45. Show that a finite cyclic group of order \( n \) has exactly one subgroup of each order \( d \) dividing \( n \), and that these are all the subgroups it has.

46. The Euler phi-function is defined for positive integers \( n \) by \( \varphi(n) = s \), where \( s \) is the number of positive integers less than or equal to \( n \) that are relatively prime to \( n \). Use Exercise 45 to show that

\[
n = \sum_{d \mid n} \varphi(d),
\]

the sum being taken over all positive integers \( d \) dividing \( n \). [Hint: Note that the number of generators of \( \mathbb{Z}_d \) is \( \varphi(d) \) by Corollary 6.16.]

47. Let \( G \) be a finite group. Show that if for each positive integer \( m \) the number of solutions \( x \) of the equation \( x^m = e \) in \( G \) is at most \( m \), then \( G \) is cyclic. [Hint: Use Theorem 10.12 and Exercise 46 to show that \( G \) must contain an element of order \( n = |G| \).]

## Section 11

### Direct Products and Finitely Generated Abelian Groups

#### Direct Products

Let us take a moment to review our present stockpile of groups. Starting with finite groups, we have the cyclic group \( \mathbb{Z}_n \), the symmetric group \( S_n \), and the alternating group \( A_n \) for each positive integer \( n \). We also have the dihedral groups \( D_n \) of Section 8, and the Klein 4-group \( V \). Of course we know that subgroups of these groups exist. Turning to infinite groups, we have groups consisting of sets of numbers under the usual addition or multiplication, as, for example, \( \mathbb{Z}, \mathbb{R}, \text{ and } \mathbb{C} \) under addition, and their nonzero elements under multiplication. We have the group \( U \) of complex numbers of magnitude 1 under multiplication, which is isomorphic to each of the groups \( \mathbb{R}_c \) under addition modulo \( c \), where \( c \in \mathbb{R}^+ \). We also have the group \( S_A \) of all permutations of an infinite set \( A \), as well as various groups formed from matrices.

One purpose of this section is to show a way to use known groups as building blocks to form more groups. The Klein 4-group will be recovered in this way from the cyclic groups. Employing this procedure with the cyclic groups gives us a large class of abelian groups that can be shown to include all possible structure types for a finite abelian group.

We start by generalizing Definition 0.4.

#### 11.1 Definition

The Cartesian product of sets \( S_1, S_2, \ldots, S_n \) is the set of all ordered \( n \)-tuples \((a_1, a_2, \ldots, a_n)\), where \( a_i \in S_i \) for \( i = 1, 2, \ldots, n \). The Cartesian product is denoted by either

\[
S_1 \times S_2 \times \cdots \times S_n
\]

or by

\[
\prod_{i=1}^{n} S_i.
\]

We could also define the Cartesian product of an infinite number of sets, but the definition is considerably more sophisticated and we shall not need it.

Now let \( G_1, G_2, \ldots, G_n \) be groups, and let us use multiplicative notation for all the group operations. Regarding the \( G_i \) as sets, we can form \( \prod_{i=1}^{n} G_i \). Let us show that we can make \( \prod_{i=1}^{n} G_i \) into a group by means of a binary operation of multiplication by
and that these

sitive integers

11.2 Theorem

Let \( G_1, G_2, \ldots, G_n \) be groups. For \((a_1, a_2, \ldots, a_n)\) and \((b_1, b_2, \ldots, b_n)\) in \( \prod_{i=1}^{n} G_i \), define \((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)\) to be the element \((a_1b_1, a_2b_2, \ldots, a_nb_n)\). 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 \( a_i b_i \in G_i \). 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:

\[
(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n) = (a_1, a_2, \ldots, a_n)(b_1c_1, b_2c_2, \ldots, b_nc_n) = (a_1(b_1c_1), a_2(b_2c_2), \ldots, a_nc_n) = ((a_1b_1)c_1, (a_2b_2)c_2, \ldots, (a_nb_n)c_n) = (a_1(b_1a_2b_2), a_2b_2c_2, \ldots, a_nb_n)(c_1, c_2, \ldots, c_n) = [(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)](c_1, c_2, \ldots, c_n).
\]

