1

General Methods and Ideas

Summary. In this chapter we will develop the formal language and some general methods and theorems. To some extent the reader is advised not to read it too systematically since most of the interesting examples will appear only in the next chapters. The exposition here is quite far from the classical point of view since we are forced to establish the language in a rather thin general setting. Hopefully this will be repaid in the chapters in which we will treat the interesting results of Invariant Theory.

1 Groups and Their Actions

1.1 Symmetric Group

In our treatment groups will always appear as transformation groups, the main point being that, given a set X, the set of all bijective mappings of X into X is a group under composition. We will denote this group $S(X)$ and call it *the symmetric group* of X.

In practice, the full symmetric group is used only for X a finite set. In this case it is usually more convenient to identify X with the discrete interval $\{1, \dots, n\}$ formed by the first n integers (for a given value of n). The corresponding symmetric group has $n!$ elements and it is denoted by S_n. Its elements are called *permutations*.

In general, the groups which appear are subgroups of the full symmetric group, defined by special properties of the set X arising from some extra structure (such as from a topology or the structure of a linear space, etc.). The groups of interest to us will usually be symmetry groups of the structure under consideration. To illustrate this concept we start with a definition:

Definition. A partition of a set X is a family of nonempty disjoint subsets A_i such that $X = \cup_i A_i$.

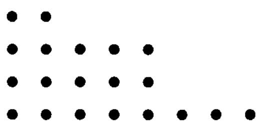
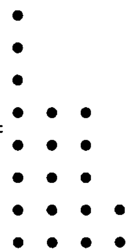
A partition of a number n is a (non-increasing) sequence of positive numbers:

$$m_1 \geq m_2 \geq \cdots \geq m_k > 0 \text{ with } \sum_{j=1}^{k} m_j = n.$$

Remark. To a partition of the set $[1, 2, \ldots, n]$ we can associate the partition of n given by the cardinalities of the sets A_i.

We will usually denote a partition by a greek letter $\lambda := m_1 \geq m_2 \geq \cdots \geq m_k$ and write $\lambda \vdash n$ to mean that it is a partition of n.

We represent graphically such a partition by a *Young diagram.* The numbers m_i appear then as the lengths of the rows (cf. Chapter 9, 2.1), e.g., $\lambda = (8, 5, 5, 2)$:

$\lambda =$  $\tilde{\lambda} =$ 

Sometimes it is useful to relax the condition and call a *partition of n* any sequence $m_1 \geq m_2 \geq \cdots \geq m_k \geq 0$ with $\sum_{j=1}^{k} m_j = n$. We then call the *height* of λ, denoted by $ht(\lambda)$, the number of nonzero elements in the sequence m_i, i.e., the number or rows of the diagram.

We can also consider the columns of the diagram which will be thought of as rows of the *dual partition*. The dual partition of λ will be denoted by $\tilde{\lambda}$. For instance, for $\lambda = (8, 5, 5, 2)$ we have $\tilde{\lambda} = (4, 4, 3, 3, 3, 1, 1, 1)$.

If $X = \cup A_i$ is a partition, the set

$$G := \{\sigma \in S_n | \sigma(A_i) = A_i, \ \forall i\},$$

is a subgroup of $S(X)$, isomorphic to the product $\prod S(A_i)$ of the symmetric groups on the sets A_i. There is also another group associated to the partition, the group of permutations which preserves the partition without necessarily preserving the individual subsets (but possibly permuting them).

1.2 Group Actions

It is useful at this stage to proceed in a formal way.

Definition 1. An action of a group G on a set X is a mapping $\pi : G \times X \to X$, denoted by $gx := \pi(g, x)$, satisfying the following conditions:

$$(1.2.1) \qquad 1x = x, \quad h(kx) = (hk)x$$

for all $h, k \in G$ and $x \in X$.

The reader will note that the above definition can be reformulated as follows:

(i) The map $\varrho(h) := x \mapsto hx$ from X to X is bijective for all $h \in G$.
(ii) The map $\varrho : G \to S(X)$ is a *group homomorphism*.

In our theory we will usually fix our attention on a given group G and consider different actions of the group. It is then convenient to refer to a given action on a set X as a *G-set.*

Examples.

(a) The action of G by left multiplication on itself.
(b) For a given subgroup H of G, the action of G on the set $G/H := \{gH | g \in G\}$ of left cosets is given by

$$a(bH) := abH. \tag{1.2.2}$$

(c) The action of $G \times G$ on G given by *left and right translations:* $(a, b)c := acb^{-1}$.
(d) The action of G by conjugation on itself.
(e) The action of a subgroup of G induced by restricting an action of G.

It is immediately useful to use *categorical* language:

Definition 2. Given two G-sets X, Y, a G-equivariant mapping, or more simply a *morphism*, is a map $f : X \to Y$ such that for all $g \in G$ and $x \in X$ we have

$$f(gx) = gf(x).$$

In this case we also say that f *intertwines* the two actions. Of course if f is bijective we speak of an *isomorphism* of the two actions. If $X = Y$ the isomorphisms of the G-action X also form a group called the *symmetries of the action.*

The class of G-sets and equivariant maps is clearly a *category.*[1]

Remark. This is particularly important when G is the homotopy group of a space X and the G-sets correspond to covering spaces of X.

