Chapter 13
Groups, Rings, and Modules

13.1 Groups and Homomorphisms

The concept of a group is defined axiomatically, analogously to the notions of vector, inner product, and affine space. Such an abstract definition is justified by the wealth of examples of groups throughout all of mathematics.

Definition 13.1 A *group* is a set G on which is defined an operation that assigns to each pair of elements of this set some third element; that is, there is defined a mapping $G \times G \to G$. The element associated with the elements g_1 and g_2 by this rule is called their *product* and is denoted by $g_1 \cdot g_2$ or simply $g_1 g_2$. For this mapping, the following conditions must also be satisfied:

(1) There exists an element $e \in G$ such that for every $g \in G$, we have the relationships $eg = g$ and $ge = g$. This element is called the *identity*.[1]

(2) For each element $g \in G$, there exist an element $g' \in G$ such that $gg' = e$ and an element $g'' \in G$ such that $g''g = e$. The element g' is called a *right inverse*, and the element g'' is called a *left inverse* of the element g.

(3) For every triple of elements $g_1, g_2, g_3 \in G$, the following relationship holds:

$$(g_1 g_2) g_3 = g_1 (g_2 g_3). \tag{13.1}$$

This last property is called *associativity*, and it is a property that we have already met repeatedly, for example in connection with the composition of mappings and matrix multiplication, and also in the construction of the exterior algebra. We considered the associative property in its most general form on p. xv, where we proved that equality (13.1) makes it possible to define the product of an *arbitrary* number of factors $g_1 g_2 \cdots g_k$, which then depends only on the order of the factors and not

[1] The identity element of a group is unique. Indeed, if there existed another identity element $e' \in G$, then by definition, we would have the equalities $ee' = e'$ and $ee' = e$, from which it follows that $e = e'$.

I.R. Shafarevich, A.O. Remizov, *Linear Algebra and Geometry*,
DOI 10.1007/978-3-642-30994-6_13, © Springer-Verlag Berlin Heidelberg 2013

on the arrangement of parentheses in the product. The reasoning given there applies, obviously, to every group.

The condition of associativity has other important consequences. From it, derives, for example, the fact that if g' is a right inverse of g, and g'' is a left inverse, then

$$g''(gg') = g''e = g'', \qquad g''(gg') = (g''g)g' = eg' = g',$$

from which it follows that $g' = g''$. Thus the left and right inverses of any given element $g \in G$ coincide. This unique element $g' = g''$ is called simply the *inverse* of g and is denoted by g^{-1}.

Definition 13.2 If the number of elements belonging to a group G is finite, then the group G is called a *finite group*, and otherwise, it is called an *infinite group*. The number of distinct elements in a finite group G is called its *order* and is denoted by $|G|$.

Let M be an arbitrary set, and let us consider the collection of all bijective mappings between M and itself. Such mappings are also called *transformations* of the set M. In the introductory section of this book, we defined the operation of composition (that is, the sequential application) of arbitrary mappings of arbitrary sets (p. xiv). It follows from the properties proved there that the collection of all transformations of a set M together with the operation of composition forms a group, where the inverse of each transformation $f : M \to M$ is given by the inverse mapping $f^{-1} : M \to M$, while the identity is obviously given by the identity mapping on the set M. Such groups are called *transformation groups*, and it is with these that the majority of applications of groups are associated.

It is sometimes necessary to consider not all the transformations of a set, but to limit our consideration to some subset. The situation that thus arises can be formulated conveniently as follows:

Definition 13.3 A subset $G' \subset G$ of elements of a group G is called a *subgroup* of G if the following conditions are satisfied:

(a) For every pair of elements $g_1, g_2 \in G'$, their product $g_1 g_2$ is again in G'.
(b) G' contains the identity element e.
(c) For every $g \in G'$, its inverse g^{-1} is again in G'.

It is obvious that a subgroup G' is itself a group. Thus from the group of all transformations, we obtain a set of examples (indeed, the majority of examples of groups). Let us enumerate some that are met most frequently.

Example 13.4 The following sets are groups under the operation of composition of mappings.

1. the set of nonsingular linear transformations of a vector space;
2. the set of orthogonal transformations of a Euclidean space;

3. the set of proper orthogonal transformations of a Euclidean space;
4. the set of Lorentz transformations of a pseudo-Euclidean space;
5. the set of nonsingular affine transformations of an affine space;
6. the set of projective transformations of a projective space;
7. the set of motions of an affine Euclidean space;
8. the set of motions of a hyperbolic space.

All the groups enumerated above are groups of transformations (the set M is obviously the underlying set of the given space). Let us note that in the case of vector and affine spaces, there is the crucial requirement of the nonsingularity of the linear or affine transformations that guarantees the bijectivity of each mapping and thus the existence of an inverse element for each element of the group.[2]

However, not all naturally occurring groups are groups of transformations. For example, with respect to the operation of addition, the set of all integers forms a group, as do the sets of the rational, real, and complex numbers, and likewise, the set of all vectors belonging to any arbitrary vector space.

Let us remark that the axioms of motion 1, 2, and 3 introduced in Sect. 12.2 can be expressed together as a single requirement, namely that the *motions form a group*.

Example 13.5 Let us consider a finite set M consisting of n elements. A transformation $f : M \to M$ is called a *permutation*, and the group of all permutations of the set M is called the *symmetric group of degree n* and is denoted by S_n. It is obvious that the group S_n is finite.

We considered permutations earlier, in Sect. 2.6, in connection with the notions of symmetric and antisymmetric functions, and we saw that for defining a permutation $f : M \to M$, one can introduce a numeration of the elements of the set M, that is, one can write the set in the form $M = \{a_1, \dots, a_n\}$ and designate the images $f(a_1), \dots, f(a_n)$ of all the elements $a_1, \dots, a_n$. Namely, let $f(a_1) = a_{j_1}, \dots, f(a_n) = a_{j_n}$. Then a permutation is defined by the matrix

$$A = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}, \tag{13.2}$$

where in the upper row are written in succession all the natural numbers from 1 to n, and in the lower row, under the number k stands the number j_k such that $f(a_k) = a_{j_k}$. Since a permutation $f : M \to M$ is a bijective mapping, it follows that the lower row contains all the numbers from 1 to n, except that they are written in some other order. In other words, $(j_1, \dots, j_n)$ is some permutation of the numbers $(1, \dots, n)$.

[2] Unfortunately, there is a certain amount of disagreement over terminology, of which the reader should be aware: above, we defined a transformation of a set as a *bijective mapping* into itself, while at the same time, a linear (or affine) transformation of a vector (or affine) space is not by definition necessarily bijective, and to have bijectivity here, it is necessary to specify that the transformations be nonsingular.

Writing a permutation in the form (13.2) allows us in particular to ascertain easily that $|S_n| = n!$. Let us prove this by induction on n. For $n = 1$, this is obvious: the group S_1 contains the single permutation that is the identity mapping on the set M consisting of a single element. Let $n > 1$. Then by enumerating the elements of the set M in every possible way, we obtain a bijection between S_n and the set of matrices A of the form (13.2), whose first row contains the elements $1, \dots, n$, and the elements $j_1, \dots, j_n$ of the second row take all possible values from 1 to n. Let A' be the matrix obtained from A by deleting its last column, containing the element j_n. Let us fix this element: $j_n = k$. Then the elements $j_1, \dots, j_{n-1}$ of the matrix A' assume all possible values from the collection of the $n - 1$ numbers $(1, \dots, \breve{k}, \dots, n)$, where the symbol $\breve{}$, as before, denotes the omission of the corresponding element. It is clear that the set of all possible matrices A' is in bijective correspondence with S_{n-1}, and by the induction hypothesis, the number of distinct matrices A' is equal to $|S_{n-1}| = (n-1)!$. But since the element $j_n = k$ can be equal to any natural number from 1 to n, the number of distinct matrices A is equal to $n(n-1)! = n!$. This gives us the equality $|S_n| = n!$.

Let us note that the numeration of the elements of the set M used for writing down permutations plays the same role as the introduction of coordinates (that is, a basis) in a vector space. Furthermore, the matrix (13.2) is analogous to the matrix of a linear transformation of a space, which is defined only after the choice of a basis and depends on that choice. However, for our further purposes, it will be more convenient to use concepts that are not connected with such a choice of numeration of elements.

We shall use the concept of transposition, which was introduced in Sect. 2.6 (p. 45). The definition given there can be formulated as follows. Let a and b be two distinct elements of the set M. Then a *transposition* is a permutation of the set M that interchanges the places of the elements a and b and leaves all other elements of the set M fixed. Denoting such a transposition by $\tau_{a,b}$, we can express this definition by the relationships

$$\tau_{a,b}(a) = b, \qquad \tau_{a,b}(b) = a, \qquad \tau_{a,b}(x) = x \tag{13.3}$$

for all $x \neq a$ and $x \neq b$.

In this notation, Theorem 2.23 from Sect. 2.6 can be formulated as follows: *every permutation g of a finite set is the product of a finite number of transpositions*, that is,

$$g = \tau_{a_1,b_1}\tau_{a_2,b_2}\cdots\tau_{a_k,b_k}. \tag{13.4}$$

As we saw in Sect. 2.6, in relationship (13.4), the number k and the choice of elements $a_1, b_1, \dots, a_k, b_k$ for the given permutation g are not uniquely defined. This means that for a given permutation g, the representation (13.4) is not unique. However, as was proved in Sect. 2.6 (Theorem 2.25), the parity of the number k of a permutation g is uniquely determined. Permutations for which the number k in the representation (13.4) is even are called *even*, and those for which the number k is odd are called *odd*.

Example 13.6 The collection of all even permutations of n elements forms a subgroup of the symmetric group S_n (it obviously satisfies conditions (a), (b), (c) in the definition of a subgroup). It is called the *alternating group of degree n* and is denoted by A_n.

Definition 13.7 Let g be an element of G. Then for every natural number n, the element $g^n = g \cdots g$ (n-fold product) is defined. For a negative integer m, the element g^m is equal to $(g^{-1})^{-m}$, and for zero, we have $g^0 = e$.

It is easily verified that for arbitrary integers m and n, we have the relationship

$$g^m g^n = g^{m+n}.$$

From this, it is clear that the collection of elements of the form g^n, where n runs over the set of integers, forms a subgroup. It is called the *cyclic* subgroup *generated by* the element g and is denoted by $\{g\}$.

