Discrete Mathematics

6. Algebraic Systems

Algebra

- *Definition:*
  - An ***Algebra*** is characterized by specifying the following three components.
    1. a set called the ***carrier*** of the algebra,
    2. ***operators*** defined on the carrier, and
    3. (distinguished elements of the carrier, called the ***constants*** of the algebra.)

Closed with respect to operation

- *Definition:*
  - Let $\circ$ and $\triangle$ be binary and unary operations on a set T and let T' be a subset of T. Then T' is ***closed with respect to*** $\circ$, if $a, b \in T'$ implies $a \circ b \in T'$. The subset T' is ***closed with respect to*** $\triangle$, if $a \in T'$ implies $\triangle a \in T'$.

Subalgebra

- *Definition:*
  - Let $A=<S, \circ, \triangle, k>$ and $A'=<S', \circ', \triangle', k'>$ be algebras. Then A' is a ***subalgebra*** of A if
    1) $S' \subseteq S$
    2) $a \circ' b = a \circ b$ for all $a, b \in S'$;
    3) $\triangle' a = \triangle a$ for all $a \in S'$;
    4) $k' = k$.

Identity and zero

- *Definition:*

  Let $\circ$ be a binary operation of S.

  - An element $1 \in S$ is an ***identity*** (or ***unit***) for the operation $\circ$ if every $x \in S$,

    $$1 \circ x = x \circ 1 = x$$

    An element $0 \in S$ is a ***zero*** for the operation $\circ$ if for every $x \in S$

    $$0 \circ x = x \circ 0 = 0$$

Identity and zero (cont.)

- *Definition:*

  Let $\circ$ be a binary operation on S.

  - An element 1_l (1_r) is a ***left (right) identity for the operation*** $\circ$ if for every $x \in S$,

    $1_l \circ x = x$ ($x \circ 1_r = x$)

    An element 0_l (0_r) is a ***left (right) zero for the operation*** $\circ$. If for every $x \in S$.

    $0_l \circ x = 0$ ($x \circ 0_r = 0$)

Inverse

- *Definition:*
  - Let $\circ$ be a binary operation on S and 1 an identity for the operation $\circ$.
  - If $x \circ y = 1$, then x is a ***left inverse*** of y and y is a ***right inverse*** of x with respect to the operation $\circ$.
  - If both $x \circ y = 1$ and $y \circ x = 1$ then x is an ***inverse*** of y with respect to the operation $\circ$.

Semigroup

- *Definition:*
  - A ***semigroup*** is an algebra with signature $<S, \circ>$ where $\circ$ is a binary associative operation.

    $$a \circ (b \circ c) = (a \circ b) \circ c$$
- *Theorem:*
  - If $<S, \circ>$ is a semigroup and $<T, \circ>$ is a subalgebra of $<S, \circ>$, the $<T, \circ>$ is a semigroup.

Monoid

- *Definition:*
  - A ***monoid*** is an algebra with signature $<S, \circ, 1>$ where $\circ$ is a binary associative operation on S and *1* is an identity for the operation $\circ$. i.e. the following axioms hold for all elements *a, b, c*$\in S$;

$$a \circ (b \circ c) = (a \circ b) \circ c$$

$$a \circ 1 = a$$

$$1 \circ a = a$$

Group

- ***Definition:***
  - A ***group*** is an algebra with signature

    $<S, \circ, \bar{}, 1>$ such that $\circ$ is an associative binary operation on S, the constant 1 is an identity for the operation on $\circ$ and $\bar{}$ is a unary operation defined over S such that for all $x \in S$, $\bar{x}$ is an inverse for x with respect to $\circ$.
- *Theorem:*
  - Let $<S, \circ, \bar{}, 1>$ be a group. Every element of S has a unique inverse in S.

