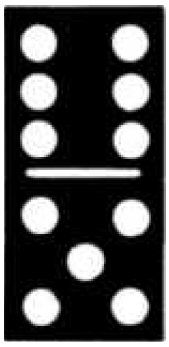
chapter 11



ALGEBRAIC SYSTEMS

GOALS

The primary goal of this chapter is to make the reader aware of what an algebraic system is and how algebraic systems can be studied at different levels of abstraction. After describing the concrete, axiomatic, and universal levels, we will introduce one of the most important algebraic systems at the axiomatic level, the group. In this chapter, group theory will be a vehicle for introducing the universal concepts of isomorphism, direct product, subsystem, and generating set. These concepts can be applied to all algebraic systems. The simplicity of group theory will help the reader obtain a good intuitive understanding of these concepts. In Chapter 15, we will introduce some additional concepts and applications of group theory. We will close the chapter with a discussion of how some computer hardware and software systems use the concept of an algebraic system.

11.1 Operations

One of the first mathematical skills that we all learn is how to add a pair of positive integers. A young child soon recognizes that something is wrong if a sum has two values, particularly if his or her sum is different from the teacher's. In addition, it is unlikely that a child would consider assigning a non-positive value to the sum of two positive integers. In other words, at an early age we probably know that the sum of two positive integers is unique and belongs to the set of positive integers. This is what characterizes all binary operations on a set.

Definition: Binary Operation. *Let S be a nonempty set. A binary operation on S is a rule that assigns to each ordered pair of elements of S a unique element of S. In other words, a binary operation is a function from $S \times S$ into S.*

Example 11.1.1. Union and intersection are both binary operations on the power set of any universe. Addition and multiplication are binary operators on the natural numbers. Addition and multiplication are binary operations on the set of 2 by 2 real matrices, $M_{2\times 2}(\mathbb{R})$. Division is a binary operation on some sets of numbers, such as the positive reals. But on the integers ($1/2 \notin \mathbb{Z}$) and even on the real numbers ($1/0$ is not defined), division is not a binary operation.

Notes:

(a) We stress that the image of each ordered pair must be in *S*. This requirement disqualifies subtraction on the natural numbers from consideration as a binary operation, since $1 - 2$ is not a natural number. Subtraction *is* a binary operation on the integers.

(b) On Notation. Despite the fact that a binary operation is a function, symbols, not letters, are used to name them. The most commonly used symbol for a binary operation is an asterisk, *. We will also use a diamond, $\diamond$, when a second symbol is needed.

(c) If * is a binary operation on S and $a, b \in S$, there are three common ways of denoting the image of the pair (a, b). They are:

$*\,a\,b$	$a * b$	$a\,b\,*$
Prefix Form	Infix Form	Postfix FOrm

We are all familiar with infix form. For example, 2 + 3 is how everyone is taught to write the sum of 2 and 3. But notice how 2 + 3 was just described in the previous sentence! The word *sum* preceded 2 and 3. Orally, prefix form is quite natural to us. The prefix and postfix forms are superior to infix form in some respects. In Chapter 10, we saw that algebraic expressions with more than one operation didn't need parentheses if they were in prefix or postfix form. However, due to our familiarity with infix form, we will use it throughout most of the remainder of this book.

Some operations, such as negation of numbers and complementation of sets, are not binary, but unary operators.

Definition: Unary Operation. *Let S be a nonempty set. A unary operator on S is a rule that assigns to each element of S a unique element of S. In other words, a unary operator is a function from S into S.*

COMMON PROPERTIES OF OPERATIONS

Whenever an operation on a set is encountered, there are several properties that should immediately come to mind. To effectively make use of an operation, you should know which of these properties it has. By now, you should be familiar with most of these properties. We will list the most common ones here to refresh your memory and define them for the first time in a general setting. Let S be any set and * a binary operation on S.

