1. Direct products and finitely generated abelian groups

We would like to give a classification of finitely generated abelian groups. We already know a lot of finitely generated abelian groups, namely cyclic groups, and we know they are all isomorphic to $\mathbb{Z}_n$ if they are finite and the only infinite cyclic group is $\mathbb{Z}$, up to isomorphism.

Is this all? No, the Klein 4-group has order four, so it is definitely finitely generated, it is abelian and yet it is not cyclic, since every element has order two and not four.

We are going to give a way to produce new groups from old groups.

Definition 1.1. *Let X and Y be two sets.*

The ***Cartesian product*** *of X and Y, denoted $X \times Y$, is the set of all ordered pairs, (x, y), $x \in X$ and $y \in Y$,*

$$X \times Y = \{\, (x, y) \,|\, x \in X, y \in Y \,\}.$$

We can also take the Cartesian product of three sets, four sets, or even n sets, $X_1, X_2, \dots, X_n$.

Given two groups H and G we are going to make the Cartesian product $H \times G$ into a group.

Definition-Theorem 1.2. *Let H and G be two groups.*

Given (h_1, g_1) and $(h_2, g_2) \in H \times G$ define the product by the rule:

$$(h_1, g_1)(h_2, g_2) = (h_1h_2, g_1g_2).$$

With this rule for multiplication, $H \times G$ becomes a group, called the ***direct product*** *of H and G.*

If H and G are abelian then so is $H \times G$.

Proof. We have to check the axioms for a group. We first check this product is associative. Suppose that $(h_i, g_i) \in H \times G$, for $i = 1$, 2 and 3. We have

$$\begin{aligned}
(h_1, g_1)[(h_2, g_2)(h_3, g_3)] &= (h_1, g_1)(h_2h_3, g_2g_3) \\
&= ((h_1(h_2h_3), g_1(g_2g_3)) \\
&= ((h_1h_2)h_3, (g_1g_2)g_3) \\
&= (h_1h_2, g_1g_2)(h_3, g_3) \\
&= [(h_1, g_1)(h_2, g_2)](h_3, g_3),
\end{aligned}$$

which is associativity.

Suppose that $e \in H$ is the identity in H and $f \in G$ is the identity in G. If $(h, g) \in H \times G$ then

$$(e, f)(h, g) = (eh, fg) = (h, g)$$

and

$$(h, g)(e, f) = (he, gf) = (h, g).$$

Thus (e, f) plays the role of the identity in $H \times G$.

Finally suppose that $(h, g) \in H \times G$. We check that $(h^{-1}, g^{-1}) \in H \times G$ is the inverse of (h, g):

$$(h^{-1}, g^{-1})(h, g) = (h^{-1}h, g^{-1}g) = (e, f)$$

and

$$(h, g)(h^{-1}, g^{-1}) = (hh^{-1}, gg^{-1}) = (e, f).$$

Thus (h^{-1}, g^{-1}) is the inverse of (h, g) and $H \times G$ is a group.

Now suppose that H and G are abelian. If $(h_i, g_i) \in H \times G$, $i = 1$ and 2 then

$$(h_1, g_1)(h_2, g_2) = (h_1h_2, g_1g_2) = (h_2h_1, g_2g_1) = (h_2, g_2)(h_1, g_1),$$

and so $H \times G$ is abelian. □

Example 1.3. *Consider the direct product of $\mathbb{Z}_2$ with itself, $\mathbb{Z}_2 \times \mathbb{Z}_2$. This group has four elements, $(0, 0)$, $(1, 0)$, $(0, 1)$ and $(1, 1)$; $(0, 0)$ is the identity. We have*

$$\begin{aligned} (0, 0) + (0, 0) &= (0, 0) \qquad & (1, 0) + (1, 0) &= (0, 0) \\ (0, 1) + (0, 1) &= (0, 0) \qquad & (1, 1) + (1, 1) &= (0, 0). \end{aligned}$$

Thus every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$, other than the identity $(0, 0)$, has order two. As this is an abelian group of order 4 it must be isomorphic to the Klein 4-group.

Example 1.4. *Consider the direct product of $\mathbb{Z}_2$ with $\mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_3$. This group has six elements, $(0, 0)$, $(1, 0)$, $(0, 1)$, $(1, 1)$, $(0, 2)$ and $(1, 2)$. We have*

$$\begin{aligned} (1, 1) + (1, 1) &= (0, 2) \qquad & (1, 1) + (0, 1) &= (1, 0) \\ (1, 1) + (1, 0) &= (0, 1) \qquad & (1, 1) + (0, 1) &= (1, 2). \end{aligned}$$

As $(1, 1) + (1, 2) = (0, 0)$, $(1, 1)$ is an element of order 6. It follows that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group with generator $(1, 1)$ so that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$.

Proposition 1.5. *Let $m_1, m_2, \dots, m_k$ be a sequence of positive integers.*

Then

$$\prod_{i=1}^{k} \mathbb{Z}_{m_i}$$

is cyclic if and only if they are pairwise coprime.

