

5. NORMAL SUBGROUPS, QUOTIENT GROUPS, AND THE ISOMORPHISM THEOREMS

Let G be a group (or semigroup). Then the collection $\mathcal{P}(G)$ of subsets of G forms a semigroup when we define $XY = \{xy \mid x \in X, y \in Y\}$. Left and right cosets of a subgroup H are special cases of this, except that we write Ha for $H\{a\}$ and aH in place of $\{a\}H$. We similarly write aHb for $\{a\}H\{b\}$.

If e is the identity of G , then $\{e\}$ is the identity of $\mathcal{P}(G)$. However, $\mathcal{P}(G)$ is very far from being a group. For example, in a group, if $x^2 = x$ then x is the identity. However, if H is a subgroup of G , then $HH = H$. However, H is not the identity of $\mathcal{P}(G)$ unless $H = \{e\}$. We are generally not interested in all of $\mathcal{P}(G)$, but rather special subsets of it that form a group.

Problem 5.A. Let H be a nonempty subset of the group G . Show that H is a subgroup iff $HH = H$.

We are interested in the following problem: if \sim is an equivalence relation, when do the equivalence classes under \sim form a group? This question arises in the following way. We know for each $a, b \in G$, we have equivalence classes \bar{a}, \bar{b} . Since ab is in the product $\bar{a}\bar{b}$, if this product is an equivalence class it must be the equivalence class \overline{ab} . This would give us the very attractive formula $\bar{a} \cdot \bar{b} = \overline{ab}$.

We have already seen an example of this. Let \sim be the equivalence relation $\equiv \pmod{n}$ on \mathbb{Z} . The group $(\mathbb{Z}_n, +)$ can be viewed as the collection of equivalence classes \bar{a} where a is an integer, and we add according to the formula $\bar{a} + \bar{b} = \overline{a + b}$. Thus \mathbb{Z}_n will be seen to be a special case of a very general construction.

The above formula has another appealing feature. If H is the collection of equivalence classes, then the map $a \mapsto \bar{a}$ will be a group homomorphism from G onto H .

In pursuing this idea of making equivalence classes into a group, we are engaging in a very common practice in mathematics. For example, in topology, one sometimes thinks of forming a cylinder by identifying two parallel sides of a rectangle. Such an identification comes from an equivalence relation. If we also identify the other two sides of the rectangle, the result is a torus, or colloquially, a donut. (We use a solid rectangle, but the we get only the surface of the resulting cylinder or torus.) If we identify two parallel sides of a rectangle “backwards” (say we identify the top left with the bottom right), we obtain a Möbius band.

Before we study the question of when the equivalence classes form a group, it is convenient to introduce some terminology. As indicated in the previous section, we say a subgroup N of G is *normal* if $aN = Na$ for all $a \in G$, and we write $N \triangleleft G$ in this case.

Lemma 5.1. *Let N be a subgroup of G . Then the following conditions are equivalent.*

- (1) $N \triangleleft G$.
- (2) $aN \subseteq Na$ for all $a \in G$.
- (3) $Na \subseteq aN$ for all $a \in G$.
- (4) $gNg^{-1} = N$ for all $g \in G$.
- (5) $gNg^{-1} \subseteq N$ for all $g \in G$.
- (6) $N \subseteq gNg^{-1}$ for all $g \in G$.

Remark. It is very important that the given conditions hold for *all* a or g in G . It is possible to have $gNg^{-1} \subseteq N$ (equivalently, $gN \subseteq Ng$) for a particular $g \in G$ without having $gNg^{-1} = N$ (equivalently, $gN = Ng$).

Proof. Because $\mathcal{P}(G)$ is a semigroup with identity $\{e\}$, it is easy to see that (1) and (4) are equivalent, (2) and (5) are equivalent, and (3) and (6) are equivalent. For example, if $aN \subseteq Na$, then $aNa^{-1} \subseteq Naa^{-1} = N$, and the reverse calculation is valid as well.

Furthermore, since we can replace a or g by a^{-1} or g^{-1} respectively (this is possible because the statements are supposed to hold for all a or all g), it is easy to see that (2) and (3) are equivalent and (5) and (6) are equivalent. For example, if (2) holds, then we have $a^{-1}N \subseteq Na^{-1}$, whence $Na = a(a^{-1}N)a \subseteq a(Na^{-1})a = aN$.

Finally, it is obvious that (1) is equivalent to (2) and (3), and that (4) is equivalent to (5) and (6). The observation in the last paragraph shows (2) implies (2) and (3) and hence (2) implies (1). A similar argument for the remaining implications finishes the proof. (Or maybe we're already finished if we look at what we've done.) ■

Problem 5.B. Let G be a group.

- (1) Justify the following fact, which was implicitly used in the last proof. If $A, B, C, D \subseteq G$, and $A \subseteq B$, then $CA \subseteq CB$, $AD \subseteq BD$, and $CAD \subseteq CBD$.
- (2) Show that we can strengthen Lemma 5.1 as follows: a subgroup N is normal in G iff every right coset of N is also a left coset.

