Chapter 10

Operational Structures

10.1 Groups

A *group* $\mathbf{G}$ is an algebra which consists of a set G and a single binary operation, which we will usually write as $\circ$, but which may sometimes be written $+$ or $\times$: $\mathbf{G} = \langle G, \circ \rangle$. To be a group, $\mathbf{G}$ must satisfy the following conditions, the group axioms:

G1: $\mathbf{G}$ is an algebra (i e. $\circ$ completely defined and G closed under $\circ$).
G2: $\circ$ is associative.
G3: G contains an identity element.
G4: Each element in G has an inverse element.

Note that a group operation does not have to be commutative. A group whose operation is commutative is a *commutative* or *Abelian group*.

We are already acquainted with some models of these group axioms.

a. The positive rational numbers with multiplication form a group: (G1) the product of any two positive rationals is a unique positive rational, (G2) multiplication is associative, (G3) 1 is the identity element, and (G4) every positive rational p/q has an inverse q/p. Furthermore this group is Abelian since multiplication is commutative.

b. The integers $\{0, 1, 2, 3\}$ form a group with the operation of addition modulo 4. (The sum of x and y modulo 4 is the remainder after dividing $x + y$ by 4; e.g. $3 + 7 = 2$ (modulo 4)) The verification of this will be left to the reader.

c. The set of all even integers under addition forms a group, but the set of all odd integers does not, since it does not contain an identity element, and it is not closed under addition.

d. The group of 'symmetries of the square' is an example of a different sort, since the elements of the set for this group are not numbers but the following rigid motions of a square:

R - a 90° clockwise rotation about its center O
R' - a 180° clockwise rotation about its center O
R'' - a 270° clockwise rotation about its center O
I - a 360° clockwise rotation about its center O
H - a reflection in the horizontal axis through O
(i e flipping the square about the horizontal axis)
V - a reflection in the vertical axis through O
D - a reflection in the diagonal in quadrant I and III
D' - a reflection in the diagonal in quadrants II and IV

The group operation is the successive performing or composition of any of these motions: e g, $R \circ R = R'$. This group is not commutative, since, for instance, $R \circ H = D$ while $H \circ R = D'$.

The best way to compute the products of this group is to cut out a square of paper and label its sides so that the manipulations can actually be performed. First consider the front of the square:

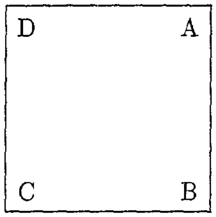

Figure 10–1.

Performing the operation defined as R will give the orientation shown in Figure 10–2:

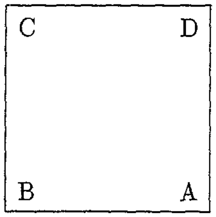

Figure 10–2.

Starting from the original orientation and performing R' gives the orientation shown in Figure 10–3; if we instead perform R'', the result is as shown in Figure 10–4.

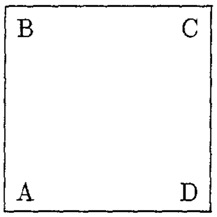

Figure 10–3.

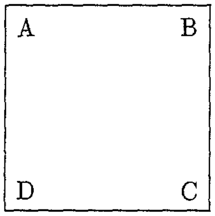

Figure 10–4.

Performing the operation I from the original starting point of Figure 10–1, or from any other configuration, does not change the orientation at all; in fact I is the identity operation for the group. The simplest way to keep track of these operations is to label the front of the square as in Figure 10–5.

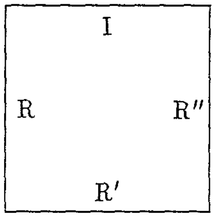

Figure 10–5.

At this point, the reader can verify such products as $R \circ R = R'$, $R \circ R' = R''$, $R' \circ R' = I$.

To label the back of the square, perform each of the reflections, starting each time from the I position, and label the side that comes out on top with the name of the operation. The relevant axes are as shown in Figure 10–6:

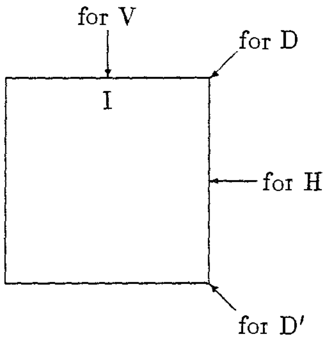

Figure 10–6.

The back of the square will then be labelled as in Figure 7, with V labelling the back of the same side that I labels on the front:

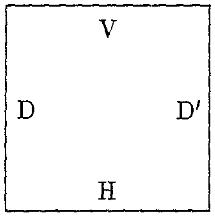

Figure 10–7.