Proof. We only do the case $k = 2$; the general case is similar. Suppose that $m = m_1$ and $n = m_2$. Suppose that m and n are coprime. The order of $\mathbb{Z}_m \times \mathbb{Z}_n$ is mn. What is the order of $(1, 1)$? We have

$$\alpha(1, 1) = (\alpha, \alpha),$$

for α any integer. If this is zero then the first and second entries are zero. The first entry is zero if and only if m divides α. The second entry is zero if and only if n divides α. If m and n are coprime then the smallest positive integer divisible by both m and n is mn. Thus $(1, 1)$ is an element of order mn and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, generated by $(1, 1)$.

Now suppose that m and n are not coprime. We have to show that $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. Let $d > 1$ be the gcd of m and n and let

$$\alpha = \frac{mn}{d}.$$

Then

$$\alpha = \frac{n}{d}m \qquad \text{and} \qquad \alpha = \frac{m}{d}n,$$

is a multiple of both m and n. Suppose that $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$. We have

$$\alpha(r, s) = (\alpha r, \alpha s) = (0, 0),$$

since αr is a multiple of m and αs is a multiple of n. Thus every element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order at most α which is less than mn and so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. □

Example 1.6. $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ *is cyclic of order* 30.

Note that the number

$$\frac{mn}{d}$$

introduced in the proof of (1.5) is the least common multiple of m and n, the smallest number divisible by both m and n. One can generalise the proof of (1.5) to:

Lemma 1.7. *If*

$$(a_1, a_2, \dots, a_n) \in \prod_{i=1}^{n} G_i$$

and a_i has order r_i in G_i then the order of $(a_1, a_2, \dots, a_n)$ is the least common multiple of $r_1, r_2, \dots, r_n$.

Example 1.8. *Consider the order of*

$$(3, 6, 5) \in \mathbb{Z}_{27} \times \mathbb{Z}_{24} \times \mathbb{Z}_{50}.$$

Now 3 *has order* 9 *in* $\mathbb{Z}_{27}$*,* 6 *has order* 4 *in* $\mathbb{Z}_{24}$ *and* 5 *has order* 10 *in* $\mathbb{Z}_{50}$*.*

The least common multiple of 9*,* 4 *and* 10 *is* 180*. Thus the order of* $(3, 6, 2)$ *is* 180*.*

Note that the product of n cyclic groups of the form $\mathbb{Z}_n$ or $\mathbb{Z}$ is always generated by the n elements, $(1, 0, \dots, 0)$, $(0, 1, \dots, 0)$, $\dots$. For example, if $n = 3$ then

$$(1, 0, 0), \qquad (0, 1, 0) \qquad \text{and} \qquad (0, 0, 1)$$

generate the product of three cyclic groups.

Note also that the group $H \times G$ contains a copy of both H and G. Indeed, consider

$$G' = \{\, (e, g) \mid g \in G \,\},$$

where e is the identity of H. There is an obvious correspondence between G and G', just send g to (e, g), and under this correspondence G and G' are isomorphic, since e just goes along for the ride.

Finally note that $H \times G$ and $G \times H$ are isomorphic; the natural map which switches the factors is an isomorphism.

Theorem 1.9 (Fundamental Theorem of finitely generated abelian groups)**.** *Every finitely generated abelian group is isomorphic to a product*

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where $p_1, p_2, \dots, p_n$ *are prime numbers and* $a_1, a_2, \dots, a_n$ *are positive integers.*

The direct product is unique, up to re-ordering the factors, so that the number of copies of $\mathbb{Z}$ *and the prime powers are unique.*

Example 1.10. *Find all abelian groups of order* 504*, up to isomorphism.*

We first find the prime factorisatiom of 504,

$$504 = 2^3 \cdot 3^2 \cdot 7.$$

Using (1.9) we have the following possibilities:

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$.
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_7$.
(3) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$.
(4) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_7$.
(5) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$.

(6) $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_7$.

Thus there are six non-isomorphic abelian groups of order 504.

Here is an interesting consequence of the fundamental theorem:

Corollary 1.11. *If m divides the order of a finite abelian group G then there is a subgroup H of G of order m.*

Proof. By (1.9) G is isomorphic to

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}$$

where $p_1, p_2, \dots, p_n$ are prime numbers and $a_1, a_2, \dots, a_n$ are positive integers. There are no factors of $\mathbb{Z}$, as G is finite. In particular the order of G is $p_1^{a_1}p_2^{a_2}p_3^{a_3}\dots p_n^{a_n}$. As m divides the order of G, we may find $0 \leq b_i \leq a_i$ such that

$$m = p_1^{b_1}p_2^{b_2}p_3^{b_3}\dots p_n^{b_n}.$$

Let $c_i = a_i - b_i$. Note that

$$p_i^{c_i}$$

is an element of $\mathbb{Z}_{p_i^{a_i}}$ of order $p_i^{b_i}$. Therefore

$$\langle p_i^{c_i} \rangle$$

is a subgroup of order $p_i^{b_i}$ and the product

$$\langle p_1^{c_1} \rangle \times \langle p_2^{c_2} \rangle \times \cdots \times \langle p_n^{c_n} \rangle,$$

has order $m = p_1^{b_1}p_2^{b_2}p_3^{b_3}\dots p_n^{b_n}$. □