There are two cases that can occur:

(a) All the elements g^n, as n runs through the set of integers, are distinct. In this case, we say that g is an element of *infinite order* in the group G.

(b) For some integers m and n, $m \neq n$, we have the equality $g^m = g^n$. Then, obviously, $g^{m-n} = e$. This means that there exists a natural number k (for instance $|m - n|$) such that $g^k = e$. In this case, we say that g is an element of *finite order* in the group G.

If g is an element of finite order, then the smallest natural number k such that $g^k = e$ is called the *order* of the element g. If for some integer n, we have $g^n = e$, then the number n is an integer multiple of the order k of the element g. Indeed, if such were not the case, then we could divide the number n by k with nonzero remainder: $n = qk + r$, where $0 < r < k$. From the equalities $g^n = e$ and $g^k = e$, we could conclude that $g^r = e$, in contradiction to the definition of the order k. If in the group G there exists an element g such that $G = \{g\}$, then the group G is called a *cyclic group*. It is obvious that if $G = \{g\}$ and the element g has finite order k, then $|G| = k$. Indeed, in this case, $e, g, g^2, \dots, g^{k-1}$ are all the distinct elements of the group G.

Now we shall move on to discuss mappings of groups (homomorphisms), which play a role in group theory analogous to that of linear transformations of vector spaces in linear algebra. Let G and G' be any two groups, and let $e \in G$ and $e' \in G'$ be their identity elements.

Definition 13.8 A mapping $f : G \to G'$ is called a *homomorphism* if for every pair of elements g_1 and g_2 of the group G, we have the relationship

$$f(g_1 g_2) = f(g_1) f(g_2), \tag{13.5}$$

where it is obviously implied that on the left- and right-hand sides of equality (13.5), the juxtaposition of elements indicates the multiplication operation in the respective group (on the left, in G; on the right, in G').

From equality (13.5), it is easy to derive the simplest properties of homomorphisms:

1. $f(e) = e'$;
2. $f(g^{-1}) = (f(g))^{-1}$ for every $g \in G$;
3. $f(g^n) = (f(g))^n$ for every $g \in G$ and every integer n.

For the proof of the first property, let us set $g_1 = g_2 = e$ in formula (13.5). Then taking into account the equality $e = ee$, which is obvious from the definition of the identity element, we obtain that

$$f(e) = f(ee) = f(e)f(e).$$

It remains only to multiply both sides of the relationship $f(e) = f(e)f(e)$ by the element $(f(e))^{-1}$ of the group G', after which we obtain the required equality $e' = f(e)$. The second property follows at once from the first: setting in (13.5) $g_1 = g$ and $g_2 = g^{-1}$, and taking into account the equality $e = gg^{-1}$, we obtain

$$e' = f(e) = f\bigl(gg^{-1}\bigr) = f(g)f\bigl(g^{-1}\bigr),$$

from which, by the definition of the inverse element, it follows that $f(g^{-1}) = (f(g))^{-1}$. Finally, the third property is obtained for positive n by induction from (13.5), and for negative n, it is also necessary to apply property 2.

Definition 13.9 A mapping $f : G \to G'$ is called an *isomorphism* if it is a homomorphism that is also a bijection. Groups G and G' are said to be *isomorphic* is there exists an isomorphism $f : G \to G'$. This is denoted as follows: $G \simeq G'$.

Example 13.10 Assigning to each nonsingular linear transformation of a vector space L of dimension n its matrix (in some fixed basis of the space L), we obtain an isomorphism between the group of nonsingular linear transformations of this space and the group of nonsingular square matrices of order n.

The notion of isomorphism plays the same role in group theory as the notion of isomorphism plays in the theory of vector spaces, and the notion of homomorphism plays the same role as the notion of arbitrary linear transformation (in vector spaces of arbitrary dimension). The analogy between these concepts is revealed particularly in the fact that the answer to the question whether a homomorphism $f : G \to G'$ is an isomorphism can be formulated in terms of its *image* and *kernel*, just as was the case for linear mappings.

The *image* of a homomorphism f is the set $f(G)$, that is, simply the image of f as a mapping of sets $G \to G'$. If follows from relationship (13.5) that $f(G)$ is a subgroup of G'. The *kernel* of a homomorphism f is the set of elements $g \in G$ such that $f(g) = e'$. It is likewise not difficult to conclude from (13.5) that the kernel is a subgroup of G.

Using the notions of image and kernel, we may say that a homomorphism $f : G \to G'$ is an isomorphism if and only if its image consists of the entire group

G' and its kernel consists of only the identity element $e \in G$. The proof of this assertion is based on relationship (13.5) and properties 1 and 2: if for two elements g_1 and g_2 of a group G, we have the equality $f(g_1) = f(g_2)$, then through right multiplying both sides by the element $(f(g_1))^{-1}$ of the group G', we obtain $e' = f(g_2)(f(g_1))^{-1} = f(g_2 g_1^{-1})$, from which it follows that $g_2 g_1^{-1} = e$, that is, $g_1 = g_2$.

It is important, however, to note that the analogy between isomorphisms of groups and isomorphisms of vector spaces does not extend all that far: most of the theorems from Chap. 3 do not have suitable analogues for groups, even for finite groups. For example, one of the most important results of Chap. 3 (Theorem 3.64) states that all vector spaces of a given finite dimension are isomorphic to one another. But there exist even finite groups of a given order that are not isomorphic; see Example 13.24 on p. 484.

Another property of groups is related to whether the product of elements in a group depends on the order in which they are multiplied. In the definition of a group, no condition of this sort was imposed, and therefore, we may assume that in general, $g_1 g_2 \neq g_2 g_1$. Very frequently, such is the case. For example, nonsingular square matrices of a given order n with the standard operation of matrix multiplication form a group, and as the example presented in Sect. 2.9 on p. 64 shows, already for $n = 2$, it is generally the case that $AB \neq BA$.

Definition 13.11 If in a group G the equality $g_1 g_2 = g_2 g_1$ holds for every pair of elements $g_1, g_2 \in G$, then G is called a *commutative group* or, more usually, an *abelian group*.[3]

For example, the groups of integers, rational numbers, real numbers, and complex numbers with the operation of addition are all abelian. Likewise, a vector space is an abelian group with respect to the operation of vector addition. It is easy to see that every cyclic group is abelian.

Let us present one result that holds for all finite groups but that is especially easy to prove (and we shall use it frequently in the sequel) for abelian groups.

Lemma 13.12 *For every finite abelian group G, the order of each of its elements divides the order of the group.*

Proof Let us denote by $g_1, g_2, \dots, g_n$ the complete set of elements of G (so we obviously have $n = |G|$), and let us right multiply each of them by some element $g \in G$. The elements thus obtained, $g_1 g, g_2 g, \dots, g_n g$, will again all be distinct. Indeed, given the equality $g_i g = g_j g$, right multiplying both sides by g^{-1} yields the equality $g_i = g_j$. Since the group G contains n elements altogether, it follows that the elements $g_1 g, g_2 g, \dots, g_n g$ are the same as the elements $g_1, g_2, \dots, g_n$, though perhaps arranged in some other order:

$$g_1 g = g_{i_1}, \qquad g_2 g = g_{i_2}, \qquad \dots, \qquad g_n g = g_{i_n}.$$

[3] Named in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829).

On multiplying these equalities, we obtain

$$(g_1g)(g_2g)\cdots(g_ng) = g_{i_1}g_{i_2}\cdots g_{i_n}. \tag{13.6}$$

Since the group G is abelian, we have

$$(g_1g)(g_2g)\cdots(g_ng) = g_1g_2\cdots g_ng^n,$$

and since $g_{i_1}, g_{i_2}, \dots, g_{i_n}$ are the same elements $g_1, g_2, \dots, g_n$, then setting $h = g_1g_2\cdots g_n$, we obtain from (13.6) the equality $hg^n = h$. Left multiplying both sides of the last equality by h^{-1}, we obtain $g^n = e$. As we saw above, it then follows that the order of the element g divides the number $n = |G|$. □

Definition 13.13 Let $H_1, H_2, \dots, H_r$ be subgroups of G. The group G is called the *direct product* of the subgroups $H_1, H_2, \dots, H_r$ if for all elements $h_i \in H_i$ and $h_j \in H_j$ from distinct subgroups, we have the relationship $h_ih_j = h_jh_i$, and every element $g \in G$ can be represented in the form

$$g = h_1h_2\cdots h_r, \quad h_i \in H_i, i = 1, 2, \dots, r,$$

and for each element $g \in G$, such a representation is unique. The fact that the group G is a direct product of subgroups $H_1, H_2, \dots, H_r$ is denoted by

$$G = H_1 \times H_2 \times \cdots \times H_r. \tag{13.7}$$

In the case of abelian groups, a different terminology is usually used, related to the majority of examples of interest. Namely, the operation defined on the group is called *addition* instead of multiplication, and it is denoted not by g_1g_2, but by $g_1 + g_2$. In keeping with this notation, the identity element is called the *zero element* and is denoted by 0, and not by e. The inverse element is called the *negative* or *additive inverse* and is denoted not by g^{-1}, but by $-g$, and the exponential notation g^n is replaced by the *multiplicative* notation ng, which is defined similarly: $ng = g + \cdots + g$ (n-fold sum) if $n > 0$, by $ng = (-g) + \cdots + (-g)$ (n-fold sum) if $n < 0$, and by $ng = 0$ if $n = 0$. The definition of homomorphism remains exactly the same in this case, where it is required only to replace in formula (13.5) the symbol for the group operation:

$$f(g_1 + g_2) = f(g_1) + f(g_2).$$

Properties 1–3 here take the following form:

1. $f(0) = 0'$;
2. $f(-g) = -f(g)$ for all $g \in G$;
3. $f(ng) = nf(g)$ for all $g \in G$ and for every integer n.

This terminology agrees with the example of the set of integers and, in the terminology we employed earlier, the example of vectors that form an abelian group with respect to the operation of addition.

