4 Normal subgroups, simplicity and Lagrange's Theorem

4.1 Cosets and normal subgroups

Definition 4.1.1. Let $H \leq G$ and $g \in G$. A *(left) coset* of H in G is something of the form

$$gH = \{gh : h \in H\}.$$

There is also something called a right coset that has the form Hg, but we won't use those in this course (they behave the same—just different notation). The set of all cosets of H in G is denoted by G/H, so

$$G/H = \{gH : g \in G\}.$$

Warning! In general G/H is not a group!

The number of distinct cosets of H in G is called the *index* of H in G and is denoted $[G : H]$.

Example 4.1.2. We have $S_3 = \{e, (12), (23), (13), (123), (132)\}$ and $H = \langle (12) \rangle \leq S_3$. So $H = \{e, (12)\}$. Now the coset $(123)H = \{(123)e, (123)(12)\} = \{(123), (13)\}$ and the coset $(12)H = \{e, (12)\} = H$ (check this). If we list all the cosets (which you should do) we find there are only three: H and $\{(123), (13)\}$ and $\{(132), (23)\}$. Notice that every element in S_3 lies in a coset and the cosets are either disjoint or equal.

Theorem 4.1.3. *Let $H \leq G$ be groups with $a, b \in G$. The following are equivalent:*

(i) $a^{-1}b \in H$

(ii) $aH = bH$

(iii) $a \in bH$

(iv) $a = bh$ *for some* $h \in H$

Corollary 4.1.4. *Suppose $H \leq G$.*

(i) For all $a, b \in G$, either $aH = bH$ or $aH \cap bH = \varnothing$. (i.e. Cosets of H in G are either disjoint or they are equal.)

(ii) every element of G lies in a coset of H; and

(iii) for all $g \in G$ we have $|H| = |gH|$.

Definition 4.1.5. A subgroup N of a group G is *normal* if $g^{-1}kg \in N$ for all $k \in N$ and all $g \in G$. Notation: $N \trianglelefteq G$. Equivalent definitions:

- $N \trianglelefteq G$ means that for all $g \in G$ we have $g^{-1}Ng = N$
- $N \trianglelefteq G$ means that for all $g \in G$ we have $Ng = gN$

What is the point?!. Normal subgroups are special because we can "divide" by them and still get a group. These are called *quotient groups*.

Example 4.1.6. The following are examples of normal subgroups.

(i) $\langle e_G \rangle \trianglelefteq G$

(ii) $G \trianglelefteq G$

(iii) If G is abelian and $H \leq G$, then $H \trianglelefteq G$.
(I.e. all subgroups of an abelian group are normal.)
Proof: We must show that the following holds *for all $h \in H$ and all $g \in G$*:

$$g^{-1}hg \in H.$$

So, fix $h \in H$ and $g \in G$. Now $g^{-1}hg = g^{-1}gh$ (because G is abelian) and this equals $e_G h = h \in H$. Hence $H \trianglelefteq G$.

(iv) $C_3 \trianglelefteq S_3$.
Proof: You will prove this on a problem sheet.

Warning! When checking if H is normal in G, you must show that $g^{-1}hg \in H$ for **every** element $h \in H$ and every $g \in G$. It is not enough to check only some elements. Also, remember not to fool yourself by assuming that G is abelian!

4.1.1 Handout for Section 4.1

Question 4.1.7. Prove the three different definitions of a normal subgroup are equivalent (i.e. if a subgroup satisfies one of them, then it satisfies them all).

Example 4.1.8. Let G be the group $(\mathbb{R}^*, \times)$, and let H be the subgroup $(\mathbb{Q}^*, \times)$.

(i) Since $\sqrt{2} \in \mathbb{R}^*$, we can consider the coset,

$$\sqrt{2}H = \{\sqrt{2} \times q : q \in \mathbb{Q}^*\} = \left\{\frac{n\sqrt{2}}{m} : n, m \in \mathbb{Z}, \quad m, n \neq 0\right\}$$

(ii) Since $\frac{1}{2} \in \mathbb{R}^*$, we can consider the coset,

$$\frac{1}{2}H = \left\{\frac{1}{2} \times q : q \in \mathbb{Q}^*\right\} = \mathbb{Q}^* = H$$

So, sometimes a coset of H is equal to H. In fact, $gH = H$ if and only if $g \in H$. We see why in our next theorem and its corollary.

Non-Example 4.1.9. The following is an example of a nontrivial proper subgroup that is not normal.

Let A be the matrix $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, and let $H = \langle A \rangle$, so $H \leq \mathrm{GL}(2, \mathbb{R})$. We claim that H is not a normal subgroup of $\mathrm{GL}(2, \mathbb{R})$.

