SOME ABSTRACT ALGEBRA – A PRIMER

Richard Grassl

University of Northern Colorado

School of Mathematical Sciences

richard.grassl@unco.edu

CLOSURE

We say that a binary operation □ on a set S is CLOSED if whenever a and b are any two elements in S then a □ b is also in S. For example, the operation + is closed on the set S = Z = {0, ±1, ±2...} since a + b is in Z. But subtraction is not closed on the set N = {0, 1, 2, 3, ...} since 1 – 3 = -2 is not in N.

The following gives the two part procedure for determining if a particular set S is closed under a particular binary operation □ :

1. Choose two arbitrary elements from S; label them a, b.
2. Show that a □ b is a number of S.

EXAMPLE. The set E = {0, 2, 4, 6, ...} is closed under addition. Let a=2m and b=2n be arbitrary elements of E. Then since 2m + 2n = 2(m+n) is an even integer the sum of 2m and 2n is in E. E is also closed under multiplication since (2m)(2n) = 4mn = 2(2mn) is even.

PROBLEMS

In each of the following if the set is closed under the operation give reasons (actually a proof); if not, provide a counterexample.

1. Is A = {0, 1, 4, 9, 16, ...} closed
   a. under addition? b. under subtraction? c. under multiplication?
2. Is B = {0, ±5, ±10, ±15, ...} closed
   a. under addition? b. under multiplication?
3. Is C = {0, 2, 4, 6}, a finite set, closed under addition?
4. Is D = {1, 3, 5, 7, ...} closed
   a. under addition? b. under multiplication?
5. Is E = { 1, 4, 7, 10, 13, ...}, the positive integers having remainder 1 upon division by 3, closed
   a. under addition? b. under multiplication?

6. Repeat #5 with F = {2, 5, 8, 11, 14, ...}.
7. The set G = {0, ±4, ±8, ±12, ...} is closed under subtraction. Give another set H that is closed under subtraction. Show that G ∩ H is also closed under subtraction.
8. Is the set of all rational numbers of the form 2^n, where n is in Z, closed under multiplication?
9. Is the set of all positive rational numbers closed under addition? Under multiplication?
10. Let I = $\{2^m \cdot 3^n$: m, n are in Z$\}$. Is I closed under multiplication?
    Hint: Is 3/8 in I? Is 1/9 in I?
11. Are the irrationals closed under multiplication?
12. Prove that if S and T are sets of integers closed under subtraction so is the intersection S ∩ T. Is the union of S and T also closed under subtraction?
13. Why does 0 always have to be a member of any set that is closed under subtraction?

UNITS MULTIPLICATION

Under units multiplication the product of any two positive integers, denoted a □ b, is the units digit of the product under ordinary multiplication. So, 5 □ 9 = 5, 7 □ 8 = 6.

14. Is the set {0, 2, 4, 6, 8} closed under units multiplication?
15. Is the set {1, 3, 7, 9} closed under units multiplication?
16. Is {1, 4, 6} closed under units multiplication? How about the set {2, 4, 8}? How about {1, 5, 9}?
17. What would you have to add to the set {1, 3, 5} to make it closed under units multiplication?

BINARY OPERATIONS

The concepts of being commutative and associative are usually introduced to students as they study the four basic arithmetic operations of addition, subtraction, multiplication and division of integers. These four operations denoted by +, −, ×, ÷ are examples of binary operations.

Let S be any set. A binary operation on *S* is a function $f : S \times S \rightarrow S$. Sometimes a binary operation is depicted using the infix notation $(m, n) \rightarrow m \square n$, rather than the prefix notation $f(m, n)$. The following are examples of binary operations on $N = \{0, 1, 2, 3, \ldots\}$.

OPERATION	INFIX NOTATION
$f(m, n) = m + n$	$m \square n = m + n$
$f(m, n) = mn$	$m \square n = mn$
$f(m, n) = GCD(m, n)$	$m \square n = GCD(m, n)$
$f(m, n) = 5^m \cdot n$	$m \square n = 5^m \cdot n$

Additional binary operations that will be of importance include

$$f(x, y) = x \div y \text{ on } S = \text{Reals}$$

$$f(m, n) = m - n \text{ on } S = Z = \{0, \pm 1, \pm 2, \ldots\}$$

$$f(m, n) = m + n - mn \text{ on } S = Z$$

$$f(m, n) = m + n - 1 \text{ on } S = Z$$

$$f(A, B) = A \cup B \text{ on } P(S) \text{ for } S = \{a, b, c\}$$

$$f(A, B) = A \cap B \text{ on } P(S) \text{ for } S = \{a, b, c\}$$

Here, $\cup$ denotes union, and $\cap$ denotes intersection. Also, P(S), the power set for S, is the set of all subsets of S. As an example, if $S = \{a, b\}$, then $P(S) = \{\varphi, \{a\}, \{b\}, \{a, b\}\}$.

