Ring Theory / Commutative Algebra

Shun / 翔海 (@shun4midx)

↳ His own notes, feel free to use them for personal use.

2-19-25 (WEEK 1)

Shun / 翔海 (@shun4midx)

RINGS AND MODULES

For $M \in {}_R\mathcal{M}$, $R \times M \to M \Leftrightarrow \exists R \xrightarrow{\text{ring homo}} \text{End}(M)$ (representation)

QUOTIENT

In fact, $R \in {}_R\mathcal{M}$, and for $I \subsetneq R$, (I = left ideal of R ⇒ I is a submodule) R/I is a left R-module

If $I \in {}_R\mathcal{M}, \mathcal{M}_R$, then I is called an ideal and R/I is a ring

⇒ The most important structure to investigate rings aren't subrings but are ideals

Today's notes have R as commutative.

DEFINITION

Let $I \subsetneq R$ be an ideal

- I is maximum if $\forall {}_R\mathcal{M} \ni J \subsetneq R$, $I \subsetneq J \Rightarrow J = R$ (not "biggest" but not comparable to anything bigger)
- I is prime if $\forall x, y \in R$, $xy \in I \Rightarrow x \in I$ or $y \in I$ or $x \notin I, y \notin I \Rightarrow xy \notin I$

FACT 1

(1) I is max $\Leftrightarrow$ R/I is a field

Proof

"⇒": $\forall \bar{0} \neq \bar{x} \in R/I$, $x \notin I \Rightarrow (x) + I \supsetneq I \Rightarrow (x) + I = R$ ($yx + a = 1$) $\Rightarrow \overline{yx} = \bar{1} \Rightarrow \bar{y} = \bar{x}^{-1}$ ✓

"⇐": let $I \subsetneq J$, pick $x \in J \setminus I$, then $\bar{x} \neq \bar{0}$ in R/I

let $\bar{y} \in R/I$, s.t. $\bar{y}\bar{x} = \bar{1}$, i.e. $yx + a = 1$ ($yx \in J$, $a \in J$) $\Rightarrow 1 \in J \Rightarrow \forall r \in R$, $1 \cdot r = r \in J$ $\therefore R = J$ (of course max) ✓

(2) I is prime $\Leftrightarrow$ R/I is an integral domain

Proof

"⇒": $\begin{cases} \bar{x}\bar{y} = \bar{0} \\ \bar{x} \neq \bar{0} \end{cases} \Rightarrow \begin{cases} xy \in I \\ x \notin I \end{cases} \Rightarrow y \in I \Rightarrow \bar{y} = 0$ $\therefore$ By def, R/I is an integral domain ("can divide") ✓

"⇐": $\begin{cases} xy \in I \\ x \notin I \end{cases} \Rightarrow \begin{cases} \bar{x}\bar{y} = \bar{0} \\ \bar{x} \neq \bar{0} \end{cases} \Rightarrow \bar{y} = \bar{0} \Rightarrow y \in I$ $\therefore$ By def, I is prime ✓

DEFINITION

$a \in R$ is nilpotent if $\exists n \in \mathbb{N}$, s.t. $a^n = 0$ (special type of zero divisors)

FACT 2

- $n_R = \{\text{nilpotent elements of } R\} \in {}_R\mathcal{M}$, i.e. it is an ideal (good thing, means we can quotient it)
- R/n_R has no non-zero nilpotent elements, which is said to be reduced

Proof

For $a \in n_R$, say $a^n = 0$, for $r \in R$, $(ra)^n = r^n a^n = 0 \Rightarrow ra \in n_R$

For $b \in n_R$, say $b^m = 0$, then $(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} = 0 \Rightarrow a+b \in n_R$ □

DEFINITION

- n_R is called the nilradical ($\sqrt{(0)}$) of R
- $\text{Max}\, R = \{\text{max ideals of } R\}$
- $\text{Spec}\, R = \{\text{prime ideals of } R\}$
- $\sqrt{I} := \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$ ("the radical of I")

Shun / 舜海 (@shun4midx)

PROPOSITION 1

$n_R = \bigcap_{P \in \operatorname{Spec} R} P$

Proof

"$\subseteq$": For $a \in n_R$, say $a^n = 0 \in P$ $\forall P \in \operatorname{Spec} R$, so by def of P, $a \in P$ $\forall P \Rightarrow a \in RHS$ ✓

"$\supseteq$": Use contraposition, and Zorn's Lemma. $I \cap \{a, a^2, a^3, \dots\} = \emptyset$ (Goal to create is by replacing $\_\_ = U$)

Let $a \notin n_R$, for $S = \{I \supseteq R \mid a^n \notin I \ \forall n \in \mathbb{N}\}$. We know $S \neq \emptyset$ since $\{0\} \in S$ ($a \notin n_R \Rightarrow a^k \neq 0 \ \forall k \in \mathbb{N}$)

Define partial order "$\leq$" in S as "$I \leq J$" $\Leftrightarrow$ "$I \subseteq J$"

Let $\{I_i \mid i \in \Lambda\}$ be a chain in S. Then, $\exists I = \bigcup_{i \in \Lambda} I_i$ is a least upper bound of $\{I_i \mid i \in \Lambda\}$. (⌜$a, b \in I \Rightarrow a \in I_i, b \in I_j \Rightarrow I_i \subseteq I_j$ or $I_j \subseteq I_i \Rightarrow ab \in I_i$ or $I_j \subseteq I$⌝)

By Zorn's Lemma, $\exists$ a max element Q in S.

Claim: $Q \in \operatorname{Spec} R$ ($\Rightarrow a \notin Q \Rightarrow a \notin RHS$)

Proof

If $x \notin Q$, then $\langle x \rangle + Q \supsetneq Q \Rightarrow \langle x \rangle + Q \notin S \Rightarrow a^n \in \langle x \rangle + Q$ (⌜$a \in U$ ($\because a \notin I$, $I \cup U = \emptyset$, $0 \notin U$ is max)⌝)

Similarly, if $y \notin Q$, $a^m \in \langle y \rangle + Q - b \in U$

$\therefore a^{n+m} \in \langle xy \rangle + Q \Rightarrow \langle xy \rangle + Q \supsetneq Q$, i.e. $xy \notin Q$ ✓ (Just proved $x \notin Q$ and $y \notin Q \Rightarrow xy \notin Q$)

($a^{n+m} \in U$ ← $ab \in U$)

COROLLARY

$\sqrt{I} = \bigcap_{\operatorname{Spec} R \supseteq P \supseteq I} P$

Proof

Let $\phi: R \to R/I$, $r \mapsto \bar{r}$. Then, $\sqrt{\bar{I}} = \phi^{-1}(n_{R/I}) = \phi^{-1}(\bigcap_{\bar{P} \in \operatorname{Spec} R/I} \bar{P}) = \bigcap_{\operatorname{Spec} R \supseteq P \supseteq I} P$ □ (⌜$\bar{P} = P/I$⌝)

OBSERVE

$$\begin{array}{ccc} R & \twoheadrightarrow & R/I \\ \cup & & \cup \\ P & \hookleftarrow & P/I \\ \cup & & \\ I & & \end{array}$$

By 3rd isom thm, $(R/I)/(P/I) \cong R/P$

$R_1 \xrightarrow{\text{ring hom } \psi} R_2$ in Ring

$P \in \operatorname{Spec} R_2 \Rightarrow \psi^{-1}(P) \in \operatorname{Spec} R_1$ ($xy \in \psi^{-1}(P) \Rightarrow \psi(xy) = \psi(x)\psi(y) \in P \Rightarrow \psi(x) \in P$ or $\psi(y) \in P \Rightarrow x \in \psi^{-1}(P)$ or $y \in \psi^{-1}(P)$)

EXAMPLE

We know usually $\sqrt{I^n} \neq I$, but if $P' \in \operatorname{Spec} R$, then $\sqrt{(P')^n} = P'$.

"$\subseteq$": $\sqrt{(P')^n} = \bigcap_{P \supseteq (P')^n} P \subseteq P'$ ✓

"$\supseteq$": $\forall x \in P'$, $x^n \in (P')^n \Rightarrow x \in \sqrt{(P')^n}$ ✓

DEFINITION

An ideal Q of R is **primary** if $Q \neq R$ and "$xy \in Q$, $x \notin Q \Rightarrow y^n \in Q$ for some $n \in \mathbb{N}$"

FACT 3

(1) Q is primary $\Leftrightarrow R/Q \neq 0$ and the **zero-divisors** in R/Q are **nilpotent**

Proof

"$\Rightarrow$": $\begin{cases} \bar{x}\bar{y} = \bar{0} \\ \bar{x} \neq 0 \end{cases} \Rightarrow \begin{cases} xy \in Q \\ x \notin Q \end{cases} \Rightarrow y^n \in Q \Rightarrow \bar{y}^n = \bar{0}$ ✓

"$\Leftarrow$": $\begin{cases} xy \in Q \\ x \notin Q \end{cases} \Rightarrow \begin{cases} \bar{x}\bar{y} = \bar{0} \text{ in } R/Q \\ \bar{x} \neq \bar{0} \end{cases} \Rightarrow \bar{y}^n = \bar{0}$ for some $n \in \mathbb{N} \Rightarrow y^n \in Q$. ✓

Shun/翔海 (@shun4midx)

(2) If Q is primary, then $\sqrt{Q}$ is the smallest prime ideal containing Q.

Proof

- "$\sqrt{Q} \in \operatorname{Spec} R$": $\begin{cases} xy \in \sqrt{Q} \Rightarrow (xy)^n = x^n y^n \in Q \\ x \notin \sqrt{Q} \Rightarrow x^m \notin Q \ \forall m \Rightarrow x^n \notin Q \end{cases} \Rightarrow (y^n)^t \in Q \Rightarrow y \in \sqrt{Q}$
- $\sqrt{Q} = \bigcap_{P \supseteq Q} P \Rightarrow \sqrt{Q} \subseteq P \Rightarrow \forall P \in \operatorname{Spec} R,\ P \supseteq Q$ □

DEFINITION

Q is P-primary if Q is primary and $\sqrt{Q} = P$

EXAMPLES

1. $R = \mathbb{Z}$ (PID)
   - $\operatorname{Max} R = \{n\mathbb{Z} \mid n \text{ is prime}\}$ ($\because R/\operatorname{Max} R$ must be a field when R is a PID)
   - $\operatorname{Spec} R = \operatorname{Max} R \cup \{\{0\}\}$
   - The primary ideals of R: Either $Q = \langle 0 \rangle$ or if $Q \neq \langle 0 \rangle$, say $Q = \langle s \rangle$ (ideals over PID are generated by 1 element only) and for some prime p, $\sqrt{Q} = \langle p \rangle$
     $\therefore p^n \in Q = \langle s \rangle$, say $p^n = st$ in $\mathbb{Z} \Rightarrow s = p^m \Rightarrow Q = \langle p^m \rangle$ □
2. $\sqrt{I} \in \operatorname{Spec} R \not\Rightarrow I$ is primary (key example)

   For $R = \mathbb{R}[x,y]$, we need $xy \in I$ and $x \notin I \Rightarrow y^n \in I$

   ↪ $I = \langle x^2, xy \rangle$ is not primary

   Notice, $I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x, y \rangle^2$.

   Now, $R/\langle x \rangle = \mathbb{R}[x,y]/\langle x \rangle \cong \mathbb{R}[y]$, which is not a field $\therefore \langle x \rangle$ is not a maximal ideal

   $R/\langle x, y \rangle \cong \mathbb{R}$, which is a field $\Rightarrow \langle x, y \rangle$ is a max ideal

   Now, we know $\sqrt{I} = \sqrt{\langle x \rangle} \cap \sqrt{\langle x, y \rangle^2} = \langle x \rangle \cap \langle x, y \rangle = \langle x \rangle$, which is primary ✓

2-21-25 (WEEK 1)

Shun / 翔海 (@shun4midx)

LOCALIZATION

Recall: "units" = elements that exist multiplicative inverse

Today, R is assumed to be commutative

Let S be a multiplicatively closed set with $1\in S$, $0\notin S$

DEFINITION

Suppose that there is a ring B and a ring homo $f:R\to B$ s.t.

(1) $f(x)$ is a unit of B $\forall x\in S$

(2) If $g:R\to A$ is another ring homo s.t. $g(x)$ is a unit of A $\forall x\in S$, then $\exists!$ ring homo $h:B\to A$ s.t. $B \xrightarrow{h} A$, $f\uparrow \circlearrowright g$, R (Universal Property)

Such B, if it exists, is unique up to isom and is called the localization of R w.r.t. S, denoted by R_S

THEOREM

R_S exists

Proof

Set $R_S = R\times S/\sim$ where $(a,s)\sim(b,t)\iff \exists u\in S$ s.t. $(at-bs)u=0$

Step 1: "$\sim$" is an equivalence relation

- $(a,s)\sim(a,s)$ since $(as-as)1=0$
- "$(a,s)\sim(b,t)\Rightarrow(b,t)\sim(a,s)$" since $(at-bs)u=0\Rightarrow(bs-at)u=0$
- $(a,s)\sim(b,t)$, $(b,t)\sim(c,u)\Rightarrow(a,s)\sim(c,u)$ since $(at-bs)v=0$, $(bu-ct)w=0\Rightarrow(at-bs)vuw=0$, $(bu-ct)wvs=0\Rightarrow(au-cs)\underbrace{tvw}_{\in S}=0$

Define $\frac{a}{t}:=[(a,t)]$

Step 2: R_S has a ring structure: $\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$, $\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$

- Well-defined:

  $\frac{a}{s}=\frac{a'}{s'}\Rightarrow(as'-a's)v=0\Rightarrow(as'-a's)vwtt'=0$

  $\frac{b}{t}=\frac{b'}{t'}\Rightarrow(bt'-b't)w=0\Rightarrow(bt'-b't)wvss'=0$

  $+)\ [(at+bs)s't'-(a't'+b's')st]vw=0$

  $\therefore as'v=a'sv$, $bt'w=b'tw\Rightarrow(abs't'-a'b'st)vw=0$

Actually, $(R_S,+,\cdot)$ forms a ring

Step 3: $f:R\to R_S$ satisfies the universal property ($a\mapsto\frac{a}{1}$)

(1) $\forall x\in S$, $f(x)=\frac{x}{1}$ $\because \frac{1}{x}\cdot\frac{x}{1}=\frac{x}{x}=\frac{1}{1}$ $\therefore\frac{x}{1}$ is a unit in R_S

(2) Let $g:R\to A$ with $g(x)$ being a unit of A $\forall x\in S$

If $\exists$ a ring homo $R_S\to A$ with $g=hf$, then $h(\frac{a}{s})=h(\frac{a}{1}\cdot\frac{1}{s})=h(\frac{a}{1})h(\frac{1}{s})=h(\frac{a}{1})(h(\frac{s}{1}))^{-1}=hf(a)(hf(s))^{-1}=g(a)g(s)^{-1}=\frac{g(a)}{g(s)}$

So, we define $h(\frac{a}{s})=g(a)g(s)^{-1}$

It is well-defined as follows: $\frac{a}{s}=\frac{b}{t}\Rightarrow(at-bs)u=0\Rightarrow(g(a)g(t)-g(b)g(s))g(u)=0\Rightarrow g(a)g(s)^{-1}=g(b)g(t)^{-1}$

PROPERTIES

- If S contains no zero divisor, then $f:R\to R_S$ is injective

  $x\mapsto\frac{x}{1}=\frac{0}{s}$, i.e. $\exists u\in S$, s.t. $\underbrace{us}_{\in S}x=0\Rightarrow us$ is not a zero divisor, so $x=0$

- If R is an integral domain (prime ideal) and $S=R\setminus\{0\}$, then R_S is called the quotient field of R which is the smallest field containing R:

  If for a field F, say $g:R\hookrightarrow F$, with $g(a)\neq0$ being a unit, by universal property, $\exists! h:R_S\to F$ which is injective since $h(\frac{a}{s})=g(a)g(s)^{-1}=0\Rightarrow g(a)=0\Rightarrow a=0\Rightarrow\frac{a}{s}=\frac{0}{s}$

  Pick $0\neq f\notin R$ (non-nilpotent), consider $S=\{1,f,f^2,\dots\}\Rightarrow R_S=R_f$

- $S=R/P$ for some $P\in \operatorname{Spec} R$, $R_S=R_P$

REMARK

$S\subseteq T$ with $1\in S$, $T\neq\emptyset$, S,T are mcs (multiplicatively closed sets)
When will $R_S\cong R_T$?
Ans: When $T\subseteq \bar{S}=R\setminus \bigcup_{P\cap S=\emptyset} P$ ($\frac{s}{t}\cdot\frac{s'}{s}=\frac{1}{t}\Rightarrow \exists u\in S$, s.t. $\underset{\in\bar{S}}{\underset{\uparrow}{t}}\underset{\in S}{\underset{\uparrow}{u}}s=\underset{\in S}{\underset{\uparrow}{s}}$, $t\in\bar{S}\Rightarrow (t)\cap S\neq\emptyset\Rightarrow s=ta$)

CONSTRUCTION FOR MODULES

For an R-module M, $1\in S\neq 0$ mcs in R, define $M_S:=\{(m,s)\mid m\in M, s\in S\}/\sim$, $(m,s)\sim(n,t)\Leftrightarrow \exists u\in S$, s.t. $u(tm-sn)=0$
$\Rightarrow$ "$\sim$" is an equivalence relation, $\frac{m}{s}:=[(m,s)]$ in M_S
Notice: M_S is an R_S-module

PROPOSITION

If $0\to M'\xrightarrow{f} M\xrightarrow{g} M''\to 0$ is exact (in ${}_R\mathcal{M}$), then $0\to M_S'\xrightarrow{f_S} M_S\xrightarrow{g_S} M_S''\to 0$ is exact
($\frac{a}{s}\mapsto\frac{f(a)}{s}$, $\frac{b}{s}\mapsto\frac{g(b)}{s}$)

