Alg-29

03 May 2021 12:47

Alg-29

Rational Root thm: Lang P141 #4

$f(x) \in \mathbb{Z}[x]$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$; $a_n \neq 0$

$(a_0, \dots a_n) = \mathbb{Z} \iff \gcd\{a_0, \dots a_n\} = 1$

If $f(\frac{r}{s}) = 0$, $(r,s) = 1$, then

$r \mid a_0$, $s \mid a_n$

Extension of arithmetic from $\mathbb{Z}$ to $\mathbb{F}[x]$, more generally to integral domain R

$\mathbb{F}$ ↑ field

$f(x) \mid g(x)$ in $\mathbb{F}[x]$ means

$\exists\ q(x)$ s.t. $g(x) = q(x) f(x)$.

Def R is an integral domain.

(1) $a, b \in R$, $b \neq 0$, $b \mid a$ (b divides a)

iff $a = cb$ for some $c \in R$.

(1) $a, b \ldots$,
iff $a = cb$ for some $c \in R$.

(2) $b, a \in R - \{0\}$. b is an associate of a iff $b = ua$ for some $u \in U(R)$ = the group of units of R.
($U(\mathbb{Z}) = \{1, -1\}$. (Write $b \sim a$.

Note $\sim$ is an equivalence relation its equivalence class is called the associate class

3. $p \in U(R)^c \cap R - \{0\}$ (nonunit & nonzero)
Lang 63 p145 is called a prime element of R
iff $p | ab \Rightarrow p | a$ or $p | b$ $\forall a, b \in R$

4 - $r \in U(R)^c \cap R - \{0\}$ is irreducible
iff $r = ab \Rightarrow a$ is a unit
or b is a unit.

Note (i) p is prime $\Rightarrow up$ is prime for $u \in U(R)$

(ii) r is irreducible $\Rightarrow ur$ is irr for $u \in U(R)$.

(ii) [illegible]

for $u \in U(R)$.

Thm Let R be a commutative ring with 1.

(1) $u \in U(R) \iff (u) = R$.

(2) $r \sim s$ i.e. $r = us$ for some $u \in U(R)$

$\iff (r) = (s)$

(3) $r \mid s \iff (s) \subseteq (r)$

(4) r properly divides s i.e. $\exists x \in U(R)^c$

s.t. $s = xr \iff (s) \subsetneq (r)$

(5) R is a PID (An integral domain in which every ideal is principal, generated by one element)

then

(1) $r \in R$ is irr $\iff (r)$ is maximal ideal

$\iff R/(r)$ is a field

(2) $p \in R$ is prime $\iff p$ is irr.

(3) $a, b \in R$ are coprimes i.e. rel. prime

$\iff ra + sb = 1$ for some $r, s \in R$

$\iff (a,d) = R$.

Ex In $\mathbb{Z}$ primes are exactly irr elements.

In $\mathbb{F}[x]$ primes are exactly irr. poly

Thm Let R be an integral domain
Then every prime is irreducible

prime $\implies$ irr.

$\Leftarrow$ is false

There is an integral dom R
and an irr. element $r \in R$
which is not prime.

Ex $\mathbb{Z}[\sqrt{-3}]$ or $\mathbb{Z}[\sqrt{-5}]$
both are integral domains
and its members are
called quadratic integers

called quadratic integers

$\mathbb{Z}$ is called rational integers

$a+b\sqrt{-3}$

To find $r \in \mathbb{Z}[\sqrt{-3}]$ which is irr but not prime: take $r = 1+\sqrt{-3}$

r is irr in $\mathbb{Z}[\sqrt{-3}]$

$r = xy$, for $x, y \in \mathbb{Z}[\sqrt{-3}]$

then show either x is a unit or y is a unit

$\underline{r \text{ is not prime}}$ $\exists\, x, y \in R$ s.t. $r \mid xy$ but $r \nmid x$ and $r \nmid y$.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2^2$

$1+\sqrt{-3} \mid 2^2$ but $\underbrace{1+\sqrt{-3} \nmid 2}$.

suppose $2 = (1+\sqrt{-3})(a+b\sqrt{-3})$
$= (a-3b) + (a+b)\sqrt{-3}$

$\Rightarrow a-3b = 2$ and $a+b=0$
$a=-b$

$\Downarrow$

$-4b = 2$ has no sol in $\mathbb{Z}$.

a contradiction

Thus $1+\sqrt{-3} \nmid 2$.

In $\mathbb{R}[x]$, $f(x) = x^2+1 \in \mathbb{R}[x]$ is irr. $\underbrace{\mathbb{R}[x]/(x^2+1)}$ is a field

$\cong$ [Cauchy

$\cong \mathbb{C}$ (Cauchy 1845)

G/N , $N \trianglelefteq G$

$gN = Ng$

$R/I \ni a+I$

$f(x) + (x^2+1)$

$f(x) \in \mathbb{R}[x]$

$\mathbb{R}[x]/(x^2+1)$

$= \{ a+bx+(x^2+1) : a, b \in \mathbb{R} \}$

$f(x) \in \mathbb{R}[x]$ By Division algo.

$\exists \; q(x), \; r(x) \in \mathbb{R}[x]$

s.t. $f(x) = q(x)(x^2+1) + r(x)$

$0 \le \deg r(x) < \deg(x^2+1) = 2$

$$\deg r(x) \leq 1.$$

$$r(x) = a + bx, \quad a, b \in \mathbb{R}.$$

$$f(x) + (x^2+1) = \underbrace{g(x)(x^2+1)} + a + bx + \underbrace{(x^2+1)}$$

$$= a + bx + (x^2+1)$$

$$a + bx + (x^2+1) \xmapsto{\varphi} a + bi$$

$$\varphi : \mathbb{R}[x]/(x^2+1) \longrightarrow \mathbb{C}$$ is a field iso

$$\varphi(x) = i$$

$$\varphi(a) = a$$

$$\varphi(x^2) = -1$$

$\boxed{\text{718-688-9445}}$