Commutative algebra

commutative
Algebra

algebraic Number theory $\longleftrightarrow$ algebraic Geometry

Old and deep: e.g. $a^2+b^2=c^2$ $\gg 2000$ years

$a^n+b^n \neq c^n$ $n>2$ 1637

1994

1 Commutative algebras

Today R: commutative ring

often R: K-algebra K = field e.g. $K=\mathbb{C}$.

Ex 1) $\mathbb{Z}$, K, $K[X]$, $K[X_1,\dots,X_n]$, H: holomorphic functions $\mathbb{C}\to\mathbb{C}$.

2) $R[X_1,\dots,X_n]$ R/I, $\prod_{i\in J} R_i$

Q How far are these from each other.

Ex $\mathbb{C}[X]/(X^4-1) \xrightarrow{\phi} \mathbb{C}[X]/(X^2+1) \times \mathbb{C}[X]/(X^2-1)$

$\bar{X} \longmapsto (\bar{X},\bar{X})$ $x^4-1=(x^2+1)(x^2-1)$

ϕ: well-def and inj. as $(X^4-1)\mid f(x) \iff (x^2+1)\mid f(x)$

$\wedge\ (x^2-1)\mid f(x)$

ϕ: surj. as $\dim_{\mathbb{C}} RHS = \dim_{\mathbb{C}} LHS = 4$

Def An ideal $I \subsetneq R$ is

1) prime if $ab\in I \Rightarrow a\in I \vee b\in I$

2) maximal if $I\subseteq J\subseteq R$ $I=J$ or $J=R$

Prop Let $I\subseteq R$ ideal

a) I prime $\iff$ R/I domain

b) I max $\iff$ R/I field.

<u>Def</u> The Krull dimension of R is

$\dim R := \sup\{n \mid p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n \quad p_i \subseteq R \text{ prime ideal}\}$

<u>Ex</u> 1) K field $\Rightarrow \dim K = 0$ $\quad \{0\}$

2) $\dim K[x]/(x^2) = 0$ $\quad$ proper ideals (0) $(\bar{x})$

not prime

3) $\dim K[x_1, \ldots, x_n] = n$

$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n)$ prime

$\Rightarrow \dim \geq n$ $\quad$ $\dim \leq n$ requires work.

4) $\dim \mathbb{Z} = 1$ $\quad (0) \subseteq (p)$

<u>Def/prop</u> Let R: domain $a, b \in R$ then

$(a) = (b) \Leftrightarrow a = ub \quad u \in R^\times$

<u>proof</u> "$\Rightarrow$" $(a) = (b) \Rightarrow a = xb \quad b = ya \qquad a = xya \qquad a = 0 \Rightarrow b = 0$

$a \neq 0 \quad xy = 1$

$\Rightarrow x, y \in R^\times$

"$\Leftarrow$" $a = ub \Rightarrow a \in (b)$

$\Rightarrow u^{-1}a = b \Rightarrow b \in (a)$

$\Bigg\} \Rightarrow (a) = (b).$ $\quad \square$

<u>Prop</u> Let R: PID $a \in R \setminus \{0\}$. TFAE

1) a irr. $\quad$ (i.e $a = xy \Rightarrow |\{x, y\} \cap R^\times| = 1$)

2) (a) prime

3) (a) maximal

<u>proof</u> 3) $\Rightarrow$ 2) ok.

2) $\Rightarrow$ 1) $\quad a = xy \Rightarrow xy \in (a) \Rightarrow x \in (a) \vee y \in (a)$

Wlog $x \in (a) \Rightarrow (x) = (a) \Rightarrow ux = a = xy \quad u \in R^\times$

$\Rightarrow u = y \in R^\times \quad y \notin R^\times.$

1) $\Rightarrow$ 3) $\quad (a) \subseteq (b) \subseteq R \Rightarrow a = xb \Rightarrow x \in R^\times$ or $b \in R^\times$

$\Updownarrow \qquad \Updownarrow$

$(a) = (b) \qquad (b) = R$

$\square$

Cor Let R : PID

1) $a \in R$ irr $\Rightarrow$ $R/(a)$ field

2) If R not field $\dim R = 1$.

