SELECTIONS FROM MODERN ABSTRACT ALGEBRA

RICHARD V. ANDREE
The University of Oklahoma

CONSTABLE AND COMPANY LTD
10 ORANGE STREET, LONDON, W. C. 2

Library of Congress Catalog Card Number: 58-6799

20416-0118

Printed in the United States of America

SELECTIONS FROM

MODERN ABSTRACT ALGEBRA

$$T_0$$

$$\left| \begin{array}{cc} J_0 & -p\,h \\ e^{\frac{i\,\pi}{2}} n_e & s\ ln^{-1}\ 1 \end{array} \right|$$

who has the acumen to help when help is needed

and has the sagacity to preserve silence when help is of no avail.

PREFACE

A modern text on abstract algebra tends to become a ten-volume series. This brief volume is not designed to replace such a series, but rather whet the student's appetite for the series, to help him decide which portions of the series are most suitable for him to take, and to help bridge the possible gap between freshman preparation and the abstract thinking required in higher mathematics. Students enjoy the work—enthusiasm runs high. The more advanced courses now contain a larger percentage of engineers, physicists, and chemists than ever before. Applications from these fields, as well as from psychology and social science, are indicated in this volume, and the student is provided with an opportunity to explore those regions nearest his own interests.

It is currently fashionable to require "a certain amount of mathematical maturity" as a prerequisite for advanced mathematics courses. This assumption is *not* made in this text. Indeed, *one important purpose of this text is to develop the "mathematical maturity" which many authors require.*

In accord with the author's conviction that students should be encouraged to use the mathematical library, there are suggestions for further reading from other texts and from the *American Mathematical Monthly*. A sincere effort has been made to suggest articles which are both palatable and authoritative.

Abstract algebra now occupies about the same relative position to mathematics in general as mathematics does to engineering and the physical sciences. In addition to being a fascinating discipline in its own right, abstract algebra provides the vocabulary and many of the general techniques used in the larger body of knowledge. It therefore seems quite appropriate to introduce abstract algebra early. A mathematics major at the University of Oklahoma usually takes this course in his sophomore year, concurrently with calculus. Engineering and science majors often fit it into their junior or senior year. The text is suitable for two, three, or four semester-hours of work, depending upon student preparation and the selection of material to be presented. Chapter 3 (Boolean Algebra) can be studied independently of the rest of the text (but not conversely). However, it has been found more effective if preceded by Sections 1–1 to 1–6. The approach to Boolean algebra via switching circuits has wide

appeal to students and illustrates how closely mathematical theory can parallel physical reality.

In a short course, optional (*) sections may be omitted or used as project material. Likewise Chapters 6 and 7 may be covered rapidly or omitted entirely if the student is familiar with their contents.

Although the author personally likes the vector space approach to matrices, it has been avoided here for two reasons. First, it seems unfair to spoil the elegance of the vector space approach for the student who later takes a course in matric theory, and, second, experience shows that the first introduction to matrices is easier if a matrix is considered as an entity—as an element of a matric algebra.

Chapter 9, which contains more advanced work on matrices, can be taken directly after Chapter 5 if the student is already familiar with determinant theory (Chapter 7), but the author's experience suggests that a better rounded course is obtained if Chapter 8 (Fields, Rings, and Ideals) is studied before Chapter 9. In a short course, it may be well to omit Chapter 9 entirely. If this is done, you may still wish to discuss Section 9–7, "What Mathematics to Take Next," with your students.

One marked difference between this book and certain other recent texts is that it selects interesting and important ideas from *various* parts of modern abstract algebra rather than being mostly devoted to the theory of matrices. Matric theory is vital, but it is only one facet of modern abstract algebra. For many students this book may well provide their maiden voyage into the abstract thinking which is the heart of mathematics. Hence, special care has been taken in the development of basic concepts such as equivalence relations and their corresponding equivalence classes.

Every student deserves the thrill of making mathematical discoveries of his own, and then of proving or disproving his conjectures. If these discoveries happen already to be known to others, this in no way need detract from his accomplishment—it may merely mean that the others were born sooner.

This text contains many indications of where and how abstract algebra is applied in the world of today, but this is not the reason students study it. They study *Selections from Modern Abstract Algebra* because it is interesting and fun.

