RELATIVISTIC THEORY OF REACTIONS

(Model Independent Methods)

by

J. WERLE

Professor of Theoretical Physics,
Institute for Nuclear Research,
University of Warsaw

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM

PWN—POLISH SCIENTIFIC PUBLISHERS
WARSZAWA
1966

CHAPTER II

GROUPS AND GROUP REPRESENTATIONS

This chapter contains a short general introduction to the theory of groups and their representations and a somewhat more comprehensive review of several special groups which are of particular interest for the quantum theory of reactions. These are the rotation, Poincaré, SU_3 and permutation groups. The first aim of this chapter is to acquaint the reader with the basic notions and theorems that will be needed in the theory of reactions. Furthermore, the present chapter is meant as a source of many more specific formulae to which we shall refer the reader very frequently in the subsequent chapters. We shall rather state and explain the contents of the theorems, omitting the proofs completely or indicating them only if they are essential for a better understanding of their physical implications. A reader who is interested in mathematical proofs may find them in the special literature on the theory of groups listed at the end of this chapter. However, in the later sections of this chapter, when we come nearer to the physical applications of special groups, several proofs that seem to be more interesting for a physicist, or simpler than usual, are indicated. In this way we hope to achieve a better understanding of the group theoretical methods without unduly expanding this part of the book.

4. Elements of abstract group theory

A set G is called a *group* if its elements satisfy the following conditions:

a) A composition rule called *group multiplication* is defined for any two elements of G taken in definite order. The result of this multiplication is again an element of the set G. I.e., if $f \in G$ and $g \in G$ then $fg = h \in G$, too.

b) The group multiplication is associative, i.e.,

$$(fg)j = f(gj). \tag{4.1}$$

c) The set G contains a left unit element e defined by the condition that for all $g \in G$

$$eg = g. \tag{4.2}$$

d) To any element $g \in G$ there exists in G an element g^{-1} called its left inverse which satisfies

$$g^{-1} g = e. \tag{4.3}$$

It follows from the above group axioms that the right unit element is equal to the left unit element, i.e., $ge = eg = g$, and that a group contains only one unit element. Furthermore, the right inverse is equal to the left one, i.e., $gg^{-1} = g^{-1}g$, and to any $g \in G$ there exists in G only one inverse g^{-1}.

Group multiplication can be non-commutative, i.e. for some elements f, $g \in G$ we can have $fg \neq gf$. If for any f, $g \in G$ we always have $fg = gf$, the group G is called *commutative* or *Abelian*. Equality (inequality) of two group elements implies equality (inequality) of their right or left products by an arbitrary element of the group and vice versa. If g runs over all the elements of G, then the product fg or gf of g by a fixed $f \in G$ does the same but in a different order.

In the following we shall be interested only in *transformation groups*. In that case group multiplication means the successive application of two transformations. The unit element e is then the identity transformation, and the inverse g^{-1} of g is the transformation which exactly cancels the effect of g. If the transformations are one-to-one their inverses are unique.

A group consisting of a finite number N of elements is called *finite of order N*. *Infinite* groups may be countable or uncountable. Among the latter ones the *continuous parameter groups* and in particular the *Lie groups* are of greatest importance. The elements of a Lie group can be specified uniquely by a finite number k of real continuously varying parameters $\alpha_1, \ldots, \alpha_k$. In other words the elements of a Lie group are unique functions of k real variables $g = g(\alpha_1, \ldots, \alpha_k)$. Of course, the functions $g(\alpha_i)$ must satisfy certain continuity and analyticity conditions which will be discussed in detail in Sec. 10.

Group theory is studying the consequences of postulating the existence of an operation of multiplication between the elements of a set. The group properties of a set are fixed if we know the result of multiplication for each ordered pair of its elements. In the case of a finite group all this information can be collected in the *multiplication table* of the group, that is a transparent way of writing N^2 equations

$$g_i g_j = g_k, \quad i, j = 1, \ldots, N, \tag{4.4}$$

which specify the results of all possible products.

A subset G' of a group G is said to be a *subgroup* of G if its elements satisfy all the group axioms with respect to the same composition rule. A subgroup of G is said to be *proper* if it is different from the group G itself and the unit element alone, which are trivial subgroups of G. The set consisting of all distinct positive and negative powers of an arbitrary element $g \in G$

$$\ldots, g^{-m}, \ldots g^{-1}, e, g, \ldots, g^{m}, \ldots \tag{4.5}$$

is an Abelian group which is called the *cyclic subgroup* of G with the *generator* g. In the case of a finite cyclic group one can express all its elements in terms of positive powers of g:

$$e, g, \ldots, g^{l-1}, \tag{4.5'}$$

where the order l of the group (4.5') is the lowest positive integer for which $g^l = e$. The number l is frequently called the *period* of the element g. A group G may contain many different cyclic subgroups. Certain elements $a_1, \ldots, a_m$ of a discrete (i.e. finite or infinite countable) group G are called generators of the group G if the set of all distinct products of their powers coincides with G. In order to specify which of these products are in fact distinct, one must state a number of relations between the generators which are of the form $g_k(a_1, \ldots a_m) = e$, $(k = 1, \ldots, s)$. A set of s such relations which imply the group multiplication table is called the set of *defining relations* for the considered group. The choice of generators and defining relations for a given group is, in general, not unique. In practice we are interested in a minimal set of generators and the simplest possible set of defining relations. The use of generators makes it possible to write down all the group properties in a very compact form which is much more economic than that given by the N^2 equations of the form (4.4) or the group multiplication table. Most group properties can be conveniently studied and formulated in terms of generators. It is interesting to note that somewhat similar concepts of generators of cyclic subgroups, minimal sets of generators, defining relations etc. can be introduced for the continuous groups, too (see Sec. 10).

Example: Consider the group of all permutations of n objects frequently called the symmetric group and denoted by the symbol S_n. It is a non-Abelian (for $n > 2$) group of order $n!$. As an example we shall discuss here the group S_3 with the following six elements

$$e = \begin{pmatrix}123\\123\end{pmatrix},\ g_1 = \begin{pmatrix}123\\231\end{pmatrix},\ g_2 = \begin{pmatrix}123\\312\end{pmatrix},\ g_3 = \begin{pmatrix}123\\132\end{pmatrix},\ g_4 = \begin{pmatrix}123\\213\end{pmatrix},\ g_5 = \begin{pmatrix}123\\321\end{pmatrix}, \tag{4.6}$$

and the multiplication table

	e	g_1	g_2	g_3	g_4	g_5
e	e	g_1	g_2	g_3	g_4	g_5
g_1	g_1	g_2	e	g_4	g_5	g_3
g_2	g_2	e	g_1	g_5	g_3	g_4
g_3	g_3	g_5	g_4	e	g_2	g_1
g_4	g_4	g_3	g_5	g_1	e	g_2
g_5	g_5	g_4	g_3	g_2	g_1	e

(4.7)

We can choose $g_1 = a$, and $g_3 = b$ as two independent generators with the following defining relations

$$a^3 = b^2 = baba = e. \tag{4.8}$$

It can easily be checked that these defining relations imply the existence of only six different products of the form $a^n b^m$ or $b^n a^m$. Setting

$$g_1 = a,\ g_2 = a^2,\ g_3 = b,\ g_4 = ab,\ g_5 = a^2 b \tag{4.9}$$

and taking account of (4.8) we obtain the multiplication table (4.7). Thus we see that the set of defining relations (4.8) is equivalent to the 36 relations of the type (4.4) which are collected in the group multiplication table (4.7) of the group S_3.