In the case of abelian groups (with the operation of addition), instead of the direct product of subgroups $H_1, H_2, \dots, H_r$ one speaks of their *direct sum*. Then the definition of the direct sum reduces to the condition that every element $g \in G$ can be represented in the form

$$g = h_1 + h_2 + \cdots + h_r, \quad h_i \in H_i, i = 1, 2, \dots, r,$$

and that for each element $g \in G$, the representation is unique. It is obvious that this last requirement is equivalent to the requirement that the equality $h_1 + h_2 + \cdots + h_r = 0$ be possible only if $h_1 = 0$, $h_2 = 0, \dots, h_r = 0$. That a group G is the direct sum of subgroups $H_1, H_2, \dots, H_r$ is denoted by

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_r. \tag{13.8}$$

It is obvious that in both cases (13.7) and (13.8), the order of the group G is equal to

$$|G| = |H_1| \cdot |H_2| \cdots |H_r|.$$

In perfect analogy to how things were done in Sect. 3.1 for vector spaces, we may define the direct product (or direct sum) of groups that in general are not originally the subgroups of any particular group and that even, perhaps, are of completely different natures from one another.

Example 13.14 If we map every orthogonal transformation $\mathcal{U}$ of a Euclidean space to its determinant $|\mathcal{U}|$, which, as we know, is equal to $+1$ or -1, we obtain a homomorphism of the group of orthogonal transformations into the symmetric group S_2 of order 2. If we map every Lorentz transformation $\mathcal{U}$ of a pseudo-Euclidean space to the pair of numbers $\varepsilon(\mathcal{U}) = (|\mathcal{U}|, \nu(\mathcal{U}))$, defined in Sect. 7.8, we obtain a homomorphism of the group of Lorentz transformations into the group $S_2 \times S_2$.

Example 13.15 Let (V, L) be an affine Euclidean space of dimension n and G the group of its motions. Then the assertion of Theorem 8.37 can be formulated as the equality $G = T_n \times O_n$, where T_n is the group of translations of the space V, and O_n is the group of orthogonal transformations of the space L. Let us note that $T_n \simeq \mathsf{L}$, where L is understood as a group under the operation of vector addition. Indeed, let us define the mapping $f : T_n \to \mathsf{L}$ that to each translation $\mathcal{T}_{\boldsymbol{a}}$ by the vector $\boldsymbol{a}$ assigns this vector $\boldsymbol{a}$. Obviously, the mapping f is bijective, and by virtue of the property $\mathcal{T}_{\boldsymbol{a}}\mathcal{T}_{\boldsymbol{b}} = \mathcal{T}_{\boldsymbol{a}+\boldsymbol{b}}$, it is an isomorphism. Thus Theorem 8.37 can be formulated as the relationship $G \simeq \mathsf{L} \times O_n$.

13.2 Decomposition of Finite Abelian Groups

Later in this chapter we shall restrict our attention to the study of finite groups. The highest goal in this area of group theory is to find a construction that gives a description of all finite groups. But such a goal is far from accessible; at least at present, we are far from attaining it. However, for finite *abelian* groups, the answer to this question turns out to be unexpectedly simple. Moreover, both the answer and its proof are very similar to Theorem 5.12 on the decomposition of a vector space as a direct sum of cyclic subspaces. For the proof, we shall require the following lemmas.

Lemma 13.16 *Let B be a subgroup of A, and a an element of the group A of order k. If there exists a number $m \in \mathbb{N}$ relatively prime to k such that $ma \in B$, then a is an element of B.*

Proof Since the numbers m and k are relatively prime, there exist integers r and s such that $kr + ms = 1$. Multiplying ma by s and adding kra to the result (which is equal to zero, since k is the order of the element a), we obtain a. But $sma = s(ma)$ belongs to the subgroup B. From this, it follows that a is also an element of B. □

Lemma 13.17 *If $A = \{a\}$ is a cyclic group of order n, and we set $b = ma$, where $m \in \mathbb{N}$ is relatively prime to n, then the cyclic subgroup $B = \{b\}$ generated by the element b coincides with A.*

Proof Since $a \in A$, we have by Lemma 13.12 that the order k of the element a divides the order of the group A, which is equal to n, and the relative primality of the numbers m and n implies the relative primality of the numbers k and m. From Lemma 13.16, it follows that $a \in B$, which means that $A \subset B$, and since we obviously have also $B \subset A$, we obtain the required equality $B = A$. □

Corollary 13.18 *Under the assumptions of Lemma 13.17, every element $c \in A$ can be expressed in the form*

$$c = md, \quad d \in A, m \in \mathbb{Z}. \tag{13.9}$$

Indeed, if in the notation of Lemma 13.17, the group A is the group $\{b\}$, then the element c has the form kb, and since $b = ma$, we obtain equality (13.9) in which $d = ka$.

Definition 13.19 A subgroup B of a group A is said to be *maximal* if $B \neq A$ and B is contained in no subgroup other than A.

It is obvious that there exist maximal subgroups in every finite group that consists of more than just a single element. Indeed, beginning with the identity subgroup (that is, the subgroup consisting of a single element), we can include it, if it is not itself maximal, in some subgroup B_1 different from A. If in B_1 we have not yet obtained a maximal subgroup, then we can include it in some subgroup B_2 different from A. Continuing this process, we eventually can go no further, since all the subgroups $B_1, B_2, \dots$ are contained in the finite group A. The last subgroup obtained when we stop the process will be maximal. We remark that we do not assert (nor is it true) that the maximal subgroup we have constructed is unique.

Lemma 13.20 *For every maximal subgroup B of a finite abelian group A, there exists an element $a \in A$ not belonging to B such that the smallest number $m \in \mathbb{N}$ for which ma belongs to B is prime, and every element $x \in A$ can be represented in the form*

$$x = ka + b, \tag{13.10}$$

for k an integer, $b \in B$.

Later, we shall denote the prime number m that appears in Lemma 13.20 by p.

Proof of Lemma 13.20 Let us take as a any element of the group A not belonging to the subgroup B. The collection of all elements of the form $ka + b$, where k is an arbitrary integer and b an arbitrary element of B, obviously forms a subgroup containing B (it is easy to see that B consists of elements x such that in the representation $x = ka + b$, the number k is equal to 0). It is obvious that this subgroup does not coincide with B, since it contains the element a (for $k = 1$ and $b = 0$), and this means, in view of the maximality of the subgroup B, that it coincides with A. From this follows the representation (13.10) for every element x in the group A.

It remains to prove that for some prime number p, the element pa belongs to B. Since the element a is of finite order, we must have $na = 0$ for some $n > 0$. In particular, $na \in B$. Let us take the smallest $m \in \mathbb{N}$ for which $ma \in B$ and prove that it is prime.

Suppose that such is not the case, and that p is a prime divisor of m. Then $m = pm_1$ for some integer $m_1 < m$. Let us set $a_1 = m_1 a$. As we have seen, the collection of all elements of the form $ka_1 + b$ (for arbitrary integer k and $b \in B$) forms a subgroup of the group A containing B. If the element a_1 were contained in B, then that would contradict the choice of m as the *smallest* natural number such that $ma \in B$. This means that $a_1 \notin B$, and in view of the maximality of the subgroup B, the subgroup that we constructed of elements of the form $ka_1 + b$ coincides with A. In particular, it contains the element a, that is, $a = ka_1 + b$ for some k and b. From this, it follows that $pa = kpa_1 + pb$. But $pa_1 = pm_1 a = ma \in B$, and since $pb \in B$, this means that $pa \in B$, which contradicts the minimality of m. This means that the assumption that m has prime divisors less than m is false, and so $m = p$ is a prime number. □

Remark 13.21 We chose as a an arbitrary element of the group A not contained in B. In particular, in place of a, we could as well choose any element $a' = a + b$, where $b \in B$. Indeed, from $a = a' - b$ and $a' \in B$ it would follow that we would also have $a \in B$.

We can now state the fundamental theorem of abelian groups.

Theorem 13.22 *Every finite abelian group is the direct sum of cyclic subgroups whose orders are equal to powers of prime numbers.*

Thus, the theorem asserts that every finite abelian group A has the decomposition

$$A = A_1 \oplus \cdots \oplus A_r, \tag{13.11}$$

where the subgroups A_i are cyclic, that is, $A_i = \{a_i\}$, and their orders are powers of prime numbers, that is, $|A_i| = p_i^{m_i}$, where p_i are prime numbers.

Proof of Theorem 13.22 Our proof is by induction on the order of the group A. For the group of order 1, the theorem is obvious. Therefore, to prove the theorem for a group A, we may assume that it has been proved for all subgroups $B \subset A$, $B \neq A$, since for an arbitrary subset $B \subset A$ with $B \neq A$, the number of elements of B is less than $|A|$.

In particular, let B be a maximal subgroup of the group A. By the induction hypothesis, the theorem is valid for this subgroup, and it therefore has the decomposition

$$B = C_1 \oplus \cdots \oplus C_r, \tag{13.12}$$

in which the C_i are cyclic subgroups each of which has order the power of a prime number:

$$C_i = \{c_i\}, \qquad p_i^{m_i} c_i = 0.$$

Lemma 13.20 holds for the subgroup B; let $a \in A$, $a \notin B$, be the element provided for in the formulation of this lemma. By hypothesis, every element $x \in B$ can be represented in the form

$$x = k_1 c_1 + \cdots + k_r c_r.$$

In particular, this holds for the element $b = pa$ (in the notation of Lemma 13.20):

$$pa = k_1 c_1 + \cdots + k_r c_r.$$

Let us select the terms $k_i c_i$ in this decomposition that can be written in the form pd_i, where $d_i \in C_i$. These are first of all, the terms $k_i c_i$ for i such that $p_i \neq p$. This follows from Corollary 13.18. Moreover, all elements of the form $k_i c_i$ possess this property if $p_i = p$ and k_i is divisible by p. Let the chosen elements be $k_i c_i$, $i = 1, \ldots, s-1$. Then for the remaining elements $k_i c_i$, $i = s, \ldots, r$, we have $p_i = p$ and k_i is not divisible by p. Setting

$$k_i c_i = pd_i, \quad d_i \in C_i, i = 1, \ldots, s-1, \quad d_1 + \cdots + d_{s-1} = d, \tag{13.13}$$

we obtain

$$pa = pd + k_s c_s + \cdots + k_r c_r.$$

We can now use the freedom in the choice of the element $a \in A$, which was mentioned in Remark 13.21, and take instead of a, the element $a' = a - d$, since $d \in B$ in view of formula (13.13). We then have

$$pa' = k_s c_s + \cdots + k_r c_r. \tag{13.14}$$

There are now two possible cases.

