PEARSON NEW INTERNATIONAL EDITION

A First Course in Abstract Algebra

John B. Fraleigh

Seventh Edition

ALWAYS LEARNING

PEARSON

SECTION 0 SETS AND RELATIONS

On Definitions, and the Notion of a Set

Many students do not realize the great importance of definitions to mathematics. This importance stems from the need for mathematicians to communicate with each other. If two people are trying to communicate about some subject, they must have the same understanding of its technical terms. However, there is an important structural weakness.

> It is impossible to define every concept.

Suppose, for example, we define the term *set* as "A **set** is a well-defined collection of objects." One naturally asks what is meant by a *collection.* We could define it as "A collection is an aggregate of things." What, then, is an *aggregate?* Now our language is finite, so after some time we will run out of new words to use and have to repeat some words already examined. The definition is then circular and obviously worthless. Mathematicians realize that there must be some undefined or primitive concept with which to start. At the moment, they have agreed that *set* shall be such a primitive concept. We shall not define *set,* but shall just hope that when such expressions as "the set of all real numbers" or "the set of all members of the United States Senate" are used, people's various ideas of what is meant are sufficiently similar to make communication feasible.

We summarize briefly some of the things we shall simply assume about sets.

1. A set S is made up of **elements,** and if a is one of these elements, we shall denote this fact by $a \in S$.
2. There is exactly one set with no elements. It is the **empty set** and is denoted by $\varnothing$.
3. We may describe a set either by giving a characterizing property of the elements, such as "the set of all members of the United States Senate," or by listing the elements. The standard way to describe a set by listing elements is to enclose the designations of the elements, separated by commas, in braces, for example, $\{1, 2, 15\}$. If a set is described by a characterizing property $P(x)$ of its elements x, the brace notation $\{x \mid P(x)\}$ is also often used, and is read "the set of all x such that the statement $P(x)$ about x is true." Thus

$$\begin{aligned}\{2, 4, 6, 8\} &= \{x \mid x \text{ is an even whole positive number} \leq 8\} \\ &= \{2x \mid x = 1, 2, 3, 4\}.\end{aligned}$$

   The notation $\{x \mid P(x)\}$ is often called "set-builder notation."
4. A set is **well defined,** meaning that if S is a set and a is some object, then either a is definitely in S, denoted by $a \in S$, or a is definitely not in S, denoted by $a \notin S$. Thus, we should never say, "Consider the set S of some positive numbers," for it is not definite whether $2 \in S$ or $2 \notin S$. On the other hand, we

From Part 0 of *A First Course in Abstract Algebra*, Seventh Edition. John B. Fraleigh.

can consider the set T of all prime positive integers. Every positive integer is definitely either prime or not prime. Thus $5 \in T$ and $14 \notin T$. It may be hard to actually determine whether an object is in a set. For example, as this book goes to press it is probably unknown whether $2^{(2^{65})} + 1$ is in T. However, $2^{(2^{65})} + 1$ is certainly either prime or not prime.

It is not feasible for this text to push the definition of everything we use all the way back to the concept of a set. For example, we will never define the number π in terms of a set.

Every definition is an *if and only if* type of statement.

With this understanding, definitions are often stated with the *only if* suppressed, but it is always to be understood as part of the definition. Thus we may define an isosceles triangle as follows: "A triangle is **isosceles** if it has two sides of equal length," when we really mean that a triangle is isosceles *if and only if* it has two sides of equal length.

In our text, we have to define many terms. We use specifically labeled and numbered definitions for the main algebraic concepts with which we are concerned. To avoid an overwhelming quantity of such labels and numberings, we define many terms within the body of the text and exercises using boldface type.

Boldface Convention

A term printed **in boldface** in a sentence is being defined by that sentence.

Do not feel that you have to memorize a definition word for word. The important thing is to *understand* the concept, so that you can define precisely the same concept in your own words. Thus the definition "An **isosceles** triangle is one having two equal sides" is perfectly correct. Of course, we had to delay stating our boldface convention until we had finished using boldface in the preceding discussion of sets, because we do not define a set!

In this section, we do define some familiar concepts as sets, both for illustration and for review of the concepts. First we give a few definitions and some notation.

0.1 Definition A set B is a **subset of a set** A, denoted by $B \subseteq A$ or $A \supseteq B$, if every element of B is in A. The notations $B \subset A$ or $A \supset B$ will be used for $B \subseteq A$ but $B \neq A$. ■

Note that according to this definition, for any set A, A itself and $\varnothing$ are both subsets of A.

0.2 Definition If A is any set, then A is the **improper subset of** A. Any other subset of A is a **proper subset of** A. ■

0.3 Example Let $S = \{1, 2, 3\}$. This set S has a total of eight subsets, namely $\emptyset$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, and $\{1, 2, 3\}$. ▲

0.4 Definition Let A and B be sets. The set $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ is the **Cartesian product** of A and B. ■

0.5 Example If $A = \{1, 2, 3\}$ and $B = \{3, 4\}$, then we have

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$ ▲

Throughout this text, much work will be done involving familiar sets of numbers. Let us take care of notation for these sets once and for all.

$\mathbb{Z}$ is the set of all integers (that is, whole numbers: positive, negative, and zero).

