2.5 Generators and Relations

There is another way to describe groups using "generators" and "relations." A set of generators for the group is given, and then certain properties that must be satisfied by those generators are listed. The latter are called the relations. Identifying the generators and relations for a group is called **giving a presentation** of the group. The group is then the set of all possible products of the generators and their inverses (these are informally called "words"). The relations say that some words are equal to the identity, so they give a way to simplify words. The description via generators and relations can be straightforward in the simplest instances, but it is quite subtle in general. We give a few examples here and defer a more thorough treatment to Section 3.4.

We have noted that $\mathbb{Z}$ requires only one generator, as do the groups $\mathbb{Z}_n$. We may describe $\mathbb{Z}_n$ (actually a group isomorphic to it) using the generator a, and the relation $a^n = 1$, in which I use 1 for the identity element. This would be written

$$\langle a | a^n = 1 \rangle$$

The homomorphism $\mathbb{Z}_n \longrightarrow \langle a | a^n = 1 \rangle$ taking 1 to a is clearly an isomorphism.

We could also describe $\mathbb{Z}_n$ in other ways. For example when p and q are distinct primes (or even just coprime to each other), we could use two generators.

$$\mathbb{Z}_{pq} \cong \langle a, b | a^p = 1, b^q = 1, ab = ba \rangle$$

This tells us that a is an element of order p, b is an element of order q and that a and b commute. The latter relation could also be written $aba^{-1}b^{-1} = 1$.

Exercises 2.5.1.

(a) Show that the presentation for $\mathbb{Z}_{pq}$ in the previous paragraph is isomorphic to the group with presentation $\langle c | c^{pq} = 1 \rangle$ via the function $c \to ab$.

The dihedral group D_n has a presentation as follows

$$\langle a, b | a^n = 1, b^2 = 1, ba = a^{n-1}b \rangle$$

The generator a is clearly playing the role of rotation by $2\pi/n$ and b the role of a reflection. The final relation tells us that in any product using a and b we can switch any occurrence of ba to be $a^{n-1}b$ and thereby rearrange so that all the as are on the left and all the bs on the right. So, just using these relations we know that any element of this group can be uniquely written $a^i b^k$ for $i \in \{0, \ldots, n-1\}$ and $k \in \{0, 1\}$. The group product is easily summarized by the following

$$(a^i)(a^j b^k) = a^{i+j} b^k$$
$$(a^i b)(a^j b^k) = a^{i-j} b^{k+1}$$

Exponents on a are computed modulo n and on b modulo 2. It is easy to verify that our earlier discussion of D_n (Section **??**) is consistent with the description here: for any reflection t_i, $t_i r = r^{-1} t_i$.

Exercises 2.5.2. Here is another group. It is called the **quaternion group**.

$$Q = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b \rangle$$

(a) Show that Q has 8 elements. List them in a useful fashion and show how to multiply them as we did for the dihedral group.

(b) Show that Q has 1 element of order 2 and 6 of order 4.

(c) Draw the lattice diagram for this group.

Exercises 2.5.3. The infinite dihedral group. Let

$$D_\infty \langle a, b \mid b^2 = 1 \rangle$$

(a) Show that D_∞ is a symmetry group of the following diagrams.

(b) What other symmetries do these diagrams have that are not captured by D_∞?

2.6 Cosets and Conjugates

Let H be a subset of G. In this section we define cosets of H and show an extremely important result (Lagrange's Theorem) that the cosets form a partition of G. We also show there is another interesting partition of G that is determined by a relation called conjugacy.

The following bit of notation is useful.

Notation 2.6.1. Let S and T be subsets of a group G.

$$ST = \{st : s \in S, t \in T\}$$

So, ST is the set of all products of an element in S (on the left) and an element of T (on the right). Similarly, for $g \in G$, $gS = \{gs : s \in S\}$. We may use analogous notation for the set of all products from 3 or more sets, taking note that for three sets, $(ST)U = S(TU)$, by associativity, so we may just call this set STU.

If the group is abelian and the operation is $+$ we write $S + T$ instead of ST.

Notice that ST and TS are not necessarily equal when the group G is not abelian.

Exercises 2.6.2. R

evisiting the properties of a subgroup.

(a) Let T be a subset of a group G. Prove that T is a subgroup of G if and only if $TT = T$ and $T^{-1}T = T$.

(b) Let T be a subset of the finite group G. Prove that $TT = T$ if and only if T is a subgroup of G.

(c) Give an example to show that for an arbitrary group show that $TT = T$ is not sufficient to ensure T is a group of G.

Definition 2.6.3. Let $H \leq G$ and let $g \in G$. The set gH is a **left coset** of H in G. Similarly, Hg is a **right coset** of H in G.

We will prove several results for left cosets. There are analogous results for right cosets.

Lemma 2.6.4. *Let G be a group and H a subgroup of G. The function*

$$\begin{aligned} \lambda_g : H &\longrightarrow gH \\ h &\longmapsto gh \end{aligned}$$

is a bijection.

Proof. The function λ_g is a surjection by the definition of gH. Suppose $gh = gh'$. Multiplying on the left by g^{-1} gives $h = h'$. This shows λ_g is injective. □

Lemma 2.6.5. *Let G be a group and H a subgroup of G. For $a, g \in G$, if $gH \cap aH \neq \emptyset$ then $gH = aH$.*

Proof. First, we show that if $g \in aH$ then $gH \subseteq aH$. Let $g \in aH$, so there is some $k \in H$ such that $g = ak$. For any $h \in H$, we have $gh = akh$ and this is an element of aH because $kh \in H$ since H is a subgroup of G. This shows $gH \subseteq aH$.

Suppose $gH \cap aH$ is nonempty, containing some element x. Then there are $h, k \in H$ such that $x = gh = ak$. Then $g = akh^{-1} \in aH$ and similarly $a = ghk^{-1} \in gH$. From the previous paragraph, we have $aH \subseteq gH$ and $gH \subseteq aH$, so $aH = gH$. □

Theorem 2.6.6 (Lagrange)**.** *Let G be a group with subgroup H. The set of cosets of H form a partition of G.*

Consequently, if G is a finite group with subgroup H then the order of H divides the order of G. In particular, the order of any element of G divides $|G|$.

Proof. Any $g \in G$ is in some coset, namely gH, so the cosets cover G. The previous lemma shows that any two unequal cosets are disjoint. Thus the cosets partition G.

Suppose G is finite. Since the cosets of H partition G, there are elements $a_1, \ldots, a_t$ such that G is the disjoint union of $a_1H, a_2H, \ldots, a_tH$. The cosets of H all have the same number of elements by Lemma 2.6.4. Thus $|G| = \sum_{i=1}^{t} |a_iH| = t|H|$, and the number of elements of G is a multiple of $|H|$.

For any $a \in G$ the number of elements in the subgroup $\langle a \rangle$ is $\operatorname{ord}(a)$. So $\operatorname{ord}(a)$ divides $|G|$. □

Definition 2.6.7. Let $H \leq G$. The **index** of H in G, written $[G : H]$, is the number of cosets of H in G, which may be infinite.

If G is finite and $H \leq G$ then $[G : H] = |G|/|H|$, since all cosets have $|H|$ elements.

Exercises 2.6.8. Recall that the exponent of a group G is the lcm of the orders of the elements (if this is finite).

(a) For a finite group G with finite exponent t show that t divides the order of G.

(b) Give an example to show that there may not be an element in G whose order is the exponent of G.

Conjugation

Now we consider conjugation.

Definition 2.6.9. Let $a \in G$ and $g \in G$. The element aga^{-1} is called the **conjugation of g by a**. If S is a subset of G, we define aSa^{-1} to be $\{asa^{-1} : s \in S\}$. It is the **conjugation of S by a**.

Proposition 2.6.10. *Conjugacy on a group G determines an equivalence relation.*

Proof. Let G be a group and define a relation on G by a is related to b if there is some g such that $b = gag^{-1}$. The relation is reflexive, because for any $a \in G$, $eae^{-1} = a$. The relation is symmetic, because if a is related to b (say $b = gag^{-1}$) then we also have $a = g^{-1}b(g^{-1})^{-1}$ so b is related to a. Finally suppose a is related to b (again $b = gag^{-1}$) and b is related to c (so there is some $h \in G$ with $c = hbh^{-1}$). Then

$$c = hbh^{-1} = h(gag^{-1})h^{-1} = (hg)a(hg)^{-1}$$

This shows that a is related to c. We have shown that conjugacy determines an equivalence relation on G. □

Exercises 2.6.11. Let $C(a) = \{g \in G : ga = ag\}$ be the **centralizer** of a.

(a) Show that $C(a)$ is a subgroup of G.

(b) Let G be a finite group. Show that the number of elements of G conjugate to a is $|G|/|C(a)|$. [Consider the cosets of $C(a)$.]

Exercises 2.6.12. Conjugates and subgroups.

(a) Show that A_n is invariant under conjugation: for any $\pi \in S_n$, $\pi A_n \pi^{-1} = A_n$.

(b) Let C_n be the rotation subgroup of D_n. Find two elements of C_4 that are conjugate as elements of D_4 but are not conjugate as elements of C_4.

(c) Find two elements of D_4 that are conjugate as elements of S_4 but are not conjugate as elements of D_4.

Exercises 2.6.13. Let H be a subgroup of a group G.

(a) Let $a \in G$. Show that aHa^{-1} is a subgroup of G.

(b) Show that there is an isomorphism between H and aHa^{-1}.

Exercises 2.6.14. Inner automorphisms.

(a) Define a function $\varphi_a : G \longrightarrow G$ by $\varphi(g) = aga^{-1}$. Show that φ_a is an automorphism of G.

(b) Show that $\varphi : G \longrightarrow \mathrm{Aut}(G)$ defined by $\varphi : a \longmapsto \varphi_a$ is a homomorphism. The image, $\{\varphi_a : a \in G\}$, is therefore a subgroup of $\mathrm{Aut}(G)$. It is called $\mathrm{Inn}(G)$, the group of **inner automorphisms** of G.

(c) What is the kernel of φ?

Proposition 2.6.15. *Let $\pi \in S_n$. For any $\sigma \in S_n$, the signature of σ and the signature of $\pi\sigma\pi^{-1}$ are the same.*

One proof is contained in the following suite of exercises.

Exercises 2.6.16. Consider conjugation by $\pi \in S_n$.

(a) Let $(a_1, a_2, \ldots, a_k) \in S_n$ be a k-cycle, so the a_i are distinct. Show that

$$\pi * (a_1, a_2, \ldots, a_k) * \pi^{-1} = \Big(\pi(a_1), \pi(a_2), \ldots, \pi(a_k)\Big)$$

[Consider two cases, $b = \pi(a_i)$ for some i, and $b \notin \{\pi(a_1), \pi(a_2), \ldots \pi(a_k)\}$. Explain why this breakdown into two cases makes sense.]

(b) If A and B are disjoint subsets of $\{1, \ldots, n\}$ show that $\pi(A)$ and $\pi(B)$ are also disjoint.

(c) If $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$ is the cycle decomposition of σ, find the cycle decomposition of $\pi\sigma\pi^{-1}$ and justify your answer.

(d) Conclude that the conjugation of any $\sigma \in S_n$ by π has the same signature as σ.

2.7 Normality and the First Isomorphism Theorem

Let's pause for a moment to think about homomorphisms, particularly the special cases: injective homomorphisms (one-to-one) and surjective homomorphisms (onto).

Suppose H is a subgroup of G. There is a injective function from H to G, which is called the **inclusion map**, that simply takes $h \in H$ to itself, as an element of G. Since H is a subgroup of G (it's multiplication is the same as the one on G), the inclusion map is an injective homomorphism from H to G.

On the other hand, suppose that H and G are arbitrary groups and that $\varphi : H \longrightarrow G$ is an injective homomorpism. Proposition 2.2.5 shows that $\varphi(H)$ is a subgroup of G. Thus the bijection $\varphi : H \longrightarrow \varphi(H)$ is actually a homomorphism of groups. This shows that the image of an injective homomorphism $\varphi : H \longrightarrow G$ is a subgroup of G that is isomorphic to H. Thus, the study of injective homomorphisms is essentially the study of subgroups.

This section and Section 2.9 are focused on surjective homomorphisms, which are intimately related to subgroups that have a special property, treated in the next proposition.

Theorem 2.7.1 (Normal Subgroups)**.** *Let N be a subgroup of G. The following are equivalent.*

(1) $Na = aN$ for all $a \in G$.

(2) $aNbN = abN$ for all $a, b \in G$.

(3) $aNa^{-1} \subseteq N$ for all $a \in G$.

(4) $aNa^{-1} = N$ for all $a \in G$.

Proof. We prove a series of implications that shows the conditions are equivalent.
(1) $\Longrightarrow$ (2): $(aN)(bN) = a(Nb)N = a(bN)N = (ab)N$. Here we have used asociativity, then the assumption in (1), and finally, $NN = N$ since N is a subgroup of G.
(2) $\Longrightarrow$ (3): Set $b = a^{-1}$. Then, using (2), $aNa^{-1}N = aa^{-1}N = eN$. In particular, this shows that $aNa^{-1} \subseteq N$.
(3) $\Longrightarrow$ (4): For any $a \in G$, applying (3) to a^{-1}, we have that $a^{-1}Na \subseteq N$. Conjugating by a, we get

$$a(a^{-1}Na)a^{-1} \subseteq aNa^{-1}$$

The left hand side is N. Thus, assuming (3) we have both $aNa^{-1} \subseteq N$ and $N \subseteq aNa^{-1}$, which proves (4).
(4) $\Longrightarrow$ (1): Multiplying $aNa^{-1} = N$ on the right by a gives (1).

These arguments may seem slippery since they involve computations with sets. The proofs can also be done elementwise. Consider (4) $\implies$ (1). Let $a \in G$. Given any $n \in N$, we know $ana^{-1} \in N$, say $ana^{-1} = n'$. Then $an = n'a \in Na$. Since n was arbitrary, $aN \subseteq Na$. The reverse containment is proven analogously, using $a^{-1}na \in N$. $\square$

Definition 2.7.2. A group satisfying the conditions of the theorem is called **normal**. We write $N \trianglelefteq G$ for N a normal subgroup of G.

