CHAPTER I

Groups

§1. MONOIDS

Let S be a set. A mapping

$$S \times S \to S$$

is sometimes called a **law of composition** (of S into itself). If x, y are elements of S, the image of the pair (x, y) under this mapping is also called their **product** under the law of composition, and will be denoted by xy. (Sometimes, we also write $x \cdot y$, and in many cases it is also convenient to use an additive notation, and thus to write $x + y$. In that case, we call this element the **sum** of x and y. It is customary to use the notation $x + y$ only when the relation $x + y = y + x$ holds.)

Let S be a set with a law of composition. If x, y, z are elements of S, then we may form their product in two ways: $(xy)z$ and $x(yz)$. If $(xy)z = x(yz)$ for all x, y, z in S then we say that the law of composition is **associative**.

An element e of S such that $ex = x = xe$ for all $x \in S$ is called a **unit element**. (When the law of composition is written additively, the unit element is denoted by 0, and is called a **zero element**.) A unit element is unique, for if e' is another unit element, we have

$$e = ee' = e'$$

by assumption. In most cases, the unit element is written simply 1 (instead of e). For most of this chapter, however, we shall write e so as to avoid confusion in proving the most basic properties.

A **monoid** is a set G, with a law of composition which is associative, and having a unit element (so that in particular, G is not empty).

S. Lang, *Algebra*

Let G be a monoid, and $x_1, \ldots, x_n$ elements of G (where n is an integer > 1). We define their product inductively:

$$\prod_{\nu=1}^{n} x_\nu = x_1 \cdots x_n = (x_1 \cdots x_{n-1})x_n.$$

We then have the following rule:

$$\prod_{\mu=1}^{m} x_\mu \cdot \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu,$$

which essentially asserts that we can insert parentheses in any manner in our product without changing its value. The proof is easy by induction, and we shall leave it as an exercise.

One also writes

$$\prod_{m+1}^{m+n} x_\nu \quad \text{instead of} \quad \prod_{\nu=1}^{n} x_{m+\nu}$$

and we define

$$\prod_{\nu=1}^{0} x_\nu = e.$$

As a matter of convention, we agree also that the empty product is equal to the unit element.

It would be possible to define more general laws of composition, i.e. maps $S_1 \times S_2 \to S_3$ using arbitrary sets. One can then express associativity and commutativity in any setting for which they make sense. For instance, for commutativity we need a law of composition

$$f : S \times S \to T$$

where the two sets of departure are the same. **Commutativity** then means $f(x, y) = f(y, x)$, or $xy = yx$ if we omit the mapping f from the notation. For associativity, we leave it to the reader to formulate the most general combination of sets under which it will work. We shall meet special cases later, for instance arising from maps

$$S \times S \to S \quad \text{and} \quad S \times T \to T.$$

Then a product $(xy)z$ makes sense with $x \in S$, $y \in S$, and $z \in T$. The product $x(yz)$ also makes sense for such elements x, y, z and thus it makes sense to say that our law of composition is associative, namely to say that for all x, y, z as above we have $(xy)z = x(yz)$.

If the law of composition of G is commutative, we also say that G is **commutative (or abelian)**.

Let G be a commutative monoid, and $x_1, \ldots, x_n$ elements of G. Let ψ be a bijection of the set of integers $(1, \ldots, n)$ onto itself. Then

$$\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu.$$

We prove this by induction, it being obvious for $n = 1$. We assume it for $n - 1$. Let k be an integer such that $\psi(k) = n$. Then

$$\prod_{1}^{n} x_{\psi(\nu)} = \prod_{1}^{k-1} x_{\psi(\nu)} \cdot x_{\psi(k)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)}$$

$$= \prod_{1}^{k-1} x_{\psi(\nu)} \cdot \prod_{1}^{n-k} x_{\psi(k+\nu)} \cdot x_{\psi(k)}.$$

Define a map φ of $(1, \ldots, n-1)$ into itself by the rule

$$\varphi(\nu) = \psi(\nu) \qquad \text{if} \quad \nu < k,$$

$$\varphi(\nu) = \psi(\nu + 1) \qquad \text{if} \quad \nu \geqq k.$$

Then

$$\prod_{1}^{n} x_{\psi(\nu)} = \prod_{1}^{k-1} x_{\varphi(\nu)} \prod_{1}^{n-k} x_{\varphi(k-1+\nu)} \cdot x_n$$

$$= \prod_{1}^{n-1} x_{\varphi(\nu)} \cdot x_n,$$

which, by induction, is equal to $x_1 \cdots x_n$, as desired.

Let G be a commutative monoid, let I be a set, and let $f: I \to G$ be a mapping such that $f(i) = e$ for almost all $i \in I$. (Here and thereafter, **almost all** will mean *all but a finite number.*) Let I_0 be the subset of I consisting of those i such that $f(i) \neq e$. By

$$\prod_{i \in I} f(i)$$

we shall mean the product

$$\prod_{i \in I_0} f(i)$$

taken in any order (the value does not depend on the order, according to the preceding remark). It is understood that the empty product is equal to e.

When G is written additively, then instead of a product sign, we write the sum sign Σ.

There are a number of formal rules for dealing with products which it would be tedious to list completely. We give one example. Let I, J be two sets, and

$f: I \times J \to G$ a mapping into a commutative monoid which takes the value e for almost all pairs (i, j). Then

$$\prod_{i \in I} \left[\prod_{j \in J} f(i,j) \right] = \prod_{j \in J} \left[\prod_{i \in I} f(i,j) \right].$$

We leave the proof as an exercise.

As a matter of notation, we sometimes write $\prod f(i)$, omitting the signs $i \in I$, if the reference to the indexing set is clear.

Let x be an element of a monoid G. For every integer $n \geqq 0$ we define x^n to be

$$\prod_{1}^{n} x,$$

so that in particular we have $x^0 = e, x^1 = x, x^2 = xx, \ldots$. We obviously have $x^{(n+m)} = x^n x^m$ and $(x^n)^m = x^{nm}$. Furthermore, from our preceding rules of associativity and commutativity, if x, y are elements of G such that $xy = yx$, then $(xy)^n = x^n y^n$. We leave the formal proof as an exercise.

If S, S' are two subsets of a monoid G, then we define SS' to be the subset consisting of all elements xy, with $x \in S$ and $y \in S'$. Inductively, we can define the product of a finite number of subsets, and we have associativity. For instance, if S, S', S'' are subsets of G, then $(SS')S'' = S(S'S'')$. Observe that $GG = G$ (because G has a unit element). If $x \in G$, then we define xS to be $\{x\}S$, where $\{x\}$ is the set consisting of the single element x. Thus xS consists of all elements xy, with $y \in S$.

By a **submonoid** of G, we shall mean a subset H of G containing the unit element e, and such that, if $x, y \in H$ then $xy \in H$ (we say that H is **closed** under the law of composition). It is then clear that H is itself a monoid, under the law of composition induced by that of G.

If x is an element of a monoid G, then the subset of powers x^n $(n = 0, 1, \ldots)$ is a submonoid of G.

The set of integers $\geqq 0$ under addition is a monoid.

Later we shall define rings. If R is a commutative ring, we shall deal with multiplicative subsets S, that is subsets containing the unit element, and such that if $x, y \in S$ then $xy \in S$. Such subsets are monoids.

A routine example. Let $\mathbf{N}$ be the natural numbers, i.e. the integers $\geqq 0$. Then $\mathbf{N}$ is an additive monoid. In some applications, it is useful to deal with a multiplicative version. See the definition of polynomials in Chapter II, §3, where a higher-dimensional version is also used for polynomials in several variables.

An interesting example. We assume that the reader is familiar with the terminology of elementary topology. Let M be the set of homeomorphism classes of compact (connected) surfaces. We shall define an addition in M. Let S, S' be compact surfaces. Let D be a small disc in S, and D' a small disc in S'. Let C, C' be the circles which form the boundaries of D and D' respectively. Let D_0, D_0' be the interiors of D and D' respectively, and glue $S - D_0$ to $S' - D_0'$ by identifying C with C'. It can be shown that the resulting surface is independent,

up to homeomorphism, of the various choices made in the preceding construction. If σ, σ' denote the homeomorphism classes of S and S' respectively, we define $\sigma + \sigma'$ to be the class of the surface obtained by the preceding gluing process. It can be shown that this addition defines a monoid structure on M, whose unit element is the class of the ordinary 2-sphere. Furthermore, if τ denotes the class of the torus, and π denotes the class of the projective plane, then every element σ of M has a unique expression of the form

$$\sigma = n\tau + m\pi$$

where n is an integer $\geqq 0$ and $m = 0$, 1, or 2. We have $3\pi = \tau + \pi$.

(The reasons for inserting the preceding example are twofold: First to relieve the essential dullness of the section. Second to show the reader that monoids exist in nature. Needless to say, the example will not be used in any way throughout the rest of the book.)

Still other examples. At the end of Chapter III, §4, we shall remark that isomorphism classes of modules over a ring form a monoid under the direct sum. In Chapter XV, §1, we shall consider a monoid consisting of equivalence classes of quadratic forms.

§2. GROUPS

A **group** G is a monoid, such that for every element $x \in G$ there exists an element $y \in G$ such that $xy = yx = e$. Such an element y is called an **inverse** for x. Such an inverse is unique, because if y' is also an inverse for x, then

$$y' = y'e = y'(xy) = (y'x)y = ey = y.$$

We denote this inverse by x^{-1} (or by $-x$ when the law of composition is written additively).

For any positive integer n, we let $x^{-n} = (x^{-1})^n$. Then the usual rules for exponentiation hold for all integers, not only for integers $\geqq 0$ (as we pointed out for monoids in §1). The trivial proofs are left to the reader.

In the definitions of unit elements and inverses, we could also define left units and left inverses (in the obvious way). One can easily prove that these are also units and inverses respectively under suitable conditions. Namely:

Let G be a set with an associative law of composition, let e be a left unit for that law, and assume that every element has a left inverse. Then e is a unit, and each left inverse is also an inverse. In particular, G is a group.

To prove this, let $a \in G$ and let $b \in G$ be such that $ba = e$. Then

$$bab = eb = b.$$

Multiplying on the left by a left inverse for b yields

$$ab = e,$$

or in other words, b is also a right inverse for a. One sees also that a is a left

inverse for b. Furthermore,

$$ae = aba = ea = a,$$

whence e is a right unit.

Example. Let G be a group and S a nonempty set. The set of maps $M(S, G)$ is itself a group; namely for two maps f, g of S into G we define fg to be the map such that

$$(fg)(x) = f(x)g(x),$$

and we define f^{-1} to be the map such that $f^{-1}(x) = f(x)^{-1}$. It is then trivial to verify that $M(S, G)$ is a group. If G is commutative, so is $M(S, G)$, and when the law of composition in G is written additively, so is the law of composition in $M(S, G)$, so that we would write $f + g$ instead of fg, and $-f$ instead of f^{-1}.

Example. Let S be a non-empty set. Let G be the set of bijective mappings of S onto itself. Then G is a group, the law of composition being ordinary composition of mappings. The unit element of G is the identity map of S, and the other group properties are trivially verified. The elements of G are called **permutations** of S. We also denote G by Perm(S). For more information on Perm(S) when S is finite, see §5 below.

Example. Let us assume here the basic notions of linear algebra. Let k be a field and V a vector space over k. Let $GL(V)$ denote the set of invertible k-linear maps of V onto itself. Then $GL(V)$ is a group under composition of mappings. Similarly, let k be a field and let $GL(n, k)$ be the set of invertible $n \times n$ matrices with components in k. Then $GL(n, k)$ is a group under the multiplication of matrices. For $n \geqq 2$, this group is not commutative.

Example. The group of automorphisms. We recommend that the reader now refer immediately to §11, where the notion of a category is defined, and where several examples are given. For any object A in a category, its automorphisms form a group denoted by Aut(A). Permutations of a set and the linear automorphisms of a vector space are merely examples of this more general structure.

Example. The set of rational numbers forms a group under addition. The set of non-zero rational numbers forms a group under multiplication. Similar statements hold for the real and complex numbers.

Example. Cyclic groups. The integers $\mathbf{Z}$ form an additive group. A group is defined to be **cyclic** if there exists an element $a \in G$ such that every element of G (written multiplicatively) is of the form a^n for some integer n. If G is written additively, then every element of a cyclic group is of the form na. One calls a a **cyclic generator**. Thus $\mathbf{Z}$ is an additive cyclic group with generator 1, and also with generator -1. There are no other generators. Given a positive integer n, the n-th roots of unity in the complex numbers form a cyclic group of order n. In terms of the usual notation, $e^{2\pi i/n}$ is a generator for this group. So is $e^{2\pi ir/n}$

with $r \in \mathbf{Z}$ and r prime to n. A generator for this group is called a **primitive** n-th root of unity.

Example. The direct product. Let G_1, G_2 be groups. Let $G_1 \times G_2$ be the direct product as sets, so $G_1 \times G_2$ is the set of all pairs (x_1, x_2) with $x_i \in G_i$. We define the law of composition componentwise by

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2).$$

Then $G_1 \times G_2$ is a group, whose unit element is (e_1, e_2) (where e_i is the unit element of G_i). Similarly, for n groups we define $G_1 \times \cdots \times G_n$ to be the set of n-tuples with $x_i \in G_i$ $(i = 1, \ldots, n)$, and componentwise multiplication. Even more generally, let I be a set, and for each $i \in I$, let G_i be a group. Let $G = \prod G_i$ be the set-theoretic product of the sets G_i. Then G is the set of all families $(x_i)_{i \in I}$ with $x_i \in G_i$. We can define a group structure on G by componentwise multiplication, namely, if $(x_i)_{i \in I}$ and $(y_i)_{i \in I}$ are two elements of G, we define their product to be $(x_i y_i)_{i \in I}$. We define the inverse of $(x_i)_{i \in I}$ to be $(x_i^{-1})_{i \in I}$. It is then obvious that G is a group called the **direct product** of the family.

Let G be a group. A **subgroup** H of G is a subset of G containing the unit element, and such that H is closed under the law of composition and inverse (i.e. it is a submonoid, such that if $x \in H$ then $x^{-1} \in H$). A subgroup is called **trivial** if it consists of the unit element alone. The intersection of an arbitrary non-empty family of subgroups is a subgroup (trivial verification).

Let G be a group and S a subset of G. We shall say that S **generates** G, or that S is a set of **generators** for G, if every element of G can be expressed as a product of elements of S or inverses of elements of S, i.e. as a product $x_1 \cdots x_n$ where each x_i or x_i^{-1} is in S. It is clear that the set of all such products is a subgroup of G (the empty product is the unit element), and is the smallest subgroup of G containing S. Thus S generates G if and only if the smallest subgroup of G containing S is G itself. If G is generated by S, then we write $G = \langle S \rangle$. By definition, a cyclic group is a group which has one generator. Given elements $x_1, \ldots, x_n \in G$, these elements generate a subgroup $\langle x_1, \ldots, x_n \rangle$, namely the set of all elements of G of the form

$$x_{i_1}^{k_1} \cdots x_{i_r}^{k_r} \quad \text{with} \quad k_1, \ldots, k_r \in \mathbf{Z}.$$

A single element $x \in G$ generates a cyclic subgroup.

Example. There are two non-abelian groups of order 8. One is the **group of symmetries of the square**, generated by two elements σ, τ such that

$$\sigma^4 = \tau^2 = e \quad \text{and} \quad \tau\sigma\tau^{-1} = \sigma^3.$$

The other is the **quaternion group**, generated by two elements, i, j such that if we put $k = ij$ and $m = i^2$, then

$$i^4 = j^4 = k^4 = e, \quad i^2 = j^2 = k^2 = m, \quad ij = mji.$$

After you know enough facts about groups, you can easily do Exercise 35.

Let G, G' be monoids. A **monoid-homomorphism** (or simply **homomorphism**) of G into G' is a mapping $f: G \to G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$, and mapping the unit element of G into that of G'. If G, G' are groups, a **group-homomorphism** of G into G' is simply a monoid-homomorphism.

We sometimes say: "Let $f: G \to G'$ be a group-homomorphism" to mean: "Let G, G' be groups, and let f be a homomorphism from G into G'."

Let $f: G \to G'$ be a group-homomorphism. Then

$$f(x^{-1}) = f(x)^{-1}$$

because if e, e' are the unit elements of G, G' respectively, then

$$e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1}).$$

Furthermore, if G, G' are groups and $f: G \to G'$ is a map such that

$$f(xy) = f(x)f(y)$$

for all x, y in G, then $f(e) = e'$ because $f(ee) = f(e)$ and also $= f(e)f(e)$. Multiplying by the inverse of $f(e)$ shows that $f(e) = e'$.

Let G, G' be monoids. A homomorphism $f: G \to G'$ is called an **isomorphism** if there exists a homomorphism $g: G' \to G$ such that $f \circ g$ and $g \circ f$ are the identity mappings (in G' and G respectively). It is trivially verified that f is an isomorphism if and only if f is bijective. The existence of an isomorphism between two groups G and G' is sometimes denoted by $G \approx G'$. If $G = G'$, we say that isomorphism is an **automorphism**. A homomorphism of G into itself is also called an **endomorphism**.

Example. Let G be a monoid and x an element of G. Let $\mathbf{N}$ denote the (additive) monoid of integers $\geqq 0$. Then the map $f: \mathbf{N} \to G$ such that $f(n) = x^n$ is a homomorphism. If G is a group, we can extend f to a homomorphism of $\mathbf{Z}$ into G (x^n is defined for all $n \in \mathbf{Z}$, as pointed out previously). The trivial proofs are left to the reader.

Let n be a fixed integer and let G be a *commutative* group. Then one verifies easily that the map

$$x \mapsto x^n$$

from G into itself is a homomorphism. So is the map $x \mapsto x^{-1}$. The map $x \mapsto x^n$ is called the n-th **power map**.

Example. Let $I = \{i\}$ be an indexing set, and let $\{G_i\}$ be a family of groups. Let $G = \prod G_i$ be their direct product. Let

$$p_i: G \to G_i$$

be the projection on the i-th factor. Then p_i is a homomorphism.

Let G be a group, S a set of generators for G, and G' another group. Let $f: S \to G'$ be a map. If there exists a homomorphism $\bar{f}$ of G into G' whose restriction to S is f, then there is only one.

In other words, f has at most one extension to a homomorphism of G into G'. This is obvious, but will be used many times in the sequel.

Let $f: G \to G'$ and $g: G' \to G''$ be two group-homomorphisms. Then the composite map $g \circ f$ is a group-homomorphism. If f, g are isomorphisms then so is $g \circ f$. Furthermore $f^{-1}: G' \to G$ is also an isomorphism. In particular, the set of all automorphisms of G is itself a group, denoted by $\mathrm{Aut}(G)$.

Let $f: G \to G'$ be a group-homomorphism. Let e, e' be the respective unit elements of G, G'. We define the **kernel** of f to be the subset of G consisting of all x such that $f(x) = e'$. From the definitions, it follows at once that the kernel H of f is a subgroup of G. (Let us prove for instance that H is closed under the inverse mapping. Let $x \in H$. Then

$$f(x^{-1})f(x) = f(e) = e'.$$

Since $f(x) = e'$, we have $f(x^{-1}) = e'$, whence $x^{-1} \in H$. We leave the other verifications to the reader.)

Let $f: G \to G'$ be a group-homomorphism again. Let H' be the **image** of f. Then H' is a subgroup of G', because it contains e', and if $f(x), f(y) \in H'$, then $f(xy) = f(x)f(y)$ lies also in H'. Furthermore, $f(x^{-1}) = f(x)^{-1}$ is in H', and hence H' is a subgroup of G'.

The kernel and image of f are sometimes denoted by $\mathrm{Ker}\, f$ and $\mathrm{Im}\, f$.

A homomorphism $f: G \to G'$ which establishes an isomorphism between G and its image in G' will also be called an **embedding**.

A homomorphism whose kernel is trivial is injective.

To prove this, suppose that the kernel of f is trivial, and let $f(x) = f(y)$ for some $x, y \in G$. Multiplying by $f(y^{-1})$ we obtain

$$f(xy^{-1}) = f(x)f(y^{-1}) = e'.$$

Hence xy^{-1} lies in the kernel, hence $xy^{-1} = e$, and $x = y$. If in particular f is also surjective, then f is an isomorphism. Thus a surjective homomorphism whose kernel is trivial must be an isomorphism. We note that an injective homomorphism is an embedding.

An injective homomorphism is often denoted by a special arrow, such as

$$f: G \hookrightarrow G'.$$

There is a useful criterion for a group to be a direct product of subgroups:

Proposition 2.1. *Let G be a group and let H, K be two subgroups such that $H \cap K = e$, $HK = G$, and such that $xy = yx$ for all $x \in H$ and $y \in K$. Then the map*

$$H \times K \to G$$

such that $(x, y) \mapsto xy$ is an isomorphism.

Proof. It is obviously a homomorphism, which is surjective since $HK = G$.

If (x, y) is in its kernel, then $x = y^{-1}$, whence x lies in both H and K, and $x = e$, so that $y = e$ also, and our map is an isomorphism.

We observe that Proposition 2.1 generalizes by induction to a finite number of subgroups $H_1, \ldots, H_n$ whose elements commute with each other, such that

$$H_1 \cdots H_n = G,$$

and such that

$$H_{i+1} \cap (H_1 \cdots H_i) = e.$$

In that case, G is isomorphic to the direct product

$$H_1 \times \cdots \times H_n.$$

Let G be a group and H a subgroup. A **left coset** of H in G is a subset of G of type aH, for some element a of G. An element of aH is called a **coset representative** of aH. The map $x \mapsto ax$ induces a bijection of H onto aH. Hence any two left cosets have the same cardinality.

Observe that if a, b are elements of G and aH, bH are cosets having one element in common, then they are equal. Indeed, let $ax = by$ with $x, y \in H$. Then $a = byx^{-1}$. But $yx^{-1} \in H$. Hence $aH = b(yx^{-1})H = bH$, because for any $z \in H$ we have $zH = H$.

We conclude that G is the disjoint union of the left cosets of H. A similar remark applies to **right cosets** (i.e. subsets of G of type Ha). The number of left cosets of H in G is denoted by $(G : H)$, and is called the (left) **index** of H in G. The index of the trivial subgroup is called the **order** of G and is written $(G : 1)$. From the above conclusion, we get:

Proposition 2.2. *Let G be a group and H a subgroup. Then*

$$(G : H)(H : 1) = (G : 1),$$

in the sense that if two of these indices are finite, so is the third and equality holds as stated. If $(G : 1)$ is finite, the order of H divides the order of G.

More generally, let H, K be subgroups of G and let $H \supset K$. Let $\{x_i\}$ be a set of (left) coset representatives of K in H and let $\{y_j\}$ be a set of coset representatives of H in G. Then we contend that $\{y_j x_i\}$ is a set of coset representatives of K in G.

Proof. Note that

$$H = \bigcup_i x_i K \qquad \text{(disjoint)},$$

$$G = \bigcup_j y_j H \qquad \text{(disjoint)}.$$

Hence

$$G = \bigcup_{i,j} y_j x_i K.$$

We must show that this union is disjoint, i.e. that the $y_j x_i$ represent distinct cosets. Suppose

$$y_j x_i K = y_{j'} x_{i'} K$$

for a pair of indices (j, i) and (j', i'). Multiplying by H on the right, and noting that x_i, $x_{i'}$ are in H, we get

$$y_j H = y_{j'} H,$$

whence $y_j = y_{j'}$. From this it follows that $x_i K = x_{i'} K$ and therefore that $x_i = x_{i'}$, as was to be shown.

The formula of Proposition 2.2 may therefore be generalized by writing

$$(G : K) = (G : H)(H : K),$$

with the understanding that if two of the three indices appearing in this formula are finite, then so is the third and the formula holds.

The above results are concerned systematically with left cosets. For the right cosets, see Exercise 10.

Example. A group of prime order is cyclic. Indeed, let G have order p and let $a \in G$, $a \neq e$. Let H be the subgroup generated by a. Then $\#(H)$ divides p and is $\neq 1$, so $\#(H) = p$ and so $H = G$, which is therefore cyclic.

Example. Let $J_n = \{1, \ldots, n\}$. Let S_n be the group of permutations of J_n. We define a **transposition** to be a permutation τ such that there exist two elements $r \neq s$ in J_n for which $\tau(r) = s$, $\tau(s) = r$, and $\tau(k) = k$ for all $k \neq r, s$. Note that the transpositions generate S_n. Indeed, say σ is a permutation, $\sigma(n) = k \neq n$. Let τ be the transposition interchanging k, n. Then $\tau\sigma$ leaves n fixed, and by induction, we can write $\tau\sigma$ as a product of transpositions in $\mathrm{Perm}(J_{n-1})$, thus proving that transpositions generate S_n.

