CS-102: Discrete Structures Tutorial #5

Lattice:	a poset in which every subset consisting of two elements has a LUB and a GLB
• Theorem:	If L_1 and L_2 are lattices, then $L = L_1 \times L_2$ is a lattice.
• Theorem:	Let L be a lattice, and $a, b, c \in L$. Then (a) $a \vee b = b$ *if and only if* $a \leq b$. (b) $a \wedge b = a$ *if and only if* $a \leq b$. (c) $a \wedge b = a$ *if and only if* $a \vee b = b$.
• Properties of Lattices	1. (a) $a \vee a = a$ (b) $a \wedge a = a$ 2. (a) $a \vee b = b \vee a$ (b) $a \wedge b = b \wedge a$ 3. (a) $a \vee (b \vee c) = (a \vee b) \vee c$ (b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ 4. (a) $a \vee (a \wedge b) = a$ (b) $a \wedge (a \vee b) = a$
• Theorem:	Let L be a lattice, and $a, b, c \in L$ 1. If $a \leq b$, then (a) $a \vee c \leq b \vee c$ (b) $a \wedge c \leq b \wedge c$ 2. $a \leq c$ *and* $b \leq c$ *if and only if* $(a \vee b) \leq c$ 3. $c \leq a$ and $c \leq b$ *if and only if* $c \leq (a \wedge b)$ 4. If $a \leq b$ and $c \leq d$, then (a) $a \vee c \leq b \vee d$ (b) $a \wedge c \leq b \wedge d$
Isomorphic lattices:	If $f : L_1 \to L_2$ is an isomorphism from the poset $(L_1, \leq_1)$ to the poset $(L_2, \leq_2)$, then L_1 is a lattice if and only if L_2 is a lattice. If a and b are elements of L_1, then $f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$. If two lattices are isomorphic, as posets, they are isomorphic lattices.
• Bounded lattices:	lattice that has a greatest element I and a least element 0
➢ Theorem:	A finite lattice is bounded.
➢ • Distributive lattice:	lattice that satisfies the distributive laws: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
➢ Complement of a:	element $a \in L$ (bounded lattice) such that $a \vee a = I$ and $a \wedge a = 0$.
➢ Theorem:	Let L be a bounded distributive lattice. If a complement exists, it is unique.
➢ • Complemented lattice:	bounded lattice in which every element has a complement
Boolean algebra:	a lattice isomorphic with $(P(S), \subseteq)$ for some finite set S
• Properties of a Boolean algebra:	Tabulated separately
• Truth tables:	Table listing the values of a function f for all elements of B_n, is called truth tables for f. They are analogous to tables that arise in logic. If x_k represent propositions, and $f(x_1, x_2, \dots, x_n)$ represents a compound sentence constructed from the x_k's; value 0 for a sentence implies that the sentence is false, and 1 implies that the sentence is true, then truth tables show how truth or falsity of $f(x_1, x_2, \dots, x_n)$ depends on the truth or falsity of its component sentences x_k .

• Boolean polynomial (or expression):	Let $x_1, x_2, \dots, x_n$ be a set of n symbols or variables. A Boolean polynomial $p(x_1, x_2, \dots, x_n)$ in the variables x_k is defined recursively as follows: 1. $x_1, x_2, \dots, x_n$ are all Boolean polynomials. 2. The symbols 0 and 1 are Boolean polynomials. 3. If $p(x_1, x_2, \dots, x_n)$ and $q(x_1, x_2, \dots, x_n)$ are two Boolean polynomials, then so are $p(x_1, x_2, \dots, x_n) \vee q(x_1, x_2, \dots, x_n)$ and $p(x_1, x_2, \dots, x_n) \wedge q(x_1, x_2, \dots, x_n)$. 4. If $p(x_1, x_2, \dots, x_n)$ is a Boolean polynomial, then so is $\left(p(x_1, x_2, \dots, x_n)\right)'$. By tradition, $(0)'$ is denoted as $0'$, $(1)'$ is denoted as $1'$, and $(x_k)'$ is denoted x_k' . 5. There are no Boolean polynomials in the variables x_k other than those that can be obtained by repeated use of rules 1, 2, 3, and 4. Boolean polynomials are also called Boolean expressions.
➢ • Minterm:	A Boolean expression of the form $x_1 \wedge x_2 \wedge \cdots \wedge x_n$, where each x_k is x_k *or* x_k' , $1 \leq k \leq n$
➢ • Theorem:	Any function $f: B_n \to B$ is produced by a Boolean expression.
• Karnaugh map:	A graphical procedure for writing a function as "or" combinations of minterms and simplifying the resultant Boolean polynomial that produces the function $f: B_n \to B$
➢ $n = 2$	see tables below
➢ $n = 3$	see table below
➢ $n = 4$	see table below

$n = 2$:

	y'	y
x'	00	01
x	10	11

$x' \wedge y'$	$x \wedge y'$
$x \wedge y'$	$x \wedge y$

$n = 3$:

000	001	011	010
100	101	111	110

$n = 4$:

0000	0001	0011	0010
0100	0101	0111	0110
1100	1101	1111	1110
1000	1001	1011	1010

Properties of a Boolean algebra $(L, \leq)$ and, the corresponding property for subsets of a set S.