Properties that apply to a single binary operation:

*Let * be a binary operation on a set S*

** is **commutative** if $a * b = b * a$ for all a, b ∈ S.*

** is **associative** if $(a * b) * c = a * (b * c)$ for all a, b, c ∈ S.*

** **has an identity** if there exists an element, e, in S such that $a * e = e * a = a$ for all a ∈ S.*

** has the **inverse property** if for each a ∈ S, there exists b ∈ S such that $a * b = b * a = e$.*

We call b an inverse of a.

** is **idempotent** if a * a = a for all a ∈ S. Properties that apply to two binary operations:*

Let ⋄ be a second binary operation on S.

*⋄ is left distributive over * if $a \diamond (b * c) = (a \diamond b) * (a \diamond c)$ for all a, b, c ∈ S.*

*⋄ is right distributive over * if $(b * c) \diamond a = (b \diamond a) * (c \diamond a)$ for all a, b, c ∈ S.*

*⋄ is distributive over * if ⋄ is both left and right distributive over *.*

Let − be a unary operation.

A unary operation — on S has the involution property if $-(-a) = a$ for all a ∈ S.

Finally, a property of sets, as they relate to operations.

*If T is a subset of S, we say that T is closed under * if a, b ∈ T implies that $a * b \in T$. In other words, by operating on elements of T with *, you can't obtain new elements that are outside of T.*

Example 11.1.2.

(a) The odd integers are closed under multiplication, but not under addition.

(b) Let p be a proposition over U and let A be the set of propositions over U that imply p. That is; $q \in A$ if $q \Rightarrow p$. Then A is closed under both conjunction and disjunction.

(c) The set positive integers that are multiples of 5 is closed under both addition and multiplication.

Note: It is important to realize that the properties listed above depend on both the set and the operation(s).

OPERATION TABLES

If the set on which an operation is defined is small, a table is often a good way of describing the operation. For example, we might want to define $\oplus$ on $\{0, 1, 2\}$ by

$$a \oplus b = \begin{cases} a + b & \text{if } a + b < 3 \\ a + b - 3 & \text{if } a + b \geq 3 \end{cases}$$

The table for $\oplus$ is

"

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The top row and left column are the column and row headings, respectively. To determine $a \oplus b$, find the entry in Row a and Column b. The following operation table serves to define * on $\{i, j, k\}$.

"

*	i	j	k
i	i	i	i
j	j	j	j
k	k	k	k

Note that; $j*k = j$, yet $k * j = k$. Thus, * is not commutative. Commutivity is easy to identify in a table: the table must be symmetric with respect to the diagonal going from the top left to lower right.

EXERCISES FOR SECTION 11.1

A Exercises

1. Determine the properties that the following operations have on the positive integers.

   (a) addition

   (b) multiplication

   (c) M defined by $a\, M\, b =$ larger of a and b

   (d) m defined by $a\, m\, b =$ smaller of a and b

   (e) @ defined by $a \text{ @ } b = a \text{\^{}} b$

2. Which pairs of operations in Exercise 1 are distributive over one another?

3. Let * be an operation on a set S and $A,\ B \subseteq S$. Prove that if A and B are both closed under *, then $A \cap B$ is also closed under *, but $A \cup B$ need not be.

4. How can you pick out the identity of an operation from its table?

5. Define a * b by $|\ a - b\ |$, the absolute value of a - b. Which properties does * have on the set of natural numbers, $\mathbb{N}$?

11.2 Algebraic Systems

An algebraic system is a mathematical system consisting of a set called the domain and one or more operations on the domain. If V is the domain and $*_1, *_2, \ldots, *_n$ are the operations, $[V; *_1, *_2, \ldots, *_n]$ denotes the mathematical system. If the context is clear, this notation is abbreviated to V.

Example 11.2.1.

(a) Let B^* be the set of all finite strings of 0's and 1's including the null (or empty) string, λ. An algebraic system is obtained by adding the operation of concatenation. The concatenation of two strings is simply the linking of the two strings together in the order indicated. The concatenation of strings a with b is denoted $a <> b$. For example, "01101" <> "101" = "01101101" and λ <> "100" = "100". Note that concatenation is an associative operation and that λ is the identity for concatenation.