Proof
- f_S is 1-1: $f_S(\frac{a}{t})=f_S(\frac{a'}{t'})\Rightarrow \frac{f(a)}{t}=\frac{f(a')}{t}\Rightarrow \exists u\in S$, s.t. $u(t'f(a)-tf(a'))=0\Rightarrow f(ut'a-uta')=0$ (f is 1-1) $\Rightarrow ut'a-uta'=0\Rightarrow \frac{a}{t}=\frac{a'}{t'}$ ✓
- g_S is onto: $\forall \frac{b}{t}\in M_S''$, let $g(a)=b\Rightarrow g_S(\frac{a}{t})=\frac{b}{t}$ ✓
- $\operatorname{Im} f_S\subseteq\ker g_S$: $g_Sf_S(\frac{a}{t})=\frac{gf(a)}{t}=\frac{0}{t}=0$ ✓
- $\ker g_S\subseteq\operatorname{Im} f_S$: Let $\frac{a}{t}\in\ker g_S$, i.e. $g_S(\frac{a}{t})=\frac{g(a)}{t}=\frac{0}{1}\Rightarrow \exists u\in S$ s.t. $ug(a)=0\Rightarrow g(ua)=0$ ($\ker g\subseteq\operatorname{Im} f$) $\Rightarrow f(b)=ua$ $\therefore \frac{a}{t}=\frac{ua}{ut}=\frac{f(b)}{ut}=f_S(\frac{b}{ut})$

FACT

$R_S\otimes_R M\cong M_S$

Proof
$f: R_S\times M\to M_S$ is bilinear ($(\frac{a}{t},m)\mapsto\frac{am}{t}$) $\Rightarrow \exists$ R-module homo $\bar{f}: R_S\otimes_R M\to M_S$ ($\frac{a}{t}\otimes m\mapsto\frac{am}{t}$)
- $\bar{f}$ is onto: $\forall \frac{m}{t}\in M_S$, $\bar{f}(\frac{1}{t}\otimes m)=\frac{m}{t}$ ✓
- $\bar{f}$ is 1-1: Let $\sum_i(\frac{a_i}{t_i})\otimes m_i\in R_S\otimes M$
  Set $t=\prod t_i$, $\bar{t}_i=\prod_{j\neq i} t_j$, then $\sum_i(\frac{a_i}{t_i})\otimes m_i=\sum_i(\frac{a_i\bar{t}_i}{t})\otimes m_i=\frac{1}{t}\otimes\sum_i \bar{t}_ia_im_i$

  If $\frac{1}{t}\otimes m\in\ker\bar{f}$, i.e. $\bar{f}(\frac{1}{t}\otimes m)=\frac{m}{t}=0$ in M_S, i.e. $\exists u\in S$, s.t. $um=0$.
  Then, $\frac{1}{t}\otimes m=\frac{u}{ut}\otimes m=\frac{1}{ut}\otimes \underset{0}{\underset{\downarrow}{um}}=0$ ✓

THEOREM

R_S is a flat R-module

Proof
Given $0\to M'\to M\to M''\to 0$ in ${}_R\mathcal{M}$, by prop, $0\to M_S'\to M_S\to M_S''\to 0$ is exact ☐
($M_S'\cong R_S\otimes_R M'$, $M_S\cong R_S\otimes_R M$, $M_S''\cong R_S\otimes_R M''$)

REMARK

Given $M\in{}_R\mathcal{M}$, TFAE:
(1) $M=0$
(2) $M_P=0$ $\forall P\in\operatorname{Spec} R$
(3) $M_Q=0$ $\forall Q\in\operatorname{Max} R$

Proof
(1)$\Rightarrow$(2)$\Rightarrow$(3) is straightforward.
Consider proving (3)$\Rightarrow$(1),
Assume $\exists\, 0\neq z\in M$

Define $\mathrm{ann}(z) := \{r \in R \mid rz \overset{\text{in } M}{=} 0\} \subseteq R \Rightarrow \exists Q \in \mathrm{Max}\, R$ s.t. $\mathrm{ann}(z) \subseteq Q$

By assumption, $\frac{z}{1} = \frac{0}{1}$ in $M_Q \Rightarrow \exists u \notin Q$, s.t. $uz = 0 \Rightarrow u \in \mathrm{ann}(z) \subseteq Q$ ~~↯~~

Shun/翔海 (@shun4midx)

2-26-25 (WEEK 2)

Shun / 宋翔海 (@shun4midx)

EUCLIDEAN DOMAINS

Today, R is an integral domain.

DEFINITION

- Any function $N: R \to \mathbb{N}$ with $N(0)=0$ is called a norm on R
- N is positive if $N(a)>0$ $\forall a \neq 0$
- R is called a Euclidean domain if $\exists$ a norm N on R, s.t. $\forall a, 0 \neq b \in R$, $\exists q, r \in R$, s.t. $a = qb + r$ and $r=0$ or $N(r) < N(b)$
  For example: $R=\mathbb{Z}$, $F[x]$, $F \leftarrow N(a)=0$ $\forall a \in F$, $\forall a, 0 \neq b \in F$, $a = ab^{-1}b + 0$
- Euclidean Algorithm for R being a ED: For $a, 0 \neq b \in R$, $a = q_1 b + r_1, \dots, r_1 = q_3 r_2 + r_3, \dots \Rightarrow \exists k$, s.t. $r_{k+1}=0$ otherwise $0 \le N(b) > N(r_1) > N(r_2) > \dots$

FACT

$r_k = \gcd(a, b)$

Proof

Let $A(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$, $A(x)^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -x \end{pmatrix}$. We find that $(a\ b) = (b\ r_1)A(q_1)$, $(b\ r_1) = (r_1\ r_2)A(q_2)$, $\dots$, $(r_{k-1}\ r_k) = (0\ k)A(q_{k+1})$

$\therefore$ We have $(a\ b) = (r_k\ 0)A(q_{k+1})A(q_k)\dots A(q_1) \Rightarrow (r_k\ 0) = (a\ b)A(q_1)^{-1}A(q_2)^{-1}\dots A(q_{k+1})^{-1}$

From the LHS, we can deduce $r_k | a$, $r_k | b$. From the RHS, we can deduce $r_k = ta + sb$ and "$c|a$, $c|b \Rightarrow c | ta+sb = r_k$"

DEFINITION

$A_D :=$ the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$ with $D \neq 1$, D being square-free.

$= \{\alpha \in \mathbb{Q}(\sqrt{D}) \mid \alpha$ is integral over $\mathbb{Z}\}$, i.e. $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$, $a_i \in \mathbb{Z}$ ($f(\alpha)$)

($p+q\sqrt{D}$, $p, q \in \mathbb{Q}$)

THEOREM

- If $D \equiv 1 \pmod 4$, $A_D = \{a + b(\frac{1+\sqrt{D}}{2}) = \frac{2a+b}{2} + \frac{b}{2}\sqrt{D}\}$
- If $D \equiv 2, 3 \pmod 4$, $A_D = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$

Proof

Let $\alpha = p + q\sqrt{D} \in A_D$, ($p$, $0 \neq q \in \mathbb{Q}$ ($g(\alpha)$); $q=0$, $x-p$)

Notice, $\alpha - p \in q\sqrt{D} \Rightarrow (\alpha - p)^2 = \alpha^2 - 2\alpha p + p^2 = q^2 D \Rightarrow \alpha^2 - 2\alpha p + (p^2 - q^2 D)$

Note: In $\mathbb{Q}[x]$, $\mathbb{Z}[x] \ni f(x) = q(x)g(x) + (ax+b)$

$f(\alpha)=0$, $g(\alpha)=0 \Rightarrow a\alpha + b = 0 \Rightarrow a=0, b=0$, i.e. $f(x) = q(x)g(x)$. All are monic $\Rightarrow g(x) \in \mathbb{Z}[x]$ by Gauss Lemma

If p is even $\Rightarrow p \in \mathbb{Z} \Rightarrow q \in \mathbb{Z}$. Since $p^2 - q^2 D \in \mathbb{Z}$, D is square-free, $\therefore q^2 p \in \mathbb{Z}$

If p is odd, say $2p = 2m+1 \Rightarrow (2p)^2 \equiv (2m+1)^2 \pmod 4 \Rightarrow 4(\underbrace{p^2 - q^2 D}_{\in \mathbb{Z}}) \equiv 0 \pmod 4$ $\therefore 4p^2 \equiv 4q^2 D \equiv 1 \pmod 4 \Rightarrow q \notin \mathbb{Z}$, $q = \frac{2n+1}{2}$. Also, $4q^2 D = (2n+1)^2 D \overset{(\text{mod } 4)}{\equiv} 0$

THEOREM

A_D is an ED if $D = 2, 3, 5, -1, -2, -3, -7, -11$

Proof

Define $N': \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$, $\alpha = p + q\sqrt{D} \mapsto (p+q\sqrt{D})(p-q\sqrt{D}) = p^2 - q^2 D$

and $N: A_D \to \mathbb{N}$, $\alpha \mapsto |N'(\alpha) = p^2 - q^2 D|$ (prevent negative values)

Now, for $\alpha, 0 \neq \beta \in A_D$, $\frac{\alpha}{\beta} = x + y\sqrt{D}$, $x, y \in \mathbb{Q}$

- $D = 2, 3, -2, -1$: Choose $a, b \in \mathbb{Z}$, s.t. $|x-a| \le \frac{1}{2}$, $|y-b| \le \frac{1}{2}$

  If $\lambda = a + b\sqrt{D}$, then $|N'(\frac{\alpha}{\beta} - \lambda)| = |(x-a)^2 - (y-b)^2 D|$. $D = 2, 3$: $\le (y-b)^2 D \le \frac{3}{4} < 1$

  $D = -2, -1$: $\le (x-a)^2 + (y-b)^2 |D| \le \frac{1}{4} + \frac{1}{4} \cdot 2 \le \frac{3}{4} < 1$

Shun/舜海 (@shun4midx)

Let $w=\alpha-\lambda\beta$, $N(w)=|N'(\beta)N'(\frac{\alpha}{\beta}-\lambda)|<|N'(\beta)|=N(\beta)$ (KEY: We need $|N'(\frac{\alpha}{\beta}-\lambda)|<1$, then we can divide easily)

- $D=5,-3,-7,-11$: Choose $a,b\in\mathbb{Z}$, s.t. $|2y-b|\le\frac{1}{2}$, $|x-a-\frac{b}{2}|\le\frac{1}{2}$. ($|y-\frac{b}{2}|\le\frac{1}{4}$)
  If $\lambda=a+b(\frac{1+\sqrt{D}}{2})$, then $|N'(\frac{\alpha}{\beta}-\lambda)|=|(x-a-\frac{b}{2})^2-(y-\frac{b}{2})^2D|\le\frac{1}{4}+\frac{|D|}{16}<1$

DEFINITION

Let $N:R\longrightarrow\mathbb{N}$ be a norm. N is a **Dedekind-Hasse norm** if N is positive and $\forall a,0\neq b\in R$, either $b|a$ or $\exists s,t\in R$, s.t. $0<N(sa-tb)<N(b)$

FACT

P is a ED with N being positive $\Rightarrow$ N is a Dedekind-Hasse norm ($s=1$, $t=q$)

THEOREM

R has a D-H norm $\Rightarrow$ R is a PID (generated by 1 element (i.e. the ring version of cyclic groups))

Proof

Let $I\neq\{0\}$ and $d\in I$, $N(d)=\min\{N(a)\mid 0\neq a\in I\}$

Claim: $I=\langle d\rangle$

Proof

$\forall 0\neq a\in I$, $\forall s,t\in R$, $sa-td\in I\Rightarrow N(sa-td)\ge N(d)$ $\therefore$ By def of D-H norm, then $d|a$, i.e. $a\in\langle d\rangle$ $\square$

DEFINITION

$\tilde{R}:=R^\times\cup\{0\}$ (units), $u\in R\setminus\tilde{R}$ is called a **universal side divisor** if $\forall x\in R$, $\exists r\in\tilde{R}$, s.t. $u|x-r$

FACT

R is a ED but not a field ($R\neq\tilde{R}$) $\Rightarrow$ R has a universal side divisor

Proof

Define $N(u):=\min\{N(a)\mid a\in R\setminus\tilde{R}\}$. $\forall x\in R$, $\exists q,r$, s.t. $x=qu+r$ $\longrightarrow$ If $r=0$, then $u|x-0$ ✓

If $r\neq 0$, then $r=x-qu\notin R\setminus\tilde{R}$ since $N(r)<N(u)\Rightarrow r\in\tilde{R}$

KEY EXAMPLE

A_{-19} is a PID but not a ED

Proof

TL;DR, we need "A_{-19} has a D-H norm" (PID) and "A_{-19} has no universal side divisor" (ED ↯)

Claim: A_{-19} has a D-H norm

Proof

Recall: $N:A_{-19}\longrightarrow\mathbb{N}$

$a+b(\frac{1+\sqrt{-19}}{2})\longmapsto|(a+\frac{b}{2})^2+\frac{b^2}{4}(19)|=|a^2+ab+5b^2|$

($\because -19\equiv 1\pmod 4$)

Given $0\neq\alpha$, $0\neq\beta\in A_{-19}$, suppose $\beta\nmid\alpha$, i.e. $\frac{\alpha}{\beta}\notin A_{-19}$. We hope "$\exists s,t\in A_{-19}$, s.t. $0<N(s\alpha-t\beta)<N(\beta)$, i.e. $0<|N'(s(\frac{\alpha}{\beta}-t))|<1$"

We write $\frac{\alpha}{\beta}=\frac{a+b\sqrt{-19}}{c}$, $a,b,c\in\mathbb{Z}$, $c>1$, $\gcd(a,b,c)=1$.

$\Rightarrow\begin{cases}\exists x,y,w\in\mathbb{Z}, \text{s.t. } ya+xb-wc=1\\ \exists z,r\in\mathbb{Z}, \text{s.t. } xa-19yb=cz+r \text{ with } |r|\le\frac{c}{2}\end{cases}$ (i.e. instead of $7=1\times4+3$, we write $7=2\times4+(-1)$, since $3>\frac{4}{2}$)

Let $s:=x+y\sqrt{-19}$, $t:=z+w\sqrt{-19}$, we get $0<|N'(s(\frac{\alpha}{\beta})-t)|=\frac{(xa-19yb-cz)^2}{c^2}+\frac{19(ya+xb-wc)^2}{c^2}\le\frac{1}{4}+\frac{19}{c^2}<1$ for $c<5$

For $c=5$, $|r|\le 2$, then $\frac{r^2}{c^2}+\frac{19}{c^2}\le\frac{4+19}{25}<1$

For $c=2$, $a\not\equiv b\pmod 2$ ($\Rightarrow$ coprime) $\Rightarrow(a-1)\equiv b\pmod 2$. Take $s=1$, $t=\frac{(a-1)+b\sqrt{-19}}{c}\in A_{-19}\Rightarrow|N'(\frac{\alpha}{\beta}-t)|=\frac{1}{4}<1$

For $c=3$, $a\equiv b\equiv 0\pmod 3$ is false $\Rightarrow a^2+b^2\not\equiv 0\pmod 3\Rightarrow a^2+19b^2\not\equiv 0\pmod 3$, say $a^2+19b^2=3q+r$, $r=1$ or 2.

Set $s:=a-b\sqrt{-19}$, $t:=q$, then $0<|N'(s(\frac{\alpha}{\beta})-t)|=|\frac{a^2+19b^2}{3}-q)^2=(\frac{r}{3})^2<1$

For $c=4$, One of a,b is odd, the other is even. $\therefore a^2+19b^2$ is odd. Write $a^2+19b^2=4q+r$, $r=1$ or 3.

Set $s:=a-b\sqrt{-19}$, $t:=q$. Then, $|N'(s(\frac{\alpha}{\beta})-t)|=(\frac{a^2+19b^2}{4}-q)^2=(\frac{r}{4})^2<1$

a and b are both odd. $\therefore a^2+19b^2\equiv 3\pmod 8$. Set $s:=\frac{a}{2}-\frac{b}{2}\sqrt{-19}$, $t:=q$. Then, $0<|N'(s(\frac{\alpha}{\beta})-t)|=(\frac{a^2+19b^2}{8}-q)^2=(\frac{3}{8})^2<1$

$\therefore$ In conclusion, A_{-19} has a D-H norm. $\square$

Claim: A_{-19} has no universal side divisor

Shun / 翔海 (@shun4midx)

Proof

Suppose that u is a usd.

Let $x=2$. (cannot for $x=1$ ⇒ not OK for some x) Then, $u \mid 2\pm 0$ or $u \mid 2\pm 1$ (unit) in A_{-19}, i.e. $u \mid 2$ or $u \mid 3$

↳ If $u \mid 2$, then we have $2=u\alpha \Rightarrow N(2)=N(u)N(\alpha) \Rightarrow 4=N(u)N(\alpha)$ with $N(\alpha)\geq 5$ ($\because \alpha$ is not a unit) $\therefore N(u)\leq 4 \Rightarrow u=\pm 2$

↳ If $u \mid 3$, then we have $3=u\alpha \Rightarrow 9=N(u)N(\alpha) \Rightarrow N(u)=3$ or $9 \Rightarrow u=\pm 3$

However, for $x=\frac{1+\sqrt{-19}}{2} \in A_{-19}$, we must have "$\pm 2, \pm 3 \mid x, x\pm 1$", but $N(x)=\frac{1}{4}+\frac{19}{4}=5$, $N(x+1)=\frac{9}{4}+\frac{19}{4}=7$, but $N(\pm 2)=4$, $N(\pm 3)=9$ ↯

(Possible u)

$\therefore$ By contradiction, A_{-19} has no universal side divisor. □

3-5-25 (WEEK 3)

Shun / 舜海 (@shun4midx)

PID AND UFD

Today, assume R is an integral domain.