PROPERTIES OF BINARY OPERATIONS

Binary operations on a set X may or may not satisfy the following properties:

Commutativity: $x \square y = y \square x$ for all x, y in X.

Associativity: $x \square (y \square z) = (x \square y) \square z$ for all x, y, z in X.

Identity: An element $e \in X$ such that $x \square e = e \square x = x$ for all x in X is called an identity for the binary operation $\square$.

Inverses: If e is an identity under $\square$, an inverse of an element a in X is an element b in X such that $a \square b = e = b \square a$.

Example 1. The operation + on Z is associative since $a + (b + c) = (a + b) + c$ for all a, b, c in Z. Since $a + b = b + a$, + is commutative. The element 0 serves as an identity e since

$0 + a = a + 0 = a$. Each element $a \in Z$ has an inverse, namely -a.

One important characterization or consequence of the notation $f : A \times A \to A$ is that the result f (m, n) or $m \square n$ must be an element in A; i.e., A must be closed under the binary operation $\square$. So divisibility, denoted ÷, is not a binary operation on N = {0, 1, 2, ... } since $m \div n = \frac{m}{n}$ is not necessarily an integer. But ÷ is a binary operation on the set R^+ of positive real numbers. Notice that since $2 \div 3 \neq 3 \div 2$, ÷ is not commutative.

Let's return to the binary operation $m \square n = 3^m \cdot n$ on N = {0, 1, 2, ... }, and show that $\square$ is not associative. The following single example accomplishes this:

$$1 \square (0 \square 1) = 1 \square 1 = 3 \text{ but } (1 \square 0) \square 1 = 0 \square 1 = 1.$$

Does $\square$ have an identity? It might be natural to try 0 or 1. Since $0 \square n = n$ but $n \square 0 = 0$, 0 is not an identity. Since $1 \square n = 3n$, 1 is not an identity. No other element in N works either; without an identity, there are no inverses.

Example 2. Union, ∪, is a binary operation on P(S) where S = {a, b, c}. Since

$A \cup (B \cup C) = (A \cup B) \cup C$, ∪ is associative. Since $\varnothing \cup A = A = A \cup \varnothing$ for all $A \in P(S)$, the empty set $\varnothing$ serves as an identity.

When the set A is finite, a binary operation $\square$ can be given by a matrix table where the element $x \square y$ is found at the intersection of row x and column y.

Example 3. Let $A = \{1, 3, 7, 9\}$ and let $x \square y$ be the digit in the units position upon ordinary multiplication of x and y. This is sometimes written as $x \square y \equiv xy \pmod{10}$. The matrix table is

□	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

This binary operation $\square : A \times A \to A$ is associative (you need to check $4 \cdot 4 \cdot 4 = 64$ cases), is commutative (from the symmetry of the table), has identity 1, and each element has an inverse as shown in the following table:

x	1	3	7	9
inverse of x	1	7	3	9

Example 4. The binary operation ∘ on A = {e, a, b} given by the table is associative, commutative, and has e as an identity. In the exercises you are asked to find inverses.

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

□	1	2	5	10
1	1	1	1	1
2	1	2	1	2
5	1	1	5	5
10	1	2	5	10

Example 5. Let A = {1, 2, 5, 10} and m □ n = GCD(m, n), the greatest common divisor of m and n. The matrix table for □ is given. With some effort, you can show that □ is associative. The table's symmetry verifies that the operation □ is commutative. In the exercises, you are asked to determine an identity and to see if there are inverses.

"AN" IDENTITY VERSUS "THE" IDENTITY

Throughout this discussion of properties we have been saying “an“ identity. Here is some good news! We can replace “an” with “the” whenever an identity exists.

THEOREM: If the binary operation □ on X has an identity, then it is unique.