If \( e_i \) is the identity element in \( G_i \), then clearly, with multiplication by components, \( (e_1, e_2, \ldots, e_n) \) is an identity in \( \prod_{i=1}^{n} G_i \). Finally, an inverse of \((a_1, a_2, \ldots, a_n)\) is \((a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})\); 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 \( \oplus\prod_{i=1}^{n} G_i \) 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 \( G_1, G_2, \ldots, G_n \) 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 the \( S_i \) has \( r_i \) elements for \( i = 1, \ldots, n \), then \( \prod_{i=1}^{n} S_i \) has \( r_1r_2\cdots r_n \) elements, for in an \( n \)-tuple, there are \( r_1 \) choices for the first component from \( S_1 \), and for each of these there are \( r_2 \) choices for the next component from \( S_2 \), and so on.

11.3 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 \( \mathbb{Z}_2 \times \mathbb{Z}_3 \).

\[
(1, 1) = (1, 1)
\]

\[
2(1, 1) = (1, 1) + (1, 1) = (0, 2)
\]

\[
3(1, 1) = (1, 1) + (1, 1) + (1, 1) = (1, 0)
\]

\[
4(1, 1) = 3(1, 1) + (1, 1) = (1, 0) + (1, 1) = (0, 1)
\]

\[
5(1, 1) = 4(1, 1) + (1, 1) = (0, 1) + (1, 1) = (1, 2)
\]

\[
6(1, 1) = 5(1, 1) + (1, 1) = (1, 2) + (1, 1) = (0, 0)
\]
Thus (1, 1) generates all of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since there is, up to isomorphism, only one cyclic group structure of a given order, we see that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to $\mathbb{Z}_4$.

11.4 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:

11.5 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 5.17. 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 $d > 1$. The $mn/d$ is divisible by both $m$ and $n$. Consequently, for any $(r, s)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$, we have

\[
\frac{(r, s) + (r, s) + \cdots + (r, s)}{mn/d} = (0, 0).
\]

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.

11.6 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 $i = 1, 2, \ldots, n$ are such that the gcd of any two of them is 1.

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

\[
n = (p_1)^{r_1}(p_2)^{r_2}\cdots(p_r)^{r_r},
\]

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

\[
\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{r_r}}.
\]

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 47 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 Z consisting of all integers that are multiples of both r and s is a subgroup of Z, and hence is a cyclic group. Likewise, the set of all common multiples of n positive integers \( r_1, r_2, \ldots, r_n \) is a subgroup of Z, and hence is cyclic.

**11.8 Definition** Let \( r_1, r_2, \ldots, r_n \) 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 \( i = 1, 2, \ldots, n \).

From Definition 11.8 and our work on cyclic groups, we see that the lcm of \( r_1, r_2, \ldots, r_n \) is the smallest positive integer that is a multiple of each \( r_i \) for \( i = 1, 2, \ldots, n \), hence the name least common multiple.

**11.9 Theorem** Let \( (a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i \). If \( a_i \) is of finite order \( r_i \) in \( G_i \), then the order of \( (a_1, a_2, \ldots, a_n) \) 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 11.5. For a power of \( (a_1, a_2, \ldots, a_n) \) to give \((e_1, e_2, \ldots, e_n)\), the power must simultaneously be a multiple of \( r_i \) 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.

**11.10 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 6.14.) 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 \( \mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24} \).

**11.11 Example** The group \( \mathbb{Z} \times \mathbb{Z} \) 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

\[
(1, 0, \ldots, 0), \quad (0, 1, 0, \ldots, 0), \quad (0, 0, 1, \ldots, 0), \quad \ldots, \quad (0, 0, 0, \ldots, 1).
\]

Such a direct product might also be generated by fewer elements. For example, \( \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \) 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

\[
\overline{G_i} = \{(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\},
\]

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

\[(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \text{ by } a_i.\]
Part II  Permutations, Cosets, and Direct Products

The group \( G_i \) is mirrored in the \( i \)th 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 11.2 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.