Note on Notation: There isn't a standard symbol for concatenation. We have chosen <> to be consist ant with the notation used in *Mathematica* for the **StringJoin** function, which does concatenation. Many programming languages use the plus sign for concatenation, but others use & or ||.

(b) Let M be any nonempty set and let * be any operation on M that is associative and has in identity in M. Our second example might seem strange, but we include it to illustrate a point. The algebraic system $[B^*; <>]$ is a special case of $[M; *]$. Most of us are much more comfortable with B^* than with M. No doubt, the reason is that the elements in B^* are more concrete. We know what they look like and exactly how they are combined. The description of M is so vague that we don't even know what the elements are, much less how they are combined. Why would anyone want to study M? The reason is related to this question: What theorems are of interest in an algebraic system? Answering this question is one of our main objectives in this chapter. Certain properties of algebraic systems are called algebraic properties, and any theorem that says something about the algebraic properties of a system would be of interest. The ability to identify what is algebraic and what isn't is one of the skills that you should learn from this chapter.

Now, back to the question of why we study M. Our answer is to illustrate the usefulness of M with a theorem about M.

Theorem 11.2.1. *If a, b are elements of M and* $a * b = b * a$, *then* $(a * b) * (a * b) = (a * a) * (b * b)$.

Proof:

$$\begin{aligned}
(a*b)*(a*b) &= a*(b*(a*b)) && \text{Why?}\\
&= a*((b*a)*b) && \text{Why?}\\
&= a*((a*b)*b) && \text{Why?}\\
&= a*(a*(b*b)) && \text{Why?}\\
&= (a*a)*(b*b) && \text{Why?}
\end{aligned}$$

The power of this theorem is that it can be applied to any algebraic system that M describes. Since B^* is one such system, we can apply Theorem 11.2.1 to any two strings that commute—for example, 01 and 0101. Although a special case of this theorem could have been proven for B^*, it would not have been any easier to prove, and it would not have given us any insight into other special cases of M .

Example 11.2.2. Consider the set of 2×2 real matrices, $M_{2\times2}(\mathbb{R})$, with the operation of matrix multiplication. In this context, Theorem 11.2.1 can be interpreted as saying that if $AB = BA$, then $(AB)^2 = A^2B^2$. One pair of matrices that this theorem applies to is $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 3 & -4 \\ -4 & 3 \end{pmatrix}$.

LEVELS OF ABSTRACTION

One of the fundamental tools in mathematics is abstraction. There are three levels of abstraction that we will identify for algebraic systems: concrete, axiomatic, and universal.

Concrete Level. Almost all of the mathematics that you have done in the past was at the concrete level. As a rule, if you can give examples of a few typical elements of the domain and describe how the operations act on them, you are describing a concrete algebraic system. Two examples of concrete systems are B^* and $M_{2\times2}(\mathbb{R})$. A few others are:

(a) The integers with addition. Of course, addition isn't the only standard operation that we could include. Technically, if we were to add multiplication, we would have a different system.

(b) The subsets of the natural numbers, with union, intersection, and complementation.

(c) The complex numbers with addition and multiplication.

Axiomatic Level. The next level of abstraction is the axiomatic level. At this level, the elements of the domain are not specified, but certain axioms are stated about the number of operations and their properties. The system that we called M is an axiomatic system. Some combinations of axioms are so common that a name is given to any algebraic system to which they apply. Any system with the properties of M is called a *monoid*. The study of M would be called monoid theory. The assumptions that we made about M, associativity and the existence of an identity, are called the monoid axioms. One of your few brushes with the axiomatic level may have been in your elementary algebra course. Many algebra texts identify the properties of the real numbers with addition and multiplication as the field axioms. As we will see in Chapter 16, "Rings and Fields," the real numbers share these axioms with other concrete systems, all of which are called fields.