Next we note that $\#(S_n) = n!$. Indeed, let H be the subgroup of S_n consisting of those elements which leave n fixed. Then H may be identified with S_{n-1}. If σ_i $(i = 1, \ldots, n)$ is an element of S_n such that $\sigma_i(n) = i$, then it is immediately verified that $\sigma_1, \ldots, \sigma_n$ are coset representatives of H. Hence by induction

$$(S_n : 1) = n(H : 1) = n!.$$

Observe that for σ_i we could have taken the transposition τ_i, which interchanges i and n (except for $i = n$, where we could take σ_n to be the identity).

§3. NORMAL SUBGROUPS

We have already observed that the kernel of a group-homomorphism is a subgroup. We now wish to characterize such subgroups.

Let $f : G \to G'$ be a group-homomorphism, and let H be its kernel. If x is an element of G, then $xH = Hx$, because both are equal to $f^{-1}(f(x))$. We can also rewrite this relation as $xHx^{-1} = H$.

Conversely, let G be a group, and let H be a subgroup. Assume that for all elements x of G we have $xH \subset Hx$ (or equivalently, $xHx^{-1} \subset H$). If we write x^{-1} instead of x, we get $H \subset xHx^{-1}$, whence $xHx^{-1} = H$. Thus our condition is equivalent to the condition $xHx^{-1} = H$ for all $x \in G$. A subgroup H satisfying this condition will be called **normal**. We shall now see that a normal subgroup is the kernel of a homomorphism.

Let G' be the set of cosets of H. (By assumption, a left coset is equal to a right coset, so we need not distinguish between them.) If xH and yH are cosets, then their product $(xH)(yH)$ is also a coset, because

$$xHyH = xyHH = xyH.$$

By means of this product, we have therefore defined a law of composition on G' which is associative. It is clear that the coset H itself is a unit element for this law of composition, and that $x^{-1}H$ is an inverse for the coset xH. Hence G' is a group.

Let $f: G \to G'$ be the mapping such that $f(x)$ is the coset xH. Then f is clearly a homomorphism, and (the subgroup) H is contained in its kernel. If $f(x) = H$, then $xH = H$. Since H contains the unit element, it follows that $x \in H$. Thus H is equal to the kernel, and we have obtained our desired homomorphism.

The group of cosets of a normal subgroup H is denoted by G/H (which we read G modulo H, or G mod H). The map f of G onto G/H constructed above is called the **canonical map**, and G/H is called the **factor group** of G by H.

Remarks

1. Let $\{H_i\}_{i \in I}$ be a family of normal subgroups of G. Then the subgroup

$$H = \bigcap_{i \in I} H_i$$

is a normal subgroup. Indeed, if $y \in H$, and $x \in G$, then xyx^{-1} lies in each H_i, whence in H.

2. Let S be a subset of G and let $N = N_S$ be the set of all elements $x \in G$ such that $xSx^{-1} = S$. Then N is obviously a subgroup of G, called the **normalizer** of S. If S consists of one element a, then N is also called the **centralizer** of a. More generally, let Z_S be the set of all elements $x \in G$ such that $xyx^{-1} = y$ for all $y \in S$. Then Z_S is called the **centralizer** of S. The centralizer of G itself is called the **center** of G. It is the subgroup of G consisting of all elements of G commuting with all other elements, and is obviously a normal subgroup of G.

Examples. We shall give more examples of normal subgroups later when we have more theorems to prove the normality. Here we give only two examples.

First, from linear algebra, note that the determinant is a homomorphism from the multiplicative group of square matrices into the multiplicative group of a field. The kernel is called the **special linear group**, and is normal.

Second, let G be the set of all maps $T_{a,b}$: $\mathbf{R} \to \mathbf{R}$ such that $T_{a,b}(x) = ax + b$, with $a \neq 0$ and b arbitrary. Then G is a group under composition of mappings. Let A be the multiplicative group of maps of the form $T_{a,0}$ (isomorphic to $\mathbf{R}^*$, the non-zero elements of $\mathbf{R}$), and let N be the group of translations $T_{1,b}$ with $b \in \mathbf{R}$. Then the reader will verify at once that $T_{a,b} \mapsto a$ is a homomorphism of G onto the multiplicative group, whose kernel is the group of translations, which is therefore normal. Furthermore, we have $G = AN = NA$, and $N \cap A = \{\mathrm{id}\}$. In the terminology of Exercise 12, G is the **semidirect product** of A and N.

Let H be a subgroup of G. Then H is obviously a normal subgroup of its normalizer N_H. We leave the following statements as exercises:

If K is any subgroup of G containing H and such that H is normal in K, then $K \subset N_H$.

If K is a subgroup of N_H, then KH is a group and H is normal in KH.
The normalizer of H is the largest subgroup of G in which H is normal.

Let G be a group and H a normal subgroup. Let $x, y \in G$. We shall write

$$x \equiv y \pmod{H}$$

if x and y lie in the same coset of H, or equivalently if xy^{-1} (or $y^{-1}x$) lie in H. We read this relation "x and y are congruent modulo H."

When G is an additive group, then

$$x \equiv 0 \pmod{H}$$

means that x lies in H, and

$$x \equiv y \pmod{H}$$

means that $x - y$ (or $y - x$) lies in H. This notation of congruence is used mostly for additive groups.

Let

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

be a sequence of homomorphisms. We shall say that this sequence is **exact** if $\operatorname{Im} f = \operatorname{Ker} g$. For example, if H is a normal subgroup of G then the sequence

$$H \xrightarrow{j} G \xrightarrow{\varphi} G/H$$

is exact (where j = inclusion and φ = canonical map). A sequence of homomorphisms having more than one term, like

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to \cdots \xrightarrow{f_{n-1}} G_n,$$

is called **exact** if it is exact at each joint, i.e. if for each $i = 1, \ldots, n-2$,

$$\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}.$$

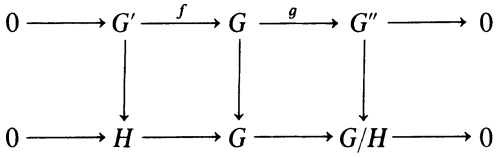
For example letting 0 be the trivial group, to say that

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$$

is exact means that f is injective, that $\operatorname{Im} f = \operatorname{Ker} g$, and that g is surjective. If $H = \operatorname{Ker} g$ then this sequence is essentially the same as the exact sequence

$$0 \to H \to G \to G/H \to 0.$$

More precisely, there exists a commutative diagram



in which the vertical maps are isomorphisms, and the rows are exact.

Next we describe some homomorphisms, all of which are called **canonical.**

(i) Let G, G' be groups and $f: G \to G'$ a homomorphism whose kernel is H. Let $\varphi: G \to G/H$ be the canonical map. Then there exists a unique homomorphism $f_*: G/H \to G'$ such that $f = f_* \circ \varphi$, and f_* is injective.

To define f_*, let xH be a coset of H. Since $f(xy) = f(x)$ for all $y \in H$, we define $f_*(xH)$ to be $f(x)$. This value is independent of the choice of coset representative x, and it is then trivially verified that f_* is a homomorphism, is injective, and is the unique homomorphism satisfying our requirements. We shall say that f_* is **induced** by f.

Our homomorphism f_* induces an isomorphism

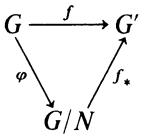
$$\lambda: G/H \to \operatorname{Im} f$$

of G/H onto the image of f, and thus f can be factored into the following succession of homomorphisms:

$$G \xrightarrow{\varphi} G/H \xrightarrow{\lambda} \operatorname{Im} f \xrightarrow{j} G'.$$

Here, j is the inclusion of $\operatorname{Im} f$ in G'.

(ii) Let G be a group and H a subgroup. Let N be the intersection of all normal subgroups containing H. Then N is normal, and hence is the smallest normal subgroup of G containing H. Let $f: G \to G'$ be a homomorphism whose kernel contains H. Then the kernel of f contains N, and there exists a unique homomorphism $f_*: G/N \to G'$, said to be induced by f, making the following diagram commutative:



As before, φ is the canonical map.

We can define f_* as in (1) by the rule

$$f_*(xN) = f(x).$$

This is well defined, and is trivially verified to satisfy all our requirements.

(**iii**) Let G be group and $H \supset K$ two normal subgroups of G. Then K is normal in H, and we can define a map of G/K onto G/H by associating with each coset xK the coset xH. It is immediately verified that this map is a homomorphism, and that its kernel consists of all cosets xK such that $x \in H$. Thus we have a canonical isomorphism

$$\boxed{(G/K)/(H/K) \approx G/H.}$$

One could also describe this isomorphism using (i) and (ii). We leave it to the reader to show that we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{id}} & & \\ 0 & \longrightarrow & H/K & \longrightarrow & G/K & \longrightarrow & G/H & \longrightarrow & 0 \end{array}$$

where the rows are exact.

(**iv**) Let G be a group and let H, K be two subgroups. Assume that H is contained in the normalizer of K. Then $H \cap K$ is obviously a normal subgroup of H, and equally obviously $HK = KH$ is a subgroup of G. There is a surjective homomorphism

$$H \to HK/K$$

associating with each $x \in H$ the coset xK of K in the group HK. The reader will verify at once that the kernel of this homomorphism is exactly $H \cap K$. Thus we have a canonical isomorphism

$$\boxed{H/(H \cap K) \approx HK/K.}$$

(**v**) Let $f: G \to G'$ be a group homomorphism, let H' be a normal subgroup of G', and let $H = f^{-1}(H')$.

$$\begin{array}{ccc} G & \longrightarrow & G' \\ \uparrow & & \uparrow \\ f^{-1}(H') & \longrightarrow & H' \end{array}$$

Then $f^{-1}(H')$ is normal in G. [*Proof*: If $x \in G$, then $f(xHx^{-1}) = f(x)f(H)f(x)^{-1}$ is contained in H', so $xHx^{-1} \subset H$.] We then obtain a homomorphism

$$G \to G' \to G'/H'$$

composing f with the canonical map of G' onto G'/H', and the kernel of this composite is H. Hence we get an injective homomorphism

$$\bar{f}: G/H \to G'/H'$$

again called canonical, giving rise to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \bar{f}} & & \\ 0 & \longrightarrow & H' & \longrightarrow & G' & \longrightarrow & G'/H' & \longrightarrow & 0. \end{array}$$

If f is surjective, then $\bar{f}$ is an isomorphism.

We shall now describe some applications of our homomorphism statements.

Let G be a group. A sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m$$

is called a **tower** of subgroups. The tower is said to be **normal** if each G_{i+1} is normal in G_i $(i = 0, \ldots, m-1)$. It is said to be **abelian** (resp. **cyclic**) if it is normal and if each factor group G_i/G_{i+1} is abelian (resp. cyclic).

Let $f: G \to G'$ be a homomorphism and let

$$G' = G'_0 \supset G'_1 \supset \cdots \supset G'_m$$

be a normal tower in G'. Let $G_i = f^{-1}(G'_i)$. Then the G_i $(i = 0, \ldots, m)$ form a normal tower. If the G'_i form an abelian tower (resp. cyclic tower) then the G_i form an abelian tower (resp. cyclic tower), because we have an injective homomorphism

$$G_i/G_{i+1} \to G'_i/G'_{i+1}$$

for each i, and because a subgroup of an abelian group (resp. a cyclic group) is abelian (resp. cyclic).

A **refinement** of a tower

$$G = G_0 \supset G_1 \supset \cdots \supset G_m$$

is a tower which can be obtained by inserting a finite number of subgroups in the given tower. A group is said to be **solvable** if it has an abelian tower, whose last element is the trivial subgroup (i.e. $G_m = \{e\}$ in the above notation).

Proposition 3.1. *Let G be a finite group. An abelian tower of G admits a cyclic refinement. Let G be a finite solvable group. Then G admits a cyclic tower whose last element is $\{e\}$.*

Proof. The second assertion is an immediate consequence of the first, and it clearly suffices to prove that if G is finite, abelian, then G admits a cyclic tower ending with $\{e\}$. We use induction on the order of G. Let x be an element of G. We may assume that $x \neq e$. Let X be the cyclic group generated by x. Let $G' = G/X$. By induction, we can find a cyclic tower in G', and its inverse image is a cyclic tower in G whose last element is X. If we refine this tower by inserting $\{e\}$ at the end, we obtain the desired cyclic tower.

Example. In Theorem 6.5 it will be proved that a group whose order is a prime power is solvable.

Example. One of the major results of group theory is the Feit-Thompson theorem that all finite groups of odd order are solvable. Cf. [Go 68].

Example. Solvable groups will occur in field theory as the Galois groups of solvable extensions. See Chapter VI, Theorem 7.2.

Example. We assume the reader knows the basic notions of linear algebra. Let k be a field. Let $G = GL(n, k)$ be the group of invertible $n \times n$ matrices in k. Let $T = T(n, k)$ be the upper triangular group; that is, the subgroup of matrices which are 0 below the diagonal. Let D be the diagonal group of diagonal matrices with non-zero components on the diagonal. Let N be the additive group of matrices which are 0 on and below the diagonal, and let $U = I + N$, where I is the unit $n \times n$ matrix. Then U is a subgroup of G. (Note that N consists of nilpotent matrices, i.e. matrices A such that $A^m = 0$ for some positive integer m. Then $(I - A)^{-1} = I + A + A^2 + \ldots + A^{m-1}$ is computed using the geometric series.) Given a matrix $A \in T$, let $\operatorname{diag}(A)$ be the diagonal matrix which has the same diagonal components as A. Then the reader will verify that we get a surjective homomorphism

$$T \to D \quad \text{given by} \quad A \mapsto \operatorname{diag}(A).$$

The kernel of this homomorphism is precisely U. More generally, observe that for $r \geqq 2$, the set N^{r-1} consists of all matrices of the form

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_{1r} & \cdots\cdots & a_{1n} \\ 0 & 0 & \cdots & 0 & 0 & a_{2,r+1} \cdots & a_{2n} \\ \vdots & \vdots & & & & \ddots & \vdots \\ 0 & 0 & \cdots\cdots\cdots\cdots & & & & a_{n-r+1,n} \\ 0 & 0 & \cdots\cdots\cdots\cdots & & & & 0 \\ & & & \cdots & & & \\ 0 & 0 & \cdots\cdots\cdots\cdots & & & & 0 \end{pmatrix}$$

Let $U_r = I + N^r$. Then $U_1 = U$ and $U_r \supset U_{r+1}$. Furthermore, U_{r+1} is normal in U_r, and the factor group is isomorphic to the additive group (!) k^{n-r}, under the the mapping which sends $I + M$ to the $n - r$-tuple $(a_{1r+1}, \ldots, a_{n-r,n}) \in k^{n-r}$. This $n - r$-tuple could be called the r-th upper diagonal. Thus we obtain an abelian tower

$$T \supset U = U_1 \supset U_2 \supset \ldots \supset U_n = \{I\}.$$

Theorem 3.2. *Let G be a group and H a normal subgroup. Then G is solvable if and only if H and G/H are solvable.*

Proof. We prove that G solvable implies that H is solvable. Let $G = G_0 \supset G_1 \supset \ldots \supset G_r = \{e\}$ be a tower of groups with G_{i+1} normal in G_i and such that G_i/G_{i+1} is abelian. Let $H_i = H \cap G_i$. Then H_{i+1} is normal in H_i, and we have an embedding $H_i/H_{i+1} \to G_i/G_{i+1}$, whence H_i/H_{i+1} is abelian, whence proving that H is solvable. We leave the proofs of the other statements to the reader.

Let G be a group. A **commutator** in G is a group element of the form $xyx^{-1}y^{-1}$ with $x, y \in G$. Let G^c be the subgroup of G generated by the commutators. We call G^c the **commutator subgroup** of G. As an exercise, prove that G^c is normal in G, and that every homomorphism $f: G \to G'$ into a commutative group G' contains G^c in its kernel, and consequently factors through the factor commutator group G/G^c. Observe that G/G^c itself is commutative. Indeed, if $\bar{x}$ denotes the image of x in G/G^c, then by definition we have $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e}$, so $\bar{x}$ and $\bar{y}$ commute. In light of the definition of solvability, it is clear that the commutator group is at the heart of solvability and non-solvability problems.

A group G is said to be **simple** if it is non-trivial, and has no normal subgroups other than $\{e\}$ and G itself.

Examples. An abelian group is simple if and only if it is cyclic of prime order. Indeed, suppose A abelian and non-trivial. Let $a \in A$, $a \neq e$. If a generates an infinite cyclic group, then a^2 generates a proper subgroup and so A is not simple. If a has finite period, and A is simple, then $A = \langle a \rangle$. Let n be the period and suppose n not prime. Write $n = rs$ with $r, s > 1$. Then $a^r \neq e$ and a^r generates a proper subgroup, contradicting the simplicity of A, so a has prime period and A is cyclic of order p.

Examples. Using commutators, we shall give examples of simple groups in Theorem 5.5 (the alternating group), and in Theorem 9.2 of Chapter XIII ($PSL_n(F)$, a group of matrices to be defined in that chapter). Since a non-cyclic simple group is not solvable, we get thereby examples of non-solvable groups.

A major program of finite group theory is the classification of all finite simple groups. Essentially most of them (if not all) have natural representations as subgroups of linear maps of suitable vector spaces over suitable fields, in a suitably natural way. See [Go 82], [Go 86], [Sol 01] for surveys. Gaps in purported proofs have been found. As of 2001, these are still incomplete.

Next we are concerned with towers of subgroups such that the factor groups G_i/G_{i+1} are simple. The next lemma is for use in the proof of the Jordan-Hölder and Schreier theorems.

Lemma 3.3. (Butterfly Lemma.) (Zassenhaus) *Let U, V be subgroups of a group. Let u, v be normal subgroups of U and V, respectively. Then*

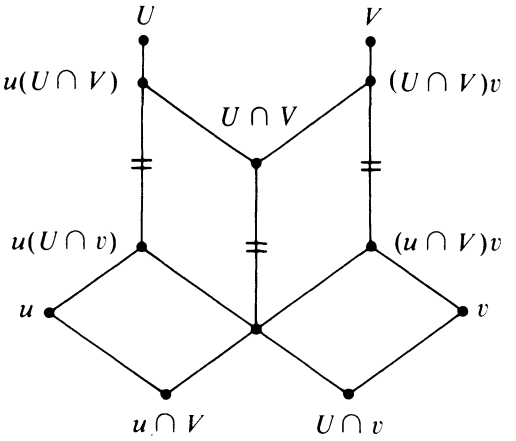
$$u(U \cap v) \quad \textit{is normal in} \quad u(U \cap V),$$

$$(u \cap V)v \quad \textit{is normal in} \quad (U \cap V)v,$$

and the factor groups are isomorphic, i.e.

$$u(U \cap V)/u(U \cap v) \approx (U \cap V)v/(u \cap V)v.$$

Proof. The combination of groups and factor groups becomes clear if one visualizes the following diagram of subgroups (which gives its name to the lemma):



In this diagram, we are given U, u, V, v. All the other points in the diagram correspond to certain groups which can be determined as follows. The intersection of two line segments going downwards represents the intersection of groups. Two lines going upwards meet in a point which represents the product of two subgroups (i.e. the smallest subgroup containing both of them).

We consider the two parallelograms representing the wings of the butterfly, and we shall give isomorphisms of the factor groups as follows:

$$\frac{u(U \cap V)}{u(U \cap v)} \approx \frac{U \cap V}{(u \cap V)(U \cap v)} \approx \frac{(U \cap V)v}{(u \cap V)v}.$$

In fact, the vertical side common to both parallelograms has $U \cap V$ as its top end point, and $(u \cap V)(U \cap v)$ as its bottom end point. We have an isomorphism

$$(U \cap V)/(u \cap V)(U \cap v) \approx u(U \cap V)/u(U \cap v).$$

This is obtained from the isomorphism theorem

$$H/(H \cap N) \approx HN/N$$

by setting $H = U \cap V$ and $N = u(U \cap v)$. This gives us the isomorphism on the left. By symmetry we obtain the corresponding isomorphism on the right, which proves the Butterfly lemma.

Let G be a group, and let

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\},$$

$$G = H_1 \supset H_2 \supset \cdots \supset H_s = \{e\}$$

be normal towers of subgroups, ending with the trivial group. We shall say that these towers are **equivalent** if $r = s$ and if there exists a permutation of the

indices $i = 1, \ldots, r-1$, written $i \mapsto i'$, such that

$$G_i/G_{i+1} \approx H_{i'}/H_{i'+1}.$$

In other words, the sequences of factor groups in our two towers are the same, up to isomorphisms, and a permutation of the indices.

Theorem 3.4. (Schreier) *Let G be a group. Two normal towers of subgroups ending with the trivial group have equivalent refinements.*

Proof. Let the two towers be as above. For each $i = 1, \ldots, r-1$ and $j = 1, \ldots, s$ we define

$$G_{ij} = G_{i+1}(H_j \cap G_i).$$

Then $G_{is} = G_{i+1}$, and we have a refinement of the first tower:

$$\begin{aligned} G = G_{11} &\supset G_{12} \supset \cdots \supset G_{1,s-1} \supset G_2 \\ &= G_{21} \supset G_{22} \supset \cdots \supset G_{r-1,1} \supset \cdots \supset G_{r-1,s-1} \supset \{e\}. \end{aligned}$$

Similarly, we define

$$H_{ji} = H_{j+1}(G_i \cap H_j),$$

for $j = 1, \ldots, s-1$ and $i = 1, \ldots, r$. This yields a refinement of the second tower. By the butterfly lemma, for $i = 1, \ldots, r-1$ and $j = 1, \ldots, s-1$ we have isomorphisms

$$G_{ij}/G_{i,j+1} \approx H_{ji}/H_{j,i+1}.$$

We view each one of our refined towers as having $(r-1)(s-1)+1$ elements, namely G_{ij} $(i = 1, \ldots, r-1; j = 1, \ldots, s-1)$ and $\{e\}$ in the first case, H_{ji} and $\{e\}$ in the second case. The preceding isomorphism for each pair of indices (i, j) shows that our refined towers are equivalent, as was to be proved.

A group G is said to be **simple** if it is non-trivial, and has no normal subgroups other than $\{e\}$ and G itself.

Theorem 3.5. (Jordan-Hölder) *Let G be a group, and let*

$$G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}$$

be a normal tower such that each group G_i/G_{i+1} is simple, and $G_i \neq G_{i+1}$ for $i = 1, \ldots, r-1$. Then any other normal tower of G having the same properties is equivalent to this one.

Proof. Given any refinement $\{G_{ij}\}$ as before for our tower, we observe that for each i, there exists precisely one index j such that $G_i/G_{i+1} = G_{ij}/G_{i,j+1}$. Thus the sequence of non-trivial factors for the original tower, or the refined tower, is the same. This proves our theorem.

Bibliography

[Go 68] D. GORENSTEIN, *Finite groups*, Harper and Row, 1968

[Go 82] D. GORENSTEIN, *Finite simple groups*, Plenum Press, 1982

[Go 83] D. GORENSTEIN, *The Classification of Finite Simple Groups*, Plenum Press, 1983

[Go 86] D. GORENSTEIN, Classifying the finite simple groups, *Bull. AMS* **14** No. 1 (1986), pp. 1–98

[So 01] R. SOLOMON, A brief history of the classification of the finite simple groups, *Bull. AMS* **38**, 3 (2001) pp. 315–352

§4. CYCLIC GROUPS

The integers $\mathbf{Z}$ form an additive group. We shall determine its subgroups. Let H be a subgroup of $\mathbf{Z}$. If H is not trivial, let a be the smallest positive integer in H. We contend that H consists of all elements na, with $n \in \mathbf{Z}$. To prove this, let $y \in H$. There exist integers n, r with $0 \leqq r < a$ such that

$$y = na + r.$$

Since H is a subgroup and $r = y - na$, we have $r \in H$, whence $r = 0$, and our assertion follows.

Let G be a group. We shall say that G is **cyclic** if there exists an element a of G such that every element x of G can be written in the form a^n for some $n \in \mathbf{Z}$ (in other words, if the map $f: \mathbf{Z} \to G$ such that $f(n) = a^n$ is surjective). Such an element a of G is then called a **generator** of G.

Let G be a group and $a \in G$. The subset of all elements a^n $(n \in \mathbf{Z})$ is obviously a cyclic subgroup of G. If m is an integer such that $a^m = e$ and $m > 0$ then we shall call m an **exponent** of a. We shall say that $m > 0$ is an **exponent** of G if $x^m = e$ for all $x \in G$.

Let G be a group and $a \in G$. Let $f: \mathbf{Z} \to G$ be the homomorphism such that $f(n) = a^n$ and let H be the kernel of f. Two cases arise:

1. The kernel is trivial. Then f is an isomorphism of $\mathbf{Z}$ onto the cyclic subgroup of G generated by a, and this subgroup is infinite cyclic. If a generates G, then G is cyclic. We also say that a has **infinite period**.

