Algebra. Lec 14. Gauss Lemma, Criteria for irreducibility

eg. $f(x) = 5x+5 \in \mathbb{Q}[x]$

$\hookrightarrow$ units $\mathbb{Q}-\{0\}$

irred.

$f(x) = 5x+5 \in \mathbb{Z}[x]$

$= 5(x+1)$

$\downarrow$

not unit in $\mathbb{Z}[x]$

not irred.

---

field of fractions

UFD. $K = \mathrm{Frac}(A) = (A-\{0\})^{-1}A$ (Motivation or preparations)

$0 \neq a \in K$. can write a as a quotient

- $a = \frac{a_1}{a_2}$. $a_1, a_2 \in A$, $a_1 \cdot a_2$ have no prime in common (reduced form)

  $\hookrightarrow$ Rmk. in UFD. A prime $\Leftrightarrow$ irred

- p. some prime in A $a = p^r \cdot b$. $b \in K$.

  r. integer

  $b = b_1/b_2$ reduced form, $p \nmid b_1$. $p \nmid b_2$

$r \triangleq$ (the order of a at p).

notation: $r = \mathrm{ord}_p a$

- $a, a' \in K$. $aa' \neq 0$

$\Rightarrow \mathrm{ord}(aa') = \mathrm{ord}_p a + \mathrm{ord}_p a'$

- $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$

$f \neq 0$. $\mathrm{ord}_p f = \min_i \mathrm{ord}_p a_i$

Content of f

$\mathrm{cont}(f) \triangleq \prod_p p^{\mathrm{ord}_p f}$

eg. $\mathbb{Z}[x]$. $f(x) \in \underbrace{(\mathbb{Z}-\{0\})^{-1}\mathbb{Z}}_{\mathbb{Q}}[x]$

$f(x) = \frac{5}{3} + \frac{3 \cdot 2}{5^2} x$

$\left.\begin{array}{l} \mathrm{ord}_2 f = 0 \\ \mathrm{ord}_3 f = -1 \\ \mathrm{ord}_5 f = -2 \end{array}\right\}$ $\Rightarrow \mathrm{cont}\, f = 2^0 \cdot 3^{-1} \cdot 5^{-2} = \frac{1}{3} \cdot \frac{1}{5^2}$

$\Rightarrow f = \frac{1}{3 \times 5^2} \underbrace{(125 + 18x)}_{\in \mathbb{Z}[x]}$

clearly. $b \in K$, $b \neq 0$: $\mathrm{cont}(bf(x)) = b\, \mathrm{cont}(f)$

$\Rightarrow f(x) = \underbrace{\mathrm{cont}(f)}_{\in K} f_1(x)$. $\underbrace{\mathrm{cont}(f_1(x)) = 1}_{}$

$\downarrow$

primitive, $f_1(x) \in A[x]$

Thm. 2.1 (Gauss Lemma)

A: UFD. $K = \mathrm{Frac}(A)$

$f, g \in K[x]. \Rightarrow \mathrm{cont}(fg) = \mathrm{Cont}(f)\,\mathrm{cont}(g)$

Pf. $\underset{\substack{\| \\ \mathrm{Cont}(f)}}{c}f_1.$ $\quad g = \underset{\substack{\| \\ \mathrm{Cont}(g)}}{d}g_1$ $\qquad \mathrm{Cont}(f_1) = 1 = \mathrm{Cont}(g_1).\ f_1, g_1 \in A[x]$

$$fg = cd f_1 g_1 \Rightarrow \mathrm{Cont}(fg) = \mathrm{Cont}(cd f_1 g_1)$$

$$= cd\,\mathrm{Cont}(f_1 g_1) \quad (**)$$

(*). if $\mathrm{cont}(f) = 1 = \mathrm{Cont}(g) \Rightarrow \mathrm{Cont}(fg) = 1$

If (*) $\Rightarrow$ w. (**) $\Rightarrow \mathrm{Cont}(fg) = cd.$ ✓

We now prove (*).

