Definition 2.6.16. Let a and b be elements of a group G. We say that b is *conjugate* to a if there is a $g \in G$ such that $b = gag^{-1}$.

You are asked to show in the Exercises that conjugacy is an equivalence relation and to find all the conjugacy equivalence classes in several groups of small order.

Definition 2.6.17. The equivalence classes for conjugacy are called *conjugacy classes.*

Note that the center of a group is related to the notion of conjugacy in the following way: The center consists of all elements whose conjugacy class is a singleton. That is, $g \in Z(G) \Leftrightarrow$ the conjugacy class of g is $\{g\}$.

Exercises 2.6

2.6.1. Consider any surjective map f from a set X onto another set Y. We can define a relation on X by $x_1 \sim x_2$ if $f(x_1) = f(x_2)$. Check that this is an equivalence relation. Show that the associated partition of X is the partition into "fibers" $f^{-1}(y)$ for $y \in Y$.

The next several exercises concern conjugacy classes in a group.

2.6.2. Show that conjugacy of group elements is an equivalence relation.

2.6.3. What are the conjugacy classes in S_3?

2.6.4. What are the conjugacy classes in the symmetry group of the square D_4?

2.6.5. What are the conjugacy classes in the dihedral group D_5?

2.6.6. Show that a subgroup is normal if, and only if, it is a union of conjugacy classes.

2.7. Quotient Groups and Homomorphism Theorems

Consider the permutation group S_n with its normal subgroup of even permutations. For the moment write $\mathcal{E}$ for the subgroup of even permutations and $\mathcal{O}$ for the coset $\mathcal{O} = (12)\mathcal{E} = \mathcal{E}(12)$ consisting of odd permutations. The subgroup $\mathcal{E}$ is the kernel of the sign homomorphism $\epsilon : S_n \longrightarrow \{1, -1\}$.

Since the product of two permutations is even if, and only if, both are even or both are odd, we have the following multiplication table for the two cosets of $\mathcal{E}$:

	$\mathcal{E}$	$\mathcal{O}$
$\mathcal{E}$	$\mathcal{E}$	$\mathcal{O}$
$\mathcal{O}$	$\mathcal{O}$	$\mathcal{E}$

The products are taken in the sense mentioned previously; namely the product of two even permutations or two odd permutations is even, and the product of an even permutation with an odd permutation is odd. Thus the multiplication on the cosets of $\mathcal{E}$ reproduces the multiplication on the group $\{1, -1\}$.

This is a general phenomenon: If N is a *normal* subgroup of a group G, then the set G/N of left cosets of a N in G has the structure of a group.

The Quotient Group Construction

Theorem 2.7.1. *Let N be a normal subgroup of a group G. The set of cosets G/N has a unique product that makes G/N a group and that makes the quotient map $\pi : G \longrightarrow G/N$ a group homomorphism.*

Proof. Let A and B be elements of G/N (i.e., A and B are left cosets of N in G). Let $a \in A$ and $b \in B$ (so $A = aN$ and $B = bN$). We would like to define the product AB to be the left coset containing ab, that is,

$$(aN)(bN) = abN.$$

But we have to check that this makes sense (i.e., that the result is independent of the choice of $a \in A$ and of $b \in B$). So let a' be another element of aN and b' another element of bN. We need to check that $abN = a'b'N$, or, equivalently, that $(ab)^{-1}(a'b') \in N$. We have

$$\begin{aligned}(ab)^{-1}(a'b') &= b^{-1}a^{-1}a'b' \\ &= b^{-1}a^{-1}a'(bb^{-1})b' = (b^{-1}a^{-1}a'b)(b^{-1}b').\end{aligned}$$

Since $aN = a'N$, and $bN = b'N$, we have $a^{-1}a' \in N$ and $b^{-1}b' \in N$. Since N is normal, $b^{-1}(a^{-1}a')b \in N$. Therefore, the final expression is a product of two elements of N, so is in N. This completes the verification that the definition of the product on G/H makes sense.

The associativity of the product on G/N follows from repeated use of the definition of the product, and the associativity of the product on G; namely

$$\begin{aligned}(aNbN)cN = abNcN = (ab)cN = a(bc)N \\ = aNbcN = aN(bNcN).\end{aligned}$$

It is clear that N itself serves as the identity for this multiplication and that $a^{-1}N$ is the inverse of aN. Thus G/N with this multiplication is a group. Furthermore, π is a homomorphism because

$$\pi(ab) = abN = aNbN = \pi(a)\pi(b).$$

The uniqueness of the product follows simply from the surjectivity of π: in order for π to be a homomorphism, it is necessary that $aNbN = abN$. ■

The group G/N is called the *quotient group* of G by N. The map $\pi : G \to G/N$ is called the quotient homomorphism. Another approach to defining the product in G/N is developed in Exercise 2.7.2.

