RINGS

View the lecture on YouTube: https://youtu.be/yKRbG9Y5pYY

RING EXAMPLES

Definition 1: Rings: A non –empty set R together with two binary operations denoted by $+$ and $.$ are called addition and multiplication which satisfy the following conditions is called a ring.

i. $(R,+)$ is an abelian group.

ii. Multiplication is an associative binary operation on *R*.

$a.(b.c) = (a.b).c,$ for all $a,b,c \in R$

iii. Multiplication is an distributive over addition.

$a.(b+c) = (a.b) + (a.c), (a+b).c = a.c + b.c \; \forall \; a,b,c \in R$

Example 1: Prove that the set F of all real numbers of the form $a + b\sqrt{2},$ where $a,b \in Q$ is a field under usual addition and multiplication of real numbers.

We have to show that F is a commutative ring with identity in which every non zero element has multiplicative inverse.

1. Closure: $a + b\sqrt{2}, c + d\sqrt{2}$ where $a,b,c,d \in Q$

   Then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in F.$

   $\therefore F$ is closed under $+$
2. Associativity: Since $+$ is associative in the set of real numbers and F is a subset, $+$ is associative in F.
3. Identity: $0 = 0 + 0\sqrt{2} \in F$ is the identity for $+$.
4. Inverse: For any element $a + b\sqrt{2} \in F$, there exists $-a - b\sqrt{2} \in F$ such that

   $(a+b)\sqrt{2} + (-a-b)\sqrt{2} = a - a + (b-b)\sqrt{2} = 0 + 0\sqrt{2}.$

Hence, the inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}.$

Also, $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$ for all $a + b\sqrt{2}, c + d\sqrt{2} \in F.$

$\therefore (F,+)$ is an abelian group.

Now, let $a + b\sqrt{2}$, and $c + d\sqrt{2} \in F.$

Then $(a + b\sqrt{2}).(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F.$

Thus F is closed under multiplication.

$1 = 1 + 0\sqrt{2} \in F$ and is the multiplicative identity.

Since the two binary operations are the usual addition and multiplication of real numbers, multiplication is associative and commutative and the two distributive laws are true.

Since, $(a+b\sqrt{2}).(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$

$= (ca+2db)+(da+cb)\sqrt{2}$

$= (c+d\sqrt{2}).(a+b\sqrt{2})$

Hence multiplication is commutative. The verification of associative and distributive law are straight forward.

To prove that multiplicative inverse exists for every non zero element of F .

Now let $a+b\sqrt{2} \in F-0$. Then a and b are not simultaneously 0.

Also, $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2}).(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2}$.

We claim that a^2-2b^2.

Case (i) $a \neq 0$ and $b = 0$, then $a^2-2b^2 = a^2 \neq 0$.

Case (ii) $a = 0$ and $b \neq 0,$ then $a^2-2b^2 = -2b^2 \neq 0$.

Case (iii) $a \neq 0$ and $b \neq 0.$ Suppose $a^2-2b^2 = 0,$

Then $a^2 = 2b^2 \Rightarrow \frac{a^2}{b^2} = 2$. Hence $\frac{a}{b} = \pm\sqrt{2}$.

Now, $\frac{a}{b} \in Q$ and $\sqrt{2} \notin Q$. This is a contradiction.

Hence, $a^2-2b^2 \neq 0$

$\therefore \frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b\sqrt{2}}{a^2-2b^2} \in F$ and is the inverse of $a+b\sqrt{2}$.

Hence F is a field.

Example 2: In $Z_6 = \{0,1,2,3,4,5\}, 2 \neq 0, 3 \neq 0$. But $2 \times_6 3 = 0$.

$\therefore 2$ and 3 are zero divisor. Hence $Z_6$is a ring with zero divisors.

Example 3: $(Q,+,.), (R,+,.), (C,+,.)$ are field.

But $(Z,+,.)$ is an integral domain but not a field.

Practice Example: Prove that $R = \{a+b\sqrt{2}, a,b \in Z\}$is an integral domain, but not a field under addition and multiplication.

Theorem 1: A ring Rhas no zero- divisors iff cancellation law is valid for multiplication in R.

Proof: Let R be a ring without zero- divisors. $ab = 0$

Let $ax = ay$ and $a = 0$.

$\therefore ax - ay = 0$. Hence $a(x - y) = 0$ and $a \neq 0$.

Since R has no zero-divisors, $x - y = 0$.

$\therefore x = y$. Thus cancellation law is valid in R.

Conversely, let the cancellation law be valid in R.

Let $ab = 0$ and $a \neq 0$, $ab = 0 \Rightarrow b = 0$, by cancellation law.

Hence R has no zero divisors.

Theorem 2: Every field is an integral domain.

Proof: Let R be a field.

To prove R is an integral domain, it is enough to prove that it has no zero divisors.