Universal Level. The final level of abstraction is the universal level. There are certain concepts, called universal algebra concepts, that can be applied to the study of all algebraic systems. Although a purely universal approach to algebra would be much too abstract for our purposes, defining concepts at this level should make it easier to organize the various algebraic theories in your own mind. In this chapter, we will consider the concepts of isomorphism, subsystem, and direct product.

GROUPS

To illustrate the axiomatic level and the universal concepts, we will consider yet another kind of axiomatic system, the group. In Chapter 5 we noted that the simplest equation in matrix algebra that we are often called upon to solve is $A X = B$, where A and B are known square matrices and X is an unknown matrix. To solve this equation, we need the associative, identity, and inverse laws. We call the systems that have these properties groups.

Definition: Group. *A group consists of a nonempty set G and an operation $*$ on G satisfying the properties*

(a) $*$ is associative on G: $(a*b)*c = a*(b*c)$ *for all a, b, c $\in$ G.*

(b) There exists an identity element, e $\in$ G such that $a*e = e*a = a$ for all a $\in$ G.

(c) For all a $\in$ G, there exists an inverse, there exist b $\in$ G such that $a*b = b*a = e$.

A group is usually denoted by its set's name, G, or occasionally by $[G; *]$ to emphasize the operation. At the concrete level, most sets have a standard operation associated with them that will form a group. As we will see below, the integers with addition is a group. Therefore, in group theory $\mathbb{Z}$ always stands for $[\mathbb{Z}; +]$.

Generic Symbols. At the axiomatic and universal levels, there are often symbols that have a special meaning attached to them. In group theory, the letter e is used to denote the identity element of whatever group is being discussed. A little later, we will prove that the inverse of a group element, a, is unique and it is inverse is usually denoted a^{-1} and is read "a inverse." When a concrete group is discussed, these symbols are dropped in favor of concrete symbols. These concrete symbols may or may not be similar to the generic symbols. For example, the identity element of the group of integers is 0, and the inverse of n is denoted by $-n$, the additive inverse of n.

The asterisk could also be considered a generic symbol since it is used to denote operations on the axiomatic level.

Example 11.2.3.

(a) The integers with addition is a group. We know that addition is associative. Zero is the identity for addition: $0 + n = n + 0 = n$ for all integers n. The additive inverse of any integer is obtained by negating it. Thus the inverse of n is $-n$.

(b) The integers with multiplication is not a group. Although multiplication is associative and 1 is the identity for multiplication, not all integers have a multiplicative inverse in $\mathbb{Z}$. For example, the multiplicative inverse of 10 is $\frac{1}{10}$, but $\frac{1}{10}$ is not an integer.

(c) The power set of any set U with the operation of symmetric difference, $\oplus$, is a group. If A and B are sets, then $A \oplus B = (A \cup B) - (A \cap B)$. We will leave it to the reader to prove that $\oplus$ is associative over $\mathcal{P}(U)$. The identity of the group is the empty set: $A \oplus \emptyset = A$. Every set is its own inverse since $A \oplus A = \emptyset$. Note that $\mathcal{P}(U)$ is not a group with union or intersection.

Definition: Abelian Group. *A group is abelian if its operation is commutative.*

Most of the groups that we will discuss in this book will be abelian. The term abelian is used to honor the Norwegian mathematician N. Abel (1802-29), who helped develop group theory.

Norwegian Stamp honoring Abel

EXERCISES FOR SECTION 11.2

A Exercises

1. Discuss the analogy between the terms generic and concrete for algebraic systems and the terms generic and trade for prescription drugs.

2. Discuss the connection between groups and monoids. Is every monoid a group? Is every group a monoid?

3. Which of the following are groups?

   (a) B^* with concatenation (Example 11.2.1a).

   (b) $M_{2\times 3}(\mathbb{R})$ with matrix addition.

   (c) $M_{2\times 3}(\mathbb{R})$ with matrix multiplication.

   (d) The positive real numbers, $\mathbb{R}^+$, with multiplication.

