inclusion homomorphism, injective) acting primitively on Ω.

Now we will analyze the structure of primitive groups by discussing Baer's theorem, which indicates that primitive groups can be divided in three main types, called type I, type II and type III. We start with the following very useful fact.

Lemma 9.8 (Dedekind's modular law). *Let A, B, C be subgroups of G and assume $A \leq B$. Then $A(B \cap C) = B \cap AC$.*
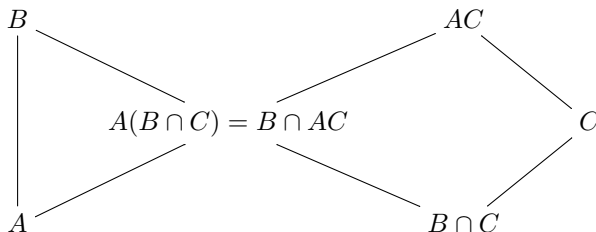
Proof. The inclusion $\subseteq$ is trivial since $A \subseteq B$ and $B \cap C \subseteq C \subseteq AC$, being $1 \in A$. Now assume $b \in B \cap AC$ and write $b = ac$ where $a \in A$, $c \in C$. Then $c = a^{-1}b \in B$ since $a \in A \subseteq B$ and B is a subgroup, therefore $c \in B \cap C$ and this implies that $b = ac \in A(B \cap C)$. $\square$

Recall that the socle of a finite group G, denoted by $\mathrm{soc}(G)$, is the subgroup of G generated by the minimal normal subgroups of G. Clearly, if $\mathrm{soc}(G)$ is a minimal normal subgroup of G, then it is the unique minimal normal subgroup of G. A group admitting a unique minimal normal subgroup is usually called *monolithic*. Note that there are monolithic groups that are not primitive, for example the cyclic group C_4.

Recall the following important fact.

Proposition 9.9 (Frattini argument)**.** *If G is a finite group, $N \trianglelefteq G$ and P is a Sylow subgroup of N then $N_G(P) \cdot N = G$. In particular, the Frattini subgroup of G is nilpotent.*

Proof. If $g \in G$ then, being $N \trianglelefteq G$, we have $P^g \leq N$ hence P^g is a Sylow subgroup of N. By Sylow's theorem, there exists $n \in N$ such that $P^g = P^n$, so that $gn^{-1} \in N_G(P)$, therefore $g \in N_G(P) \cdot N$. This proves that $G = N_G(P) \cdot N$. If N is the Frattini subgroup $\Phi(G)$ of G then P must be normal in G, otherwise $N_G(P) \cdot N$ would be contained in a maximal subgroup of G. This implies that all Sylow subgroups of N are normal in N, hence N is nilpotent. $\square$

Using this, it is easy to see that a monolithic group G is primitive if and only if its socle is not contained in the Frattini subgroup of G. In the following result, primitive groups of type I and II are monolithic, while primitive groups of type III are not.

Theorem 9.10 (Baer)**.** *Let G be a finite group. Then G is primitive if and only if there exists a proper subgroup U of G such that $UN = G$ whenever N is a nontrivial normal subgroup of G. Now assume this is the case, and let M be a core-free maximal subgroup of G. If N is a nontrivial normal subgroup of G then $C_G(N) \cap M = \{1\}$, moreover either $C_G(N) = \{1\}$ or $C_G(N)$ is a minimal normal subgroup of G. Furthermore, precisely one of the following conditions holds.*

1. $N = \mathrm{soc}(G)$ *is an abelian minimal normal subgroup of G complemented by M. In this case G is called affine or primitive of type I.*

2. $N = \mathrm{soc}(G)$ *is a nonabelian minimal normal subgroup of G supplemented by M. In this case G is called primitive of type II.*

3. *G admits precisely two minimal normal subgroups A, B and $N = \mathrm{soc}(G) = A \times B$. Moreover A and B are nonabelian, $A = C_G(B)$,*

$B = C_G(A)$, *M complements both A and B in G and $A \cong AB \cap M \cong$*
B. In this case G is called primitive of type III.

Proof. If G is primitive and M is a core-free maximal subgroup of G
then M does not contain any nontrivial normal subgroup of G and
$M < MN \leq G$ for all $N \trianglelefteq G$, therefore $MN = G$ for all $\{1\} \neq N \trianglelefteq G$.
Conversely if G is a finite group and the proper subgroup U of G satisfies
$UN = G$ whenever N is a nontrivial normal subgroup of G then let M
be a maximal subgroup of G containing U. We have $M_G = \{1\}$, because
otherwise, since $M_G \trianglelefteq G$, we would have $G = UM_G \leq M$, a contradiction.
So G is primitive.

Now let G be primitive and let M be a core-free maximal subgroup of
G.

If N is a nontrivial normal subgroup of G then $C_G(N)$ is the kernel
of the conjugation action $G \to \mathrm{Aut}(N)$, hence $C_G(N) \trianglelefteq G$, therefore
$M \cap C_G(N) \trianglelefteq M$, so M is contained in the normalizer $N_G(M \cap C_G(N))$. But
N is also contained in such normalizer, hence $G = MN \leq N_G(M \cap C_G(N))$
which implies that $M \cap C_G(N) \trianglelefteq G$. Since $M_G = \{1\}$, we deduce that
$M \cap C_G(N) = \{1\}$. If $C_G(N) \neq \{1\}$ then, since G is finite, there exists a
minimal normal subgroup X of G contained in $C_G(N)$. Since $M_G = \{1\}$
we have $XM = G$. By Dedekind's law

$$C_G(N) = C_G(N) \cap G = C_G(N) \cap XM = X(C_G(N) \cap M) = X.$$

This implies that $C_G(N)$ is a minimal normal subgroup of G.

If G admits three distinct minimal normal subgroups A, B, C then B,
C are contained in $C_G(A)$ being $A \cap B = \{1\}$ and $A \cap C = \{1\}$ and
this contradicts the fact that $C_G(A)$, if nontrivial, is a minimal normal
subgroup of G. This proves that G admits at most two minimal normal
subgroups.

Assume first that G contains only one minimal normal subgroup, call it
N. Since M is a core-free maximal subgroup, $MN = G$. If N is nonabelian
then G is a primitive group of type II. Assume now that N is abelian. Then
$N \leq C_G(N)$ and, since $C_G(N)$ is a minimal normal subgroup of G, we
deduce that $C_G(N) = N$. This implies that $M \cap N = M \cap C_G(N) = \{1\}$,
in other words M is a complement for N in G hence G is a primitive group
of type I.