Then the rest of the products can be verified; e.g., $H \circ R' = V$, $V \circ D = R$. Note that when you have, for instance, performed V and then want to perform D, you must find what is *then* the appropriate diagonal axis and reflect the square (i.e., turn it over) through that axis; the product is R, since the two operations in succession lead to the same orientation that R leads to directly.

It is recommended that such a square actually be constructed since this example recurs in several subsequent illustrations and problems.

From the group axioms we can prove the following elementary theorems.

THEOREM 10.1 *In any group, the equations $x \circ a = b$ and $a \circ y = b$ have the unique solutions $x = b \circ a^{-1}$ and $y = a^{-1} \circ b$ respectively* ■

Proof:

$$\begin{array}{rcll} (b \circ a^{-1}) \circ a & = & b \circ (a^{-1} \circ a) & \text{associativity} \\ b \circ (a^{-1} \circ a) & = & b \circ e & \text{def inverse} \\ b \circ e & = & b & \text{def identity} \end{array}$$

Hence $(b \circ a^{-1}) \circ a = b$, so $x = b \circ a^{-1}$ is a solution of $x \circ a = b$. It is also the unique solution, since

$$x = x \circ e = x \circ (a \circ a^{-1}) = (x \circ a) \circ a^{-1}$$

So if $x \circ a = b$, substitute b for $(x \circ a)$ in the last member of the equality above and observe that $x = b \circ a^{-1}$. Similarly for the unique solution $y = a^{-1} \circ b$ to $a \circ y = b$. ■

The theorem provides an answer to the following general question: Consider any two elements of a group, a and b (they need not be distinct); will it be possible to find in the group more elements x such that $x \circ a = b$? The theorem says that there will always be exactly one such an element, namely whatever element is obtained by performing the operation on b and the inverse of a.

The first part of the proof shows that $b \circ a^{-1}$ is indeed such an x, by putting $b \circ a^{-1}$ in for x in the product $x \circ a$ and showing from the group axioms that the result must indeed be b. But this does not show that $b \circ a^{-1}$ is the *only* such x. The second part of the proof does this, in an indirect way. First it is established that for *any* element x of a group, $x = (x \circ a) \circ a^{-1}$. Now consider an arbitrary element x for which $x \circ a = b$. (We know already that there is at least one such element, but so far there could be more than one) Then since $x = (x \circ a) \circ a^{-1}$ for *any* x, if we have an x for which $x \circ a = b$, we see that for such an x we can deduce $x = b \circ a^{-1}$; i.e., any solution of $x \circ a = b$ must be identical to the original solution, namely $b \circ a^{-1}$, which is to say that the solution is unique.

COROLLARY 10.1 *A group has only one identity element.* ■

Proof: By the group definition, there is at least one solution to $e \circ x = e$, i.e. $x = e$. By Theorem 10.1, this is the only solution. ■

COROLLARY 10.2 *A group has only one inverse a^{-1} for each element a* ■

Proof: By the group definition, there is at least one solution $y = a^{-1}$ to $a \circ y = e$. By Theorem 10 1, this solution is unique. ■

THEOREM 10.2 *A group with 4 or fewer elements must be commutative.* ■

Proof:
case (i): 1 element - trivial
case (ii): 2 distinct elements e and a,

$$e \circ a = a \circ e = a \text{ (identity)}$$

case (iii): 3 distinct elements e, a and b,

$$e \circ a = a \circ e = a \text{ (identity)}$$

$$e \circ b = b \circ e = b \text{ (identity)}$$

But $a \circ b \neq a$ because then b would equal e; and $a \circ b \neq b$ because then a would equal e; hence $a \circ b = e$. Similarly for $b \circ a$ hence $a \circ b = b \circ a = e$.

case (iv): 4 distinct elements e, a, b and c,

$$e \circ a = a \circ e = a, e \circ b = b \circ e = b \text{ and } e \circ c = c \circ e = c \text{ (identity)}$$

Consider any two non-identity elements, e.g. a and b. The product $a \circ b$ cannot be either a or b, as above. If $a \circ b = e$, then $b = a^{-1}$ and hence $b \circ a = e$ also. If $a \circ b = c$, then $b \circ a$ cannot be a or b (violation of uniqueness of identity element), or e; in the last case b would be the inverse of a, so $a \circ b = e$, but we already have $a \circ b = c$. Hence $b \circ a = c$ also. In either case the group is commutative. ■

From the fact that the theorem only mentions up to 4-member groups, it should not be inferred that groups with 5 or more members may be non-commutative. In fact, it is provable, but tedious, that all 5-member groups must also be commutative. Groups with 6 or more members need not be commutative, however.