Example 2.7.2. (Finite cyclic groups as quotients of $\mathbb{Z}$). The construction of $\mathbb{Z}_n$ in Section 1.7 is an example of the quotient group construction. The (normal) subgroup in the construction is $n\mathbb{Z} = \{\ell n : \ell \in \mathbb{Z}\}$. The cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are of the form $k + n\mathbb{Z} = [k]$; the distinct cosets are $[0] = n\mathbb{Z}, [1] = 1 + n\mathbb{Z}, \dots, [n-1] = n - 1 + n\mathbb{Z}$. The product (sum) of two cosets is $[a]+[b] = [a+b]$. So the group we called $\mathbb{Z}_n$ is precisely $\mathbb{Z}/n\mathbb{Z}$. The quotient homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ is given by $k \mapsto [k]$.

Example 2.7.3. Now consider a cyclic group G of order n with generator a. There is a homomorphism $\varphi : \mathbb{Z} \to G$ of $\mathbb{Z}$ *onto* G defined by $\varphi(k) = a^k$. The kernel of this homomorphism is precisely all multiples of n, the order of a; $\ker(\varphi) = n\mathbb{Z}$. I claim that φ "induces" an isomorphism $\tilde{\varphi} : \mathbb{Z}_n \to G$, defined by $\tilde{\varphi}([k]) = a^k = \varphi(k)$. It is necessary to check that this makes sense (i.e., that $\tilde{\varphi}$ is well defined) because we have attempted to define the value of $\tilde{\varphi}$ on a coset $[k]$ in terms of a particular representative of the coset. Would we get the same result if we took another representative, say $k+17n$ instead of k? In fact, we would get the same answer: If $[a] = [b]$, then $a-b \in n\mathbb{Z} = \ker(\varphi)$, and, therefore, $\varphi(a)-\varphi(b) = \varphi(a-b) = 0$. Thus $\varphi(a) = \varphi(b)$. This shows that the map $\tilde{\varphi}$ is well defined.

Next we have to check the homomorphism property of $\tilde{\varphi}$. This property is valid because $\tilde{\varphi}([a][b]) = \tilde{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}([a])\tilde{\varphi}([b])$.

The homomorphism $\tilde{\varphi}$ has the same range as φ, so it is surjective. It also has trivial kernel: If $\tilde{\varphi}([k]) = 0$, then $\varphi(k) = 0$, so $k \in n\mathbb{Z} = [0]$, so $[k] = [0]$. Thus $\tilde{\varphi}$ is an isomorphism.

Example 2.7.4. Take the additive abelian group $\mathbb{R}$ as G and the subgroup $\mathbb{Z}$ as N. Since $\mathbb{R}$ is abelian, all of its subgroups are normal, and, in particular, $\mathbb{Z}$ is a normal subgroup.

The cosets of $\mathbb{Z}$ in $\mathbb{R}$ were considered in Exercise 2.5.11, where you were asked to verify that the cosets are parameterized by the set of real numbers t such that $0 \le t < 1$. In fact, two real numbers are in the same coset modulo $\mathbb{Z}$ precisely if they differ by an integer, $s \equiv t \pmod{\mathbb{Z}} \Leftrightarrow s - t \in \mathbb{Z}$. For any real number t, let $[[t]]$ denote the greatest integer less than or equal to t. Then $t - [[t]] \in [0, 1)$ and $t \equiv (t - [[t]]) \pmod{\mathbb{Z}}$. On the other hand, no two real numbers in $[0, 1)$ are congruent modulo $\mathbb{Z}$. Thus we have a bijection between $\mathbb{R}/\mathbb{Z}$ and $[0, 1)$ which is given by $[t] \mapsto t - [[t]]$.

We get a more instructive geometric picture of the set $\mathbb{R}/\mathbb{Z}$ of cosets of $\mathbb{R}$ modulo $\mathbb{Z}$ if we take, instead of the half–open interval $[0, 1)$, the closed interval $[0, 1]$ but *identify* the endpoints 0 and 1: The picture is a circle of circumference 1. Actually we can take a circle of any convenient size, and it is more convenient to take a circle of radius 1, namely

$$\{e^{2\pi it} : t \in \mathbb{R}\} = \{e^{2\pi it} : 0 \le t < 1\}.$$

So now we have bijections between set $\mathbb{R}/\mathbb{Z}$ of cosets of $\mathbb{R}$ modulo $\mathbb{Z}$, the set $[0, 1)$, and the unit circle $\mathbb{T}$, given by

$$[t] \mapsto t - [[t]] \mapsto e^{2\pi it} = e^{2\pi i(t - [[t]])}.$$

Let us write φ for the map $t \mapsto e^{2\pi it}$ from $\mathbb{R}$ onto the unit circle, and $\tilde{\varphi}$ for the map $[t] \mapsto \varphi(t) = e^{2\pi it}$. Our discussion shows that $\tilde{\varphi}$ is well defined. We know that the unit circle $\mathbb{T}$ is itself a group, and we recall that that the exponential map $\varphi : \mathbb{R} \to \mathbb{T}$ is a group homomorphism, namely,

$$\varphi(s + t) = e^{2\pi i(s+t)} = e^{2\pi is}e^{2\pi it} = \varphi(s)\varphi(t).$$

Furthermore, the kernel of φ is precisely $\mathbb{Z}$.