The author will welcome an opportunity to correspond with you concerning the use of this text. It is his sincere hope that you and your students will enjoy *Selections from Modern Abstract Algebra.*

ACKNOWLEDGEMENTS

The lecture notes which sparked this book were first used in 1954 by the author for a two-hour sophomore-level course in abstract algebra at the University of Oklahoma. The engineering students quickly discovered

the advantages of an undergraduate course containing Boolean algebra, and introductions to the theories of groups and matrices. The demand for the course increased and, as it was offered more frequently, its revision became an almost continuous process. Colleagues at various institutions used portions of the notes in their classes and offered helpful suggestions. Among those who used the notes are: J. C. Brixey (University of Oklahoma), Emil Grosswald (University of Pennsylvania), V. O. McBrien (Holy Cross), C. O. Oakley (Haverford College), G. E. Schweigert (University of Pennsylvania), O. T. Shannon (Arkansas A, M and N College), and R. J. Swords (Holy Cross). In addition to this, portions of these notes were used at graduate summer institutes for high-school mathematics teachers at the University of Oklahoma (Norman), and at Montana State College (Bozeman). Professor E. Grosswald used them for a similar group at the University of Pennsylvania. Chapter 3 on Boolean algebra was duplicated separately by Professor F. E. McFarlin for use by the Department of Electrical Engineering at Oklahoma State University (Stillwater), and the University of Pennsylvania (Philadelphia). Mr. E. L. Walters (Wm. Penn High School, York, Pennsylvania) used them for enrichment material with a group of advanced high-school students.

Many friends read and made constructive suggestions on the notes; among them were: Bess E. Allen (Wayne University), J. H. Barrett (University of Utah), B. H. Bissinger (Lebanon Valley College), R. B. Crouch (New Mexico College of A. and M. Arts), J. C. Eaves (University of Kentucky), C. L. Farrar (University of Oklahoma), R. A. Good (University of Maryland), D. W. Hall (Harpur College), R. W. House (Pennsylvania State University), M. Gweneth Humphreys (Randolph-Macon Women's College), C. F. Koehler (Loyola College), Violet H. Larney (New York State College for Teachers), D. R. Lintvedt (Upsala College), C. C. MacDuffee (University of Wisconsin), J. E. Maxfield (Naval Ordnance Test Station), Margaret W. Maxfield (Naval Ordnance Test Station), B. E. Meserve (New Jersey State Teachers College), A. L. Mullikin (University of Oklahoma), D. A. Norton (University of California), R. L. San Soucie (Sylvania Electric), Augusta L. Schurrer (Iowa State Teacher's College), W. R. Utz (University of Missouri), R. J. Wisner (Haverford College), and J. L. Zemmer, Jr. (University of Missouri).

The most important contribution was certainly that of the author's wife, Josephine Peet Andree who combines a sound mathematical preparation with the rare qualities of patience, pedigogical judgment, and understanding.

Important contributions were also made, sometimes under duress, by the several hundred students who used this text in its various duplicated forms, and by the excellent editorship of Professor B. W. Jones (University of Colorado).

Galley proof was read by Professor Walter Stuermann (University

of Tulsa), Professor D. J. Lewis (Notre Dame), Mrs. R. V. Andree, and Mrs. R. A. Andree in addition to the author. Each merits sincere thanks, both from the author and from the reader.

R.V.A. January, 1958

Norman, Oklahoma

CONTENTS

1

NUMBER THEORY & PROOF

1-1 Introduction

The *integers* consist of the "counting numbers" or natural whole numbers $1, 2, 3, 4, \cdots$ (positive integers), their negatives $-1, -2, -3, -4, -5, \cdots$ (negative integers), and zero 0. In later chapters, when rational numbers, real numbers, or complex numbers are used, it will be assumed that you know the meanings of these terms. Briefly: A *rational number* is a quotient of two integers a/b with $b \neq 0$.† A *real number* is a number which represents a distance or its negative. A *complex number* is an ordered pair of real numbers, (a, b) or equivalently, a number of the form $a + bi$, where a and b are real and $i^2 = -1$. A more complete discussion of the real number system is presented in the book *What is Mathematics?* by Courant & Robbins (Oxford).

