Chapter 14
Elements of Representation Theory

Representation theory is one of the most "applied" branches of algebra. It has many applications in various branches of mathematics and mathematical physics. In this chapter, we shall be concerned with the problem of finding all finite-dimensional representations of finite groups. But there is an analogous theory that has been developed for certain types of infinite groups, which is important in many other branches of mathematics.

14.1 Basic Concepts of Representation Theory

Let us recall some definitions from the previous chapter that will play a key role here.

A homomorphism of a group G into a group G' is a mapping $f : G \to G'$ such that for every pair of elements $g_1, g_2 \in G$, we have the relationship

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

An isomorphism of a group G onto a group G' is a bijective homomorphism $f : G \to G'$. Groups G and G' are said to be *isomorphic* if there exists an isomorphism $f : G \to G'$ between them. This is denoted by $G \simeq G'$.

Definition 14.1 A *representation* of a group G is a homomorphism of G into the group of nonsingular linear transformations of a vector space L. The space L is called the *space* of the representation or the *representation space*, and its dimension, that is, $\dim \mathsf{L}$, is the *dimension* of the representation.

Thus in order to specify a representation of a group G, it is necessary to associate with each element $g \in G$ a nonsingular linear transformation $\mathcal{A}_g : \mathsf{L} \to \mathsf{L}$ such that for $g_1, g_2 \in G$, the condition

$$\mathcal{A}_{g_1 g_2} = \mathcal{A}_{g_1} \mathcal{A}_{g_2} \tag{14.1}$$

I.R. Shafarevich, A.O. Remizov, *Linear Algebra and Geometry*,
DOI 10.1007/978-3-642-30994-6_14, © Springer-Verlag Berlin Heidelberg 2013

is satisfied. Since the group of nonsingular linear transformations of an n-dimensional vector space is isomorphic to the group of nonsingular square matrices of order n, to give a representation, it suffices to associate with each element $g \in G$ a nonsingular square matrix A_g such that (14.1) is satisfied.

It follows at once from (14.1) that for a representation $\mathcal{A}_g$ and any number of elements $g_1, \ldots, g_k$ of the group G, we have the relationship

$$\mathcal{A}_{g_1 \cdots g_k} = \mathcal{A}_{g_1} \cdots \mathcal{A}_{g_k}. \tag{14.2}$$

Moreover, it is obvious that if e is the identity element of G, then

$$\mathcal{A}_e = \mathcal{E}, \tag{14.3}$$

where $\mathcal{E}$ is the identity linear transformation of the space L. And if g^{-1} is the inverse of the element g, then

$$\mathcal{A}_{g^{-1}} = \mathcal{A}_g^{-1}, \tag{14.4}$$

that is, $\mathcal{A}_{g^{-1}}$ is the transformation that is the inverse of $\mathcal{A}_g$.

Example 14.2 Let $G = \mathrm{GL}_n$ be the group of nonsingular square matrices of order n. For each matrix $g \in \mathrm{GL}_n$, let us set

$$\mathcal{A}_g = |g|.$$

Since $|g|$ is a number, which by assumption is different from zero, we have a one-dimensional representation. It is obvious that for every integer n, the equality

$$\mathcal{B}_g = |g|^n$$

will also define a one-dimensional representation.

Example 14.3 Let $G = S_n$ be the symmetric group of degree n, that is, the group of permutations of an n-element set M, and let L be a vector space of dimension n, in which we have chosen a basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$. For the representation

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

let us define $\mathcal{A}_g$ as the linear transformation such that

$$\mathcal{A}_g(\boldsymbol{e}_1) = \boldsymbol{e}_{j_1}, \qquad \mathcal{A}_g(\boldsymbol{e}_2) = \boldsymbol{e}_{j_2}, \qquad \ldots, \qquad \mathcal{A}_g(\boldsymbol{e}_n) = \boldsymbol{e}_{j_n}.$$

Then we obtain an n-dimensional representation of the group S_n.

To avoid having to use a specific numeration of the elements of the set M, let us associate with the element $a \in M$, the basis vector $\boldsymbol{e}_a$. Then the representation described above is given by the formula

$$\mathcal{A}_g(\boldsymbol{e}_a) = \boldsymbol{e}_b \quad \text{if } g(a) = b,$$

for every transformation $g : M \to M$.

Example 14.4 Let $G = S_3$ be the symmetric group of degree 3, and let L be a two-dimensional space with basis $\boldsymbol{e}_1, \boldsymbol{e}_2$. Let us define a vector $\boldsymbol{e}_3$ by $\boldsymbol{e}_3 = -(\boldsymbol{e}_1 + \boldsymbol{e}_2)$. For the representation

$$g = \begin{pmatrix} 1 & 2 & 3 \\ j_1 & j_2 & j_3 \end{pmatrix},$$

let us define $\mathcal{A}_g$ as the transformation such that

$$\mathcal{A}_g(\boldsymbol{e}_1) = \boldsymbol{e}_{j_1}, \qquad \mathcal{A}_g(\boldsymbol{e}_2) = \boldsymbol{e}_{j_2}.$$

It is easily verified that in this way, we obtain a two-dimensional representation of the symmetric group S_3.

Example 14.5 Let $G = \mathrm{GL}_2$ be the group of nonsingular matrices of order 2, and let L be the space of polynomials in the two variables x and y whose total degree in both variables does not exceed n. For a nonsingular matrix

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

let us define $\mathcal{A}_g$ as the linear transformation of the space L taking polynomials $f(x, y)$ to $f(ax + by, cx + dy)$, that is,

$$\mathcal{A}_g\big(f(x, y)\big) = f(ax + by, cx + dy).$$

It is easy to verify that relationship (14.1) is satisfied in this case, that is, we have a representation of the group of nonsingular matrices of order 2. Its dimension is equal to the dimension of the space of polynomials in x and y whose dimension (in both variables combined) does not exceed n; that is, as is easily seen, it is equal to $(n + 1)(n + 2)/2$.

Example 14.6 For any group and an n-dimensional space L, the representation defined by the formula $\mathcal{A}_g = \mathcal{E}$, where $\mathcal{E}$ is the identity transformation on the space L, is called the *n-dimensional identity representation*.

In the definition of a representation, the space L can also be *infinite-dimensional*. In this case, the representation is also said to be *infinite-dimensional*. For example, defining a representation just as in Example 14.5, but taking for L the space of all continuous functions, we obtain an infinite-dimensional representation. In the sequel, we shall consider only finite-dimensional representations, and we shall always consider the space L to be complex.

Example 14.7 Representations of the symmetric group S_n are of interest in many problems. All such representations are known, but we shall describe here only the one-dimensional representations of the group S_n. In this case, a nonsingular linear transformation $\mathcal{A}_g$ is given by a matrix of order 1, that is, a single complex number (which, of course, is nonzero). We thereby arrive at a function on the group taking

numeric values. Let us denote this function by $\varphi(g)$. Then by definition, it must satisfy the conditions $\varphi(g) \neq 0$ and

$$\varphi(gh) = \varphi(g)\varphi(h) \tag{14.5}$$

for all elements g and h in the group S_n.

