回忆

1. Gauss引理：本原多项式之积仍本原

2. 定理：整系数多项式在 $\mathbb{Z}[x]$ 不可约 $\Rightarrow$ 它在 $\mathbb{Q}[x]$ 中也不可约

3. Eisenstein判别法：一个首一整系数多项式的非首项系数都被某个素数 p 整除，但尾项系数不被 p^2 整除，则该多项式在 $\mathbb{Q}$ 上不可约

注：$f \in F[x] \setminus \{0\}$ 称为首一的，如果

$$lc(f) = 1.$$

例：~~设 p 是素~~ 设 $n>1$. 证明

$$x^n + 2x + 2$$

在 $\mathbb{Q}[x]$ 中不可约.

证：$2|2$，$2|2$ 但 $2^2 \nmid 2$.

由 Eisenstein 判别法. x^2+2x+2 不可约

例：设 p 是素数，证明

$$f = x^{p-1} + x^{p-2} + \cdots + 1$$

在 $\mathbb{Q}[x]$ 中不可约.

证：$f(x) = \dfrac{x^p - 1}{x-1} \Rightarrow f(x+1) = \dfrac{(x+1)^p - 1}{x}$

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

$$= x^{p-1} + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-2}x^2 + \binom{p}{p-1}$$

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

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

$$\begin{tikzcd}
\mathbb{Q}[x] \arrow[dr, "\varphi_{x+1}\ \ x \mapsto x+1"] & \\
\mathbb{Q} \arrow[u] \arrow[r] & \mathbb{Q}[x]
\end{tikzcd}$$

~~$\mathbb{Q}[x]$~~

φ_{x+1} 是同态

同理 φ_{x-1} 也是同态

$\forall g \in \mathbb{Q}[x]$ $\quad \varphi_{x+1} \circ \varphi_{x-1}(g) = \varphi_{x+1}(g(x-1))$

$$= g$$

$$\varphi_{x-1} \circ \varphi_{x+1}(g) = g$$

于是 φ_{x+1} 是同构。下面证 $f(x)$ 不可约

设 $f(x)=g(x)h(x)$，其中 $g,h\in\mathbb{Q}[x]$

则 $f(x+1)=\varphi_{x+1}(gh)=\varphi_{x+1}(g)\varphi_{x+1}(h)$

$=g(x+1)h(x+1)$

$\because f(x+1)$ 不可约 $\therefore g(x+1)\in\mathbb{Q}$ 或 $h(x+1)\in\mathbb{Q}$

不妨设 $g(x+1)\in\mathbb{Q}$ $\quad g=\varphi_{x-1}(g(x+1))\in\mathbb{Q}$

$\Rightarrow f$ 不可约 $\quad\square$

§4.5 重数

定义：设 $f\in F[x]\setminus F$，$p\in F[x]$ 不可约

如果对某个非负整数 m，有

$p^m\mid f$ 但 $p^{m+1}\nmid f$，则

称 m 是 p 在 f 中的重数 (multiplicity)

当 $m=1$ 时，p 称为 f 的单因子

$m>1$ 时 p 称为 f 的重因子

例 设 $f=\underbrace{(x-1)}_{p_1}\underbrace{(x^2+1)^3}_{p_2}\in\mathbb{Q}[x]$ ②

则 p_1 在 f 中的重数是 1，p_2 在 f 中的重数为

定义：设 $\alpha\in F$ 使得 $f(\alpha)=0$

则 $x-\alpha$ 在 f 中的重数称为 α 在 f 中的重数。当重数为 1 时，α 称为 f 的单根，否则为重根。

例：$f(x)=(x-1)^2x$

0 是 f 的单根，1 是 f 的二重根

~~定理 4.6 设 $f\in F[x]$，$\alpha_1,\dots,\alpha_r$ 是 f 在 F 中互不相同的根，其重数分别为 $m_1,\dots,m_r$，则 $m_1+\dots+m_r\le\deg(f)$~~

期末线性代数部分不考的内容

1. 矩阵分块不专门考
2. 线性流形，超平面不考
3. 多重斜对称线性函数不考
4. 加边子式不考.

