对 k 归纳：当 $k=0$ 时

$$f = f_e x^e + f_{e-1} x^{e-1} + \cdots + f_0$$

$$f - f_e g_e^{-1} g = f_e x^e + f_{e-1} x^{e-1} + \cdots + f_0 - (f_e x^e + f_e g_e^{-1} g_{e-1} x^{e-1} + \cdots + f_e g_e^{-1} g_0)$$

$$= (f_{e-1} - f_e g_e^{-1} g_{e-1}) x^{e-1} + \cdots + (f_0 - f_e g_e^{-1} f_0)$$

$=: r$

则 $\deg(r) < e$. 令 $q = f_e g_e^{-1}$ 则

$$f = q g + r.$$ 引理成立.

设 $\deg(f) - \deg(g) < k$ 时 引理成立

考虑 $\deg(f) = e+k$ 的情形. 此时

$$f = f_{e+k} x^{e+k} + f_{e+k-1} x^{e+k-1} + \cdots + f_0$$

$$f - f_{e+k} g_e^{-1} x^k g = f - (f_{e+k} x^{e+k} + f_{e+k} g^{-1} g_{e-1} x^{e+k-1} + \cdots + f_{e+k} g_e^{-1} g_0 x^k) =: h$$

则 $\deg(h) < e+k$.

由归纳假设 $\exists\, p, r \in R[x]$ 使得

$h = pg + r$. 其中 $\deg(r) < \deg g$

于是

$$f = f_{e+k} g_e^{-1} x^k g + h$$
$$= f_{e+k} g_e^{-1} x^k g + pg + r$$
$$= (f_{e+k} g_e^{-1} x^k + p) g + r$$

令 $q = f_{e+k} g_e^{-1} x^k + p$ 即可. 存在性成立

设 $f = ug + v$, 其中 $u, v \in R[x]$

$\deg v < \deg g$.

则 $qg + r = ug + v$

$$(q-u) g = v + r$$

如果 $q - u \neq 0$. 则由推论知

$$\deg((q-u)g) = \deg(q-u) + \deg(g) \geq e$$

而由 $\deg(v+r) < e$ 与 $(q-u)g = v+r$ 矛盾

□

于是 $q - u = 0 \Rightarrow v = r$.

注 称 r 为 f 除于 g 的余式

q ······ 商.

定理 2.3 设 F 是域. 则 $\forall f, g \in F[x]$

$g \neq 0$. f 关于 g 的余式和商存在且唯一

证: $\because g \neq 0 \therefore lc(g) \neq 0 \Rightarrow lc(g)$ 可逆.

由引理 2.2. 定理 2.3 成立

例: 设 $f = x^2 - \bar{3}$, $g = \bar{5}x + \bar{2} \in \mathbb{Z}_7[x]$

求 f 关于 g 的商和余式.

$lc(g) = \bar{5}$ $\quad lc(g)^{-1} = \bar{3}$

$\cancel{f = x^2}$

$f - \bar{3}x(\underbrace{\bar{5}x+\bar{2}}_{g}) = f - (x^2 + \bar{6}x)$

$= \bar{6}x - \bar{3}$

$\bar{6}x - \bar{3} - \bar{6}\cdot\bar{3}(\underbrace{\bar{5}x+\bar{2}}_{g}) = -\bar{3} + \bar{6}\cdot\bar{3}\cdot\bar{2}$

$= \bar{4} + \bar{1} = \bar{5}$

商 $q = \bar{3}x + \bar{4}$. 余式 $r = \bar{5}$.

§2.5 一元多项式的根

定义 设 F 是域, $f \in F[x]$. 如果 $\alpha \in F$ 使得 $f(\alpha) = 0$, 则称 α 是域 F 中 f 的一个根.

定理 2.4. (余式定理)

设 F 是域 $f \in F[x]$. ~~如果 $\alpha \in F$~~

则 $\alpha \in F$ 是 f 的根 $\Longleftrightarrow \exists q \in F[x]$

使得 $f(x) = q(x)(x-\alpha)$.

证: 设 $\alpha \in F$.

