A group $(G,*)$ is a set G equipped with an associative map $* : G \times G \to G$ so that G has an identity and inverses with respect to $*$. If $*$ is commutative, then G is abelian. A subgroup H of a group G is a nonempty subset $H \subseteq G$ which is closed under $*$ and taking inverses, and is denoted $H \leq G$. For any subgroup $H \leq G$, then $e_H = e_G$ and inverses in H and G are identical.

Subgroup test. If G is a group and $H \subseteq G$, then $H \leq G$ if and only if H is nonempty and $xy^{-1} \in H$ for all $x, y \in H$.

The subgroup of a group G generated by a nonempty set $X \subseteq G$ is

$$\langle X \rangle := \{x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k} \mid a_i \in \{\pm 1\}, x_i \in X \text{ for all } 1 \leq i \leq k,\ k \geq 0\}$$

and can equivalently be characterised as the intersection of all subgroups of G which contain X. In this sense, $\langle X \rangle$ is the 'smallest' subgroup of G which contains X. A group G is finitely generated if there exists a finite set $X \subseteq G$ such that $G = \langle X \rangle$. A group G is cyclic if there exists $g \in G$ such that $G = \langle \{g\} \rangle := \langle g \rangle$.

The order of a group G is the number of elements of the group, and is denoted $|G|$. If G contains infinitely many elements, then $|G| := \infty$. The order of an element $a \in G$ is the order of $\langle a \rangle \leq G$.

The cyclic group of order $n \in \mathbb{Z}_{>0}$ is $C_n := \langle g \mid g^n = e \rangle$. (Strictly speaking, I'm cheating here: this is a group presentation of C_n which we'll see later.)

Let G be a group and $H \leq G$. A left coset of H in G is $gH := \{gh : h \in H\}$ for some $g \in G$. A right coset of H in G is $Hg := \{hg : h \in H\}$ for some $g \in G$. There is an equivalence relation on G given by $g_1 \sim g_2$ iff $g_1 \in g_2 H$ for all $g_1, g_2 \in G$. An analogous equivalence relation exists on G for right cosets of H in G.

Lagrange's theorem. If G is a group and $H \leq G$, then $|G| = [G : H]|H|$ where $[G : H]$ is the index, meaning the number of left (or equivalently, right) cosets, of H in G.

GROUP ACTIONS AND SYLOW THEOREMS.

The converse of Lagrange's theorem doesn't generally hold, but there exist partial converses, such as:

Cauchy's theorem. If G is a group and p is a prime which divides $|G|$, then there exists $H \leq G$ such that $|H| = p$.

A p-group is a group in which every element is of order p^k. A p-subgroup is a subgroup which is a p-group. A finite group G is a p-group if and only if $|G| = p^k$ for some $k \in \mathbb{Z}$.

A left group action of a group G on a set X is a map $\alpha : G \times X \to X$ such that $\alpha(e, x) = x$ and $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ for all $g, h \in G$ and $x \in X$. A right group action is defined analogously. It's common to write $g.x := \alpha(g, x)$ for a group action α, $g \in G$ and $x \in X$. Given a group action, the orbit of an element $x \in X$ is $G.x := \{g.x : g \in G\} \subseteq X$ and the stabiliser of $x \in X$ is $\mathrm{Stab}_G(x) := \{g : g.x = x\} \subseteq G$. A fixed point of a group action is $x \in X$ such that $G.x = \{x\}$.

If G is a finite group which acts upon a set X, then $\mathrm{Stab}_G(x) < G$ for each $x \in X$. Moreover, there exists an equivalence relation $\sim$ on X such that for all $x, y \in X$, $x \sim y$ iff there exists $g.x = y$. That is, a group action partitions a set into orbits. Lastly, we have:

Orbit-stabiliser theorem. If G is a finite group which acts on a set X, then $|G| = |G.x||\mathrm{Stab}_G(x)|$ for all $x \in X$.

A pair of elements $a, b \in G$ are conjugate if there exists $g \in G$ such that $a = gbg^{-1}$. A group G acts on itself by conjugation via the map $G \times G \to G$, $(g, a) \mapsto gag^{-1}$. The conjugacy class $\mathrm{Cl}(a)$ of an element $a \in G$ is the orbit of a under conjugation; hence, conjugation partitions a group into conjugacy classes so that the class equation $|G| = \sum_i |\mathrm{Cl}(a_i)|$ for a finite set $\{a_1, \ldots, a_k\} \subset G$.