We now have a good geometric picture of the quotient group $\mathbb{R}/\mathbb{Z}$ *as a set*, but we still have to discuss the group structure of $\mathbb{R}/\mathbb{Z}$. The definition of the product (addition!) on $\mathbb{R}/\mathbb{Z}$ is $[t] + [s] = [t + s]$. But observe that

$$\tilde{\varphi}([s] + [t]) = \tilde{\varphi}([s + t]) = e^{2\pi i(s+t)} = e^{2\pi is}e^{2\pi it} = \tilde{\varphi}(s)\tilde{\varphi}(t).$$

Thus $\tilde{\varphi}$ is a group isomorphism from the quotient group $\mathbb{R}/\mathbb{Z}$ to $\mathbb{T}$.

Our work can be summarized in the following diagram, in which all of the maps are group homomorphisms, and the map π is the quotient map from $\mathbb{R}$ to $\mathbb{R}/\mathbb{Z}$.

$$\begin{tikzcd}
\mathbb{R} \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathbb{T} \\
\mathbb{R}/\mathbb{Z} \arrow[ur, "\cong", "\tilde{\varphi}"'] &
\end{tikzcd}$$

Example 2.7.5. Recall from Exercise 2.4.20 the "$Ax + b$" group or affine group $\mathrm{Aff}(n)$ consisting of transformations of $\mathbb{R}^n$ of the form

$$T_{A,\boldsymbol{b}}(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{b},$$

where $A \in \mathrm{GL}(n, \mathbb{R})$ and $\boldsymbol{b} \in \mathbb{R}^n$. Let N be the subset consisting of the transformations $T_{E,\boldsymbol{b}}$, where E is the identity transformation,

$$T_{E,\boldsymbol{b}}(\boldsymbol{x}) = \boldsymbol{x} + \boldsymbol{b}.$$

The composition rule in $\mathrm{Aff}(n)$ is

$$T_{A,\boldsymbol{b}} T_{A',\boldsymbol{b}'} = T_{AA',A\boldsymbol{b}'+\boldsymbol{b}}.$$

The inverse of $T_{A,\boldsymbol{b}}$ is $T_{A^{-1},-A^{-1}\boldsymbol{b}}$. N is a subgroup isomorphic to the additive group $\mathbb{R}^n$ because

$$T_{E,\boldsymbol{b}} T_{E,\boldsymbol{b}'} = T_{E,\boldsymbol{b}+\boldsymbol{b}'},$$

and N is normal. In fact,

$$T_{A,\boldsymbol{b}} T_{E,\boldsymbol{c}} T_{A,\boldsymbol{b}}^{-1} = T_{E,A\boldsymbol{c}}.$$

Let us examine the condition for two elements $T_{A,\boldsymbol{b}}$ and $T_{A',\boldsymbol{b}'}$ to be congruent modulo N. The condition is

$$T_{A',\boldsymbol{b}'}^{-1} T_{A,\boldsymbol{b}} = T_{A'^{-1},-A'^{-1}\boldsymbol{b}'} T_{A,\boldsymbol{b}} = T_{A'^{-1}A,A'^{-1}(\boldsymbol{b}-\boldsymbol{b}')} \in N.$$

This is equivalent to $A = A'$. Thus the class of $T_{A,\boldsymbol{b}}$ modulo N is $[T_{A,\boldsymbol{b}}] = \{T_{A,\boldsymbol{b}'} : \boldsymbol{b}' \in \mathbb{R}^n\}$, and the cosets of N can be parameterized by $A \in \mathrm{GL}(n)$. In fact, the map $[T_{A,\boldsymbol{b}}] \mapsto A$ is a bijection between the set $\mathrm{Aff}(n)/N$ of cosets of $\mathrm{Aff}(n)$ modulo N and $\mathrm{GL}(n)$.

Let us write φ for the map $\varphi : T_{A,\boldsymbol{b}} \mapsto A$ from $\mathrm{Aff}(n)$ to $\mathrm{GL}(n)$, and $\tilde{\varphi}$ for the map $\tilde{\varphi} : [T_{A,\boldsymbol{b}}] \mapsto A$ from $\mathrm{Aff}(n)/N$ to $\mathrm{GL}(n)$. The map φ is a (surjective) homomorphism, because

$$\varphi(T_{A,\boldsymbol{b}} T_{A',\boldsymbol{b}'}) = \varphi(T_{AA',A\boldsymbol{b}'+\boldsymbol{b}}) = AA' = \varphi(T_{A,\boldsymbol{b}})\varphi(T_{A',\boldsymbol{b}'}),$$

and furthermore the kernel of φ is N.

The definition of the product in $\mathrm{Aff}(n)/N$ is

$$[T_{A,\boldsymbol{b}}][T_{A',\boldsymbol{b}'}] = [T_{A,\boldsymbol{b}}T_{A',\boldsymbol{b}'}] = [T_{AA',\boldsymbol{b}+A\boldsymbol{b}'}].$$

It follows that

$$\tilde{\varphi}([T_{A,\boldsymbol{b}}][T_{A',\boldsymbol{b}'}]) = \tilde{\varphi}([T_{AA',\boldsymbol{b}+A\boldsymbol{b}'}]) = AA' = \tilde{\varphi}([T_{A,\boldsymbol{b}}])\tilde{\varphi}([T_{A',\boldsymbol{b}'}]),$$

and, therefore, $\tilde{\varphi}$ is an isomorphism of groups.