DEFINITION

Let $p \in R \setminus \tilde{R}$ ($\tilde{R} = R^\times \cup \{0\}$). We say p is a **prime** if "$p \mid ab \Rightarrow p \mid a$ or $p \mid b$", and we say p is **irreducible** if "$p = ab \Rightarrow a \in R^\times$ or $b \in R^\times$"

FACT 1

1. Prime $\Rightarrow$ irreducible

   Proof

   $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Say $p \mid a$, then $a = pc \Rightarrow p = pcb \Rightarrow cb = 1$, so $b \in R^\times$. Similar for $p \mid b \Rightarrow a \in R^\times$

2. Irreducible $\not\Rightarrow$ prime (☆ important)

   Example: In A_{-5} (mod 4 $\equiv -1$, so norm has no $\frac{1}{2}$), we have $2(3) = (1+\sqrt{-5})(1-\sqrt{-5})$

   ↳ "$1+\sqrt{-5}$ is irred": $1+\sqrt{-5} = \alpha\beta \Rightarrow N(1+\sqrt{-5}) = 6 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = 1$ or $N(\beta) = 1$ ($\alpha \in A_{-5}^\times$, $\beta \in A_{-5}^\times$)

   ↳ $(1+\sqrt{-5}) \nmid 2, 3$: If $2 = (1+\sqrt{-5})\alpha$, then $N(2) = N(1+\sqrt{-5})N(\alpha) \Rightarrow N(\alpha) = \frac{2}{3} \notin \mathbb{N}$ ↯

PROPOSITION 1

Let R be a PID and $p \in R \setminus \tilde{R}$. TFAE:

(a) p is irr

(b) $\langle p \rangle \in \operatorname{Max} R$

(c) $\langle p \rangle \in \operatorname{Spec} R$

(d) p is a prime

Proof

"(a) $\Rightarrow$ (b)": $\exists M \in \operatorname{Max} R$, s.t. $\langle p \rangle \subseteq M = \langle m \rangle$ (PID) $\Rightarrow$ "$p = um \Rightarrow u \in R^\times$ or $m \in R^\times$" ($1 \in \langle m \rangle = R$) $\Rightarrow m = u^{-1}p \Rightarrow \langle m \rangle \subseteq \langle p \rangle \Rightarrow \langle p \rangle = \langle m \rangle = M \in \operatorname{Max} R$

"(b) $\Rightarrow$ (c)": OK

"(c) $\Rightarrow$ (d)": $p \mid ab \Rightarrow ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle \Rightarrow p \mid a$ or $p \mid b$

"(d) $\Rightarrow$ (a)": By fact

DEFINITION

R is a **unique factorization domain** (UFD) if:

- $\forall a \in R \setminus \tilde{R}$, $\exists u \in R^\times$, irr p_i: $\forall i = 1, \dots, r$, s.t. $a = up_1p_2 \cdots p_r$
- If $a = up_1 \cdots p_r = vq_1 \cdots q_\ell$, then $r = \ell$ and $p_i \sim q_i$ ("associated": i.e. differ by a unit) after some change of the indecies $\forall i = 1, \dots, r$

PROPOSITION 2

R is a UFD $\Leftrightarrow$ { ACC (Ascending Chain Condition) on principal ideals, i.e. $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots$ and $\exists k$, s.t. $\langle a_k \rangle = \langle a_{k+1} \rangle = \dots$; irr $\Rightarrow$ prime }

Proof

"$\Rightarrow$": · Assume that $0 \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \subsetneq \cdots$

$\because \langle a_1 \rangle \neq R$, $\langle a_2 \rangle \neq R$

$\therefore a_1, a_2 \in R \setminus \tilde{R}$, say $a_1 = up_1 \cdots p_n$, $a_2 = vq_1 \cdots q_m$

Now, $a_1 \in \langle a_2 \rangle \Rightarrow a_2 \mid a_1 \Rightarrow a_1 = a_2 b \Rightarrow up_1 \cdots p_n = vq_1 \cdots q_m b$

$\langle a_1 \rangle \neq \langle a_2 \rangle \Rightarrow a_1 \nmid a_2 \Rightarrow b \notin R^\times \Rightarrow b = v'q_1' \cdots q_r'$, $r \geq 1$.

By uniqueness (UFD), $n = m + r$, $r \geq 1 \Rightarrow n > m$, $q_i \sim p_i$ $\forall i = 1, \dots, m$. We conclude that $a_2 = u'p_1 \cdots p_m$

Similarly, $a_3 = u''p_1 \cdots p_s$, $s \leq m < n$, etc… However, $\{p_i\}$ is a finite set ↯

- Let a be irr and $a|bc$, say $bc=ad$.
  - ↳ $b=0$ or $c=0$: $a|bc=0 \Rightarrow a|0 \Rightarrow a|b$ or $a|c$
  - ↳ $b\in R^\times$ or $c\in R^\times$: Say $b\in R^\times$, $c=adb^{-1} \Rightarrow a|c$. Similarly, $c\in R^\times \Rightarrow a|b$.
  - ↳ $b\in R\setminus\tilde{R}$ or $c\in R\setminus\tilde{R}$: Let $b=up_1\cdots p_n$, $c=vq_1\cdots q_m$, then a is irr and $uvp_1\cdots p_nq_1\cdots q_m=ad \Rightarrow a|p_i$ or $a|q_j \Rightarrow a|b$ or $a|c$

"$\Leftarrow$": Existence: Let $a\in R\setminus\tilde{R}$.

Claim: a has at least one irr factor

Proof

If a is irr, then done. Otherwise, $a=a_1b_1$, $a_1, b_1\notin R^\times$.

$\Rightarrow$ If a_1 is irr, then done. Otherwise $a_1=a_2b_2$, $a_2, b_2\notin R^\times$.

⋮

$\therefore$ Eventually, $\exists\, a_n$ that is irr. Otherwise, we find $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \langle a_3\rangle \subsetneq \cdots$ nonending ↯

Now, if a is irr, then done. Otherwise, $a=p_1a_1$ with irr p_1 and $a_1\notin R^\times$.

If a_1 is irr, then done. Otherwise, $a_1=p_2a_2$ with irr p_2 and $a_2\notin R^\times$.

⋮

Eventually, $\exists$ irr a_n and $a_{n-1}=p_na_n$ (Key) Otherwise, we find $\langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots$ nonending ↯

Hence, $a=p_1\cdots p_na_n=p_1\cdots p_np_{n+1}$, which is a prime decomposition. ✓

Uniqueness: Let $a=up_1\cdots p_n=vq_1\cdots q_m$

By induction on n, $n=1 \Rightarrow up_1=vq_1\cdots q_m \Rightarrow p_1=u^{-1}vq_1\cdots q_m \Rightarrow m=1$ and $p_1\sim q_1$

For $n>1$, $p_1|q_1\cdots q_m \Rightarrow p_1|q_i$ for some i, say $q_i=q_1$, write $q_1=p_1w$ (irr = prime)

Then, $up_1\cdots p_n=vwp_1q_2\cdots q_m \Rightarrow$ By induction hypothesis, $n-1=m-1 \Rightarrow n=m$ and $p_i\sim q_i$ $\forall i=2,\ldots,m$. ✓

THEOREM

PID $\Rightarrow$ UFD

Proof

- "irr $\Rightarrow$ prime": Ref above
- "$\langle a_1\rangle\subseteq\langle a_2\rangle\subseteq\ldots$": Let $I=\bigcup_{i=1}^{\infty}\langle a_i\rangle$, which is also an ideal. Say $I=\langle a\rangle$ and $a\in\langle a_\ell\rangle$ for some ℓ.
  Then, $I=\langle a\rangle\subseteq\langle a_\ell\rangle\subseteq\langle a_{\ell+1}\rangle\subseteq\ldots\subseteq I \Rightarrow \langle a_\ell\rangle=\langle a_{\ell+1}\rangle=\ldots$ ✓

RING OF GAUSSIAN INTEGERS

Gaussian Integers: A_{-1} is a ED, PID, and UFD. (We underline things to prove here in orange)

- $A_{-1}^\times=\{\pm1,\pm i\}$: $N(\alpha)=N(a+bi)=a^2+b^2=1 \Leftrightarrow a=\pm1$, $b=0$ or $a=0$, $b=\pm1$ ✓
- $\alpha\in A_{-1}\setminus\tilde{A}_{-1}$ is a Gauss prime $\Rightarrow N(\alpha)=p$ or p^2 for some prime integer p.
  - ↳ Write $N(\alpha)=\alpha\bar{\alpha}=p_1\cdots p_n$, prime integers p_i. Then, $\alpha|p_1\cdots p_n \Rightarrow \alpha|p_i$ for some i.
  Say $p_i=\alpha\beta \Rightarrow p_i=\bar{p}_i=\bar{\alpha}\bar{\beta} \Rightarrow \bar{\alpha}|p_i$. So, $\alpha\bar{\alpha}=N(\alpha)|p_i^2 \Rightarrow N(\alpha)=p$ or p^2 ✓
- If $N(\alpha)=p^2$, say $p=\alpha\beta \Rightarrow \bar{p}=\bar{\alpha}\bar{\beta}$. So, $p^2=N(\alpha)N(\beta) \Rightarrow N(\beta)=1 \Rightarrow \beta\in A_{-1}^\times \Rightarrow p\sim\alpha$ is a Gauss prime

CLAIM

$p\sim\alpha$ is a Gauss prime $\Leftrightarrow x^2+1$ is irr in $\mathbb{Z}/p\mathbb{Z}[x]$

Proof

Consider $\varphi: \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[i]=A_{-1}$, $f(x)\mapsto f(i)$

Then, $\ker\varphi=\{f(x)\mid f(i)=0\}=\langle x^2+1\rangle$ (Proof: Gauss Lemma in the next section)

By 1st Isom thm, $\mathbb{Z}[x]/\langle x^2+1\rangle\cong\mathbb{Z}[i]=A_{-1}$.

Now, p is a Gauss prime $\Leftrightarrow \langle p\rangle\in\operatorname{Max}A_{-1}$

By 3rd Isom thm, $\mathbb{Z}[x]/\langle p, x^2+1\rangle \cong \mathbb{Z}[x]/\langle p\rangle/\langle p, x^2+1\rangle/\langle p\rangle \cong \mathbb{Z}[x]/\langle p\rangle/\langle x^2+1\rangle$ is a field, i.e. $\mathbb{Z}[i]/\langle p\rangle$ is a field $\Leftrightarrow \langle x^2+1\rangle\in\operatorname{Max}\mathbb{Z}/p\mathbb{Z}[x]$

$\Leftrightarrow x^2+1$ is irr in $\mathbb{Z}/p\mathbb{Z}[x]$

Shun/翔海 (@shun4midx)

CLAIM

p is not a Gauss prime $\Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

Proof

Say $p=\bar{\alpha}\alpha \Leftrightarrow x^2+1$ is irr in $\mathbb{Z}/p\mathbb{Z}[x]$

$\Leftrightarrow x^2\equiv -1 \pmod p$ has integer solution

$\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $a^2\equiv -1 \pmod p$

$\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $O(\bar{a})=4$ in $(\mathbb{Z}/p\mathbb{Z}^\times, \bar{1})$ or $p=2$

(Lagrange) $\Leftrightarrow \exists a\in\mathbb{Z}$, s.t. $4\mid|\mathbb{Z}/p\mathbb{Z}^\times|=p-1 \Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

- Opposite direction: $2^2=4\mid p-1=|\mathbb{Z}/p\mathbb{Z}^\times|$. By Sylow I, $\exists H\le \mathbb{Z}/p\mathbb{Z}^\times$ (cyclic), s.t. $|H|=|\langle\bar{a}\rangle|=4$

$\therefore p=a^2+b^2=N(a+bi) \Leftrightarrow p\equiv 1 \pmod 4$ or $p=2$

CLAIM

$n=A^2+B^2 \Leftrightarrow n=2^k p_1^{a_1}\cdots p_r^{a_r} q_1^{b_1}\cdots q_s^{b_s}$, $p_i\equiv 1 \pmod 4$, $q_j\equiv 3 \pmod 4$, $b_i\equiv 0 \pmod 2$

Proof

"$\Rightarrow$": For $n=N(A+Bi)=N(\alpha_1)N(\alpha_2)\cdots N(\alpha_k)$, write $A+Bi=\alpha_1\cdots\alpha_k$, α_i: Gauss prime

Here, $N(\alpha_i)=p$ or $p^2 \Leftrightarrow$ ($p=2$ or $p\equiv 1 \pmod 4$ (related to p as norm)) or $p\equiv 3 \pmod 4$ (related to p^2 as norm)

"$\Leftarrow$": $2=(1-i)(1+i)$, $(1+i)\sim(1-i)$, write $p_i=\alpha_i\bar{\alpha}_i$

Let $(1+i)^k\alpha_1^{a_1}\cdots\alpha_r^{a_r}q_1^{\frac{b_1}{2}}\cdots q_s^{\frac{b_s}{2}}=A+Bi$, then $(1-i)^k\bar{\alpha}_1^{a_1}\cdots\bar{\alpha}_r^{a_r}\bar{q}_1^{\frac{b_1}{2}}\cdots\bar{q}_s^{\frac{b_s}{2}}=A-Bi$

Multiplying the two, we get $n=A^2+B^2$

3-7-25 (WEEK 3)

Shun / 翔海 (@shun4midx)

GAUSS LEMMAS AND IRREDUCIBILITY

- $\varphi: \mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}[i]$
  $f(x) \mapsto f(i)$

We have $\ker\varphi = \langle x^2+1 \rangle$
By long division, $\forall f(x)$, $\exists q(x) \in \mathbb{Z}[x]$, s.t. $f(x) = q(x)(x^2+1) + (ax+b)$

for today's notes, R is an integral domain.

QUESTION

When is $R[x]$ a UFD? (For example, R is a field. How about if R is a UFD?)

STRATEGY

Let F be the quotient field of R, then $R[x] \hookrightarrow F[x]$ and $F[x]$ is a UFD.
We intend to compare the factorization of $f(x) \in R[x]$ in $F[x]$ and a factorization in $R[x]$

DEFINITION

Let R be a UFD ($\Rightarrow$ GCD domain) and $f(x) \in R[x]$ (gcd is unique up to a unit factor)

- $f(x) = a_n x^n + \dots + a_0$ is said to be primitive if a gcd of $a_n, \dots, a_0$ is 1
- $\text{cont}(f) :=$ a gcd of $a_0, \dots, a_n$ which is unique up to a unit factor in R
  ("content")

PROPOSITION 1 (GAUSS LEMMA)

Let R be a UFD and $f(x), g(x) \in R[x]$. Then, $\text{cont}(fg) = \text{cont}(f)\,\text{cont}(g)$

Proof

Step 1: f, g primitive $\Rightarrow fg$ primitive

Let $f(x) = a_n x^n + \dots + a_0$, $a_{-1} := 0$, $a_i := 0$ $\forall i > n$
$g(x) = b_m x^m + \dots + b_0$, $b_{-1} := 0$, $b_j := 0$ $\forall j > m$

Suppose $f(x)g(x) = c\,h(x)$ with c being a non-unit and $h(x)$ being primitive (c: cont(fg))

Take a prime factor $p \mid c$ and assume that $p \nmid a_r$, $p \mid a_i$, $i = -1, \dots, r-1$ and $p \nmid b_s$, $p \mid b_j$, $j = -1, \dots, s-1$

Then, the coefficient of x^{r+s} in $f(x)g(x)$ is $a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1} + a_r b_s + \dots + a_{r+s} b_0$
(from $p \mid c$; $a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1}$: divisible by p; $a_{r+s} b_0$: divisible by p)

However, $p \mid a_0 b_{r+s} + \dots + a_{r+s} b_0 \Rightarrow p \mid a_r b_s \Rightarrow p \mid a_r$ or $p \mid b_s$ ↯

Step 2: $\text{cont}(fg) = \text{cont}(f)\,\text{cont}(g)$

Write $f(x) = \text{cont}(f) f_1(x)$, $g(x) = \text{cont}(g) g_1(x)$, then $fg = \text{cont}(f)\,\text{cont}(g)\, f_1(x) g_1(x) \Rightarrow \text{cont}(fg) = \text{cont}(f)\,\text{cont}(g)$ □ ($f_1 g_1$: primitive)

PROPOSITION 2

Let R be a UFD and F be the quotient field. For $f(x) \in R[x]$, if $f(x) = A(x)B(x)$ with $A(x), B(x) \in F[x]$, then $\exists r, s \in F$, s.t. $rA(x) = a_1(x) \in R(x)$, $sB(x) = b_1(x) \in R[x]$ and $f(x) = a(x)b(x)$

Proof

Write $A(x) = \frac{l_1}{t_1} a_1(x)$, $B(x) = \frac{l_2}{t_2} b_1(x)$, where a_1, b_1 are primitive in $R[x]$ and $l_i, t_i \in R$ with $\gcd(l_i, t_i) = 1$ $\forall i = 1, 2$
By assumption, $f(x) = \frac{l_1 l_2}{t_1 t_2} a_1(x) b_1(x) \Rightarrow t_1 t_2 f(x) = l_1 l_2 a_1(x) b_1(x) \Rightarrow t_1 t_2 \,\text{cont}(f) = l_1 l_2 u$ for some $u \in R^\times$.

So, $f(x) = \frac{u^{-1} t_1 t_2 \,\text{cont}(f)}{t_1 t_2} a_1(x) b_1(x)$, so $a_1(x) = \frac{u^{-1} t_1 \,\text{cont}(f)}{l_1} A(x)$, $b_1(x) = \frac{t_2}{l_2} B(x)$

Shun/翔海 (@shun4midx)

- In $A_0 \ni p+q\sqrt{D}$, show "$x^2-2px+(p^2-Dq^2) \in \mathbb{Z}[x]$" satisfies $f(x)=0$ for $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0$
  Say $f(x)=q(x)g(x)+ax+b$, write $g(x)=x^2-\frac{a}{c}x+\frac{b}{d}$. Then, $f(x)=\frac{k}{t}\bar{q}(x)\frac{1}{cd}(dcx^2-adx+bc) \Rightarrow k \sim tcd$, i.e. $k=\pm tcd$
  $\therefore f(x)=\pm\bar{q}(x)(dcx^2-adx+bc) \Rightarrow$ Comparing, we get $dc|1 \Rightarrow d,c=\pm 1 \Rightarrow g(x)\in\mathbb{Z}[x]$ ✓

COROLLARY

If $f(x)$ is primitive of deg >0, then $f(x)$ is irr in $F[x] \Leftrightarrow f(x)$ is irr in $R[x]$

PROPOSITION 3

R is a UFD $\Rightarrow R[x]$ is a UFD (e.g. $\mathbb{Z}[x_1,\dots,x_n]$; $\mathbb{Q}[x_1,\dots,x_n]$ are UFDs)

Proof

Let F be the quotient field of R.

Existence: Given $f(x)\in R[x]\setminus\widetilde{R[x]}$, write $f(x)=\text{cont}(f)\underbrace{f_1(x)}_{\text{primitive}}$

Assume that $f_1(x)$ is not a unit in $R[x]$, i.e. $\deg f_1>0$ $(R[x]^\times=R^\times)$

- $\text{cont}(f)\in R$, which is a UFD, so $\text{cont}(f)$ has unique factorization
- $f_1(x)$ has a unique factorization
  $f_1(x)\in R[x]\subseteq F[x]$ is a UFD $\Rightarrow f_1(x):=p_1(x)p_2(x)\dots p_r(x)$ with irr p_i in $F[x]$
  By prop 2, $\exists r_i\in F$, s.t. $q_i(x)=r_ip_i(x)\in R[x]$ $\forall i$ and $f_1(x)=q_1(x)q_2(x)\dots q_r(x)$

  Note that f_1 is primitive $\Rightarrow q_i$ is primitive $\forall i$, and $q_i(x)=r_ip_i(x)$ is irr in $F[x] \Rightarrow q_i(x)$ is irr in $R[x]$.

