Mathematical Proofs
A Transition to Advanced Mathematics

Chapter 15
Proofs in Group Theory

Gary Chartrand Albert D. Polimeni Ping Zhang

Binary Operations

Definition

By a **binary operation** $*$ on a nonempty set S, we mean a function from $S \times S$ to S, that is, $*$ is a function that maps every ordered pair of elements of S to an element of S. Thus, $* : S \times S \to S$.

In particular, if the ordered pair (a, b) in $S \times S$ is mapped into the element c in S by a binary operation $*$ (that is, c is the image of (a, b) under $*$), then we write $c = a * b$ rather than the more awkward notation $*((a, b)) = c$. Consequently, addition $+$ and multiplication $\cdot$ are binary operations on $\mathbf{Z}$.

For example, under addition, the ordered pair $(3, 5)$ is mapped into $3 + 5 = 8$; while under multiplication, $(3, 5)$ is mapped into $3 \cdot 5 = 15$.

Binary Operations

Subtraction is also a binary operation on $\mathbf{Z}$ but it is not a binary operation on $\mathbf{N}$ since, for example, subtraction maps the ordered pair $(3, 5)$ into $3 - 5 = -2$, which does not belong to $\mathbf{N}$. Therefore, subtraction is not a function from $\mathbf{N} \times \mathbf{N}$ to $\mathbf{N}$ since it is not defined at $(3, 5)$, as well as at many other ordered pairs of positive integers.

Similarly, division is not a binary operation on $\mathbf{Z}$ or on $\mathbf{N}$ because it is not defined for many ordered pairs, including $(1, 0) \in \mathbf{Z} \times \mathbf{Z}$ and $(2, 3) \in \mathbf{N} \times \mathbf{N}$ because $1/0 \notin \mathbf{Z}$ and $2/3 \notin \mathbf{N}$.

However, division is a binary operation on the set $\mathbf{Q}^+$ of positive rational numbers since the quotient of two positive rational numbers is once again a positive rational number.

Binary Operations

Not only are addition and multiplication binary operations on $\mathbf{Z}$, they are binary operations on $\mathbf{Q}$ and $\mathbf{R}$, as well as on $\mathbf{R}^+$ (the positive real numbers) and $\mathbf{Q}^+$. For the set $\mathbf{R}^*$ of nonzero real numbers, multiplication is a binary operation but addition is not (since $1 + (-1) = 0 \notin \mathbf{R}^*$, for example).

Definition

If $*$ is a binary operation on a set S, then, by definition, $a * b \in S$ for all $a, b \in S$. If T is a nonempty subset of S and $a, b \in T$, then certainly $a * b \in S$; however, $a * b$ need not belong to T. A nonempty subset T of S is said to be **closed** under $*$ if whenever, $a, b \in T$, then $a * b \in T$ as well.

If $*$ is a binary operation on S, then certainly S is closed under $*$. Although subtraction is a binary operation on $\mathbf{Z}$, the subset $\mathbf{N}$ of $\mathbf{Z}$ is not closed under subtraction.

Binary Operations

Among familiar sets with familiar binary operations are:

(*a*) the set $\mathbf{Z}_n = \{[0], [1], \cdots, [n-1]\}$ of the integers modulo $n \geq 2$ under addition

$$[a] + [b] = [a + b]$$

and under multiplication

$$[a] \cdot [b] = [ab];$$

(*b*) the set $M_2(\mathbf{R})$ of all 2×2 matrices over $\mathbf{R}$ (that is, whose entries are real numbers) under matrix addition

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

and under matrix multiplication

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix};$$

Binary Operations

(c) the set $\mathcal{F}_{\mathbf{R}} = \mathbf{R}^{\mathbf{R}}$ of functions from $\mathbf{R}$ to $\mathbf{R}$ under function addition

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

under function multiplication

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

and under function composition

$$(f \circ g)(x) = f(g(x));$$

(d) the power set $\mathcal{P}(A)$ of a set A under set union, under set intersection and under set difference.

Binary Operations

For a more abstract example of a binary operation, let $S = \{a, b, c\}$. A binary operation $*$ on S is illustrated in the table below, where $a * a = b$, $a * b = c$, $a * c = a$, etc. Since every element in the table belongs to S, it follows that $*$ is indeed a binary operation on S.

$*$	a	b	c
a	b	c	a
b	a	c	a
c	c	a	b

Example 1

Result For $a, b \in \mathbf{R} - \{-2\}$, define

$$a * b = ab + 2a + 2b + 2,$$

where the operations indicated in $ab + 2a + 2b + 2$ are ordinary addition and multiplication in $\mathbf{R}$. Then $*$ is a binary operation on $\mathbf{R} - \{-2\}$.