i.e. for each prime p. $\mathrm{ord}_p(fg) = 0$

$f = a_n x^n + \cdots + a_0 \in A[x]$

$g = b_m x^m + \cdots + b_0. \in A[x]$

<u>claim.</u> $\forall p$. prime in A. p does not divide all coff of fg

Consider coff of x^{r+s}. in $f(x)g(x)$

$c = a_r b_s + a_{r+1} b_{s-1} + a_{r-1} b_{s+1} + \cdots$

$$\left.\begin{array}{lll} p \nmid a_r & p \mid a_{r+1} & p \mid a_{r+2} \\ p \nmid b_s & p \mid b_{s+1} & p \mid b_{s+2} \end{array}\right\} \Longrightarrow p \nmid c$$

so we just from n to 1 find first r. $p \nmid a_r$

m to 1 find first s. $p \nmid b_s$ $\square$

<u>Another proof</u>

$f \cdot g$. primitive. (i.e. $\mathrm{Cont} = 1$)

$\Longrightarrow fg$ primitive.

pf. p: prime in A

$A \to A/(p) = \bar{A}$

$A[x] \to \bar{A}[x]$ ring hom

$f \longmapsto \bar{f}$

$g \longmapsto \bar{g}$

primitive

$fg \longmapsto \overline{fg} = \bar{f} \cdot \bar{g}$, $\because \bar{f}, \bar{g} \neq 0$.

($\bar{A}[x]$ domain.) ex.

$\Longrightarrow \overline{fg} \neq 0$ primitive. $\square$

Cor. 2.2. $f(x) \in A[x]$

if $f(x) = g(x)h(x)$. $g, h \in K[x]$

let $g(x) = \text{cont}(g)\, g_1 = c_g g_1$

$h(x) = \text{cont}(h)\, h_1 = c_h h_1$

$\Rightarrow f(x) = c_g c_h\, g_1(x)\, h_1(x)$

$\Rightarrow c_g c_h \in A$

In particular. if $f, g \in A[x]$. $\text{cont}(f) = \text{cont}(g) = 1$

$\text{cont}(f) = \text{cont}(g)\,\text{cont}(h)$

$\Rightarrow \text{cont}(h) = 1 \Rightarrow h \in A[x]$.

Rmk. $f(x) \in A[x]$

$$f(x) = \underset{\substack{\cap \\ K[x]}}{g(x)}\ \underset{\substack{\cap \\ K[x]}}{h(x)}$$

$$= \underset{\substack{\cap \\ A}}{(c_g c_h)}\ \underset{\substack{\cap \\ A[x]}}{g_1(x)}\ \underset{\substack{\cap \\ A[x]}}{h_1(x)}$$

Rmk $f(x) \in A[x]$. f: primitive ($\text{cont}(f) = 1$)

f: irred in $A[x] \Leftrightarrow f$: irred in $K[x]$

Thm. A: UFD $\Rightarrow$ $A[x]$: UFD

Pf. $f \in A[x]$ $f \neq 0$.

$f \in A[x] \subseteq K[x]$

apply the unique factorization of $K[x]$

$$\underset{}{f(x)} = \underset{\underset{K}{\cap}}{\hat{c}}\ \underset{\underset{K[x]}{\cap}}{\tilde{p}_1(x)}\ \underset{\underset{K[x]}{\cap}}{\tilde{p}_2(x)} \cdots \underset{\underset{K[x]}{\cap}}{\tilde{p}_r(x)}$$

$\tilde{p}_i$: irred in $K[x]$

use the Gauss lemma

$$f(x) = \underset{\underset{A}{\cap}}{c}\ \underset{\underset{A[x]}{\cap}}{p_1(x)}\ \underset{\underset{A[x]}{\cap}}{p_2(x)} \cdots \underset{\underset{A[x]}{\cap}}{p_r(x)}$$

cont $(p_i) = 1$ p_i : irred in $K[x]$

$\Rightarrow$ p_i : irred in $A[x]$

Now if $f(x) = c\ p_1(x) \cdots p_r(x)$

$= d\ q_1(x) \cdots q_s(x)$

p_i, q_j : irred in $A[x]$

$\Rightarrow$ from the unique fac of $K[x]$ $\Rightarrow$ $r = s$ after renumbering

$p_i = a_i q_i$

a_i unit in $K[x]$

$\Rightarrow$ cont (p_i) = cont (a_i) cont (q_i) $\Rightarrow$ a_i. unit in $A[x]$

$\Rightarrow$ $c = (\text{unit in } A) \cdot d$ $\square$

HW

- Gaussian primes.
- D-F. Sec 9.4 ex 1, 2, 3, 4

  Lang. Chap V. ex 1, 2, 3, 4, 5, 6.