(Assuming x, y, and z are arbitrary elements in L, and A, B, and C are arbitrary subsets of S. The greatest and least elements of L are denoted by I and 0, respectively)

Boolean algebra $(L, \leq)$	**Subsets of a set S**
1. $x \leq y$ if and only if $x \vee y = y$.	1'. $A \subseteq B$ if and only if $A \cup B = B$.
2. $x \leq y$ if and only if $x \wedge y = x$.	2'. $A \subseteq B$ if and only if A∩B=A.
3. (a) $x \vee x = x$. (b) $x \wedge x = x$.	3'. (a) $A \cup A = A$. (b) $A \cap A = A$.
4. (a) $x \vee y = y \vee x$. (b) $x \wedge y = y \wedge x$.	4'. (a) $A \cup B = B \cup A$. (b) $A \cap B = B \cap A$.
5. (a) $x \vee (y \vee z) = (x \vee y) \vee z$. (b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.	5'. (a) $A \cup (B \cup C) = (A \cup B) \cup C$. (b) $A \cap (B \cap C) = (A \cap B) \cap C$.
6. (a) $x \vee (x \wedge y) = x$. (b) $x \wedge (x \vee y) = x$.	6'. (a) $A \cup (A \cap B) = A$. (b) $A \cap (A \cup B) = A$.
7. $0 \leq x \leq I$ for all x *in* L.	7'. $\emptyset \subseteq A \subseteq S$ for all A *in* $P(S)$.
8. (a) $x \vee 0 = x$. (b) $x \wedge 0 = 0$.	8'. (a) $A \cup \emptyset = A$. (b) $A \cap \emptyset = \emptyset$.
9. (a) $x \vee I = I$. (b) $x \wedge I = x$.	9'. (a) $A \cup S = S$. (b) $A \cap S = A$.
10. (a) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. (b) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.	10'. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Boolean algebra *(L,≤)*	Subsets of a set *S*
11. Every element x has a unique complement x' satisfying (a) $x \vee x' = I$. (b) $x \wedge x' = 0$.	11'. Every element A has a unique complement $\bar{A}$ satisfying (a) $A \cup \bar{A} = S$. (b) $A \cap \bar{A} = \emptyset$.
12. (a) $0' = I$. (b) $I' = 0$.	12'. (a) $\bar{\emptyset} = S$. (b) $\bar{S} = \emptyset$.
13. $(x')' = x$.	13'. $(\bar{\bar{A}}) = A$.
14. (a) $(x \wedge y) = x \vee y$. (b) $(x \vee y) = x \wedge y$.	14'. (a) $(A \cap B) = A \cup B$. (b) $(A \cup B) = A \cap B$.

.