Proof. We need to show that if $a, b \in \mathbf{R} - \{-2\}$, then $a * b \in \mathbf{R} - \{-2\}$.

Example 1 (continued)

Assume, to the contrary, that there exists some pair $x, y \in \mathbf{R} - \{-2\}$ such that $x * y \notin \mathbf{R} - \{-2\}$. Thus,

$$x * y = xy + 2x + 2y + 2 = -2.$$

This equation is equivalent to

$$(x + 2)(y + 2) = 0,$$

so either $x = -2$ or $y = -2$, which is impossible since $x, y \in \mathbf{R} - \{-2\}$. Hence, $*$ is a binary operation on $\mathbf{R} - \{-2\}$. □

Binary Operations

Defintions

A nonempty set S with a binary operation $*$ is often denoted by $(S, *)$. We refer to $(S, *)$ as an **algebraic structure**. There are certain properties that $(S, *)$ may possess that will be of special interest to us. In particular,

G1 $(S, *)$ is **associative** if $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$;

G2 $(S, *)$ has an element e, called an **identity element** (or simply an **identity**), if $a * e = e * a = a$ for each $a \in S$;

G3 $(S, *)$ has an identity e and, for each element $a \in S$, there is an element $s \in S$, called an **inverse** for a, such that $a * s = s * a = e$;

G4 $(S, *)$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.

Definition

Two elements $a, b \in S$ are said to **commute** if $a * b = b * a$.

If every two elements of S commute, then $(S, *)$ satisfies property G4. By property G2, an identity commutes with every element of S; and by property G3, each element of S commutes with an inverse of this element (assuming, of course, that it has an inverse).

Binary Operations

An algebraic structure $(S, *)$ may satisfy all, some or none of the properties G1 – G4; however, $(S, *)$ cannot satisfy G3 without first satisfying G2.

For elements $a, b, c \in S$, the expression $a * b * c$ is, strictly speaking, not defined. Since $*$ is a *binary* operation, it is only defined for *pairs* of elements of S. There are two standard interpretations of $a * b * c$. Namely, does $a * b * c$ mean $a * (b * c)$ or does $a * b * c$ mean $(a * b) * c$?

On the other hand, if $(S, *)$ satisfies property G1 (the associative property), then $a * (b * c) = (a * b) * c$ and so either interpretation is acceptable in this case. For this reason, we often write $a * b * c$ (without any parentheses).

Ordinarily, however, we will continue to write $a * (b * c)$ or $(a * b) * c$ to emphasize the importance of parentheses, even when $(S, *)$ satisfies the associative property.

Binary Operations

Certainly $(\mathbf{Z}, +)$ satisfies properties G1 – G4, where 0 is an identity element and $-n$ is an inverse for the integer n.

Moreover, $(\mathbf{R}, \cdot)$ satisfies properties G1, G2 and G4, where the integer 1 is an identity element. Turning to property G3, we see that every real number r has $1/r$ as an inverse, except 0, which has no inverse since there is no real number s such that $0 \cdot s = s \cdot 0 = 1$. Thus, $(R, \cdot)$ does not satisfy G3.

In the case of $(\mathbf{R}^*, \cdot)$, where, recall, $\mathbf{R}^*$ is the set of all nonzero real numbers, all four properties G1 – G4 are satisfied.

Binary Operations

The algebraic structure $(\mathbf{Z}_n, +)$, $n \geq 2$, also satisfies all of the properties G1 – G4, where $[0]$ is an identity and $[-a]$ is an inverse of $[a]$.

On the other hand, $(\mathbf{Z}_n, \cdot)$ satisfies only G1, G2 and G4, where $[1]$ is an identity; however $(\mathbf{Z}_n, \cdot)$ does not satisfy G3 since, for example, there is no element $[s] \in \mathbf{Z}_n$ such that $[0][s] = [1]$ in $\mathbf{Z}_n$ and so $[0]$ does not have an inverse.

Binary Operations

The algebraic structure $(M_2(\mathbf{R}), +)$ satisfies all of the properties G1 – G4, where $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is an identity and $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ is an inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

The algebraic structure $(M_2(\mathbf{R}), \cdot)$ only satisfies G1 and G2, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity. For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to have an inverse, the number $ad - bc$ (the determinant of A) must be nonzero. Thus, $(M_2(\mathbf{R}), \cdot)$ does not satisfy G3. Also,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

shows that $(M_2(\mathbf{R}), \cdot)$ does not satisfy property G4.

Example 2

A binary operation $*$ is defined on the set $S = \{a, b, c\}$ by $x * y = x$ for all $x, y \in S$. Determine which of the properties $\mathrm{G1} - \mathrm{G4}$ are satisfied by $(S, *)$.