Homomorphism

- *Definition:*
  - Let $A=<S, \circ, \triangle, k>$ and $A'=<S', \circ', \triangle', k'>$ be two algebras with the same signature and let the function $h:S \rightarrow S'$ be such that

$$h(x \circ y)=h(x) \circ' h(y)$$

$$h(\triangle x)=\triangle' h(x)$$

$$h(k)=k'$$

  - then h is called ***homomorphism*** for A to A'.

Homomorphism

- *Definition:*
  - *h* is ***epimorphism*** if *h* is onto and homomorphism.
  - *h* is ***monomorphism*** if *h* is one-to-one and homomorphism.
  - *h* is ***isomorphism*** if *h* is bijection and homomorphism.

Congruence relation

- *Definition:*
  - Given an algebra $A=<S, \circ, \triangle>$, an equivalence relation E on S is a ***right (left) congruence relation*** on A iff for every x, y, and z in S.

$$<x, y> \in E \Rightarrow <x \circ z, y \circ z> \in E \text{ for all } z \in S$$

$$(<x, y> \in E \Rightarrow <z \circ x, z \circ y> \in E \text{ for all } z \in S)$$

$$<x, y> \in E \Rightarrow <\triangle x, \triangle y> \in E$$

Congruence relation (cont.)

- *Definition:*
  - Given an algebra $A=<S, \circ, \triangle>$, an equivalence relation E on S is a congruence relation on A iff it is ***left and right congruence relation on A.***
- *Theorem:*
  - Let $A=<S, \circ>$ be an algebra with a binary operation $\circ$ and let E be an equivalence relation on S. Then E is a congruence relation on A iff for every x_1, x_2, y_1, and y_2 in S,

$$<x_1, x_2>\in E \wedge <y_1, y_2>\in E \Rightarrow <x_1 \circ y_1, x_2 \circ y_2>\in E$$

Lattices

- *Definition:*
  - A poset is a ***lattice*** if every pair of elements has a lub (join) and a glb (meet).

- *Theorem:*

  Let $<L, \leq>$ be a lattice, For any $a, b, c \in L$,

  (i) $a*a=a$ *(i′)* $a+a=a$ *(idempotent)*

  (ii) $a*b=b*a$ *(ii′)* $a+b=b+a$ *(Commutative)*

  (iii) $(a*b)*c= a*(b*c)$ *(iii′)* $(a+b)+c= a+(b+c)$ *(Associative)*

  (iv) $a*(a+b)=a$ *(iv′)* $a+(a*b)=a$ *(Absorption)*

Lattices (cont.)

- *Theorem:*
  - Let $<L, \leq>$ be a lattice for any $a, b \in L$, the following property holds.

    $a \leq b \Leftrightarrow a*b=a \Leftrightarrow a+b=b$
- *Theorem:*
  - Let $<L, \leq>$ be a lattice, For any $a, b, c \in L$, the following properties hold.

    $b \leq c \Rightarrow a*b \leq a*c,\ a+b \leq a+c$

Lattices (cont.)

- *Theorem:*
  - Let $<L, \leq>$ be a lattice, For any $a, b, c \in L$, the following properties hold.

    $a \leq b \wedge a \leq c \Rightarrow a \leq b+c$

    $a \leq b \wedge a \leq c \Rightarrow a \leq b*c$

    $b \leq a \wedge c \leq a \Rightarrow b*c \leq a$

    $b \leq a \wedge c \leq a \Rightarrow b+c \leq a$
- *Theorem:*
  - Let $< L, \leq>$ be a lattice, For any $a, b, c \in L$, the following inequalities hold.

    $a+(b*c) \leq (a+b)*(a+c)$

    $(a*b)+(a*c) \leq a*(b+c)$

Lattices (cont.)