Proof: You can easily prove by induction that for $n \in \mathbb{N}$ we have $A^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$. And (by multiplying out) you can check that $A^{-n} = \begin{pmatrix} 1 & -2n \\ 0 & 1 \end{pmatrix}$. Hence

$$H = \left\{\begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}.$$

Now we know what H looks like, we can test for normality. To show H is not normal, we only need to find a single pair $A^n \in H$ and $B \in \mathrm{GL}(2, \mathbb{R})$ for which $B^{-1}A^nB \notin H$. Let $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$. Then

$$B^{-1}AB = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} -11 & -16 \\ 9 & 13 \end{pmatrix} \notin H.$$

Proof of Theorem 4.1.3. These were proved in Algebraic Structures, but here is one of the implications to help jog your memory. All are nice and short and are good exercises for you.
[(i) $\implies$ (ii)]: Suppose $a^{-1}b \in H$. Then there exists $h \in H$ such that $a^{-1}b = h$, and so we know two things: $b = ah$ and $a = bh^{-1}$. Now anything in aH has the form ah' for some $h' \in H$, but $ah' = bh^{-1}h' \in bH$. Therefore $aH \subseteq bH$. On the other hand, anything in bH has the form bh' for some $h' \in H$, but $bh' = ahh' \in aH$. Therefore $bH \subseteq aH$. Hence $aH = bH$. □

Proof of Corollary 4.1.4. All this was covered in Algebraic Structures, but here is the proof of (i) again because it is nice: Suppose $aH \cap bH \neq \varnothing$. Then there exists $g \in aH \cap bH$. Hence there exists $h_1, h_2 \in H$ such that $g = ah_1 = bh_2$. Therefore $a = b(h_2h_1^{-1}) \in bH$. By Theorem 4.1.3 (iii) this is equivalent to $aH = bH$. □

4.2 Simplicity and Lagrange's Theorem

Groups in which *no* nontrivial proper subgroup is normal are special, and play a special role in group theory.

Definition 4.2.1. A group G is *simple* if its only normal subgroups are $\langle e_G \rangle$ and G.
We will talk lots about simple groups later—they are very important.

Example 4.2.2. Any cyclic group of prime order, C_p, is simple. Exercise: why? [Hint: try to write down *any* subgroup of C_5 and see what happens; then try again with C_7. Now try in general with C_p.]

The following observation is frequently useful.

Lemma 4.2.3. (Order Switching Lemma). *Let $N \trianglelefteq G$. Suppose $g \in G$ and $k \in N$. Then there exist $k', k'' \in N$ such that*

$$gk = k'g \quad \text{and} \quad kg = gk''.$$

Warning! This only works when one of the groups is normal!

Proof. Now $gk \in gN = Ng$. Since everything in Ng can be written $k'g$ for some $k' \in N$, we must have that $gk = k'g$ for some $k' \in N$. A similar argument works for $kg \in Ng = gN$. □

Lemma 4.2.4. *Let G be a group, with $H \leq G$ and $N \trianglelefteq G$. Then:*

(i) $HN = NH$

(ii) $H \cap N \trianglelefteq H$, *and*

(iii) $HN \leq G$

Proof. You proved all of these things on problem sheets. □

You have already seen Lagrange's theorem, but it is so important we cover it again here.

Theorem 4.2.5. (Lagrange's Theorem). *Let H be a subgroup of a finite group G. Then,*

$$|G| = [G : H] \cdot |H|.$$

In particular, the order of H divides the order of G.

Proof. Every element of G lies in some coset of H (by 4.1.4), so we can write G as a union of cosets,

$$G = \bigcup_{g \in G} gH.$$

Some of these cosets will be equal and (because G is finite) there are only finitely many distinct cosets, so we can write

$$G = g_1H \cup g_2H \cup \dots g_nH,$$

where all the cosets g_iH are distinct. Recall that the number of distinct cosets of H in G is called the index of H in G and is denoted by $[G : H]$. Hence $n = [G : H]$.
By Theorem 4.1.4, distinct cosets are in fact disjoint. Therefore:

(i) Every element in G lies in one of the cosets g_iH for some $1 \leq i \leq n$; and

(ii) No element in G lies in two or more of these cosets.

Hence $|G| = |g_1H| + |g_2H| + \dots + |g_nH|$. By 4.1.4, all the cosets have the same size, so $|G| = n|g_1H| = n|H| = [G : H] \cdot |H|$. In particular, this implies that $|H|$ divides $|G|$. □

A partial converse to Lagrange's Theorem is due to Cauchy. We do not prove it here, since one can easily deduce it from the Sylow Theorems that we will prove later in the course.

Theorem 4.2.6. (Cauchy's Theorem). *If G is a finite group and p is a prime number dividing $|G|$, then G contains a subgroup of order p.*

4.2.1 Handout for Section 4.2

Here is an example of an infinite permutation group with an infinite normal subgroup (so the group is non-simple).

Definition 4.2.7. Let $\mathrm{Sym}(\mathbb{Z})$ be the group of all permutations of the integers. This is an infinite permutation group. A permutation $\sigma \in \mathrm{Sym}(\mathbb{Z})$ is called *finitary* if it only moves finitely many things in $\mathbb{Z}$. For example, the permutation $(\ldots\ -2\ -1\ 0\ 1\ 2\ \ldots)$ is not finitary, but $(1\ 2\ 3)$ is finitary. The group $\mathrm{FS}(\mathbb{Z})$ consists of all finitary permutations in $\mathrm{Sym}(\mathbb{Z})$. It is a normal subgroup of $\mathrm{Sym}(\mathbb{Z})$ (you will prove this on a problem sheet). Hence $\mathrm{Sym}(\mathbb{Z})$ is not simple.