Solution. Let x, y and z be any three elements of S (distinct or not). Then $x * (y * z) = x * y = x$, while $(x * y) * z = x * z = x$. Thus, $(S, *)$ is associative. Now $(S, *)$ has no identity since for every element $e \in S$, it follows that $e * a = e * b = e$ and so it is impossible for $e * a = a$ *and* $e * b = b$. Since $(S, *)$ has no identity, the question of inverses does not apply here. Certainly, $(S, *)$ is not commutative since $a * b = a$ while $b * a = b$. ⧫

Example 3

Let $*$ be the binary operation defined on $\mathbf{Z}$ by $a * b = a + b - 1$ for $a, b \in \mathbf{Z}$, where the operations indicated in $a + b - 1$ are ordinary addition and subtraction. Determine which of the four properties $\mathrm{G1} - \mathrm{G4}$ are satisfied by $(\mathbf{Z}, *)$.

Solution. For integers a, b and c,

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2,$$

while

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2.$$

Thus, $a * (b * c) = (a * b) * c$ and $(\mathbf{Z}, *)$ is associative.

Example 3 (continued)

Since

$$a + b - 1 = b + a - 1,$$

it follows that $a * b = b * a$ for all $a, b \in \mathbf{Z}$ and so $(\mathbf{Z}, *)$ is commutative.

Let a be an integer. Observe that

$$a * 1 = a + 1 - 1 = a.$$

Thus, 1 is an identity for $(\mathbf{Z}, *)$. For $b = -a + 2 \in \mathbf{Z}$, we have

$$a * b = a * (-a + 2) = a + (-a + 2) - 1 = 1.$$

Hence, b is an inverse of a and every integer has an inverse. Therefore, $(\mathbf{Z}, *)$ satisfies all four properties G1 – G4. ♦

Groups

Definition

A **group** is a nonempty set G together with a binary operation $*$ that satisfies the following three properties:

- G1 **Associative Law:** $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$;
- G2 **Existence of Identity:** There exists an element $e \in G$ such that $a * e = e * a = a$ for every $a \in G$;
- G3 **Existence of Inverses:** For each element $a \in G$, there exists an element $s \in G$ such that $a * s = s * a = e$.

Hence, a group is a special kind of algebraic structure $(G, *)$, namely, one that satisfies properties G1 – G3. If the operation $*$ is clear, then we often denote this group simply by G rather than by $(G, *)$.

Definition

An element $e \in G$ satisfying property G2 is called an **identity** for the group G, while an element s satisfying property G3 is called an **inverse** of a.

If a group G also satisfies the commutative property G4, then G is called an **abelian group**.

The **order of a group** G, denoted by $|G|$, is the cardinality of G. If the order of G is finite, then G is a **finite group**; while if G has an infinite number of elements, then G is an **infinite group**.

All of the groups discussed so far are infinite groups except for $(\mathbf{Z}_n, +)$ which has order n.

Definition

If a finite group G has relatively few elements, then we often describe the operation $*$ by means of a table, called a **group table** (or **operation table**).

Below are the group tables for $(\mathbf{Z}_3, +)$ and $(\mathbf{Z}_4, +)$.

$+$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Although $(\mathbf{Z}_n, +)$ is a group for every integer $n \geq 2$, $(\mathbf{Z}_n, \cdot)$ is not a group for any $n \geq 2$, since, as we have mentioned, the element $[0]$ has no inverse. This suggests considering the set $\mathbf{Z}_n^* = \mathbf{Z}_n - \{[0]\} = \{[1], [2], \cdots, [n-1]\}$, $n \geq 2$, under multiplication.

For some integers $n \geq 2$, multiplication is not a binary operation on $\mathbf{Z}_n^*$. For example, $[2] \in \mathbf{Z}_4^*$ but $[2] \cdot [2] = [0] \notin \mathbf{Z}_4^*$.

On the other hand, multiplication is a binary operation on $\mathbf{Z}_5^*$. In fact, $(\mathbf{Z}_5^*, \cdot)$ satisfies properties G1, G2 and G4, where [1] is an identity. Since

$$[1] \cdot [1] = [1],\ [2] \cdot [3] = [3] \cdot [2] = [1] \text{ and } [4] \cdot [4] = [1],$$

every element of $(\mathbf{Z}_5^*, \cdot)$ has an inverse. Therefore, $(\mathbf{Z}_5^*, \cdot)$ satisfies property G3 as well and so is an abelian group.

Theorem

The set $\mathbf{Z}_n^*$, $n \geq 2$, is a group under multiplication if and only if n is a prime.