The complex numbers contain all the real numbers, rational numbers, and integers as subsets. The real numbers contain all the rational numbers and the integers as subsets (but not all the complex numbers). The rational numbers contain all the integers as a subset (but not all the real nor complex numbers). The integers do not contain all of any of the other sets. This entire paragraph may be expressed in one line using the symbol "$\subset$" to mean "contained in" or "form a subset of":

$$\text{Integers} \subset \text{Rationals} \subset \text{Reals} \subset \text{Complex Numbers}$$

It may be of interest to note that the properties of the rational numbers, real numbers, and even of the complex numbers can be derived from those of the integers by using logical reasoning. L. Kronecker (1823–1891, German) is reputed to have said, "God gave us the integers, all else is the work of man."

†The symbol "$\neq$" is read "not equal to."

1–2 The Modulo 7 System

This section introduces a new arithmetic. To remind you that this is a new system, the congruence sign, $\equiv$, will be used in place of the usual $=$, equal sign. This system has only seven numbers in it: 0, 1, 2, 3, 4, 5, 6. It is called the modulo 7, or "mod 7," system.

The rules for addition in the mod 7 system are the same as those for ordinary addition *except that, if the sum is larger than 6, the sum is divided by 7, the quotient discarded, and the remainder is used in place of the ordinary sum.* Thus, $1 + 3 \equiv 4 \pmod 7$ and $2 + 3 \equiv 5 \pmod 7$; but $5 + 4 \equiv 2 \pmod 7$, since when 9 is divided by 7 the remainder is 2. Also, $6 + 5 \equiv 4 \pmod 7$, since the remainder 4 is obtained when 11 is divided by 7. In a similar fashion: $5 + 2 \equiv 0 \pmod 7$, $4 + 1 + 3 + 5 \equiv 6 \pmod 7$, and $4 + 0 + 2 + 3 + 6 \equiv 1 \pmod 7$.)

The rules for multiplication in the mod 7 system are also like those of ordinary multiplication except that, if the product is larger than 6, the product is divided by 7 and the *remainder* is used in place of the ordinary product. Thus: $2 \times 2 \equiv 4 \pmod 7$, but $5 \times 2 \equiv 3 \pmod 7$, since if 10 is divided by 7, a remainder of 3 results. Also, $6 \times 3 \equiv 4 \pmod 7$, since, when 18 is divided by 7, the remainder is 4. In a similar fashion, $4 \times 3 \equiv 5 \pmod 7$, $5 \times 6 \equiv 2 \pmod 7$, and $2 \times 3 \times 4 \times 5 \equiv 1 \pmod 7$, the remainder when 120 is divided by 7. Practice until you can do sums and products easily in the mod 7 system. *Briefly*: $a \equiv b \pmod 7$ *means* $a = b + 7k$ *for some integer* k. (Why?)

There are no negative numbers in the mod 7 system. None are needed. The ordinary negative number -2 is the solution of the ordinary equation $x + 2 = 0$. In the mod 7 system, the number 5 is a solution of the equation $x + 2 \equiv 0 \pmod 7$, since $(5 + 2)$ has the remainder 0 when divided by 7. In other words: 5, in the mod 7 system, plays a role similar to that of -2 in the ordinary system. In the mod 7 system, the number 6 plays a role similar to -1 in the ordinary numbers, since $6 + 1 \equiv 0 \pmod 7$ and $-1 + 1 = 0$.

There are no fractions in the mod 7 system and none are needed. The ordinary fraction 5/3 is the solution of the equation $3x = 5$. In the mod 7 system, the equation $3x \equiv 5 \pmod 7$ has the solution $x \equiv 4 \pmod 7$. (Try it and see.) The mod 7 equation $5x \equiv 2 \pmod 7$ has $x \equiv 6 \pmod 7$ as solution, while $4x \equiv 6 \pmod 7$ has the solution $x \equiv 5 \pmod 7$.

The equation $5x^3 + x^2 + 5x + 2 \equiv 0 \pmod 7$ may be shown to have $x \equiv 3 \pmod 7$ as a solution by direct substitutions. (Try it.) Can you find two other solutions?

To reiterate, there are only seven numbers in the entire mod 7 system. There are no negative numbers and no fractions, yet equations can be solved. Best of all, since there are only seven numbers, *all* the solutions of a given equation can be found by merely substituting each of the seven

numbers, in turn, for x to see which, if any, of them satisfy the equation.

The mod 7 system is a finite set of numbers, whereas the integers, rational numbers, and real numbers discussed above are each infinite sets.

