CHAPTER 5

Direct and Semidirect Products and Abelian Groups

In this chapter we consider two of the easier methods for constructing larger groups from smaller ones, namely the notions of direct and semidirect products. This allows us to state the Fundamental Theorem on Finitely Generated Abelian Groups, which in particular completely classifies all finite abelian groups.

5.1 DIRECT PRODUCTS

We begin with the definition of the direct product of a finite and of a countable number of groups (the direct product of an arbitrary collection of groups is considered in the exercises).

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 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 operation defined componentwise:

$$(g_1, g_2, \ldots) \star (h_1, h_2, \ldots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \ldots).$$

Although the operations may be different in each of the factors of a direct product, we shall, as usual, write all abstract groups multiplicatively, so that the operation in (1) above, for example, becomes simply

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n).$$

Examples

(1) Suppose $G_i = \mathbb{R}$ (operation addition) for $i = 1, 2, \ldots, n$. Then $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n-factors) is the familiar Euclidean n-space $\mathbb{R}^n$ with usual vector addition:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

(2) To illustrate that groups forming the direct product (and corresponding operations) may be completely general, let $G_1 = \mathbb{Z}$, let $G_2 = S_3$ and let $G_3 = GL_2(\mathbb{R})$, where the group operations are addition, composition, and matrix multiplication, respectively. Then the operation in $G_1 \times G_2 \times G_3$ is defined by

$$(n, \sigma, \begin{pmatrix} a & b \\ c & d \end{pmatrix})\,(m, \tau, \begin{pmatrix} p & q \\ r & s \end{pmatrix}) = (n + m, \sigma \circ \tau, \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}).$$

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).

Proof: Let $G = G_1 \times G_2 \times \cdots \times G_n$. The proof that the group axioms hold for G is straightforward since each axiom is a consequence of the fact that the same axiom holds in each factor, G_i, and the operation on G is defined componentwise. For example, the associative law is verified as follows:

Let $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n)$, and $(c_1, c_2, \ldots, c_n) \in G$. Then

$$\begin{aligned}(a_1, a_2, \ldots, a_n)\big[(b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)\big] &= (a_1, a_2, \ldots, a_n)(b_1c_1, b_2c_2, \ldots, b_nc_n) \\ &= (a_1(b_1c_1), a_2(b_2c_2), \ldots, a_n(b_nc_n)) \\ &= ((a_1b_1)c_1, (a_2b_2)c_2, \ldots, (a_nb_n)c_n) \\ &= \big[(a_1, a_2, \cdots, a_n)(b_1, b_2, \ldots, b_n)\big](c_1, c_2, \ldots, c_n),\end{aligned}$$

where in the third step we have used the associative law in each component. The remaining verification that the direct product is a group is similar: the identity of G is the n-tuple $(1_1, 1_2, \ldots, 1_n)$, where 1_i is the identity of G_i and the inverse of $(g_1, g_2, \ldots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$, where g_i^{-1} is the inverse of g_i in G_i.

The formula for the order of G is clear.

If the factors of the direct product are rearranged, the resulting direct product is isomorphic to the original one (cf. Exercise 7).

The next proposition shows that a direct product, $G_1 \times G_2 \times \cdots \times G_n$, contains an isomorphic copy of each G_i. One can think of these specific copies as the "coordinate axes" of the direct product since, in the case of $\mathbb{R} \times \mathbb{R}$, they coincide with the x and y axes. One should be careful, however, not to think of these "coordinate axes" as the *only* copies of the groups G_i in the direct product. For example in $\mathbb{R} \times \mathbb{R}$ any line through the origin is a subgroup of $\mathbb{R} \times \mathbb{R}$ isomorphic to $\mathbb{R}$ (and $\mathbb{R} \times \mathbb{R}$ has infinitely many pairs of lines which are coordinate axes, viz. any rotation of a given coordinate system). The second part of the proposition shows that there are *projection homomorphisms* onto each of the components.

Proposition 2. Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$ 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 to 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 identify 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 $\pi_i : G \to G_i$ by

$$\pi_i((g_1, g_2, \ldots, g_n)) = g_i.$$

Then π_i is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) \mid g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

(here the 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 $xy = yx$.