Criteria for irreducibility

Thm. 3.1 (Eisenstein)

A: UFD. $K = \mathrm{Frac}(A)$

$f(x) = a_n x^n + \cdots + a_0 \in A[x]$ $\quad \deg f = n$.

p: prime in A

$a_n \not\equiv 0 \pmod p$. $a_i \equiv 0 \pmod p$. $\quad a_0 \not\equiv 0 \pmod{p^2}$

$i = 0, \ldots, n-1$.

$\Rightarrow f(x)$: irred in $K[x]$

pf. Extracting out gcd of all coff of f.

$\therefore$ may assume. $\mathrm{cont}(f) = 1$

if $f(x)$: not irred in $K[x]$ $\Rightarrow$ $f(x)$: not irred in $A[x]$

$\therefore f(x) = g(x) h(x)$. $g, h \in A[x]$

$= (b_d x^d + \cdots + b_0)(c_m x^m + \cdots + c_0)$

$p \mid b_0 c_0 \quad p^2 \nmid b_0 c_0 \quad$ say $p \nmid b_0$. $p \mid c_0$.

$p \nmid b_d c_m$. $\Rightarrow p \nmid c_m$.

If $p|c_0$ $p|c_1$ $\cdots$ $p|c_{r-1}$ $p\nmid c_r$

Consider $a_r = \underbrace{b_0 c_r}_{\text{not divisible by } p} + \underbrace{b_1 c_{r-1} + b_2 c_{r-2} + \cdots}_{\text{divisible by } p}$

$\therefore p \nmid a_r$ $\times$

---

eg. ① $a \in \mathbb{Z}$, $a \neq 0$. a: sequarefree. $a \neq \pm 1$

$\underline{x^n - a}$: irred over $\mathbb{Q}$

$\Rightarrow$ irred over $\mathbb{Z}$

② $3x^5 - 15$ take $p = 5$

irred over $\mathbb{Q}$

③ $2x^{10} - 21$. take $p = 3$ or 7

irred over $\mathbb{Q}$ & $\mathbb{Z}$

④ $f(x) = x^{p-1} + \cdots + 1. = \frac{x^p - 1}{x - 1}$ p: prime

irred over $\mathbb{Q}$

$\Leftarrow$ $f(x+1)$ irred.

$f(x+1) = \frac{x^p + px^{p-1} + \cdots + px + 0}{x}$ ✓

eg. E: field. $t \in$ some field. Containing E

t: transidental $/E$

$K = \mathrm{Frac}(E(t))$

domain why? for $E(t) \cong E(x)$

$1 \in K$

$t \in K$

<u>claim</u>. $x^n - t \in K[x]$. irred. $\overset{\text{Gauss Lemma}}{\Longrightarrow}$ ($\because$ irred in $E[t]$)

($\because$ t: prime in $E[t]$.

for. $E[t]/(t) \cong E$ field. $\Rightarrow$ t prime)

Thm. reduction

$\varphi: A \to B$ ring hom $K = \mathrm{Frac}(A)$

A, B domain $L = \mathrm{Frac}(B)$

$f \in A[x]$, $\varphi f \neq 0$. $\deg(\varphi f) = \deg(f)$

If. φf: irred in $L[x]$ then f does not have a factorization

$f(x) = g(x)h(x)$, $g, h \in A[x]$ $\deg g \geq 1$. $\deg h \geq 1$

Pf If $f(x) = \underset{A[x]}{\underset{\cup}{g(x)}}\ \underset{A[x]}{\underset{\cup}{h(x)}}$

$$\underbrace{\varphi f(x)}_{\substack{\deg \varphi f \\ \| \\ \deg f}} = (\varphi g)(x)(\varphi h)(x)$$

$\Rightarrow$ $\deg g = \deg \varphi g$

$\deg f = \deg \varphi f$ $\quad \not\longrightarrow$ w. φf irred.

eg. p. prime number

$x^p - x - 1$ irred over $\mathbb{Z}/p\mathbb{Z}$ (will show this later)

$x^5 - 5x^4 - 6x - 1$. irred over $\mathbb{Q}$ ($\mathbb{Z}$)

Do. $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/5\mathbb{Z}$.

$$x^5 - 5x^4 - 6x - 1 \to \underset{(\mathbb{Z}/5\mathbb{Z})[x]}{\underset{\cup}{x^5 - x - 1}} \qquad \square$$