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. In it we use the following argument to prove that 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.*

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

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 2.7.1,

$$\begin{aligned}(KH)(KH) &= K(HK)H \\ &= K(KH)H \qquad \text{since it is assumed that } KH = HK \\ &= (KK)(HH) \\ &= KH \qquad \text{since } K \text{ and } H \text{ are groups and closed under multiplication}\end{aligned}$$

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

For the converse, 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 $H \cap N$ 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 the canonical homomorphism $G \xrightarrow{\pi} G/N$ and restrict it to the subgroup H. Call the restricted homomorphism $\pi' : H \longrightarrow G/N$. The kernel of π' contains the elements of H that map to eN, that is $H \cap N$. The image is $\{hN : h \in H\} = HN/N$ 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 Corollary 3.1.4, we say that G is the **internal semi-direct product** of N by H and we write $G = N \rtimes H$.

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 $N \trianglelefteq G$. Suppose also that $G = KN$ 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 $(knk^{-1})n^{-1} \in N$ since it is the product of two elements of N. Similarly, since K is normal, $nk^{-1}n^{-1} \in K$ so $k(nk^{-1}n^{-1}) \in K$. 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 (and is consequently a homomorphism):

$$\begin{aligned}
\varphi\big((k_1, n_1)\big)\varphi\big((k_2, n_2)\big) &= (k_1 n_1)(k_2 n_2) \\
&= k_1(n_1 k_2)n_2 \\
&= k_1(k_2 n_1)n_2 \\
&= (k_1 k_2)(n_1 n_2) \\
&= \varphi\big((k_1 k_2, n_1 n_2)\big) \\
&= \varphi\big((k_1, n_1)(k_2, n_2)\big)
\end{aligned}$$

Thus φ is an isomorphism. Note that the product in the last line is in $K \times H$, while the products in every other line are in G. □

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 the 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 they 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 $\overline{H} = \{e_G\} \times H$. These are two subroups of $G \times H$, and the interesection of $\overline{G}$ and $\overline{H}$ is the identity element of $G \times H$. 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 is easy to verify that every element of $\mathbb{Z}_6$ can be written as a sum of something in K and something in N. 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 $\mathbb{Z}_3$. We know from Corollary 2.4.5 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 that is the internal semi-direct product of the normal subgroup N and another subgroup H. So, we are assuming that $NH = G$ and $N \cap H = \{e\}$. This is 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,

$$\begin{aligned} n_1h_1n_2h_2 &= n_1h_1n_2h_1^{-1}h_1h_2 \\ &= n_1\varphi_{h_1}(n_2)h_1h_2 \end{aligned}$$

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 $\varphi : H \longrightarrow \mathrm{Aut}(N)$ 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 makes sense!

Using the notation in Definition 3.1.10, verify the following.

(a) (e_H, e_N) is the identity element.

(b) Each element does have an inverse.

(c) The associative law holds.

Exercises 3.1.12. Some familiar semidirect products.

Several familiar groups are internal semidirect products of much simpler groups. Verify that each of the following is an internal semidirect product of the two given subgroups by using Corollary 3.1.4. In each case identify the homorphism from one subgroup to the automorphism group of the other.

(a) D_n is the semidirect product of its rotation group and the group generated by any reflection. There is an implicit homomorphism $\varphi : C_2 \longrightarrow \mathrm{Aut}(C_n)$. What is it?

(b) $S_n = A_n \rtimes \langle (1,2) \rangle$.

(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 $\{1, 2, 3, 4\}$.

(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 $T = U \rtimes D$.

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

$$\pi(g^{-1}h) = \pi(g^{-1})\pi(h) = \pi(g^{-1})\pi\big(\alpha \circ \pi(g)\big) = \pi(g)\big(\pi \circ \alpha\big)\big(\varphi(g)\big)$$

Since $\pi \circ \alpha$ is the identity map on G/N,

$$= \pi(g^1)(\pi(g)) = \pi(gg^{-1}) = eN$$

Consequently $g^{-1}h = n$ 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 $H \cap N = \{e\}$. □

Exercises 3.1.14. Semidirect products and matrix groups

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: $n \times n$ 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 prime numbers p and which n is $\mathrm{GL}_n(\mathbb{F}_p)$ a direct product as above?

Exercises 3.1.15. External semidirect products of cyclic groups.