$f(x) = q(x)(x-\alpha) + r$

其中 $q \in F[x]$ $\quad deg(q) = deg(f) - 1$, 且 $r \in F$

$f(\alpha) = 0 \Longleftrightarrow q(\alpha)(\alpha-\alpha) + r = 0 \Longleftrightarrow r = 0$

$\Longleftrightarrow f(x) = q(x)(x-\alpha)$ ☒

定理 2.5 设 F 是域 $f \in F[x]$, $deg(f) = d > 0$.

则 f 在 F 中至多有 d 个互不相同的根

证: 反证: 假设 $\alpha_1, \alpha_2, \ldots \alpha_{d+1}$ 是 f 的互不相同的根. 由定理 2.4 $\exists q \in F[x]$ 使得 $deg\, q = d-1$

$f(x) = q(x)(x - \alpha_{d+1})$

$\forall i \in \{1, 2, \ldots d\}$, $0 = f(\alpha_i) = q(\alpha_i)(\alpha_i - \alpha_{d+1})$

有 d 个互不相同的根

于是 $q(x)$ 有 d 个互不相同的根

对 g 重复上述步骤 可推出 $F[x]$ 中~~有~~ $d-2$ 次的多项式有 $d-1$ 个互不相同的根
以此类推，$F[x]$ 存在一个一次多项式有两个不同的根 . →← ☒

§3 域上一元多项式的因式分解

本节中 F 是域

§3.1 多项式的最大公因子和最小公倍式.

定义: (i) 设 $f, h \in F[x]$ 且 $h \neq 0$. 如果存在 $q \in F[x]$ 使得 $f = qh$. 则称 h 整除 f
记为 $h \mid f$

(ii) 再设 $g \in F[x]$. 如果 $h \mid f$ 且 $h \mid g$
则称 h 是 f 和 g 的公因子

(iii) 设 h 是 f 和 g 的公因子. 如果
$\forall$ f 和 g 的公因子 p 都有 $p \mid h$
则称 h 是 f 和 g 的最大公因子

例:

引理3.1 ~~设 $a, b \in \mathbb{Z}$, d~~ 设 $f, g \in F[x]$, $a, b \in F[x]$
h 是它们的公因子.
则 $h \mid (af+bg)$

证: 与第一章引理3.1 类似.

问题 $f, g \in F[x] \setminus \{0\}$. 计算 f, g 的最大公因子.

令 $r_0 = f$, $r_1 = g$ 由带余除法

$$r_0 = q_2 r_1 + r_2 \qquad \deg(r_1) > \deg(r_2)$$
$$r_1 = q_3 r_2 + r_3 \qquad \deg(r_2) > \deg(r_3)$$
$$\vdots$$
$$r_{k-2} = q_k r_{k-1} + r_k \qquad \deg(r_{k-1}) > \deg(r_k)$$
$$0$$
$$r_{k-1} = q_{k+1} r_k$$

断言 r_k 是 f 和 g 的最大公因子

断言的证明

$$r_k \mid r_{k-1} \xRightarrow[\text{引理3.1}]{} r_k \mid r_{k-2} \xRightarrow[\substack{\text{引理3.1} \\ r_k \mid r_{k-1}}]{} r_k \mid r_{k-3}$$

$$\Rightarrow \cdots \Rightarrow r_k \mid r_1 \Rightarrow r_k \mid r_0$$

于是 r_k 是 f 和 g 的公因子.

设 p 是 f, g 的公因子

$p \mid r_0,\ p \mid r_1 \xRightarrow{\text{引理3.1}} p \mid r_2 \xRightarrow{\text{引理3.1}} p \mid r_3 \Rightarrow \cdots \Rightarrow p \mid r_k$

于是 r_k 是 f 和 g 公因子.

~~定~~: 定义: 设 $a, b \in F[x]$. 如果 $\exists \lambda \in F\setminus\{0\}$
~~使得~~ 使得 $a = \lambda b$. 则称 a. b 相伴
记为 $a \sim_F b$.

证 "$\sim_F$" 是等价关系.

命题3.1. 设 $f, g \in F[x]\setminus\{0\}$, h 是 f 和 g 的最大公因子. ~~如果 a 也~~ 则 $a \in F[x]$
f 和 g 的最大公因子 $\Leftrightarrow$ ~~则~~ $a \sim_F h$

证: $\Leftarrow$ 设 $a = \lambda h$. 其中 $\lambda \in F\setminus\{0\}$

$\because \exists\ u, v \in F[x]$

$f = uh \quad g = vh$

$\therefore f = \lambda^{-1} u a \quad g = \lambda^{-1} v a$

于是 a 也是 f 和 g 的公因子

设 b 是 f 和 g 的公因子

则 $\exists\ w \in F[x]$ 使得 $h = wb$

$a = \lambda h = (\lambda w) b \Rightarrow b \mid a$

所以 a 是 f, g 的最大公因子.