Example. The equivariant maps of the action of G on itself by left multiplication are the right multiplications. They form a group isomorphic to the *opposite* of G (but also to G). Note: We recall that the *opposite* of a multiplication $(a, b) \mapsto ab$ is the operation $(a, b) \mapsto ba$. One can define opposite group or opposite ring by taking the opposite of multiplication.

More generally:

Proposition. *The invertible equivariant maps of the action of G on G/H by left multiplication are induced by the right multiplications with elements of the normalizer $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$ of H (cf. 2.2). They form a group Γ isomorphic to $N_G(H)/H$.*

---

[1] Our use of categories will be extremely limited to just a few basic functors and universal properties.

Proof. Let $\sigma : G/H \to G/H$ be such a map. Hence, for all $a, b \in G$, we have $\sigma(a\,bH) = a\sigma(bH)$. In particular if $\sigma(H) = uH$ we must have that

$$\sigma(H) = uH = \sigma(hH) = huH, \ \forall h \in H, \implies Hu \subset uH.$$

If we assume σ to be invertible, we see that also $Hu^{-1} \subset u^{-1}H$, hence $uH = Hu$ and $u \in N_G(H)$. Conversely, if $u \in N_G(H)$, the map $\sigma(u) : aH \to auH = aHu$ is well defined and an element of Γ. The map $u \to \sigma(u^{-1})$ is clearly a surjective homomorphism from $N_G(H)$ to Γ with kernel H. □

Exercise. Describe the set of equivariant maps $G/H \to G/K$ for 2 subgroups.

2 Orbits, Invariants and Equivariant Maps

2.1 Orbits

The first important notion in this setting is given by the following:

Consider the binary relation R in X given by xRy if and only if there exists $g \in G$ with $gx = y$.

Proposition. *R is an equivalence relation.*

Definition. The equivalence classes under the previous equivalence are called G-orbits (or simply orbits). The orbit of a given element x is formed by the elements gx with $g \in G$ and is denoted by Gx. The mapping $G \to Gx$ given by $g \mapsto gx$ is called the *orbit map*.

The orbit map is equivariant (with respect to the left action of G). The set X is partitioned into its orbits, and the set of all orbits (quotient set) is denoted by X/G.

In particular, we say that the action of G is *transitive* or that X is a *homogeneous space* if there is a unique orbit.

More generally, we say that a subset Y of X is G *stable* if it is a union of orbits. In this case, the action of G on X induces naturally an action of G on Y. Of course, the complement $C(Y)$ of Y in X is also G stable, and X is decomposed as $Y \cup C(Y)$ into two stable subsets.

The finest decomposition into stable subsets is the decomposition into orbits.

Basic examples.

i. Let $\sigma \in S_n$ be a permutation and A the cyclic group which it generates. Then the orbits of A on the set $\{1, \dots, n\}$ are the *cycles* of the permutation.
ii. Let G be a group and let H, K be subgroups. We have the action of $H \times K$ on G induced by the left and right action. The orbits are the *double cosets.* In particular, if either H or K is 1, we have left or right cosets.
iii. Consider G/H, the set of left cosets gH, with the action of G given by 1.2.2. Given a subgroup K of G, it still acts on G/H. The K orbits in G/H are in bijective correspondence with the double cosets KgH.

iv. Consider the action of G on itself by conjugation $(g, h) \to ghg^{-1}$. Its orbits are the *conjugacy classes.*
v. An action of the additive group $\mathbb{R}_+$ of real numbers on a set X is called a 1-*parameter group of transformations*, or in more physical language, a *reversible dynamical system.*

In example (v) the parameter t is thought of as *time,* and an orbit is seen as the time evolution of a physical state. The hypotheses of the group action mean that the evolution is reversible (i.e., all the group transformations are invertible), and the *forces* do not vary with time so that the evolution of a state depends only on the time lapse (group homomorphism property).

The previous examples also suggest the following general fact:

Remark. Let G be a group and K a normal subgroup in G. If we have an action of G on a set X, we see that G acts also on the set of K orbits X/K, since $gKx = Kgx$. Moreover, we have $(X/K)/G = X/G$.

2.2 Stabilizer

The study of group actions should start with the elementary analysis of a single orbit. The next main concept is that of *stabilizer*:

Definition. Given a point $x \in X$ we set $G_x := \{g \in G | gx = x\}$. G_x is called the *stabilizer* (or *little group*) of x.

Remark. The term *little group* is used mostly in the physics literature.

Proposition. *G_x is a subgroup, and the action of G on the orbit Gx is isomorphic to the action on the coset space G/G_x.*

Proof. The fact that G_x is a subgroup is clear. Given two elements $h, k \in G$ we have that $hx = kx$ if and only if $k^{-1}hx = x$ or $k^{-1}h \in G_x$.

The mapping between G/G_x and Gx which assigns to a coset hG_x the element hx is thus well defined and bijective. It is also clearly G-equivariant, and so the claim follows. □

Example. For the action of $G \times G$ on G by left and right translations (Example (c) of 1.2), G is a single orbit and the stabilizer of 1 is the subgroup $\Delta := \{(g, g) | g \in G\}$ isomorphic to G embedded in $G \times G$ diagonally.