It is easy to find all possible values $\varphi(\tau)$ if τ is a transposition. Namely, setting $g = h = \tau$ and using the facts that $\tau^2 = e$ (the identity transformation) and that obviously, $\varphi(e) = 1$, we obtain from relationship (14.5) the equality $\varphi(\tau)^2 = 1$, from which follows $\varphi(\tau) = \pm 1$. It is theoretically possible that for some transpositions, $\varphi(\tau) = 1$, while for others, $\varphi(\tau) = -1$. However, in reality, such is not the case, and one of the equalities $\varphi(\tau) = 1$ and $\varphi(\tau) = -1$ holds for all transpositions τ, with the choice of sign depending only on the one-dimensional representation φ. Let us prove this.

Let $\tau = \tau_{a,b}$ and $\tau' = \tau_{c,d}$ be two transpositions, where a, b, c, d are elements of the set M (see formula (13.3)). Obviously, there exists a permutation g of the set M such that $g(c) = a$ and $g(d) = b$. Then as is easily verified, based on the definition of a transposition, we have the equality $g^{-1}\tau_{a,b}g = \tau_{c,d}$, that is, $\tau' = g^{-1}\tau g$. In view of relationships (14.2), (14.4), and (14.5), we obtain from the last equality that

$$\varphi(\tau') = \varphi(g)^{-1}\varphi(\tau)\varphi(g) = \varphi(\tau),$$

which proves our assertion for all transpositions τ and τ'. We shall now make use of the fact that every element g of the group S_n is the product of a finite number of transpositions; see formula (13.4). Taking the aforesaid into account, it follows from this that

$$\varphi(g) = \varphi(\tau_{a_1,b_1})\varphi(\tau_{a_2,b_2}) \cdots \varphi(\tau_{a_k,b_k}) = \varphi(\tau)^k, \tag{14.6}$$

where $\varphi(\tau) = +1$ or -1.

Thus there are two possible cases. The first case is that for all transpositions $\tau \in S_n$, the number $\varphi(\tau)$ is equal to 1. In view of formula (14.6), for every transposition $g \in S_n$, we have $\varphi(g) = 1$, that is, the function φ on S_n is identically equal to 1, and therefore, it gives the one-dimensional identity representation of the group S_n. The second case is that for all transpositions $\tau \in S_n$, we have $\varphi(\tau) = -1$. Then, in view of formula (14.6), for a transposition $g \in S_n$, we have $\varphi(g) = (-1)^k$, where k corresponds to the parity of the transposition g. In other words, $\varphi(g) = 1$ if the transposition g is even, and $\varphi(g) = -1$ if the transposition g is odd. From relationship (13.4), it follows at once that such a function φ indeed determines a one-dimensional representation of the group S_n, which we denote by $\varepsilon(g)$.

Thus we have obtained the following result: *the symmetric group S_n has exactly two one-dimensional representations: the identity and $\varepsilon(g)$.*

One-dimensional representations of the group S_n and related groups (such as the alternating group A_n) play a large role in a variety of questions in algebra. For example, one of the best-known results in algebra is the derivation of formulas for the solution of equations of degrees 3 and 4. For a long time, mathematicians were thwarted in their attempts to find analogous formulas for equations of degree 5 and

higher. Finally, it was proved that such an attempt was futile, that is, that *there exists no formula that expresses the roots of a polynomial equation of degree* 5 *or greater in terms of its coefficients using the usual arithmetic operations and the extraction of roots of arbitrary degree.* A key point in the proof of this assertion was the establishment of the fact that the alternating group A_n for $n \geq 5$ has no one-dimensional representation other than the identity. For $n = 3$ and 4, such representations of the group A_n exist, and that is what explains the existence of formulas for the solution of equations of those degrees.

Now let us establish what representations we shall consider to be identical.

Definition 14.8 Two representations $g \mapsto \mathcal{A}_g$ and $g \mapsto \mathcal{A}'_g$ of the same group G with spaces L and L' of the same dimension are said to be *equivalent* if there exists an isomorphism $\mathcal{C} : \mathsf{L}' \to \mathsf{L}$ of the vector spaces L' and L such that

$$\mathcal{A}'_g = \mathcal{C}^{-1} \mathcal{A}_g \mathcal{C} \tag{14.7}$$

for every element $g \in G$.

Let $\boldsymbol{e}'_1, \ldots, \boldsymbol{e}'_n$ be a basis of the space L' and let $\boldsymbol{e}_1 = \mathcal{C}(\boldsymbol{e}'_1), \ldots, \boldsymbol{e}_n = \mathcal{C}(\boldsymbol{e}'_n)$ be the corresponding basis of the space L, since the linear transformation $\mathcal{C} : \mathsf{L}' \to \mathsf{L}$ is an isomorphism. Comparing relationship (14.7) with the change-of-matrix formula (3.43), we see that this definition means that the matrix of the transformation $\mathcal{A}'_g$ with basis $\boldsymbol{e}'_1, \ldots, \boldsymbol{e}'_n$ coincides with the matrix of the transformation $\mathcal{A}_g$ with basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$. Thus the representations $\mathcal{A}_g$ and $\mathcal{A}'_g$ are equivalent if and only if one can choose bases in the spaces L and L' such that for each element $g \in G$, the transformations $\mathcal{A}_g : \mathsf{L} \to \mathsf{L}$ and $\mathcal{A}'_g : \mathsf{L}' \to \mathsf{L}'$ have identical matrices.

Let $g \mapsto \mathcal{A}_g$ be a representation of the group G, and let L be its representation space. A subspace $\mathsf{M} \subset \mathsf{L}$ is said to be *invariant* with respect to the representation $\mathcal{A}_g$ if it is invariant with respect to all linear transformations $\mathcal{A}_g : \mathsf{L} \to \mathsf{L}$ for all $g \in G$. Let us denote by $\mathcal{B}_g$ the restriction of $\mathcal{A}_g$ to the subspace M. It is obvious that $\mathcal{B}_g$ is a representation of the group G with representation space M. The representation $\mathcal{B}_g$ is said to be the representation *induced* by the representation $\mathcal{A}_g$ with invariant subspace M. This is also expressed by saying that the representation $\mathcal{B}_g$ *is contained in* the representation $\mathcal{A}_g$.

Example 14.9 Let us consider the n-dimensional representation of the group S_n described in Example 14.3. As is easily verified, the collection of all vectors of the form $\sum_{a \in M} \alpha_a \boldsymbol{e}_a$, where α_a is an arbitrary scalar satisfying $\sum_{a \in M} \alpha_a = 0$, forms a subspace $\mathsf{L}' \subset \mathsf{L}$ of dimension $n - 1$, invariant with respect to this representation. The representation thus induced in L' is an $(n-1)$-dimensional representation of the group S_n. In the case $n = 3$, it is equivalent to the representation of the group S_3 described in Example 14.4.

Example 14.10 In Example 14.5, let us denote by M_k $(k = 0, \ldots, n)$ the subspace consisting of polynomials of degree at most k in the variables x and y. Each of M_k is an invariant subspace of every M_l with index $l \geq k$.

Definition 14.11 A representation is said to be *reducible* if its representation space L has an invariant subspace different from $(\mathbf{0})$ and from all of L. Otherwise, it is said to be *irreducible*.

Examples 14.3 and 14.5 give reducible representations. Clearly, the n-dimensional identity representation is reducible if $n > 1$: every subspace of the representation space is invariant. Every one-dimensional representation is irreducible.