"$\Rightarrow$" $a \mid h$ 且 $h \mid a \Rightarrow \deg h = \deg a$.
于是 $a = \lambda h$ 其中 $\lambda \in F\setminus\{0\}$ ▨

记号: 设: $f, g \in F[x]\setminus\{0\}$. 记 f 和 g 中首项系数为1
$\gcd(f, g)$ 的最大公因子.

定理3.1 (Bezout's relation) 设 $f, g \in F[x]\setminus\{0\}$
则存在 $u, v \in F[x]$ 使得

$$uf + vg = \gcd(f, g)$$

证 (优雅版)

设 $S = \{af + bg \mid a, b \in F[x]\}$

设 $h \in S\setminus\{0\}$ 且 $\deg(h)$ 最小

令 $h = uf + vg$ 其中 $u, v \in F[x]$

如果 $h \nmid f$. 则由带余除法.

$f = gh + r \quad r \neq 0.\ \deg(r) < \deg h$

$$r = f - gh = f - g(uf+vg)$$

$$= (1-gu)f + (-gv)g \in S$$ 矛盾

于是 $h \mid f$. 同理 $h \mid g$.

设 $a \mid f$ 且 $a \mid g$. 由引理 3.1 $a \mid h$

于是 h 是 f, g 的最大公因子

$$\gcd(f,g) = lc(h)^{-1} h = (lc(h^{-1})u) f + (lc(h^{-1})v) g$$ 得

定义：设 $f, g \in F[x]\setminus\{0\}$, 如果 $\gcd(f,g)=1$, 则称 f 与 g 互素.

定理 3.2 设 $f, g \in F[x]\setminus\{0\}$, 则

f, g 互素 $\Longleftrightarrow \exists\, u, v \in F[x]$, 使得

$$uf + vg = 1.$$

证 与第一章定理 8.2 类似.

注：关于最小公倍式有类似第一章第8节的讨论 这里略去.

多项式 Bezout 关系在线性代数中的应用.

~~命题 8.2~~ 设 $A \in M_n(F)$, V_A 代表 $A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ 的解空间

~~命题~~ 8.2 设 $f, g \in F[x]\setminus\{0\}$, $\gcd(f,g)=1$

$A \in M_n(F)$, 则

$$V_{f(A)g(A)} = V_{f(A)} \oplus V_{g(A)}$$

证：由定理 8.2, $\exists\, u, v \in F[x]$

$$uf + vg = 1$$

于是 $u(A)f(A) + v(A)g(A) = E$ (命题 2.3)

$\forall\, \vec{w} \in V_{f(A)g(A)}$,

$$\vec{w} = \underbrace{u(A)f(A)\vec{w}}_{\vec{w}_1} + \underbrace{v(A)g(A)\vec{w}}_{\vec{w}_2}$$

$$g(A)\vec{w}_1 = g(A)u(A)f(A)\vec{w} = u(A)g(A)f(A)\vec{w} = \vec{0}$$

$$\vec{w}_1 \in V_{g(A)}$$

同理 $\vec{w}_2 \in V_{f(A)}$

于是 $\vec{w} = \vec{w}_1 + \vec{w}_2 \in V_{g(A)} + V_{f(A)}$

~~再之 设 $\vec{w} \in V_{f(A)} + V_{g(A)}$~~

即 $V_{f(A)g(A)} \subset V_{f(A)} + V_{g(A)}$

反之 $V_{f(A)} \subset V_{f(A)g(A)}$, $V_{g(A)} \subset V_{f(A)g(A)}$

所以 $V_{f(A)} + V_{g(A)} \subset V_{f(A)g(A)}$

由此得出 $V_{f(A)g(A)} = V_{f(A)} + V_{g(A)}$

设 $\vec{w} \in V_{f(A)} \cap V_{g(A)}$

$$\vec{w} = u(A)f(A)\vec{w} + v(A)g(A)\vec{w} = \vec{0}$$

于是 $V_{f(A)g(A)} = V_{f(A)} \oplus V_{g(A)}$ □

推论8.1 由命题8.1中记号

$$\operatorname{rank}(f(A)) + \operatorname{rank}(g(A)) = n + \operatorname{rank}(f(A)g(A))$$