PROOF: Proceed using a proof by contradiction. Suppose there are two different identities; call them *e* and *f*.

Since $x \square e = x = e \square x$ for all x in X, it must hold for $x = f$, i.e., $f \square e = f = e \square f$.

Since $x \square f = x = f \square x$ for all x in X, it must hold for $x = e$, i.e., $e \square f = e = f \square e$.

But then $e \square f = f$ and $e \square f = e$, or $e = f$ contradicting the fact that they were different.

Similarly inverses are unique. Let e be the identity for an associative operation $\circ$ on X, and let g and h be two inverses for some a in X. Then $g = g \circ e = g \circ (a \circ h) = (g \circ a) \circ h = e \circ h = h$. You should give reasons for each step.

MEET AND JOIN

There are two binary operations on **B** = {0, 1} that are basic in computer design and operation. The meet ∧ and join ∨ operations are given by the tables below.

∧	0	1
0	0	0
1	0	1

∨	0	1
0	0	1
1	1	1

The meet operation is similar to intersection ∩ and join is similar to union ∪ , and behave like the logical connectives "and" and "or," respectively. Each of ∧ and ∨ are commutative and associative. Are there identities, inverses?

BITWISE ADDITION MODULO 2

Another binary operator having applications in coding theory is based on the table below.

$\oplus$	0	1
0	0	1
1	1	0

Here, $a \oplus b$ is 0 if $a + b$ is even and $a \oplus b = 1$ if $a + b$ is odd. Equivalently, $a \oplus b = 0$ if $a = b$, and $a \oplus b = 1$ if $a \neq b$. The binary operation $\oplus$ on $\boldsymbol{B} = \{0, 1\}$ is called "bitwise addition modulo 2". On $\mathbf{B}^2 = \{00, 01, 10, 11\}$, the table for $\oplus$ is given.

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

The operation is performed bitwise; $10 \oplus 01 = 11$ since $1 \oplus 0 = 1$ and $0 \oplus 1 = 1$. You are asked to investigate properties of $\oplus$ in the exercises.

PROBLEMS

1. Is subtraction a commutative binary operation on Z ? Explain.

(a) Is subtraction associative on Z ?

(b) Is multiplication commutative on Z ?

(c) Does multiplication have an identity on Z ? Are there inverses?

2. Give an example of subsets A and B of Z so that

(a) subtraction is not a binary operation on A.

(b) multiplication is not a binary operation on B.

3. Let S = {a, b, c}, and P(S) be the power set of S.

(a) Is $\cup$ on P(S) commutative? Explain.

(b) Does {a} have an inverse?

4. Let S = {a, b, c, d}.

(a) Is $\cap$ on P(S) commutative, associative? Explain.

(b) Does $\cap$ have an identity?

(c) What is the inverse of A = {b, d} under $\cap$?

5. Let $\circ$ be the binary operation on N = {0, 1, 2, 3, ... } with $m \circ n = (5^m)(2n + 1)$.

(a) Compute $2 \circ 3$ and $3 \circ 2$. Is $\circ$ commutative?

(b) Is $\circ$ associative? Does $\circ$ have an identity?

6. Let $\circ$ be the binary operation $m \circ n = m + n - mn$ on Z. Is $\circ$ commutative, associative? Does $\circ$ have an identity?

7. Make a table of inverses for the operation in example 4.

8. Let A = { 1, -1, i, -i } and let □ denote ordinary complex multiplication.

(a) Make the matrix table for □. (b) Is □ associative, commutative?

(c) Does □ have an identity?

(d) Give a table of inverses for the elements of A.

9. What is the identity for the binary operation in example 5? Are there inverses?

10. Let A = {1, 2, 5, 10} and define a binary operation on Z by m □ n = LCM(m, n).

Make the matrix table for □ and decide whether □ is commutative, has an identity, inverses.

11. Let A = Z = {0, ±1, ±2, ±3, ... } and define a binary operation on Z by m □ n = m + n - 1.

(a) Is □ commutative? (b) Does □ have an identity?

(c) Are there inverses?

12. Define the operation □ on Z^+ as follows: m □ n = GCD(m, n) + LCM(m, n). Is □ associative?

13. (a) Is m □ n = $3^m \cdot n$ commutative on N = {0, 1, 2, 3, ... } ?

