## 1. Subgroups generated by subsets of a group

Throughout this lesson, $G$ denotes a group.

**Proposition 1.1.** *If $\mathcal{A}$ is any nonempty collection of subgroups of $G$, then*

$$\bigcap_{H\in\mathcal{A}} H \leq G.$$

**Definition 1.2.** Let $A$ be any subset of $G$. The **subgroup generated by** $A$ is

$$\langle A\rangle := \bigcap_{\substack{A\subseteq H\\ H\leq G}} H.$$

This definition says that $\langle A\rangle$ is the smallest subgroup of $G$ that contains $A$. It is clear that the subgroup generated by a subgroup $H$ is $H$ itself. What would be the subgroup generated by $\varnothing$?

**Remark 1.2.1.** (i) If $A$ is a finite set, say $A = \{a_1, \dots, a_n\}$, then we simply write

$$\langle A\rangle = \langle a_1, \dots, a_n\rangle.$$

(ii) Recall from the previous lesson that $\langle a\rangle$ denotes the cyclic subgroup generated by $a$. With the definition above, it is easy to see that this is the same as the subgroup generated by $\{a\}$. Thus the notation is unambiguous.

(iii) If $A, B \subseteq G$, then we write $\langle A, B\rangle$ to mean $\langle A\cup B\rangle$. This subgroup is denoted $A \vee B$.

**Definition 1.3.** Let $A \subseteq G$. Define

$$\overline{A} = \left\{a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n} \mid n\in\mathbb{Z}_{\geq 0}, a_i\in A,\ k_i = \pm 1 \text{ for all } 0\leq i\leq n\right\}$$

Note that $n$ can vary and the $a_i$ may repeat. We form finite products of elements of $A$ because it would not make sense to form an infinite product of elements in a group. These finite products are called words. Note that $A$ is not required to be finite. We convey $\overline{\varnothing} = \{1\}$. This way $\overline{A}$ is never empty.

**Proposition 1.4.** *If $A$ is any subset of $G$, then $\langle A\rangle = \overline{A}$.*

*Proof.* We leave to the student to prove that $\overline{A}$ is a subgroup. It is clear that $A \subseteq \overline{A}$. Then $\langle A\rangle \subseteq \overline{A}$ since $\langle A\rangle$ is the smallest subgroup that contains $A$ and $\overline{A}$ is one of the groups that contain $A$. On the other hand, the product of any two elements of $A$ belongs to $\langle A\rangle$ because $\langle A\rangle$ contains $A$ and it is closed under products. However, $\overline{A}$ consists exactly of any finite product of elements of $A$. Hence it easy follows $\overline{A} \subseteq \langle A\rangle$. The proof is complete. $\square$

**Remark 1.4.1.** In light of this result, we write

$$\langle A \rangle = \left\{ a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \mid n \in \mathbb{Z}^+, a_i \in A, \, k_i \in \mathbb{Z} \text{ and } a_i \neq a_{i+1} \text{ for any } 1 \leq i \leq n \right\}$$

## 2. Normality, quotient groups and homomorphisms

A useful reference for this section is Hungerford, chapter 1, section 5.

There are two standard groups associated to any group-homomorphism: its kernel and its image. These are important concepts that you need to master.

**Definition 2.1.** Let $\psi\colon G \to H$ be a morphism of groups. The kernel of $\psi$ is

$$\operatorname{Ker} \psi = \{ g \in G \mid \psi(g) = 1_H \} .$$

The image of $\psi$ is

$$\operatorname{Im} \psi = \{ \psi(g) \mid g \in G \}$$

**Exercise 1** (Classwork). With $\psi$ as above, prove $\operatorname{Ker} \psi \leq G$ and $\operatorname{Im} \psi \leq H$.

**Proposition 2.2.** *Let $\psi\colon G \to H$ be a group-homomorphism.*

*(i)* $\psi(1_G) = 1_H$

*(ii)* $\psi(g^{-1}) = (\psi(g))^{-1}$

*(iii)* $\psi(g^n) = (\psi(g))^n$

*Proof.* See Dummit & Foote, page 75. □

The only way to interpret $\psi(g)^{-1}$ is as the inverse of $\psi(g)$. Thus we may drop the parenthesis in $(\psi(g))^{-1}$.