证: 由命题8.1和维数公式

$$\dim V_{f(A)g(A)} = \dim V_{f(A)} + \dim V_{g(A)}$$

$$n - \operatorname{rank}(f(A)g(A)) = n - \operatorname{rank}(f(A)) + n - \operatorname{rank}(g(A))$$

$$\Rightarrow \operatorname{rank}(f(A)) + \operatorname{rank}(g(A)) = n + \operatorname{rank}(f(A)g(A))$$

例: 设 σ 为 $\mathbb{R}^n \to \mathbb{R}^n$ 线性映射且满足 $\sigma^2 = \sigma$

求证: $\mathbb{R}^n = \ker(\sigma) \oplus \operatorname{im}(\sigma)$

证: 设 A 为 σ 的矩阵表示, 则 $A^2 = A$

令 $p = x^2 - x = \underbrace{x}_{f}\underbrace{(x-1)}_{g}$, $\gcd(f,g) = 1$

由命题8.2 $V_{p(A)} = V_A \oplus V_{A-E}$ (*)

$$\mathbb{R}^n = V_A \oplus V_{A-E}$$

$V_A = \ker(\sigma)$. 设 $\vec{x} \in V_{A-E}$

$(A - E)(\vec{x}) = \vec{0} \Rightarrow \vec{x} = A\vec{x} \Rightarrow$

$\vec{x} \in \operatorname{Im}(\sigma)$

设 $\vec{v} \in \operatorname{im}(\sigma)$. $\exists\, \vec{u} \in \mathbb{R}^n$

$\vec{v} = A\vec{u} \Rightarrow A\vec{v} = A^2\vec{u} = A\vec{u} = \vec{v}$

$\Rightarrow (A-E)(\vec{v}) = \vec{0} \Rightarrow \vec{v} \in V_{A-E}$

于是 $V_{A-E} = \operatorname{im}(\sigma)$. 由(*).

$\mathbb{R}^n = \ker(\sigma) \oplus \operatorname{im}(\sigma)$ □

~~定义~~ ~~设~~

例：设 $A\in M_n(\mathbb{R})$ 且 $A^2=E$．证明
$\mathrm{rank}(A+E)+\mathrm{rank}(A-E)=n$．

证：设 $p=x^2-1=\underbrace{(x-1)}_{f}\underbrace{(x+1)}_{g}$，$\gcd(f,g)=1$

$P(A)=O_{n\times n}$　$V_p=V_f\oplus V_g$

由推论3.1　$n+\mathrm{rank}(P(A))=\mathrm{rank}(A+E)+\mathrm{rank}(A-E)$
$\quad\quad\quad \| \quad n$

$\boxed{/}$

§3.2 F[x] 中的因式分解．

定义：设 $f\in F[x]\setminus\{0\}$．如果 f 不能写成 F[x] 中两个次数低于 f 的多项式之积，则称 f 是 F[x] 中的不可约元（不可约多项式）

注：$F\setminus\{0\}$ 的元素显然是不可约的，称为平凡不可约元

引理~~命题~~ 3.2　设 $f\in F[x]\setminus\{0\}$．则 f 是若干个不可约元之积

证：设 $d=\deg(f)$．对 d 归纳．
$d=0$，$d=1$ 显然．
设 ~~f(x)次数~~ 命题对小于 d 次的多项式成立
若 f 本身不可约．则无需再证．
否则　$f=gh$．　$g,h\in F[x]$　$\deg(g)<d$
$\deg(h)<d$．由归纳假设
g,h 都是不可约多项式之积．
于是 f 也是

$\boxed{/}$

引理3.3．设 $f,g,h\in F[x]$．f 不可约
如果 $f\mid gh$，则 $f\mid g$ 或 $f\mid h$．

证：设 $f\nmid g$．令 $a=\gcd(f,g)$
则 $a\mid f$．因为 f 不可约，所以
$a\sim_F f$ 或 ~~$a\sim_F$~~ $a=1$．
若 $a\sim_F f$．则 $f\mid g$ $\rightarrow\leftarrow$
于是 $a=1$．$\exists\, u,v\in F[x]$　$uf+vg=1$（定理3.2
$ufh+vgh=h$．

