At the end of **??**, we briefly discussed homomorphisms. We shall now study a closely related concept: normal subgroups. The study of normal subgroups is closely connected with the study of group homomorphisms.

Definition 0.1 (Normal subgroup). A subgroup N of a group G is **normal** if for all $g \in G$,

$$gN = Ng.$$

Notationally, we will write $N \trianglelefteq G$. When we wish to additionally say that $N \neq G$, we shall write $N \triangleleft G$.

That is to say, the left coset of N is equal to the right coset of N. An equivalent criterion is given below, which may be taken to be the definition of normality. The definition above was chosen due to ease of application.

Lemma 0.2. *Let G be a group and N a subgroup of G. Then N is normal in G if and only if for all $g \in G$,*

$$gNg^{-1} \subseteq N.$$

Proof. See Exercise 0.3. □

Exercise 0.3. Prove Lemma 0.2

Warning. *This does not imply that $gn = ng$ for every $n \in N$.*

Let us now see examples of normal subgroups.

Example 0.4. Any subgroup of an Abelian group is normal. Moreover, any nontrivial group always has at least 2 normal subgroups. Which ones?[1] //

Example 0.5. Let $D_4 = \langle s, r : r^4 = s^2 = 1, sr^j = r^{-j}s\rangle$ be the dihedral group of order 8. Then D_4 has a normal subgroup, namely $N = \langle r\rangle$, the subgroup of rotations. This will actually follow from Example 0.7, but we can directly verify this fact here. Let us pick $g \in D_4$, and notice that if g is a pure rotation, $gN \in N$ and so $gN = Ng$. Let us assume that $g = s$ (the general case follows easily from this - why?), then using the group relation $sr^j = r^{-j}s$, we quickly observe that $sN = Ns$. //

At this point, the reader may be wondering whether "is a normal subgroup of" is a transitive relation. This may feel intuitively true; after all, the relation of being a subgroup of is in fact transitive. Unfortunately, this is untrue.

Example 0.6 (Normality is not transitive)**.** Let $G = D_4$. Let $H = \langle r^2, s\rangle$ and let $K = \langle s\rangle$. Then $K \trianglelefteq H \trianglelefteq G$, but K is not normal in G, since $rsr^{-1} = sr^2 \notin K$. //

Example 0.7 (Index 2 subgroups are normal)**.** Any subgroup of index 2 is normal. In other words, if H is a subgroup of G, and $|G/H| = 2$, then H is normal in G. See Exercise 0.34 for more details. //

Example 0.8 (Alternating group)**.** Recall that A_n is the alternating group, the subgroup of all the even permutations in S_n. Leveraging Example 0.7, we can swiftly say that A_n is normal in S_n. //

Recall that given subgroups H, K of a group G, it may not be true that HK is a subgroup of G. However, if H is instead a normal subgroup of G, then this will be true.

Example 0.9 ("Product" of subgroup with a normal subgroup is a subgroup)**.** Let H be normal in G and K a subgroup of G. Of course HK is nonempty. Given elements $a = h_1k_1, b = h_2k_2 \in HK$, we notice that $ab^{-1} = h_1(k_1k_2^{-1}h_2^{-1})$. Consider the expression in parentheses. Since H is normal in G there is some h' such that $k_1k_2^{-1}h_2^{-1} = h'k_1k_2^{-1}$. So this means $ab^{-1} = h_1h'k_1k_2^{-1}$ which is in HK.

We have thus proven the following proposition: Let H be normal in G and K be a subgroup of G. Then, HK is a subgroup of G. //

Warning. *If H is not normal, then HK may not be a subgroup. Let $G = D_3$, let $H = \{e, s\}$ and let $K = \{e, rs\}$. Then, $HK = \{e, s, rs, srs = r^{-1}\}$, which cannot be a subgroup due Lagrange's Theorem.*

0.1 Quotient groups

We have previously discussed a product of groups. This concept was rather simple. But what about the quotient of groups. Can we "divide" a group by another group?

[1] The whole group and the trivial subgroup.