Uniqueness: Assume that $f_1(x)=p_1(x)p_2(x)\dots p_r(x)=q_1(x)q_2(x)\dots q_s(x)$ where p_i, q_j are irr in $R[x]$.
By corollary of prop 2, p_i, q_j are irr in $F[x]$
By uniqueness of $F[x]$, $r=s$ and $p_i\sim q_i$ in $F[x]$ after some change of the indices
$\Rightarrow p_i(x)=\frac{t_i}{k_i}q_i(x)$ for $k_i,t_i\in R \Rightarrow t_ip_i(x)=k_iq_i(x) \Rightarrow t_i=u_ik_i$ for some $u_i\in R^\times$, so $p_i(x)=u_i^{-1}q_i(x)$, i.e. $p_i\sim q_i$ in $R[x]$

EXAMPLE

$\mathbb{Z}[x]$ is a UFD but not a PID

Proof

Say $\langle f(x)\rangle=\langle x,2\rangle$, then $f(x)|2$ and $f(x)|x \Rightarrow f(x)=\pm 1 \Rightarrow \langle f(x)\rangle=\mathbb{Z}[x]$ (but $1\notin\langle x,2\rangle$) $\nrightarrow$

FACT

Let $I\subsetneq R$ and $f_1(x)\in R[x]$ be monic with deg $f>0$. If $\bar{f}(x)$ is irr in $R/I[x]$, then $f(x)$ is irr in $R[x]$

Proof

If $f(x)=g(x)h(x)$ with $g,h\in R[x]\setminus\widetilde{R[x]}$, then f is monic $\Rightarrow$ primitive $\Rightarrow \deg g>0$ and $\deg h>0$.

Now, consider $\bar{f}(x)=\bar{g}(x)\bar{h}(x)$ in $R/I[x]$
Since f is monic and $1\notin I$, $\deg\bar{f}=\deg f=\deg g+\deg h\geq\deg\bar{g}+\deg\bar{h}\geq\deg\bar{f}$
Moreover, $\deg g\geq\deg\bar{g}$ and $\deg h\geq\deg\bar{h}$, so $\deg\bar{g}=\deg g\geq 1$ and $\deg\bar{h}=\deg h\geq 1$, i.e. $\bar{f}$ is reducible in $R/I[x]$

EXAMPLES (The converse of the fact may not always hold)

(1) x^4+1 is irr in $\mathbb{Z}[x]$ but is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$ $(x^4+\bar{1}=x^4-\bar{1}=(x^2-\bar{1})(x^2+\bar{1})=(x+\bar{1})^4)$

(2) x^3+x+1 is irr in $\mathbb{Q}[x]$ (hence also irr in $\mathbb{Z}[x]$)
In $\mathbb{Z}/2\mathbb{Z}[x]$, $\bar{f}(\bar{0})=\bar{1}$ and $\bar{f}(\bar{1})=\bar{1}$ $\therefore \bar{f}$ is irr in $\mathbb{Z}/2\mathbb{Z}[x] \Rightarrow$ irr in $\mathbb{Z}[x]$ (Notice how much easier the process was!)

EISENSTEIN CRITERION

Shun/翔海 (@shun4midx)

Let $P \in \operatorname{Spec} R$ and $f(x) = a_n x^n + \dots + a_0$ be primitive in $R[x]$.
Assume that $a_n \notin P$, $a_{n-1}, \dots, a_0 \in P$, $a_0 \notin P^2$. Then, $f(x)$ is irr in $R[x]$

Proof

Suppose $f(x) = g(x)h(x)$ with $\deg g > 0$, $\deg h > 0$.
Consider $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ in $R/P[x]$
$\bar{a}_n x^n$ $\bar{b}_r x^r$ $\overline{c_{n-r}}\, x^{n-r}$
Given $\Rightarrow$ Implied
Now, as R is an integral domain, thus $\deg f = \deg g + \deg h$

Write $g(x) = b_r x^r + \dots + b_0$, $b_{r-1}, \dots, b_0 \in R$
$h(x) = c_{n-r} x^{n-r} + \dots + c_0$, $c_{n-r-1}, \dots, c_0 \in R$
However, $a_0 = c_0 b_0 \in P^2$ ↯ $\therefore f(x)$ is irr in $R(x)$ □

EXAMPLE

$f(x) = x^2 + px + p^2$ is irr in $\mathbb{Z}[x]$ (Violating criteria for Eisenstein criterion does NOT mean it is reducible)

Proof

- f has no linear factor: If $f(\alpha) = 0$, then $\alpha = -kp$ for $k \in \mathbb{N}$ ↯ $(x + kp)$ can't be a factor since the last term is p^2
- Thus $f = gh$, $\deg g \geq 2$, $\deg h \geq 2$.
  Consider $x^n = \bar{f} = \bar{g}\bar{h}$ in $\mathbb{Z}/p\mathbb{Z}(x)$, then $g = x^r + \dots + b_1 x + b_0$, $h = x^{n-r} + \dots + c_1 x + c_0$, $p \mid b_1$, $p \mid b_0$, $p \mid c_1$, $p \mid c_0$. Then, $p = b_1 c_0 + c_1 b_0 \equiv 0 \pmod{p^2}$ ↯

3-12-25 (WEEK 4)

Shun / 舜海 (@shun4midx)

RESULTANT

DEFINITION

Let R be a commutative ring and $f(x)=a_nx^n+\dots+a_0$, $g(x)=b_mx^m+\dots+b_0 \in R[x]$.

The resultant of f and g is the determinant here:

$$R(f,g)=\det A=\begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & a_0 & \\ & & \ddots & & & \ddots \\ & & & a_n & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_m & \cdots & b_0 & \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \} m \text{ rows} \\ \\ \} n \text{ rows} \end{matrix}$$

PROPOSITION 1

$\exists\, r(x), s(x) \in R[x]$ with $\deg r \le m-1$, $\deg s \le n-1$, s.t. $r(x)f(x)+s(x)g(x)=R(f,g)$

Proof

$$x^{m-1}f(x): \quad a_nx^{n+m-1}+a_{n-1}x^{n+m-2}+\dots+a_0x^{m-1}$$
$$x^{m-2}f(x): \quad a_nx^{n+m-2}+\dots+a_1x^{m-1}+a_0x^{m-2}$$
$$\vdots$$
$$f(x): \quad a_nx^n+\dots+a_0$$
$$x^{n-1}g(x): \quad b_mx^{n+m-1}+b_{m-1}x^{n+m-2}+\dots$$
$$\vdots$$
$$g(x): \quad b_mx^m+\dots+b_0$$

Thus,

$$A\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} x^{m-1}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix} \Rightarrow \text{By Cramer's Rule, } 1=\frac{1}{\det A}\begin{vmatrix} a_n & x^{m-1}f(x) \\ \vdots & \vdots \\ b_m & g(x) \end{vmatrix} \Rightarrow R(f,g)=r(x)f(x)+s(x)g(x)$$

COROLLARY

f and g have a common divisor of $\deg \ge 1 \Rightarrow R(f,g)=0$ (Say $h \mid f, h \mid g \Rightarrow h \mid R(s,g) \overset{?}{=} rf+sg$)

PROPOSITION 2

Let $f(x)=a_n\prod_{i=1}^{n}(x-y_i)=\sum_{i=0}^{n}a_ix^i$, and $g(x)=b_m\prod_{j=1}^{m}(x-z_j)=\sum_{j=0}^{m}b_jx^j \in R(y_1,\dots,y_n,z_1,\dots,z_m)[x]$, where $a_n, b_m \in R$, $a_0/a_n \dots a_{n-1}/a_n$ are elementary symmetric functions in $y_1,\dots,y_n$ (w.r.t. $z_1,\dots,z_m$) up to sign. Then, $R(f,g)=a_n^m b_m^n \prod_{i,j}(y_i-z_j)=a_n^m\prod_{i=1}^{n}g(y_i)=(-1)^{mn}b_m^n\prod_{j=1}^{m}f(z_j)$

Proof

- $R(f,g)$ is a homogeneous poly of deg mn in $R(y_1,\dots,y_n,z_1,\dots,z_m]$

$$\begin{vmatrix} a_n & a_{n-1} & \cdots & & & \\ & a_n & a_{n-1} & \cdots & & \\ & & \ddots & & & \ddots \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & \\ & \ddots & & & & b_0 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} y_1^{n+m-1} \\ y_1^{n+m-2} \\ \vdots \\ y_1^n \\ \vdots \\ 1 \end{matrix} = \begin{vmatrix} \deg 1 & \cdots & \deg n+m \\ & & \end{vmatrix}$$

↑ Multiply

So, $R(f,g)$ is a homo poly of deg: $\frac{(n+m)(n+m+1)}{2}-\frac{n(n+1)}{2}-\frac{m(m+1)}{2}=mn$ ✓

- $g(y_i) \mid R(f,g)\ \forall i$

$$\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & \\ & \ddots & \ddots & & \ddots & a_0 \\ b_m & b_{m-1} & & & & \\ & b_m & \cdots & & & \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} y_i^{m+n-1} \\ y_i^{m+n-2} \\ \vdots \\ y_i \\ 1 \end{matrix} = \begin{vmatrix} y_i^{m-1}f(y_i) \\ y_i^{m-2}f(y_i) \\ \vdots \\ f(y_i) \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} 0 \\ \\ \\ \\ \\ \\ \end{matrix} = g(y_i)\begin{vmatrix} \deg 1 & \cdots & \deg n+m-1 \\ & & \end{vmatrix} \Rightarrow g(y_j) \mid y_j^{m+n}R(f,g) \Rightarrow g(y_i) \mid R(f,g)\ \forall i$$

- $\prod_{i,j}(y_i-z_j) \mid R(f,g)$: Since $g(y_i) \mid R(f,g)$, i.e. $\prod_{j=1}^{m}(y_i-z_j) \mid R(f,g)\ \forall i$ and $\prod_j(y_i-z_j)$ and $\prod_j(y_k-z_j)$ have no common factor

Shun / 翔海 (@shun4midx)

- Since $\deg \prod_{i,j}(y_i - z_j) = \deg R(f,g) = \min$ in $y_1,\dots,y_n,z_1,\dots,z_m$, and $R(f,g) = c\prod_{i,j}(y_i - z_j)$ for some $c \in R$.
  When we take $y_1 = \dots = y_n = 0$, $z_1 = \dots = z_m = 1$, we get $a_0 = \dots = a_{n-1} = 0$, $b_0 = (-1)^m b_m$
  Thus, $LHS = a_n^m b_0^n = (-1)^{nm} a_n^m b_m^n$
  $RHS = (-1)^{nm} c$ //

COROLLARY
Let $f,g \in F[x]$ with F being a field and $a_n b_m \neq 0$. Then, $R(f,g) = 0 \Leftrightarrow f$ and g have a root in common

Proof
$\exists$ field $\Omega \supset F$, s.t. $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ for $\alpha_j, \beta_j \in \Omega$ and then $R(f,g) = a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$
Hence, $R(f,g) = 0 \Leftrightarrow \prod_{i,j}(\alpha_i - \beta_j) = 0 \Leftrightarrow \alpha_i = \beta_j$ for some i, j □

FIELD EXTENSION (VERY ROUGH SKETCH)
qwq don't attack me I still dk Galois Theory ._. here's just smth I came up with to explain
ボクは代数学が本当にできないqwq ~ TT (始めてノートに日本語を使うね~...)

$f(x) \in F[x] \Rightarrow \exists \alpha \in F_1 \supset F$ s.t. $f(\alpha) = 0$

Proof
As $F[x]$ is a UFD, $f(x) = \underbrace{f_1(x)}_{\text{irr}} \cdots \underbrace{f_r(x)}_{\text{irr}}$ (UFD)

Consider $F_1 = F[x]/\langle f_1(x)\rangle$ (Max $F[x]$) which is a field
Let $\alpha = \bar{x}$ in F_1, then $f_1(\alpha) = \overline{f_1(x)} = \bar{0}$ in $F_1 \Rightarrow f(\alpha) = f_1(\alpha)\cdots f_r(\alpha) = 0$ ✓

Furthermore, we can find $\Omega \supset F_1$ s.t. $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ in $\Omega[x]$:
Let $\alpha \in F_1$ s.t. $f(\alpha) = 0 \Rightarrow f(x) = g(x)(x - \alpha)$ with $g(x) \in F_1[x]$. Here, $\deg g \leq n-1$. By induction, $g(x) = a_n \prod_{j=2}^{n}(x - \alpha_j)$, $\alpha_j \in \Omega \supset F$ ✓

Also, $R(f,g) = 0 \Leftrightarrow f, g$ have a common root $\Leftrightarrow$ say $\exists f(\alpha) = 0$, then $\exists$ minimal poly $m_\alpha(x) \mid f(x)$,
$\Updownarrow$ f, g have a common factor $\quad g(\alpha) = 0 \Rightarrow m_\alpha(x) \mid g(x)$ too ✓

DEFINITION
If $f(x) = a_n \prod_{j=1}^{n}(x - \alpha_j)$, $\alpha_j \in \Omega$, then we define the discriminant of f to be $D(f) = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2$

PROPOSITION 3 (Derivative)
$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} D(f)$

Proof
$f'(x) = a_n \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j)$
By prop 2, $R(f, f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$ and $f'(\alpha_i) = a_n \prod_{j \neq i}(\alpha_i - \alpha_j)$ $\forall i$ □

COROLLARY
f has a repeated root $\Leftrightarrow D(f) = 0 \Leftrightarrow R(f, f') = 0$

EXAMPLE
$f(x) = x^3 + px + q$, $f'(x) = 3x^2 + p$
Then, $R(f, f') = \begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = 4p^3 + 27q^2$

EXAMPLE
$f = x^2 + 2xy^2 + y + 1$
Here, repeated roots are when: $D(f) = (2y^2 - 1)^2 - 4(1)(y+1) = 0$

QUESTION
How to solve $f(x,y) = 0$ and $g(x,y) = 0$ with $f(x,y), g(x,y) \in \mathbb{C}(x,y)$? (Assuming $f(x) = 0$ is something we can solve)

Shun / 舜海 (@shun4midx)

STRATEGY

Write $f(x,y)=a_n(y)x^n+\dots+a_0(y)$, $g(x,y)=b_m(y)x^m+\dots+b_0(y)$ with $a_i(y),\ b_i(y)\in\mathbb{C}[y]$.
By prop 1, $\exists\ r(x,y),\ s(x,y)\in\mathbb{C}[x,y]$, $\deg_x r\le m-1$, $\deg_x s\le n-1$, s.t. $r(x,y)f(x,y)+s(x,y)g(x,y)=R(f,g,x)\in\mathbb{C}[y]$
If $(a,b)\in\mathbb{C}^2$ with $f(a,b)=0$, $g(a,b)=0$, then $R(f,g)(b)=0$

PROPOSITION 4

Let $f(x,y)=y^n+a_1(x)y^{n-1}+\dots+a_n(x)$, $g(x,y)=y^m+b_1(x)y^{m-1}+\dots+b_m(x)\in\mathbb{C}[x,y]$.
If a gcd of $f(x,y)$ and $g(x,y)$ is 1, then $f(x,y)=0$, $g(x,y)=0$ has only finitely-many solutions

Proof

(If not, then $rf+sg=0\Rightarrow rf=-sg\Rightarrow r|g$, i.e. $g=r\tilde{r}\Rightarrow f=-s\tilde{r}\Rightarrow\tilde{r}|f$ ↯)

Let $\varphi(x)=R(f,g,y)$. By assumption, $\varphi(x)\not\equiv 0$
$\therefore$ φ has finitely many roots, say $a_1,\dots,a_r$
Then, $\forall i$, $f(a_i,y)=0$, $g(a_i,y)=0$ has only finitely many solutions

EXAMPLE

$$\begin{cases} f(x,y)=x^2+2y^2-3=0 \\ g(x,y)=x^2+xy+y^2-3=0 \end{cases}$$

$$R(f,g,x)=\begin{vmatrix} 1 & 0 & 2y^2-3 & \\ & 1 & 0 & 2y^2-3 \\ 1 & y & y^2-3 & \\ & 1 & y & y^2-3 \end{vmatrix}=3y^4-3y^2=3y^2(y-1)(y+1)\Rightarrow y=0,\pm 1.$$

$y=0\Rightarrow x=\pm\sqrt{3}$
$y=1\Rightarrow x=1$
$y=-1\Rightarrow x=-1$

EXAMPLE

Let $f(x)=x^3+4x^2-x-4$
$R(f,f')=-450$.

Find all prime integers p, s.t. $f(x)\pmod p$ has a repeated root $\Rightarrow p=2,3,5$
$p=2\Rightarrow x=1$
$p=3\Rightarrow x=-1$
$p=5\Rightarrow x=1$

3-14-25 (WEEK 4)

Shun / 翔海 (@shun4midx)

GRÖBNER BASIS (I) (Sorry for the late upload... Hope the longer length makes up for it. 本当にごめん...)

DEFINITION

Let R be a commutative ring. R is a **Noetherian ring** if every ideal of R is finitely generated

FACT

Let R be commutative. TFAE

(1) Each ideal of R is finitely generated

(2) ACC on ideals of R, i.e. $I_1 \subseteq I_2 \subseteq \dots \Rightarrow \exists k$, s.t. $I_k = I_{k+1} = \dots$

(3) Maximal condition on ideals: S is a nonempty set of ideals of $R \Rightarrow \exists$ maximum element of S.

Proof

(1) $\Rightarrow$ (2): Let $I = \bigcup_{i=1}^{\infty} I_i$, which is an ideal of R, say $I = \langle a_1, \dots, a_n \rangle$ and $a_i \in I_{k_i}$

If $k = \max\{k_i : i = 1, \dots, n\}$, then $a_i \in I_k \ \forall i = 1, \dots, n$, i.e. $I \subseteq I_k \subseteq I_{k+1} \subseteq \dots \subseteq I \Rightarrow I = I_k = I_{k+1} = \dots$

(2) $\Rightarrow$ (1): Let I be an ideal of R. Assume I is not finitely generated. Take $a_1 \in I$

Since $I \neq \langle a_1 \rangle$, $\exists a_2 \in I \setminus \langle a_1 \rangle$. Since $I \neq \langle a_1, a_2 \rangle$, then $\exists a_3 \in I \setminus \langle a_1, a_2 \rangle$, ...

$\therefore \langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots$ $\nrightarrow$ (ofc not ACC)

(2) $\Rightarrow$ (3): Assume $\nexists$ max element in S.