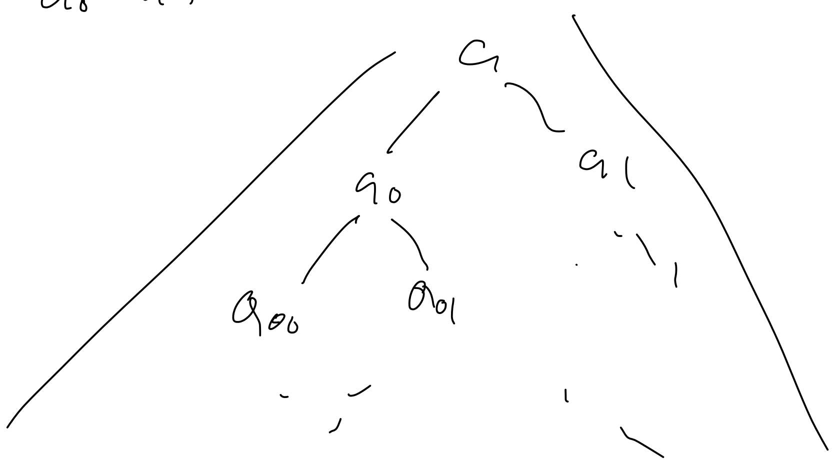
$(0) \subset (p)$ max. $\Leftarrow$ prime

② Factorization

Let R: domain $a \in R \setminus \{0\}$ $a \notin R^\times$

a not irr $\Rightarrow$ $a = a_0 a_1$ $a_0, a_1 \notin R^\times$

a_0 not irr $\Rightarrow$ $a_0 = a_{00} a_{01}$ $a_{00}, a_{01} \notin R^\times$ etc



Q 1) Does this stop i.e. $a = p_1 \cdots p_n$ p_i irr.?

2) Are $(p_1), (p_2), \ldots, (p_n)$ unique up to order.

If $\forall a$ 1), 2) hold we call R unique factorization domain.

Ex $\mathbb{Z}$, $K[x_1, \ldots, x_n]$ UFD

Ex $R = \mathbb{Z}[\sqrt{5}i]$ i.e. $R = \operatorname{im} \phi$ $\phi : \mathbb{Z}[x] \longrightarrow \mathbb{C}$, $x \longmapsto \sqrt{5}i$

is not a UFD $2 \cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$

irreducible

Ex $R = H$: holomorphic functions. $\sin z = (z - n\pi) \dfrac{\sin z}{(z - n\pi)}$ $n \in \mathbb{Z}$

Thm R : PID $\Rightarrow$ R : UFD

Thm (Gauss) R : UFD $\Rightarrow$ $R[x]$: UFD

Cor R : UFD $R[x_1, \ldots, x_n]$: UFD

③ Noetherian ring

Def/prop Let R : commutative ring, TFAE

1) Any ideal is fin. gen.
2) $I_0 \subseteq I_1 \subseteq \cdots \subseteq R \Rightarrow \exists N : \forall i \geq N \; I_i = I_N$
3) Any set $\Sigma \neq \emptyset$ of ideals in R has a maximal element.

Then we call R noetherian

proof "1) $\Rightarrow$ 2)" in 2) set $I = \bigcup I_i \subseteq R$ ideal

1) $\Rightarrow$ $I = (g_1, \ldots, g_m) \Rightarrow \exists N : g_j \in I_N$

$\Rightarrow I = I_N \Rightarrow I_N \supseteq I_i$.

"2) $\Rightarrow$ 3)" Follows by Zorns lemma

as any chain in $(\Sigma, \subseteq)$ has a maximal element (upper bound)

$\Rightarrow \Sigma$ has a max element.

"3) $\Rightarrow$ 1)" Let $I \subseteq R$ ideal

Write $\Sigma = \{ J \subseteq I \mid J \text{ f.g.} \}$ 3) $\Rightarrow$ Σ has max el. J_0.

Claim $J_0 = I$

If $a \in I$ then $J_0 + (a) \in \Sigma \Rightarrow J_0 = J_0 + (a)$

$\Rightarrow a \in J_0 \Rightarrow I \subseteq J_0 \subseteq I \Rightarrow I = J_0$ $\square$

Ex Any PID is Noetherian.