**Theorem 2.3.** *Let $N \leq G$. The following conditions are equivalent.*

*(i) Left congruence modulo $N$ and right congruence modulo $N$ define the same partition of $G$.*

*(ii) For any $g \in G$, $Ng = gN$.*

*(iii) For any $g \in G$, $gNg^{-1} \subseteq N$. Here $gNg^{-1} = \{gxg^{-1} \mid x \in N\}$.*

*(iv) For any $g \in G$, $gNg^{-1} = N$. This means any $g \in G$ normalizes $N$.*

**Definition 2.4.** If $N \leq G$ satisfies $gNg^{-1} = N$ for any $g \in G$, then we say $N$ is a normal subgroup of $G$. In this case we use the notation $N \trianglelefteq G$.

By the previous result, $N$ is normal if it satisfies any of the equivalent conditions of Theorem 2.3. The easiest way to verify a subgroup is normal is condition (iii). Thus

$$N \trianglelefteq G \iff gNg^{-1} \subseteq N$$

for any $g \in G$.

**Proposition 2.5.** *The kernel of any group-homomorphism is a normal subgroup.*

*Proof.* Classwork. □

**Question 1.** Is the image a normal subgroup?

**Theorem 2.6.** *Let $K$ and $N$ be subgroups of a group $G$ with $N \trianglelefteq G$. Then*

*(i)* $N \cap K \trianglelefteq K$

*(ii)* $N \trianglelefteq N \vee K$

*(iii)* $NK = N \vee K = KN$

*(iv) If $K$ is normal in $G$ and $K \cap N = \{e\}$, then $nk = kn$ for all $k \in K$ and $n \in N$.*

**Exercise 2.** Provide examples that show when these conditions fail if $N$ is not required to be normal in $G$.

*Proof.* (i) We have to prove that $a(N \cap K)a^{-1} \subseteq N \cap K$ for any $a \in K$. Let $n \in N \cap K$ and $a \in K$. Then $ana^{-1} \in N$ because $N \trianglelefteq G$. Since $n, a \in K$ and $K \leq G$, we have $ana^{-1} \in K$. Thus $ana^{-1} \in N \cap K$.

(ii) Trivial (Why? Note $N \leq N \vee K$)

(iii) Exercise

(iv) Exercise

□

**Exercise 3.** Prove (iii) and (iv) of the preceding theorem.

We have introduced normal subgroups for a reason: to make the quotient set of a group by a (normal) subgroup into a group. In this way we can build new groups out of old. Regarding the quotient set $G/N$, two elements of $G$, say $g$ and $g'$ define the same equivalence class precisely when $g' = gn$ for some $n \in N$, equivalently when $g^{-1}g' \in N$. The condition that $N$ be normal is precisely what we need to get a well-defined way of multiplying these equivalence classes.

**Theorem 2.7.** *If $N \trianglelefteq G$, then*

$$G/N = \{ \, xN \mid x \in G \, \}$$

*is a group under the operation $(xN)(yN) = (xy)N$. Moreover, the order of $G/N$ is $|G : N|$.*

*Proof.* It suffices to show that the operation is well-defined, that is, whenever we multiply two equivalence classes we must always get the same result no matter the representatives chosen.

If $aN = xN$ and $bN = yN$, then $ax^{-1} = m \in N$ and $by^{-1} = n \in N$ for some $m, n \in N$. Our goal is to prove that $abN = xyN$, i.e., that $(ab)(xy)^{-1} \in N$. Note

$$(ab)(xy)^{-1} = aby^{-1}x^{-1} = anx^{-1} = (ana^{-1})ax^{-1} = (ana^{-1})m.$$

Since $N$ is normal, $aNa^{-1} \subseteq N$ so $ana^{-1} \in N$; and we already knew $m \in N$. Because $N$ is closed under products, $(ana^{-1})m \in N$. This part of the proof is complete. The student should verify that the order of $G/N$ is $|G : N|$. $\square$

You may want to take look at this post.

