Rings and Semi Rings

Dr. P. Gurivi Reddy
Reader in Mathematics, SKR & SKR Govt. College for Women (A), Kadapa

***Abstract*—Algebraic systems endowed with a partial or full order met with in several disciplines of mathematics. In recent times the study of partially ordered semigroups, groups, semirings, semi modules, rings and fields have been increasing widely. Though ring theory and field theory are two important developed theories in algebra, semiring theory and semi module theory have been slower to develop but it is now attracting the attention of several algebraists due to its applications to theoretical computer science, optimization theory, automata theory, formal language theory and the mathematical modelling of quantum physics.**

I. INTRODUCTION

The concept of semiring was first introduced by Vandiver in 1934. However, the developments of the theory in semirings have been taking place since 1950. The theory of rings and the theory of ‘semigroups have considerable impact on the developments of the theory of semirings. The works of eminent people like s. Bourne [4,5] P; J. Allen (1,2), K. lseki (9, lO,11) M.P. Grillet (6.14) H.E. Stone (18) and T.J. Weinert (20,21) are to be mentioned in the theory of semirings using ring theory techniques. P.H. Karvellas (13). M. Satyanarayana (15) H.J. Weinert (19) Andre Barbuda (3) John Zelemikow (22) and J. Hanumanthachari and K. Venuraju (7) have contributed to the theory of semirings using semigroup techniques. Recently the semiring theory has prompted some developments in ordered semigroups. In this direction the works of H.J.Weinert (19). M. Sathyanarayana (16,17), J. tianumanthachari, K. Venuraju (8) and H.J. Weinert (19), D.Umamaheswar Reddy (23) N.Fathimoon (24) T. Vasanthi (25), G. Shobhalatha (26) are to be mentioned.

The theory of ideals and, quasi-ideals for semirings has been studied by lseki (9,10,11). Historically semirings first appear implicitly in Dedkind [27] and later in Macalay [32], Noether 1121 and Lorenzen in connection with the study of ideals of a ring. They also appear in lbert [28J and Huntington [29]. However, semirings first appear explicitly I Vandiver [30], also in connection with the axiomatization of arithmetic of natural numbers. Semirings have been studied by various researches in an attempt to broaden techniques coming from semigroup theory or ring theory or in connection with applications.

The basic concept like binary operation. an algebraic structure. semigroups, semirings, power set, power semirings, ordered relation, partially ordered relation, Ideals, principal Ideals. maximal ideals, quasi-ideals, prime ideals, power semirings, Boolean algebra. vector space, linearly dependent, linearly independent, basis, order semirings.

Algebraic preliminaries:

Definition: A binary operation '.' on a set S is a mapping from SxS to S. That is. '.' is a rule which assigns to each ordered pair of elements from S an element of S.

Definition: A group (G, .) or simply G consists of a set with a binary operation '.' on G satisfying the following properties.

(i) For every a,b,c ∈ G. ab(c)=a(bc). (Associative)

(ii) There exists an element e ∈ G such that every a in G, a.e=e.a=a(Identity)

(iii) For every a ∈ G , there exists an element a^{-1} in G such that a a^{-1} =a^{-1} a=e (Inverse)

Definition: A group G is abelian (or commutative) if, a.b=b.a for all

a,b ∈ G

Note that a group G is called an additive group when the operation

is additive (+), where as a group G is called a multiplicative group when the operation is multiplicative (*). In a group with an additive operation,

we have a + (-a) =(-a)+a=O. where the inverse element of a is written as -

a. In this case, the identity of' element e is 0. Under the multiplicative
operation, the identity element e is 1 and inverse element of a is written
as a^{-1}', so that a a^{-1}=a^{-1} a= I.
Definition: Let G be a group. If G has finite number of elements say n, then we say that the order of G is n. We write this symbolically by o(G)=n, and in this case we say G is a finite group.

Definition: A nonempty subset H of' a finite group G is a subgroup if H is a group with the same binary operation on G.

Theorem: Let G be a group with binary operation, and let g be an element of G. Then H= {g is an integer} is a subgroup of G. A group G is said to be cyclic if there exists an element g ∈G such that every element of G can be written as g" for some integer n. In this case, G is called the cyclic group generated by g and g is called a generator of G. I f H is a subgroup of the cyclic group G, then H is called a cyclic subgroup of G.