The centraliser $C_G(a)$ of an element $a \in G$ is the stabiliser of a under conjugation, given explicitly as the subset of G with respect to which a is invariant under conjugation, $C_G(a) := \{g : a = gag^{-1}\}$.

Immediately, $C_G(a) < G$. Also, $|G| = |Cl(a)||C_G(a)|$ for each $a \in G$ and thus $|\mathrm{Cl}(a)| = [G : C_G(a)]$ by Lagrange's theorem.

A pair of subsets $T, S \subseteq G$ are conjugate if there exists $g \in G$ such that $T = gSg^{-1}$. That is, conjugation by g induces a one-to-one correspondence between T and S. The centraliser $C_G(S)$ of a subset $S \subseteq G$ is $C_G(S) := \{g \ : \ s = gsg^{-1} \text{ for all } s \in S\} \leq G$. The centre $Z(G)$ of a group G is $Z(G) := C_G(G)$. The normaliser $N_G(S)$ of a subset $S \subseteq G$ is $N_G(S) := \{g \ : \ S = gSg^{-1}\} \leq G$ such that $C_G(S) \subset N_G(S)$.

A subgroup $H \leq G$ is normal if $H = gHg^{-1}$ for all $g \in G$, and is denoted $H \lhd G$. Equivalently, $H \lhd G$ iff $gHg^{-1} \leq H$ iff $G = N_G(H)$ iff left and right cosets of H in G coincide. Given an arbitary subgroup $K \leq G$, the normaliser $N_G(K)$ is equal to the union of all subgroups (*i.e.* the 'largest' subgroup) which contain K as a normal subgroup.

Our group action technology and a pair of lemmas, which are:

1. If p is a prime and G is a finite-p group which acts on a finite set X, then the number of fixed points in X is congruent to $|X|$ modulo p,

2. If G is a finite group and $H \leq G$, then $[G : N_G(H)]$ equals the number of distinct conjugate subgroups of H in G and moreover, for each prime p which divides $|G|$ and Sylow p-subgroup $P \leq G$, we have $n_p = [G : N_G(P)]$,

allow us to prove:

Sylow theorems. Let G be a group and p be a prime such that k is the largest exponent for which p^k divides $|G|$.

1. There exists a subgroup of G whose order is p^k. Such a subgroup is called a Sylow p-subgroup.
2. For each Sylow p-subgroup $P \leq G$ and p-subgroup $H \leq G$, there exists $g \in G$ such that $H \subseteq gPg^{-1}$. Hence, any two Sylow p-subgroups of G are conjugate.
3. The number n_p of Sylow p-subgroups of G divides $|G|/p^k$, is congruent to 1 modulo p and equals $[G : N_G(P)]$ for each Sylow p-subgroup $P \leq G$.

As a consequence of the Sylow theorems, a Sylow p-subgroup of G is normal iff $n_p = 1$. A subgroup $H \leq G$ is simple if H contains only $\{e\}$ and H as normal subgroups; that is, H contains no 'non-trivial' normal subgroups.

ISOMORPHISM THEOREMS.

Given a pair of groups G and H, a group homomorphism is a map $\phi : G \to H$ such that for all $g, h \in G$, $\phi(gh) = \phi(g)\phi(h)$. A group isomorphism is a bijective group homomorphism. If $\phi : G \to H$ is a group homomorphism, then $\phi(e_G) = e_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$. The kernel $\ker\phi$ of a group homomorphism $\phi : G \to H$ is $\ker\phi := \{g \ : \ \phi(g) = e_H\} \subseteq G$. A subgroup $N \leq G$ is normal in G iff there exists a group H and a group homomorphism $\phi : G \to H$ such that $\ker\phi = N$.

A factor group G/N is the set of left (or equivalently, right) cosets of a normal subgroup $N \lhd G$ in G equipped with the group operation $(gN) * (hN) = (gh)N$ for each $g, h \in G$. There is a canonical surjective group homomorphism $\mathrm{can} : G \to G/N, g \mapsto gN$.

Universal property of factor groups. Let G be a group and $N \lhd G$. For each group H and group homomorphism $\psi : G \to H$ with $N \subseteq \ker\psi$, there exists a unique group homomorphism $\overline{\psi} : G/N \to H$ such that $\psi = \overline{\psi} \circ \mathrm{can}$.