A word of warning: There exist equations, such as $x^2 \equiv 6 \pmod 7$, which have no solution at all. This is not particularly surprising. The ordinary equation $x^2 = -1$ has no solution in the set of *real numbers*. In this book, the word "solve" will mean "find all possible solutions or prove that none exist."

The mod 7 system is introduced here to provide laboratory material for your algebraic experiments in Chapter 1. Modular systems are studied in more detail in Chapter 2.

Problem Set 1-2

1. Add: $4 + 3 + 6 + 5 + 2 + 4 \pmod 7$.
2. Add: $1 + 2 + 3 + 4 + 5 + 6 \pmod 7$.
3. Solve: $3x \equiv 5 \pmod 7$.
4. Solve: $6x - 5 \equiv 3 \pmod 7$.
5. Solve: $297x + 6 \equiv 0 \pmod 7$. Although 297 does *not* occur in the mod 7 system, $297x$ still has meaning, since $297x$ represents the sum of $\underbrace{x + x + \cdots + x}_{297 \text{ terms}}$. This problem emphasizes the need for distinguishing between the set from which the unknowns of the equation are taken and the set from which the coefficients of the equation are taken.
6. Solve: $x^2 \equiv 4 \pmod 7$.
7. Solve: $x^2 \equiv 2 \pmod 7$.
8. Solve: $x^2 \equiv 3 \pmod 7$.
9. Solve: $x^3 \equiv 6 \pmod 7$.
10. Solve: $x^3 \equiv 5 \pmod 7$.
11. (a) Make a table listing the seven numbers in the mod 7 system. Next to each number x, place its square, x^2; cube, x^3; fourth power, x^4; fifth power, x^5; sixth power, x^6; seventh power, x^7; and eighth power, x^8; all mod 7.
    (b) Compute, using the table of part (a), the values $(5)^{236} \pmod 7$, and $(3)^{179} \pmod 7$.
    (c) Will $x^4 \equiv 5 \pmod 7$ have a solution?
    (d) For what values of b will $x^5 \equiv b \pmod 7$ have solutions?
12. Solve: $4x^2 + 3x + 4 \equiv 0 \pmod 7$. Notice that in the mod 7 system the solutions are not complex.
13. Construct addition and multiplication tables for the mod 7 system.

14. If the symbol $\equiv$ is to be an equals (or equivalence) relation, it must satisfy the following postulates:
    1. *Reflexive*: $a \equiv a \pmod 7$.
    2. *Symmetric*: If $a \equiv b \pmod 7$, then $b \equiv a \pmod 7$.
    3. *Transitive*: If $a \equiv b \pmod 7$ and $b \equiv c \pmod 7$, then $a \equiv c \pmod 7$.

    Use the definition "$a \equiv b \pmod 7$ means $a = b + 7k$, for some integer k" to show that the mod 7 system does satisfy these requirements. [HINT: Given $a \equiv b \pmod 7$, to prove that $b \equiv a \pmod 7$. This means that, if one assumes that there exists a k, such that $a = b + 7k$, then one may deduce that $b = a + 7(-k)$, and hence that $b \equiv a \pmod 7$. (Why?)]

15. Show from the definition of $a \equiv b \pmod 7$ that, if $b \equiv 2 \pmod 7$ and $c \equiv 5 \pmod 7$, then $b + c \equiv 2 + 5 \equiv 0 \pmod 7$, and that $b \times c \equiv 2 \times 5 \equiv 3 \pmod 7$. [HINT: Since $b = 2 + k \cdot 7$ and $c = 5 + j \cdot 7$, then $b + c = (2 + k7) + (5 + j7) = (2 + 5) + (k + j)7$. Also, $b \times c = (2 + k7) \times (5 + j7) = 2 \times 5 + (2j + 5k + 7jk)7$.]

16. The days of the week can be thought of as forming a mod 7 system in which the names of the days are replaced by integers mod 7. Starting with Sunday $\leftrightarrow 0$, Monday $\leftrightarrow 1$, $\cdots$, Saturday $\leftrightarrow 6$, solve the following problem. If Christmas, the 359th day of the year, falls on Sunday, on what day does July 4, the 185th day, fall? On what day does September 1, the 244th day, fall?

17. How many different congruences (equations) of the form $Ax \equiv B \pmod 7$ with $A \not\equiv 0$ are there?

18. Does the relation $\sim$ (is similar to) satisfy the reflexive, symmetric, and transitive postulates given in Problem 14, if the elements $(a, b, c, \cdots)$ are triangles? [HINT: Replace "$\equiv$" by "$\sim$" and see.]