We can summarize our findings in the diagram:

$$\begin{tikzcd}
\mathrm{Aff}(n) \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathrm{GL}(n) \\
\mathrm{Aff}(n)/N \arrow[ur, "\cong", "\tilde{\varphi}"'] &
\end{tikzcd}$$

Homomorphism Theorems

The features that we have noticed in the several examples are quite general:

Theorem 2.7.6. *(Homomorphism theorem). Let $\varphi : G \longrightarrow \overline{G}$ be a surjective homomorphism with kernel N. Let $\pi : G \longrightarrow G/N$ be the quotient homomorphism. There is a group isomorphism $\tilde{\varphi} : G/N \longrightarrow \overline{G}$ satisfying $\tilde{\varphi} \circ \pi = \varphi$. (See the following diagram.)*

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

Proof. There is only one possible way to define $\tilde{\varphi}$ so that it will satisfy $\tilde{\varphi} \circ \pi = \varphi$, namely $\tilde{\varphi}(aN) = \varphi(a)$.

It is necessary to check that $\tilde{\varphi}$ is well-defined, i.e., that $\tilde{\varphi}(aN)$ does not depend on the choice of the representative of the coset aN. Suppose that $aN = bN$; we have to check that $\varphi(a) = \varphi(b)$. But

$$\begin{aligned}
aN = bN &\Leftrightarrow b^{-1}a \in N = \ker(\varphi) \\
&\Leftrightarrow e = \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a) \\
&\Leftrightarrow \varphi(b) = \varphi(a).
\end{aligned}$$

The same computation shows that $\tilde{\varphi}$ is injective. In fact,

$$\begin{aligned}\tilde{\varphi}(aN) = \tilde{\varphi}(bN) &\Rightarrow \varphi(a) = \varphi(b)\\ &\Rightarrow aN = bN.\end{aligned}$$

The surjectivity of $\tilde{\varphi}$ follows from that of φ, since $\varphi = \tilde{\varphi} \circ \pi$.

Finally, $\tilde{\varphi}$ is a homomorphism because

$$\tilde{\varphi}(aNbN) = \tilde{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(aN)\tilde{\varphi}(bN).$$

■

A slightly different proof is suggested in Exercise 2.7.1.

The two theorems (Theorems 2.7.1 and 2.7.6) say that normal subgroups and (surjective) homomorphisms are two sides of one coin: Given a normal subgroup N, there is a surjective homomorphism with N as kernel, and, on the other hand, a surjective homomorphism is essentially determined by its kernel.

Theorem 2.7.6 also reveals the best way to understand a quotient group G/N. The best way is to find a natural model, namely some naturally defined group $\overline{G}$ together with a surjective homomorphism $\varphi : G \to \overline{G}$ with kernel N. Then, according to the theorem, $G/N \cong \bar{G}$. With this in mind, we take another look at the examples given above, as well as several more examples.

Example 2.7.7. Let a be an element of order n in a group H. There is a homomorphism $\varphi : \mathbb{Z} \to H$ given by $k \mapsto a^k$. This homomorphism has range $\langle a \rangle$ and kernel $n\mathbb{Z}$. Therefore, by the homomorphism theorem, $\mathbb{Z}/n\mathbb{Z} \cong \langle a \rangle$. In particular, if $\zeta = e^{2\pi i/n}$, then $\varphi(k) = \zeta^k$ induces an isomorphism of $\mathbb{Z}/n\mathbb{Z}$ onto the group C_n of n^{th} roots of unity in $\mathbb{C}$.

Example 2.7.8. The homomorphism $\varphi : \mathbb{R} \to \mathbb{C}$ given by $\varphi(t) = e^{2\pi i t}$ has range $\mathbb{T}$ and kernel $\mathbb{Z}$. Thus by the homomorphism theorem, $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

Example 2.7.9. The map $\varphi : \mathrm{Aff}(n) \to \mathrm{GL}(n)$ defined by $T_{A,\boldsymbol{b}} \mapsto A$ is a surjective homomorphism with kernel $N = \{T_{E,\boldsymbol{b}} : \boldsymbol{b} \in \mathbb{R}^n\}$. Therefore, by the homomorphism theorem, $\mathrm{Aff}(n)/N \cong \mathrm{GL}(n)$.

Example 2.7.10. The set $\mathrm{SL}(n, \mathbb{R})$ of matrices of determinant 1 is a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$. In fact, $\mathrm{SL}(n, \mathbb{R})$ is the kernel of the homomorphism $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$, and this implies that $\mathrm{SL}(n, \mathbb{R})$ is a normal subgroup. It also implies that the quotient group $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R})$ is naturally isomorphic to $\mathbb{R}^*$.

Example 2.7.11. Consider $G = \mathrm{GL}(n, \mathbb{R})$, the group of n-by-n invertible matrices. Set $Z = G \cap \mathbb{R}E$, the set of invertible scalar matrices. Then Z is evidently a normal subgroup of G, and is, in fact, the center of G. A coset of Z in G has the form $[A] = AZ = \{\lambda A : \lambda \in \mathbb{R}^*\}$, the set of all nonzero multiples of the invertible matrix A; two matrices A and B are equivalent modulo Z precisely if one is a scalar multiple of the other. By our general construction of quotient groups, we can form G/Z, whose elements are cosets of Z in G, with the product $[A][B] = [AB]$. G/Z is called the *projective linear group.*

The rest of this example is fairly difficult, and it might be best to skip it on the first reading. We would like to find some natural realization or model of the quotient group. Now a natural model for a group is generally as a group of transformations of something or the other, so we would have to look for some objects which are naturally transformed not by matrices but rather by matrices modulo scalar multiples.

