.1. The Basic Tools

Going from the well-behaved case of the cyclic groups C_n to the non-abelian case is really hard, and sometimes requires extra hypotheses. We should think of normal subgroups as analogous to divisors of an integer, and simple groups as prime numbers.

Definition .1.1

For any $n > 1$, there is a surjective homomoprhism $\operatorname{sgn} : S_n \twoheadrightarrow S_2$.

First, there is an injective homomorphism:

$$\begin{aligned} \rho : S_n &\hookrightarrow \{n \times n \text{ integer matrices with } \det \text{ equal to } \pm 1\} \\ \sigma &\mapsto \left(A_{ij} = \delta_{i\sigma(j)}\right) \end{aligned}$$

where $\delta_{k\ell}$ is the Kroenecker Delta (which is 1 when $k = \ell$ and zero otherwise). Then $\det \circ \rho$ is a surjective homomorphism $S_n \twoheadrightarrow \{\pm 1\}$, where $\{\pm 1\}$ is a group under multiplication. We call this homomorphism $\operatorname{sgn} : S_n \twoheadrightarrow S_2$.

We define $A_n := \ker \operatorname{sgn}$, and we say $\sigma \in S_n$ is **even** if $\operatorname{sgn} \sigma = 1$ and otherwise we say σ is **odd**.

Great fact: If $n \geq 5$ then A_n is simple.

Note: Any 2-cycle is odd.

Easy: Every element of S_n is a product of disjoint cycles (Hint: take a starting point, run it through σ over and over again until you get back to the starting point).

Consequence: Every element of S_n is a product of 2-cycles, since every cycle is a product of 2-cycles. Why? Well

$$(14)(13)(12) = (1234)$$

and likewise for any other cycle.

Restated: S_n is generated by the two-cycles.

This gives an immediate proof of the following:

Proposition .1.1

An element σ of S_n is even if and only if it can be written as a product of an even # of 2-cycles if and only if it cannot be written as the product of an odd # of 2-cycles.

Proposition .1.2

A_n is generated by 3-cycles.

Proof. From the above, we know A_n is all products of an even # of 2-cycles. Thus it suffices to show that 3-cycles are exactly products of two 2-cycles:

$$\begin{aligned} (ij)(ij) &= \mathrm{Id} \\ (ij)(ik) &= (ikj) && (i, j \neq k) \\ (ij)(k\ell) &= (ki\ell)(ijk) && (i, j \neq k,\ i, j \neq \ell) \end{aligned}$$

Thus every product of two 2-cycles is a product of some # of 3-cycles and every 3-cycle is in A_n. Great!

Proposition .1.3

Let H be a subgroup of G, recall that:

$$\begin{aligned} H \text{ is normal} &\iff gHg^{-1} \subseteq H \quad \forall\, g \in G \\ &\iff gHg^{-1} = H \quad \forall\, g \in G \\ &\iff gH = Hg \quad \forall\, g \in G \\ &\iff H \text{ is the kernel of some homomorphism } \varphi : K \to G \end{aligned}$$

And in fact we have:

$$aHbH = a(Hb)H = a(bH)H = abHH = abH$$

This is suggesting we define a group. Namely G/H (the set of left cosets of H) is a group with operation $(aH)(bH) = (ab)H$.

Proof. If H is normal in G, then $gHg^{-1} \subseteq H$, and then $g^{-1}Hg \subseteq H$, so $H \subseteq gHg^{-1}$.

The backwards direction of this is clear, and the second holds if and only if the third holds by multiplication by g (resp. g^{-1}) on the right.

Now for the last bit, we know all kernels of homomorphisms are normal from last time. If $H \trianglelefteq G$ then we can write:

$$\begin{gathered} G \to G/H \\ g \mapsto gH \end{gathered}$$

is a surjective homomorphism with kernel H.

Definition .1.2

If $H \trianglelefteq G$, then G/H is a group, called the quotient group. The operation is

$$(aH)(bH) = (ab)H.$$

And it is well defined because by the above proposition if H is normal that as sets

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)H.$$

Details to be checked that this is a group.

So if $H \trianglelefteq G$ then G/H is a group, called the quotient group.

Lemma .1.4

If $[G : H] = 2$ (the **index** of H in G, that is $|G/H|$), then $H \trianglelefteq G$.

Proof. If $g \in H$ then $gH = H = Hg$. Then if $g \notin H$ then $gH = G \setminus H = Hg$.

Note: There is a bijection between G/H and the set of right cosets Hg for $g \in G$ given by inversion:

$$gH \mapsto Hg^{-1}$$

Note: Automorphisms of G preserve "reasonable" properties. E.g. if $\sigma \in \operatorname{Aut} G$ and $H \leq G$ then $H \trianglelefteq G$ if and only if $\sigma(H) \trianglelefteq H$. Also $[G : H] = [G : \sigma(H)]$. Also H is abelian if and only if $\sigma(H)$ is abelian.

So for instance, if H is the unique subgroup of G with a given index $[G : H]$, then $H \trianglelefteq G$ (since H must be preserved by conjugation by any $g \in G$).