Exercises 2.7.3.

(a) Let H be a subgroup of a group G such that for any $a \in G$ there is a b in G such that $aH = Hb$. (Every left coset is also a right coset, but not necessarily defined by the same element of G.) Prove that H is normal in G.

Let N be normal in G. Suppose $aN = bN$ and $rN = sN$. Then $a \in bN$ and $r \in sN$, so $ar \in bNsN = bsN$. By Lemma 2.6.5, $arN = bsN$. Consequently, there is a well-defined operation on cosets of N in G that takes the pair (aN, bN) to abN (it doesn't matter which element we choose to represent each coset). The next theorem shows that this gives a group structure on the cosets of N in G.

Theorem 2.7.4. *Let N be a normal subgroup of G. Let G/N be the set of cosets of N in G with the binary operation by $aN * bN = abN$. Then G/N is a group.*

Proof. We have proven above that the product $aNbN$ is well defined and equal to abN. Associativity is inherited from associativity of $*_G$ (check!). The identity is eN. The inverse of aN is $a^{-1}N$. $\square$

We call G/N the **quotient** of G by N and the homomorphism $G \longrightarrow G/N$ is called the **quotient map**. Some sources call G/N a **factor** group.

Every subgroup of an abelian group A is normal in A, so for any subgroup B of A there is quotient group A/B.

Example 2.7.5. In $\mathbb{Z}$ the only subgroups are $n\mathbb{Z}$. The quotient group $\mathbb{Z}/n\mathbb{Z}$ has the distinct elements $a + n\mathbb{Z}$ for $a \in \{0, \ldots, n-1\}$. Clearly this is just another way to think about the additive group of integers modulo n. It is isomorphic to $\mathbb{Z}_n$.

Exercises 2.7.6. Additional properties of normal subgroups.

(a) Let N be a normal subgroup of G. For any subgroup H of G, $H \cap N$ is a normal subgroup of H.

(b) If $\varphi : G \longrightarrow H$ is a homomorphism and N is normal in H, then $\varphi^{-1}(N)$ is normal in G.

(c) Show that any subgroup of index 2 is normal.

Exercises 2.7.7. The **center** of G is the set of elements in G that commute with all elements of G, $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$.

(a) Prove that any subgroup of the center of G, including $Z(G)$ itself, is normal in G.

(b) Find the center of D_4; it is not trivial.

Exercises 2.7.8. Example of normal subgroups.

(a) Find all normal subgroups of D_4, D_5, and D_6.

(b) Find all normal subgroups of A_4.

(c) Find all normal subgroups of the quaternions, Q.

Isomorphism and Factor Theorems

We are now in the position to say more about the relationship between homomorphisms and normal subgroups.

Theorem 2.7.9 (First Isomorphism)**.** *Let $\varphi : G \longrightarrow H$ be a surjective homomorphism with kernel K. Then K is a normal subgroup of G and G/K is isomorphic to H.*

Proof. First we prove that K is normal by showing $aKa^{-1} \subseteq K$ for all $a \in G$. For any $k \in K$,

$$\varphi(aka^{-1}) = \varphi(a)\varphi(k)\varphi(a^{-1}) = \varphi(a)e_H\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H$$

Thus $aka^{-1} \in K$.

Let $g \in aK$, so $g = ak$ for some $k \in K$. Then $\varphi(g) = \varphi(a)\varphi(k) = \varphi(a)$. Consequently, all elements of a fixed coset of K ahve the same image under φ, so there is a well defined map $\tilde{\varphi} : G/K \to H$ taking aK to $\varphi(a)$.

To show $\tilde{\varphi}$ is a homomorphism, let aK and bK be elements of G/K. Since K is normal, $\tilde{\varphi}(aKbK) = \tilde{\varphi}(abK) = \varphi(ab)$ by the definition of multiplication in G/K and the definition of $\tilde{\varphi}$. Since φ is a homomorphism, $\varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}(aK)\tilde{\varphi}(bK)$. thus $\tilde{\varphi}(aKbK) = \tilde{\varphi}(aK)\tilde{\varphi}(bK)$, which shows $\tilde{\varphi}$ is a homomorphism.

Since φ is surjective, for any $h \in H$ there is some $a \in G$ such that $\varphi(a) = h$. Then $\tilde{\varphi}(aK) = h$, so $\tilde{\varphi}$ is surjective.

To show that $\tilde{\varphi}$ is injective, suppose $\tilde{\varphi}(aK) = e_H$. Then $\varphi(a) = e_H$ so $a \in K$ and $aK = e_GK$. Thus the kernel of $\tilde{\varphi}$ just contains just the identity element of G/K. □

Here is a typical snappy use of the First Isomorphism theorem.

Theorem 2.7.10. *Let $G_1, G_2, \ldots G_r$ be groups and let $N_1, N_2, \ldots, N_r$ be normal subgroups, $N_i \trianglelefteq G_i$. There is a well defined map*

$$\begin{aligned}(G_1 \times G_2 \times \cdots \times G_r)/(N_1 \times N_2 \times \cdots \times N_r) &\longrightarrow (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r)\\ (g_1, g_2, \ldots, g_r)\,(N_1 \times N_2 \times \cdots \times N_r) &\longmapsto (g_1N_1, g_2N_2, \ldots g_rN_r)\end{aligned}$$

and it is an isomorphism.

Proof. By the Direct Product Theorem 2.3.4, the projection of $G_1 \times G_2 \times \cdots \times G_r$ onto G_i is a homomorphism. Composing this with the quotient map $G_i \longrightarrow G_i/N_i$, we get maps $G_1 \times G_2 \times \cdots \times G_r \longrightarrow G_i/N$. Proposition 2.3.6 then gives a homomorphism

$$G_1 \times G_2 \times \cdots \times G_r \xrightarrow{\varphi} (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r),$$

To be specific, let us show that φ respects products. $(g_1, g_2, \ldots, g_r)$ and $(g_1', g_2', \ldots, g_r')$ be elements of $G_1 \times G_2 \times \cdots \times G_r$. Then

$$\begin{aligned}\varphi\Big((g_1, g_2, \ldots, g_r) * (g_1', g_2', \ldots, g_r')\Big) &= \varphi\Big(\,(g_1g_1', g_2, g_2', \ldots, g_rg_r')\,\Big)\\ &= (g_1g_1'N_1, g_2g_2'N, \ldots, g_rg_r'N_r)\\ &= (g_1N_1, g_2N_2, \ldots, g_rN_r) * (g_1'N_1, g_2'N_2, \ldots, g_r'N_r)\\ &= \varphi(g_1, g_2, \ldots, g_r) * \varphi(g_1', g_2', \ldots, g_r')\end{aligned}$$

We used, in order, the definition of multiplication in $G_1 \times G_2 \times \cdots \times G_r$, the definition of φ, the definition of multiplication in $G_1/N_1 \times G_2/N/2 \times \cdots \times G_r/N_r$ (and the N_i being normal), and finally, the definition of φ.

The kernel of φ is the set of $(g_1, \ldots, g_r)$ such that $g_1N_1, g_2N_2, \ldots, g_rN_r = N_1 \times N_2 \times \cdots \times N_r$. Each g_i must be in N_i. So, the kernel is $e_1N_1 \times e_2N_2 \times \cdots \times e_rN_r$. Surjectivity is easy to check, so the first isomorphism theorem now gives the result. □

A generalization of the first isomorphism theorem that we will often use treats the case when $\varphi : G \longrightarrow H$ is not necessarily surjective.

Theorem 2.7.11 (Factor)**.** *Let $\varphi : G \longrightarrow H$ be a homomorphism of groups with kernel K. Let N be a normal subgroup of G that is contained in K. Then φ can be factored into the canonical surjective homomorphism $\pi : G \longrightarrow G/N$ followed by a homomorphism $\bar{\varphi} : G/N \longrightarrow H$.*

By letting $N = K$ we conclude that any homomorphism can be factored into a surjective homomorphism followed by an injective homomorphism.

Proof. Define $\tilde{\varphi}$ by $gN \longmapsto \varphi(g)$. This is well defined because N is contained in the kernel of φ so for any $n \in N$, $\varphi(gn) = \varphi(g)\varphi(n) = \varphi(g)e_H = \varphi(g)$. From this definition it is immediate that $\tilde{\varphi} \circ \pi = \varphi$.

The proof that $\tilde{\varphi}$ is a homomorphism is similar to the proof of the First Isomorphism Theorem.

When $N = K$, we want to show that $\tilde{\varphi}$ is injective. Suppose $\tilde{\varphi(gN)} = e_H$. By the definition of $\tilde{\varphi}$, we have $\varphi(g) = e_H$. Thus $g \in K$, and therefore $gK = eK$, the identity element of G/K. □

The Factor Theorem and First Isomorphism Theorem give us a framework for understanding the material that we have seen earlier. As we said above the group $\mathbb{Z}_n$ is just the quotient of $\mathbb{Z}$ by its normal subgroup $n\mathbb{Z}$ (well isomorphic to it). In the context of groups we have given a shorthand notation to $\mathbb{Z}/n\mathbb{Z}$, calling it $\mathbb{Z}_n$.

Recall that Proposition 2.2.4 says that given any group G and $g \in G$ there is a homomorphism $\mathbb{Z} \longrightarrow G$ taking 1 to g. If g has infinite order then the cyclic group, $\langle g \rangle$, is isomorphic to $\mathbb{Z}$. If g has finite order n then the factor theorem says that $\mathbb{Z}_n$ is isomorphic to $\langle g \rangle$ via the homomorphism taking 1 (in $\mathbb{Z}_n$) to g.

2.8 More Examples of Groups

Before continuing the theoretical development we introduce a few more interesting families of groups. The first set are abelian, derived from the number systems discussed in Section 1.2. The second family is matrix groups, which are (generally) non-abelian.

Groups from Familiar Number Systems

We have already treated the additive group of the integers, $\mathbb{Z}$ as well as its subgroups $n\mathbb{Z}$. We have also used the integers modulo n, which we can now identify as the quotient group of $\mathbb{Z}$ by its subgroup $n\mathbb{Z}$. As pointed out in Section 1.2, the additive group of the fields $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) and $\mathbb{C}$ (complex numbers) are abelian groups. They are complicated as groups because they are not finitely generated. The next exercise shows that the quotient $\mathbb{Q}/\mathbb{Z}$ is interesting; every element has finite order, but the group is not finitely generated.

Exercises 2.8.1.

(a) Consider the group $\mathbb{Q}/\mathbb{Z}$. Show that every element has finite order.

(b) On a number line, sketch a region that contains one element for each equivalence class of $\mathbb{Q}/\mathbb{Z}$.

(c) Show that for any integer n there is an element of order n in $\mathbb{Q}/\mathbb{Z}$.

(d) How many elements of order n are there in $\mathbb{Q}/\mathbb{Z}$?

(e) Show that for any finite set $\{r_1, r_2, \ldots, r_t\}$ of rational numbers,

$$\langle r_1 + \mathbb{Z}, r_2 + \mathbb{Z}, \ldots, r_t + \mathbb{Z} \rangle \neq \mathbb{Q}/\mathbb{Z}$$

This shows that the group $\mathbb{Q}/\mathbb{Z}$ is not finitely generated.

We can also consider the multiplicative groups from familiar number systems.

Example 2.8.2. As we noted in Section 1.1 there is both an additive and a multiplicative structure $\mathbb{Z}/n$, to the integers modulo n. For an integer a that is comprime to n there are integers u, v such that $ua + nv = 1$ by the GCD theorem. Then u is the multiplicative inverse of a modulo n. The converse is also true, if $a + n\mathbb{Z}$ has multiplicative inverse $u + n\mathbb{Z}$ then ua differs from a multiple of n by 1, so the GCD of a and n is 1. The set of **units** in $\mathbb{Z}_n$, is the set of those elements with a multiplicative inverse. One can check that this set forms an abelian group under multiplication, written U_n: 1 is the identity element, every element has an inverse by definition, the product of two units is also a unit (with $(ab)^{-1} = a^{-1}b^{-1}$), and multiplication is associative and commutative.

For a prime number p, every nonzero element in $\mathbb{Z}/p$ is a unit, so $\mathbb{Z}/p$ is a field. When considering it as a field we will write it $\mathbb{F}_p$.

Exercises 2.8.3.

(a) Prove that $\operatorname{Aut}(\mathbb{Z}_n) \cong U_n$, the group of units in $\mathbb{Z}_n$.

(b) We will prove in Section 3.2 that every finite abelian group is isomorphic to a cyclic group or a direct product of such. For each of $n = 8, 9, 10, 11, 12$ find the product of cyclic groups that is isomorphic to U_n.

Returning to the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, we now consider their multiplicative groups $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$.

Example 2.8.4. In $\mathbb{Q}^*$, the subgroup generated by 2 is $\{2^i : i \in \mathbb{Z}\}$. The subgroup generated by 2 and 2 is $\langle 2, 3\rangle = \{2^i 3^j : i, j \in \mathbb{Z}\}$. There is only one element of finite order in $\mathbb{Q}^*$, other than the identity element, namely -1, which has order 2.

Similarly the only non-identity element of $\mathbb{R}^*$ which has finite order is -1. To get elements of order n we are, in effect, looking for solutions of $x^n - 1$, that is nth roots of unity. These live in the complex number field $\mathbb{C}$.

Exercises 2.8.5. An isomorpism between an additive group and a multiplicative group.

(a) Show that there is a homomorphism from $\mathbb{Q}, +$ to $\mathbb{C}^*, *$, namely $a \longmapsto e^{a2\pi i}$.

(b) Show that the image is the set of all nth roots of unity (for $n \in \mathbb{N}$) and that this forms a subgroup of $\mathbb{C}^*$ under multiplication.

(c) What is the kernel?

Exercises 2.8.6.

(a) Show that the positive rational numbers $\mathbb{Q}^{**} = \{a \in \mathbb{Q} : a > 0\}$ form a subgroup of $\mathbb{Q}^*$.

(b) Show that $\mathbb{Q}^*$ is isomorphic to the direct product of $\mathbb{Q}^{**}$ and $\langle -1\rangle$.