Corollary: I f G is a finite group of order n, then g" =e for all g E G. A proof can be found in any group Theory books.

Corollary: The order of every element of a finite group is a divisor of the order of the group.
A proof can be found in any group Theory books.

Corollary: I f G is a finite group of order p where p is a prime integer, then G is cyclic and every element of G except the identity is a generator of G.
A proof' can be found in any group theory books.

Definition: A homomorphism from (G_1,.) to (G2, *) is a mapping from G_1 to G2 such that f(ab)= f(a)* f(b). for all a,b ∈G/

Definition: Let (G_1,.) and (G_2,*) be groups and let j be a homomorphism from G_1 to G_2. If f is both one-one and onto, then f is called an isomorphism.
If' f is an isomorphism, then GI and G2 are said to be isomorphic, and we write $G_1 = G_2$.

Rings, Fields and Relations:
Definition: A ring is a set K together with two binary operations + and - called addition and multiplication. such that
1. (R, +) is an abelian group
2. The product r, s of any two elements r, s ∈R is in R and multiplication is associative.
3. For all r, s, t ∈R, r.(s+t)=r.s + r.t and (r + s)t= r t + st (distributive law).
We denote the ring by (R, +) or simply by R. In general, the neutral element in (K, +) will always be denoted by 0, the additive inverse of r ∈K is - r. Instead of r.s we will denote it by rs. Clearly these rings are "associative rings". Let R be a ring, K is said to be commutative, if a .b = b .a for all a, b ∈ R such that 1.r=r.1 for all r ∈R, then 1 is called the identity (or unit) element. I f r .s = 0 implies r = 0 or s = 0 for all r, s E R then R is called integral. A commutative integral ring with identity is called in integral domain. If R\ (0) is a group then R is called a skew field or a division ring. If moreover, R is commutative we speak of a field. The characteristic of R is the smallest natural number k with kr = r+. . ..+r (k times) equal to zero for all r E R. We then write k = characteristic R. If no such k exists we put characteristic R=O.

Example: Q be the set of all rationals. (Q, +,) is a field of characteristic 0.

Example: Let 7, be the set of integers. (Z, + , -) is a ring which is in fact an integral domain.

Example: Let Z28 = (0, 1. 2, ... 27). Z28 with usual addition and multiplication modulo 28 as a group. Clearly Z∈g is a commutative ring with 7.4 =0 (mod 28) that is Z28 has zero divisors.

Example: Let Z23= (0, 1, 2, ... 22) be the ring of integers modulo 23. Z23 is a field of characteristic 23.

Definition: Let F be a field. A proper subset S of F is said to be a subfield if S itself is a field under the operations of F.

Definition: Let F be a field, If F has no proper subfields then F is said to be a prime field.

Example: Z, = {0, 1. 2 ..... p-1} where p is a prime, is a prime field of characteristic p.

Example: Let Q be the field of rationals. Q has no

proper subfield. Q is the prime field of characteristic 0; all prime fields of characteristic 0 are isomorphic to Q.

Example: Let R be the field of reals. R has the subset Q ∈ R and Q is a field: so R is not a prime field and characteristic K=O.

Definition: Let R be any ring. A proper subset S of R is said to be a subring of R if's is a ring under the operations o1'R.

Example: Let {0, 1. 2, ... 19) is the ring of integers modulo 20.

Example: Let Z be the ring of integers 5Z ⊂ Z is the subring of Z.

Example: Let R be a commutative ring and R[x] be the polynomial ring. R ∈ R[x] is a subring of R[x]. In fact R[x] is an integral domain if and only if R is an integral domain.

Definition: Let R and S be any two rings. A map f: R +S is said
to be a ring homomorphism if f(a + b)= f(a)+ f(b).

Definition: Let R be a ring. 1 a non-empty subset of R is called right
(left) ideal of R if
1 I is a subring.
2. If I is simultaneously both n right and a left ideal of R we say I is an ideal
of R. Thus ideals are subrings but all subrings are not ideals.

Example: Let Z, be the ring of integers, pZ = (0, + p, 12p,. . .) for any p
∈ Z is an ideal of'Z.

Example: Let R[x) be a polynomial ring. P(x) = po + P1 + . - ..+ pn' be a
polynomial of degree n (p, * 0). Clearly p(x) generates an ideal. We leave
if for the reader to check this fact. We denote the ideal generated by p(x)
by (PW.)