以下内容不考

§1 复数域

§1.1 二次域的构造

设 $(F, +, 0_F, \cdot, 1_F)$ 是域. $d \in F$. 但不存在 $a \in F$ 使得 $a^2 = d$. 换言之

"$\sqrt{d}$" $\notin F$

例: $F = \mathbb{Q}$. $d = 2$.

令 $F(\sqrt{d}) = \{\alpha + \beta\sqrt{d} \mid \alpha, \beta \in F\}$

例 $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$

~~练习~~

在 $F(\sqrt{d})$ 中定义

$$(\alpha + \beta\sqrt{d}) + (\lambda + \mu\sqrt{d}) = (\alpha+\lambda) + (\beta+\mu)\sqrt{d},$$

其中 $\alpha, \beta, \lambda, \mu \in F$

并且 $0 = 0_F + 0_F\sqrt{d}$

则 $(F(\sqrt{d}), +, 0)$ 是交换群

$$(\alpha + \beta\sqrt{d}) + (-\alpha + (-\beta)\sqrt{d}) = 0.$$

注:

定义: $(\alpha + \beta\sqrt{d})(\lambda + \mu\sqrt{d})$

$$= (\alpha\lambda + \beta\mu d) + (\alpha\mu + \beta\lambda)\sqrt{d}$$

则 $(F(\sqrt{d}), \cdot, 1)$ 是 ~~交换~~ 交换含幺半群

其中 $1 = 1_F + 0_F\sqrt{d}$

于是 $(F(\sqrt{d}), +, 0, \cdot, 1)$ 是交换环

下面验证 $F(\sqrt{d})$ 是域

设 $x=\alpha+\beta\sqrt{d}$，其中 $\alpha,\beta\in F$，不全为零

设 $y=\alpha-\beta\sqrt{d}$

$$xy=(\alpha+\beta\sqrt{d})(\alpha-\beta\sqrt{d})$$
$$=\alpha^2-\beta^2 d\ \in F$$

若 $\alpha^2-\beta^2 d=0$，则 $\alpha^2=\beta^2 d$

情形1 $\beta=0_F$，则 $\alpha=0_F$ 矛盾

情形2 $\beta\neq 0_F$ 则 β 在 F 中可逆

且 $d=\alpha^2\beta^{-2}=(\alpha\beta^{-1})^2$

$\because \alpha\beta^{-1}\in F$ $\therefore$ d 在 F 中有平方根 $\alpha\beta^{-1}$

$\rightarrow\leftarrow$

于是 $\alpha^2-\beta^2 d\neq 0$

$$x\left(y(\alpha^2-\beta^2 d)^{-1}\right)=1$$

$\Rightarrow$ x 可逆 $F(\sqrt{d})$ 是域

例 在 $\mathbb{Q}(\sqrt{2})$ 中求 $x=1+3\sqrt{2}$ 的逆

$$(1+3\sqrt{2})(1-3\sqrt{2})=1-18=-17$$

$$(1+3\sqrt{2})\left[\frac{-1}{17}(1-3\sqrt{2})\right]=1$$

$$x^{-1}=\frac{-1}{17}(1-3\sqrt{2}).$$

$\square$

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{R}$$
$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{3})\subset\mathbb{R}$$

§1.2 复数域

定义：$\mathbb{C}=\{x+y\sqrt{-1}\mid x,y\in\mathbb{R}\}$

称 $\mathbb{C}$ 为复数域. 记 $\sqrt{-1}$ 为 i

$\forall z\in\mathbb{C}$. $z=x+yi$, $x,y\in\mathbb{R}$

称 x 为 z 的实部. 记为 $\mathrm{Re}(z)$

y 为 z 的虚部. 记为 $\mathrm{Im}(z)$.

i — imaginary unit

$\mathbb{C}$ 中的运算

设 $z_1=x_1+y_1i$, $z_2=x_2+y_2i$, $x_1,x_2,y_1,y_2\in\mathbb{R}$

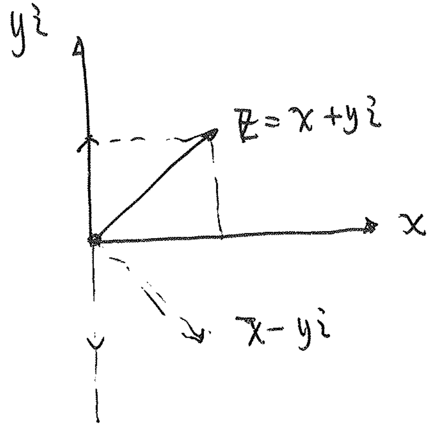
$$z_1+z_2=(x_1+x_2)+(y_1+y_2)i$$

$$z_1z_2=(x_1+y_1i)(x_2+y_2i)=(x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)i$$