$\mathbb{Q}$ is the set of all rational numbers (that is, numbers that can be expressed as quotients m/n of integers, where $n \neq 0$).

$\mathbb{R}$ is the set of all real numbers.

$\mathbb{Z}^+$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ are the sets of positive members of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, respectively.

$\mathbb{C}$ is the set of all complex numbers.

$\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ are the sets of nonzero members of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, respectively.

0.6 Example The set $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane that we use in first-semester calculus to draw graphs of functions. ▲

Relations Between Sets

We introduce the notion of an element a of set A being *related* to an element b of set B, which we might denote by $a \mathscr{R} b$. The notation $a \mathscr{R} b$ exhibits the elements a and b in left-to-right order, just as the notation (a, b) for an element in $A \times B$. This leads us to the following definition of a relation $\mathscr{R}$ as a *set*.

0.7 Definition A **relation** between sets A and B is a subset $\mathscr{R}$ of $A \times B$. We read $(a, b) \in \mathscr{R}$ as "a is related to b" and write $a \mathscr{R} b$. ■

0.8 Example **(Equality Relation)** There is one familiar relation between a set and itself that we consider every set S mentioned in this text to possess: namely, the equality relation $=$ defined on a set S by

$$= \text{ is the subset } \{(x, x) \mid x \in S\} \text{ of } S \times S.$$

Thus for any $x \in S$, we have $x = x$, but if x and y are different elements of S, then $(x, y) \notin =$ and we write $x \neq y$. ▲

We will refer to any relation between a set S and itself, as in the preceding example, as a **relation on** S.

0.9 Example The graph of the function f where $f(x) = x^3$ for all $x \in \mathbb{R}$, is the subset $\{(x, x^3) \mid x \in \mathbb{R}\}$ of $\mathbb{R} \times \mathbb{R}$. Thus it is a relation on $\mathbb{R}$. The function is completely determined by its graph. ▲

The preceding example suggests that rather than define a "function" $y = f(x)$ to be a "rule" that assigns to each $x \in \mathbb{R}$ exactly one $y \in \mathbb{R}$, we can easily describe it as a certain type of subset of $\mathbb{R} \times \mathbb{R}$, that is, as a type of relation. We free ourselves from $\mathbb{R}$ and deal with any sets X and Y.

0.10 Definition A **function** ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ. Such a function is also called a **map** or **mapping** of X into Y. We write $\phi : X \to Y$ and express $(x, y) \in \phi$ by $\phi(x) = y$. The **domain** of ϕ is the set X and the set Y is the **codomain** of ϕ. The **range** of ϕ is $\phi[X] = \{\phi(x) \mid x \in X\}$. ■

0.11 Example We can view the addition of real numbers as a function $+ : (\mathbb{R} \times \mathbb{R}) \to \mathbb{R}$, that is, as a mapping of $\mathbb{R} \times \mathbb{R}$ into $\mathbb{R}$. For example, the action of $+$ on $(2, 3) \in \mathbb{R} \times \mathbb{R}$ is given in function notation by $+((2, 3)) = 5$. In set notation we write $((2, 3), 5) \in +$. Of course our familiar notation is $2 + 3 = 5$. ▲

Cardinality

The number of elements in a set X is the **cardinality** of X and is often denoted by $|X|$. For example, we have $|\{2, 5, 7\}| = 3$. It will be important for us to know whether two sets have the same cardinality. If both sets are finite there is no problem; we can simply count the elements in each set. But do $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ have the same cardinality? To convince ourselves that two sets X and Y have the same cardinality, we try to exhibit a pairing of each x in X with only one y in Y in such a way that each element of Y is also used only once in this pairing. For the sets $X = \{2, 5, 7\}$ and $Y = \{?, !, \#\}$, the pairing

$$2 \leftrightarrow ?, \quad 5 \leftrightarrow \#, \quad 7 \leftrightarrow !$$

shows they have the same cardinality. Notice that we could also exhibit this pairing as $\{(2, ?), (5, \#), (7, !)\}$ which, as a subset of $X \times Y$, is a *relation* between X and Y. The pairing

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & -4 & 4 & -5 & \cdots \end{array}$$

shows that the sets $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinality. Such a pairing, showing that sets X and Y have the same cardinality, is a special type of relation $\leftrightarrow$ between X and Y called a **one-to-one correspondence.** Since each element x of X appears precisely once in this relation, we can regard this one-to-one correspondence as a *function* with domain X. The range of the function is Y because each y in Y also appears in some pairing $x \leftrightarrow y$. We formalize this discussion in a definition.