Let us prove that the representation in Example 14.4 is irreducible. Indeed, any invariant subspace different from $(\mathbf{0})$ and L must be one-dimensional. Let $\boldsymbol{u}$ be a basis vector of such a subspace. The condition of invariance means that

$$\mathcal{A}_g(\boldsymbol{u}) = \lambda_g \boldsymbol{u}$$

for every $g \in S_3$, where λ_g is some scalar depending on the element g, that is, $\boldsymbol{u}$ is a common eigenvector for all transformations $\mathcal{A}_g$. It is easy to verify that this is impossible: the eigenvectors of the transformation $\mathcal{A}_{g_1}$ with $g_1 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ have the form $\alpha(\boldsymbol{e}_1 + \boldsymbol{e}_2)$ and $\beta(\boldsymbol{e}_1 - \boldsymbol{e}_2)$, and the eigenvectors of the transformation $\mathcal{A}_{g_2}$ with $g_2 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$ have the form $\gamma \boldsymbol{e}_2$ and $\delta(2\boldsymbol{e}_1 + \boldsymbol{e}_2)$, and these clearly cannot coincide.

Definition 14.12 A representation $\mathcal{A}_g$ is said to be the *direct sum* of the r representations

$$\mathcal{A}_g^{(1)}, \ldots, \mathcal{A}_g^{(r)}$$

if its representation space L is the direct sum of the r invariant subspaces

$$\mathsf{L} = \mathsf{L}_1 \oplus \cdots \oplus \mathsf{L}_r, \tag{14.8}$$

and $\mathcal{A}_g$ induces in every L_i a representation equivalent to $\mathcal{A}_g^{(i)}$, $i = 1, \ldots, r$.

Example 14.13 The n-dimensional identity representation is the direct sum of n one-dimensional identity representations. To convince oneself of this, it suffices to decompose the space of this representation in some way into a direct sum of one-dimensional subspaces.

Example 14.14 In the situation of Example 14.9, let us denote by L_1 an invariant subspace L' of dimension $n-1$, and let us denote by L_2 the one-dimensional subspace spanned by the vector $\sum_{a \in M} \boldsymbol{e}_a$. Clearly, L_2 is also an invariant subspace of this representation, and we have the decomposition $\mathsf{L} = \mathsf{L}_1 \oplus \mathsf{L}_2$. In particular, the representation introduced in Example 14.3, for $n = 3$, is the direct sum of the representation of Example 14.4 and the one-dimensional identity representation.

It can happen that the representation space L has an invariant subspace L_1, yet it is impossible to find a complementary invariant subspace L_2 such that $\mathsf{L} = \mathsf{L}_1 \oplus \mathsf{L}_2$. In other words, the representation is reducible, but it is not the direct sum of two other representations.

Example 14.15 Let $G = \{g\}$ be an infinite cyclic group, and let L be a two-dimensional space with basis $\boldsymbol{e}_1, \boldsymbol{e}_2$. Let us denote by $\mathcal{A}_n$ the transformation having

in this basis the matrix $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$. It is obvious that $\mathcal{A}_n \mathcal{A}_m = \mathcal{A}_{n+m}$. From this, it follows that on setting $\mathcal{A}_{g^n} = \mathcal{A}_n$, we obtain a representation of the group G. The line $\mathsf{L}_1 = \langle \boldsymbol{e}_2 \rangle$ is an invariant subspace: $\mathcal{A}_n(\boldsymbol{e}_2) = \boldsymbol{e}_2$. However, there are no other invariant subspaces. Thus, for instance, the transformation $\mathcal{A}_1$ has no eigenvectors other than $\boldsymbol{e}_2$. Therefore, our representation is reducible, but it is not a direct sum.

Let us note that in Example 14.15, the group G was infinite. It turns out that for finite groups, such a phenomenon cannot occur. Namely, in the following section, it will be proved that if a representation $\mathcal{A}_g$ of a finite group is reducible, that is, the vector space L of this representation contains an invariant subspace L_1, then L is the direct sum of L_1 and another invariant subspace L_2. Hence it follows that every representation of a finite group is the direct sum of irreducible representations. As regards irreducible representations, it will be proved in Sect. 14.3 that (up to equivalence) there is only of finite number of them.

From this point on, to the end of this book, we shall always assume that a group G is finite, with the sole exception of Example 14.36.

14.2 Representations of Finite Groups

The proof of the fundamental property of representations of finite groups formulated at the end of the preceding section uses several properties of complex vector spaces.

Let us consider a representation of a finite group G. Let L be its representation space. Let us define on L some Hermitian form $\varphi(\boldsymbol{x}, \boldsymbol{y})$ for which the corresponding quadratic-Hermitian form $\psi(\boldsymbol{x}) = \varphi(\boldsymbol{x}, \boldsymbol{x})$ is positive definite, and thus it takes positive values for all $\boldsymbol{x} \neq \boldsymbol{0}$. For example, if $\mathsf{L} = \mathbb{C}^n$, then for vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ with coordinates $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$, let us set

$$\varphi(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} x_i \overline{y}_i .$$

In the sequel, we shall denote $\varphi(\boldsymbol{x}, \boldsymbol{y})$ by $(\boldsymbol{x}, \boldsymbol{y})$ and call it a *scalar product* in the space L. The concepts and simple results that we proved in Chap. 7 for Euclidean spaces can be transferred to this case verbatim. Let us list those of them that we are now going to use:

1. The *orthogonal complement* of a subspace $\mathsf{L}' \subset \mathsf{L}$ is the collection of all vectors $\boldsymbol{y} \in \mathsf{L}$ for which $(\boldsymbol{x}, \boldsymbol{y}) = 0$ for all $\boldsymbol{x} \in \mathsf{L}'$. The orthogonal complement of a subspace L' is itself a subspace of L and is denoted by $(\mathsf{L}')^{\perp}$. We have the decomposition $\mathsf{L} = \mathsf{L}' \oplus (\mathsf{L}')^{\perp}$.
2. A *unitary transformation* (the analogue of orthogonal transformation for the case of a complex space) is a linear transformation $\mathcal{U} : \mathsf{L} \to \mathsf{L}$ such that for all vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathsf{L}$, we have the relationship

$$\big(\mathcal{U}(\boldsymbol{x}), \mathcal{U}(\boldsymbol{y})\big) = (\boldsymbol{x}, \boldsymbol{y}).$$

3. The complex analogue of Theorem 7.24 is this: if a subspace $\mathsf{L}' \subset \mathsf{L}$ is invariant with respect to a unitary transformation $\mathcal{U}$, then its orthogonal complement $(\mathsf{L}')^{\perp}$ is also invariant with respect to $\mathcal{U}$.

Definition 14.16 A representation $\mathcal{U}_g$ of a group G is said to be *unitarizable* if it is possible to introduce a scalar product on its representation space L such that all transformations $\mathcal{U}_g$ become unitary.

The property of a representation being unitarizable obviously remains true under a change to an equivalent representation.

