9.2 Theorem Let $G_1, G_2, \cdots, G_n$ be groups. For $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)$ to be the element $(a_1b_1, a_2b_2, \cdots, a_nb_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, the **direct product of the groups** G_i, under this binary operation.

Proof Note that since $a_i \in G_i, b_i \in G_i$, and G_i is a group, we have $a_ib_i \in G_i$. Thus the definition of the binary operation on $\prod_{i=1}^{n} G_i$ given in the statement of the theorem makes sense; that is, $\prod_{i=1}^{n} G_i$ is closed under the binary operation.

The associative law in $\prod_{i=1}^{n} G_i$ is thrown back onto the associative law in each component as follows:

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

If e_i is the identity element in G_i, then clearly, with multiplication by components, $(e_1, e_2, \cdots, e_n)$ is an identity in $\prod_{i=1}^{n} G_i$. Finally, an inverse of $(a_1, a_2, \cdots, a_n)$ is $(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$; compute the product by components. Hence $\prod_{i=1}^{n} G_i$ is a group. ◆

In the event that the operation of each G_i is commutative, we sometimes use additive notation in $\prod_{i=1}^{n} G_i$ and refer to $\prod_{i=1}^{n} G_i$ as the **direct sum of the groups** G_i. The notation $\oplus_{i=1}^{n} G_i$ is sometimes used in this case in place of $\prod_{i=1}^{n} G_i$, especially with abelian groups with operation $+$. The direct sum of abelian groups $G_1, G_2, \cdots, G_n$ may be written $G_1 \oplus G_2 \oplus \cdots \oplus G_n$. We leave to Exercise 46 the proof that a direct product of abelian groups is again abelian.

It is quickly seen that if B_i has r_i elements for $i = 1, \cdots, n$, then $\prod_{i=1}^{n} B_i$ has $r_1r_2 \cdots r_n$ elements, for in an n-tuple, there are r_1 choices for the first component from B_1, and for each of these there are r_2 choices for the next component from B_2, and so on.

9.3 Example Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, which has $2 \cdot 3 = 6$ elements, namely (0, 0), (0, 1), (0, 2), (1, 0), (1, 1), and (1, 2). We claim that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is only necessary to find a generator. Let us try (1, 1). Here the operations in $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are written additively, so we do the same in the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$.

$$\begin{aligned}
(1, 1) &= (1, 1) \\
2(1, 1) &= (1, 1) + (1, 1) = (0, 2) \\
3(1, 1) &= (1, 1) + (1, 1) + (1, 1) = (1, 0) \\
4(1, 1) &= 3(1, 1) + (1, 1) = (1, 0) + (1, 1) = (0, 1) \\
5(1, 1) &= 4(1, 1) + (1, 1) = (0, 1) + (1, 1) = (1, 2) \\
6(1, 1) &= 5(1, 1) + (1, 1) = (1, 2) + (1, 1) = (0, 0)
\end{aligned}$$

Thus (1, 1) generates all of $\mathbb{Z}_2 \times \mathbb{Z}_3$. Since there is, up to isomorphism, only one cyclic group structure of a given order, we see that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$. ▲

9.4 Example Consider $\mathbb{Z}_3 \times \mathbb{Z}_3$. This is a group of nine elements. We claim that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is *not* cyclic. Since the addition is by components, and since in $\mathbb{Z}_3$ every element added to itself three times gives the identity, the same is true in $\mathbb{Z}_3 \times \mathbb{Z}_3$. Thus no element can generate the group, for a generator added to itself successively could only give the identity after nine

summands. We have found another group structure of order 9. A similar argument shows that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Thus $\mathbb{Z}_2 \times \mathbb{Z}_2$ must be isomorphic to the Klein 4-group. ▲

The preceding examples illustrate the following theorem:

9.5 Theorem The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime, that is, the gcd of m and n is 1.

Proof Consider the cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by (1, 1) as described by Theorem 5.19. As our previous work has shown, the order of this cyclic subgroup is the smallest power of (1, 1) that gives the identity (0, 0). Here taking a power of (1, 1) in our additive notation will involve adding (1, 1) to itself repeatedly. Under addition by components, the first component $1 \in \mathbb{Z}_m$ yields 0 only after m summands, $2m$ summands, and so on, and the second component $1 \in \mathbb{Z}_n$ yields 0 only after n summands, $2n$ summands, and so on. For them to yield 0 simultaneously, the number of summands must be a multiple of both m and n. The smallest number that is a multiple of both m and n will be mn if and only if the gcd of m and n is 1; in this case, (1, 1) generates a cyclic subgroup of order mn, which is the order of the whole group. This shows that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn, and hence isomorphic to $\mathbb{Z}_{mn}$ if m and n are relatively prime.

For the converse, suppose that the gcd of m and n is $d > 1$. Then mn/d is divisible by both m and n. Consequently, for any (r, s) in $\mathbb{Z}_m \times \mathbb{Z}_n$, we have

$$\underbrace{(r,s) + (r,s) + \cdots + (r,s)}_{mn/d \text{ summands}} = (0,0).$$

Hence no element (r, s) in $\mathbb{Z}_m \times \mathbb{Z}_n$ can generate the entire group, so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic and therefore not isomorphic to $\mathbb{Z}_{mn}$. ◆

This theorem can be extended to a product of more than two factors by similar arguments. We state this as a corollary without going through the details of the proof.

9.6 Corollary The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, \cdots, n$ are such that the gcd of any two of them is 1.

9.7 Example The preceding corollary shows that if n is written as a product of powers of distinct prime numbers, as in

$$n = (p_1)^{n_1}(p_2)^{n_2} \cdots (p_r)^{n_r},$$

then $\mathbb{Z}_n$ is isomorphic to

$$\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{n_r}}.$$

In particular, $\mathbb{Z}_{72}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_9$. ▲

We remark that changing the order of the factors in a direct product yields a group isomorphic to the original one. The names of elements have simply been changed via a permutation of the components in the n-tuples.

Exercise 57 of Section 6 asked you to define the least common multiple of two positive integers r and s as a generator of a certain cyclic group. It is straightforward to prove that the subset of $\mathbb{Z}$ consisting of all integers that are multiples of both r and s is a subgroup of $\mathbb{Z}$, and hence is a cyclic group. Likewise, the set of all common multiples of n positive integers $r_1, r_2, \cdots, r_n$ is a subgroup of $\mathbb{Z}$, and hence is cyclic.

9.8 Definition Let $r_1, r_2, \cdots, r_n$ be positive integers. Their **least common multiple** (abbreviated lcm) is the positive generator of the cyclic group of all common multiples of the r_i, that is, the cyclic group of all integers divisible by each r_i for $i = 1, 2, \cdots, n$. ■

From Definition 9.8 and our work on cyclic groups, we see that the lcm of $r_1, r_2, \cdots, r_n$ is the smallest positive integer that is a multiple of each r_i for $i = 1, 2, \cdots, n$, hence the name *least common multiple*.

9.9 Theorem Let $(a_1, a_2, \cdots, a_n) \in \prod_{i=1}^{n} G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, \cdots, a_n)$ in $\prod_{i=1}^{n} G_i$ is equal to the least common multiple of all the r_i.

Proof This follows by a repetition of the argument used in the proof of Theorem 9.5. For a power of $(a_1, a_2, \cdots, a_n)$ to give $(e_1, e_2, \cdots, e_n)$, the power must simultaneously be a multiple of r_1 so that this power of the first component a_1 will yield e_1, a multiple of r_2, so that this power of the second component a_2 will yield e_2, and so on. ◆

9.10 Example Find the order of (8, 4, 10) in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

Solution Since the gcd of 8 and 12 is 4, we see that 8 is of order $\frac{12}{4} = 3$ in $\mathbb{Z}_{12}$. (See Theorem 6.15.) Similarly, we find that 4 is of order 15 in $\mathbb{Z}_{60}$ and 10 is of order 12 in $\mathbb{Z}_{24}$. The lcm of 3, 15, and 12 is $3 \cdot 5 \cdot 4 = 60$, so (8, 4, 10) is of order 60 in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. ▲