0.12 Definition *A function $\phi : X \to Y$ is **one to one** if $\phi(x_1) = \phi(x_2)$ only when $x_1 = x_2$ (see Exercise 37). The function ϕ is **onto** Y if the range of ϕ is Y. ■

* We should mention another terminology, used by the disciples of N. Bourbaki, in case you encounter it elsewhere. In Bourbaki's terminology, a one-to-one map is an **injection,** an onto map is a **surjection,** and a map that is both one to one and onto is a **bijection.**

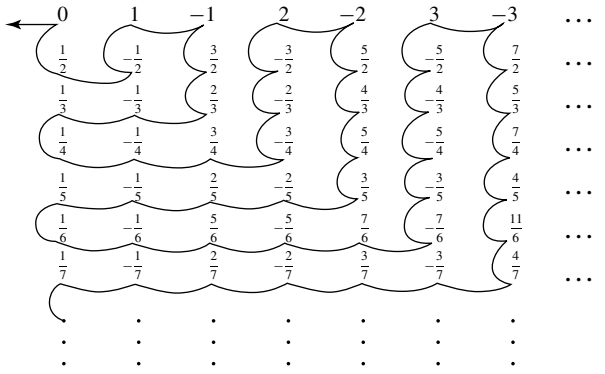
If a subset of $X \times Y$ is a *one-to-one* function ϕ mapping X *onto* Y, then each $x \in X$ appears as the first member of exactly one ordered pair in ϕ and also each $y \in Y$ appears as the second member of exactly one ordered pair in ϕ. Thus if we interchange the first and second members of all ordered pairs (x, y) in ϕ to obtain a set of ordered pairs (y, x), we get a subset of $Y \times X$, which gives a one-to-one function mapping Y onto X. This function is called the **inverse function** of ϕ, and is denoted by ϕ^{-1}. Summarizing, if ϕ maps X one to one onto Y and $\phi(x) = y$, then ϕ^{-1} maps Y one to one onto X, and $\phi^{-1}(y) = x$.

0.13 Definition Two sets X and Y have the **same cardinality** if there exists a one-to-one function mapping X onto Y, that is, if there exists a one-to-one correspondence between X and Y. ■

0.14 Example The function $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$ is not one to one because $f(2) = f(-2) = 4$ but $2 \neq -2$. Also, it is not onto $\mathbb{R}$ because the range is the proper subset of all nonnegative numbers in $\mathbb{R}$. However, $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$ is both one to one and onto $\mathbb{R}$. ▲

We showed that $\mathbb{Z}$ and $\mathbb{Z}^+$ have the same cardinality. We denote this cardinal number by $\aleph_0$, so that $|\mathbb{Z}| = |\mathbb{Z}^+| = \aleph_0$. It is fascinating that a proper subset of an infinite set may have the same number of elements as the whole set; an **infinite set** can be defined as a set having this property.

We naturally wonder whether all infinite sets have the same cardinality as the set $\mathbb{Z}$. A set has cardinality $\aleph_0$ if and only if *all* of its elements could be listed in an infinite row, so that we could "number them" using $\mathbb{Z}^+$. Figure 0.15 indicates that this is possible for the set $\mathbb{Q}$. The square array of fractions extends infinitely to the right and infinitely downward, and contains all members of $\mathbb{Q}$. We have shown a string winding its way through this array. Imagine the fractions to be glued to this string. Taking the beginning of the string and pulling to the left in the direction of the arrow, the string straightens out and all elements of $\mathbb{Q}$ appear on it in an infinite row as $0, \frac{1}{2}, -\frac{1}{2}, 1, -1, \frac{3}{2}, \cdots$. Thus $|\mathbb{Q}| = \aleph_0$ also.



0.15 Figure

If the set $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$ has cardinality $\aleph_0$, all its elements could be listed as unending decimals in a column extending infinitely downward, perhaps as

$$\begin{array}{l} 0.3659663426\cdots \\ 0.7103958453\cdots \\ 0.0358493553\cdots \\ 0.9968452214\cdots \\ \vdots \end{array}$$

We now argue that any such array must omit some number in S. Surely S contains a number r having as its nth digit after the decimal point a number different from 0, from 9, and from the nth digit of the nth number in this list. For example, r might start $.5637\cdots$. The 5 rather than 3 after the decimal point shows r cannot be the first number in S listed in the array shown. The 6 rather than 1 in the second digit shows r cannot be the second number listed, and so on. Because we could make this argument with *any list,* we see that S has too many elements to be paired with those in $\mathbb{Z}^+$. Exercise 15 indicates that $\mathbb{R}$ has the same number of elements as S. We just denote the cardinality of $\mathbb{R}$ by $|\mathbb{R}|$. Exercise 19 indicates that there are infinitely many different cardinal numbers even greater than $|\mathbb{R}|$.

Partitions and Equivalence Relations

Sets are **disjoint** if no two of them have any element in common. Later we will have occasion to break up a set having an algebraic structure (e.g., a notion of addition) into disjoint subsets that become elements in a related algebraic structure. We conclude this section with a study of such breakups, or *partitions* of sets.

0.16 Definition A **partition** of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. The subsets are the **cells** of the partition. ■

When discussing a partition of a set S, we denote by $\bar{x}$ the cell containing the element x of S.

0.17 Example Splitting $\mathbb{Z}^+$ into the subset of even positive integers (those divisible by 2) and the subset of odd positive integers (those leaving a remainder of 1 when divided by 2), we obtain a partition of $\mathbb{Z}^+$ into two cells. For example, we can write

$$\overline{14} = \{2, 4, 6, 8, 10, 12, 14, 16, 18, \cdots\}.$$

We could also partition $\mathbb{Z}^+$ into three cells, one consisting of the positive integers divisible by 3, another containing all positive integers leaving a remainder of 1 when divided by 3, and the last containing positive integers leaving a remainder of 2 when divided by 3.