**Remark 2.7.1.** In additive notation,

(i) $G/N = \{g + N \mid g \in G\}$

(ii) $(a + N) + (b + N) = (a + b) + N$

The next result states that the kernel of any group-homomorphism is a normal subgroup, and that given normal subgroups occur as kernels.

**Theorem 2.8.**

*(i) If $f : G \to H$ is a group-homomorphism, then $\operatorname{Ker} f \trianglelefteq G$.*

*(ii) Conversely, if $N \trianglelefteq G$, then the map (called canonical projection) $\pi : G \to G/N$ defined by $a \mapsto aN$ is an surjective group-homomorphism with*

$$\operatorname{Ker} \pi = N.$$

*Proof.* (i) If $x \in \operatorname{Ker} f$ and $a \in G$, then

$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)1_H f(a^{-1}) = 1_H$$

meaning $axa^{-1} \in \operatorname{Ker} f$. Thus $a \operatorname{Ker} f a \subseteq \operatorname{Ker} f$ for any $a \in G$.

(ii) Is is clear that $\pi$ is surjective. (Make sure it is clear to you.) Further, $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$ so $\pi$ is a morphism of groups. Finally,

$$\begin{aligned}\operatorname{Ker} \pi &= \{a \in G \mid \pi(a) = 1_{G/N}\} \\ &= \{a \in G \mid aN = N\} \\ &= N.\end{aligned}$$

The proof is complete. $\square$

The next results tell us how to factor a group-homomorphism.

**Theorem 2.9.** *If $f : G \to H$ is a group homomorphism and $N \trianglelefteq G$ is a subgroup contained in $\operatorname{Ker} f$, then there is a unique group-homomorphism $\overline{f} \colon G/N \to H$ such that $f = \overline{f} \circ \pi$, i.e., such that the following diagram commutes.*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/N \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

*In addition,*

*(i)* $\operatorname{Im} f = \operatorname{Im} \overline{f}$,

*(ii)* $\operatorname{Ker} \overline{f} = \operatorname{Ker} f / N$, *and*

*(iii)* $\overline{f}$ *is an isomorphism if and only if* $f$ *is an epimorphism and* $N = \operatorname{Ker} f$.

*Proof.* Define $\overline{f}\colon G/N \to H : aN \mapsto f(a)$. Then $\overline{f}$ is well-defined, for if $aN = bN$, then $ab^{-1} \in N \leq \operatorname{Ker} f$, whence $f(ab^{-1}) = 1_H$ and so $f(a) = f(b)$. Moreover

$$\overline{f}((aN)(bN)) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

Finally,

(i) $f(a) \in \operatorname{Im} f$ if and only if $f(a) = \overline{f}(aN) \in \operatorname{Im} \overline{f}$. Hence $\operatorname{Im} f = \operatorname{Im} \overline{f}$.

(ii) Note

$$\begin{aligned} \operatorname{Ker} \overline{f} &= \{x \in G/N \mid \overline{f}(x) = 1_H\} \\ &= \{aN \mid f(a) = 1_H\} \\ &= \{aN \mid a \in \operatorname{Ker} f\} \\ &= \operatorname{Ker} f / N \end{aligned}$$

(iii) By (i), $\overline{f}$ is epic if and only if $f$ is. Note $\overline{f}$ is monic if and only if $\operatorname{Ker} \overline{f} = \{1_{G/N}\} = \{N\}$ if and only if $\operatorname{Ker} f / N = \{N\}$ if and only if $\operatorname{Ker} f = N$. (Keep in mind that $N \trianglelefteq \operatorname{Ker} f$ by hypothesis, and $\operatorname{Ker} f / N = N$ implies $aN = N$ for all $a \in \operatorname{Ker} f$.) Hence the result.

The proof is now complete. $\square$

**Exercise 4.** Prove that if $|G/N| = 1$, then $G = N$.

The important relationship between group-homomorphisms and quotient groups (also called factor groups) is a consequence of the result just proven.