Let H be a proper subgroup of G and g an arbitrary element of G. The sets gH and Hg, with fixed $g \in G$, are called *left and right cosets* of H. Two left cosets $g_i H$ and $g_k H$ (or two right cosets Hg_i and Hg_k) of the same subgroup H contain either exactly the same elements of G or have no common elements at all. Taking all different left (or right) cosets of H we can decompose the group G into the sum

$$G = eH + g_1 H + \ldots + g_{\nu-1} H, \tag{4.10}$$

where $g_1 \in G$, $g_1 \notin H$, $g_2 \in G$, $g_2 \notin H$, $g_2 \notin g_1 H$ and so on. The number ν is called the *index* of H in G. In the case of a finite group G of order N and a subgroup H of order n the number ν of different cosets of H is finite. Since each coset contains n different elements of G, it follows that the order n of H must be a divisor of the order N of G, i.e., $N = \nu n$.

Two elements $g, h \in G$ are said to be mutually *conjugate* if there exists such an element $a \in G$ that

$$h = aga^{-1}. \tag{4.11}$$

The set K_g of all elements of G which are conjugate to g is called the *class* of elements conjugate to g. Taking another element $f \in G$, but $f \notin K_g$, we

can find another class K_f which has no elements in common with K_g. Continuing this procedure we can divide all the group elements into separate classes so that every element of G appears once, and only once, in any one of the classes. The unit element of any group forms a class by itself. Therefore, no other class can contain the unit element. In an Abelian group each class contains only one element, since $ghg^{-1} = hgg^{-1} = h$.

The operation of conjugation does not change the multiplication table, since $g_i g_k = g_h$ implies $ag_i a^{-1} ag_k a^{-1} = ag_i g_k a^{-1} = ag_h a^{-1}$. Therefore, if a set H with elements h is a subgroup of G then the set $H' = gHg^{-1}$ with elements ghg^{-1} is another subgroup of G, with the same multiplication table, which is called conjugate to H. If for arbitrary $g \in G$ all the conjugate subgroups gHg^{-1} are identical (i.e., contain the same elements)

$$gHg^{-1} = H, \tag{4.12}$$

we call H an *invariant* or *normal subgroup*. The left and right cosets gH and Hg of a normal subgroup are identical: $gH = Hg$. A normal subgroup H of G consists of whole undivided classes of G. A subgroup of index two is always a normal subgroup. Groups which contain no proper normal subgroups are said to be *simple*. Groups which contain no proper, normal, Abelian subgroups are said to be *semisimple*.

Consider the products of an element of the coset gH by an element of the coset fH where H is a normal subgroup of G. All such products belong to the coset gfH. Hence, we can define a new type of multiplication of cosets

$$(gH)(fH) = (gfH). \tag{4.13}$$

The set of all different cosets of a normal subgroup H is a group with respect to this multiplication law. This so-called *quotient* (or *factor*) group F is not a subgroup of G as its elements are whole sets (cosets). The unit element of F is the normal subgroup H itself. The inverse of the coset gH is $g^{-1}H$. We write symbolically

$$F = G/H. \tag{4.14}$$

A one-to-one correspondence between elements of two groups $G \leftrightarrow F$ is called *isomorphism* if also products correspond to products, i.e., if always

$$g_i \leftrightarrow f_i, \quad g_k \leftrightarrow f_k, \quad g_i g_k \leftrightarrow f_i f_k. \tag{4.15}$$

Two groups between which such a correspondence or mapping can be established are called *isomorphic*. Two isomorphic groups must have the same order and the same multiplication table, and consequently are regarded

as the same abstract group. An isomorphism of a group with itself is called *automorphism*. An example of automorphism, which is called inner, is given by the conjugation $g_i \leftrightarrow ag_i a^{-1}$ with fixed $a \in G$.

A many-to-one correspondence $G \to F$ which preserves products, i.e., for which

$$g_i \to f_i, \quad g_k \to f_k, \quad g_i g_k \to f_i f_k \tag{4.16}$$

is called *homomorphism*. The group G is then said to be a *covering group* for F, or to be *homomorphic* to F. The group F is said to be a *homomorphic image* or *homomorph* of G. Isomorphism is obviously a special case of homomorphism. A homomorphism which is not isomorphism is called proper.

The unit element e of G must correspond in homomorphism to the unit element e' of F. Denote the set of all elements $c_i \in G$ which correspond to the unit element e' of F by the symbol

$$C = (c_1 = e, c_2, \ldots). \tag{4.17}$$

Since in homomorphism $c_i c_j \to e'\, e' = e'$, the set C contains all the products and inverses of the c_i. The set C is thus a subgroup of G and, since

$$gc_i g^{-1} \to fe' f^{-1} = e', \tag{4.18}$$

it is an invariant subgroup of G. Consequently all the elements of G which belong to the same coset gC correspond to the same element f of F. Therefore, only groups possessing invariant subgroups can have proper homomorphic images. Inequivalent cosets spanned on C are, obviously, in one-to-one correspondence with F. In other words, if G has a proper homomorphic image F, then it must contain a proper invariant subgroup C called the *kernel* of homomorphism. The *quotient group* G/C is then isomorphic with F.

Let G' and G'' be two groups. The set G of all pairs $(g'; g'')$, where $g' \in G'$ and $g'' \in G''$, forms a group with respect to the following multiplication rule

$$(g_1'; g_1'')(g_2'; g_2'') = (g_1' g_2'; g_1'' g_2''). \tag{4.19}$$

The group G is called the *direct product* of G' and G'' and denoted by

$$G = G' \otimes G''. \tag{4.20}$$

The unit element of G is $e = (e'; e'')$. It can easily be shown that G' and G'' are isomorphic to the invariant subgroups $G' \otimes e''$ and $e' \otimes G''$ of G which have only the unit element $(e'; e'')$ in common. Every element of $G' \otimes e''$ commutes with every element of $e' \otimes G''$.

