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 $A \in \{A_1, A_2, \dots, A_k\}$ 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 $\beta_1, \beta_2, \dots, \beta_t$ 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 $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_t}$ such that

1. $\beta_j \geq 1$ for all $j \in \{1, 2, \dots, t\}$,
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 $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

1.3 Table of Groups of Small Order

Order	No. of Isomorphism Types	Abelian Groups	Non-abelian Groups
1	1	Z_1	none
2	1	Z_2	none
3	1	Z_3	none
4	2	$Z_4,\ Z_2 \times Z_2$	none
5	1	Z_5	none
6	2	Z_6	S_3
7	1	Z_7	none
8	5	$Z_8,\ Z_4 \times Z_2,$ $Z_2 \times Z_2 \times Z_2$	$D_8,\ Q_8$
9	2	$Z_9,\ Z_3 \times Z_3$	none
10	2	Z_{10}	D_{10}
11	1	Z_{11}	none
12	5	$Z_{12},\ Z_6 \times Z_2$	$A_4,\ D_{12},\ Z_3 \rtimes Z_4$
13	1	Z_{13}	none
14	2	Z_{14}	D_{14}
15	1	Z_{15}	none
16	14	$Z_{16},\ Z_8 \times Z_2,\ Z_4 \times Z_4,$ $Z_4 \times Z_2 \times Z_2,$ $Z_2 \times Z_2 \times Z_2 \times Z_2$	not listed
17	1	Z_{17}	none
18	5	$Z_{18},\ Z_6 \times Z_3$	$D_{18},\ S_3 \times Z_3,$ $(Z_3 \times Z_3) \rtimes Z_2$
19	1	Z_{19}	none
20	5	$Z_{20},\ Z_{10} \times Z_2$	$D_{20},\ Z_5 \rtimes Z_4,\ F_{20}$

Note. The group F_{20} of order 20 has generators and relations

$$\langle x, y \mid x^4 = y^5 = 1, xyx^{-1} = y^2 \rangle.$$

This group is called the *Frobenius group* of order 20 and can be viewed as the subgroup $F_{20} = \langle (2354), (12345) \rangle$ of S_5.

1.4 Recognizing Direct Products

Definition. Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.

1. Define $[x, y] = x^{-1}y^{-1}xy$, called the *commutator* of x and y.
2. Define $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$, the group generated by commutators of elements of A and from B.
3. Define $G' = \langle [x, y] \mid x, y \in G \rangle$, the subgroup of G generated by commutators of elements from G, called the *commutator subgroup* of G.

Proposition 7. Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

1. $xy = yx[x, y]$ (in particular, $xy = yx$ if and only if $[x, y] = 1$).

2. $H \trianglelefteq G$ if and only if $[H, G] \leq H$.

3. $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G, G'char$G$ and G/G' is abelian

4. G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.

5. If $\varphi \colon G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G' i.e., $G' \leq \ker\varphi$ and the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/G' \arrow[d] \\ & A \end{tikzcd}$$

Proposition 8. Let H and K be subgroups of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, then each element of HK can be written uniquely as the product hk, for some $h \in H$ and $k \in K$.

Theorem 9. Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and

2. $H \cap K = 1$.

Then $HK \cong H \times K$.

Note. The above conditions are simply the necessary conditions to ensure that the map

$$\begin{aligned} \varphi \colon HK &\to H \times K \\ hk &\mapsto (h, k) \end{aligned}$$

is well defined and an isomorphism.

Definition. If G is a group and H and K are normal subgroups of G with $H \cap K = 1$, we call HK the *internal direct product* of H and K. We shall (when emphasis is called for) call $H \times K$ the *external direct product* pf H and K. (The distinction here is purely notational by Theorem 9).

1.5 Semidirect Products

Theorem 10. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H determined by φ. Let G be the set of order pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

1. This multiplication makes G into a group of order $|G| = |H||K|$.

2. The sets $\{(h,1) \mid h \in H\}$ and $\{(1,k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h,1)$ for $h \in H$ and $k \mapsto (1,k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively;

$$H \cong \{(h,1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1,k) \mid k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in 2. we have

3. $H \trianglelefteq G$

4. $H \cap K = 1$

5. for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$

Definition. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The group described in Theorem 10 is called the *semidirect product* of H and K with respect to φ and will be denoted by $H \rtimes_\varphi K$ (when there is no danger of confusion we shall simply write $H \rtimes K$).

Proposition 11. Let H and K be groups and let $\varphi\colon K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

1. the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence and isomorphism)

2. φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$

3. $K \trianglelefteq H \rtimes k$.

Theorem 12. Suppose G is a group with subgroups H and K such that

1. $H \trianglelefteq G$, and

2. $H \cap K = 1$.

Let $\varphi\colon K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying 1. and 2., then G is the semidirect product of H and K.

Definition. Let H be a subgroup of the group G. A subgroup K of G is called a *complement* for H in G if $G = HK$ and $H \cap K = 1$.

Note. With the above terminology, the criterion for recognizing a semidirect product is simply that there must exist a complement for some proper normal subgroup of G.