Definition: Let 4: R 4 R' be a ring homomorphism the kernel of 4 denoted by ker 4 ={x ∈ R/ 4 (x) = 0) is an ideal of R.

Definition: Let R be any ring, I an ideal of R. The set R/I = (a + I / a E R) is defined as the quotient ring. For this quotient ring, 1 serves as the additive identity.

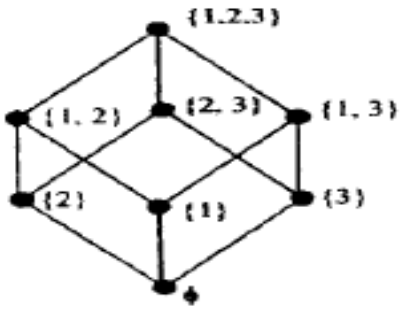
Definition: Let A and B be non-empty sets. A relation R from A to B is a subset of A x B. Relations from A to A are called relations on A.
A relation R on a non-empty set A may have some of the following
properties:
R is reflexive if for all a in A we have aRa.
K is symmetric if' for a and b in A: aRb implies bRa.
R is anti symmetric if for all a and b in A: aRb and bRa imply a = b.
R is transitive if for a, b, c in A: aRb and bRc imply aRc.
A relation R on A is an equivalence relation if R is reflexive, symmetric
and transitive.

Definition: A relation R on a set A is called a partial order (relation) if R is reflexive, anti symmetric and transitive. In this case (A, R) is a partially ordered set or poset. We denote the partial order relation by r or z.

Definition: A partial order relation I on A is called a total order if
for each a, b E A, either a ≤ b or b ≤ a. (A, I) is called a chain or a totally
ordered set.

Example: Let A = {1, 2, 3, 4, 7), (A, 5) is a total order, Here ' s ' is the usual "less than or equal to" relation. Hasse diagram of the poset A is as follows:

Example: Let X = { 1. 2, 3), the power set of X is denoted by P(X) = { 4, X, {a}, { b}, {c), {a,b), {a,c)). P(X) under the relation ' c ' "inclusion" as subsets or containment relation is a partial order on P(X). Hasse diagram of the poset P(X) described is as follows

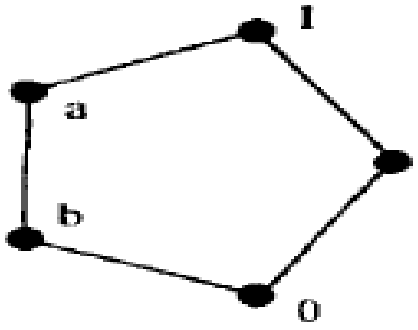


Definition: Let (A, ≤) be a poset and B G A.
i. a ∈ A is called an upper bound of R if and only if S, r all be B, b5a.
ii. a ∈A is called a lower bound of B if and only if for all b∈B. a~b.
I . The greatest among the lower bounds, whenever it exists is called the infimum of B, and is denoted by inf B.
iv. The least upper bound B whenever it exists is called the supremum of H and is denoted by sup 13.

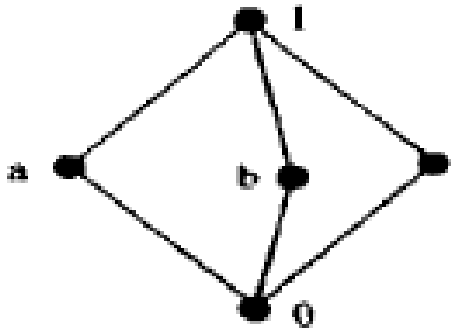
Result:
1. Every ordered set is lattice ordered.
2. In a lattice ordered set (L, ≤) the following statements are equivalent for all x and y in L.
a. x ≤y
b. Sup (x,y) = y
c. Inf(x,y) = x.
A proof can be found in any discreet mathematical structure's textbooks.

Definition: An algebraic lattice (L, ∩, U) is a non-empty set L with two binary operations n join) and u (meet) (also called union or sum and intersection or product respectively) which satisfy the following conditions for all x,y,z ∈L.
Two applications namely x∩x = x n (x u (x n y)) = x lead to the
additional condition L, x n x = x,x u x = x.L, is the commutative law, Id, is
the associative law, I, is the absorption law and I, is the idempotent law.

