THE MAXIMAL SUBGROUPS OF THE SYMMETRIC GROUP

MARTINO GARONZI

Lecture notes of the Minicourse “The maximal subgroups of the symmetric group” given at the “Escola de Álgebra” in Unicamp (Campinas, São Paulo, Brazil) on December 3-7 2018. Version 1. I will improve the notes and release a more complete version in the future. I am grateful for any comment, criticism and correction.

Contents

1. Basic notions about group actions 1
2. The symmetric group 2
3. The maximal subgroups of $S_5$ 3
4. Imprimitivity blocks 4
5. Maximal imprimitive subgroups 5
6. Intransitive maximal subgroups 7
7. Primitive maximal subgroups 7
   7.1. Characteristically simple groups 7
   7.2. Primitive groups 8
   7.3. Multiple transitivity 10
   7.4. Jordan groups 11
   7.5. Primitive actions: O’Nan-Scott 13
References 15

1. Basic notions about group actions

All group actions we consider are on the right. $G$ acts on $X$ by the rule $(x, g) \mapsto xg$ if and only if the map $\gamma_g : X \to X$, $x \mapsto xg$ induces a homomorphism $G \to Sym(X)$, $g \mapsto \gamma_g$. The kernel of this homomorphism is the kernel of the action and the action is called faithful if it has trivial kernel. The orbits of the action are the sets $O(x) = \{xg : g \in G\}$ for any $x \in X$. The action is called transitive if there is some $x \in X$ such that $O(x) = X$ (i.e. there is only one orbit), in other words for any $x, y \in X$ there exists $g \in G$ with $xg = y$. The stabilizer of $x \in X$ is $G_x = \{g \in G : xg = x\} \leq G$.

For example consider the action by right multiplication of $G$ on $X = \{Ht : t \in G\}$, the kernel is $H_G = \bigcap_{g \in G} H^g$ where the notation is $H^g = g^{-1}Hg$. $H_G$ is called the normal core of $H$ in $G$.

Counting principle (Orbit-Stabilizer lemma): if $G$ acts transitively on $X$ and $x \in X$ then $|X| = |G : G_x|$. 

1
The action 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 $|G| = |X|$. An example of a regular action is that of the Klein 4-group acting naturally on $\{1, 2, 3, 4\}$. More in general if $G$ is a semidirect product $N \rtimes H$ 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 $G$ acting transitively 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 (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 the number of orbits is $|X|/|G|$ because $f_1 = |X|$ and $f_g = 0$ for every $1 \neq g \in G$. Therefore if the action is regular (semiregular and transitive) then $|G| = |X|$.

2. 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.

**Proposition 1.** If $H < S_n$ and $H \neq A_n$ then $|S_n : H| \geq n$. If $H < A_n$ then $|A_n : H| \geq n$.

**Proof.** Let $m = |S_n : H|$. $S_n$ acts transitively (hence non-trivially) by right multiplication on $X = \{Hx : x \in S_n\}$, 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 $K = \ker(\varphi)$. Since $H \neq A_n$ we have $m \geq 3$ so $|S_n : K| \geq 3$ (a transitive group on $m$ points has always order at least $m$). The case $n \leq 4$ can be done by hand, and we know that 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 $n \leq m$. A similar argument applies to show that if $H < A_n$ then $|A_n : H| \geq n$. \hfill $\Box$

We will now discuss the subgroups of $S_n$ of index $n$.

**Proposition 2.** If $n \neq 6$ then the unique subgroups of $S_n$ of index $n$ are the point stabilizers. Moreover $S_n$ has two conjugacy classes of subgroups of index 6.

**Proof.** We need to recall that if $x \in A_n$ then the conjugacy class of $x$ in $A_n$ is not equal to its conjugacy class in $S_n$ if and only if $x$ is the products of disjoint cycles of pairwise distinct odd lengths. So for example if $n \geq 5$ then all the 3-cycles are conjugated in $A_n$.

Let $H$ be a subgroup of $S_n$ of index $n$. First observe that $H \cong S_{n-1}$. Indeed $S_n$ acts faithfully on the set of the $n$ right cosets of $H$ by right multiplication and this gives $\varphi : S_n \to S_n$, however $\varphi(H)$ is contained in the stabilizer of $H$, which has
order \((n - 1)!\). It follows that \(H\) is a group of order \((n - 1)!\) isomorphic to \(\varphi(H)\) which is contained in a point stabilizer, that is isomorphic to \(S_{n-1}\). It follows that \(H \cong S_{n-1}\). Similarly any subgroup of \(A_n\) of index \(n\) is isomorphic to \(A_{n-1}\).

Now consider an isomorphism \(f : A_{n-1} \cong H < S_n\). The idea is to show that if \(x\) is a 3-cycle in \(A_{n-1}\) then \(\varphi(x)\) is also a 3-cycle \((x\) centralizes some \(A_{n-4}\) so \(K = \varphi(A_{n-4})\) is centralized by the element \(\varphi(x)\) of order 3 and has an orbit of size \(n - t \geq n - 4\) - it cannot act nontrivially on less than \(n - 4\) elements - now proceed to show that \(\varphi(x)\) must be a 3-cycle). Now show that \(\varphi((123)), \ldots \varphi((1, 2, n - 1))\) must be of the form \((abx)\) where the \(x\)'s are \(n - 3\) elements, pairwise distinct, and \(a, b\) are fixed, so they generate the stabilizer of the one element fixed by all of them (obs: if \(r, s \neq 1, 2\) then \(\varphi((12r)), \varphi((12s))\) are 3-cycles that generate some \(A_4\) so they are of the form \((abx), (aby)\) where \(a, b\) are fixed and \(x, y\) depend on \(r, s\)). Generalize this to \(S_n\).

\(S_5\) 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. \(\square\)

**Corollary 1.** If \(n \geq 3\) and \(n \neq 6\) then \(\text{Aut}(S_n) \cong S_n \cong \text{Aut}(A_n)\). Moreover \(A_6\) has index 4 in \(\text{Aut}(A_6)\).