Permutation Groups

Definition

Recall that a **permutation** of a nonempty set A is a bijective function $f : A \to A$, that is, f is one-to-one and onto. In Chapter 10, it was shown that:

(1) the composition of every two permutations of A is a permutation of A;

(2) composition of permutations of A is an associative operation;

(3) the identity function $i_A : A \to A$ defined by $i_A(a) = a$ for all $a \in A$ is a permutation of A;

(4) every permutation of A has an inverse, which is also a permutation of A.

Permutation Groups

Definition

By a **permutation group** we mean a group $(G, \circ)$, where G is a set of permutations of some set A and $\circ$ denotes composition.

Let S_A denote the set of *all* permutations of A. Then by the properties of permutations (1) – (4), we have the following result.

Theorem

For every nonempty set A, the algebraic structure $(S_A, \circ)$ is a permutation group.

Definition

The group $(S_A, \circ)$ is called the **symmetric group** on A. Therefore, every symmetric group is a permutation group.

Permutation Groups

Definition

If $A = \{1, 2, \cdots, n\}$, where $n \in \mathbf{N}$, the group S_A is commonly denoted by S_n. The group $(S_n, \circ)$ has $n!$ elements and is commonly called the **symmetric group** (of degree n). The symmetric group $(S_n, \circ)$ is therefore a finite group of order $n!$.

The symmetric group of order 6 is $S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$, where

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Recall that with this notation for a permutation, an element of $\{1, 2, 3\}$ listed in the first row maps into the element in the second row directly below it. Thus, α_1 is the identity of S_3.

Permutation Groups

Let's consider the composition $\alpha_3 \circ \alpha_6$.

$$\alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

For example,

$$(\alpha_3 \circ \alpha_6)(1) = \alpha_3(\alpha_6(1)) = \alpha_3(3) = 1.$$

Also, $(\alpha_3 \circ \alpha_6)(2) = 3$ and $(\alpha_3 \circ \alpha_6)(3) = 2$. Therefore,

$$\alpha_3 \circ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha_2.$$

Similarly $\alpha_6 \circ \alpha_3 = \alpha_4$. Hence, $\alpha_3 \circ \alpha_6 \neq \alpha_6 \circ \alpha_3$. Therefore, $(S_3, \circ)$ is a nonabelian group. This shows that there is a nonabelian group of order 6. There is no nonabelian group having order less than 6, however.

Permutation Groups

When taking the composition of two elements $\alpha, \beta \in S_n$, where $n \in \mathbf{N}$, we often write $\alpha \circ \beta$ as $\alpha\beta$ and say that we are "multiplying" α and β. With this notation, we have $\alpha_3\alpha_6 = \alpha_2$, $\alpha_6\alpha_3 = \alpha_4$, $\alpha_3^2 = \alpha_3\alpha_3 = \alpha_1$ and $\alpha_6^2 = \alpha_6\alpha_6 = \alpha_5$. The group table for $(S_3, \circ)$ is shown in the figure below (containing all 36 products!).

	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_1	α_2	α_3	α_4	α_5	α_6
α_2	α_2	α_1	α_5	α_6	α_3	α_4
α_3	α_3	α_6	α_1	α_5	α_4	α_2
α_4	α_4	α_5	α_6	α_1	α_2	α_3
α_5	α_5	α_4	α_2	α_3	α_6	α_1
α_6	α_6	α_3	α_4	α_2	α_1	α_5

Permutation Groups

A permutation group need not consist of all permutations of some set A. For example, if we consider the subsets $G_1 = \{\alpha_1, \alpha_2\}$ and $G_2 = \{\alpha_1, \alpha_5, \alpha_6\}$ of S_3, then $(G_1, \circ)$ and $(G_2, \circ)$ are both permutation groups. Their group tables are shown below.

	α_1	α_2
α_1	α_1	α_2
α_2	α_2	α_1

	α_1	α_5	α_6
α_1	α_1	α_5	α_6
α_5	α_5	α_6	α_1
α_6	α_6	α_1	α_5

Theorem

Every group $(G, *)$ satisfies:

(a) **The Left Cancellation Law** Let $a, b, c \in G$. If $a * b = a * c$, then $b = c$.

(b) **The Right Cancellation Law** Let $a, b, c \in G$. If $b * a = c * a$, then $b = c$.

Proof. We prove (a) only since the proof of (b) is similar. Assume that $a * b = a * c$ and let s be an inverse for a. Then $s * (a * b) = s * (a * c)$. So,

$$s * (a * b) = (s * a) * b = e * b = b,$$

while

$$s * (a * c) = (s * a) * c = e * c = c.$$

Therefore, $b = c$. □

Theorem

Let $(G, *)$ be a group and let $a, b \in G$. The linear equations $a * x = b$ and $x * a = b$ have unique solutions in G.

