Lagrange's Theorem

We define the order of an element $g \in G$ as $|g| = \min\{m > 0 \mid g^m = e\}$ (allowing $|g| = \infty$).

Lemma 1 (Coset Equality Lemma)

$$gH = kH \Leftrightarrow k^{-1}g \in H$$

Proof: Right implication is trivial, and left implication is shown as $gH = k(k^{-1}g)H \subseteq kH$, and $kH = g(g^{-1}k)H \subseteq gH$ so $gH = kH$.
By Lagrange's theorem, we have that the order of any subgroup divides the order of the original group (provided the original group is finite). This is proven by showing that the set of cosets of a subgroup partition the original group, and taking the coset of a subgroup neither increases nor decreases its elements.

From Lagrange's theorem we may formalise many of our intuitions regarding the notion of group order. We have immediately that $g^{|G|} = e$, and then both Fermat's little theorem and Euler's theorem in relation to $\mathbb{Z}_n^*$. The former states that $a^{p-1} = 1 \mod p$ if p is prime and $p \nmid a$, while the latter is the more general case that $a^{\phi(n)} = 1 \mod n$ with $\phi(n) = |\{k \in \mathbb{N} \mid n > k, \text{hcf}(k, n) = 1\}|$.

Important Groups

While the point of the course isn't to memorise facts about a list of groups, it's useful to have a decent knowledge of common groups, especially for being able to provide counterexamples.

The Dihedral Groups (D_{2n})
For $n \geq 3$, D_{2n} is a dihedral group generated by two elements r (rotation) and s (reflection), where r has order n, s order 2, and $r^{-1}s = sr$. The group as a whole has order $2n$, as we have n different orientation preserving rotations in addition to the n reflections of each such rotation. Subgroups of dihedral groups are either cyclic or dihedral. Dihedral groups, while always non-abelian, are very close to being abelian by their structure, so occasionally demonstrate similar properties.

The Cyclic Groups (C_n)
Probably the most basic groups: a cyclic group is any group generated by a single element. If that element has finite order, then the resulting group is isomorphic to C_n. One can generally refer to C_n equivalently by $\mathbb{Z}/n\mathbb{Z}$ (under addition), and $C_{\phi(n)}$ is isomorphic to $\mathbb{Z}_n^*$ where ϕ is Euler's totient function. A common related group is $V_4 \cong C_2 \times C_2$, also known as Klein's group, which shows up regularly in finite groups.

An important property of cyclic groups is that all subgroups are also cyclic. Verify this via contradiction, taking $\min\{r \mid g^r \in H\}$ where $H \leq \langle g \rangle$. This is useful for applications to number theory, noting that we thus get for any $m, n \in \mathbb{Z}$ some $h, l \geq 0$ such that $\langle m, n \rangle = \langle h \rangle$ and $\langle m \rangle \cap \langle n \rangle = \langle l \rangle$. Commonly we can write $h = \gcd(m, n)$ and $l = \text{lcm}(m, n)$. From here Bezout's lemma ought to be clear, and furthermore one can construct an isomorphism between C_{mn} and $C_m \times C_n$ when m and n are coprime (Chinese remainder theorem).

Permutation Groups (S_n)
Defined as the set of permutations (bijections) of n elements. $|S_n| = n!$. Technically S_n is a shorthand for $\text{Sym}(\{1, 2, \ldots, n\})$, where $\text{Sym}(X) = \{\text{The set of bijections of } X\}$. In the context of permutations in this course we usually refer to finite sets, however the Sym notation is still occasionally useful, for example to note that $\text{Sym}(\{2, 3, 4\}) \cong S_3$ is a subgroup of S_4.

Permutation groups tend to require their own notation for permutations, which itself prompts proof of its own validity. The most important result after developing the cycle notation is that cycle type is preserved by conjugation (and the proof is fairly straightforward as well, which is helpful). This greatly simplifies proofs related to isomorphisms or normal subgroups, and just generally deals with a lot of claims that one would otherwise have to verify by hand.

Alternating Groups (A_n)

Not quite as common as permutation groups, but the nth alternating group A_n is the subgroup of S_n formed only of even permutations. The first year course doesn't go into much detail as to the properties of the alternating groups, but one should have an intuition for it as essentially the largest proper normal subgroup of S_n (and indeed it is the only proper nontrivial normal subgroup for $n \geq 5$).