Case 1. The number $s - 1$ is equal to r, and then equality (13.14) gives

$$pa' = 0.$$

In this case, the group A decomposes as a direct sum of cyclic subgroups as follows:

$$A = C_1 \oplus \cdots \oplus C_r \oplus C_{r+1},$$

where $C_{r+1} = \{a'\}$ is a subgroup of order p.

Indeed, Lemma 13.20 asserts that every element $x \in A$ can be represented in the form $ka' + b$, and since in view of (13.12), the element b can be represented in the form

$$b = k_1 c_1 + \cdots + k_r c_r,$$

it follows that x has the form

$$x = k_1 c_1 + \cdots + k_r c_r + ka'. \tag{13.15}$$

This proves the first condition in the definition of a direct sum.

Let us prove the uniqueness of representation (13.15). For this, it suffices to prove that the equality

$$k_1 c_1 + \cdots + k_r c_r + ka' = 0 \tag{13.16}$$

is possible only for $k_1 c_1 = \cdots = k_r c_r = ka' = 0$. Let us rewrite (13.16) in the form

$$ka' = -k_1 c_1 - \cdots - k_r c_r. \tag{13.17}$$

This means that the element ka' belongs to B. If the number k were not divisible by p, then k and p would be relatively prime, since the element a' has order p, and by Lemma 13.16, we would then obtain that $a' \in B$. But this contradicts the choice of the element a and the construction of the element a'. This means that p must divide k, and since $pa' = 0$, it follows that we also have $ka' = 0$. Thus equality (13.17) is reduced to $k_1 c_1 + \cdots + k_r c_r = 0$, and from the fact that the group B is the direct sum of subgroups $C_1, \ldots, C_r$, we obtain that $k_1 c_1 = 0, \ldots, k_r c_r = 0$.

Case 2. The number $s - 1$ is less than r. Let us set $k_s c_s = d_s, \ldots, k_r c_r = d_r$, and for $i = 1, \ldots, s - 1$, let us set $c_i = d_i$. By Lemma 13.17, the element d_i generates the same cyclic subgroup C_i as c_i. For $i \le s - 1$, this assertion is a tautology, and for $i > s - 1$, it follows from the fact that the numbers k_i are by assumption not divisible by p, and $p^{m_i}c_i = 0$ for all $i \geq s$. Equality (13.14) can then be rewritten as follows:

$$pa' = d_s + \cdots + d_r. \tag{13.18}$$

Let $m_s \leq \cdots \leq m_r$. Let us denote by C'_r the cyclic group generated by the element a', that is, let us set $C'_r = \{a'\}$. Let us prove that the order of the element a', and therefore the order of the group C'_r, is equal to p^{m_r+1}:

$$\left|C'_r\right| = p^{m_r+1}. \tag{13.19}$$

Indeed, in view of (13.18), we have

$$p^{m_r+1}a' = p^{m_r}d_s + \cdots + p^{m_r}d_r = 0,$$

since $p^{m_i}d_i = 0$, $m_i \leq m_r$. On the other hand, in view of relationship (13.18), we have

$$p^{m_r}a' = p^{m_r-1}d_s + \cdots + p^{m_r-1}d_r \neq 0,$$

since $p^{m_r-1}d_r \neq 0$, and in view of (13.12), the sum of the elements $p^{m_r-1}d_i \in C_i$ cannot equal 0 if at least one term is not equal to 0. This proves (13.19).

Now let us prove that

$$A = C_1 \oplus \cdots \oplus C_{r-1} \oplus C'_r, \tag{13.20}$$

that is, that every element $x \in A$ can be uniquely represented in the form

$$x = y_1 + \cdots + y_{r-1} + y'_r, \quad y_1 \in C_1, \ldots, y_{r-1} \in C_{r-1}, y'_r \in C'_r. \tag{13.21}$$

First let us prove the possibility of representation (13.21). Since every element $x \in A$ can be represented in the form $ka' + b$, $b \in B$, it suffices to prove that it is possible to represent separately a' and an arbitrary element $b \in B$ in the form (13.21). This is obvious for an element a', since it belongs to the cyclic group $C'_r = \{a'\}$. As for elements of B, each $b \in B$ can be represented in the form

$$b = k_1d_1 + \cdots + k_rd_r,$$

according to formula (13.12) and in view of the fact that $C_i = \{d_i\}$. Therefore, it suffices to prove that each of the elements d_i can be represented in the form (13.21). For $d_1, \ldots, d_{r-1}$, this is obvious, since

$$d_i \in C_i = \{d_i\}, \quad i = 1, \ldots, r-1.$$

Finally, in view of (13.18), we have

$$d_r = -d_s - \cdots - d_{r-1} + pa',$$

and this is the representation of the element d_r that we need.

Let us now prove the uniqueness of representation (13.21). For this, it suffices to prove that the equality

$$k_1d_1 + \cdots + k_{r-1}d_{r-1} + k_ra' = 0 \tag{13.22}$$

is possible only for $k_1d_1 = \cdots = k_ra' = 0$. Let us suppose that k_r is relatively prime to p. Then

$$k_ra' = -k_1d_1 - \cdots - k_{r-1}d_{r-1},$$

and in view of the fact that $p^{m_r+1}a' = 0$, we obtain by Lemma 13.16 that $a' \in B$. But the element $a \in A$ was chosen as an element not belonging to the subgroup B. This means that the element a' also does not belong to B.

Let us now consider the case in which the number k_r is divisible by p. Let $k_r = pl$. Then

$$pla' = -k_1d_1 - \cdots - k_{r-1}d_{r-1}.$$

Let us replace pa' on the left-hand side of this relationship by the expression $d_s + \cdots + d_r$ on the basis of equality (13.18). On transferring all terms to the left-hand side, we obtain

$$ld_s + \cdots + ld_r + k_1d_1 + \cdots + k_{r-1}d_{r-1} = 0.$$

From the fact that by hypothesis, the group B is the direct sum of groups $C_1, \dots, C_r$, it follows that in this equality, $ld_r = 0$. Since the order of the element d_r is equal to p^{m_r}, this is possible only if p^{m_r} divides l, and this means that p^{m_r+1} divides k_r. But we have seen that the order of the element a' is equal to p^{m_r+1}, and this means that $k_ra' = 0$. Then it follows from equality (13.22) that $k_1d_1 + \cdots + k_{r-1}d_{r-1} = 0$. And since by the induction hypothesis, the group B is the direct sum of the groups $C_1, \dots, C_r$, it follows that $k_1d_1 = \cdots = k_{r-1}d_{r-1} = 0$. This completes the proof of the theorem. □

13.3 The Uniqueness of the Decomposition

The theorem on the uniqueness of the Jordan normal form has an analogue in the theory of finite abelian groups.

Theorem 13.23 *For different decompositions of the finite abelian group A into a direct sum of cyclic subgroups whose orders are prime powers, whose existence is established in Theorem 13.22,*

$$A = A_1 \oplus \cdots \oplus A_r, \quad |A_i| = p_i^{m_i}, \tag{13.23}$$

the orders $p_i^{m_i}$ of the cyclic subgroups A_i are unique. In other words, if

$$A = A'_1 \oplus \cdots \oplus A'_s$$

is another such decomposition, then $s = r$, and the subgroups A'_i can be reordered in such a way that the equality $|A'_i| = |A_i|$ is satisfied for all $i = 1, \dots, r$.

Proof We shall show how the orders of the cyclic subgroups in the decomposition (13.23) are uniquely determined by the group A itself. For any natural number k, let us denote by kA the collection of elements a of the group A that can be represented in the form $a = kb$, where b is some element of this group. It is obvious that the collection of elements kA forms a subgroup of the group A. Let us prove that the orders $|kA|$ of these subgroups (for various k) determine the orders of the cyclic groups $|A_i|$ in the decomposition (13.23).

Let us consider an arbitrary prime number p and analyze the case that k is a power of a prime number p, that is, $k = p^i$. Let us factor the order $|p^i A|$ of the group $p^i A$ into a product of a power of p and numbers n_i relatively prime to p:

$$\left|p^i A\right| = p^{r_i} n_i, \quad (n_i, p) = 1. \tag{13.24}$$

On the other hand, for a prime number p, let us denote by l_i the number of subgroups A_i of order p^i appearing in the decomposition (13.23). We shall present an explicit formula that expresses the numbers l_i in terms of r_i. Since these latter numbers are determined only by the group A, it follows that the numbers l_i also do not depend on the decomposition (13.23) (in particular, they are equal to zero if and only if all prime numbers p_i for which $|A_i| = p_i^{m_i}$ differ from p).

First of all, let us calculate the order of the group A in another way. Let us note that $A = p^0 A$, so that this is the case $i = 0$. The definition of the number l_i shows that in the decomposition (13.23), we have l_1 groups of order p, l_2 groups of order $p^2, \dots,$ and the remaining groups have orders relatively prime to p. Hence it follows that

$$|A| = p^{l_1} p^{2l_2} \cdots n_0, \quad (n_0, p) = 1.$$

Let us set

$$|A| = p^{r_0} n_0, \quad (n_0, p) = 1.$$

Then we can write the relationship above in the form

$$l_1 + 2l_2 + 3l_3 + \cdots = r_0. \tag{13.25}$$

Now let us consider the case that $k = p^i > 1$, that is, the number i is greater than 0. First of all, it is obvious that for every natural number k, it follows from (13.23) that

$$kA = kA_1 \oplus kA_2 \oplus \cdots \oplus kA_r.$$

It is obvious that all properties of a direct sum are satisfied.

