1 Direct and Semidirect Products and Abelian Groups

1.1 Direct Products

Definition.

1. The *direct product* $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, G_2, \ldots, G_n$ with operations $\star_1, \star_2, \ldots, \star_n$, respectively, is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with the operation defined componentwise:
$$(g_1, g_2, \ldots, g_n) \star (h_1, h_2, \ldots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2. \ldots g_n \star_n h_n).$$

2. Similarly, the *direct product* $G_1 \times G_2 \times \cdots$ of the groups $G_1, G_2, \ldots$ with operations $\star_1, \star_2, \ldots$, respectively, is the set of sequences $(g_1, g_2, \ldots)$ where $g_i \in G_i$ with the operation defined componentwise:
$$(g_1, g_2, \ldots) \star (h_1, h_2, \ldots) = (g_1 \star_1 h_1, g_2 \star_2 h_2. \ldots).$$

Proposition 1. If $G_1, \ldots, G_n$ are groups, their direct product is a group of order $|G_1||G_2| \cdots |G_n|$ (if any G_i is infinite, so is the direct product).

Proposition 2. Let $G_1, G_2, \ldots, G_n$ be group and let $G = G_1 \times G_2 \times \cdots \times G_n$ be their direct product.

1. For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic G_i:
$$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\},$$
(here g_i appears in the i^{th} position). If we identity G_i with this subgroup, then $G_i \trianglelefteq G$ and
$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. For each fixed i define $\pi_i \colon G \to G_i$ by
$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i.$$
Then π_i is a surjective homomorphism with
$$\begin{aligned} \ker\pi_i &= \{(g_1, g_2, \ldots, g_{i-1}, 1, g_{i+1}) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$
(here 1 appears in position i).

3. Under the identifications in part 1, if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$.

1.2 The Fundamental Theorem of Finitely Generated Abelian Groups

Definition.

1. A group G is *finitely generated* if there is some finite subset A of G such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$ let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the *free abelian group of order r*.

Theorem 3. (The Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s},$$

   for some $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions:

   (a) $r \geq 0$ and $n_j \geq 2$ for all j, and

   (b) $n_{i+1} \mid n_i$ for all $1 \leq i \leq s-1$

2. the expression in 1. is unique: if $G \cong \mathbb{Z}^t \times Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_u}$, where t and $m_1, m_2, \ldots, m_u$ satisfy (a) and (b), then $t = r$ and $m_i = n_i$ for all i.

Definition. The integer r in Theorem 3 is called the *free rank* or *Betti number* of G and the integers $n_1, n_2, \ldots, n_s$ are called the *invariant factors* of G. The description of G in Theorem 3(1) is called the *invariant factor decomposition* of G.

Note. There is a bijection between the set of isomorphism classes of finite abelian groups of order n and the set of integer sequences $n_1, n_2, \ldots, n_s$ such that

1. $n_j \geq 2$ for all $j \in \{1, 2, \ldots, s\}$,

2. $n_{i+1} \mid n_i, 1 \leq i \leq s-1$, and

3. $n_1 n_2 \cdots n_s = n$.

Also notice that every prime divisor of n must be a divisor of n_1 due to (2).

Corollary 4. If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, Z_n.

Theorem 5. Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

1. $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$

2. for each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^\alpha$,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \ldots + \beta_t = \alpha$ (where t and $\beta_1, \beta_2, \ldots, \beta_t$ depend on i)

3. the decomposition in 1. and 2. is unique, i.e., if $G \cong B_1 \times B_2 \times \cdots \times B_m$, with $|B_i| = p_i^{\alpha_i}$ for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Definition. The integers p^{β_j} described in the proceeding theorem are called the *elementary divisors* of G. The description of G in Theorem 5(1) and 5(2) is called the *elementary divisor decomposition* of G.

Note. For a group of order p^β the invariant factors will be $p^{\beta_1}, p^{\beta_2}, \ldots, p^{\beta_t}$ such that

1. $\beta_j \geq 1$ for all $j \in \{1, 2, \ldots, t\}$,
2. $\beta_i \geq \beta_{i+1}$ for all i, and
3. $\beta_1 + \beta_2 + \ldots + \beta_t = \beta$

Proposition 6. Let $m, n \in \mathbb{Z}^+$.

1. $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.
2. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.