Generalizing, for each positive integer n, we can partition $\mathbb{Z}^+$ into n cells according to whether the remainder is $0, 1, 2, \cdots, n-1$ when a positive integer is divided by n. These cells are the **residue classes modulo** n in $\mathbb{Z}^+$. Exercise 35 asks us to display these partitions for the cases $n = 2$, 3, and 5. ▲

Each partition of a set S yields a relation $\mathscr{R}$ on S in a natural way: namely, for $x, y \in S$, let $x \mathscr{R} y$ if and only if x and y are in the same cell of the partition. In set notation, we would write $x \mathscr{R} y$ as $(x, y) \in \mathscr{R}$ (see Definition 0.7). A bit of thought shows that this relation $\mathscr{R}$ on S satisfies the three properties of an *equivalence relation* in the following definition.

0.18 Definition An **equivalence relation** $\mathscr{R}$ on a set S is one that satisfies these three properties for all $x, y, z \in S$.

1. (Reflexive) $x \mathscr{R} x$.
2. (Symmetric) If $x \mathscr{R} y$, then $y \mathscr{R} x$.
3. (Transitive) If $x \mathscr{R} y$ and $y \mathscr{R} z$ then $x \mathscr{R} z$. ■

To illustrate why the relation $\mathscr{R}$ corresponding to a partition of S satisfies the symmetric condition in the definition, we need only observe that if y is in the same cell as x (that is, if $x \mathscr{R} y$), then x is in the same cell as y (that is, $y \mathscr{R} x$). We leave the similar observations to verify the reflexive and transitive properties to Exercise 28.

0.19 Example For any nonempty set S, the equality relation $=$ defined by the subset $\{(x, x) \mid x \in S\}$ of $S \times S$ is an equivalence relation. ▲

0.20 Example **(Congruence Modulo *n*)** Let $n \in \mathbb{Z}^+$. The equivalence relation on $\mathbb{Z}^+$ corresponding to the partition of $\mathbb{Z}^+$ into residue classes modulo n, discussed in Example 0.17, is **congruence modulo *n***. It is sometimes denoted by $\equiv_n$. Rather than write $a \equiv_n b$, we usually write $a \equiv b \pmod{n}$, read, "a is congruent to b modulo n." For example, we have $15 \equiv 27 \pmod{4}$ because both 15 and 27 have remainder 3 when divided by 4. ▲

0.21 Example Let a relation $\mathscr{R}$ on the set $\mathbb{Z}$ be defined by $n \mathscr{R} m$ if and only if $nm \geq 0$, and let us determine whether $\mathscr{R}$ is an equivalence relation.

Reflexive $a \mathscr{R} a$, because $a^2 \geq 0$ for all $a \in \mathbb{Z}$.

Symmetric If $a \mathscr{R} b$, then $ab \geq 0$, so $ba \geq 0$ and $b \mathscr{R} a$.

Transitive If $a \mathscr{R} b$ and $b \mathscr{R} c$, then $ab \geq 0$ and $bc \geq 0$. Thus $ab^2c = acb^2 \geq 0$. If we knew $b^2 > 0$, we could deduce $ac \geq 0$ whence $a \mathscr{R} c$. We have to examine the case $b = 0$ separately. A moment of thought shows that $-3 \mathscr{R} 0$ and $0 \mathscr{R} 5$, but we do *not* have $-3 \mathscr{R} 5$. Thus the relation $\mathscr{R}$ is not transitive, and hence is not an equivalence relation. ▲

We observed above that a partition yields a natural equivalence relation. We now show that an equivalence relation on a set yields a natural partition of the set. The theorem that follows states both results for reference.

0.22 Theorem **(Equivalence Relations and Partitions)** Let S be a nonempty set and let $\sim$ be an equivalence relation on S. Then $\sim$ yields a partition of S, where

$$\bar{a} = \{x \in S \mid x \sim a\}.$$

Also, each partition of S gives rise to an equivalence relation $\sim$ on S where $a \sim b$ if and only if a and b are in the same cell of the partition.

Proof We must show that the different cells $\bar{a} = \{x \in S \mid x \sim a\}$ for $a \in S$ do give a partition of S, so that every element of S is in some cell and so that if $a \in \bar{b}$, then $\bar{a} = \bar{b}$. Let $a \in S$. Then $a \in \bar{a}$ by the reflexive condition (1), so a is in *at least one* cell.

Suppose now that a were in a cell $\bar{b}$ also. We need to show that $\bar{a} = \bar{b}$ as sets; this will show that a cannot be in more than one cell. There is a standard way to show that two sets are the same:

Show that each set is a subset of the other.

We show that $\bar{a} \subseteq \bar{b}$. Let $x \in \bar{a}$. Then $x \sim a$. But $a \in \bar{b}$, so $a \sim b$. Then, by the transitive condition (3), $x \sim b$, so $x \in \bar{b}$. Thus $\bar{a} \subseteq \bar{b}$. Now we show that $\bar{b} \subseteq \bar{a}$. Let $y \in \bar{b}$. Then $y \sim b$. But $a \in \bar{b}$, so $a \sim b$ and, by symmetry (2), $b \sim a$. Then by transitivity (3), $y \sim a$, so $y \in \bar{a}$. Hence $\bar{b} \subseteq \bar{a}$ also, so $\bar{b} = \bar{a}$ and our proof is complete. ◆

Each cell in the partition arising from an equivalence relation is an **equivalence class**.