The operation on a finite group is often given by a matrix. Rows and columns are labelled with members of the set. The value of $a \circ b$ is placed in the cell at the a^{th} row and the b^{th} column. Because of its similarity to the multiplication table of the natural numbers less than 10, such a matrix is generally referred to as a 'multiplication table'. Finding the value of $a \circ b$ is called 'multiplying a by b' even when the operation bears no resemblance to the operation of multiplication A word of caution: when constructing an example of a finite group by its multiplication table, it is quite easy to check for closure, the identity element and inverses by direct inspection of the table. It is also straightforward to tell from the table whether a group is commutative or not, i.e the table is symmetric around the diagonal. But a group operation must also be associative, and there is no simple way to check associativity by inspection of the table; rather, one has to check each instance of the operation

10.2 Subgroups, semigroups and monoids

We define a subgroup G' as a subalgebra of G which is itself a group We give the following examples of subgroups as illustration.

a. The group of even integers with addition is a proper subgroup of the group of all integers with addition.

b. The group of all rotations of the square $\langle\{I, R, R', R''\}, \circ\rangle$ where $\circ$ is composition of operations as described above, is a subgroup of the group of all symmetries of the square as in Example (d) above.

c. The system $\langle\{I, R, R'\}, \circ\rangle$ is *not* a subgroup of the group of all symmetries of the square; it is not a group and it is not even a subalgebra of the original group, because the given set $\{I, R, R'\}$ is not closed under the operation $\circ$.

d. The set of all non-negative integers with addition is a *subalgebra* of the group of all integers with addition, because the non-negative integers are closed under addition. But it is not a *subgroup* because it is not itself a group: it is associative, and has an identity element (0), but all of the members of the set except 0 lack inverses.

The *order* of any group **G** is the number of members in the set G. An important theorem of group theory states that the order of any subgroup exactly divides, i e. without remainder, the order of the parent group. For instance, only subgroups of order 1, 2 and 4 are possible for a 4-member group, these being the integral divisors of 4. The theorem does not guarantee that every subset having the proper number of members will give rise to a subgroup – only that if a subgroup exists, its order is a divisor of the order of the group. An immediate consequence of this theorem is that a group **G** of order 5 has only the trivial subgroups of order 1 (the identity element itself) and of order 5 (itself) as subgroup, since 5 has no other divisors.

A second theorem, of which we omit the proof since it uses notions that are not introduced here, states that if a group is *finite*, then all its non-empty subalgebras are also subgroups The practical consequence of this theorem is that in checking whether a given system is a subgroup of a finite group, one only needs to verify that the given subset is not empty and is closed under the group operation, i.e. is a subalgebra. If these two conditions are met, there will necessarily be an identity element and inverses for each element. Example (b) above is such a case. Example (d) above shows the failure of a subalgebra to be a subgroup in an infinite case.

A third theorem about subgroups will be proven here.

THEOREM 10.3 *The intersection* $\mathbf{G}' \cap \mathbf{G}''$ *of two subgroups* $\mathbf{G}'$ *and* $\mathbf{G}''$ *of a group* **G** *is itself* a *subgroup of* **G**. ■

Proof:

(i) If a, b are in $\mathbf{G}' \cap \mathbf{G}''$, they must both be in both $\mathbf{G}'$ and $\mathbf{G}''$. $\mathbf{G}'$ and $\mathbf{G}''$ are groups, so $a \circ b$ is in both, hence $a \circ b$ is in $\mathbf{G}' \cap \mathbf{G}''$.

(ii) If a is in $\mathbf{G}' \cap \mathbf{G}''$, it is in both $\mathbf{G}'$ and $\mathbf{G}''$. $\mathbf{G}'$ and $\mathbf{G}''$ are groups, so a^{-1} is in both, hence $\mathbf{G}' \cap \mathbf{G}''$ must contain a^{-1}.

(iii) Since $\mathbf{G}'$ and $\mathbf{G}''$ are groups, they both contain e; hence $\mathbf{G}' \cap \mathbf{G}''$ must contain e. ■

There are some useful algebraic structures which are weaker than groups and satisfy only some of the group axioms.

A *semigroup* is defined as an algebra which consists of a set and a binary associative operation $(G1 + G2)$. There need not be an identity element nor inverses for all the elements.

A *monoid* is defined as a semigroup which has an identity element ($G1$, $G2, G3$). There need not be inverses for all the elements. An *Abelian monoid* is a monoid with a commutative operation.