Proof. We prove only that $a * x = b$ has a unique solution. Let e be an identity for G, let s be an inverse of a and let $x = s * b$. Then

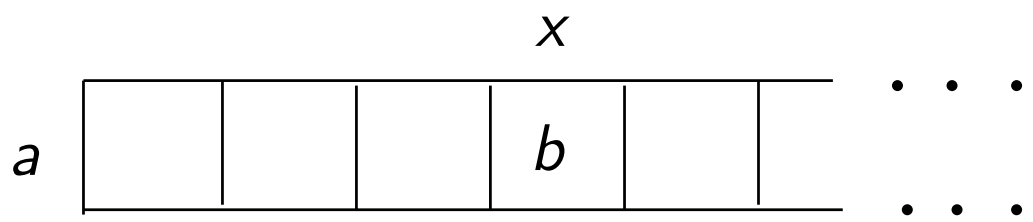
$$a * x = a * (s * b) = (a * s) * b = e * b = b.$$

So $x = s * b$ is a solution of the equation $a * x = b$.

It remains to show that $s * b$ is the only solution of $a * x = b$. Suppose that x_1 and x_2 are solutions of $a * x = b$. Then $a * x_1 = b$ and $a * x_2 = b$. Thus, $a * x_1 = a * x_2$. Applying the Left Cancellation Law, we have $x_1 = x_2$. □

Fundamental Properties of Groups

The preceding theorem provides some interesting information for us. Suppose that we have a group table for a group G and we are looking at the row corresponding to the element a. Then this row contains the elements $a * g$ for all $g \in G$. Let $b \in G$. There exists $x \in G$ such that $a * x = b$. That is, the element b must appear in the row corresponding to a.



On the other hand, the element b cannot appear twice in this row since the equation $a * x = b$ has a unique solution. Hence, we can conclude that every element of G appears exactly once in every row in the group table of G. By considering the equation $x * a = b$, we can likewise conclude that every element of G appears exactly once in every column in the group table of G.

Fundamental Properties of Groups

As with composition in a symmetric group, it is customary in a group G to refer to the binary operation $*$ as "multiplication" and to indicate the "product" of elements a and b in G by ab rather than $a * b$ to simplify the notation. We thus write $a * a = aa = a^2$. The lone exception to this practice is when we have a group whose operation is addition, in which case we continue to use $+$ as the operation. It is also common practice never to use $+$ as an operation when the group is nonabelian.

Fundamental Properties of Groups

Theorem

Let G be a group. Then

(a) G has a unique identity and

(b) each element in G has a unique inverse.

Proof. Assume that e and f are two identities in G. Since e is an identity, $ef = f$; and since f is an identity, $ef = e$. Thus, $e = ef = f$. This verifies (a).

Next let $g \in G$ and suppose that s and t are both inverses of g. So, $gs = sg = e$ and $gt = tg = e$. Since $gs = gt$, it follows by the Left Cancellation Law that $s = t$. This verifies (b). □

Fundamental Properties of Groups

It is customary to denote the (unique) inverse of an element a in a group by a^{-1}. If the operation in a group under consideration is addition, then we follow the standard practice of denoting the identity by 0 and the inverse of a by $-a$. We now present two theorems involving inverses in a group.

Theorem

Let G be a group. If $a \in G$, then

$$\left(a^{-1}\right)^{-1} = a.$$

Proof. Since $aa^{-1} = a^{-1}a = e$, the element a is the inverse of a^{-1}, that is, $\left(a^{-1}\right)^{-1} = a$. □

Theorem

Let G be a group. If $a, b \in G$, then

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

Proof. To show that $b^{-1}a^{-1}$ is the inverse of ab, it suffices to show that

$$(ab)\left(b^{-1}a^{-1}\right) = e \text{ and } \left(b^{-1}a^{-1}\right)(ab) = e.$$

We verify the first of these as the proof of the second equality is similar. Observe that

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \\ &= (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e.\end{aligned}$$

□

Subgroups

There have been occasions when we were considering a group $(G, *)$ and a subset H of G such that H is a group under the same operation $*$, that is, $(H, *)$ is also a group.

Definition

If $(G, *)$ is a group and H is a subset of G such that $(H, *)$ is a group, then $(H, *)$ is called a **subgroup** of G.

For example, $(\mathbf{Z}, +)$ is a subgroup of $(\mathbf{Q}, +)$, which, in turn, is a subgroup of $(\mathbf{R}, +)$.

Theorem (The Subgroup Test)

A nonempty subset H of a group G is a subgroup of G if and only if (1) $ab \in H$ for all $a, b \in H$ and (2) $a^{-1} \in H$ for all $a \in H$.

Proof. We first show that if H is a subgroup of G, then properties (1) and (2) are satisfied.

Since H is closed under multiplication, property (1) is certainly satisfied.