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 26.) But it was Kummer's student Leopold Kronecker (see the Historical Note in Section 29) 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 11.12 restricted to finite groups.

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 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 all sufficiently small abelian groups, in particular, about all finite abelian groups.

11.12 Theorem  (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

\[
\mathbb{Z}_{(p_i^{y_i})} \times \mathbb{Z}_{(p_i^{y_i})} \times \cdots \times \mathbb{Z}_{(p_i^{y_i})} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},
\]
and the $e_j$ in internal direct 2 is called the $r_j$ as applied to 3 regarding the omit the words 1 be clear from

ealogies. As in the work ore general, appropriate portant re- d from the nt in di f er- us in the de- gains in sim- al adm issible st out d to develop finite abelian a version of


Section 11  Direct Products and Finitely Generated Abelian Groups

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.

11.13 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 11.12. 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 $2^33^25$. Then using Theorem 11.12, 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. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
6. $\mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Thus there are six different abelian groups (up to isomorphism) of order 360.

**Applications**

We conclude this section with a sampling of the many theorems we could now prove regarding abelian groups.

11.14 Definition A group $G$ is decomposable if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise $G$ is indecomposable.

11.15 Theorem The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

**Proof** Let $G$ be a finite indecomposable abelian group. Then by Theorem 11.12, $G$ is isomorphic to a direct product of cyclic groups of prime power order. Since $G$ is indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime number.

Conversely, let $p$ be a prime. Then $\mathbb{Z}_{p^r}$ is indecomposable, for if $\mathbb{Z}_{p^s}$ were isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, where $i + j = r$, then every element would have an order at most $p^{\max(i,j)} < p^r$.

11.16 Theorem If $m$ divides the order of a finite abelian group $G$, then $G$ has a subgroup of order $m$.

**Proof** By Theorem 11.12, we can think of $G$ as being

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_1)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}.$$
where not all primes }p_i\text{ need be distinct. Since } (p_1)^{r_1}(p_2)^{r_2} \cdots (p_n)^{r_n} \text{ is the order of } G, \text{ then } m \text{ must be of the form } (p_1)^{s_1}(p_2)^{s_2} \cdots (p_n)^{s_n}, \text{ where } 0 \leq s_i \leq r_i. \text{ By Theorem 6.14, } (p_i)^{r_i-s_i} \text{ generates a cyclic subgroup of } Z_{(p_i)^{r_i}} \text{ of order equal to the quotient of } (p_i)^{r_i} \text{ by the gcd of } (p_i)^{r_i} \text{ and } (p_i)^{r_i-s_i}. \text{ But the gcd of } (p_i)^{r_i} \text{ and } (p_i)^{r_i-s_i} \text{ is } (p_i)^{r_i-s_i}. \text{ Thus } (p_i)^{r_i-s_i} \text{ generates a cyclic subgroup of } Z_{(p_i)^{r_i}} \text{ of order }

\frac{(p_i)^{r_i}}{(p_i)^{r_i-s_i}} = (p_i)^{s_i}.

Recalling that } a \text{ denotes the cyclic subgroup generated by } a, \text{ we see that }

\frac{(p_i)^{r_i-s_i} \times (p_2)^{r_2-s_2} \times \cdots \times (p_n)^{r_n-s_n}}

\text{is the required subgroup of order } m.

