9. Describe the strategy of the proof of Theorem 4. Outline the proof.

30. Let S be a nonempty set with a [illegible] such that any equivalence relation on S is a congruence relation.

9.4 Groups

In this section we examine a special type of monoid, called a group, that has applications in every area where symmetry occurs. Applications of groups can be found in mathematics, physics, and chemistry, as well as in less obvious areas such as sociology. Recent and exciting applications of group theory have arisen in fields such as particle physics and in the solutions of puzzles such as Rubik's cube. In this book, we shall present an important application of group theory to binary codes in Section 11.2.

A **group** $(G, *)$ is a monoid, with identity e, that has the additional property that for every element $a \in G$ there exists an element $a' \in G$ such that $a * a' = a' * a = e$. Thus a group is a set together with a binary operation $*$ on G such that

1. $(a * b) * c = a * (b * c)$ for any elements a, b, and c in G.
2. There is a unique element e in G such that

$$a * e = e * a \qquad \text{for any } a \in G.$$

3. For every $a \in G$, there is an element $a' \in G$, called an **inverse** of a, such that

$$a * a' = a' * a = e.$$

Observe that if $(G, *)$ is a group, then $*$ is a binary operation, so G must be closed under $*$; that is,

$$a * b \in G \qquad \text{for any elements } a \text{ and } b \text{ in } G.$$

To simplify our notation, from now on when only one group $(G, *)$ is under consideration and there is no possibility of confusion, we shall write the product $a * b$ of the elements a and b in the group $(G, *)$ simply as ab, and we shall also refer to $(G, *)$ simply as G.

A group G is said to be **Abelian** if $ab = ba$ for all elements a and b in G.

Example 1 The set of all integers $\mathbb{Z}$ with the operation of ordinary addition is an Abelian group. If $a \in \mathbb{Z}$, then an inverse of a is its opposite $-a$. ◆

Example 2 The set $\mathbb{Z}^+$ under the operation of ordinary multiplication is not a group since, for example, the element 2 in $\mathbb{Z}^+$ has no inverse. However, this set together with the given operation is a monoid. ◆

Example 3 The set of all nonzero real numbers under the operation of ordinary multiplication is a group. An inverse of $a \neq 0$ is $1/a$. ◆

Example 4 Let G be the set of all nonzero real numbers and let

$$a * b = \frac{ab}{2}.$$

Show that $(G, *)$ is an Abelian group.

Solution

We first verify that $*$ is a binary operation. If a and b are elements of G, then $ab/2$ is a nonzero real number and hence is in G. We next verify associativity. Since

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4}$$

and since

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)c}{4},$$

the operation $*$ is associative.

The number 2 is the identity in G, for if $a \in G$, then

$$a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a.$$

Finally, if $a \in G$, then $a' = 4/a$ is an inverse of a, since

$$a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a.$$

Since $a * b = b * a$ for all a and b in G, we conclude that G is an Abelian group. ◆

Before proceeding with additional examples of groups, we develop several important properties that are satisfied in any group G.

THEOREM 1 Let G be a group. Each element a in G has only one inverse in G.

Proof

Let a' and a'' be inverses of a. Then

$$a'(aa'') = a'e = a'$$

and

$$(a'a)a'' = ea'' = a''.$$

Hence, by associativity,

$$a' = a''.$$ ■

From now on we shall denote the inverse of a by a^{-1}. Thus in a group G we have

$$aa^{-1} = a^{-1}a = e.$$

THEOREM 2 Let G be a group and let a, b, and c be elements of G. Then

(a) $ab = ac$ implies that $b = c$ (**left cancellation property**).

(b) $ba = ca$ implies that $b = c$ (**right cancellation property**).

Proof

(a) Suppose that

$$ab = ac.$$

Multiplying both sides of this equation by a^{-1} on the left, we obtain

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c && \text{by associativity} \\ eb &= ec && \text{by the definition of an inverse} \\ b &= c && \text{by definition of an identity.} \end{aligned}$$

(b) The proof is similar to that of part (a). ■

Corollary 1 Let G be a group and $a \in G$. Define a function $M_a: G \to G$ by the formula $M_a(g) = ag$. Then M_a is one to one.

Proof
This is a direct consequence of Theorem 2. ■

THEOREM 3 Let G be a group and let a and b be elements of G. Then

(a) $(a^{-1})^{-1} = a$.