   (e) The nonzero real numbers, $\mathbb{R}^*$, with multiplication.

   (f) $\{1, -1\}$ with multiplication.

   (g) The positive integers with the operation M defined by $a\, M\, b$ = larger of a and b.

4. Prove that, $\oplus$, defined by $A \oplus B = (A \cup B) - (A \cap B)$ is an associative operation on $\mathcal{P}(U)$.

5. The following problem supplies an example of a non-abelian group. A rook matrix is a matrix that has only 0's and 1's as entries such that each row has exactly one 1 and each column has exactly one 1. The term rook matrix is derived from the fact that each rook matrix represents the placement of n rooks on an $n\times n$ chessboard such that none of the rooks can attack one another. A rook in chess can move only vertically or horizontally, but not diagonally. Let R_n be the set of $n\times n$ rook matrices. There are six 3×3 rook matrices:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad R_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad R_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$F_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad F_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad F_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(a) List the 2×2 rook matrices. They form a group, R_2, under matrix multiplication. Write out the multiplication table. Is the group abelian?

(b) Write out the multiplication table for R_3 . This is another group. Is it abelian?

(c) How many 4×4 rook matrices are there? How many $n\times n$ rook matrices are there?

6. For each of the following sets, identify the standard operation that results in a group. What is the identity of each group?

   (a) The set of all 2×2 matrices with real entries and nonzero determinants.

   (b) The set of 2×3 matrices with rational entries.

B Exercises

7. Let $V = \{e, a, b, c\}$. Let $*$ be defined (partially) by $x * x = e$ for all $x \in V$. Write a complete table for $*$ so that $[V; *]$ is a group.

11.3 Some General Properties of Groups

In this section, we will present some of the most basic theorems of group theory. Keep in mind that each of these theorems tells us something about every group. We will illustrate this point at the close of the section.

Theorem 11.3.1. *The identity of a group is unique.*

One difficulty that students often encounter is how to get started in proving a theorem like this. The difficulty is certainly not in the theorem's complexity. Before actually starting the proof, we rephrase the theorem so that the implication it states is clear.

Theorem 11.3.1 *(Rephrased). If $G = [G; *]$ is a group and e is an identity of G, then no other element of G is an identity of G.*

Proof (Indirect): Suppose that $f \in G$, $f \neq e$, and f is an identity of G. We will show that $f = e$, a contradiction, which completes the proof:

$f = f * e$ Since e is an identity.

$= e.$ Since f is an identity. ■

Theorem 11.3.2. *The inverse of any element of a group is unique.*

The same problem is encountered here as in the previous theorem. We will leave it to the reader to rephrase this theorem. The proof is also left to the reader to write out in detail. Here is a hint: If b and c are both inverses of a, then you can prove that $b = c$. If you have difficulty with this proof, note that we have already proven it in a concrete setting in Chapter 5.

The significance of Theorem 11.3.2 is that we can refer to the inverse of an element without ambiguity. The notation for the inverse of a is usually a^{-1}. (note the exception below).

Example 11.3.1.

(a) In any group, e^{-1} is the inverse of the identity e, which always is e.

(b) $\left(a^{-1}\right)^{-1}$ is the inverse of a^{-1} , which is always equal to a (see Theorem 11.3.3 below).

(c) $(x * y * z)^{-1}$ is the inverse of $x * y * z$.

(d) In a concrete group with an operation that is based on addition, the inverse of a is usually written $-a$. For example, the inverse of $k - 3$ in the group $[\mathbb{Z}; +]$ is written $-(k - 3) = 3 - k$. In the group of 2×2 matrices over the real numbers, the inverse of $\begin{pmatrix} 4 & 1 \\ 1 & -3 \end{pmatrix}$ is written $-\begin{pmatrix} 4 & 1 \\ 1 & -3 \end{pmatrix}$, which equals $\begin{pmatrix} -4 & -1 \\ -1 & 3 \end{pmatrix}$.