11.17 Theorem

If } m \text{ is a square free integer, that is, } m \text{ is not divisible by the square of any prime, then every abelian group of order } m \text{ is cyclic.}

**Proof**

Let } G \text{ be an abelian group of square free order } m. \text{ Then by Theorem 11.12, } G \text{ is isomorphic to }

Z_{(p_1)^{r_1}} \times Z_{(p_2)^{r_2}} \times \cdots \times Z_{(p_n)^{r_n}},

\text{where } m = (p_1)^{r_1}(p_2)^{r_2} \cdots (p_n)^{r_n}. \text{ Since } m \text{ is square free, we must have all } r_i = 1 \text{ and all } p_i \text{ distinct primes. Corollary 11.6 then shows that } G \text{ is isomorphic to } Z_{p_1 p_2 \cdots p_n}, \text{ so } G \text{ is cyclic.}

**EXERCISES 11**

**Computations**

1. List the elements of } Z_2 \times Z_4. \text{ Find the order of each of the elements. Is this group cyclic?}

2. Repeat Exercise 1 for the group } Z_3 \times Z_4.

In Exercises 3 through 7, find the order of the given element of the direct product.

3. (2, 6) in } Z_4 \times Z_{12}

4. (2, 3) in } Z_6 \times Z_{15}

5. (8, 10) in } Z_{12} \times Z_{18}

6. (3, 10, 9) in } Z_4 \times Z_{12} \times Z_{15}

7. (3, 6, 12, 16) in } Z_4 \times Z_{12} \times Z_{20} \times Z_{24}

8. What is the largest order among the orders of all the cyclic subgroups of } Z_6 \times Z_8? \text{ of } Z_{12} \times Z_{15}?

9. Find all proper nontrivial subgroups of } Z_2 \times Z_2.

10. Find all proper nontrivial subgroups of } Z_2 \times Z_2 \times Z_2.

11. Find all subgroups of } Z_2 \times Z_4 \text{ of order 4.}

12. Find all subgroups of } Z_2 \times Z_2 \times Z_4 \text{ that are isomorphic to the Klein 4-group.}

13. Disregarding the order of the factors, write direct products of two or more groups of the form } Z_n \text{ so that the resulting product is isomorphic to } Z_{50} \text{ in as many ways as possible.}

14. Fill in the blanks.

a. The cyclic subgroup of } Z_{24} \text{ generated by } 18 \text{ has order } .

b. } Z_3 \times Z_4 \text{ is of order } .

c. The

d. The

e. } Z_2 \times Z_3 >

15. Find the

16. Are the

17. Find the

18. Are the

19. Find the

20. Are the

In Exercises order.

21. Order 8

24. Order 7

26. How m

27. Followi there ar rs abeli

28. Use Ex

29. a. Let , up to

b. Let up to

i.

30. Indicate

31. Consider and the joining and group and counter

a. Un

b. If G

c. If G

d. If G
order of $G$

11. Exercises

15. Find the maximum possible order for some element of $Z_4 \times Z_6$.

16. Are the groups $Z_2 \times Z_{12}$ and $Z_4 \times Z_6$ isomorphic? Why or why not?

17. Find the maximum possible order for some element of $Z_8 \times Z_{10} \times Z_{24}$.

18. Are the groups $Z_8 \times Z_{10} \times Z_{24}$ and $Z_4 \times Z_{12} \times Z_{40}$ isomorphic? Why or why not?

19. Find the maximum possible order for some element of $Z_4 \times Z_{18} \times Z_{15}$.

20. Are the groups $Z_4 \times Z_{18} \times Z_{15}$ and $Z_3 \times Z_{36} \times Z_{10}$ isomorphic? Why or why not?

In Exercises 21 through 25, proceed as in Example 11.13 to find all abelian groups, up to isomorphism, of the given order.

21. Order 8

22. Order 16

23. Order 32

24. Order 720

25. Order 1089

26. How many abelian groups (up to isomorphism) are there of order 24? of order 25? of order (24)(25)?

27. Following the idea suggested in Exercise 26, let $m$ and $n$ be relatively prime positive integers. Show that if there are (up to isomorphism) $r$ abelian groups of order $m$ and $s$ of order $n$, then there are (up to isomorphism) $rs$ abelian groups of order $mn$.

28. Use Exercise 27 to determine the number of abelian groups (up to isomorphism) of order (10)^5.

29. a. Let $p$ be a prime number. Fill in the second row of the table to give the number of abelian groups of order $p^n$, up to isomorphism.