**Proof.** The idea is that \(\text{Aut}(S_n)\) acts on the family of subgroups of \(S_n\) of index \(n\), which, being \(n \neq 6\), are all the \(n\) point stabilizers. This action is faithful, hence we get \(\text{Aut}(S_n) \to S_n\) injective. On the other hand being \(Z(S_n) = \{1\}\) the canonical “conjugation” homomorphism \(S_n \to \text{Aut}(S_n)\) is injective hence \(S_n \cong \leq \text{Aut}(S_n) \cong S_n\) implying \(\text{Aut}(S_n) \cong S_n\). The case \(n = 6\) is treated separately. \(\square\)

\begin{center}
\begin{tikzcd}
M_{10} \arrow[leftrightarrow]{r}
& \text{Aut}(A_6) \arrow[leftrightarrow]{r} & S_6 \arrow[leftrightarrow]{r}
& \text{PGL}_2(9) \arrow[leftrightarrow]{r}
& A_6
\end{tikzcd}
\end{center}

\(\text{Out}(A_6) = \text{Aut}(A_6)/A_6 \cong C_2 \times C_2\).

**Exercise:** let \(\sigma = (1 \ldots n) \in S_n\). The centralizer of \(\sigma\) in \(S_n\) is \(\langle \sigma \rangle\).

3. **The Maximal Subgroups of \(S_5\)**

Recall that the unique normal subgroups of \(S_n\) are \(\{1\}\), \(A_n\) and \(S_n\) except when \(n = 4\), in which case we have an additional normal subgroup, the Klein 4 group.

**Generalized Cayley theorem:** if \(G\) acts transitively on a set \(\Omega\) of size \(n\) with point stabilizer \(H\) then \(|G : H| = n\) (counting principle - orbit-stabilizer lemma), the action is equivalent to the right multiplication action of \(G\) on \(\{Hx : x \in G\}\) and setting \(H_G = \bigcap_{g \in G} H^g\) the normal core of \(H\) in \(G\), the quotient \(G/H_G\) is isomorphic to a subgroup of the symmetric group \(S_n\), in particular \(|G : H_G|\) divides...
any transitive group of prime degree is primitive (see for example our discussion of 

\[ \Omega \] being a block, and \( \omega \) is a block for every \( \omega \in \Omega \): these are called the trivial blocks. Also, \( \{ \omega \} \) is an example of block that, in general, is not an orbit. If \( B \) is a block then \( Bg \) is a block for all \( g \in G \) and the “translates” of \( B \) (the blocks \( Bg \)) form a partition of \( \Omega \), moreover \( |B| = |Bg| \) for all \( g \in G \) hence \( |B| \) divides \( |\Omega| \) and the partitions consists of \( |\Omega|/|B| \) blocks. Calling \( a = |B| \) and \( b = |\Omega|/|B| \) we obtain that if \( G \) acts transitively \( n = ab \), therefore we immediately deduce that any transitive group of prime degree is primitive (see for example our discussion of
Proof. Observe that if the point stabilizer $M$ is a prime. The point stabilizer is $\{\text{block system}\}$ and $G$ is said to be primitive if it does not admit any nontrivial block, and imprimitive otherwise. Observe that if $n > 2$ and $G$ is primitive then it is transitive because the $G$-orbits are blocks and $n > 2$ (observe that if $n = 2$ then all the subsets of $\{1, 2\}$ are blocks for $G$ independent of $G$).

**Easy example:** consider $\sigma = (123456)$ and $G = \langle \sigma \rangle < S_6$, as a permutation group of degree 6. Looking at $\sigma^2 = (135)(246)$ and $\sigma^3 = (14)(25)(36)$ we realize that the nontrivial imprimitivity blocks of $G$ are $\{1, 3, 5\}$, $\{2, 4, 6\}$ (which form one block system) and $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$ (which form another block system). This is how the cycle $(123456)$ acts on each non-trivial block system.

```
1 ---- 2
|     |
|     |
3 ---- 4
      |
      5---- 6
```

**Proposition 3.** Suppose $n > 2$ and $G$ acts transitively. $G$ is primitive if and only if the point stabilizer $M = G_\alpha$ (for any $\alpha \in \Omega$) is a maximal subgroup of $G$.

**Proof.** Observe that if $B$ is a block containing $\alpha$ then $G_B = \{g \in G : Bg = B\}$ (the setwise stabilizer of $B$) is a subgroup of $G$ containing $G_\alpha$. Indeed if $g \in G_\alpha$ then $\alpha \in B \cap Bg$ hence $B = Bg$ since $B$ is a block. This proves that if $G_\alpha$ is maximal then $G$ is primitive. Conversely if $M < K < G$ the set $B = \{Mk : k \in K\}$ is a nontrivial block for $G$. Indeed if $g \in G$ and $Mk \in B \cap Bg$ there is some $t \in K$ with $Mk = Mtg$ so $g \in t^{-1}Mk \subseteq K$ and this implies $Bg = B$. \qed

An easy example of a primitive group is $\langle (1 \ldots p) \rangle$ acting on $\{1, \ldots, p\}$ where $p$ is a prime. The point stabilizer is $\{1\}$.

**Exercise:** $G \leq S_n$ is called 2-transitive on $\Omega = \{1, \ldots, n\}$ if it is transitive and its point stabilizer has precisely two orbits on $\Omega$. Show that any 2-transitive group is primitive. Show that the converse does not hold (consider the dihedral group of prime degree $p$).

## 5. Maximal imprimitive subgroups

If $H$ and $K$ are two groups and $K \leq S_n$, then $H \wr K$ 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 $t_i^{-1} = x_{i\pi^{-1}}^{-1} = x_{i(\pi^{-1})^{-1}}$ hence

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

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

The following result is due to Frobenius.
Theorem 1. 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 $\xi$ be any homomorphism with domain $H$. Then the map $f : G \to \xi(H) \wr S_n$ given by

$$x \mapsto (\xi(x_1x_1^{-1}),\ldots,\xi(x_nx_n^{-1}))\pi,$$

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

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

$$f(xy) = (\xi(x_{i}y_{i}x_{i\tau}^{-1}))\pi\tau = (\xi(x_{i}x_{i}^{-1})\xi(x_{i}y_{i}x_{i\tau}^{-1}))\pi\tau = f(x) \cdot \pi^{-1}(\xi(x_{i}y_{i}x_{i\tau}^{-1}))\pi\tau = f(x)(\xi(x_{i}y_{i}x_{i\tau}^{-1}))\pi\tau = f(x)f(y).$$