$\because$ $f_1 | fh$, $f_2 | gh$

$\therefore$ $f | h$ $\boxtimes$

定理 3.3. 设 $f \in F[x] \setminus F$

则存在非零不可约元 $p_1, \cdots p_m$ 使得

$$f = p_1 \cdots p_m. \qquad (*)$$

如果 $f = g_1 \cdots g_n$，其中 $g_1, \cdots g_n$ 是非零不可约元，则 $m = n$. 且在适当调整下标后，我们有

$$p_1 \sim_F g_1, \quad \cdots, \quad p_m \sim g_m$$

证：(*) 由引理 3.2 给出.

由 $g_1 \cdots g_n = p_1 \cdots p_m$

由重复应用引理 3.3. 可知

$\exists\, i \in \{1, \cdots m\}$ 使得 $g_1 | p_i$.

不妨设 $i=1$.

因为 g_1, p_1 都是非零不可约元

所以 $g_1 \sim p_1$ 设 $g_1 = \lambda_1 p_1$. $\lambda_1 \in F$

则 $g_2 \cdots g_n = \lambda_1 (p_2 \cdots p_m)$

重复应用上述推理过程，和调整下标得

$g_2 \sim_F p_2, \cdots, g_n \sim_F p_n$ 且

$1 = \lambda_1 \cdots \lambda_n\, p_{n+1} \cdots p_m$，其中 $\lambda_1, \cdots \lambda_n \in F$

$\Rightarrow m = n.$ $\boxtimes$

推论 3.2 设 $f \in F[x] \setminus F$，则存在唯一 $\lambda \in F$. 两两互不相伴的非零不可约元，首一，

$p_1, \cdots p_k,$

和正整数 $m_1, \cdots m_k$. 使得

$$f = \lambda p_1 \cdots p_k$$

注：$f \in F[x]$ 称为首一的. 如果它的首项系数是 1.

证：由 (*). 设 $\tilde{p}_i = lc(p_i)^{-1} p_i$.

则 $f = \lambda \tilde{p}_1 \cdots \tilde{p}_m$ 其中 $\tilde{p}_1, \cdots \tilde{p}_m$ 都是首一，非零的不可约元. 于是若

$\tilde{p}_i \sim_F \tilde{p}_j \Rightarrow \tilde{p}_i = \tilde{p}_j$

不妨设 $\tilde{p}_1, \cdots \tilde{p}_k$ 两两不相伴.

而 $\forall j \in \{k+1, \dots, m\}$, $\exists i \in \{1, \dots, k\}$ 使得

$$\tilde{p}_j \sim_F \tilde{p}_i$$

即 $\tilde{p}_j = \tilde{p}_i$

则 $\exists\, m_1, \dots, m_k \in \mathbb{Z}^+$, 使得

$$f = \lambda \tilde{p}_1^{m_1} \cdots \tilde{p}_k^{m_k}$$

唯一性由定理3.3直接得出

注: 类似地，我们可以证明算术基本定理. 即 $\forall n \in \mathbb{Z}^+ \setminus \{1\}$. 存在唯一的素数

$p_1, \dots, p_k$ 和 $m_1, \dots, m_k \in \mathbb{Z}^+$

使得 $n = p_1^{m_1} \cdots p_k^{m_k}$

证明思路

引理3.4 对应于第一章定理8.4

引理3.3 对应于第一章§8 例题第二个例子.

相伴意味着相等 $\square$

§3.3 整数环上的Gauss引理.

定义: 设 $a_1, a_2, \dots a_m \in \mathbb{Z}$, $d \in \mathbb{Z} \setminus \{0\}$

(i) 如果 $d | a_1, d | a_2, \dots d | a_m$, 则称 d 是 $a_1, a_2, \dots a_m$ 的公因子

(ii) 设 d 是 $a_1, a_2, \dots a_m$ 的公因子.

~~如果~~ g 是 $a_1, a_2, \dots a_m$ 的任意公因子

如果 $d | g$. 则称 g 是 $a_1, \dots a_m$ 是 $a_1, a_2, \dots a_m$ 的最大公因子.