9.11 Example The group $\mathbb{Z} \times \mathbb{Z}_2$ is generated by the elements (1, 0) and (0, 1). More generally, the direct product of n cyclic groups, each of which is either $\mathbb{Z}$ or $\mathbb{Z}_m$ for some positive integer m, is generated by the n n-tuples

$$(1, 0, 0, \cdots, 0), \quad (0, 1, 0, \cdots, 0), \quad (0, 0, 1, \cdots, 0), \quad \cdots, \quad (0, 0, 0, \cdots, 1).$$

Such a direct product might also be generated by fewer elements. For example, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$ is generated by the single element (1, 1, 1). ▲

Note that if $\prod_{i=1}^{n} G_i$ is the direct product of groups G_i, then the subset

$$\bar{G}_i = \{(e_1, e_2, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \mid a_i \in G_i\},$$

that is, the set of all n-tuples with the identity elements in all places but the ith, is a subgroup of $\prod_{i=1}^{n} G_i$. It is also clear that this subgroup $\bar{G}_i$ is naturally isomorphic to G_i; just rename

$$(e_1, e_2, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \text{ by } a_i.$$

The group G_i is mirrored in the ith component of the elements of $\bar{G}_i$, and the e_j in the other components just ride along. We consider $\prod_{i=1}^{n} G_i$ to be the *internal direct product* of these subgroups $\bar{G}_i$. The direct product given by Theorem 9.2 is called the *external direct product* of the groups G_i. The terms *internal* and *external,* as applied to a direct product of groups, just reflect whether or not (respectively) we are regarding the component groups as subgroups of the product group. We shall usually omit the words *external* and *internal* and just say *direct product*. Which term we mean will be clear from the context.

The Structure of Finitely Generated Abelian Groups

Some theorems of abstract algebra are easy to understand and use, although their proofs may be quite technical and time-consuming to present. This is one section in the text where we explain the meaning and significance of a theorem but omit its proof. The

HISTORICAL NOTE

In his *Disquisitiones Arithmeticae,* Carl Gauss demonstrated various results in what is today the theory of abelian groups in the context of number theory. Not only did he deal extensively with equivalence classes of quadratic forms, but he also considered residue classes modulo a given integer. Although he noted that results in these two areas were similar, he did not attempt to develop an abstract theory of abelian groups.

In the 1840s, Ernst Kummer in dealing with ideal complex numbers noted that his results were in many respects analogous to those of Gauss. (See the Historical Note in Section 30.) But it was Kummer's student Leopold Kronecker (see the Historical Note in Section 39) who finally realized that an abstract theory could be developed out of the analogies. As he wrote in 1870, "these principles [from the work of Gauss and Kummer] belong to a more general, abstract realm of ideas. It is therefore appropriate to free their development from all unimportant restrictions, so that one can spare oneself from the necessity of repeating the same argument in different cases. This advantage already appears in the development itself, and the presentation gains in simplicity, if it is given in the most general admissible manner, since the most important features stand out with clarity." Kronecker then proceeded to develop the basic principles of the theory of finite abelian groups and was able to state and prove a version of Theorem 9.12 restricted to finite groups.

meaning of any theorem whose proof we omit is well within our understanding, and we feel we should be acquainted with it. It would be impossible for us to meet some of these fascinating facts in a one-semester course if we were to insist on wading through complete proofs of all theorems. The theorem that we now state gives us complete structural information about many abelian groups, in particular, about all finite abelian groups.

9.12 Theorem **(Primary Factor Version of the Fundamental Theorem of Finitely Generated Abelian Groups)** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.

Proof The proof is omitted here. ◆

9.13 Example Find all abelian groups, up to isomorphism, of order 360. The phrase *up to isomorphism* signifies that any abelian group of order 360 should be structurally identical (isomorphic) to one of the groups of order 360 exhibited.

Solution We make use of Theorem 9.12. Since our groups are to be of the finite order 360, no factors $\mathbb{Z}$ will appear in the direct product shown in the statement of the theorem.

First we express 360 as a product of prime powers $2^3 3^2 5$. Then using Theorem 9.12, we get as possibilities

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

2. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

3. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$