As a useful corollary, if $\phi : G \to K$ is a surjective group homomorphism and $\psi : G \to H$ is a group homomorphism with $\ker\phi \subseteq \ker\psi$, then there exists a unique group homomorphism $\overline{\psi} : K \to H$ such that $\psi = \overline{\psi} \circ \phi$.

First isomorphism theorem. If G, H are groups and $\phi : G \to H$ is a group homomorphism, then $\ker\phi \lhd G$, $\mathrm{im}\phi \leq H$ and there exists a group isomorphism $\overline{\phi} : G/\ker\phi \to \mathrm{im}\phi$ given by $gN \mapsto \phi(g)$ with $N := \ker\phi$. If ϕ is surjective, then $G/\ker\phi \cong H$.

If G is a group and $N \lhd G$, then we make two observations: first, if $K \leq G/N$, then $\mathrm{can}^{-1}(K) \leq G$ with $N \subseteq \mathrm{can}^{-1}(K)$ and moreover, $\mathrm{can}^{-1}(K) \lhd G$ if and only if $K \lhd G/N$; second, if $N \leq H \leq G$, then $H = \mathrm{can}^{-1}(\mathrm{can}(H))$. Combining these allows us to prove:

Correspondence theorem. Let G be a group, $N \lhd G$ and $\mathrm{can} : G \to G/N$ denote the canonical surjection. There is a bijection between subgroups of G which contain N and subgroups of G/N given by $H \mapsto \mathrm{can}(H)$ which restricts to a bijection between normal subgroups of G which contain N and normal subgroups of G/N.

Furthermore, if $A, B \leq G$, then $A \subseteq B$ iff $\mathrm{can}(A) \subseteq \mathrm{can}(B)$.

which in turn allows us to prove:

Third isomorphism theorem. If G is a group and $N \leq H \leq G$ are such that $N, H \lhd G$, then $(G/N)/(H/N) \cong G/H$.

Given a pair of subsets $X, Y \subseteq G$, define $XY := \{xy \ : \ x \in X, y \in Y\}$.

Second isomorphism theorem. If G is a group, $N \lhd G$ and $H \leq G$, then

1. $HN \leq G$,
2. $N \lhd HN$,
3. $H \cap N \lhd H$,
4. $HN/N \cong H/(H \cap N)$.

GROUP PRESENTATIONS.

The free group on generators $x_1, \ldots, x_n$ is the set of all words in the symbols $x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}$ equipped with concatenation, and is denoted $\langle x_1, \ldots, x_n \rangle$.

Given an arbitrary group G, the normal closure $\mathrm{ncl}_G(S)$ of a subset $S \subseteq G$ is the intersection of all normal subgroups of G which contain S; that is, $\mathrm{ncl}_G(S)$ is the 'smallest' normal subgroup of G which contains S. The group generated by $x_1, \ldots, x_n$ subject to 'relations' $r_1, \ldots, r_k \in \langle x_1, \ldots, x_n \rangle$ is

$$\langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_k \rangle := \langle x_1, \ldots, x_n \rangle / \mathrm{ncl}_G(\{r_1, \ldots, r_k\}).$$

If a group G is isomorphic to $\langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_k \rangle$, then the latter is a 'presentation' of G. Also, $\langle x_1, \ldots, x_n \,|\, r_1, \ldots, r_k \rangle$ is equivalently the free group $\langle x_1, \ldots, x_n \rangle$ subjected to the additional conditions $r_1 = \cdots = r_k = e$ and all logical consequences thereof.

The n-th dihedral group D_n is the group of symmetries of a regular n-sided polygon; formally, D_n is defined for each $n \in \mathbb{Z}_{\geq 3}$ as the group generated by two elements, g and h, where g denotes reflection across a line through a specified, fixed vertex and h denotes rotation by $2\pi/n$ radians. There is a group presentation for D_n given by $D_n \cong \left\langle g, h \,|\, g^2, h^n, (gh)^2 \right\rangle$ for each $n \geq 3$.

Universal property of free groups. Let G be a group generated by a set $\{s_1, \ldots, s_n\}$ and $F = \langle S_1, \ldots, S_n \rangle$ be the free group generated by the letters $S_1, \ldots, S_n$. There exists a unique surjective group homomorphism $\pi : F \to G$ such that $\pi(S_i) = s_i$ for each $i \in \{1, \ldots, n\}$.