设 $z=x+yi$, x,y 不全为零的实数

$$z(x-yi)=x^2+y^2>0$$

$$z^{-1}=\frac{1}{x^2+y^2}(x-yi)$$



定义: 设 $z=x+yi$

其中 $x,y\in\mathbb{R}$

z 的~~共轭~~定义为

$$\bar{z}=x-yi$$

注: $\bar{\bar{z}}=x+yi=z$

命题 1.1. $\varphi:\mathbb{C}\to\mathbb{C}$, $z\mapsto\bar{z}$ 是同构 (自同构)

证: 设 $z_1=x_1+y_1i$, $z_2=x_2+y_2i$, $x_1,x_2,y_1,y_2\in\mathbb{R}$

$$\varphi(z_1+z_2)=\varphi((x_1+x_2)+(y_1+y_2)i)=(x_1+x_2)-(y_1+y_2)i$$

$$=(x_1-y_1i)+(x_2-y_2i)=\bar{z}_1+\bar{z}_2=\varphi(z_1)+\varphi(z_2)$$

$$\varphi(z_1z_2)=\varphi((x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)i)$$

$$=(x_1x_2-y_1y_2)-(x_1y_2+x_2y_1)i$$

$$\varphi(z_1)\varphi(z_2)=(x_1-y_1i)(x_2-y_2i)=x_1x_2+y_1y_2-(x_1y_2+x_2y_1)i$$

$$\Rightarrow\ \varphi(z_1z_2)=\varphi(z_1z_2).$$

$$\varphi(1)=1.$$

φ 是同态 且 $\varphi\circ\varphi=id_{\mathbb{C}}$ $\Rightarrow\varphi$ 是同构

注 ~~利用~~ 记号

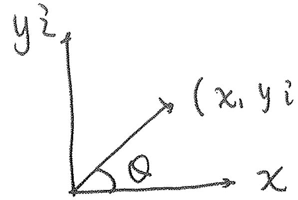
$$\overline{z_1+z_2}=\bar{z}_1+\bar{z}_2$$

$$\overline{z_1z_2}=\bar{z}_1\bar{z}_2$$

$$\bar{\bar{z}}=z$$

设 $z=x+yi$, $x,y\in\mathbb{R}$ $\quad z\bar{z}=x^2+y^2\in\mathbb{R}$.

§1.3. 复数的极坐标表示



(x, yi) 代表 $z=x+yi$

定义 $\sqrt{x^2+y^2}$ 为 z 的模长（记为$|z|$），z 与 x 轴的夹角为 z 的幅角。则 $x=|z|\cos\theta$, $y=|z|\sin\theta$

↳ 把 x 轴逆时针转至 z

把

$$z=|z|(\cos\theta+i\sin\theta),$$

称为 z 的极坐标表示。

命题 1.2 (i) 设 $z_1=|z_1|(\cos\theta_1+i\sin\theta_1)$

$z_2=|z_2|(\cos\theta_2+i\sin\theta_2)$

则 $z_1z_2=|z_1||z_2|[\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2)]$

(ii) 设 $z=|z|(\cos\theta+i\sin\theta)$

则 $\forall n\in \cancel{N}$ $z^n=|z|^n(\cos n\theta+i\sin n\theta)$

当 $z\neq0$ 时 $\forall n\in\mathbb{Z}$

$$z^n=|z|^n(\cos n\theta+i\sin n\theta)$$

特别地

$$z^{-1}=\frac{1}{|z|}(\cos(-\theta)+i\sin(-\theta))$$

证: (i)

$$z_1z_2=|z_1||z_2|(\cos\theta_1+i\sin\theta_1)(\cos\theta_2+i\sin\theta_2)$$

$$=|z_1||z_2|(\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2+(\cos\theta_1\sin\theta_2+\cos\theta_2\sin\theta_1)i)$$