19. Does the relation $\not\equiv$ satisfy the three postulates of Problem 14, if the elements a, b, c are integers?

20. Which of the postulates of Problem 14 are satisfied if "$\equiv$" is replaced by "$\mid$" (divides)?

21. Find a relationship, other than those mentioned in the text, which satisfies the three postulates of Problem 14. [HINT: Try "Is a brother or half brother of," "Is a descendant of," "Has the same parents as," "Is the same color (or age) as," "Has long blond hair like," and other similar relationships. Does it make a difference whether the relation is defined over the set of all people or merely the set of all men?]

1–3 The Modulo 6 System

It is reasonable and prudent to inquire whether other positive integers, say 6, also yield a modular system similar to the mod 7 system. Certainly

it is feasible to define addition and multiplication mod 6 just as we did mod 7.

$$a \equiv b \pmod 6 \quad \text{means} \quad a = b + 6k \quad \text{for some integer } k.$$

The modulo 6 system contains six numbers, 0, 1, 2, 3, 4, 5. There are no negative numbers, for none are needed. (Why?) There are no fractions. If an equation has solutions, they can be found by direct substitution, since there are only six numbers in the mod 6 system. There are, however, important differences between the mod 6 system and either the real number system or the mod 7 system. In the real number system (and also in the mod 7 system, as you will prove in Chapter 2), a product is equal to zero *if, and only if,* at least one of its factors is zero, i.e.,

if either $A = 0$ or $B = 0$, then $A \cdot B = 0$ and conversely
if $A \cdot B = 0$, then either $A = 0$ or $B = 0$ (or both).

This important property is basic in the solution of equations.

In the mod 6 system, the "if" part—"*If either* $A = 0$ *or* $B = 0$, *then* $A \cdot B = 0$"—is still satisfied; but the "only if" part—"*If* $A \cdot B = 0$, *then either* $A = 0$ *or* $B = 0$"—does not hold. A single counterexample is sufficient to show this. (Why?) Take $A = 4$ and $B = 3$, neither of which is equivalent to 0 modulo 6. However, $4 \cdot 3 \equiv 12 \equiv 0 \pmod 6$.

An important difference between the mod 7 system and the mod 6 system is that, in the mod 7 system (as in the real numbers), the congruence (equation) $Ax \equiv B \pmod 7$, with $A \not\equiv 0$, always has a solution. (You can prove this now by examining the 42 possible cases. In Chapter 2, the problem is solved more easily.) In the mod 6 system, there are linear equations such as $4x \equiv 5 \pmod 6$ and $2x \equiv 3 \pmod 6$, which have no solution at all. (Try them and see.)

The proof that a polynomial equation has no more solutions than its degree uses the fact that a product of two factors is zero if, and only if, at least one of the factors is zero. Since the mod 6 system does not have this property, it is possible that an equation mod 6 may have more solutions than its degree. Indeed, this proves to be the case. Both $x \equiv 2 \pmod 6$ and $x \equiv 5 \pmod 6$ are solutions of $2x \equiv 4 \pmod 6$ while $4x^2 \equiv 4 \pmod 6$ has $x \equiv 1, 2, 4, 5$ as solutions. However, $5x^2 \equiv 4 \pmod 6$ has no solution. It is interesting to note that, while $4x^2 \equiv 4 \pmod 6$ has four solutions, $x^2 \equiv 1 \pmod 6$, obtained by dividing the previous equation by 4, has only two solutions.

Apparently these modular systems need closer examination before general conclusions can be drawn. Before doing so, let us investigate certain properties of ordinary integers and consider some remarks on the nature of proofs. Modular systems in general are considered in Chapter 2.

