1. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$, 若 $\alpha=\frac{k}{l}\in\mathbb{Q}$, $\gcd(k,l)=1$ 为其根, 证明: $k\mid a_0$ 且 $l\mid a_n$.

$k,l\in\mathbb{Z}$ "有理根定理"

证明:

法1: 由 $f(\alpha)=0$ 可得: $a_n(\frac{k}{l})^n+\cdots+a_1(\frac{k}{l})+a_0=0$

等式两边同时乘 l^n 得: $a_nk^n+a_{n-1}k^{n-1}l+\cdots+a_1kl^{n-1}+a_0l^n=0$

那么 $k\mid a_0l^n$ 且 $l\mid a_nk^n$

$a\mid bc$, $\gcd(a,b)=1\Rightarrow a\mid c$.

$\because \gcd(k,l)=1$ $\therefore \gcd(k,l^n)=1 \overset{k\mid a_0l^n}{\Longrightarrow} k\mid a_0$

$\gcd(l,k^n)=1 \overset{l\mid a_nk^n}{\Longrightarrow} l\mid a_n$

法2: 在 $\mathbb{Q}(x)$ 中 $x-\frac{k}{l}\mid f(x)$

从而在 $\mathbb{Z}[x]$ 中, $lx-k$ 是本原多项式, $lx-k\mid f(x)$ (参见定理6.32的证明)

设 $f(x)=(lx-k)(b_{n-1}x^{n-1}+\cdots+b_1x+b_0)$ 其中 $b_i\in\mathbb{Z}$.

故 $a_0=-kb_0$, $a_n=lb_{n-1}$ 可见 $k\mid a_0$ 且 $l\mid a_n$.

注: 有理根定理只是必要条件, 不是充分条件.

2. 设 D 是 UFD, $a, b_1, \ldots b_n \in D^*$. 证明: 如果 $\gcd(a, b_i) = 1$, $i = 1 \ldots n$, 则

$$\gcd(a, b_1 \ldots b_n) = 1.$$

证明: 反证法: 假设 $\gcd(a, b_1 \cdots b_n) \neq 1$.

任取 a 和 $b_1 \cdots b_n$ 的不可约公因子 p. p 也是素元.

$p \mid a$ 且 $p \mid b_1 \cdots b_n$ 由素元的性质 $\exists i$ st. $p \mid b_i$

即 $p \mid \gcd(a, b_i) \Rightarrow \gcd(a, b_i) \neq 1 \rightarrow\leftarrow$ 口

注: 1. 要求 $\gcd(a, b_1 \cdots b_n)$, 不是 $\gcd(a, b_1, \cdots, b_n)$

2. 典型错误:

设 $\gcd(a, b_1 \cdots b_n) = g \neq 1$ 那么 $g \mid a$ 且 $g \mid b_1 \cdots b_n$ ~~$\Rightarrow$~~ $\exists i$ st. $g \mid b_i$

$6 \mid 2 \cdot 3$ 但 $6 \nmid 2$, $6 \nmid 3$

$\min\{n_1, n_2+n_3\} = \min\{n_1, n_2\} + \min\{n_1 - \min\{n_1, n_2\}, n_3\}$.

$p^{n_1} \quad p^{n_2} \cdot p^{n_3}$

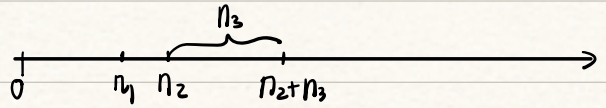
$\gcd(a, b\cdot c) = \gcd(a,b)\cdot \gcd\left(\frac{a}{\gcd(a,b)}, c\right)$

~~$\gcd(a,b\cdot c) = \frac{\gcd(a,b)\cdot \gcd(a,c)}{\gcd(a,b,c)}$~~.

分类讨论：

1°：

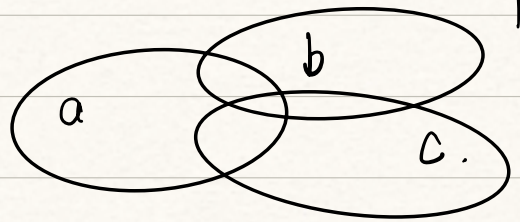
2°：



3°：

3^5 $3^3\cdot 3^3$ $\frac{3^3\cdot 3^3}{3^3}$

用韦恩图不准确.



3. 判断整系数多项式 x^2+4, x^3+4, x^4+4 和 $x^5+12x^3+36x+12$ 在 $\mathbb{Q}[x]$ 中是否不可约.

解：由题 1. 若 x^2+4 在 $\mathbb{Q}[x]$ 中有一次因式，则其有理根 $\alpha=\frac{k}{l}$ 满足 $k|4, l|1$

即 $\alpha\in\mathbb{Z}$，易验证 x^2+4 没有整数根，故 x^2+4 在 $\mathbb{Q}[x]$ 中不可约.

同理 x^3+4 在 $\mathbb{Q}[x]$ 中不可约. 另：$f(x-1)=(x-1)^3+4=x^3-3x^2+3x+3$ 取 $p=3$ 由 Eisenstein 判别法 √.