$f(x) = 1$ if and only if the permutation $\pi$ corresponding to $x$ is the identity and $x_{i}x_{i}^{-1} \in \ker(\xi)$ for all $i = 1,\ldots,n$, in other words $x$ belongs to the normal core of $\ker(\xi)$ in $G$, because $x \in H_G$ and $\ker(\xi) \leq H$. \hfill \Box

Now assume $G \leq S_n$ acts imprimitively on $\Omega = \{1,\ldots,n\}$. This means that there is a nontrivial imprimitivity block $B$ for $G$, let $a = |B|$. Let $H = \{g \in G : g(B) = B\}$, 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 $\Omega$ we have $ab = n$. Of course we have a homomorphism $\xi : H \to Sym(B) \cong S_b$ induced by the action of $H$ on $B$. By Theorem 1 we deduce a homomorphism $f : G \to \xi(H) \wr S_n \leq S_n \wr S_b$ with kernel the normal core of $\ker(\xi)$ in $G$. Observe that if $h \in \ker(\xi)$ then $h$ fixes $B$ pointwise, and if $h \in \ker(\xi)^{\circ}$ then $ghg^{-1} \in \ker(\xi)$ so $h$ fixes $Bg$ pointwise. This implies that $(\ker(\xi))_G = \{1\}$ hence $f$ is injective. Also, we may restrict the codomain of $f$ to $\xi(H) \wr K$ where $K$ is the largest subgroup of $S_b$ for which the restriction makes sense. $\xi(H)$ and $K$ could be called “components” of $G$.

This means that 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 $\xi(H)$ 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 $K$. This gives an embedding 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 $A \wr B \wr C = A \wr (B \wr C)$.

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).
The full wreath product $S_n \wr S_b$ embeds into $S_n$ (where $n = ab$) as an imprimitive subgroup. Actually it is a maximal imprimitive subgroup, meaning that it is not properly contained in any imprimitive subgroup of $S_n$, in other words if $S_n \wr S_b$ is contained in an imprimitive subgroup $S_c \wr S_d$ then $a = c$ and $b = d$.

We will see that if $a \geq 5$ then $S_n \wr S_b$ is also a primitive group (abstractly) but the degree of primitivity is much larger: $a^b$ (the point stabilizer being the normalizer of $(S_{a-1})^b$). 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 Wielandt 1969, Praeger and Saxl 1980, taken to $2^n$ by Maróti in 2002).

**Exercise:** 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:** 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 $\Omega$ is transitive if and only if $m = 1$.
- The action of $P$ on $\Omega$ is primitive if and only if $m = k = 1$.

6. **Intransitive maximal subgroups**

The subgroups defined by the action on two orbits $A, B$ whose union is $\{1, \ldots, n\}$ are called “maximal intransitive subgroups” and have the shape $H = S_a \times S_b$, where $a = |A|, b = |B|, a + b = n$. We study the maximality of $G = S_a \times S_b$ inside $S_n$. If $G$ is not maximal then it is properly contained in $K < S_n$ which therefore is transitive on $\Omega$ (to take $t \leq a$ to $r > a$ use something taking the first orbit to the second). Suppose $K$ is imprimitive. Then clearly $A = \{1, \ldots, a\}$ and $B = \{a + 1, \ldots, n\}$ are contained in maximal imprimitivity blocks, however since they are orbits they are maximal imprimitivity blocks. This is only possible if $a = b = n/2$, hence $S_a \times S_b$ is maximal whenever $a \neq b$ and $a + b = n$. If $a = b = n/2$ then $S_a \times S_b = S_a \times S_a$ is not maximal: it is properly contained in the wreath product $S_n \wr S_2$, which (as we will see) is a maximal subgroup of $S_{2n}$ (imprimitive). If $K$ is primitive then it contains a 2-cycle and Jordan theorem (see below) implies that $K = S_n$.

7. **Primitive maximal subgroups**

7.1. **Characteristically simple groups.** A group $G$ is called characteristically simple if its only characteristic subgroups are $\{1\}$ and $G$. For example if $N$ is a minimal normal subgroup of a finite group $G$ then $N$ is characteristically simple (because characteristic in normal implies normal).

**Proposition 4.** If $S$ is a nonabelian simple group the normal subgroups of $S^n$ are its subproducts $S_{i_1} \times \cdots \times S_{i_m}$ where $m \leq n$ and $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$.

**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 $N \ni g_x g^{-1} = ([x^{-1}, s_1], 1, 1, \ldots, 1)$. Let $t = [x^{-1}, s_1]$. Of course $t \neq 1$ at least for some $x$ (being $S$ simple) so the conjugates of $t$ generate $S$ hence $N$ 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.

**Proposition 5.** Let $G$ be a finite group. $G$ is characteristically simple if and only
if there exist a simple group $S$ and a natural number $n$ such that $G \cong S^n$.

**Proof.** See [5, Theorem 8.10].

**Exercise:** 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:** if $|G| \geq 3$ then $\text{Aut}(G) \neq \{1\}$.

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

**Exercise:** Let $T$ be a nonabelian simple group. Prove that $\text{Aut}(T^n) \cong \text{Aut}(T) \wr S_n$. Use the embedding theorem with $H = N_{\text{Aut}(T^n)}(R) \to \text{Aut}(R)$ where $R = T \times \{1\} \times \cdots \times \{1\}$.

### 7.2. Primitive groups.

A finite group $G$ is called primitive of degree $n$ if it admits a maximal subgroup
$M$ of index $n$ such that $M_G = \{1\}$. We shall see such group as a permutation
group by means of its right multiplication action on $\Omega = \{Mx : x \in G\}$. The
-corresponding homomorphism $\gamma : G \to \text{Sym}(\Omega)$ is injective because its kernel is
$M_G = \{1\}$, and the permutation group $\gamma(G) \cong G$ on $\Omega$ is primitive in the sense
that it has no nontrivial blocks (as we have seen). We list some properties of such
a group.

First observe that if $A,B$ are minimal normal subgroups of a group $X$ and
$A \cap B = \{1\}$ then $ab = ba$ for all $a \in A$, $b \in B$. Indeed $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1}$ belongs to both $A$ and $B$. Also, it is easy to see that if $N$ is any normal
-subgroup of a group $A$ then its centralizer in $A$ is also a normal subgroup of $A$.