Binary operation	✓ A binary operation on a set A is an ***everywhere defined function*** $f: A \times A \to A$. ✓ It is customary to denote binary operations by the symbol $*$, instead of f, and to denote the element assigned to (a, b) by $a * b$, instead of $*\,(a, b)$ ✓ If $A = \{a_1, a_2, \dots\ a_n\}$, a binary operation * on A is defined by the table $\begin{array}{c\|ccccc} * & a_1 & \cdots & a_j & \cdots & a_n \\ \hline a_1 & a_1 * a_1 & \cdots & a_1 * a_j & \cdots & a_1 * a_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_i & a_i * a_1 & \cdots & a_i * a_j & \cdots & a_i * a_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_n & a_n * a_1 & \cdots & a_n * a_n & \cdots & a_n * a_n \end{array}$
Semigroup	A nonempty set S together with an associative binary operation $*$ defined on S, denoted by $(S,*)$ or, when it is clear what the operation $*$ is, simply by S. $a * b$ is referred to as the product of a and b. $(S,*)$ is said to be commutative if $*$ is a commutative operation.
free semigroup generated by A	If $A = \{a_1, a_2, \dots\ a_n\}$ is a non-empty set, A^* the set of all finite sequences of elements of A and catenation is a binary operation $\cdot$ on A^*. Semigroup $(A^*, \cdot)$ is called the free semigroup generated by A.
identity element	An element e in a semigroup $(S,*)$ is called an identity element if $e * a = a * e = a, \forall a \in S$
monoid	A semigroup $(S,*)$ that has an identity
subsemigroup	Let $(S,*)$ be a semigroup; if T, a subset of S is closed under the operation $*$ (*i.e.* $a * b \in T$ whenever $a, b \in T$), then $(T,*)$ is called a subsemigroup of $(S,*)$.
submonoid	Let $(S,*)$ be a monoid with identity e; if T, a non-empty subset of S, is closed under the operation $*$ and $e \in T$, then $(T,*)$ is called a submonoid of $(S,*)$.
isomorphism between two semigroups	Let $(S,*)$ and $(T,*')$ be two semigroups. A function *f*:*S*→*T* is called an **isomorphism** from $(S,*)$ to $(T,*')$ if it is a *one-to-one correspondence* from *S* to *T*, and if $f(a * b) = f(a) * f(b)$, $\forall a, b \in S$; and is denoted *by* $S \simeq T$.
Homomorphism and homomorphic image	Let $(S,*)$ and $(T,*')$ be two semigroups. An *everywhere defined* function $f: S \to T$ is called a **homomorphism** from $(S,*)$ to $(T,*')$ if $f(a * b) = f(a) * f(b)$, $\forall a, b \in S$. If f is also onto, we say that T is a **homomorphic image** of S.

Theorem	If $a_1, a_2, \dots\ a_n$, $n \geq 3$, are arbitrary elements of a semigroup, then all products of the elements $a_1, a_2, \dots\ a_n$ that can be formed by inserting meaningful parentheses arbitrarily are equal.
Theorem	$(S,*)$ and $(T,*')$ be monoids with identities e and e', respectively. Let $f: S \to T$ be an isomorphism. Then $f(e) = e'$.
Theorem	$(S,*)$ and $(T,*')$ be monoids with identities e and e', respectively. Let $f: S \to T$ be a homomorphism from $(S,*)$ onto $(T,*')$. Then $f(e) = e'$.
Theorem	Let f be a homomorphism from a semigroup $(S,*)$ to a semigroup $(T,*')$. If S' is a semigroup of $(S,*)$, then $f(S') = \{t \in T \mid t = f(s), for\ some\ s \in S\}$
Theorem	If f is a homomorphism from a commutative semigroup $(S,*)$ onto a semigroup $(T,*')$ then $(T,*')$is also commutative.
Theorem	If $(S,*)$ and $(T,*')$ are semigroups, then $(S \times T,*'')$ is a semigroup, where $*''$ is defined by $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$.
Theorem	Let R be a congruence relation on the semigroup $(S,*)$. Consider the relation $\circledast$: *S/R*×*S/R* → *S/R* in which the ordered pair $([a], [b])$ is, related to $[a * b]$, for a and b in S **(a)** $\circledast$ is a function from *S/R*×*S/R* to *S/R*, and as usual $\circledast$*([a], [b]) is denoted* by $[a] \circledast [b]$. Thus $[a] \circledast [b] = [a * b]$. **(b)** *(S/R,* $\circledast$*)* is a semigroup.
Corollary	Let R be a congruence relation on the monoid $(S,*)$. If the operation $\circledast$ in *S/R is defined by* $[a] \circledast [b] = [a * b]$, then *(S/R,* $\circledast$*)* is a monoid.
Theorem	Let R be a congruence relation on a semigroup (S,$*$), and let (S/R, $\circledast$) be the corresponding quotient semigroup. The function $f_R: S \to S/R$ defined by $f_R(a) = [a]$ is an onto homomorphism, called the ***natural homomorphism***.
Theorem	***(Fundamental Homomorphism Theorem)*** Let $f: S \to T$ be a homomorphism of the semigroup $(S,*)$ onto the semigroup $(T,*')$. Let R be the relation on S defined by aRb *if and only if* $f(a) = f(b)$, for a and b in S. Then **(a)** R is a congruence relation. **(b)** $(T,*')$ and the quotient semigroup (S/R, $\circledast$) are isomorphic.
group	A **group** $(G,*)$ is a monoid, with identity e, that has the additional property that for every element $a \in G$ there exists an element $a' \in G$, called the *inverse* of a such that $a' * a = a * a' = e$. A group with finite number of elements, is called a **finite** group; **order** of *G is* $\|G\|$ <u>Note</u>: When only one group $(G,*)$ is under consideration and there is no possibility of confusion, the product $a * b$ of the elements a and b in the group $(G,*)$ is written as ab, and $(G,*)$ is referred to as G
Abelian group	A group G is said to be **Abelian** if $ab = ba$ for all elements a and b in G