<table>
<thead>
<tr>
<th>$n$</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b. Let $p$, $q$, and $r$ be distinct prime numbers. Use the table you created to find the number of abelian groups, up to isomorphism, of the given order.

i. $p^3q^4r^7$  

ii. $(qr)^7$  

iii. $q^5r4q^3$

30. Indicate schematically a Cayley digraph for $Z_m \times Z_n$ for the generating set $S = \{(1, 0), (0, 1)\}$.

31. Consider Cayley digraphs with two arc types, a solid one with an arrow and a dashed one with no arrow, and consisting of two regular $n$-gons, for $n \geq 3$, with solid arc sides, one inside the other, with dashed arcs joining the vertices of the inner $n$-gon to the outer one. Figure 7.9(b) shows such a Cayley digraph with $n = 3$, and Figure 7.11(b) shows one with $n = 4$. The arrows on the outer $n$-gon may have the same (clockwise or counterclockwise) direction as those on the inner $n$-gon, or they may have the opposite direction. Let $G$ be a group with such a Cayley digraph.

a. Under what circumstances will $G$ be abelian?

b. If $G$ is abelian, to what familiar group is it isomorphic?

c. If $G$ is abelian, under what circumstances is it cyclic?

d. If $G$ is not abelian, to what group we have discussed is it isomorphic?
Concepts

32. Mark each of the following true or false.
   a. If $G_1$ and $G_2$ are any groups, then $G_1 \times G_2$ is always isomorphic to $G_2 \times G_1$.
   b. Computation in an external direct product of groups is easy if you know how to compute in each component group.
   c. Groups of finite order must be used to form an external direct product.
   d. A group of prime order could not be the internal direct product of two proper nontrivial subgroups.
   e. $Z_2 \times Z_4$ is isomorphic to $Z_8$.
   f. $Z_2 \times Z_4$ is isomorphic to $S_3$.
   g. $Z_3 \times Z_6$ is isomorphic to $S_4$.
   h. Every element in $Z_4 \times Z_2$ has order 8.
   i. The order of $Z_{12} \times Z_{15}$ is 60.
   j. $Z_m \times Z_n$ has $mn$ elements whether $m$ and $n$ are relatively prime or not.

33. Give an example illustrating that not every nontrivial abelian group is the internal direct product of two proper nontrivial subgroups.

34. a. How many subgroups of $Z_3 \times Z_6$ are isomorphic to $Z_3 \times Z_6$?
   b. How many subgroups of $Z \times Z$ are isomorphic to $Z \times Z$?

35. Give an example of a nontrivial group that is not of prime order and is not the internal direct product of two nontrivial subgroups.

36. Mark each of the following true or false.
   a. Every abelian group of prime order is cyclic.
   b. Every abelian group of prime power order is cyclic.
   c. $Z_8$ is generated by $\{4, 6\}$.
   d. $Z_8$ is generated by $\{4, 5, 6\}$.
   e. All finite abelian groups are classified up to isomorphism by Theorem 11.12.
   f. Any two finitely generated abelian groups with the same Betti number are isomorphic.
   g. Every abelian group of order divisible by 5 contains a cyclic subgroup of order 5.
   h. Every abelian group of order divisible by 4 contains a cyclic subgroup of order 4.
   i. Every abelian group of order divisible by 6 contains a cyclic subgroup of order 6.
   j. Every finite abelian group has a Betti number of 0.

37. Let $p$ and $q$ be distinct prime numbers. How does the number (up to isomorphism) of abelian groups of order $p^aq^b$ compare with the number (up to isomorphism) of abelian groups of order $p^aq^b$?

38. Let $G$ be an abelian group of order 72.
   a. Can you say how many subgroups of order 8 $G$ has? Why, or why not?
   b. Can you say how many subgroups of order 4 $G$ has? Why, or why not?

39. Let $G$ be an abelian group. Show that the elements of finite order in $G$ form a subgroup. This subgroup is called the **torsion subgroup** of $G$.

Exercises 40 through 43 deal with the concept of the torsion subgroup just defined.