On the other hand if a group G contains two invariant subgroups R' and R'' which have only the unit element in common and any element $g \in G$ can be uniquely expressed in the form: $g = r'r''$, with $r' \in R'$ and $r'' \in R''$, then the group G is the direct product $G = R' \otimes R''$. It can easily be shown that under the stated assumptions $r'r'' = r''r'$.

Let A be a group of automorphisms of a group G and denote by $a(g)$ the image of $g \in G$ under the automorphism $a \in A$. Then the *semidirect product* $G \square A$, of G and A, is the group of all ordered pairs $(g; a)$ with the multiplication defined by

$$(g_1; a_1)(g_2; a_2) = (g_1 a_1(g_2); a_1 a_2). \tag{4.21}$$

Consequently $H = G \square A$ implies that G is an invariant (normal) subgroup of H and $H/G = A$.

Suppose that every element h of a group H can be written uniquely in the form $h = ga$ where g and a are suitable elements of two subgroups G and A of H which have only the unit element in common. If G is a normal subgroup of H then A is obviously a group of automorphisms of G and the multiplication law (4.21) is satisfied by the ordinary group multiplication within H: $g_1 a_1 g_2 a_2 = g_1 a_1 g_2 a_1^{-1} a_1 a_2$. Clearly we can regard this as an equivalent but apparently a bit less abstract definition of the semidirect product group.

We shall see in Sec. 13 that the Poincaré group is a semidirect product of the group of translations by the Lorentz group. Another example is the group S_3. Owing to the defining relations (4.8) the cyclic group $C_2 = (e, b)$ is in fact a group of automorphisms of the cyclic group $C_3 = (e, a, a^2)$. Therefore, $S_3 = C_3 \square C_2$.

A function φ is said to be defined on a group G if to each element $g \in G$ a unique complex (or real) number $\varphi(g)$ is assigned. In the case of a finite group of order N we can write any group function $\varphi(g)$ in the form of a column and regard it as a vector in a certain N-dimensional space. If we define

$$|\varphi\rangle = \sum_i \varphi(g_i)|e_i\rangle, \quad \langle\varphi| = \sum_i \overline{\varphi}(g_i)\langle e_i|, \tag{4.22}$$

we can in fact use all the known rules of the vector calculus.

The average of a function $\varphi(g)$ defined on a finite group is given by

$$Av[\varphi(g)] = \frac{1}{N}\sum_{g_i} \varphi(g_i) = \frac{1}{N}\sum_i \langle e_i|\varphi\rangle. \tag{4.23}$$

(and $g_i h$ and g_i)

Since for any fixed $h \in G$ the product hg_i runs over all elements of G, we have

$$\sum_{g_i} \varphi(hg_i) = \sum_{g_i} \varphi(g_i h) = \sum_{g_i} \varphi(g_i). \tag{4.24}$$

Consequently, the average of a function defined on a finite group has the following properties

$$\begin{aligned} &\text{a) } Av[\varphi(g)] = c \text{ if } \varphi(g) = c = \text{const for all } g \in G,\\ &\text{b) } Av[\varphi(g)] \geqslant 0 \text{ if } \varphi(g) \geqslant 0 \quad \text{,, ,, ,, ,}\\ &\text{c) } Av[\varphi(hg)] = Av[\varphi(gh)] = Av[\varphi(g)] \text{ for any fixed } h \in G. \end{aligned} \tag{4.25}$$

The properties of functions defined on infinite groups are much more involved. Since the group space is then infinite dimensional, the scalar product of two bounded group functions ($\langle\psi|\varphi\rangle$) may be infinite. Similarly, the operation of averaging may become meaningless for some groups as it may involve division by an infinite number.

In the case of a continuous k-parameter group $G_{(k)}$ a group function $\varphi(g)$ can be regarded as an ordinary function $\varphi(\alpha_1, \ldots, \alpha_k)$ of k real variables $\alpha_1, \ldots, \alpha_k$ that are necessary for specifying the group elements. Many important theorems on finite groups cannot be extended on arbitrary continuous parameter groups just because it is in general not possible to define the operations of sum and average over the group manifold preserving the properties (4.24) and (4.25) which are essential in many proofs of the theorems in question. However, if we restrict ourselves to compact groups we can fulfil the mentioned requirements. A group is called compact if the group manifold is compact, (see Sec. 1), or equivalently, if any function $\varphi(\alpha_i)$ which is continuous in all points of the group manifold of $G_{(k)}$ is also bounded. In the case of a compact continuous k-parameter group the sum over the group elements is to be replaced by a suitable integral over the group manifold with a properly chosen weight (or density) function $\varrho(\alpha_i)$ which is necessary because of the requirements (4.25). For compact groups the group volume

P. 14 See also Greiner

$$V = \int \varrho(\alpha_1, \ldots, \alpha_k)\, d\alpha_1 \ldots d\alpha_k = \int \varrho(\alpha)\, d\alpha, \tag{4.26}$$

which in (4.23) replaces the number N of group elements, is also finite. Therefore, we can define the average of a group function by the expression

$$Av[\varphi] = \frac{1}{V}\int \varphi(\alpha)\varrho(\alpha)\, d\alpha. \tag{4.27}$$

The scalar product of two group functions $\varphi(\alpha)$ and $\psi(\alpha)$ is then given by the formula

$$\langle\psi|\varphi\rangle = \int \overline{\psi}(\alpha)\varphi(\alpha)\varrho(\alpha)\,d\alpha. \tag{4.28}$$

For the average of the scalar product (4.28) we shall use in the following sections the symbol

$$(\psi|\varphi) = Av[\overline{\psi}(g)\varphi(g)] = \frac{1}{V}\langle\psi|\varphi\rangle. \tag{4.29}$$

Clearly the actual form of the weight function $\varrho(\alpha)$ which fulfils the requirements (4.25), and in particular the invariance requirement (4.25c), can depend on the choice of parameters α. However, the values of the integrals involved in the expressions (4.26–29) must be independent of the adopted parametrization.

5. Group representations

A group of linear operators $T(g)$ which acts in a vector space $\mathfrak{L}$ and is a homomorph of a group G is said to be a *representation* of G in $\mathfrak{L}$. In the following we shall be interested in representations acting in finite or infinite dimensional separable Hilbert spaces.

Since isomorphism is a special case of homomorphism, $T(g)$ can be either an isomorphic (*faithful*) or a non-isomorphic (*unfaithful*) representation of G. A simple group can have only faithful nontrivial representations. Representations of G which are not isomorphic with G are isomorphic or (faithful) representations of the quotient group G/C where C is the kernel of homomorphism $G \to T(g)$.

