groups from old groups.

Definition. Let $H_1, \ldots, H_n$ be groups. The (external) *direct product* of $H_1, \ldots, H_n$ is the cartesian set product

$$H_1 \times \cdots \times H_n$$

with multiplication

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Remark. Since each H_i is a group it is immediate that the direct product is also a group with identity $(1_{H_1}, \ldots, 1_{H_n})$. The inverse of $(a_1, a_2, \ldots, a_n)$ is $(a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$. The associatative law follows from the fact that it holds in each component.

Next result tells us that the internal direct product is the same as the external direct product.

Lemma 2.3 *Suppose G is the internal direct product of $H_1, \ldots, H_n$. Then*

$$G \cong H_1 \times \cdots \times H_n.$$

Proof (See sheet 4)

II. Abelian groups.

In this section, we will use additive notation. Thus we use $+$ for the group operation, $-a$ for the inverse of a and 0 for the group identity. We also talk about direct sums rather than direct products.

Notice that every subgroup of an abelian group G is normal. Thus for subgroups $H_1, H_2, \ldots, H_n$ of G we have that $H_1 + \cdots + H_n$ is an internal direct sum of $H_1, \ldots, H_n$ if

$$H_i \cap \sum_{j \neq i} H_j = \{0\}$$

for $i = 1, \ldots, n$. The external direct sum of $H_1, \ldots, H_n$ is also denoted

$$H_1 \oplus H_2 \oplus \cdots \oplus H_n$$

instead of $H_1 \times H_2 \times \cdots \times H_n$.

The cyclic group generated by a, $\langle a \rangle = \{na : n \in \mathbb{Z}\}$, will often be denoted $\mathbb{Z}a$.

Definition. Let G be any abelian group and let p be a prime. The subset

$$G_p = \{x \in G : \ o(x) \text{ is a power of } p\}$$

is called the *p-primary subgroup* of G.

Lemma 2.4 *G_p is a subgroup of G.*

Proof As the order of 0 is $1 = p^0$, it is clear that $0 \in G_p$. Now let $x, y \in G_p$ with orders p^n, p^m. Then $p^{\max\{n,m\}}(x+y) = p^{\max\{n,m\}}x + p^{\max\{n,m\}}y = 0 + 0 = 0$ and thus $o(x+y)$ divides $p^{\max\{n,m\}}$ and is thus also a power of p. Hence $x + y \in G_p$ and as $o(-x) = o(x) = p^n$ we also have that $-x \in G_p$. Hence $G_p \leq G$. $\square$

Remark. If G is finite then $|G_p|$ must be a power of p. This follows from Exercise 4(a) on sheet 3. If there was another prime $q \neq p$ that divided $|G_p|$ then by this exercise we would have an element in G_p of order q but this contradicts the definition of G_p.

Definition. An abelian group is said to be a *p-group* if $G = G_p$.

Next lemma reduces the study of finite abelian groups to the study of finite abelian groups of prime power order.

Lemma 2.5 *Let G be a finite abelian group where $|G| = p_1^{r_1} \cdots p_n^{r_n}$ for some positive integers $r_1, \ldots, r_n$. Then G is the internal direct sum of $G_{p_1}, G_{p_2}, \ldots, G_{p_n}$. Furthermore $|G_{p_i}| = p_i^{r_i}$.*

Proof Let $x \in G$. Then by Lagrange's Theorem $o(x)$ divides $|G|$, say $o(x) = p_1^{s_1} \cdots p_n^{s_n}$. The numbers

$$q_1 = \frac{o(x)}{p_1^{s_1}}, \ldots, q_n = \frac{o(x)}{p_n^{s_n}}$$

are then coprime and we can find integers $a_1, \ldots, a_n$ such that $a_1q_1 + \cdots + a_nq_n = 1$. Thus

$$x = (a_1q_1 + \cdots + a_nq_n)x = a_1q_1x + \cdots + a_nq_nx$$

and as $p_i^{s_i}(a_iq_ix) = a_io(x)x = 0$ we have that $a_iq_ix \in G_{p_i}$. Thus $G = G_{p_1} + \cdots + G_{p_n}$. To see that the sum is direct let $x \in G_{p_i} \cap \sum_{j \neq i} G_{p_j}$, say

$$x = x_i = \sum_{j \neq i} x_j$$

where the order of x_k is p^{e_k}. Then $p_i^{e_i}x = 0$ and also $(\prod_{j \neq i} p_j^{e_j})x = 0$ and the order of x divides two coprime numbers. Hence $o(x) = 1$ and thus $x = 0$. This shows that the intersection is trivial and hence we have a direct sum.

By the remark made before the Lemma, we know that $|G_{p_i}| = p_i^{s_i}$ for some integer s_i. Since G is the direct sum of $G_{p_1}, \ldots, G_{p_n}$, we have

$$p_1^{r_1} \cdots p_n^{r_n} = |G| = \prod_{i=1}^{n} |G_{p_i}| = p_1^{s_1} \cdots p_n^{s_n}.$$

Comparison of the two sides gives $s_i = r_i,\ i = 1, \ldots, n$. $\square$

Remark. Thus $G \cong G_{p_1} \oplus \cdots \oplus G_{p_n}$. And the study of finite abelian groups reduces to understanding the finite abelian p-groups.