Now, as in the case examined above, let us calculate the order of the group $p^i A$ in another way. It is obvious that $|p^i A| = |p^i A_1| \cdots |p^i A_r|$. If for some j, we have $|A_j| = p_j^{m_j}$ and $p_j \neq p$, then Lemma 13.17 shows that $p^i A_j = A_j$, and we have

$|p^i A_j| = |A_j| = p_j^{m_j}$, which is relatively prime to p. Thus in the decomposition $|p^i A| = |p^i A_1| \cdots |p^i A_r|$, all the factors $|p^i A_j|$, where $|A_j| = p_j^{m_j}$ and $p_j \neq p$, together give a number that is relatively prime to p, and in formula (13.24), they make no contribution to the number r_i. It remains to consider the case $p_j = p$. Since A_j is a cyclic group, it follows that $A_j = \{a_j\}$. It is then clear that $p^i A_j = \{p^i a_j\}$. Let us find the order of the element $p^i a_j$. Since $p^{m_j} a_j = 0$, we have $p^{m_j - i}(p^i a_j) = 0$ if $i \le m_j$, and $p^i a_j = 0$ if $i = m_j$.

Let us prove that $p^{m_j - i}$ is precisely the same as the order of the element $p^i a_j$. Let this order be equal to some number s. Then s must divide $p^{m_j - i}$, which means that it is of the form p^t. If $t < m_j - i$, then the equality $p^t(p^i a_j) = 0$ would show that $p^{t+i} a_j = 0$, that is, that the element a_j had order less than p^{m_j}. This means that $|p^i A_j| = p^{m_j - i}$ for $i \le m_j$. The fact that $p^i A_j = 0$ for $i \ge m_j$ (which means that $|p^i A_j| = 1$) is obvious.

We can now literally repeat the argument that we used earlier. We see that in the decomposition

$$p^i A = p^i A_1 \oplus p^i A_2 \oplus \cdots \oplus p^i A_r,$$

subgroups of order p occur when $m_j - i = 1$, that is, $m_j = i + 1$, and this means that in our adopted notation, they occur l_{i+1} times. Likewise, the subgroups of order p^2 occur when $m_j = i + 2$, that is, l_{i+2} times, and so on. Moreover, certain subgroups will have order relatively prime to p. This means that

$$\left|p^i A\right| = p^{l_{i+1}} p^{2l_{i+2}} \cdots n_i, \quad \text{where } (n_i, p) = 1.$$

In other words, in accordance with our previous notation, we have

$$l_{i+1} + 2l_{i+2} + \cdots = r_i. \tag{13.26}$$

In particular, formula (13.25) is obtained from (13.26) for $i = 0$.

If we now subtract from each formula (13.26) the following one, we obtain that for all $i = 1, 2, \ldots$, we have the equalities

$$l_i + l_{i+1} + \cdots = r_{i-1} - r_i.$$

Repeating the same process, we obtain

$$l_i = r_{i-1} - 2r_i + r_{i+1}.$$

These relationships prove Theorem 13.23. □

Theorems 13.22 and 13.23 make it easy to give the number of distinct (up to isomorphism) finite abelian groups of a given order.

Example 13.24 Suppose, for example, that we would like to determine the number of distinct abelian groups of order $p^3 q^2$, where p and q are distinct prime numbers. Theorem 13.22 shows that such a group can be represented in the form

$$A = C_1 \oplus \cdots \oplus C_s,$$

where C_i are cyclic groups whose orders are prime powers. From this decomposition, it follows that

$$|A| = |C_1| \cdots |C_s|.$$

In other words, among the groups C_i, there is either one cyclic group of order p^3, or one of order p^2 and one of order p, or three of order p. And likewise, there is one of order q^2 or two of order q. Combining all these possibilities (three for groups of order p^i and two for groups of order q^j), we obtain six variants. Theorem 13.23 guarantees that of the six groups thus obtained, none is isomorphic to any of the others.

13.4 Finitely Generated Torsion Modules over a Euclidean Ring*

The proofs of the theorem on finite abelian groups and the theorem on Jordan normal form (just like the proofs of the corresponding uniqueness theorems) are so obviously parallel to each other that they surely are special cases of some more general theorems. This is indeed the case, and the main goal of this chapter is the proof of these general theorems. For this, we shall need two abstract (that is, defined axiomatically) notions.

Definition 13.25 A *ring* is a set R on which are defined two operations (that is, two mappings $R \times R \to R$), one of which is called *addition* (for which an element that is the image of two elements $a \in R$ and $b \in R$ is called their *sum* and is denoted by $a + b$), and the second of which is *multiplication* (the element that is the image of $a \in R$ and $b \in R$ is called their *product* and is denoted by ab). For these operations of addition and multiplication, the following conditions must be satisfied:

(1) With respect to the operation of addition, the ring is an abelian group (the identity element is denoted by 0).

(2) For all $a, b, c \in R$, we have

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

(3) For all $a, b, c \in R$, the associative property holds:

$$a(bc) = (ab)c.$$

In the sequel, we shall denote a ring by the letter R and assume that it has a multiplicative identity, that is, that it contains an element, which we shall denote by 1, satisfying the condition

$$a \cdot 1 = 1 \cdot a = a \quad \text{for all } a \in R.$$

In this chapter, we shall be considering only *commutative* rings, that is, it will be assumed that

$$ab = ba \quad \text{for all } a, b \in R.$$

We have already encountered the most important special case of a ring, namely an algebra, in connection with the construction of the exterior algebra of a vector space, in Chap. 10. Let us recall that an algebra is a ring that is a vector space, where, of course, consistency of the notions entering into these definitions is assumed. This means that for every scalar α (in the field over which the vector space in question is defined) and for all elements a, b of the ring R, we have the equality $(\alpha a)b = \alpha(ab)$. On the other hand, we are quite familiar with an example of a ring that is not an algebra in any natural sense, namely the ring of integers $\mathbb{Z}$ with the usual arithmetic operations of addition and multiplication.

Let us note a connection among the concepts we have introduced. If all nonzero elements of a commutative ring form a group with respect to the operation of multiplication, then such a ring is called a *field*. We assume that the reader is familiar with the simplest properties of fields and rings.

The concept that generalizes both the concept of vector space (over some field $\mathbb{K}$) with a linear transformation given on it and that of an abelian group is that of a *module*.

Definition 13.26 An abelian group M (its operation is written as addition) is a *module M* over a ring R if there is defined an additional operation of multiplication of the elements of the ring R by elements of the module M that produces elements of the module that have the following properties:

$$a(\boldsymbol{m}+\boldsymbol{n}) = a\boldsymbol{m} + a\boldsymbol{n},$$

$$(a+b)\boldsymbol{m} = a\boldsymbol{m} + b\boldsymbol{m},$$

$$(ab)\boldsymbol{m} = a(b\boldsymbol{m}),$$

$$1\boldsymbol{m} = \boldsymbol{m},$$

for all elements $a, b \in R$ and all elements $\boldsymbol{m}, \boldsymbol{n} \in M$.

For convenience, we shall denote the elements of the ring using ordinary letters $a, b, \dots$, and elements of the module using boldface letters: $\boldsymbol{m}, \boldsymbol{n}, \dots$.

Example 13.27 An example of a module that we have encountered repeatedly is that of a vector space over an arbitrary field $\mathbb{K}$ (here the ring R is the field $\mathbb{K}$). On the other hand, every abelian group G is a module over the ring of integers $\mathbb{Z}$: the operation defined on it of integral multiplication $k\boldsymbol{g}$ for $k \in \mathbb{Z}$ and $\boldsymbol{g} \in G$ obviously possesses all the required properties.

Example 13.28 Let L be a vector space (real, complex, or over an arbitrary field $\mathbb{K}$) and let $\mathcal{A} : \mathsf{L} \to \mathsf{L}$ be a fixed linear transformation. Then we may consider L as a module over the ring R of polynomials in the single variable x (real, complex, or over a field $\mathbb{K}$), assuming, as we did earlier, for a polynomial $f(x) \in R$ and vector $\boldsymbol{e} \in \mathsf{L}$,

$$f(x)\boldsymbol{e} = f(\mathcal{A})(\boldsymbol{e}). \tag{13.27}$$

It is easily verified that all the properties appearing in the definition of a module are satisfied.

Our immediate objective will be to find a restriction of the general notion of module that covers vector spaces and abelian groups and then to prove theorems for these that generalize Theorems 5.12 and 13.22.

These two examples—the ring of integers $\mathbb{Z}$ and the ring of polynomials in a single complex variable (for simplicity, we shall restrict our attention to the special case $\mathbb{K} = \mathbb{C}$, but many results are valid in the general case)—have many similar properties, the most important of which is the uniqueness of the decomposition into irreducible factors, that is, prime numbers in the case of the ring of integers, and linear polynomials in the case of the ring of polynomials with complex coefficients. Both of these properties, in turn, derive from a single property: the possibility of division with remainder, which we shall introduce in the definition of certain rings for which it is possible to generalize the reasoning from previous sections.

Definition 13.29 A ring R is called a *Euclidean ring* if

$$ab \neq 0 \quad \text{for all } a, b \in R, a \neq 0 \text{ and } b \neq 0,$$

and for nonzero elements a of the ring, a function $\varphi(a)$ is defined taking nonnegative integer values and exhibiting the following properties:

(1) $\varphi(ab) \geq \varphi(a)$ for all elements $a, b \in R$, $a \neq 0$, $b \neq 0$.
(2) For all elements $a, b \in R$, where $a \neq 0$, there exist $q, r \in R$ such that

$$b = aq + r \tag{13.28}$$

and either $r = 0$ or $\varphi(r) < \varphi(a)$.

For the ring of integers, these properties are satisfied for $\varphi(a) = |a|$, while for the ring of polynomials, they are satisfied for $\varphi(a)$ equal to the degree of the polynomial a.

Definition 13.30 An element a of a ring R is called a *unit* or *reversible element* if there exists an element $b \in R$ such that $ab = 1$. An element b is called a *divisor* of the element a (one also says that *a is divisible by b* or that *b divides a*) if there exists an element c such that $a = bc$.

Clearly the property of divisibility is unchanged under multiplication of a or b by a unit. Two elements that differ by a unit are called *associates*. For example, in the ring of integers, the units are $+1$ and -1, and associates are integers that are either equal or differ by a sign. In the ring of polynomials, the units are the constant polynomials other than the one that is identically zero, and associates are polynomials that differ from each other by a constant nonzero multiple.

An element p of a ring is *prime* if it is not a unit and has no divisors other than its associates and units.

The theory of decomposition into prime factors in a Euclidean ring repeats exactly what is known for the ring of integers.