Recall also that if $H \leq S_n$ acts regularly then $|H| = n$. Now let $G$ be a primitive
group of degree $n$.

1. If $H \leq G$ is transitive then $C_G(H)$ is semiregular. Indeed if $g \in C_G(H)$
   fixes $a \in \Omega$ then whenever $h \in H$ we have $(ah)g = (ag)h = ah$ therefore $g$
   fixes $ah$ for all $h \in H$; being $H$ transitive $g$ fixes every $\omega \in \Omega$ hence $g = 1$.
2. If $N$ is a nontrivial normal subgroup of $G$ then it is transitive. Indeed if
   $\omega \in \Omega$ then $\omega N$ is a block: if $g \in G$ and $n \in N$ with $\omega ng \in N\omega$ then
   there is $m \in N$ with $\omega ng = \omega m$ therefore if $\ell \in N$ then $\omega \ell = \omega ngm^{-1}\ell = \omega m(gm^{-1}\ell g^{-1})g \in \omega Ng$, this implies $\omega Ng \subseteq \omega N$ hence they are equal
   (having the same size).
3. $G$ has at most two minimal normal subgroups. Indeed if $N$ is a minimal
   normal subgroup then it is transitive, $L = C_G(N)$ is normal in $G$ (hence
   transitive if non-trivial) and semiregular so it is regular if non-trivial, and
   it contains every minimal normal subgroup of $G$ distinct from $N$ because
   the intersection between two minimal normal subgroups is trivial. However
   $N$ is contained in $C_G(L)$ hence $N$, $C_G(L)$ are both regular so $N = C_G(L)$
(they both have size $n$). If $N = L$ then $N$ is the unique minimal normal subgroup of $G$, otherwise the two minimal normal subgroups are $N$ and $L$. 

(4) If $G$ has two minimal normal subgroups then $N$ is nonabelian. Indeed if $N$ is abelian then $N \leq C_G(N)$ and $|N| = |C_G(N)| = n$ hence $N = C_G(N)$, in particular there cannot be other minimal normal subgroups.

**Exercise:** Let $S$ be a group, prove that $\Delta = \{(s,s) : s \in S\}$ is a maximal subgroup of $S \times S$ if and only if $S$ is a simple group. Moreover in this case $S \times S$ is a primitive group and $|S|$ is its unique primitivity degree (meaning that every core-free maximal subgroup of $S \times S$ has index $|S|$).

If a minimal normal subgroup $N$ of $G$ is abelian then it is the unique minimal normal subgroup, let us study the structure of $G$ in this case. The core-free maximal subgroup $M$ intersects $N$ trivially because $M \cap N$ is normal in $M$ (being $N$ normal in $G$) and it is normal in $N$ (being $N$ abelian) hence it is normal in $MN$, however $MN = G$ because $M$ is maximal and does not contain $N$ (being $M_G = \{1\}$). By minimality of $N$ since $M \cap N \leq G$ we deduce $M \cap N = \{1\}$ hence $G$ is a semidirect product $N \rtimes H$. Since $N$ is characteristically simple $N = C_p^m$ for some prime $p$ and some positive integer $m$, hence we may see $N$ (additively) as a vector space of dimension $m$ over $\mathbb{F}_p$. Since there are no other minimal normal subgroups $H$ acts faithfully on $N$ by conjugation and minimality of $N$ translates into irreducibility of the linear action of $H$, in other words $H$ an irreducible subgroup of $GL(m,p)$. Conversely it is easy to see that if $V$ is a finite vector space over the field $\mathbb{F}_p$ ($p$ is a prime!) and $H$ is an irreducible subgroup of $GL(V)$ then $V \rtimes H$ with the natural action of $H$ is a primitive group whose only primitivity degree is $|V|$ (which in particular is a prime power). Such type of group is called an affine group.

As a consequence we obtain the following. Suppose the group $G$ has nontrivial center. Then $G$ is primitive if and only if $G$ is cyclic of prime order $p$, which therefore is its only primitivity degree. To see this let $N$ be a minimal normal subgroup of $G$ contained in the center of $G$ (so that $N$ has prime order $p$), then by the above discussion $G$ is a semidirect product $N \rtimes M$ which therefore is a direct product being $N$ central, $G = N \times M$. It follows that $M \leq G$, in other words $M = M_G$, however $M_G = \{1\}$ by assumption so $M = \{1\}$ and $G = N \cong C_p$.

On the opposite side of the spectrum $N$ is nonabelian, in which case $N = T^n$ for some non-abelian simple group $T$. Suppose $C_G(N) = \{1\}$, then the conjugation action of $G$ on $N$ embeds $G$ in $\text{Aut}(N)$, so that $N \leq G \leq \text{Aut}(N)$. If $n = 1$ then $N = T$ is a nonabelian simple group. In this case $G$ is called almost-simple. Equivalently, an almost-simple group is a group $G$ admitting a nonabelian simple normal subgroup $T$ with the property that $C_G(T) = \{1\}$. Equivalently, $G$ lies between $S$ and $\text{Aut}(S)$. An obvious example of almost-simple group is the symmetric group itself, $S_n$, when $n \geq 5$, indeed $A_n$ is a simple non-abelian normal subgroup of $S_n$ and $C_{S_n}(A_n) = \{1\}$.

**Proposition 6.** Let $n \geq 5$ and $m$ a positive integer. $G = S_n \wr S_m$ (the wreath product) is a primitive group of degree $n^m$.

**Proof.** First we prove that $G = S_n \wr S_m = (S_n)^m \rtimes S_m$ is a primitive group. For this define $N = A_n^m$, it is a non-abelian normal subgroup of $G$ (being $a \geq 5$), and it is a minimal normal subgroup because since $A_n$ is a non-abelian simple group (being
a ≥ 5) the normal subgroups of \( N \) are its subproducts and they are not normal in \( G \) because of the fact that \( S_n \) acts transitively on the set of the \( b \) factors, which are the minimal normal subgroups of \( N \). Moreover \( C_G(N) = \{1\} \). To see this first observe that \( C_G(N) ≤ S^m_n \) because any element with a nontrivial component in \( S_b \) does not centralize all the elements that have 1 in all positions except one, so \( C_G(N) ≤ C_{S_n}(A_n)$ but \( C_{S_n}(A_n) = \{1\} \) (because of the normal structure of the symmetric group) hence \( C_G(N) = \{1\} \). This implies that \( N \) is the unique minimal normal subgroup of \( G \): any other minimal normal subgroup would have to centralize \( N \).

