Friday 11/18/05

Ring + Modules.

R:• abelian gp under +, 0 = identity, $-r$: inverse of r.
  • multiplication • which is association, with identity = 1
    $r.s \in R$, $r(s.t) = (r.s).t$
  • distributive laws $r.(s+t) = r.s + r.t$

Examples of Ring:
1. $R = \mathbb{Z}$
2. $R =$ a field $F \supset \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathbb{Z}/p\mathbb{Z}$
   where any $r \neq 0$ has a multiplicative inverse r^{-1}: $r.r^{-1} = 1$
3. $R = M_n(F)$ $n \times n$ matrices, $n > 1$, $r.s \neq s.r$ (non commutative)

NOTE: We will only study COMMUTATIVE rings. Where $r.s = s.r$ $\forall s, r$

For us, "ring" = "commutative ring"

3. $\mathbb{Z}/n\mathbb{Z}$ is a finite ring, which is not a field when n ≠ prime
   eg $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

Now consider $\{r \in R,$ r has a multiplicative inverse:
$\exists s$ st. $sr = rs = 1\} = R^* \subset R$

R^* : - abelian group with identity = 1 under multiplication
  - not closed under +
  - group of units of a ring R.
$R^* = F - \{0\}$ for $R = F$ a field.

Claim: The ring $R = \{0\}$ is a ring with $0 = 1$
All other rings have $0 \neq 1$

Pf) In general, if $a \in R$: $0.a = 0$
$0.a = (0+0).a = 0.a + 0.a$

Subtract $0 \cdot a$ from both sides of equation

$$0 = 0 \cdot a$$

Assume, $a \neq 0$ in R

If $0 = 1$, then $0 \cdot a = 1 \cdot a = a$

$$0 = a$$

Thus if $0 = 1$, all elements in $R = 0$: $R = \{0\}$

Otherwise, $0 \neq 1$, R has at least 2 elements.

Now consider $R \subset \mathbb{C}$. subsets of $\mathbb{C}$ which are closed under $+, \cdot$ which contains $0, -r, 1$.

Examples

1. $R = \mathbb{Z}$, $R^* = \mathbb{Z}^* = \langle \pm 1 \rangle$.

2. $R = \mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\}$: Gaussian integers

$(a+bi) + (c+di) = (a+c) + (b+d)i$

$(a+bi)(c+di) = (ac - bd) + (ad+bc)i$

$-(a+bi) = -a - bi$

$0 = 0 + 0i$

$1 = 1 + 0i$

$R^* = \langle \pm 1, \pm i \rangle$: cyclic group of order 4 generated by i.

$\{i, i^2 = -1, i^3 = -i, i^4 = 1\}$. Why?

Claim: If $a+bi$ is a unit in R, then $a^2 + b^2 = 1$

So either $\begin{cases} a = \pm 1, & b = 0 \to \pm 1 \\ b = \pm 1, & a = 0 \to \pm i \end{cases}$

Pf: Suppose $(a+bi)(c+di) = 1$

Complex conjugate $(a-bi)(c-di) = 1$

multiply these identities

$$(a+bi)(c+di)(a-bi)(c-di) = 1$$

$$(a^2+b^2)(c^2+d^2) = 1$$

a^2+b^2, c^2+d^2 are integers, positive

$\to a^2+b^2 = c^2+d^2 = 1$!

Ring Homomorphism : $f: R \to R'$

homomorphism of abelian groups: $f(a+b) = f(a)+f(b)$

preserves multiplication: $f(a \cdot b) = f(a) \cdot f(b)$

$f(1) = ?$

$\ker(f) \subset R$

$\{a \in R : f(a) = 0_R\}$: a subgroup of R under +

ker(f) is:

Closed under · by any element in R:

$a \in \ker f$, $b \in R$: $a, b \in \ker f$: $f(a \cdot b) = f(a) \cdot f(b) = 0 \cdot f(b) = 0 \in R'$

→ a new concept

thus ker f is a Ideal : $I \subset R$. subgroup under +, closed under multiplication by any element in R.

- Analogy : Ideal ↔ normal subgroup

kernel ↔ kernel.

Thus. we will define a quotient ring $R/I = R'$ and a hom $f: R \to R'$ with $\ker f = I$.

For example, if $R = \mathbb{Z}$, the ideals are $I = n\mathbb{Z}$

quotient ring : $\mathbb{Z}/n\mathbb{Z}$

→ In this quotient ring :

$(a + n\mathbb{Z})(b + n\mathbb{Z}) = ab + n\mathbb{Z}$

When is it well-defined ? ≅ when $n\mathbb{Z}$ is an ideal

Generalization of an ideal $I \subset R$. is an R-module M.

(1) abelian group with identity M

(2) scalar multiplication by $r \in R$ on $m \in M$

$r \cdot m \in M$.

$r(m+n) = rm + rn$

→ If R is a field F an R-module is just a vector space over F.