Indeed, let $g \mapsto \mathcal{U}_g$ be a unitarizable representation of some group G with space L and Hermitian form $\varphi(\boldsymbol{x}, \boldsymbol{y})$. Let us consider an arbitrary isomorphism $\mathcal{C} : \mathsf{L}' \to \mathsf{L}$. As we know, it determines an equivalent representation $g \mapsto \mathcal{U}'_g$ of the same group with space L'. Let us show that the representation $g \mapsto \mathcal{U}'_g$ is also unitarizable. As the scalar product in L' let us choose the form defined by the relationship

$$\psi(\boldsymbol{u}, \boldsymbol{v}) = \varphi\big(\mathcal{C}(\boldsymbol{u}), \mathcal{C}(\boldsymbol{v})\big) \tag{14.9}$$

for vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathsf{L}'$. It is obvious that $\psi(\boldsymbol{u}, \boldsymbol{v})$ is a Hermitian form on L' and that $\psi(\boldsymbol{u}, \boldsymbol{u}) > 0$ for every nonnull vector $\boldsymbol{u} \in \mathsf{L}'$. Let us verify that the scalar product $\psi(\boldsymbol{u}, \boldsymbol{v})$ indeed establishes the unitarizability of the representation $g \mapsto \mathcal{U}'_g$. Substituting the vectors $\mathcal{U}'_g(\boldsymbol{u})$ and $\mathcal{U}'_g(\boldsymbol{v})$ into equality (14.9), taking into account (14.7) and the unitarizability of the representation $g \mapsto \mathcal{U}_g$, we obtain the relationship

$$\begin{aligned}\psi\big(\mathcal{U}'_g(\boldsymbol{u}), \mathcal{U}'_g(\boldsymbol{v})\big) &= \psi\big(\mathcal{C}^{-1}\mathcal{U}_g\mathcal{C}(\boldsymbol{u}), \mathcal{C}^{-1}\mathcal{U}_g\mathcal{C}(\boldsymbol{v})\big) \\ &= \varphi\big(\mathcal{U}_g\mathcal{C}(\boldsymbol{u}), \mathcal{U}_g\mathcal{C}(\boldsymbol{v})\big) = \varphi\big(\mathcal{C}(\boldsymbol{u}), \mathcal{C}(\boldsymbol{v})\big) = \psi(\boldsymbol{u}, \boldsymbol{v}),\end{aligned}$$

which means that the representation $g \mapsto \mathcal{U}'_g$ is unitarizable.

Lemma 14.17 *If a space* L *of a unitarizable representation* $\mathcal{U}_g$ *of a group* G *contains an invariant subspace* L'*, then it also contains a second invariant subspace* L'' *such that* $\mathsf{L} = \mathsf{L}' \oplus \mathsf{L}''$.

Proof Let us take as L'' the orthogonal complement $(\mathsf{L}')^{\perp}$. Then the space L'' is invariant with respect to all transformations $\mathcal{U}_g$, and we have the decomposition $\mathsf{L} = \mathsf{L}' \oplus \mathsf{L}''$. □

The application of this lemma to representations of finite groups is based on the following fundamental fact.

Theorem 14.18 *Every representation* $\mathcal{A}_g$ *of a finite group* G *is unitarizable.*

Proof Let us introduce a scalar product on the representation space L in such a way that all linear transformations $\mathcal{A}_g$ become unitary. For this, let us take an arbitrary scalar product $[\boldsymbol{x}, \boldsymbol{y}]$ in the space L, defined by an arbitrary Hermitian form $\varphi(\boldsymbol{x}, \boldsymbol{y})$,

such that the associated quadratic form $\varphi(\boldsymbol{x}, \boldsymbol{x})$ is positive definite: $\varphi(\boldsymbol{x}, \boldsymbol{x}) > 0$ for every $\boldsymbol{x} \neq \boldsymbol{0}$. Let us now set

$$(\boldsymbol{x}, \boldsymbol{y}) = \sum_{g \in G} \big[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{y})\big], \tag{14.10}$$

where the sum is taken over all elements g of the group G. We shall prove that $(\boldsymbol{x}, \boldsymbol{y})$ is also a scalar product and that with respect to it, all transformations $\mathcal{A}_g$ are unitary.

The required properties of a scalar product for $(\boldsymbol{x}, \boldsymbol{y})$ derive from the analogous properties of $[\boldsymbol{x}, \boldsymbol{y}]$ and from the fact that $\mathcal{A}_g$ is a linear transformation:

1. $(\boldsymbol{y}, \boldsymbol{x}) = \sum_{g \in G} \big[\mathcal{A}_g(\boldsymbol{y}), \mathcal{A}_g(\boldsymbol{x})\big] = \sum_{g \in G} \overline{\big[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{y})\big]} = \overline{(\boldsymbol{x}, \boldsymbol{y})}$,
2. $(\lambda \boldsymbol{x}, \boldsymbol{y}) = \sum_{g \in G} \big[\mathcal{A}_g(\lambda \boldsymbol{x}), \mathcal{A}_g(\boldsymbol{y})\big] = \sum_{g \in G} \lambda \big[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{y})\big] = \lambda(\boldsymbol{x}, \boldsymbol{y})$,
3. $(\boldsymbol{x}_1 + \boldsymbol{x}_2, \boldsymbol{y}) = \sum_{g \in G} \big[\mathcal{A}_g(\boldsymbol{x}_1 + \boldsymbol{x}_2), \mathcal{A}_g(\boldsymbol{y})\big]$
$= \sum_{g \in G} \big[\mathcal{A}_g(\boldsymbol{x}_1) + \mathcal{A}_g(\boldsymbol{x}_2), \mathcal{A}_g(\boldsymbol{y})\big] = (\boldsymbol{x}_1, \boldsymbol{y}) + (\boldsymbol{x}_2, \boldsymbol{y})$,
4. $(\boldsymbol{x}, \boldsymbol{x}) = \sum_{g \in G} \big[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{x})\big] > 0, \quad$ if $\boldsymbol{x} \neq \boldsymbol{0}$.

For the proof of the last property, it is necessary to observe that in this sum, all terms $[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{x})]$ are positive. This follows from the analogous property of the scalar product $[\boldsymbol{x}, \boldsymbol{y}]$, that is, from the fact that $[\boldsymbol{x}, \boldsymbol{x}] > 0$ for all $\boldsymbol{x} \neq \boldsymbol{0}$. Since the linear transformation $\mathcal{A}_g : \mathsf{L} \to \mathsf{L}$ is nonsingular, it takes every nonnull vector $\boldsymbol{x}$ to a nonnull vector $\mathcal{A}_g(\boldsymbol{x})$.

Let us now verify that with respect to the scalar product $(\boldsymbol{x}, \boldsymbol{y})$, every transformation $\mathcal{A}_h$, $h \in G$, is unitary. In view of (14.10), we have

$$\begin{aligned}\big(\mathcal{A}_h(\boldsymbol{x}), \mathcal{A}_h(\boldsymbol{y})\big) &= \sum_{g \in G} \big[\mathcal{A}_g\big(\mathcal{A}_h(\boldsymbol{x})\big), \mathcal{A}_g\big(\mathcal{A}_h(\boldsymbol{y})\big)\big] \\ &= \sum_{g \in G} \big[\mathcal{A}_g \mathcal{A}_h(\boldsymbol{x}), \mathcal{A}_g \mathcal{A}_h(\boldsymbol{y})\big]. \end{aligned} \tag{14.11}$$

Let us set $gh = u$. In view of property (14.1), we have $\mathcal{A}_g \mathcal{A}_h = \mathcal{A}_{gh} = \mathcal{A}_u$. Therefore, we may rewrite equality (14.11) in the form

$$\big(\mathcal{A}_h(\boldsymbol{x}), \mathcal{A}_h(\boldsymbol{y})\big) = \sum_{u = gh} \big[\mathcal{A}_u(\boldsymbol{x}), \mathcal{A}_u(\boldsymbol{y})\big]. \tag{14.12}$$

Let us now observe that as g runs through all elements of the group G while h is fixed, the element $u = gh$ also runs through all elements of the group G. This follows from the fact that for every element $u \in G$, the element $g = uh^{-1}$ satisfies the relationship $gh = u$, and that for distinct g_1 and g_2, we thereby obtain distinct elements u_1 and u_2.