We are left to construct a maximal subgroup \( M \) with trivial normal core and of index \( a^b \). Let \( M := N_G(K) \) where \( K = S^m_{n-1} \), being \( S_{n-1} \) any point stabilizer in \( S_n \). We have \( M ∩ N = N_N(K) = K \) being \( N_{S_n}(S_{n-1}) = S_{n-1} \) being \( S_{n-1} \) maximal in \( S_n \). If \( M \) is a maximal subgroup of \( G \) then since it does not contain \( N \) its normal core is trivial, being \( N \) the unique minimal normal subgroup of \( G \), also \( MN = G \) for the same reason hence

\[
|G : M| = |MN : M| = |N : M ∩ N| = |S^m_n : S^m_{n-1}| = n^m.
\]

We are then left to show that \( M \) is a maximal subgroup of \( G \). If \( H \) is a maximal subgroup of \( G \) containing \( M \) then \( H ∩ N \) contains \( K \), however it must be equal to \( K \) because since \( NH = G \) and \( N \) acts (by conjugation) trivially on its direct factors, \( H \) acts transitively on the factors of \( N \) hence it induces isomorphisms between the projections \( π_i(H ∩ N) \) (where \( π_i : N → \{1\} × ⋯ × \{1\} × A_n × \{1\} × ⋯ × \{1\} \), the \( i \)-th factor), which therefore are all isomorphic and contain \( S_{n-1} \) (for more details see below, O’Nan-Scott theorem). Since \( S_{n-1} \) is maximal in \( S_n \) we deduce that \( H ∩ N = K \). Since \( H ∩ N \) is normal in \( H \), \( H \) is then contained in the normalizer \( N_G(K) \) which equals \( M \), so \( H = M \). □

For example \( S_5 ∧ S_2 \), which is imprimitive of degree 5 · 2 = 10, is a primitive group of degree 5² = 25.

Observe that \( nm \) is comparatively much smaller than \( n^m \). This is because if a group is primitive, its primitivity degrees are “large” (in a sense to be defined).

### 7.3. Multiple transitivity.

Obvious examples of primitive groups are \( S_n \) and \( A_n \) (of degree \( n \)), for this observe that the point stabilizers are maximal in both cases: they have index \( n \) and we have seen that \( S_n \) has no proper subgroup of index less than \( n \) other than \( A_n \), similarly \( A_n \) has no proper subgroups of index less than \( n \).

Let \( G ≤ \Sigma_n \) act naturally on \( Ω = \{1, \ldots, n\} \). For \( 1 ≤ k ≤ n \) define \( O_k(Ω) \) to be the set of \( k \)-tuples \( (α_1, \ldots, α_k) \) of pairwise distinct elements of \( Ω \). We have a natural action of \( G \) on \( O_k(Ω) \). We say that \( G \) is \( k \)-transitive if it acts transitively on \( O_k(Ω) \). We say that \( G \) is sharply \( k \)-transitive if it acts regularly on \( O_k(Ω) \). Since \( |O_k(Ω)| = n(n-1) \cdots (n-k+1) \) this is the order of any sharply \( k \)-transitive group of degree \( n \), and it is a divisor of the order of any \( k \)-transitive group. Obviously if \( G \) is \( k \)-transitive then it is \( m \)-transitive for all \( 1 ≤ m ≤ k \).

**Proposition 7.** Let \( k ≥ 2 \). If \( G \) acts faithfully and \( k \)-transitively on a set of size \( n \geq 3 \) then the action is primitive.
Proof. Since $G$ is 2-transitive we may assume $k = 2$. Let $B \subseteq X$ be such that $|B| > 1$ and $B \neq X$, and take $x, y \in B$ distinct and $z \notin B$. Since $G$ acts 2-transitively there exists $g \in G$ with $xg = x$ and $yg = z$, so $B$ is not an imprimitivity block for $G$. □

**Proposition 8.** $G \leq S_n$ is $(n - 2)$-transitive if and only if $G = A_n$ or $G = S_n$.

**Proof.** Clearly $S_n$ is $n$-transitive and $A_n$ is $(n - 2)$-transitive (if you don’t believe: exercise). Also $|O_{n-2}(\Omega)| = n(n-1)\cdots(n-(n-2)+1) = n!/2$ hence $A_n$ is actually sharply $(n - 2)$-transitive. Since $A_n$ is the only subgroup of $S_n$ of index 2, it follows that $A_n$ is the only sharply $(n - 2)$-transitive group of degree $n$. Moreover if $G \leq S_n$ is $(n - 2)$-transitive then $|O_{n-2}(\Omega)| = n!/2$ divides $|G|$, so for the same reason $G = A_n$ or $G = S_n$. □

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

**Lemma 1.** Let $1 \leq k \leq n$. The transitive group $G \leq S_n$ is $k$-transitive if and only if the stabilizer of $\alpha \in \Omega$ in $G$ is $(k - 1)$-transitive on $\Omega - \{\alpha\}$.

**Exercise:** 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).

### 7.4. Jordan groups.

Let $G$ act faithfully on a set $\Omega$. A subset $\Delta$ of $\Omega$ is called a Jordan set if the pointwise stabilizer of $\Omega - \Delta$ acts transitively on $\Delta$. Let $G(\Delta)$ be such pointwise stabilizer. Since any Jordan set is contained in a $G$-orbit we may assume $G$ is transitive on $\Omega$. Obviously $\Omega$ itself is a Jordan set and every one element subset of $\Omega$ is also a Jordan set. $\Omega$ and the one-element subsets of $\Omega$ are called “improper” Jordan sets, all the others are called “proper”. If $G$ acts $k$-transitively then $\Delta \subseteq \Omega$ is a Jordan set whenever $|\Omega - \Delta| < k$.