Definition. Let G be a finite group. The *exponent* of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$. (Or with additive notation $nx = 0$ for all $x \in G$).

Abelian groups of exponent p as vector spaces. Let G be a finite abelian group of exponent p. Then $px = 0$ for all $x \in G$ and the group addition induces a scalar multiplication from the field Z_p as follows. For $[m] = m + \mathbb{Z}p$ we let $[m]x = mx = \underbrace{x + \cdots + x}_{m}$. This is well defined and turns G into a vector space over $\mathbb{Z}_p$. One also has that a subset H of G is a subgroup of the group G if and only if H is a subspace of the vector space G. (See Sheet 5, exercise 1 for the details).

Lemma 2.6 *Let G be a finite abelian group of exponent p. Then G can be written as an internal direct sum of cyclic groups of order p.*

Proof Viewing G as a vector space over $\mathbb{Z}_p$ we know that it has a basis $x_1, \ldots, x_n$ as all these elements are non-trivial and as the exponent of G is p, they must all be of order p. To say that these elements form a basis for the vector space G is the same as saying that we have a direct sum of one dimensional subspaces

$$G = \mathbb{Z}_p x_1 + \cdots + \mathbb{Z}_p x_n.$$

This happens if and only if

$$\mathbb{Z}_p x_j \cap \sum_{k \neq j} \mathbb{Z}_p x_k = \{0\}$$

for $j = 1, \ldots, n$. But as $\mathbb{Z}_p x_k = \mathbb{Z} x_k$, this is the same as saying that

$$\mathbb{Z} x_j \cap \sum_{k \neq j} \mathbb{Z} x_k = \{0\}$$

for $j = 1, \ldots, n$ which is the same as saying that

$$G = \mathbb{Z} x_1 + \cdots + \mathbb{Z} x_r$$

is an internal direct sum of cyclic subgroup of order p. $\Box$.

Remark. If we have the direct sum $G = \mathbb{Z} x_1 + \cdots + \mathbb{Z} x_n$ then $|G| = p^n$. The number of direct summands is thus unique and is $\log_p(|G|)$.

Lemma 2.7 *We have that sum $H_1 + \cdots + H_n$ is direct if and only if for any $x_i \in H_i,\ i = 1, \ldots, n$ we have*

$$x_1 + \cdots + x_n = 0 \Rightarrow x_1 = \ldots = x_n = 0.$$

Proof To prove this, notice first that a direct sum would have this property by Proposition 2.2. Conversely, suppose that this property holds and take some $x_i = \sum_{j \neq i}(-x_j)$ in $H_i \cap \sum_{j \neq i} H_j$. Then $x_1 + \cdots + x_n = 0$ and thus $x = x_i = 0$ by the property. So the intersection is trivial and the sum is direct. $\Box$.

Proposition 2.8 *Let G be a finite abelian p-group. G can be written as an internal direct sum of non-trivial cyclic groups. Furthermore the number of cyclic summands of any given order is unique for G.*

Proof (See later).

From Lemma 2.5 and Proposition 2.8 we can derive the main result of this chapter.

Theorem 2.9 *(The Fundamental Theorem for finite abelian groups). Let G be a finite abelian group. G can be written as an internal direct sum of non-trival cyclic groups of prime power order. Furthermore the number of cyclic summands for any given order is unique for G.*

Remark. Suppose that $G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$ is a direct sum of cyclic group of prime power order. Notice that

$$G = \mathbb{Z}x_{\sigma(1)} + \mathbb{Z}_{\sigma(2)} + \cdots + \mathbb{Z}_{\sigma(n)}$$

for all $\sigma \in S_n$.

Convention. We order the cyclic summands as follows. First we order them with respect to the primes involved in ascending order. Then for each prime we order the summands in ascending order.

Example. If G is finite abelian group written as an internal direct sum

$$G = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4 + \mathbb{Z}x_5$$

of cyclic groups of orders $9, 2, 4, 3, 4$, then we order the summands so that they come instead in orders $2, 4, 4, 3, 9$. Notice then that G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

Remarks. (1) This discussion shows that any finite abelian group is isomorphic to a unique external direct sum

$$\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$$

where $p_1 \leq p_2 \leq \cdots \leq p_r$ and if $p_i = p_{i+1}$ then $e_i \leq e_{i+1}$.

(2) Finding all abelian groups of a given order $n = p_1^{m_1} \cdots p_r^{m_r}$, where $p_1 < p_2 < \cdots < p_r$ are primes, reduces then to the problem of finding, for $i = 1, \ldots, r$, all possible partitions $(p_i^{e_1}, \ldots, p_i^{e_l})$ of the number $p_i^{m_i}$. This means that

$$1 \leq e_1 \leq e_2 \leq \ldots \leq e_l \quad \text{and} \quad e_1 + \cdots + e_l = m_i.$$

Example. Find (up to isomorphism) all abelian groups of order 72.

Solution. We have $72 = 2^3 \cdot 3^2$. The possible partitions of 2^3 are $(8),\ (2,4),\ (2,2,2)$ whereas the possible partions for 3^2 are $(3^2),\ (3,3)$. We then have that the abelian groups of order 72 are

$$\begin{array}{lll} \mathbb{Z}_8 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9, \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{array}$$