Finally assume that G contains precisely two minimal normal subgroups,
A and B. Clearly $N = \mathrm{soc}(G) = A \times B$. The fact that $A \cap B = \{1\}$ implies
that $A \leq C_G(B)$ and $B \leq C_G(A)$, so since $C_G(A)$ and $C_G(B)$ are minimal
normal subgroups of G, we deduce that $A = C_G(B)$ and $B = C_G(A)$. In
particular A and B are nonabelian. Moreover $M \cap A = M \cap C_G(B) = \{1\}$
and $M \cap B = M \cap C_G(A) = \{1\}$, so M complements both A and B in G.
By Dedekind's law,

$$A(AB \cap M) = AB \cap AM = AB \cap G = AB,$$

$$B(AB \cap M) = AB \cap BM = AB \cap G = AB,$$

therefore

$$A \cong A/A \cap B \cong AB/B = B(AB \cap M)/B \cong AB \cap M,$$

$$B \cong B/A \cap B \cong AB/A = A(AB \cap M)/A \cong AB \cap M.$$

It follows that $A \cong AB \cap M \cong B$. $\square$

It is worth noting that the two minimal normal subgroups of a primitive group G of type III, although isomorphic, are not G-isomorphic, in other words no isomorphism between them is compatible with the conjugation action of G. The reason is that G-isomorphic normal subgroups of G must have the same centralizer.

Exercise 9.11. *What are the primitive groups with nontrivial center?*

Exercise 9.12. *For which values of n is the dihedral group D_{2n} (of order $2n$) primitive?*

It follows from Baer's theorem that primitive groups of type I are of the form $\mathbb{F}_p^n \rtimes M$ where M is an irreducible subgroup of $\mathrm{GL}(\mathbb{F}_p^n)$. If q is any prime power, the full affine group $\mathbb{F}_q^n \rtimes GL(\mathbb{F}_q^n)$ is denoted by $\mathrm{AGL}(\mathbb{F}_q^n)$ or $\mathrm{AGL}(n, q)$.

We will now describe the primitive groups of type II.

Proposition 9.13. *Let G be a finite group. The following are equivalent.*

1. *G is primitive of type II.*

2. *There exists a minimal normal subgroup N of G such that $C_G(N) = \{1\}$.*

3. *There exists a nonabelian minimal normal subgroup N of G such that, up to isomorphism, $N \leq G \leq \mathrm{Aut}(N)$, where N is embedded in $\mathrm{Aut}(N)$ via the natural conjugation action $N \to \mathrm{Aut}(N)$.*

Proof. By Baer's theorem, (1) implies (2). If (2) holds then the conjugation action $G \to \mathrm{Aut}(N)$ has kernel $C_G(N) = \{1\}$, so (3) follows. If (3) holds then any element of the centralizer $C_G(N)$ is an automorphism of N fixing N pointwise, hence $C_G(N) = \{1\}$ and (2) follows.

We are left to prove that (2) implies (1). The Frattini subgroup of G is nilpotent, however N is not nilpotent being a direct product of nonabelian simple groups. Since every subgroup of a nilpotent group is nilpotent, this implies that there exists a maximal subgroup M of G not containing N. In particular N is not contained in the normal core M_G of M in G. The intersection $N \cap M_G$ is normal in G and contained in N, so since N is a minimal normal subgroup, $N \cap M_G = \{1\}$. This implies that

$M_G \leq C_G(N) = \{1\}$, hence $M_G = \{1\}$. Moreover, N is the unique minimal normal subgroup of G since any other minimal normal subgroup would be contained in $C_G(N) = \{1\}$. This proves that G is primitive of type II. $\square$

A finite group G is called *almost-simple* if it is primitive of type II and its socle is a simple group, which is therefore nonabelian. Equivalently, G admits a nonabelian simple normal subgroup S such that $C_G(S) = \{1\}$. Equivalently, there exists a nonabelian simple group S such that $S \leq G \leq \operatorname{Aut}(S)$. Of course, every nonabelian simple group is in particular almost-simple. An easy example of an almost-simple group which is not simple is the symmetric group S_n for $n \geq 5$, its socle being the nonabelian simple group A_n. Actually, as we have seen, if $n \neq 6$ then S_n is the full automorphism group of A_n.

Proposition 9.14. *Let G be a finite group. Then the following are equivalent.*

1. *G is primitive of type II.*

2. *There exists an almost-simple group X with socle S and a transitive group $K \leq S_m$ such that G is isomorphic to a subgroup of $X \wr K$ containing S^m and the restriction of the natural projection $G \to K$ is surjective.*

Proof. Assume (2) holds. Let $S = \operatorname{soc}(X)$, a nonabelian simple group. Then $N = S^m$ is a minimal normal subgroup of G since S is simple and K acts transitively on the components. We are left to check that $C_G(N) = \{1\}$. If $g \in C_G(N)$ then of course the permutational part of g is trivial since g must fix all the direct factors of N. So g has type $(x_1, \ldots, x_m)$ and x_i is an element of X centralizing S, so since $C_X(S) = \{1\}$ we deduce that $x_i = 1$ for all i.

Assume (1) holds. Let $N = T_1 \times \ldots \times T_m$ be the socle of G, where the T_i's are pairwise isomorphic nonabelian simple groups. Denote by R the first factor, $R := T_1 \times \{1\} \times \ldots \times \{1\}$. Let $H := N_G(R)$ and $C := C_G(R) \trianglelefteq H$. Note that since $R \cong T_1$ is a nonabelian simple group, $R \cap C = \{1\}$. We claim that $X := H/C$ is an almost-simple group with socle RC/C. Clearly RC/C is a normal subgroup of H/C and $RC/C \cong R/R \cap C \cong R$ is nonabelian simple. We are left to show that $C_{H/C}(RC/C)$ is trivial. Assume that $h \in H$ is such that hC centralizes RC/C, in other words $hCrC = rChC$ for all $r \in R$, then $h^{-1}r^{-1}hr \in R \cap C = \{1\}$ for all $r \in R$ and this implies that $h \in C$, in other words $hC = C$.

We now apply the embedding argument to the natural homomorphism $\xi : H \to \operatorname{Aut}(R)$. Note that $\ker(\xi) = C$, $\xi(H) \cong H/C = X$ and the conjugates of C in G are precisely the centralizers of the direct factors of N, therefore an element belongs to the normal core $\ker(\xi)_G$ if and only if

it centralizes all of the factors, in other words $\ker(\xi)_G = C_G(N) = \{1\}$. The group K is the image of the homomorphism $G \to S_m$ given by the conjugation action of G on the direct factors of N, which is transitive being N a minimal normal subgroup of G. □

In particular, from this proposition it follows that we have a whole family of examples of primitive groups of type II which are not almost-simple: all the wreath products $X \wr K$ where X is an almost-simple group and K is a transitive group of permutations of degree at least 2. For example $S_n \wr S_m$ is of this type when $n \geq 5$, $m \geq 2$. Moreover, we deduce that primitive groups of type II are strongly related to wreath products of this type. An example of primitive group of type II which is not almost-simple and not a wreath product is the following, for all $m \geq 2$, where X is an almost-simple group with socle S.

$$\{(x_1, \ldots, x_m)\pi \in X \wr S_m \ : \ x_1 \equiv \ldots \equiv x_m \mod S\}.$$

We will now describe the primitive groups of type III.