Given these definitions, any group is a subgroup of itself, and a semigroup and a monoid as well. Every monoid is a semigroup, but not vice versa. Here are some telling examples.

a. The set of all non-negative integers with addition is an Abelian monoid.

b. The set of all positive integers (excluding zero) with addition is a semigroup but not a monoid.

Since both ordinary addition and ordinary multiplication are associative, it can be deduced that addition and multiplication modulo any n are also associative. Therefore any system with addition or multiplication, either ordinary or modulo some n, is a semigroup if it is closed and is a monoid if it also contains the appropriate identity element 0 or 1.

c. The set of all positive even integers with ordinary multiplication is a semigroup but not a monoid, since 1 is missing.

d. The set of all positive odd integers with ordinary multiplication is a monoid. (Closed since multiplication of odd integers yields only odd integers)

e. The set $\{0, 1, 2, 3, 4\}$ with multiplication modulo 5 is a monoid.

f. The set of all multiples of 10 which are greater than 100, i.e.

$$\{110, 120, 130, \ldots\}$$

with ordinary addition is a semigroup, but not a monoid.

None of the above examples are groups; in each example, one or more elements lack inverses. Note that where multiplication (modulo n) is involved no system which contains 0 can be a group, since 0 has no multiplicative inverse.

Submonoids are defined analogously to subgroups. $\mathbf{M}$ is a submonoid of the monoid $\mathbf{M}'$ iff $\mathbf{M}$ is a monoid and its identity element is the same as in $\mathbf{M}'$. The stipulation that the identity elements must be the same is not necessary for subgroups, since there it is an automatic consequence. It is possible to find subsets of a monoid that themselves form monoids, however, but with different identity elements.

10.3 Integral domains

An *integral domain* $\mathbf{D}$ is an algebra consisting of a set D and two binary operations called ‘addition’ and ‘multiplication’, written $a + b$ and $a \cdot b$, respectively; $\mathbf{D} = \langle D, +, \ \rangle$, which satisfies the following axioms:

D1: $\mathbf{D}$ is an algebra.
D2: The set D with the operation $+$ forms an Abelian group with identity 0.
D3: The set D with the operation $\cdot$ forms an Abelian monoid with identity 1, and $1 \neq 0$
D4: (Cancellation Law) If $c \neq 0$ and $c \cdot a = c \ \ b$, then $a = b$
D5: (Distributive Law) For all a, b, c in D, $a \cdot (b + c) = (a \cdot b) + (a \ \ c)$.

The assumption in D3 that $1 \neq 0$ eliminates the ‘trivial’ case of the set containing only 0, which would otherwise be an integral domain under ordinary addition and multiplication Axiom D4, which says that multiplication obeys the cancellation law except in the case of the additive identity 0, in effect recaptures a great deal of the structure lost by not requiring multiplicative inverses In fact, whenever D is a *finite* set, Axiom D4 insures that every element except 0 has a multiplicative inverse

Note that the distributive law is not symmetric between $\cdot$ and $+$; it will not in general be true that $a + (b \cdot c) = (a + b) \ \ (a + c)$. Aside from the requirement that $1 \neq 0$, the distributive law is the only axiom which requires there to be some connection between the two operations Because integral domains have two operations, we need to introduce some new notation for inverses In a group, where there is only one operation, a^{-1} unambiguously designated the inverse of a with respect to the given operation For integral domains, we will use a^{-1} to designate the multiplicative inverse of a (if it has one; since not all elements need have inverses, this notation can be used only where it can be shown that an inverse exists). We will introduce the notation $-a$ to stand for the additive inverse of a, which by D2 always exists. Thus by definition $-a$ is the element which when added to a gives 0. For all of the infinite models mentioned below, this notation corresponds to our ordinary use of the minus sign, but it would be advisable to regard that correspondence as accidental (although clearly it is not) and throughout this section simply read ‘$-a$’ as ‘the additive inverse of a’.

In integral domains, as in ordinary arithmetic, the minus sign is also used as a binary operator, corresponding to the operation of subtraction.

We can define $b - a$ as that element x such that $x + a = b$ By Theorem 10.1 for groups the equation $x + a = b$ has the unique solution $b + (-a)$, so the operation $b - a$ is well defined. Thus the two uses of the minus sign are closely related We could also have defined subtraction first, and then define $-a$ as $0 - a$ There is never any ambiguity, since subtraction is a binary operation, whereas the sign for the additive inverse is always prefixed to a single element

The standard model of an integral domain is the set of all integers, positive, negative and 0, with ordinary addition and multiplication. Other examples of infinite integral domains are the set of all rational numbers and the set of real numbers, again with ordinary addition and multiplication. A less obvious model is the set of all rational numbers whose denominator is 1 or a power of 2. Still other models can be constructed. None of these sets form a group with multiplication, because there is no multiplicative inverse for 0 in any of them, i.e no number which when multiplied by 0 gives 1. In the domain of the rationals or of the reals, 0 is the only element without a multiplicative inverse; in the domain of the integers, however, none of the elements except 1 itself has a multiplicative inverse.