Result:
1. Let (L, ≤) be a lattice ordered set. If we define x∩ y = inf(x,y) and
x u y = sup (x,y) then (L, ∩, U) is an algebraic lattice.
2. Let (I, ∩, U) be an algebric lattice. If we define x ∩ y if and only of
x n -V = x (or x 5 y if and if x u = y) then (L, ≤) is a lattice ordered set.
Thus it can be verified that the above result yields a one to one
relationship between algebric lattices and lattice ordered sets. Therefore A proof can be found in any discrete mathematical structures text books.
Example: L, be a lattice given by the following Hasse diagram:



This lattice will be called as the pentagon Lattice.
Example: Let L, be the lattice given by the following Hasse diagram:



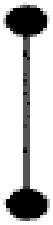
This lattice will be called as the diamond lattice.
Definition: Let (L, ≤) be a lattice. If' ≤ ' is a total order on L and L is lattice order, we call L a chain lattice. Thus we see in a chain lattice I, we have for every pair a,b € I, we have either a < b or b <a.

Example: Let L be [a, b] any closed interval on the real

line [a, b] under the total order is a chain lattice.

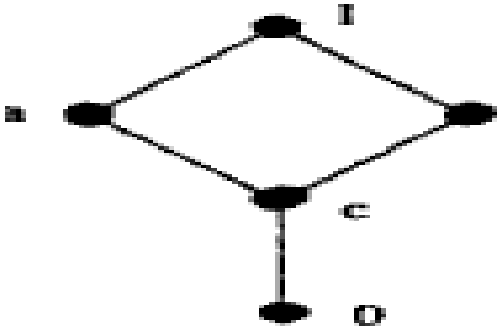
Example: [-a, I] is a chain lattice of infinite cardinality.

Example: 'Takc [0, I] = I, the two element set. L is the only 2 element
lattice and it is a chain lattice having the following Hasse diagram and will be denoted by C2

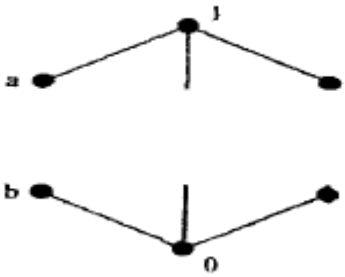


Definition: A non-empty subset S of lattice L is called a sub lattice of'L if S is a lattice with respect to the restriction of ∩ and u of L onto S.
A proof can be found in any discrete mathematical structures text books.

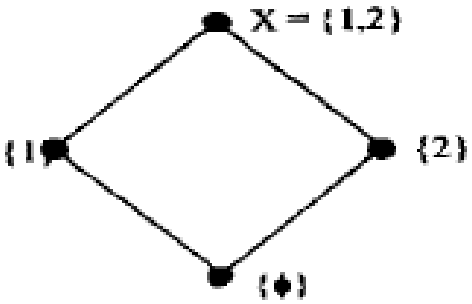
Example: 'The following lattice L given by the Hasse diagram is
distributive.



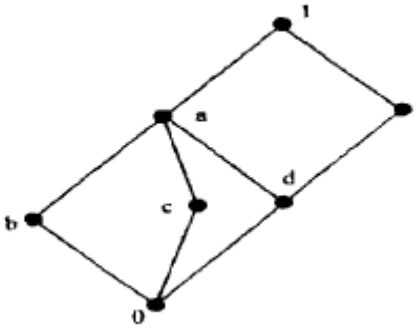
Example: The following lattice given by the Hass diagram is not a
distributive.



Example: P(X) the power set of X where X = { 1.2 } is a lattice with 4 elements given be the following Hasse diagram:

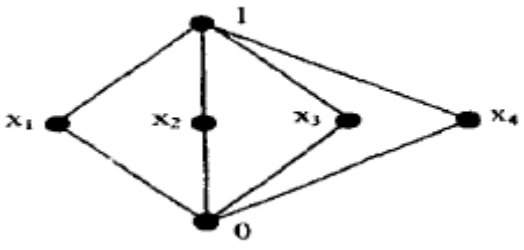


Example: The lattice Is modular and not distributive



Definition: A lattice L with 0 and 1 is called complement if for each x €j there is at least one element y, y is called a cornplernent of x.

Example: The lattice with the following Hasse diagram:



Result: If 1, is a distributive lattice then each x E L has at most one complement which is denoted by x'.
A proof can be found in any discrete mathematical structures text books.