Proposition 9.15. *Let G be a finite group. The following are equivalent.*

1. *G is primitive of type III.*

2. *There exist a nonabelian minimal normal subgroup N of G and a subgroup $M \leq G$ complementing both N and $C_G(N)$.*

Proof. (1) implies (2) by Baer's Theorem. Now assume (2) holds. Since $N \cap M = \{1\}$ we deduce $N \cap M_G = \{1\}$, hence $M_G \leq C_G(N)$. Since M complements $C_G(N)$, we deduce that $M_G = \{1\}$. We claim that M is a maximal subgroup of G. Assume that $M \leq S < G$. Then $S \cap N \trianglelefteq S$ and $S \cap N$ is normalized by $C_G(N)$, therefore $S \cap N \trianglelefteq C_G(N)S \geq C_G(N)M = G$, therefore $S \cap N \trianglelefteq G$. Since N is a minimal normal subgroup of G not contained in S, we deduce that $S \cap N = \{1\}$. Therefore

$$M \cong M/M \cap N \cong MN/N = G/N = SN/N \cong S/S \cap N \cong S$$

hence $|M| = |S|$. Since M and S are finite and $M \leq S$, this implies that $M = S$. This proves that M is a core-free maximal subgroup of G, so G is primitive and therefore G is primitive of type III being N a nonabelian minimal normal subgroup of G with nontrivial centralizer $C_G(N) \neq N$. □

Note that if $G \leq \mathrm{Sym}(\Omega)$ is primitive of type III then both minimal normal subgroups A, B of G act regularly on Ω, in particular $|A| = |B| = |\Omega|$. Indeed, the fact that G is transitive and $AM = G = BM$ imply that A and B act transitively, and we have seen that the centralizer of a transitive normal subgroup is semiregular, hence $A = C_G(B)$ and $B = C_G(A)$ are regular.

In particular, primitive groups of type I and III admit precisely one primitivity degree, which equals the order of one of their minimal normal subgroups.

Let X be a primitive group of type II with socle L. Then

$$G := \{(x, y) \in X \times X \; : \; xL = yL\}$$

is a primitive group of type III. This follows from the above proposition: $L \times \{1\}$ is a minimal normal subgroup of G and the subgroup $M := \{(x, x) \; : \; x \in X\} < G$ complements both $L \times \{1\}$ and $C_G(L \times \{1\}) = \{1\} \times L$.

Exercise 9.16. *Let S be a nonabelian simple group. Prove that S has at least 2 primitivity degrees.*

Exercise 9.17. *Let X be an almost-simple group. Prove that $X \times X$ is primitive if and only if X is simple.*

9.3   Primitive actions: O'Nan-Scott

See also [1, General remarks and notation 1.1.40], [6, Chapter 4], [17, Pages 26, 27] and [15, Chapter 7]. The notation for this section is the same as in [1].

We want to study the primitive actions of a primitive group. This amounts to studying the point stabilizers, in other words, we want to study the core-free maximal subgroups of a given primitive group and their indeces, which are precisely the primitivity degrees of G. Note that a group G may have several primitivity degrees, for example the simple group A_5 has maximal subgroups of index 5 (the point stabilizers) and maximal subgroups of index 6 (the Sylow 5-subgroup normalizers).

Another example is given by the symmetric group S_n acting naturally on the set Ω consisting of subsets of $\{1, \ldots, n\}$ of size k, where k is a fixed number with $1 \leq k < n$. This action is clearly faithful and transitive of degree $|\Omega| = \binom{n}{k}$. The point stabilizers are precisely the maximal intransitive subgroups $S_k \times S_{n-k}$, therefore such action is primitive if $k \neq n/2$.

Before stating the O'Nan-Scott theorem, we need to talk about the product action. Consider the wreath product $G = S_n \wr S_m$. We have seen that it admits a faithful imprimitive action of degree nm. Consider now the product action of G, that is, the action of G on $\{1, \ldots, n\}^m$ given by

$$(a_1, \ldots, a_m)^{(\sigma_1, \ldots, \sigma_m)\pi} := (a_{1\pi^{-1}}\sigma_{1\pi^{-1}}, \ldots, a_{m\pi^{-1}}\sigma_{m\pi^{-1}}).$$

It is clear that this is a faithful transitive action. Moreover the stabilizer of $(i, i, \ldots, i)$ is isomorphic to $S_{n-1} \wr S_m$.

For the following observe that if A, B are subgroups of G such that AB is a subgroup of G then $|AB : A| = |B : A \cap B|$.

Lemma 9.18. *Assume that $n \geq 5$ and let S_n act naturally on $\Gamma := \{1, \ldots, n\}$. Then the product action of $G = S_n \wr S_m$ on Γ^m is primitive.*

Proof. Since $n \geq 5$, Proposition 9.14 implies that G is a primitive group of type II. We are left to show that $M := S_{n-1} \wr S_m$ is a core-free maximal subgroup of G. It is clearly core-free because A_n^m is the unique minimal normal subgroup of G and M does not contain it. We need to show that M is a maximal subgroup of G.

Let $K := (S_{n-1})^m \leq B := (S_n)^m$. We claim that $M = N_G(K)$. The inclusion $M \leq N_G(K)$ is clear since $K \trianglelefteq M$. Now

$$B \cap N_G(K) = N_B(K) = N_{S_n^m}(S_{n-1}^m) = (N_{S_n}(S_{n-1}))^m = S_{n-1}^m = K,$$

since S_{n-1} is maximal and not normal in S_n. It is clear that the permutational factor S_m is contained in $N_G(K)$, therefore $G = BS_m \leq B \cdot N_G(K)$ hence $G = B \cdot N_G(K)$. Therefore

$$|G : N_G(K)| = |B \cdot N_G(K) : N_G(K)| = |B : B \cap N_G(K)|$$
$$= |B : K| = |B : M \cap B| = |BM : M| = |G : M|.$$

Since $M \leq N_G(K)$, it follows that $M = N_G(K)$.

Let H be a maximal subgroup of G containing M. We claim that $H = M$. This follows if we can show that $H \cap B = K$. Indeed, assuming $H \cap B = K$, since $H \cap B \trianglelefteq H$ we have that that $H \leq N_G(H \cap B) = N_G(K)$ and $N_G(K) \neq G$ being K not normal in G. Since H is maximal in G, we deduce that $H = N_G(H \cap B) = N_G(K) = M$. Therefore it is enough to show that $H \cap B = K$. The inclusion $H \cap B \supseteq K$ is clear.

We are left to prove that $K \subseteq H \cap B$. Write $B = B_1 \times \ldots \times B_m$ and

$$R_i = \{1\} \times \ldots \times \{1\} \times B_i \times \{1\} \times \ldots \times \{1\}$$

for $i \in \{1, \ldots, m\}$. G acts transitively on $\Gamma = \{R_1, \ldots, R_m\}$ by conjugation with kernel equal to B. Since $H \geq M$ and $G = BM$, we have $G = BH$, hence H acts transitively on Γ. Let $\pi_i : B \to R_i$ be the canonical projections, $i \in \{1, \ldots, m\}$. Fix $i, j \in \{1, \ldots, m\}$ and let $h \in H$ be such that $R_i^h = R_j$. Composing the conjugation by h, $\gamma_h : H \cap B \to H \cap B$, with the canonical projection we find a surjective homomorphism

$$H \cap B \xrightarrow{\gamma_h} H \cap B \xrightarrow{\pi_j|_{H \cap B}} \pi_j(H \cap B)$$

whose kernel is $\ker(\pi_i|_{H \cap B})$. The isomorphism theorem implies that $\pi_i(H \cap B) \cong \pi_j(H \cap B)$.

