

NORMAL SUBGROUPS

Definitions. We generalize the ideas above.

Proposition 1. Let (G, \circ) be a group, and $K \leq G$ be a subgroup. The following are equivalent:

- i. There exists a group homomorphism $\varphi : G \rightarrow H$ such that $K = \ker(\varphi)$.
- ii. $g \circ K = K \circ g$ for all $g \in G$.
- iii. The normalizer of K in G is $N_G(K) = G$.
- iv. $g \circ K \circ g^{-1} \subseteq K$ for all $g \in G$.

Any subgroup $K \leq G$ satisfying any of the equivalent statements above is said to be a *normal subgroup*. We write $K \trianglelefteq G$.

Proof. (i \implies ii) Assume that $K = \ker(\varphi)$ for some $\varphi : G \rightarrow H$. According to Proposition 2 above, $g \circ K = X_{\varphi(g)} = K \circ g$ for all $g \in G$.

(ii \iff iii) The normalizer of K in G is $N_G(K) = \{g \in G \mid g \circ K = K \circ g\}$. Hence $g \circ K = K \circ g$ for all $g \in G$ if and only if $N_G(K) = G$.

(ii \implies iv) Assume that $g \circ K = K \circ g$ for all $g \in G$. Fix $g \in G$, and consider $g \circ u \circ g^{-1}$ for $u \in K$. Then $g \circ u \in g \circ K = K \circ g$, so $g \circ u = v \circ g$, which means $g \circ u \circ g^{-1} = v \in K$. Hence $g \circ K \circ g^{-1} \subseteq K$ for all $g \in G$.

(iv \implies i) Assume that $g \circ K \circ g^{-1} \subseteq K$ for all $g \in G$. First we show that the collection of left cosets $H = \{\bar{g} = g \circ K \mid g \in G\}$ is a group. Consider the map $\circ : H \times H \rightarrow H$ which sends $(\bar{g}, \bar{h}) \mapsto \overline{g \circ h}$. We show this is well-defined. Say $\bar{g}_1 = \bar{g}_2$ and $\bar{h}_1 = \bar{h}_2$. Then $g_1 = g_2 \circ u$ and $h_1 = h_2 \circ v$ for some $u, v \in K$, so that

$$g_1 \circ h_1 = (g_2 \circ u) \circ (h_2 \circ v) = g_2 \circ h_2 \circ w \quad \text{where} \quad w = (h_2^{-1} \circ u \circ h_2) \circ v.$$

The element $h_2^{-1} \circ u \circ h_2 \in h_2^{-1} \circ K \circ h_2 \subseteq K$, so that $w \in K$. Hence $\overline{g_1 \circ h_1} = \overline{g_2 \circ h_2 \circ w} = \overline{g_2 \circ h_2} \circ \bar{w} = \overline{g_2 \circ h_2}$, so that \circ is a binary operation. Now we show that (H, \circ) is a group. Axiom (G1: Closure) holds because $\bar{g} \circ \bar{h} = \overline{g \circ h} \in H$. Axiom (G2: Associativity) holds because

$$(\bar{g} \circ \bar{h}) \circ \bar{k} = \overline{(g \circ h) \circ k} = \overline{g \circ (h \circ k)} = \bar{g} \circ (\bar{h} \circ \bar{k}).$$

Axiom (G3: Identity) holds because $\bar{e} = e \circ K = K$ is the identity. Axiom (G4: Inverses) holds because $\overline{g^{-1}} = g^{-1} \circ K$ is the inverse of $\bar{g} = g \circ K$. Finally, consider the map $\varphi : G \rightarrow H$ defined by $g \mapsto g \circ K$. Clearly this is a group homomorphism. The kernel is

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = \bar{1}\} = \{g \in G \mid g \circ K = K\} = \{g \in G \mid g \in K\} = K.$$

Hence K is indeed the kernel of some group homomorphism. □

Examples. Let (G, \circ) be a group.