Example. In the case of a 1-parameter subgroup acting continuously on a topological space, the stabilizer is a closed subgroup of $\mathbb{R}$. If it is not the full group, it is the set of integral multiples $ma, m \in \mathbb{Z}$ of a positive number a. The number a is to be considered as the first time in which the orbit returns to the starting point. This is the case of a *periodic orbit.*

Remark. Given two different elements in the same orbit, their stabilizers are conjugate. In fact, $G_{hx} = hG_xh^{-1}$. In particular when we identify an orbit with a coset space G/H this implicitly means that we have made the choice of a point for which the stabilizer is H.

Remark. The orbit cycle decomposition of a permutation π can be interpreted in the previous language. Giving a permutation π on a set S is equivalent to giving an action of the group of integers $\mathbb{Z}$ on S.

Thus S is canonically decomposed into orbits. On each orbit the permutation π induces, by definition, a *cycle*.

To study a single orbit, we need only remark that a finite orbit under $\mathbb{Z}$ is equivalent to the action of $\mathbb{Z}$ on some $\mathbb{Z}/(n)$, $n > 0$. On $Z/(n)$ the generator 1 acts as the cycle $\overline{x} \to \overline{x} + \overline{1}$.

Fixed point principle. *Given two subgroups H, K of G we have that H is conjugate to a subgroup of K if and only if the action of H on G/K has a fixed point.*

Proof. This is essentially tautological, $H \subset gKg^{-1}$ is equivalent to saying that gK is a fixed point under H. □

Consider the set of all subgroups of a group G, with G acting on this set by conjugation. The orbits of this action are the *conjugacy classes of subgroups*. Let us denote by $[H]$ the conjugacy class of a subgroup H.

The stabilizer of a subgroup H under this action is called its *normalizer*. It should not be confused with the *centralizer* which, for a given subset A of G, is the stabilizer under conjugation of all of the elements of A.

Given a group G and an action on X, it is useful to introduce the notion of *orbit type*.

Observe that for an orbit in X, the conjugacy class of the stabilizers of its elements is well defined. We say that two orbits are of the same *orbit type* if the associated stabilizer class is the same. This is equivalent to saying that the two orbits are isomorphic as G-spaces. It is often useful to partition the orbits according to their orbit types.

Exercise. Determine the points in G/H with stabilizer H.

Exercise. Show that the group of symmetries of a G action permutes transitively orbits of the same type.

Suppose that G and X are finite and assume that we have in X, n_i orbits of type $[H_i]$. Then we have, from the partition into orbits, the formula

$$\frac{|X|}{|G|} = \sum_i \frac{n_i}{|H_i|},$$

where we denote by $|A|$ the cardinality of a finite set A.

The next exercise is a challenge to the reader who is already familiar with these notions.

Exercise. Let G be a group with $p^m n$ elements, p a prime number not dividing n. Deduce the theorems of Sylow by considering the action of G by left multiplication on the set of all subsets of G with p^m elements ([Wie]).

Exercise. Given two subgroups H, K of G, describe the orbits of H acting on G/K. In particular, give a criterion for G/K to be a single H-orbit. Discuss the special case $[G : H] = 2$.

2.3 Invariants

From the elements of X, we may single out those for which the stabilizer is the full group G. These are the *fixed points* of the action or *invariant points*, i.e., the points whose orbit consists of the point alone.

These points will usually be denoted by X^G.

$$X^G := \{\textit{fixed points} \text{ or } \textit{invariant points}\}.$$

We have thus introduced in a very general sense the notion of *invariant*. Its full meaning for the moment is completely obscure; we must first proceed with the formal theory.

2.4 Basic Constructions

One of the main features of set theory is the fact that it allows us to perform constructions. Out of given sets we construct new ones. This is also the case of G-sets. Let us point out at least two constructions:

(1) Given two G-sets X, Y, we give the structure of a G-set to their disjoint sum $X \sqcup Y$ by acting separately on the two sets and to their product $X \times Y$ by

$$g(x, y) := (gx, gy), \tag{2.4.1}$$

(i.e., once the group acts on the elements it acts also on the pairs.)

(2) Consider now the set Y^X of all maps from X to Y. We can act with G (verify this) by setting

$$(gf)(x) := gf(g^{-1}x). \tag{2.4.2}$$

Notice that in the second definition we have used the action of G twice. The particular formula given is justified by the fact that it is really the only way to get a group action using the two actions.

Formula 2.4.2 reflects a general fact well known in category theory: maps between two objects X, Y are a covariant functor in Y and a contravariant functor in X.

We want to immediately make explicit a rather important consequence of our formalism:

Proposition. *A map $f : X \to Y$ between two G-sets is equivariant (cf. 1.2) if and only if it is a fixed point under the G-action on the maps.*

Proof. This statement is really a tautology, but nevertheless it deserves to be clearly understood. The proof is trivial following the definitions. Equivariance means that $f(gx) = gf(x)$. If we substitute x with $g^{-1}x$, this reads $f(x) = gf(g^{-1}x)$, which, in functional language means that the function f equals the function gf, i.e., it is invariant. □

Exercises.