**Corollary 2.10** (First Isomorphism Theorem)**.** *If* $f\colon G \to H$ *is a group-homomorphism,*

$$G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

*Proof.* Let $\psi\colon G \to \operatorname{Im} f : g \mapsto f(g)$. This way we force $\psi$ to be surjective. Now apply Theorem 2.9 with $\psi$ and $N = \operatorname{Ker} \psi$. Clearly $\operatorname{Ker} \psi = \operatorname{Ker} f$. The following diagram commutes.

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[d, "\pi"'] & \operatorname{Im} f \\ G/\operatorname{Ker} f \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

$\square$

The Diamond Theorem says that we can cancel out by paying off the intersection.

**Corollary 2.11** (Second Isomorphism Theorem (Diamond Theorem))**.** *If $K, N \leq G$ and $N \trianglelefteq G$, then*
$$\frac{NK}{N} \cong \frac{K}{N \cap K}.$$

*Proof.* We know $N \trianglelefteq NK$ by Theorem 2.6. Let $f = \pi \circ \iota$, where
$$K \xhookrightarrow{\iota} NK \xrightarrow{\pi} \tfrac{NK}{N}$$

Note $f$ is a group-homomorphism with $\operatorname{Ker} f = K \cap N$. Indeed,
$$\begin{aligned} \operatorname{Ker} f &= \{x \in K \mid f(x) = N\} \\ &= \{x \in K \mid xN = N\} \\ &= \{x \in K \mid x \in N\} \\ &= K \cap N, \end{aligned}$$

where we have used
$$xN = N \ \text{ if and only if } \ x \in N.$$

Let us see $f$ is epic. Let $nkN \in NK/N$. The normality of $N$ implies that $nkN = Nnk = Nk$, so
$$nkN = Nk = f(k).$$

Hence $\operatorname{Im} f = NK/N$ and by the First Isomorphism Theorem,
$$\frac{K}{N \cap K} \cong \frac{NK}{N}.$$

End of the proof. □

**Corollary 2.12** (Third Isomorphism Theorem)**.** *If $H, K \trianglelefteq G$ and $K \leq H$, then*
$$\frac{H}{K} \trianglelefteq \frac{G}{K} \quad \textit{and} \quad \frac{G/K}{H/K} \cong \frac{G}{H}.$$

*Proof.* (i) Prove that $\frac{H}{K} \trianglelefteq \frac{G}{K}$.

(ii) Define $\psi\colon G/K \to G/H : gK \mapsto gH$ and prove $\psi$ is a well-defined epic homomorphism.

(iii) By the First Isomorphism Theorem,
$$\frac{G/K}{\operatorname{Ker} \psi} \cong G/H.$$

(iv) Notice that
$$\begin{aligned} \operatorname{Ker} \psi &= \{gK \mid g \in G,\ \psi(gK) = 1_{G/H}\} \\ &= \{gK \mid g \in G,\ gH = H\} \\ &= \{gK \mid g \in H\} \\ &= H/K \end{aligned}$$

and conclude.

□

There is still one more isomorphism theorem.

**Corollary 2.13.** *Let $N \trianglelefteq G$. There is a one-to-one correspondence between subgroups of $G$ that contain $N$ and subgroups of $G/N$. In particular, every subgroup of $G/N$ is of the form $A/N$ with $N \leq A \leq G$. Furthermore, for all $A, B \leq G$ such that $N \leq A$ and $N \leq B$, it holds*

*(i) $A \leq B$ if and only if $A/N \leq B/N$, and*

*(ii) $A \trianglelefteq G$ if and only if $A/N \trianglelefteq G/N$.*

*Proof.* Trivialito. (If it is not clear, then the proof is left as an exercise.) □

**Exercise 5.** With the notations as in the statement of the Fourth Isomorphism Theorem, prove

(i) if $A \leq B$, then $|B : A| = |B/N : A/N|$

(ii) $\langle A, B\rangle/N = \langle A/N, B/N\rangle$

(iii) $(A \cap B)/N = A/N \cap B/N$

Here ends the group theory that you will see in this course.