In Section 8 5.5, we introduced an axiomatic characterization of several types of orderings for sets in general. Here we will show a different approach to a linear or simple ordering which can be used only for integral domains, since it makes use of the notions of addition and multiplication. The relation $\leq$ as defined below is a simple linear ordering, although we will not prove that assertion here.

Not all integral domains can be ordered; thus the ordered integral domains are a much more restricted class of systems that the integral domains. More restricted still are the ordered integral domains whose positive elements (to be defined below) are well-ordered. These integral domains in fact turn out to be isomorphic to the set of all integers with ordinary addition and multiplication and, of course, to each other. For this reason, these notions of ordering are of central importance in characterizing axiomatically our ordinary system of arithmetic with integers.

DEFINITION 10.1 *An integral domain* $\mathbf{D}$ *is said to be ordered by a relation* $\leq$ *if the following axioms hold:*

(i) Addition law. *For all a,b,c and d if* $a \leq b$ *and* $c \leq d$, *then* $a + c \leq b + d$

(ii) Multiplication law. *If* $a \leq b$ *and* $0 \leq c$, *then* $a \cdot c \leq b \cdot c$

(iii) Law of trichotomy. *For any a and b, one and only one of the following holds: $a < b$, $a = b$, or $a > b$ (also called connectedness).*

■

We have already shown that subtraction can be defined in any integral domain: $b - a$ is equal to $b + (-a)$. We now make use of subtraction to define the properties of being *positive* or *negative* for elements of ordered integral domains.

DEFINITION 10.2 *An element a of an ordered integral domain is* positive *if and only if $a > 0$; a is* negative *if and only if $a < 0$. The three basic axioms for the* ordering relation $<$ *are reflected by three similar properties of positive elements:*

(i′) Addition. *The sum of two positive elements is positive.*

(ii′) Multiplication. *The product of two positive elements is positive.*

(iii′) Trichotomy. *For any given element a, one and only one of the following holds: a is positive, $a = 0$ or $-a$ is positive.*

■

The proof of these is left to the reader.

As remarked above, not all integral domains can be ordered. Among the integral domains which can be ordered are the familiar infinite ones: the set of integers, or the set of all rational numbers, or the set of all real numbers, all with ordinary addition and multiplication and $\leq$ interpreted as 'less than or equal to' in the usual sense. If we add to the axioms for ordering a further axiom for well-ordering for positive elements only, we will have a formal system all of whose models turn out to be isomorphic to the integers with respect to addition, multiplication and $\leq$.

DEFINITION 10.3 *A subset S of an ordered integral domain is* well-ordered *if each non-empty subset S' of S contains a smallest element, i.e. an element a such that $a < x$ for every x in S'.* ■

The new axiom for well-orderings, which depends on the prior introduction of the axioms for orderings and on the definition of 'positive' already given, can be stated as follows:

Well-ordering axiom: The positive elements are well-ordered.

To illustrate the use of the well-ordering principle, we prove that in any well-ordered integral domain, there is no element between 0 (the additive identity) and 1 (the multiplicative identity) For the standard model, namely the integers, the theorem may seem obvious, but it is not so obvious how to prove it from the axioms for the well-ordered integral domains

THEOREM 10.4 *There is no element between 0 and 1 in any well-ordered integral domain.* ■

Proof: Assume, for a *reductio ad absurdum* proof, that there is at least one element c with $0 < c < 1$, i.e. the class of such elements is not empty. By the well-ordering axiom, there is a *least* element m in this class, and $0 < m < 1$, so $0 < m$ and $0 < (1-m)$. By the multiplication law for positive elements of an ordered integral domain, $0 < m \cdot (1-m)$, i.e. $0 < m - m^2$, so $m^2 < m$. By the same axiom, $0 < m \cdot m$, i.e. $0 < m^2$ Then by the transitivity of $<$, $0 < m^2 < m < 1$. The m^2 is another element in the class of elements between 0 and 1, which is, moreover, smaller than m. But m was by definition the minimum element in the class, (contradiction!). So there is no element between 0 and 1. ■