2. The kernel is not trivial. Let d be the smallest positive integer in the kernel. Then d is called the **period** of a. If m is an integer such that $a^m = e$ then $m = ds$ for some integer s. We observe that the elements $e, a, \ldots, a^{d-1}$ are

distinct. Indeed, if $a^r = a^s$ with $0 \leqq r, s \leqq d - 1$, and say $r \leqq s$, then $a^{s-r} = e$. Since $0 \leqq s - r < d$ we must have $s - r = 0$. The cyclic subgroup generated by a has order d. Hence by Proposition 2.2:

Proposition 4.1. *Let G be a finite group of order $n > 1$. Let a be an element of G, $a \neq e$. Then the period of a divides n. If the order of G is a prime number p, then G is cyclic and the period of any generator is equal to p.*

Furthermore:

Proposition 4.2. *Let G be a cyclic group. Then every subgroup of G is cyclic. If f is a homomorphism of G, then the image of f is cyclic.*

Proof. If G is infinite cyclic, it is isomorphic to $\mathbf{Z}$, and we determined above all subgroups of $\mathbf{Z}$, finding that they are all cyclic. If $f: G \to G'$ is a homomorphism, and a is a generator of G, then $f(a)$ is obviously a generator of $f(G)$, which is therefore cyclic, so the image of f is cyclic. Next let H be a subgroup of G. We want to show H cyclic. Let a be a generator of G. Then we have a surjective homomorphism $f: \mathbf{Z} \to G$ such that $f(n) = a^n$. The inverse image $f^{-1}(H)$ is a subgroup of $\mathbf{Z}$, and therefore equal to $m\mathbf{Z}$ for some positive integer m. Since f is surjective, we also have a surjective homomorphism $m\mathbf{Z} \to H$. Since $m\mathbf{Z}$ is cyclic (generated additively by m), it follows that H is cyclic, thus proving the proposition.

We observe that two cyclic groups of the same order m are isomorphic. Indeed, if G is cyclic of order m with generator a, then we have a surjective homomorphism $f: \mathbf{Z} \to G$ such that $f(n) = a^n$, and if $k\mathbf{Z}$ is the kernel, with k positive, then we have an isomorphism $\mathbf{Z}/k\mathbf{Z} \approx G$, so $k = m$. If $u: G_1 \to \mathbf{Z}/m\mathbf{Z}$ and $v: G_2 \to \mathbf{Z}/m\mathbf{Z}$ are isomorphisms of two cyclic groups with $\mathbf{Z}/m\mathbf{Z}$, then $v^{-1} \circ u: G_1 \to G_2$ is an isomorphism.

Proposition 4.3.

(i) *An infinite cyclic group has exactly two generators (if a is a generator, then a^{-1} is the only other generator).*

(ii) *Let G be a finite cyclic group of order n, and let x be a generator. The set of generators of G consists of those powers x^v of x such that v is relatively prime to n.*

(iii) *Let G be a cyclic group, and let a, b be two generators. Then there exists an automorphism of G mapping a onto b. Conversely, any automorphism of G maps a on some generator of G.*

(iv) *Let G be a cyclic group of order n. Let d be a positive integer dividing n. Then there exists a unique subgroup of G of order d.*

(v) *Let G_1, G_2 be cyclic of orders m, n respectively. If m, n are relatively prime then $G_1 \times G_2$ is cyclic.*

(vi) *Let G be a finite abelian group. If G is not cyclic, then there exists a prime p and a subgroup of G isomorphic to $C \times C$, where C is cyclic of order p.*

Proof. We leave the first three statements to the reader, and prove the others.

(iv) Let $d|n$. Let $m = n/d$. Let $f : \mathbf{Z} \to G$ be a surjective homomorphism. Then $f(m\mathbf{Z})$ is a subgroup of G, and from the isomorphism $\mathbf{Z}/m\mathbf{Z} \approx G/f(m\mathbf{Z})$ we conclude that $f(m\mathbf{Z})$ has index m in G, whence $f(m\mathbf{Z})$ has order d. Conversely, let H be a subgroup of order d. Then $f^{-1}(H) = m\mathbf{Z}$ for some positive integer m, so $H = f(m\mathbf{Z})$, $\mathbf{Z}/m\mathbf{Z} \approx G/H$, so $n = md$, $m = n/d$ and H is uniquely determined.

(v) Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be cyclic groups of orders m, n, relatively prime. Consider the homomorphism $\mathbf{Z} \to A \times B$ such that $k \mapsto (a^k, b^k)$. An element in its kernel must be divisible both by m and n, hence by their product since m, n are relatively prime. Conversely, it is clear that $mn\mathbf{Z}$ is contained in the kernel, so the kernel is $mn\mathbf{Z}$. The image of $\mathbf{Z} \to A \times B$ is surjective by the Chinese remainder theorem. This proves **(v)**. (A reader who does not know the Chinese remainder theorem can see a proof in the more general context of Chapter II, Theorem 2.2.)

(vi) This characterization of cyclic groups is an immediate consequence of the structure theorem which will be proved in §8, because if G is not cyclic, then by Theorem 8.1 and **(v)** we are reduced to the case when G is a p-group, and by Theorem 8.2 there are at least two factors in the direct product (or sum) decomposition, and each contains a cyclic subgroup of order p, whence G contains their direct product (or sum). Statement **(vi)** is, of course, easier to prove than the full structure theorem, and it is a good exercise for the reader to formulate the simpler arguments which yield **(vi)** directly.

Note. For the group of automorphisms of a cyclic group, see the end of Chapter II, §2.

§5. OPERATIONS OF A GROUP ON A SET

Let G be a group and let S be a set. An **operation** or an **action** of G on S is a homomorphism

$$\pi : G \to \mathrm{Perm}(S)$$

of G into the group of permutations of S. We then call S a **G-set**. We denote the permutation associated with an element $x \in G$ by π_x. Thus the homomorphism is denoted by $x \mapsto \pi_x$. Given $s \in S$, the image of s under the permutation π_x is $\pi_x(s)$. From such an operation we obtain a mapping

$$G \times S \to S,$$

which to each pair (x, s) with $x \in G$ and $s \in S$ associates the element $\pi_x(s)$. We often abbreviate the notation and write simply xs instead of $\pi_x(s)$. With the simpler notation, we have the two properties:

For all $x, y \in G$ and $s \in S$, we have $x(ys) = (xy)s$.
If e is the unit element of G, then $es = s$ for all $s \in S$.

Conversely, if we are given a mapping $G \times S \to S$, denoted by $(x, s) \mapsto xs$, satisfying these two properties, then for each $x \in G$ the map $s \mapsto xs$ is a permutation of S, which we then denote by $\pi_x(s)$. Then $x \mapsto \pi_x$ is a homomorphism of G into $\mathrm{Perm}(S)$. So an operation of G on S could also be defined as a mapping $G \times S \to S$ satisfying the above two properties. The most important examples of representations of G as a group of permutations are the following.

1. Conjugation. For each $x \in G$, let $\mathbf{c}_x: G \to G$ be the map such that $\mathbf{c}_x(y) = xyx^{-1}$. Then it is immediately verified that the association $x \mapsto \mathbf{c}_x$ is a homomorphism $G \to \mathrm{Aut}(G)$, and so this map gives an operation of G on itself, called **conjugation**. The kernel of the homomorphism $x \mapsto \mathbf{c}_x$ is a normal subgroup of G, which consists of all $x \in G$ such that $xyx^{-1} = y$ for all $y \in G$, i.e. all $x \in G$ which commute with every element of G. This kernel is called the **center** of G. Automorphisms of G of the form $\mathbf{c}_x$ are called **inner**.

To avoid confusion about the operation on the left, we don't write xy for $\mathbf{c}_x(y)$. Sometimes, one writes

$$\mathbf{c}_{x^{-1}}(y) = x^{-1}yx = y^x,$$

i.e. one uses an exponential notation, so that we have the rules

$$y^{(xz)} = (y^x)^z \quad \text{and} \quad y^e = y$$

for all $x, y, z \in G$. Similarly, ${}^xy = xyx^{-1}$ and ${}^z({}^xy) = {}^{zx}y$.

We note that G also operates by conjugation on the set of subsets of G. Indeed, let S be the set of subsets of G, and let $A \in S$ be a subset of G. Then xAx^{-1} is also a subset of G which may be denoted by $\mathbf{c}_x(A)$, and one verifies trivially that the map

$$(x, A) \mapsto xAx^{-1}$$

of $G \times S \to S$ is an operation of G on S. We note in addition that if A is a subgroup of G then xAx^{-1} is also a subgroup, so that G operates on the set of subgroups by conjugation.

If A, B are two subsets of G, we say that they are **conjugate** if there exists $x \in G$ such that $B = xAx^{-1}$.

2. Translation. For each $x \in G$ we define the translation $T_x: G \to G$ by $T_x(y) = xy$. Then the map

$$(x, y) \mapsto xy = T_x(y)$$

defines an operation of G on itself. *Warning*: T_x is not a group-homomorphism! Only a permutation of G.

Similarly, G operates by translation on the set of subsets, for if A is a subset of G, then $xA = T_x(A)$ is also a subset. If H is a subgroup of G, then $T_x(H) = xH$ is in general not a subgroup but a coset of H, and hence we see that G operates by translation on the set of cosets of H. We denote the set of left cosets of H by G/H. Thus even though H need not be normal, G/H is a G-set. It has become customary to denote the set of *right* cosets by $H\backslash G$.

The above two representations of G as a group of permutations will be used frequently in the sequel. In particular, the representation by conjugation will be used throughout the next section, in the proof of the Sylow theorems.

3. Example from linear algebra. We assume the reader knows basic notions of linear algebra. Let k be a field and let V be a vector space over k. Let $G = GL(V)$ be the group of linear automorphisms of V. For $A \in G$ and $v \in V$, the map $(A, v) \mapsto Av$ defines an operation of G on V. Of course, G is a subgroup of the group of permutations $\mathrm{Perm}(V)$. Similarly, let $V = k^n$ be the vector space of (vertical) n-tuples of elements of k, and let G be the group of invertible $n \times n$ matrices with components in k. Then G operates on k^n by $(A, X) \mapsto AX$ for $A \in G$ and $X \in k^n$.

Let S, S' be two G-sets, and $f : S \to S'$ a map. We say that f is a **morphism of G-sets**, or a **G-map**, if

$$f(xs) = xf(s)$$

for all $x \in G$ and $s \in S$. (We shall soon define categories, and see that G-sets form a category.)

We now return to the general situation, and consider a group operating on a set S. Let $s \in S$. The set of elements $x \in G$ such that $xs = s$ is obviously a subgroup of G, called the **isotropy** group of s in G, and denoted by G_s.

When G operates on itself by conjugation, then the isotropy group of an element is none other than the normalizer of this element. Similarly, when G operates on the set of subgroups by conjugation, the isotropy group of a subgroup is again its normalizer.

Let G operate on a set S. Let s, s' be elements of S, and y an element of G such that $ys = s'$. Then

$$G_{s'} = yG_sy^{-1}$$

Indeed, one sees at once that yG_sy^{-1} leaves s' fixed. Conversely, if $x's' = s'$ then $x'ys = ys$, so $y^{-1}x'y \in G_s$ and $x' \in yG_sy^{-1}$. Thus the isotropy groups of s and s' are conjugate.

Let K be the kernel of the representation $G \to \mathrm{Perm}(S)$. Then directly from the definitions, we obtain that

$$K = \bigcap_{s \in S} G_s = \text{intersection of all isotropy groups.}$$

An action or operation of G is said to be **faithful** if $K = \{e\}$; that is, the kernel of $G \to \mathrm{Perm}(S)$ is trivial. A **fixed point** of G is an element $s \in S$ such that $xs = s$ for all $x \in G$ or in other words, $G = G_s$.

Let G operate on a set S. Let $s \in S$. The subset of S consisting of all elements xs (with $x \in G$) is denoted by Gs, and is called the **orbit** of s under G. If x and y are in the same coset of the subgroup $H = G_s$, then $xs = ys$, and conversely (obvious). In this manner, we get a mapping

$$f: G/H \to S$$

given by $f(xH) = xs$, and it is clear that this map is a morphism of G-sets. In fact, one sees at once that it induces a bijection of G/H onto the orbit Gs. Consequently:

Proposition 5.1. *If G is a group operating on a set S, and $s \in S$, then the order of the orbit Gs is equal to the index $(G : G_s)$.*

In particular, when G operates by conjugation on the set of subgroups, and H is a subgroup, then:

Proposition 5.2. *The number of conjugate subgroups to H is equal to the index of the normalizer of H.*

Example. Let G be a group and H a subgroup of index 2. Then H is normal in G.

Proof. Note that H is contained in its normalizer N_H, so the index of N_H in G is 1 or 2. If it is 1, then we are done. Suppose it is 2. Let G operate by conjugation on the set of subgroups. The orbit of H has 2 elements, and G operates on this orbit. In this way we get a homomorphism of G into the group of permutations of 2 elements. Since there is one conjugate of H unequal to H, then the kernel of our homomorphism is normal, of index 2, hence equal to H, which is normal, a contradiction which concludes the proof.

For a generalization and other examples, see Lemma 6.7.

In general, an operation of G on S is said to be **transitive** if there is only one orbit.

Examples. The symmetric group S_n operates transitively on $\{1, 2, \ldots, n\}$. (See p. 30.) In Proposition 2.1 of Chapter VII, we shall see a non-trivial example of transitive action of a Galois group operating on the primes lying above a given prime in the ground ring. In topology, suppose we have a universal covering space $p : X' \to X$, where X is connected. Given $x \in X$, the fundamental group $\pi_1(X)$ operates transitively on the inverse image $p^{-1}(x)$.

Example. Let $\mathfrak{H}$ be the upper half-plane; that is, the set of complex numbers $z = x + iy$ such that $y > 0$. Let $G = SL_2(\mathbf{R})$ (2×2 matrices with determinant 1). For

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, \text{ we let } \alpha z = \frac{az + b}{cz + d}.$$

Readers will verify by brute force that this defines an operation of G on $\mathfrak{H}$. The isotropy group of i is the group of matrices

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \quad \text{with } \theta \text{ real.}$$

This group is usually denoted by K. The group G operates transitively. You can verify all these statements as easy exercises.

Let G operate on a set S. Then two orbits of G are either disjoint or are equal. Indeed, if Gs_1 and Gs_2 are two orbits with an element s in common, then $s = xs_1$ for some $x \in G$, and hence $Gs = Gxs_1 = Gs_1$. Similarly, $Gs = Gs_2$. Hence S is the disjoint union of the distinct orbits, and we can write

$$S = \bigcup_{i \in I} Gs_i \qquad \text{(disjoint)}, \qquad \text{also denoted } S = \coprod_{i \in I} Gs_i,$$

where I is some indexing set, and the s_i are elements of distinct orbits. If S is finite, this gives a decomposition of the order of S as a sum of orders of orbits, which we call the **orbit decomposition formula**, namely

$$\boxed{\operatorname{card}(S) = \sum_{i \in I} (G : G_{s_i}).}$$

Let x, y be elements of a group (or monoid) G. They are said to **commute** if $xy = yx$. If G is a group, the set of all elements $x \in G$ which commute with all elements of G is a subgroup of G which we called the **center** of G. Let G act on itself by conjugation. Then x is in the center if and only if the orbit of x is x itself, and thus has one element. In general, the order of the orbit of x is equal to the index of the normalizer of x. Thus when G is a finite group, the above formula reads

$$\boxed{(G : 1) = \sum_{x \in C} (G : G_x)}$$

where C is a set of representatives for the distinct conjugacy classes, and the sum is taken over all $x \in C$. This formula is also called the **class formula**.

The class formula and the orbit decomposition formula will be used systematically in the next section on Sylow groups, which may be viewed as providing examples for these formulas.

Readers interested in Sylow groups may jump immediately to the next section. The rest of this section deals with special properties of the symmetric group, which may serve as examples of the general notions we have developed.

The symmetric group. Let S_n be the group of permutations of a set with n elements. This set may be taken to be the set of integers $J_n = \{1, 2, \ldots, n\}$. Given any $\sigma \in S_n$, and any integer i, $1 \leqq i \leqq n$, we may form the orbit of i under the cyclic group generated by σ. Such an orbit is called a **cycle** for σ, and may be written

$$[i_1 i_2 \cdots i_r], \qquad \text{so} \quad \sigma(i_1) = i_2, \ldots, \sigma(i_{r-1}) = i_r, \ \sigma(i_r) = i_1.$$

Then $\{1, \ldots, n\}$ may be decomposed into a disjoint union of orbits for the cyclic group generated by σ, and therefore into disjoint cycles. Thus the effect of σ on $\{1, \ldots, n\}$ is represented by a product of disjoint cycles.

Example. The cycle [132] represents the permutation σ such that

$$\sigma(1) = 3, \qquad \sigma(3) = 2, \quad \text{and} \quad \sigma(2) = 1.$$

We have $\sigma^2(1) = 2$, $\sigma^3(1) = 1$. Thus $\{1, 3, 2\}$ is the orbit of 1 under the cyclic group generated by σ.

Example. In Exercise 38, one will see how to generate S_n by special types of generators. Perhaps the most important part of that exercise is that if n is prime, σ is an n-cycle and τ is a transposition, then σ, τ generate S_n. As an application in Galois theory, if one tries to prove that a Galois group is all of S_n (as a group of permutations of the roots), it suffices to prove that the Galois group contains an n-cycle and a transposition. See Example 6 of Chapter VI, §2.

We want to associate a sign ± 1 to each permutation. We do this in the standard way. Let f be a function of n variables, say $f: \mathbf{Z}^n \to \mathbf{Z}$, so we can evaluate $f(x_1, \ldots, x_n)$. Let σ be a permutation of J_n. We define the function $\pi(\sigma)f$ by

$$\pi(\sigma)f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Then for $\sigma, \tau \in S_n$ we have $\pi(\sigma\tau) = \pi(\sigma)\pi(\tau)$. Indeed, we use the definition applied to the function $g = \pi(\tau)f$ to get

$$\begin{aligned} \pi(\sigma)\pi(\tau)f(x_1, \ldots, x_n) &= (\pi(\tau)f)(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \\ &= f(x_{\sigma\tau(1)}, \ldots, x_{\sigma\tau(n)}) \\ &= \pi(\sigma\tau)f(x_1, \ldots, x_n). \end{aligned}$$

Since the identity in S_n operates as the identity on functions, it follows that we have obtained an operation of S_n on the set of functions. We shall write more simply σf instead of $\pi(\sigma)f$. It is immediately verified that for two functions f, g we have

$$\sigma(f + g) = \sigma f + \sigma g \quad \text{and} \quad \sigma(fg) = (\sigma f)(\sigma g).$$

If c is constant, then $\sigma(cf) = c\sigma(f)$.

Proposition 5.3. *There exists a unique homomorphism $\varepsilon: S_n \to \{\pm 1\}$ such that for every transposition τ we have $\varepsilon(\tau) = -1$.*

Proof. Let Δ be the function

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_j - x_i),$$

the product being taken for all pairs of integers i, j satisfying $1 \leqq i < j \leqq n$. Let τ be a transposition, interchanging the two integers r and s. Say $r < s$. We wish to determine

$$\tau\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_{\tau(j)} - x_{\tau(i)}).$$

For one factor involving $j = s$, $i = r$, we see that τ changes the factor $(x_s - x_r)$ to $-(x_s - x_r)$. All other factors can be considered in pairs as follows:

$$\begin{aligned} &(x_k - x_s)(x_k - x_r) \quad \text{if } k > s, \\ &(x_s - x_k)(x_k - x_r) \quad \text{if } r < k < s, \\ &(x_s - x_k)(x_r - x_k) \quad \text{if } k < r. \end{aligned}$$

Each one of these pairs remains unchanged when we apply τ. Hence we see that $\tau\Delta = -\Delta$.

Let $\varepsilon(\sigma)$ be the sign 1 or -1 such that $\sigma\Delta = \varepsilon(\sigma)\Delta$ for a permutation σ. Since $\pi(\sigma\tau) = \pi(\sigma)\pi(\tau)$, it follows at once that ε is a homomorphism, and the proposition is proved.

In particular, if $\sigma = \tau_1 \cdots \tau_m$ is a product of transpositions, then $\varepsilon(\sigma) = (-1)^m$. As a matter of terminology, we call σ **even** if $\varepsilon(\sigma) = 1$, and **odd** if $\varepsilon(\sigma) = -1$. The even permutations constitute the kernel of ε, which is called the **alternating group** A_n.

Theorem 5.4. *If $n \geqq 5$ then S_n is not solvable.*

Proof. We shall first prove that if H, N are two subgroups of S_n such that $N \subset H$ and N is normal in H, if H contains every 3-cycle, and if H/N is abelian, then N contains every 3-cycle. To see this, let i, j, k, r, s be five distinct integers in J_n, and let $\sigma = [ijk]$ and $\tau = [krs]$. Then a direct computation gives their commutator

$$\sigma\tau\sigma^{-1}\tau^{-1} = [rki].$$

Since the choice of i, j, k, r, s was arbitrary, we see that the cycles $[rki]$ all lie in N for all choices of distinct r, k, i, thereby proving what we wanted.

Now suppose that we have a tower of subgroups

$$S_n = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_m = \{e\}$$

such that H_v is normal in H_{v-1} for $v = 1, \ldots, m$, and H_v/H_{v-1} is abelian. Since S_n contains every 3-cycle, we conclude that H_1 contains every 3-cycle. By induction, we conclude that $H_m = \{e\}$ contains every 3-cycle, which is impossible, thus proving the theorem.

Remark concerning the sign $\varepsilon(\sigma)$. *A priori*, we defined the sign for a given n, so we should write $\varepsilon_n(\sigma)$. However, suppose $n < m$. Then the restriction of ε_m to S_n (viewed as a permutation of J_n leaving the elements of J_m not in J_n fixed) gives a homomorphism satisfying the conditions of Proposition 5.3, so this restriction is equal to ε_n. Thus $A_m \cap S_n = A_n$.

Next we prove some properties of the alternating group.

(a) *A_n is generated by the 3-cycles. Proof:* Consider the product of two transpositions $[ij][rs]$. If they have an element in common, the product is either the identity or a 3-cycle. If they have no element in common, then

$$[ij][rs] = [ijr][jrs],$$

so the product of two transpositions is also a product of 3-cycles. Since an even permutation is a product of an even number of transpositions, we are done.

(b) *If $n \geqq 5$, all 3-cycles are conjugate in A_n. Proof:* If γ is a permutation, then for a cycle $[i_1 \ldots i_m]$ we have

$$\gamma[i_1 \ldots i_m]\gamma^{-1} = [\gamma(i_1) \ldots \gamma(i_m)].$$

Given 3-cycles $[ijk]$ and $[i'j'k']$ there is a permutation γ such that $\gamma(i) = i'$, $\gamma(j) = j'$, and $\gamma(k) = k'$. Thus two 3-cycles are conjugate in S_n by some element γ. If γ is even, we are done. Otherwise, by assumption $n \geqq 5$ there exist r, s not equal to any one of the three elements i, j, k. Then $[rs]$ commutes with $[ijk]$, and we replace γ by $\gamma[rs]$ to prove (b).

Theorem 5.5. *If $n \geqq 5$ then the alternating group A_n is simple.*

Proof. Let N be a non-trivial normal subgroup of A_n. We prove that N contains some 3-cycle, whence the theorem follows by (b). Let $\sigma \in N$, $\sigma \neq id$, be an element which has the maximal number of fixed points; that is, integers i such that $\sigma(i) = i$. It will suffice to prove that σ is a 3-cycle or the identity. Decompose J_n into disjoint orbits of $\langle\sigma\rangle$.Then some orbits have more than one element. Suppose all orbits have 2 elements (except for the fixed points). Since σ is even, there are at least two such orbits. On their union, σ is represented as

a product of two transpositions $[ij][rs]$. Let $k \neq i, j, r, s$. Let $\tau = [rsk]$. Let $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1}$. Then σ' is a product of a conjugate of σ and σ^{-1}, so $\sigma' \in N$. But σ' leaves i, j fixed, and any element $t \in J_n$, $t \neq i, j, r, s, k$ left fixed by σ is also fixed by σ', so σ' has more fixed points than σ, contradicting our hypothesis.

So we are reduced to the case when at least one orbit of $\langle\sigma\rangle$ has $\geqq 3$ elements, say $i, j, k, \ldots$. If σ is not the 3-cycle $[ijk]$, then σ must move at least two other elements of J_n, otherwise σ is an odd permutation $[ijkr]$ for some $r \in J_n$, which is impossible. Then let σ move r, s other than i, j, k, and let $\tau = [krs]$. Let σ' be the commutator as before. Then $\sigma' \in N$ and $\sigma'(i) = i$, and all fixed points of σ are also fixed points of σ' whence σ' has more fixed points than σ, a contradiction which proves the theorem.

Example. For $n = 4$, the group A_4 is not simple. As an exercise, show that A_4 contains a unique subgroup of order 4, which is not cyclic, and which is normal. This subgroup is also normal in S_4. Write down explicitly its elements as products of transpositions.

§6. SYLOW SUBGROUPS

Let p be a prime number. By a ***p*-group**, we mean a finite group whose order is a power of p (i.e. p^n for some integer $n \geqq 0$). Let G be a finite group and H a subgroup. We call H a ***p*-subgroup** of G if H is a p-group. We call H a ***p*-Sylow** subgroup if the order of H is p^n and if p^n is the highest power of p dividing the order of G. We shall prove below that such subgroups always exist. For this we need a lemma.