At least two natural models are available for G/Z. One is as transformations of projective $(n-1)$–dimensional space $\mathbb{P}^{n-1}$, and the other is as transformations of G itself.

Projective $(n-1)$–dimensional space consists of n-vectors modulo scalar multiplication. More precisely, we define an equivalence relation $\sim$ on the set $\mathbb{R}^n \setminus \{\mathbf{0}\}$ of nonzero vectors in $\mathbb{R}^n$ by $\boldsymbol{x} \sim \boldsymbol{y}$ if there is a nonzero scalar λ such that $\boldsymbol{x} = \lambda \boldsymbol{y}$. Then $\mathbb{P}^{n-1} = (\mathbb{R}^n \setminus \{\mathbf{0}\})/\sim$, the set of equivalence classes of vectors. There is another picture of $\mathbb{P}^{n-1}$ that is a little easier to visualize; every nonzero vector $\boldsymbol{x}$ is equivalent to the unit vector $\boldsymbol{x}/||\boldsymbol{x}||$, and furthermore two unit vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ are equivalent if and only if $\boldsymbol{a} = \pm\boldsymbol{b}$; therefore, $\mathbb{P}^{n-1}$ is also realized as $S^{n-1}/\pm$, the unit sphere in n–dimensional space, modulo equivalence of antipodal points. Write $[\boldsymbol{x}]$ for the class of a nonzero vector $\boldsymbol{x}$.

There is a homomorphism of G into $\mathrm{Sym}(\mathbb{P}^{n-1})$, the group of invertible maps from $\mathbb{P}^{n-1}$ to $\mathbb{P}^{n-1}$, defined by $\varphi(A)([x]) = [Ax]$; we have to check, as usual, that $\varphi(A)$ is a well-defined transformation of $\mathbb{P}^{n-1}$ and that φ is a homomorphism. I leave this as an exercise. What is the kernel of φ? It is precisely the invertible scalar matrices Z. We have $\varphi(G) \cong G/Z$, by the homomorphism theorem, and thus G/Z has been identified as a group of transformations of projective space.

A second model for G/Z is developed in Exercise 2.7.6, as a group of transformations of G itself.

Everything in this example works in exactly the same way when $\mathbb{R}$ is replaced by $\mathbb{C}$. When moreover $n = 2$, there is a natural realization of $\mathrm{GL}(n, \mathbb{C})/Z$ as "fractional linear transformations" of $\mathbb{C}$. For this, see Exercise 2.7.5.

Proposition 2.7.12. *(Correspondence of subgroups) Let $\varphi : G \longrightarrow \overline{G}$ be a homomorphism of G* onto *$\overline{G}$, and let N denote the kernel of φ.*

(a) *The map $\overline{B} \mapsto \varphi^{-1}(\overline{B})$ is a bijection between subgroups of $\overline{G}$ and subgroups of G containing N.*

(b) *Under this bijection, normal subgroups of $\overline{G}$ correspond to normal subgroups of G.*

Proof. For each subgroup $\overline{B}$ of $\overline{G}$, $\varphi^{-1}(\overline{B})$ is a subgroup of G by Proposition 2.4.12, and furthermore $\varphi^{-1}(\overline{B}) \supseteq \varphi^{-1}\{e\} = N$.

To prove (a), we show that the map $A \mapsto \varphi(A)$ is the inverse of the map $\overline{B} \mapsto \varphi^{-1}(\overline{B})$. If $\overline{B}$ is a subgroup of $\overline{G}$, then $\varphi(\varphi^{-1}(\overline{B}))$ is a subgroup of $\overline{G}$, that a priori is contained in $\overline{B}$. But since φ is surjective, $\overline{B} = \varphi(\varphi^{-1}(\overline{B}))$.

For a subgroup A of G containing N, $\varphi^{-1}(\varphi(A))$ is a subgroup of G which *a priori* contains A. If x is in that subgroup, then there is an $a \in A$ such that $\varphi(x) = \varphi(a)$. This is equivalent to $a^{-1}x \in \ker(\varphi) = N$. Hence, $x \in aN \subseteq aA = A$. This shows that $\varphi^{-1}(\varphi(A)) = A$, which completes the proof of part (a).

Let $B = \varphi^{-1}(\overline{B})$. For part (b), we have to show that $\overline{B}$ is normal in $\overline{G}$ if, and only if, B is normal in G.

Suppose $\overline{B}$ is normal in $\overline{G}$. Let $g \in G$ and $x \in B$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in \overline{B},$$

because $\varphi(x) \in \overline{B}$, and $\overline{B}$ is normal in $\overline{G}$. But this means that $gxg^{-1} \in \varphi^{-1}(\overline{B}) = B$, and thus B is normal in G.

