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

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 $f(x)g(x) = \underbrace{c}_{\text{cont}(fg)} h(x)$ with c being a non-unit and $h(x)$ being primitive

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

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

However, $p | \underbrace{a_0 b_{r+s} + \dots + a_{r+s} b_0}_{\text{from } p|c} \Rightarrow p | a_r b_s \Rightarrow p | a_r$ or $p | b_s$ $\rightarrow\!\times$

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 $fg = \text{cont}(f)\,\text{cont}(g) \underbrace{f_1(x) g_1(x)}_{\text{primitive}} \Rightarrow \text{cont}(fg) = \text{cont}(f)\,\text{cont}(g)$ □

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 $A(x) = \frac{\ell_1}{t_1} a_1(x)$, $B(x) = \frac{\ell_2}{t_2} b_1(x)$, where a_1, b_1 are $\underbrace{\text{primitive}}_{\text{primitive}}$ in $R[x]$ and $\ell_i, t_i \in R$ with $\gcd(\ell_i, t_i) = 1\ \forall i = 1, 2$

By assumption, $f(x) = \frac{\ell_1 \ell_2}{t_1 t_2} a_1(x) b_1(x) \Rightarrow t_1 t_2 f(x) = \ell_1 \ell_2 \underline{a_1(x) b_1(x)} \Rightarrow t_1 t_2\, \text{cont}(f) = \ell_1 \ell_2 u$ for some $u \in R^\times$.

So, $f(x) = \frac{u^{-1} \cancel{t_1 t_2}\, \text{cont}(f)}{\cancel{t_1 t_2}} a_1(x) b_1(x)$, so $a_1(x) = \frac{u^{-1} t_1\, \text{cont}(f)}{\ell_1} A(x)$, $b_1(x) = \frac{t_2}{\ell_2} B(x)$

- In $A_D \ni p+q\sqrt{D}$, 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, $f(x)=\frac{\ell}{t}\bar{q}(x)\frac{1}{cd}(dcx^2-ax+b) \Rightarrow \ell \sim tcd$, i.e. $\ell = \pm tcd$
  $\therefore f(x)=\pm\bar{q}(x)(dcx^2-ax+b) \Rightarrow$ Comparing, we get $dc \mid 1 \Rightarrow d,c=\pm 1 \Rightarrow g(x)\in\mathbb{Z}[x]$ ✓

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 $f_1(x)=p_1(x)p_2(x)\cdots p_r(x)=q_1(x)q_2(x)\cdots q_s(x)$ 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
$\Rightarrow p_i(x)=\frac{t_i}{\ell_i}q_i(x)$ for $\ell_i,t_i\in R\Rightarrow t_ip_i(x)=\ell_iq_i(x)\Rightarrow t_i=u_i\ell_i$ 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 $f(x)\mid 2$ and $f(x)\mid x\Rightarrow f(x)=\pm1 \overset{\text{but } 1\notin\langle x,2\rangle}{\Rightarrow} \langle f(x)\rangle=\mathbb{Z}[x]$ $\rightarrow\!\times\!\leftarrow$

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 $\deg\bar{g}=\deg g\geq1$ and $\deg\bar{h}=\deg h\geq1$, 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 $R[x]$

<u>Proof</u>

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 $R/P[x]$

$$\underset{\bar{a}_n x^n}{\bar{f}(x)} = \underset{\bar{b}_r x^r}{\bar{g}(x)}\;\underset{\overline{c_{n-r}}\, x^{n-r}}{\bar{h}(x)}$$

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, $a_0 = c_0 b_0 \in P^2$ $\rightarrow\!\leftarrow$ $\therefore f(x)$ is irr in $R(x)$ $\square$

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)

<u>Proof</u>

- f has no linear factor: If $f(\alpha) = 0$, then $\alpha = -kp$ for $k \in \mathbb{N}$ $\rightarrow\!\leftarrow$ $(x + kp)$ 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, $p = b_1 c_0 + c_1 b_0 \equiv 0 \pmod{p^2}$ $\rightarrow\!\leftarrow$