Proof: (1) Since the operation in G is defined componentwise, it follows easily from the subgroup criterion that $\{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}$ is a subgroup of G. Furthermore, the map $g_i \mapsto (1, 1, \ldots, 1, g_i, 1, \ldots, 1)$ is seen to be an isomorphism of G_i with this subgroup. Identify G_i with this isomorphic copy in G.

To prove the remaining parts of (1) consider the map

$$\varphi : G \longrightarrow G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

defined by

$$\varphi(g_1, g_2, \ldots, g_n) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$$

(i.e., φ erases the i^{th} component of G). The map φ is a homomorphism since

$$\begin{aligned} \varphi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) &= \varphi((g_1h_1, \ldots, g_nh_n)) \\ &= (g_1h_1, \ldots, g_{i-1}h_{i-1}, g_{i+1}h_{i+1}, \ldots, g_nh_n) \\ &= (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)(h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n) \\ &= \varphi((g_1, \ldots, g_n))\varphi((h_1, \ldots, h_n)). \end{aligned}$$

Since the entries in position j are arbitrary elements of G_j for all j, φ is surjective. Furthermore,

$$\ker \varphi = \{(g_1, \ldots, g_n) \mid g_j = 1 \text{ for all } j \neq i\} = G_i.$$

This proves that G_i is a normal subgroup of G (in particular, it again proves this copy of G_i is a subgroup) and the First Isomorphism Theorem gives the final assertion of part (1).

In (2) the argument that π_i is a surjective homomorphism and the kernel is the subgroup described is very similar to that in part (1), so the details are left to the reader.

In part (3) if $x = (1, \ldots, 1, g_i, 1, \ldots, 1)$ and $y = (1, \ldots, 1, g_j, 1, \ldots, 1)$, where the indicated entries appear in positions i, j respectively, then

$$xy = (1, \ldots, 1, g_i, 1, \ldots, 1, g_j, 1, \ldots, 1) = yx$$

(where the notation is chosen so that $i < j$). This completes the proof.

A generalization of this proposition appears as Exercise 2.

We shall continue to identify the "coordinate axis" subgroups described in part (1) of the proposition with their isomorphic copies, the G_i's. The i^{th} such subgroup is often called the i^{th} *component* or i^{th} *factor* of G. For instance, when we wish to calculate in $Z_n \times Z_m$ we can let x be a generator of the first factor, let y be a generator of the second factor and write the elements of $Z_n \times Z_m$ in the form $x^a y^b$. This replaces the formal ordered pairs $(x, 1)$ and $(1, y)$ with x and y (so $x^a y^b$ replaces (x^a, y^b)).

Examples

(1) Under the notation of Proposition 2 it follows from part (3) that if $x_i \in G_i$, $1 \leq i \leq n$, then for all $k \in \mathbb{Z}$

$$(x_1 x_2 \ldots x_n)^k = x_1^k x_2^k \ldots x_n^k.$$

Since the order of $x_1 x_2 \ldots x_n$ is the smallest positive integer k such that $x_i^k = 1$ for all i, we see that

$$|x_1 x_2 \ldots x_n| = \text{l.c.m.}(|x_1|, |x_2|, \ldots, |x_n|)$$

(where this order is infinite if and only if one of the x_i's has infinite order).

(2) Let p be a prime and for $n \in \mathbb{Z}^+$ consider

$$E_{p^n} = Z_p \times Z_p \times \cdots \times Z_p \qquad (n \text{ factors}).$$

Then E_{p^n} is an abelian group of order p^n with the property that $x^p = 1$ for all $x \in E_{p^n}$. This group is the *elementary abelian* group of order p^n described in Section 4.4.

(3) For p a prime, we show that the elementary abelian group of order p^2 has exactly $p+1$ subgroups of order p (in particular, there are more than the two obvious ones). Let $E = E_{p^2}$. Since each nonidentity element of E has order p, each of these generates a cyclic subgroup of E of order p. By Lagrange's Theorem distinct subgroups of order p intersect trivially. Thus the $p^2 - 1$ nonidentity elements of E are partitioned into subsets of size $p - 1$ (i.e., each of these subsets consists of the nonidentity elements of some subgroup of order p). There must therefore be

$$\frac{p^2 - 1}{p - 1} = p + 1$$

subgroups of order p. When $p = 2$, E is the Klein 4-group which we have already seen has 3 subgroups of order 2 (cf. also Exercises 10 and 11).