(i) Show that the orbits of G acting on $G/H \times G/K$ are in canonical 1-1 correspondence with the double cosets HgK of G.

(ii) Given a G equivariant map $\pi : X \to G/H$ show that:

  (a) $\pi^{-1}(H)$ is stable under the action of H.

  (b) The set of G orbits of X is in 1-1 correspondence with the H-orbits of $\pi^{-1}(H)$.

  (c) Study the case in which $X = G/K$ is also homogeneous.

2.5 Permutation Representations

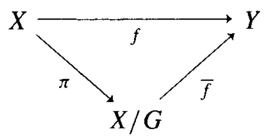
We will often consider a special case of the previous section, the case of the trivial action of G on Y. In this case of course the action of G on the functions is simply

$$ {}^{g}f(x) = (gf)(x) = f(g^{-1}x). \tag{2.5.1} $$

Often we write ${}^{g}f$ instead of gf for the function $f(g^{-1}x)$. A mapping is equivariant if and only if it is constant on the orbits. In this case we will always speak of an *invariant function*. In view of the particular role of this idea in our treatment, we repeat the formal definition.

Definition 1. A function f on a G-set X is called *invariant* if $f(g^{-1}x) = f(x)$ for all $x \in X$ and $g \in G$.

As we have just remarked, a function is invariant if and only if it is constant on the orbits. Formally we may thus say that the quotient mapping $\pi := X \to X/G$ is an invariant map and any other invariant function factors as



We want to make explicit the previous remark in a case of importance.

Let X be a finite G-set. Consider a field F (a ring would suffice) and the set F^X of functions on X with values in F.

An element $x \in X$ can be identified with the characteristic function of $\{x\}$. In this way X becomes a basis of F^X as a vector space.

The induced group action of G on F^X is by linear transformations which permute the basis elements.

F^X is called a *permutation representation,* and we will see its role in the next sections. Since a function is invariant if and only if it is constant on orbits we deduce:

Proposition. *The invariants of G on F^X form the subspace of F^X having as a basis the characteristic functions of the orbits.*

In other words given an orbit $\mathcal{O}$ consider $u_{\mathcal{O}} := \sum_{x \in \mathcal{O}} x$. The elements $u_{\mathcal{O}}$ form a basis of $(F^X)^G$.

We finish this section with two examples which will be useful in the theory of symmetric functions.

Consider the set $\{1, 2, \ldots, n\}$ with its canonical action of the symmetric group S_n. The maps from $\{1, 2, \ldots, n\}$ to the field $\mathbb{R}$ of real numbers form the standard vector space $\mathbb{R}^n$. The symmetric group acts by permuting the coordinates, and in every orbit there is a unique vector $(a_1, a_2, \ldots, a_n)$ with $a_1 \geq a_2 \geq \cdots \geq a_n$.

The set of these vectors can thus be identified with the orbit space. It is a convex cone with boundary, comprising the elements in which at least two coordinates are equal.

Exercise. Discuss the orbit types of the previous example.

Definition 2. A function $M : \{1, 2, \ldots, n\} \to \mathbb{N}$ (to the natural numbers) is called a *monomial.* The set of monomials is a semigroup by the addition of values, and we indicate by x_i the monomial which is the characteristic function of $\{i\}$.

As we have already seen, the symmetric group acts on these functions by $(\sigma f)(k) := f(\sigma^{-1}(k))$, and the action is compatible with the addition. Moreover $\sigma(x_i) = x_{\sigma(i)}$.

Remark. It is customary to write the semigroup law of monomials multiplicatively. Given a monomial M such that $M(i) = h_i$, we have $M = x_1^{h_1} x_2^{h_2} \cdots x_n^{h_n}$. The number $\sum_i h_i$ is the *degree* of the monomial.

Representing a monomial M as a vector $(h_1, h_2, \ldots, h_n)$, we see that every monomial of degree d is equivalent, under the symmetric group, to a unique vector in which the coordinates are non-increasing. The nonzero coordinates of such a vector thus form a partition $\lambda(M) \vdash d$, with at most n parts, of the degree of the monomial.

The permutation representation associated to the monomials with coefficients in a commutative ring F is the *polynomial ring* $F[x_1, \ldots, x_n]$ in the given variables.

The invariant elements are called *symmetric polynomials.*

From what we have proved, a basis of these symmetric polynomials is given by the sums

$$m_\lambda := \sum_{\lambda(M)=\lambda} M$$

of monomials with exponents the integers h_i of the partition λ. m_λ is called a *monomial symmetric function.*

Exercise. To a monomial M we can also associate a partition of the set $\{1, 2, \dots, n\}$ by the equivalence $i \cong j$ iff $M(i) = M(j)$. Show that the stabilizer of M is the group of permutations which preserve the sets of the partition (cf. 1.1). If F is a field of characteristic 0, given M with $\lambda(M) = \lambda = \{h_1, h_2, \dots, h_n\}$, we have

$$m_\lambda = \frac{1}{\prod_i h_i!} \sum_{\sigma \in S_n} \sigma(M).$$

2.6 Invariant Functions

It is time to develop some other examples. First, consider the set $\{1, \dots, n\}$ and a ring A (in most applications A will be the integers or the real or complex numbers).