Definition: A complemented distributive lattice is

called a Boolean algebra (or a Boolean lattice). Distributive in a Boolean algebra
guarantees the uniqueness of complements.

II. VECTOR ALGEBRA PRELIMINARIES

Definition: A vector space (or a linear space) consists of the following
1. A field F of scalars.
2. A set V of objects called vectors.
i. Addition is commutative, a+b=b+a
ii. Addition is associative; a+(b+c)=(a+b)+c
iii. There is a unique vector 0 in V, called the zero vector, such that a+0=0+a= 0
iv. A rule (or operation) called scalar multiplication which associates with each scalar c in 1; and a vector u in V a vector c cx in V called the product of 'c and cr in V It is important to state that vector space is a composite object consisting of a field F, a set of 'vectors' and two operations with certain special properties. The same set of vectors my be part of a number of distinct vector spaces. When there is no chance of confusion, we may simply refer to the vector space as V. We shall say 'V is a vector space over the field F'.

Example: Let R[x] be the polynomial ring where R is the field of reals. R[x] is a vector space over R.

Example: Let Q be the field of rationals and R the field of reals. R is a vector space over Q.
Note that Q is not a vector space over R

Definition: Let V be a vector space over the field F. Let P be a vector in V, p is said to be a linear combination of vectors a ,, ..., u ,, in V

Definition: Let V be vector space over the field F. A subspace of V is a subset W of V which is itself a vector space over F with the operations of vector addition and scalar multiplication on V.

Definition: Let S be a set of vectors in a vector space V. The subspace spanned by S is defined to be the intersection W of all subspaces of V which contain S. A set that is not linearly dependent is called linearly independent. I f the set S contains only finitely many vectors cr,.u, ... u,, we sometimes say that a,. tx, ... tx,, are dependent (or independent) instead of saying S is dependent (r independent).

Definition: 1,et V be a vector space over the field F.A basis for V is a linearly independent set of vectors in V, which spans the space V. The space V is finite dimensional if it has a finite basis which spans V, otherwise we say V is infinite dimensional.

Example: Let V=F x F x F = {(XI, XZ, x,)/ XI. x*, x3 E F } where F is a field. V is a vector space over F. The set P = {(I, 0, O), (0, I , 0), (0, 0,
1)) is a basis for V.

Example: Let F be a field and Fn = F x .... x F(n times), Fn is a vector space over F.A set of basis for F" over F is /I = { (1, 0, 0, ..., O), (0, I , 0,..., 0), (0, 0, 1 , 0, .. ., 0), ..., (0, 0, .., 0, l)}. It can be shown, Fn is spanned by P the dimension of Fn is n. We call this particular basis as the standard basis of Fn.

Example: Let F,[x] be a vector space over the field F; where F,[x] contains all polynomials of degree less or equal to n. Now P= { 1, x, x2,. . ... x") is a basis of Fn[x]. The dimension of Fn[xJ is n+l.

Example: Let F[xj be the polynomial ring which is a vector space over F.

2 Now the set { 1, x, x ,. . .., xn, ... } is a basis of F[x]. 'The dimension of the vector space F[x] over F is infinite.

Remark: A vector space V over F can have many basis but for that vector space the number of elements in each of the basis is the same; which is the dimension of V. A proof can be found in any vector algebra text books

Definition: Let L (V. W) denote the collection of all linear transformation of the vector space V to W, V and W vector spaces defined over the field F. L(V, W) is a vector space over F

REFERENCES

[1] A fundamental theorem of homomorphism l'or semirings". Proc. Amer. Math. Soc. 2 1 (1969), 4 12-4 16.
[2] "An extensior~ of the I-Iilbert basis theorem to

semirings". Publ. Math. Debreccn, 22(1975),
[3] 3 1-34. 3. 4. A. Batbedat S. Bourne "Algebras, pre-rings, semirings and rectangular bands". Seniigroup Forum. Vol. 30 (1984), 23 1-233.
[4] "The Jacobson radical of' a semiring." Proc. Nat. Acad. v01.37(195 1), 163- 170) Sci.. [J.S.A., "On the homornorphism theorem for semirings." Proc. Nat. Acad. Sci. LJ.S.A.. V01.38 (1952). 118-1 19.
[5] "Subdivision rings of a Semirings." Fund. Math., Vo1.67 (1 970). 67-76.