(b) How many ordered pairs (m, n) can you find so that m □ n = 18?

14. Which properties are satisfied by ⊕, bitwise addition modulo 2?

15. Show that m □ n = $n2^m$ is not associative on N = {0, 1, 2,...}. Is □ commutative?

16. Let m ∘ n = m + n – 3 on Z. What is the identity? What is the inverse of an element p?

GROUPS

A group is an algebraic structure that consists of two items: a set of elements G, and a binary operation $\circ$. This structure satisfies FOUR axioms:

CLOSURE: For any elements a and b in G $a \circ b$ is also in G.

IDENTITY: There is a unique element e in G such that for any $a \in G$ we have $a \circ e = a = e \circ a$.

INVERSES: For every element a in G there is an element a^{-1} in G so that $a \circ a^{-1} = e = a^{-1} \circ a$.

ASSOCIATIVITY: For any three elements a, b, c in G we have $(a \circ b) \circ c = a \circ (b \circ c)$.

A general group can be denoted as $(G, \circ)$ indicating the importance of having both a carrier set G and a binary operation $\circ$. When the operation is clear from a particular context we may write just G for that group.

Example 1. $(Z, +)$ is a group under the usual addition operation. Choose a, b in Z. Since $a + b$ is an integer CLOSURE holds. The identity e is 0 since $0 + a = a = a + 0$ for any $a \in G$. The inverse of a is -a (we could write $a^{-1} = -a$) since $a + (-a) = 0 = (-a) + a$. ASSOCIATIVITY holds since $(a + b) + c = a + (b + c)$.

Example 2. In the exercises you will show that the following are groups: $(Q, +)$, $(R, +)$, $(Q^+, \times)$, $(R^+, \times)$ where Q = Rationals, R = Reals, Q^+ = positive Rationals, R^+ = positive Reals.

Example 3. In the exercises you will show that the following are not groups: $(Z, -)$, $(Z, \div)$.

ABELIAN GROUPS

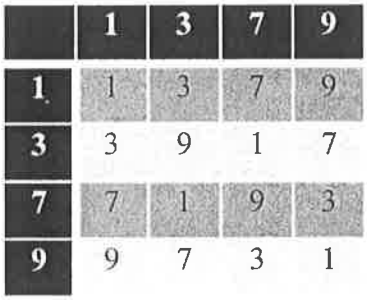
Some groups have an additional fifth property called commutativity. A binary operation $\circ$ on a set G is commutative if $a \circ b = b \circ a$ for all a, b in G. We also say that the group $(G, \circ)$ is an abelian group, named after Niels Abel, a major contributor in the development of group theory. He also proved the insolvability of the fifth-degree polynomial equation, one of his greatest achievements.

The examples involving Z, Q, and R above are all abelian groups.

GROUP TABLES

When the set G is finite (most of the above examples were infinite) the four group properties can be readily detected from an operation table. We saw earlier that the set

G = {1, 3, 7, 9} was closed under units multiplication denoted ⊗. The operation table follows.



	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The symbol a⊗ b means take a from the left most column and "multiply" by b from the very top row. The 16 interior elements are just 1, 3, 7 and 9 showing closure. The element 1 acts like the identity – look at the top interior row and left most interior column. Inverses are easy to find; just locate the 1's in the table. Since 1⊗1 = 1, 3⊗7 = 1 and 9 ⊗ 9 = 1 we have the following table of inverses.

x	1	3	7	9
x^{-1}	1	7	3	9

Associativity is inherited from multiplication in Z; we now know that $(G, \circ)$ is a group. In fact, the symmetry of the table shows that G is an abelian group.

Example 4. Here is an example of a group that involves functions and algebra. The operation is compositions of functions. Let f(x) = x, g(x) = $\frac{1}{1-x}$ and h(x) = $\frac{x-1}{x}$. G = {f, g, h} is a group with identity function f. The "product" gh is g(h(x)) = g($\frac{x-1}{x}$) = $\frac{1}{1-\left(\frac{x-1}{x}\right)}$ = $\frac{x}{x-(x-1)}$ = x.

Conclusion: gh = f. You should form the other products and make the group table.

CONSEQUENCES OF THE 4 GROUP AXIOMS

Theorem 1. If ab = ac in a group G then b = c. (This is called left cancellation).