A function f from $\{1, \dots, n\}$ to A may be thought of as a vector, and displayed, for instance, as a row with the notation $(a_1, a_2, \dots, a_n)$ where $a_i := f(i)$. The set of all functions is thus denoted by A^n. The symmetric group acts on such functions according to the general formula 2.5.1:

$$\sigma(a_1, a_2, \dots, a_n) = (a_{\sigma^{-1}1}, a_{\sigma^{-1}2}, \dots, a_{\sigma^{-1}n}).$$

In this simple example, we already see that the group action is linear. We will refer to this action as the *standard permutation action*.

We remark that if $\underline{e}_i$ denotes the canonical basis vector with coordinates 0 except 1 in the i^{th} position, we have $\sigma(\underline{e}_i) = \underline{e}_{\sigma(i)}$. This formula allows us to describe the matrix of σ in the given basis: it is the matrix $\delta_{\sigma^{-1}(j),i}$. These matrices are called *permutation matrices*.

If we consider a G-set X and a ring A, the set of functions on X with values in A also forms a ring under pointwise sum and multiplication, and we have:

Remark. The group G acts on the functions with values in A as a group of ring automorphisms.

In this particular example it is important to proceed further. Once we have the action of S_n on A^n we may continue and act on the functions on A^n! In fact let us consider the *coordinate functions*: $x_i : (a_1, a_2, \dots, a_n) \to a_i$. It is clear from the general formulas that the symmetric group permutes the coordinate functions and $\sigma(x_i) = x_{\sigma(i)}$. The reader may note the fact that the inverse has now disappeared.

If we have a ring R and an action of a group G on R as ring automorphisms it is clear that:

Proposition. *The invariant elements form a subring of R.*

Thus we can speak of *the ring of invariants* R^G.

2.7 Commuting Actions

We need another generality. Suppose that we have two group actions on the same set X, i.e., assume that we have two groups G and H acting on the same set X.

We say that the two actions commute if $gh(x) = hg(x)$ for all $x \in X$, $g \in G$ and $h \in H$.

This means that every element of G gives rise to an H equivariant map (or we can reverse the roles of G and H). It also means that we really have an action of the product group $G \times H$ on X given by $(g, h)x = ghx$.

In this case, we easily see that if a function f is G-invariant and $h \in H$, then hf is also G-invariant. Hence H acts on the set of G-invariant functions.

More generally, suppose that we are given a G action on X and a normal subgroup K of G. It is easily seen that the quotient group G/K acts on the set of K-invariant functions and a function is G-invariant if and only if it is K and G/K-invariant.

Example. The right and left actions of G on itself commute (Example 1.2c).

3 Linear Actions, Groups of Automorphisms, Commuting Groups

3.1 Linear Actions

In §2.5, given an action of a group G on a set X and a field F, we deduced an action over the set F^X of functions from X to F, which is linear, i.e., given by linear operators.

In general, the groups G and the sets X on which they act may have further structures, as in the case of a topological, or differentiable, or algebraic action. In these cases it will be important to restrict the set of functions to the ones compatible with the structure under consideration. We will do it systematically.

If X is finite, the vector space of functions on X with values in F has, as a possible basis, the characteristic functions of the elements. It is convenient to identify an element x with its characteristic function and thus say that our vector space has X as a basis (cf. §2.5).

A function f is thus written as $\sum_{x \in X} f(x)x$. The linear action of G on F^X induces on this basis the action from which we started. We call such an action a *permutation representation*.

In the algebraic theory we may in any case consider the set of all functions which are finite sums of the characteristic functions of points, i.e., the functions which are 0 outside a finite set.

These are usually called *functions with finite support*. We will often denote these functions by the symbol $F[X]$, which is supposed to remind us that its elements are linear combinations of elements of X.

In particular, for the left action of G on itself we have the *algebraic regular representation* of G on $F[G]$. We shall see that this representation is particularly important.

Let us stress a feature of this representation.

We have two actions of G on G, the left and the right action, which commute with each other. In other words we have an action of $G \times G$ on G, given by $(h, k)g = hgk^{-1}$ (for which $G = G \times G/\Delta$ where $\Delta = G$ embedded diagonally; cf. 1.2c and 2.2).

Thus we have the corresponding two actions on $F[G]$ by $(h, k)f(g) = f(h^{-1}gk)$ and we may view the right action as symmetries of the left action and conversely. Sometimes it is convenient to write ${}^h f^k = (h, k)f$ to stress the left and right actions.

After these basic examples we give a general definition:

Definition 1. Given a vector space V over a field F (or more generally a module), we say that an action of a group G on V is linear if every element of G induces a linear transformation on V. A linear action of a group is also called a *linear representation*;[2] a vector space V that has a G-action is called a *G-module*.

In different language, let us consider the set of all linear invertible transformations of V. This is a group under composition (i.e., it is a subgroup of the group of all invertible transformations) and will be called the *general linear group* of V, denoted by the symbol $GL(V)$.

