# Alg-27

$L, M \leq R$, a ring

$LM \overset{\text{def}}{=} \{lm : l \in L,\ m \in M\}$

Not $L(M+N) = LM + LN$ in gen.

Now $L$ & $M$ are two sided ideals of a commutative ring

$$LM = \left\{ \sum_{i=1}^{n} l_i m_i \ ; \ \forall n \geq 1, \ \forall l_i \in L, \ \forall m_i \in M \right\}$$

is an ideal of $R$

$LM$ is a subgroup of $R$

$\Rightarrow LM = ML$.

Algebra of ideals of commutative ring (play spectacular roles in Algebraic geometry & Algebraic number theory)

$K$ is a finite field, $\mathrm{Ch}\, K = p$

$\varphi_p : K \to K$ defined by

$\varphi_p(a) = a^p$, $a \in K$. Then

$\varphi_p$ is auto.

$\varphi_p$ is auto.

- $\varphi_p(a+b) = \varphi_p(a) + \varphi_p(b)$
- $\varphi_p(ab) = \varphi_p(a)\varphi_p(b)$

$\Rightarrow \varphi_p$ is homo

$a \in \ker \varphi_p \Rightarrow \varphi_p(a) = 0 = a^p$

$\Rightarrow a = 0$

---

$I \subseteq R$ ideal, $R$ a commutative ring with 1

Thm (1) $I$ is a prime ideal $\iff R/I$ is an integral domain

(2) $R/I$ is a field $\iff I$ is a maximal ideal.

$I$ is maximal $\Rightarrow$ $I$ is prime ideal

$\Leftarrow$

$\mathbb{Z} \supseteq I$ is an ideal

$I = n\mathbb{Z}$, $\mathbb{Z}/I$ is a ring $\mathbb{Z}/n\mathbb{Z}$ is integral domain $\iff n = p$ prime

$I = n\mathbb{Z}$ is a prime ideal

$\Leftrightarrow$ $n$ is prime

$n = p$

$p$ is prime $\Leftrightarrow p\mathbb{Z} = I$ is a maximal ideal

prime ideal $\not\Rightarrow$ maximal ideal

Ex. $R = \mathbb{Z}[x]$ is an integral domain

$I = (x) = \{x h(x) : h(x) \in \mathbb{Z}[x]\}$

$R$ is a commutative ring with $1$

$a_1 \dots a_n \in R$

$I = (a_1 \dots a_n) = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r_1 \dots r_n \in R\}$

$I$ is a prime ideal ($ab \in I \Rightarrow a \in I$ or $b \in I$)

$a(x)b(x) \in I \Rightarrow a(x)b(x) = x h(x)$

$x \mid x h(x) \Rightarrow x \mid a(x)b(x) \Rightarrow x \mid a(x)$ or $x \mid b(x)$

If $x \mid a(x) \Rightarrow a(x) = x h_1(x) \in I$

or $x \mid b(x) \Rightarrow b(x) = x h_2(x) \in I$

or $x \mid b(x) \Rightarrow b(x) = x\eta_2(x)$ ...

↑ irreducible poly (it corresponds to prime of integers)

So $I$ is a prime ideal

$I$ is not maximal

$I = (x) \subsetneq (2,x) = J \subsetneq \mathbb{Z}[x]$

$1 \notin (2,x)$

$1 = 2p(x) + xq(x)$

---

Generalize construction of $\mathbb{Q}$, the field of rationals, from $\mathbb{Z}$, an integral domain (such as $\mathbb{Z}/p\mathbb{Z}$, $F[x]$, ↑ field.

$R[x]$ is an integral domain where $R$ is an integral.

$R$ is an integral domain, $R[x]$ is integral $R[x_1][x_2] = R[x_1, x_2]$

$x_1$ & $x_2$ are indeterminate. ↑ integral domain!

dmain
yes

$R[x_1]$ = the ring of poly in the indeterminate $x_1$

$$f(x_1) = a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_m x_1^m$$

$a_0, \ldots, a_m \in R$.

---

$\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$. $b \in \mathbb{Z}$

$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$.

is an equivalence rel. on

$S = \mathbb{Z} \times \mathbb{Z}^* = \{(a,b) : a \in \mathbb{Z},\ b \in \mathbb{Z} - \{0\}\}$

$\frac{1}{2} = \frac{2}{4} = \frac{4}{8} = \cdots$

$[(1,2)] = \frac{1}{2}$

---

R is an integral domain (eg $\mathbb{Z}_p$ or $\mathbb{Z}[x]$)

$S = \{(a,b) : a \in R,\ b \in R - \{0\}\} = R \times R^*$

$(a,b), (c,d) \in S$, define

$(a,b) \sim (c,d) \iff ad = bc$.

equivalence relation

$(a,b)$

Then $\sim$ is an equivalence relation on $S$: (1) $(a,b) \sim (a,b)$

(2) $(a,b) \sim (c,d)$

$\Rightarrow (c,d) \sim (a,b)$

(3) $(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$

$\Rightarrow (a,b) \sim (e,f)$.

$[(a,b)]$, the equivalence class of $(a,b) \in S$

$$S/\sim \; = K = \{ [(a,b)] : (a,b) \in S \}$$

$K$ is a field under

$$[(a,b)] + [(c,d)] = [(ad+bc, bc)]$$ and

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

$\frac{a}{b} + \frac{c}{d}$

$\frac{a}{b} \cdot \frac{c}{d}$ ...

Then $K$ is a field under these sum & product.

$$[(a,b)] \equiv \frac{a}{b} \in K, \quad a \in R, \; b \in R - \{0\}$$

the field $K$ is also called the fraction field of $R$, and

$K = \mathrm{Frac}(R)$

the fraction field of $R$,
integral domain $K = \mathrm{Frac}(R)$

Ex $\mathbb{F}$ is a field, $\mathbb{F}[x]$ is an integral. $\mathrm{Frac}(\mathbb{F}[x]) = \left\{ \frac{f(x)}{g(x)} : g(x) \neq \text{the zero poly} \right\}$

$\mathbb{F}(x)$ is a field

$\mathbb{F}[x]$ is an integral domain

$\mathbb{Q}[\sqrt{2}]$ is an integral domain, infact it is a field, $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}[\sqrt{2}]$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are infinite fields of $\mathrm{ch}(K) = 0$ where $K = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$

$\mathrm{ch}(\mathbb{Z}_p) = p$

$\mathrm{Frac}(\mathbb{Z}_p[x]) \equiv \mathbb{F}_p(x)$ ← infinite field

$\mathrm{ch}(\mathbb{F}_p(x)) = p$

$\mathbb{Z}_p \equiv \mathbb{F}_p$

$\mathbb{F}$ is a finite field with $q$ elements. Then $q = p^n$ for some prime $p$ and some $n > 0$ integer.

$|\mathbb{F}| = q > 1$, $\mathbb{F}_p = \mathbb{Z}_p \subseteq \mathbb{F}$.

$\mathrm{ch}\,\mathbb{F} = p$ prime

$\mathbb{F}$ is a vector space over $\mathbb{Z}_p$

$\dim_{\mathbb{F}_p} \mathbb{F} = n$ $\quad \mathbb{F} \simeq (\mathbb{Z}_p)^n$ as v.s.

$= \mathbb{Z}_{p^n}$.

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ are ∞ as $\mathbb{Q}$-v.s. $\dim_{\mathbb{Q}}$