假设 x^4+4 在 $\mathbb{Q}[x]$ 中可约，则 x^4+4 在 $\mathbb{Z}[x]$ 中可约.

又 x^4+4 无整数根，故 x^4+4 无一次因式.

设 $x^4+4=(x^2+ax+b)(x^2+cx+d)$，其中 $a,b,c,d\in\mathbb{Z}$.

[x^0] [x^1] [x^2] [x^3]

那么 $bd=4$, $ad+bc=0$, $d+ac+b=0$, $c+a=0$

$\Rightarrow bd=4$, $d-b=0$, $d-a^2+b=0$, $a+c=0$.

$\Rightarrow b=d=2$, $a=\pm2$, $c=\mp2$.

即 $x^4+4=(x^2+2x+2)(x^2-2x+2)$. 另：$x^4+4=(x^2+2)^2-(2x)^2$

$x^5+12x^3+36x+12$ 在 $\mathbb{Q}[x]$ 中不可约.

由 Eisenstein 判别法：取 $p=3$，$3\mid 12$，$3\mid 36$，$3\nmid 1$ 且 $3^2\nmid 12$.

4. 已知 $f(x)=x^p-x-1$ 在 $\mathbb{Z}_p[x]$ 中不可约，其中 p 为素数. 证明:

$$f(x)=x^p-x-1 \text{ 和 } g(x)=x^p+(p-1)x+p-1$$

在 $\mathbb{Q}[x]$ 上不可约.

Berlekamp算法

提示: 利用环同态:

$$\begin{array}{rccc} \phi_p: & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x] \\ & \sum_i a_i x^i & \mapsto & \sum_i \bar{a}_i x^i. \end{array}$$

证明: 断言: 若 $h(x)\in\mathbb{Z}[x]$ 首一 且 $h(x)$ 在 $\mathbb{Q}[x]$ 中可约. 则 $\phi_p(h)$ 在 $\mathbb{Z}_p[x]$ 中可约.

断言的证明:

由Gauss引理的推论(定理6.32) $h(x)$ 可写成两个 $\mathbb{Z}[x]$ 中正次数多项式之积.

设 $h(x)=u(x)\cdot v(x)$ 由环同态: $\phi_p(h)=\phi_p(u)\cdot\phi_p(v)$.

$\because \deg(\phi_p(u))=\deg(u)$, $\deg(\phi_p(v))=\deg(v)$. $\phi_p(u)$ 和 $\phi_p(v)$ 都不是可逆元.

$\therefore \phi_p(h)$ 在 $\mathbb{Z}_p[x]$ 中可约.

由 $\phi_p(f(x))=x^p-x-1$. $\phi_p(g(x))=x^p-x-1$. 以及 x^p-x-1 在 $\mathbb{Z}_p[x]$ 中不可约.

那么 $f(x)$ 和 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

注：

(1) 反之不成立：取 $h(x)=x^2+1$ 则 $h(x)$ 在 $\mathbb{Z}_2[x]$ 中可约，但在 $\mathbb{Q}[x]$ 中不可约.

"$\varphi_p(Lc(h))\neq 0$" $2x^2+3x+1=(2x+1)(x+1)\in\mathbb{Q}[x]$. $\varphi_2(2x^2+3x+1)=x+1$ 不可约.

(2) 更正习题课讲义一：$f(x)\in F[x]$, $f(x)$ 有重因式 $\Leftrightarrow \gcd(f(x),f'(x))=1$ 在任意数域 F 中都成立.

但在特征为 p 时，只是证明需要修正.

(3) 环同态的应用：

证明 Gauss 引理：设 $f(x),g(x)\in\mathbb{Z}[x]$ 本原多项式. 证明 $h(x)=f(x)\cdot g(x)$ 是本原多项式.

假设 $h(x)$ 各项系数有公共的素因子 p. 那么 $\varphi_p(h)=0$.

又 $\varphi_p(h)=\varphi_p(f)\cdot\varphi_p(g)$.

$\because f$ 和 g 都是本原多项式 $\therefore \varphi_p(f)\neq 0$, $\varphi_p(g)\neq 0$ $\rightarrow\leftarrow$

思考：用环同态 φ_p 证明 Eisenstein 判别法.

(4) 环同构保持(不)可约性 e.g. $\psi_n:\mathbb{Z}[x]\to\mathbb{Z}[x]$ $\forall n\in\mathbb{Z}$.

$$f(x)\mapsto f(x+n)$$

回忆证明 $x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbb{Q}[x]$ 中不可约

(5) $f(x)\in\mathbb{Z}[x]$. 若 $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约，那么 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约. (不需要 $f(x)$ 是本原多项式)

若 $f(x)$ 在 $\mathbb{Q}[x]$ 上不可约，那么 $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约. (需要 $f(x)$ 是本原多项式)

$2x$ 不是本原多项式 $\gcd(2,0)=2$.

5. 设 $f(x)$ 是无穷阶可导的实函数, 其导数记为 f', k 阶导数记为 $f^{(k)}$.

(a) 设 $f \in \mathbb{R}[x]$. 证明: f, f', f'' 在 $\mathbb{R}$ 上线性无关当且仅当 $\deg(f) \geq 2$.