If we take $V = F^n$ (or equivalently, if V is finite dimensional and we identify V with F^n by choosing a basis), we can identify $GL(V)$ with the group of $n \times n$ invertible matrices with coefficients in F, denoted by $GL(n, F)$.

According to our general principles, a linear action is thus a homomorphism ϱ from G to $GL(V)$ (or to $GL(n, F)$).

When we are dealing with linear representations we usually also consider equivariant linear maps between them, thus obtaining a category and a notion of isomorphism.

Exercise. Two linear representations $\rho_1, \rho_2 : G \to GL(n, F)$ are isomorphic if and only if there is an invertible matrix $X \in GL(n, F)$ such that $X\rho_1(g)X^{-1} = \rho_2(g)$ for all $g \in G$.

Before we proceed any further, we should remark on an important feature of the theory.

Given two linear representations U, V, we can form their direct sum $U \oplus V$, which is a representation by setting $g(u, v) = (gu, gv)$. If $X = A \sqcup B$ is a G-set, where A and B are two disjoint G stable subsets, we clearly have $F^{A \sqcup B} = F^A \oplus F^B$. Thus the decomposition into a direct sum is a generalization of the decomposition of a space into G-stable sets.

If X is an orbit it cannot be further decomposed as a set, while F^X might be decomposable. The simplest example is $G = \{1, \tau = (12)\}$ the group with two elements of permutations of $[1, 2]$. The space F^X decomposes (char$F \neq 2$), setting

[2] Sometimes we drop the term *linear* and just speak of *a representation.*

$$u_1 := \frac{e_1 + e_2}{2}, \quad u_2 := \frac{e_1 - e_2}{2};$$

we have $\tau u_1 = u_1,\ \tau(u_2) = -u_2$.

We have implicitly used the following ideas:

Definition 2.

(i) Given a linear representation V, a subspace U of V is a *subrepresentation* if it is stable under G.
(ii) V is a *decomposable representation* if we can find a decomposition $V = U_1 \oplus U_2$ with the U_i proper subrepresentations. Otherwise it is called *indecomposable.*
(iii) V is an *irreducible* representation if the only subrepresentations of V are V and 0.

We will study in detail some of the deep connections between these notions.

We will stress in a moment the analogy with the abstract theory of modules over a ring A. First we consider two basic examples:

Example. Let A be the group of all invertible $n \times n$ matrices over a field F.

Consider B^+ and B^-, the subgroups of all upper (resp., lower) triangular invertible matrices. Here "upper triangular" means "with 0 below the diagonal."

Exercise. The vector space F^n is irreducible as an A module, indecomposable but not irreducible as a B^+ or B^- module.

Definition 3. Given two linear representations U, V of a group G, the space of G-equivariant linear maps is denoted by $\hom_G(U, V)$ and called the space of *intertwining* operators.

In this book we will almost always treat finite-dimensional representations. Thus, unless specified otherwise, our vector spaces will always be assumed to be finite dimensional.

3.2 The Group Algebra

It is quite useful to rephrase the theory of linear representations in a different way. Consider the space $F[G]$:

Theorem.

(i) The group multiplication extends to a bilinear product on $F[G]$ under which $F[G]$ is an associative algebra with 1 called ***the group algebra.***
(ii) Linear representations of G are the same as $F[G]$-modules.

Proof. The first part is immediate. As for the second, given a linear representation of G we have the module action $\left(\sum_{g\in G} a_g g\right)v := \sum_{g\in G} a_g(gv)$. The converse is clear. □

It is useful to view the product of elements $a, b \in F[G]$ as a *convolution of functions*:

$$(ab)(g) = \sum_{h,k \in G \,|\, hk=g} a(h)b(k) = \sum_{h \in G} a(h)b(h^{-1}g) = \sum_{h \in G} a(gh)b(h^{-1}).$$

Remark. Convolution can also be defined for special classes of functions on infinite groups which do not have finite support. One such extension comes from functional analysis and it applies to L^1-functions on locally compact groups endowed with a Haar measure (Chapter 8). Another extension comes in the theory of reductive algebraic groups (cf. Chapter 7).

Remark. (1) Consider the left and right action on the functions $F[G]$.

Let $h, k, g \in G$ and identify g with the characteristic function of the set $\{g\}$. Then ${}^hg^k = hgk^{-1}$ (as functions).

The space $F[G]$ as a $G \times G$ module is the permutation representation associated to $G = G \times G/\Delta$ with its $G \times G$ action (cf. 2.2 and 3.1). Thus a space of functions on G is stable under left (resp. right) action if and only if it is a left (resp. right) ideal of the group algebra $F[G]$.

(2) Notice that the direct sum of representations is the same as the direct sum as modules. Also a G-linear map between two representations is the same as a module homomorphism.

Example. Let us consider a finite group G, a subgroup K and the linear space $F[G/K]$, which as we have seen is a permutation representation.