Since $\pi_i(K) \cong S_{n-1}$ is a maximal subgroup of $B_i \cong S_n$ and $K \leq H \cap B$, we have $\pi_i(K) \leq \pi_i(H \cap B) \leq B_i$ therefore either $\pi_i(H \cap B) = \pi_i(K)$ or $\pi_i(H \cap B) = B_i$. In the first case

$$|H \cap B| \leq \prod_{i=1}^{m} |\pi_i(H \cap B)| = \prod_{i=1}^{m} |\pi_i(K)| = (n-1)!^m = |K|$$

hence $H \cap B = K$ being $H \cap B \geq K$.

Now assume that $\pi_i(H \cap B) = B_i$ for all $i \in \{1, \ldots, m\}$.

Let $i \in \{1, \ldots, m\}$. We claim that $H \cap R_i \trianglelefteq R_i$. If $y \in H \cap R_i$ then $\pi_j(y) = 1$ for every $j \neq i$. If $r \in R_i$ then, being $\pi_i(H \cap B) = B_i$, there exists $x \in H \cap B$ such that $\pi_i(x) = \pi_i(r)$. Since x, y, r are m-tuples and $y \in R_i$, the fact that $\pi_i(x) = r$ implies that $r^{-1}yr = x^{-1}yx \in H$. This proves the claim.

But since $H \cap R_i$ contains $K \cap R_i \cong S_{n-1}$, $H \cap R_i$ is nontrivial and it is not the alternating group A_n, hence $H \cap R_i = R_i$, in other words $R_i \leq H$. This holds for every $i \in \{1, \ldots, m\}$, hence $B \leq H$. This contradicts the fact that $H \neq HB = G$. The proof is completed. $\qquad\square$

We are now ready to state the O'Nan-Scott theorem. The following formulation is taken from [17].

Theorem 9.19 (O'Nan-Scott theorem)**.** *If G is any proper subgroup of S_n, other than A_n, then G is a subgroup of one or more of the following subgroups.*

1. *An intransitive group $S_k \times S_m$ where $n = k + m$.*

2. *An imprimitive group $S_k \wr S_m$ where $n = km$.*

3. *A primitive wreath product $S_k \wr S_m$ where $n = k^m$.*

4. *An affine group $\mathrm{AGL}_d(p) = \mathbb{F}_p^d \rtimes \mathrm{GL}_d(\mathbb{F}_p)$ where $n = p^d$.*

5. *A group of shape $T^m.(\mathrm{Out}(T) \times S_m)$ where T is a non-abelian simple group, acting on the cosets of a subgroup $\mathrm{Aut}(T) \times S_m$, where $n = |T|^{m-1}$.*

6. *An almost-simple group acting on the cosets of a core-free maximal subgroup of index n.*

Note that this theorem does not say that the groups listed are maximal in S_n. But certainly every maximal subgroup of S_n is of one of the types listed.

9.4   Proof of the O'Nan-Scott theorem

This proof follows the line of [17], [1] and [9]. Set $\Omega := \{1, \ldots, n\}$, let $\alpha \in \Omega$ and let U be the stabilizer of α in G. We know that U is a core-free maximal subgroup of G.

Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group with socle N and let U be the stabilizer of a point of Ω, which is a core-free maximal subgroup of G. Set $K := U \cap N$. Then $|G : U| = |UN : U| = |N : K|$. Moreover $K \trianglelefteq U$, so U

is contained in the normalizer $N_G(K)$. Since $K \trianglelefteq U$, we have $U \leq N_G(K)$, and since U is maximal in G, either $U = N_G(K)$ or $N_G(K) = G$. In the latter case $K \trianglelefteq G$, hence the fact that $U_G = \{1\}$ forces $K = \{1\}$. This implies that either $K = \{1\}$ or $U = N_G(K)$. We know that $K = \{1\}$ if G is primitive of type I or III, so we will discuss these cases first.

9.4.1 Primitive groups of type I

If G is primitive of type I then the socle N of G is abelian and it is the unique minimal normal subgroup of G, moreover N is complemented by U, in other words $G \cong N \rtimes U$. The action of U on $N = \mathbb{F}_p^d$ is $\mathbb{F}_p$-linear, faithful and irreducible, hence U is an irreducible subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$. This is the affine case. In this case, G can be embedded in $\mathrm{AGL}(\mathbb{F}_p^d)$ which is a primitive subgroup of S_{p^d} with point stabilizer $\mathrm{GL}_d(\mathbb{F}_p)$.

9.4.2 Primitive groups of type III

If G is primitive of type III then the socle of G is $N = A \times B$ where A, B are the two minimal normal subgroups of G, both nonabelian and $A \cong AB \cap U \cong B$. We know that U is a complement of both A and B, hence A and B act regularly on Ω. The isomorphism $A \cong AB \cap U \cong B$ is explicited as follows. For every $a \in A$, since G is a semidirect product $B \rtimes U$, there is a unique $b_a \in B$ such that $ab_a \in U$. The map $f : A \to B$, $a \mapsto b_a$ is a group isomorphism since $a_1 a_2 b_{a_1} b_{a_2} = a_1 b_{a_1} a_2 b_{a_2} \in U$ for every $a_1, a_2 \in A$ and the inverse $f^{-1} : B \to A$ sends $b \in B$ to the unique $a_b \in A$ such that $a_b b \in U$. We can define an element $\sigma \in \mathrm{Sym}(\Omega)$ as follows. Fix $\omega \in \Omega$. Every element of Ω can be uniquely written as ωa where $a \in A$. Define $(\omega a)\sigma := \omega(af)$. We claim that $af = \sigma^{-1} a \sigma$ for all $a \in A$, proving that $B = \sigma^{-1} A \sigma$. Indeed, if $x \in \Omega$, then we can write $x = \omega(a^* f)$ for a unique $a^* \in A$ and, if $a \in A$,

$$x\sigma^{-1} a\sigma = (\omega(a^* f))\sigma^{-1} a\sigma = (\omega a^*)\sigma\sigma^{-1} a\sigma = (\omega a^* a)\sigma$$
$$= \omega((a^* a)f) = \omega(a^* f)(af) = x(af).$$

Therefore A and B are conjugate in $\mathrm{Sym}(\Omega)$ via σ, hence G is properly contained in $\langle G, \sigma \rangle \leq \mathrm{Sym}(\Omega)$ since A is normal in G but it is not normalized by σ. Moreover $B^\sigma = C_G(A)^\sigma = C_G(A^\sigma) = C_G(B) = A$, hence σ normalizes $A \times B$, in other words $A \times B$ is normal in $\langle G, \sigma \rangle$. This implies that $\langle G, \sigma \rangle$ is not equal to $\mathrm{Sym}(\Omega)$, since the only proper nontrivial normal subgroup of $\mathrm{Sym}(\Omega)$ is $\mathrm{Alt}(\Omega)$ and $\mathrm{Alt}(\Omega)$ is not a direct product of two nontrivial subgroups. This implies that the primitive groups of type III are not maximal in $\mathrm{Sym}(\Omega)$ hence we may ignore them.