If two Jordan sets $\Delta_1$, $\Delta_2$ intersect then their union is a Jordan set because the pointwise stabilizer of $\Omega - (\Delta_1 \cup \Delta_2)$ contains $\langle G(\Delta_1), G(\Delta_2) \rangle$. Therefore if $\Delta_1$ is a maximal Jordan set then one of the following occurs: $\Delta_1 \cap \Delta_2 = \emptyset$, $\Delta_2 \subseteq \Delta_1$ or $\Delta_1 \cup \Delta_2 = \Omega$.

If $B \subseteq \Omega$ is an imprimitivity block of $G$ and $\Delta$ is a Jordan set with $B \cap \Delta \neq \emptyset$ then one of $B$ and $\Delta$ contains the other. Indeed if $\alpha \in B \cap \Delta$ and there exist $\beta \in B - \Delta$ and $\gamma \in \Delta - B$ then a permutation mapping $\alpha$ to $\delta$ cannot fix $\beta$ (by definition of block), and this contradicts the fact that $\Delta$ is a Jordan set.

**Theorem 2** (Jordan’s Theorem). A finite primitive group having a proper Jordan set is 2-transitive.

**Proof.** Suppose $G$ is primitive on $\Omega$. If $\Delta$ is a proper subset of $\Omega$ with $|\Delta| > 1$ let

$$B = \{ \beta \in \Omega : \beta \in \Delta g \leftrightarrow \alpha \in \Delta g \ \forall g \in G \}. $$

Then $B$ is an imprimitivity block for $G$: if $\gamma \in B \cap Bg$ then $\gamma, \gamma^{-1} \in B$, so if $h \in G$ then $\gamma \in \Delta h$ if and only if $\gamma^{-1} \in \Delta h$, if and only if $\alpha \in \Delta h$, if and only if $\gamma^{-1} \in \Delta h$, if and only if $\gamma \in \Delta h$, if and only if $\alpha \in \Delta h$, if and only if $\delta \in \Delta h$,
if and only if $\delta g^{-1} \in \Delta h$. Since $B \neq \Omega$ and $G$ is primitive, $B = \{\alpha\}$. Now call $n = |\Omega|$, and let $\Delta$ be a maximal Jordan set of $G$, with $|\Delta| = k$. By the above observation for any $\alpha \in \Omega$ the translates of $\Delta$ not containing $\alpha$ cover $\Omega - \{\alpha\}$ (if not some $\beta$ would be left uncovered hence $\alpha \sim \beta$), so since no two of them have union $\Omega$ (their union cannot contain $\alpha$) their are pairwise disjoint hence $k$ divides $n - 1$. Since $G$ is transitive any point $\alpha \in \Omega$ is outside the same number $(n-1)/k$ of translates of $\Delta$. The total number of translates of $\Delta$ is therefore $n(n-1)/k(n-k)$ (multiplying $n(n-1)/k$ would count each point $n-k$ times). Since $k$ divides $n-1$ both $k$ and $n-k$ are coprime to $n$ (writing $kt = n-1$ we have $n-k = 1$ and $(n-k)t - n(t-1) = 1$). This implies that $k(n-k)$ divides $n-1$, and this can only happen if $k = 1$ or $n-k = 1$. If $k = 1$ then $\Delta$ is improper, so $n-k = 1$ which means that the stabilizer of one point acts transitively on the other points, in other words the action of $G$ on $\Omega$ is 2-transitive. \(\square\)

The more general version of Jordan theorem is the following (see Isaacs, Finite Group Theory).

**Theorem 3** (Jordan). Suppose $G \leq S_n$ acts primitively on $\Omega = \{1, \ldots, n\}$ and $\Delta$ is a Jordan set for $G$. If $|\Delta| \geq 2$ and $G(\Delta)$ acts primitively on $\Delta$ then the action of $G$ on $\Omega$ is $(|\Omega - \Delta| + 1)$-transitive.

We will not prove this theorem. Instead we will study some of its consequences.

If $G \leq S_n$ acts primitively on $\Omega = \{1, \ldots, n\}$ and contains a transposition $(\alpha, \beta)$ then $G = S_n$. Indeed $\{\alpha, \beta\}$ is a Jordan set of $G$ and the action on $G$ on $\{\alpha, \beta\}$ is primitive because 2 is a prime number. By Jordan theorem the action of $G$ is $(n-1)$-transitive hence $|O_{n-1}(\Omega)| = n!$ divides $|G|$ so $G = S_n$.

Similarly if $G \leq S_n$ acts primitively on $\Omega = \{1, \ldots, n\}$ and contains a 3-cycle $(\alpha, \beta, \gamma)$ then $G = A_n$ or $G = S_n$. Indeed $\{\alpha, \beta, \gamma\}$ is a Jordan set of $G$ and the action on $G$ on $\{\alpha, \beta, \gamma\}$ is primitive because 3 is a prime number. By Jordan theorem the action of $G$ is $(n-2)$-transitive hence $|O_{n-2}(\Omega)| = n!/2$ divides $|G|$ so $G \geq A_n$.

More in general we have:

**Theorem 4.** Let $G \leq S_n$ act primitively on $\Omega = \{1, \ldots, n\}$ and assume $G$ contains a $p$-cycle $\gamma$, where $p$ is a prime such that $p \leq n-3$. Then $G = A_n$ or $G = S_n$.

*Proof.* The cases $p = 2$ and $p = 3$ have already been considered above, so now assume $p \geq 5$. Let $\Delta$ be the set of points moved by $\gamma$, so that $|\Delta| = p$. $\Delta$ is a Jordan set and since $p$ is a prime $G(\Delta)$ acts primitively on $\Delta$. By Jordan theorem we deduce that $G$ is $(n-p+1)$-transitive, so it is $(n-p)$-transitive. Let $H \leq G$ be the setwise stabilizer of $\Omega - \Delta$, then $H/G(\Delta)$ is isomorphic to $Sym(\Omega - \Delta)$ (this is because any permutation of $\Omega - \Delta$ is induced by an element of $G$, being $G$ $(n-p)$-transitive and $|\Omega - \Delta| = n-p$).