EXERCISES 0

In Exercises 1 through 4, describe the set by listing its elements.

1. $\{x \in \mathbb{R} \mid x^2 = 3\}$

2. $\{m \in \mathbb{Z} \mid m^2 = 3\}$

3. $\{m \in \mathbb{Z} \mid mn = 60 \text{ for some } n \in \mathbb{Z}\}$

4. $\{m \in \mathbb{Z} \mid m^2 - m < 115\}$

In Exercises 5 through 10, decide whether the object described is indeed a set (is well defined). Give an alternate description of each set.

5. $\{n \in \mathbb{Z}^+ \mid n \text{ is a large number}\}$

6. $\{n \in \mathbb{Z} \mid n^2 < 0\}$

7. $\{n \in \mathbb{Z} \mid 39 < n^3 < 57\}$

8. $\{x \in \mathbb{Q} \mid x \text{ is almost an integer}\}$

9. $\{x \in \mathbb{Q} \mid x \text{ may be written with denominator greater than } 100\}$

10. $\{x \in \mathbb{Q} \mid x \text{ may be written with positive denominator less than } 4\}$

11. List the elements in $\{a, b, c\} \times \{1, 2, c\}$.

12. Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$. For each relation between A and B given as a subset of $A \times B$, decide whether it is a function mapping A into B. If it is a function, decide whether it is one to one and whether it is onto B.

a. $\{(1, 4), (2, 4), (3, 6)\}$

b. $\{(1, 4), (2, 6), (3, 4)\}$

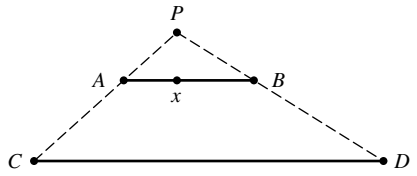
c. $\{(1, 6), (1, 2), (1, 4)\}$

d. $\{(2, 2), (1, 6), (3, 4)\}$

e. $\{(1, 6), (2, 6), (3, 6)\}$

f. $\{(1, 2), (2, 6), (2, 4)\}$

13. Illustrate geometrically that two line segments AB and CD of different length have the same number of points by indicating in Fig. 0.23 what point y of CD might be paired with point x of AB.



0.23 Figure

14. Recall that for $a, b \in \mathbb{R}$ and $a < b$, the **closed interval** $[a, b]$ in $\mathbb{R}$ is defined by $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$. Show that the given intervals have the same cardinality by giving a formula for a one-to-one function f mapping the first interval onto the second.

a. $[0, 1]$ and $[0, 2]$ **b.** $[1, 3]$ and $[5, 25]$ **c.** $[a, b]$ and $[c, d]$

15. Show that $S = \{x \in \mathbb{R} \mid 0 < x < 1\}$ has the same cardinality as $\mathbb{R}$. [*Hint:* Find an elementary function of calculus that maps an interval one to one onto $\mathbb{R}$, and then translate and scale appropriately to make the domain the set S.]

For any set A, we denote by $\mathscr{P}(A)$ the collection of all subsets of A. For example, if $A = \{a, b, c, d\}$, then $\{a, b, d\} \in \mathscr{P}(A)$. The set $\mathscr{P}(A)$ is the **power set** of A. Exercises 16 through 19 deal with the notion of the power set of a set A.

16. List the elements of the power set of the given set and give the cardinality of the power set.

a. $\varnothing$ **b.** $\{a\}$ **c.** $\{a, b\}$ **d.** $\{a, b, c\}$

17. Let A be a finite set, and let $|A| = s$. Based on the preceding exercise, make a conjecture about the value of $|\mathscr{P}(A)|$. Then try to prove your conjecture.

18. For any set A, finite or infinite, let B^A be the set of all functions mapping A into the set $B = \{0, 1\}$. Show that the cardinality of B^A is the same as the cardinality of the set $\mathscr{P}(A)$. [*Hint:* Each element of B^A determines a subset of A in a natural way.]

19. Show that the power set of a set A, finite or infinite, has too many elements to be able to be put in a one-to-one correspondence with A. Explain why this intuitively means that there are an infinite number of infinite cardinal numbers. [*Hint:* Imagine a one-to-one function ϕ mapping A into $\mathscr{P}(A)$ to be given. Show that ϕ cannot be onto $\mathscr{P}(A)$ by considering, for each $x \in A$, whether $x \in \phi(x)$ and using this idea to define a subset S of A that is not in the range of ϕ.] Is *the set of everything* a logically acceptable concept? Why or why not?

20. Let $A = \{1, 2\}$ and let $B = \{3, 4, 5\}$.

a. Illustrate, using A and B, why we consider that $2 + 3 = 5$. Use similar reasoning with sets of your own choice to decide what you would consider to be the value of

i. $3 + \aleph_0$, ii. $\aleph_0 + \aleph_0$.

b. Illustrate why we consider that $2 \cdot 3 = 6$ by plotting the points of $A \times B$ in the plane $\mathbb{R} \times \mathbb{R}$. Use similar reasoning with a figure in the text to decide what you would consider to be the value of $\aleph_0 \cdot \aleph_0$.