Conversely, suppose B is normal in G. For $\bar{g} \in \overline{G}$ and $\bar{x} \in \overline{B}$, there exist $g \in G$ and $x \in B$ such that $\varphi(g) = \bar{g}$ and $\varphi(x) = \bar{x}$. Therefore,

$$\bar{g}\bar{x}\bar{g}^{-1} = \varphi(gxg^{-1}).$$

But $gxg^{-1} \in B$, by normality of B, so $\bar{g}\bar{x}\bar{g}^{-1} \in \varphi(B) = \overline{B}$. Therefore, $\overline{B}$ is normal in $\overline{G}$. ∎

Proposition 2.7.13. *Let $\varphi : G \longrightarrow \overline{G}$ be a surjective homomorphism with kernel N. Let $\overline{K}$ be a normal subgroup of $\overline{G}$ and let $K = \varphi^{-1}(\overline{K})$. Then $G/K \cong \overline{G}/\overline{K}$. Equivalently, $G/K \cong (G/N)/(K/N)$.*

Proof. Write ψ for the quotient homomorphism $\psi : \overline{G} \longrightarrow \overline{G}/\overline{K}$. Then $\psi \circ \varphi : G \longrightarrow \overline{G}/\overline{K}$ is a surjective homomorphism, because it is a composition of surjective homomorphisms. The kernel of $\psi \circ \varphi$ is the set of $x \in G$ such that $\varphi(x) \in \ker(\psi) = \overline{K}$; that is, $\ker(\psi \circ \varphi) = \varphi^{-1}(\overline{K}) = K$. According to the homomorphism theorem, Theorem 2.7.6,

$$\overline{G}/\overline{K} \cong G/\ker(\psi \circ \varphi) = G/K.$$

More explicitly, the isomorphism $G/K \longrightarrow \overline{G}/\overline{K}$ is

$$xK \mapsto \psi \circ \varphi(x) = \varphi(x)\overline{K}.$$

Using the homomorphism theorem again, we can identity $\overline{G}$ with G/N. This identification carries $\overline{K}$ to the image of K in G/N, namely K/N. Therefore,

$$(G/N)/(K/N) \cong \overline{G}/\overline{K} \cong G/K.$$

■

The following is a very useful generalization of the homomorphism theorem.

Proposition 2.7.14. *Let $\varphi : G \to \overline{G}$ be a surjective homomorphism of groups with kernel K. Let $N \subseteq K$ be a subgroup that is normal in G, and let $\pi : G \to G/N$ denote the quotient map. Then there is a surjective homomorphism $\tilde{\varphi} : G/N \to \overline{G}$ such that $\tilde{\varphi} \circ \pi = \varphi$. (See the following diagram.) The kernel of $\tilde{\varphi}$ is $K/N \subseteq G/N$.*

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

Proof. Let us remark that the conclusion follows from Proposition 2.7.13 and the homomorphism theorem. The map $\tilde{\varphi}$ is

$$G/N \longrightarrow (G/N)/(K/N) \cong G/K \cong \overline{G}.$$

However, it is more transparent to prove the result from scratch, following the model of the homomorphism theorem.

As in the proof of the homomorphism theorem, there is only one way to define $\tilde{\varphi}$ consistent with the requirement that $\tilde{\varphi} \circ \pi = \varphi$, namely $\tilde{\varphi}(aN) = \varphi(a)$. It is necessary to check that this is well defined and a homomorphism. But if $aN = bN$, then $b^{-1}a \in N \subseteq K = \ker(\varphi)$, so $\varphi(b^{-1}a) = e$, or $\varphi(a) = \varphi(b)$. This shows that the map $\tilde{\varphi}$ is well defined. The homomorphism property follows as in the proof of the homomorphism theorem. ■

Corollary 2.7.15. *Let $N \subseteq K \subseteq G$ be subgroups with both N and K normal in G. Then $xN \mapsto xK$ defines a homomorphism of G/N onto G/K with kernel K/N.*

Proof. The statement is the special case of the Proposition with $\overline{G} = G/K$ and $\varphi : G \to G/K$ the quotient map. Notice that applying the homomorphism theorem again gives us the isomorphism

$$(G/N)/(K/N) \cong G/K.$$

■

Example 2.7.16. What are all the subgroups of $\mathbb{Z}_n$? Since $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, the subgroups of $\mathbb{Z}_n$ correspond one to one with subgroups of $\mathbb{Z}$ containing the kernel of the quotient map $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, namely $n\mathbb{Z}$. But the subgroups of $\mathbb{Z}$ are cyclic and of the form $k\mathbb{Z}$ for some $k \in Z$. So when does $k\mathbb{Z}$ contain $n\mathbb{Z}$? Precisely when $n \in k\mathbb{Z}$, or when k divides n. Thus the subgroups of $\mathbb{Z}_n$ correspond one to one with *positive integer divisors of* n. The image of $k\mathbb{Z}$ in $\mathbb{Z}_n$ is cyclic with generator $[k]$ and with order n/k.

Example 2.7.17. When is there a surjective homomorphism from one cyclic group $\mathbb{Z}_k$ to another cyclic group $\mathbb{Z}_\ell$?