THEOREM 10.5 *A set S of positive integers which includes 1, and which includes $n+1$ whenever it includes n, includes every positive integer.* ■

Proof: We will prove by *reductio ad absurdum* that the set S', consisting of those positive integers not in S, is empty. Assume that S' is not empty, then it contains a least element m. But $m \neq 1$ by hypothesis. By Theorem 4 there is no positive integer smaller than 1, so $m > 1$. That means $m - 1$ is positive. Since m is the smallest positive integer not in the set S, $m - 1$ is in the set S, since $m - 1 < m$. Then, by hypothesis, $(m-1)+1$ is also in S, but $(m-1)+1 = m$, so m in in S. Contradiction! ■

We can now prove directly that Peano's fifth postulate (see Sections 8.4 and 8 5.7) holds for the positive integers.

Principle of Finite Induction. Associate with each positive integer n a statement $P(n)$ which is either true or false. If (i) $P(1)$ is true, and (ii) for all k, $P(k)$ implies $P(k+1)$, then $P(n)$ is true for all positive integers n.

Proof: The set of those integers k for which $P(k)$ is true satisfies the hypothesis, and hence the conclusion of Theorem 10.5. ■

To illustrate the application of the principle of finite induction in proofs, we will use it to prove one of the laws of exponents in integral domains, for which we first need to give a definition.

DEFINITION 10 4 *A positive power a^n of a in any integral domain D is defined recursively by (i) $a^1 = a$, (ii) $a^{n+1} = a^n \cdot a$.* ■

Using this definition, we can prove by induction that in any integral domain $(a \cdot b)^n = a^n \cdot b^n$ for all n. First of all, we view the statement of the theorem as expressing a property of n; $P(n) = (a \cdot b)^n = a^n \ b^n$. This is the first step in setting up any proof by induction, but it is often left implicit.

The proof itself has two parts: first we prove $P(1)$, and then we prove that for arbitrary k, $P(k)$ implies $P(k+1)$.

$$\begin{array}{llrcll}
(i) & P(1): & & & & \\
 & & (a \cdot b)^1 & = & a \cdot b & \text{by definition} \\
 & & & = & a^1 \ b^1 & \text{by definition} \\
(ii) & P(k) \rightarrow P(k+1): & & & & \\
 & & (a \cdot b)^k & = & a^k \cdot b^k & \text{cond. premise} \\
 & & (a \cdot b)^{k+1} & = & (a \cdot b)^k \cdot (a \cdot b) & \text{by definition} \\
 & & & = & (a^k \cdot b^k) \cdot (a \cdot b) & \text{cond. premise} \\
 & & & = & a^k \cdot (b^k \cdot (a \cdot b)) & \text{associativity} \\
 & & & = & a^k \cdot ((b^k \cdot a) \cdot b) & \text{associativity} \\
 & & & = & a^k \cdot ((a \cdot b^k) \cdot b) & \text{commutativity} \\
 & & & = & a^k \cdot (a \cdot (b^k \cdot b)) & \text{associativity} \\
 & & & = & (a^k \cdot a) \cdot (b^k \cdot b) & \text{associativity} \\
 & & & = & a^{k+1} \cdot b^{k+1} & \text{by definition} \\
 & \multicolumn{4}{r}{[(a \cdot b)^k = a^k \cdot b^k] \rightarrow [(a \cdot b)^{k+1} = a^{k+1} \cdot b^{k+1}]} & \text{cond proof}
\end{array}$$

From (i) and (ii) it follows by the principle of finite induction that $P(n)$ is true for all positive integers n, i.e. that for all positive n, $(a \cdot b)^n = a^n \cdot b^n$.

We have introduced here the well-ordering principle, and hence induction, for the positive integers. An alternative approach is to state both the well-ordering principle and induction for the non-negative integers, in which case the first step in an induction proof would be for the case of $n = 0$. The two approaches are interdefinable.

10.4 Morphisms

Since the notions of homomorphism and isomorphism are defined for algebras in general, it is possible to define a morphism between algebras of different sorts, as long as they have the same number of operations. Here we give an example of a homomorphism between a monoid and a group, and then discuss some group isomorphisms and an isomorphism between two integral domains.