21. How many numbers in the interval $0 \leq x \leq 1$ can be expressed in the form .##, where each # is a digit $0, 1, 2, 3, \cdots, 9$? How many are there of the form .#####? Following this idea, and Exercise 15, decide what you would consider to be the value of $10^{\aleph_0}$. How about $12^{\aleph_0}$ and $2^{\aleph_0}$?

22. Continuing the idea in the preceding exercise and using Exercises 18 and 19, use exponential notation to fill in the three blanks to give a list of five cardinal numbers, each of which is greater than the preceding one.

$$\aleph_0, |\mathbb{R}|, \_\_, \_\_, \_\_.$$

In Exercises 23 through 27, find the number of different partitions of a set having the given number of elements.

23. 1 element **24.** 2 elements **25.** 3 elements

26. 4 elements **27.** 5 elements

28. Consider a partition of a set S. The paragraph following Definition 0.18 explained why the relation

$$x \mathscr{R} y \text{ if and only if } x \text{ and } y \text{ are in the same cell}$$

satisfies the symmetric condition for an equivalence relation. Write similar explanations of why the reflexive and transitive properties are also satisifed.

In Exercises 29 through 34, determine whether the given relation is an equivalence relation on the set. Describe the partition arising from each equivalence relation.

29. $n \mathscr{R} m$ in $\mathbb{Z}$ if $nm > 0$ **30.** $x \mathscr{R} y$ in $\mathbb{R}$ if $x \geq y$

31. $x \mathscr{R} y$ in $\mathbb{R}$ if $|x| = |y|$ **32.** $x \mathscr{R} y$ in $\mathbb{R}$ if $|x - y| \leq 3$

33. $n \mathscr{R} m$ in $\mathbb{Z}^+$ if n and m have the same number of digits in the usual base ten notation

34. $n \mathscr{R} m$ in $\mathbb{Z}^+$ if n and m have the same final digit in the usual base ten notation

35. Using set notation of the form $\{\#, \#, \#, \cdots\}$ for an infinite set, write the residue classes modulo n in $\mathbb{Z}^+$ discussed in Example 0.17 for the indicated value of n.

a. $n = 2$ **b.** $n = 3$ **c.** $n = 5$

36. Let $n \in \mathbb{Z}^+$ and let $\sim$ be defined on $\mathbb{Z}$ by $r \sim s$ if and only if $r - s$ is divisible by n, that is, if and only if $r - s = nq$ for some $q \in \mathbb{Z}$.

a. Show that $\sim$ is an equivalence relation on $\mathbb{Z}$. (It is called "congruence modulo n" just as it was for $\mathbb{Z}^+$. See part b.)

b. Show that, when restricted to the subset $\mathbb{Z}^+$ of $\mathbb{Z}$, this $\sim$ is the equivalence relation, *congruence modulo n*, of Example 0.20.

c. The cells of this partition of $\mathbb{Z}$ are *residue classes modulo n* in $\mathbb{Z}$. Repeat Exercise 35 for the residue classes modulo n in $\mathbb{Z}$ rather than in $\mathbb{Z}^+$ using the notation $\{\cdots, \#, \#, \#, \cdots\}$ for these infinite sets.

37. Students often misunderstand the concept of a one-to-one function (mapping). I think I know the reason. You see, a mapping $\phi : A \to B$ has a *direction* associated with it, from A to B. It seems reasonable to expect a one-to-one mapping simply to be a mapping that carries one point of A into one point of B, in the direction indicated by the arrow. But of course, *every* mapping of A into B does this, and Definition 0.12 did not say that at all. With this unfortunate situation in mind, make as good a pedagogical case as you can for calling the functions described in Definition 0.12 *two-to-two functions* instead. (Unfortunately, it is almost impossible to get widely used terminology changed.)

PART I

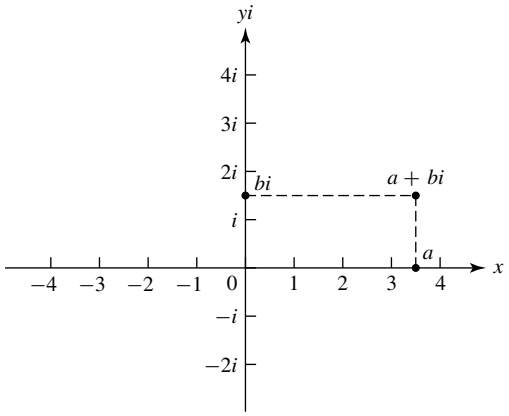
Groups and Subgroups

SECTION 1 Introduction and Examples

In this section, we attempt to give you a little idea of the nature of abstract algebra. We are all familiar with addition and multiplication of real numbers. Both addition and multiplication combine two numbers to obtain one number. For example, addition combines 2 and 3 to obtain 5. We consider addition and multiplication to be *binary operations*. In this text, we abstract this notion, and examine sets in which we have one or more binary operations. We think of a binary operation on a set as giving an algebra on the set, and we are interested in the *structural properties* of that algebra. To illustrate what we mean by a structural property with our familiar set $\mathbb{R}$ of real numbers, note that the equation $x + x = a$ has a solution x in $\mathbb{R}$ for each $a \in \mathbb{R}$, namely, $x = a/2$. However, the corresponding multiplicative equation $x \cdot x = a$ does not have a solution in $\mathbb{R}$ if $a < 0$. Thus, $\mathbb{R}$ with addition has a different algebraic structure than $\mathbb{R}$ with multiplication.