Let us return to the problem of making equivalence classes into a group. If N is a normal subgroup of G , then right and left cosets of N are the same, and they are the equivalence classes of the relation \equiv_N . Let G/N denote the set of cosets of N in G . We will show that the elements of G/N form a group, which we call the *quotient group* of G by N (or of G modulo N).

If $a, b \in G$, then $(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab$, where we used normality after the second $=$ and the fact that N is a subgroup after the last $=$. If we write $\bar{a} = Na$, this shows the formula $\bar{a}\bar{b} = \overline{ab}$ is valid in this case. We know multiplication in G/N is associative since it is a subset of $\mathcal{P}(G)$, where multiplication is associative. However, G/N will not be a subgroup of $\mathcal{P}(G)$. Indeed, the identity in G/N is N since $NNa = Na$ and $NaN = NNa = Na$. Finally, $(Na)^{-1} = Na^{-1}$. (If we defined X^{-1} in the obvious way for any subset X , we would have $(Na)^{-1} = a^{-1}N^{-1} = a^{-1}N = Na^{-1}$ also. But note that $XX^{-1} \neq \{e\}$ in general.)

Proposition 5.2. *Let G be a group and let $N \triangleleft G$. Then the set G/N of cosets of N in G forms a group with operation $NaNb = Nab$. The function $\phi : G \rightarrow G/N$ defined by $\phi(g) = Ng$ is a group homomorphism onto G/N , and if $a, b \in G$, then $\phi(a) = \phi(b)$ iff $Na = Nb$.*

Proof. Everything in the proposition has been proved (the last claim follows instantly from the definition of ϕ). ■

The quotient group construction G/N is an example of making equivalence classes into a group. The next problem shows that it is the only example.

Problem 5.C. Let G be a group and let \sim be an equivalence relation on G such that the set $H = G/\sim$ of equivalence classes of \sim becomes a group under the multiplication on $\mathcal{P}(G)$ (i.e., $\bar{a}\bar{b} = \overline{ab}$). Prove that (a) $N = \bar{e}$ is a normal subgroup of G , (b) the relation \sim is the same as the relation \equiv_N , and (c) $H = G/N$ as a group.

Hint: Set $N = \bar{e}$. Then $NN = \bar{e}\bar{e} = \bar{e} = N$ by hypothesis, so N is a subgroup. Use the fact that $geg^{-1} = e$ to show N is normal. This proves (a).

If $a \sim b$, then $\bar{a} = \bar{b}$. Use this to prove $ab^{-1} \in N$. Show conversely that if $ab^{-1} \in N$, then $a \sim b$. This proves (b).

Finally, observe that (c) follows from (a) and (b).

The quotient group construction, and the general construction of new objects by “identification” is not a trivial one. Don't be surprised if you need to work with these ideas for a while to become comfortable with them.

We have seen one example of the quotient construction: \mathbb{Z}_n is the same as (at least isomorphic to) the quotient group $\mathbb{Z}/n\mathbb{Z}$.

For another example, consider $G = S_3$ and $N = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. We showed in the last section that $N \triangleleft G$, so we can form the group G/N . We know the number of elements in G/N is $[G : N] = |G|/|N| = 2$. Since there is only one group with 2 elements, we conclude that G/N is the cyclic group with 2 elements ($G/N \cong \mathbb{Z}_2$). Note that the two elements of G/N are the set N of even permutations in S_3 and the set $G \setminus N$ of odd permutations in S_3 .

We have given an abstract reason for wishing to consider quotient groups, but there is also a concrete reason. They enable us to display a lot of isomorphisms between groups. We turn next to a set of results known as “The Isomorphism Theorems”. Of these, the first is the most important. It is central to the study of groups and it has analogues that are just as central in the study of rings, vector spaces, and other algebraic systems.

Before we can state the result, we need another concept, which is also central to the study of algebraic systems. If $\phi : G \rightarrow H$ is a function of *sets*, then it can fail to be one-to-one because a single pair of elements has the same image under ϕ , or because ϕ causes numerous sets of elements to be identified. (In fact, we saw in the last section that this identification corresponds to an equivalence relation.) When ϕ is a homomorphism of groups, however, the failure of a function to be one-to-one is much more uniform.

Let $\phi : G \rightarrow H$ be a homomorphism of groups. We define the *kernel* of ϕ to be $\ker \phi = \{g \in G \mid \phi(g) = e\}$ and the *image* of ϕ to be $\text{im } \phi = \{\phi(g) \mid g \in G\}$. (Note that “image” is defined for any function, but “kernel” can only be defined when H is a group.)

Lemma 5.3. *Let $\phi : G \rightarrow H$ be a homomorphism of groups.*

- (1) $\ker \phi$ is a normal subgroup of G .
- (2) $\text{im } \phi$ is a subgroup of H .
- (3) If $a, b \in G$, then $\phi(a) = \phi(b)$ iff the cosets $(\ker \phi)a$ and $(\ker \phi)b$ are equal.