We can identify the functions on G/K with the functions

$$F[G]^K = \{a \in F[G] | ah = a, \ \forall h \in K\} \tag{3.2.1}$$

on G which are invariant under the right action of K. In this way the element $gK \in G/K$ is identified with the characteristic function of the coset gK, and $F[G/K]$ is identified with the left ideal of the group algebra $F[G]$ having as basis the characteristic functions χ_{gK} of the left cosets of K.

If we denote by $u := \chi_K$ the characteristic function of the subgroup K, we see that $\chi_{gK} = gu$ and that u generates this module over $F[G]$.

Given two subgroups H, K and the linear spaces $F[G/H], F[G/K] \subset F[G]$, we want to determine their intertwiners. We assume char $F = 0$.

For an intertwiner f, and $u := \chi_H$ as before, let $f(u) = a \in F[G/K]$. We have $hu = u, \ \forall h \in H$ and so, since f is an intertwiner, $a = f(u) = f(hu) = ha$. Thus we must have that a is also left invariant under H. Conversely, given such an a, the map $b \mapsto \frac{ba}{|H|}$ is an intertwiner mapping u to a. Since u generates $F[G/H]$ as a module we see that:

Proposition. *The space* $\hom_G(F[G/H], F[G/K])$ *of intertwiners can be identified with the (left) H-invariants of $F[G/K]$, or with the H-K invariants ${}^HF[G]^K$ of $F[G]$. It has as basis the characteristic functions of the double cosets HgK.*

In particular, for $H = K$ we have that the functions which are biinvariants under H form under convolution the endomorphism algebra of $F[G/H]$. Since we identify $F[G/H]$ with a subspace of $F[G]$, the claim is that multiplication on the left by a function that is biinvariant under H maps $F[G/H]$ into itself and identifies this space of functions with the full algebra of endomorphisms of $F[G/H]$.

These functions have as basis the characteristic functions of the double cosets HgH; one usually indicates by $T_g = T_{HgH}$ the corresponding operator. $\mathrm{End}(F[G/H])$ and T_g are called the *Hecke algebra* and *Hecke operators*, respectively. The multiplication rule between such operators depends on the multiplication on cosets $HgHHkH = \cup Hh_iH$, and each double coset appearing in this product appears with a positive integer multiplicity so that $T_gT_h = \sum n_i T_{h_i}$.[3]

There are similar results when we have three subgroups H, K, L and compose

$$\hom_G(F[G/H], F[G/K]) \times \hom_G(F[G/K], F[G/L]) \xrightarrow{\circ} \hom_G(F[G/H], F[G/L]).$$

The notion of permutation representation is a special case of that of *induced representation.* If M is a representation of a subgroup H of a group G we consider the space of functions $f : G \to M$ with the constraint:

$$\mathrm{Ind}_H^G M := \{f : G \to M | f(gh^{-1}) = hf(g), \forall h \in H, g \in G\}. \tag{3.2.2}$$

On this space of functions we define a G-action by $(gf)(x) := f(g^{-1}x)$. It is easy to see that this is a well-defined action. Moreover, we can identify $m \in M$ with the function f_m such that $f_m(x) = 0$ if $x \notin H$ and $f_m(h) = h^{-1}m$ if $h \in H$. Now $M \subset \mathrm{Ind}_H^G M$.

Exercise. Verify that by choosing a set of representatives of the cosets G/H, we have the vector space decomposition

$$\mathrm{Ind}_H^G M := \oplus_{g \in G/H}\, gM. \tag{3.2.3}$$

3.3 Actions on Polynomials

Let V be a G-module. Given a linear function $f \in V^*$ on V, by definition the function gf is given by $(gf)(v) = f(g^{-1}v)$ and hence it is again a linear function.

Thus G acts dually on the space V^* of linear functions. It is clear that this is a linear action, which is called the *contragredient* action.

In matrix notation, using dual bases, the contragredient action of an operator T is given by the inverse transpose of the matrix of T.

[3] It is important in fact to use these concepts in a much more general way as done by Hecke in the theory of modular forms. Hecke studies the action of $Sl(2, Z)$ on $M_2(Q)$ the 2×2 rational matrices. In this case one has also double cosets, a product structure on $M_2(Q)$ and the fact that a double coset is a finite union of right or left cosets. These properties suffice to develop the Hecke algebra. In this case this algebra acts on a different space of functions, the modular forms (cf. [Ogg]).

We will use the notation $\langle\varphi|v\rangle$ for the value of a linear form on a vector, and thus we have (by definition) the identity

$$\langle g\varphi|v\rangle = \langle\varphi|g^{-1}v\rangle. \tag{3.3.1}$$

Alternatively, it may be convenient to define on V^* a *right action* by the more symmetric formula

$$\langle\varphi g|v\rangle = \langle\varphi|gv\rangle. \tag{3.3.2}$$

Exercise. Prove that the dual of a permutation representation is isomorphic to the same permutation representation. In particular, one can apply this to the dual of the group algebra.

In the set of all functions on a finite-dimensional vector space V, the polynomial functions play a special role. By definition a polynomial function is an element of the subalgebra (of the algebra of all functions with values in F) generated by the linear functions.

If we choose a basis and consider the coordinate functions $x_1, x_2, \dots, x_n$ with respect to the chosen basis, a polynomial function is a usual polynomial in the x_i. If F is infinite, the expression as a polynomial is unique and we can consider the x_i as given variables.