Sometimes two different sets with what we naturally regard as very different binary operations turn out to have the same algebraic structure. For example, we will see in Section 3 that the set $\mathbb{R}$ with addition has the same algebraic structure as the set $\mathbb{R}^+$ of positive real numbers with multiplication!

This section is designed to get you thinking about such things informally. We will make everything precise in Sections 2 and 3. We now turn to some examples. Multiplication of complex numbers of magnitude 1 provides us with several examples that will be useful and illuminating in our work. We start with a review of complex numbers and their multiplication.



1.1 Figure

Complex Numbers

A real number can be visualized geometrically as a point on a line that we often regard as an x-axis. A complex number can be regarded as a point in the Euclidean plane, as shown in Fig. 1.1. Note that we label the vertical axis as the yi-axis rather than just the y-axis, and label the point one unit above the origin with i rather than 1. The point with Cartesian coordinates (a, b) is labeled $a + bi$ in Fig. 1.1. The set $\mathbb{C}$ of **complex numbers** is defined by

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

We consider $\mathbb{R}$ to be a subset of the complex numbers by identifying a real number r with the complex number $r + 0i$. For example, we write $3 + 0i$ as 3 and $-\pi + 0i$ as $-\pi$ and $0 + 0i$ as 0. Similarly, we write $0 + 1i$ as i and $0 + si$ as si.

Complex numbers were developed after the development of real numbers. The complex number i was *invented* to provide a solution to the quadratic equation $x^2 = -1$, so we require that

$$i^2 = -1. \tag{1}$$

Unfortunately, i has been called an **imaginary number,** and this terminology has led generations of students to view the complex numbers with more skepticism than the real numbers. Actually, *all* numbers, such as $1, 3, \pi, -\sqrt{3}$, and i are inventions of our minds. There is no physical entity that *is* the number 1. If there were, it would surely be in a place of honor in some great scientific museum, and past it would file a steady stream of mathematicians, gazing at 1 in wonder and awe. A basic goal of this text is to show how we can invent solutions of polynomial equations when the coefficients of the polynomial may not even be real numbers!

Multiplication of Complex Numbers

The product $(a + bi)(c + di)$ is defined in the way it must be if we are to enjoy the familiar properties of real arithmetic and require that $i^2 = -1$, in accord with Eq. (1).

Namely, we see that we want to have

$$\begin{aligned}(a+bi)(c+di) &= ac + adi + bci + bdi^2 \\ &= ac + adi + bci + bd(-1) \\ &= (ac - bd) + (ad + bc)i.\end{aligned}$$

Consequently, we define multiplication of $z_1 = a + bi$ and $z_2 = c + di$ as

$$z_1 z_2 = (a + bi)(c + di) = (ac - bd) + (ad + bc)i, \tag{2}$$

which is of the form $r + si$ with $r = ac - bd$ and $s = ad + bc$. It is routine to check that the usual properties $z_1 z_2 = z_2 z_1$, $z_1(z_2 z_3) = (z_1 z_2)z_3$ and $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$ all hold for all $z_1, z_2, z_3 \in \mathbb{C}$.

1.2 Example Compute $(2 - 5i)(8 + 3i)$.

Solution We don't memorize Eq. (2), but rather we compute the product as we did to motivate that equation. We have

$$(2 - 5i)(8 + 3i) = 16 + 6i - 40i + 15 = 31 - 34i. \quad \blacktriangle$$

To establish the geometric meaning of complex multiplication, we first define the **absolute value** $|a + bi|$ of $a + bi$ by

$$|a + bi| = \sqrt{a^2 + b^2}. \tag{3}$$

This absolute value is a nonnegative real number and is the distance from $a + bi$ to the origin in Fig. 1.1. We can now describe a complex number z in the polar-coordinate form

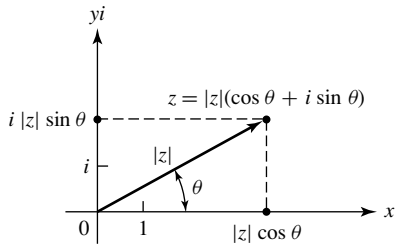
$$z = |z|(\cos\theta + i\sin\theta), \tag{4}$$

where θ is the angle measured counterclockwise from the x-axis to the vector from 0 to z, as shown in Fig. 1.3. A famous formula due to Leonard Euler states that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Euler's Formula

We ask you to derive Euler's formula formally from the power series expansions for e^θ, $\cos\theta$ and $\sin\theta$ in Exercise 41. Using this formula, we can express z in Eq. (4) as