Thus in equality (14.12), the element u runs through the entire group G, and we can rewrite this equality in the form

$$\big(\mathcal{A}_h(\boldsymbol{x}), \mathcal{A}_h(\boldsymbol{y})\big) = \sum_{g\in G}\big[\mathcal{A}_g(\boldsymbol{x}), \mathcal{A}_g(\boldsymbol{y})\big],$$

whence in view of definition (14.10), it follows that $(\mathcal{A}_h(\boldsymbol{x}), \mathcal{A}_h(\boldsymbol{y})) = (\boldsymbol{x}, \boldsymbol{y})$, that is, the transformation $\mathcal{A}_h$ is unitary with respect to the scalar product $(\boldsymbol{x}, \boldsymbol{y})$. □

Corollary 14.19 *If the space* L *of a representation of a finite group contains an invariant subspace* L'*, then it contains another invariant subspace* L'' *such that* $\mathsf{L} = \mathsf{L}' \oplus \mathsf{L}''$.

This follows directly from Lemma 14.17 and from Theorem 14.18.

Corollary 14.20 *Every representation of a finite group is a direct sum of irreducible representations.*

Proof If the space L of our representation $\mathcal{A}_g$ does not have an invariant subspace different from $(\mathbf{0})$ and all of L, then this representation itself is irreducible, and our assertion is true (although trivially so). But if the space L has an invariant subspace L', then by Corollary 14.19, there exists an invariant subspace L'' such that $\mathsf{L} = \mathsf{L}' \oplus \mathsf{L}''$.

Let us apply the same argument to each of the spaces L' and L''. Continuing this process, we will eventually come to a halt, since the dimensions of the obtained subspaces are continually decreasing. As a result, we arrive at such a decomposition (14.8) with some number $r \geq 2$ such that the invariant subspaces L_i contain no invariant subspaces other than $(\mathbf{0})$ and all of L_i. This means precisely that the representations $\mathcal{A}_g^{(1)}, \dots, \mathcal{A}_g^{(r)}$ induced in the subspaces $\mathsf{L}_1, \dots, \mathsf{L}_r$ by our representation $\mathcal{A}_g$ are irreducible, and the representation $\mathcal{A}_g$ decomposes as a direct sum $\mathcal{A}_g^{(1)}, \dots, \mathcal{A}_g^{(r)}$. □

Theorem 14.21 *If a representation* $\mathcal{A}_g$ *decomposes into a direct sum of irreducible representations* $\mathcal{A}_g^{(1)}, \dots, \mathcal{A}_g^{(r)}$*, then every irreducible representation* $\mathcal{B}_g$ *contained in* $\mathcal{A}_g$ *is equivalent to one of the* $\mathcal{A}_g^{(i)}$.

Proof Let $\mathsf{L} = \mathsf{L}_1 \oplus \dots \oplus \mathsf{L}_r$ be a decomposition of the space L of the representation $\mathcal{A}_g$ into a direct sum of invariant subspaces such that $\mathcal{A}_g$ induces in L_i the representation $\mathcal{A}_g^{(i)}$, and let M be the invariant subspace L in which $\mathcal{A}_g$ induces the representation $\mathcal{B}_g$.

Then in particular, for every vector $\boldsymbol{x} \in \mathsf{M}$, we have the decomposition

$$\boldsymbol{x} = \boldsymbol{x}_1 + \dots + \boldsymbol{x}_r, \quad \boldsymbol{x}_i \in \mathsf{L}_i. \tag{14.13}$$

It determines a linear transformation $\mathcal{P}_i : \mathsf{M} \to \mathsf{L}_i$ that is the projection of the subspace M onto L_i parallel to $\mathsf{L}_1 \oplus \dots \oplus \mathsf{L}_{i-1} \oplus \mathsf{L}_{i+1} \oplus \dots \oplus \mathsf{L}_r$; see Example 3.51 on

p. 103. In other words, the transformations $\mathcal{P}_i : \mathsf{M} \to \mathsf{L}_i$ are defined by the conditions

$$\mathcal{P}_i(\boldsymbol{x}) = \boldsymbol{x}_i, \quad i = 1, \ldots, r. \tag{14.14}$$

The proof of the theorem is based on the relationships

$$\mathcal{A}_g \mathcal{P}_i(\boldsymbol{x}) = \mathcal{P}_i \mathcal{A}_g(\boldsymbol{x}), \quad i = 1, \ldots, r, \tag{14.15}$$

which are valid for every vector $\boldsymbol{x} \in \mathsf{M}$. For the proof of relationships (14.15), let us apply the transformation $\mathcal{A}_g$ to both sides of equality (14.13). We then obtain

$$\mathcal{A}_g(\boldsymbol{x}) = \mathcal{A}_g(\boldsymbol{x}_1) + \cdots + \mathcal{A}_g(\boldsymbol{x}_r). \tag{14.16}$$

Since $\mathcal{A}_g(\boldsymbol{x}) \in \mathsf{M}$ and $\mathcal{A}_g(\boldsymbol{x}_i) \in \mathsf{L}_i$, $i = 1, \ldots, r$, it follows that relationship (14.16) is decomposition (14.13) for the vector $\mathcal{A}_g(\boldsymbol{x})$, whence follows equality (14.15).

From the irreducibility of the representations $\mathcal{A}_g^{(1)}, \ldots, \mathcal{A}_g^{(r)}$ and $\mathcal{B}_g$, it follows that the projection $\mathcal{P}_i$ defined by formula (14.14) is either identically zero or an isomorphism of the spaces M and L_i. Indeed, let the vector $\boldsymbol{x} \in \mathsf{M}$ be contained in the kernel of the transformation $\mathcal{P}_i$, that is, $\mathcal{P}_i(\boldsymbol{x}) = \boldsymbol{0}$. Then clearly, $\mathcal{A}_g \mathcal{P}_i(\boldsymbol{x}) = \boldsymbol{0}$, and in view of relationship (14.15), we obtain that $\mathcal{P}_i \mathcal{A}_g(\boldsymbol{x}) = \boldsymbol{0}$, that is, the vector $\mathcal{A}_g(\boldsymbol{x})$ is also contained in the kernel of $\mathcal{P}_i$. From the irreducibility of the representations $\mathcal{A}_g^{(i)}$, it now follows that the kernel either is equal to $(\boldsymbol{0})$ or coincides with the entire space M (in the latter case, the projection $\mathcal{P}_i$ will obviously be the null transformation). In exactly the same way, from equality (14.15), it follows that the image of the transformation $\mathcal{P}_i$ either equals $(\boldsymbol{0})$ or coincides with the subspace L_i.