(b) 设 $f(x) = x^2 e^x$. 求最小正整数 n 使得 $f, f', \ldots, f^{(n)}$ 在 $\mathbb{R}$ 上线性相关.

(a) 证明: 充分性: 若 $\deg(f) \geq 2$. 设 $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$ 其中 $n \geq 2$. $a_n \neq 0$.

则 $f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$, $\deg(f') = n-1$. $f'' = n(n-1) a_n x^{n-2} + \cdots + 2a_2$. $\deg(f'') = n-2$.

设 $c_0, c_1, c_2 \in \mathbb{R}$ 使得 $c_0 f + c_1 f' + c_2 f'' = 0$.

$\Rightarrow c_0 \cdot a_n = 0 \Rightarrow c_0 = 0 \Rightarrow c_1 f' + c_2 f'' = 0$.

$\Rightarrow c_1 \cdot n \cdot a_n = 0 \Rightarrow c_1 = 0 \Rightarrow c_2 \cdot f'' = 0 \Rightarrow c_2 = 0$.

故 f, f', f'' 在 $\mathbb{R}$ 上线性无关.

证明 $f_1, \ldots, f_n$ 在 F 上线性无关的范式:

设 $\lambda_1, \ldots, \lambda_n \in F$ s.t. $\lambda_1 f_1 + \cdots + \lambda_n f_n = 0$

那么 $\lambda_1 = \cdots = \lambda_n = 0$.

必要性: 若 $\deg(f) < 2$. 则可设 $f = a_1 x + a_0 \in \mathbb{R}[x]$.

$f' = a_1$, $f'' = 0$. 那么 f, f', f'' 一定在 $\mathbb{R}$ 上线性相关.

(b) 由 $f(x) = x^2 e^x$. 得: $f'(x) = (x^2 + 2x) \cdot e^x$. $f''(x) = (x^2 + 4x + 2) \cdot e^x$. $f'''(x) = (x^2 + 6x + 6) \cdot e^x$.

$$f'''(x) - 3f''(x) + 3f'(x) - f(x) = 0$$

但 $f(x), f'(x), f''(x)$ 在 $\mathbb{R}$ 上线性无关

故 n 最小取 3.

$$\begin{array}{c} f \quad f' \quad f'' \quad f''' \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 6 \\ 0 & 0 & 2 & 6 \end{pmatrix} \end{array}$$

2. 商空间

V 是 F 上的线性空间，W_1, W_2 是 V 的子空间，$\alpha \in V$，若 $\alpha + W_1 = W_2$ 则 $\alpha \in W_1$，$W_1 = W_2$.

证明：注意到 $0 \in W_2$，那么 $0 = \alpha + (-\alpha)$，$-\alpha \in W_1 \Rightarrow \alpha \in W_1$，$W_1 = W_2$

注：上述结论对 $\mathrm{char}F$ 没有限制，习题课上讲的证明是对 $\mathrm{char}(F)=0$ 成立，上述证明为更正版。

推论：$\alpha_1, \alpha_2 \in V$，$\alpha_1 + W_1 = \alpha_2 + W_2$，那么 $W_1 = W_2$，$\alpha_1 - \alpha_2 \in W_1$

3. 空间的直和

$W = V_1 \oplus V_2 \oplus \cdots \oplus V_k$，那么 $\forall \alpha \in W$ 可唯一地表示为 $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_k$，$\alpha_i \in V_i$.

从而映射 $\pi_i : \alpha \mapsto \alpha_i$ 是 W 上的线性算子且 $\pi_1 + \cdots + \pi_k = \mathcal{E}$.

当 $i \neq j$ 时 $\pi_i \pi_j = 0$，$\pi_i^2 = \pi_i$.

反之也成立，设 $\pi_1, \cdots, \pi_k : W \to W$ 是满足下列条件的有限个线性映射的集合：

$$\sum_{i=1}^{k} \pi_i = \mathcal{E},\ \pi_i^2 = \pi_i,\ 1 \le i \le k;\ \pi_i \pi_j = 0,\ i \neq j$$ 正交的等方算子组.

那么 $W = V_1 \oplus \cdots \oplus V_k$ 其中 $V_i = \mathrm{Im}\,\pi_i$

证明：$\forall \alpha \in W$，$\alpha = \pi_1(\alpha) + \cdots + \pi_k(\alpha) \Rightarrow W \subseteq V_1 + \cdots + V_k$

又因为 $V_i = \mathrm{Im}\,\pi_i$ 是 W 的子空间，故 $V_1 + \cdots + V_k \subseteq W$.

$W = V_1 + \cdots + V_k$.

$\forall i = 1, \cdots, k$ 设 $x \in V_i \cap \sum_{j \neq i} V_j$. $x = \pi_i(x_i) = \sum_{j \neq i} \pi_j(x_j)$

在等式两边同时作用 π_i 可得: $\pi_i(x_i) = x = 0$.

因此 $V_i \cap \sum_{j \neq i} V_j = \{0\}$. 即 $W = V_1 \oplus \cdots \oplus V_k$.