Lemma 6.1. *Let G be a finite abelian group of order m, let p be a prime number dividing m. Then G has a subgroup of order p.*

Proof. We first prove by induction that if G has exponent n then the order of G divides some power of n. Let $b \in G$, $b \neq 1$, and let H be the cyclic subgroup generated by b. Then the order of H divides n since $b^n = 1$, and n is an exponent for G/H. Hence the order of G/H divides a power of n by induction, and consequently so does the order of G because

$$(G : 1) = (G : H)(H : 1).$$

Let G have order divisible by p. By what we have just seen, there exists an element x in G whose period is divisible by p. Let this period be ps for some integer s. Then $x^s \neq 1$ and obviously x^s has period p, and generates a subgroup of order p, as was to be shown.

Theorem 6.2. *Let G be a finite group and p a prime number dividing the order of G. Then there exists a p-Sylow subgroup of G.*

Proof. By induction on the order of G. If the order of G is prime, our assertion is obvious. We now assume given a finite group G, and assume the theorem proved for all groups of order smaller than that of G. If there exists a proper subgroup H of G whose index is prime to p, then a p-Sylow subgroup of H will also be one of G, and our assertion follows by induction. We may therefore assume that every proper subgroup has an index divisible by p. We now let G act on itself by conjugation. From the class formula we obtain

$$(G:1) = (Z:1) + \sum (G:G_x).$$

Here, Z is the center of G, and the term $(Z:1)$ corresponds to the orbits having one element, namely the elements of Z. The sum on the right is taken over the other orbits, and each index $(G:G_x)$ is then > 1, hence divisible by p. Since p divides the order of G, it follows that p divides the order of Z, hence in particular that G has a non-trivial center.

Let a be an element of order p in Z, and let H be the cyclic group generated by a. Since H is contained in Z, it is normal. Let $f: G \to G/H$ be the canonical map. Let p^n be the highest power of p dividing $(G:1)$. Then p^{n-1} divides the order of G/H. Let K' be a p-Sylow subgroup of G/H (by induction) and let $K = f^{-1}(K')$. Then $K \supset H$ and f maps K onto K'. Hence we have an isomorphism $K/H \approx K'$. Hence K has order $p^{n-1}p = p^n$, as desired.

For the rest of the theorems, we systematically use the notion of a fixed point. Let G be a group operating on a set S. Recall that a **fixed point** s of G in S is an element s of S such that $xs = s$ for all $x \in G$.

Lemma 6.3. *Let H be a p-group acting on a finite set S. Then:*

(a) *The number of fixed points of H is $\equiv \#(S) \bmod p$.*

(b) *If H has exactly one fixed point, then $\#(S) \equiv 1 \bmod p$.*

(c) *If $p \mid \#(S)$, then the number of fixed points of H is $\equiv 0 \bmod p$.*

Proof. We repeatedly use the orbit formula

$$\#(S) = \sum (H : H_{s_i}).$$

For each fixed point s_i we have $H_{s_i} = H$. For s_i not fixed, the index $(H : H_{s_i})$ is divisible by p, so (a) follows at once. Parts (b) and (c) are special cases of (a), thus proving the lemma.

Remark. In Lemma 6.3(c), if H has one fixed point, then H has at least p fixed points.

Theorem 6.4. *Let G be a finite group.*

(i) *If H is a p-subgroup of G, then H is contained in some p-Sylow subgroup.*

(ii) *All p-Sylow subgroups are conjugate.*

(iii) *The number of p-Sylow subgroups of G is* $\equiv 1 \bmod p$.

Proof. Let P be a p-Sylow subgroup of G. Suppose first that H is contained in the normalizer of P. We prove that $H \subset P$. Indeed, HP is then a subgroup of the normalizer, and P is normal in HP. But

$$(HP : P) = (H : H \cap P),$$

so if $HP \neq P$, then HP has order a power of p, and the order is larger than $\#(P)$, contradicting the hypothesis that P is a Sylow group. Hence $HP = P$ and $H \subset P$.

Next, let S be the set of all conjugates of P in G. Then G operates on S by conjugation. Since the normalizer of P contains P, and has therefore index prime to p, it follows that $\#(S)$ is not divisible by p. Now let H be any p-subgroup. Then H also acts on S by conjugation. By Lemma 6.3(a), we know that H cannot have 0 fixed points. Let Q be a fixed point. By definition this means that H is contained in the normalizer of Q, and hence by the first part of the proof, that $H \subset Q$, which proves the first part of the theorem. The second part follows immediately by taking H to be a p-Sylow group, so $\#(H) = \#(Q)$, whence $H = Q$. In particular, when H is a p-Sylow group, we see that H has only one fixed point, so that **(iii)** follows from Lemma 6.3(b). This proves the theorem.

Theorem 6.5. *Let G be a finite p-group. Then G is solvable. If its order is* > 1, *then G has a non-trivial center.*

Proof. The first assertion follows from the second, since if G has center Z, and we have an abelian tower for G/Z by induction, we can lift this abelian tower to G to show that G is solvable. To prove the second assertion, we use the class equation

$$(G : 1) = \operatorname{card}(Z) + \sum (G : G_x),$$

the sum being taken over certain x for which $(G : G_x) \neq 1$. Then p divides $(G : 1)$ and also divides every term in the sum, so that p divides the order of the center, as was to be shown.

Corollary 6.6. *Let G be a p-group which is not of order* 1. *Then there exists a sequence of subgroups*

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_n = G$$

such that G_i *is normal in G and* G_{i+1}/G_i *is cyclic of order p.*

Proof. Since G has a non-trivial center, there exists an element $a \neq e$ in the center of G, and such that a has order p. Let H be the cyclic group generated by a. By induction, if $G \neq H$, we can find a sequence of subgroups as stated above in the factor group G/H. Taking the inverse image of this tower in G gives us the desired sequence in G.

We now give some examples to show how to put some of the group theory together.

Lemma 6.7. *Let G be a finite group and let p be the smallest prime dividing the order of G. Let H be a subgroup of index p. Then H is normal.*

Proof. Let $N(H) = N$ be the normalizer of H. Then $N = G$ or $N = H$. If $N = G$ we are done. Suppose $N = H$. Then the orbit of H under conjugation has $p = (G : H)$ elements, and the representation of G on this orbit gives a homomorphism of G into the symmetric group on p elements, whose order is $p!$. Let K be the kernel. Then K is the intersection of the isotropy groups, and the isotropy group of H is H by assumption, so $K \subset H$. If $K \neq H$, then from

$$(G : K) = (G : H)(H : K) = p(H : K),$$

and the fact that only the first power of p divides $p!$, we conclude that some prime dividing $(p - 1)!$ also divides $(H : K)$, which contradicts the assumption that p is the smallest prime dividing the order of G, and proves the lemma.

Proposition 6.8. *Let p, q be distinct primes and let G be a group of order pq. Then G is solvable.*

Proof. Say $p < q$. Let Q be a Sylow subgroup of order q. Then Q has index p, so by the lemma, Q is normal and the factor group has order p. But a group of prime order is cyclic, whence the proposition follows.

Example. Let G be a group of order 35. We claim that G is cyclic.

Proof. Let H_7 be the Sylow subgroup of order 7. Then H_7 is normal by Lemma 6.7. Let H_5 be a 5-Sylow subgroup, which is of order 5. Then H_5 operates by conjugation on H_7, so we get a homomorphism $H_5 \to \mathrm{Aut}(H_7)$. But $\mathrm{Aut}(H_7)$ is cyclic of order 6, so $H_5 \to \mathrm{Aut}(H_7)$ is trivial, so every element of H_5 commutes with elements of H_7. Let $H_5 = \langle x \rangle$ and $H_7 = \langle y \rangle$. Then x, y commute with each other and with themselves, so G is abelian, and so G is cyclic by Proposition 4.3(**v**).

Example. The techniques which have been developed are sufficient to treat many cases of the above types. For instance every group of order < 60 is solvable, as you will prove in Exercise 27.

§7. DIRECT SUMS AND FREE ABELIAN GROUPS

Let $\{A_i\}_{i \in I}$ be a family of abelian groups. We define their **direct sum**

$$A = \bigoplus_{i \in I} A_i$$

to be the subset of the direct product $\prod A_i$ consisting of all families $(x_i)_{i \in I}$ with

$x_i \in A_i$ such that $x_i = 0$ for all but a finite number of indices i. Then it is clear that A is a subgroup of the product. For each index $j \in I$, we map

$$\lambda_j : A_j \to A$$

by letting $\lambda_j(x)$ be the element whose j-th component is x, and having all other components equal to 0. Then λ_i is an injective homomorphism.

Proposition 7.1. *Let $\{f_i : A_i \to B\}$ be a family of homomorphisms into an abelian group B. Let $A = \oplus A_i$. There exists a unique homomorphism*

$$f : A \to B$$

such that $f \circ \lambda_j = f_j$ for all j.

Proof. We can define a map $f : A \to B$ by the rule

$$f((x_i)_{i \in I}) = \sum_{i \in I} f_i(x_i).$$

The sum on the right is actually finite since all but a finite number of terms are 0. It is immediately verified that our map f is a homomorphism. Furthermore, we clearly have $f \circ \lambda_j(x) = f_j(x)$ for each j and each $x \in A_j$. Thus f has the desired commutativity property. It is also clear that the map f is uniquely determined, as was to be shown.

The property expressed in Proposition 7.1 is called the **universal property** of the direct sum. Cf. §11.

Example. Let A be an abelian group, and let $\{A_i\}_{i \in I}$ be a family of subgroups. Then we get a homomorphism

$$\bigoplus_{i \in I} A_i \to A \quad \text{such that} \quad (x_i) \mapsto \sum x_i.$$

Theorem 8.1 will provide an important specific application.

Let A be an abelian group and B, C subgroups. If $B + C = A$ and $B \cap C = \{0\}$ then the map

$$B \times C \to A$$

given by $(x, y) \mapsto x + y$ is an isomorphism (as we already noted in the non-commutative case). Instead of writing $A = B \times C$ we shall write

$$A = B \oplus C$$

and say that A is the **direct sum** of B and C. We use a similar notation for the direct sum of a finite number of subgroups $B_1, \ldots, B_n$ such that

$$B_1 + \cdots + B_n = A$$

and

$$B_{i+1} \cap (B_1 + \cdots + B_i) = 0.$$

In that case we write

$$A = B_1 \oplus \cdots \oplus B_n.$$

Let A be an abelian group. Let $\{e_i\}$ $(i \in I)$ be a family of elements of A. We say that this family is a **basis** for A if the family is not empty, and if every element of A has a unique expression as a linear combination

$$x = \sum x_i e_i$$

with $x_i \in \mathbf{Z}$ and almost all $x_i = 0$. Thus the sum is actually a finite sum. An abelian group is said to be **free** if it has a basis. If that is the case, it is immediate that if we let $Z_i = \mathbf{Z}$ for all i, then A is isomorphic to the direct sum

$$A \approx \bigoplus_{i \in I} Z_i.$$

Next let S be a set. We shall define the free abelian group generated by S as follows. Let $\mathbf{Z}\langle S\rangle$ be the set of all maps $\varphi : S \to \mathbf{Z}$ such that $\varphi(x) = 0$ for almost all $x \in S$. Then $\mathbf{Z}\langle S\rangle$ is an abelian group (addition being the usual addition of maps). If k is an integer and x is an element of S, we denote by $k \cdot x$ the map φ such that $\varphi(x) = k$ and $\varphi(y) = 0$ if $y \neq x$. Then it is obvious that every element φ of $\mathbf{Z}\langle S\rangle$ can be written in the form

$$\varphi = k_1 \cdot x_1 + \cdots + k_n \cdot x_n$$

for some integers k_i and elements $x_i \in S$ $(i = 1, \ldots, n)$, all the x_i being distinct. Furthermore, *φ admits a unique such expression*, because if we have

$$\varphi = \sum_{x \in S} k_x \cdot x = \sum_{x \in S} k'_x \cdot x$$

then

$$0 = \sum_{x \in S} (k_x - k'_x) \cdot x,$$

whence $k'_x = k_x$ for all $x \in S$.

We map S into $\mathbf{Z}\langle S\rangle$ by the map $f_S = f$ such that $f(x) = 1 \cdot x$. It is then clear that f is injective, and that $f(S)$ generates $\mathbf{Z}\langle S\rangle$. If $g : S \to B$ is a mapping of S into some abelian group B, then we can define a map

$$g_* : \mathbf{Z}\langle S\rangle \to B$$

such that

$$g_*\left(\sum_{x \in S} k_x \cdot x\right) = \sum_{x \in S} k_x g(x).$$

This map is a homomorphism (trivial) and we have $g_* \circ f = g$ (also trivial). It is the only homomorphism which has this property, for any such homomorphism g_* must be such that $g_*(1 \cdot x) = g(x)$.

It is customary to identify S in $\mathbf{Z}\langle S\rangle$, and we sometimes omit the dot when we write $k_x x$ or a sum $\sum k_x x$.

If $\lambda : S \to S'$ is a mapping of sets, there is a unique homomorphism $\bar{\lambda}$ making the following diagram commutative:

$$\begin{array}{ccc} S & \xrightarrow{f_S} & \mathbf{Z}\langle S\rangle \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \bar{\lambda}} \\ S' & \xrightarrow[f_{S'}]{} & \mathbf{Z}\langle S'\rangle \end{array}$$

In fact, $\bar{\lambda}$ is none other than $(f_{S'} \circ \lambda)_*$, with the notation of the preceding paragraph. The proof of this statement is left as a trivial exercise.

We shall denote $\mathbf{Z}\langle S\rangle$ also by $F_{\mathrm{ab}}(S)$, and call $F_{\mathrm{ab}}(S)$ the **free abelian group generated by** S. We call elements of S its **free generators**.

As an exercise, show that every abelian group A is isomorphic to a factor group of a free abelian group F. If A is finitely generated, show that one can select F to be finitely generated also.

If the set S above consists of n elements, then we say that the free abelian group $F_{\mathrm{ab}}(S)$ is the free abelian group on n generators. If S is the set of n letters $x_1, \ldots, x_n$, we say that $F_{\mathrm{ab}}(S)$ is the free abelian group with free generators $x_1, \ldots, x_n$.

An abelian group is **free** if and only if it is isomorphic to a free abelian group $F_{\mathrm{ab}}(S)$ for some set S. Let A be an abelian group, and let S be a basis for A. Then it is clear that A is isomorphic to the free abelian group $F_{\mathrm{ab}}(S)$.

As a matter of notation, if A is an abelian group and T a subset of elements of A, we denote by $\langle T\rangle$ the subgroup generated by the elements of T, i.e., the smallest subgroup of A containing T.

Example. The Grothendieck group. Let M be a commutative monoid, written additively. There exists a commutative group $K(M)$ and a monoid-homomorphism

$$\gamma : M \to K(M)$$

having the following universal property. If $f: M \to A$ is a homomorphism into an abelian group A, then there exists a unique homomorphism f_*: $K(M) \to A$ making the following diagram commutative:

$$\begin{array}{ccc} M & \xrightarrow{\gamma} & K(M) \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f_*} & \\ & A & \end{array}$$

Proof. Let $F_{\mathrm{ab}}(M)$ be the free abelian group generated by M. We denote the generator of $F_{\mathrm{ab}}(M)$ corresponding to an element $x \in M$ by $[x]$. Let B be the subgroup generated by all elements of type

$$[x + y] - [x] - [y]$$

where $x, y \in M$. We let $K(M) = F_{ab}(M)/B$, and let

$$\gamma : M \to K(M)$$

be the map obtained by composing the injection of M into $F_{ab}(M)$ given by $x \mapsto [x]$, and the canonical map

$$F_{ab}(M) \to F_{ab}(M)/B.$$

It is then clear that γ is a homomorphism, and satisfies the desired universal property.

The universal group $K(M)$ is called the **Grothendieck group**.

We shall say that the **cancellation law** holds in M if, whenever $x, y, z \in M$, and $x + z = y + z$, we have $x = y$.

We then have an important criterion when the universal map γ above is injective:

If the cancellation law holds in M, then the canonical map γ of M into its Grothendieck group is injective.

Proof. This is essentially the same proof as when one constructs the integers from the natural numbers. We consider pairs (x, y) with $x, y \in M$ and say that (x, y) is equivalent to (x', y') if $y + x' = x + y'$. We define addition of pairs componentwise. Then the equivalence classes of pairs form a group, whose 0 element is the class of $(0,0)$ [or the class of (x,x) for any $x \in M$]. The negative of an element (x, y) is (y, x). We have a homomorphism

$$x \mapsto \text{class of } (0, x)$$

which is injective, as one sees immediately by applying the cancellation law. Thus we have constructed a homomorphism of M into a group, which is injective. It follows that the universal homomorphism must also be injective.

Examples. See the example of projective modules in Chapter III, §4. For a relatively fancy context, see: K. KATO, Logarithmic structures of Fontaine-Illusie, *Algebraic Geometry, Analysis and Number Theory, Proc. JAMI Conference*, J. Igusa (Ed.), Johns Hopkins Press (1989) pp. 195–224.

Given an abelian group A and a subgroup B, it is sometimes desirable to find a subgroup C such that $A = B \oplus C$. The next lemma gives us a condition under which this is true.

Lemma 7.2. *Let $A \xrightarrow{f} A'$ be a surjective homomorphism of abelian groups, and assume that A' is free. Let B be the kernel of f. Then there exists a subgroup C of A such that the restriction of f to C induces an isomorphism of C with A', and such that $A = B \oplus C$.*

Proof. Let $\{x_i'\}_{i \in I}$ be a basis of A', and for each $i \in I$, let x_i be an element of A such that $f(x_i) = x_i'$. Let C be the subgroup of A generated by all elements x_i, $i \in I$. If we have a relation

$$\sum_{i \in I} n_i x_i = 0$$

with integers n_i, almost all of which are equal to 0, then applying f yields

$$0 = \sum_{i \in I} n_i f(x_i) = \sum_{i \in I} n_i x_i',$$

whence all $n_i = 0$. Hence our family $\{x_i\}_{i \in I}$ is a basis of C. Similarly, one sees that if $z \in C$ and $f(z) = 0$ then $z = 0$. Hence $B \cap C = 0$. Let $x \in A$. Since $f(x) \in A'$ there exist integers n_i, $i \in I$, such that

$$f(x) = \sum_{i \in I} n_i x_i'.$$

Applying f to $x - \sum_{i \in I} n_i x_i$, we find that this element lies in the kernel of f, say

$$x - \sum_{i \in I} n_i x_i = b \in B.$$

From this we see that $x \in B + C$, and hence finally that $A = B \oplus C$ is a direct sum, as contended.

Theorem 7.3. *Let A be a free abelian group, and let B be a subgroup. Then B is also a free abelian group, and the cardinality of a basis of B is $\leqq$ the cardinality of a basis for A. Any two bases of B have the same cardinality.*

Proof. We shall give the proof only when A is finitely generated, say by a basis $\{x_1, \ldots, x_n\}$ ($n \geqq 1$), and give the proof by induction on n. We have an expression of A as direct sum:

$$A = \mathbf{Z}x_1 \oplus \cdots \oplus \mathbf{Z}x_n.$$

Let $f\colon A \to \mathbf{Z}x_1$ be the projection, i.e. the homomorphism such that

$$f(m_1x_1 + \cdots + m_nx_n) = m_1x_1$$

whenever $m_i \in \mathbf{Z}$. Let B_1 be the kernel of $f \mid B$. Then B_1 is contained in the free subgroup $\langle x_2, \ldots, x_n \rangle$. By induction, B_1 is free and has a basis with $\leqq n - 1$ elements. By the lemma, there exists a subgroup C_1 isomorphic to a subgroup of $\mathbf{Z}x_1$ (namely the image of $f \mid B$) such that

$$B = B_1 \oplus C_1.$$

Since $f(B)$ is either 0 or infinite cyclic, i.e. free on one generator, this proves that B is free.

(When A is not finitely generated, one can use a similar transfinite argument. See Appendix 2, §2, the example after Zorn's Lemma.)

We also observe that our proof shows that there exists at least one basis of B whose cardinality is $\leqq n$. We shall therefore be finished when we prove the last statement, that any two bases of B have the same cardinality. Let S be one basis, with a finite number of elements m. Let T be another basis, and suppose that T has at least r elements. It will suffice to prove that $r \leqq m$ (one

can then use symmetry). Let p be a prime number. Then B/pB is a direct sum of cyclic groups of order p, with m terms in the sum. Hence its order is p^m. Using the basis T instead of S, we conclude that B/pB contains an r-fold product of cyclic groups of order p, whence $p^r \leqq p^m$, and $r \leqq m$, as was to be shown. (Note that we did not assume a priori that T was finite.)

The number of elements in a basis of a free abelian group A will be called the **rank** of A.

§8. FINITELY GENERATED ABELIAN GROUPS

The groups referred to in the title of this section occur so frequently that it is worth while to state a theorem which describes their structure completely. Throughout this section we write our abelian groups additively.

Let A be an abelian group. An element $a \in A$ is said to be a **torsion** element if it has finite period. The subset of all torsion elements of A is a subgroup of A called the **torsion subgroup** of A. (If a has period m and b has period n then, writing the group law additively, we see that $a \pm b$ has a period dividing mn.)

The torsion subgroup of A is denoted by A_{tor}, or simply A_t. An abelian group is called a **torsion group** if $A = A_{\text{tor}}$, that is all elements of A are of finite order.

A finitely generated torsion abelian group is obviously finite. We shall begin by studying torsion abelian groups. If A is an abelian group and p a prime number, we denote by $A(p)$ the subgroup of all elements $x \in A$ whose period is a power of p. Then $A(p)$ is a torsion group, and is a p-group if it is finite.

Theorem 8.1 *Let A be a torsion abelian group. Then A is the direct sum of its subgroups $A(p)$ for all primes p such that $A(p) \neq 0$.*

Proof. There is a homomorphism

$$\bigoplus_p A(p) \to A$$

which to each element (x_p) in the direct sum associates the element $\sum x_p$ in A. We prove that this homomorphism is both surjective and injective. Suppose x is in the kernel, so $\sum x_p = 0$. Let q be a prime. Then

$$x_q = \sum_{p \neq q} (-x_p).$$

Let m be the least common multiple of the periods of elements x_p on the right-hand side, with $x_q \neq 0$ and $p \neq q$. Then $mx_q = 0$. But also $q^r x_q = 0$ for some positive integer r. If d is the greatest common divisor of m, q^r then $dx_q = 0$, but $d = 1$, so $x_q = 0$. Hence the kernel is trivial, and the homomorphism is injective.

As for the surjectivity, for each positive integer m, denote by A_m the kernel of multiplication by m, i.e. the subgroup of $x \in A$ such that $mx = 0$. We prove:

If $m = rs$ with r, s positive relative prime integers, then $A_m = A_r + A_s$.

Indeed, there exist integers u, v such that $ur + vs = 1$. Then $x = urx + vsx$, and $urx \in A_s$ while $vsx \in A_r$, and our assertion is proved. Repeating this process inductively, we conclude:

$$\text{If } m = \prod_{p|m} p^{e(p)} \text{ then } A_m = \sum_{p|m} A_{p^{e(p)}}.$$

Hence the map $\bigoplus A(p) \to A$ is surjective, and the theorem is proved.

Example. Let $A = \mathbf{Q}/\mathbf{Z}$. Then $\mathbf{Q}/\mathbf{Z}$ is a torsion abelian group, isomorphic to the direct sum of its subgroups $(\mathbf{Q}/\mathbf{Z})(p)$. Each $(\mathbf{Q}/\mathbf{Z})(p)$ consists of those elements which can be represented by a rational number a/p^k with $a \in \mathbf{Z}$ and k some positive integer, i.e. a rational number having only a p-power in the denominator. See also Chapter IV, Theorem 5.1.

In what follows we shall deal with finite abelian groups, so only a finite number of primes (dividing the order of the group) will come into play. In this case, the direct sum is "the same as" the direct product.

Our next task is to describe the structure of finite abelian p-groups. Let $r_1, \ldots, r_s$ be integers $\geqq 1$. A finite p-group A is said to be of **type $(p^{r_1}, \ldots, p^{r_s})$** if A is isomorphic to the product of cyclic groups of orders p^{r_i} $(i = 1, \ldots, s)$. We shall need the following remark.

Remark. Let A be a finite abelian p-group. Let b be an element of A, $b \neq 0$. Let k be an integer $\geqq 0$ such that $p^k b \neq 0$, and let p^m be the period of $p^k b$. Then b has period p^{k+m}. [*Proof*: We certainly have $p^{k+m}b = 0$, and if $p^n b = 0$ then first $n \geqq k$, and second $n \geqq k + m$, otherwise the period of $p^k b$ would be smaller than p^m.]

Theorem 8.2. *Every finite abelian p-group is isomorphic to a product of cyclic p-groups. If it is of type $(p^{r_1}, \ldots, p^{r_s})$ with*

$$r_1 \geqq r_2 \geqq \cdots \geqq r_s \geqq 1,$$

then the sequence of integers $(r_1, \ldots, r_s)$ is uniquely determined.