9.4.3   Primitive groups of type II

Assume now G is primitive of type II with nonabelian socle $N = T^m = T_1 \times \ldots \times T_m$. Set $H := N_G(T_1)$, $C := C_G(T_1)$. We know that $X := H/C$ is an almost-simple group with socle isomorphic to T_1 and G embeds in the wreath product $X \wr K$, where $K \leq S_m$ is the transitive group induced by the action of G on the m direct factors of N. If $m = 1$ then $T_1 = N \trianglelefteq G$, $H = G$ and $C = C_G(N) = \{1\}$, therefore $G \cong X$ is almost-simple and we are in case (6) of the theorem. Assume now that $m > 1$. A subgroup of G is called U-invariant if its normalizer in G contains U. For example, since $U \cap N$ is normal in U, it is U-invariant.

Lemma 9.20. *$U \cap N$ is a maximal proper U-invariant subgroup of N.*

Proof. It is clear that $U \cap N$ is a proper U-invariant subgroup of N. Now assume by contradiction that $U \cap N < L < N$ where L is U-invariant. In particular LU is a subgroup of G. We claim that $U < LU < G$, contradicting the maximality of U. Indeed, if $U = LU$ then $L \leq U$, a contradiction, and if $LU = G$ then $L \trianglelefteq G$ contradicting the fact that N is a minimal normal subgroup of G. $\qquad\square$

We want to show that we are in one of the following cases.

- *Twisted wreath product type.* This case is defined by the fact that $U \cap N = \{1\}$, in other words G is a semidirect product $N \rtimes U$. The corresponding primitivity degree is $|N|$.

- *Product type.* U is a conjugate of $N_G(R^m)$ where R is a proper nontrivial subgroup of T, which is the intersection between T and a core-free maximal subgroup of X. The corresponding primitivity degree is $|T : R|^m$.

- *Simple diagonal type.* $U = N_G(\Delta)$ where Δ is a diagonal subgroup of T^m, that is, a subgroup of the form

$$\{(x, x^{\phi_2}, \ldots, x^{\phi_m}) \ : \ x \in T\} \leq N = T^m,$$

  where $\phi_2, \ldots, \phi_m$ are automorphisms of T. The corresponding primitivity degree is $|T|^{m-1}$.

- *Diagonal type in product action.* $U = N_G(\Delta_1 \times \ldots \times \Delta_l)$ where l divides m, $l > 1$, $lk = m$ and each $\Delta_i \cong T$ is a diagonal subgroup of T^k. The corresponding primitivity degree is $|T|^{l(k-1)}$.

Call $\pi_1, \ldots, \pi_m$ the projections $\pi_i : T^m = T_1 \times \ldots \times T_m \to T_i$. Observe that since N is a minimal normal subgroup of G and the normalizer $N_G(U \cap N)$ is a subgroup of G containing U, either U complements N

in G or $N_G(U \cap N) = U$. Define $U_i := \pi_i(U \cap N)$ for $i = 1, \ldots, m$. The same argument used in the proof of Lemma 9.18 shows that $U_i \cong U_j$ for every $i, j \in \{1, \ldots, m\}$. If $U_1 \neq T_1$ then, since $U \cap N$ is contained in $U_1 \times \ldots \times U_m$ and the latter is a proper U-invariant subgroup of N, Lemma 9.20 implies that $U \cap N = U_1 \times \ldots \times U_m$.

There are three possibilities for U_1. In the following discussion we will use Proposition 9.14.

Case 1. $U_1 = \{1\}$.

This implies that $U_i = \{1\}$ for every i, so $U \cap N = \{1\}$. In other words U complements N, so $G = N \rtimes U$ and the primitivity degree is $n = |N| = |T|^m$. This is the so-called twisted wreath product type. We know that G embeds in $X \wr S_m$ where $X = N_G(T_1)/C_G(T_1)$ is almost-simple with socle isomorphic to T, in particular X embeds in $\mathrm{Aut}(T) \leq \mathrm{Sym}(T)$. Setting $k = |T| = |T_1 : U_1|$, we obtain that G embeds in $S_k \wr S_m$ with product action of degree $n = k^m$.

Case 2. $\{1\} < U_1 < T_1$.

This implies that $\{1\} < U_i < T_i$ for every i. Since $U \cap N = U_1 \times \ldots \times U_m$ and the U_i are pairwise isomorphic, the degree of the primitive action of G is

$$n = |G : U| = |UN : U| = |N : U \cap N| = |T^m : U_1 \times \ldots \times U_m| = |T_1 : U_1|^m.$$

Let $H := N_G(T_1)$, $V := H \cap U = N_U(T_1)$ and $C := C_G(T_1)$.

We claim that U_1 is a maximal proper V-invariant subgroup of T_1. Assume by contradiction that $U_1 < R < T_1$ and R is V-invariant. Since $UN = G$, the group U acts transitively on the m factors of N, hence for each $i \in \{1, \ldots, m\}$ there exists $u_i \in U$ such that $T_1^{u_i} = T_i$. Set $\widetilde{R} := R \times R^{u_2} \times \ldots \times R^{u_m}$. Note that $U_1 = (U \cap N) \cap T_1 = U \cap T_1$ hence

$$U_1^{u_i} = (U \cap T_1)^{u_i} = U \cap T_1^{u_i} = U \cap T_i = (U \cap N) \cap T_i = U_i.$$

Therefore $U_i = U_1^{u_i} < R^{u_i}$. This implies that $U \cap N$ is properly contained in $\widetilde{R}$. Since $U \cap N$ is a maximal proper U-invariant subgroup of N, in order to obtain a contradiction it is enough to prove that $\widetilde{R}$ is U-invariant. Let $x \in U$. Fix $i \in \{1, \ldots, m\}$ and let j be such that $T_i^x = T_j$. Then $R^{u_i x} \leq T_j = T_1^{u_j}$, therefore $R^{u_i x u_j^{-1}} \leq T_1$. On the other hand $u_i x u_j^{-1}$ belongs to U and normalizes T_1, therefore it belongs to $H \cap T_1 = V$. Since R is V-invariant, we deduce that $R^{u_i x u_j^{-1}} = R$, in other words $R^{u_i x} = R^{u_j}$. This implies that $\widetilde{R}^x = \widetilde{R}$. This holds for every $x \in U$, hence $\widetilde{R}$ is U-invariant.

We have $VCT_1 = H$, since

$$H \supseteq VCT_1 \supseteq VN = (H \cap U)N = H \cap UN = H \cap G = H.$$

This implies that VC/C is a core-free subgroup of $X = H/C$. Indeed, since X is almost-simple, its unique minimal normal subgroup is T_1C/C and this is supplemented by VC/C since $VCT_1 = H$.