General Linear Groups ($GL(n, \mathbb{F})$)

This is the set of invertible $n \times n$ matrices in the field $\mathbb{F}$. For the purpose of this course one primarily considers $GL(2, \mathbb{R})$, and its subgroups. An important note is the existence of $O(2)$ as a subgroup, which is the set of orthogonal 2×2 matrices, geometrically representing the set of isometric transformations of 2D space. Every dihedral group can have its transformations represented as elements of $O(2)$, and consequently for any n, $D_{2n} \leq O(2)$. Going further we also have $SO(2)$ as the special orthogonal group – the set of orthogonal matrices with determinant 1 (noting that orthogonal matrices can only have determinant ± 1 in the first place). This is the set of 2D rotations, and every cyclic group is a subgroup of $SO(2)$ (additionally it is isomorphic to S^1).

Homomorphisms and Isomorphisms

Definition 1 *Let G and H be groups. A homomorphism $\phi : G \to H$ is a map such that for all $g_1, g_2 \in G$:*

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$$

We thus define an **automorphism** of G as an isomorphism from G to G (forming $\text{Aut}(G)$ under composition), an **endomorphism** of G a homomorphism from G to G, a **monomorphism** an injective homomorphism and an **epimorphism** a surjective homomorphism.

Definition 2 *Let G be a group and $H \leq G$. Then H is a normal subgroup of G ($H \lhd G$) if $gH = Hg$ for all $g \in G$. Equivalently, if $g^{-1}hg = \theta_g(h) \in H$ for all $g \in G$, $h \in H$.*

We also define the image $\text{im}\,\phi$ and kernel $\ker\phi$ of any homomorphism exactly as one would expect. We have that both are subgroups of their respective groups, and $\ker\phi \lhd G$ (these are just definition chases). When viewing that G/N is a group iff $N \lhd G$, we can view any homomorphism as with type $G \to H \cong G/N$ for some H, N the kernel with the image under each gN the element corresponded to in H under its isomorphism.

We write the centre of G as $Z(G) = \{g \in G \mid \forall h \in G.\ gh = hg\}$. This is always normal in G.

By introducing the notion of normal subgroups, we may consider quotient groups, defined on G/H for $H \lhd G$ with $g_1H * g_2H = (g_1g_2)H$.

For this to be well-defined we require that if $x_1H = y_1H$ and $x_2H = y_2H$ then $x_1x_2H = y_1y_2H$. Equivalently if $x_1^{-1}y_1, x_2^{-1}y_2 \in H$, then $(x_1x_2)^{-1}y_1y_2 \in H$ (equivalent to $x_2^{-1}(x_1^{-1}y_1)x_2(x_2^{-1}y_2) \in H$, which holds if H is normal).

Why is $S/\sim$ the set of equivalence classes of S under $\sim$? $\sim$ is a partition of S, rather than a subgroup, so this doesn't seem to make much sense.

The answer is that the coset definition is a special case of the $/$ notation. This is not true for general sets.

First Isomorphism Theorem

(*Also Noether's first isomorphism theorem*)

Let $\phi : G \to H$ be a homomorphism between two groups. Then the map $g\ker\phi \mapsto \phi(g)$ gives an isomorphism

$$\frac{G}{\ker\phi} \cong \text{im}\,\phi$$

This theorem allows us to determine the number of homomorphisms between groups, as we immediately get the corollary that $|G| = |\ker\phi| \times |\text{im}\,\phi|$. First, determine the normal subgroups of the domain (the possible kernels), the number of subgroups of the codomain isomorphic to G/N ($n(N)$). Finally, for each N determine the number of automorphisms of G/N ($|\text{Aut}(G/N)|$).

Group Actions

A group action is a method of interpreting each element of a group G as a unique map $S \to S$ on a set S.
Definition 3 *A left action of a group G on a set S is a map*

$$\rho : G \times S \to S$$

such that $\rho(e, s) = s$ for all $s \in S$, and $\rho(g, \rho(h, s)) = \rho(gh, s)$ for all $g, h \in G$, $s \in S$.
We write $\rho(g, s)$ as $g \cdot s$ normally.

The orbit of any $s \in S$, $\text{Orb}(s)$, under G is defined as

$$\text{Orb}(s) = \{g \cdot s \mid g \in G\}$$

The stabiliser of any $s \in S$, $\text{Stab}(s)$, under G is defined as

$$\text{Stab}(s) = \{g \in G \mid g \cdot s = s\}$$

We can immediately gather from these definitions that S is partitioned by the orbits, by defining an equivalence relation $x \sim y \Leftrightarrow \exists g \in G :\ x = g \cdot y$. We also gather that each stabiliser is a subgroup of G.

Theorem 2 *Let G be a finite group acting on a set S and let $s \in S$. Then*

$$|G| = |\text{Stab}(s)| \times |\text{Orb}(s)|$$