Exercises [A]

1. In the group consisting of the rational numbers under addition, what is the inverse of 4? What does Theorem G3 tell us about the solution of (a) $x + 4 = 10$? (b) $x - 4 = 10$?
2. In the group consisting of the non-zero rational numbers under multiplication, what is the inverse of 3? What does Theorem G3 tell us about the solution of (a) $3x = 5$? (b) $\frac{1}{3}x = 4$?
3. Solve $5x + 4 = 12$ in the set of rational numbers, justifying each step by a theorem.
4. Solve $3x - 7 = -12$ in the set of rational numbers, justifying each step by a theorem.
5. Without using Theorem G3, show that in any group (not necessarily commutative) if $a \circ x = b$ and $a \circ y = b$, then $x = y$.
6. (a) Prove that in any group $(a')' = a$.
   (b) Interpret (a) in the rational numbers under addition.
   (c) Interpret (a) in the non-zero rational numbers under multiplication.
7. (a) Prove that in any group $(a \circ b)' = b' \circ a'$.
   (b) Interpret (a) in the rational numbers under addition.
   (c) Interpret (a) in the non-zero rational numbers under multiplication.
8. Prove that if a group is such that for every element x of the group $x \circ x = e$, then the group is commutative.

Exercises [B]

1. Let S be a set with a binary operation $\circ$. Prove that if there is an element in S which satisfies the Identity law under $\circ$, then there is only one such element. We call such an element *the* identity element for $\circ$.
(*Hint:* Suppose e and e' both satisfy the Identity law for $\circ$. Prove $e = e'$.)

2. Let S be a set with an associative binary operation $\circ$. Prove that no element a of S can satisfy the Inverse law under $\circ$ with more than one element of S. (*Hint*: Given any element a in S, assume there exist elements a' and a'' in S such that $a \circ a' = a' \circ a = e$ and $a \circ a'' = a'' \circ a = e$, and proceed from there.) We call such an element (if one exists) *the* inverse of a under $\circ$.

3. We say that a subset H of a group G is a subgroup of G if and only if H satisfies the definition of a group itself. An alternate definition for a subgroup is the following: Let G be a group under operation $*$, and let H be a non-empty subset of G. Then H is called a subgroup of G if for any elements a, b in H, the elements a^{-1}, b^{-1}, and $a * b$ are also in H. Show that H satisfies the definition of a group with operation $*$ if it satisfies the alternate definition of a subgroup.

4. Let G be a group under operation $*$ and let H be a non-empty subset of G. Show that H is a subgroup of G if and only if $a^{-1} * b$ is in H whenever a, b are in H. Use the second definition of subgroup above.

5. Prove that if $*$ is an associative binary operation on a set S and a, b, c, d are elements of S, then $((a * b) * c) * d = (a * b) * (c * d)$.

6. Let H, K be subsets of a group G. Prove that if H and K are both subgroups of G, then $H \cap K$ is a subgroup of G. (Using the alternate definition of a subgroup, it is only necessary to prove that for any elements a, b in $H \cap K$, the elements a^{-1}, b^{-1}, and $a * b$ are in $H \cap K$, when $*$ denotes the operation.)

6. Let H, K be subsets of a group G. Prove that if H and K are both subgroups of G, then $H \cap K$ is a subgroup of G. (Using the alternate definition of a subgroup, it is only necessary to prove that for any elements a, b in $H \cap K$, the elements a^{-1}, b^{-1}, and $a * b$ are in $H \cap K$, when $*$ denotes the operation.)

1.7 Fields

The group is important as a mathematical structure because so many sets in mathematics, considered with respect to a binary operation, are groups. The integers, the reals, and the complex numbers are all groups under addition, as is the set of integers (mod n). (See page 44.) The rational numbers form a group under addition and the non-zero rational numbers form a group under multiplication.

This *double* group structure of the rational numbers provides a system which is closed under the operations of addition, subtraction, multiplication, and division (excepting division by zero). Not only the rational numbers but the real numbers and the complex numbers have this double group structure. It would seem that this double group structure is a basic form for us to consider in connection with number systems. It is called a *field* and is defined as follows:

▶ We say that a set F with at least two elements is a field with respect to the two operations $+$ (addition) and $\cdot$ (multiplication) if the following three conditions are satisfied:

1. *F is a commutative group under addition.*
   This means that F must contain an additive identity, and also an additive inverse $-a$ for each element a. We often call the additive identity the zero element, or zero, and represent it by 0.
2. *The set of non-zero elements of F is a commutative group under multiplication.*
   There must be a non-zero element of F which is a multiplicative identity, and also a multiplicative inverse $\frac{1}{a}$ for each non-zero element a. We often call the multiplicative identity the unit element, or unity, and represent it by 1.
3. *The operation of multiplication is distributive over addition.*
   For all a, b, c in F, $a \cdot (b + c) = a \cdot b + a \cdot c$, or, with the usual notation, $a(b + c) = ab + ac$.

While strictly speaking the field consists of the set F and the operations $+, \cdot$, we often take the operations as understood and refer to the set as the field. Thus, we refer to the field of rational numbers and the field of real numbers.