(c) Extend this result to the multiplicative group of the real numbers, $\mathbb{R}^*$.

Matrix Groups

We will work primarily with matrix groups over the fields, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{F}_p$, but the general results below are true for any field, so we express them for a general field F. We denote the multiplicative group of F by F^*.

Definition 2.8.7. Let F be a field and let n be an integer. The set of $n \times n$ matrices over F with nonzero determinant is called the **General Linear Group** and is written $\mathrm{GL}_n(F)$. The subgroup consisting of the matrices with determinant 1 is the **Special Linear Group** and is written $\mathrm{SL}_n(F)$. The next proposition shows that these are indeed groups with the identity matrix, I_n as identity element.

Proposition 2.8.8. *Let F be a field and let n be an integer. The set of $n \times n$ matrices over F with nonzero determinant forms a group. The determinant function*

$$\det : \mathrm{GL}_n(F) \longrightarrow F$$

is a homomorphism, and its kernel is $\mathrm{SL}_n(F)$.

Proof. Matrix multiplication is associative: One can show that for $n \times n$ matrices A, B, C, the i, j component of the product of $A(BC)$ and of $(AB)C$ is

$$\sum_{s=1}^{n} \sum_{t=1}^{n} a_{is} b_{st} c_{tj}$$

Thus $A(BC) = (AB)C$. (Associativity holds for any product of matrices that is well defined. We are treating the special case where they are all square of the same dimension.)

The result from linear algebra (which we assume here) that the determinant of a product of two matrices is the product of their determinants shows, in particular, that the product of two matrices with nonzero determinant also has nonzero determinant. So $\mathrm{GL}_n(F)$ is closed under multiplication. The identity matrix, I_n, and the usual formula for the inverse of a matrix perform the expected roles to make $\mathrm{GL}_n(F)$ a group. The determinant function respects products, so it gives a homomorphism to F. The kernel is the subgroup of matrices with determinant 1, that is $\mathrm{SL}_n(F)$. □

Exercises 2.8.9. There are many interesting subgroups of the general linear group.

(a) Show that the general linear group has these subgroups:

- The diagonal matrices with nonzero entries on the diagonal.
- The matrices of the form aI_n for $a \in F$ are called the constant diagonal matrices. Taking a nonzero we get the subgroup $F^* I_n$ of $\mathrm{GL}_n(F)$. Show that $F^* I_n$ is the center of $\mathrm{GL}_n(F)$ when $n > 1$.
- The upper triangular matrices with nonzero entries on the diagonal.
- The **orthogonal group** $\mathrm{O}(n, F)$ is the group of matrices Q such that Q^{-1} is the transpose of Q.

(b) For any subgroup H of F^* the set of all matrices with determinant in H is a subgroup of $\mathrm{GL}(n, F)$.

There are two other matrix groups of particular interest. In the exercises above, it is claimed that, for $n > 1$, the constant diagonal matrices, $F^* I_n$ form the center of $\mathrm{GL}_n(F)$. In particular $F^* I_n$ is normal in $\mathrm{GL}_n(F)$.

Definition 2.8.10. The quotient group $\mathrm{GL}_n(F)/F^*I_n$ is called the **Projective General Linear Group** and is written $\mathrm{PGL}_n(F)$. The quotient group $\mathrm{SL}_n(F)/\Big(F^*I_n \cap \mathrm{SL}_n(F)\Big)$ is called the **Projective Special Linear Group** and is written $\mathrm{PSL}_n(F)$.

Exercises 2.8.11.

(a) Show that the subgroup of upper triangular 2×2 matrices is conjugate to the group of lower triangular matrices. [Hint: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.]

(b) Show that the set of matrices with nonzero determinant of the form $\begin{bmatrix} 0 & a \\ b & c \end{bmatrix}$ is a coset of the upper triangular matrices.

Example 2.8.12. In $\mathrm{GL}(2, \mathbb{C})$ consider the matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad C = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

The set of matrices $Q = \{\pm I, \pm A, \pm B, \pm C\}$ is called the quaternion matrix group.

Exercises 2.8.13.

(a) Show by brute force that the quaternion matrix group is indeed a group.

(b) Find the order of each element of Q.

(c) Show that no two of the groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, D_4, and Q are isomorphic. [Investigate the number of elements of order 4.]

Exercises 2.8.14.

(a) Show that D_4 is isomorphic to the matrix group with elements $\{\pm I, \pm A, \pm B, \pm C\}$ where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(b) Draw the lattice diagram for this matrix group (it looks just like D_4, but use the elements here).

(c) More generally find a subgroup of $\mathrm{GL}_2(\mathbb{R})$ that is isomorphic to D_n. (Remember your trigonometry.)

Another interesting class of matrices is permutation matrices. Let $\sigma \in S_n$. Consider the matrix P^σ that has a single 1 in each column with the other entries being 0, specifically, $P^\sigma_{i,\sigma(i)} = 1$. Notice that P^σ can be considered as a matrix over any field F. For $v \in F^n$, and $i \in \{1, \dots, n\}$ the $\sigma(i)$ component of the vector $P^\sigma(v)$ is v_i. So, P^σ permutes the components of v. Another way to say this is that the ith component of $P^\sigma(v)$ is $v_{\sigma^{-1}(i)}$.

In particular, the null space of P^σ is trivial, so $P^\sigma \in \mathrm{GL}_n(F)$.

Proposition 2.8.15. *The function from S_n to $\mathrm{GL}_n(F)$ taking σ to P^σ is an injective homomorphism.*

Proof. We must check that $P^\pi P^\sigma = P^{\pi\sigma}$, which we do by verifying that for any $v \in F^n$, the ith components of $P^\pi\big(P^\sigma(v)\big) = P^{\pi\sigma}(v)$ are the same. The ith component of $P^{\pi\sigma}(v)$ is $v_{(\pi\sigma)^{-1}(i)}$. The ith component of $P^\pi\big(P^\sigma(v)\big)$ is the $\pi^{-1}(i)$ component of $P^\sigma(v)$, which is the $\sigma^{-1}\big(\pi^{-1}(i)\big)$ component of v. Since $\pi\sigma = \sigma^{-1}\pi^{-1}$, the two matrices $P^\pi P^\sigma$ and $P^{\pi\sigma}$ are giving the same answer.

Injectivity is clear because the only permutation σ such that p^σ takes each basis vector to itself is the identity permutation.

□

2.9 Structure in the Quotient Group: The Third Isomorphism Theorem and the Correspondence Theorem

The next step is to understand the structure of a quotient group. The two main results—the third isomorphism theorem and the correspondence theorem—have fairly simple statements, which obscure some subtle issues. The proof of the third isomorphism theorem is a consequence of the first isomorphism theorem.

Theorem 2.9.1 (Third Isomorphism)**.** *Let N and K be normal subgroups of G with K contained in N. Then N/K is a normal subgroup of G/K and*

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

Proof. We have two well defined quotient groups of G: G/K and G/N. I claim that there is a well-defined function from G/K to G/N taking gK to gN. To prove this, we have to check that if two cosets aK and bK are equal then the cosets aN and bN are also equal. Suppose $aK = bK$. Then $a^{-1}b \in K$ and since $K \subseteq N$ we have $a^{-1}b \in N$. Consequently $aN = bN$, so there is a function taking aK to aN.

It is easy to check that the function $\varphi : G/K \longrightarrow G/N$ defined above is surjective and a homomorphism. Given any gN there is an element, namely gK, that clearly maps to it, $\varphi(gK) = gN$, so we get surjectivity. Finally, φ respects multiplication: $\varphi(gK * g'K) = \varphi(gg'K) = gg'N = gN * g'N = \varphi(gK) * \varphi(g'K)$

The kernel of φ is $\{gK : gN = eN\}$. But $gN = eN$ if and only if $g \in N$. So the kernel is N/K. Applying the First Isomorphism Theorem 2.7.9 to $\varphi : G/K \longrightarrow G/N$,

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

□

The more powerful theorem is the correspondence theorem, which we may be seen as a strengthening of the First Isomorphism Theorem. Before stating it, let us recall some simple facts about functions. Let $f : X \to Y$ and let $A \subseteq X$ and $B \subseteq Y$. Then $A \subseteq f^{-1}(f(A))$ because for any $a \in A$, $a \in f^{-1}(f(a)$. On the other hand, for an element $b \in B$, if x is a preimage of b then $f(x) = b$, but there may be no preimage for b, so we know only that $f(f^{-1}(B)) \subseteq B$. But, if f is surjective then for each $b \in B$ there is some $x \in X$ such that $f(x) = b$. Thus for f surjective, $f(f^{-1}(B)) = B$. Respecting containment is also immediate: If $A \subseteq A' \subseteq X$ then $f(A) \subseteq f(A')$ and similarly if $B \subseteq B' \subseteq Y$ then $f^{-1}(B) \subseteq f^{-1}(B')$.

Theorem 2.9.2 (Correspondence)**.** *Let $\varphi : G \longrightarrow H$ be a surjective homomorphism with kernel K. There is a one-to-one correspondence, given by φ, between subgroups of G/K and subgroups of G containing K.*

$$\begin{aligned} G &\longrightarrow H \\ A &\longleftrightarrow \varphi(A) \\ \varphi^{-1}(B) &\longleftrightarrow B \end{aligned}$$

The correspondence respects containment, normality, and quotients as follows. For A, A' containing K,

- *$K \leq A \leq A'$ if and only if $\varphi(A) \leq \varphi(A')$.*
- *A is normal in G if and only if $\varphi(A)$ is normal in H.*
- *When A is normal in G, the map φ induces an isomorphism $G/A \cong H/\varphi(A)$.*

Proof. Let A be a subgroup of G containing K and let B be a subgroup of H. From Proposition 2.2.5 we know that $\varphi(A)$ is a subgroup of H and $\varphi^{-1}(B)$ is a subgroup of G. Based on the above discussion, we know $\varphi(\varphi^{-1}(B)) = B$ and $A \subseteq \varphi^{-1}(\varphi(A)$ so we need to show that $\varphi^{-1}(\varphi(A)) \subseteq A$ to get the one-to-one correspondence. Let $g \in \varphi^{-1}(\varphi(A))$. Then $\varphi(g) = \varphi(a)$ for some $a \in A$. Consequently, $\varphi(ga^{-1}) = e_H$ and therefore $ga^{-1} \in \ker(\varphi) = K$. Since $K \subseteq A$, $ga^{-1} \in A$ so $g \in A$. Thus $\varphi^{-1}(\varphi(A)) = A$. Thus, we have established the one-to-one correspondence.

We have also shown in a problem in Exercise 2.7.6 that if B is normal in H then $\varphi^{-1}(B)$ is normal. These results are true for an arbitrary homomorphism. Let's now show that when φ is surjective, if A is normal in G then $\varphi(A)$ is normal in H.

Let $h \in H$. We need to show $h\varphi(A)h^{-1} = \varphi(A)$, or equivalently, $h\varphi(a)h^{-1} \in \varphi(A)$ for all $a \in A$. Since φ is surjective, there is some $g \in G$ such that $\varphi(g) = h$.

$$h\varphi(a)h^{-1} = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(gag^{-1}) \in \varphi(A)$$

The last step holds because A is normal in G, so $gag^{-1} \in A$.

Now we apply the first isomorphism theorem. Let B be normal in H. We have a composition of surjective homomorphisms

$$G \longrightarrow H \longrightarrow H/B$$

whose kernel is $\varphi^{-1}(B)$. Letting $A = \varphi^{-1}(B)$, the first isomorphism theorem says that $G/A \cong H/\varphi(A)$. □

We can derive the Third Isomorphism Theorem as a corollary of the Correspondence Theorem.

Corollary 2.9.3 (Third Isomorphism Theorem)**.** *Let KN and N be normal subgroups of G with $K \leq N$. Then $G/N \cong (G/K)\Big/(N/K)$.*

Proof. Apply the correspondence theorem to $G \longrightarrow G/K$. The subgroup N of G corresponds to the subgroup N/K of G/K. Thus $G/N \cong (G/K)\Big/(N/K)$. □

The Third Isomorphism Theorem gives a framework for understanding the lattices of subgroups

ADD EXAMPLES

$\mathbb{Z}_n$

$\mathbb{Z}_4 \times \mathbb{Z}_4$

Exercises 2.9.4. For each of the following groups G and for each of the normal subgroups $N \trianglelefteq G$, identify the sublattice of the G that has the same structure as the lattice of the quotient group G/N.

(a) D_4

(b) A_4

2.10 Problems

Exercises 2.10.1. Define a *hemigroup* to be a set G with an operation $*$ that is associative, has an identity element, and such that each element has a *right* inverse.

(a) Show that the right inverse of a is also a left inverse of a, so that a hemigroup is actually a group.

Exercises 2.10.2. Let $(U_n, *)$ be the group of invertible elements of $\mathbb{Z}_n$. Find all n such that $(U_n, *)$ is isomorphic to

(a) $(\mathbb{Z}_2, +)$;

(b) $(\mathbb{Z}_4, +)$;

(c) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

Exercises 2.10.3. Some subgroups of abelian groups. Let A be an abelian group and let m be an integer.

(a) Show that multiplication by m gives a homomorphism of A:

$$\begin{aligned} \varphi_m : A &\longrightarrow A \\ a &\longrightarrow ma \end{aligned}$$

(b) Show that the image and kernel are the groups mA and $A[m]$ from Exercise 2.1.19.

(c) If A is a finite group that has no elements of order m then multiplication by m gives an isomorphism of A.

(d) If m and n are coprime show that $A[m] \cap A[n] = \{0\}$.

Exercises 2.10.4. The torsion subgroup of an abelian group. Let A be an infinite abelian group. Let $\operatorname{Tor}(A)$ be the set of elements with finite order, which is called the **torsion subgroup** of A.

(a) Show that $\operatorname{Tor}(A)$ is, indeed, a normal subgroup of A.

(b) Show that $\operatorname{Tor}(A) = \bigcup_{m \in \mathbb{N}} A[m]$. (Note that, even inside an abelian group, the union of subgroups is not usually a group!)

(c) Show that $\operatorname{Tor}(A/\operatorname{Tor}(A))$ is trivial. That is, letting $T = \operatorname{Tor}(A)$, the only element of finite order in A/T is the identity element, $e + T$.