If an element a is not prime, then it has a divisor b such that $a = bc$, with c not a unit. This means that a is not a divisor of b, and there exists the representation $b = aq + r$ with $\varphi(r) < \varphi(a)$. But $r = b - aq = b(1 - cq)$, and therefore $\varphi(r) \geq \varphi(b)$, that is, $\varphi(b) \leq \varphi(r) < \varphi(a)$, which means that $\varphi(b) < \varphi(a)$. Applying the same reasoning to b, we finally arrive at a prime divisor a, and we shall show that every element can be represented as the product of primes. The same argument as used in the case of integers or polynomials shows the uniqueness of this decomposition in the following precise sense.

Theorem 13.31 *If some element a in a Euclidean ring R has two factorizations into prime factors,*

$$a = p_1 \cdots p_r, \qquad a = q_1 \cdots q_s,$$

then $r = s$, and with a suitable numeration of the factors, p_i and q_i are associates for all i.

As in the ring of integers, in every Euclidean ring, each element $a \neq 0$ that is not a unit can be written in the form

$$a = u p_1^{n_1} \cdots p_r^{n_r},$$

where u is a unit, all the p_i are prime elements with no two of them associates, and n_i are natural numbers. Such a representation is unique in a natural sense.

As in the ring of integers or of polynomials in one variable, representation (13.28) for $r \neq 0$ can be applied to elements b and r and repeated until we arrive at $r = 0$. We will thus obtain a *greatest common divisor* (gcd) of the elements a and b, that is, a common divisor such that every other common divisor is a divisor of it. The greatest common divisor of a and b is denoted by $d = (a, b)$ or $d = \gcd(a, b)$. This process, as it is for integers, is called the *Euclidean algorithm* (whence the name *Euclidean ring*). It follows from the Euclidean algorithm that a greatest common divisor of elements a and b can be written in the form $d = ax + by$, where x and y are some elements of the ring R.

Two elements a and b are said to be *relatively prime* if their only common divisors are units. Then we may consider that $\gcd(a, b) = 1$, and as follows from the Euclidean algorithm, there exist elements $x, y \in R$ such that

$$ax + by = 1. \tag{13.29}$$

Let us now recall that the theorem on Jordan normal form holds in the case of *finite-dimensional* vector spaces, and that the fundamental theorem of abelian groups holds for *finite* abelian groups. Let us now derive analogous finiteness conditions for modules.

Definition 13.32 A module M is said to be *finitely generated* if it contains a finite collection of elements $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$, called *generators*, such that every element $\boldsymbol{m} \in M$ can be expressed in the form

$$\boldsymbol{m} = a_1\boldsymbol{m}_1 + \cdots + a_r\boldsymbol{m}_r \tag{13.30}$$

for some elements $a_1, \dots, a_r$ of the ring R.

For a vector space considered as a module over a certain field, this is the definition of finite dimensionality, and representation (13.30) is a representation of a vector $\boldsymbol{m}$ in the form of a linear combination of vectors $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$ (let us note that the system of vectors $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$ will in general not be a basis, since we did not introduce the concept of linear independence). In the case of a finite abelian group, we may generally take for $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$, all the elements of the group.

Let us formulate one additional condition of the same type.

Definition 13.33 An element $\boldsymbol{m}$ of a module M over a ring R is said to be a *torsion element* if there exists an element $a_{\boldsymbol{m}} \neq 0$ of the ring R such that

$$a_{\boldsymbol{m}}\boldsymbol{m} = \boldsymbol{0},$$

where $\boldsymbol{0}$ is the null element of the module M, and the subscript in $a_{\boldsymbol{m}}$ is introduced to show that this element depends on $\boldsymbol{m}$. A module is called a *torsion module* if all of its elements are torsion elements.

In a finitely generated torsion module, there is an element $a \neq 0$ of the ring R such that $a\boldsymbol{m} = \boldsymbol{0}$ for all elements $\boldsymbol{m} \in M$. Indeed, it suffices to set $a = a_{\boldsymbol{m}_1} \cdots a_{\boldsymbol{m}_r}$ for the elements $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r$ in representation (13.30). If the ring R is Euclidean, then we can conclude that $a \neq 0$. For the case of a finite abelian group, we may take a to be the order of the group.

Example 13.34 Let M be a module determined by a vector space L of dimension n and by a linear transformation $\mathcal{A}$ according to formula (13.27). For an arbitrary vector $\boldsymbol{e} \in \mathsf{L}$, let us consider the vectors

$$\boldsymbol{e}, \qquad \mathcal{A}(\boldsymbol{e}), \qquad \dots, \qquad \mathcal{A}^n(\boldsymbol{e}).$$

Their number, $n + 1$, is greater than the dimension n of the space L, and therefore, these vectors are linearly dependent, which means that there exists a polynomial $f(x)$, not identically zero, such that $f(\mathcal{A})(\boldsymbol{e}) = \boldsymbol{0}$, that is, in our module M, the element $\boldsymbol{e}$ is a torsion element.

But if, as we did in Example 13.27, we view a vector space as a module over the field $\mathbb{R}$ or $\mathbb{C}$, then not a single nonnull vector will be a torsion element of the module.

Let M be a module over a ring R. A subgroup M' of the group M is called a *submodule* if for all elements $a \in R$ and $\boldsymbol{m}' \in M'$, we have $a\boldsymbol{m}' \in M'$.

Example 13.35 It is obvious that every subgroup of an abelian group viewed as a module over the ring of integers is a submodule. Analogously, for a vector space viewed as a module over a ring coinciding with a suitable field, every subspace is a submodule. If M is a module defined by a vector space L and a linear transformation $\mathcal{A}$ of L according to formula (13.27), then as is easily verified, every submodule of M is a vector subspace that is invariant with respect to the transformation $\mathcal{A}$.

If $M' \subset M$ is a submodule, and $\boldsymbol{m}$ is any element of the module M, then it is easily verified that the collection of all elements of the form $a\boldsymbol{m} + \boldsymbol{m}'$, where a is an arbitrary element of the ring R, and $\boldsymbol{m}'$ is an arbitrary element of the submodule M', is a submodule. We shall denote it by $(\boldsymbol{m}, M')$.

Since we are assuming that the ring R is Euclidean, it follows that for every torsion element $\boldsymbol{m} \in M$, there exists an element $a \in R$ that exhibits the property $a\boldsymbol{m} = \boldsymbol{0}$ and is such that $\varphi(a)$ is the smallest value among all elements with this property. Then every element c for which $c\boldsymbol{m} = \boldsymbol{0}$ is divisible by a. Indeed, if such were not the case, we would have the relationship

$$c = aq + r, \qquad \varphi(r) < \varphi(a),$$

and clearly $r\boldsymbol{m} = \boldsymbol{0}$, which contradicts the definition of a. In particular, two such elements a and a' divide each other; that is, they are associates. The element $a \in R$ is called the *order* of the element $\boldsymbol{m} \in M$. One must keep in mind that this expression is not quite precise, since order is defined only up to associates.

Example 13.36 If, as in Example 13.28, a module is a vector space L viewed as a module over the polynomial ring $f(x)$ with the aid of formula (13.27), then every element $\boldsymbol{e} \in \mathsf{L}$ is a torsion element, and its order is the same as the minimal polynomial of the vector $\boldsymbol{e}$ (see the definition on p. 146), and the indicated property (every element c for which $cm = 0$ is divisible by the order of the element m) coincides with Theorem 4.23.

Definition 13.37 A submodule M' of a module M is said to be *cyclic* if it contains an element $\boldsymbol{m}'$ such that all the elements of the module M' can be represented in the form $a\boldsymbol{m}'$ with some $a \in R$. This is written $M' = \{\boldsymbol{m}'\}$.

Definition 13.38 A module M is called the *direct sum* of its submodules $M_1, \dots, M_r$ if every element $\boldsymbol{m} \in M$ can be written as a sum

$$\boldsymbol{m} = \boldsymbol{m}_1 + \cdots + \boldsymbol{m}_r, \qquad \boldsymbol{m}_i \in M_i,$$

and such a representation is unique. It is obvious that to establish the uniqueness of this decomposition, it suffices to prove that if $\boldsymbol{m}_1 + \cdots + \boldsymbol{m}_r = \boldsymbol{0}$, $\boldsymbol{m}_i \in M_i$, then $\boldsymbol{m}_i = \boldsymbol{0}$ for all i. This can be written as the equality

$$M = M_1 \oplus \cdots \oplus M_r.$$

The fundamental theorem that we shall prove, which contains Theorem 5.12 on the Jordan normal form and Theorem 13.22 on finite abelian groups as special cases, is the following.

Theorem 13.39 *Every finitely generated torsion module M over a Euclidean ring R is the direct sum of cyclic submodules*

$$M = C_1 \oplus \cdots \oplus C_r, \quad C_i = \{\boldsymbol{m}_i\}, \tag{13.31}$$

such that the order of each element $\boldsymbol{m}_i$ is a power of a prime element of the ring R.

Example 13.40 If M is a finite abelian group viewed as a module over the ring of integers, then this theorem reduces directly to the fundamental theorem of finite abelian groups (Theorem 13.22).

Let the module M be determined by the finite-dimensional complex vector space L and the linear transformation $\mathcal{A}$ of L according to formula (13.27). Then the C_i are vector subspaces invariant with respect to $\mathcal{A}$, and in each of these, there exists a vector $\boldsymbol{m}_i$ such that all the remaining vectors can be written in the form $f(\mathcal{A})(\boldsymbol{m}_i)$. The prime elements in the ring of complex polynomials are the polynomials of the form $x - \lambda$. By assumption, for each vector $\boldsymbol{m}_i$, there exist some λ_i and a natural number n_i such that

$$(\mathcal{A} - \lambda_i \mathcal{E})^{n_i}(\boldsymbol{m}_i) = \boldsymbol{0}.$$

If we take the smallest possible value n_i, then as proved in Sect. 5.1, the vectors

$$\boldsymbol{m}_i, \qquad (\mathcal{A} - \lambda_i \mathcal{E})(\boldsymbol{m}_i), \qquad \ldots, \qquad (\mathcal{A} - \lambda_i \mathcal{E})^{n_i-1}(\boldsymbol{m}_i)$$

will form a basis of this subspace, that is, C_i is a cyclic subspace corresponding to the principal vector $\boldsymbol{m}_i$. We obtain the fundamental theorem on Jordan form (Theorem 5.12).