Problem Set 1-3

1. Add $4 + 3 + 6 + 5 + 2 + 4 \pmod 6$.
2. Add $1 + 2 + 3 + 4 + 5 + 6 \pmod 6$.
3. Solve: $3x \equiv 5 \pmod 6$.
4. Solve: $6x - 5 \equiv 3 \pmod 6$.
5. Solve: $297x + 6 \equiv 0 \pmod 6$. Although 297 does *not* occur in the mod 6 system, $297x$ still has meaning, since $297x$ represents the sum of $\underbrace{x + x + \cdots + x}_{297 \text{ terms}}$. This problem emphasizes the need for distinguishing between the set from which the unknowns of the equation are taken and the set from which the coefficients of the equation are taken.
6. Solve: $x^2 \equiv 4 \pmod 6$.
7. Solve: $x^2 \equiv 2 \pmod 6$.
8. Solve: $x^2 \equiv 3 \pmod 6$.
9. Solve: $x^3 \equiv 6 \pmod 6$.
10. Solve: $x^3 \equiv 5 \pmod 6$.
11. Solve: $4x \equiv 3 \pmod 6$.
12. Solve: $2x \equiv 6 \pmod 6$.
13. Solve: $4x \equiv 6 \pmod 6$.
14. (a) Make a table listing the six numbers in the mod 6 system. Next to each number x, place its square, x^2; cube, x^3; fourth power, x^4; fifth power, x^5; sixth power, x^6; seventh power, x^7; and eighth power, x^8; all mod 6.
    (b) Compute, using the table of part (a), the values $(5)^{236}$ and $(3)^{179}$ will have in the mod 6 system.
    (c) Will $x^4 \equiv 5 \pmod 6$ have a solution?
    (d) For what values of b will $x^5 \equiv b \pmod 6$ have solutions?
15. Solve: $4x^2 + 3x + 4 \equiv 0 \pmod 6$. Notice that in the mod 6 system the solutions are *not* complex or imaginary numbers.
16. Construct addition and multiplication tables for the mod 6 system.
17. If the symbol $\equiv$ is to be an equals (or equivalence) relation, it must satisfy the following postulates:

    1. *Reflexive*: $a \equiv a \pmod 6$.
    2. *Symmetric*: If $a \equiv b \pmod 6$, then $b \equiv a \pmod 6$.
    3. *Transitive*: If $a \equiv b \pmod 6$ and $b \equiv c \pmod 6$, then $a \equiv c \pmod 6$.

Use the definition "$a \equiv b \pmod 6$ means $a = b + 6k$ for some integer k" to show that the mod 6 system does satisfy these requirements.

18. Show that, if $b \equiv 2 \pmod 6$ and $c \equiv 5 \pmod 6$, then $b + c \equiv 2 + 5 \equiv 1 \pmod 6$, and $b \times c \equiv 2 \times 5 \equiv 4 \pmod 6$. [HINT: Since $b = 2 + 6k$ and $c = 5 + 6j$, then $b + c = (2 + 6k) + (5 + 6j) = (2 + 5) + (k + j)6$. Also, $b \times c = (2 + 6k) \times (5 + 6j) = 2 \times 5 + (2j + 5k + 6jk)6$.]

19. Discover three different congruences of the form $Ax \equiv B \pmod 6$ with $A \not\equiv 0$ which have *no* solution. Do not use examples from the text.

20. Discover two different congruences of the form $Ax \equiv B \pmod 6$ with $A \not\equiv 0$ which have *more than one* solution. Do not use examples from the text.

21. Make up a congruence of the form $Ax \equiv B \pmod 6$, with $A \not\equiv 0$, which has exactly one solution. Prove that only one solution exists by actually substituting the six possible values.

1–4 Integral Domains

An *integral domain* is defined to be a set of elements $a, b, c, \cdots$ having two operations, $+$ and $\times$, and an equals relation,† which satisfies the following postulates. The integers serve as one example of a set which satisfies these postulates; there are other examples. In each postulate it is assumed that a, b, c are elements of the integral domain.

1. *Closure*: For each pair a, b of elements of the integral domain, $a + b$ and $a \times b$ are also elements of the integral domain and are unique.
2. *Commutative Laws*: For each pair a, b of elements of the domain, $a + b = b + a$ and $a \times b = b \times a$.
3. *Associative Laws*: For each set of three elements a, b, c, $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$.
4. *Additive Identity (Zero)*: There exists an element z such that, for every element b, $b + z = z + b = b$, and $b \times z = z \times b = z$. (In the case of integers, z = zero.)
5. *Multiplicative Identity (Unity)*: There exists an element u such that, for every element b, $b \times u = u \times b = b$. (In the case of integers, $u = 1$.)

---

†In addition to the postulates given in Problem 17, Set 1–3, an equals relation must also be well defined with respect to the given operations; that is, $a = b$ must imply $a + c = b + c$ and $a \cdot c = b \cdot c$.