(d) Give an example of a finitely generated abelian group in which the identity element together with the elements of infinite order do *not* form a subgroup. (As opposed to the torsion subgroup.)

Exercises 2.10.5. "Almost" abelian groups. A group is **metabelian** when it has a normal subgroup N such that N and G/N are both abelian. A group is

metacyclic when it has a normal subgroup N such that N and G/N are both cyclic.

(a) Show that S_3 is metacyclic.

(b) Show that A_4 is metabelian but not metacyclic.

(c) Prove that any subgroup of a metabelian group is also metabelian.

(d) Prove that any quotient group of a metabelian group is metabelian. [Look carefully at the proof of the 2nd isomorphism theorem and adapt it to this question.]

Exercises 2.10.6. A matrix group. Let G be the group of all matrices of the form with $a, b, c \in \mathbb{Q}$.

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

(a) Find the center C of G and show that C is isomorphic to the additive group $\mathbb{Q}$.

(b) Show that G/C is isomorphic to $\mathbb{Q} \times \mathbb{Q}$.

(c) Conclude that G is metabelian.

Exercises 2.10.7. Let $H = H(F)$ be the set of 3 by 3 upper triangular matrices over a field F with 1s on the diagonal.

(a) Give a brief explanation of why this is indeed a subgroup of $\mathrm{GL}(3, F)$.

(b) Show that the following 3 types of matrices generate this group.

$$\begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$$

(c) Let $F = \mathbb{F}_p$. Explain why H is then generated by 3 matrices, those in the form above with $a = b = c = 1$.

(d) Show that $H(\mathbb{F}_2) \cong D_4$.

(e) (HW) Show that the center $Z(H)$ consists of all matrices of the form $\begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Furthermore $Z(H) \cong (F, +)$.

(f) (HW) Show that $H/Z(H)$ is isomorphic to $F \times F$.

(g) (HW) Conclude that H is metabelian.

Exercises 2.10.8. Upper triangular matrices.

(a) Let F be a field and let F^* be its multiplicative group. Show that there is a homomorphism

$$\begin{aligned}\{\text{upper triangular matrices in } \mathrm{GL}(2,F)\} &\longrightarrow (F^*)^2\\ \begin{bmatrix} a & b\\ 0 & c\end{bmatrix} &\longmapsto (a,c)\end{aligned}$$

(b) Show that kernel is isomorphic to $(F,+)$ the additive group of F.

Exercises 2.10.9. General linear group.

(a) Which has more elements, unit group of $\mathrm{Mat}(2,\mathbb{Z}/4)$ or $\mathrm{GL}(2,\mathbb{F}_4)$? Find the number of elements in each and characterize $U(\mathrm{Mat}(2,\mathbb{Z}_4)$.

(b) Try to generalize: How many elements are there in $\mathrm{GL}(n,\mathbb{F}_p)$? In $\mathrm{SL}(n,\mathbb{F}_p)$?

Exercises 2.10.10. Some normal subgroups

(a) Show that the intersection of two normal subgroups of G is normal in G.

(b) Let G be a group, possibly infinite. Let I be some indexing set and for each $i \in I$ let H_i be a subgroup of G. Prove that for any $a \in G$,

$$a\Big(\bigcap_{i\in I} H_i\Big)a^{-1} = \bigcap_{i\in I} aH_ia^{-1}$$

(c) Let H be a subgroup of G and let $N = \bigcap_{g\in G} g^{-1}Hg$. Prove that N is normal in G.

(d) Let $n \in \mathbb{N}$ and let K be the intersection of all subgroups of G of order n. Prove that K is normal in G.

An earlier exercise showed that every group of index 2 is normal. Here is a generalization due to Lam [MAA Monthly Mar. 2004 p. 256].

Theorem 2.10.11. *Let H be a subgroup of G with $[G : H] = p$ a prime number. The following are equivalent.*

(1) H is normal in G.

(2) For any $a \in G \setminus H$, $a^p \in H$.

(3) For any $a \in G \setminus H$, $a^n \in H$ for some positive integer n that has no prime divisor less than p.

(4) For any $a \in G - H$, $a^2, a^3, \ldots, a^{p-1} \notin H$.

Exercises 2.10.12.

(a) Prove Lam's theorem by showing (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) $\Longrightarrow$ (1). The last step is the one requiring some cleverness.

(b) Show that Lam's theorem implies that any group whose index is the smallest prime dividing $|G|$ is normal in G.

Exercises 2.10.13. Inner automorphisms of a group. For $a \in G$ let φ_a be the **inner automorphism** defined by a and consider the function $\varphi : a \longmapsto \varphi_a$.

$$\begin{aligned} \varphi_a : G &\longrightarrow G \\ g &\longmapsto aga^{-1} \end{aligned} \qquad\qquad \begin{aligned} \varphi : G &\longrightarrow \mathrm{Aut}(G) \\ a &\longmapsto \varphi_a \end{aligned}$$

Clearly $\mathrm{im}(\varphi) = \mathrm{Inn}(G)$.

(a) Show that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

(b) Show that φ is a homomorphism and that $\mathrm{im}(\varphi) \cong G/Z(G)$.

Exercises 2.10.14. Computing some simple automorphism groups.

(a) Compute $\mathrm{Aut}(Q)$ for Q the quaternion matrix group.

(b) Show that $\mathrm{Aut}(D_4) \cong D_4$

Exercises 2.10.15. Automorphism group of $\mathbb{Z}/p^n$.

(a) Prove that $\mathrm{Aut}(\mathbb{F}_p^2) \cong \mathrm{GL}(2, \mathbb{F}_p)$ for p prime.

(b) Find an element of $\mathrm{Aut}(\mathbb{F}_4 \times \mathbb{F}_4)$ that is not in $\mathrm{GL}(2, \mathbb{F}_4)$.

Exercises 2.10.16. Classification of the groups of order 8. Let G be a group of order 8. Prove each of the following.

(a) If G has an element of order 8 then $G \cong \mathbb{Z}_8$.

(b) If every nonzero element of G has order 2 then G is abelian and isomorphic to $\mathbb{Z}_8$.

(c) Suppose G has no element of order 8 and some element $a \in G$ has order 4.

- If G is abelian then it is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.
- NEED TO FINISH! If G

Exercises 2.10.17. Symmetries of a solid.

(a) Enumerate the faces of a tetrahedron as follows. Each rigid motion from the tetrahedron to itself defines a permutation of the vertices. There are 12 such permutations. Write them down in an organized fashion, and briefly describe each.

(b) Enumerate the faces of a cube as follows. Each rigid motion from the cube to itself defines a permutation of the vertices. There are 24 such permutations. Write them down in an organized fashion, and briefly describe each.

Exercises 2.10.18. Counting in S_n.

(a) How many k-cycles are there in S_n?

(b) How many product of disjoint transpositions are there in S_n?

Exercises 2.10.19.

(a) Let A_1, A_2, B_1, B_2 be normal subgroups of a group G with $B_1 \leq A_1$ and $B_2 \leq A_2$ and finally $A_1 \cap A_2 = \{1\}$. Then B_1B_2 is normal subgroup in A_1A_2 and there holds

$$(A_1A_2)/(B_1B_2) \cong (A_1/B_1) \oplus (A_2/B_2).$$

v

Exercises 2.10.20. The normalizer and centralizer of a subgroup. Let K be a subgroup of G and define

$$N_G(K) = \{g \in G : gKg^{-1} = K\}$$
$$C_G(K) = \{g \in G : gkg^{-1} = k \text{ for all } k \in K\}$$

These are called the **normalizer** of K in G and the **centralizer** of K in G.

(a) Show that $N_G(K)$ is a subgroup of G.

(b) Show that K is a normal subgroup of $N_G(K)$.

(c) If $H \leq G$ and K is a normal subgroup of H show that $H \leq N_G(H)$. So, $N_G(K)$ is the largest subgroup of G in which K is normal.

(d) Show that $C_G(K)$ is a normal subgroup of $N_G(K)$.

(e) Show that $N_G(K)/C_G(K)$ is isomorphic to a subgroup of $\mathrm{Aut}(K)$.

Exercises 2.10.21. The commutator subgroup. In a group G, the **commutator** of a, b is $aba^{-1}b^{-1}$. Notice that this is e_G iff a and b commute. The **commutator subgroup** of a group G is the group G' generated by the commutators.

$$G' = \langle aba^{-}b^{-1} : a, b \in G\rangle$$

(a) Compute the commutator subgroup of D_n (two cases: n odd and n even). Think of D_n as generated by r, t with $r^n = t^2 = e$ and $tr = r^{n-1}t$.

(b) Write down the commutator of the conjugation of a by x and the conjugation of b by x.

(c) Prove that G' is a normal subgroup of G. It is enough to show that the conjugation of any commutator is another commutator.

(d) Prove that G/G' is abelian.

(e) Prove that G/N abelian implies $G' \leq N$. So, the commutator subgroup of G is the smallest normal subgroup N group such that the quotient G/N is abelian.

Exercises 2.10.22. Let G be a group. For $a, b \in G$ define the commutator $[a, b] := aba^{-1}b^{-1}$ of a and b. For arbitrary subgroups U, V of G define $[U, V] := \langle [u, v] \mid u \in U, v \in V \rangle$. Now show the following:

(a) If U, V are normal subgroups of G, then so is $[U, V]$.

(b) $[G, G]$ is the smallest normal subgroup of G for which the quotient group is abelian.

(c) Setting $G^{(0)} := G$ and $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$ for all $i \in \mathbb{N}$, we find that G is solvable if and only if there exists $n \in \mathbb{N}$ such that $G^{(n)} = \{1\}$.

(d) For $n \geq 5$ let U be a subgroup of S_n and N a normal subgroup of U for which U/N is abelian. Show that if U contains all 3-cycles of S_n, then also N will contain these.

Hint: If $a, b, c, d, e \in \{1, \ldots, n\}$ are distinct elements, then there holds the equation

$$(a, b, c) = (a, b, d)(c, e, a)(d, b, a)(a, e, c).$$

(e) Show that this implies that the symmetric group S_n is not solvable for $n \geq 5$.

Chapter 3

Classification and Structure of Groups

3.1 Interaction between Two Subgroups: The Second Isomorphism Theorem and Semi-Direct Products

We now consider two subgroups of a group G and prove several results about the interaction between them. At first we make no additional assumptions on the two subgroups groups, then we assume that one is normal in G, and finally that both are. The main result is the second isomorphism theorem. But,we also get two key corollaries that introduce the notion of an internal direct product (as opposed to the external direct product that we have been using), and the more general notion of a semi-direct product (both internal and external).

Lemma 3.1.1. *Let K, H be subgroups of G. The following are equivalent:*

(1) $G = KH$ and $K \cap H = \{e_G\}$

(2) Every element of G can be uniquely written as kh for $k \in K$ and $h \in H$.

Proof. $G = KH$ is equivalent to saying that every element of G can be written in the form kh. We'll next show $K \cap H = \{e_G\}$ if and only if any expression for $g \in G$ as a product kh, with $k \in K$ and $h \in H$, is unique.

Suppose $K \cap H = \{e_G\}$ and $k_1h_1 = k_2h_2$. Then $k_1^{-1}k_2 = h_1h_2^{-1}$. Since this is in both K and in H, it must be the identity. Therefore, $h_1 = h_2$ and $k_1 = k_2$, which proves uniqueness.

Now suppose that $K \cap H \neq e_G$; say $g \in K \cap H$ is not equal to e_G. Setting $h = g$ and $k = e_G$ gives one way to express g in the form kh, while setting $h = e_G$ and $k = g$ gives a different way. Thus we have non-uniqueness. □

As another prelude to the second isomorphism theorem we have the following lemma. We will use a concise argument to prove a subset B of a group G is a subgroup. We show that $B^{-1} \subseteq B$ (closure under inversion) and $BB \subseteq B$ (closure under products).

Lemma 3.1.2. *Let H, K be subgroups of G.*

$$HK = KH \qquad \Longleftrightarrow KH \text{ is a subgroup of } G$$

Proof. Suppose $HK = KH$ we will show KH is a subgroup of G. We see KH is closed under inversion: $(kh)^{-1} = h^{-1}k^{-1} \in HK = KH$. We can show that KH is also closed under products with an element-wise argument, but let's use the associativity identified in Notation 2.6.1,

$$(KH)(KH) = K(HK)H = K(KH)H = (KK)(HH) = KH.$$

Since KH is closed under inversion and under products, it is a subgroup of G.

Suppose KH is a subgroup of G. Since KH is closed under inversion, $KH = (KH)^{-1} = H^{-1}K^{-1} = HK$. This gives the reverse implication of the lemma. □

Suppose now that H, N are subgroups of G with N *normal in* G. We can conclude the following.

- $HN = NH$ since $gN = Ng$ for any $g \in G$.
- HN is therefore a subgroup of G by the lemma.
- N is normal in HN, since it is normal in any subgroup of G that contains it.

Theorem 3.1.3 (Second Isomorphism)**.** *Let N be normal in G and H a subgroup of G. Then $HN \cap N$ is normal in H and $H/(H \cap N) \cong HN/N$.*

When these groups are finite we may take cardinalities to get

$$|H||N| = |HN||H \cap N|$$

Proof. Consider $G \xrightarrow{\pi} G/N$ restricted to the subgroup H, and call the restricted homomorphism $\pi' : H \longrightarrow G/N$. The kernel of π' is $H \cap N$. The image is $HN/N = \{hN : h \in H\}$ and HN is a subgroup of G as we noted above. By the first isomorphism theorem, $H/(H \cap N) \cong HN/N$. □

The following special case is of interest. It combines the assumptions of Theorem 3.1.3 with those of Lemma 3.1.1.

Corollary 3.1.4. *Let H and N be subgroups of G with $N \trianglelefteq G$. Suppose $G = HN$ and $H \cap N = \{e_G\}$. Then $G/N \cong H$.*

Proof. One simply substitutes G for HN and notes $H \cong H/\langle e_G \rangle$. □

Definition 3.1.5. In the situation of the corollary we say that G is the **internal semi-direct product** of N by H and we write $G \cong N \rtimes H$.