However, there is certainly at least one such index i among the numbers $1, \ldots, r$ for which the transformation $\mathcal{P}_i$ is not identically zero. For this, we must take an arbitrary nonnull vector $\boldsymbol{x} \in \mathsf{M}$ one of whose components $\boldsymbol{x}_i$ in the decomposition (14.13) is not equal to zero, and therefore, $\mathcal{P}_i(\boldsymbol{x}) \neq \boldsymbol{0}$. Taking into account the previous arguments, this shows that the corresponding transformation $\mathcal{P}_i$ is an isomorphism of the vector spaces M and L_i, and relationship (14.15) shows the equivalence of the corresponding representations $\mathcal{B}_g$ and $\mathcal{A}_g^{(i)}$. □

Corollary 14.22 *In a given representation are contained only finitely many distinct—in the sense of equivalence—irreducible representations.*

Indeed, all irreducible representations contained in the given one are equivalent to one of those encountered in an arbitrary decomposition of this representation as a direct sum of irreducible representations.

Remark 14.23 From Theorem 14.21 there follows a certain property of *uniqueness* of the decompositions of a representation into irreducible representations. Namely, however we decompose a representation, we shall encounter in the decomposition the same (up to equivalence) irreducible representations. Indeed, let us select a certain decomposition of our representation into irreducible representations. An irreducible representation encountered in any other decomposition appears in our representation, which means that by Theorem 14.21, it is equivalent to one of the terms

of the chosen decomposition. A stronger property of uniqueness consists in the fact that if in one decomposition there appear k terms equivalent to a given irreducible representation, then the same number of such terms will appear as well in every other decomposition. We shall not require this assertion in the sequel, and we shall therefore not prove it.

14.3 Irreducible Representations

In this section, we shall prove that a finite group has only a finite number of distinct (up to equivalence) irreducible representations. We shall accomplish this as follows: We shall construct one particularly important representation called a *regular representation*, for which we then shall prove that every irreducible representation is contained within it. The finiteness of the number of such representations will then result from Corollary 14.22. The space of a regular representation consists of *all possible functions on the group*. This is a special case of the general notion of the space of functions on an arbitrary set (see Example 3.36, p. 94).

For an arbitrary finite group G, let us consider the vector space $\mathsf{M}(G)$ of functions on this group. Since the group G is finite, the space $\mathsf{M}(G)$ has finite dimension: $\dim \mathsf{M}(G) = |G|$.

Definition 14.24 The *regular* representation of a group G is the representation $\mathcal{R}_g$ whose representation space is the space $\mathsf{M}(G)$ of functions on the group G, and in which the element $g \in G$ is associated with the linear transformation $\mathcal{R}_g$ that takes the function $f(h) \in \mathsf{M}(G)$ to the function $\varphi(h) = f(hg)$:

$$\big(\mathcal{R}_g(f)\big)(h) = f(hg). \tag{14.17}$$

Formula (14.17) means that the result of applying the linear transformation $\mathcal{R}_g$ to the function f is a "translated" function f, in the sense that the value $\mathcal{R}_g(f)$ on the element $h \in G$ is equal to $f(hg)$. We shall omit the obvious verification of the fact that the transformation of the space $\mathsf{M}(G)$ thus obtained is linear. Let us verify that $\mathcal{R}_g$ is a representation, that is, that it satisfies the requirements (14.1).

Let us set $\mathcal{R}_{g_1 g_2}(f) = \varphi$. By formula (14.17), we have

$$\varphi(h) = f(hg_1g_2).$$

Let $\mathcal{R}_{g_2}(f) = \psi$. Then

$$\psi(u) = f(ug_2).$$

Finally, if $\mathcal{R}_{g_1}\mathcal{R}_{g_2}(f) = \varphi_1$, then $\varphi_1 = \mathcal{R}_{g_1}(\psi)$ and $\varphi_1(u) = \psi(ug_1)$. Substituting $u = hg_1$ into the previous formula, we obtain that $\varphi_1(u) = \psi(ug_1) = f(ug_1g_2)$ for every element $u \in G$. This means that $\varphi = \varphi_1$ and $\mathcal{R}_{g_1g_2} = \mathcal{R}_{g_1}\mathcal{R}_{g_2}$.

Example 14.25 Let G be a group of order two, consisting of elements e and g, where $g^2 = e$. A particular instance of this group is S_2, the symmetric group of

degree 2. The space $\mathsf{M}(G)$ is two-dimensional, and every function $f \in \mathsf{M}(G)$ is defined by two numbers, $\alpha = f(e)$ and $\beta = f(g)$, that is, it can be identified with the vector (α, β). As with any representation, $\mathcal{R}_e$ is the identity transformation. Let us determine what $\mathcal{R}_g$ is. By formula (14.17), we have

$$\big(\mathcal{R}_g(f)\big)(e) = f(g) = \beta, \qquad \big(\mathcal{R}_g(f)\big)(g) = f\big(g^2\big) = f(e) = \alpha.$$

This means that the linear transformation $\mathcal{R}_g$ takes the vector (α, β) to the vector (β, α), that is, it represents a reflection with respect to the line $\alpha = \beta$.

Theorem 14.26 *Every irreducible representation of a finite group G is contained in its regular representation $\mathcal{R}_g$.*

Proof Let $\mathcal{A}_g$ be an irreducible representation with space L. Let us denote by l an arbitrary nonnull linear function on the space L and let us associate with each vector $\boldsymbol{x} \in \mathsf{L}$ the function $f(h) = l(\mathcal{A}_h(\boldsymbol{x})) \in \mathsf{M}(G)$ obtained when the vector $\boldsymbol{x}$ is fixed and the element h runs through all possible values of the group G. It is obvious that in this way, we obtain a linear transformation $\mathcal{C} : \mathsf{L} \to \mathsf{M}'$ defined by the relationship

$$\mathcal{C}(\boldsymbol{x}) = l\big(\mathcal{A}_h(\boldsymbol{x})\big), \tag{14.18}$$

where M' is some subspace of the vector space $\mathsf{M}(G)$. Here by construction, $\mathcal{C}(\mathsf{L}) = \mathsf{M}'$, that is, M' is the image of the transformation $\mathcal{C}$.

We shall prove the following properties:

(1) For all elements $g \in G$ and vectors $\boldsymbol{x} \in \mathsf{L}$, we have the relationship

$$(\mathcal{C}\mathcal{A}_g)(\boldsymbol{x}) = (\mathcal{R}_g\mathcal{C})(\boldsymbol{x}). \tag{14.19}$$

(2) The subspace M' is invariant with respect to the representation $\mathcal{R}_g$.
(3) The transformation $\mathcal{C}$ is an isomorphism of the spaces L and M'.

Comparing formulas (14.19) and (14.7), taking into account the remaining two properties, we conclude that the irreducible representation $\mathcal{A}_g$ is equivalent to the representation induced by the regular representation $\mathcal{R}_g$ in the invariant subspace $\mathsf{M}' \subset \mathsf{M}(G)$. By virtue of the definitions given above, this means that $\mathcal{A}_g$ is contained in $\mathcal{R}_g$, as asserted in the statement of the theorem.

Proof of property (1). Let us set $\mathcal{C}(\boldsymbol{x}) = f \in \mathsf{M}(G)$. Then by definition, $f(h) = l(\mathcal{A}_h(\boldsymbol{x}))$ for every element $h \in G$. Applying formula (14.17), we obtain the relationship

$$(\mathcal{R}_g\mathcal{C})(\boldsymbol{x}) = \mathcal{R}_g(f) = \varphi, \tag{14.20}$$

where φ is the function on the group G defined by the relationship $\varphi(h) = l(\mathcal{A}_{hg}(\boldsymbol{x}))$.