Take $I_1 \in S$. Since I_1 is not max, $\exists I_2 \in S$, s.t. $I_1 \subsetneq I_2$. Since I_2 is not max, $\exists I_3$, s.t. $I_2 \subsetneq I_3 \dots$.

$\therefore \exists I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ $\nrightarrow$

(3) $\Rightarrow$ (2): Let $S = \{I_1, I_2, \dots\}$

By assumption, $\exists$ **max** I_k in S.

$\therefore I_k \supseteq I_{k+1}, I_k \supseteq I_{k+2}, \dots$. Thus, $I_k = I_{k+1} = I_{k+2} = \dots$ $\square$

HILBERT BASIS THEOREM

If R is Noetherian, then $R[x_1, \dots, x_n]$ is also Noetherian

Proof

Assume that $\exists I \subsetneq R[x_1, \dots, x_n]$ that is not finitely generated

Choose $f_1 \in I$, s.t. f_1 is least degree in I.

$\Rightarrow \exists f_2 \in I$, s.t. f_2 is least degree in $I \setminus \langle f_1 \rangle$

$\vdots$

Let $\deg f_i = n_i$ and the leading term of f_i be a_i.

$\Rightarrow n_1 \leq n_2 \leq n_3 \leq \dots$

Claim: $\langle a_1 \rangle \subsetneq \langle a_1, a_2 \rangle \subsetneq \langle a_1, a_2, a_3 \rangle \subsetneq \dots$ does not satisfy ACC

Proof

If $\exists k$, s.t. $\langle a_1, \dots, a_k \rangle = \langle a_1, \dots, a_k, a_{k+1} \rangle$, then $a_{k+1} = \sum_{i=1}^{k} r_i a_i$

Hence, $f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{i+1} - n_i} f_i < \deg f_{k+1}$

However, $f_{k+1} - \sum_{i=1}^{k} r_i x^{n_{i+1} - n_i} f_i \in I \setminus \langle f_1, \dots, f_k \rangle$ $\nrightarrow$

(compare degrees)

QUESTION

Given $f \in F[x_1, \dots, x_n]$, $I \subseteq F[x_1, \dots, x_n]$, how to check if $f \in I$?

- Let $I = \langle f_1, \dots, f_s \rangle$. If $f = \sum_{i=1}^{s} h_i f_i + r$ with remainder r, then $r = 0 \Leftrightarrow r = I$

EXAMPLE 1

$f_1 = xy + 1$, $f_2 = y^2 - 1$, $I = \langle f_1, f_2 \rangle$, $f = xy^2 - x = x f_2 \in I$, but $f = y f_1 - (x + y)$

Shun / 郑羽海 (@shun4midx)

DIVISION ALGORITHM IN $F[x_1, \dots, x_n]$

EXAMPLE 2

Say $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$

1. Choose a lexicographical ordering: $x > y$
2. The multidegree: $\partial(f) = (2,1)$, $\partial(f_1) = (1,1)$, $\partial(f_2) = (0,2)$
3. The leading term: $LT(f) = x^2y$, $LT(f_1) = xy$, $LT(f_2) = y^2$
4. $LT(f) = x\,LT(f_1)$: $f = xf_1 + x^2y + y^2 + x = xf_1 + yf_1 + y^2 + x + y = xf_1 + yf_1 + f_2 + (x + y + 1)$
   No term in $x^2 + x + 1$ is divisible by $LT(f_1), LT(f_2)$. $\Rightarrow$ Stop

However, this division is not unique. In fact, $f = xf_1 + (x+1)f_2 + (x+1)$

SUMMARY OF THE ALGORITHM

Fix a monomial ordering and $I = \langle f_1, \dots, f_m \rangle$

Then $\forall f \in F[x_1, \dots, x_n]$, $f = \underbrace{\sum_{i=1}^m h_i f_i}_{f_I} + \underbrace{r}_{\bar{f}^G,\ G = \{f_1, \dots, f_m\}}$, where $h_i, r \in F[x_1, \dots, x_n]$ $\forall i$ and either $r = 0$ or no term of r is divisible by any $LT(f_1), \dots, LT(f_m)$ (Denote by NTOR)

GRÖBNER BASIS

DEFINITION

Fix a monomial ordering (Denote by FAMO) and let $I \subseteq F[x_1, \dots, x_n]$. We say $LT(I) = \langle LT(f) \mid f \in I \rangle$

REMARK

Let $I = \langle f_1, \dots, f_m \rangle$. In general, $\langle LT(f_1), \dots, LT(f_m) \rangle \subsetneq LT(I)$

For example, $f_1 = xy^2 + y$, $f_2 = x^2y$. $xf_1 - yf_2 = xy \in \langle f_1, f_2 \rangle$ but $xy \notin \langle xy^2, x^2y \rangle$.

DEFINITION

$\{g_1, \dots, g_m\}$ is called a Gröbner basis for I if $\langle g_1, \dots, g_m \rangle = I$ and $\langle LT(g_1), \dots, LT(g_m) \rangle = LT(I)$

PROPOSITION 1

$LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle \Rightarrow I = \langle g_1, \dots, g_m \rangle$

Proof

$\forall f \in I$, $f = \sum_{i=1}^m h_i f_i + r$, either $r = 0$ or NTOR.

Assume that $r \neq 0$. Since $r = f - f_I \in I$, thus $LT(r) \in LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle$

Then, $LT(r) = \tilde{h}_1 LT(g_1) + \dots + \tilde{h}_m LT(g_m)$, so not NTOR. ~~$\times$~~

$\therefore r = 0$, i.e. $f \in \langle g_1, \dots, g_m \rangle$ $\square$

PROPOSITION 2

Each ideal I has a Gröbner basis

Proof

By Hilbert basis theorem, $LT(I)$ is finitely generated, say $LT(I) = \langle f_1, \dots, f_m \rangle$

Write $f_i = \sum_{j=1}^{m_i} h_{ij} LT(g_{ij})$ with $g_{ij} \in I$ and $h_{ij} \in F[x_1, \dots, x_n] \Rightarrow LT(I) = \langle LT(g_{ij}) \mid \substack{i=1,\dots,m \\ j=1,\dots,m_i} \rangle$

$\therefore \{g_{11}, \dots, g_{mm_i}\}$ is a Gröbner basis of I. $\square$

Shun / 舜海 (@shun4midx)

PROPOSITION 3

Assume that $\{g_1, \dots, g_m\}$ is a Gröbner basis of I.

- $\forall f \in F[x_1, \dots, x_n]$, $\exists! f_I \in I, r$ s.t. $f = f_I + r$, $r = 0$ or NTOR
- $f \in I \Leftrightarrow r = 0$

Proof

- By division algorithm, $f = f_I + r$.
  Now, if $f_I + r = f_I' + r'$, then $r - r' = f_I' - f_I \in I$
  Also, if $r - r' \neq 0$, then $LT(r - r') \in LT(I) = \langle LT(g_1), \dots, LT(g_m) \rangle$ ~~—x—~~
  $\therefore r - r' = 0 \Rightarrow f_I = f_I'$ ✓
- If $f \in I$, then $f = f_I + r \Rightarrow r = f - f_I \in I \Rightarrow r = 0$ □

HOW DO WE CONSTRUCT A GRÖBNER BASIS?

DEFINITION

Let $f, g \in F[x_1, \dots, x_m]$ and M be the monic least common multiple of $LT(f)$ and $LT(g)$. Then, $S(f,g) = \frac{M}{LT(f)} f - \frac{M}{LT(g)} g$ is called an S-polynomial of f, g.

BUCHBURGER'S ALGORITHM

Let $I = \langle g_1, \dots, g_m \rangle$ and $G = \{g_1, \dots, g_m\}$
A Gröbner basis can be constructed by the algorithm:
↳ $G_0 := G$
↳ $G_{i+1} := G_i \cup (\{\overline{S(f,g)}^{G_i} \mid f, g \in G_i\} \setminus \{0\})$

If $G_i = G_{i+1}$, then G_i is a Gröbner basis

EXAMPLE 4

Let $x > y$ and $I = \langle f_1 = x^3y - xy^2 + 1, f_2 = x^2y^2 - y^3 - 1 \rangle$, $G_0 = \{f_1, f_2\}$, $S(f_1, f_2) = x + y =: f_3$, $G_1 = \{f_1, f_2, f_3\}$

$\overline{S(f_1, f_3)}^{G_1} = 0$, $\overline{S(f_2, f_3)}^{G_1} = y^4 - y^3 - 1 = f_4 \Rightarrow G_2 = \{f_1, f_2, f_3, f_4\}$

$\overline{S(f_1, f_4)}^{G_2} = \overline{S(f_2, f_4)}^{G_2} = \overline{S(f_3, f_4)}^{G_2} = 0$
$\therefore G_2$ is a Gröbner basis

KEY LEMMA

Let $f_1, \dots, f_m \in F[x_1, \dots, x_n]$ and $a_1, \dots, a_m \in F$, s.t. $\partial(f_1) = \partial(f_2) = \dots = \partial(f_m) = \alpha$ and $\partial(\sum_{i=1}^m a_i f_i) < \alpha$. Then, $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$

Proof

Write $f_i := c_i f_i'$ with $c_i \in F$ and f_i' be monic with multidegree α. (Note: $S(f_1, f_2) = \frac{1}{c_1} f_1 - \frac{1}{c_2} f_2 = f_1' - f_2'$)
Then, $h = \sum_{i=1}^m a_i c_i f_i' = a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \dots + (a_1 c_1 + \dots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') + \underbrace{(a_1 c_1 + \dots + a_m c_m)}_{0 \ (\because \text{degree})} f_m'$ □

BUCHBURGER'S CRITERION

Assume that $I = \langle g_1, \dots, g_m \rangle$
Then, $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of $I \Leftrightarrow \overline{S(g_i, g_j)}^{G} = 0 \ \forall i, j$ ($\because S(g_i, g_j) \equiv 0 \pmod G$)

Proof

"$\Rightarrow$": Since $S(g_i, g_j) \in I$, by prop 3, $\overline{S(g_i, g_j)}^{G} = 0$
"$\Leftarrow$": For $f \in I$, write $f = \sum_{i=1}^m h_i g_i$. Define $\alpha = \max\{\partial(h_1 g_1), \dots, \partial(h_m g_m)\}$
We have $\partial(f) \leq \alpha$, so we can select an expression $f = \sum_{i=1}^m h_i g_i$ for f s.t. α is minimal
Claim: $\partial(f) = \alpha$ ($\Rightarrow LT(f) = \sum_{\partial(h_i g_i) = \alpha} LT(h_i) LT(g_i) \Rightarrow LT(f) \in \langle LT(g_1), \dots, LT(g_m) \rangle$)
Proof
Assume that $\partial(f) < \alpha$

Rewrite $f=\sum_{i=1}^{m} h_i g_i = \sum_{\partial(h_i g_i)=\alpha} LT(h_i) g_i + \sum_{\partial(h_i g_i)<\alpha} (h_i - LT(h_i)) g_i + \sum_{\partial(h_i g_i)<\alpha} h_i g_i$

Shun / 翔海 (@shun4midx)

Let $LT(h_i) = a_i h_i^\circ$ with h_i° being a monic monomial.
Comparing the multidegree on both sides, we get $\partial(\sum_{\partial(h_i g_i)=\alpha} a_i h_i^\circ g_i) < \alpha$

By key lemma, $\sum_{\partial(h_i g_i)=\alpha} a_i h_i^\circ g_i = c_{12} S(h_{i_1}^\circ g_{i_1}, h_{i_2}^\circ g_{i_2}) + c_{23} S(h_{i_2}^\circ g_{i_2}, h_{i_3}^\circ g_{i_3}) + \underbrace{\cdots}_{\text{finite}}$, where $\partial(h_{i_1} g_{i_1}) = \partial(h_{i_2} g_{i_2}) = \underbrace{\cdots}_{\text{finite}} = \alpha$

By def, if we set $M_{st} = x^{\beta_{st}}$ = the monic lcm of $LT(g_{i_s}), LT(g_{i_t})$ where the multidegree is β_{st}
Then, $S(h_{i_s}^\circ g_{i_s}, h_{i_t}^\circ g_{i_t}) = \frac{x^\alpha}{LT(h_{i_s}^\circ g_{i_s})} h_{i_s}^\circ g_{i_s} - \frac{x^\alpha}{LT(h_{i_t}^\circ g_{i_t})} h_{i_t}^\circ g_{i_t}$
$= x^{\alpha-\beta_{st}} \left(\frac{x^{\beta_{st}}}{h_{i_s}^\circ LT(h_{i_s}^\circ g_{i_s})} h_{i_s}^\circ g_{i_s} - \frac{x^{\beta_{st}}}{h_{i_t}^\circ LT(h_{i_t}^\circ g_{i_t})} h_{i_t}^\circ g_{i_t} \right)$
$= x^{\alpha-\beta_{st}} S(g_{i_s}, g_{i_t})$

Do division on $g_1, \ldots, g_m k$, since $\overline{S(g_{i_s}, g_{i_{s+1}})}^G = 0$

By assumption, $\forall$ fixed s, $S(g_{i_s}, g_{i_{s+1}}) = \sum_{j=1}^{m} l_j g_j$ with $\partial(l_j g_j) < \beta_{s(s+1)}$, i.e. $\partial(S(g_{i_s}, g_{i_{s+1}})) < \beta_{s(s+1)}$
$\therefore$ We found $\partial(x^{\alpha-\beta_{s(s+1)}} l_j g_j) < \alpha$ $\forall j$, which contradicts the minimality of α ~~$\times$~~ $\square$

3-19-24 (WEEK 5)

Shun / 羊羽海 (@shun4midx)

GRÖBNER BASIS (II)

THEOREM 1

The Buchburger's algorithm will terminate

Proof

- $\langle LT(G_i)\rangle \subsetneq \langle LT(G_{i+1})\rangle$ if $G_i \neq G_{i+1}$:
  $G_i \neq G_{i+1} \Rightarrow \exists f, g \in G_i$, s.t. $\overline{S(f,g)}^{G_i} \neq 0 \Rightarrow LT(\overline{S(f,g)}^{G_i}) \notin \langle LT(G_i)\rangle$ ($\in \langle LT(G_{i+1})\rangle$)
- If this algorithm doesn't terminate, then $\exists\ \langle LT(G_0)\rangle \subsetneq \langle LT(G_1)\rangle \subsetneq \dots$
  This contradicts the Noetherian property of $F[x_1, \dots, x_n]$ ~~→~~

DEFINITION

A Gröbner basis $G = \{g_1, \dots, g_m\}$ of I is said to be **minimal** if each $LT(g_i)$ is monic $\forall i$, and $\forall j$, $LT(g_j) \notin \langle LT(G \setminus \{g_j\})\rangle$

(If $LT(g_j) \in \langle LT(G\setminus\{g_j\})\rangle$, then $\langle LT(G\setminus\{g_j\})\rangle = \langle LT(G)\rangle = LT(I)$, i.e. $G\setminus\{g_j\}$ is still a Gröbner basis of I)

DEFINITION

A minimal Gröbner basis $\{g_1, \dots, g_m\}$ is said to be **reduced** if $\forall j$, no term in g_j is divisible by any $LT(g_1), \dots, \widehat{LT(g_j)}, \dots, LT(g_m)$

In this case, g_j is said to be reduced for G

THEOREM 2

For a given monomial ordering, every non-zero ideal I in $F[x_1, \dots, x_n]$ has a unique reduced Gröbner basis

$\Rightarrow$ Corollary: $I, J \subseteq F[x_1, \dots, x_n]$, $I = J \Leftrightarrow I$ and J have the same reduced Gröbner basis)

Proof

Existence: Let G be a minimal Gröbner basis of I.

For $g \in G$, let $g' = \overline{g}^{G\setminus\{g\}}$ and set $G' = (G\setminus\{g\}) \cup \{g'\}$

Claim: G' is still a Gröbner basis of I

Proof

Observe that when we divide g by $G\setminus\{g\}$, $LT(g)$ goes to the remainder since $LT(g) \notin \langle LT(G\setminus\{g\})\rangle$

This implies that $LT(g') = LT(g) \Rightarrow \langle LT(G')\rangle = \langle LT(G)\rangle = LT(I)$ and G' is still a minimal Gröbner basis

Now, take other elements of G and apply the same process until they are all reduced

Uniqueness: Let G and $\tilde{G}$ be two reduced Gröbner bases of I. In particular, G and $\tilde{G}$ are minimal

Claim: $LT(G) = LT(\tilde{G})$ and thus G and $\tilde{G}$ have the same number of elements

Proof

$\forall LT(g) \in LT(G) \subseteq LT(I) = \langle LT(\tilde{G})\rangle$, say $LT(g) = \sum_{\tilde{g}\in\tilde{G}} h_{\tilde{g}} LT(\tilde{g}) \Rightarrow LT(\tilde{g}) \mid LT(g)$ for some $\tilde{g} \in \tilde{G}$

Similarly, $\exists g' \in G$, s.t. $LT(g') \mid LT(\tilde{g}) \Rightarrow LT(g') \mid LT(g) \Rightarrow LT(g') = LT(g) \Rightarrow LT(g) = LT(\tilde{g})$ since G is minimal.

We conclude that $\forall g \in G$, $\exists \tilde{g} \in \tilde{G}$ s.t. $LT(g) = LT(\tilde{g})$. By symmetry, $\forall \tilde{g} \in \tilde{G}$, $\exists g \in G$, s.t. $LT(\tilde{g}) = LT(g)$ □

For $g \in G$, let $\tilde{g} \in \tilde{G}$, s.t. $LT(g) = LT(\tilde{g})$. $\because g - \tilde{g} \in I \ \therefore \overline{g-\tilde{g}}^{G} = 0$

But $LT(g), LT(\tilde{g})$ cancel in $g - \tilde{g}$ and the remaining terms are divisible by none of $LT(G) = LT(\tilde{G})$ since $G, \tilde{G}$ are reduced.