Note that the order is important: $N \rtimes H$ and $H \rtimes N$ mean two different things. The first assumes N is normal in G and the second assumes H is normal in G.

If both H and N are normal then the two semidirect products are isomorphic to each other and to the direct product, as the following corollary shows.

Corollary 3.1.6. *Suppose $K \trianglelefteq G$ and $N \trianglelefteq G$ and $G = KN$ and $K \cap N = \{e_G\}$. Then elements of K and N commute: for any $k \in K$ and $n \in N$, $kn = nk$. Furthermore, $G \cong K \times N$.*

Proof. To prove that elements of K and N commute with each other it is sufficient to show that $knk^{-1}n^{-1} = e$. Since N is normal, $knk^{-1} \in N$ and therefore $knk^{-1}n^{-1} \in N$. Similarly, since K is normal, $nk^{-1}n^{-1} \in K$ so $knk^{-1}n^{-1} \in K$. Now $K \cap N = \{e\}$ gives the result.

Consider the map $K \times N \xrightarrow{\varphi} G$ defined by $(k, n) \longmapsto kn$. The map is well defined. It is injective since $kn = e$ gives $k = n^{-1} \in K \cap N = \{e\}$. It is surjective since $G = KN$. It respects multiplication (so is a homomorphism):

$$\begin{aligned}
\varphi\big((k_1, n_1)\big)\varphi\big((k_2, n_2)\big) &= (k_1n_1)(k_2n_2)\\
&= k_1(n_1k_2)n_2\\
&= k_1(k_2n_1)n_2\\
&= (k_1k_2)(n_1n_2)\\
&= \varphi\big((k_1k_2, n_1n_2)\big)\\
&= \varphi\big((k_1, n_1)(k_2, n_2)\big)
\end{aligned}$$

Thus φ is an isomorphism. □

Definition 3.1.7. In the situation of the last corollary, G is often called the **internal direct product** of K and N.

The distinction between internal direct product and the usual (external) direct product of two arbitrary groups G and H is subtle as the next examples show. The first example shows that the external direct product of two groups is also the internal direct product of two of its subgroups (in a way that seems perhaps pedantic). The second example shows the real motivation for distinguishing internal direct products, they can be rather hidden, and give insight into the structure of a group.

Example 3.1.8. Let G and H be two groups and consider the external direct product $G \times H$. Let $\overline{G} = G \times \{e_H\}$ and similarly $\overline{H} = \{e_G\} \times H$. The interesection of $\overline{G}$ and $\overline{H}$ is the identity element of $G \times H$ and it is easy to see that every element of $G \times H$ may be written as a product of something in $\overline{G}$ and $\overline{H}$. Thus $G \times H$ is the internal direct product of $\overline{G}$ and $\overline{H}$.

Example 3.1.9. Consider $\mathbb{Z}_6$. It has two proper subgroups $K = \{0, 3\}$ and $N = \{0, 2, 4\}$ both of which are normal since $\mathbb{Z}_6$ is abelian. It can be seen that everything in $\mathbb{Z}_6$ can be written as a sum of something in K and something in N, and clearly $K \cap N = \{0\}$. Thus $\mathbb{Z}_6$ is the internal direct product of H and K. Of course, in $\mathbb{Z}_6$, the subgroup $\{0, 3\}$ is isomorphic to $\mathbb{Z}_2$, and $\{0, 2, 4\}$ is isomorphic to $\mathbb{Z}_3$ and we know from Corollary 2.4.29 that $\mathbb{Z}_6$ is isomorphic to the external direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$. More generally, for m and n coprime, $\mathbb{Z}_{mn}$ is the internal direct product of its subgroups $\langle m \rangle$ and $\langle n \rangle$.

One can also define the external semi-direct product of of two groups.

Definition 3.1.10. Let N, H be two groups and let $\varphi : H \longrightarrow \mathrm{Aut}(N)$ be a homomorphism. Write $\varphi(h)$ as φ_h. Define a new group with elements $N \times H$ and multiplication defined by

$$(n_1, h_1) * (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1, h_2)$$

This is the **external semi-direct product** of N and H defined by φ and is written $N \rtimes_\varphi H$.

The relationship between the internal and external semi-direct product is even more subtle than that for the internal and external direct product. Consider a group G with two subgroups N, H with N normal and H not normal and such that $NH = G$ and $N \cap H = \{e\}$. There is a bijective map from the Cartesian product $N \times H$ to G taking (n, h) to nh. It is not a homomorphism. But it is true that in G,

$$\begin{aligned} n_1 h_1 n_2 h_2 &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 \\ &= n_1 \varphi_{h_1}(n_2) h_1 h_2 \end{aligned}$$

Where φ_{h_1} is conjugation by h_1. Because N is normal in G, φ_h is an automorphism of N and, indeed, we have a homomorphism $\varphi : H \longrightarrow \operatorname{Aut}(N)$ that takes h to φ_h. Thus, if we use φ to to define the external semi-direct product $N \trianglelefteq_\varphi H$ we get an isomorphism with G.

Exercises 3.1.11. The definition of external semi-direct product makes sense!

(a) Verify that (e_H, e_K) is the identity element.

(b) Show that each element does have an inverse.

(c) Show that the associative law holds.

Exercises 3.1.12. Verify the following are semi-direct products.

(a) $D_n \cong C_n \rtimes_\varphi C_2$ where $\varphi : C_2 \longrightarrow \operatorname{Aut}(C_n)$ takes the non-identity element of C_2 to the automorphism of C_n taking n to n^{-1}.

(b) $S_n = A_n \rtimes \langle(1,2)\rangle$. What is the map φ?

(c) $S_4 = V \rtimes S_3$ where V is Klein-4 subgroup with elements of the form $(a,b)(c,d)$ with a, b, c, d distinct elements of $\{1,2,3,4\}$. What is the map φ?

(d) In $\mathrm{GL}_n(F)$, for F a field, let T be the upper triangular matrices with nonzeros on the diagonal; let U be the upper triangular matrices with 1's on the diagonal and let D be the diagonal matrices with nonzero elements on the diagonal. For $n = 2$, show that $T = U \rtimes D$. Describe the map $\varphi : D \longrightarrow \operatorname{Aut}(U)$.

(e) Do the previous problem for arbitrary n.

Proposition 3.1.13. *Let N be a normal subgroup of G and let $\pi : G \longrightarrow G/N$ be the quotient homomorphism. Suppose that there is a homomorphism $\alpha : G/N \longrightarrow G$ such that $\pi \circ \alpha$ is the identity map on G/N. Then G is the internal direct product $N \rtimes \alpha(G/N)$.*

Proof. Let the image of α be $H = \alpha(G/N)$, which is a subgroup of G. By Corollary 3.1.4, we need only show that $HN = G$ and that $H \cap N$ is trivial.

Let $g \in G$. Let $h = \alpha \circ \pi(g)$. This is an element of H, since it is in the image of α. I claim $gh^{-1} \in N$. This is because

$$\begin{aligned}\pi(gh^{-1}) &= \pi(g)\pi(h^{-1}) = \pi(g)\pi\big(\alpha \circ \pi(g^{-1})\big) = \pi(g)\big(\pi \circ \alpha \circ \pi\big)(g^{-1})\big) \\ &= \pi(g)(\pi(g^{-1})\big) = \pi(g)\pi(g^{-1}) = eN\end{aligned}$$

Consequently $gh^{-1} = n$ for some $n \in N$ and therefor $g = hn$. Since g was an arbitrary element of G we have shown $G = HN$.

Now suppose that $h \in H \cap N$. Since $h \in H$, there is some $gN \in G/N$ such that $h = \alpha(gN)$. We know that $\pi \circ \alpha$ is the identity on H, so

$$\alpha\Big(\pi\big(\alpha(g)\big)\Big) = \big(\alpha \circ \pi\big)\big(\alpha(g)\big) = \alpha(g) = h.$$

On the other hand, since $h \in N$,

$$\alpha\Big(\pi\big(\alpha(g)\big)\Big) = \alpha\big(\pi(h)\big) = \alpha(eN) = e.$$

Consequently, $h = e$ and we have shown $H \cap N = \{e\}$. $\square$

Exercises 3.1.14. Let F be a field. Let $\mathrm{GL}_n(F)$ be the general linear group: $n \times n$ matrices over F with nonzero determinant. Let $\mathrm{SL}_n(F))$ be the special linear group: matrices with determinant 1. Let F^*I be the nonzero multiples of the identity matrix. In this problem we investigate the finite fields F and values of n for which $\mathrm{GL}_n(F) \cong \mathrm{SL}_n(F) \times F^*I$.

(a) For the fields $F = \mathbb{F}_3$ and $F = \mathbb{F}_5$, show that $\mathrm{GL}_n(F)$ is a direct product as above for n odd, but not for n even.

(b) For the field $F = \mathbb{F}_7$, show that $\mathrm{GL}_n(F)$ is a direct product as above for n coprime to 6, and is not otherwise.

(c) (Challenge) For which fields $\mathbb{F}_q$ and which n is $\mathrm{GL}_n(\mathbb{F}_q)$ a direct product as above?

Exercises 3.1.15. External semi-direct products of cyclic groups.

(a) Use the definition of external semi-direct product to create the other non-abelian group of order 12 (besides D_6 and A_4), $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ where φ is the only possible map $\mathbb{Z}_4 \longrightarrow \mathrm{Aut}(\mathbb{Z}_3)$ that is not trivial. Let a be the generator for $\mathbb{Z}_3$ and b the generator for $\mathbb{Z}_4$. Show the following:

(1) Every element can be represented uniquely as a^ib^j for $i \in \{0, 1, 2\}$ and $b \in \{0, 1, 2, 3\}$

(2) The group can be presented as $\langle a, b | a^3 = b^4 = 1, ba = a^2b\rangle$

(3) Find the inverse of a^ib^j.

(4) Find a general formula for $a^ib^j * a^mb^n$. It may be useful to break this into cases.

(b) Use the definition of external semi-direct product to create the only non-abelian group of order 21 (the smallest non-abelian group of odd order), $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$. Let a be the generator for $\mathbb{Z}_7$ and b the generator for $\mathbb{Z}_3$. Show how to represent, invert, and multiply elements of this group as you did in the previous problem.

(c) (Challenge Problem) Use the definition of external semi-direct product to construct semi-direct products $\mathbb{Z}_m \rtimes \mathbb{Z}_n$. You will need to start with a homomorphism $\varphi : \mathbb{Z}_n \longrightarrow \mathrm{Aut}(\mathbb{Z}_m)$. See how many of the small non-abelian groups you can find in the table of small abelian groups on Wikipedia.

3.2 Finitely Generated Abelian Groups

In this section we show that the structure of finitely generated abelian groups is fairly simple. Any finitely generated abelian group is isomorphic to a direct product of cyclic groups that can be put in a standard, uniquely determined, format. We proceed in several steps, each subsection below gives a complete story about a particular class of abelian groups; each extends the result of the previous subsection to a broader class of abelian groups.

Our first step is to show that a direct product of cyclic groups can be put into a standard format that elucidates its structure. There are actually two such formats, one using *elementary divisors* and the other using *invariant factors.* In particular, two groups are isomorphic if and only if their standard formats are the same. Our next step is to show that any *finite abelian* group is actually a direct product of cyclic groups, and it therefore can be placed in the two standard formats. This result has one very technical lemma whose proof we sketch. Finally, we state and prove some aspects of the more general result that any *finitely generated abelian* group can be written as a direct product of a finite group (with standard formats above) and a group that is isomorphic to $\mathbb{Z}^r$ for some integer r.

We will write the group operation additively. For A an abelian group, $a \in A$, and m an integer, we write mA for $a + \cdots + a$ with m summands. Think of ma as repeated addition, not multiplication. The order of a is the smallest positive integer m such that $ma = 0$. One can check that $ma + na = (m + n)a$ and $(mn)a = m(na)$. If B is a subgroup of A (it is normal since A is abelian) we write a coset as $a + B$ and the identity element of A/B is $0 + B$.

A key tool in this chapter is Corollary 2.4.29, which says that for coprime integers m and n the group $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$. The corollary says more, that there is a unique isomorphism that takes $[1]_{mn}$ to $\big([1]_m, [1]_n\big)$, but we only need the existence of the isomorphism in this section. An easy induction argument establishes the following result

Proposition 3.2.1. *Let $m_1, m_2, \ldots, m_t$ be pairwise coprime positive integers and let $m = \prod_{i=1}^{t} m_i$, then*

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$$

Products of Cyclic Groups

Let's start with abelian groups that we understand well, cyclic groups, and direct products of cyclic groups. The notation in the theorems below is a bit heavy, so we start with an example.

Example 3.2.2. Consider the group $\mathbb{Z}_{60} \times \mathbb{Z}_{12} \times \mathbb{Z}_8 \times \mathbb{Z}_{25}$. Using Proposition 3.2.1,

$$\begin{aligned}
\mathbb{Z}_{60} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
\mathbb{Z}_{12} &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \\
\mathbb{Z}_8 &\cong \mathbb{Z}_8 \\
\mathbb{Z}_{75} &\cong \mathbb{Z}_3 \times \mathbb{Z}_{25}
\end{aligned}$$

Let's take the direct product of all these factors ordering them by the prime involved (2, 3,or 5) and for each prime, the highest power of that prime first.

$$\begin{aligned}
\mathbb{Z}_{60} \times \mathbb{Z}_{12} \times \mathbb{Z}_8 \times \mathbb{Z}_{25} \cong \quad & \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \\
& \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
& \times \mathbb{Z}_{25} \times \mathbb{Z}_5
\end{aligned} \tag{3.1}$$

Now, we regroup by combining the highest powers of each prime.

$$\begin{aligned}
\cong \quad & \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\
& \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\
& \times \mathbb{Z}_4 \times \mathbb{Z}_3
\end{aligned}$$

Finally, we have

$$\mathbb{Z}_{60} \times \mathbb{Z}_{12} \times \mathbb{Z}_8 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{600} \times \mathbb{Z}_{60} \times \mathbb{Z}_{12} \tag{3.2}$$

Both factorizations are of interest: one (3.1) into cyclic groups of prime power order, the other (3.2) combining the factors prime power factors in a greedy fashion.

