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 product 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 $xHx^{-1} = H$.