We now show that the identity e of G is also the identity of H. Let f be the identity of H. Thus, $f \cdot f = f$. Since e is the identity of G, it follows that $f \cdot e = f$. Therefore, $f \cdot f = f \cdot e$. By the Left Cancellation Law, $f = e$. Hence, as claimed, the identity e of G is also the identity of H.

Proof (continued)

Next, let $a \in H$. Since $a \in G$, it follows that the inverse a^{-1} of a belongs to G and so $aa^{-1} = e$. It remains to show that $a^{-1} \in H$. Since H is a subgroup of G, a has an inverse a' in H. Thus, $aa' = e$ in H and $aa' = e$ in G as well. Therefore, $aa' = aa^{-1}$. By the Left Cancellation Law again, $a' = a^{-1}$ and so property (2)

$$a^{-1} \in H \text{ for all } a \in H$$

is satisfied.

Proof (continued)

Next, we verify the converse, namely if H is a nonempty subset of G satisfying properties (1) and (2), then H is a subgroup of G.

Let $a, b, c \in H$. Since $H \subseteq G$, it follows that $a, b, c \in G$. Since G is a group, $a(bc) = (ab)c$ by property G1. Thus, multiplication is associative in H as well. From property (1), it follows that H is closed under multiplication and from property (2), every element of H has an inverse. It remains only to show that H contains an identity. Since $H \neq \emptyset$, there exists an element $a \in H$. By (2), $a^{-1} \in H$; and by (1), $aa^{-1} = e \in H$. Since H contains the identity e of G, it follows that $xe = ex = x$ for all $x \in H$ and so e is the identity of H as well. □

Example 4

Result Let $H = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} : a, b, c \in \mathbf{R} \right\}$. Then $(H, +)$ is a group.

Proof. We show in fact that $(H, +)$ is a subgroup of $(M_2(\mathbf{R}), +)$. Certainly, H is a nonempty subset of $M_2(\mathbf{R})$ since the zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ belongs to H. Let $A, B \in H$. Then

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} b_1 & b_2 \\ b_3 & 0 \end{bmatrix},$$

where $a_i, b_i \in \mathbf{R}$ $(1 \leq i \leq 3)$.

Example 4 (continued)

Then

$$A + B = \begin{bmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & 0 \end{bmatrix} \in H$$

and the inverse of A is

$$-A = \begin{bmatrix} -a_1 & -a_2 \\ -a_3 & 0 \end{bmatrix} \in H.$$

Consequently, by the Subgroup Test, H is a subgroup of $M_2(\mathbf{R})$ and so $(H, +)$ is a group. □

Subgroups

If G is an abelian group, then we know that every two elements of G commute. But even if G is nonabelian, we know that its identity commutes with every element of G. However, there may very well be other elements of G that commute with all elements of G.

Definition

The set of all elements in a group G that commute with every element in G is called the **center** of G and, in fact, is always a subgroup of G.

This subgroup is often denoted by $Z(G)$. Since $Z(G) = G$ if and only if G is abelian, the center is most interesting when G is nonabelian.

Example 5

Result For a group G, the center

$$Z(G) = \{a \in G \ : \ ga = ag \text{ for all } g \in G\}$$

is a subgroup of G.

Proof. Since $eg = ge$ for all $g \in G$, it follows that $e \in Z(G)$ and so $Z(G)$ is nonempty. First, we show that $Z(G)$ is closed under multiplication. Let $a, b \in Z(G)$. Thus, $ag = ga$ and $bg = gb$ for all $g \in G$. We show that $ab \in Z(G)$. Since

$$(ab)\,g = a\,(bg) = a\,(gb) = (ag)b = (ga)b = g\,(ab)\,,$$

$ab \in Z(G)$. Hence, $Z(G)$ is closed under multiplication.

Example 5 (continued)

Next we show that every element of $Z(G)$ has an inverse in $Z(G)$. Let $a \in Z(G)$ and $g \in G$. We show that $a^{-1} \in Z(G)$, that is, a^{-1} and g commute. Since a commutes with all elements of G, it follows that a and g^{-1} commute and so $ag^{-1} = g^{-1}a$. Since every element of G has a unique inverse,

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

Then

$$\left(ag^{-1}\right)^{-1} = \left(g^{-1}\right)^{-1} a^{-1} = ga^{-1}$$

and

$$\left(g^{-1}a\right)^{-1} = a^{-1}\left(g^{-1}\right)^{-1} = a^{-1}g.$$

Therefore, $a^{-1}g = ga^{-1}$. □

Subgroups

Definiton

For $A = \{1, 2, \cdots, n\}$, $n \geq 2$ and $k \in A$, let G_k consist of those permutations α in the symmetric group $(S_n, \circ)$ such that $\alpha(k) = k$ (that is, G_k consists of all those permutations of A that "stabilize" or fix k). The set G_k is called the **stabilizer** of k in S_n.