This shows that $\overline{g-\tilde{g}}^{G} = g - \tilde{g} = 0 \Rightarrow g = \tilde{g}$ □

Shun/翔海 (@shun4midx)

EXAMPLE 1

Let $I=\langle f_1=x^2+xy^5+y^4,\ f_2=xy^6-xy^3+y^5-y^2,\ f_3=xy^5-xy^2\rangle$, $x>y$

$\overline{S(f_1,f_2)}^{G_0}=0$

$\overline{S(f_1,f_3)}^{G_0}=0$

$\overline{S(f_2,f_3)}^{G_0}=y^5-y^2=f_4$

$G_1=\{f_1,f_2,f_3,f_4\}$

$\overline{S(f_3,f_4)}^{G_1}=0,\ \overline{S(f_2,f_4)}^{G_1}=0,\ \overline{S(f_1,f_4)}^{G_1}=0$

$\Rightarrow G=\{x^2+xy^5+y^4,\ xy^6-xy^3+y^5-y^2,\ xy^5-xy^2,\ y^5-y^2\}$

$\Rightarrow$ Reduced $=\{x^2+xy^5+y^4,\ y^5-y^2\}$

APPLICATIONS

QUESTIONS

Suppose $S=\{f_1,\dots,f_m\}\subseteq F[x_1,\dots,x_n]$. Let $Z(S)=\{(a_1,\dots,a_n)\mid f_i(a_1,\dots,a_n)=0\ \forall i=1,\dots,m\}$ be the zero locus of S. How do we find $Z(S)$? How do we solve $\{f_1=0,\dots,$ and $f_m=0\}$?

FACT

Let $I=\langle S\rangle$. Then, $Z(I)=Z(S)$

Proof

$\because S\subseteq I\ \therefore$ of course $Z(I)\subseteq Z(S)$ ✓

Conversely, $\forall f\in I$, write $f=\sum_{i=1}^m h_i g_i$, $g_i\in S$, $h_j\in F[x_1,\dots,x_n]$

For any $(a_1,\dots,a_n)\in Z(S)$, $g_i(a_1,\dots,a_n)=0\ \forall i\Rightarrow f(a_1,\dots,a_n)=0$. □

DEFINITION

Let I be an ideal of $F[x_1,\dots,x_n]$.

$I_i:=I\cap F[x_{i+1},\dots,x_n]$ is called the i^{th} elimination ideal of I w.r.t. $x_1>x_2>\dots>x_n$.

in $F[x_{i+1},\dots,x_n]$

ELIMINATION THEOREM

Let $G=\{g_1,\dots,g_m\}$ be a Gröbner basis for $I\neq 0$ w.r.t. $x_1>x_2>\dots$

Then, $G_i=G\cap F[x_{i+1},\dots,x_n]$ is a Gröbner basis of I_i in $F[x_{i+1},\dots,x_n]$

In particular, $I_i=\{0\}\Leftrightarrow G\cap F[x_{i+1},\dots,x_n]=\emptyset$

Proof

By def, $\langle LT(G_i)\rangle\subseteq LT(I_i)$

Conversely, let $f\in I_i\subseteq I$, write $F[x_{i+1},\dots,x_n]\ni LT(f)=\sum_{i=1}^m h_i LT(g_i)=\sum a_{kj}X^{\alpha_{kj}}LT(g_k)-LT(f)$

(a_{kj} is a multiset)

So, $a_{kj}\neq 0\Rightarrow LT(g_k)\in F[x_{i+1},\dots,x_n]\Rightarrow g_k\in F[x_{i+1},\dots,x_n]$ since $x_1>x_2>\dots>x_n>x_{n+1}$

$\Rightarrow g_k\in G_i$

Hence, $LT(f)\in\langle LT(G_i)\rangle$

In conclusion, $G=G_0\cup G_1\cup\dots\cup G_{n-1}$

Shun/翔海 (@shun4midx)

THEOREM 3

Let I, J be ideals of $F[x_1, \dots, x_n]$. Then,

(1) $tI + (1-t)J$ is an ideal of $F[t, x_1, \dots, x_n]$
(└ $F[t, x_1, \dots, x_n]I$)

(2) $I \cap J = (tI + (1-t)J) \cap F[x_1, \dots, x_n]$ which is the first elimination ideal of $tI + (1-t)J$ w.r.t. $t > x_1 > x_2 > \cdots$ (Notice that t is first)

Proof

(1) OK

(2) "$\subseteq$": For $f \in I \cap J$, $f = tf + (1-t)f \in RHS$ ✓ ($f \in I$, $f \in J$)

"$\supseteq$": For $f \in RHS$, say $f = t\tilde{f}_1 + (1-t)\tilde{f}_2$, $\tilde{f}_1 \in F[t, x_1, \dots, x_n]I$, $\tilde{f}_2 \in F[t, x_1, \dots, x_n]J$, say: $\tilde{f}_1 = \sum (h_i t + r_i) f_i$ and $\tilde{f}_2 = \sum (h_j' t + r_j') f_j'$

($f_i \in F[x_2, \dots, x_n] \subseteq F[t, x_1, \dots, x_n]$, $f_i \in I$; $f_j' \in J$)

Note: f has no variable t

Take $t = 0$, $f = \sum r_j' f_j' \in J$

$t = 1$, $f = \sum (h_i(1, x_1, \dots, x_n) + r_i) f_i \in I$

$\therefore f \in I \cap J$ ✓

EXAMPLE 2

$I = \langle y^2, x - yz \rangle$, $J = \langle x, z \rangle$

$tI + (1-t)J = \langle \underbrace{ty^2}_{f_1}, \underbrace{tx - ty z}_{f_2}, \underbrace{x - tx}_{-f_3}, \underbrace{z - tz}_{-f_4} \rangle$ ∵ we need "monic"

$G_0 = \{f_1, f_2, f_3, f_4\}$

$\overline{S(f_1, f_2)}^{G_0} = 0$

$\overline{S(f_1, f_3)}^{G_0} = xy^2 = f_5$

$\overline{S(f_1, f_4)}^{G_0} = y^2 z = f_7$

$\overline{S(f_2, f_3)}^{G_0} = x - yz = f_6$

$G_1 = \{f_1, \dots, f_7\}$

$\Rightarrow \overline{S(f_i, f_j)}^{G_1} = 0 \ \forall i, j$

$\therefore I \cap J = \langle xy^2, y^2 z, x - yz \rangle$

3-21-25 (WEEK 5)

Shun/翔海 (@shun4midx)

NOETHERIAN AND ARTINIAN

DEFINITION

Say $M \in {}_R\mathcal{M}$.

- M is Noetherian if it satisfies ACC on submodules
- M is Artinian if it satisfies DCC on submodules

FACTS

1. TFAE: (a) M is Noetherian
   (b) Each submodule of M is finitely generated
   (c) Any nonempty collection of submodules of M has a max member
2. M is Artinian $\Leftrightarrow$ Any nonempty collection of submodules of M has a min member

Note: If R is not commutative, we would say it's left-Noetherian/left-Artinian instead
For simplicity, assume R is commutative, then R is a Noetherian/Artinian ring and M is a Noetherian/Artinian R-module.

QUESTION

How do we define a reasonable notation for the size of a module?

DEFINITION

A chain $M = C_0 \supseteq C_1 \supseteq C_{r-1} \supseteq C_r = 0$ is called a composition series if each factor C_{i-1}/C_i is simple, i.e. $\neq 0$ and has no submodule other than 0 and itself.

Here, r is called the composition length

MAIN THEOREM

If M has a composition series, then all its composition series have the same length, denoted by $\ell(M)$ ($\ell(M) := \infty$ if M has no composition series)

Strategy
Apply Schrier refinement thm and Jordan-Hölder thm

SCHRIER REFINEMENT THEOREM

For any two chains in M, $M = C_0 \supseteq C_1 \supseteq \dots \supseteq C_r = 0$ as chain C and $M = D_0 \supseteq D_1 \supseteq \dots D_s = 0$ as chain D, they have isomorphic refinements $\tilde{C} \cong \tilde{D}$ ($\leftarrow \tilde{r} = \tilde{s}$, $\tilde{C}_{i-1}/\tilde{C}_i \cong \tilde{D}_{i'-1}/\tilde{D}_{i'}$, $i \mapsto i'$ is a permutation of $\{1, \dots, \tilde{r}\}$)

JORDAN-HÖLDER THEOREM

Any two composition series C and D are isomorphic

Proof
If we have Schrier refinement thm, then $C \to \tilde{C}$, $D \to \tilde{D} \Rightarrow \because \tilde{C} \cong \tilde{D} \therefore C \cong D$ □

PROOF OF SCHRIER REFINEMENT THEOREM

Define $C_{ij} = (C_{i-1} \cap D_j) + C_i$ for $i = 1, \dots, r$, $j = 0, \dots, s$
$D_{ji} = (D_{j-1} \cap C_i) + D_j$ for $i = 0, \dots, r$, $j = 1, \dots, s$
$\therefore$ We construct $M = C_0 = C_{10} \supseteq C_{11} \supseteq C_{12} \supseteq \dots \supseteq C_{1s} = C_1 = C_{20} \supseteq C_{21} \supseteq \dots \supseteq C_{rs} = 0$
and also $M = D_0 = D_{10} \supseteq D_{11} \supseteq D_{12} \supseteq \dots \supseteq D_{1r} = D_1 = D_{20} \supseteq D_{21} \supseteq \dots \supseteq D_{rs} = 0$
Assuming none of the elements overlap, then we have both chains of length rs
Notice, (Butterfly lemma)

$$C_{i,j-1}/C_{ij} = \frac{(C_{i-1} \cap D_{j-1}) + C_i}{(C_{i-1} \cap D_j) + C_i} \cong \frac{C_{i-1} \cap D_{j-1}}{C_i \cap D_{j-1} + C_{i-1} \cap D_j} \cong \frac{(D_{j-1} \cap C_{i-1}) + D_j}{(D_{j-1} \cap C_i) + D_j} \cong D_{j,i-1}/D_{ji}$$

If $C_{i,j-1}=C_{ij}$, then we get $D_{j,i-1}/D_{ji} \cong C_{i,j-1}/C_{ij}=0 \Rightarrow D_{j,i-1}=D_{ji}$, so ommit $C_{i,j-1}$ and $D_{j,i-1}$, which means our length is still preserved and equal. □

THEOREM

TFAE

(a) M has a composition series

(b) M is both Noetherian and Artinian

Proof

(a) $\Rightarrow$ (b): Suppose $\ell(M)=n$ and $M=D_0 \supsetneq D_1 \supsetneq \dots \supsetneq D_n=0$ as a composition series

Assume M is not Noetherian, i.e. $\exists\, 0=N_1 \subsetneq N_2 \subsetneq \dots \subsetneq N_n \subsetneq \dots$

Define a chain C: $M=C_0 \supsetneq C_1=N_n \supsetneq \dots \supsetneq C_n=N_1=0$

$\therefore$ By Schrier's thm, $\exists\, \tilde{C} \equiv \tilde{0}=D \Rightarrow \tilde{C}$ is a composition series ⟶⟵

(b) $\Rightarrow$ (a): $\because M$ is Noetherian

$\therefore \exists$ a max submodule C_1 of $M \Rightarrow \exists$ a max submodule C_2 of $C_1 \Rightarrow \dots$

In other words, $M=C_0 \supsetneq C_1 \supsetneq C_2 \supsetneq \dots$

$\because M$ is Artinian

$\therefore \exists\, n$, s.t. $C_n=0$

$\therefore$ We have constructed M as a composition series (of finite length). □

EXAMPLE OF WHY NOT ALL RINGS ARE ARTINIAN

$\ell(\mathbb{Z})=\infty$

- $\mathbb{Z}$ is Noetherian since it is a PID
- However, $\mathbb{Z}$ is not Artinian! Consider the following infinitely long DCC: $\langle 2\rangle \supsetneq \langle 2^2\rangle \supsetneq \langle 2^3\rangle \supsetneq \dots$

EXAMPLE OF AN ARTINIAN RING

Say $m=p_1 \cdots p_r$

Claim: $\mathbb{Z}/\langle m\rangle \supsetneq \langle p_1\rangle/\langle m\rangle \supsetneq \langle p_1p_2\rangle/\langle m\rangle \supsetneq \dots \supsetneq \langle p_1p_2\cdots p_r\rangle/\langle m\rangle = 0$ is a composition series

Proof

Notice, $\mathbb{Z}/\langle m\rangle / \langle p_1\rangle/\langle m\rangle \cong \mathbb{Z}/\langle p_1\rangle$ is a field and is hence simple

Then, $\langle p_1\rangle/\langle m\rangle / \langle p_1p_2\rangle/\langle m\rangle \cong \langle p_1\rangle/\langle p_1p_2\rangle$ is simple since $\langle p_1\rangle \supseteq I \supseteq \langle p_1p_2\rangle$

$\therefore \ell(\mathbb{Z}/\langle m\rangle)=r$

ARTINIAN RING

PROPOSITION

If R is Artinian, then $\#\operatorname{Max} R<\infty$

Proof

Define $S:=\{\bigcap_{\text{finite}} m \mid m\in \operatorname{Max} R\} \neq \emptyset \Rightarrow \exists$ a minimal member (has a "stopping condition" for DCC), say $m_1\cap\dots\cap m_k$ (both are max ideals)

Now, for $m\in \operatorname{Max} R$, $m\cap(m_1\cap\dots\cap m_k)=m_1\cap\dots\cap m_k \Rightarrow m\supseteq m_1\cap\dots\cap m_k \Rightarrow m\supseteq m_l$ for some $l \Rightarrow m=m_l$

(Otherwise, $\exists\, x_i\in m_i\setminus m$, $x_1\cdots x_k \in m_1\cap\dots\cap m_k \subseteq m$)

PROPOSITION 2

If R is Artinian and $\operatorname{Max} R=\{m_1,\dots,m_k\}$, then $\exists\, n_1,\dots,n_k\in\mathbb{N}$, s.t. $\{0\}=m_1^{n_1}\cdots m_k^{n_k}=\bigcap_{i=1}^{k} m_i^{n_i}$

($\sqrt{m_i^{n_i}+m_j^{n_j}}=\sqrt{m_i^{n_i}}+\sqrt{m_j^{n_j}}=\sqrt{m_i+m_j}=\sqrt{R}=R$)

Proof

Since R is Artinian, it satisfies DCC, so $\exists\, n_i\in\mathbb{N}$, s.t. $m_i^{n_i}=m_i^{n_i+1}$ (何でもこのdescending chainは終る事ができる)

If $m_1^{n_1}m_2^{n_2}\cdots m_k^{n_k}\neq 0$, then $S=\{J\subseteq R \mid Jm_1^{n_1}\cdots m_k^{n_k}\neq 0\}\neq\emptyset$ (RES ✓)

Let $0\neq J_0$ be a minimal member of S. Pick $0\neq x\in J_0$, s.t. $\langle x\rangle\in S \Rightarrow \langle x\rangle=J_0$, since $\langle x\rangle\subseteq J_0$

Shun / 翔海 (@shun4midx)

Observe that $xm_1^{n_1}\cdots m_k^{n_k} = (xm_1\cdots m_k)(m_1^{n_1}\cdots m_k^{n_k-1}) \neq 0$

$\Rightarrow xm_1\cdots m_k \in S \Rightarrow xm_1\cdots m_k = (m_1\cdots m_k)xR = \langle x\rangle = xR$. By Nakayama lemma, $xR=0 \Rightarrow x=0$ ↯

($xR\cdots R = xR = \langle x\rangle$)

PROPOSITION 3

If R is Artinian, then $R \cong R_1 \times \cdots \times R_k$, where R_i is an Artinian local ring (one maximal ideal)

Proof (critical race theory じゃなくて www, Chinese remainder theorem だよ)

By CRT, $R = R/\langle 0\rangle = R/m_1^{n_1}\cdots m_k^{n_k} = R/m_1^{n_1}\cap\cdots\cap m_k^{n_k} \cong R/m_1^{n_1}\times\cdots\times R/m_k^{n_k}$

Write $R_i = R/m_i^{n_i}$. If $\bar{m}\in \mathrm{Max}R_i$, say $\bar{m} = m/m_i^{n_i}$, then $m \supseteq m_i^{n_i} \Rightarrow m \supseteq m_i \Rightarrow m = m_i$.

That is, $\mathrm{Max}R_i = \{\bar{m}_i\}$ □

PROPOSITION 4

In a ring R, if we can find max ideals $m_1,\ldots,m_n$ not necessarily different R, s.t. $m_1\cdots m_n = 0$, then R is Noetherian $\Leftrightarrow$ R is Artinian

Proof

Consider $R \supseteq m_1 \supseteq m_1m_2 \supseteq \cdots \supseteq m_1\cdots m_n = 0$

Let $M_i = m_1\cdots m_{i-1}/m_1\cdots m_i$, which is an R/m_i-module (a field) since $m_iM_i = 0$

Thus, M_i is Artinian $\Leftrightarrow$ M_i is Noetherian

Also, $0 \to m_1\cdots m_i \to m_1\cdots m_{i-1} \to M_i \to 0$

$m_0 = R$ is Artinian $\Leftrightarrow$ m_1, M_1 are Artinian $\Leftrightarrow$ m_1, m_2, M_1M_2 are Artinian $\Leftrightarrow \cdots\cdots \Leftrightarrow 0 = m_1\cdots m_n, M_1, \ldots, M_n$ are Artinian

(└ $0 \to m_1 \to R \to M_1 \to 0$)

$\Leftrightarrow 0 = m_1\cdots m_n, M_1, \ldots M_n$ are Noetherian $\Leftrightarrow \cdots \Leftrightarrow m_1, M_1$ are Noetherian $\Leftrightarrow m_0 = R$ is Noetherian

REMARK

R is Artinian $\Leftrightarrow$ R is Noetherian and $\mathrm{Max}R = \mathrm{Spec}R$ $\forall R$

Proof

"$\Rightarrow$": Proposition 2 + Proposition 4 + $\mathrm{Max}R = \mathrm{Spec}R$ in Artinian rings ✓

"$\Leftarrow$": $\langle 0\rangle = \bigcap_{i=1}^{k} q_i$ ← primary decomposition (来週の水曜日はこのノートを書くよ!)