Theorem	Let G be a group. Each element a in G has only one inverse in G.
Theorem	Let G be a group and let a, b, and c be elements of G. Then (a) $ab = ac \Rightarrow b = c$ (**left cancellation property**). (b) $ba = ca \Rightarrow b = c$ (**right cancellation property**).
Corollary	Let G be a group and $a \in G$. Define a function $M_a: G \to G$ by the formula $M_a(g) = ag$. Then the function M_a is one to one.
Theorem	Let G be a group and let a and b be elements of G. Then **(a)** $(a^{-1})^{-1} = a$. **(b)** $(ab)^{-1} = b^{-1}a^{-1}$.
Theorem	Let G be a group, and let a and b be elements of G. Then **(a)** $ax = b$ has a unique solution in G. **(b)** $ya = b$ has a unique solution in G.
Multi-plication table of a group	The multiplication table of a group $G = \{a_1, a_2, \ldots\ a_n\}$ under the binary operation $*$ must satisfy the following properties:

	1. The row labeled by e must be $a_1, a_2, \ldots\ a_n$ and the column labeled by e must be $\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{matrix}$ **2.** each row and column is a permutation of the elements $a_1, a_2, \ldots\ a_n$ of G, and each row (and each column) determines a different permutation.
subgroup	Let H be a subset of a group G such that **(a)** The identity e of G belongs to H. **(b)** If a and b belong to H, then $ab \in H$. **(c)** If $a \in H$, then $a^{-1} \in H$. Then H is called a **subgroup** of G
Theorem	Let $(G,*)$ and $(G',*')$ be two groups, and let $f: G \to G'$ be a homomorphism from G to G'. (a) If e is the identity in G and e' is the identity in G', then $f(e) = e'$. (b) If $a \in G$, then $f(a^{-1}) = \left(f(a)\right)^{-1}$. (c) If H is a subgroup of G, then $f(H) = \{f(h) \mid h \in H\}$ is a subgroup of G'.

I: Lattices

1.1. Determine which of the Hasse diagrams given in Figs.5 to 10 represent a Lattice. Justify your answer.

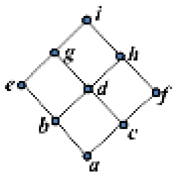


Fig.5

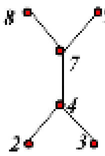


Fig.6

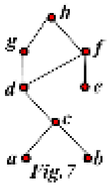


Fig.7

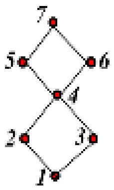


Fig.8

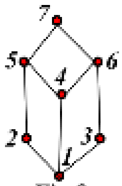


Fig.9

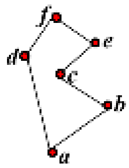


Fig.10

1.2. Is the poset $A = \{2, 3, 6, 12, 24, 36, 72\}$ under the relation of divisibility a lattice?

1.3. If L1 and L2 are the lattices shown in Fig.11, draw the Hasse diagram of L1 × L2 with the product partial order.

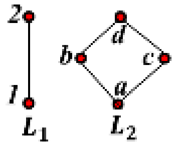


Fig.11

1.4. A lattice, L is said to be modular if, $a, b, c \in L$; $a \leq c$ implies that $a \vee (b \wedge c) = (a \vee b) \wedge c$.

(a) Show that a distributive lattice is modular.
(b) Show that the lattice shown in Fig.12 is a non-distributive lattice that is modular.

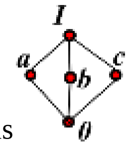


Fig.12

1.5. Given D_n is the set of all positive divisors on n ($n \in Z^+$). Find the complement of each element in (a) D_{20} (b) D_{30} (c) D_{42}. Which of these have a complemented lattice.

