Section 3.2 More on Cosets, And Lagrange's Theorem

Before our feature presentation, some words about some useful techniques.

(1) **Using Generators to Check if a Subgroup is Normal**

Recall $H \trianglelefteq G$ means $gH = Hg$, $gHg^{-1} = H$, $gHg^{-1} \subseteq H$ $\forall g \in G$

Suppose $H = \langle h_1, h_2, \dots, h_k \rangle \leq G = \langle g_1, g_2, \dots, g_\ell \rangle$

To show $H \trianglelefteq G$, you only need check

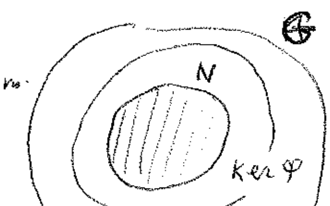
$g_i h_j g_i^{-1} \in H$ for $1 \leq j \leq k$ and $1 \leq i \leq \ell$.

Reason: Suppose we've confirmed this.
For $H \trianglelefteq G$, must show $ghg^{-1} \in H$ $\forall h \in H, g \in G$.

e.g.
$$\begin{aligned} ghg^{-1} &= g_1 g_3 (h_4^2 h_1)(g_1 g_3)^{-1} \\ &= g_1 \big(\underbrace{g_3 h_4 g_3^{-1}}_{\in H} \underbrace{g_3 h_4 g_3^{-1}}_{\in H} \underbrace{g_3 h_1 g_3^{-1}}_{\in H}\big) g_1^{-1} \\ &= g_1 \left(\text{prod of powers of } h_i\right) g_1^{-1} \\ &= \text{etc} \in H \end{aligned}$$

(2) **Connecting homomorphisms $\varphi : G \to H$ to $\varphi : G/N \to H$**

Useful fact: Suppose $\varphi : G \to H$ is a homomorphism and $N \trianglelefteq G$. Define $\varphi' : G/N \to H$ as $\varphi'(gN) = \varphi(g)$. Then φ' is a well-defined homomorphism $\iff N \leq \ker\varphi$



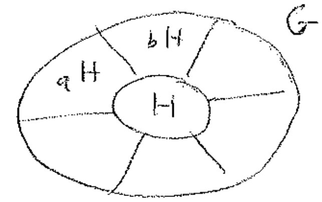
Proof: Suppose φ' is a homomorphism.
$x \in N \Rightarrow xN = 1N \Rightarrow \varphi'(xN) = \varphi'(1 \cdot N)$
$\Rightarrow \varphi(x) = \varphi(1) = 1 \Rightarrow x \in \ker\varphi$

Conversely suppose $N \leq \ker\varphi$. Suppose $xN = yN$. Then $x^{-1}y \in N \subseteq \ker\varphi$ so $\varphi(x^{-1}y) = \cancel{\varphi(x)^{-1}\varphi(y) = 1} \Rightarrow \varphi(x) = \varphi(y)$

Theorem 8 (Lagranges Theorem)

$$\begin{pmatrix} G \text{ finite} \\ \text{and } H \leq G \end{pmatrix} \Longrightarrow \begin{pmatrix} |H| \text{ divides } |G|, \text{ and} \\ \text{there are } \frac{|G|}{|H|} \text{ left cosets of } H \end{pmatrix}$$

Basic Idea Left cosets of H partition G into subsets of equal cardinality $|H|$.



Thus $|G| = |H| \cdot (\#\text{ of cosets})$ and Theorem follows.

Corollary If $x \in G$, then $|x|$ divides $|G|$
In particular $x^{|G|} = 1$.

Corollary If $|G|$ is prime, then G is cyclic.
(i.e. $G \cong \mathbb{Z}/p\mathbb{Z}$ with $p = |G|$ prime)

Corollary $|G/N| = \dfrac{|G|}{|N|}$

Definition If $H \leq G$, the number of left cosets in G is called the index of H in G, denoted $|G:H|$. So $|G:H| = \frac{|G|}{|H|}$ if G is finite.

Example $5\mathbb{Z} \leq \mathbb{Z}$ $\qquad |\mathbb{Z} : 5\mathbb{Z}| = 5$
$\{1,-1\} \leq Q_8$ $\qquad |Q_8 : \{\pm 1\}| = 4$

Note Converse of Lagrange's Theorem is false. If p divides G, G does not necessarily have a subgroup of order p.

This section gives some *partial* converses, but we delay full treatment of this topic until the next chapter.

For *now*, the following will be useful in the *next section*.

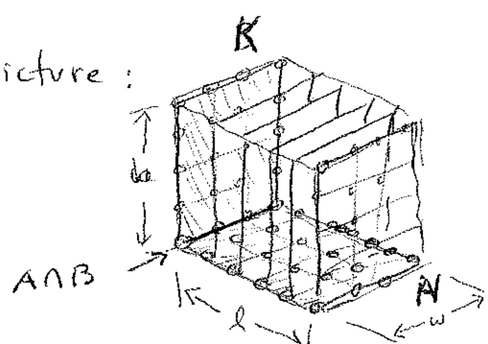
Definition If $H, K \le G$, then $HK = \{hk \mid h \in H, k \in K\}$.

There is no reason to expect this to be a subgroup. (It may or may not be, depending on H, K, G.)

Note $HK = \bigcup_{h \in H} hK$ = union of cosets $\subseteq G$.

Proposition 13 $|HK| = \dfrac{|H||K|}{|H \cap K|}$

Intuitive picture:



$$|HK| = lwh = \frac{lw\,hw}{w} = \frac{|H|\,|K|}{|H \cap K|}$$

The proof makes this idea precise.

Proposition 14 $HK \le G \iff HK = KH$

Corollary 15 If $H, K \le G$ and $N \le N_G(K)$, then $HK \le G$. In particular, if $K \trianglelefteq G$, then $HK \le G$ for any $H \le G$.