Suppose $a, b \epsilon R$ with $ab = 0, a \neq 0$, then there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

$ab = 0 \Longrightarrow a^{-1}.ab = a^{-1}.0 \Longrightarrow (a^{-1}a)b = 0 \Longrightarrow b = 0$.

If $b \neq 0$, then we can prove that $a = 0$.

$\therefore a.b = 0 \Longrightarrow a = 0$ or $b = 0$.

$\therefore R$ has no zero divisors.

Hence R is an integral domain.

Theorem 3: Every finite integral domain is a field.

Proof: Let $(R, +, .)$ be a finite integral domain.

$\therefore R$ is a commutative ring with identity and without zero divisors.

Claim: To prove R is a field, it is enough to prove that every non-zero element in R has multiplicative inverse.

Let $R = \{0,1, a_2, a_3, \ldots . a_n\}, a \in R$ and $a \neq 0$.

Multiplying the non-zero elements of R by a, we get the set $\{a.1, aa_2, aa_3, \ldots .. aa_n\}$.

These elements are non-zero and they are distinct.

Suppose $a.a_j = a.a_k, j \neq k$, then $a.(a_j - a_k) = 0$.Since $a \neq 0, a_j = a_k$,

which is a contradiction to the fact that a_k are distinct elements in R.

$\therefore a.a_j \neq a.a_k$

Since R is finite, these n elements are same as the n non-zero element in R in some order by pigeon hole principle.

$\therefore 1 = a.a_i$ for some $a_i \in R$. Since R is commutative, $a.a_i = a_i.a = 1$.

$\therefore$ Every non- zero element in R has multiplicative inverse.

Hence any finite integral domain is a field.

Definition 2: Let $(R, +, .)$ be a ring with unity 1. An element $u \in R$ is called a unit in R if there exists a $v \in R$ such that $u.v = v.u = 1$.

Example 4: In Z_4, 1 and 3 are the units.

In Z_5, $\{1,2,3,4\}$ are the set of units.

Theorem 4: Z_4 is an integral domain if and only if n is a prime.

Proof: Clearly Z_n is a commutative ring with identity. To prove that n is a prime.

Suppose n is a composite number.

Then there exists $1 < a < n,\ 1 < b < n$ such that $a.b = n$.

Let $a, b \epsilon Z_n$, and $a \neq 0, b \neq 0$,

$a \odot b = 0. \therefore n$ is a prime.

Conversely suppose n is a prime.

To prove that Z_n has no zero divisor.

Suppose Z_n has zero divisors.

Then there exists $a, b\ \in Z_n$, $a \neq 0, b \neq 0$ such that $a \odot b = 0$.

$1 \leq a, b\ \leq n$ and n divides $a.b$. That is , n divides a or n divides b.

Which is a contradiction. Since n is a prime.

$\therefore Z_n$ has no zero divisor.

Hence, Z_n is an integral domain.

Definition 3: Let $(R, +, .), (S, \oplus, \odot)$ be two rings. These two rings are said to isomorphic if there exists a map $f: R \to S$ such that

(i) f is one-one.

(ii) f is onto.

(iii) $f(a + b) = f(a) \oplus f(b)$ and $f(a, b) = f(a) \odot f(b)$ for all $a, b\ \in R$.

Theorem 5: Let R and S be two isomorphic rings, then the following hold:

(i) If R is commutative, then S is commutative.

(ii) If R has multiplicative identity, then S has multiplicative identity.

(iii) If R is an integral domain, so is S.

(iv) If R is a field, so is S.

Proof:

(i) Let $f: R \to S$ be an isomorphism between the two rings R and S let $a', b' \epsilon S$.

Since f is onto, there exists $a, b\epsilon R$ such that $(a) = a'$, and $f(b) = b'$.

Now, $a'b' = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b'a'$.

$\therefore$ S is a commutative ring.

(ii) Let $1 \epsilon R$ be the identity element of R.

Let $a' \epsilon S$. Then there exists $a \epsilon R$ such that $f(a) = a'$.

Now, $f(1) = a' = f(1)f(a) = f(1.a) = f(a) = a'$.

Similarly, $a' f(a) = a'$ and hence $f(1)$ is identity element in S.

$\therefore$ S is a ring with identity.

(iii) Let be R be an integral domain. Then by (i) and (ii) S is a commutative ring with identity.

To prove that S has no zero divisors.

Let $a', b' \epsilon S$ and let $a'.b' = 0$.

Since f is onto there exists $a, b \epsilon R$ such that $f(a) = a'$ and $f(b) = b'$

$\therefore a'b' = f(a)f(b) = f(ab) = 0 \Longrightarrow ab = 0.$ (Since f is $1 - 1.$)

$a = 0$ or $b = 0$ (since R is an integral domain).

f(a)=0 or $f(b) = 0 \Rightarrow a' = 0$ or $b' = 0$

S is an integral domain.

(iv) To prove that every non zero element in S has an inverse.