The following proofs are just adaptations of the computations in the example to deal with the general context.

Theorem 3.2.3. *Let $m_1, \ldots, m_t$ be positive integers and $A = \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t$. Let $P = \{p_1, \ldots, p_s\}$ be the set of all primes dividing $m_1 m_2 \cdots m_t$ and let the m_j have factorizations $m_j = \prod_{i=1}^{s} p_i^{e_{ij}}$ (allowing some $e_{ij} = 0$). Then*

$$A \cong A_1 \times \cdots \times A_s$$

where $A_i = \mathbb{Z}/p_i^{e_{i1}} \times \mathbb{Z}/p_i^{e_{i2}} \times \cdots \mathbb{Z}/p_i^{e_{it}}$.

Furthermore $|A_i| = p^{e_i}$ where $e_i = \sum_{j=1}^{t} e_{ij}$.

Proof. By Proposition 3.2.1, $\mathbb{Z}/m_j \cong \mathbb{Z}/p_1^{e_{1j}} \times \cdots \times \mathbb{Z}/p_s^{e_{sj}}$. Thus

$$\begin{aligned}
A = &\quad \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t \\
\cong &\quad \mathbb{Z}/p_1^{e_{11}} \times \cdots \times \mathbb{Z}/p_s^{e_{s1}} \\
&\times \mathbb{Z}/p_1^{e_{12}} \times \cdots \times \mathbb{Z}/p_s^{e_{s2}} \\
&\quad \cdots \\
&\times \mathbb{Z}/p_1^{e_{1t}} \times \cdots \times \mathbb{Z}/p_s^{e_{st}}
\end{aligned}$$

Rearranging terms so that the jth column of factors becomes the jth row, and the ith row becomes the ith column, we have

$$\begin{aligned}
\cong &\quad \mathbb{Z}/p_1^{e_{11}} \times \cdots \times \mathbb{Z}/p_1^{e_{1t}} \\
&\times \mathbb{Z}/p_2^{e_{21}} \times \cdots \times \mathbb{Z}/p_2^{e_{2t}} \\
&\quad \cdots \\
&\times \mathbb{Z}/p_s^{e_{s1}} \times \cdots \times \mathbb{Z}/p_s^{e_{st}} \\
\cong &\quad A_1 \times \cdots \times A_s
\end{aligned}$$

The cardinality of A_i is just the product of the cardinalities of its factors. So, letting $e_i = \sum_{j=1}^{t} e_{ij}$, we have $|A_i| = p^{e_i}$. □

Definition 3.2.4. The multiset $\left\{p_i^{e_{ij}} : i = 1, \ldots, s; \text{ and } j = 1, \ldots t\right\}$ is the set of **elementary divisors** of A.

Theorem 3.2.5. *With the notation of the previous theorem, for each i let $f_{i1} \geq f_{i2} \cdots \geq f_{it}$ be a permutation of the exponents $e_{i1}, \ldots e_{it}$ putting them in decreasing order. For $j = 1, \ldots, t$, let $n_j = \prod_{i=1}^{s} p_i^{f_{ij}}$. Then $n_t \mid n_{t-1} \mid \cdots \mid n_1$ and $A \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$.*

Proof. The fact that $n_j \mid n_{j-1}$ follows from $f_{ij} \leq f_{i,j-1}$. Revisiting the previous proof, we enter after the point where we rearranged the factors. In each line we then permute the e_{ij} to have them in decreasing order $(f_{i1}, \ldots, f_{it})$. The final step is to rearrange again by combining all the largest prime power factors to create $\mathbb{Z}_{n_1}$ and proceeding iteratively with the next largest prime power factors. As with the previous theorem this is just an application of Proposition 3.2.1.

$$\begin{aligned}
A = &\quad \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_t \\
\cong &\quad \mathbb{Z}/p_1^{e_{11}} \times \cdots \times \mathbb{Z}/p_1^{e_{1t}} \\
&\times \mathbb{Z}/p_2^{e_{21}} \times \cdots \times \mathbb{Z}/p_2^{e_{2t}} \\
&\qquad \cdots \\
&\times \mathbb{Z}/p_s^{e_{s1}} \times \cdots \times \mathbb{Z}/p_s^{e_{st}} \\
\cong &\quad \mathbb{Z}/p_1^{f_{11}} \times \cdots \times \mathbb{Z}/p_1^{f_{1t}} \\
&\times \mathbb{Z}/p_2^{f_{21}} \times \cdots \times \mathbb{Z}/p_2^{f_{2t}} \\
&\qquad \cdots \\
&\times \mathbb{Z}/p_s^{f_{s1}} \times \cdots \times \mathbb{Z}/p_1^{f_{st}} \\
\cong &\quad \mathbb{Z}/p_1^{f_{11}} \times \cdots \times \mathbb{Z}/p_s^{f_{s1}} \\
&\times \mathbb{Z}/p_1^{f_{12}} \times \cdots \times \mathbb{Z}/p_s^{f_{s2}} \\
&\qquad \cdots \\
&\times \mathbb{Z}/p_1^{f_{1t}} \times \cdots \times \mathbb{Z}/p_s^{f_{st}} \\
\cong &\quad \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t
\end{aligned}$$

□

Definition 3.2.6. The n_j (that are not 1) in the previous theorem are called the **invariant factors** of A.

Exercises 3.2.7.

(a) Find the elementary divisors and the invariant factors for $\mathbb{Z}/50 \times \mathbb{Z}/75 \times \mathbb{Z}/136 \times \mathbb{Z}/21000$.

(b) Let $n_1, n_2, \ldots, n_r$ be integers larger than 1. Under what conditions will $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ have r invariant factors?

Exercises 3.2.8. There is a well defined homomorphism $\mathbb{Z}_{2400} \longrightarrow \mathbb{Z}_d$ that takes $[1]_{2400}$ to $[1]_d$ for any d that divides 2400. Given several divisors of 2400 we can use the universal property of a direct product 2.3.6 to get a homomorphism into the direct product of several such groups, for example

$$\mathbb{Z}_{2400} \xrightarrow{\varphi} \mathbb{Z}_{40} \times \mathbb{Z}_{30} \times \mathbb{Z}_{16}$$

(a) What is the kernel?

(b) Find the elementary divisors of (i) $\mathbb{Z}_{2400}$, (ii) $\mathbb{Z}_{40} \times \mathbb{Z}_{30} \times \mathbb{Z}_{16}$, and (iii) the kernel of the homomorphism φ.

(c) Find the invariant factors of (i) $\mathbb{Z}_{2400}$, (ii) $\mathbb{Z}_{40} \times \mathbb{Z}_{30} \times \mathbb{Z}_{16}$, and (iii) the kernel of the homomorphism φ.

Finite Abelian Groups

In the previous section we showed that a product of cyclic groups can be written in two different forms that illuminate the structure better. One form uses cyclic groups of prime power order (and gives the elementary divisors of the group) and the other uses a format that identifies the largest cyclic component and, after splitting off that component, the next largest cyclic component, and so forth. This gives the invariant factors of the group. We now want to show that this classification applies to any finite abelian group.

The first step is to split a group into pieces that are, in a sense, coprime. We then apply induction to write the group as a direct product of groups that have prime power order. The difficult step is to show that a group of prime power order is actually a product of cyclic groups (whose orders are a power of the same prime).

Definition 3.2.9. Let A be an abelian group. For $m \in \mathbb{N}$ let

$$\begin{aligned} mA &= \{ma : a \in A\} \\ A[m] &= \{a : ma = 0\} \end{aligned}$$

For p a prime define the p**-torsion subgroup** of A to be

$$A(p) = \left\{ a \in A : \operatorname{ord}(a) = p^k \text{ for some } k \right\}$$

An abelian group such that $A = A(p)$ is called a p-group.

Exercises 3.2.10.

(a) Prove that mA, $A[n]$ and $A(p)$ are all subgroups of A.

(b) Prove that $A(p) = \cup_{i=0}^{\infty} A[p^i]$, and that, for A finite, $A(p) = A[p^k]$ for some large enough k.

Proposition 3.2.11. *Suppose that A is abelian with $|A| = mn$ and m, n coprime. Then*

(1) $mA = A[n]$

(2) A is the internal direct product of $A[m]$ and $A[n]$

Proof. Let $u, v \in \mathbb{Z}$ be such that $um + vn = 1$. Let $a \in A[n]$. Then $a = (um + vn)a = u(ma) + v(na) = m(ua)$, since we assume $na = 0$. This shows that $A[n] \subseteq mA$. On the other hand, an arbitrary element of mA can be written ma for $a \in A$. Since $|A| = mn$, $n(ma) = (nm)a = 0$, and this shows $mA \subseteq A[n]$ (we have used Lagrange's Theorem that the order of a divides the order of the group).

For the second claim of the proposition, we show that $A[m] \cap A[n] = \{0\}$ and that $A[m] + A[n] = A$. Then, by Corollary 3.1.6, $A \cong A[m] \times A[n]$.

Let $a \in A$. Since $a = (mu + nv)a = m(ua) + n(va)$ we see that $a \in mA + nA$, which by the previous paragraph is equal to $A[n] + A[m]$. Thus $A[m] + A[n] = A$. On the other hand, if $a \in A[m] \cap A[n]$ then and $a = (um + vn)a = u(ma) + v(na) = 0 + 0$. Thus $A[m] \cap A[n] = \{0\}$. We have shown that A is the internal direct product of $A[m]$ and $A[n]$. □

The next proposition shows that our decomposition is uniquely determined.

Proposition 3.2.12. *Let A_1, A_2, B_1 and B_2 be finite groups. Suppose that $A_1 \times B_1 \cong A_2 \times B_2$ where everything in A_i has order dividing m and everything in B_i has order dividing n, with m and n coprime. Then $A_1 \cong A_2$ and $B_1 \cong B_2$.*

Proof. Assume $A_1 \times B_1 \cong A_2 \times B_2$.

$$\begin{aligned} m(A_i \times B_i) &= mA_i \times mB_i \\ &= \{(0, mb) : b \in B_i\} \\ &= \{0\} \times B_i \end{aligned}$$

The first step because $m(a, b) = (ma, mb)$ and the last step because multiplication by m (coprime to n) gives an automorphism of B_i. Since $m(A_1 \times B_1) \cong m(A_2 \times B_2)$ we get $B_1 \cong B_2$. Similarly we show $A_1 \cong A_2$. □

Corollary 3.2.13. *Let $|A| = p_1^{e_1} \dots p_s^{e_s}$ then*

$$A \cong A[p_1^{e_1}] \times \cdots \times A[p_s^{e_s}] = A(p_1) \times \cdots \times A(p_s)$$

This factorization is unique up to reordering.

Proof. Existence of the factorization follows from Proposition 3.2.11 by induction:

$$\begin{aligned} A &\cong A[p_1^{e_1}] \times A[p_2^{e_2} p_3^{e_3} \cdots p_s^{e_s}] \\ &\cong A[p_1^{e_1}] \times A[p_2^{e_2}] \times A[p_3^{e_3} p_4^{e_4} \cdots p_s^{e_s}] \end{aligned}$$

and so forth. There is one subtlety though; we have used $A[p_2^{e_2}] = \Big(A[p_2^{e_2} p_3^{e_3} \cdots p_s^{e_s}]\Big)[p_2^{e_2}]$. This is easily verified. Any nonzero element of A whose order is a power of p_2 is in each of these groups, and nothing else is.

Uniqueness follows from a similar inductive application of Proposition 3.2.12 □

The previous corollary is the first step in the classification of finite abelian groups. The next step is to classify groups satisfying the following definition.

Definition 3.2.14. Let p be a prime number. An abelian **p-group** is an abelian group A in which every element of A has order that is a power of p.

The key lemma follows. Its proof is quite technical and not very illuminating, so I sketch the proof in [Hun12][Sec 8.2].

Lemma 3.2.15. *Let A be an abelian p-group and let a be an element of maximal order. Then $A = K + \langle a \rangle$ and $K \cap \langle a \rangle = \{0\}$ for some subgroup K of A. Thus A is isomorphic to the direct product of K and $\langle a \rangle$.*

Proof. Let a be an element of maximal order in the abelian p-group A; this order is a power of p. Let K be as large as possible such that $K \cap \langle a \rangle = \{0\}$. We want to show that $K + \langle a \rangle = A$. Then Corollary 3.1.6 says that $A \cong K \times \langle a \rangle$.

Suppose $b \in A \setminus (K + \langle a \rangle)$. Do some tricks to show:

(1) There is a $c \in A \setminus (K + \langle a \rangle)$ such that $pc \in K + \langle a \rangle$. [Take the minimal r such that $p^r b \in K + \langle a \rangle$, then let $c = p^{r-1} b$.]

(2) There is a $d \in A \setminus (K + \langle a \rangle)$ such that $pd \in K$. [Let $pc = k + ma$, argue that $m = pm'$, for some integer m' using that a has maximal degree in A and $K \cap \langle a \rangle = \{0\}$. Then set $d = c - m'a$.]

By assumption on K, $(K + \langle d \rangle) \cap \langle a \rangle \neq \{0\}$, so there is some $k \in K$, and nonzero $r, s \in \mathbb{Z}$ such that $k + rd = sa$.

Now we consider two cases: If $p \mid r$ then $rd \in K$ and consequently $sa \in K$. This contradicts $K \cap \langle a \rangle = \{0\}$. If $p \nmid r$ then there are u, v such that $up + vr = 1$. Then $d = u(pd) + v(rd)$. The first term is in K and the second in $K + \langle a \rangle$, so $d \in K + \langle a \rangle$, which is a contradiction.

Summarizing, we assumed K maximal such that $K \cap \langle a \rangle = \{0\}$. Supposing the existence of some $b \in A \setminus (K + \langle a \rangle)$, we showed there was some $d \in A \setminus (K + \langle a \rangle)$ such that $pd \in K$. From the maximality assumption on K, there is some element of $(K + \langle d \rangle) \cap \langle a \rangle$, which we can write as $k + rd = sa$ for $k \in K$ and $r, s \in \mathbb{Z}$. There are two possibilities, p divides r or not. Both lead to a contradiction. Thus A must be equal to $K + \langle a \rangle$. □

Theorem 3.2.16. *Let $A = A(p)$ be an abelian p-group. Then A is the direct product of cyclic groups each of which has order a power of p. Consequently, the order of A is also a power of p.*

The decomposition is unique (up to reordering). Put another way, two abelian p-groups are isomorphic if and only if their decompositions have the same number of factors for each power of p.