1.3 Figure

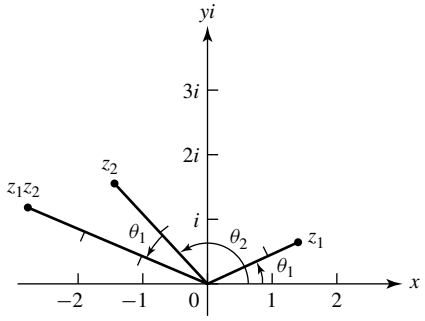
$z = |z|e^{i\theta}$. Let us set

$$z_1 = |z_1|e^{i\theta_1} \qquad \text{and} \qquad z_2 = |z_2|e^{i\theta_2}$$

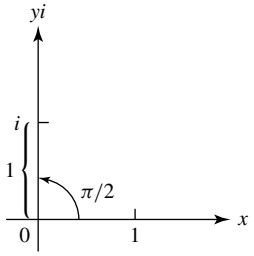
and compute their product in this form, assuming that the usual laws of exponentiation hold with complex number exponents. We obtain

$$\begin{aligned} z_1 z_2 &= |z_1|e^{i\theta_1}|z_2|e^{i\theta_2} = |z_1||z_2|e^{i(\theta_1+\theta_2)} \\ &= |z_1||z_2|[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)]. \end{aligned} \tag{5}$$

Note that Eq. 5 concludes in the polar form of Eq. 4 where $|z_1 z_2| = |z_1||z_2|$ and the polar angle θ for $z_1 z_2$ is the sum $\theta = \theta_1 + \theta_2$. Thus, geometrically, we multiply complex numbers by multiplying their absolute values and adding their polar angles, as shown in Fig. 1.4. Exercise 39 indicates how this can be derived via trigonometric identities without recourse to Euler's formula and assumptions about complex exponentiation.



1.4 Figure



1.5 Figure

Note that i has polar angle $\pi/2$ and absolute value 1, as shown in Fig. 1.5. Thus i^2 has polar angle $2(\pi/2) = \pi$ and $|1 \cdot 1| = 1$, so that $i^2 = -1$.

1.6 Example Find all solutions in $\mathbb{C}$ of the equation $z^2 = i$.

Solution Writing the equation $z^2 = i$ in polar form and using Eq. (5), we obtain

$$|z|^2(\cos 2\theta + i\sin 2\theta) = 1(0 + i).$$

Thus $|z|^2 = 1$, so $|z| = 1$. The angle θ for z must satisfy $\cos 2\theta = 0$ and $\sin 2\theta = 1$. Consequently, $2\theta = (\pi/2) + n(2\pi)$, so $\theta = (\pi/4) + n\pi$ for an integer n. The values of n yielding values θ where $0 \le \theta < 2\pi$ are 0 and 1, yielding $\theta = \pi/4$ or $\theta = 5\pi/4$. Our solutions are

$$z_1 = 1\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \qquad \text{and} \qquad z_2 = 1\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right)$$

or

$$z_1 = \frac{1}{\sqrt{2}}(1+i) \qquad \text{and} \qquad z_2 = \frac{-1}{\sqrt{2}}(1+i). \qquad \blacktriangle$$

1.7 Example Find all solutions of $z^4 = -16$.

Solution As in Example 1.6 we write the equation in polar form, obtaining

$$|z|^4(\cos 4\theta + i \sin 4\theta) = 16(-1 + 0i).$$

Consequently, $|z|^4 = 16$, so $|z| = 2$ while $\cos 4\theta = -1$ and $\sin 4\theta = 0$. We find that $4\theta = \pi + n(2\pi)$, so $\theta = (\pi/4) + n(\pi/2)$ for integers n. The different values of θ obtained where $0 \le \theta < 2\pi$ are $\pi/4$, $3\pi/4$, $5\pi/4$, and $7\pi/4$. Thus one solution of $z^4 = -16$ is

$$2\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right) = 2\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) = \sqrt{2}(1 + i).$$

In a similar way, we find three more solutions,

$$\sqrt{2}(-1 + i), \qquad \sqrt{2}(-1 - i), \qquad \text{and} \qquad \sqrt{2}(1 - i). \qquad \blacktriangle$$

The last two examples illustrate that we can find solutions of an equation $z^n = a + bi$ by writing the equation in polar form. There will always be n solutions, provided that $a + bi \neq 0$. Exercises 16 through 21 ask you to solve equations of this type.

We will not use addition or division of complex numbers, but we probably should mention that addition is given by

$$(a + bi) + (c + di) = (a + c) + (b + d)i. \tag{6}$$

and division of $a + bi$ by nonzero $c + di$ can be performed using the device

$$\begin{aligned}\frac{a + bi}{c + di} &= \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} \\ &= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.\end{aligned} \tag{7}$$

Algebra on Circles

Let $U = \{z \in \mathbb{C} \mid |z| = 1\}$, so that U is the circle in the Euclidean plane with center at the origin and radius 1, as shown in Fig. 1.8. The relation $|z_1 z_2| = |z_1||z_2|$ shows that the product of two numbers in U is again a number in U; we say that U is *closed* under multiplication. Thus, we can view multiplication in U as providing algebra on the circle in Fig. 1.8.

As illustrated in Fig. 1.8, we associate with each $z = \cos\theta + i \sin\theta$ in U a real number $\theta \in \mathbb{R}$ that lies in the half-open interval where $0 \le \theta < 2\pi$. This half-open interval is usually denoted by $[0, 2\pi)$, but we prefer to denote it by $\mathbb{R}_{2\pi}$ for reasons that will be apparent later. Recall that the angle associated with the product $z_1 z_2$ of two complex numbers is the sum $\theta_1 + \theta_2$ of the associated angles. Of course if $\theta_1 + \theta_2 \ge 2\pi$