$$=|z_1||z_2|(\cos(\theta_1+\theta_2)+\sin(\theta_1+\theta_2)i)$$

(ii) 当 $n\in\mathbb{N}$ 时. ~~利~~用(i) 对于 n 直接归纳

当 $z\neq0$ 时, $|z|\neq0$

$$z\left(\frac{1}{|z|}(\cos(-\theta)+i\sin(-\theta))\right)$$

$$=|z|(\cos\theta+i\sin\theta)\frac{1}{|z|}(\cos(-\theta)+i\sin(-\theta))$$

$$=\cos0+i\sin0=1.$$

于是 $z^{-1}=\frac{1}{|z|}(\cos(-\theta)+i\sin(-\theta))$

由此 对 $n\in\mathbb{N}$ 时结合（利用1 得）

$$z^{-n}=\cancel{\frac{1}{|z|^n}}|z|^{-n}(\cos(-n\theta)+i\sin(-n\theta))$$

□

注：$z^{-1}=\frac{1}{|z|}(\cos\theta - i\sin\theta)$. $(z\neq 0)$

§1.4 单位根

定义：设 $n\in\mathbb{Z}^+$，$x^n=1$ 在 $\mathbb{C}$ 中的解

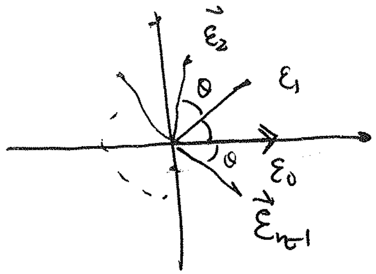
称为 n 次单位根

命题1.3 设 $n\in\mathbb{Z}^+$，则 $\mathbb{C}$ 中恰含有

n 个互不相同的 n次单位根

$$\varepsilon_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$$

证： $k=0,1,\dots,n-1$



$\theta=\frac{2\pi}{n}$

$$\varepsilon_k^n=\cos 2k\pi+i\sin 2k\pi$$
$$=1$$

于是 ε_k 是单位根

由定理2.5 $\varepsilon_0,\varepsilon_1,\dots\varepsilon_{n-1}$ 是所有的

n 次单位根

定理1.1 设 $U_n=\{\varepsilon_0,\varepsilon_1,\dots\varepsilon_{n-1}\}$

如命题1.1给出. 则 $(U_n,\cdot,1)$ 是一个

n 阶循环群

证：$U_n\subset\mathbb{C}^*=\mathbb{C}\setminus\{0\}$

而 $(\mathbb{C}^*,\cdot,1)$ 是群，于是

只要证 U_n 是 $\mathbb{C}^*$ 的子群即可

设 $\varepsilon_k,\varepsilon_l\in U_n$

$$(\varepsilon_k\varepsilon_l^{-1})^n=\varepsilon_k^n(\varepsilon_l^n)^{-1}=1^{-1}=1.$$

$$\Rightarrow \varepsilon_k\varepsilon_l^{-1}\in U_n \Rightarrow U_n\text{是子群}$$

(第四章引理2.4) ▯

由命题1.2(ii) $\varepsilon_k=\varepsilon_1^k \Rightarrow U_n=\langle\varepsilon_k\rangle$.. ▨

定义：设 $\varepsilon_l\in U_n$. 如果 $U_n=\langle\varepsilon_l\rangle$

则称 ε_l 是 n 次本原单位根

问题：求 U_n 中的本原单位根

因为 U_n 是 n 阶循环群，所以 U_n 与 $(\mathbb{Z}_n, +, \bar{0})$ 同构。于是只要找出 $(\mathbb{Z}_n, +, \bar{0})$ 的生成元即可

引理 1.1 $\bar{l} \in \mathbb{Z}_n$ 是 $(\mathbb{Z}_n, +, \bar{0})$ 的生成元 $\Leftrightarrow \gcd(l, n) = 1$