Apart from ordinary representations for which for any $g, f \in G$

$$T(g)T(f) = T(gf), \tag{5.1}$$

we have to do in quantum physics with representations "*up to a phase factor*" for which

$$T(g)T(f) = \eta(g,f)T(gf), \tag{5.1'}$$

where $\eta(g,f)$ is a numerical factor of modulus one. However, in all cases of physical interest a covering group G' can be found which contains G as an invariant subgroup and has the property that the group of operators T is an ordinary representation of G'.

If the Hilbert space $\mathfrak{H}$ in which the operators $T(g)$ are acting has n dimensions, the representation $T(g)$ is said to be n-dimensional. Any group of arbitrary order can have both finite and infinite dimensional representations.

By a similarity transformation

$$T'(g) = A^{-1}T(g)A \tag{5.2}$$

one can obtain from $T(g)$ another representation $T'(g)$. However, a transformation of this type can always be interpreted as the result of a change of basis in the Hilbert space $\mathfrak{H}$. Since a similarity transformation does not change any algebraic relations between operators, we call the representation $T'(g)$ *equivalent* to $T(g)$. From the class of equivalent representations we can choose the most convenient one which may satisfy some additional requirements.

From two representations $T_1(g)$ and $T_2(g)$ acting in $\mathfrak{H}_1$ and $\mathfrak{H}_2$ another representation $T(g)$ acting in $\mathfrak{H}_1 \oplus \mathfrak{H}_2$ can be formed by taking the direct sum

$$T(g) = T_1(g) \oplus T_2(g), \tag{5.3}$$

or in the matrix form

$$T(g) = \begin{Vmatrix} T_1(g) & 0 \\ 0 & T_2(g) \end{Vmatrix}. \tag{5.4}$$

The action of such a $T(g)$ on any vector

$$|w\rangle \stackrel{\text{def}}{=} |x\rangle + |y\rangle, \quad \text{where } |x\rangle \in \mathfrak{H}_1, \quad |y\rangle \in \mathfrak{H}_2, \tag{5.5}$$

is given by the formula

$$T(g)|w\rangle = T_1(g)|x\rangle + T_2(g)|y\rangle. \tag{5.6}$$

Consider now an arbitrary representation $T(g)$ in some Hilbert space $\mathfrak{H}$. We call $T(g)$ *reducible* if the space $\mathfrak{H}$ contains a proper subspace $\mathfrak{H}_1$ which is invariant under all $T(g)$, i.e., if

$$T(g)|x\rangle = |y\rangle \in \mathfrak{H}_1, \quad \text{for all } |x\rangle \in \mathfrak{H}_1 \text{ and all } g \in G. \tag{5.7}$$

If no such subspace of $\mathfrak{H}$ exists we call $T(g)$ the *irreducible representation* and $\mathfrak{H}$ the *irreducible space*. A reducible representation $T(g)$ induces in the invariant subspace $\mathfrak{H}_1$ a "simpler" representation $T_1(g)$ of the group defined by

$$T(g)|x\rangle = T_1(g)|x\rangle, \quad |x\rangle \in \mathfrak{H}_1. \tag{5.8}$$

In a suitable orthonormal basis in $\mathfrak{H}$ the matrices $T(g)$ then have the form

$$T(g) = \begin{Vmatrix} T_1(g) & R(g) \\ 0 & Q(g) \end{Vmatrix}. \tag{5.9}$$

Quotient group

From Wikipedia, the free encyclopedia

In mathematics, specifically group theory, a **quotient group** (or **factor group**) is a group obtained by aggregating similar elements of a larger group using an equivalence relation. For example, the cyclic group of addition modulo n can be obtained from the integers by identifying elements that differ by a multiple of n and defining a group structure that operates on each such class (known as a congruence class) as a single entity.

In a quotient of a group, the equivalence class of the identity element is always a normal subgroup of the original group, and the other equivalence classes are the cosets of this normal subgroup. The resulting quotient is written G / N, where G is the original group and N is the normal subgroup. (This is pronounced "G mod N," where "mod" is short for modulo.)

Much of the importance of quotient groups is derived from their relation to homomorphisms. The first isomorphism theorem states that the image of any group G under a homomorphism is always isomorphic to a quotient of G. Specifically, the image of G under a homomorphism $\varphi\colon G \to H$ is isomorphic to $G / \ker(\varphi)$ where $\ker(\varphi)$ denotes the kernel of φ.

The dual notion of a quotient group is a subgroup, these being the two primary ways of forming a smaller group from a larger one. Any normal subgroup has a corresponding quotient group, formed from the larger group by eliminating the distinction between elements of the subgroup. In category theory, quotient groups are examples of quotient objects, which are dual to subobjects. For other examples of quotient objects, see quotient ring, quotient space (linear algebra), quotient space (topology), and quotient set.

Contents

Product of subsets of a group

Main article: Product of group subsets

In the following discussion, we will use a binary operation on the *subsets* of G: if two subsets S and T of G are given, we define their product as $ST = \{st : s \in S \wedge t \in T\}$. This operation is associative and has as identity element the singleton $\{e\}$, where e is the identity element of G. Thus, the set of all subsets of G forms a monoid under this operation.

In terms of this operation we can first explain what a quotient group is, and then explain what a normal

subgroup is:

A quotient group of a group G *is a partition of* G *which is itself a group under this operation.*

It is fully determined by the subset containing e. A normal subgroup of G is the set containing e in any such partition. The subsets in the partition are the cosets of this normal subgroup.

A subgroup N of a group G is normal if and only if the coset equality $aN = Na$ holds for all a in G. In terms of the binary operation on subsets defined above, a normal subgroup of G is a subgroup that commutes with every subset of G and is denoted $N \lhd G$. A subgroup that permutes with every subgroup of G is called a permutable subgroup.

Definition

Let N be a normal subgroup of a group G. We define the set G/N to be the set of all left cosets of N in G, i.e., $G/N = \{ aN : a \text{ in } G \}$. The group operation on G/N is the product of subsets defined above. In other words, for each aN and bN in G/N, the product of aN and bN is $(aN)(bN)$. This operation is closed, because $(aN)(bN)$ really is a left coset:

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)NN = (ab)N.$$

The normality of N is used in this equation. Because of the normality of N, the left cosets and right cosets of N in G are equal, and so G/N could be defined as the set of right cosets of N in G. Because the operation is derived from the product of subsets of G, the operation is well-defined (does not depend on the particular choice of representatives), associative, and has identity element N. The inverse of an element aN of G/N is $a^{-1}N$.