Proof: Multiply each side of ab = ac on the left by a^{-1}. You get $(a^{-1}a)b = (a^{-1}a)c$ or b = c. A similar result holds for right cancellation. But be careful "mixed" cancellation may not work, i.e. ab = ca does not necessarily imply b = c.

Theorem 2. In the multiplication table for a group $G = \{g_1, g_2, \ldots, g_n\}$ each element of G appears exactly once in each row.

Proof: The entries on row r are $rg_1, rg_2, rg_3, \ldots, rg_n$. If two of these are the same, say $rg_i = rg_j$ then $g_i = g_j$ upon left multiplication by r^{-1}. But this is a contradiction. Why? It can also be shown that elements in any column are distinct.

Theorem 3. For any $a \in G$, $(a^{-1})^{-1} = a$.

Proof: $a\,a^{-1} = e$. This is like saying that the inverse of 2 in $(Q^+, \times)$ is $2^{-1} = \frac{1}{2}$ since $2 \cdot \frac{1}{2} = 1$, the identity.

Theorem 4. $(abc)^{-1} = c^{-1}\,b^{-1}\,a^{-1}$. (The sock-shoe theorem).

Proof: $(abc)(c^{-1}\,b^{-1}\,a^{-1}) = ab(c\,c^{-1})\,b^{-1}\,a^{-1} = a(b\,b^{-1})\,a^{-1} = a\,a^{-1} = e$.

Theorem 5. If $a = a^{-1}$ for all $a \in G$, then G is abelian.

Proof: $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. This result is equivalent to saying that if the operation table has e, the identity, down the main diagonal then G is abelian. The reason: $a = a^{-1}$ implies $a^2 = e$.

A GROUP GENERATOR

Sometimes there is an element in a group G whose powers (sums) generate the entire group. In G = {1, 3, 7, 9} under units multiplication, 3 is such an element since $3^0 = 1$, $3^1 = 3$, $3^2 = 9$, $3^3 = 7$. We can write [3] = {1, 3, 7, 9} to show that 3 is a generator. It is also true that [7] = [3], but [9] ≠ {1, 3, 7, 9}. A group that has a generator is called cyclic. Hence {1, 3, 7, 9} is a cyclic group. {1, -1, i, -i} is also a cyclic group, under complex multiplication, generated by either i or -i. (Z, +) is an additive cyclic group generated by 1 or -1. For an additive group, powers are replaced by sums: 2 = 1 + 1, 3 = 1 + 1 + 1, 4 = 1 + 1 + 1 + 1, … and so on. In summary, for a group whose operation is multiplication a^m means $a \cdot a \cdot a \cdot \ldots \cdot a$; if the operation is addition $m \cdot a$ means $a + a + a + \ldots + a$.

SUBGROUPS

Let (G, ∘) be a group and let H be a subset of the set G. (H, ∘) is a subgroup of (G, ∘) if (H, ∘) is closed under ∘, has the e of G as the identity and contains inverses. Associativity is inherited from (G, ∘). Examples are easy to find. (Z, +) is a subgroup of (Q, +). {1, 9} is a subgroup of {1, 3, 7, 9} under mod 10 multiplication. The set {1, -1} is a subgroup of {1, -1, i, -i} which itself is a subgroup of all complex numbers under multiplication. The set of all integral multiples of 3, H = {0, ±3, ±6, …} is a subgroup of {Z, +}. Can you give a subset S of (Z, +) such that S is closed under addition but is not a subgroup?

MODULAR GROUPS

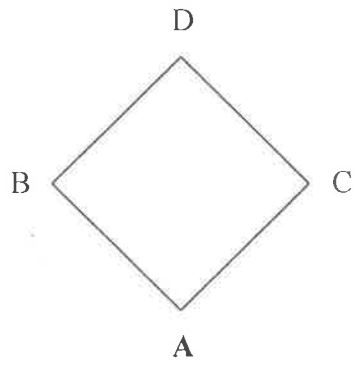
Clock arithmetic provides a fruitful source of nice finite groups. Recalling that 13 o'clock is really just 1 o'clock upon subtraction of 12, we can make a clock with just the four numbers 0, 1, 2, 3 the remainders when any integer n is divided by 4. We can write $7 \equiv 3 \pmod 4$ for example. This is read as 7 is congruent to 3 modulo 4. In general $a \equiv b \pmod m$ means that a and b have the same remainder when divided by m; or that a – b is divisible by m.