Prop If R : Noetherian domain then any $b \in R \setminus \{0\}$, $b \notin R^\times$ factors into irr.
(not nec. uniquely)

proof Assume not

$$b = b_0$$
$$b_n = a_{n+1} b_{n+1}$$

$a_i, b_i \in R \setminus (\{0\} \cup R^\times)$
b_i don't factor.

Now $(b_1) \subseteq (b_2) \subseteq \cdots$

R : Noetherian $\exists n$: $(b_n) = (b_{n+1})$

$\Rightarrow b_{n+1} = u b_n \quad u \in R^\times$

$\Rightarrow a_{n+1} = u \quad ↯$ $\square$

Thm R : PID $\Rightarrow$ R : UFD

proof R Noeth. So we only need uniqueness

Same proof as for integers.

key (a) prime $\Leftrightarrow$ a irr element for $a \neq 0$.

Prop Let R : Noetherian

① If $I \subseteq R$ ideal R/I : Noetherian.

② If $S \subseteq R$ multiplicative $S^{-1}R$: Noetherian.

proof Exercise. Note in ② we may assume S is regular by ①

Thm (Hilbert's Basis Theorem)

If R comm. Noetherian ring, then $R[x]$ is Noetherian.

Corollary If K : field then $K[x_1, \dots x_n]$ is Noetherian. i.e. any ideal in $K[x_1, \dots x_n]$ is f.g.

Corollary If K : field any comm. f.g. K-alg is Noetherian.

proof A : f.g. $\Rightarrow \exists \underset{\text{Noeth}}{K[x_1, \dots x_n]} \xrightarrow{\phi} A$ surj.

$\Rightarrow$ $\operatorname{im}\phi = A$
$\cong K[x_1, \dots x_n]/\ker\phi$.

<u>proof</u> Let $I \subseteq R[x]$ we show I f.g.

set $I_n = \{a \in R \mid \underbrace{ax^n + b_{n-1}x^{n-1} + \dots b_0}_{} \in I$ for $b_i \in R\} \subseteq R$

in part. $I_0 = I \cap R$

<u>Claim</u> $\underset{1}{I_n \subseteq R}$ ideal $\underset{2}{I_n \subseteq I_{n+1}}$.

1 add $\underbrace{\qquad}$ and mult $\underbrace{\qquad}$ by $r \in R$

2 mult. $\underbrace{\qquad}$ by x

Now $I_0 \subseteq I_1 \dots$ R Noetherian $\Rightarrow \exists N$

st $I_n = I_N \quad \forall n \geq N$.

For $i \leq N$ $I_i = (a_{i,1}, \dots, a_{i,m_i}) \subseteq R$ ← Noetherian

for some $a_{ij} \in R$.

By def I_i there is

$$f_{ij}(x) = a_{ij} x^i + \dots \in I$$

<u>Claim</u> $I = I' := (f_{ij} \mid 0 \leq i \leq N, 1 \leq j \leq m_i)$

$I' \subseteq I$ clear. show $I \subseteq I'$.

Let $g \in I$ we show $g \in I'$ by induction on $\deg g = n$.

$n = 0$ $g \in I \cap R = I_0 = (\underset{f_{01}}{a_{01}}, \dots, \underset{f_{0m_0}}{a_{0m_0}}) \Rightarrow g \in I'$.

$n > 0 \Rightarrow g(x) = bx^n + \cdots \in I$

$\Rightarrow b \in I_n = I_i$ where $i = \min(N, n)$

$\Rightarrow b = \sum_{j=1}^{m_i} c_j a_{ij}$ for some $c_j \in R$

set $f(x) = \left(\sum_{j=1}^{m_i} c_j f_{ij}\right) x^{n-i} = bx^n + \cdots \in I'$

So $\deg(g-f) < n$. since $g - f \in I$

we have $g - f \in I'$ by induction.

$\Rightarrow g \in I' + f = I'$

Ex ① $\mathbb{Z}[\sqrt{5}i] \simeq \mathbb{Z}[x]/(x^2+5)$ Noetherian domain. but not UFD.

② $K[x_1, \ldots, x_n]$ Noeth. UFD

③ $K[x_1, x_2, \ldots]$ Not Noeth. but UFD. Exercise.

④ H : holomorphic functions is not Noetherian but a domain.