$a_1, a_2 \dots a_m$ 的最大正公因子记为 $\gcd(a_1, a_2, \dots a_m)$

定义: 设 $f \in \mathbb{Z}[x] \setminus \{0\}$. $\deg f = d$

$$f = f_d x^d + f_{d-1} x^{d-1} + \dots + f_0,$$

$$f_i \in \mathbb{Z}$$

$\gcd(f_d, f_{d-1}, \dots f_0)$ 称为 f 的容数

记为 ~~content~~ $\mathrm{cont}(f)$.

如果 $\mathrm{cont}(f) = 1$, 则称 f 是本原的

$$f = \mathrm{cont}(f) \cdot \tilde{f}$$

其中 $\tilde{f} \in \mathbb{Z}[x]$. 本原 称为 f 的本原部分, 记为pp(f)

Gauss引理 设 $f, g \in \mathbb{Z}[x]$ 都是本原的

则 fg 也是本原的

证：设 $f = f_d x^d + f_{d-1}x^{d-1} + \cdots + f_0$

$g = g_e x^e + g_{e-1}x^{e-1} + \cdots + g_0$

假设 $\mathrm{cont}(fg) \neq 1$. 则 $\exists$ ~~素~~数 p, $p \mid \mathrm{cont}(fg)$

因为 $\mathrm{cont}(f)=1$, 所以 $\exists\, i \in \{0,1,\ldots,d\}$, 使得

$p \mid f_d, \ldots, p \mid f_{i+1}$ 但 $p \nmid f_i$

同理 $\exists\, j \in \{0,1,\ldots,e\}$ 使得

$p \mid g_e, \ldots, p \mid g_{j+1}$ 但 $p \nmid g_j$

设 c 是 fg 中 x^{i+j} 的系数，则

$$c = \sum_{l+m=i+j} f_l g_m$$

当 $l > i$ 时 $p \mid f_l \Rightarrow p \mid f_l g_m$

当 $l < i$ 时，$m > j \Rightarrow p \mid g_m \Rightarrow p \mid f_l g_m$

$\because p \mid c \quad \therefore p \mid f_i g_j$

$\Rightarrow p \mid f_i$ 或 $p \mid g_j$ （见第一章§8. 倒数第2个引理）

矛盾 $\square$

引理 3.4 设 $a_1, \ldots, a_m, t \in \mathbb{Z}\setminus\{0\}$

则 $|t| \gcd(a_1,\ldots,a_m) = \gcd(ta_1,\ldots,ta_m)$

证：设 $b = \gcd(a_1,\ldots,a_m)$, $c = \gcd(ta_1,\ldots,ta_m)$

我们要证：$|t|\, b = c$

$\forall i \in \{1,\ldots,m\}$ $b \mid a_i \Rightarrow tb \mid ta_i$

$\Rightarrow tb \mid c \Rightarrow \exists u \in \mathbb{Z}$, $c = tbu$

由 $c \mid ta_i \Rightarrow ta_i = v_i c$, $v_i \in \mathbb{Z}$

$= v_i t b u$

$a_i = v_i b u \Rightarrow bu \mid a_i \Rightarrow bu \mid b$

$\Rightarrow u = \pm 1$

$\Rightarrow c = \pm tb$ $\square$

定理

设 $f \in \mathbb{Z}[x]\setminus\mathbb{Z}$ 如果 $f = gh$, 其中 $g, h \in \mathbb{Z}[x]$

$\deg g < \deg(f)$, $\deg h < \deg f$

则称 f 在 $\mathbb{Z}$ 上可约. 否则称 f 在 $\mathbb{Z}$ 上不可约

定理3.6 设 $f \in \mathbb{Z}[x]$. 如果 f 在 $\mathbb{Z}[x]$ 中不可约，则 f 在 $\mathbb{Q}[x]$ 中也不可约