Proof. Note first that a non-trivial abelian p-group must have order divisible by p since Lagrange's Theorem **??** says that the order of an element of the group (which, by assumption, is a power of p) must divide the order of the group. We will show that the order of an abelian p-group must actually be equal to a power of p.

We proceed by induction on the largest power of p that divides the cardinality of the abelian group. Our induction hypothesis for $t \geq 0$ is that any abelian p-group with order that is divisible by p^t but not by p^{t+1} is isomorphic to the direct product of cyclic groups whose orders are a power of p. An immediate consequence is that the order of such a group is a power of p, so the order is exactly p^t. We noted above that the induction hypothesis is true for $t = 0$, in which case the abelian p-group is trivial.

Let $t \geq 1$. Let A be an abelian p-group of cardinality $p^t m$ with m not divisible by p. Using the lemma we can write A as a direct sum $A = K + \langle a \rangle$ with $K \cap \langle a \rangle = \{0\}$. The subgroup $\langle a \rangle$ is cyclic of order p^s for some $s > 0$ and therefore $|K| \leq p^{t-s}m$. Applying the induction hypothesis to K, shows that $m = 1$ and K is isomorphic to the direct product of cyclic groups whose order is a power of p. Since $\langle a \rangle$ is also cyclic of order p^s, we have that A is the direct product of cyclic groups of order a power of p.

To prove uniqueness (up to reordering) we note first that if two groups have the same number of factors for each power of p they are isomorphic. We will write factorizations by writing the factors in increasing powers of p as follows

$$A \cong (\mathbb{Z}/p)^{k_1} \times (\mathbb{Z}/p^2)^{k_2} \times \cdots \times (\mathbb{Z}/p^r)^{k_r}$$

We now show that we can recover the k_i by operating on A. In other words, two factorizations, one with $k_1, k_2 \ldots$ and one with $m - 1, m_2, \ldots$ are isomorphic if and only if $k_i = m_i$.

We can recover the k_i iteratively. Since $\log_p(|\mathbb{Z}/p^n|) = n$, we have $\log_p(|A|) = \sum_{i=1}^{r} ik_i$. Notice that $p^{n-1}\mathbb{Z}/p^n \cong \mathbb{Z}/p$ and $p^k\mathbb{Z}/p^n$ is trivial for $k \geq n$. Thus the subgroup $p^{r-1}A$ is isomorphic to

$$p^{r-1}A \cong (\mathbb{Z}/p)^{k_r}$$

Thus we have $\log_p(|p^{r-1}A|) = k_r$. Similar computations for p^iA with $i = r-2, r-3, \ldots, 1$ allows one to recover the other k_i. (Try it as an exercise!)

□

From Corollary 3.2.13 and the previous theorem we obtain the fundamental theorem for finite abelian groups..

Theorem 3.2.17 (Fundamental Theorem of Finite Abelian Groups)**.** *Let A be an abelian group of order $p_1^{e_1} \dots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

$$A(p_i) \cong \mathbb{Z}/p_i^{e_{i,1}} \times \mathbb{Z}/p_i^{e_{i,2}} \times \dots \mathbb{Z}/p_i^{e_{i,s_i}}$$

then for each i, $\sum_{\ell=1}^{s_i} e_{i,\ell} = e_i$. The decomposition is unique, up to reordering.

Exercises 3.2.18. Consider the following problems for $n = 72000$ and $n = 84000$.

(a) Classify all abelian groups of order 84,000.

(b) Let $n = 72,000$. How many abelian groups are there of order n?

(c) How many of these abelian groups have 2 invariant factors?

(d) How many abelian groups are there of order $p^6q^5r^4$ where p, q, r are distinct primes?

(e) How many have k invariant factors, for $k = 1, 2, 3, 4, 5, 6$? Check your answer against the response to the previous question.

Exercises 3.2.19. Let p, q and r be prime and let $n = p^6q^2r^3$.

(a) How many abelian groups are there of order n?

(b) How many of these groups have exactly *two* invariant factors?

Exercises 3.2.20. Here is another approach to proving uniqueness in the classification of finite abelian groups.

(a) Show that $p^k\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-k}}$ for $k \leq n$. Seen another way, there is an exact sequence

$$0 \longrightarrow \mathbb{Z}_{p^m} \xrightarrow{\cdot p^k} \mathbb{Z}_{p^{k+m}} \longrightarrow \mathbb{Z}_{p^k} \longrightarrow 0$$

(b) Show that $p^{k-1}\mathbb{Z}_{p^n} \Big/ p^k\mathbb{Z}_{p^n} \cong \mathbb{Z}_p$ for $k \leq n$.

(c) Suppose that $A \cong (\mathbb{Z}_p)^{k_1} \times (\mathbb{Z}_{p^2})^{k_2} \times \cdot \times (\mathbb{Z}_{p^n})^{k_n}$. Show that $p^{t-1}A/p^tA \cong (\mathbb{Z}_p)^{k_t+\dots+k_n}$.

(d) Conclude the uniqueness part of the classification of finite abelian groups: If

$$(\mathbb{Z}_p)^{k_1} \times (\mathbb{Z}_{p^2})^{k_2} \times \cdot \times (\mathbb{Z}_{p^n})^{k_n} \cong (\mathbb{Z}_p)^{m_1} \times (\mathbb{Z}_{p^2})^{m_2} \times \cdot \times (\mathbb{Z}_{p^n})^{m_n}$$

then $k_i = m_i$.

Finitely Generated Abelian Groups

Our final step is to generalize the results on classification to finitely generated abelian groups. The strategy is simple. Let A be a finitely generated group. The **torsion subgroup** of A is the set of elements of finite order. The first proposition below shows that it is indeed a subgroup of A. The torsion subgroup has to be a finite group, since it is finitely generated, so it is classified by the results above. The next big step is to show that A has a subgroup that is isomorphic to $\mathbb{Z}^r$ such that A is the direct product of that subgroup and $\operatorname{Tor}(A)$. Thus, a finitely generated abelian group is isomorphic to a finite direct product of cyclic groups that are either infinite of prime power order.

Proposition 3.2.21. *Let A be an abelian group. Let*

$$\operatorname{Tor}(A) = \{a \in A : a \textit{ has finite order}\}$$

(1) $\operatorname{Tor}(A)$ is a normal subgroup of A.

(2) All elements of $A/\operatorname{Tor}(A)$ (except the identity) have infinite order.

Proof. This was Exercise 2.10.4. Let $T = \operatorname{Tor}(A)$. Clearly $0 \in T$, so T is nonempty. If $a \in T$ has order m then so does $-a = (m-1)a$. If b is another element in T and it has order n, then $a + b$ has order at most mn since

$$mn(a + b) = (mn)a + (mn)b = n(ma) + n(mb) = 0$$

Thus T is closed under inversion and multiplication, so it is a subgroup of A. Normality is immediate since A is abelian.

If $b + T$ has finite order m in A/T then

$$mb + T = m(b + T) = 0 + T$$

This shows that $mb \in T$, so mb has some finite order n in A. Then $(nm)b = n(mb) = 0$, so b itself has finite order. Thus $b \in T$ and $b + T = 0 + T$. So the only element of finite order in $A/\operatorname{Tor}(A)$ is the identity element. □

Definition 3.2.22. A group that has no elements of finite order, other than the identity, is said to be **torsion free**.

Let A be an abelian group and let $S = \{a_1, a_2, \ldots, a_r\}$ be a set of elements in A. We say that the elements of S are **independent** when for any integers $m_1, \ldots m_r$ that are not all zero, $m_1 a_1 + m_2 a_2 + \cdots + m_r a_r \neq 0$.

A **free abelian group of rank** r is a group that is isomorphic to $\mathbb{Z}^r$. It will have r elements that are independent and also generate A. We will generally use

e_i for the element of $\mathbb{Z}^r$ that is 1 in the ith component and 0 elsewhere. Borrowing from the language of vector spaces, we say that the e_i are the standard basis for $\mathbb{Z}^r$.

Proposition 3.2.23. *The rank of a finitely generated free abelian group is unique.*

Proof. Let $A \cong \mathbb{Z}^r$. Then $A/2A \cong \mathbb{Z}^r/(2\mathbb{Z}^r) \cong (\mathbb{Z}/2\mathbb{Z})^r$. The final isomorphism comes from Theorem 2.7.10 and the observation that $2\mathbb{Z}^r = 2\mathbb{Z} \times 2\mathbb{Z} \times \cdots \times 2\mathbb{Z}$ (both containments are easy to show). Since $(\mathbb{Z}/2\mathbb{Z})^r$ has 2^r elements, we may recover the rank by computing $\log_2(|A/2A|)$. □

Exercises 3.2.24.

(a) Let A be an abelian group. Suppose $f : A \to \mathbb{Z}$ is a surjective homomorphism with kernel K. Show that A has an element a such that A is the internal direct product $K \times \langle a \rangle$.

(b) In the previous problem, suppose f is not surjective but $f(A) = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Show that it still holds that there is an element $a \in A$ such that A is the internal direct product $K \times \langle a \rangle$.

(c) Suppose that A is torsion free and $mA \cong \mathbb{Z}^r$. Show that $A \cong \mathbb{Z}^r$.

We need two results before proving that a finitely generated torsion free abelian group is actually isomorphic to $\mathbb{Z}^r$ for some r.

Proposition 3.2.25. *Let $A \leq \mathbb{Z}^r$. Then A is isomorphic to $\mathbb{Z}^s$ for some integer $s \leq r$.*

Proof. We proceed by induction on r. For $r = 1$ we already know the subgroups of $\mathbb{Z}$. They are the trivial group (rank 0) and $n\mathbb{Z}$, which is isomorphic to $\mathbb{Z}$.

Assume the statement of the theorem is true for integers less than r. Let $A \leq \mathbb{Z}^r$ and let e_i be the element of $\mathbb{Z}^r$ that is 1 in the ith component and 0 elsewhere. Consider projection onto the rth component $\mathbb{Z}^r \xrightarrow{\pi} \mathbb{Z}$. The kernel of this map is $\mathbb{Z}^{r-1}$ with generators $\{e_1, \ldots, e_{r-1}\}$. Let $A \xrightarrow{\iota} \mathbb{Z}^r$ be the embedding of A in $\mathbb{Z}^r$ and consider the composite $\pi \circ \iota$. The kernel of this map is $B = A \cap \mathbb{Z}^{r-1}$. By the induction hypothesis, B is isomorphic to $\mathbb{Z}^s$ for some integer $s \leq r - 1$.

If $B = A$ we are done. Otherwise, $\pi \circ \iota$ has image $n\mathbb{Z}$ for some $n > 0$. Let $a \in A$ be a preimage of n. By Exercise 3.2.24(b) we have $A \cong B \times \langle a \rangle \cong \mathbb{Z}^s \times \mathbb{Z} = \mathbb{Z}^{s+1}$. □

Proposition 3.2.26. *Let A be a finitely generated, torsion-free abelian group. Then A is a free abelian group of finite rank.*

Proof. Let $b_1, \ldots, b_r$ be a maximal independent set in A. These elements are independent and there is no set of $r + 1$ elements in A that is independent.

Let B be the subgroup of A generated by $b_1, \ldots, b_r$, that is $B = \{\sum_{i=1}^r m_i b_i : m_i \in \mathbb{Z}\}$. Consider A/B. I claim that it is a torsion group; every element has finite order.

For any $a \in A$, there are integers $m_0, \ldots, m_r$ such that $m_0 a + m_1 b_1 + m_2 b_2 + \cdots + m_r b_r = 0$, for otherwise $\{a, b_1, \ldots b_r\}$ would be an independent set, contradicting maximality of $\{b_1, \ldots b_r\}$. Furthermore m_0 is not zero, since $\{b_1, \ldots b_r\}$ is independent, so $m_0 a$ is a nonzero element of B. Thus for any $a \in A$ there is an m_0 such that $m_0(a + B) = m_0 a + B = 0 + B$.

We have shown every element of A/B has finite order. Since it is also finitely generated it is a finite group. Thus the exponent of A/B (the lcm of the orders of elements of A/B) is some finite $m \in \mathbb{N}$. Then, $m(A/B)$ is the trivial subgroup $\{0 + B\}$ inside A/B. This shows mA is a subgroup of the free abelian group B. Thus by Proposition 3.2.25 mA is free abelian of rank $s \leq r$, where r is the rank of B. Applying Exercise 3.2.24(c) we have that A itself is free of rank s. This concludes the proof.

It is worth noting that, since $B \leq A$, Proposition 3.2.25 says that the rank of B is at most the rank of A, so $r \leq s$. We already showed $s \leq r$, so A and B have the same rank. □

The proof of the following theorem is similar to Proposition 3.1.13. Exercise 3.2.24(a) was a special case (with $r = 1$).

Proposition 3.2.27. *Let A be a finitely generated abelian group. and let $\varphi : A \longrightarrow \mathbb{Z}^r$ be a surjective homomorphism with kernel K. There exists a subgroup $B \leq A$ such that φ restricted to B is an isomorphism. Furthermore $A = K \times B$ (We use $=$ rather than $\cong$ because A is the internal direct product of the two subgroups).*

Proof. Let $b_1, \ldots, b_r \in A$ map to the elements e_i of $\mathbb{Z}^r$. Let $B = \langle b_1, \ldots, b_r \rangle = \{m_1 b_1 + \cdots + m_r b_r : m_i \in \mathbb{Z}\}$. We know that the b_i are independent, because their images in $\mathbb{Z}^r$ are independent. In other words, since φ is a homomorphism, $\sum_{i=1}^r m_i b_i = 0$ would imply that $\sum_{i=1}^r m_i e_i = 0$. The latter is only true if all m_i are zero. Thus $\varphi|_B$ is injective. Furthermore $\varphi : B \longrightarrow \mathbb{Z}^r$ is surjective since the e_i are in the image and they generate $\mathbb{Z}^r$. Thus $\varphi|_B$ is an isomorphism.

