induction hypothesis. Now let $\{\mathrm{id}\} \neq N \trianglelefteq A_n$, we want to show that $N = A_n$.

Step 1. $N \cap G(n) \neq \{\mathrm{id}\}$.

We argue by contradiction and suppose that $N \cap G(n) = \{\mathrm{id}\}$. This means that the only element in N that fixes n is id. Now take $\alpha, \beta \in N$ and suppose that $\alpha(n) = \beta(n)$. Then $\alpha^{-1}\beta(n) = \alpha^{-1}(\alpha(n)) = n$ and by what we have just said it follows that $\alpha^{-1}\beta = \mathrm{id}$ or $\alpha = \beta$. Hence, a permutation α in N is determined by $\alpha(n)$ and since there are at most n values, we have that $|N| \leq n$. But his contradicts Lemma 4.3.

Step 2. $N = A_n$.

Now $\{\mathrm{id}\} \neq N \cap G(n) \trianglelefteq G(n)$ (by the 2nd Isomorphism Theorem) and since $G(n)$ is simple by induction hypothesis, it follows that $N \cap G(n) = G(n)$. In particular, N contains a 3-cycle and thus $N = A_n$ by Lemma 4.2. $\Box$

II. Group actions

Theorem 4.5 *(Cayley). Any group G is isomorphic to a subgroup of Sym (G).*

Proof For $a \in G$ consider the map $L_a : G \to G, x \mapsto ax$. Notice that L_a is bijective with inverse $L_{a^{-1}}$ and thus $L_a \in \mathrm{Sym}\,(G)$. Now consider the map

$$\phi : G \to \mathrm{Sym}\,(G), a \mapsto L_a.$$

Notice that $(L_a \circ L_b)(x) = abx = L_{ab}(x)$ and thus $\phi(ab) = L_{ab} = L_a \circ L_b = \phi(a) \circ \phi(b)$. Thus ϕ is a homomorphism. This homomorphism is injective since if $\phi(a) = \phi(b)$ then $a = a \cdot 1 = L_a(1) = L_b(1) = b \cdot 1 = b$. Thus G is ismorphic to $\mathrm{im}\,\phi$ where the latter is a subgroup of $\mathrm{Sym}\,(G)$. $\Box$

Definition. Let X be a set and G a group. We say that X is a G-set if we have a right multiplication from G, i.e. a map

$$\phi : X \times G \to X, (x, g) \mapsto x \cdot g$$

satisfying

(a) $x \cdot 1 = x \quad \forall x \in X$
(b) $(x \cdot a) \cdot b = x \cdot (ab) \;\; \forall a, b \in G$ and $x \in X$.

Remark. One also says that G acts on X. Notice that $x \cdot g$ is just a notation for $\phi(x, g)$. Notice also that for every $a \in G$ we have that the map $X \to X : x \mapsto x \cdot a$ is a permutation with inverse $X \to X : x \mapsto x \cdot a^{-1}$.

Examples. (1) Let $X = G$ be a group. We can consider this as a G-set with respect to the natural right group multiplication $x * g = xg$. Clearly $x * 1 = x1 = x$ and $(x * a) * b = (xa)b = x(ab) = x * (ab)$ by the associativity in G.

(2) Let $H \leq G$ and let X be the collection of all the right cosets of H in G. We can again consider X as a G-set with respect to the natural right group multiplications $Hg*a = Hga$ again it is easy to see that $Hg*1 = Hg$ and $(Hg*a)*b = Hg*(ab) = Hgab$.

(3) Let G be a group and $X = G$. We define a group action by G on X by letting $x * a = a^{-1}xa = x^a$. Then X becomes a G-set as $x^1 = x$ and $(x^a)^b = x^{ab}$.

(4) Let X be the collection of all the subgroups of G. We can consider X as a G-set with respect to the conjugation action. That is the right multiplication is given by $H * g = g^{-1}Hg = H^g$. Again X is a G-set.

