(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.
(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)
(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

1.5 THE QUATERNION GROUP

The *quaternion group*, Q_8, is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

$$1 \cdot a = a \cdot 1 = a, \qquad \text{for all } a \in Q_8$$

$$(-1) \cdot (-1) = 1, \qquad (-1) \cdot a = a \cdot (-1) = -a, \quad \text{for all } a \in Q_8$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

$$i \cdot j = k, \qquad j \cdot i = -k$$
$$j \cdot k = i, \qquad k \cdot j = -i$$
$$k \cdot i = j, \qquad i \cdot k = -j.$$

As usual, we shall henceforth write ab for $a \cdot b$. It is tedious to check the associative law (we shall prove this later by less computational means), but the other axioms are easily checked. Note that Q_8 is a non-abelian group of order 8.

EXERCISES

1. Compute the order of each of the elements in Q_8.
2. Write out the group tables for S_3, D_8 and Q_8.
3. Find a set of generators and relations for Q_8.

1.6 HOMOMORPHISMS AND ISOMORPHISMS

In this section we make precise the notion of when two groups "look the same," that is, have exactly the same group-theoretic structure. This is the notion of an *isomorphism* between two groups. We first define the notion of a *homomorphism* about which we shall have a great deal more to say later.

Definition. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \qquad \text{for all } x, y \in G$$

is called a *homomorphism*.

When the group operations for G and H are not explicitly written, the homomorphism condition becomes simply

$$\varphi(xy) = \varphi(x)\varphi(y)$$

but it is important to keep in mind that the product xy on the left is computed in G and the product $\varphi(x)\varphi(y)$ on the right is computed in H. Intuitively, a map φ is a homomorphism if it respects the group structures of its domain and codomain.

Definition. The map $\varphi : G \to H$ is called an *isomorphism* and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

(1) φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and

(2) φ is a bijection.

In other words, the groups G and H are isomorphic if there is a bijection between them which preserves the group operations. Intuitively, G and H are the same group except that the elements and the operations may be written differently in G and H. Thus any property which G has which depends only on the group structure of G (i.e., can be derived from the group axioms — for example, commutativity of the group) also holds in H. Note that this formally justifies writing all our group operations as $\cdot$ since changing the symbol of the operation does not change the isomorphism type.

Examples

(1) For any group G, $G \cong G$. The identity map provides an obvious isomorphism but not, in general, the *only* isomorphism from G to itself. More generally, let $\mathcal{G}$ be any nonempty collection of groups. It is easy to check that the relation $\cong$ is an equivalence relation on $\mathcal{G}$ and the equivalence classes are called *isomorphism classes*. This accounts for the somewhat symmetric wording of the definition of "isomorphism."

(2) The exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$ defined by $\exp(x) = e^x$, where e is the base of the natural logarithm, is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$. Exp is a bijection since it has an inverse function (namely $\log_e$) and exp preserves the group operations since $e^{x+y} = e^x e^y$. In this example both the elements and the operations are different yet the two groups are isomorphic, that is, as groups they have identical structures.

(3) In this example we show that the isomorphism type of a symmetric group depends only on the cardinality of the underlying set being permuted.

Let Δ and Ω be nonempty sets. The symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$. We can see this intuitively as follows: given that $|\Delta| = |\Omega|$, there is a bijection θ from Δ onto Ω. Think of the elements of Δ and Ω as being glued together via θ, i.e., each $x \in \Delta$ is glued to $\theta(x) \in \Omega$. To obtain a map $\varphi : S_\Delta \to S_\Omega$ let $\sigma \in S_\Delta$ be a permutation of Δ and let $\varphi(\sigma)$ be the permutation of Ω which moves the elements of Ω in the same way σ moves the corresponding glued elements of Δ; that is, if $\sigma(x) = y$, for some $x, y \in \Delta$, then $\varphi(\sigma)(\theta(x)) = \theta(y)$ in Ω. Since the set bijection θ has an inverse, one can easily check that the map between symmetric groups also has an inverse. The precise technical definition of the map φ and the straightforward, albeit tedious, checking of the properties which ensure φ is an isomorphism are relegated to the following exercises.

Conversely, if $S_\Delta \cong S_\Omega$, then $|\Delta| = |\Omega|$; we prove this only when the underlying

sets are finite (when both Δ and Ω are infinite sets the proof is harder and will be given as an exercise in Chapter 4). Since any isomorphism between two groups G and H is, a priori, a bijection between them, a necessary condition for isomorphism is $|S_\Delta| = |S_\Omega|$. When Δ is a finite set of order n, then $|S_\Delta| = n!$. We actually only proved this for S_n, however the same reasoning applies for S_Δ. Similarly, if Ω is a finite set of order m, then $|S_\Omega| = m!$. Thus if S_Δ and S_Ω are isomorphic then $n! = m!$, so $m = n$, i.e., $|\Delta| = |\Omega|$.

Many more examples of isomorphisms will appear throughout the text. When we study different structures (rings, fields, vector spaces, etc.) we shall formulate corresponding notions of isomorphisms between respective structures. One of the central problems in mathematics is to determine what properties of a structure specify its isomorphism type (i.e., to prove that if G is an object with some structure (such as a group) and G has property $\mathcal{P}$, then any other similarly structured object (group) X with property $\mathcal{P}$ is isomorphic to G). Theorems of this type are referred to as *classification theorems*. For example, we shall prove that

any non-abelian group of order 6 is isomorphic to S_3

(so here G is the group S_3 and $\mathcal{P}$ is the property "non-abelian and of order 6"). From this classification theorem we obtain $D_6 \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find explicit maps between these groups. Note that it is not true that any group of order 6 is isomorphic to S_3. In fact we shall prove that up to isomorphism there are precisely two groups of order 6: S_3 and $\mathbb{Z}/6\mathbb{Z}$ (i.e., any group of order 6 is isomorphic to one of these two groups and S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$). Note that the conclusion is less specific (there are two possible types); however, the hypotheses are easier to check (namely, check to see if the order is 6). Results of the latter type are also referred to as classifications. Generally speaking it is subtle and difficult, even in specific instances, to determine whether or not two groups (or other mathematical objects) are isomorphic — constructing an explicit map between them which preserves the group operations or proving no such map exists is, except in tiny cases, computationally unfeasible as indicated already in trying to prove the above classification of groups of order 6 without further theory.

It is occasionally easy to see that two given groups are *not* isomorphic. For example, the exercises below assert that if $\varphi : G \to H$ is an isomorphism, then, in particular,

(a) $|G| = |H|$

(b) G is abelian if and only if H is abelian

(c) for all $x \in G$, $|x| = |\varphi(x)|$.

Thus S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic (as indicated above) since one is abelian and the other is not. Also, $(\mathbb{R}-\{0\}, \times)$ and $(\mathbb{R}, +)$ cannot be isomorphic because in $(\mathbb{R}-\{0\}, \times)$ the element -1 has order 2 whereas $(\mathbb{R}, +)$ has no element of order 2, contrary to (c).

Finally, we record one very useful fact that we shall prove later (when we discuss free groups) dealing with the question of homomorphisms and isomorphisms between two groups given by generators and relations:

Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H