- Let $G^c = \langle [g, h] \mid g, h \in G \rangle$ be the commutator subgroup. Then $N_G(G^c) = G$, so that $G^c \trianglelefteq G$.
- Let $H \leq Z(G)$ be a subgroup contained in the center of G . Then $N_G(H) = G$, so that $H \trianglelefteq G$ is normal in G . In particular, the center is normal in G .
- Say that $N, K \trianglelefteq G$ are normal in G . Then the meet $N \wedge K = N \cap K \trianglelefteq G$ is normal in G . Similarly, the join $N \vee K = \langle N \cup K \rangle \trianglelefteq G$ is also normal in G .

COUNTING COSETS

Definitions. Let (G, \circ) be a group, and $H \leq G$ be a subgroup. A *left coset* and *right coset* is a set in the form

$$g \circ H = \{g \circ h \mid h \in H\}, \quad H \circ g = \{h \circ g \mid h \in H\}$$

for any $g \in G$. Denote the collection of left cosets and right cosets by

$$G/H = \{\bar{g} = g \circ H \mid g \in G\}, \quad H \backslash G = \{H \circ g \mid g \in G\}.$$

The bimorphism $G/H \rightarrow H \backslash G$ defined by $g \circ H \mapsto H \circ g$ shows that there is a one-to-one correspondence between the left and right cosets of H in G . We have the *coset decomposition*

$$G = \bigcup_{g \in G} g \circ H = \bigcup_{g \in G} H \circ g.$$

Recall that $g \circ H = H \circ g$ for all $g \in G$ if and only if G/H is a group. The *index of H in G* is defined as the number of left cosets: $|G : H| = |G/H|$.

Example. Fix a positive integer n , and consider $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. The groups $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ are infinite, but G/H is finite. In fact, $|G : H| = n$.

Lagrange's Theorem. The following theorem computes the number of cosets when G is a finite group.

Proposition 2 (Lagrange's Theorem). *Let (G, \circ) be a finite group with identity e . Let $H \leq G$ be a subgroup.*

- (1) *The order $|H|$ divides the order $|G|$.*
- (2) *The number of left cosets is $|G : H| = |G|/|H|$.*
- (3) *$x^{|G|} = e$ for any $x \in G$.*

Lagrange's Theorem states that if G is finite, then any subgroup $H \leq G$ must have order dividing G . This limits the possibilities for the subgroups of a given group. For instance, if H is a nontrivial, proper subgroup of the dihedral group D_{2p} for a prime p , then either $|H| = 2$ or p . Such a subgroup H must be cyclic. Conversely, if m is an integer dividing $|G|$, then there does not have to exist a subgroup $H \leq G$ with $|H| = m$.

Proof. (1), (2) The set $\bar{G} = G/H$ forms a partition for G , so write G as a disjoint union

$$G = (g_1 \circ H) \cup (g_2 \circ H) \cup \dots \cup (g_n \circ H)$$

for some set of coset representatives g_k for elements in the set $\bar{G} = \{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_n\}$.

Fix $g \in G$, and consider the map $\varphi : H \mapsto g \circ H$ defined by $h \mapsto g \circ h$. This is an epimorphism i.e., a surjection. If $\varphi(h_1) = \varphi(h_2)$, then $g \circ h_1 = g \circ h_2$. Multiplying both sides by g^{-1} gives $h_1 = h_2$. Hence φ is a monomorphism i.e., an injection. This shows that φ is a bimorphism. In particular $|H| = |g \circ H|$, so that

$$|G| = |g_1 \circ H| + |g_2 \circ H| + \dots + |g_n \circ H| = \underbrace{|H| + |H| + \dots + |H|}_{n \text{ times}} = n |H|.$$

In particular, $|H|$ divides $|G|$, and $|G : H| = |\bar{G}| = n = |G|/|H|$.