- *Theorem:*

  Let $<A, *, +>$ be an algebra which satisfies the

  1. Idempotent law, $(a*a=a,\ \ a+a=a)$
  2. Commutative law, $(a*b=b*a,\ \ a+b=b+a)$
  3. Associative law, $(\ (a*b)*c= a*(b*c),\ \ (a+b)+c= a+(b+c)\ )$
  4. Absorption law $(\ a*(a+b)=a,\ \ a+(a*b)=a\ )$

  Then there exists a lattice $<A, \leq>$, such that * is a glb, + is a lub, and is $\leq$ defined as follows:

  $x \leq y$ iff $x*y=x$

  $x \leq y$ iff $x+y=y$

- *Lemma:*
  - $x*y=x \Leftrightarrow x+y=y$

Lattices (cont.)

- *Definition:*

  A ***lattice*** is an algebraic system $\langle L, *, + \rangle$ with two binary operations * and + on L which are both (1) commutative and (2) associative and (3) satisfy the absorption law.

- *Definition:*

  Let $\langle L, *, + \rangle$ be a lattice and let $S \subseteq L$ be a subset of L. The algebra $\langle S, *, + \rangle$ is a ***sublattice*** of $\langle L, *, + \rangle$ iff S is closed under both operations * and +.

Lattices (cont.)

- *Definition:*

  Let $<L, *, +>$ and $<S, \wedge, \vee>$ be two lattice. A mapping $g:L \rightarrow S$ is called a ***lattice homomorphism*** from the lattice $<L, *, +>$ to $<S, \wedge, \vee>$ if for any $a, b \in L$, $g(a*b)=g(a) \wedge g(b)$ and $g(a+b)=g(a) \vee g(b)$.

- *Definition:*

  Let $<P, \leq>$ and $<Q, \leq'>$ be two partially ordered sets, A mapping $f: P \rightarrow Q$ is said to be ***order-preserving*** relative to the ordering $\leq$ in P and $\leq'$ in Q iff for any $a,b \in P$ such that $a \leq b$, $f(a) \leq' f(b)$ in Q.

Lattices (cont.)

- *Definition:*

  Two partially ordered sets $<P, \leq>$ and $<Q, \leq'>$ are called ***order-isomorphic*** if there exists a mapping $f:P \rightarrow Q$ which is bijective and if both f and f^{-1} are order-preserving.

- *Definition:*

  A lattice is called ***complete*** if each of its nonempty subsets has a least upper bound and a greatest lower bound.

Lattices (cont.)

- *Definition:*

  The least and the greatest elements of a lattice, if they exist, are called the ***bounds*** of the lattice, and are denoted by *0* and *1* respectively.

- *Definition:*

  In a bounded lattice $<L, *, +, 0, 1>$, an element $b \in L$ is called a ***complement*** of an element $a \in L$, if $a*b=0$, $a+b=1$.

- *Theorem:*

  1(0) is the only complement of *0(1)*.

Lattices (cont.)

- *Definition:*

  A lattice $<L, *, +, 0, 1>$ is said to be a ***complemented lattice*** if every element of L has at least one complement.

- *Definition:*

  A lattice $<L, *, +>$ is called a ***distributive lattice*** if for any $a, b, c \in L$,

  $$a*(b+c)=(a*b)+(a*c) \qquad a+(b*c)=(a+b)*(a+c)$$

- *Theorem:*

  Every chain is a distributive lattice.

Exercise

1. Let the algebra, $A=\langle I, + \rangle$, where I is a set of integers and + is a binary addition operation. For the binary relations R on I where$(x, y) \in R$ if and only if $|x-y|<10$, prove or disprove that relation is a congruence relation on A.

2. Let $\langle R,+,0 \rangle$ and $\langle R,\cdot,1 \rangle$ be two algebra where R is a set of reals, + is a binary addition, and ·is a binary multiplication. When the function, $f:R \rightarrow R$, is defined such that $f(x) = 2x$, answer the following with justification.
   - (a) Is f homomorphism from $\langle R,+,0 \rangle$ to $\langle R,\cdot,1 \rangle$?
   - (b) Is f injective (one-to-one)?
   - (c) Is f surjective (onto)?