Proof. We shall prove the existence of the desired product by induction. Let $a_1 \in A$ be an element of maximal period. We may assume without loss of generality that A is not cyclic. Let A_1 be the cyclic subgroup generated by a_1, say of period p^{r_1}. We need a lemma.

Lemma 8.3. *Let $\bar{b}$ be an element of A/A_1, of period p^r. Then there exists a representative a of $\bar{b}$ in A which also has period p^r.*

Proof. Let b be any representative of $\bar{b}$ in A. Then $p^r b$ lies in A_1, say $p^r b = na_1$ with some integer $n \geqq 0$. We note that the period of $\bar{b}$ is $\leqq$ the period of b. If $n = 0$ we are done. Otherwise write $n = p^k \mu$ where μ is prime to p. Then μa_1 is also a generator of A_1, and hence has period p^{r_1}. We may assume $k \leqq r_1$. Then $p^k \mu a_1$ has period $p^{r_1 - k}$. By our previous remarks, the element b has period

$$p^{r + r_1 - k}$$

whence by hypothesis, $r + r_1 - k \leqq r_1$ and $r \leqq k$. This proves that there exists an element $c \in A_1$ such that $p^r b = p^r c$. Let $a = b - c$. Then a is a representative for $\bar{b}$ in A and $p^r a = 0$. Since period $(a) \leqq p^r$ we conclude that a has period equal to p^r.

We return to the main proof. By induction, the factor group A/A_1 has a product expression

$$A/A_1 = \bar{A}_2 \times \cdots \times \bar{A}_s$$

into cyclic subgroups of orders $p^{r_2}, \ldots, p^{r_s}$ respectively, and we may assume $r_2 \geqq \cdots \geqq r_s$. Let $\bar{a}_i$ be a generator for $\bar{A}_i$ $(i = 2, \ldots, s)$ and let a_i be a representative in A of the same period as $\bar{a}_i$. Let A_i be the cyclic subgroup generated by a_i. We contend that A is the direct sum of $A_1, \ldots, A_s$.

Given $x \in A$, let $\bar{x}$ denote its residue class in A/A_1. There exist integers $m_i \geqq 0$ $(i = 2, \ldots, s)$ such that

$$\bar{x} = m_2 \bar{a}_2 + \cdots + m_s \bar{a}_s.$$

Hence $x - m_2 a_2 - \cdots - m_s a_s$ lies in A_1, and there exists an integer $m_1 \geqq 0$ such that

$$x = m_1 a_1 + m_2 a_2 + \cdots + m_s a_s.$$

Hence $A_1 + \cdots + A_s = A$.

Conversely, suppose that $m_1, \ldots, m_s$ are integers $\geqq 0$ such that

$$0 = m_1 a_1 + \cdots + m_s a_s.$$

Since a_i has period p^{r_i} $(i = 1, \ldots, s)$, we may suppose that $m_i < p^{r_i}$. Putting a bar on this equation yields

$$0 = m_2 \bar{a}_2 + \cdots + m_s \bar{a}_s.$$

Since A/A_1 is a direct product of $\bar{A}_2, \ldots, \bar{A}_s$ we conclude that each $m_i = 0$ for $i = 2, \ldots, s$. But then $m_1 = 0$ also, and hence all $m_i = 0$ $(i = 1, \ldots, s)$. From this it follows at once that

$$(A_1 + \cdots + A_i) \cap A_{i+1} = 0$$

for each $i \geqq 1$, and hence that A is the direct product of $A_1, \ldots, A_s$, as desired.

We prove uniqueness, by induction. Suppose that A is written in two ways as a direct sum of cyclic groups, say of type

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{and} \quad (p^{m_1}, \ldots, p^{m_k})$$

with $r_1 \geqq \cdots \geqq r_s \geqq 1$ and $m_1 \geqq \cdots \geqq m_k \geqq 1$. Then pA is also a p-group, of order strictly less than the order of A, and is of type

$$(p^{r_1-1}, \ldots, p^{r_s-1}) \quad \text{and} \quad (p^{m_1-1}, \ldots, p^{m_k-1}),$$

it being understood that if some exponent r_i or m_j is equal to 1, then the factor corresponding to

$$p^{r_i-1} \quad \text{or} \quad p^{m_j-1}$$

in pA is simply the trivial group 0. By induction, the subsequence of

$$(r_1 - 1, \ldots, r_s - 1)$$

consisting of those integers $\geqq 1$ is uniquely determined, and is the same as the corresponding subsequence of

$$(m_1 - 1, \ldots, m_k - 1).$$

In other words, we have $r_i - 1 = m_i - 1$ for all those integers i such that $r_i - 1$ or $m_i - 1 \geqq 1$. Hence $r_i = m_i$ for all these integers i, and the two sequences

$$(p^{r_1}, \ldots, p^{r_s}) \quad \text{and} \quad (p^{m_1}, \ldots, p^{m_k})$$

can differ only in their last components which can be equal to p. These correspond to factors of type $(p, \ldots, p)$ occurring say ν times in the first sequences and μ times in the second sequence. Thus for some integer n, A is of type

$$(p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\nu \text{ times}}) \quad \text{and} \quad (p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{\mu \text{ times}}).$$

Thus the order of A is equal to

$$p^{r_1+\cdots+r_n}p^{\nu} = p^{r_1+\cdots+r_n}p^{\mu},$$

whence $\nu = \mu$, and our theorem is proved.

A group G is said to be **torsion free**, or without torsion, if whenever an element x of G has finite period, then x is the unit element.

Theorem 8.4. *Let A be a finitely generated torsion-free abelian group. Then A is free.*

Proof. Assume $A \neq 0$. Let S be a finite set of generators, and let $x_1, \ldots, x_n$ be a maximal subset of S having the property that whenever $v_1, \ldots, v_n$ are integers such that

$$v_1x_1 + \cdots + v_nx_n = 0,$$

then $v_j = 0$ for all j. (Note that $n \geqq 1$ since $A \neq 0$). Let B be the subgroup generated by $x_1, \ldots, x_n$. Then B is free. Given $y \in S$ there exist integers $m_1, \ldots, m_n, m$ not all zero such that

$$my + m_1x_1 + \cdots + m_nx_n = 0,$$

by the assumption of maximality on $x_1, \ldots, x_n$. Furthermore, $m \neq 0$; otherwise all $m_j = 0$. Hence my lies in B. This is true for every one of a finite set of generators y of A, whence there exists an integer $m \neq 0$ such that $mA \subset B$. The map

$$x \mapsto mx$$

of A into itself is a homomorphism, having trivial kernel since A is torsion free. Hence it is an isomorphism of A onto a subgroup of B. By Theorem 7.3 of the preceding section, we conclude that mA is free, whence A is free.

Theorem 8.5. *Let A be a finitely generated abelian group, and let A_{tor} be the subgroup consisting of all elements of A having finite period. Then A_{tor} is finite, and A/A_{tor} is free. There exists a free subgroup B of A such that A is the direct sum of A_{tor} and B.*

Proof. We recall that a finitely generated torsion abelian group is obviously finite. Let A be finitely generated by n elements, and let F be the free abelian group on n generators. By the universal property, there exists a surjective homomorphism

$$F \xrightarrow{\varphi} A$$

of F onto A. The subgroup $\varphi^{-1}(A_{\text{tor}})$ of F is finitely generated by Theorem 7.3. Hence A_{tor} itself is finitely generated, hence finite.

Next, we prove that A/A_{tor} has no torsion. Let $\bar{x}$ be an element of A/A_{tor} such that $m\bar{x} = 0$ for some integer $m \neq 0$. Then for any representative of x of $\bar{x}$ in A, we have $mx \in A_{\text{tor}}$, whence $qmx = 0$ for some integer $q \neq 0$. Then $x \in A_{\text{tor}}$, so $\bar{x} = 0$, and A/A_{tor} is torsion free. By Theorem 8.4, A/A_{tor} is free. We now use the lemma of Theorem 7.3 to conclude the proof.

The rank of A/A_{tor} is also called the **rank** of A.

For other contexts concerning Theorem 8.5, see the structure theorem for modules over principal rings in Chapter III, §7, and Exercises 5, 6, and 7 of Chapter III.

§9. THE DUAL GROUP

Let A be an abelian group of exponent $m \geqq 1$. This means that for each element $x \in A$ we have $mx = 0$. Let Z_m be a cyclic group of order m. We denote by $A^\wedge$, or $\text{Hom}(A, Z_m)$ the group of homomorphisms of A into Z_m, and call it the **dual** of A.

Let $f : A \to B$ be a homomorphism of abelian groups, and assume both have exponent m. Then f induces a homomorphism

$$f^\wedge : B^\wedge \to A^\wedge.$$

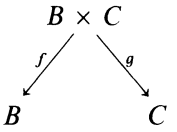
Namely, for each $\psi \in B^\wedge$ we define $f^\wedge(\psi) = \psi \circ f$. It is trivially verified that $f^\wedge$ is a homomorphism. The properties

$$\mathrm{id}^\wedge = \mathrm{id} \quad \text{and} \quad (f \circ g)^\wedge = g^\wedge \circ f^\wedge$$

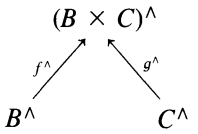
are trivially verified.

Theorem 9.1. *If A is a finite abelian group, expressed as a product $A = B \times C$, then $A^\wedge$ is isomorphic to $B^\wedge \times C^\wedge$ (under the mapping described below). A finite abelian group is isomorphic to its own dual.*

Proof. Consider the two projections



of $B \times C$ on its two components. We get homomorphisms



and we contend that these homomorphisms induce an isomorphism of $B^\wedge \times C^\wedge$ onto $(B \times C)^\wedge$.

In fact, let ψ_1, ψ_2 be in $\mathrm{Hom}(B, Z_m)$ and $\mathrm{Hom}(C, Z_m)$ respectively. Then $(\psi_1, \psi_2) \in B^\wedge \times C^\wedge$, and we have a corresponding element of $(B \times C)^\wedge$ by defining

$$(\psi_1, \psi_2)(x, y) = \psi_1(x) + \psi_2(y),$$

for $(x, y) \in B \times C$. In this way we get a homomorphism

$$B^\wedge \times C^\wedge \to (B \times C)^\wedge.$$

Conversely, let $\psi \in (B \times C)^\wedge$. Then

$$\psi(x, y) = \psi(x, 0) + \psi(0, y).$$

The function ψ_1 on B such that $\psi_1(x) = \psi(x, 0)$ is in $B^\wedge$, and similarly the function ψ_2 on C such that $\psi_2(y) = \psi(0, y)$ is in $C^\wedge$. Thus we get a homomorphism

$$(B \times C)^\wedge \to B^\wedge \times C^\wedge,$$

which is obviously inverse to the one we defined previously. Hence we obtain an isomorphism, thereby proving the first assertion in our theorem.

We can write any finite abelian group as a product of cyclic groups. Thus to prove the second assertion, it will suffice to deal with a cyclic group.

Let A be cyclic, generated by one element x of period n. Then $n \mid m$, and Z_m has precisely one subgroup of order n, Z_n, which is cyclic (Proposition 4.3(**iv**)).

If $\psi : A \to Z_m$ is a homomorphism, and x is a generator for A, then the period of x is an exponent for $\psi(x)$, so that $\psi(x)$, and hence $\psi(A)$, is contained in Z_n. Let y be a generator for Z_n. We have an isomorphism

$$\psi_1 : A \to Z_n$$

such that $\psi_1(x) = y$. For each integer k with $0 \leqq k < n$ we have the homomorphism $k\psi_1$ such that

$$(k\psi_1)(x) = k \cdot \psi_1(x) = \psi_1(kx).$$

In this way we get a cyclic subgroup of $A^\wedge$ consisting of the n elements $k\psi_1$ $(0 \leqq k < n)$. Conversely, any element ψ of $A^\wedge$ is uniquely determined by its effect on the generator x, and must map x on one of the n elements kx $(0 \leqq k < n)$ of Z_n. Hence ψ is equal to one of the maps $k\psi_1$. These maps constitute the full group $A^\wedge$, which is therefore cyclic of order n, generated by ψ_1. This proves our theorem.

In considering the dual group, we take various cyclic groups Z_m. There are many applications where such groups occur, for instance the group of m-th roots of unity in the complex numbers, the subgroup of order m of $\mathbf{Q}/\mathbf{Z}$, etc.

Let A, A' be two abelian groups. A **bilinear** map of $A \times A'$ into an abelian group C is a map

$$A \times A' \to C$$

denoted by

$$(x, x') \mapsto \langle x, x' \rangle$$

having the following property. For each $x \in A$ the function $x' \mapsto \langle x, x' \rangle$ is a homomorphism, and similarly for each $x' \in A'$ the function $x \mapsto \langle x, x' \rangle$ is a homomorphism.

As a special case of a bilinear map, we have the one given by

$$A \times \mathrm{Hom}(A, C) \to C$$

which to each pair (x, f) with $x \in A$ and $f \in \mathrm{Hom}(A, C)$ associates the element $f(x)$ in C.

A bilinear map is also called a **pairing**.

An element $x \in A$ is said to be **orthogonal** (or **perpendicular**) to a subset S' of A' if $\langle x, x' \rangle = 0$ for all $x' \in S'$. It is clear that the set of $x \in A$ orthogonal to S' is a subgroup of A. We make similar definitions for elements of A', orthogonal to subsets of A.

The **kernel** of our bilinear map on the left is the subgroup of A which is orthogonal to all of A'. We define its kernel on the right similarly.

Given a bilinear map $A \times A' \to C$, let B, B' be the respective kernels of our bilinear map on the left and right. An element x' of A' gives rise to an element of $\mathrm{Hom}(A, C)$ given by $x \mapsto \langle x, x' \rangle$, which we shall denote by $\psi_{x'}$. Since $\psi_{x'}$ vanishes on B we see that $\psi_{x'}$ is in fact a homomorphism of A/B into C.

Furthermore, $\psi_{x'} = \psi_{y'}$ if x', y' are elements of A' such that

$$x' \equiv y' \pmod{B'}.$$

Hence ψ is in fact a homomorphism

$$0 \to A'/B' \to \mathrm{Hom}(A/B, C),$$

which is injective since we defined B' to be the group orthogonal to A. Similarly, we get an injective homomorphism

$$0 \to A/B \to \mathrm{Hom}(A'/B', C).$$

Assume that C is cyclic of order m. Then for any $x' \in A'$ we have

$$m\psi_{x'} = \psi_{mx'} = 0,$$

whence A'/B' has exponent m. Similarly, A/B has exponent m.

Theorem 9.2. *Let $A \times A' \to C$ be a bilinear map of two abelian groups into a cyclic group C of order m. Let B, B' be its respective kernels on the left and right. Assume that A'/B' is finite. Then A/B is finite, and A'/B' is isomorphic to the dual group of A/B (under our map ψ).*

Proof. The injection of A/B into $\mathrm{Hom}(A'/B', C)$ shows that A/B is finite. Furthermore, we get the inequalities

$$\mathrm{ord}\ A/B \leqq \mathrm{ord}(A'/B')^{\wedge} = \mathrm{ord}\ A'/B'$$

and

$$\mathrm{ord}\ A'/B' \leqq \mathrm{ord}(A/B)^{\wedge} = \mathrm{ord}\ A/B.$$

From this it follows that our map ψ is bijective, hence an isomorphism.

Corollary 9.3. *Let A be a finite abelian group, B a subgroup, $A^{\wedge}$ the dual group, and $B^{\perp}$ the set of $\varphi \in A^{\wedge}$ such that $\varphi(B) = 0$. Then we have a natural isomorphism of $A^{\wedge}/B^{\perp}$ with $B^{\wedge}$.*

Proof. This is a special case of Theorem 9.2.

§10. INVERSE LIMIT AND COMPLETION

Consider a sequence of groups $\{G_n\}$ $(n = 0, 1, 2, \ldots)$, and suppose given for all $n \geqq 1$ homomorphisms

$$f_n \colon G_n \to G_{n-1}.$$

Suppose first that these homomorphisms are surjective. We form infinite sequences

$$x = (x_0, x_1, x_2, \ldots) \quad \text{such that } x_{n-1} = f_n(x_n).$$

By the assumption of surjectivity, given $x_n \in G_n$ we can always lift x_n to G_{n+1} via f_{n+1}, so such infinite sequences exist, projecting to any given x_0. We can define multiplication of such sequences componentwise, and it is then immediately verified that the set of sequences is a group, called the **inverse limit** of the family $\{(G_n, f_n)\}$. We denote the inverse limit by $\varprojlim (G_n, f_n)$, or simply $\lim G_n$ if the reference to f_n is clear.

Example. Let A be an additive abelian group. Let p be a prime number. Let $p_A: A \to A$ denote multiplication by p. We say that A is **p-divisible** if p_A is surjective. We may then form the inverse limit by taking $A_n = A$ for all n, and $f_n = p_A$ for all n. The inverse limit is denoted by $V_p(A)$. We let $T_p(A)$ be the subset of $V_p(A)$ consisting of those infinite sequences as above such that $x_0 = 0$. Let $A[p^n]$ be the kernel of p_A^n. Then

$$T_p(A) = \varprojlim A[p^{n+1}].$$

The group $T_p(A)$ is called the **Tate group** associated with the p-divisible group A. It arose in fairly sophisticated contexts of algebraic geometry due to Deuring and Weil, in the theory of elliptic curves and abelian varieties developed in the 1940s, which are far afield from this book. Interested readers can consult books on those subjects.

The most common p-divisible groups are obtained as follows. First, let A be the subgroup of $\mathbf{Q}/\mathbf{Z}$ consisting of those rational numbers (mod $\mathbf{Z}$) which can be expressed in the form a/p^k with some positive integer k, and $a \in \mathbf{Z}$. Then A is p-divisible.

Second, let $\boldsymbol{\mu}[p^n]$ be the group of p^n-th roots of unity in the complex numbers. Let $\boldsymbol{\mu}[p^\infty]$ be the union of all $\boldsymbol{\mu}[p^n]$ for all n. Then $\boldsymbol{\mu}[p^\infty]$ is p-divisible, and isomorphic to the group A of the preceding paragraph. Thus

$$T_p(\boldsymbol{\mu}) = \varprojlim \boldsymbol{\mu}[p^n].$$

These groups are quite important in number theory and algebraic geometry. We shall make further comments about them in Chapter III, §10, in a broader context.

Example. Suppose given a group G. Let $\{H_n\}$ be a sequence of normal subgroups such that $H_n \supset H_{n+1}$ for all n. Let

$$f_n: G/H_n \to G/H_{n-1}$$

be the canonical homomorphisms. Then we may form the inverse limit $\varprojlim G/H_n$. Observe that G has a natural homomorphism

$$g: G \to \varprojlim G/H_n,$$

which sends an element x to the sequence $(\ldots, x_n, \ldots)$, where x_n = image of x in G/H_n.

Example. Let $G_n = \mathbf{Z}/p^{n+1}\mathbf{Z}$ for each $n \geqq 0$. Let

$$f_n: \mathbf{Z}/p^{n+1}\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$$

be the canonical homomorphism. Then f_n is surjective, and the limit is called

the group of p-**adic integers**, denoted by $\mathbf{Z}_p$. We return to this in Chapter III, §10, where we shall see that $\mathbf{Z}_p$ is also a ring.

After these examples, we want to consider the more general situation when one deals not with a sequence but with a more general type of family of groups, which may not be commutative. We therefore define inverse limits of groups in general.

Let I be a set of indices. Suppose given a relation of partial ordering in I, namely for some pairs (i, j) we have a relation $i \leqq j$ satisfying the conditions: For all i, j, k in I, we have $i \leqq i$; if $i \leqq j$ and $j \leqq k$ then $i \leqq k$; if $i \leqq j$ and $j \leqq i$ then $i = j$. We say that I is **directed** if given $i, j \in I$, there exists k such that $i \leqq k$ and $j \leqq k$. Assume that I is directed. By an **inversely directed family** of groups, we mean a family $\{G_i\}_{i \in I}$ and for each pair $i \leqq j$ a homomorphism

$$f_i^j \colon G_j \to G_i$$

such that, whenever $k \leqq i \leqq j$ we have

$$f_k^i \circ f_i^j = f_k^j \quad \text{and} \quad f_i^i = \mathrm{id}.$$

Let $G = \prod G_i$ be the product of the family. Let Γ be the subset of G consisting of all elements (x_i) with $x_i \in G_i$ such that for all i and $j \geqq i$ we have

$$f_i^j(x_j) = x_i.$$

Then Γ contains the unit element, and is immediately verified to be a subgroup of G. We call Γ the **inverse limit** of the family, and write

$$\Gamma = \varprojlim G_i.$$

Example. Let G be a group. Let $\mathfrak{F}$ be the family of normal subgroups of finite index. If H, K are normal of finite index, then so is $H \cap K$, so $\mathfrak{F}$ is a directed family. We may then form the inverse limit $\varprojlim G/H$ with $H \in \mathfrak{F}$. There is a variation on this theme. Instead of $\mathfrak{F}$, let p be a prime number, and let $\mathfrak{F}_p$ be the family of normal subgroups of finite index equal to a power of p. Then the inverse limit with respect to subgroups $H \in \mathfrak{F}_p$ can also be taken. (Verify that if H, K are normal of finite p-power index, so is their intersection.)

A group which is an inverse limit of finite groups is called **profinite**.

Example from applications. Such inverse limits arise in Galois theory. Let k be a field and let A be an infinite Galois extension. For example, $k = \mathbf{Q}$ and A is an algebraic closure of $\mathbf{Q}$. Let G be the Galois group; that is, the group of automorphisms of A over k. Then G is the inverse limit of the factor groups G/H, where H ranges over the Galois groups of A over K, with K ranging over all finite extensions of k contained in A. See the Shafarevich conjecture in the chapter on Galois theory, Conjecture 14.2 of Chapter VI.

Similarly, consider a compact Riemann surface X of genus $\geqq 2$. Let $p : X' \to X$ be the universal covering space. Let $\mathbf{C}(X) = F$ and $\mathbf{C}(X') = F'$ be the function fields. Then there is an embedding $\pi_1(X) \hookrightarrow \mathrm{Gal}(F'/F)$. It is shown in complex analysis that $\pi_1(X)$ is a free group with one commutator

relation. The full Galois group of F'/F is the inverse limit with respect to the subgroups of finite index, as in the above general situation.

Completion of a group

Suppose now that we are given a group G, and first, for simplicity, suppose given a sequence of normal subgroups $\{H_r\}$ with $H_r \supset H_{r+1}$ for all r, and such that these subgroups have finite index. A sequence $\{x_n\}$ in G will be called a **Cauchy sequence** if given H_r there exists N such that for all $m, n \geqq N$ we have $x_n x_m^{-1} \in H_r$. We say that $\{x_n\}$ is a **null sequence** if given r there exists N such that for all $n \geqq N$ we have $x_n \in H_r$. As an exercise, prove that the Cauchy sequences form a group under termwise product, and that the null sequences form a normal subgroup. The factor group is called the **completion** of G (with respect to the sequence of normal subgroups).

Observe that there is a natural homomorphism of G into its completion; namely, an element $x \in G$ maps to the sequence $(x, x, x, \ldots)$ modulo null sequences. The kernel of this homomorphism is the intersection $\cap H_r$, so if this intersection is the unit element of G, then the map of G into its completion is an embedding.

Theorem 10.1. *The completion and the inverse limit* $\varprojlim G/H_r$ *are isomorphic under natural mappings.*

Proof. We give the maps. Let $x = \{x_n\}$ be a Cauchy sequence. Given r, for all n sufficiently large, by the definition of Cauchy sequence, the class of x_n mod H_r is independent of n. Let this class be $x(r)$. Then the sequence $(x(1), x(2), \ldots)$ defines an element of the inverse limit. Conversely, given an element $(\bar{x}_1, \bar{x}_2, \ldots)$ in the inverse limit, with $\bar{x}_n \in G/H_n$, let x_n be a representative in G. Then the sequence $\{x_n\}$ is Cauchy. We leave to the reader to verify that the Cauchy sequence $\{x_n\}$ is well-defined modulo null sequences, and that the maps we have defined are inverse isomorphisms between the completion and the inverse limit.

We used sequences and denumerability to make the analogy with the construction of the real numbers clearer. In general, given the family $\mathfrak{F}$, by a Cauchy family we mean a family $\{x_j\}_{j \in J}$ indexed by an arbitrary directed set J, such that for every $H \in \mathfrak{F}$ there exists $j \in J$ such that for all $k, k' \geqq j$ we have $x_k x_{k'}^{-1} \in H$. In practice, one can work with sequences, because groups that arise naturally are such that the set of subgroups of finite index is denumerable. This occurs when the group G is finitely generated.