(b) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof

(a) We show that a acts as an inverse for a^{-1}:

$$a^{-1}a = aa^{-1} = e.$$

Since the inverse of an element is unique, we conclude that $(a^{-1})^{-1} = a$.

(b) We easily verify that

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

and, similarly,

$$(b^{-1}a^{-1})(ab) = e,$$

so

$$(ab)^{-1} = b^{-1}a^{-1}.$$ ■

THEOREM 4 Let G be a group, and let a and b be elements of G. Then

(a) The equation $ax = b$ has a unique solution in G.

(b) The equation $ya = b$ has a unique solution in G.

Proof

(a) The element $x = a^{-1}b$ is a solution of the equation $ax = b$, since

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Suppose now that x_1 and x_2 are two solutions of the equation $ax = b$. Then

$$ax_1 = b \quad \text{and} \quad ax_2 = b.$$

Hence

$$ax_1 = ax_2.$$

Theorem 2 implies that $x_1 = x_2$.

(b) The proof is similar to that of part (a). ■

groups involve only the semigroup and [illegible]

corollary is an immediate consequence of Theorems 3 and 4 of Section 9.3.

Corollary 1 **(a)** If R is a congruence relation on a group G, then the function $f_R: G \to G/R$, given by $f_R(a) = [a]$, is a group homomorphism.

(b) If $f: G \to G'$ is a homomorphism from the group $(G, *)$ onto the group $(G', *')$, and R is the relation defined on G by $a \; R \; b$ if and only if $f(a) = f(b)$, for a and b in G, then

1. R is a congruence relation.
2. The function $\overline{f}: G/R \to G'$, given by $\overline{f}([a]) = f(a)$, is an isomorphism from the group $(G/R, \circledast)$ onto the group $(G', *')$. ■

Congruence relations on groups have a very special form, which we will now develop. Let H be a subgroup of a group G, and let $a \in G$. The **left coset** of H in G determined by a is the set $aH = \{ah \mid h \in H\}$. The **right coset** of H in G determined by a is the set $Ha = \{ha \mid h \in H\}$. Finally, we will say that a subgroup H of G is **normal** if $aH = Ha$ for all a in G.

Warning If $Ha = aH$, it does *not* follow that, for $h \in H$ and $a \in G$, $ha = ah$. It does follow that $ha = ah'$, where h' is some element in H.

THEOREM 3 Let R be a congruence relation on a group G, and let $H = [e]$, the equivalence class containing the identity. Then H is a normal subgroup of G and, for each $a \in G$, $[a] = aH = Ha$.

Proof

Let a and b be any elements in G. Since R is an equivalence relation, $b \in [a]$ if and only if $[b] = [a]$. Also, G/R is a group by Theorem 2. Therefore, $[b] = [a]$ if and only if $[e] = [a]^{-1}[b] = [a^{-1}b]$. Thus $b \in [a]$ if and only if $H = [e] = [a^{-1}b]$. That is, $b \in [a]$ if and only if $a^{-1}b \in H$ or $b \in aH$. This proves that $[a] = aH$ for every $a \in G$. We can show similarly that $b \in [a]$ if and only if $H = [e] = [b][a]^{-1} = [ba^{-1}]$. This is equivalent to the statement $[a] = Ha$. Thus $[a] = aH = Ha$, and H is normal. ■

Combining Theorem 3 with Corollary 1, we see that in this case the quotient group G/R consists of all the left cosets of $N = [e]$. The operation in G/R is given by

$$(aN)(bN) = [a] \circledast [b] = [ab] = abN$$

and the function $f_R: G \to G/R$, defined by $f_R(a) = aN$, is a homomorphism from G onto G/R. For this reason, we will often write G/R as G/N.

left cosets of the subgroup $\{1, 9\}$.

be a finite group and H a subgroup of G. Prove set of distinct left cosets of H is a partition of G.

38. Use the results of Exercises 27 and 37 to describe the relationship between the order of H and the order of G.

9.6 Other Mathematical Structures

Rings

In earlier sections, we have seen many cases where a set S has two binary operations defined on it. Here we study such structures in more detail. In particular, let S be a nonempty set with two binary operations $+$ and $*$ such that $(S, +)$ is an Abelian group and $*$ is distributive over $+$. (The operation symbols are the same as those for the most well-known such structure, the real numbers.) The structure $(S, +, *)$ is called a **ring** if $*$ is associative. If $*$ is associative and commutative, we call $(S, +, *)$ a **commutative ring**. If $(S, *)$ is a monoid, then $(S, +, *)$ is a **ring with identity**. The identity for $*$ is usually denoted by 1; the identity for $+$ is usually denoted by 0.