1.6. Determine whether each lattice given in Figs. 13 to 16 is distributive, complemented, or both.

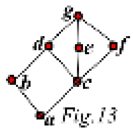


Fig.13

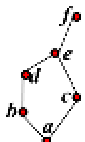


Fig.14

Fig.15

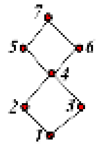


Fig.16

1.7. In a distributed lattice, show that $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$.

II: Finite Boolean Algebras

2.1. Determine whether the poset with Hasse diagram given in Figs. 17 to 24 is a Boolean algebra. Justify your answer.

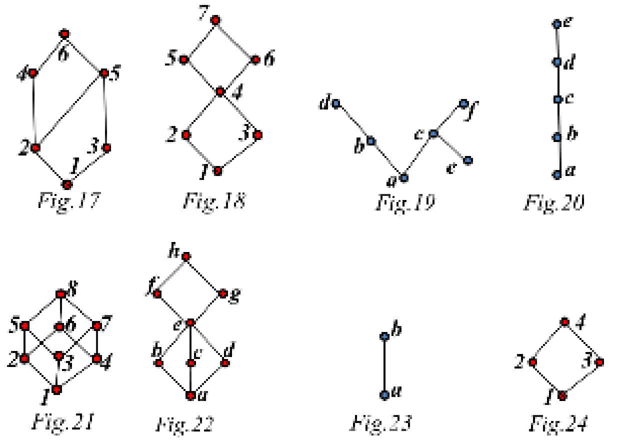


Fig.17 Fig.18 Fig.19 Fig.20

Fig.21 Fig.22 Fig.23 Fig.24

2.2. Determine whether the poset given below is a Boolean algebra. Justify your answer.

(a) D_{60} (b) D_{210} (c) D_{385} (d) D_{646}

2.3. Let A = {a, b, c, d, e, f, g, h} and R be the relation defined by

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

a. Show that (A, R) is a poset.

b. Does the poset (A, R) have a least element and a greatest element? If so, identify them.

c. Show that the poset (A, R) is complemented and list all pairs of complements.

d. Prove or disprove that (A, R) is a Boolean algebra.

2.4. Let A = {a, b, c, d, e, f, g, h} and R be the relation defined by the matrix M_R. Prove or disprove that (A, R) is a Boolean algebra

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

III: Functions of Boolean Algebra

3.1. Give the Boolean function described by the logic diagram given in Figs.25 and 26. Use the properties of a Boolean algebra to refine the functions to use minimal number of variables and operations. Draw the logic diagrams for the new function.

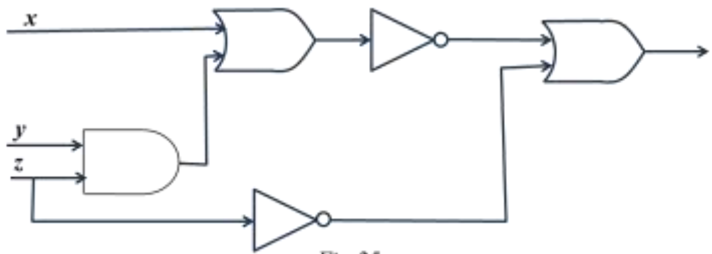


Fig.25

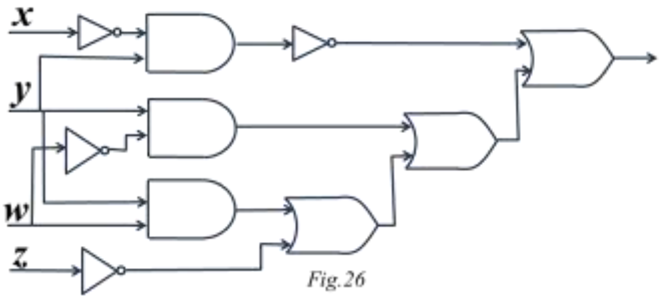


Fig.26

3.2. Let $S(f) = \{b_1, b_2, \dots, b_k\}$, and for each i, let $f_i: B_n \to B$ be the function defined by

$f_{i(b_i)} = 1$

$f_{i(b)} = 0, if\ b \neq b_i$

Let $f: B_3 \to B$ with

$S(f) = \{(0,0,0), (0,1,0), (1,0,0), (1,1,0), (1,1,1)\}$. Write the reduced Boolean expression for f using Karnaugh Map.

3.3. Let $g: B_4 \to B$ with *min-terms* $x' \wedge y' \wedge z \wedge w'$, $x' \wedge y \wedge z \wedge w'$, $x \wedge y' \wedge z \wedge w$, $x \wedge y \wedge z \wedge w'$ and $x \wedge y \wedge z \wedge w$. Write the reduced Boolean expression for g using Karnaugh Map.

IV: Binary Operation on a Set

4.1. Determine whether the description of $*$ is a valid definition of a binary operation on the set as given below: -

(a) On R, where *a***b* is *ab (i.e. multiplication).*
(b) On Z^+, where *a***b* is *a/b*.
(c) On Z, where *a***b* is a^b.
(d) On Z^+, where *a***b* is $a - b$.
(e) On R, where *a***b* is $a\sqrt{b}$.