Proof. (1) Since $\phi(e) = e$, we have $e \in \ker \phi$. If $x, y \in \ker \phi$, then $\phi(xy) = \phi(x)\phi(y) = ee = e$, so $xy \in \ker \phi$. Moreover, $\phi(x^{-1}) = (\phi(x))^{-1} = e^{-1} = e$, so $x^{-1} \in \ker \phi$. This proves $\ker \phi$ is a subgroup.

If $g \in G, x \in \ker \phi$, then $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = e$. This proves $\ker \phi$ is normal in G .

- (2) Exercise.
- (3) Exercise. ■

Corollary 5.4. *Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then ϕ is one-to-one if and only $\ker \phi = \{e\}$.*

Proof. Exercise. ■

Example 5.5. (1) Consider the function $\det : GL_n(R) \rightarrow GL_1(R)$. Since 1 is the identity of $GL_1(R)$, the kernel of this map consists of all matrices of determinant 1. That is, $\ker \det = SL_n(R)$. This proves $SL_n(R) \triangleleft GL_n(R)$; of course it is easy to prove normality directly.

- (2) Consider the function $\phi : GL_1(\mathbb{C}) \rightarrow H$, where H is the multiplicative group of positive real numbers, defined by $\phi(z) = |z|$. Then $\ker \phi = U_1$, the circle group.
- (3) The function $\text{sgn} : S_3 \rightarrow \{\pm 1\}$ defined by taking the sign of a permutation has kernel $N = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$. For general n , we have a sign map $\text{sgn} : S_n \rightarrow \{\pm 1\}$; its kernel consists of all even permutations in S_n . We denote $\ker \text{sgn}$ by A_n and call this the *alternating group* of degree n . Of course $A_n \triangleleft S_n$.

Theorem 5.6 (First Isomorphism Theorem). *Let $\phi : G \rightarrow H$ be a homomorphism of groups. Then $G/\ker \phi \cong \text{im } \phi$.*

Proof. We will explicitly construct the isomorphism. For ease of notation, set $K = \ker \phi$ and $L = \text{im } \phi$.

Define $\psi : G/K \rightarrow L$ by $\psi(Kg) = \phi(g)$. By Lemma 5.3, $\phi(g) = \phi(g')$ iff $Kg = Kg'$, so ψ is both well-defined and one-to-one. Plainly $\text{im } \psi = \text{im } \phi = L$, so ψ is onto. Finally, $\psi(KaKb) = \psi(Kab) = \phi(ab) = \phi(a)\phi(b) = \psi(Ka)\psi(Kb)$, whence ψ is an isomorphism of groups. ■

Example 5.7. All the homomorphisms in Example 5.5 are onto. Therefore we can apply the first isomorphism theorem as follows.

- (1) $GL_n(R)/SL_n(R) \cong GL_1(R)$.
- (2) $GL_1(\mathbb{C})/U_1$ is isomorphic to the multiplicative group of positive real numbers.
- (3) $S_n/A_n \cong \{\pm 1\}$, if $n \geq 2$.

Here is another example that illustrates the power of the First Isomorphism Theorem. Let H be any cyclic group, say $H = \langle x \rangle$. Then we can define a homomorphism $\phi : \mathbb{Z} \rightarrow H$ by $\phi(m) = x^m$, and this homomorphism is onto. Thus $H \cong \mathbb{Z}/\ker \phi$. If H is infinite, then ϕ is one-to-one and we obtain $\mathbb{Z} \cong H$ (yes?). If $|H| = n$ is finite, then $\text{ord } h = n$, and $\ker \phi = n\mathbb{Z}$. Hence $H \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Thus we have re-proved the theorem that any two cyclic groups of the same order are isomorphic.

We will state but not prove the Second and Third Isomorphism Theorems. At least part of the proof of each one involves applying the First Isomorphism Theorem.

Proposition 5.8 (Second Isomorphism Theorem). *Let G be a group and N a normal subgroup. For a subgroup H of G , define $H/N = \{Nh \mid h \in H\}$. (This notation is typically only used when $N \subseteq H$, in which case it corresponds to the usual quotient group H/N .)*

- (1) *There is a bijective correspondence between subgroups of G containing N and subgroups of G/N , given by $H \mapsto H/N$. Moreover, $H \triangleleft G$ iff $H/N \triangleleft G/N$.*
- (2) *If $H \triangleleft G$ and $N \subseteq H$, then $(G/N)/(H/N) \cong G/H$.*

Proof. Exercise. ■

As an example, Proposition 5.8 tells us that $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong \mathbb{Z}_3$. However, $\mathbb{Z}_{12}/5\mathbb{Z}_{12} \not\cong \mathbb{Z}_5$: what's the difference?

Proposition 5.9 (Third Isomorphism Theorem). *Let G be a group, H, N be subgroups, and suppose $N \triangleleft G$. Then HN is a subgroup of G , $N \triangleleft HN$, $H \cap N \triangleleft H$, and $HN/N \cong H/(H \cap N)$.*

Proof. Exercise. ■

INDEX OF DEFINITIONS

alternating group, 3

image, 3

kernel, 3

normal, 1

quotient group, 2