Example 1 Let $S = \mathbb{Z}$, the integers, and let $+$ and $*$ be the usual addition and multiplication of integers. Then $(S, +, *)$ is a commutative ring with identity. ◆

Example 2 Let S be the set of all 2×2 matrices, and let $+$ and $*$ be the operations of addition and multiplication of matrices defined in Section 1.5. Then it follows from theorems proved in Section 1.5 that S is a noncommutative ring. Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then I is an identity for matrix multiplication, that is, $AI = IA = A$ for all A in S. This means that $(S, +, *)$ is a ring with identity that is not commutative. ◆

Recall that if a, b, and n are integers, with $n > 1$, then we say that a is congruent to b mod n, written $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n, or, alternatively, if a and b have the same remainder when divided by n. We showed in Section 9.4 that congruence mod n is an equivalence relation on the integers and that the set $\mathbb{Z}_n$ consisting of all equivalence classes is an Abelian group with respect to addition mod n. If we denote the equivalence class of an integer a by the expression $\bar{a}$, then $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$, and $\bar{a} + \bar{b} = \overline{a+b}$.

We now define a multiplication in $\mathbb{Z}_n$. Suppose that a, b, x, and y are integers and that $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$. These assumptions imply that for some integers s and t, we have $a = x + sn$ and $b = y + tn$. Then $ab = xy + xtn + ysn + stn^2$, which means that $ab - xy = n(xt + ys + stn)$, so $ab \equiv xy \pmod{n}$. Thus we can define $\bar{a} * \bar{b}$ to be $\overline{ab}$ and the definition does not depend on the integers picked to represent each equivalence class.

Example 3 The set $\mathbb{Z}_n$ with addition mod n and the multiplication defined previously is a commutative ring with identity. The computations

$$(\bar{a} * \bar{b}) * \bar{c} = \overline{ab} * \bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a} * \overline{bc} = \bar{a} * (\bar{b} * \bar{c})$$

and

$$\begin{aligned} \bar{a} * (\bar{b} + \bar{c}) &= \bar{a} * \overline{(b+c)} \\ &= \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = (\bar{a} * \bar{b}) + (\bar{a} * \bar{c}) \end{aligned}$$

show that multiplication is associative and distributive over addition. In a similar way we can prove that multiplication is associative and that $\bar{1}$ is the identity for multiplication. ♦

Generally, we will refer to $+$ and $*$ as addition and multiplication even when they are not the usual operations with these names.

Many properties of the ring of integers are true for any commutative ring with identity. Two examples are given in the next theorem.

THEOREM 1 Let R be a commutative ring with additive identity 0 and multiplicative identity 1. Then

(a) For any x in R, $0 * x = 0$.

(b) For any x in R, $-x = (-1) * x$.

Proof

(a) Let y denote the element $0 * x$. Since R is a ring, we have

$$y + y = 0 * x + 0 * x = (0 + 0) * x = 0 * x = y.$$

But $(R, +)$ is an Abelian group, so

$$0 = (-y) + y = (-y) + (y + y) = [(-y) + y] + y = 0 + y = y,$$

which shows part (a).

(b) Since $x + ((-1) * x) = (1 * x) + ((-1) * x) = (1 + (-1)) * x = 0 * x = 0$, part (b) follows. ■

In the proof of Theorem 1(b), we use the fact that an inverse in an Abelian group is unique, so that if an element behaves as an inverse, then it must be an inverse.

A nonzero element x of a commutative ring R with identity 1 is said to have a multiplicative inverse y if $x * y = y * x = 1$. If such a y exists, it is unique (Theorem 1 in Section 1.6). We therefore speak of *the* multiplicative inverse of x and denote it by x^{-1}, or sometimes by $1/x$.

The only integers with inverses in $\mathbb{Z}$ are 1 and -1, but the situation in the rings $\mathbb{Z}_n$ is different. We can show that if a is relatively prime to n, that is, if $\text{GCD}(a, n) = 1$, then $\bar{a}$ has a multiplicative inverse in $\mathbb{Z}_n$. In fact, it follows from Theorem 4(a) of Section 1.4 that there are integers k and s satisfying the equation $ak + ns = 1$, or $1 - ak = ns$. This means that $\bar{1} = \overline{ak} = \bar{a} * \bar{k}$, and we see that $\bar{a}$ has the multiplicative inverse $\bar{k}$.