For example, consider the group with addition modulo 6:

$$G = \{0, 1, 2, 3, 4, 5\}.$$

Let

$$N = \{0, 3\}.$$

The quotient group is:

$$\begin{aligned} G/N &= \{ aN : a \in G \} = \{ a\{0,3\} : a \in \{0,1,2,3,4,5\} \} = \\ &\quad \{ 0\{0,3\}, 1\{0,3\}, 2\{0,3\}, 3\{0,3\}, 4\{0,3\}, 5\{0,3\} \} = \\ &\quad \{ \{(0+0) \bmod 6, (0+3) \bmod 6\}, \{(1+0) \bmod 6, (1+3) \bmod 6\}, \\ &\qquad \{(2+0) \bmod 6, (2+3) \bmod 6\}, \{(3+0) \bmod 6, (3+3) \bmod 6\}, \\ &\qquad \{(4+0) \bmod 6, (4+3) \bmod 6\}, \{(5+0) \bmod 6, (5+3) \bmod 6\} \} = \\ &\quad \{ \{0,3\}, \{1,4\}, \{2,5\}, \{3,0\}, \{4,1\}, \{5,2\} \} = \\ &\quad \{ \{0,3\}, \{1,4\}, \{2,5\}, \{0,3\}, \{1,4\}, \{2,5\} \} = \\ &\quad \{ \{0,3\}, \{1,4\}, \{2,5\} \}. \end{aligned}$$

The basic argument above is still valid if G/N is defined to be the set of all right cosets.

Motivation for definition

The reason G/N is called a quotient group comes from division of integers. When dividing 12 by 3 one obtains the answer 4 because one can regroup 12 objects into 4 subcollections of 3 objects. The

If G is a Lie group and N is a normal Lie subgroup of G, the quotient G / N is also a Lie group. In this case, the original group G has the structure of a fiber bundle (specifically, a principal N-bundle), with base space G / N and fiber N.

For a non-normal Lie subgroup N, the space G / N of left cosets is not a group, but simply a differentiable manifold on which G acts. The result is known as a homogeneous space.

See also

- Quotient ring, also called a *factor ring*
- Group extension
- Extension problem
- Lattice theorem
- Quotient category
- Short exact sequence

Notes

1. ^ Dummit & Foote (2003, p. 120)

References

- Dummit, David S.; Foote, Richard M. (2004), *Abstract Algebra* (3rd ed.), New York: Wiley, ISBN 978-0-471-43334-7
- Herstein, I.N. (1975), *Topics in Algebra* (2nd ed.), New York: Wiley, ISBN 0-471-02371-X

Factor (quotient) group gymnastics

for $SU(2) \longrightarrow SO(3)$

See sketches in Naber's slides: 2 points of $SU(2)$ correspond to 1 point of $SO(3)$ 

With phase ψ for rotation around some axis, $U(\psi+2\pi) = -U(\psi)$

Consider the products in $SU(2)$:

$$c_1 = a(\psi_2)\,b(\psi_1) = c_1$$
$$c_2 = a(\psi_2+2\pi)\,b(\psi_1) = -I\,c_1$$
$$c_3 = a(\psi_2+2\pi)\,b(\psi_1+2\pi) = +I\,c_1$$
$$c_4 = a(\psi_1)\,b(\psi_1+2\pi) = -I\,c_1$$

These correspond to $c_1(I, -I) = c_1 K$

(K: kernel.)

The multiplications leading to $c_1 \to c_4$ can be considered to be obtained from

$$c_1 K = aK\,bK = ab\,KK \quad (\because Kb = bK)$$

Anyway, $c_1 \to c_4$ all give the same $SO(3)$ map. Γ

So $SO(3)$ is homomorphic to $SU(2)/K$: $SO(3) \simeq SU(2)/K$

K is homomorphic to $\mathbb{Z}_2$ - the 2 element additive cyclic group.

So $SO(3) \simeq SU(2)/\mathbb{Z}_2$

Roman

APPENDIX 2

The Rudiments of Group Theory

In this Appendix we undertake the almost hopeless task of collecting, for the convenience of the reader, but certainly not as a substitute for his more serious study from competent textbooks (see the list of References), the most important definitions and some theorems (without proofs) of group theory.

A2–1 Basic notions. Let us consider a set of abstract entities

$$G = \{g_0, g_1, \ldots, g_\alpha, \ldots, g_\beta, \ldots\},$$

where there is defined between the elements a *composition law* with the following properties:*

(i) The composition is always *performable*. If $g_\alpha \in G$ and $g_\beta \in G$, then $g_\beta g_\alpha = g_\gamma \in G$.

(ii) The composition obeys the *associative law*

$$g_\alpha(g_\beta g_\gamma) = (g_\alpha g_\beta) g_\gamma.$$

(iii) There exists a *unit element* g_0 in G such that for any $g_\alpha \in G$ we have

$$g_0 g_\alpha = g_\alpha g_0 = g_\alpha.$$

(iv) To any element $g_\alpha \in G$ there exists another element g_ρ (to be denoted specifically by g_α^{-1}) such that

$$g_\alpha g_\alpha^{-1} = g_\alpha^{-1} g_\alpha = g_0.$$

The element g_α^{-1} is called the inverse of g_α.

If the axioms (i) through (iv) are fulfilled, then the set G is called a *group* in respect to the composition law.

If, in addition, it so happens that $g_\alpha g_\beta = g_\beta g_\alpha$ for any pair of group elements, then one speaks of a commutative or *Abelian group*.

The number of elements of the group is called the *order* of the group. Correspondingly one speaks of finite and infinite groups. Infinite groups of particular

* The composition of two elements will be denoted by writing them next to one another: $g_\beta g_\alpha$. The order is important, in general $g_\beta g_\alpha \neq g_\alpha g_\beta$. The composition is usually referred to as multiplication; $g_\beta g_\alpha$ is the "product" of g_α and g_β.

interest are the so-called *continuous groups*. For such groups the notation g_α for individual group elements is not quite correct, since the set of elements is noncountable. Each group element is then labeled uniquely by a continuously varying (real or complex) *parameter* α and g_α is therefore a piecewise continuous single-valued function over the manifold α. In most cases it is necessary to label each group element not by one but by a whole set of parameters, $\alpha \equiv (\alpha_1, \alpha_2, \ldots, \alpha_p)$. We then say that the group has p *parameters*. We note that any one-parameter group is Abelian. The unit element of the group is usually characterized by the particular set of parameters $\alpha_1 = \alpha_2 = \ldots = \alpha_p = 0$, but sometimes it is advantageous to introduce a different set of parameters. Two elements of which all the parameters differ only by an infinitesimal amount, $\beta_i = \alpha_i + \epsilon_i$ ($\epsilon_i \ll 1$), are said to lie infinitesimally close to each other. If the group is parametrized so that for the unit element $\alpha_i = 0$ ($i = 1, 2, \ldots, p$), then all elements whose parameters are infinitesimally small numbers ϵ_i are said to lie in the vicinity of the unit element. In order to be able to express the composition law in terms of the parameters, we always make the restriction that the parameters (γ) of the product element $g_\gamma = g_\beta g_\alpha$ as well as those of the inverse element g_α^{-1} are *continuously differentiable functions* of the parameters (β) and (α) or, in the second case, of (α). We will say more about continuous groups in Section A2–3.