We claim that VC is a maximal subgroup of H, which implies that VC/C is a core-free maximal subgroup of the almost-simple group $X = H/C$, therefore X is a primitive group of degree $|X : VC/C|$. First, note that $VC \neq H$ because if this is not the case then $T_1 \leq H = VC = CV$, therefore, being $U_1 \neq \{1\}$, and being T_1 a simple group, we have

$$T_1 = \langle U_1^{T_1} \rangle \leq \langle U_1^{CV} \rangle = \langle U_1^V \rangle \leq U,$$

a contradiction. Assume the group M is such that $VC \leq M < H$, then $M \cap T_1$ is a V-invariant subgroup of T_1 and $U_1 \leq M \cap T_1$. If $T_1 \leq M$ then $H = VCT_1 \leq M$ and $H = M$, contradicting our assumption. Hence $U_1 \leq M \cap T_1 \neq T_1$. By maximality of U_1 as proper V-invariant subgroup of T_1, we deduce that $U_1 = M \cap T_1$, hence

$$M = M \cap H = M \cap VCT_1 = VC(M \cap T_1) = VCU_1 = VC,$$

being $U_1 \leq V$. This proves the claim.

Since $U_1 \leq VC \cap T_1 < T_1$, U_1 is a maximal proper V-invariant subgroup of T_1 and $VC \cap T_1$ is V-invariant, we deduce that equality holds: $U_1 = VC \cap T_1$. Since $H = VCT_1$, we have

$$|H/C : VC/C| = |H : VC| = |VCT_1 : VC| = |T_1 : VC \cap T_1| = |T_1 : U_1|.$$

We deduce that $X = H/C$ is primitive of degree $k = |T_1 : U_1|$ with point stabilizer VC/C, hence X embeds into S_k. Moreover, U_1C/C equals the intersection between T_1C/C and the core-free maximal subgroup VC/C of H/C. Indeed, it is clear that $U_1C/C \leq T_1C/C \cap VC/C$, however, using that $H = VCT_1$, we have

$$|T_1C/C \cap VC/C| = \frac{|T_1C/C| \cdot |VC/C|}{|H/C|} = \frac{|T_1| \cdot |VC|}{|H|}$$
$$= |T_1 \cap VC| = |U_1| = |U_1C/C|.$$

Now, G embeds into $X \wr K$ where K is a transitive subgroup of S_m and X embeds into S_k, therefore G embeds into $S_k \wr S_m$ and looking at the point stabilizers we deduce that the action of G is equivalent to the product action of degree $k^m = n$ induced by $S_k \wr S_m$ on $\{1, \ldots, k\}^m$.

Case 3. $U_1 = T_1$.

This implies that $U_i = T_i$ for every i. For $x = (t_1, \ldots, t_m) \in N$, let the support of x be the set

$$\mathrm{supp}(x) := \{i \in \{1, \ldots, m\} \ : \ t_i \neq 1\} \subseteq \{1, \ldots, m\}.$$

Let Ω_1 be a minimal nonempty subset of $\{1, \ldots, m\}$ such that $U \cap N$ contains an element whose support is Ω_1. Let

$$A := A_{\Omega_1} = \{x \in U \cap N \ : \ \mathrm{supp}(x) \subseteq \Omega_1\}.$$

By minimality of Ω_1, if $x \in A$ and $x \neq 1$ then $\mathrm{supp}(x) = \Omega_1$. Moreover, it is clear that A is a normal subgroup of $U \cap N$.

Fix $i \in \Omega_1$. We claim that for every $s \in T$ there exists a unique $g_{s,i} \in A$ such that $\pi_i(g_{s,i}) = s$ and that the map $f_i : T \to A$ defined by $f_i(s) := g_{s,i}$ is a group isomorphism whose inverse is $\pi_i|_A$. The uniqueness follows from the fact that if $g \in A$ is such that $\pi_i(g) = s$ then the element $gg_{s,i}^{-1}$ belongs to A and $\pi_i(gg_{s,i}^{-1}) = 1$, hence $gg_{s,i}^{-1} = 1$ by minimality of Ω_1. To prove the existence, we need to prove that $\pi_i(A) = T_i$. Let $L_i := \pi_i(A) \leq T_i$. Then $L_i \neq \{1\}$ by definition of Ω_1. Since T_i is a simple group, to show that $L_i = T_i$ it is enough to show that L_i is normal in T_i. If $t \in T_i$ then, since $U_i = T_i$, there exists $u \in U \cap N$ with $\pi_i(u) = t$. If $x \in A$ then, since $u \in N$, x and x^u have the same support, hence $x^u \in A$. This implies that $\pi_i(x^u) \in L_i$ and this exactly says that $t^{-1}\pi_i(x)t \in L_i$. Now we prove that f_i is a group isomorphism. If $g \in A$ then, letting $s := \pi_i(g)$, it is clear that $f_i(s) = g$, this proves that f_i is surjective. If $s, t \in T$ are such that $f_i(s) = f_i(t)$ then applying π_i we find $s = t$, this proves injectivity. Since $\pi_i(g_{1,i}) = \pi_i(1) = 1$, it follows that $f_i(1) = g_{1,i} = 1$. If $s, t \in T$ then $\pi_i(g_{s,i}g_{t,i}) = \pi_i(g_{st,i}) = st$, it follows that $f_i(st) = f_i(s)f_i(t)$.

We deduce that A is a diagonal subgroup of T^{Ω_1}: indeed, setting $k := |\Omega_1|$,

$$A = \{(s, \phi_2(s), \ldots, \phi_k(s)) \ : \ s \in T\} \leq T^{\Omega_1},$$

where $\phi_i = \pi_i|_A \circ f_1 \in \mathrm{Aut}(T)$ for $i = 1, \ldots, k$.

The natural action of G on the m direct factors of N gives an action of G on $\{1, \ldots, m\}$. We claim that Ω_1 is an imprimitivity block for this action. Assume Ω_1 is the support of some $x \in U \cap N$. If $g = nu \in G$ with $n \in N$, $u \in U$, then $\Omega_2 := \Omega_1^g = \Omega_1^u$ is the support of $y := x^u \in U \cap N$. Assume $\Omega_1 \cap \Omega_2 \neq \varnothing$. We claim that $\Omega_1 = \Omega_2$. Let $i \in \Omega_1 \cap \Omega_2$, so that $\pi_i(x) \neq 1 \neq \pi_i(y)$. Since T_i is simple, the conjugacy class of $\pi_i(x)$ in T_i generates T_i and $Z(T_i) = \{1\}$. Since $\pi_i(y) \neq 1$ there exists $t \in T_i$ such that $\pi_i(x)^t$ does not commute with $\pi_i(y)$. Since $U_i = T_i$, there exists $v \in U \cap N$ such that $\pi_i(v) = t$, therefore $\pi_i(x^v) = \pi_i(x)^t$. Moreover $\mathrm{supp}(x^v) = \mathrm{supp}(x) = \Omega_1$ and $\pi_i(x^v) \neq 1$ being $\pi_i(x) \neq 1$. Up to replacing x with x^v, we may assume that $\pi_i(x)$ and $\pi_i(y)$ do not commute. If $j \in \Omega_1 - \Omega_2$ then $\pi_j(x) \neq 1$, $\pi_j(y) = 1$, and if $j \in \Omega_2 - \Omega_1$ then $\pi_j(x) = 1$, $\pi_j(y) \neq 1$, therefore $\pi_j([x,y]) = 1$ unless possibly if $j \in \Omega_1 \cap \Omega_2$, where $[x,y] := x^{-1}y^{-1}xy \in U \cap N$. This says that $\mathrm{supp}([x,y]) \subseteq \Omega_1 \cap \Omega_2$, therefore $\Omega_1 = \Omega_1 \cap \Omega_2$ by minimality of Ω_1, in other words $\Omega_1 \subseteq \Omega_2$. Since $\Omega_2 = \Omega_1^u$, $|\Omega_1| = |\Omega_2|$, hence $\Omega_1 = \Omega_2$.