- (3) Let $H = \langle x \rangle$, and denote $|H| = |x| = m$. Then we have $|G| = n |H| = mn$, so that

$$x^{|G|} = x^{mn} = (x^m)^n = e^n = e.$$

This completes the proof. □

ISOMORPHISM THEOREMS

First Isomorphism Theorem. We list the first of the four "Isomorphism Theorems."

Proposition 3 (First Isomorphism Theorem). *Let (G, \star) and (H, \diamond) be groups with identities 1_G and 1_H , respectively. Let $\varphi : G \rightarrow H$ be a group homomorphism.*

- (1) *$\ker(\varphi) \trianglelefteq G$ is a normal subgroup.*
- (2) *$G/\ker(\varphi) \simeq \text{im}(\varphi)$.*
- (3) *$|G : \ker(\varphi)| = |\varphi(G)|$.*

Proof. (1) This was shown earlier in the lecture.

(2) Denote $\bar{G} = G/\ker(\varphi)$, and consider the map $\bar{\varphi} : \bar{G} \rightarrow H$ defined by $\bar{g} \mapsto \varphi(g)$. Recall that (\bar{G}, \star) is a group. We show that this is a well-defined group homomorphism. If $\bar{g}_1 = \bar{g}_2$, then $g_1 = g_2 \star u$ for some $u \in \ker(\varphi)$. Then we have

$$\bar{\varphi}(\bar{g}_1) = \varphi(g_1) = \varphi(g_2 \star u) = \varphi(g_2) \diamond \varphi(u) = \varphi(g_2) \diamond 1_H = \varphi(g_2) = \bar{\varphi}(\bar{g}_2).$$

For $\bar{g}, \bar{h} \in \bar{G}$, we have

$$\bar{\varphi}(\bar{g} \star \bar{h}) = \bar{\varphi}(\overline{g \star h}) = \varphi(g \star h) = \varphi(g) \diamond \varphi(h) = \bar{\varphi}(\bar{g}) \diamond \bar{\varphi}(\bar{h}).$$

The map $\bar{\varphi} : \bar{G} \rightarrow H$ is surjective onto $\text{im}(\varphi) \subseteq H$, so it suffices to show that $\bar{\varphi}$ is injective. Say that $\bar{\varphi}(g_1) = \bar{\varphi}(g_2)$. Then $\varphi(g_1) = \varphi(g_2)$, so that $\varphi(g_2^{-1} \star g_1) = \varphi(g_2)^{-1} \diamond \varphi(g_1) = 1_H$. Hence $g_2^{-1} \star g_1 = u \in K$, so that $g_1 = g_2 \star u$. This shows that $\bar{g}_1 = \bar{g}_2$.

(3) The map $\bar{\varphi} : G/\ker(\varphi) \rightarrow \varphi(G)$ is an isomorphism, so $|G/\ker(\varphi)| = |\varphi(G)|$. \square

Second Isomorphism Theorem. A subgroup $K \trianglelefteq G$ is a normal subgroup of G if and only if $N_G(K) = G$. Say that $H \leq G$ is a subgroup. If $K \subseteq H$, then we may ask if $K \trianglelefteq H$ is a normal subgroup of H .

Proposition 4. Let (G, \circ) be a group and $H \leq G$ be a subgroup. Then the following are equivalent for a subgroup $K \leq H$:

- i. $K \trianglelefteq H$ is a normal subgroup of H .
- ii. $N_H(K) = H$.
- iii. $H \leq N_G(K)$.

Proof. (i \iff ii) If $K \trianglelefteq H$, then $g \circ K = K \circ g$ for all $g \in H$. This is equivalent to $N_H(K) = H$.

(ii \iff iii) The normalizer of K in H is

$$N_H(K) = \{g \in H \mid g \circ K = K \circ g\} = \{g \in G \mid g \circ K = K \circ g, g \in H\} = N_G(K) \cap H.$$

If $N_H(K) = H$ then $H = N_H(K) \leq N_G(K)$. Conversely, if $H \leq N_G(K)$ then $N_H(K) = N_G(K) \cap H = H$. \square