Definition. Let Z_n = {0, 1, 2, 3, … n−1}. The sum a + b of any two elements in Z_n is just the remainder when a + b is divided by n. With this definition of sum we can see that (Z_n, +) is a group. Lets form the operation table for Z_4 = {0, 1, 2, 3}.

	0	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The table shows closure, and that 0 is the identity. Locate the 0's in the table to see that the inverse of 0 is 0, the inverse of 1 is 3 (since 1 + 3 = 0), the inverse of 2 is 2, and the inverse of 3 is 1. This new sum rule is an associative binary operation on Z_4 since ordinary addition is associative on Z, the usual integers. In similar analysis, (Z_n, +) is an additive group.

Example 5. Z_6 = {0, 1, 2, 3, 4, 5} is a group with a number of subgroups. A = {0}, B = {0, 3}, C = {0, 2, 4} and D = {0, 1, 2, 3, 4, 5} are all subgroups of Z_6. The following picture, called a lattice of subgroups, shows the relationships between the subgroups.



The upward sloping lines indicate subgroup inclusion: $A\subseteq B$, $A\subseteq C$, $B\subseteq D$, $C\subseteq D$ and $A\subseteq B\subseteq D$, $A\subseteq C\subseteq D$, two chains of length three.

Example 6. The modular groups Z_n are cyclic. For Z_4, 1 is a generator since

$$\begin{aligned} 1 \cdot 1 &= 1 = 1 \\ 2 \cdot 1 &= 1 + 1 = 2 \\ 3 \cdot 1 &= 1 + 1 + 1 = 3 \\ 4 \cdot 1 &= 1 + 1 + 1 + 1 = 0 \end{aligned}$$

In additive notation $3 \cdot 1$ means add there 1's together. In Z_6, only 1 and 5 are generators. For example, 3 is not a generator since you can only make 0 and 3 using multiples $m \cdot 3$ of 3. Try it! Likewise, the element 2 will only generate 0, 2, 4. The previous example prompts the question: which elements in Z_n are generators? The following chart might provide a clue as you pursue this question in the exercises.

n	Z_n	generators
2	{0, 1}	1
3	{0, 1, 2}	1, 2
4	{0, 1, 2, 3}	1, 3
5	{0, 1, 2, 3, 4}	1, 2, 3, 4
6	{0, 1, 2, 3, 4, 5}	1, 5

PROBLEMS

1. Show that each of the following are groups.
   (a) (Q, +) (b) (R, +) (c) (Q^+, x) (d) (R^+, x)
2. Show that the following are not groups.
   (a) (Z, -) (b) (Z, ÷) (c) (Z, x)
3. Make the multiplication table for A = {4, 8, 12, 16} under multiplication mod 20. Does A have an identity?
4. Is B = {2, 4, 6, 8} under units multiplication a group? Is B cyclic? Is B Abelian?

5. Verify that 7 is a generator of the group {1, 3, 7, 9} under units multiplication, but that 9 is not a generator.

6. Let S ={e, a, b, c}. Make the 4 x 4 group operation table assuming that e is the identity and that $a^2 = b^2 = c^2 = e$. Is S cyclic? Abelian?

7. Show that G = {1, -1, i, -i} is a group under ordinary complex multiplication. Is G cyclic?

8. Show that G = {00, 01, 10, 11} is a group using bitwise addition mod 2.

9. Give an example of a group that illustrates Theorem 5.

10. Prove that in a group $(abcd)^{-1} = d^{-1}c^{-1}b^{-1}a^{-1}$. Why is this called the sock-shoe theorem?

11. Make the group table for G = {000, 001, 010, 011, 100, 101, 110, 111} using bitwise addition mod 2. Is G Abelian? Is G cyclic?

12. Is {1, 3} a subgroup of {1, 3, 7, 9} under mod 10 multiplication?

13. Verify that H = {0, ±7, ±14, ...} is a subgroup of Z under addition.

14. Is the set of all complex numbers α with $|\alpha| \leq 1$ a subgroup of the group of all nonzero complex numbers under multiplication? Here, if $\alpha = a + bi$, $|\alpha| = \sqrt{a^2 + b^2}$, its distance from the origin.