The ring of polynomial functions on V will be denoted by $P[V]$ and the ring of formal polynomials by $F[x_1, x_2, \dots, x_n]$.

Choosing a basis, we always have a surjective homomorphism $F[x_1, x_2, \dots, x_n] \to P[V]$ which is an isomorphism if F is infinite.

Exercise. If F is a finite field with q elements, prove that $P[V]$ has dimension q^n over F, and that the kernel of the map $F[x_1, x_2, \dots, x_n] \to P[V]$ is the ideal generated by the elements $x_i^q - x_i$.

Since the linear functions are preserved under a given group action we have:

Proposition. *Given a linear action of a group G on a vector space V, G acts on the polynomial functions $P[V]$ as a group of ring automorphisms by the rule $(gf)(v) = f(g^{-1}v)$.*

Of course, the full linear group acts on the polynomial functions. In the language of coordinates we may view the action as a linear change of coordinates.

Exercise. Show that we always have a linear action of $GL(n, F)$ on the formal polynomial ring $F[x_1, x_2, \dots, x_n]$.

3.4 Invariant Polynomials

We assume the base field to be infinite for simplicity although the reader can see easily what happens for finite fields. One trivial but important remark is that the group action on $P[V]$ preserves the degree.

Recall that a function f on V is *homogeneous of degree* k if $f(\alpha v) = \alpha^k f(v)$ for all α and v.

The set $P_q[V]$ of homogeneous polynomials of degree q is a subspace, called in classical language the space of *quantics*. If $\dim(V) = n$, one speaks of n-*ary* quantics.[4]

In general, a direct sum of vector spaces $U = \oplus_{k=0}^{\infty} U_k$ is called a *graded vector space*. A subspace W of U is called *homogeneous*, if, setting $W_i := W \cap U_i$, we have $W = \oplus_{k=0}^{\infty} W_k$.

The space of polynomials is thus a graded vector space $P[V] = \oplus_{k=0}^{\infty} P_k[V]$. One has immediately $(gf)(\alpha v) = f(\alpha g^{-1} v) = \alpha^k (gf)(v)$, which has an important consequence:

Theorem. *If a polynomial f is an invariant (under some linear group action), then its homogeneous components are also invariant.*

Proof. Let $f = \sum f_i$ be the decomposition of f into homogeneous components, $gf = \sum gf_i$ is the decomposition into homogeneous components of gf. If f is invariant $f = gf$, then $f_i = gf_i$ for each i since the decomposition into homogeneous components is unique. □

In order to summarize the analysis done up to now, let us also recall that an algebra A is called a *graded algebra* if it is a graded vector space, $A = \oplus_{k=0}^{\infty} A_k$ and if for all h, k we have $A_h A_k \subset A_{h+k}$.[5]

Proposition. *The spaces $P_k[V]$ are subrepresentations. The set $P[V]^G$ of invariant polynomials is a graded subalgebra.*

3.5 Commuting Linear Actions

To some extent the previous theorem may be viewed as a special case of the more general setting of commuting actions.

Given two representations $\varrho_i : G \to GL(V_i)$, $i = 1, 2$, consider the linear transformations between V_1 and V_2 which are G equivariant. It is clear that they form a linear subspace of the space of all linear maps between V_1 and V_2.

The space of all linear maps will be denoted by $\hom(V_1, V_2)$, while the space of equivariant maps will be denoted by $\hom_G(V_1, V_2)$. In particular, when the two spaces coincide we write $\mathrm{End}(V)$ or $\mathrm{End}_G(V)$ instead of $\hom(V, V)$ or $\hom_G(V, V)$.

These spaces $\mathrm{End}_G(V) \subset \mathrm{End}(V)$ are in fact now algebras, under composition of operators. Choosing bases we have that $\mathrm{End}_G(V)$ is the set of all matrices which commute with all the matrices coming from the group G.

Consider now the set of invertible elements of $\mathrm{End}_G(V)$, i.e., the group H of all linear operators which commute with G.

By the remarks of §3.3, H preserves the degrees of the polynomials and maps the algebra of G-invariant functions into itself. Thus we have:

---

[4] E.g., quadratics, cubics, quartics, quintics, etc., $q = 2, 3, 4, 5, \ldots$.

[5] We are restricting to $\mathbb{N}$ gradings. The notion is more general: any monoid could be used as a set of indices for the grading. In this book we will use only $\mathbb{N}$ and $\mathbb{Z}/(2)$ in Chapter 5.

Remark. H induces a group of automorphisms of the graded algebra $P[V]^G$.

We view this remark as a generalization of Theorem 3.4 since the group of scalar multiplications commutes (by definition of linear transformation) with all linear operators. Moreover it is easy to prove:

Exercise. Given a graded vector space $U = \oplus_{k=0}^{\infty} U_k$, define an action ϱ of the multiplicative group F^* of F setting $\varrho(\alpha)(v) := \alpha^k v$ if $v \in U_k$. Prove that a subspace is stable under this action if and only if it is a graded subspace (F is assumed to be infinite).