4.2. Determine whether the binary operation $*$ is commutative and whether it is associative on the set:-

(a) On Z^+, where *a***b* is $a+b+2$.
(b) On Z, where *a***b* is *ab*.
(c) On R, where *a***b* is $a \times |b|$.
(d) On the set of nonzero real numbers, where *a***b* is *a/b*.
(e) On R, where *a***b* is the minimum of *a* and *b*.
(f) On the set of $n \times n$ Boolean matrices, where $\boldsymbol{A} * \boldsymbol{B}$ is $\boldsymbol{A} \odot \boldsymbol{B}$.
(g) On R, where *a***b* is *ab*/3.
(h) On R, where *a***b* is $ab+2b$.
(i) On a lattice *A*, where *a***b* is $a \vee b$.

(j) On the set of 2×1 matrices, where $\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a + c \\ b + d + 1 \end{bmatrix}$.

(k) On the set of rational numbers, where $a * b = \frac{a+b}{2}$

4.3. Prove or disprove that the binary operation on Z^+ of $a * b = GCD(a, b)$ has the idempotent property.

4.4. Prove or disprove the binary operation on that the set of rational numbers, where $a * b = \frac{a+b}{2}$ has the idempotent property.

4.5. Fill in the following table so that the binary operation $*$ is commutative and has the idempotent property.

$*$	a	b	c
a		c	
b			
c	c	a	

4.6. Consider the binary operation $*$ defined on the set $A = \{a, b, c, d\}$ by the following table.

$*$	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Compute

(a) $c * d$ and $d * c$.

(b) $b * d$ and $d * b$.

(c) $a * (b * c)$ and $(a * b) * c$.

(d) Is $*$ commutative? associative?

4.7. Define a binary operation on a set S by $a * b = b$. Is $*$ associative? commutative? idempotent?

V: Semigroups

5.1 Let $A = \{a, b\}$. Which of the following tables define a semigroup on A? Which define a monoid on A?

(a)

$*$	a	b
a	a	b
b	a	a

(b)

$*$	a	b
a	a	b
b	b	b

5.2. Do the following tables define a semigroup or a monoid?

(a)

$*$	a	b	c
a	c	b	a
b	b	c	b
c	a	b	c

(b)

$*$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

5.3. For the following, determine whether the set together with the binary operation is a semigroup, a monoid, or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid, determine if it is commutative.

(a) Z^+, where $*$ is defined as ordinary multiplication.

(b) Z^+, where $a * b$ is defined as max (a, b).

(c) Z^+, where $a * b$ is defined as GCD(a, b).

(d) Z^+, where $a * b$ is defined as a.

(e) The nonzero real numbers, where $*$ is ordinary multiplication.

(f) *P(S)*, with *S* a set, where $*$ is defined as $\cap$.

(g) A Boolean algebra *B*, where $a * b$ is defined as $a \wedge b$.

(h) $S = \{1,2,3,6,12\}$, where $a * b$ is defined as $HCF(a, b)$.

(i) $S = \{1,2\ 3,6\ 9\ 18\}$, where $a * b$ is defined as $LCM(a, b)$.

(j) Z, where $a * b = a + b - ab$.

(k) The even integers, where $a * b$ is defined as $\frac{ab}{2}$

(l) The set of 2×1 matrices, where $\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a + c \\ b + d + 1 \end{bmatrix}$

(m) The set of integers of the form $3k + 1$, $k \in Z+$, where $*$ is ordinary multiplication.

5.4. Complete the following table to obtain a semigroup

$*$	a	b	c
a	c	a	b
b	a	b	c
c			a

5.5. Complete the following table so that it defines a monoid.

$*$	a	b	c	d
a	c	d	a	b
b		a	b	
c			c	
d	b		d	a

5.6. Let $S = \{a, b\}$. Write the operation table for the semigroup S^S, where S^S is the set of all functions from S to S. Is the semigroup commutative?

5.7. Let $S = \{a, b\}$. Write the operation table for the semigroup $(P(S), \cup)$.

5.8. Let $A = \{a, b, c\}$, consider the semigroup $(A *, \circ)$, where $\cdot$ is the operation of catenation. If $\alpha = abac$, $\beta = cba$, and $\gamma = babc$, compute

(a) $(\alpha \circ \beta) \circ \gamma$ (b) $\gamma \circ (\alpha \circ \alpha)$ (c) $(\gamma \circ \beta) \circ \alpha$

5.9. What is required for a subset of the elements of a semigroup to be a sub-semigroup?

5.10. What is required for a subset of the elements of a monoid to be a sub-monoid?

5.11. Prove or disprove that the intersection of two sub-semigroups of a semigroup $(S, *)$ is a sub-semigroup of $(S, *)$.