More generally, a family $\{H_i\}$ of normal subgroups $\subset \mathfrak{F}$ is called **cofinal** in $\mathfrak{F}$ if given $H \in \mathfrak{F}$ there exists i such that $H_i \subset H$. Suppose that there exists such a family which is denumerable; that is, $i = 1, 2, \ldots$ ranges over the positive integers. Then it is an exercise to show that there is an isomorphism

$$\varprojlim_i G/H_i \approx \varprojlim_{H \in \mathfrak{F}} G/H,$$

or equivalently, that the completion of G with respect to the sequence $\{H_i\}$ is "the same" as the completion with respect to the full family $\mathfrak{F}$. We leave this verification to the reader.

The process of completion is frequent in mathematics. For instance, we shall mention completions of rings in Chapter III, §10; and in Chapter XII we shall deal with completions of fields.

§11. CATEGORIES AND FUNCTORS

Before proceeding further, it will now be convenient to introduce some new terminology. We have met already several kinds of objects: sets, monoids, groups. We shall meet many more, and for each such kind of objects we define special kinds of maps between them (e.g. homomorphisms). Some formal behavior will be common to all of these, namely the existence of identity maps of an object onto itself, and the associativity of maps when such maps occur in succession. We introduce the notion of category to give a general setting for all of these.

A **category** $\mathfrak{A}$ consists of a collection of objects $\mathrm{Ob}(\mathfrak{A})$; and for two objects $A, B \in \mathrm{Ob}(\mathfrak{A})$ a set $\mathrm{Mor}(A, B)$ called the set of **morphisms** of A into B; and for three objects $A, B, C \in \mathrm{Ob}(\mathfrak{A})$ a law of composition (i.e. a map)

$$\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \to \mathrm{Mor}(A, C)$$

satisfying the following axioms:

CAT 1. Two sets $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(A', B')$ are disjoint unless $A = A'$ and $B = B'$, in which case they are equal.

CAT 2. For each object A of $\mathfrak{A}$ there is a morphism $\mathrm{id}_A \in \mathrm{Mor}(A, A)$ which acts as right and left identity for the elements of $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(B, A)$ respectively, for all objects $B \in \mathrm{Ob}(\mathfrak{A})$.

CAT 3. The law of composition is associative (when defined), i.e. given $f \in \mathrm{Mor}(A, B)$, $g \in \mathrm{Mor}(B, C)$ and $h \in \mathrm{Mor}(C, D)$ then

$$(h \circ g) \circ f = h \circ (g \circ f),$$

for all objects A, B, C, D of $\mathfrak{A}$.

Here we write the composition of an element g in $\mathrm{Mor}(B, C)$ and an element f in $\mathrm{Mor}(A, B)$ as $g \circ f$, to suggest composition of mappings. In practice, in this book we shall see that most of our morphisms are actually mappings, or closely related to mappings.

The collection of all morphisms in a category $\mathfrak{A}$ will be denoted by $\mathrm{Ar}(\mathfrak{A})$ ("arrows of $\mathfrak{A}$"). We shall sometimes use the symbols "$f \in \mathrm{Ar}(\mathfrak{A})$" to mean

that f is a morphism of $\mathfrak{A}$, i.e. an element of some set $\mathrm{Mor}(A, B)$ for some $A, B \in \mathrm{Ob}(\mathfrak{A})$.

By abuse of language, we sometimes refer to the collection of objects as the category itself, if it is clear what the morphisms are meant to be.

An element $f \in \mathrm{Mor}(A, B)$ is also written $f: A \to B$ or

$$A \xrightarrow{f} B.$$

A morphism f is called an **isomorphism** if there exists a morphism $g: B \to A$ such that $g \circ f$ and $f \circ g$ are the identities in $\mathrm{Mor}(A, A)$ and $\mathrm{Mor}(B, B)$ respectively. If $A = B$, then we also say that the isomorphism is an **automorphism**.

A morphism of an object A into itself is called an **endomorphism**. The set of endomorphisms of A is denoted by $\mathrm{End}(A)$. It follows at once from our axioms that $\mathrm{End}(A)$ is a monoid.

Let A be an object of a category $\mathfrak{A}$. We denote by $\mathrm{Aut}(A)$ the set of automorphisms of A. This set is in fact a group, because all of our definitions are so adjusted so as to see immediately that the group axioms are satisfied (associativity, unit element, and existence of inverse). Thus we now begin to see some feedback between abstract categories and more concrete ones.

Examples. Let $\mathfrak{S}$ be the category whose objects are sets, and whose morphisms are maps between sets. We say simply that $\mathfrak{S}$ is the category of sets. The three axioms **CAT 1, 2, 3** are trivially satisfied.

Let **Grp** be the category of groups, i.e. the category whose objects are groups and whose morphisms are group-homomorphisms. Here again the three axioms are trivially satisfied. Similarly, we have a category of monoids, denoted by **Mon**.

Later, when we define rings and modules, it will be clear that rings form a category, and so do modules over a ring.

It is important to emphasize here that there are categories for which the set of morphisms is not an abelian group. Some of the most important examples are:

The category $\mathfrak{C}^0$, whose objects are open sets in $\mathbf{R}^n$ and whose morphisms are continuous maps.

The category $\mathfrak{C}^\infty$ with the same objects, but whose morphisms are the C^∞ maps.

The category **Hol**, whose objects are open sets in $\mathbf{C}^n$, and whose morphisms are holomorphic maps. In each case the axioms of a category are verified, because for instance for **Hol**, the composite of holomorphic maps is holomorphic, and similarly for the other types of maps. Thus a C^0-isomorphism is a continuous map $f: U \to V$ which has a continuous inverse $g: V \to U$. Note that a map may be a C^0-isomorphism but not a C^∞-isomorphism. For instance, $x \mapsto x^3$ is a C^0-automorphism of $\mathbf{R}$, but its inverse is not differentiable.

In mathematics one studies manifolds in any one of the above categories. The determination of the group of automorphisms in each category is one of the basic problems of the area of mathematics concerned with that category. In

complex analysis, one determines early the group of holomorphic automorphisms of the unit disc as the group of all maps

$$z \mapsto e^{i\theta} \frac{c - z}{1 - \bar{c}z}$$

with θ real and $c \in \mathbf{C}$, $|c| < 1$.

Next we consider the notion of operation in categories. First, observe that if G is a group, then the G-sets form a category, whose morphisms are the maps $f : S \to S'$ such that $f(xs) = xf(s)$ for $x \in G$ and $s \in S$.

More generally, we can now define the notion of an operation of a group G on an object in any category. Indeed, let $\mathfrak{A}$ be a category and $A \in \mathrm{Ob}(\mathfrak{A})$. By an **operation** of G on A we shall mean a homomorphism of G into the group $\mathrm{Aut}(A)$. In practice, an object A is a set with elements, and an automorphism in $\mathrm{Aut}(A)$ operates on A as a set, i.e. induces a permutation of A. Thus, if we have a homomorphism

$$\rho : G \to \mathrm{Aut}(A),$$

then for each $x \in G$ we have an automorphism $\rho(x)$ of A which is a permutation of A.

An operation of a group G on an object A is also called a **representation** of G on A, and one then says that G is **represented** as a group of automorphisms of A.

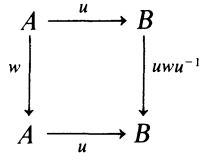
Examples. One meets representations in many contexts. In this book, we shall encounter representations of a group on finite-dimensional vector spaces, with the theory pushed to some depth in Chapter XVIII. We shall also deal with representations of a group on modules over a ring. In topology and differential geometry, one represents groups as acting on various topological spaces, for instance spheres. Thus if X is a differential manifold, or a topological manifold, and G is a group, one considers all possible homomorphims of G into $\mathrm{Aut}(X)$, where Aut refers to whatever category is being dealt with. Thus G may be represented in the group of C^0-automorphims, or C^∞-automorphisms, or analytic automorphisms. Such topological theories are not independent of the algebraic theories, because by functoriality, an action of G on the manifold induces an action on various algebraic functors (homology, K-functor, whatever), so that topological or differential problems are to some extent analyzable by the functorial action on the associated groups, vector spaces, or modules.

Let A, B be objects of a category $\mathfrak{A}$. Let $\mathrm{Iso}(A, B)$ be the set of isomorphisms of A with B. Then the group $\mathrm{Aut}(B)$ operates on $\mathrm{Iso}(A, B)$ by composition; namely, if $u \in \mathrm{Iso}(A, B)$ and $v \in \mathrm{Aut}(B)$, then $(v, u) \mapsto v \circ u$ gives the operation. If u_0 is one element of $\mathrm{Iso}(A, B)$, then the orbit of u_0 is all of $\mathrm{Iso}(A, B)$, so $v \mapsto v \circ u_0$ is a bijection $\mathrm{Aut}(B) \to \mathrm{Iso}(A, B)$. The inverse mapping is given by $u \mapsto u \circ u_0^{-1}$. This trivial formalism is very basic, and is applied constantly to each one of the classical categories mentioned above. Of course, we also have

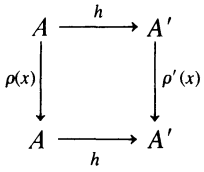
a similar bijection on the other side, but the group $\mathrm{Aut}(A)$ operates *on the right* of $\mathrm{Iso}(A, B)$ by composition. Furthermore, if $u: A \to B$ is an isomorphism, then $\mathrm{Aut}(A)$ and $\mathrm{Aut}(B)$ are isomorphic under conjugation, namely

$$w \mapsto uwu^{-1} \quad \text{is an isomorphism} \quad \mathrm{Aut}(A) \to \mathrm{Aut}(B).$$

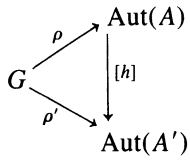
Two such isomorphisms differ by an inner automorphism. One may visualize this system via the following commutative diagram.



Let $\rho : G \to \mathrm{Aut}(A)$ and $\rho' : G \to \mathrm{Aut}(A')$ be representations of a group G on two objects A and A' in the same category. A **morphism** of ρ into ρ' is a morphism $h: A \to A'$ such that the following diagram is commutative for all $x \in G$:



It is then clear that representations of a group G in the objects of a category $\mathfrak{A}$ themselves form a category. An **isomorphism of representations** is then an isomorphism $h : A \to A'$ making the above diagram commutative. An isomorphism of representations is often called an equivalence, but I don't like to tamper with the general system of categorical terminology. Note that if h is an isomorphism of representations, then instead of the above commutative diagram, we let $[h]$ be conjugation by h, and we may use the equivalent diagram



Consider next the case where $\mathfrak{A}$ is the category of abelian groups, which we may denote by **Ab**. Let A be an abelian group and G a group. Given an operation of G on the abelian group A, i.e. a homomorphism

$$\rho : G \to \mathrm{Aut}(A),$$

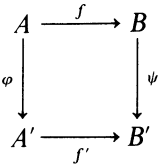
let us denote by $x \cdot a$ the element $\rho_x(a)$. Then we see that for all $x, y \in G$, a, $b \in A$, we have:

$$x \cdot (y \cdot a) = (xy) \cdot a, \qquad x \cdot (a + b) = x \cdot a + x \cdot b,$$
$$e \cdot a = a, \qquad x \cdot 0 = 0.$$

We observe that when a group G operates on itself by conjugation, then not only does G operate on itself as a set but also operates on itself as an object in the category of groups, i.e. the permutations induced by the operation are actually group-automorphisms.

Similarly, we shall introduce later other categories (rings, modules, fields) and we have given a general definition of what it means for a group to operate on an object in any one of these categories.

Let $\mathfrak{A}$ be a category. We may take as objects of a new category $\mathfrak{C}$ the morphisms of $\mathfrak{A}$. If $f: A \to B$ and $f': A' \to B'$ are two morphisms in $\mathfrak{A}$ (and thus objects of $\mathfrak{C}$), then we define a **morphism** $f \to f'$ (in $\mathfrak{C}$) to be a pair of morphisms (φ, ψ) in $\mathfrak{A}$ making the following diagram commutative:



In that way, it is clear that $\mathfrak{C}$ is a category. Strictly speaking, as with maps of sets, we should index (φ, ψ) by f and f' (otherwise **CAT 1** is not necessarily satisfied), but such indexing is omitted in practice.

There are many variations on this example. For instance, we could restrict our attention to morphisms in $\mathfrak{A}$ which have a fixed object of departure, or those which have a fixed object of arrival.

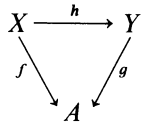
Thus let A be an object of $\mathfrak{A}$, and let $\mathfrak{A}_A$ be the category whose objects are morphisms

$$f: X \to A$$

in $\mathfrak{A}$, having A as object of arrival. A morphism in $\mathfrak{A}_A$ from $f: X \to A$ to $g: Y \to A$ is simply a morphism

$$h: X \to Y$$

in $\mathfrak{A}$ such that the diagram is commutative:



Universal objects

Let $\mathfrak{C}$ be a category. An object P of $\mathfrak{C}$ is called **universally attracting** if there exists a unique morphism of each object of $\mathfrak{C}$ into P, and is called **universally repelling** if for every object of $\mathfrak{C}$ there exists a unique morphism of P into this object.

When the context makes our meaning clear, we shall call objects P as above **universal**. Since a universal object P admits the identity morphism into itself, it is clear that if P, P' are two universal objects in $\mathfrak{C}$, then there exists a unique isomorphism between them.

Examples. Note that the trivial group consisting only of one element is universal (repelling and attracting) in the category of groups. Similarly, in Chapter II on rings, you will see that the integers $\mathbf{Z}$ are universal in the category of rings (universally repelling).

Next let S be a set. Let $\mathfrak{C}$ be the category whose objects are maps $f: S \to A$ of S into abelian groups, and whose morphisms are the obvious ones: If $f: S \to A$ and $f': S \to A'$ are two maps into abelian groups, then a morphism of f into f' is a (group) homomorphism $g: A \to A'$ such that the usual diagram is commutative, namely $g \circ f = f'$. Then the free abelian group generated by S is universal in this category. This is a reformulation of the properties we have proved about this group.

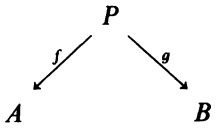
Let M be a commutative monoid and let $\gamma\colon M \to K(M)$ be the canonical homomorphism of M into its Grothendieck group. Then γ is universal in the category of homomorphisms of M into abelian groups.

Throughout this book in numerous situations, we define universal objects. Aside from products and coproducts which come immediately after these examples, we have direct and inverse limits; the tensor product in Chapter XVI, §1; the alternating product in Chapter XIX, §1; Clifford algebras in Chapter XIX, §4; *ad lib.*

We now turn to the notion of product in an arbitrary category.

Products and coproducts

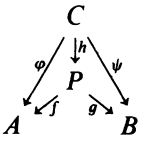
Let $\mathfrak{A}$ be a category and let A, B be objects of $\mathfrak{A}$. By a **product** of A, B in $\mathfrak{A}$ one means a triple (P, f, g) consisting of an object P in $\mathfrak{A}$ and two morphisms



satisfying the following condition: Given two morphisms

$$\varphi: C \to A \quad \text{and} \quad \psi: C \to B$$

in $\mathfrak{A}$, there exists a unique morphism $h: C \to P$ which makes the following diagram commutative:



In other words, $\varphi = f \circ h$ and $\psi = g \circ h$.

More generally, given a family of objects $\{A_i\}_{i\in I}$ in $\mathfrak{A}$, a **product** for this family consists of $(P, \{f_i\}_{i\in I})$, where P is an object in $\mathfrak{A}$ and $\{f_i\}_{i\in I}$ is a family of morphisms

$$f_i : P \to A_i,$$

satisfying the following condition: Given a family of morphisms

$$g_i : C \to A_i,$$

there exists a unique morphism $h : C \to P$ such that $f_i \circ h = g_i$ for all i.

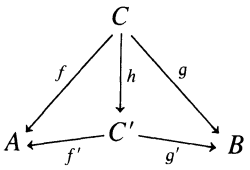
Example. Let $\mathfrak{A}$ be the category of sets, and let $\{A_i\}_{i\in I}$ be a family of sets. Let $A = \prod_{i\in I} A_i$ be their cartesian product, and let $p_i : A \to A_i$ be the projection on the i-th factor. Then $(A, \{p_i\})$ clearly satisfies the requirements of a product in the category of sets.

As a matter of notation, we shall usually write $A \times B$ for the product of two objects in a category, and $\prod_{i\in I} A_i$ for the product of an arbitrary family in a category, following the same notation as in the category of sets.

Example. *Let $\{G_i\}_{i\in I}$ be a family of groups, and let $G = \prod G_i$ be their direct product. Let $p_i : G \to G_i$ be the projection homomorphism. Then these constitute a product of the family in the category of groups.*

Indeed, if $\{g_i : G' \to G_i\}_{i\in I}$ is a family of homomorphisms, there is a unique homomorphism $g : G' \to \prod G_i$ which makes the required diagram commutative. It is the homomorphism such that $g(x')_i = g_i(x')$ for $x' \in G'$ and each $i \in I$.

Let A, B be objects of a category $\mathfrak{A}$. We note that the product of A, B is universal in the category whose objects consist of pairs of morphisms $f : C \to A$ and $g : C \to B$ in $\mathfrak{A}$, and whose morphisms are described as follows. Let $f' : C' \to A$ and $g' : C' \to B$ be another pair. Then a morphism from the first pair to the second is a morphism $h : C \to C'$ in $\mathfrak{A}$, making the following diagram commutative:



The situation is similar for the product of a family $\{A_i\}_{i\in I}$.

We shall also meet the dual notion: Let $\{A_i\}_{i\in I}$ be a family of objects in a category $\mathfrak{A}$. By their **coproduct** one means a pair $(S, \{f_i\}_{i\in I})$ consisting of an object S and a family of morphisms

$$\{f_i : A_i \to S\},$$

satisfying the following property. Given a family of morphisms $\{g_i : A_i \to C\}$, there exists a unique morphism $h : S \to C$ such that $h \circ f_i = g_i$ for all i.

In the product and coproduct, the morphism h will be said to be the morphism **induced** by the family $\{g_i\}$.

Examples. Let $\mathcal{S}$ be the category of sets. *Then coproducts exist*, i.e. every family of objects has a coproduct. For instance, let S, S' be sets. Let T be a set having the same cardinality as S' and disjoint from S. Let $f_1 : S \to S$ be the identity, and $f_2 : S' \to T$ be a bijection. Let U be the union of S and T. Then (U, f_1, f_2) is a coproduct for S, S', viewing f_1, f_2 as maps into U.

Let $\mathcal{S}_0$ be the category of pointed sets. Its objects consist of pairs (S, x) where S is a set and x is an element of S. A morphism of (S, x) into (S', x') in this category is a map $g : S \to S'$ such that $g(x) = x'$. *Then the coproduct of* (S, x) *and* (S', x') *exists in this category*, and can be constructed as follows. Let T be a set whose cardinality is the same as that of S', and such that $T \cap S = \{x\}$. Let $U = S \cup T$, and let

$$f_1 : (S, x) \to (U, x)$$

be the map which induces the identity on S. Let

$$f_2 : (S', x') \to (U, x)$$

be a map sending x' to x and inducing a bijection of $S' - \{x'\}$ on $T - \{x\}$. Then the triple $((U, x), f_1, f_2)$ is a coproduct for (S, x) and (S', x') in the category of pointed sets.

Similar constructions can be made for the coproduct of arbitrary families of sets or pointed sets. The category of pointed sets is especially important in homotopy theory.

Coproducts are universal objects. Indeed, let $\mathfrak{A}$ be a category, and let $\{A_i\}$ be a family of objects in $\mathfrak{A}$. We now define $\mathfrak{C}$. We let objects of $\mathfrak{C}$ be the families of morphisms $\{f_i : A_i \to B\}_{i \in I}$ and given two such families,

$$\{f_i : A_i \to B\} \quad \text{and} \quad \{f_i' : A_i \to B'\},$$

we define a morphism from the first into the second to be a morphism $\varphi : B \to B'$ in $\mathfrak{A}$ such that $\varphi \circ f_i = f_i'$ for all i. Then a coproduct of $\{A_i\}$ is simply a universal object in $\mathfrak{C}$.

The coproduct of $\{A_i\}$ will be denoted by

$$\coprod_{i \in I} A_i.$$

The coproduct of two objects A, B will also be denoted by $A \amalg B$.

By the general uniqueness statement, we see that it is uniquely determined, up to a unique isomorphism. See the comment, top of p. 58.

Example. Let R be the category of commutative rings. Given two such rings A, B one may form the tensor product, and there are natural ring-homomorphisms $A \to A \otimes B$ and $B \to A \otimes B$ such that

$$a \mapsto a \otimes 1 \text{ and } b \mapsto 1 \otimes b \text{ for } a \in A \text{ and } b \in B.$$

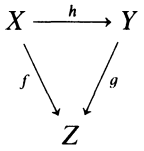
Then the tensor product is a coproduct in the category of commutative rings.

Fiber products and coproducts
Pull-backs and push-outs

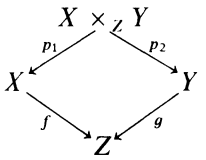
Let $\mathcal{C}$ be a category. Let Z be an object of $\mathcal{C}$. Then we have a new category, that of objects over Z, denoted by $\mathcal{C}_Z$. The objects of $\mathcal{C}_Z$ are morphisms:

$$f: X \to Z \text{ in } \mathcal{C}$$

A morphism from f to $g: Y \to Z$ in $\mathcal{C}_Z$ is merely a morphism $h: X \to Y$ in $\mathcal{C}$ which makes the following diagram commutative.



A **product** in $\mathcal{C}_Z$ is called the **fiber product** of f and g in $\mathcal{C}$ and is denoted by $X \times_Z Y$, together with its natural morphisms on X, Y over Z, which are sometimes not denoted by anything, but which we denote by p_1, p_2.



Fibered products and coproducts exist in the category of abelian groups

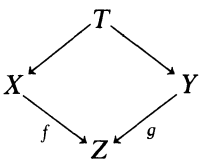
The fibered product of two homomorphisms $f: X \to Z$ and $g: Y \to Z$ is the subgroup of $X \times Y$ consisting of all pairs (x, y) such that

$$f(x) = g(y).$$

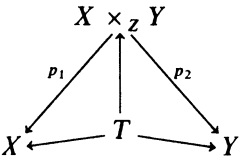
The coproduct of two homomorphisms $f: Z \to X$ and $g: Z \to Y$ is the factor group $(X \oplus Y)/W$ where W is the subgroup of $X \oplus Y$ consisting of all elements $(f(z), -g(z))$ with $z \in Z$.
We leave the simple verification to the reader (see Exercises 50–56).

In the fiber product diagram, one also calls p_1 the **pull-back** of g by f, and p_2 the **pull-back** of f by g. The fiber product satisfies the following universal mapping property:

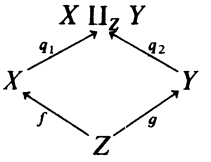
Given any object T in $\mathcal{C}$ and morphisms making the following diagram commutative:



there exists a unique morphism $T \to X \times_Z Y$ *making the following diagram commutative:*



Dually, we have the notion of **coproduct** in the category of morphisms $f: Z \to X$ with a fixed object Z as the object of departure of the morphisms. This category could be denoted by $\mathfrak{C}^Z$. We reverse the arrows in the preceding discussion. Given two objects f and $g: Z \to Y$ in this category, we have the notion of their coproduct. It is denoted by $X \amalg_Z Y$, with morphisms q_1, q_2, as in the following commutative diagram:



satisfying the dual universal property of the fiber product. We call it the **fibered coproduct**. We call q_1 the **push-out** of g by f, and q_2 the **push-out** of f by g.

Example. Let $\mathfrak{S}$ be the category of sets. Given two maps f, g as above, their product is the set of all pairs $(x, y) \in X \times Y$ such that $f(x) = g(y)$.

Functors

Let $\mathfrak{A}$, $\mathfrak{B}$ be categories. A **covariant functor** F of $\mathfrak{A}$ into $\mathfrak{B}$ is a rule which to each object A in $\mathfrak{A}$ associates an object $F(A)$ in $\mathfrak{B}$, and to each morphism $f: A \to B$ associates a morphism $F(f): F(A) \to F(B)$ such that:

FUN 1. For all A in $\mathfrak{A}$ we have $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.

FUN 2. If $f: A \to B$ and $g: B \to C$ are two morphisms of $\mathfrak{A}$ then

$$F(g \circ f) = F(g) \circ F(f).$$

Example. If to each group G we associate its set (stripped of the group structure) we obtain a functor from the category of groups into the category of sets, provided that we associate with each group-homomorphism itself, viewed only as a set-theoretic map. Such a functor is called a **stripping** functor or **forgetful functor**.

We observe that a functor transforms isomorphisms into isomorphisms, because $f \circ g = \mathrm{id}$ implies $F(f) \circ F(g) = \mathrm{id}$ also.

We can define the notion of a **contravariant functor** from $\mathfrak{A}$ into $\mathfrak{B}$ by using essentially the same definition, but reversing all arrows $F(f)$, i.e. to each morphism $f: A \to B$ the contravariant functor associates a morphism

$$F(f): F(B) \to F(A)$$

(going in the opposite direction), such that, if

$$f: A \to B \quad \text{and} \quad g: B \to C$$

are morphisms in $\mathfrak{C}$, then

$$F(g \circ f) = F(f) \circ F(g).$$

Sometimes a functor is denoted by writing f_* instead of $F(f)$ in the case of a covariant functor, and by writing f^* in the case of a contravariant functor.