The most important groups (both finite and continuous) in physics are those whose elements can be realized by geometrical or physical transformations. These groups will be referred to as *transformation groups*. The composition law is here stated as the outcome of the *successive application* of two definite transformations belonging to the group. Well-known instances are the permutation group of n objects (finite group, order $n!$) or the rotation group in, say, three dimensions (a continuous group, which has three real parameters). Such transformation groups are usually defined in terms of linear transformations on a set of variables. For example, the rotation group can be defined as the set of all homogeneous linear transformations on the three-dimensional real Euclidean space R_3 which leave the value of $x^2 + y^2 + z^2$ unchanged. Nevertheless, it should be pointed out that this is but a *realization* of an *abstract* group in terms of concrete transformations; the structure of the group is fully characterized by the composition law in terms of abstract group elements.

Any subset H of a group G which forms in itself a group (with respect to the composition defined for the elements of G) is called a *subgroup* of G. Any group possesses two *trivial subgroups:* g_0 and G. If H is a subgroup of G, it must contain the unit element g_0 of G. For finite groups, the order of a subgroup H is always a divisor of the order of the group G.

Let H be a subgroup of G with the elements

$$H = \{h_0 = g_0, h_1, h_2, \ldots, h_\alpha, \ldots, h_\beta, \ldots\}.$$

Let g_α be an arbitrary element of G, and let us form the set of elements

$$L_\alpha = \{g_\alpha h_0 = g_\alpha, g_\alpha h_1, \ldots, g_\alpha h_\alpha, \ldots, g_\alpha h_\beta, \ldots\}. \qquad \text{(A2–1a)}$$

but not in H ?

The elements of this set are, of course, all elements of the group G, but in general L_α will not be a group. We call the set L_α the *left coset* of G with respect to g_α modulo H. It is customary to introduce the symbolic notation

$$L_\alpha = g_\alpha H. \tag{A2–1b}$$

In this definition it is understood that g_α must not be an element of the subgroup H, because then we would have $g_\alpha H = H$. If, however, g_α does not belong to H, then it can be shown that $g_\alpha H$ and H have no common element.

Taking different elements g_α, g_β, etc., we get different left cosets $g_\alpha H$, $g_\beta H$, etc. There are two possibilities:

(a) the two cosets $g_\alpha H$ and $g_\beta H$ have no element in common;

(b) the two cosets have all elements in common and are said to be equivalent. This happens if and only if $g_\beta^{-1} g_\alpha$ belongs to the subgroup H.

By analogy to left cosets, we can define *right cosets* of G with respect to g_α modulo H,

$$R_\alpha = H g_\alpha, \tag{A2–2a}$$

with

$$R_\alpha = \{h_0 g_\alpha = g_\alpha, h_1 g_1, \ldots, h_\alpha g_\alpha, \ldots, h_\beta g_\alpha, \ldots\}. \tag{A2–2b}$$

In general, a left and a right coset $g_\alpha H$ and $H g_\alpha$ are not identical sets. If, however, it so happens that

$$g_\alpha H = H g_\alpha, \tag{A2–3}$$

for every element g_α of G, then H is called an *invariant subgroup* of G. If we define the set

$$g_\alpha^{-1} H g_\alpha = \{g_\alpha^{-1} h_0 g_\alpha, g_\alpha^{-1} h_1 g_\alpha, \ldots, g_\alpha^{-1} h_\alpha g_\alpha, \ldots, g_\alpha^{-1} h_\beta g_\alpha, \ldots\},$$

then the condition for H being an invariant subgroup can be reformulated as

$$g_\alpha^{-1} H g_\alpha = H, \qquad \text{for every } g_\alpha \in G. \tag{A2–4}$$

If H is an invariant subgroup, this *does not* imply that all *elements* of H commute with all elements g_α of G. But if G is Abelian, all subgroups of G are invariant.

A group which has no (nontrivial) invariant subgroup is called *simple*. If it has invariant subgroups but none of them is Abelian, then the group is called *semisimple*.

Let $g_\alpha \in G$ and $g_\beta \in G$. The group element $g_\beta^{-1} g_\alpha g_\beta$ is said to be *conjugate* to g_α. Keeping g_α fixed and letting g_β go through all other elements of the group G, we obtain a set

$$C_\alpha = \{g_0^{-1} g_\alpha g_0 = g_\alpha, g_1^{-1} g_\alpha g_1, \ldots, g_\beta^{-1} g_\alpha g_\beta, \ldots\}, \tag{A2–5}$$

which will be called the *class* of element g_α. Any two elements of a class are conjugate to each other, and conversely, the set of all elements that are mutually conjugate form a class. If two classes C_α and C_β have but one common element,

then the two classes are equivalent.* Thus the classification of group elements into mutually exclusive classes is unique; the possible set of *all* different classes exhausts the group. We note that in an Abelian group, each group element forms a class in itself. Furthermore, for *any* kind of group, the unit element g_0 is always a class by itself. Likewise, any element g_α which commutes with all other elements of the group forms a class by itself.

If we use the concept of classes and the definition (A2–4) of an invariant subgroup, the latter can be reformulated in the following useful manner: H is an invariant subgroup of G if its elements are all those of one or of several classes of G.

Let H be an invariant subgroup of G. Let us form all nonequivalent cosets

$$g_1 H = f_1, \quad \ldots, \quad g_\alpha H = f_\alpha, \ldots. \tag{A2–6a}$$

It can now be readily seen that the *set F of sets*

$$F = \{f_0, f_1, \ldots, f_\alpha, \ldots\} \tag{A2–6b}$$

forms a group† with respect to the composition law defined in G. Here $f_0 = H$ and the f_α are given by (A2–6a). The group F is called the *factor* (or *quotient*) *group* of G with respect to H and is denoted by

$$F = G/H. \tag{A2–6c}$$

For clarity we point out that the set (group) F is, in detail,

$$F = \{h_0, h_1, \ldots, h_\alpha, \ldots; g_1 h_0, g_1 h_1, \ldots, g_1 h_\alpha, \ldots; \ldots; g_\alpha h_0, g_\alpha h_1, \ldots, g_\alpha h_\alpha, \ldots; \ldots\}. \tag{A2–6d}$$

The product $f_\beta f_\alpha$ means the set

$$f_\gamma = \{g_\beta h_0 g_\alpha h_0, g_\beta h_0 g_\alpha h_1, \ldots, g_\beta h_0 g_\alpha h_\alpha, \ldots, g_\beta h_1 g_\alpha h_0, g_\beta h_1 g_\alpha h_1, \ldots, g_\beta h_1 g_\alpha h_\alpha, \ldots, g_\beta h_\alpha g_\alpha h_\alpha, \ldots\}.$$

From the point of view of the definition of the factor group, all elements $(g_\alpha h_0, \ldots, g_\alpha h_\alpha, \ldots)$ written in (A2–6d) between semicolons are to be considered as one single element. The unit element of F is the subgroup H itself. The composition of f_β and f_α is a composition of sets based on the group element composition defined in G.