On the other hand, substituting the vector $\mathcal{A}_g(\boldsymbol{x})$ for $\boldsymbol{x}$ in formula (14.18), we obtain the equality

$$\mathcal{C}\big(\mathcal{A}_g(\boldsymbol{x})\big) = (\mathcal{C}\mathcal{A}_g)(\boldsymbol{x}) = \varphi_1(h), \tag{14.21}$$

where the function $\varphi_1(h)$ is defined by the relationship

$$\varphi_1(h) = l\big(\mathcal{A}_h \mathcal{A}_g(\boldsymbol{x})\big) = l\big(\mathcal{A}_{hg}(\boldsymbol{x})\big),$$

and clearly, it coincides with $\varphi(h)$. Taking into account that $\varphi(h) = \varphi_1(h)$, we see that equalities (14.20) and (14.21) yield that $(\mathcal{C}\mathcal{A}_g)(\boldsymbol{x}) = (\mathcal{R}_g\mathcal{C})(\boldsymbol{x})$.

Proof of property (2). We must prove that for every element $g \in G$, the image of the linear transformation $\mathcal{R}_g(\mathsf{M}')$ is contained in M'. Let $f \in \mathsf{M}'$, that is, by the definition of the image, $f = \mathcal{C}(\boldsymbol{x})$ for some $\boldsymbol{x} \in \mathsf{L}$. Then taking into account formula (14.19) proved above, we have the equality

$$\mathcal{R}_g(f) = (\mathcal{R}_g\mathcal{C})(\boldsymbol{x}) = (\mathcal{C}\mathcal{A}_g)(\boldsymbol{x}) = \mathcal{C}(\boldsymbol{y}),$$

where the vector $\boldsymbol{y} = \mathcal{A}_g(\boldsymbol{x})$ is in L, and by our construction, this means that $\mathcal{R}_g(f) \in \mathsf{M}'$. This proves the required inclusion $\mathcal{R}_g(\mathsf{M}') \subset \mathsf{M}'$.

Proof of property (3). Since by construction, the space M' is the image of the transformation $\mathcal{C} : \mathsf{L} \to \mathsf{M}'$, it remains only to show that the transformation $\mathcal{C}$ is bijective, that is, that its kernel is equal to $(\mathbf{0})$. This means that we must prove that the equality $\boldsymbol{x} = \mathbf{0}$ follows from the equality $\mathcal{C}(\boldsymbol{x}) = \mathbf{0}'$ (where $\mathbf{0}'$ denotes the function identically equal to zero on the group G). Let us denote the kernel of the transformation $\mathcal{C}$ by L'. As we know, it is a subspace of L. Let us show that L' is invariant with respect to the representation $\mathcal{A}_g$.

Indeed, let us suppose that $\mathcal{C}(\boldsymbol{x}) = \mathbf{0}'$ for some vector $\boldsymbol{x} \in \mathsf{L}$, and let us set $\boldsymbol{y} = \mathcal{A}_g(\boldsymbol{x})$. On applying the transformation $\mathcal{C}$ to the vector $\boldsymbol{y}$, taking into account formula (14.19), we obtain

$$\mathcal{C}(\boldsymbol{y}) = \big(\mathcal{C}\mathcal{A}_g(\boldsymbol{x})\big) = (\mathcal{R}_g\mathcal{C})(\boldsymbol{x}) = \mathcal{R}_g\big(\mathcal{C}(\boldsymbol{x})\big) = \mathcal{R}_g\big(\mathbf{0}'\big) = \mathbf{0}'.$$

But from the irreducibility of the representation $\mathcal{A}_g$, it now follows that either $\mathsf{L}' = \mathsf{L}$ or $\mathsf{L}' = (\mathbf{0})$. The former would mean that $l(\mathcal{A}_h(\boldsymbol{x})) = 0$ for all $h \in G$ and $\boldsymbol{x} \in \mathsf{L}$. But then even for $h = e$, we would have the equality $l(\mathcal{A}_e(\boldsymbol{x})) = l(\mathcal{E}(\boldsymbol{x})) = l(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in \mathsf{L}$, which is impossible, since in the definition of the transformation $\mathcal{C}$, the function l was chosen to be not identically zero. This means that the subspace L' is equal to $(\mathbf{0})$, which is what was to be proved. □

Corollary 14.27 *A finite group has only a finite number of distinct* (*up to equivalence*) *irreducible representations.*

Example 14.28 Let $\mathcal{A}_g$ be the one-dimensional identity representation of the group G. Then the space L is one-dimensional. Let $\boldsymbol{e}$ be a basis of L. Let us define the function l by the condition $l(\alpha\boldsymbol{e}) = \alpha$. Formula (14.18) gives for the vector $\boldsymbol{x} = \alpha\boldsymbol{e}$, the value

$$\mathcal{C}(\alpha\boldsymbol{e}) = f, \quad \text{where } f(h) = l\big(\mathcal{A}_h(\alpha\boldsymbol{e})\big) = l(\alpha\boldsymbol{e}) = \alpha.$$

Thus to the vector $\alpha\boldsymbol{e}$ is associated the function f, which takes for all $h \in G$ the same value α. Obviously, such constant functions indeed form an invariant subspace with respect to the regular representation, and the representation induced in it is the identity, as asserted by Theorem 14.26.

14.4 Representations of Abelian Groups

Let us first of all recall that we are assuming throughout that the space L of a representation is complex.

Theorem 14.29 *An irreducible representation of an abelian group is one-dimensional.*

Proof Let g be a fixed element of the group G. Its associated linear transformation $\mathcal{A}_g : \mathsf{L} \to \mathsf{L}$ has at least one eigenvalue λ. Let $\mathsf{M} \subset \mathsf{L}$ be the eigensubspace corresponding to the eigenvalue λ, that is, the collection of all vectors $\boldsymbol{x} \in \mathsf{L}$ such that

$$\mathcal{A}_g(\boldsymbol{x}) = \lambda \boldsymbol{x}. \tag{14.22}$$

By construction, $\mathsf{M} \neq (\mathbf{0})$. We shall now prove that M is an invariant subspace of our representation. It will then follow from the irreducibility of the representation that $\mathsf{M} = \mathsf{L}$, and then equality (14.22) will hold for every vector $\boldsymbol{x} \in \mathsf{L}$. In other words, $\mathcal{A}_g = \lambda \mathcal{E}$, and the matrix of the transformation $\mathcal{A}_g$ is equal to λE. A matrix of this type is called a *scalar matrix*. This reasoning holds for every $g \in G$; we have only to note that the eigenvalue λ in formula (14.22) depends on the element g, and the remainder of the argument does not depend on it. Thus we may conclude that the matrices of all transformations $\mathcal{A}_g$ are scalar matrices, and if $\dim \mathsf{L} > 1$, then every subspace of the space L is invariant. Consequently, if a representation is irreducible, it is one-dimensional.