To explain the concept of quotient groups, we shall turn first to modular arithmetic. Let us consider the set $\mathbb{Z}$, and we declare the equivalence relation $x \sim y$ if and only if $x \mod 3 = y \mod 3$. This partitions $\mathbb{Z}$ into the following sets:

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{ 0, \pm 3, \pm 6, \cdots \} \\ 1 + 3\mathbb{Z} &= \{ 1, \pm 4, \pm 7, \cdots \} \\ 2 + 3\mathbb{Z} &= \{ 2, \pm 5, \pm 8, \cdots \} . \end{aligned}$$

When we add 1 and 1 modulo 3, we get 2 modulo 3. Notice that if we add up the stuff in the set $1 + 3\mathbb{Z}$ to themselves, we also obtain $2 + 3\mathbb{Z}$. This suggests that we should perhaps define the group operation in $\mathbb{Z}/\sim$ by setting $(x + N) + (y + N) = x + y + N$, where $N = 3\mathbb{Z}$.

Can we replicate this construction for any subgroup of $\mathbb{Z}$ whatsoever? It turns out that the answer is yes. What about for a general group? Can we replicate this idea? Yes, but we would require that the subgroup be normal. Of course, in abelian groups, every subgroup is normal. But it turns out that in order for the operation to be well defined it was sufficient to assume that the subgroup is normal.

Theorem 0.10 (Existence of quotient groups)**.** Let G be a group and N be a normal subgroup of G. Then the set G/N with the operation $(xN)(yN) := xyN$ is a group.

Proof. We first show that this operation is well defined. Suppose $xN = x'N$ and $yN = y'N$. Then there is some $n_1, n_2 \in N$ such that $x' = xn_1, y' = yn_2$. So $x'y'N = xn_1yn_2N = xn_1yN = xn_1Ny = xyN$. (Recall that in **??** we proved some properties about cosets). We leave it to the reader to verify that this operation is associative, has identity and inverses. □

Interestingly enough, the converse is true: If the operation $xNyN := xyN$ defines a group (on the set of left cosets G/N), then N is normal in G. We leave this as a good exercise in Exercise 0.27. Additionally, note that if N is not normal, then the product operation as defined there may not yield a left coset.

Example 0.11. In S_3, let $H = \{ (1), (12) \}$. Then $(13)H(23)H$ is not equal to $(13)(23)H$. //

We now make some remarks about notation. It may seem confusing that $gNhN = ghN$, but since G/N is a group, we should view gN and hN as elements of the group G/N. If you find this confusing, you may instead treat gN as $\tilde{g}$ and $\tilde{h}$, although be aware that this technique may lead to you forgetting about the properties of cosets.

The next theorem gives us a criterion for determining if G is not Abelian.

Theorem 0.12. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof. Firstly, $Z(G)$ is normal (Exercise 0.25). If G is Abelian then $Z(G) = G$, it thus suffices to show that $G/Z(G)$ is the trivial group. Suppose $gZ(G)$ generates $G/Z(G)$. If $a \in G$, then $aZ(G) = g^iZ(G)$ for some i, so that $a = g^iz$ for some $z \in Z(G)$. We observe that this implies a commutes with g, since g^i and z both commute with g. But this shows that every element of G commutes with g, so that $g \in Z(G)$. □

The quotient group $G/Z(G)$ is also useful for other purposes.

Proposition 0.13. Let G be a group. Then $G/Z(G)$ is isomorphic to $\mathrm{Inn}(G)$.

0.2 Homomorphisms and the first isomorphism theorem

Recall that we defined group homomorphisms in **??**. We now undertake a deeper study of them.

First, let us start with a definition that is likely familiar to you, if you've had linear algebra.

Definition 0.14 (Kernel of a homomorphism)**.** Let $\phi : G \to H$ be a group homomorphism. The **kernel of** ϕ is the set of all g which are mapped to the identity by ϕ;

$$\ker\phi := \{\, g \in G : \phi(g) = e \,\}\,.$$

The image of a homomorphism will be simply denoted $\phi[G]$, since it is not sufficiently important in group theory to get a special designation. Let us now see a few more properties of homomorphisms. Recall that we have proven more properties previously on **??** and **??**.