Definition. Let X be a G-set. The *stabilizer* of $x \in X$ is

$$G_x = \{g \in G : \, x \cdot g = x\}$$

and the G-*orbit* of $x \in X$ is

$$x \cdot G = \{x \cdot g : \, g \in G\}.$$

Lemma 4.6 $G_x \leq G$

Proof Firstly by condition (a) we have $1 \in G_x$. Now suppose that $a, b \in G_x$. Using condition (b) we then have $x \cdot (ab) = (x \cdot a) \cdot b = x \cdot b = x$ and $ab \in G_x$. It remains to show that G_x is closed under taking inverses. But this follows from

$$x = x \cdot 1 = x \cdot (aa^{-1}) = (x \cdot a) \cdot a^{-1} = x \cdot a^{-1}.$$

This finishes the proof. $\Box$

Theorem 4.7 *(The Orbit Stabilizer Theorem). Let X be a G-set and $x \in X$. Let $\mathcal{H}$ be the collection of all the right cosets of G_x in G. The map*

$$\Psi : \mathcal{H} \to x \cdot G, \, G_x a \mapsto x \cdot a$$

is a bijection. In particular

$$|x \cdot G| = |\mathcal{H}| = [G : G_x].$$

(In other words the cardinality of the G-orbit generated by x is the same as the cardinality of the collection of the right cosets of G_x in G).

Proof $\underline{\Psi \text{ is well defined and injective}}$. We have

$$x \cdot a = x \cdot b \Leftrightarrow x \cdot ab^{-1} = x \Leftrightarrow ab^{-1} \in G_x \Leftrightarrow G_x b = G_x a.$$

As Ψ is clearly surjective, this finishes the proof. $\Box$

Proposition 4.8 *Let X be a G-set. The relation*

$$x \sim y \quad \textit{if} \quad y \in x \cdot G$$

is an equivalence relation on X and the equivalence classes are the G-orbits.

Proof As $x = x \cdot 1$ it is clear that $x \sim x$ and we have that $\sim$ is reflexive. Now suppose that $y = x \cdot a$. Then $x = y \cdot a^{-1}$. This shows that $\sim$ is symmetric. It now remains to show that $\sim$ is transitive. But if $y = x \cdot a$ and $z = y \cdot b$ then $x \cdot (ab) = (x \cdot a) \cdot b = y \cdot b = z$. Hence we get $x \sim z$ from $x \sim y$ and $y \sim z$ and this shows that $\sim$ is transitive and thus an equivalence relation.

Finally $x \sim y$ iff $y \in x \cdot G$. Hence the equivalence class containing x is the G-orbit $x \cdot G$. $\square$

Corollary 4.9 *Suppose that the G-orbits of X are are $x_i \cdot G$, $i \in I$. Then*

$$|X| = \sum_{i \in I} [G : G_{x_i}].$$

Proof We have that $X = \cup_{i \in I} x_i G$ where the union in pairwise disjoint. Thus

$$|X| = \sum_{i \in I} |x_i \cdot G| = \sum_{i \in I} [G : G_{x_i}].$$

Where the final equality follows from the Orbit Stabilizer Theorem.

5 Finite groups and Sylow Theory

Definition. Let G be a group and $x \in G$. The *centralizer* of x in G is

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

Remark. We are going to see shortly that $C_G(x)$ is a stabilizer of x with respect to a certain action. Hence it will follow that $C_G(x)$ is a subgroup of G. This we can also see more directly.

Conjugacy action and the class equation. Let G be a finite group. We can then think of G as a G-set where the right multiplication is defined by

$$x * g = x^g = g^{-1}xg.$$

The G-orbit $x * G$ is then $\{x * g = x^g : \; g \in G\} = x^G$, the *conjugacy class* of x, and the stabilizer of x is

$$G_x = \{g \in G : \; x = x * g = g^{-1}xg\} = \{g \in G : \; xg = gx\} = C_G(x).$$

The orbit- stabiliser theorem thus tells us that

$$|x^G| = [G : C_G(x)]$$

We next write G as a disjoint union of G-orbits, that is conjugacy classes:

$$\begin{aligned} G \;\; = \;\; & \underbrace{a_1^G \cup a_2^G \cup \cdots \cup a_r^G}_{\text{each of size } \geq 2} \\ & \cup \underbrace{b_1^G \cup b_2^G \cup \cdots b_s^G}_{\text{each of size } 1} \end{aligned}$$