Here, $\sqrt{q_i} = m_i$

Since m_i is finitely generated (∴ Noetherian), $\exists n_i$, s.t. $m_i^{n_i} \subseteq q_i$. Hence, $m_1^{n_1}\cap\cdots\cap m_k^{n_k} = m_1^{n_1}\cdots m_k^{n_k} \subseteq q_1\cap\cdots\cap q_k = 0$

$\therefore m_1^{n_1}\cdots m_k^{n_k} = 0$, so R is Artinian □

3-26-25 (WEEK 6)

Shun / 翔海 (@shun4midx)

PRIMARY DECOMPOSITION

For this section, let R be a commutative ring

DEFINITION

- An ideal I of R is **irreducible** if $I=q_1\cap q_2 \Rightarrow I=q_1$ or $I=q_2$ (i.e. int of proper ideals)
- We define the **quotient ideal** $(I:x)=\{r\in R \mid rx\in I\}$, which is also an ideal

PROPOSITION

In a Noetherian R, each irr ideal is **primary**

Proof

Let $xy\in I$, and $x\notin I$ (Hope for "$y\in I$")

Consider the ascending chain $(I:y)\subseteq(I:y^2)\subseteq(I:y^3)\subseteq\dots$

As R is Noeth, thus $\exists n$, s.t. $(I:y^n)=(I:y^{n+1})=\dots$

Claim: $(\langle y^n\rangle_R+I)\cap(\langle x\rangle+I)=I$ ($\Rightarrow \langle y^n\rangle+I=I\Rightarrow y^n\in I$)

Proof

Let $b=r_1y^n+\underbrace{a_1}_{\in I}=r_2x+\underbrace{a_2}_{\in I}\Rightarrow r_1y^{n+1}=r_2\underbrace{xy}_{\in I}+\underbrace{a_2}_{\in I}y-\underbrace{a_1}_{\in I}y\in I$

$\therefore r\in(I:y^{n+1})=(I:y^n)\Rightarrow r_1y^n\in I\Rightarrow b\in I$ □

PROPOSITION

In a Noeth ring R, each I is a finite intersection of irr ideals

Proof (Proof by contradiction)

If not, $\emptyset\neq S=\{I\subsetneq R \mid I$ is not a finite intersection of irr ideals$\}$

$\because R$ is Noeth

$\therefore \exists$ a max element $I_0\in S$

We find that I_0 must be **reducible**, say $I_0=I_1\cap I_2$ with $\underbrace{I_0\subsetneq I_1,\ I_0\subsetneq I_2}_{\text{intersection of proper ideals}}\Rightarrow I_1, I_2\notin S$

$\therefore I_1$ is a finite intersection of irr ideals, I_2 is a finite intersection of irr ideals

$\therefore$ So is I_0. ↯

SUMMARY

Prop 1 + Prop 2 $\Rightarrow \{R:\text{Noeth}_{I\subseteq R}$, $I=q_1\cap\dots\cap q_n$, q_i: primary (i.e. we have the existence of decomposition, how about uniqueness?)

UNIQUENESS THEOREM

FACT 1

If q_i is P-primary $\forall i=1,\dots,n$, then $q=\bigcap_{i=1}^n q_i$ is also P-primary

Proof

- $\sqrt{q}=\bigcap_{i=1}^n\sqrt{q_i}=P$
- $xy\in q$ and $x\notin q\Rightarrow xy\in q_i\ \forall i$ and $x\notin q_j$ for some $j\Rightarrow y^n\in q_j\Rightarrow y\in\sqrt{q_j}\subseteq\sqrt{q}$, i.e. $y^m\in q$ for some m. □

FACT 2

Let q be P-primary and $x\in R$

(1) If $x\in q$, then $(q:x)=R$

(2) If $x\notin q$, then $(q:x)$ is a P-primary ideal

(3) If $x\notin P$, then $(q:x)=q$ (Proof: $y\in(q:x)\Rightarrow xy\in q$, $x\notin P\Rightarrow xy\in q$, $x^n\notin q\ \forall n\Rightarrow y\in q$)

Shun / 舜海 (@shun4midx)

Proof

(1) $1 \cdot x \in q \Rightarrow 1 \in (q:x) \Rightarrow (q:x) = R$

(2) "$\sqrt{(q:x)} = P$": For $y \in (q:x)$, $xy \in q$ and $x \notin q \Rightarrow y^n \in q \Rightarrow y \in \sqrt{q} = p$, so $q \subseteq (q:x) \subseteq p \Rightarrow p = \sqrt{q} \subseteq \sqrt{(q:x)} \subseteq \sqrt{p} = p$ (sandwich)

$yz \in (q:x)$ and $y \notin (q:x) \Rightarrow xyz \in q$, $xy \notin q \Rightarrow z^n \in q \subseteq (q:x)$

DEFINITION

$I = q_1 \cap \dots \cap q_n$ is **minimal** if $\sqrt{q_1}, \dots, \sqrt{q_n}$ (radicals) are distinct, and $q_i \not\supseteq \bigcap_{j \neq i} q_j \ \forall i = 1, \dots, n$

UNIQUENESS THEOREM

Let $I = \bigcap_{i=1}^n q_i$ be a minimal primary decomposition

If $p_i = \sqrt{q_i}\ \forall i = 1, \dots, n$, then $\{p_i\} = \{\sqrt{(I:x)} \mid x \in R, \sqrt{(I:x)} \in \mathrm{Spec}(R)\}$ which is indep of the particular decomp of p_i

Proof

If $x \in R \setminus I$, $(I:x) = (\bigcap_{i=1}^n q_i : x) = \bigcap_{i=1}^n (q_i : x) \Rightarrow \sqrt{(I:x)} = \bigcap_{x \notin q_i} \sqrt{(q_i:x)} = \bigcap_{x \notin q_i} p_i$ (sandwich)

"RHS $\subseteq$ LHS": $\sqrt{(I:x)} \in \mathrm{Spec} R \Rightarrow p_j \supseteq \sqrt{(I:x)} \supseteq p_j$ for some j, i.e. $\sqrt{(I:x)} = p_j$

"LHS $\subseteq$ RHS": $\because q_i \not\supseteq \bigcap_{j \neq i} q_j \ \forall i = 1, \dots, n \ \therefore \exists x_i \in \bigcap_{j \neq i} q_j \setminus q$

$\Rightarrow p_i = \sqrt{(q_i : x_i)} = \bigcap_{j=1} \sqrt{(q_j : x_i)} = \sqrt{(I : x_i)}$ $\square$

$(q_j : x_i) = R$

OBSERVE

For any $I = q_1 \cap \dots \cap q_m$ in $F[x_1, \dots, x_n]$, $\sqrt{I} = P_1 \cap \dots \cap P_m$

Consider the zero-locus (roots) Z, $Z(I) = Z(\sqrt{I}) = Z(P_1) \cup \dots \cup Z(P_m)$ ↙ just "$fg = 0 \Rightarrow f = 0$ or $g = 0$" 之類的

Why: $q_1 \cap \dots \cap q_m \supseteq q_1 \cdots q_m \Rightarrow Z(q_1 \cap \dots \cap q_m) \subseteq Z(q_1 \cdots q_m) = Z(q_1) \cup \dots \cup Z(q_m)$

$Z(I) = Z(\sqrt{I})$ (!)

"$\supseteq$": $x \in Z(q_i) \Rightarrow f(x) = 0 \ \forall x \in q_i$, so $g(x) = 0 \ \forall x \in q_1 \cap \dots \cap q_m$ ✓

EXAMPLE

$I = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x, y \rangle^2$ (P_1 = $\langle x \rangle$, P_2^2 = $\langle x, y \rangle^2$) ← we call P_1, P_2 its **associated primes**

THEOREM (RADICALS)

Let $I = \langle f_1, \dots, f_s \rangle \subsetneq F[x_1, \dots, x_n]$. Then, $f \in \sqrt{I} \iff (f_1, \dots, f_s, 1 - tf) = F(x_1, \dots, x_n, t)$

Proof

"$\Rightarrow$": $f^m \in I \Rightarrow 1 = t^m f^m + (1 - t^m f^m) = t^m f^m + (1 - tf)(1 + tf + t^2 f^2 + \dots + t^{m-1} f^{m-1})$ ✓ (rewriting identity; $1 - t^m f^m \in I$)

"$\Leftarrow$": Let $1 = \sum_{i=1}^s h_i f_i + h(1 - tf)$ (★)

$h_i, h \in F[x_1, \dots, x_n, t]$

Consider the F-algebra homomorphism, $\varphi : F[x_1, \dots, x_n, t] \to F(x_1, \dots, x_n)$ ($(\cdot)$ denotes rational function, $[\cdot]$ is polynomial)

$x_i \mapsto x_i$

$t \mapsto \frac{1}{f}$

$1 \mapsto 1$, $\frac{1}{t} \mapsto f$, $f \mapsto f$, $1 - tf \mapsto 0$

Apply φ to (★), $1 = \varphi(1) = \sum_{i=1}^s \varphi(h_i)\varphi(f_i) + \varphi(h)(\varphi(1) - \varphi(t)\varphi(f))$

$= \sum_{i=1}^s \frac{p_i}{f^{\gamma_i}} f_i$, $p_i \in F[x_1, \dots, x_n]$

Let $\rho = \max\{\gamma_i\}$, then $f^\rho \in I$ $\square$ (fraction addition denominator LCM)

EXAMPLE 2

$I = \langle xy^2 + 2y^2, x^2 - 2x + 1 \rangle$, $f = y - x^2 + 1$, $f \notin \sqrt{I}$

$J = \langle xy^2 + 2y^2, x^2 - 2x + 1, 1 - t(y - x^2 + 1) \rangle$ has the reduced Gröbner basis $\{1\} \Rightarrow f \in \sqrt{I}$

Alternate method:

I has Gröbner basis $G = \{x^4 - 2x^2 + 1, y^2\}$. $\overline{(y - x^2 + 1)^2}^G = -2x^2 y + 2y$, $\overline{(y - x^2 + 1)^3}^G = 0$, so OK.

Basically... We need Gröbner basis no matter what. We can use the J shortcut, but if we need to find t's power, we still need brute force.

EXAMPLE 3

Shun / 翔海 (@shun4midx)

$I=(xz-y^2, x^3-yz)$ ... What are its associated primes?

For $I \subseteq F[x,y,z]$, we have:

- $(I:x)$: $I \cap \langle x \rangle \Rightarrow tI+(1-t)\langle x \rangle$ has the reduced Gröbner basis G and $G \cap F[x,y,z] = \{\underbrace{x^2z-xy^2}_{f_1}, \underbrace{x^4-xyz}_{f_2}, \underbrace{x^3y-xz^2}_{f_3}\}$

  $\therefore I \cap \langle x \rangle = (f_1, f_2, f_3)$

  Then, $(I:x) = (\frac{f_1}{x}, \frac{f_2}{x}, \frac{f_3}{x}) = \langle xz-y^2, x^3-yz, x^2y-z^2 \rangle$ (ofc just divide by x)

  Is $(I:x)$ an associated prime?

  Now, notice $(I:x)$ has the reduced Gröbner basis $G = \{x^3-yz, x^2y-z^2, xy^3-z^3, xz-y^2, y^5-z^4\}$ (Notice with parametrization, $x=t^3$, $y=t^4$, $z=t^5$ makes this 0 xd)

  Define $\varphi: F[x,y,z] \longrightarrow F[t]$

  $$\begin{aligned} x &\longmapsto t^3 \\ y &\longmapsto t^4 \\ z &\longmapsto t^5 \end{aligned}$$

  Now, $\ker\varphi = (G) = \langle (I:x) \rangle \Rightarrow F[x,y,z]/\langle (I:x) \rangle \hookrightarrow F[t]$, which is an integral domain

  $\therefore$ $(I:x)$ is a prime ideal. □

Remark: Even though this is still seemingly Algebra-heavy, this is quite a geometrical approach at the problem xddd (Please don't get mad at me qwq~ I suck lol it's just some cool angle of interpretation imo, idrk Algebraic Geometry ._.)

3-28-25 (WEEK 6)

Shun/翔海 (@shun4midx)

NAKAYAMA'S LEMMA AND ARTIN-REES LEMMA

Here, R is commutative and $M \in_R m$.

DEFINITION

The Jacobson radical of R is $J_R := \bigcap_{m \in \mathrm{Max}R} m$ (nilradical was intersection of prime ideals)

PROPERTIES

(1) $I \subsetneq R \Rightarrow (I, J_R) \subsetneq R$: $I \subsetneq R \Rightarrow \exists m \in \mathrm{Max}R$ s.t. $I \subseteq m$, $J_R \subseteq m \Rightarrow \langle I, J_R \rangle \subseteq m \subsetneq R$

(2) $n_R \subseteq J_R$

(3) $x \in J_R \Leftrightarrow 1-rx \in R^\times$ $\forall r \in R$: "$\Rightarrow$": $1-rx \notin R^\times \Rightarrow \langle 1-rx \rangle \subsetneq m \Rightarrow 1-rx \overset{\in m}{\in} m \Rightarrow 1 \in m$ $\lightning$ $\therefore 1-rx \in R^\times$ ✓

"$\Leftarrow$": If $x \notin m$ for a $m \in \mathrm{Max}R$, then $\langle x \rangle + m = R$, say $1 = rx + z \overset{\in m}{\Rightarrow} m \ni z = 1-rx \in R^\times \Rightarrow m = R$ $\lightning$ $\therefore x \in J_R$.

NAKAYAMA LEMMA

If M is finitely generated and $I \subseteq J_R$ s.t. $IM = M$, then $M = 0$

Proof

Assume that $M \neq 0$. Let n be the smallest integer, s.t. M is generated by n elements, say $x_1, \cdots, x_n$

$\because IM = M \ni x_n$

$\therefore x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_nx_n$ with $a_i \in I$.

$\Rightarrow \underbrace{(1-a_n)}_{\in R^\times \because a_n \in I \subseteq J_R} x_n = a_1x_1 + \cdots + a_{n-1}x_{n-1}$ $\therefore M = \langle x_1, \cdots, x_{n-1} \rangle$ $\lightning$ □

COROLLARY 1

For a finitely generated M, $N \subseteq M$, $I \subseteq J_R$, then $I+MN \Rightarrow M = N$

Proof

M is finitely generated $\Rightarrow M/N$ is finitely generated

We know $I(M/N) = \frac{IM+N}{N} = \frac{M}{N} \Rightarrow$ By Nakayama lemma, $M/N = 0 \Rightarrow M = N$ □

COROLLARY 2

For a local (R, m), finitely generated M, if $M/mM = \langle \bar{x}_1, \cdots, \bar{x}_m \rangle_{R/m}$ with $\dim_{R/m} M/mM = n$, then $M = \langle x_1, \cdots, x_n \rangle_R$

(local: only has 1 max)

Proof

Let $N = \langle x_1, \cdots, x_n \rangle_R$. Then, $\frac{N+mM}{mN} = \langle \bar{x}_1, \cdots, \bar{x}_n \rangle = M/mM \Rightarrow N + mM = M \Rightarrow N = M$ □

COROLLARY 3

For a local (R, m), finitely generated M, N, $f: M \to N$ in ${}_RM$, $\bar{f}: M/mM \to N/mN$ is a linear transformation

Proof

(1) "$\bar{f}$ is onto $\Rightarrow f$ is onto": $\mathrm{Im}(f) = \frac{f(M)+mN}{mN} = N/mN \Rightarrow f(M) + mN = N \Rightarrow f(M) = N$

(2) Assume M, N are free, then $\bar{f}$ is 1-1 $\Rightarrow f$ is 1-1:

$M = (x_1, \cdots, x_\ell) \cong R^\ell$ (free $\Rightarrow$ no relation)

$\Updownarrow$ ↘ free basis

$M/mM = \langle \bar{x}_1, \cdots, \bar{x}_\ell \rangle \cong (R/m)^\ell$

↘ basis

Similarly, $N = (y_1, \cdots, y_k) \cong R^k \Leftrightarrow N/mN = \langle \bar{y}_1, \cdots, \bar{y}_k \rangle$

Since $\bar{f}$ is 1-1, $\dim \mathrm{Im}\bar{f} = \ell$, say $\langle \bar{w}_1, \cdots, \bar{w}_\ell \rangle = \mathrm{Im}\bar{f}$ "Assume not"

Let $v_i \in M$, s.t. $f(v_i) = w_i$ with $\underbrace{(\bar{v}_1, \cdots, \bar{v}_\ell)}_{m/mM}(R/m) \cong \underbrace{\mathrm{Im}\bar{f}}_{(\bar{w}_1, \cdots, \bar{w}_\ell)_{R/m} \Rightarrow \mathrm{Im}f = \langle w_1, \cdots, w_\ell \rangle_R}$ ↘ $\cdots \Rightarrow \langle \bar{w}_1, \cdots, \bar{w}_\ell, \overline{w_{\ell+1}}, \cdots, \bar{w}_k \rangle \Rightarrow N/mN = \langle w_1, \cdots, w_\ell, w_{\ell+1}, \cdots, w_k$

$\therefore M = (v_1, \cdots, v_\ell)$

Now, for $x \in \ker f$, say $x = \sum_{i=0}^{\ell} a_i v_i$, $f(x) = \sum_{i=0}^{\ell} a_i w_i \Rightarrow a_i = 0$ $\forall i \Rightarrow x = 0 \Rightarrow f$ is 1-1 □ $\therefore$ (1)+(2) $\Rightarrow M, N$: finite free, $\bar{f}$ isom $\Rightarrow f$ isom $\Rightarrow M \cong N$

Shun/舜海 (@shun4midx)

DEFINITION

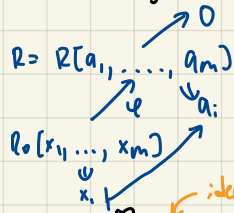
- A filtration of M is $M=M_0\supseteq M_1\supseteq M_2\supseteq\dots$
- Let $I\subseteq R$. $\{M_i\}_{i=0,1,\dots}$ is an I-filtration if $IM_n\subseteq M_{n+1}$ $\forall n$ (e.g. $M_n:=I^nM$)
- I-filtration $\{M_i\}_{i=0,1,\dots}$ is stable if $IM_n=M_{n+1}$ $\forall n\gg 0$.
- $R=\bigoplus_{i=0}^{\infty}R_i$ is a graded ring R if $R_iR_j\subseteq R_{i+j}$
- $M=\bigoplus_{i=0}^{\infty}M_i$ is a graded module over a graded ring if $R_iM_j\subseteq M_{i+j}$

THEOREM

Let R be a graded ring. Then, Noeth $R\Leftrightarrow$ Noeth R_0 and $R=R_0[a_1,\dots,a_m]$, $a_i\in R$

Proof

"$\Leftarrow$": $R=R[a_1,\dots,a_m]\cong R_0[x_1,\dots,x_m]/\ker\varphi$: Noeth



"$\Rightarrow$": Let $R^+=\bigoplus_{i=1}^{\infty}R_i\subseteq R$ and $R_0\cong R/R^+$; ideal $\therefore R^+\subseteq R$

$R^+=(z_1,\dots,z_l)_R$ and $z_i:=z_{i,1}+z_{i,2}+\dots+z_{i,l_i}$ ($z_{i,j}\in R_{i_j}$)

$\Rightarrow (z_{i,j}\mid i=1,\dots,l;\ j=1,\dots,l_i)_R$

$\Rightarrow (a_1,\dots,a_m)_R$, $a_i\in R_{d_i>0}$ $\forall i=1,\dots,n$

Claim: $R_k\subseteq R_0[a_1,\dots,a_m]$ $\forall k\geq 0$ ($\Rightarrow R=R_0[a_1,\dots,a_m]$)