Let us recall that we proved Theorem 5.12 by induction on the dimension of the space. More precisely, for a linear transformation $\mathcal{A}$ on the space L, we constructed a subspace L' invariant with respect to $\mathcal{A}$ of dimension 1 less and proved the theorem for L on the assumption that it had been proved already for L'. In fact, this meant that we constructed a sequence of nested subspaces

$$\mathsf{L} = \mathsf{L}_0 \supset \mathsf{L}_1 \supset \mathsf{L}_2 \supset \cdots \supset \mathsf{L}_n \supset \mathsf{L}_{n+1} = (\boldsymbol{0}), \tag{13.32}$$

invariant with respect to $\mathcal{A}$ and such that $\dim \mathsf{L}_{i+1} = \dim \mathsf{L}_i - 1$. Then we reduced the proof of Theorem 5.12 for L to the proof of the theorem for L_1, then for L_2, and so on. Now our first goal will be to construct in every finitely generated torsion module a sequence of submodules analogous to the sequence of subspaces (13.32).

Lemma 13.41 *In every finitely generated torsion module M over a Euclidean ring R, there exists a sequence of submodules*

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_n \supset M_{n+1} = \{\boldsymbol{0}\} \tag{13.33}$$

such that $M_i \neq M_{i+1}$, $M_i = (\boldsymbol{m}_i, M_{i+1})$, *where* $\boldsymbol{m}_i$ *are elements of the module* M, *and for each of these, there exists a prime element* p_i *of the ring* R *such that* $p_i\boldsymbol{m}_i \in M_{i+1}$.

Proof By the definition of a finitely generated module, there exists a finite number of generators $\boldsymbol{m}_1, \dots, \boldsymbol{m}_r \in M$ such that the elements $a_1\boldsymbol{m}_1 + \cdots + a_r\boldsymbol{m}_r$ exhaust all the elements of the module M as $a_1, \dots, a_r$ run through all elements of the ring R. The collection of elements of the form $a_k\boldsymbol{m}_k + \cdots + a_r\boldsymbol{m}_r$, where $a_k, \dots, a_r$ are all possible elements of the ring R, obviously forms a submodule of the module M. Let us denote it by $\overline{M}_k$. It is obvious that $\overline{M}_k \supset \overline{M}_{k+1}$ and $\overline{M}_k = (\boldsymbol{m}_k, \overline{M}_{k+1})$. Without loss of generality, we may assume that $\boldsymbol{m}_k \notin \overline{M}_{k+1}$, since otherwise, the element $\boldsymbol{m}_k$ can be excluded from among the generators. The constructed chain of submodules $\overline{M}_k$ is still not the chain of submodules M_i that figures in Lemma 13.16. We obtain that chain from the chain of submodules $\overline{M}_k$ by putting several intermediate submodules between the modules $\overline{M}_k$ and $\overline{M}_{k+1}$.

Since $\boldsymbol{m}_k \in M$ is a torsion element, there exists an element $a \in R$ for which $a\boldsymbol{m}_k = \boldsymbol{0}$ and in particular, $a\boldsymbol{m}_k \in \overline{M}_{k+1}$. Let $\overline{a}$ be an element of the ring R for which $\overline{a}\boldsymbol{m}_k \in \overline{M}_{k+1}$ and $\varphi(\overline{a})$ assumes the smallest value among elements with this property. If the element $\overline{a}$ is prime, then we set $p_i = \overline{a}$, and then it is unnecessary to place a submodule between $\overline{M}_k$ and $\overline{M}_{k+1}$. But if $\overline{a}$ is not prime, then let p_1 be one of its prime divisors and $\overline{a} = p_1\overline{b}$. Let us set $\boldsymbol{m}_{k,1} = \overline{b}\boldsymbol{m}_k$ and $\overline{M}_{k,1} = (\boldsymbol{m}_{k,1}, \overline{M}_{k+1})$. Then clearly, $p_1\boldsymbol{m}_{k,1} \in \overline{M}_{k,1}$ and $\overline{b}\boldsymbol{m}_k \in \overline{M}_{k,1}$. As we have seen, $\varphi(\overline{b}) < \varphi(\overline{a})$ (strict inequality). Therefore, repeating this process a finite number of times, we will place a finite number of submodules (13.33) with the required properties between $\overline{M}_k$ and $\overline{M}_{k+1}$. □

Remark 13.42 It is possible to show that the length of every chain of the form (13.33) satisfying the conditions of Lemma 13.16 is the same number n. Moreover, every chain of submodules

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_m$$

in which $M_i \neq M_{i+1}$ has length $m \leq n$, and this holds with much milder restrictions on the ring R and module M than we have assumed in this chapter. What is of essence here is only that between any two neighboring submodules M_i and M_{i+1}, there does not exist an "intermediate" submodule M_i' different from M_i and M_{i+1} such that $M_i \supset M_i' \supset M_{i+1}$.

For example, let us consider an n-dimensional vector space L over a field $\mathbb{K}$ as a module over the ring $R = \mathbb{K}$. Let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_n$ be some basis. Then the subspaces $\mathsf{L}_i = \langle \boldsymbol{a}_i, \dots, \boldsymbol{a}_n \rangle$, $i = 1, \dots, n$, have the indicated property. Using this, we could give a definition of the dimension of a vector space without appealing to the notion of linear dependence. Thus the length n of all chains of the form (13.33) satisfying the conditions of Lemma 13.16 is the "correct" generalization of dimension of a space to finitely generated torsion modules.

The following lemma is analogous to the one we used in the proof of Theorems 5.12 and 13.22.

Lemma 13.43 *If the order of an element* $\boldsymbol{m}$ *of a module* M *is the power of a prime element*, $p^n\boldsymbol{m}=\boldsymbol{0}$, *and an element* $\boldsymbol{x}$ *of the cyclic submodule* $\{\boldsymbol{m}\}$ *is not divisible by* p (*that is, not representable in the form* $\boldsymbol{x}=p\boldsymbol{y}$, *where* $\boldsymbol{y}\in M$), *then* $\{\boldsymbol{m}\}=\{\boldsymbol{x}\}$.

Proof It is obvious that $\{\boldsymbol{x}\}\subset\{\boldsymbol{m}\}$. Thus it remains to show that $\{\boldsymbol{m}\}\subset\{\boldsymbol{x}\}$, and for this, it suffices to ascertain that $\boldsymbol{m}\in\{\boldsymbol{x}\}$. By assumption, $\boldsymbol{x}=a\boldsymbol{m}$, where a is some element of the ring R. If a is divisible by p, then clearly, $\boldsymbol{x}$ is also divisible by p. Indeed, if $a=pb$ with some $b\in R$, then from the equality $\boldsymbol{x}=a\boldsymbol{m}$, we obtain $\boldsymbol{x}=p\boldsymbol{y}$, where $\boldsymbol{y}=b\boldsymbol{m}$, contradicting the assumption that $\boldsymbol{x}$ is not divisible by p.

This means that a and p are relatively prime, and consequently, in view of the uniqueness of the decomposition into prime elements of the ring R, a is also relatively prime to p^n. Then on the basis of the Euclidean algorithm, we can find elements u and v in R such that $au+p^nv=1$. Multiplying both sides of this equality by $\boldsymbol{m}$, we obtain that $\boldsymbol{m}=u\boldsymbol{x}$, which means that $\boldsymbol{m}\in\{\boldsymbol{x}\}$. □

Lemma 13.44 *Let* M_1 *be a submodule of the module* M *over a Euclidean ring* R *such that* $M=(\boldsymbol{m},M_1)$ *and* $M\neq M_1$. *Then if for some* $a,p\in R$, *we have the inclusions* $a\boldsymbol{m}\in M_1$ *and* $p\boldsymbol{m}\in M_1$, *where the element* p *is prime*, *then* a *is divisible by* p.

Proof Let us assume that a is not divisible by p. Since the element p is prime, we have $(a,p)=1$, and from the Euclidean algorithm in the ring R, it follows that there exist two elements $u,v\in R$ for which $au+pv=1$. Multiplying both sides of this equality by $\boldsymbol{m}$, taking into account the inclusions $a\boldsymbol{m}\in M_1$ and $p\boldsymbol{m}\in M_1$, we obtain that $\boldsymbol{m}\in M_1$. By definition, $(\boldsymbol{m},M_1)$ consists of elements $b\boldsymbol{m}+\boldsymbol{m}'$ for all possible $b\in R$ and $\boldsymbol{m}'\in M_1$. Therefore, $M=(\boldsymbol{m},M_1)=M_1$, which contradicts the assumption of the lemma. □

Proof of Theorem 13.39 The proof is an almost verbatim repetition of the proof of Theorems 5.12 and 13.22. We may use induction on the length n of the chain (13.33), that is, we may assume the theorem to be true for the module M_1. Let

$$M_1=C_1\oplus\cdots\oplus C_r, \tag{13.34}$$

where $C_i=\{\boldsymbol{c}_i\}$ are cyclic submodules, and the order of each element $\boldsymbol{c}_i$ is the power of a prime element. By Lemma 13.16, $M=(\boldsymbol{m},M_1)$ and $p\boldsymbol{m}\in M_1$, where p is a prime element. Then based on the decomposition (13.34), we have

$$p\boldsymbol{m}=\boldsymbol{z}_1+\cdots+\boldsymbol{z}_r,\quad \boldsymbol{z}_i\in C_i. \tag{13.35}$$

We shall select those elements $\boldsymbol{z}_i$ that are divisible by p. By a change in numeration, we may assume that these are the first $s-1$ terms. Let us set $\boldsymbol{z}_i=p\boldsymbol{z}_i'$ for $i=1,\dots,s-1$. We must now consider two cases.