Let $a' \epsilon S$ and $a' \neq 0$. There exists $a \epsilon R - \{0\}$ such that $f(a) = a'$.

Now, $f(a^{-1})a' = f(a^{-1})a = f(a^{-1}a) = f(1)$.

Hence $f(a^{-1})$ is the inverse of a' in S

$\therefore$ S is a field.

Definition 1: Let $(R,+,.)$ be a ring. A non-empty subset S of R is called a subring of R if S is a ring with respect to the same binary operations $+$ and . defined in R.

Examples:

(i) $(2Z,+,.)$ is a subring of $(Z,+,.)$.

(ii) $(Z,+,.)$ is a subring of $(Q,+,.)$.

(iii)$(2Z,+,.)$ with $a*b=\frac{ab}{2}$ is a ring but not a subring of $(Z,+,.)$.

Theorem 6: Let $(R,+,.)$ be a ring. A non-empty subset S of R is called a subring of R if and only if $a-b\,\epsilon\, S$ and $a.b\,\epsilon\, S$.

Proof: Let $(R,+,.)$ be a ring. Then S itself is a ring under the same operations $+$, . as defined in R.

If $a,b\,\epsilon\, S$, then $-b\,\epsilon\, S$. Since S is a subring.

Hence $a+(-b)=a-b\,\epsilon\, S$. Also $a\,.\,b\,\epsilon\, S$.

Conversely, let S be a non-empty subset of R such that $a,b\,\epsilon\, S\Rightarrow a-b\,\epsilon\, S$ and $a.b\,\epsilon\, S$.

Since S is non-empty, take any element $x\epsilon\, S$. Then $x\,,x\,\epsilon\, S\Rightarrow x-x\,\epsilon\, S$ ie $0\,\epsilon\, S$.

Let a be any element in S.

Then $0,a\,\epsilon\, S\Rightarrow 0-a\,\epsilon\, S\Rightarrow -a\,\epsilon$ S. Clearly, $+$ in S is closed, associative and commutative. Also, . in S is associative and distributive over $+$.

Hence $(S,+,.)$ is a subring of R.

Theorem 7: The intersection of two subrings of a ring R is again a subring of R.

Proof: Let S_1, S_2 be two subrings of a ring R.

To prove that $S_1\cap S_2$ is a subring of R.

Since $0\in S_1$ and $0\in S_2$, we get $0\in S_1\cap S_2$.

$\therefore S_1\cap S_2$ is non-empty.

Let $,b\,\epsilon\, S_1\cap S_2$. Then $a,b\,\epsilon\, S_1$ and $a,b\,\epsilon\, S_2$.

$\therefore a-b\,,a.b\,\epsilon\, S_1$ and $a-b\,,a.b\,\epsilon\, S_2\Rightarrow a-b\,,a.b\,\epsilon\, S_1\cap S_2$

Hence $S_1\cap S_2$ is a subring of R.

Note: The union of two subrings of a ring need not be a subring.

Theorem 8: Let $(R,+,.)$ be a ring. Let S_1, S_2 be two subrings of a ring R. Then $S_1\cup S_2$ is a subring of R iff $S_1\subset S_2$ or $S_2\subset S_1$.

Definition : Left Ideal

Let R be a ring. A non- empty subset I of R is called a left ideal of R if

(i) $a, b \in I \implies a - b \in I$.

(ii) $r \in R, a \in I \implies ra \in I$.

Definition : Right Ideal

Let R be a ring. A non- empty subset I of R is called a right ideal of R if

(i) $a, b \in I \implies a - b \in I$.

(ii) $r \in R, a \in I \implies ar \in I$.

Definition : Ideal

Let R be a ring. A non- empty subset I of R is called an ideal of R if

(i) $a, b \in I \implies a - b \in I$.

(ii) $r \in R, a \in I \implies ra \in I$ and $ar \in I$.

Theorem 9: Every left ideal of R is a subring of R.

Proof: Let I be a left ideal of the ring R. Let $a, b \epsilon I$.

Then by definition $a - b \epsilon I$ and $a, b \epsilon I$.

Hence I is a subring of R.

Remark : A subring of a ring R need not be an ideal of R.

Example: Z is subring of Q, but Z is not an ideal of Q.

Since $8 \in Z$ and $\frac{1}{3} \in Q \implies 8.\frac{1}{3} \notin Z$.

Note: For any ring R, $\{0\}$ and R are always ideal of R called improper ideals. Other ideals are called proper ideals.

Theorem 10: A field has no proper ideals.

Proof: Let I be an ideal of the field F. Suppose $I \neq \{0\}$.

We shall prove that $I = F$. Since $I \neq \{0\}$, there exists a non-zero element $a \in I$. Also $a^{-1} \in F$ such that $a. a^{-1} = 1 \in I$.

Let $r \in F, 1 \in I \implies r. 1 \epsilon I$. Thus $F \subseteq I$.

But , $I \subseteq F$.

Hence, $I = F$.