Proposition 0.15. Let $\phi : G \to H$ be a homomorphism. Then, the following properties are true:

1. $\ker\phi$ is a subgroup of G;
2. $\phi(g) = \phi(h)$ if and only if $g\ker\phi = h\ker\phi$.
3. If $h \in \phi[G]$ and $\phi(g) = h$, then $\phi^{-1}[\{\, h \,\}] = g\ker\phi$.
4. If N is normal in G, then $\phi[N]$ is normal in $\phi[G]$.
5. $\phi[Z(G)]$ is a subgroup of $Z(\phi[G])$.
6. If K is normal in H, then $\phi^{-1}[K]$ is normal in G.
7. If $\ker\phi$ is finite and has n things in it, then ϕ is an n to 1 mapping.

Proof. We leave the proof of (1) to the reader. For (2), notice that $\phi(g) = \phi(h)$ if and only if $\phi(gh^{-1}) = e$. This is true if and only if $gh^{-1} \in \ker\phi$, if and only if $g\ker\phi = h\ker\phi$. Everything else shall be left to the reader. □

The reader may have also observed that property (2) seems very indicative of a equivalence relation. See Exercise 0.28 for more details.

Property (6) of Proposition 0.15 can be used to deduce the following very important property of kernels.

Corollary 0.16 (Kernels are normal)**.** If ϕ is a homomorphism then $\ker\phi$ is normal.

Proof. Consider $\phi^{-1}[\{\, e \,\}]$. □

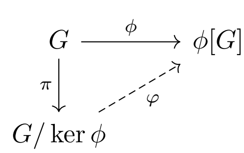
0.3 Isomorphism Theorems

We have previously mentioned that the study of normal subgroups is the same as the study of homomorphisms. Let us now make this notion precise with the First Isomorphism Theorem. This is sometimes called the Fundamental Theorem of Group Homomorphisms, which really goes to show just how important this theorem is.

Theorem 0.17 (First Isomorphism Theorem)**.** Suppose G is a group and $\phi : G \to H$ is a homomorphism. Then the group $G/\ker\phi$ is isomorphic to $\phi[G]$ by the isomorphism $\varphi(g\ker\phi) = \phi(g)$.

Proof. See Exercise 0.29. □

We may depict the relationship of this theorem with the following commutative diagram:



Here, π denotes the natural projection which sends the element g to the left coset $g\ker\phi$, i.e. $\pi(g) = g\ker\phi$. The commutative diagram can be read as saying that $\phi = \varphi \circ \pi$. We won't go into too much detail into how to read commutative diagrams here for now.

Using the first isomorphism theorem, we can turn back to our motivating example for the study of normal subgroups, and see what we mean by $\mathbb{Z}/3\mathbb{Z}$ is really just $\mathbb{Z}_3$.
Example 0.18. Let n be a positive integer. Define $\phi(m) = m \mod n$. Then ϕ is easily seen to be a (surjective) group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$ and the kernel of ϕ is $n\mathbb{Z}$. So the first isomorphism theorem tells us that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. //

The first isomorphism theorem makes computations involving kernels and homomorphisms much easier.
Example 0.19. Let G be the general linear group of 2 by 2 matrices over $\mathbb{R}$, and let N be the special linear group of 2 by 2 matrices over $\mathbb{R}$. Let ϕ be the determinant function. Notice that ϕ is a surjective group homomorphism onto the group of nonzero real numbers under multiplication, and the kernel of ϕ is precisely N. Thus this shows that G/N is isomorphic to the nonzero reals under multiplication. //

Although we have labelled the following as theorems, they really are corollaries to Theorem 0.17.

Theorem 0.20 (Second Isomorphism Theorem)**.** Suppose K is a subgroup of G, and N is normal in G. Then $K/(K \cap N)$ is isomorphic to KN/N.

Proof. See Exercise 0.30. Note that by Example 0.9, we have the fact that KN is a subgroup of G. □

Theorem 0.21 (Third Isomorphism Theorem)**.** Suppose M, N are normal in G and that N is a subgroup of M. Then $(G/N)/(M/N)$ is isomorphic to G/M.

Proof. See Exercise 0.31. □

The reader may be wondering whether all normal subgroups are kernels of some sort of homomorphism. The answer is yes. If N is a normal subgroup of G, let us define[2] $\pi : G \to G/N$ by $\pi(g) = gN$. We leave it to the reader (Exercise 0.32) to verify this is indeed a homomorphism, and it has kernel N.