Let $P = \langle \gamma \rangle \leq G$. Then $P \leq G(\Delta)$ and since $G(\Delta)$ acts faithfully on $\Delta$ we deduce that $|G(\Delta)|$ divides $p!$. Therefore $P$ is a Sylow $p$-subgroup of $G(\Delta)$ and by the Frattini argument, since $G(\Delta) \trianglelefteq H$, we obtain $H = G(\Delta)N$ where $N = N_H(P)$. Therefore $N/N(\Delta) \cong H/G(\Delta) \cong Sym(\Omega - \Delta)$. Since $|\Omega - \Delta| \geq 3$ the symmetric
group of \( \Omega - \Delta \) contains a 3-cycle, which therefore belongs to the derived subgroup of \( Sym(\Omega - \Delta) \) (the alternating group). Let then \( x \in N' = [N, N] \) be such that the permutation induced by \( x \) on \( \Omega - \Delta \) is a 3-cycle.

Let \( C = C_N(P) \). Since the automorphism group of \( P \) is abelian (being \( P \) cyclic of order \( p \)), \( N/C \) is abelian, so \( x \in N' \leq C \) hence \( x \) commutes with \( \gamma \). So the permutation induced by \( x \) on \( \Delta \) commutes with a \( p \)-cycle acting on the \( p \) points of \( \Delta \). Since the centralizer of a \( p \)-cycle in \( S_p \) is generated by such \( p \)-cycle, we deduce that \( p \) divides the order of \( x \) and \( x^p \) acts trivially on \( \Delta \). Since \( x \) induces a 3-cycle on \( \Omega - \Delta \) and 3 does not divide \( p \) we deduce that \( x^p \) induces a 3-cycle on \( \Omega - \Delta \). Therefore \( x^p \) fixes the elements of \( \Delta \) and acts as a 3-cycle on \( \Omega - \Delta \), so \( x \) is a 3-cycle belonging to \( G \). We know that this implies that \( G \geq A_n \).

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. Similarly the same is true for \( A_n \) (the proof of this is a bit more tricky).

7.5. Primitive actions: O’Nan-Scott. See also [6, Chapter 7].

We have seen that primitive groups with abelian socle are precisely the affine groups. Now let \( G \) be a primitive group with nonabelian socle \( N = soc(G) \). We know that \( N \) is a product of at most two minimal normal subgroups, but in this discussion we will assume \( N \) itself is a minimal normal subgroup of \( G \). We know that \( N = S^m \) for some nonabelian simple group \( S \) and some positive integer \( m \).

Let \( G \) be a primitive monolithic group with socle \( N = soc(G) = T_1 \times \cdots \times T_m = T^m \), where \( T \) is a nonabelian simple group. We apply Theorem 1 to \( H = N_G(T_1) \) and \( \xi : H \to Aut(T_1) \), the conjugation action. Observe that ker(\( \xi \)) = \( C_G(T_1) \) and since the conjugation action of \( G \) on \( N \) permutes the factors \( T_1, \ldots , T_m \), the normal core of \( C_G(T_1) \) in \( G \) is \( C_G(N) = \{1\} \). Define \( X := N_G(T_1)/C_G(T_1) \), which is an almost-simple group with socle \( T := T_1C_G(T_1)/C_G(T_1) \cong T_1 \). Obviously \( X \) is isomorphic to the image of \( \xi \). The minimal normal subgroups of \( T^m = T_1 \times \cdots \times T_m \) are precisely its factors \( T_1, \ldots , T_m \). Since automorphisms send minimal normal subgroups to minimal normal subgroups, it follows that \( G \) acts on the \( m \) factors of \( N \). Let \( \rho : G \to S_m \) be the homomorphism induced by the conjugation action of \( G \) on the set \( \{T_1, \ldots , T_m \} \). The group \( K := \rho(G) \) is a transitive permutation group of degree \( m \). By Theorem 1 \( G \) embeds in the wreath product \( X \wr K \).

Let \( X \) be an almost-simple group with socle \( S \) and let \( K \) be a faithful transitive group of degree \( m \). The wreath product \( G = X \wr K \) is itself a primitive monolithic group. To see this let \( N = soc(G) \). We argue that \( N \) is the unique minimal normal subgroup of \( G \). Indeed another minimal normal subgroup would lie in \( C_G(N) \) so it is enough to show that \( C_G(N) = \{1\} \). Let \( (x_1, \ldots , x_n) \pi \) lie in \( C_G(N) \). By considering the conjugates of \((s, 1, \ldots , 1) \) where \( 1 \neq s \in S \) we see that \( \pi = 1 \) and if \( i \in \{1, \ldots , n \} \) then \( x_i \in C_X(s) \) for all \( s \in S \) hence \( x_i \notin C_X(S) = \{1\} \).

This means that any primitive group \( G \) with nonabelian socle is a subgroup of \( X \wr K \) where \( X \) is an almost-simple group with socle \( S \), \( K \) is a transitive group
of degree \( m \) and \( G \) projects surjectively onto \( K \). Of course these are not all the conditions \( G \) must satisfy to be primitive, but they are necessary conditions.

Let \( G \) be a primitive group with nonabelian socle \( N = S^m \). What we want to do now is to study the primitive actions of \( G \). Let \( M \) be a maximal subgroup of \( G \) with trivial normal core, so that \( MN = G \). Then \( N \cap M \) is normal in \( M \). We claim that \( N \cap M \) is a maximal proper \( M \)-invariant subgroup of \( N \). Indeed if \( N \cap M < L < N \) is \( M \)-invariant then \( M < LM < G \), contradicting the maximality of \( M \). Indeed:

- If \( M = LM \) then \( L \leq M \cap N \) a contradiction.
- If \( LM = G \) then \( L \leq G \) contradicting the fact that \( N \) is a minimal normal subgroup of \( G \).

We want to show that the maximal subgroups \( M \) of \( G \) which supplement the socle (i.e. \( MN = G \)) are of the following three types:

- **Complement.** \( M \cap N = \{1\} \) so that \( G \) is a semidirect product \( N \rtimes M \).
- **Product type.** A conjugate of \( N_G(H^m) \) where \( H \) is the intersection between \( S \) and a maximal subgroup of \( X \).
- **Diagonal type.** \( M = N_G(\Delta_1 \times \ldots \times \Delta_l) \) where each \( \Delta_i \) is a diagonal and \( m/l \) is a prime number.