5.12. Prove or disprove that the intersection of two sub-monoids of a monoid *(S,∗)* is a sub-monoid of *(S,∗)*.

5.13. Let $A=\{0,1\}$, and consider the semigroup $(A^*, \cdot)$, where $\cdot$ is the operation of catenation. Let T be the subset of A^* consisting of all sequences having an odd number of 1's. Is $(T, \cdot)$ a sub-semigroup of $(A, \cdot)$?

5.14. Let $A=\{a,b\}$. Are there two semigroups $(A, *)$ and $(A, *')$ that are not isomorphic?

5.15. An element x in a monoid is called an idempotent if $x^2 = x * x = x$. Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

5.16. Let $(S_1, *_1)$, $(S_2, *_2)$, and $(S_3, *_3)$ be semigroups and $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be homomorphisms. Prove that $g \circ f$ is a homomorphism from S_1 to S_3.

5.17. Let $(S_1, *_1)$, $(S_2, *_2)$, and $(S_3, *_3)$ be semigroups, and let $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be isomorphisms. Show that $g \circ f: S_1 \to S_3$ is an isomorphism.

5.18. Let R^+ be the set of all positive real numbers. Show that the function $f: R^+ \to R$ defined by $f(x) = \ln(x)$ is an isomorphism of the semigroup $(R^+, \times)$ to the semigroup $(R, +)$, where × and + are ordinary multiplication and addition, respectively.

5.19. Let $(S, *)$ be a semigroup and A, a finite subet of S. Define $\hat{A}$ to be the set of all finite products of elements in A.

(a) Prove that $\hat{A}$ is a subsemigroup of $(S, *)$.

(b) Prove that $\hat{A}$ is the smallest subsemigroup of $(S, *)$
that contains A.

VI: Products and Quotients of Semigroups

6.1. Let $(S, *)$ and $(T, *)$ be commutative semigroups. Show that $S \times T$ is also a commutative semigroup.

6.2. Let $(S, *)$ and $(T, *)$ be semigroups. Show that the function $f: S \times T \to S$ defined by $f(s, t) = s$ is a homomorphism of the semigroup $S \times T$ onto the semigroup S.

6.3. Prove that if $(S, *)$ and $(T, *)$ are semigroups, then $(S \times T, *)$ is a semigroup, where $*$ is defined by $(s_1, t_1) * (s_2, t_2) = (s_1 * s_2, t_1 * t_2)$.

6.4. Determine whether the relation R on the semigroup S is a congruence relation for the following: -

(a) $S = Z$ under the operation of ordinary addition; aRb if and only if $a + b$ is even.

(b) S is the set of all rational numbers under the operation of addition; $a/b\ R\ c/d$ if and only if $ad = bc$.

(c) $S = Z$ under the operation of ordinary addition; aRb if and only if $a \equiv b (mod\ 3)$.

(d) $S = Z^+$ under the operation of ordinary multiplication; aRb if and only if $|a - b| \leq 2$.

(e) $S = \{0,1\}$ under the operation $*$ defined by the table. aRb if and only if $a * a = b * b$. (Hint: Observe that if x is any element in S, then $x * x = 0$.)

$*$	0	1
0	0	1
1	1	0

6.5 Given $S = \{3k + 1, k \in Z^+\}$ is a semigroup under the operation of ordinary multiplication, and R an equivalence relation on S defined by aRb if and only if $a \equiv b (mod\ 5)$. Identify the quotient semigroups S/R.

6.6. Show that the composition of two congruence relations on a semigroup need not be a congruence relation.

6.7. Describe the quotient semigroup for S and R given $S = Z$ under the operation of ordinary addition; aRb if and only if $a \equiv b (mod\ 3)$.

6.8. Describe the quotient semigroup for $S = Z$ with ordinary addition and R defined by aRb if and only if $a \equiv b (mod\ 5)$.

6.9. Consider the monoid $S = \{e, a, b, c\}$ with the following operation table.

*	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	c	b	c
c	c	b	b	a

Consider the congruence relation
$R = \{(e,e), (e,a), (a,e), (a,a), (b,b), (b,c)\ (c,b), (c,c)\}$ on S.
(a) Write the operation table of quotient monoid S/R.
(b) Describe the natural homomorphism $f_R: S \to S/R$.