Suppose first that $\psi : \mathbb{Z}_k \to \mathbb{Z}_\ell$ is a surjective homomorphism such that $\psi[1] = [1]$. Let φ_k and φ_ℓ be the natural quotient maps of $\mathbb{Z}$ onto $\mathbb{Z}_k$ and $\mathbb{Z}_\ell$ respectively. We have maps

$$\mathbb{Z} \xrightarrow{\varphi_k} \mathbb{Z}_k \xrightarrow{\psi} \mathbb{Z}_\ell,$$

and $\psi \circ \varphi_k$ is a surjective homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_\ell$ such that $\psi \circ \varphi_k(1) = [1]$; therefore, $\psi \circ \varphi_k = \varphi_\ell$. But then the kernel of φ_k is contained in the kernel of φ_ℓ, which is to say that every integer multiple of k is divisible by ℓ. In particular, k is divisible by ℓ.

The assumption that $\psi[1] = [1]$ is not essential and can be eliminated as follows: Suppose that $\psi : \mathbb{Z}_k \to \mathbb{Z}_\ell$ is a surjective homomorphism with $\psi([1]) = [a]$. The cyclic subgroup group generated by $[a]$ is all of $\mathbb{Z}_\ell$, and in particular $[a]$ has order ℓ. Thus there is a surjective homomorphism $\mathbb{Z} \to \mathbb{Z}_\ell$ defined by $n \mapsto [na]$, with kernel $\ell\mathbb{Z}$.

It follows from the homomorphism theorem that there is an isomorphism $\theta : \mathbb{Z}_\ell \to \mathbb{Z}_\ell$ such that $\theta([1]) = [a]$. But then $\theta^{-1} \circ \psi : \mathbb{Z}_k \to \mathbb{Z}_\ell$ is a surjective homomorphism such that $\theta^{-1} \circ \psi([1]) = \theta^{-1}([a]) = [1]$. It follows that k is divisible by ℓ.

Conversely, if k is divisible by ℓ, then $k\mathbb{Z} \subseteq \ell\mathbb{Z} \subseteq Z$. Since $\mathbb{Z}$ is abelian, all subgroups are normal, and by the corollary, there is a surjective homomorphism $\mathbb{Z}_k \to \mathbb{Z}_\ell$ such that $[1] \mapsto [1]$.

We conclude that there is a surjective homomorphism from $\mathbb{Z}_k$ to $\mathbb{Z}_l$ if, and only if, ℓ divides k.

Proposition 2.7.18. *Let $\varphi : G \longrightarrow \bar{G}$ be a surjective homomorphism with kernel N. Let A be a subgroup of G. Then*

(a) $\varphi^{-1}(\varphi(A)) = AN = \{an : a \in A \text{ and } n \in N\}$,

(b) *AN is a subgroup of G containing N.*

(c) $AN/N \cong \varphi(A) \cong A/(A \cap N)$.

Proof. Let $x \in G$. Then

$$\begin{aligned} x \in \varphi^{-1}(\varphi(A)) &\Leftrightarrow \text{there exists } a \in A \text{ such that } \varphi(x) = \varphi(a) \\ &\Leftrightarrow \text{there exists } a \in A \text{ such that } x \in aN \\ &\Leftrightarrow x \in AN. \end{aligned}$$

Thus, $AN = \varphi^{-1}(\varphi(A))$, which, by Proposition 2.7.12, is a subgroup of G containing N. Now applying Theorem 2.7.6 to the restriction of φ to AN gives the isomorphism $AN/N \cong \varphi(AN) = \varphi(A)$. On the other hand, applying the theorem to the restriction of φ to A gives $A/(A \cap N) \cong \varphi(A)$. ■

Example 2.7.19. Let G be the symmetry group of the square, which is generated by elements r and j satisfying $r^4 = e = j^2$ and $jrj = r^{-1}$. Let N be the subgroup $\{e, r^2\}$; then N is normal because $jr^2j = r^{-2} = r^2$. What is G/N? The group G/N has order 4 and is generated by two commuting elements rN and jN each of order 2. (Note that rN and jN commute because $rN = r^{-1}N$, and $jr^{-1} = rj$, so $jrN = jr^{-1}N = rjN$.) Hence, G/N is isomorphic to the group $\mathcal{V}$ of symmetries of the rectangle. Let $A = \{e, j\}$. Then AN is a four–element subgroup of G (also isomorphic to $\mathcal{V}$) and $AN/N = \{N, jN\} \cong \mathbb{Z}_2$. On the other hand, $A \cap N = \{e\}$, so $A/(A \cap N) \cong A \cong \mathbb{Z}_2$.

Example 2.7.20. Let $G = \mathrm{GL}(n, \mathbb{C})$, the group of n-by-n invertible complex matrices. Let Z be the subgroup of invertible scalar matrices. G/Z is the complex projective linear group. Let $A = \mathrm{SL}(n, \mathbb{C})$.

Then $AZ = G$ because for any invertible matrix X, we have $X = \det(X)X'$, where $X' = \det(X)^{-1}X \in A$. On the other hand, $A \cap Z$ is the group of invertible scalar matrices with determinant 1; such a matrix must have the form ζE where ζ is an n^{th} root of unity in $\mathbb{C}$. We have $G/Z = AZ/Z = A/(A \cap Z) = A/\{\zeta E : \zeta \text{ is a root of unity}\}$.