Consider the monoid $\mathbf{M} = \langle N, +\rangle$ consisting of all the non-negative integers with the operation of ordinary addition $\mathbf{M}$ is not a group because of the absence of inverses. Let the group $\mathbf{G} = \langle G = \{0, 1, 2, 3, 4\}, + \text{ mod } 5\rangle$. We can define a homomorphism from $\mathbf{M}$ to $\mathbf{G}$ by the function $F(n)$ which maps each non-negative integer in N onto the element of G which is congruent with it modulo 5 (Numbers which are congruent mod 5 leave the same remainder after division by 5) For example, $F(16) = 1$, $F(23) = 3$, $F(45) = 0$, etc. The function F establishes a homomorphism, since $F(x) + F(y)$ ((mod 5)) $= F(x + y)$. The *kernel* of a homomorphism F is defined as the set of elements of the domain of F which are mapped onto the identity element in the range of F In this example, the kernel of the homomorphism $F : \mathbf{M} \rightarrow \mathbf{G}$ is the set of all non-negative multiples of $5 : \{0, 5, 10, 15, \ldots\}$.

The definition of isomorphisms for groups is a direct application of the definition of isomorphisms for algebras in general. Since a group has only one operation, we can say simply that an isomorphism between two groups $\mathbf{G} = \langle G, \circ\rangle$ and $\mathbf{G}' = \langle G', \circ'\rangle$ is a one-to-one correspondence between their elements which preserves the group operation, which may be distinct operations in the two groups. I.e., if a is mapped to a', and b to b' and vice versa, then $a \circ b$ is mapped to $a' \circ' b'$ and vice versa. Putting it more formally, an isomorphism between two groups $\mathbf{G} = \langle G, \circ\rangle$ and $\mathbf{G}' = \langle G', \circ'\rangle$ is a one-to-one correspondence $F : \mathbf{G} \rightarrow \mathbf{G}'$ such that for all x, y in G, $F(x) \circ' F(y) = F(x \circ y)$. Here are two examples of such group isomorphisms.

Example 1: The group of integers $\{1, 2, 3, 4\}$ under multiplication modulo 5 is isomorphic with the group of the integers $\{0, 1, 2, 3\}$ under addition modulo 4, with the correspondence

$$1 \longleftrightarrow 0, 2 \longleftrightarrow 1, 3 \longleftrightarrow 3, 4 \longleftrightarrow 2$$

This is best illustrated by the group tables

+ (mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

× (mod 5)	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Example 2: The group of integers $\{0,1,2,3\}$ under addition modulo 4 is also isomorphic with the group of rotations of the square: let

$$0 \longleftrightarrow I, 1 \longleftrightarrow R, 2 \longleftrightarrow R', 3 \longleftrightarrow R''$$

We can prove that isomorphisms are equivalence relations on the set of all groups.

THEOREM 10.6 *The relation 'is isomorphic to' is a reflexive, symmetric and transitive relation between groups.* ■

Proof: The reflexive property is trivial, since every group is isomorphic to itself by the identity mapping. As for the symmetric property, let F be an isomorphic correspondence between G and G'. Since F is one-to-one, it has an inverse F^{-1} which is an isomorphism of G' onto G Finally, if F_1 maps G isomorphically onto G', and F_2 maps G' isomorphically onto G'', then the composition of $F_2 \circ F_1$, the function whose value for a given argument a is the value of F_2 applied to $F_1(a)$, is an isomorphism of G with G''. ■

An isomorphism between two integral domains **D** and **D**$'$ is a one-to-one correspondence of the elements a of D with the elements a' of D', which satisfies for all elements a, b in D the conditions

1) $(a+b)' = a' + b'$

2) $(a \cdot b)' = a' \cdot b'$

For an example of an isomorphism between two integral domains, let us start from the following facts about reckoning with even and odd numbers.

even + *even* = *odd* + *odd* = *even*
even + *odd* = *odd* + *even* = *odd*
even · *even* = *even* · *odd* = *odd* · *even* = *even*
odd · *odd* = *odd*

We can regard these identities as definitions of operations of 'addition' and 'multiplication' in a new algebra of the two elements 'even' and 'odd'. This algebra is isomorphic to the finite integral domain $\mathbf{I_2}$ of integers modulo 2, with ordinary addition and multiplication modulo 2, under the correspondence *even* $\longleftrightarrow$ 0 and *odd* $\longleftrightarrow$ 1.

Exercises

1. Show that the integers 0,1,2, and 3 form a group with the operation of addition modulo 4, i e. show that each of the four group axioms is satisfied. You need not give a full demonstration of associativity—just 2 or 3 examples.

2. Which of the following are groups?

(a) The integers 1,3,5,7,8 under multiplication modulo 11.

(b) The integers 1,3,4,5,9 under multiplication modulo 11.

(c) The system described by the following multiplication table:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	a
d	d	c	b	b

(d) The system described by the following table:

$\circ$	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

(e) The set of all subsets of $S = \{x_1, x_2\}$ with the operation of set union.

(f) The same set S as in (e) with the operation of set intersection.