证："$\Rightarrow$" 设 $\bar{l}$ 是 $(\mathbb{Z}_n, +, \bar{0})$ 的生成元

则 $\exists m \in \mathbb{Z}$ 使得

$$m\bar{l} = \bar{1}$$

$$\Rightarrow ml \equiv 1 \mod n \Rightarrow \gcd(l, n) = 1$$

"$\Leftarrow$" 若 $\gcd(l, n) = 1$. 则 $\exists u, v \in \mathbb{Z}$

使得 $ul + vn = 1$

$$\Rightarrow \cancel{ul \equiv 1 \mod n}$$

$$\Rightarrow u\bar{l} = \bar{1} \quad (\text{在 } \mathbb{Z}_n \text{ 中})$$

设：$\varphi: U_n \longrightarrow \mathbb{Z}_n$

$$\varepsilon_k \to \bar{k}.$$

φ 是同构 于是 ε_k 是本原的 $\Leftrightarrow \gcd(k, n) = 1$

例：求 U_{12} 中的本原单位根

$\cos\frac{2\pi}{12} + i\sin\frac{2\pi}{12}$, $\cos\frac{10\pi}{12} + i\sin\frac{10\pi}{12}$

$\cos\frac{14\pi}{12} + i\sin\frac{14\pi}{12}$, $\cos\frac{22\pi}{12}, i\sin\frac{22\pi}{12}$

例：设 $U_4 = \{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3\}$, $a, b, c, d \in \mathbb{C}$

证明 $\cancel{\Delta_4 =} \begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix}$,

$= f_0 f_1 f_2 f_3$. ~~其~~中 $f_i = a + b\varepsilon_i + c\varepsilon_i^2 + d\varepsilon_i^3$

$$f_i = a + b\varepsilon_i + c\varepsilon_i^2 + d\varepsilon_i^3 \qquad (\varepsilon_i^4 = 1)$$

$$\varepsilon_i f_i = d + a\varepsilon_i + b\varepsilon_i^2 + c\varepsilon_i^3$$

$$\varepsilon_i^2 f_i = c + d\varepsilon_i + a\varepsilon_i^2 + b\varepsilon_i^3$$

$$\varepsilon_i^3 f_i = b + c\varepsilon_i + d\varepsilon_i^2 + a\varepsilon_i^3$$

$$f_i \begin{pmatrix} 1 \\ \varepsilon_i \\ \varepsilon_i^2 \\ \varepsilon_i^3 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix} \begin{pmatrix} 1 \\ \varepsilon_i \\ \varepsilon_i^2 \\ \varepsilon_i^3 \end{pmatrix}$$

$i = 0, 1, 2, 3.$

$$\left(f_0\begin{pmatrix}1\\ \varepsilon_0\\ \varepsilon_0^2\\ \varepsilon_0^3\end{pmatrix},\ f_1\begin{pmatrix}1\\ \varepsilon_1\\ \varepsilon_1^2\\ \varepsilon_1^3\end{pmatrix},\ f_2\begin{pmatrix}1\\ \varepsilon_2\\ \varepsilon_2^2\\ \varepsilon_2^3\end{pmatrix},\ f_3\begin{pmatrix}1\\ \varepsilon_3\\ \varepsilon_3^2\\ \varepsilon_3^3\end{pmatrix} \right)$$

$$= \underbrace{\begin{pmatrix} a & b & c & d\\ d & a & b & c\\ c & d & a & b\\ b & c & d & a\end{pmatrix}}_{C_4} \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1\\ \varepsilon_0 & \varepsilon_1 & \varepsilon_2 & \varepsilon_3\\ \varepsilon_0^2 & \varepsilon_1^2 & \varepsilon_2^2 & \varepsilon_3^2\\ \varepsilon_0^3 & \varepsilon_1^3 & \varepsilon_2^3 & \varepsilon_3^3\end{pmatrix}}_{V_4}$$

$$f_0 f_1 f_2 f_3 \det(V_4) = \det(C_4)\det(V_4)$$

$\because \det(V_4) \neq 0 \quad \therefore \det(C_4) = f_0 f_1 f_2 f_3$

§1.5 Euler"公式"

$$\boxed{e^{i\theta} = \cos\theta + i\sin\theta} \qquad \theta \in \mathbb{R}$$

设 $x \in \mathbb{R}$ $\quad e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

$$e^{xi} = \sum_{n=0}^{\infty} \frac{(xi)^n}{n!}$$

$$= \sum_{n=0}^{\infty} \frac{x^n}{n!} i^n$$

$$= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{2n!} + \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}$$