Example. The association $S \mapsto F_{\text{ab}}(S)$ is a covariant functor from the category of sets to the category of abelian groups.

Example. The association which to each group associates its completion with respect to the family of subgroups of finite index is a functor from the category of groups to the category of groups.

Example. Let p be a prime number. Let $\mathfrak{C}$ be the category of p-divisible abelian groups. The association $A \mapsto T_p(A)$ is a covariant functor of $\mathfrak{C}$ into abelian groups (actually $\mathbf{Z}_p$-modules).

Example. Exercise 49 will show you an example of the group of automorphisms of a forgetful functor.

Example. Let **Man** be the category of compact manifolds. Then the homology is a covariant functor from **Man** into graded abelian groups. The cohomology is a contravariant functor into the category of graded algebras (over the ring of coefficients). The product is the cup product. If the cohomology is taken with coefficients in a field of characteristic 0 (for simplicity), then the cohomology commutes with products. Since cohomology is contravariant, this means that the cohomology of a product is the coproduct of the cohomology of the factors. It turns out that the coproduct is the tensor product, with the graded product, which also gives an example of the use of tensor products. See M. GREENBERG and J. HARPER, *Algebraic Topology* (Benjamin-Addison-Wesley), 1981, Chapter 29.

Example. Let $\mathfrak{C}$ be the category of pointed topological spaces (satisfying some mild conditions), i.e. pairs (X, x_0) consisting of a space X and a point x_0. In topology one defines the connected sum of such spaces (X, x_0) and (Y, y_0), glueing X, Y together at the selected point. This connected sum is a coproduct in the category of such pairs, where the morphisms are the continuous maps $f: X \to Y$ such that $f(x_0) = y_0$. Let π_1 denote the fundamental group. Then $(X, x_0) \mapsto \pi_1(X, x_0)$ is a covariant functor from $\mathfrak{C}$ into the category of groups, commuting with coproducts. (The existence of coproducts in the category of groups will be proved in §12.)

Example. Suppose we have a morphism $f: X \to Y$ in a category $\mathfrak{C}$. By **a section** of f, one means a morphism $g: Y \to X$ such that $g \circ f = \mathrm{id}$. Suppose there exists a covariant functor H from this category to groups such that $H(Y) = \{e\}$ and $H(X) \neq \{e\}$. Then there is no section of f. This is immediate from the formula $H(g \circ f) = \mathrm{id}$, and $H(f) =$ trivial homomorphism. In topology one uses the homology functor to show, for instance, that the unit circle X is not a retract of the closed unit disc with respect to the inclusion mapping f. (Topologists use the word "retract" instead of "section".)

Example. Let $\mathfrak{A}$ be a category and A a fixed object in $\mathfrak{A}$. Then we obtain a covariant functor

$$M_A: \mathfrak{A} \to \mathfrak{S}$$

by letting $M_A(X) = \mathrm{Mor}(A, X)$ for any object X of $\mathfrak{A}$. If $\varphi: X \to X'$ is a morphism, we let

$$M_A(\varphi): \mathrm{Mor}(A, X) \to \mathrm{Mor}(A, X')$$

be the map given by the rule

$$g \mapsto \varphi \circ g$$

for any $g \in \mathrm{Mor}(A, X)$,

$$A \xrightarrow{g} X \xrightarrow{\varphi} X'.$$

The axioms **FUN 1** and **FUN 2** are trivially verified.

Similarly, for each object B of $\mathfrak{A}$, we have a contravariant functor

$$M^B: \mathfrak{A} \to \mathfrak{S}$$

such that $M^B(Y) = \mathrm{Mor}(Y, B)$. If $\psi: Y' \to Y$ is a morphism, then

$$M^B(\psi): \mathrm{Mor}(Y, B) \to \mathrm{Mor}(Y', B)$$

is the map given by the rule

$$f \mapsto f \circ \psi$$

for any $f \in \mathrm{Mor}(Y, B)$,

$$Y' \xrightarrow{\psi} Y \xrightarrow{f} B.$$

The preceding two functors are called the **representation functors**.

Example. Let $\mathfrak{A}$ be the category of abelian groups. Fix an abelian group A. The association $X \mapsto \mathrm{Hom}(A, X)$ is a covariant functor from $\mathfrak{A}$ into itself. The association $X \mapsto \mathrm{Hom}(X, A)$ is a contravariant functor of $\mathfrak{A}$ into itself.

Example. We assume you know about the tensor product. Let A be a commutative ring. Let M be an A-module. The association $X \mapsto M \otimes X$ is a covariant functor from the category of A-modules into itself.

Observe that products and coproducts were defined in a way compatible with the representation functor into the category of sets. Indeed, given a product P

of two objects A and B, then for every object X the set $\mathrm{Mor}(X, P)$ is a product of the sets $\mathrm{Mor}(X, A)$ and $\mathrm{Mor}(X, B)$ in the category of sets. This is merely a reformulation of the defining property of products in arbitrary categories. The system really works.

Let $\mathfrak{A}$, $\mathfrak{B}$ be two categories. The functors of $\mathfrak{A}$ into $\mathfrak{B}$ (say covariant, and in one variable) can be viewed as the objects of a category, whose morphisms are defined as follows. Let L, M be two such functors. A **morphism** $H: L \to M$ (also called a **natural transformation**) is a rule which to each object X of $\mathfrak{A}$ associates a morphism

$$H_X: L(X) \to M(X)$$

such that for any morphism $f: X \to Y$ the following diagram is commutative:

$$\begin{array}{ccc} L(X) & \xrightarrow{H_X} & M(X) \\ {\scriptstyle L(f)}\downarrow & & \downarrow{\scriptstyle M(f)} \\ L(Y) & \xrightarrow[H_Y]{} & M(Y) \end{array}$$

We can therefore speak of **isomorphisms** of functors. A functor is **representable** if it is isomorphic to a representation functor as above.

As Grothendieck pointed out, one can use the representation functor to transport the notions of certain structures on sets to arbitrary categories. For instance, let $\mathfrak{A}$ be a category and G an object of $\mathfrak{A}$. We say that G is a **group object** in $\mathfrak{A}$ if for each object X of $\mathfrak{A}$ we are given a group structure on the set $\mathrm{Mor}(X, G)$ in such a way that the association

$$X \mapsto \mathrm{Mor}(X, G)$$

is functorial (i.e. is a functor from $\mathfrak{A}$ into the category of groups). One sometimes denotes the set $\mathrm{Mor}(X, G)$ by $G(X)$, and thinks of it as the set of points of G in X. To justify this terminology, the reader is referred to Chapter IX, §2.

Example. Let **Var** be the category of projective non-singular varieties over the complex numbers. To each object X in **Var** one can associate various groups, e.g. $\mathrm{Pic}(X)$ (the group of divisor classes for rational equivalence), which is a contravariant functor into the category of abelian groups. Let $\mathrm{Pic}_0(X)$ be the subgroup of classes algebraically equivalent to 0. Then Pic_0 is representable.

In the fifties and sixties Grothendieck was the one who emphasized the importance of the representation functors, and the possibility of transposing to any category notions from more standard categories by means of the representation functors. He himself proved that a number of important functors in algebraic geometry are representable.

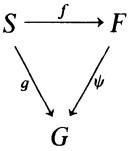
§12. FREE GROUPS

We now turn to the coproduct in the category of groups. First a remark. Let $G = \prod G_i$ be a direct product of groups.

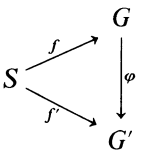
We observe that each G_j admits an injective homomorphism into the product, on the j-th component, namely the map $\lambda_j : G_j \to \prod_i G_i$ such that for x in G_j, the i-th component of $\lambda_j(x)$ is the unit element of G_i if $i \neq j$, and is equal to x itself if $i = j$. This embedding will be called the **canonical** one. But we still don't have a coproduct of the family, because the factors commute with each other. To get a coproduct one has to work somewhat harder.

Let G be a group and S a subset of G. We recall that G is **generated** by S if every element of G can be written as a finite product of elements of S and their inverses (the empty product being always taken as the unit element of G). Elements of S are then called **generators**. If there exists a finite set of generators for G we call G **finitely generated**. If S is a set and $\varphi : S \to G$ is a map, we say that φ **generates** G if its image generates G.

Let S be a set, and $f : S \to F$ a map into a group. Let $g : S \to G$ be another map. If $f(S)$ (or as we also say, f) generates F, then it is obvious that there exists at most one homomorphism ψ of F into G which makes the following diagram commutative:



We now consider the category $\mathfrak{C}$ whose objects are the maps of S into groups. If $f : S \to G$ and $f' : S \to G'$ are two objects in this category, we define a morphism from f to f' to be a homomorphism $\varphi : G \to G'$ such that $\varphi \circ f = f'$, i.e. the diagram is commutative:



By a **free group** determined by S, we shall mean a universal element in this category.

Proposition 12.1. *Let S be a set. Then there exists a free group (F, f) determined by S. Furthermore, f is injective, and F is generated by the image of f.*

Proof. (I owe this proof to J. Tits.) We begin with a lemma.

Lemma 12.2. *There exists a set I and a family of groups $\{G_i\}_{i\in I}$ such that, if $g\colon S \to G$ is a map of S into a group G, and g generates G, then G is isomorphic to some G_i.*

Proof. This is a simple exercise in cardinalities, which we carry out. If S is finite, then G is finite or denumerable. If S is infinite, then the cardinality of G is $\leqq$ the cardinality of S because G consists of finite products of elements of $g(S)$. Let T be a set which is infinite denumerable if S is finite, and has the same cardinality as S if S is infinite. For each non-empty subset H of T, let Γ_H be the set of group structures on H. For each $\gamma \in \Gamma_H$, let H_γ be the set H, together with the group structure γ. Then the family $\{H_\gamma\}$ for $\gamma \in \Gamma_H$ and H ranging over subsets of T is the desired family.

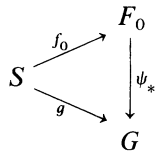
We return to the proof of the proposition. For each $i \in I$ we let M_i be the set of mappings of S into G_i. For each map $\varphi \in M_i$, we let $G_{i,\varphi}$ be the set-theoretic product of G_i and the set with one element $\{\varphi\}$, so that $G_{i,\varphi}$ is the "same" group as G_i indexed by φ. We let

$$F_0 = \prod_{i\in I} \prod_{\varphi \in M_i} G_{i,\varphi}$$

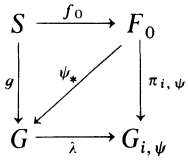
be the Cartesian product of the groups $G_{i,\varphi}$. We define a map

$$f_0 : S \to F_0$$

by sending S on the factor $G_{i,\varphi}$ by means of φ itself. We contend that given a map $g\colon S \to G$ of S into a group G, there exists a homomorphism $\psi_*\colon F_0 \to G$ making the usual diagram commutative:



That is, $\psi_* \circ f_0 = g$. To prove this, we may assume that g generates G, simply by restricting our attention to the subgroup of G generated by the image of g. By the lemma, there exists an isomorphism $\lambda : G \to G_i$ for some i, and $\lambda \circ g$ is an element ψ of M_i. We let $\pi_{i,\psi}$ be the projection on the (i, ψ) factor, and we let $\psi_* = \lambda^{-1} \circ \pi_{i,\psi}$. Then the map ψ_* makes the following diagram commutative.

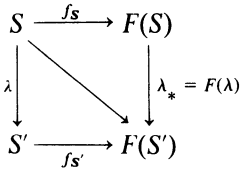


We let F be the subgroup of F_0 generated by the image of f_0, and we let f simply be equal to f_0, viewed as a map of S into F. We let g_* be the restriction of ψ_* to F. In this way, we see at once that the map g_* is the unique one making

our diagram commutative, and thus that (F, f) is the required free group. Furthermore, it is clear that f is injective.

For each set S we select one free group determined by S, and denote it by $(F(S), f_S)$ or briefly by $F(S)$. It is generated by the image of f_S. One may view S as contained in $F(S)$, and the elements of S are called **free** generators of $F(S)$. If $g: S \to G$ is a map, we denote by $g_*: F(S) \to G$ the homomorphism realizing the universality of our free group $F(S)$.

If $\lambda: S \to S'$ is a map of one set into another, we let $F(\lambda): F(S) \to F(S')$ be the map $(f_{S'} \circ \lambda)_*$.



Then we may regard F as a functor from the category of sets to the category of groups (the functorial properties are trivially verified, and will be left to the reader).

If λ is surjective, then $F(\lambda)$ is also surjective.

We again leave the proof to the reader.

If two sets S, S' have the same cardinality, then they are isomorphic in the category of sets (an isomorphism being in this case a bijection!), and hence $F(S)$ is isomorphic to $F(S')$. If S has n elements, we call $F(S)$ the **free group on n generators**.

Let G be a group, and let S be the same set as G (i.e. G viewed as a set, without group structure). We have the identity map $g: S \to G$, and hence a surjective homomorphism

$$g_*: F(S) \to G$$

which will be called **canonical**. Thus every group is a factor group of a free group.

One can also construct groups by what is called **generators and relations**. Let S be a set, and $F(S)$ the free group. We assume that $f: S \to F(S)$ is an inclusion. Let R be a set of elements of $F(S)$. Each element of R can be written as a finite product

$$\prod_{\nu=1}^{n} x_\nu$$

where each x_ν is an element of S or an inverse of an element of S. Let N be the smallest normal subgroup of $F(S)$ containing R, i.e. the intersection of all normal subgroups of $F(S)$ containing R. Then $F(S)/N$ will be called the group **determined by the generators S and the relations R**.

Example. One shows easily that the group determined by one generator a, and the relation $\{a^2\}$, has order 2.

The canonical homomorphism $\varphi: F(S) \to F(S)/N$ satisfies the universal mapping property for homomorphisms ψ of $F(S)$ into groups G such that $\psi(x) = e$ for all $x \in R$. In view of this, one sometimes calls the group $F(S)/N$ the group determined by the generators S, and the relations $x = e$ (for all $x \in R$). For instance, the group in the preceding example would be called the group determined by the generator a, and the relation $a^2 = e$.

Let G be a group generated by a finite number of elements, and satisfying the relation $x^2 = e$ for all $x \in G$. What does G look like? It is easy to show that G is commutative. Then one can view G as a vector space over $\mathbf{Z}/2\mathbf{Z}$, so G is determined by its cardinality, up to isomorphism.

In Exercises 34 and 35, you will prove that there exist certain groups satisfying certain relations and with a given order, so that the group presented with these generators and relations can be completely determined. *A priori*, it is not even clear if a group given by generators and relations is finite. Even if it is finite, one does not know its order *a priori*. To show that a group of certain order exists, one has to use various means, a common means being to represent the group as a group of automorphisms of some object, for instance the symmetries of a geometric object. This will be the method suggested for the groups in Exercises 34 and 35, mentioned above.

Example. Let G be a group. For $x, y \in G$ define $[x, y] = xyx^{-1}y^{-1}$ (the commutator) and ${}^xy = xyx^{-1}$ (the conjugate). Then one has the cocycle relation

$$[x, yz] = [x, y]^y[x, z].$$

Furthermore, suppose $x, y, z \in G$ and

$$[x, y] = y, \quad [y, z] = z, \quad [z, x] = x.$$

Then $x = y = z = e$. It is an exercise to prove these assertions, but one sees that certain relations imply that a group generated by x, y, z subject to those relations is necessarily trivial.

Next we give a somewhat more sophisticated example. We assume that the reader knows the basic terminology of fields and matrices as in Chapter XIII, but applied only to 2×2 matrices. Thus $SL_2(F)$ denotes the group of 2×2 matrices with components in a field F and determinant equal to 1.

Example. $SL_2(F)$. Let F be a field. For $b \in F$ and $a \in F$, $a \neq 0$, we let

$$u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad s(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \text{and } w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then it is immediately verified that:

SL 0. $s(a) = wu(a^{-1})wu(a)wu(a^{-1})$.

SL 1. u is an additive homomorphism.

SL 2. s is a multiplicative homomorphism.

SL 3. $w^2 = s(-1)$.

SL 4. $s(a)u(b)s(a^{-1}) = u(ba^2)$.

Now, conversely, suppose that G is an arbitrary group with generators $u(b)$ ($b \in F$) and w, such that if we define $s(a)$ for $a \neq 0$ by **SL 0**, then the relations **SL 1** through **SL 4** are satisfied. Then **SL 3** and **SL 4** show that $s(-1)$ is in the center, and $w^4 = e$. In addition, one verifies that:

SL 5. $ws(a) = s(a^{-1})w$.

Furthermore, one has the theorem:

Let G be the free group with generators $u(b)$, w and relations **SL 1** *through* **SL 4**, *defining $s(a)$ as in* **SL 0**. *Then the natural homomorphism*

$$G \to SL_2(F)$$

is an isomorphism.

Proofs of all the above statements will be found in my **SL_2(R)**, Springer Verlag, reprint of Addison-Wesley, 1975, Chapter XI, §2. It takes about a page to carry out the proof.

If $F = \mathbf{Q}_p$ is the field of p-adic numbers, then Ihara [Ih 66] proved that every discrete torsion free subgroup of $SL_2(\mathbf{Q}_p)$ is free. Serre put this theorem in the context of a general theory concerning groups acting on trees [Se 80].

[Ih 66] Y. IHARA, On discrete subgroups of the two by two projective linear group over p-adic fields, *J. Math. Soc. Japan* **18** (1966) pp. 219–235

[Se 80] J.-P. SERRE, *Trees*, Springer Verlag 1980

Further examples. For further examples of free group constructions, see Exercises 54 and 56. For examples of free groups occurring (possibly conjecturally) in Galois theory, see Chapter VI, §2, Example 9, and the end of Chapter VI, §14.

Proposition 12.3. *Coproducts exist in the category of groups.*

Proof. Let $\{G_i\}_{i \in I}$ be a family of groups. We let $\mathfrak{C}$ be the category whose objects are families of group-homomorphisms

$$\{g_i : G_i \to G\}_{i \in I}$$

and whose morphisms are the obvious ones. We must find a universal element in this category. For each index i, we let S_i be the same set as G_i if G_i is infinite, and we let S_i be denumerable if G_i is finite. We let S be a set having the same cardinality as the set-theoretic disjoint union of the sets S_i (i.e. their coproduct in the category of sets). We let Γ be the set of group structures on S, and for each $\gamma \in \Gamma$, we let Φ_γ be the set of all families of homomorphisms

$$\varphi = \{\varphi_i : G_i \to S_\gamma\}.$$

Each pair (S_γ, φ), where $\varphi \in \Phi_\gamma$, is then a group, using φ merely as an index. We let

$$F_0 = \prod_{\gamma \in \Gamma} \prod_{\varphi \in \Phi_\gamma} (S_\gamma, \varphi),$$

and for each i, we define a homomorphism $f_i : G_i \to F_0$ by prescribing the component of f_i on each factor (S_γ, φ) to be the same as that of φ_i.

Let now $g = \{g_i : G_i \to G\}$ be a family of homomorphisms. Replacing G if necessary by the subgroup generated by the images of the g_i, we see that $\text{card}(G) \leqq \text{card}(S)$, because each element of G is a *finite* product of elements in these images. Embedding G as a factor in a product $G \times S_\gamma$ for some γ, we may assume that $\text{card}(G) = \text{card}(S)$. There exists a homomorphism $g_* : F_0 \to G$ such that

$$g_* \circ f_i = g_i$$

for all i. Indeed, we may assume without loss of generality that $G = S_\gamma$ for some γ and that $g = \psi$ for some $\psi \in \Phi_\gamma$. We let g_* be the projection of F_0 on the factor (S_γ, ψ).

Let F be the subgroup of F_0 generated by the union of the images of the maps f_i for all i. The restriction of g_* to F is the unique homomorphism satisfying $f_i \circ g_* = g_i$ for all i, and we have thus constructed our universal object.

Example. Let G_2 be a cyclic group of order 2 and let G_3 be a cyclic group of order 3. What is the coproduct? The answer is neat. It can be shown that $G_2 \amalg G_3$ is the group generated by two elements S, T with relations $S^2 = 1$, $(ST)^3 = 1$. The groups G_2 and G_3 are embedded in $G_2 \amalg G_3$ by sending G_2 on the cyclic group generated by S and sending G_3 on the cyclic group generated by ST. The group can be represented as follows. Let

$$G = SL_2(\mathbf{Z})/\pm 1.$$

As we have seen in an example of §5, the group G operates on the upper half-plane $\mathfrak{H}$. Let S, T be the maps given by

$$S(z) = -1/z \quad \text{and} \quad T(z) = z + 1.$$

Thus S and T are represented by the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

and satisfy the relations $S^2 = 1$, $(ST)^3 = 1$. Readers will find a proof of several properties of S, T in Serre's *Course in Arithmetic* (Springer Verlag, 1973, Chapter VII, §1), including the fact that S, T generate G. It is an exercise from there to show that G is the coproduct of G_2 and G_3 as asserted.

Observe that these procedures go directly from the universal definition and construction in the proofs of Proposition 12.1 and Proposition 12.3 to the more explicit representation of the free group or the coproduct as the case may be. One relies on the following proposition.

Proposition 12.4. *Let G be a group and $\{G_i\}_{i \in I}$ a family of subgroups. Assume:*

(a) *The family generates G.*

(b) *If*

$$x = x_{i_1} \cdots x_{i_n} \quad \text{with } x_{i_\nu} \in G_{i_\nu},\ x_{i_\nu} \neq e \text{ and } i_\nu \neq i_{\nu+1} \text{ for all } \nu,$$

then $x \neq e$.

Then the natural homomorphism of the coproduct of the family into G sending G_i on itself by the identity mapping is an isomorphism. In other words, simply put, G is the coproduct of the family of subgroups.

Proof. The homomorphism from the coproduct into G is surjective by the assumption that the family generates G. Suppose an element is in the kernel. Then such an element has a representation

$$x_{i_1} \cdots x_{i_n}$$

as in (b), mapping to the identity in G, so all $x_{i_\nu} = e$ and the element itself is equal to e, whence the homomorphism from the coproduct into G is injective, thereby proving the proposition.

Exercises 54 and 56 mentioned above give one illustration of the way Proposition 12.4 can be used. We now show another way, which we carry out for two subgroups. I am indebted to Eilenberg for the neat arrangement of the proof of the next proposition.

Proposition 12.5. *Let A, B be two groups whose set-theoretic intersection is $\{1\}$. There exists a group $A \circ B$ containing A, B as subgroups, such that $A \cap B = \{1\}$, and having the following property. Every element $\neq 1$ of $A \circ B$ has a unique expression as a product*

$$a_1 \cdots a_n \qquad (n \geqq 1, a_i \neq 1 \text{ all } i)$$

with $a_i \in A$ or $a_i \in B$, and such that if $a_i \in A$ then $a_{i+1} \in B$ and if $a_i \in B$ then $a_{i+1} \in A$.

Proof. Let $A \circ B$ be the set of sequences

$$a = (a_1, \ldots, a_n) \qquad (n \geqq 0)$$

such that either $n = 0$, and the sequence is empty or $n \geqq 1$, and then elements in the sequence belong to A or B, are $\neq 1$, and two consecutive elements of the sequence do not belong both to A or both to B. If $b = (b_1, \ldots, b_m)$, we define the product ab to be the sequence

$$(a_1, \ldots, a_n, b_1, \ldots, b_m) \qquad \text{if} \quad a_n \in A, b_1 \in B \quad \text{or} \quad a_n \in B, b_1 \in A,$$

$$(a_1, \ldots, a_n b_1, \ldots, b_m) \qquad \text{if} \quad a_n, b_1 \in A \quad \text{or} \quad a_n, b_1 \in B, \quad \text{and} \quad a_n b_1 \neq 1,$$

$$(a_1, \ldots, a_{n-1})(b_2, \ldots, b_m) \qquad \text{by induction, if} \quad a_n, b_1 \in A \quad \text{or} \quad a_n, b_1 \in B \quad \text{and} \quad a_n b_1 = 1.$$

The case when $n = 0$ or $m = 0$ is included in the first case, and the empty sequence is the unit element of $A \circ B$. Clearly,

$$(a_1, \ldots, a_n)(a_n^{-1}, \ldots, a_1^{-1}) = \text{unit element},$$

so only associativity need be proved. Let $c = (c_1, \ldots, c_r)$.