Example 4 The integer 25 is relatively prime to 384, so $\overline{25}$ has a multiplicative inverse in $\mathbb{Z}_{384}$. To find it, we use the Euclidean algorithm developed in Section 1.4.

$$\begin{aligned} 384 &= 15 \times 25 + 9 \\ 25 &= 2 \times 9 + 7 \\ 9 &= 1 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \end{aligned}$$

By successive substitutions, we get

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 = 7 - 3(9 - 7) = (4 \cdot 7) - (3 \cdot 9) \\ &= 4(25 - 2 \cdot 9) - (3 \cdot 9) = (4 \cdot 25) - (11 \cdot 9) \\ &= (4 \cdot 25) - 11(384 - 15 \cdot 25) = (169 \cdot 25) - 11 \cdot (384). \end{aligned}$$

This shows that $169 \cdot 25 \equiv 1 \pmod{384}$, so the multiplicative inverse of $\overline{25}$ in $\mathbb{Z}_{384}$ is $\overline{169}$. ◆

Fields

Suppose that F is a commutative ring with identity. We say that F is a **field** if every nonzero element x in F has a multiplicative inverse. In the following table, we summarize the properties of a field F.

Field Properties

F has two binary operations: an addition $+$ and a multiplication $*$, and two special elements denoted 0 and 1, so that for all x, y, and z in F.

(1) $x + y = y + x$	**(2)** $x * y = y * x$
(3) $(x + y) + z = x + (y + z)$	**(4)** $(x * y) * z = x * (y * z)$
(5) $x + 0 = x$	**(6)** $x * 1 = x$
(7) $x * (y + z) = (x * y) + (x * z)$	**(8)** $(y + z) * x = (y * x) + (z * x)$

(9) For each x in F there is a unique element in F denoted by $-x$ so that $x + (-x) = 0$.

(10) For each $x \neq 0$ in F there is a unique element in F denoted by x^{-1} so that $x * x^{-1} = 1$.

Example 5 The collection $\mathbb{R}$ of all real numbers, with ordinary addition and multiplication, is a field. Here $x^{-1} = 1/x$. The field properties shown in the preceding table are the standard rules of arithmetic. ◆

Example 6 The collection $\mathbb{Q}$ of all rational numbers, with ordinary addition and multiplication, is a field. ◆

The preceding examples are typical of fields. Fields obey virtually all the familiar rules of arithmetic and algebra, and most algebraic techniques can be used in any field. Remarkably, there are fields with only a finite number of elements. The following theorem introduces the finite fields most important to our future discussions.

THEOREM 2 The ring $\mathbb{Z}_n$ is a field when n is a prime.

Proof
Recall that n is a prime if it has no divisors other than itself and 1. If $\bar{a}$ is any nonzero element of $\mathbb{Z}_n$, then a is not divisible by n, so $\text{GCD}(a, n) = 1$. It follows from the discussion preceding Example 4 that $\bar{a}$ has a multiplicative inverse, so $\mathbb{Z}_n$ is a field. ■

Example 7 By Theorem 2, $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ is a field. Since $2+3 = 5$, we have $\bar{2}+\bar{3} = \bar{0}$, so $-\bar{2} = \bar{3}$ and $-\bar{3} = \bar{2}$. Similarly, $-\bar{4} = \bar{1}$ and $-\bar{1} = \bar{4}$. For notational convenience, we denote the multiplicative inverse of a nonzero element $\bar{a}$ in this field by $\frac{1}{\bar{a}}$, and the product of elements $\bar{a}$ and $\bar{b}$ by $\bar{a} \cdot \bar{b}$. Then, since $2 \cdot 3 = 6 = 1 \cdot 5 + 1$, we see that $\bar{2} \cdot \bar{3} = \bar{1}$. Thus $\frac{1}{\bar{2}} = \bar{3}$ and $\frac{1}{\bar{3}} = \bar{2}$. Similarly, since $4 \cdot 4 = 16 = 3 \cdot 5 + 1$, we

have $\frac{\bar{1}}{\bar{4}} = \bar{4}$ and, as in the real number field, $\bar{1}$ is also its own multiplicative inverse. We can use these facts in the same way we would for real numbers. For example, suppose we want to solve the following system of equations simultaneously:

$$\begin{cases} \bar{3}x + \bar{2}y = \bar{4} \\ \bar{2}x + \bar{4}y = \bar{2}. \end{cases}$$