Proof

By induction on k, $k=0$: OK

For $k>0$, let $a\in R_k\subseteq R^+$, $a=\sum_i r_ia_i$ ($r_i\in R_{k-d_i}$; $d_i<k$, $a_i\in R_{d_i}$) $\therefore r_i\in$ RHS $\square$

ARTIN-REES LEMMA

GENERAL FORM

For Noeth R, $I\subseteq R$, M is a finitely generated R-module, $\{M_i\}$ is a stable I-filtration

If $N\subseteq M$ and $N_n=N\cap M_n$, then $\{N_i\}$ is also a stable I-filtration

Proof

For a Noeth M, finitely generated M: $\forall i$, $M=(v_1,\dots,v_m)_R\Rightarrow 0\to\ker\varphi\to R^{\oplus m}\to M\to 0$ (Noeth, Noeth)

- Define $S=S_I(R):=\bigoplus_{n=0}^{\infty}I^nt^n\subseteq R[t]\subseteq\bigoplus_{n=0}^{\infty}Rt^n$

  $\because R$ is Noeth $\Rightarrow I=(a_1,\dots,a_m)$ and $S=R[a_1t,\dots,a_mt]$ $\therefore S$ is Noeth

  Define $\tilde{M}:=\bigoplus_{n=0}^{\infty}M_nt^n$ which is a graded S-module ($I^kt^kM_jt^j\subseteq M_{j+k}t^{k+j}$)

  $U_m:=M_0+M_1t+\dots+M_mt^m$: A finitely generated R-module $=(\star_1,\dots,\star_s)_R$

  $L_m:=(U_m)_S=U_m\oplus IM_mt^{m+1}\oplus I^2M_mt^{m+2}\oplus\dots$

  Also, $L_m\subseteq L_{m+1}$ and $\bigcup_{n\geq 0}L_m=\tilde{M}$

  $\therefore L_m$ is a finitely generated S-module $=(\star_1,\dots,\star_s)_S$

Observe, with how S is Noeth, $\tilde{M}$ is finitely generated over $S\Leftrightarrow\tilde{M}$ is Noeth $\Leftrightarrow\tilde{M}=L_{n_0}$ for some $n_0\Leftrightarrow M_{n_0+m}=I^mM_{n_0}$ $\forall m\geq 0\Leftrightarrow\{M_i\}$ is I-stable

Now, $I(N\cap M_n)\subseteq IN\cap IM_n\subseteq N\cap M_n=N_{n+1}\Rightarrow\{N_i\}$ is an I-filtration

Similarly, $\tilde{N}=\bigoplus_{n=0}^{\infty}N_nt^n$ is an S-submodule of $M\Rightarrow\tilde{N}$ is a finitely generated S-module $\square$

COROLLARY

For a Noeth R, finitely generated R-module M, $I\subseteq R$, $N\subseteq M$, then $I^{n_0+m}M\cap N=I^m(I^{n_0}M\cap N)$ $\forall m\geq 0$

Proof

Let $M_n=I^nM$, then $N^n=I^nM\cap N$. By thm, $\{N_n\}$ is I-stable, i.e. $\exists n_0$, s.t. $I^mN_{n_0}=N_{n_0+m}$ $\square$

Shun/翔海 (@shun4midx)

KRULL THEOREM

For a Noeth R, $I \subseteq J_R$, finitely generated R-module M, then $\bigcap_{n=0}^{\infty} I^n M = \{0\}$

Proof

Let $N := \bigcap_{n=0}^{\infty} I^n M \subseteq M$ and $N \cap I^n M = N$ (Noeth $\Rightarrow$ finitely generated)

By Artin-Rees lemma, $\exists n_0 \in \mathbb{N}$, s.t. $I^m (N \cap I^n M) = I^{m+n_0} M \cap N \ \forall m \geq 0$. If $m=1$, we get $IN = N$. By Nakayama lemma, $N = 0$. ∎

COROLLARY + REMARK

For a Noeth local $(R, \mathfrak{m})$, we get $\bigcap_{n=0}^{\infty} \mathfrak{m}^n = \{0\}$

Then, $\forall x \in R$, $\exists k$, s.t. $x \in \mathfrak{m}^k$ but $x \notin \mathfrak{m}^{k+1}$ $\Rightarrow$ We can define "order" with $o(x) = k$

By defining "distance" as $2^{-o(x)}$, we can do completion like in analysis.

4-2-25 (WEEK 7)

Shun / 郑翔海 (@shun4midx)

HILBERT POLYNOMIAL

MOTIVATION

For a Noeth local R and a fin gen R-module M, $\{m\} = \mathrm{Max}\, R$, how do we study m?

KRULL'S THEOREM (RECALL)

$\bigcap_{i=0}^{\infty} m^i M = \{0\} \Rightarrow \forall v \in M, \exists k \in \mathbb{N}\cup\{0\}$, s.t. $v \in m^k M$ but $v \notin m^{k+1} M$ with $m^0 := R$. Here, we define the order $o(v) := k$

Now, how do we investigate R-module M/mM?
Notice, if we separate based on order: $M/mM,\ mM/m^2M,\ \dots,\ m^{l-1}M/m^lM$
As $\forall k$, $m(m^{k-1}M/m^kM) = 0$, thus $m^{k-1}M/m^kM$ is an R/m-module, i.e. a field. (vector space!)

How do we consider its dimension then? Consider $\sum_{i=0}^{\infty} \dim m^iM/m^{i+1}M\, t^i$

DEFINITION

Let G be an abelian group and $\varphi : {}_R\mathcal{M} \longrightarrow G$, $M \longmapsto \varphi(M)$ ("generating function" to calculate dim). We say φ is an Euler-Poincaré mapping if $\varphi(0) = 0$ and $\forall\ 0 \to M_1 \to M_2 \to M_3 \to 0$ in ${}_R\mathcal{M}$, $\varphi(M_3) = \varphi(M_1) + \varphi(M_2)$

DEFINITION

$R = \bigoplus_{i\ge 0} R_i$ is a graded Noeth, and $M = \bigoplus_{i\ge 0} M_i$ is a fin gen R-module, where R_0 is Noeth, $R = R_0[a_1, \dots, a_n]$ with $a_i \in R_{d_i}$, $d_i > 0$, $M = (x_1, \dots, x_m)_R$ with $x_i \in M_{k_i}$ and M_i are fin gen R_0-modules. Then, for Euler-Poincaré mapping $\varphi : {}_R\mathcal{M}^{(\infty)} \xrightarrow{\text{fin gen}} \mathbb{Z}$, we define:
$P_M(t) := \sum_{i=0}^{\infty} \varphi(M_i)\, t^i \in \mathbb{Z}[[t]]$ is called a Poincaré series

DEFINITION

$p(z) \in \mathbb{Q}[z]$ is called a numerical polynomial if $p(n) \in \mathbb{Z}$ $\forall n \gg 0$, $n \in \mathbb{Z}$

PROPOSITION

If $p(z)$ is numerical, then $\exists\ c_0, \dots, c_r \in \mathbb{Z}$, s.t. $p(z) = c_0\binom{z}{r} + c_1\binom{z}{r-1} + \dots + c_{r-1}\binom{z}{1} + c_r$, where even for $z \in \mathbb{R}$, $\binom{z}{r} := \frac{z(z-1)\cdots(z-r+1)}{r!}$
In particular, $p(n) \in \mathbb{Z}$ $\forall n \in \mathbb{Z}$

Proof
Since $\binom{z}{r} = \frac{z^r}{r!} + \dots$, $\binom{z}{0} := 1$, thus by viewing $\binom{z}{r}$ as a z-polynomial, $\{\binom{z}{r} \mid r \in \mathbb{N}\cup\{0\}\}$ forms a basis for $\mathbb{Q}[z]$ over $\mathbb{Q}$.
Then, we can write $p(z) = c_0\binom{z}{r} + c_1\binom{z}{r-1} + \dots + c_0(1)$ with $c_i \in \mathbb{Q}$

By induction on $\deg p$,
- $\deg p = 0$: $p(z) = c \in \mathbb{Z}$, ok ✓
- Recall: $\binom{z+1}{r} - \binom{z}{r} = \binom{z}{r-1}$
- $\because \deg(p(z+1) - p(z)) < \deg(p(z))$ and "numerical" still is true
  $\therefore$ By induction hypothesis, $\exists\ c_0', \dots, c_{r-1}' \in \mathbb{Z}$, s.t. $p(z+1) - p(z) = c_0'\binom{z}{r-1} + \dots + c_{r-1}'$

Notice, $\binom{z}{r-1}, \dots, \binom{z}{0}$ are lin indep, i.e. $c_i' = c_i$ $\forall i$, so $c_r = \underbrace{p(n)}_{\in\mathbb{Z}} - \underbrace{(c_0\binom{n}{r} + c_1\binom{n}{r-1} + \dots + c_{r-1}\binom{n}{1})}_{\in\mathbb{Z}}$ for some $n \gg 0$, i.e. $c_r \in \mathbb{Z}$. □

PROPOSITION 2

If $f : \mathbb{Z} \to \mathbb{Z}$, s.t. $f(n+1) - f(n) = Q(n)$ $\forall n \gg 0$ with numerical $Q(z)$, then $f(n) = p(n)$ $\forall n \gg 0$ for some numerical poly $p(z)$

Proof
Write $Q(z) = c_0\binom{z}{r} + \dots + c_r$ with $c_i \in \mathbb{Z}$. Let $\tilde{p}(z) = c_0\binom{z}{r+1} + \dots + c_r\binom{z}{1}$ (rewrite r only)
Then, $\tilde{p}(z+1) - \tilde{p}(z) = Q(z) \Rightarrow \tilde{p}(n+1) - \tilde{p}(n) = f(n+1) - f(n)$ $\forall n \gg 0$
$\therefore f(n+1) - \tilde{p}(n+1) = f(n) - \tilde{p}(n)$ $\forall n \gg 0$ (i.e. constant)

Say $f(n)-\tilde{p}(n)=C_{r+1}$ $\forall n\gg 0$. Let $p(z)=\tilde{p}(z)+C_{r+1}$. Then, $f(n)=p(n)$ $\forall n\gg 0$.

Shun/鞏浚海 (@shun4midx)

THEOREM (HILBERT-SERRE)

(1) $P_\varphi(M,t)=\dfrac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})}$ for some $f(t)\in\mathbb{Z}[t]$, $d_i\in\mathbb{N}$

(2) If $d_i=1$ $\forall i=1,\dots,n$ and $P_\varphi(M,t)=\frac{h(t)}{(1-t)^d}$, $(1-t)\nmid h(t)$, then $\exists!$ $p(z)\in\mathbb{Q}[z]$ of deg $d-1$, s.t. $\varphi(M_n)=p(n)$ $\forall n\gg 0$

Proof

(1) By induction on n,

- $n=0$: $R=R_0$, M is a fin gen R-module, say $M=\langle \underbrace{x_1}_{\in M_{\ell_1}},\dots,\underbrace{x_m}_{\in M_{\ell_m}}\rangle_R$

  $\therefore M_i=0$ $\forall i>\max\{\ell_1,\dots,\ell_m\}\Rightarrow \varphi(M_i)=0$ $\forall i\gg 0\Rightarrow P_\varphi(M,t)$ is a polynomial

- $n>0$: Consider $0\to K_i\to M_i\xrightarrow{\cdot a_n} M_{i+d_n}\to L'_{i+d_n}\to 0$
  ($K_i=\ker(\cdot a_n)$, $L'_{i+d_n}=\operatorname{Coker}(\cdot a_n)$)

  Let $K=\bigoplus_{i\ge 0}K_i\subseteq M$, $L=\bigoplus_{i\ge 0}L_i=M/\sim$, which are fin gen R-modules and annihilated by a_n

  Also, we have $0\to K_i\to M_i\to \mathrm{Im}(\cdot a_n)\to 0$ and $0\to \mathrm{Im}(\cdot a_n)\to M_{i+d_n}\to L_{i+d_n}\to 0$

  $$\Rightarrow\begin{cases}\varphi(K_i)+\varphi(\mathrm{Im}(\cdot a_n))=\varphi(M_i)\\ \varphi(\mathrm{Im}(\cdot a_n))+\varphi(L_{i+d_n})=\varphi(M_{i+d_n})\end{cases}\Rightarrow \varphi(K_i)-\varphi(M_i)+\varphi(M_{i+d_n})-\varphi(L_{i+d_n})=0$$

  Multiply by t^{i+d_n}, we get $t^{d_n}(\varphi(K_i)t^i-\varphi(M_i)t^i)+\varphi(M_{i+d_n})t^{i+d_n}-\varphi(L_{i+d_n})t^{i+d_n}=0$

  Take summation from $i=0$ to ∞, $t^{d_n}(P_\varphi(K,t)-P_\varphi(M,t))+P_\varphi(M,t)-P_\varphi(L,t)-\underbrace{(\sum_{i=0}^{d_n-1}\varphi(M_i)t^i-\sum_{i=0}^{d_n-1}\varphi(L_i)t^i)}_{=:g(t)\in\mathbb{Z}[t]}$

  $\therefore (1-t^{d_n})P_\varphi(M,t)=P_\varphi(L,t)-t^{d_n}P_\varphi(K,t)+g(t)$

  As L,K are $R_0[a_1,\dots,a_{n-1}]$-modules,

  $$P_\varphi(L,t)=\frac{f_1(t)}{\prod_{i=1}^{n-1}(1-t^{d_i})},\quad P_\varphi(K,t)=\frac{f_2(t)}{\prod_{i=1}^{n-1}(1-t^{d_i})}$$

  $$\therefore P_\varphi(M,t)=\frac{f(t)}{\prod_{i=1}^{n}(1-t^{d_i})}\ \square$$

(2) By (1), write $P_\varphi(M,t)=\frac{h(t)}{(1-t)^d}$, $(1-t)\nmid h(t)$, $h(t)=\sum_{i=0}^{N}a_it^i$

Since $(1-t)^{-d}=1-\binom{-d}{1}t+\binom{-d}{2}t^2-\dots+(-1)^{d-1}\binom{-d}{d-1}t^{d-1}+\dots$, notice $\binom{-d}{i}=(-1)^i\binom{d+i-1}{d-1}$

$=\sum_{i=0}^{\infty}\binom{d+i-1}{d-1}t^i$

$\therefore$ Comparing the coef of t^m in $P_\varphi(M,t)$, we get $\varphi(M_m)=\sum_{i=0}^{N}a_i\binom{d+(m-i)-1}{d-1}=\underbrace{(\sum_{i=0}^{N}a_i)}_{\neq 0\text{ since }(1-t)\nmid h(t)\Rightarrow h(1)\neq 0\ \therefore\text{degree is this val}}\frac{m^{d-1}}{(d-1)!}$ $\forall m\gg N$

THEOREM

For Noeth local (R,m), fin gen R-module M, and $F=R/m$, then:

(1) $\dim_F M/mM<\infty$ ($M/mM\leftrightarrow M/mM\oplus mM/m^2M\oplus\dots\oplus m^{d-1}M/m^dM$)

(2) If d is the least number of generators of m, then $\exists g(z)\in\mathbb{Q}[z]$ of deg $\le d$, s.t. $g(n)=\dim_F M/m^nM$ $\forall n\gg 0$

Proof

Let $\mathrm{gr}_m(R)=R/m\oplus m/m^2\oplus m^2/m^3\oplus\dots=\bigoplus_{i\ge 1}m^i/m^{i+1}$, $m_0:=R$

Define $\forall x_i+m^{i+1}\in m^i/m^{i+1}$, $x_j+m_{j+1}\in m^j/m^{j+1}$, $(x_i+m^{i+1})(x_j+m^{j+1}):=x_ix_j+m^{i+j+1}$

- Well-defined: $x_i'-x_i\in m^{i+1}$, $x_j'-x_j\in m^{j+1}\Rightarrow x_i'x_j'-x_ix_j=\underbrace{x_i'}_{\in m^i}\underbrace{(x_j'-x_j)}_{\in m^{j+1}}+\underbrace{(x_i'-x_i)}_{\in m^{i+1}}\underbrace{x_j}_{\in m^j}\in m^{i+j+1}$

Define $\mathrm{gr}_m(M)=\bigoplus_{i\ge 0}m^iM/m^{i+1}M$: $\mathrm{gr}_m(R)\times\mathrm{gr}_m(M)\longrightarrow\mathrm{gr}_m(M)$

$(x_i+m^{i+1},a_j+m^{j+1}M)\longmapsto x_ia_j+m^{i+j+1}M$

With Rees lemma, via $\varphi: S\underbrace{(m}_{\text{max ideal}}(R)\longrightarrow \mathrm{gr}_m(R)$ $\Longrightarrow$ a graded ring homo $\Rightarrow S/mS\cong\underbrace{\mathrm{gr}_m(R)}_{\text{Noeth}}$

($S(m(R)=R\oplus mt\oplus m^2t^2\oplus\dots$, $\mathrm{gr}_m(R)=R/m\oplus m/m^2\oplus\dots$)

Similarly, $\mathrm{gr}_m(M)=\tilde{M}/m\tilde{M}$ for some $\tilde{M}=M\oplus mMt\oplus m^2Mt^2\oplus\dots$, thus $\tilde{M}$ is Noeth $\Rightarrow \mathrm{gr}_m(M)$ is a fin gen $\mathrm{gr}_m(R)$-module

$\therefore m^iM/m^{i+1}M$ is a fin gen R/m-module. Also, $\dim_F M/mM=\sum_{i=1}^{d}\dim_F m^{i-1}M/m^iM<\infty$

Shun / 翔海 (@shun4midx)

(2) Let $\langle a_1, \dots, a_d \rangle_R = m$, then $\mathrm{gr}_m(R) = R/m[\bar{a}_1, \dots, \bar{a}_d]$, $\bar{a}_i \in m/m^2$

By Hilbert-Serre (2), $\exists!\ p(z) \in \mathbb{Q}[z]$ of $\deg \le d-1$, s.t. $p(n) = \dim_F m^n M / m^{n+1} M$ $\forall n \gg 0$ $\Rightarrow$ $\dim_F M/m^{n+1}M - \dim_F M/m^n M = p(n)$

$\therefore$ By prop 2, $\exists\, g(z) \in \mathbb{Q}(z)$ with $\deg \le d$, s.t. $g(n) = \dim M/m^n M$ $\forall n \gg 0$. $\square$