15. Make the operation table for Z_6 and find all subgroups.

16. Make the operation table for Z_8 and find all subgroups.

17. Without making the addition table for Z_{12} can you give all the closed subsets of Z_{12}? Are these in fact subgroups? Draw the lattice of subgroups of Z_{12}.

18. Show that in $(Z_n, +)$, the additive groups of integers modulo n, that the inverse of any $a \neq 0$ is n - a.

19. Explain why $(Z_4, \bullet)$ is not a group, where multiplication is modulo 4.

20. Verify associativity for the following sum in Z_7:

(3 + 5) + 6 and 3 + (5 + 6)

21. Find all the generators for the cyclic group Z_5, and verify that each in fact generates all of Z_5.

22. Determine those elements in Z_n that are generators.

23. Solve the quadratic equation $x(x+1) = 0$

(a) in Z_4 (b) in Z_5 (c) in Z_6

24. Make the group multiplication table for $G = \{e, a, a^2, a^3, a^4\}$ where e is the identity and $a^5 = e$. Hint: $a^3 \cdot a^4 = a^7 = a^5 \cdot a^2 = a^2$.

25. Let G be a group. Prove that for any $a \in G$, $H = \{x \in G: x = a^n \text{ for } n \in Z\}$ is a subgroup of G (generated by a).

SYMMETRY AND THE ALPHABET

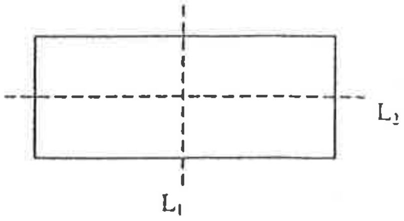
The figure to the right has four types of symmetry that leaves the figure fixed:

1. Do nothing

2. Flip about L_1

3. Flip about L_2

4. Clockwise rotation through 180°



Below each of the letters of the alphabet give the number of types of symmetry associated with each letter. A few samples are given.

A	B	C	D	E
2	2	2		
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y
Z				

THE KLEIN 4 – GROUP

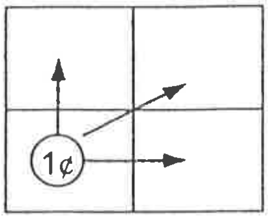
A penny can be moved on a 2 × 2 board in four ways:

S = same

V = vertical

H = horizontal

D = diagonal



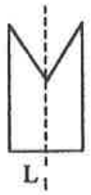
Fill in the operation table giving the result of a move followed by another move. The operation ∘ is "followed by".

1. Does it matter where you start?
2. Is *V* followed by *H* the same as *H* followed by *V*?
3. Describe the main diagonal of your table.
4. Can you have $V \circ H = D \circ H$?

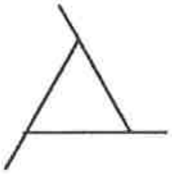
∘	S	V	H	D
S				
V				
H				
D				

SYMMETRY – GROUPS – OPERATION TABLES

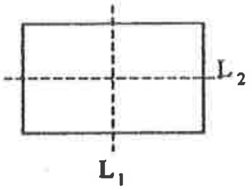
A symmetry of a figure is a rigid motion that leaves the figure unchanged. Lets take the following three figures and give their symmetries:



1. do nothing
2. flip about the axis L_1.



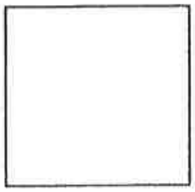
1. do nothing
2. rotate 120°
3. rotate 240°



1. do nothing
2. flip about L_1
3. flip about L_2
4. 180° rotation

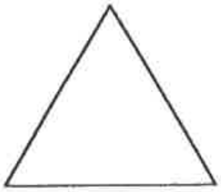
It is convenient to agree that rotation means clockwise.

Task 1 Describe the symmetries of a square.



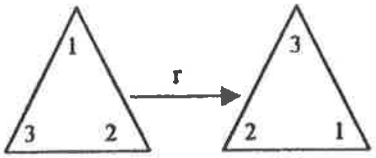
1. do nothing
2.
3.
4.
5.
6.
7.
8.

Task 2 Describe the symmetries of an equilateral triangle.

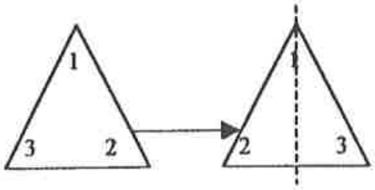


1.
2.
3.
4.
5.
6.