We could begin by multiplying the first equation by $\frac{\bar{1}}{\bar{3}} = \bar{2}$, to obtain $x + \bar{4}y = \bar{3}$ (since $\bar{2} \cdot \bar{4} = \bar{3}$), or $x = \bar{3} - \bar{4}y = \bar{3} + (-\bar{4})y = \bar{3} + y$, using Theorem 1(b). We then substitute for x in the second equation and obtain

$$\bar{2} \cdot (\bar{3} + y) + \bar{4}y = \bar{1} + y = \bar{2},$$

where we have used the facts that $\bar{2} \cdot \bar{3} = \bar{1}$ and $\bar{2} + \bar{4} = \bar{1}$. We see that $y = \bar{1}$, so $x = \bar{4}$. ◆

The reader is invited to check this result by substituting into the system of equations.

Fermat's Little Theorem

An important property of any field F is that the set F' of nonzero elements of F is an Abelian group under multiplication. We need to show that F' is closed under multiplication, that is, that the product of nonzero elements of F is nonzero. Then the result will follow from properties (2), (4), (6), and (10) of fields. Suppose that $a * b = 0$ in F. If a is not 0, then we can multiply both sides of the equation $a * b = 0$ by a^{-1} and obtain

$$b = a^{-1} * 0 = 0$$

by Theorem 1(a). Thus either a or b must be 0. It follows that the product of nonzero elements in F is nonzero, and thus F' is closed under multiplication and is therefore an Abelian group.

The following result has many mathematical uses and parts (b) and (c) will be used for our treatment of public key cryptology in Chapter 11.

THEOREM 3

(a) If $G = \{g_1, g_2, \ldots, g_n\}$ is a finite Abelian group with identity denoted by e, and a is any element of G, then $a^n = e$.

(b) Fermat's Little Theorem: If p is a prime number, and $\text{GCD}(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

(c) If p is a prime number, and a is any integer, then $a^p \equiv a \pmod{p}$.

Proof

(a) Corollary 1 in Section 9.4 shows that multiplication by an element in a group is a one-to-one function. Therefore, the products $ag_1, ag_2, \ldots, ag_n$ are all distinct, and are simply the elements $g_1, g_2, \ldots, g_n$ possibly arranged in a different order. It follows from this and the commutativity of multiplication in G that

$$g_1 g_2 \cdots g_n = (ag_1)(qg_2) \cdots (ag_n) = g_1 g_2 \cdots g_n (a^n).$$

Part (a) results from multiplying each side of this equation on the left by $(g_1 g_2 \cdots g_n)^{-1}$.

(b) If p is a prime, then $\mathbb{Z}_p$ is a field by Theorem 2, so the nonzero elements form an Abelian group under multiplication. The identity of this group is $\bar{1}$. Since this group has $p-1$ elements, part (a) implies that if $\bar{a} \neq \bar{0}$, then $[\bar{a}]^{p-1} = \bar{1}$. This is equivalent to part (b).

(c) If a is not divisible by p, then we can apply Fermat's Little Theorem, and the result follows by multiplying both sides of the congruence by a. If a is divisible by p, then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$, so a^p and a are congruent to one another. ■

Example 8 By Fermat's Little Theorem, $12^{30} \equiv 1 \pmod{31}$ and $74^{83} \equiv 74 \pmod{83}$. ◆

Example 9 What is the remainder when 4^{900} is divided by 53?

Solution

We know by Fermat's Little Theorem that $4^{52} \equiv 1 \pmod{53}$. Since

$$900 = (17 \times 52) + 16,$$

we have

$$4^{900} = 4^{(17\times 52)+16} = (4^{52})^{17}4^{16} \equiv 4^{16} \pmod{53}.$$

Now

$$4^3 = 64 \equiv 11 \pmod{53}$$
$$4^6 \equiv 11^2 \equiv 15 \pmod{53}$$
$$4^{12} \equiv 15^2 \equiv 13 \pmod{53}$$
$$4^{16} \equiv 4^{12} \cdot 128 \equiv 13 \cdot 22 \equiv 21 \pmod{53}.$$

Thus the remainder after dividing 4^{900} by 53 is 21. ◆