The conclusion that now follows from Proposition 3.1.13, but we will prove it directly by using Corollary 3.1.6. The argument above shows that $K \cap B = \{0\}$. We will show $K + B = A$, which gives $A \cong K \times B$.

Let $a \in A$ and let $\varphi(a) = \sum_{i=1}^r m_i e_i$. Let $b = \sum_{i=1}^r m_i b_i$ and consider $a - b$. It is easy to see that $\varphi(a - b) = 0$ so $a - b = k$ for some $k \in K$. Thus $a \in K + B$. Since a was arbitrary $A = K + B$.

□

Theorem 3.2.28. *Let A be a finitely generated abelian group. There is a unique integer $r \geq 0$ such that A has a subgroup B that is a free abelian group of rank r. For any such B, A is the internal direct product of* $\operatorname{Tor}(A)$ *and B. Furthermore* $\operatorname{Tor}(A)$ *is a finite abelian group, so it is the direct product of cyclic groups of prime power order.*

Proof. Proposition 3.2.21 shows that $A/\operatorname{Tor}(A)$ is torsion free. Proposition 3.2.26 shows that $A/\operatorname{Tor}(A)$ must then be free of some uniquely defined rank r. Proposition 3.2.27 shows that A has a subgroup B that maps isomorphically to $A/\operatorname{Tor}(A)$ and that $A = \operatorname{Tor}(A) \times B$.

Finally, we note that A is finitely generated and the quotient group A/B is isomorphic to $\operatorname{Tor}(A)$. Thus $\operatorname{Tor}(A)$ is finitely generated and a torsion group. Therefore it is finite and is classified by Theorem 3.2.17, $\operatorname{Tor}(A)$ is also finitely generated. □

Exercises 3.2.29. Infinitely generated abelian groups can be more complicated than finite ones. Consider the group $\mathbb{Q}/\mathbb{Z}$.

(a) On a number line, sketch a region that contains exactly one element for each equivalence class of $\mathbb{Q}/\mathbb{Z}$.

(b) Show that for any integer n there is an element of order n in $\mathbb{Q}/\mathbb{Z}$.

(c) How many elements of order n are there in $\mathbb{Q}/\mathbb{Z}$?

(d) Show that every element has finite order.

(e) Show that every nontrivial cyclic subgroup is generated by $\frac{1}{n}$ for some integer $n > 1$.

(f) Show that $\mathbb{Q}/\mathbb{Z}$ is not finitely generated as an abelian group.

(g) Show that $\mathbb{Q}/\mathbb{Z}$ cannot be written as a direct product of $\langle a \rangle$ and another group H for any nonzero $a \in \mathbb{Q}/\mathbb{Z}$.

3.3 Simple Groups and the Classification of Finite Groups

In the previous section we saw that finite abelian groups have a very simple structure; they are direct products of cyclic groups, each having order a power of a prime. In this section we take steps to understand the the classification of arbitrary finite groups.

The model for classification is unique factorization of integers: Every positive integer is the product of prime numbers in a unique way. Finite abelian groups have a somewhat more complicated factorization because the constituents of the unique factorization may involve $\mathbb{Z}_{p^r}$ for arbitrary r. So, $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ are distinct even though they have the same number of elements.

The classification of finite groups is vastly more complicated than the classification of finite abelian groups. We would like to say that every finite group is "built" from a set of groups that are analogous to the prime numbers, indivisible themselves. The "building" process is much more complicated then simply forming a direct product. As we have seen, for example, S_3 is the semi-direct product $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$ (with the action of $\mathbb{Z}_2$ on $\mathbb{Z}_3$ being $a \mapsto -a$), while $\mathbb{Z}_6$ is the direct product $\mathbb{Z}_3 \times \mathbb{Z}_2$. We will consider S_3 as built from the groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$, just in a different way than $\mathbb{Z}_6$ is built, so S_3 and $\mathbb{Z}_6$ have the same constituent parts, but a different pasting together of the parts.

As another example consider the quaternion group Q, which is not even a semi-direct product. We will say that it is built from 3 copies of $\mathbb{Z}_2$ (as are all groups of order 8). The reasoning is this: $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ has a normal subgroup generated by i with 4 elements. The quotient $Q/\langle i \rangle$ is isomorphic to $\mathbb{Z}_2$. That normal subgroup generated by i is isomorphic to $\mathbb{Z}_4$, and has a proper normal subgroup generated by i^2 that is isomorphic to $\mathbb{Z}_2$. The quotient $\langle i \rangle / \langle i^2 \rangle$ is isomorphic to $\mathbb{Z}_2$. We have what is called a composition series

$$\langle 1 \rangle \trianglelefteq \langle i^2 \rangle \trianglelefteq \langle i \rangle \trianglelefteq Q$$

Each subgroup is normal in the next in the sequence. Furthermore, the quotients in this case are $\mathbb{Z}_2$ at each step, and $\mathbb{Z}_2$ is a group that has no normal subgroup except for the group itself and the trivial group.

Definition 3.3.1. A group G is **simple** when the only normal subgroups of G are $\langle e_G \rangle$ and G.

A **composition series** for a group G is a sequence of subgroups
$G_0 = \langle e_G \rangle$, G_1, G_2, $\dots$, $G_n = G$ such that G_i is a normal subgroup of G_{i+1} and G_{i+1}/G_i is simple. The simple quotients are called **composition factors** of G. We will write

$$G = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots G_{n-1} \trianglelefteq G_n = G$$

The **length** of the composition series is n.

Proposition 3.3.2. *The only simple finite abelian groups are $\mathbb{Z}_p$ for p prime.*

Proof. We have already shown that every finite abelian group is isomorphic to the direct product of cyclic groups of prime power order. But $\mathbb{Z}_{p^r}$ is not simple. It is contructed from r copies of $\mathbb{Z}_p$. There is in fact a unique composition series

$$\langle 0 \rangle \trianglelefteq \langle p^{r-1} \rangle \trianglelefteq \langle p^{r-2} \rangle \trianglelefteq \dots \langle p^2 \rangle \trianglelefteq \langle p \rangle \trianglelefteq \langle 1 \rangle = \mathbb{Z}_{p^r}$$

□

Here are the two big theorems on classifying finite groups. The first is essentially a uniqueness theorem about the composition factors of a group.

Theorem 3.3.3 (Jordan Holder)**.** *Suppose G has two composition series*

$$\begin{aligned}\langle e_G\rangle = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq G_3 \ldots G_{n-1} \trianglelefteq G_n = G\\ \langle e_G\rangle = G'_0 \trianglelefteq G'_1 \trianglelefteq G'_2 \trianglelefteq G'_3 \ldots G'_{m-1} \trianglelefteq G'_m = G\end{aligned}$$

Then $m = n$ and the lists of simple groups from the two series, $G_1/G_0, \ldots, G_n/G_{n-1}$ and $G'_1/G'_0, \ldots, G'_m/G'_{m-1}$ are the same up to reordering.

The proof takes several steps and is a bit technical, so we refer to skip it here.

The second big theorem identifies all the simple groups. It was a massive project in the late 20th century. See the Wikipedia article.

Theorem 3.3.4 (Finite Simple Groups)**.** *Every finite simple group is isomorphic to one of the following:*

(1) a cyclic group of prime order, $\mathbb{Z}_p$,

(2) an alternating group A_n, for $n \geq 5$,

(3) a group of Lie type,

(4) one of 27 "sporadic groups" (including the Tits group).

We have already shown that $\mathbb{Z}_p$ is simple. In the rest of this section we get halfway through the identification of simple groups ;-) by proving that A_n is simple for $n \geq 5$. We start with two simple lemmas, then prove A_5 is simple, then extend by induction to A_n for $n > 5$.

Lemma 3.3.5. *Let $n \geq 4$. If $N \trianglelefteq A_n$ and N contains a 3-cycle then $N = A_n$.*

Proof. Suppose for simplicity $(1, 2, 3) \in N$. Let $a \in \{4, \ldots, n\}$. Conjugate with $(1, 2)(3, a)$ to get another element of N.

$$(1, 2)(3, a)(1, 2, 3)(1, 2)(3, a) = (2, 1, a) \in N$$

Now for $b \neq 1, 2, a$ conjugate with $(1, a)(2, b)$

$$(1, a)(2, b)(1, a, 2)(1, a)(2, b) = (a, 1, b) \in N$$

Finally, the same trick can be used to give an arbitrary $(a, b, c) \in N$. We know from Exercise 2.4.17 that the 3-cycles generate A_n, so $N = A_n$. □

Lemma 3.3.6. *Let $N \trianglelefteq A_n$ with $n \geq 5$. If N contains a product of two distinct transpositions then $N = A_n$.*

Proof. Let $\sigma = \tau_1\tau_2 \in N$. If τ_1 and τ_2 do not have disjoint support then their product is a 3-cycle, and we can apply the last lemma. Suppose they have disjoint support, $\sigma = (a,b)(c,d)$. Since $n \geq 5$ there is another element in $\{1,\dots,n\}$, call it x. Since N is normal, conjugating gives another element of N,

$$(a,b,x)\big((a,b)(c,d)\big)(a,x,b) = (x,a)(c,d) \in N.$$

Now take the product of the two elements of N that we have identified,

$$\Big((a,b)(c,d)\Big)\Big(x,a)(c,d)\Big) = (a,x,b) \in N$$

Since N has a 3-cycle, $N = A_n$ by the previous lemma. □

Proposition 3.3.7. *A_5 is simple.*

Proof. Let N be a non-trivial normal subgroup in A_5. Let σ be an element of N that is not the identity and consider its signature. The possibilities are $2,2,1$ or $3,1,1$ or 5. In the lemmas above, we have shown that if σ is a product of disjoint transpositions, or if it is a 3-cycle, then $N = A_n$. Suppose the 5-cycle $\sigma = (a,b,c,d,f)$ is in N and let $\delta = (a,b,c)$. Note that $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ because the conjugation of σ by an element of A_n lands in N, and N is closed under multiplication. On the other hand,

$$\begin{aligned}(\sigma^{-1}\delta\sigma)\delta^{-1} &= (b,c,d)(c,b,a)\\ &= (a,d,b)\end{aligned}$$

This shows N contains a 3-cycle, so $N = A_n$. □

Theorem 3.3.8. *A_n is simple for $n \geq 5$.*

Proof. We proceed by induction, the case $n = 5$ has been established. Assume that A_i is simple for $i < n$; we'll prove that A_n is simple. We start with several observations about $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. First, G_i is a subgroup and $G_i \cong A_{n-1}$. Second, the G_i are all conjugate subgroups in A_n since $G_i = (1,i,2)G_1(1,2,i)$ (check!). Finally, we show in the next paragraph that $A_n = \langle G_1,\dots,G_n\rangle$.

Any $\sigma \in A_n$ can be written as a product of an even number of transpositions. Since $n \geq 5$, the product of a pair of transpositions must fix some i, and is therefore in G_i. For example $(1,2)(3,4) \in G_5$. Pairing off consecutive terms in the factorization of σ we see that σ can be written as a product of elements in the groups G_i. Thus $A_n = \langle G_1,\dots,G_n\rangle$.

The strategy now is to show that if N is normal in A_n with $N \neq \{\text{id}\}$ then $N \cap G_i \neq \{\text{id}\}$ for some i. This in turn, by the following argument, implies that $N = A_n$. By the induction hypothesis, each G_i is simple. Since $N \cap G_i$ is a nontrivial normal subgroup of G_i, we have $N \cap G_i = G_i$. We noted above that the G_i are conjugate, so for any j there is some $\pi \in A_n$ such that $G_j = \pi G_i \pi^{-1}$. But then

$$\begin{aligned} G_j &= \pi G_i \pi^{-1} \\ &= \pi(N \cap G_i)\pi^{-1} \\ &= (\pi N \pi^{-1}) \cap (\pi G_i \pi^{-1}) \\ &= N \cap G_j \end{aligned}$$

Since $N \cap G_j = G_j$ for all j and the G_j generate A_n we have $N = A_n$.

Finally, to complete the proof, we will show that for a nontrivial $N \trianglelefteq A_n$ we must have $N \cap G_i \neq \{\text{id}\}$ for some i. Suppose that N contains an element σ whose cycle decomposition has a cycle of length at least 3; say $\sigma(a) = b$, $\sigma(b) = c$ with a, b, c distinct. Let d, f be different from a, b, c (we are using $n \geq 5$) and let $\tau = (a, d, f)$. Then $(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and straightforward computation shows $\tau\sigma\tau^{-1}\sigma^{-1}(c) = c$. This shows that $N \cap G_c \neq \{\text{id}\}$ and therefore, by the previous paragraph, that $N = A_n$.

If N contains no element whose cycle decomposition has a cycle of length at least 3, then all elements of N are products of disjoint transpositions. Suppose σ is such a nontrivial element of N. We may assume that σ doesn't fix anything, for we have already shown this would imply $A_n = G$. We are assuming $n \geq 6$, so σ has at least 3 transpositions $\sigma = (a, b)(c, d)(f, g) \cdots$. Conjugate by $\tau = (a, b)(c, f)$ and multiply by σ^{-1} and we have $(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and $\tau\sigma\tau^{-1}\sigma^{-1}(b) = b$. As above this implies that $N = A_n$.

Thus for $n \geq 5$, any normal subgroup of A_n is either trivial or A_n itself. □

Exercises 3.3.9. This problem fleshes out some details in the proof of Theorem 3.3.8: A_n is simple for $n > 5$.

- **(a)** Within the alternating group A_n for each $i = 1, \ldots, n$, let $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. Show that G_i is a subgroup of A_n.
- **(b)** Find a $\pi \in A_n$ such that each $G_i = \pi G_j \pi^{-1}$.
- **(c)** Justify the statement in the fourth paragraph of the proof of 3.3.8 "Then $(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and straightforward computation shows $\tau\sigma\tau^{-1}\sigma^{-1}(c) = c$."
- **(d)** Justify the statement in the fifth paragraph of the proof of 3.3.8 "$(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ and $\tau\sigma\tau^{-1}\sigma^{-1}(b) = b$."