Theorem 11.3.3. *If a is an element of group G, then $\left(a^{-1}\right)^{-1} = a$.*

Theorem 11.3.3 (Rephrased). *If a has inverse b and b has inverse c, then a = c.*

Proof:

$a = a * (b * c)$ because c is the inverse of b

$= (a * b) * c$ why?

$= e * c$ why?

$= c.$ by the identity property of e. ■

Theorem 11.3.4. *If a and b are elements of group G, then $(a * b)^{-1} = b^{-1} * a^{-1}$*

Note: This theorem simply gives you a formula for the inverse of a * b. This formula should be familiar. In Chapter 5 we saw that if A and B are invertible matrices, then (AB)~ I = B~ I A~ I .

Proof: Let $x = b^{-1} * a^{-1}$. We will prove that x inverts $a * b$. Since we know that the inverse is unique, we will have prove the theorem.

$$\begin{aligned}(a * b) * x &= (a * b) * (b^{-1} * a^{-1}) \\ &= a * (b * (b^{-1} * a^{-1})) \\ &= a * ((b * b^{-1}) * a^{-1}) \\ &= a * (e * a^{-1}) \\ &= a * a^{-1} \\ &= e\end{aligned}$$

Similarly, $x * (a * b) = e$; therefore, $(a * b)^{-1} = x = b^{-1} * a^{-1}$ ■

Theorem 11.3.5. Cancellation Laws. *If a, b, and c are elements of group G, both a * b = a * c and b * a = c * a imply that b = c.*

Proof: Since $a * b = a * c$, we can operate on both $a * b$ and $a * c$ on the left with a^{-1} :

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

Applying the associative property to both sides we get

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

or

$$e * b = e * c$$

and finally

$$b = c.$$

This completes the proof of the left cancellation law. The right law can be proven in exactly the same way. ■

Theorem 11.3.6. Linear Equations in a Group. *If G is a group and a, b, $\in$ G, the equation $a * x = b$ has a unique solution, $x = a^{-1} * b$. In addition, the equation $x * a = b$ has a unique solution, $x = b * a^{-1}$.*

Proof: (for $a * x = b$):

$$\begin{aligned}a * x &= b \\ &= e * b \\ &= (a * a^{-1}) * b \\ &= a * (a^{-1} * b)\end{aligned}$$

By the cancellation law, we can conclude that $x = a^{-1} * b$.

If c and d are two solutions of the equation $a * x = b$, then $a * c = b = a * d$ and, by the cancellation law, $c = d$. This verifies that $a^{-1} * b$ is the only solution of $a * x = b$. ■

Note: Our proof of Theorem 11.3.6 was analogous to solving $4x = 9$ in the following way:

$$4x = 9 = \left(4 \cdot \frac{1}{4}\right) 9 = 4\left(\frac{1}{4} 9\right)$$

Therefore, by cancelling 4,

$$x = \frac{1}{4} \cdot 9 = \frac{9}{4}.$$

Exponentiation in a Group

If a is an element of a group G, then we establish the notation that

$a * a = a^2$
$a * a * a = a^3$
etc.

In addition, we allow negative exponent and define, for example, $a^{-2} = (a^2)^{-1}$

Although this should be clear, proving exponentiation properties requires a more precise recursive definition:

Definition: Exponentiation in a Group. *For $n \geq 0$, define a^n recursively by $a^0 = e$ and if $n > 0$, $a^n = a^{n-1} * a$. Also, if $n > 1$, $a^{-n} = (a^n)^{-1}$.*

Example 11.3.2.

(a) In the group of positive real numbers with multiplication,

$$5^3 = 5^2 \cdot 5 = \left(5^1 \cdot 5\right) \cdot 5 = \left(\left(5^0 \cdot 5\right) \cdot 5\right) \cdot 5 = ((1 \cdot 5) \cdot 5) \cdot 5 = 5 \cdot 5 \cdot 5 = 125.$$

and

$$5^{-3} = (125)^{-1} = \frac{1}{125}$$

(b) In a group with addition, we use a different form of notation, reflecting the fact that in addition repeated terms are multiples, not powers. For example, in $[\mathbb{Z}; +]$, a + a is written as 2 a, $a + a + a$ is written as 3 a, etc. The inverse of a multiple of a such as $-(a + a + a + a + a) = -(5\,a)$ is written as $(-5)\,a$.