Case 1: The number $s-1$ is equal to r. Then $p\boldsymbol{m} = p\boldsymbol{m}'$, where $\boldsymbol{m}' = \boldsymbol{z}_1' + \cdots + \boldsymbol{z}_r'$. Let us set $\boldsymbol{m} - \boldsymbol{m}' = \overline{\boldsymbol{m}}$. It is obvious that $p\overline{\boldsymbol{m}} = \boldsymbol{0}$. We shall prove that the module M can be written in the form

$$M = \{\overline{\boldsymbol{m}}\} \oplus C_1 \oplus \cdots \oplus C_r.$$

Indeed, by assumption, every element $\boldsymbol{x} \in M$ can be represented in the form $\boldsymbol{x} = a\boldsymbol{m} + \boldsymbol{y}$, where $a \in R$ and $\boldsymbol{y} \in M_1$, which means also in the form $\boldsymbol{x} = a\overline{\boldsymbol{m}} + \boldsymbol{y}'$, where $\boldsymbol{y}' = a\boldsymbol{m}' + \boldsymbol{y} \in M_1$.

Let us prove that for two such representations

$$\boldsymbol{x} = a\overline{\boldsymbol{m}} + \boldsymbol{y}, \qquad \boldsymbol{x} = a'\overline{\boldsymbol{m}} + \boldsymbol{y}', \tag{13.36}$$

we have the equalities $a\overline{\boldsymbol{m}} = a'\overline{\boldsymbol{m}}$ and $\boldsymbol{y} = \boldsymbol{y}'$. From this it will follow that

$$M = \{\overline{\boldsymbol{m}}\} \oplus M_1 = \{\overline{\boldsymbol{m}}\} \oplus C_1 \oplus \cdots \oplus C_r,$$

which in our case, is relationship (13.31).

We obtain from equalities (13.36) that $\overline{a}\overline{\boldsymbol{m}} = \overline{\boldsymbol{y}}$, where $\overline{a} = a - a'$, $\overline{\boldsymbol{y}} = \boldsymbol{y}' - \boldsymbol{y}$, and by assumption, $\overline{\boldsymbol{y}} \in M_1$. By Lemma 13.16, there exists a prime element p of the ring R such that $p\boldsymbol{m} \in M_1$, and this means that $p\overline{\boldsymbol{m}} \in M_1$. By Lemma 13.20, from the inclusions $\overline{a}\overline{\boldsymbol{m}} \in M_1$ and $p\overline{\boldsymbol{m}} \in M_1$, it follows that the element $\overline{a}$ is divisible by p, that is, $\overline{a} = bp$ for some $b \in R$. From this, we obviously obtain that $\overline{a}\overline{\boldsymbol{m}} = b(p\overline{\boldsymbol{m}}) = \boldsymbol{0}$. Consequently, $a\overline{\boldsymbol{m}} = a'\overline{\boldsymbol{m}}$ and $\boldsymbol{y} = \boldsymbol{y}'$.

Case 2: The number $s-1$ is less than r. If an element $\boldsymbol{c}_i$ has order $p_i^{n_i}$ and p_i is not an associate of p, then $p_i^{n_i}$ is not divisible by p, and therefore, every element of the module $C_i = \{\boldsymbol{c}_i\}$ is divisible p, by Lemma 13.17. Therefore, among the chosen $s-1$ submodules C_i are all those such that the order of the element $\boldsymbol{c}_i$ is $p_i^{n_i}$, and p_i is not an associate of p. Since the order of an element is in general defined only up to replacing it by an associate, we may consider that in the remaining submodules $C_s = \{\boldsymbol{c}_s\}, \dots, C_r = \{\boldsymbol{c}_r\}$, the order of the element $\boldsymbol{c}_i$ is a power of p.

By construction, in the decomposition (13.35), we have $\boldsymbol{z}_i = p\boldsymbol{z}_i'$, $\boldsymbol{z}_i' \in C_i$, for all $i = 1, \dots, s-1$. Setting $\boldsymbol{z}_1' + \cdots + \boldsymbol{z}_{s-1}' = \boldsymbol{z}'$ and $\boldsymbol{m} - \boldsymbol{z}' = \overline{\boldsymbol{m}}$, we obtain the equality

$$p\overline{\boldsymbol{m}} = \boldsymbol{z}_s + \cdots + \boldsymbol{z}_r. \tag{13.37}$$

Since the order of the element $\boldsymbol{c}_i$ for $i = s, \dots, r$ is a power of p, the order of an arbitrary element $\boldsymbol{z}_i$ in the decomposition (13.37) is also a power of p. Let us denote it by p^{n_i}. Obviously, we may choose the numeration of the terms in formula (13.37) in such a way that the numbers n_i do not decrease: $1 \le n_s \le n_{s+1} \le \cdots \le n_r$. Let us prove that the order of the element $\overline{\boldsymbol{m}}$ is equal to p^{n_r+1} and that we have the equality

$$M = \{\overline{\boldsymbol{m}}\} \oplus C_1 \oplus \cdots \oplus C_{s-1} \oplus \cdots \oplus C_{r-1},$$

that is, in the decomposition, all submodules C_i occur other than C_r. With this, relationship (13.31) will be proved in the second case as well; that is, the proof of Theorem 13.39 will be complete.

Multiplying both sides of equality (13.37) by p^{n_r} and using the fact that $p^{n_r}z_i = \mathbf{0}$ for all $i = s, \dots, r$, we obtain that $p^{n_r+1}\overline{\boldsymbol{m}} = \mathbf{0}$. If the order a of an element $\overline{\boldsymbol{m}}$ is not an associate of p^{n_r+1}, then it divides it, and is equal, up to an associate, to p^k for some $k < n_r + 1$. Multiplying relationship (13.37) by p^{k-1} and using the fact that the submodules $C_1, \dots, C_r$ form a direct sum, we obtain that $p^{k-1}z_i = \mathbf{0}$ for all $i = s, \dots, r$. In particular, $p^{k-1}z_r = \mathbf{0}$, and this contradicts the assumption $k < n_r + 1$ and that the order of the element z_r is equal to p^{n_r}. Thus the order of the element $\overline{\boldsymbol{m}}$ is equal to p^{n_r+1}.

Let us note that by construction, in the decomposition (13.37), the element z_r is not divisible by p.

From what we have proved, on the basis of Lemma 13.17, it follows that $\{z_r\} = \{\boldsymbol{c}_r\} = C_r$. From this it follows that every element $\boldsymbol{m} \in M$ can be represented as a sum of elements of the modules

$$\{\overline{\boldsymbol{m}}\}, C_1, \dots, C_{s-1}, \dots, C_{r-1}. \tag{13.38}$$

Indeed, an analogous assertion holds for the modules

$$\{\overline{\boldsymbol{m}}\}, C_1, \dots, C_{s-1}, \dots, C_r, \tag{13.39}$$

since by our construction, $\overline{\boldsymbol{m}} = \boldsymbol{m} - z'$ and $z' = z'_1 + \cdots + z'_{s-1}$, where $z'_i \in C_i$. Consequently, $\boldsymbol{m} = \overline{\boldsymbol{m}} + z'_1 + \cdots + z'_{s-1}$, which means that every element $\boldsymbol{m} \in M$ is a sum of elements of the modules (13.39).

We now must verify that every element of the submodule C_r can be represented as a sum of elements of the submodules (13.38). Since $C_r = \{z_r\}$, it suffices to verify this for a single element z_r. But relationship (13.37) gives us precisely the required representation:

$$z_r = p\overline{\boldsymbol{m}} - z_s - \cdots - z_{r-1}.$$

It remains to verify the second condition entering into the definition of a direct sum: that such a representation is unique. To this end, it suffices to prove that in the relationship

$$a\overline{\boldsymbol{m}} + \boldsymbol{f}_1 + \cdots + \boldsymbol{f}_{s-1} + \cdots + \boldsymbol{f}_{r-1} = \mathbf{0}, \quad \boldsymbol{f}_i \in C_i, \tag{13.40}$$

all the terms must equal $\mathbf{0}$.

Indeed, from relationship (13.40), taking into account (13.34), it follows that $a\overline{\boldsymbol{m}} \in M_1$. But by the construction of the element $\overline{\boldsymbol{m}}$, we then also have $a\boldsymbol{m} \in M_1$. By Lemma 13.20, from the inclusions $a\boldsymbol{m} \in M_1$ and $p\boldsymbol{m} \in M_1$, we have that the element a is divisible by p, that is, $a = bp$ for some $b \in R$. Furthermore, we know that

$$p\overline{\boldsymbol{m}} = z_s + \cdots + z_r,$$

and moreover, the order of the element z_r is p^{n_r}, while the order of the element $\overline{\boldsymbol{m}}$ is p^{n_r+1}. On substituting all these relationships into decomposition (13.40), we obtain

$$b(z_s + \cdots + z_r) + \boldsymbol{f}_1 + \cdots + \boldsymbol{f}_{s-1} + \cdots + \boldsymbol{f}_{r-1} = \mathbf{0}.$$

Then it follows from formula (13.34) that $b\boldsymbol{z}_r = \boldsymbol{0}$, and since the order of the element $\boldsymbol{z}_r$ is equal to p^{n_r}, we have that p^{n_r} divides b. This means that the element a is divisible by p^{n_r+1}, and $a\overline{\boldsymbol{m}} = \boldsymbol{0}$. But then from equality (13.40), it follows that $\boldsymbol{f}_1 + \cdots + \boldsymbol{f}_{r-1} = \boldsymbol{0}$. Using again the induction hypothesis (13.34), we obtain that $\boldsymbol{f}_1 = \boldsymbol{0}, \dots, \boldsymbol{f}_{r-1} = \boldsymbol{0}$. This completes the proof of Theorem 13.39. □

For Theorem 13.39, we have the same uniqueness theorem as in the case of Theorem 5.12 and Theorem 13.22. Namely, if

$$M = C_1 \oplus \cdots \oplus C_r, \quad C_i = \{\boldsymbol{m}_i\}, \qquad M = D_1 \oplus \cdots \oplus D_s, \quad D_j = \{\boldsymbol{n}_j\}$$

are two decompositions of finitely generated torsion modules M in which the orders of elements $\boldsymbol{m}_i$ and $\boldsymbol{n}_j$ are prime powers, that is, $p_i^{r_i}\boldsymbol{m}_i = \boldsymbol{0}$ and $q_j^{s_j}\boldsymbol{n}_j = \boldsymbol{0}$, where p_i and q_j are prime elements, then with a suitable numeration of the terms C_i and D_j, elements p_i and q_i are associates, and $r_i = s_i$. However, a natural proof of this theorem would require some new concepts, and we shall not pursue this here.