Recall that $Z(G)$ is the set of all those elements that commute with every element of G and that this is a normal subgroup of G. Now $x \in Z(G)$ if and only if $x = g^{-1}xg = x^g$ for all $g \in G$. It follows that $x \in Z(G)$ if and only if it's conjucacy class $\{x^g : \; g \in G\}$ consists only of one element x. Therefore $Z(G) = \{b_1, \ldots, b_s\}$ and

$$G = Z(G) \cup a_1^G \cup a_2^G \cup \cdots \cup a_r^G.$$

and $|G| = |Z(G)| + \sum_{i=1}^{r} |a_i^G|$. Using the Orbit-Stabilizer Theorem we can deduce from this the *class equation*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(a_i)]$$

where the sum is taken over the r conjugacy classes with more than one element (so each $[G : C_G(a_i)] > 1$).

Definition. Let p be a prime. A finite group G is said to be a p-group if $|G| = p^m$ for some $m \geq 0$.

Remark. The trivial group $G = \{1\}$ is a p-group for any prime p.

Theorem 5.1 *If G is a non-trivial finite p-group, then $Z(G)$ is non-trivial.*

Proof We use the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

Since $1 \neq |G|$ is of p-power order it follows that $|G|$ and each index $[G : C_G(a_i)]$ are divisible by p. From the class equation it then follows that $|Z(G)|$ is divisible by p. In particular it has at least two elements. $\Box$

Example. The result above does not hold for finite groups in general. For example $Z(S_3) = \{1\}$.

Theorem 5.2 *(Cauchy). Let G be a finite group with order that is divisible by a prime p. Then G contains an element of order p.*

Remark. From exercise 4 on sheet 3, we know that this is true when G is abelian.

Proof We prove this by induction on $|G|$. If $|G| = 1$ then the result is trivial ($|G|$ is then not divisible by any prime p so the statement will not get contradicted). Now suppose that $|G| \geq 2$ and that the result holds for all groups of smaller order. Consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^{r} \underbrace{[G : C_G(a_i)]}_{\text{each } \geq 2}.$$

If any of the $|C_G(a_i)|$ is divisible by p, then, as $|C_G(a_i)| < |G|$, we can use the induction hypothesis to conclude that $C_G(a_i)$ contains an element of order p (and thus G as well). Thus we can assume that none of $|C_G(a_i)|$ are divisible by p. But then, as $|G| = [G : C_G(a_i)] \cdot |C_G(a_i)|$, all the indices $[G : C_G(a_i)]$ are divisible by p and the class equation implies that $|Z(G)|$ is divisible by p. But $Z(G)$ is abelian so it follows from the remark that it then contains an element of order p. $\Box$

Theorem 5.3 *Let G be a finite p-group and suppose that $|G| = p^n$. There exist a chain of normal subgroups of G*

$$\{1\} = H_0 < H_1 < \ldots < H_n = G$$

where $|H_i| = p^i$ for $i = 0, 1, \ldots, n$.

Proof. We use induction on $|G| = p^n$. If $n = 0$ then $\{1\} = H_0 = G$ is the chain we want. Now suppose that $n \geq 1$ and that the result holds for all p-groups of smaller order. By Theorem 5.1, we have that $Z(G)$ is non-trivial and by Cauchy's Thoerem (the abelian version suffices) we know that there is a subgroup H_1 of $Z(G)$ such that $|H_1| = p$. Notice that $H_1 \trianglelefteq G$ (as all the elements of H_1 commute with all the elements of G and thus

$gH_1 = H_1g$ for all $g \in G$). Now $|G/H_1| = p^{n-1}$ and by induction hypothesis, there is a normal chain of subgroups

$$\{1\} = K_0 < K_1 < \cdots < K_{n-1} = G/H_1.$$

By the Correspondence Theorem this chain corresponds to a normal chain of intermediate subgroups between H_1 and G

$$H_1 < H_2 < \cdots < H_n = G$$

where $K_{i-1} = H_i/H_1$. Then $|H_i| = |K_{i-1}| \cdot |H_1| = p^{i-1} \cdot p = p^i$ and the chain

$$\{1\} = H_0 < H_1 < \cdots < H_n = G$$

is the chain we want. $\square$.