Let us now consider two groups

$$G = \{g_0, g_1, \ldots, g_\alpha, \ldots, g_\beta, \ldots\}, \quad \text{and} \quad C = \{c_0, c_1, \ldots, c_\alpha, \ldots, c_\beta, \ldots\}.$$

* The term "equivalent" for sets is used here and in the following in the sense that A and B are equivalent if, apart from order, they contain the same elements.

† This follows from the theorem which states that if H is an invariant subgroup and $g_\alpha H$ and $g_\beta H$ are two (nonequivalent) cosets, then the product of an element of $g_\alpha H$ with an element of $g_\beta H$ is an element of the coset $g_\beta g_\alpha H$. In formulas, we have $(g_\beta H)(g_\alpha H) = (g_\beta g_\alpha H)$.

Roman – Advanced Q.T.

Consider a discrete gp G with 100 elements and an ISG F of 10 elements

Then there are 10 ~~cos~~ distinct cosets of 10 elements each as $10 \times 10 = 100$, so exhausting the whole gp.
It is not that we take 100 elements, left multiplied onto each of the 10 elements of the ISG - because many of the 1000 products won't be distinct!

$G/F = \{ gF : g \in G \}$ with F treated as a single object

In bundle language, G is the total space; $\{ G, P_F, G/F \}$ (Total, base)
G/F is the base space
P_F is the projection

We write $G/F = \{ gF : g \in G \}$ ~~but we should note that~~
This would look like $\{ g_1 F, g_2 F, \ldots g_{100} F \}$ but since many of these will be the same, ~~we can~~ then we can pick out the distinct sets and rewrite this as the 10 cosets $\{ g_1 F, g_2 F, \ldots g_{10} F \}$

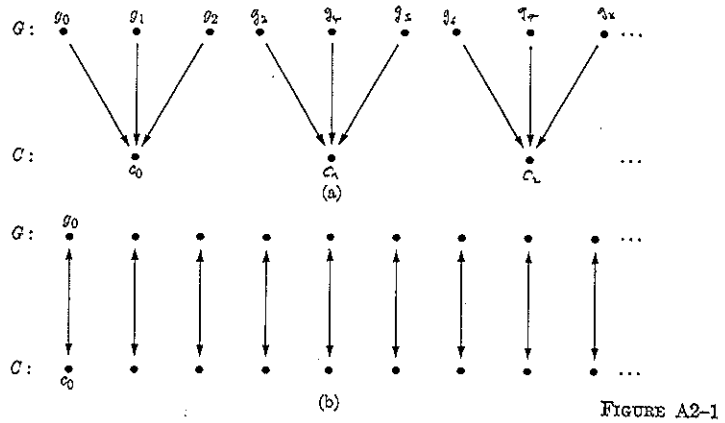

FIGURE A2–1

If one can establish a correspondence (mapping) of G onto C such that to any element of G there corresponds one and only one element of C,

$$g_0 \longrightarrow c_0, \qquad g_\alpha \longrightarrow c_\alpha, \quad \text{any } \alpha, \tag{A2–7a}$$

such that

$$\text{if } g_\beta g_\alpha = g_\gamma, \quad \text{then} \quad c_\beta c_\alpha = c_\gamma, \tag{A2–7b}$$

then we say that C is *homomorphic* to G, and we denote this relation by writing $C \sim G$. The group C is often called the homomorphic image of G. If the mapping is one-to-one, i.e., if to any element of G there corresponds one and only one element of C and *vice versa* such that (A2–7b) holds, then we call the mapping an *isomorphism* and write $C \approx G$. Note that in case of homomorphism there are several different elements of G which have as their image a single element of C. Figure A2–1(a) shows a homomorphism and Fig. A2–1(b) an isomorphism. Isomorphism is transitive: if $G \approx C$ and $C \approx D$, then $G \approx D$; and it is also reflexive: if $G \approx C$, then $C \approx G$.

If both G and C are finite groups and have the same order N, then any homomorphism is automatically an isomorphism. If, however, the orders are different and $N_G > N_C$, then, in the best case, one can have only a homomorphism. Note that with infinite groups (even if both G and C are continuous) a homomorphism does not necessarily imply an isomorphism.

Suppose we have a homomorphism $C \sim G$. It can be shown that the homomorphic image of an invariant subgroup H of G will be an invariant subgroup D of C. Furthermore, the set of elements $g_0, g_1, \ldots, g_\rho, \ldots$ which have as their image in C the unit element c_0, form an invariant subgroup of G. This invariant subgroup

$$K = \{g_0, g_1, \ldots, g_\rho, \ldots\}$$

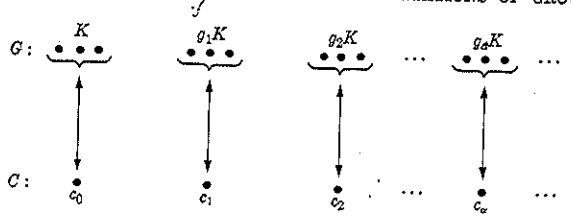

FIGURE A2–2

of G is called the *kernel* of the homomorphism. Moreover, the set of elements $g_\sigma, g_\pi, \ldots, g_\kappa, \ldots$ which has as its homomorphic image in C the single element $c_\varphi \neq c_0$ is a coset of the kernel K. [In Fig. A2–1(a) the elements g_0, g_1, g_2 form an invariant subgroup K of G; all other "triplets" of elements are various cosets of G modulo K.]

In summary, the following two theorems can be established:

(a) If G has an invariant subgroup H, then G is homomorphic to the factor group G/H.

(b) If G is homomorphic to a group C, then G/K is isomorphic to C. Here K, the kernel, is an invariant subgroup of G and consists of all elements of G which are mapped onto the unit element of C. (This theorem is illustrated in Fig. A2–2.)

We note the following terminology: If a group G is homomorphic to one of its own subgroups G', then we call this homomorphism an *endomorphism*. If, moreover, this mapping is a one-to-one mapping, it is called an *automorphism*.