We now make use of the concept of factor groups to prove the following useful theorem. This theorem is used to prove the Sylow Theorem's.

Theorem 0.22 (Cauchy's Theorem (for finite abelian groups))**.** Let G be a finite abelian group and let p be a prime that divides $|G|$. Then, G contains an element of order p.

Proof. We induct on the order of G. Let $|G| = n$. Clearly if $|G| = 1$ it is trivial. Suppose the statement is true when $|G| < n$. Let $a \in G$, $a \neq e$. If $|a| = r$ and p divides r, then the element $a^{r/p}$ has order p. If not, then p, r are coprime. Let us consider $G/\langle a \rangle$. This group has order $|G|/r$, and necessarily p divides the order of this group. Thus there is some $b\langle a \rangle \in G/\langle a \rangle$ which has order p. Let $|b| = s$; we claim p divides s. Indeed, $(a\langle a \rangle)^s = a^s\langle a \rangle = \langle a \rangle$, and $a^p\langle a \rangle = \langle a \rangle$. So p divides s. Now $b^{s/p}$ has order p. □

0.4 Exercises and Problems

Exercise 0.23. Let G be a group and let $x, y \in G$. Let H be a subgroup of G. Show that if $xH = Hy$, then $xHy^{-1} \subseteq H$.
Exercise 0.24 (Internal direct products)**.** Let G be a group. We say that G is the **internal direct product of** H **and** K and write $G = H \times K$ if

1. H, K are normal subgroups of G,
2. $HK = G$,
3. $H \cap K = \{ e \}$.

[2]The reason for the use of the symbol π is because we are essentially projecting the elements down to G/N. Sometimes this is called the natural homomorphism from G to G/N. I'm not sure if this is categorically natural, so let me know.

Note that this seemes similar to a vector space being a direct sum of subspaces.

Show that G is isomorphic to $H \times K$. This justifies the abuse of the group product notation. Extend this to the case where G is an internal direct product of a finite number of groups.

Exercise 0.25 (Center is always normal)**.** Let G be a group. Show that $Z(G)$ is normal subgroup of G. In addition, prove that if H is a subgroup of $Z(G)$, then H is normal in G.

Exercise 0.26 (Stronger version of Theorem 0.12)**.** Let G be a group. Let H be a subgroup of $Z(G)$. Show that if G/H is cyclic, then G is Abelian.

Exercise 0.27 (Converse of Theorem 0.10)**.** Suppose G is a group and N is a subgroup of G such that for all $x, y \in G$, we have $xNyN = xyN$. Show that N is normal.

Exercise 0.28. Let $\phi : G \to H$ be a homomorphism. Define the equivalence relation $\sim$ on G by $x \sim y$ if and only if $\phi(x) = \phi(y)$. Prove that $\sim$ is an equivalence relation, and the equivalence class $[g]_\sim$ is precisely $g \ker \phi$.

Exercise 0.29. Prove the First Isomorphism Theorem (Theorem 0.17).

Exercise 0.30. Prove the Second Isomorphism Theorem (Theorem 0.20).

Exercise 0.31. Prove the Third Isomorphism Theorem (Theorem 0.21).

Exercise 0.32 (Every normal subgroup is a kernel)**.** If N is a normal subgroup of G, let us define $\pi : G \to G/N$ by $\pi(g) = gN$. Prove that π is a homomorphism and it has kernel N.

Exercise 0.33. Prove that $\mathbb{Q}$ under addition has no proper subgroup with finite index.

Exercise 0.34 (Index 2 subgroups are normal)**.** Let G be a group and H be a subgroup such that $[G : H] = 2$. Prove that H is normal in G. *Hint: Think about the pigeonhole principle*

Exercise 0.35. Show that the intersection of any arbitrary collection of normal subgroups is normal.

Note: The tools to do the following exercise have not been developed in this book yet.

Exercise 0.36. Show that if $\{ N_\alpha : \alpha \in \Lambda \}$ is a collection of normal subgroups of G, then $\langle N_\alpha : \alpha \in \Lambda \rangle$, the smallest normal subgroup that contains all N_α, is normal in G.

For an added challenge, do this with the intersection definition.