Our goal here is to study more deeply such symmetries; introduction of good notation is necessary to stay organized. We will use the symmetries of an equilateral triangle as our basic example. First, label the vertices and draw the action caused by a rotation and a flip:

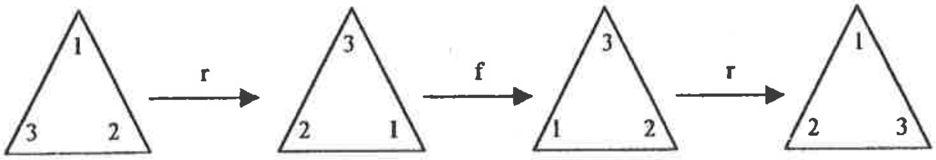


a clockwise rotation through 120°



a flip about an altitude holding vertex 1 fixed.

Combinations of rotations and flips give rise to other symmetries:



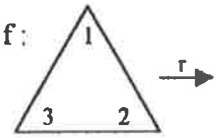
If we view the first or left most triangle as being in original position the movement of the vertices

1 goes to 3 , 2 goes to 1 , 3 goes to 2

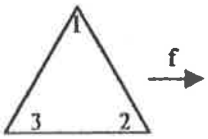
could be expressed in the cycle form (132). Similarly the flip f is (23), where vertices 2 and 3 are switched and 1 stays fixed.

Task 3 Complete the sequence of pictures that will show:

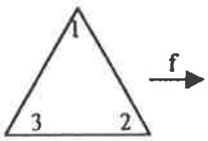
r , followed by r , then f :



f , then r , then f :



f , then f , then r :



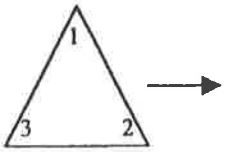
Task 4 For convenience we could let fr^2f stand for f, then r, then r, then f. Say in your own words what each of these mean.

$frfrf$ means

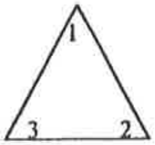
r^2fr^2f means

Task 5 Draw the sequence of triangles to prove that $fr = r^2f$

fr :



r^2f :



Task 6 In addition to the flip $f = (23)$, there are two more flips. Express each in terms of just r and f.

Task 7 Show that your six symmetries of an equilateral triangle can be expressed as $\{1, r, r^2, f, rf, r^2f\}$ where 1 means "do nothing."

Task 8 SOME ALGEBRA

You showed in task 5 that $fr = r^2 f$. This relationship can be used to show that the "product" of $r^2 f$ and rf, in that order, is just r.

$$(r^2f)(rf) = r^2(fr)f = r^2(r^2f)f = r^4f^2 = r \cdot 1 = r$$

Explain why $r^3 = 1$:

Explain why $f^2 = 1$:

Similarly, express each of the following products as one of our six symmetries:

$(rf)(r^2f) =$

$f(rf) =$

$r^2(r^2f) =$

$(r^2f)(r^2) =$

Task 9 A MULTIPLICATION TABLE

Complete the operation table where the operation is "followed by." Each of the 36 entries should be one of our six symmetries. Multiply row entry by column entry in that order.

Δ	1	r	r^2	f	rf	r^2f
1						
r						
r^2						
f						
rf						
r^2f						

Task 10 We saw that in cycle form r = (132) and f = (23). Express each of the remaining four symmetries in cycle form.

1 = (1) (This is a convention which shows that no vertex moved).

r^2 =

r f=

r^2f=

Task 11 You could label four of the square symmetries as 1 , r , r^2 , r^3 . Interpret these as rotations. What would 1 , r , r^2 , r^3 , r^4 mean in a regular pentagon ?

In algebra you have $r^m r^n = r^{m+n}$ and $r^0 = 1$. What do these rules mean in the setting of symmetries of regular n-gons ?

What do you think r^{-1} means ? What is f^{-1} , the inverse of f ?

Using your 6 by 6 multiplication table, determine the inverse of each symmetry:

symmetry	1	r	r^2	f	rf	r^2f
inverse						

Task 12 Use r for a 90° rotation and f to denote a flip about the diagonal fixing 1 and 3 and give the eight symmetries of the square in terms of r and f.