To conclude this section on generalities, we introduce the concept of the direct product group. Let $A = \{a_0, a_1, \ldots, a_\alpha, \ldots, a_\beta, \ldots\}$ and $B = \{b_0, b_1, \ldots, b_\alpha, \ldots, b_\beta \ldots\}$ be two groups of linear transformations, both sets acting on the same number of variables. Suppose all elements of A commute with all elements of B. Consider now the set of transformations which are obtained by taking all possible combinations of the elements of A and B. This set is

$$\begin{aligned} M &= \{a_0b_0, a_0b_1, \ldots, a_0b_\alpha, \ldots, a_1b_0, \ldots, a_1b_\alpha, \ldots, a_\alpha b_\beta, \ldots\} \\ &= \{m_0, m_1, \ldots, m_\gamma, \ldots, m_\varphi, \ldots\}. \end{aligned} \tag{A2–8a}$$

It is easy to show that the set M is a group. It is called the *direct product* of the groups A and B and we denote it symbolically by

$$M = A \times B. \tag{A2–8b}$$

A2–2 Representations of groups. If a set of $n \times n$ matrices satisfies, with respect to ordinary matrix multiplication, the axioms* (i), (iii), and (iv) on p. 664, then this set forms a group D of linear transformations in n dimensions. This group, consisting of matrices, may be either finite or infinite. In the latter case, if the group is continuously infinite, the elements of each matrix belonging to the

* The associative axiom (ii) is automatically fulfilled.

Homomorphism

From Wikipedia, the free encyclopedia

In abstract algebra, a **homomorphism** is a structure-preserving map between two algebraic structures (such as groups, rings, or vector spaces). The word *homomorphism* comes from the ancient Greek language: *ὁμός (homos)* meaning "same" and *μορφή (morphe)* meaning "shape". Isomorphisms, automorphisms, and endomorphisms are all types of homomorphism.

Contents

Definition and illustration

Definition

The definition of homomorphism depends on the type of algebraic structure under consideration. Particular definitions of homomorphism include the following:

- A group homomorphism is a homomorphism between two groups.
- A ring homomorphism is a homomorphism between two rings.
- A linear map is a homomorphism between two vector spaces.
- An algebra homomorphism is a homomorphism between two algebras.
- A functor is a homomorphism between two categories.

The common theme is that a homomorphism is a function between two algebraic objects that respects the algebraic structure.

For example, a group is an algebraic object consisting of a set together with a single binary operation, satisfying certain axioms. If $(G, *)$ and $(H, *')$ are groups, a **homomorphism** from $(G, *)$ to $(H, *')$ is a function $f: (G, *) \to (H, *')$ such that $f(g_1 * g_2) = f(g_1) *' f(g_2)$ for any elements $g_1, g_2 \in G$.

When an algebraic structure includes more than one operation, homomorphisms are required to preserve each operation. For example, a ring possesses both addition and multiplication, and a homomorphism from the ring $(R, +, *, 0, 1)$ to the ring $(R', +', *', 0', 1')$ is a function such that

$$f(r + s) = f(r) +' f(s) \qquad \text{and} \qquad f(r * s) = f(r) *' f(s)$$

for any elements r and s of the domain ring.

The notion of a homomorphism can be given a formal definition in the context of universal algebra, a field which studies ideas common to all algebraic structures. In this setting, a homomorphism $f: A \to B$ is a function between two algebraic structures of the same type such that

$$f(\mu_A(a_1, \ldots, a_n)) = \mu_B(f(a_1), \ldots, f(a_n))$$

for each n-ary operation μ and for all elements $a_1, \ldots, a_n \in A$.

Basic examples

The real numbers are a ring, having both addition and multiplication. The set of all 2×2 matrices is also a ring, under matrix addition and matrix multiplication. If we define a function between these rings as follows:

$$f(r) = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

where r is a real number. Then f is a homomorphism of rings, since f preserves both addition:

$$f(r + s) = \begin{pmatrix} r+s & 0 \\ 0 & r+s \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} + \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = f(r) + f(s)$$

and multiplication:

$$f(rs) = \begin{pmatrix} rs & 0 \\ 0 & rs \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = f(r)\, f(s).$$

For another example, the nonzero complex numbers form a group under the operation of multiplication, as do the nonzero real numbers. (Zero must be excluded from both groups since it does not have a multiplicative inverse, which is required for elements of a group.) Define a function f from the nonzero complex numbers to the nonzero real numbers by

$$f(z) = |z|.$$

That is, $f(z)$ is the absolute value (or modulus) of the complex number z. Then f is a homomorphism of groups, since it preserves multiplication:

$$f(z_1 z_2) = |z_1 z_2| = |z_1|\,|z_2| = f(z_1)\, f(z_2).$$

Note that f cannot be extended to a homomorphism of rings (from the complex numbers to the real numbers), since it does not preserve addition:

$$|z_1 + z_2| \neq |z_1| + |z_2|.$$

Informal discussion

Because abstract algebra studies sets endowed with operations that generate interesting structure or properties on the set, functions which preserve the operations are especially important. These functions are known as *homomorphisms*.

Homomorphisms are also used in the study of formal languages[2] (although within this context, often they are briefly referred to as morphisms[3]). Given alphabets Σ_1 and Σ_2, a function $h : \Sigma_1^* \to \Sigma_2^*$ such that $h(uv) = h(u)h(v)$ for all u and v in Σ_1^* is called a *homomorphism* (or simply *morphism*) on Σ_1^*.[4] Let e denote the empty word. If h is a homomorphism on Σ_1^* and $h(x) \neq e$ for all $x \neq e$ in Σ_1^*, then h is called an *e-free homomorphism*.

This type of homomorphism can be thought of as (and is equivalent to) a monoid homomorphism where Σ^* the set of all words over a finite alphabet Σ is a monoid (in fact it is the free monoid on Σ) with operation concatenation and the empty word as the identity.

See also

- continuous function
- diffeomorphism
- homomorphic encryption
- homomorphic secret sharing – a simplistic decentralized voting protocol
- morphism

References

1. ^ Exercise 4 in section I.5, in Saunders Mac Lane, *Categories for the Working Mathematician*, ISBN 0-387-90036-5
2. ^ Seymour Ginsburg, *Algebraic and automata theoretic properties of formal languages*, North-Holland, 1975, ISBN 0-7204-2506-9.
3. ^ T. Harju, J. Karhumäki, Morphisms in *Handbook of Formal Languages*, Volume I, edited by G. Rozenberg, A. Salomaa, Springer, 1997, ISBN 3-540-61486-9.
4. ^ In homomorphisms on formal languages, the * operation is the Kleene star operation. The · and ○ are both concatenation, commonly denoted by juxtaposition.

A monograph available free online:

- Burris, Stanley N., and H.P. Sankappanavar, H. P., 1981. *A Course in Universal Algebra. (http://www.thoralf.uwaterloo.ca/htdocs/ualg.html)* Springer-Verlag. ISBN 3-540-90578-2.