We claim that $|\Omega_1| \neq 1$. If Ω_1 has size 1, say $\Omega_1 = \{i\}$, then there exists an element $x \in U \cap N$ such that $\pi_i(x) \neq 1$ and $\pi_j(x) = 1$ for every $j \neq i$. Since $U_i = T_i$, for every $t \in T_i$ there exists $u \in U \cap N$ with $\pi_i(u) = t$, hence $U \cap N$ contains the whole conjugacy class of x, so it contains the i-th factor, being T a simple group. Since U acts transitively on the factors, U

contains N, a contradiction.

Assume the block system consists of l blocks $\Omega_1, \ldots, \Omega_l$, each of size $k > 1$. We have $N = T^{kl}$. We may consider the normal subgroups $A_{\Omega_j} \trianglelefteq U \cap N$, $j = 1, \ldots, l$, defined in the same way as for A_{Ω_1} above. Note that the group they generate is a direct product $A_{\Omega_1} \times \ldots \times A_{\Omega_l} \cong T^l$. Moreover this product equals $U \cap N$. To prove this, fix $g \in U \cap N$ and, for every $j \in \{1, \ldots, l\}$, let $x_j \in A_{\Omega_j}$ be such that there exists $i = i(j) \in \Omega_j$ with the property that $\pi_i(g) = \pi_i(x_j)$. We claim that $g = x_1 \ldots x_l$. We need to show that $\pi_r(g) = \pi_r(x_1 \ldots x_l)$ for all $r = 1, \ldots, m = kl$. Fix $r \in \{1, \ldots, m\}$ and let $j \in \{1, \ldots, l\}$ be such that $r \in \Omega_j$. By definition of x_j, there exists $i \in \Omega_j$ with $\pi_i(g) = \pi_i(x_j)$, in other words $\pi_i(h) = 1$ where $h = g^{-1} x_j \in U \cap N$. If x is any element of A_{Ω_j} then $\pi_i(h^{-1} x h) = \pi_i(x)$, therefore $h^{-1} x h = x$ being $A_{\Omega_j} \trianglelefteq U \cap N$ and being the restriction $\pi_i|_{A_{\Omega_j}} : A_{\Omega_j} \to T$ injective. This implies that $h \in C_{U \cap N}(A_{\Omega_j})$, therefore $\pi_r(h) = 1$, hence $\pi_r(g) = \pi_r(x_j) = \pi_r(x_1 \ldots x_l)$.

We deduce that $U \cap N = A_{\Omega_1} \times \ldots \times A_{\Omega_l}$, in particular $U \cap N \cong T^l$. Therefore

$$n = |G : U| = |UN : U| = |N : U \cap N| = |T|^{(k-1)l}.$$

Now consider

$$Y := T^{\Omega_1} = \prod_{i \in \Omega_1} T_i, \quad H := N_G(Y), \quad \xi : H \to \mathrm{Aut}(Y), \quad C := \ker(\xi) = C_G(Y).$$

Observe that H is precisely the setwise stabilizer of the block Ω_1, in particular H acts transitively on Ω_1 (see the proof of Proposition 5.2), therefore YC/C is a minimal normal subgroup of H/C.

Let $A := A_{\Omega_1}$, $V := U \cap H$. Note that since Y is a direct power of a nonabelian simple group and A is a full diagonal subgroup of Y, we have $\langle A^Y \rangle = Y$. Now, the argument used in the proof of the case $1 < U_1 < T_1$ with U_1 replaced by A, T_1 replaced by Y proves that $VCY = H$, $Y \cap VC = A$, YC/C is the unique minimal normal subgroup of H/C and $\xi(H) \cong H/C$ is a primitive group of type II with point stabilizer the core-free maximal subgroup VC/C. Moreover $VC/C \cap YC/C = AC/C \cong A$, therefore H/C is a primitive group of simple diagonal type. Now an application of the embedding argument gives that G lies inside a wreath product $H/C \wr S_l \leq S_r \wr S_l$ where $r = |T|^{k-1}$ and we are in case (3) of the theorem.

Now assume there is only one block, $l = 1$. Then $m = k > 1$ and $U \cap N \cong S$, $N \cong T^m$. In this case $n = |T|^{m-1}$. Without loss of generality, $\Delta := U \cap N = \{(s, \ldots, s) : s \in T\}$. G is a subgroup of $X \wr S_m$ and $U = N_G(\Delta)$. Note that $(x_1, \ldots, x_m)\pi \in X \wr S_m$ normalizes Δ if and only if

$$(s, \ldots, s)^{(x_1, \ldots, x_m)\pi} \in \Delta \qquad \forall s \in T,$$

and this means $s^{x_1} = \ldots = s^{x_m}$ for all $s \in T$. This implies that $s^{x_i x_j^{-1}} = s$ for all $s \in T$ and for all $i, j \in \{1, \ldots, m\}$ and, since the x_i are automorphisms of T, we deduce the necessary and sufficient condition $x_1 = \ldots = x_m$. This implies that

$$U = N_G(\Delta) \leq \{(a, a, \ldots, a)\pi \; : \; a \in \operatorname{Aut}(T), \; \pi \in S_m\} \cong \operatorname{Aut}(T) \times S_m$$

hence $G = N \cdot N_G(\Delta)$ is contained in the group

$$\{(a_1, \ldots, a_m)\pi \in \operatorname{Aut}(T) \wr S_m \; : \; a_i \equiv a_j \mod \operatorname{Inn}(T) \; \forall i, j\},$$

which is an extension $T^m.(\operatorname{Out}(T) \times S_m)$ with point stabilizer isomorphic to $\operatorname{Aut}(T) \times S_m$. We are in case (5) of the theorem, the simple diagonal type. $\qquad \square$

One should be careful about going "backwards" in this reasoning: for example, if G is a primitive group of type II with socle N and Δ is a diagonal subgroup of N, the normalizer $N_G(\Delta)$ does not need to be a core-free maximal subgroup of G.