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

定义 $\quad e^{ix} = \cos x + i\sin x$

当 $x = \pi$ 时,

$$e^{i\pi} = -1 \Rightarrow e^{i\pi} + 1 = 0.$$

当 $x = 2\pi$ $\quad e^{2\pi i} = 1 \quad e^{2\pi i} - 1 = 0$

设 $z = x + yi$

$$e^z = e^{x+yi} = e^x e^{yi} = e^x(\cos y + i\sin y)$$

$\cancel{z = e^{|z|}(\cos\theta)}$ $\quad z = |z| e^{i\theta}$ $\quad \cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$ $\quad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2}$

§1.6 代数学基本定理

定理：设 $f\in\mathbb{C}[x]$，且 $\deg f>0$

则 f 在 $\mathbb{C}$ 中有根.

推论1.1 $\mathbb{C}[x]$ 中的不可约多项式只可能是一次的.

证：设 $f\in\mathbb{C}[x]\setminus\mathbb{C}$，不可约

由代数学基本定理，$\exists\alpha\in\mathbb{C}$ 使得

$$f(\alpha)=0$$

由定理2.5 $(x-\alpha)\mid f$，于是 f 的次数是1

推论1.2、$\mathbb{R}[x]$ 中不可约多项式的次数一定小于3.

证：设 $f\in\mathbb{R}[x]\setminus\mathbb{R}$ 不可约

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

$$d>1$$

~~由代数~~

则 $f(x)$ 不可能有实根（定理2.5）

由代数学基本定理，f 由非实根

$\alpha\in\mathbb{C}$ 则 $\bar{\alpha}\neq\alpha$.

$\because$ $f(\alpha)=f_d\alpha^d+f_{d-1}\alpha^{d-1}+\cdots+f_0=0$

$\therefore$ $\overline{f_d\alpha^d+f_{d-1}\alpha^{d-1}+\cdots+f_0}=\bar{0}$

$$\bar{f_d}\,\bar{\alpha}^d+\bar{f}_{d-1}\bar{\alpha}^{d-1}+\cdots+\bar{f_0}=0$$

$$f_d\bar{\alpha}^d+f_{d-1}\bar{\alpha}^{d-1}+\cdots+f_0=0$$

即 $f(\bar{\alpha})=0$. 由定理2.5

把 $f(x)=(x-\alpha)g(x)$, $g(x)\in\mathbb{C}[x]$

$f(\bar{\alpha})=(\bar{\alpha}-\alpha)g(\bar{\alpha})=0$ 但 $\bar{\alpha}-\alpha\neq0$

$\Rightarrow g(\bar{\alpha})=0\Rightarrow(x-\bar{\alpha})\mid g(x)$

$\Rightarrow f(x)=(x-\alpha)(x-\bar{\alpha})h(x)$

$$=\underbrace{[x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}]}_{g(x)}h(x)$$

$\because$ $\alpha+\bar{\alpha}$, $\alpha\bar{\alpha}\in\mathbb{R}$

$\therefore$ $f(x)=g(x)h(x)$, 其中 $g\in\mathbb{R}[x]$

从而 $h(x)=quo(f,g)\in\mathbb{R}[x]$

$\Rightarrow\quad f=gh \quad g,h\in\mathbb{R}[x]$

因 $\deg g=2$. $\quad\deg(f)=2$ 因

于是 $h\in\mathbb{R}\setminus\{0\}$

注 这定理

由定理4.4：$\forall f(x)\in\mathbb{C}[x]$

$$f(x)=\alpha(\lambda_1x+\mu_1)\cdots(\lambda_mx+\mu_m)$$

$\alpha,\lambda_1,\mu_1\cdots\lambda_m,\mu_m\in\mathbb{C}$, $\alpha\lambda_1\cdots\lambda_m\neq0$

$$f(x)=(\underbrace{\alpha\lambda_1\cdots\lambda_m}_{\beta})(x+\mu_1/\lambda_1)\cdots(x+\mu_m/\lambda_m)$$

$$=\beta(x-\gamma_1)^{m_1}\cdots(x-\gamma_k)^{m_k}$$

其中 $\beta=lc(f)$, $\gamma_1\cdots\gamma_k\in\mathbb{C}$ 两两不同

$m_1\cdots m_k\in\mathbb{Z}^+$

$\gamma_1,\cdots\gamma_k$ 是 f 的互不相同的复根，重数为 $m_1,\cdots m_k$

进而，$m_1+\cdots+m_k=n$

注：由定理4.4 $\forall f(x)\in\mathbb{R}[x]$

则 $f(x)=\alpha p_1\cdots p_m$. 其中 $p_1,\cdots p_m$ 是一次式、二次的不可约多项式.