Example 6

Result For integers k and n with $1 \leq k \leq n$ and $n \geq 2$, the stabilizer G_k of k in S_n is a subgroup of S_n.

Proof. We use the Subgroup Test. Surely, the identity α_0 in S_n belongs to G_k, so $G_k \neq \emptyset$. Let $\alpha, \beta \in G_k$. Thus,

$$\alpha(k) = \beta(k) = k.$$

Hence,

$$(\alpha \circ \beta)(k) = \alpha(\beta(k)) = \alpha(k) = k$$

and so $\alpha \circ \beta \in G_k$.

Example 6 (continued)

Consider the inverse α^{-1} of α. Thus, $\alpha^{-1} \circ \alpha = \alpha_0$. Therefore,

$$(\alpha^{-1} \circ \alpha)(k) = \alpha_0(k) = k.$$

Hence,

$$(\alpha^{-1} \circ \alpha)(k) = \alpha^{-1}(\alpha(k)) = \alpha^{-1}(k) = \alpha_0(k) = k.$$

Thus, $\alpha^{-1} \in G_k$. By the Subgroup Test, G_k is a subgroup of S_n. □

Theorem

Let H be a subgroup of a group $(G, \cdot)$. The relation R defined on G by $a \ R \ b$ if $a = bh$ for some $h \in H$ is an equivalence relation.

Proof. First, we show that R is reflexive. Let $a \in G$. Since $a = ae$ (where e is the identity of G and therefore of H), $a \ R \ a$ and so R is reflexive. Next, we show that R is symmetric. Assume that $a \ R \ b$, where $a, b \in G$. Then $a = bh$ for some $h \in H$. Since H is a group, $h^{-1} \in H$ and so

$$ah^{-1} = (bh)h^{-1} = b(hh^{-1}) = be = b,$$

or $b = ah^{-1}$. Therefore, $b \ R \ a$ and R is symmetric.

Proof (continued)

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in G$. Then $a = bh_1$ and $b = ch_2$ for elements h_1 and h_2 in H. Therefore,

$$a = bh_1 = (ch_2)h_1 = c(h_2h_1).$$

Since $h_2, h_1 \in H$, it follows that $h_2h_1 \in H$ as well. Thus, $a\ R\ c$ and so R is transitive. □

Definition

For each element $g \in G$, the equivalence class $[g]$ is defined by

$$\begin{aligned}[g] &= \{x \in G : \ x \ R \ g\} \\ &= \{x \in G : \ x = gh \text{ for some } h \in H\} \\ &= \{gh : \ h \in H\}.\end{aligned}$$

The set $\{gh : \ h \in H\}$ is often denoted by gH and is called a **left coset** of H in G, that is, $[g] = gH$.

We saw in Chapter 9 that for an equivalence relation defined on a set S, the distinct equivalence classes form a partition of S. Consequently, this equivalence relation results in a partition of G into the distinct left cosets of H in G.

Subgroups

An important characteristic of a left coset gH of H in G is that gH and H have the same number of elements, that is, $|gH| = |H|$. In order to see this, we show for an element $g \in G$ that there is a bijection from H to gH. Let $\phi : H \to gH$ be defined by $\phi(h) = gh$. First, we show that ϕ is one-to-one. Assume that $\phi(h_1) = \phi(h_2)$. Then $gh_1 = gh_2$. By the Left Cancellation Law, $h_1 = h_2$. Therefore, ϕ is one-to-one. Next, we show that ϕ is onto. Let $gh \in gH$. Since $\phi(h) = gh$, it follows that ϕ is onto and so ϕ is a bijection and $|gH| = |H|$. Therefore, every two left cosets of H in G have the same number of elements.

Lagrange's Theorem

If H is a subgroup of order m in a (finite) group G of order n, then $m \mid n$.

Proof. We have already seen that the distinct left cosets of H in G form a partition of G and that every two left cosets have the same number of elements. Suppose that there are k left cosets of G. Then $n = mk$ and so $m \mid n$. □

Isomorphic Groups

Definition

Two groups $(G, *)$ and $(H, \circ)$ are **isomorphic** if there exists a bijective function $\phi : G \to H$ satisfying the property

$$\phi(a * b) = \phi(a) \circ \phi(b)$$

for all $a, b \in G$. Any such function ϕ that satisfies the property above is said to be **operation-preserving**. Thus, for $(G, *)$ and $(H, \circ)$ to be isomorphic, there must be a bijective, operation-preserving function $\phi : G \to H$. If ϕ has these properties, then ϕ is called an **isomorphism**. If $\phi : G \to H$ is an isomorphism, then ϕ is also a bijective function. Thus, ϕ has an inverse function $\phi^{-1} : H \to G$, which is also an isomorphism.