First consider the case $m = 0$, i.e. b is empty. Then clearly $(ab)c = a(bc)$ and similarly if $n = 0$ or $r = 0$. Next consider the case $m = 1$. Let $b = (x)$ with $x \in A$, $x \neq 1$. We then verify in each possible case that $(ab)c = a(bc)$. These cases are as follows:

$$(a_1, \ldots, a_n, x, c_1, \ldots, c_r) \qquad \text{if} \quad a_n \in B \quad \text{and} \quad c_1 \in B,$$

$$(a_1, \ldots, a_n x, c_1, \ldots, c_r) \qquad \text{if} \quad a_n \in A, a_n x \neq 1, c_1 \in B,$$

$$(a_1, \ldots, a_n, xc_1, \ldots, c_r) \qquad \text{if} \quad a_n \in B, c_1 \in A, xc_1 \neq 1,$$

$$(a_1, \ldots, a_{n-1})(c_1, \ldots, c_r) \qquad \text{if} \quad a_n = x^{-1} \quad \text{and} \quad c_1 \in B,$$

$$(a_1, \ldots, a_n)(c_2, \ldots, c_r) \quad \text{if} \quad a_n \in B \quad \text{and} \quad c_1 = x^{-1},$$

$$(a_1, \ldots, a_{n-1}, a_n x c_1, c_2, \ldots, c_r) \quad \text{if} \quad a_n, c_1 \in A, a_n x c_1 \neq 1,$$

$$(a_1, \ldots, a_{n-1})(c_2, \ldots, c_r) \quad \text{if} \quad a_n, c_1 \in A \quad \text{and} \quad a_n x c_1 = 1.$$

If $m > 1$, then we proceed by induction. Write $b = b'b''$ with b' and b'' shorter. Then

$$(ab)c = (a(b'b''))c = ((ab')b'')c = (ab')(b''c),$$

$$a(bc) = a((b'b'')c) = a(b'(b''c)) = (ab')(b''c)$$

as was to be shown.

We have obvious injections of A and B into $A \circ B$, and identifying A, B with their images in $A \circ B$ we obtain a proof of our proposition.

We can prove the similar result for several factors. In particular, we get the following corollary for the free group.

Corollary 12.6. *Let $F(S)$ be the free group on a set S, and let $x_1, \ldots, x_n$ be distinct elements of S. Let $\nu_1, \ldots, \nu_r$ be integers $\neq 0$ and let $i_1, \ldots, i_r$ be integers,*

$$1 \leqq i_1, \ldots, i_r \leqq n$$

such that $i_j \neq i_{j+1}$ for $j = 1, \ldots, r-1$. Then

$$x_{i_1}^{\nu_1} \cdots x_{i_r}^{\nu_r} \neq 1.$$

Proof. Let $G_1, \ldots, G_n$ be the cyclic groups generated by $x_1, \ldots, x_n$. Let $G = G_1 \circ \cdots \circ G_n$. Let

$$F(S) \to G$$

be the homomorphism sending each x_i on x_i, and all other elements of S on the unit element of G. Our assertion follows at once.

Corollary 12.7. *Let S be a set with n elements $x_1, \ldots, x_n$, $n \geqq 1$. Let $G_1, \ldots, G_n$ be the infinite cyclic groups generated by these elements. Then the map*

$$F(S) \to G_1 \circ \cdots \circ G_n$$

sending each x_i on itself is an isomorphism.

Proof. It is obviously surjective and injective.

Corollary 12.8. *Let $G_1, \ldots, G_n$ be groups with $G_i \cap G_j = \{1\}$ if $i \neq j$. The homomorphism*

$$G_1 \amalg \cdots \amalg G_n \to G_1 \circ \cdots \circ G_n$$

of their coproduct into $G_1 \circ \cdots \circ G_n$ induced by the natural inclusion $G_i \to G_1 \circ \cdots \circ G_n$ is an isomorphism.

Proof. Again, it is obviously injective and surjective.

EXERCISES

1. Show that every group of order $\leqq 5$ is abelian.
2. Show that there are two non-isomorphic groups of order 4, namely the cyclic one, and the product of two cyclic groups of order 2.
3. Let G be a group. A **commutator** in G is an element of the form $aba^{-1}b^{-1}$ with a, $b \in G$. Let G^c be the subgroup generated by the commutators. Then G^c is called the **commutator subgroup**. Show that G^c is normal. Show that any homomorphism of G into an abelian group factors through G/G^c.
4. Let H, K be subgroups of a finite group G with $K \subset N_H$. Show that
$$\#(HK) = \frac{\#(H)\#(K)}{\#(H \cap K)}.$$
5. **Goursat's Lemma.** Let G, G' be groups, and let H be a subgroup of $G \times G'$ such that the two projections $p_1 : H \to G$ and $p_2 : H \to G'$ are surjective. Let N be the kernel of p_2 and N' be the kernel of p_1. One can identify N as a normal subgroup of G, and N' as a normal subgroup of G'. Show that the image of H in $G/N \times G'/N'$ is the graph of an isomorphism
$$G/N \approx G'/N'.$$
6. Prove that the group of inner automorphisms of a group G is normal in $\mathrm{Aut}(G)$.
7. Let G be a group such that $\mathrm{Aut}(G)$ is cyclic. Prove that G is abelian.
8. Let G be a group and let H, H' be subgroups. By a **double coset** of H, H' one means a subset of G of the form HxH'.
   (a) Show that G is a disjoint union of double cosets.
   (b) Let $\{c\}$ be a family of representatives for the double cosets. For each $a \in G$ denote by $[a]H'$ the conjugate $aH'a^{-1}$ of H'. For each c we have a decomposition into ordinary cosets
   $$H = \bigcup_c x_c(H \cap [c]H'),$$
   where $\{x_c\}$ is a family of elements of H, depending on c. Show that the elements $\{x_c c\}$ form a family of left coset representatives for H' in G; that is,
   $$G = \bigcup_{x_c} \bigcup_{x_c} x_c c H',$$
   and the union is disjoint. (Double cosets will not emerge further until Chapter XVIII.)
9. (a) Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index. [*Hint*: If $(G : H) = n$, find a homomorphism of G into S_n whose kernel is contained in H.]
   (b) Let G be a group and let H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.
10. Let G be a group and let H be a subgroup of finite index. Prove that there is only a finite number of right cosets of H, and that the number of right cosets is equal to the number of left cosets.

11. Let G be a group, and A a normal abelian subgroup. Show that G/A operates on A by conjugation, and in this manner get a homomorphism of G/A into $\mathrm{Aut}(A)$.

Semidirect product

12. Let G be a group and let H, N be subgroups with N normal. Let γ_x be conjugation by an element $x \in G$.
    (a) Show that $x \mapsto \gamma_x$ induces a homomorphism $f: H \mapsto \mathrm{Aut}(N)$.
    (b) If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if f is trivial, i.e. $f(x) = \mathrm{id}_N$ for all $x \in H$.

    We define G to be the **semidirect product** of H and N if $G = NH$ and $H \cap N = \{e\}$.

    (c) Conversely, let N, H be groups, and let $\psi: H \to \mathrm{Aut}(N)$ be a given homomorphism. Construct a semidirect product as follows. Let G be the set of pairs (x, h) with $x \in N$ and $h \in H$. Define the composition law

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_1) x_2, h_1 h_2).$$

    Show that this is a group law, and yields a semidirect product of N and H, identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$.

13. (a) Let H, N be normal subgroups of a finite group G. Assume that the orders of H, N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \approx HN$.
    (b) Let $H_1, \ldots, H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that

$$H_1 \times \ldots \times H_r \approx H_1 \cdots H_r.$$

    Example. If the Sylow subgroups of a finite group are normal, then G is the direct product of its Sylow subgroups.

14. Let G be a finite group and let N be a normal subgroup such that N and G/N have relatively prime orders.
    (a) Let H be a subgroup of G having the same order as G/N. Prove that $G = HN$.
    (b) Let g be an automorphism of G. Prove that $g(N) = N$.

Some operations

15. Let G be a finite group operating on a finite set S with $\#(S) \geqq 2$. Assume that there is only one orbit. Prove that there exists an element $x \in G$ which has no fixed point, i.e. $xs \neq s$ for all $s \in S$.

16. Let H be a proper subgroup of a finite group G. Show that G is not the union of all the conjugates of H. (But see Exercise 23 of Chapter XIII.)

17. Let X, Y be finite sets and let C be a subset of $X \times Y$. For $x \in X$ let $\varphi(x)$ = number of elements $y \in Y$ such that $(x, y) \in C$. Verify that

$$\#(C) = \sum_{x \in X} \varphi(x).$$

Remark. A subset C as in the above exercise is often called a **correspondence**, and $\varphi(x)$ is the number of elements in Y which correspond to a given element $x \in X$.

18. Let S, T be finite sets. Show that $\#\mathrm{Map}(S, T) = (\#T)^{\#(S)}$.

19. Let G be a finite group operating on a finite set S.
    (a) For each $s \in S$ show that
    $$\sum_{t \in Gs} \frac{1}{\#(Gt)} = 1.$$
    (b) For each $x \in G$ define $f(x)$ = number of elements $s \in S$ such that $xs = s$. Prove that the number of orbits of G in S is equal to
    $$\frac{1}{\#(G)} \sum_{x \in G} f(x).$$

Throughout, p is a prime number.

20. Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

21. Let G be a finite group and H a subgroup. Let P_H be a p-Sylow subgroup of H. Prove that there exists a p-Sylow subgroup P of G such that $P_H = P \cap H$.

22. Let H be a normal subgroup of a finite group G and assume that $\#(H) = p$. Prove that H is contained in every p-Sylow subgroup of G.

23. Let P, P' be p-Sylow subgroups of a finite group G.
    (a) If $P' \subset N(P)$ (normalizer of P), then $P' = P$.
    (b) If $N(P') = N(P)$, then $P' = P$.
    (c) We have $N(N(P)) = N(P)$.

Explicit determination of groups

24. Let p be a prime number. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.

25. Let G be a group of order p^3, where p is prime, and G is not abelian. Let Z be its center. Let C be a cyclic group of order p.
    (a) Show that $Z \approx C$ and $G/Z \approx C \times C$.
    (b) Every subgroup of G of order p^2 contains Z and is normal.
    (c) Suppose $x^p = 1$ for all $x \in G$. Show that G contains a normal subgroup $H \approx C \times C$.

26. (a) Let G be a group of order pq, where p, q are primes and $p < q$. Assume that $q \not\equiv 1 \bmod p$. Prove that G is cyclic.
    (b) Show that every group of order 15 is cyclic.

27. Show that every group of order < 60 is solvable.

28. Let p, q be distinct primes. Prove that a group of order p^2q is solvable, and that one of its Sylow subgroups is normal.

29. Let p, q be odd primes. Prove that a group of order $2pq$ is solvable.

30. (a) Prove that one of the Sylow subgroups of a group of order 40 is normal.
(b) Prove that one of the Sylow subgroups of a group of order 12 is normal.

31. Determine all groups of order $\leqq 10$ up to isomorphism. In particular, show that a non-abelian group of order 6 is isomorphic to S_3.

32. Let S_n be the permutation group on n elements. Determine the p-Sylow subgroups of S_3, S_4, S_5 for $p = 2$ and $p = 3$.

33. Let σ be a permutation of a finite set I having n elements. Define $e(\sigma)$ to be $(-1)^m$ where

$$m = n - \text{number of orbits of } \sigma.$$

If $I_1, \ldots, I_r$ are the orbits of σ, then m is also equal to the sum

$$m = \sum_{v=1}^{r} [\text{card}(I_v) - 1].$$

If τ is a transposition, show that $e(\sigma\tau) = -e(\sigma)$ be considering the two cases when i, j lie in the same orbit of σ, or lie in different orbits. In the first case, $\sigma\tau$ has one more orbit and in the second case one less orbit than σ. In particular, the sign of a transposition is -1. Prove that $e(\sigma) = \varepsilon(\sigma)$ is the sign of the permutation.

34. (a) Let n be an even positive integer. Show that there exists a group of order $2n$, generated by two elements σ, τ such that $\sigma^n = e = \tau^2$, and $\sigma\tau = \tau\sigma^{n-1}$. (Draw a picture of a regular n-gon, number the vertices, and use the picture as an inspiration to get σ, τ.) This group is called the **dihedral group**.
(b) Let n be an odd positive integer. Let D_{4n} be the group generated by the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

where ζ is a primitive n-th root of unity. Show that D_{4n} has order $4n$, and give the commutation relations between the above generators.

35. Show that there are exactly two non-isomorphic non-abelian groups of order 8. (One of them is given by generators σ, τ with the relations

$$\sigma^4 = 1, \qquad \tau^2 = 1, \qquad \tau\sigma\tau = \sigma^3.$$

The other is the quaternion group.)

36. Let $\sigma = [123 \cdots n]$ in S_n. Show that the conjugacy class of σ has $(n-1)!$ elements. Show that the centralizer of σ is the cyclic group generated by σ.

37. (a) Let $\sigma = [i_1 \cdots i_m]$ be a cycle. Let $\gamma \in S_n$. Show that $\gamma\sigma\gamma^{-1}$ is the cycle $[\gamma(i_1) \cdots \gamma(i_m)]$.
(b) Suppose that a permutation σ in S_n can be written as a product of r disjoint cycles, and let $d_1, \ldots, d_r$ be the number of elements in each cycle, in increasing order. Let τ be another permutation which can be written as a product of disjoint cycles, whose cardinalities are $d'_1, \ldots, d'_s$ in increasing order. Prove that σ is conjugate to τ in S_n if and only if $r = s$ and $d_i = d'_i$ for all $i = 1, \ldots, r$.

38. (a) Show that S_n is generated by the transpositions $[12], [13], \ldots, [1n]$.
(b) Show that S_n is generated by the transpositions $[12], [23], [34], \ldots, [n-1, n]$.

(c) Show that S_n is generated by the cycles $[12]$ and $[123 \ldots n]$.

(d) Assume that n is prime. Let $\sigma = [123 \ldots n]$ and let $\tau = [rs]$ be any transposition. Show that σ, τ generate S_n.

Let G be a finite group operating on a set S. Then G operates in a natural way on the Cartesian product $S^{(n)}$ for each positive integer n. We define the operation on S to be n-**transitive** if given n distinct elements $(s_1, \ldots, s_n)$ and n distinct elements $(s'_1, \ldots, s'_n)$ of S, there exists $\sigma \in G$ such that $\sigma s_i = s'_i$ for all $i = 1, \ldots, n$.

39. Show that the action of the alternating group A_n on $\{1, \ldots, n\}$ is $(n-2)$-transitive.

40. Let A_n be the alternating group of even permutations of $\{1, \ldots, n\}$. For $j = 1, \ldots, n$ let H_j be the subgroup of A_n fixing j, so $H_j \approx A_{n-1}$, and $(A_n : H_j) = n$ for $n \geqq 3$. Let $n \geqq 3$ and let H be a subgroup of index n in A_n.
    (a) Show that the action of A_n on cosets of H by left translation gives an isomorphism A_n with the alternating group of permutations of A_n/H.
    (b) Show that there exists an automorphism of A_n mapping H_1 on H, and that such an automorphism is induced by an inner automorphism of S_n if and only if $H = H_i$ for some i.

41. Let H be a simple group of order 60.
    (a) Show that the action of H by conjugation on the set of its Sylow subgroups gives an imbedding $H \hookrightarrow A_6$.
    (b) Using the preceding exercise, show that $H \approx A_5$.
    (c) Show that A_6 has an automorphism which is not induced by an inner automorphism of S_6.

Abelian groups

42. Viewing $\mathbf{Z}, \mathbf{Q}$ as additive groups, show that $\mathbf{Q}/\mathbf{Z}$ is a torsion group, which has one and only one subgroup of order n for each integer $n \geqq 1$, and that this subgroup is cyclic.

43. Let H be a subgroup of a finite abelian group G. Show that G has a subgroup that is isomorphic to G/H.

44. Let $f : A \to A'$ be a homomorphism of abelian groups. Let B be a subgroup of A. Denote by A^f and A_f the image and kernel of f in A respectively, and similarly for B^f and B_f. Show that $(A : B) = (A^f : B^f)(A_f : B_f)$, in the sense that if two of these three indices are finite, so is the third, and the stated equality holds.

45. Let G be a finite cyclic group of order n, generated by an element σ. Assume that G operates on an abelian group A, and let $f, g : A \to A$ be the endomorphisms of A given by

$$f(x) = \sigma x - x \quad \text{and} \quad g(x) = x + \sigma x + \cdots + \sigma^{n-1}x.$$

Define the **Herbrand quotient** by the expression $q(A) = (A_f : A^g)/(A_g : A^f)$, provided both indices are finite. Assume now that B is a subgroup of A such that $GB \subset B$.
    (a) Define in a natural way an operation of G on A/B.
    (b) Prove that

$$q(A) = q(B)q(A/B)$$

in the sense that if two of these quotients are finite, so is the third, and the stated equality holds.
    (c) If A is finite, show that $q(A) = 1$.

(This exercise is a special case of the general theory of Euler characteristics discussed in Chapter XX, Theorem 3.1. After reading this, the present exercise becomes trivial. Why?)

Primitive groups

46. Let G operate on a set S. Let $S = \bigcup S_i$ be a partition of S into disjoint subsets. We say that the partition is **stable** under G if G maps each S_i onto S_j for some j, and hence G induces a permutation of the sets of the partition among themselves. There are two partitions of S which are obviously stable: the partition consisting of S itself, and the partition consisting of the subsets with one element. Assume that G operates transitively, and that S has more than one element. Prove that the following two conditions are equivalent:

PRIM 1. The only partitions of S which are stable are the two partitions mentioned above.

PRIM 2. If H is the isotropy group of an element of S, then H is a maximal subgroup of G.

These two conditions define what is known as a **primitive group**, or more accurately, a **primitive operation** of G on S.

Instead of saying that the operation of a group G is 2-transitive, one also says that it is **doubly transitive**.

47. Let a finite group G operate transitively and faithfully on a set S with at least 2 elements and let H be the isotropy group of some element s of S. (All the other isotropy groups are conjugates of H.) Prove the following:
    (a) G is doubly transitive if and only if H acts transitively on the complement of s in S.
    (b) G is doubly transitive if and only if $G = HTH$, where T is a subgroup of G of order 2 not contained in H.
    (c) If G is doubly transitive, and $(G : H) = n$, then
    $$\#(G) = d(n - 1)n,$$
    where d is the order of the subgroup fixing two elements. Furthermore, H is a maximal subgroup of G, i.e. G is primitive.

48. Let G be a group acting transitively on a set S with at least 2 elements. For each $x \in G$ let $f(x)$ = number of elements of S fixed by x. Prove:
    (a) $\sum_{x \in G} f(x) = \#(G)$.
    (b) G is doubly transitive if and only if
    $$\sum_{x \in G} f(x)^2 = 2\ \#(G).$$

49. **A group as an automorphism group.** Let G be a group and let $\mathbf{Set}(G)$ be the category of G-sets (i.e. sets with a G-operation). Let F: $\mathbf{Set}(G) \to \mathbf{Set}$ be the forgetful functor, which to each G-set assigns the set itself. Show that $\mathrm{Aut}(F)$ is naturally isomorphic to G.

Fiber products and coproducts
Pull-backs and push-outs

50. (a) Show that fiber products exist in the category of abelian groups. In fact, if X, Y are abelian groups with homomorphisms $f: X \to Z$ and $g: Y \to Z$ show that $X \times_Z Y$ is the set of all pairs (x, y) with $x \in X$ and $y \in Y$ such that $f(x) = g(y)$. The maps p_1, p_2 are the projections on the first and second factor respectively.
    (b) Show that the pull-back of a surjective homomorphism is surjective.

51. (a) Show that fiber products exist in the category of sets.
    (b) In any category $\mathcal{C}$, consider the category $\mathcal{C}_Z$ of objects over Z. Let $h: T \to Z$ be a fixed object in this category. Let F be the functor such that

$$F(X) = \mathrm{Mor}_Z(T, X),$$

    where X is an object over Z, and Mor_Z denotes morphisms over Z. Show that F transforms fiber products over Z into products in the category of sets. (Actually, once you have understood the definitions, this is tautological.)

52. (a) Show that push-outs (i.e. fiber coproducts) exist in the category of abelian groups. In this case the fiber coproduct of two homomorphisms f, g as above is denoted by $X \oplus_Z Y$. Show that it is the factor group

$$X \oplus_Z Y = (X \oplus Y)/W,$$

    where W is the subgroup consisting of all elements $(f(z), -g(z))$ with $z \in Z$.
    (b) Show that the push-out of an injective homomorphism is injective.

Remark. After you have read about modules over rings, you should note that the above two exercises apply to modules as well as to abelian groups.

53. Let H, G, G' be groups, and let

$$f: H \to G, \qquad g: H \to G'$$

be two homomorphisms. Define the notion of coproduct of these two homomorphisms over H, and show that it exists.

54. (Tits). Let G be a group and let $\{G_i\}_{i \in I}$ be a family of subgroups generating G. Suppose G operates on a set S. For each $i \in I$, suppose given a subset S_i of S, and let s be a point of $S - \bigcup_i S_i$. Assume that for each $g \in G_i - \{e\}$, we have

$$gS_j \subset S_i \text{ for all } j \neq i, \quad \text{and} \quad g(s) \in S_i \text{ for all } i.$$

    Prove that G is the coproduct of the family $\{G_i\}_{i \in I}$. (*Hint*: Suppose a product $g_1 \cdots g_m = \mathrm{id}$ on S. Apply this product to s, and use Proposition 12.4.)

55. Let $M \in GL_2(\mathbf{C})$ (2×2 complex matrices with non-zero determinant). We let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ and for } z \in \mathbf{C} \text{ we let } M(z) = \frac{az + b}{cz + d}.$$

    If $z = -d/c$ ($c \neq 0$) then we put $M(z) = \infty$. Then you can verify (and you should have seen something like this in a course in complex analysis) that $GL_2(\mathbf{C})$ thus operates on $\mathbf{C} \cup \{\infty\}$. Let λ, λ' be the eigenvalues of M viewed as a linear map on $\mathbf{C}^2$. Let W, W' be the corresponding eigenvectors,

$$W = {}^t(w_1, w_2) \text{ and } W' = {}^t(w_1', w_2').$$

By a **fixed point** of M on $\mathbf{C}$ we mean a complex number z such that $M(z) = z$. *Assume that M has two distinct fixed points $\neq \infty$.*

(a) Show that there cannot be more than two fixed points and that these fixed points are $w = w_1/w_2$ and $w' = w_1'/w_2'$. In fact one may take

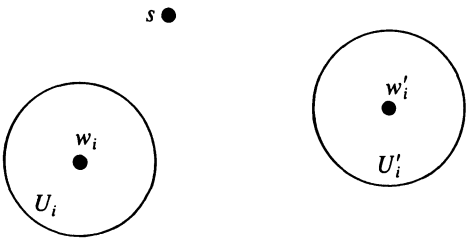
$$W = {}^t(w, 1), \quad W' = {}^t(w', 1).$$

(b) Assume that $|\lambda| < |\lambda'|$. Given $z \neq w$, show that

$$\lim_{k \to \infty} M^k(z) = w'.$$

[*Hint*: Let $S = (W, W')$ and consider $S^{-1}M^kS(z) = \alpha^k z$ where $\alpha = \lambda/\lambda'$.]

56. (Tits) Let $M_1, \ldots, M_r \in GL_2(\mathbf{C})$ be a finite number of matrices. Let λ_i, λ_i' be the eigenvalues of M_i. Assume that each M_i has two distinct complex fixed points, and that $|\lambda_i| < |\lambda_i'|$. Also assume that the fixed points for $M_1, \ldots, M_r$ are all distinct from each other. Prove that there exists a positive integer k such that $M_1^k, \ldots, M_r^k$ are the free generators of a free subgroup of $GL_2(\mathbf{C})$. [*Hint*: Let w_i, w_i' be the fixed points of M_i. Let U_i be a small disc centered at w_i and U_i' a small disc centered at w_i'. Let $S_i = U_i \cup U_i'$. Let s be a complex number which does not lie in any S_i. Let $G_i = \langle M_i^k \rangle$. Show that the conditions of Exercise 54 are satisfied for k sufficiently large.].



57. Let G be a group acting on a set X. Let Y be a subset of X. Let G_Y be the subset of G consisting of those elements g such that $gY \cap Y$ is not empty. Let $\overline{G}_Y$ be the subgroup of G generated by G_Y. Then $\overline{G}_Y Y$ and $(G - \overline{G}_Y)Y$ are disjoint. [*Hint*: Suppose that there exist $g_1 \in \overline{G}_Y$ and $g_2 \in G$ but $g_2 \notin \overline{G}_Y$, and elements $y_1, y_2, \in Y$ such that $g_2 y_1 = g_2 y_2$. Then $g_2^{-1} g_1 y_1 = y_2$, so $g_2^{-1} g_1 \in G_Y$ whence $g_2 \in \overline{G}_Y$, contrary to assumption.]

Application. Suppose that $X = GY$, but that X cannot be expressed as a disjoint union as above unless one of the two sets is empty. Then we conclude that $G - \overline{G}_Y$ is empty, and therefore G_Y generates G.

Example 1. Suppose X is a connected topological space, Y is open, and G acts continuously. Then all translates of Y are open, so G is generated by G_Y.

Example 2. Suppose G is a discrete group acting continuously and discretely on X. Again suppose X connected and Y closed, and that any union of translates of Y by elements of G is closed, so again $G - \overline{G}_Y$ is empty, and G_Y generates G.