\( NB: \) the subgroups of diagonal type \( N_G(\Delta_1 \times \ldots \times \Delta_l) \) with \( m/l \) not a prime are not maximal. Actually each of them is contained in the normalizer of a refined product of diagonals.

\( NB: \) the primality of \( m/l \) is not sufficient to establish that the diagonal type subgroup is maximal. But if it is not maximal then it is contained in a maximal subgroup which contains the socle.

Take a maximal subgroup \( M \) of \( G \) supplementing the socle \( N \), i.e. such that \( MN = G \). Call \( \pi_1, \ldots, \pi_m \) the projections \( \pi_i : S^m = S_1 \times \ldots \times S_m \to S_i \). Observe that since \( N \) is a (the) minimal normal subgroup of \( G \) and the normalizer in \( G \) of \( M \cap N \) is a subgroup of \( G \) containing \( M \), either \( M \) complements \( N \) or \( N_G(M \cap N) = M \).

**Proposition 9.** \( \pi_i(M \cap N) \cong \pi_j(M \cap N) \) for every \( i \neq j \).

**Proof.** Notice that \( M \) is transitive on the factors \( S_i \) of \( N \), because \( G \) is transitive, \( N \) acts trivially on each factor and \( G = NM \). So there exists an element \( h \) of \( M \) such that the conjugation by \( h \) sends \( S_i \) to \( S_j \), so it determines an automorphism of \( M \cap N \) which induces an isomorphism

\[ \pi_i(M \cap N) \cong M \cap N/\ker(\pi_i|_{M \cap N}) \cong M \cap N/\ker(\pi_j|_{M \cap N}) \cong \pi_j(M \cap N). \]

This proves the statement.

There are three possibilities for \( \pi_1(M \cap N) \).

1. \( \pi_1(M \cap N) = \{1\} \). This implies that \( \pi_i(M \cap N) = 1 \) for every \( i \), so \( M \cap N = 1 \). In other words \( M \) complements \( N \), so \( G = N \rtimes M \) and the primitivity degree is \( |N| = |S|^m \).

2. \( \pi_1(M \cap N) = S \). Then each \( \pi_i|_{M \cap N} \) is surjective. Consider

\[ D_{ij} = \pi_i(\ker(\pi_j|_{M \cap N})) \]

for every \( i, j \). Observe that \( D_{ij} \) is a normal subgroup of \( S_i \). Indeed if \( x \in \ker(\pi_j|_{M \cap N}) \) and \( s \in S_i \) then there exists \( t \in M \cap N \) with \( \pi_i(t) = s \)
hence $s^{-1} \pi_i(x)s = \pi_i(t^{-1}xt)$ and $\pi_j(t^{-1}xt) = \pi_j(t)^{-1} \pi_j(x) \pi_j(t) = 1$ being $\pi_j(x) = 1$. This proves that $s^{-1} \pi_i(x)s \in D_{ij}$ so that $D_{ij} \leq S_i$.

Since $S_i$ is simple we have two cases: $D_{ij} = S_i$ or $D_{ij} = \{1\}$. Observe that $D_{ii} = \{1\}$. Fix $i$ and assume that $D_{ij} = \{1\}$ for all $j \in \{1, \ldots, m\}$. This means that $\ker(\pi_j|M \cap N) = \{1\}$ for all $j$, so the projections $\varphi_j = \pi_j|M \cap N : M \cap N \to S_j$ are all isomorphisms. Let $\alpha_{ij} := \varphi_j \circ \varphi_i^{-1}$, it is an isomorphism $S_i \to S_j$, and $M \cap N$ is contained in $\{x \in N : \alpha_{ij}(\pi_i(x)) = \pi_j(x) : \forall i, j\}$. By maximality of $M \cap N$ as proper $M$-invariant subgroup of $N$ this proves that equality holds. In other words $M \cap N$ is a “diagonal subgroup” \{$(s, s^{\alpha_2}, \ldots, s^{\alpha_m}) : s \in S$\} where $\alpha_i$ is an isomorphism $S \to S$ for all $i$. Up to conjugation in $Aut(N)$ it follows that $M \cap N$ is isomorphic to $(s, s, \ldots, s) : s \in S$.

In the general case $M \cap N$ will be a direct product of diagonals as above. Specifically there exists a number $l$ dividing $m$ and $l$ diagonals $\Delta_1, \ldots, \Delta_l$ of length $m/l$ such that $M \cap N = \Delta_1 \times \ldots \times \Delta_l$ (by maximality of $M \cap N$ as proper $M$-invariant subgroup of $N$ it is enough to show $\leq$). In this case the maximality of $M$ implies that $m/l$ is a prime. To understand this it is sufficient to give an example: if $m = 4$, the normalizer of the diagonal $(x, x^{\varphi_2}, x^{\varphi_3}, x^{\varphi_4})$ is contained in the normalizer of $(x, y, x^{\varphi_3}, y^{\varphi_4})$.

(3) $1 < \pi_i(M \cap N) < S$. Let $V_i := \pi_i(M \cap N) \leq S_i$. We have $V_i \cong V_j$ for every $i, j$, and every such isomorphism can be realized as the conjugation by an element of $M$. In this case $M \cap N \leq V_1 \times \ldots \times V_m$ and it is possible to show that in fact equality holds, and $V \cong V_i$ is the intersection between $X$ and a maximal subgroup of $S$. [More details in the next version of the notes.]

Using this we may list the primitivity degrees of a given primitive group. This is easy now because if $G$ is a monolithic primitive group with socle $N$ and point stabilizer $M$ then being $M \cap N = G$ we have $|G : M| = |N : N \cap M|$ (being $|G| = |M| |N| = |M| |N| / |M \cap N|$). For example let $S$ be a nonabelian simple group. The degrees of primitivity of $G = S \rtimes C_n$ are $|S : M|^n$ for $M$ maximal in $S$ and $|S|^{n/p}$ where $p$ is a prime dividing $n$ (see the diagonal type case). Observe that in principle $|N|$ could be a primitivity degree, you need to check the specific case. For example the degrees of primitivity of $A_5 \rtimes C_2$ are $5^2 = 25$, $6^2 = 36$, $10^2 = 100$ and $|A_5| = 60$, $|A_5|^2$ is not a primitivity degree because the complements of the socle are not maximal: exercise).

References