It remains to prove the invariance of the subspace M. It is here that we shall specifically use the commutativity of the group G. Let $\boldsymbol{x} \in \mathsf{M}$, $h \in G$. We shall prove that $\mathcal{A}_h(\boldsymbol{x}) \in \mathsf{M}$. Indeed, if $\mathcal{A}_h(\boldsymbol{x}) = \boldsymbol{y}$, then

$$\begin{aligned} \mathcal{A}_g(\boldsymbol{y}) &= \mathcal{A}_g\big(\mathcal{A}_h(\boldsymbol{x})\big) = \mathcal{A}_{gh}(\boldsymbol{x}) = \mathcal{A}_{hg}(\boldsymbol{x}) = \mathcal{A}_h\big(\mathcal{A}_g(\boldsymbol{x})\big) = \mathcal{A}_h(\lambda \boldsymbol{x}) \\ &= \lambda \mathcal{A}_h(\boldsymbol{x}) = \lambda \boldsymbol{y}, \end{aligned}$$

that is, the vector $\boldsymbol{y}$ belongs to M. □

In view of Theorem 14.29, every irreducible representation of an abelian group can be represented in the form $\mathcal{A}_g = \chi(g)$, where $\chi(g)$ is a number. Condition (14.1) can then be written in the following form:

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2). \tag{14.23}$$

Definition 14.30 A function $\chi(g)$ on an abelian group G taking complex values and satisfying relationship (14.23) is called a *character*.

By Theorem 14.29, every irreducible representation of a finite abelian group is a character $\chi(g)$. On the other hand, it follows from Theorem 14.26 that this representation is contained in the regular representation. In other words, in the space $\mathsf{M}(G)$ of functions on the group G, there exists an invariant subspace M' in which

the regular representation induces a representation equivalent to ours. Since our representation is one-dimensional, the subspace M' is also one-dimensional. Let some function $f \in \mathsf{M}(G)$ be a basis in M'. Then since the representation induced by the regular representation in M' has matrix $\chi(g)$, and $\mathcal{R}_g(f)(h) = f(hg)$, we must have the relationship

$$f(hg) = \chi(g) f(h).$$

Let us set $h = e$ in this equality and let us also set $f(e) = \alpha$. We obtain that $f(g) = \alpha\chi(g)$, that is, we may take as a basis of the subspace M' the character χ itself (indeed, it is a function on G, and this means that $\chi \in \mathsf{M}(G)$). As we have seen, we then have $\mathsf{M}(G) = \mathsf{M}' \oplus \mathsf{M}''$, where M'' is also an invariant subspace. Applying analogous arguments to M'' and to all invariant subspaces of dimension greater than 1 that we obtain along the way, we finally arrive at a decomposition of the subspace $\mathsf{M}(G)$ as a direct sum of one-dimensional invariant subspaces. We have thereby proved the following result.

Theorem 14.31 *The space $\mathsf{M}(G)$ of functions on a finite abelian group G can be decomposed as a direct sum of one-dimensional subspaces that are invariant with respect to the regular representation. In each such subspace, one can take as a basis vector some character $\chi(g)$. Then the matrix of the representation that is induced in this subspace coincides with this same character $\chi(g)$.*

It is obvious that we thereby establish a bijective relationship between the characters of the group G and one-dimensional invariant subspaces of the space $\mathsf{M}(G)$ of functions on this group. Indeed, two distinct characters χ_1 and χ_2 cannot be basis vectors of one and the same representation: that would mean that

$$\chi_1(g) = \alpha\chi_2(g) \quad \text{for all } g \in G.$$

Setting here $g = e$, we obtain $\alpha = 1$, since χ_1 and χ_2 are homomorphisms of the group G into $\mathbb{C}$, and therefore, $\chi_1(e) = \chi_2(e) = 1$.

Since by Corollary 14.19, a regular representation can be decomposed into a direct sum of irreducible representations, we obtain the following results for every finite abelian group G.

Corollary 14.32 *The characters form a basis of the space $\mathsf{M}(G)$ of functions on the group G.*

This assertion can be reformulated as follows.

Corollary 14.33 *The number of distinct characters of a group G is equal to its order.*

This follows from Corollary 14.32 and the fact that the dimension of the space $\mathsf{M}(G)$ is equal to the order of the group G.

Corollary 14.34 *Every function on the group G is a linear combination of characters.*

Example 14.35 Let $G = \{g\}$ be a cyclic group of finite order n, $g^n = e$. Let us denote by $\xi_0, \dots, \xi_{n-1}$ the distinct nth roots of 1, and let us set

$$\chi_i\left(g^k\right) = \xi_i^k, \quad k = 0, 1, \dots, n-1.$$

It is easily verified that χ_i is a character of the group G and that the characters χ_i corresponding to ξ_i, the distinct nth roots of 1, are themselves distinct. Since their number is equal to $|G|$, they must be all the characters of the group G. By Corollary 14.32, they form a basis of the space $\mathsf{M}(G)$. In other words, in an n-dimensional space, the vectors $1, \xi_i, \dots, \xi_i^{n-1}$ corresponding to the nth roots of 1 form a basis. This can also be verified directly by calculating the determinant consisting of the coordinates of these vectors as a Vandermonde determinant (p. 41).

Example 14.36 Let us denote by S the group of rotations of the circle in the plane. The elements of the group S correspond to points of the circle: if we associate with a real number φ the point of the circle with argument φ, then with any one point of the circle will be associated numbers that differ from one another by an integer multiple of 2π. Therefore, this group S is frequently called the *circle group*.

After choosing a certain integer m, let us associate with the point t of the circle S having argument φ the number $\cos m\varphi + i \sin m\varphi$, where i is the imaginary unit. It is obvious that adding an integer multiple of 2π to φ does not change this number, which means that it is uniquely defined by the point $t \in S$. Let us set

$$\chi_m(t) = \cos m\varphi + i \sin m\varphi, \quad m = 0, \pm 1, \pm 2, \dots. \tag{14.24}$$

It is not difficult to verify that the function $\chi_m(t)$ is a character of the group S. For an infinite group such as S, it is natural to introduce into the definition of a character in addition to the requirement (14.23), the requirement that the function $\chi_m(t)$ be continuous. The reason for such a requirement for the group S is as follows: it is necessary that the real and complex parts of the functions $\chi_m(t)$ be continuous functions.

It is possible to prove that the characters $\chi_m(t)$ defined by formula (14.24) are continuous and that they comprise all the continuous characters of the circle. This explains to a large degree the role of the trigonometric functions $\cos m\varphi$ and $\sin m\varphi$ in mathematics: they are the real and imaginary parts of the continuous characters of the circle.

Corollary 14.34 asserts that every function on a finite abelian group can be represented as a linear combination of characters. In the case of an infinite group such as S, some analytic restrictions, which we shall not specify here, are naturally imposed on such a function. We shall only mention the significance of functions on the group S. Such a function $f(t)$ can be represented as a function $F(\varphi)$ of the argument φ of the point $t \in S$. It must not, however, depend on the choice of the argument φ of the point t, that is, it must not change on the addition to φ of an integer multiple of 2π. In other words, $F(\varphi)$ must be a periodic function with period 2π.

The analogue of Corollary 14.34 for the group S asserts that such a function can be represented as a linear combination (in the given case, infinite) of functions $\chi_m(\varphi)$, $m = 0, \pm 1, \pm 2, \ldots$. In other words, this is a theorem about the fact that a periodic function (with certain analytic restrictions) can be decomposed into a Fourier series.