6.10. Given $S = Z$ under the operation of ordinary addition; aRb if and only if a and b are both even or a and b are both odd. Describe the quotient semigroup for S and R. Prove or disprove that Z_2 is isomorphic to this semigroup.

6.11. Consider the semigroup $S = \{a, b, c, d\}$ with the following operation table.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Consider the congruence relation R on S given by
$R = \{(a,a), (a,b), (b,a), (b,b), (c,c), (c,d), (d,c), (d,d)\}$.
(a) Write the operation table of the quotient semigroup S/R.
(b) Describe the natural homomorphism $f_R: S \to S/R$.
(c) Prove or disprove that Z_4 is isomorphic to the semigroup.

6.12. Prove the fundamental homomorphic theorem.

<u>VII: Groups and subgroups</u>

7.1. Determine whether the set together with the binary operation is a group. If it is a group, determine if it is Abelian; specify the identity and the inverse of a generic
element.
(a) Z, where $*$ is ordinary multiplication.
(b) Q, the set of all rational numbers under the operation of
addition.
(c) R, under the operation of multiplication.
(d) Z+, under the operation of addition.
(e) The set of odd integers under the operation of multiplication.
(f) The set P(S), where S is a nonempty set , $A * B = A \bigoplus B$. (the symmetric difference of A and B, defined as the set of all elements that belong to A or to B, but not to both A and B)

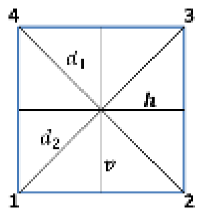
7.2 Let $S = \{x | x\ \in \mathbb{R}\ and\ x = 0, x =\ -1\}$ consider the following functions $f_i: S \to S, 1 \le i \le 6$;
$f_1(x) = x,\ f_2(x) = 1 - x,\ f_3(x) = \frac{1}{x},\ f_4(x) = \frac{1}{1-x},$
$f_5(x) = 1 - \frac{1}{x}, \quad f_6(x) = \frac{x}{x-1}$. Show that $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a group under the operation of composition. Give the multiplication table of G.

7.3. Consider S_3, the group of symmetries of the equilateral triangle, and the group of the previous question, Prove or disprove that these two groups are isomorphic.

7.4. Let $(G,*)$ be the Abelian group, with $G = \{set\ of\ non - zero\ real\ numbers\}$ and $a * b = \frac{ab}{2}$. Solve the following equations:
(a) $3 * x = 4$ (b) $y * 5 = -2$

7.5. Let $i = \sqrt{-1}$, $S = \{1, -1, i, -i\}$ Consider the group $(S,*)$, where $*$ is complex number multiplication. Is this group Abelian? 17. Find all subgroups of group $(S,*)$.

7.6. Consider the square shown opposite. The symmetries of the square are as follows:



Rotations f_1, f_2, f_3, and f_4 through 0°, 90°, 180°, and 270°, respectively, f_5 and f_6, reflections about the lines v and h, respectively f_7 and f_8, reflections about the diagonals d_1 and d_2 respectively. Write the multiplication table of D, the group of symmetries of the square.

7.7. Let G be a finite group with identity e, and let a be an arbitrary element of G. Prove that there exists a nonnegative integer n such that $a^n = e$.

7.8. Let G be the group of integers under the operation of addition, and let $H = \{3k | k \in Z\}$. Is H a subgroup of G?

7.9. Let G be an Abelian group with identity e, and let $H = \{x | x^2 = e\}$. Show that H is a subgroup of G.

7.10. Let G be a group, and let $H = \{x | x \in G\ and\ xy = yx\ \forall y \in G\}$. Prove that H is a subgroup of G.

7.11. Let A_n be the set of all even permutations in the set of all permutations of n elements, S_n. Show that A_n is a subgroup of S_n.

7.12. Find all subgroups of D, the group of symmetries of the square.

7.13. Prove that the function $f(x) = |x|$ is a homomorphism from the group G of nonzero real numbers under multiplication to the group G of positive real numbers under multiplication.

7.14. Let G be a group. Show that the function $f: G \to G$ defined by $f(a) = a^2$ is a homomorphism if and only if G is Abelian.

7.15. Let G be a group and let *a* be a fixed element of G. Show that the function $f_a: G \to G$ defined by $f_a(x) = axa^{-1}$, for $x \in G$, is an isomorphism.

7.16. Let G be a group. Show by mathematical induction that if $ab = ba$, then $(ab)^n = a^n b^n$ for $n \in Z^+$.

7.17. Prove that in the multiplication table of a group every element appears exactly once in each row and column. Also prove that this condition is necessary, but not sufficient, for a multiplication table to be that of a group.