Based on the definitions for exponentiation above, there are several properties that can be proven. They are all identical to the exponentiation properties from elementary algebra.

Theorem 11.3.7. Properties of Exponentiation*. If a is an element of a group G, and n and m are integers,*

(a) $a^{-n} = \left(a^{-1}\right)^n$ *and hence* $\left(a^n\right)^{-1} = \left(a^{-1}\right)^n$

(b) $a^{n+m} = a^n * a^m$

(c) $\left(a^n\right)^m = a^{n\,m}$

We will leave the proofs of these properties to the interested reader. All three parts can be done by induction. For example the proof of (b) would start by defining the proposition $p(m)$, $m \geq 0$, to be $a^{n+m} = a^n * a^m$ for all n . The basis is $p(0)$: $a^{n+0} = a^n * a^0$.

Our final theorem is the only one that contains a hypothesis about the group in question. The theorem only applies to finite groups.

Theorem 11.3.8. *If G is a finite group,* $|G| = n$*, and a is an element of G, then there exists a positive integer m such that* $a^m = e$ *and* $m \leq n$.

Proof: Consider the list a, a^2, …, a^{n+1} . Since there are $n + 1$ elements of G in this list, there must be some duplication. Suppose that $a^p = a^q$, with $p < q$. Let $m = q - p$. Then

$$a^m = a^{q-p} = a^q * a^{-p} = a^q * \left(a^p\right)^{-1} = a^q * \left(a^q\right)^{-1} = e$$

Furthermore, since $1 \leq p < q \leq n + 1$, $m = q - p \leq n$. ■

Consider the concrete group $[\mathbb{Z}; +]$. All of the theorems that we have stated in this section except for the last one say something about $\mathbb{Z}$. Among the facts that we conclude from the theorems about $\mathbb{Z}$ are:

Since the inverse of 5 is -5, the inverse of -5 is 5.

The inverse of $-6 + 71$ is $-(71) + -(-6) = -71 + 6$.

The solution of $12 + x = 22$ is $x = -12 + 22$.

$-4\,(6) + 2\,(6) = (-4 + 2)\,(6) = -2\,(6) = -(2)\,(6))$.

$7\,(4\,(3)) = (7 \cdot 4)\,(3) = 28\,(3)$ (twenty-eight 3s).

EXERCISES FOR SECTION 11.3

A Exercises

1. Let $[G; *]$ be a group and a be an element of G. Define $f : G \to G$ by $f(x) = a * x$.

   (a) Prove that f is a bijection.

   (b) On the basis of part a, describe a set of bijections on the set of integers.

2. Rephrase Theorem 11.3.2 and write out a clear proof.

3. Prove by induction on n that if $a_1, a_2, \ldots, a_n$ are elements of a group G, $n \geq 2$, then

   $$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n{}^{-1} * \cdots * a_2{}^{-1} * a_1{}^{-1}.$$

   Interpret this result in terms of $[\mathbb{Z}; +]$ and $[\mathbb{R}; *]$.

4. True or false? If a, b, c are elements of a group G, and $a * b = c * a$, then $b = c$. Explain your answer.

5. Prove Theorem 11.3.7.

6. Each of the following facts can be derived by identifying a certain group and then applying one of the theorems of this section to it. For each fact, list the group and the theorem that are used.

(a) $\left(\frac{1}{3}\right)5$ is the only solution of $3x = 5$.

(b) $-(-(-18)) = -18$.

(c) If A, B, C are 3×3 matrices over the real numbers, with $A + B = A + C$, then $B = C$.

(d) There is only one subset of the natural numbers for which $K \oplus A = A$ for every $A \subseteq N$.