<u>证:</u> 设 f 在 $\mathbb{Q}[x]$ 中可约，则 $\exists\, g, h \in \mathbb{Q}[x]$

使得 $f = gh$. * $\deg g < \deg f$, $\deg h < \deg f$

对系数清分母后 和约去本原，有整数 u, v，使得

$$uf = v g_0 h_0$$

其中 $g_0, h_0 \in \mathbb{Z}[x]$ 本原，$\deg g_0 = \deg g$

$\deg h_0 = \deg h$，且 $\gcd(u,v)=1$，$u>0$

于是 $u\,\mathrm{cont}(f)\,\mathrm{pp}(f) = v g_0 h_0$

令 $s = g_0 h_0$. 由 Gauss 引理，s 本原

令 $a = vs$ 则

$\mathrm{cont}(a) = v = u\,\mathrm{cont}(f)$ （引理 3.4）

于是 $u \mid \cancel{\mathrm{cont}}\ v \Rightarrow u = 1$

$$f = (v g_0) h_0.$$

f 在 $\mathbb{Z}$ 上可约. $\rightarrow\leftarrow$ ☒

定理3.7 （Eisenstein 判别法）

设 $f = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$

p 是素数. 如果 $p \mid f_{n-1}, \ldots, p \mid f_1$, ~~但~~, $p \mid f_0$

但 $p^2 \nmid f_0$ 则 f 在 $\mathbb{Q}[x]$ 中不可约.

Pf 假设 f 在 $\mathbb{Q}[x]$ 中可约，则由定理3.6

f 在 $\mathbb{Z}[x]$ 中可约. 于是存在

$g, h \in \mathbb{Z}[x]$ 首一 （因为 f 首一）

$\deg g = d > 0$　$\deg h = n-d > 0$ 使得

$$f = gh$$

令 $g = x^d + g_{d-1}x^{d-1} + \cdots + g_0$,　$h = x^{n-d} + h_{n-d-1}x^{n-d-1} + \cdots + h_0$

我们有

$$(*)\quad x^n + f_{n-1}x^{n-1} + \cdots + f_0 = (x^d + g_{d-1}x^{d-1} + \cdots + g_0)(x^{n-d} + h_{n-d-1}x^{n-d-1} + \cdots + h_0)$$

令 $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$, $m \mapsto \bar{m}$ 是自然投射

$\tilde{\pi}_p : \mathbb{Z} \to \mathbb{Z}_p[x]$ 环同态, $m \to \bar{m}$

$\exists\ \tilde{\pi}_{p,x} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ 环同态

$\tilde{\pi}_{p,x}|_{\mathbb{Z}} = \pi_p$.　$\tilde{\pi}_{p,x}(x) = x$.

于是 $\widetilde{\pi}_{p,x}(f) = \overline{\pi_{p,x}}(g.h)$

由 (*)

$$x^n + \overline{f_{n-1}}x^{n-1} + \cdots + \overline{f_0} = (x^{d} + \overline{g_{d-1}}x^{d-1} + \cdots + \overline{g_0})(x^{n-d} + \overline{h_{n-d-1}}x^{n-d-1} + \cdots + \overline{h_0}) = 0$$

$\Rightarrow \overline{g_0} = \overline{h_0} = 0 \Rightarrow p \mid g_0,\ p \mid h_0$

$\because f_0 = g_0 h_0 \quad \therefore p \mid f_0 \rightarrow\leftarrow$ ▨

例：$\forall n \in \mathbb{Z}^+$，$x^n + 2x + 2$ 在 $\mathbb{Q}[x]$ 中不可约

例：设 p 是素数，证明

$f(x) = x^p + x^{p-1} + \cdots + 1$ 在 $\mathbb{Q}[x]$ 中不可约.

$\varphi: \mathbb{Q}[x] \to \mathbb{Q}[x]$

$\varphi|_{\mathbb{Q}} = id \quad \varphi(x) = x+1$

是同构. $\because \varphi^{-1}: x \to x-1$

于是只要证 $f(x+1)$ 不可约

注意到 $f(x) = \dfrac{x^p - 1}{x-1}$

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}$$

$\because p \mid \binom{p}{1},\ p \mid \binom{p}{2}, \ldots\ p \mid \binom{p}{p-1}$

但 $p^2 \nmid \binom{p}{p-1} = p$ 　于是 $f(x+1)$ 不可约

于是 f 在 $\mathbb{Q}[x]$ 不可约.

例：$x^2 - 2$ 在 $\mathbb{Q}[x]$ 上不可约 $(\because \sqrt{2} \notin \mathbb{Q})$

但 $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ 　$x^2 - 2$ 在 $\mathbb{R}[x]$ 上可约.

$x \pm \sqrt{2} \in \mathbb{R}[x]$