Isomorphic Groups

Theorem

Let $(G, *)$ and $(H, \circ)$ be isomorphic groups, where the identity of G is e and the identity of H is f. If $\phi : G \to H$ is an isomorphism, then

(a) $\phi(e) = f$ and

(b) $\phi\left(g^{-1}\right) = (\phi(g))^{-1}$ for all $g \in G$.

Proof. First, we prove (a). Let $h \in H$. Since ϕ is onto, there exists $g \in G$ such that $\phi(g) = h$. Since $e * g = g * e = g$ and ϕ is operation-preserving, it follows that

$$\phi(e) \circ \phi(g) = \phi(e * g) = \phi(g) = \phi(g * e) = \phi(g) \circ \phi(e)$$

and so

$$\phi(e) \circ h = h \circ \phi(e) = h.$$

This implies that $\phi(e)$ is the identity of H and so $\phi(e) = f$.

Proof (continued)

Next, we prove (b). Let $g \in G$. Since $g * g^{-1} = g^{-1} * g = e$, it follows that

$$\phi\left(g * g^{-1}\right) = \phi\left(g^{-1} * g\right) = \phi(e)$$

and so

$$\phi(g) \circ \phi\left(g^{-1}\right) = \phi\left(g^{-1}\right) \circ \phi(g) = \phi(e) = f.$$

This says that $\phi\left(g^{-1}\right)$ is the inverse of $\phi(g)$, that is, $\phi\left(g^{-1}\right) = (\phi(g))^{-1}$. □

Example 7

Result The groups $(\mathbf{Z}, +)$ and $(\mathbf{Q}, +)$ are not isomorphic.

Proof. Assume, to the contrary, that $(\mathbf{Z}, +)$ and $(\mathbf{Q}, +)$ are isomorphic. Then there exists an isomorphism $\phi : \mathbf{Z} \to \mathbf{Q}$. Let $\phi(1) = a \in \mathbf{Q}$. Since $\phi(0) = 0$, it follows that $a \neq 0$. Thus, $a/2 \in \mathbf{Q}$ and $a/2 \neq 0$. Since ϕ is onto, there exists an integer $n \neq 0$ such that $\phi(n) = a/2$. Then

$$\phi(2n) = \phi(n + n) = \phi(n) + \phi(n) = \frac{a}{2} + \frac{a}{2} = a.$$

Since ϕ is one-to-one, $2n = 1$. However then, $n = 1/2 \notin \mathbf{Z}$, which is a contradiction. □

Isomorphic Groups

Example 8

Result The groups $(2\mathbf{Z}, +)$ and $(\mathbf{Z}, +)$ are isomorphic.

Proof. Define the function $\phi : \mathbf{Z} \to 2\mathbf{Z}$ by $\phi(n) = 2n$ for each $n \in \mathbf{Z}$. First, we show that f is one-to-one. Assume that $\phi(a) = \phi(b)$. Then $2a = 2b$. Dividing by 2, we obtain $a = b$ and so ϕ is one-to-one. Now, we show that ϕ is onto. Let $n \in 2\mathbf{Z}$. Since n is even, $n = 2k$ for some integer k. Then $\phi(k) = 2k = n$. This shows that ϕ is onto. Finally, we show that ϕ is operation-preserving. Let $a, b \in \mathbf{Z}$. Then

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b).$$ □

Isomorphic Groups

It should be obvious that every group G is isomorphic to itself. In fact, the identity function $i_G : G \to G$ defined by $i_G(g) = g$ for all $g \in G$ is an isomorphism. However, other permutations of G can be isomorphisms.

Example 9

Result Let G be a group and let $g \in G$. The function $\phi : G \to G$ defined by $\phi(a) = gag^{-1}$ for all $a \in G$ is an isomorphism.

Proof. First, we show that f is one-to-one. Assume that $\phi(a) = \phi(b)$. Then

$$gag^{-1} = gbg^{-1}.$$

Canceling g on the left and g^{-1} on the right, we obtain $a = b$. Next, we show that ϕ is onto. Let $c \in G$. Then

$$\phi\left(g^{-1}cg\right) = g\left(g^{-1}cg\right)g^{-1} = \left(gg^{-1}\right)c\left(g^{-1}g\right) = ece = c.$$

Finally, we show that ϕ is operation-preserving. Let $a, b \in G$. Then

$$\phi(ab) = g(ab)g^{-1} = \left(gag^{-1}\right)\left(gbg^{-1}\right) = \phi(a)\phi(b). \qquad \square$$