The same holds with $\mathbb{C}$ replaced by $\mathbb{R}$, and here the result is more striking, because $\mathbb{R}$ contains few roots of unity. If n is odd, the only n^{th} root of unity in $\mathbb{R}$ is 1, so we see that the projective linear group is isomorphic to $\mathrm{SL}(n, \mathbb{R})$. On the other hand, if n is even, then -1 is also an n^{th} root of unity and the projective linear group is isomorphic to $\mathrm{SL}(n, \mathbb{R})/\{\pm 1E\}$.

Exercises 2.7

2.7.1. Let $\varphi : G \longrightarrow \overline{G}$ be a surjective homomorphism with kernel N. Let $\pi : G \longrightarrow G/N$ be the quotient homomorphism. Show that for $x, y \in G$, $x \sim_{\varphi} y \Leftrightarrow x \sim_{\pi} y \Leftrightarrow x \sim_N y$. Conclude that the map $\tilde{\varphi} : G/N \longrightarrow \overline{G}$ defined by $\tilde{\varphi}(aN) = \varphi(a)$ is well defined and bijective.

2.7.2. Here is a different approach to the definition of the product on G/N, where N is a normal subgroup of G.

(a) Define the product of *arbitrary* subsets A and B of G to be

$$\{ab : a \in A \text{ and } b \in B\}.$$

Verify that this gives an associative product on subsets.

(b) Take $A = aN$ and $B = bN$. Verify that the product AB *in the sense of part (a)* is equal to abN. Your verification will use that N is a normal subgroup of G.

(c) Observe that it follows from parts (a) and (b) that $(aN)(bN) = abN$ is a well–defined, associative product on G/N.

2.7.3. Consider the affine group $\mathrm{Aff}(n)$ consisting of transformations of $\mathbb{R}^n$ of the form $T_{A,\boldsymbol{b}}(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{b}$ ($A \in \mathrm{GL}(n, \mathbb{R})$ and $\boldsymbol{b} \in \mathbb{R}^n$).

(a) Show that the inverse of $T_{A,\boldsymbol{b}}$ is $T_{A^{-1},-A^{-1}\boldsymbol{b}}$.

(b) Show that $T_{A,\boldsymbol{b}}T_{E,\boldsymbol{c}}T_{A,\boldsymbol{b}}^{-1} = T_{E,Ac}$. Conclude that $N = \{T_{E,\boldsymbol{b}} : \boldsymbol{b} \in \mathbb{R}^n\}$ is a normal subgroup of $\mathrm{Aff}(n)$.

2.7.4. Suppose G is finite. Verify that

$$|AN| = \frac{|A|\,|N|}{|A \cap N|}.$$

2.7.5. Consider the set of *fractional linear transformations* of the complex plane with ∞ adjoined, $\mathbb{C} \cup \{\infty\}$,

$$T_{a,b;c,d}(z) = \frac{az+b}{cz+d}$$

where $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an invertible 2-by-2 complex matrix. Show that this is a group of transformations and is isomorphic to $\mathrm{GL}(2,\mathbb{C})/Z(\mathrm{GL}(2,\mathbb{C}))$.

2.7.6. Recall that an automorphism of a group G is a group isomorphism from G to G. Denote the set of all automorphisms of G by $\mathrm{Aut}(G)$.

(a) Show that $\mathrm{Aut}(G)$ of G is also a group.

(b) Recall that for each $g \in G$, the map $c_g : G \longrightarrow G$ defined by $c_g(x) = gxg^{-1}$ is an element of $\mathrm{Aut}(G)$. Show that the map $c : g \mapsto c_g$ is a homomorphism from G to $\mathrm{Aut}(G)$.

(c) Show that the kernel of the map c is $Z(G)$.

(d) In general, the map c is not surjective. The image of c is called the *group of inner automorphisms* and denoted $\mathrm{Int}(G)$. Conclude that $\mathrm{Int}(G) \cong G/Z(G)$.

2.7.7. Let D_4 denote the group of symmetries of the square, and N the subgroup of rotations. Observe that N is normal and check that D_4/N is isomorphic to the cyclic group of order 2.

2.7.8. Find out whether every automorphism of S_3 is inner. Note that any automorphism φ must permute the set of elements of order 2, and an automorphism φ is completely determined by what it does to order 2 elements, since all elements are products of 2–cycles. Hence, there can be at most as many automorphisms of S_3 as there are permutations of the three–element set of 2–cycles, namely 6; that is, $|\mathrm{Aut}(S_3)| \le 6$. According to Exercises 2.5.13 and 2.7.6, how large is $\mathrm{Int}(S_3)$? What do you conclude?

2.7.9. Let G be a group and let C be the subgroup generated by all elements of the form $xyx^{-1}y^{-1}$ with $x, y \in G$. C is called the *commutator subgroup* of G. Show that C is a normal subgroup and that G/C is abelian. Show that if H is a normal subgroup of G such that G/H is abelian, then $H \supseteq C$.

2.7.10. Show that any quotient of an abelian group is abelian.

2.7.11. Prove that if $G/Z(G)$ is cyclic, then G is abelian.

2.7.12. Suppose $G/Z(G)$ is abelian. Must G be abelian?