(a) Use the definition of external semidirect 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 $a^i b^j$ for $i \in \{0, 1, 2\}$ and $b \in \{0, 1, 2, 3\}$

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

(3) Find the inverse of $a^i b^j$.

(4) Find a general formula for $(a^i b^j)(a^m b^n)$. 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 2.4.5, 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

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

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

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

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 $f_{ij} \leq f_{i,j-1}$ for each i. 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.

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

□

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. DISSECTING A HOMOMORPHISM.

For any d that divides 2400, there is a well defined homomorphism $\mathbb{Z}_{2400} \longrightarrow \mathbb{Z}_d$ that takes $[1]_{2400}$ to $[1]_d$. Given several divisors of 2400 we can use the universal property of a direct product 2.4.4 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 of φ?

(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

$$mA = \{ma : a \in A\}$$
$$A[m] = \{a : ma = 0\}$$

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, $A[m]$ 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 argument above, 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 $A[p_2^{e_2}] = \left(A[p_2^{e_2} p_3^{e_3} \cdots p_s^{e_s}]\right)[p_2^{e_2}]$. 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 2.7.7 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 $p_1^{e_1} \ldots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

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

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. Classifying abelian groups

Consider the following problems for $n = 72000$ and $n = 84000$ and $n = p^6q^5r^4$ with p, q, r distinct primes.

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

(b) List all possibilities (you can use "choose one of these, one of these, ...".

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

Exercises 3.2.19. Another approach to proving uniqueness

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 $p^{t-1}A/p^tA \cong (\mathbb{Z}_p)^{k_t+\cdots+k_n}$.

(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 $\mathrm{Tor}(A)$. 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 3.2.20. *Let A be an abelian group. Let*

$$\mathrm{Tor}(A) = \{a \in A : a \text{ has finite order}\}$$

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

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

Proof. This was Exercise 2.11.4. Let $T = \mathrm{Tor}(A)$. 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 $A/\mathrm{Tor}(A)$ is the identity element. □

Definition 3.2.21. 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, $m_1a_1 + m_2a_2 + \cdots + m_ra_r \neq 0$.

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 3.2.22. *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 2.8.10 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 3.2.23.

(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 3.2.24. *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 3.2.23(b) we have $A \cong B \times \langle a \rangle \cong \mathbb{Z}^s \times \mathbb{Z} = \mathbb{Z}^{s+1}$. □

Proposition 3.2.25. *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 3.2.24 mA is free abelian of rank $s \leq r$, where r is the rank of B. Applying Exercise 3.2.23(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 3.2.24 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 3.2.23(a) was a special case (with $r = 1$).

Proposition 3.2.26. *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 3.2.27. *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 $\mathrm{Tor}(A)$ and B. Furthermore $\mathrm{Tor}(A)$ is a finite abelian group, so it is the direct product of cyclic groups of prime power order.*

Proof. Proposition 3.2.20 shows that $A/\mathrm{Tor}(A)$ is torsion free. Proposition 3.2.25 shows that $A/\mathrm{Tor}(A)$ must then be free of some uniquely defined rank r. Proposition 3.2.26 shows that A has a subgroup B that maps isomorphically to $A/\mathrm{Tor}(A)$ and that $A = \mathrm{Tor}(A) \times B$.

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

Exercises 3.2.28. Infinitely generated abelian groups

These can be much 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, $\ldots$, $G_n = G$ 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

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

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 A is isomorphic to the direct product of cyclic groups of prime power order. Each of the factors of the direct product corresponds to a normal subgroup of A. Since a simple group has no proper normal subgroups, the only possible simple groups are those whose order is a power of a prime. But $\mathbb{Z}_{p^r}$ is not simple for $r > 1$. It is contructed from r copies of $\mathbb{Z}_p$. There is in fact a unique composition series for $\mathbb{Z}_{p^r}$ when $r > 1$.

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

□

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*

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

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

The proof takes several steps and is a bit technical, so we will skip it here and suggest other references. [Hun03] [Chap 8].

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 2.5.18 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 $\{1, \ldots, n\}$, 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 $A_n = \langle G_1, \ldots, G_n \rangle$.

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 $A_n = \langle G_1, \ldots, G_n \rangle$.

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. $\square$

Exercises 3.3.9. DETAILS SIMPLICITY OF A_n

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 $\tau\sigma\tau^{-1}\sigma^{-1}(b) = b$."