40. Find the order of the torsion subgroup of $Z_4 \times Z \times Z_3$; of $Z_{12} \times Z \times Z_{12}$. 

41. Find
42. Find
43. An all every subgr
44. The j can a num
   a. Fi
   b. Fi
   c. D

Proof Sy:

45. Give

Theory

46. Prow
47. Let $G$
48. Follk
   G if integ
   all el
49. Find

Let $H$ an
for $G$ to:

50. Let i way:
   a. E
   b. h

51. Let j that
   Shov
52. Shov
   som
53. Prov
   is a
54. Let G s
41. Find the torsion subgroup of the multiplicative group $R^*$ of nonzero real numbers.

42. Find the torsion subgroup $T$ of the multiplicative group $C^*$ of nonzero complex numbers.

43. An abelian group is **torsion free** if $e$ is the only element of finite order. Use Theorem 11.12 to show that every finitely generated abelian group is the internal direct product of its torsion subgroup and of a torsion-free subgroup. (Note that $\{e\}$ may be the torsion subgroup, and is also torsion free.)

44. The part of the decomposition of $G$ in Theorem 11.12 corresponding to the subgroups of prime-power order can also be written in the form $Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_r}$, where $m_i$ divides $m_{i+1}$ for $i = 1, 2, \ldots, r - 1$. The numbers $m_i$ can be shown to be unique, and are the **torsion coefficients** of $G$.
   
   a. Find the torsion coefficients of $Z_4 \times Z_9$.
   
   b. Find the torsion coefficients of $Z_6 \times Z_{12} \times Z_{20}$.
   
   c. Describe an algorithm to find the torsion coefficients of a direct product of cyclic groups.

**Proof Synopsis**

45. Give a two-sentence synopsis of the proof of Theorem 11.5.

**Theory**

46. Prove that a direct product of abelian groups is abelian.

47. Let $G$ be an abelian group. Let $H$ be the subset of $G$ consisting of the identity $e$ together with all elements of $G$ of order 2. Show that $H$ is a subgroup of $G$.

48. Following up the idea of Exercise 47 determine whether $H$ will always be a subgroup for every abelian group $G$ if $H$ consists of the identity $e$ together with all elements of $G$ of order 3; of order 4. For what positive integers $n$ will $H$ always be a subgroup for every abelian group $G$, if $H$ consists of the identity $e$ together with all elements of $G$ of order $n$? Compare with Exercise 48 of Section 5.

49. Find a counterexample of Exercise 47 with the hypothesis that $G$ is abelian omitted.

Let $H$ and $K$ be subgroups of a group $G$. Exercises 50 and 51 ask you to establish necessary and sufficient criteria for $G$ to appear as the internal direct product of $H$ and $K$.

50. Let $H$ and $K$ be groups and let $G = H \times K$. Recall that both $H$ and $K$ appear as subgroups of $G$ in a natural way. Show that these subgroups $H$ (actually $H \times \{e\}$) and $K$ (actually $\{e\} \times K$) have the following properties.
   
   a. Every element of $G$ is of the form $hk$ for some $h \in H$ and $k \in K$.
   
   b. $hk = kh$ for all $h \in H$ and $k \in K$.
   
   c. $H \cap K = \{e\}$.

51. Let $H$ and $K$ be subgroups of a group $G$ satisfying the three properties listed in the preceding exercise. Show that for each $g \in G$, the expression $g = h k$ for $h \in H$ and $k \in K$ is unique. Then let each $g$ be renamed $(h, k)$. Show that, under this renaming, $G$ becomes structurally identical (isomorphic) to $H \times K$.

52. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $Z_p \times Z_p$ for some prime $p$.

53. Prove that if a finite abelian group has order a power of a prime $p$, then the order of every element in the group is a power of $p$. Can the hypothesis of commutativity be dropped? Why, or why not?

54. Let $G$, $H$, and $K$ be finitely generated abelian groups. Show that if $G \times K$ is isomorphic to $H \times K$, then $G \cong H$. 