Exercise 9.21. *Why is 60^2 not a primitivity degree for $A_5 \wr S_2$? Why is 60 not a primitivity degree for $S_5 \wr S_2$?*

Chapter 10

Not only symmetric groups

Many properties of a group can be detected by looking at primitive quotients. Here we use the abstract definition of primitive group: a finite group G is called primitive if it admits a core-free maximal subgroup. Observe that if G is any finite group and M is a maximal subgroup of G then G/M_G is a primitive group, since the normal core of M/M_G in G/M_G is $(M/M_G)_{G/M_G} = M_G/M_G$.

Let $\Phi(G)$ denote the Frattini subgroup of G, that is, the intersection of the maximal subgroups of G. The well-known Frattini argument implies that the Frattini subgroup of any finite group is nilpotent.

Recall that a chief factor of a group G is a quotient H/K where $K \trianglelefteq G$ and H/K is a minimal normal subgroup of G/K. The chief factor H/K is called central if $H/K \leq Z(G/K)$, it is called Frattini if $H/K \leq \Phi(G/K)$, it is called non-Frattini if $H/K \not\leq \Phi(G/K)$. A chief factor H/K is non-Frattini if and only if it admits a supplement in G, that is, there exists $M/K < G/K$ such that $HM = G$. If H/K is an abelian chief factor of G then it is non-Frattini if and only if it is complemented.

Let G be a finite group. Then we have the following: G is nilpotent if and only if every non-Frattini chief factor is central, G is supersolvable if and only if every non-Frattini chief factor has prime order, G is solvable if and only if every non-Frattini chief factor is abelian. Other properties that can be detected similarly looking at chief factors are p-solvability, p-supersolvability, p-nilpotency, where p is a prime number.

A subdirect product of a family of groups $\{X_1, \ldots, X_n\}$ is a subgroup H of $X_1 \times \ldots \times X_n$ such that the restrictions to H of the projections $\pi_i : X \to X_i$ are surjective. Observe that if $\mathcal{N}$ is a family of normal subgroups of G with trivial intersection then the canonical map $G \to \prod_{N \in \mathcal{N}} G/N$ is injective hence G is a subdirect product of the family $\{G/N \; : \; N \in \mathcal{N}\}$

and every chief factor of G is G-isomorphic to a chief factor of some G/N where $N \in \mathcal{N}$.

Recall that two groups A, B on which G acts are said to be G-isomorphic, notation $A \cong_G B$, if there is an isomorphism $A \to B$ compatible with the action of G. For example if A and B are normal subgroups of G and G acts on A and B by conjugation then endowing $A/A \cap B$ with the canonical conjugation action of G, we have $AB/B \cong_G A/A \cap B$. Since G acts by conjugation on every chief factor of G, it makes sense to talk about G-isomorphic chief factors.

Proposition 10.1. *Let G be a finite group. Then we have the following.*

1. *If H/K is a non-Frattini chief factor of G then there exists a primitive quotient of G whose socle is G-isomorphic to H/K.*

2. *$G/\Phi(G)$ is a subdirect product of $\prod_{M \in \mathcal{M}} G/M_G$ where $\mathcal{M}$ is the family of maximal subgroups of G.*

3. *The prime divisors of $|G|$ are precisely the prime divisors of the orders of the primitive quotients of G.*

In particular, parts (1) and (2) imply that properties like solvability, nilpotency and supersolvability are recognizable looking at primitive quotients, in the sense that they are properties P such that G satisfies property P if and only if every primitive quotient of G satisfies property P. This is because, since $\Phi(G)$ is nilpotent, if P is any of these properties then G satisfies P if and only if $G/\Phi(G)$ does.

Proof of proposition 10.1. H/K has the type S^n where S is a simple group. If S is nonabelian then $G/C_G(H/K)$ is a primitive group of type II with socle G-isomorphic to H/K. If S is abelian then, since H/K is non-Frattini and abelian, there exists a complement T/K of H/K in G/K. Set $C/K := C_{T/K}(H/K)$. Then $C \unlhd G$ and G/C is a primitive group of type I with socle G-isomorphic to H/K.

Part (2). Since $\Phi(G)$ is the intersection of the maximal subgroups of G, it is also equal to the intersection of the normal cores of the maximal subgroups of G. Therefore the canonical map $G \to \prod_{M \in \mathcal{M}} G/M_G$ has kernel equal to $\Phi(G)$. The conclusion follows by the isomorphism theorem.

Part (3) follows from part (2) if we can show that every prime divisor of $|G|$ divides $|G/\Phi(G)|$. If there exists a prime divisor p of $|G|$ which does not divide $|G/\Phi(G)|$ then $\Phi(G)$ contains a Sylow p-subgroup P of G, and since $\Phi(G)$ is nilpotent and P is characteristic in $\Phi(G)$, P is normal in G, so by the Schur-Zassenhaus theorem P admits a complement H in G. Let M be a maximal subgroup of G containing H, then M does not contain P, so M does not contain $\Phi(G)$, a contradiction. $\square$

Bibliography

[1] Ballester-Bolinches A.; Ezquerro L. M.; Classes of Finite Groups; Springer, 2006.

[2] Blackburn S. R.; Sets of permutations that generate the symmetric group pairwise. J. Combin. Theory Ser. A, 113 (2006), no. 7, 1572–1581.

[3] Bochert, A.; Über die transitivitätsgrenze der Substitutionengruppen, welche die Alternierende ihres Grades nicht einhalten. Math. Ann. 33 (1889), 572–583.

[4] Cameron, P. J.; Permutation groups. London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999.

[5] Cameron, P. J.; Finite permutation groups and finite simple groups. Bull. London Math. Soc. 13 (1981), 1–22.

[6] Dixon, John D.; Mortimer, B.; Permutation groups. Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

[7] Isaacs M.; Finite Group Theory. American Mathematical Society, 2008.

[8] Liebeck, M. W.; On minimal degrees and base sizes of primitive permutation groups. Arch. Math. 43 (1984), 11–15.

[9] Liebeck M. W.; Praeger C. E.; Saxl, J.; On the O'Nan-Scott theorem for finite primitive permutation groups. J. Austral. Math. Soc. Ser. A 44 (1988), no. 3, 389–396.

[10] Liebeck M. W.; Praeger C. E.; Saxl J.; A classification of the maximal subgroups of the finite alternating and symmetric groups. Journal of Algebra 111 (1987), 365–383.

[11] Maróti, A.; On the orders of primitive groups. J. Algebra 258 (2002), no. 2, 631–640.

[12] Praeger, C.; Saxl J.; On the order of primitive permutation groups. Bull. London Math. Soc. 12 (1980), 303–308.

[13] Pyber, L; On the orders of doubly transitive permutation groups, elementary estimates. J. Comb. Theory (A) 62 (1993), 361–366.

[14] Rose J. S.; A course on group theory. Cambridge University Press, 1978.

[15] Schneider, C.; Praeger, C.; Permutation Groups and Cartesian Decompositions. London Mathematical Society Lecture Notes, 2018.

[16] Wielandt, H.; Finite Permutation Groups. 1964, Academic Press.

[17] Wilson, R.; The finite simple groups. 2009, Springer.

Martino Garonzi
Departamento de matemática
Universidade de Brasília
Campus Universitário Darcy Ribeiro
Brasília - DF, 70910–900, Brazil
martino@mat.unb.br