(g) The set of rigid motions of a square $\{I, H, V, R'\}$ and the operation of performing them successively.

(h) The set of rigid motions of a square $\{I, D, R\}$ and the operation of performing them successively.

3. (a) Draw the group operation table for the group of symmetries of the square $\{I, R, R', R'', H, V, D, D'\}$

   (b) There are three different subgroups having exactly four elements. Find them and draw their group operation tables

   (c) There are five different subgroups having exactly two elements. Find them and draw their tables.

   (d) Show which of the subgroups in (b) are isomorphic

   (e) Show a non-trivial automorphism for one of the subgroups of (b).

   (f) Show a homomorphism of one of the subgroups of (b) with one of the subgroups of (c).

4. Prove that the set consisting of the identity element alone is a subgroup for any group

5. (a) Does the set $\{1, 2, 3, 4, 5\}$ form a group with multiplication modulo 6? Justify your answer

   (b) Show that the set $\{1, 2, 3, 4, 5, 6\}$ forms a group with multiplication modulo 7.

   (c) Find three different proper subgroups of the group in (b).

   (d) Find a set of integers which forms a group with *addition* modulo some n which is isomorphic to the group in (b).

   (e) Can you find a general condition on n which will identify all those n's for which the set $\{1, 2, \ldots, n-1\}$ forms a group with multiplication modulo n? Prove your assertion if possible, otherwise explain why you think it is correct.

6. Prove that if $\mathbf{S}$ is a subgroup of $\mathbf{S}'$ and $\mathbf{S}'$ is a subgroup of $\mathbf{S}''$, then $\mathbf{S}$ is a subgroup of $\mathbf{S}''$.

7. (a) The set R of all strictly positive rational numbers with multiplication forms a monoid which is also a group. Find a *sub*-monoid R_0 of R such that R_0 is *not* a group.

   (b) Is the set of all rational numbers with multiplication a semigroup? A monoid? A group?

8. Determine whether the set-theoretic operation 'symmetric difference' is commutative, associative and idempotent. Is there an identity element for this operation? What sets, if any, have inverses? Given the set

$A = \{a, b\}$ what sort of operational structure is formed by the powerset of A with the operation of symmetric difference?

9. Let $A = \{a, b\}$ Show that $\langle \wp(A), \cup \rangle$ and $\langle \wp(A), \cap \rangle$ are both semigroups but not groups Find an isomorphism between them

10. (a) Prove that if a, b and c are any elements of an integral domain **D**, then $a + b = a + c$ implies $b = c$. (Hint: make use of the fact that a has an additive inverse.)

(b) Prove that for all a in D, $a \circ 0 = 0 \circ a = 0$. (Hint: Use $a + 0 = a$ and the distributive law to prove that $a \circ (a + 0) = a \circ a$ and $a \circ (a + 0) = (a \circ a) + (a \circ 0)$. Note: $\circ$ is used here for 'multiplication'.)

(c) Justify each step in the following proof of $(-a) \circ (-b) = a \circ b$. (Note: $-a$ and $-b$ are names given to the additive inverses of a and b).

(1) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ b + [a \circ (-b) + (-a) \circ (-b)]$

(2) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ b + [a + (-a)] \circ (-b)$

(3) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ b + 0 \circ (-b)$

(4) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ b$

(5) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ [b + (-b)] + (-a) \circ (-b)$

(6) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = a \circ 0 + (-a) \circ (-b)$

(7) $[a \circ b + a \circ (-b)] + (-a) \circ (-b) = (-a) \circ (-b)$

(8) $(-a) \circ (-b) = a \circ b$

11. Prove the law of transitivity for $<$ in an ordered integral domain, i.e. for any a,b, and c, if $a < b$ and $b < c$ then $a < c$.

12. Using the definition of positive elements, deduce the three basic laws of positive elements, (i′), (ii′) and (iii′) in Def 10.2, from the laws for $<$.

13. The definition of any positive power a^n of a in any integral domain **D** is given by:

$$\begin{aligned} a^1 &= a \\ a^{n+1} &= a^n \circ a \end{aligned}$$

(a) Prove by induction that $a^m \circ a^n = a^{m+n}$ in any integral domain. (Hint: Use induction on n; in the second part of the induction, assume that $a^m \circ a^n = a^{m+n}$ for all m and for $n = k$ and prove that it must then hold for all m and for $n = k + 1$).

(b) Prove by induction that in any integral domain $(a^m)^n = (a^n)^m$. (Hint: You will probably want to make use of the theorem that $a^n \circ b^n = (a \circ b)^n$ which was proven in this chapter)