$$f(x)=lc(f)(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}(x^2+\beta_1x+\gamma_1)^{n_1}\cdots(x^2+\beta_lx+\gamma_l)^{n_l}$$

其中 $\alpha_1,\cdots\alpha_k\in\mathbb{R}$. 两两不同. $m_1,\cdots m_k\in\mathbb{Z}^+$

$\beta_1,\gamma_1,\cdots\beta_l,\gamma_l\in\mathbb{R}$.

$x^2+\beta_jx+\gamma_j$ 没有实根，$j=1\cdots l$.

$x^2+\beta_1x+\gamma_1,\cdots x^2+\beta_lx+\gamma_l$ 两两不同（两两不相伴），$n_1,\cdots n_l\in\mathbb{Z}^+$

$\boxed{\text{求根与因式分解？}}$

§1.7 ~~$\mathbb{Z}[\sqrt{-5}]$~~ $\mathbb{Z}[\sqrt{-5}]$

$$\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$$

$\mathbb{Z}[\sqrt{-5}]$ 是交换环

$\because$ $\mathbb{Z}[\sqrt{-5}]\subset\mathbb{C}$ $\therefore$ $\mathbb{Z}[\sqrt{-5}]$ 是整环.

$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$$

若 $3=(a+b\sqrt{-5})(c+d\sqrt{-5})$

其中 $a,b,c,d\in\mathbb{R}$

$$\bar{3}=3=(a-b\sqrt{-5})(c-d\sqrt{-5})$$

$$9=(a^2+5b^2)(c^2+5d^2)$$

不妨设 $(a^2+5b^2)\le(c^2+5d^2)$

则 $a^2+5b^2=1$ 或 $a^2+5b^2=3$

$\because a,b\in\mathbb{Z}$. $a^2+5b^2\neq 3$

$\therefore$ $a^2+5b^2=1\Rightarrow b=0,\ a=\pm1$

$\Rightarrow a+b\sqrt{-5}$ 可逆

$\Rightarrow$ 3 不能写成两个不可逆元之积

如果 $2+\sqrt{-5}=(a+b\sqrt{-5})(c+d\sqrt{-5})$,

$2-\sqrt{-5}=(a-b\sqrt{-5})(c-d\sqrt{-5})$

$9=(a^2+5b^2)(c^2+5d^2)$

类似地可证: $a^2+5b^2=1$. $a=\pm1,\ b=0$

$\Rightarrow$ $2+\sqrt{-5}$ 也不能写成两个不可逆元之积

同理 $2-\sqrt{-5}$

问题: $3\overset{?}{\sim}2+\sqrt{-5}$ (在 $\mathbb{Z}[\sqrt{-5}]$ 中)

问题: $\mathbb{Z}[\sqrt{-5}]$ 中的可逆元是什么样的?

$$(a+b\sqrt{-5})(c+d\sqrt{-5})=1$$

$$(a-b\sqrt{-5})(c-d\sqrt{-5})=1$$

$$(a^2+5b^2)(c^2+5d^2)=1$$

$\Rightarrow$ $a^2+5b^2=1$ $c^2+5d^2=1$

$\Rightarrow$ $a=\pm1,\ c=\pm1$

$\Rightarrow$ $b=d=0$.

$\mathbb{Z}[\sqrt{-5}]$ 中的可逆元是 ±1

$\Rightarrow$ $3\not\sim 2+\sqrt{-5}$, $3\not\sim 2-\sqrt{-5}$

1.8 复数的矩阵表示

设 $F=\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a,b\in\mathbb{R} \right\}$

设 $A_1, A_2 \in F$. 可直接计算验证

$A_1+A_2,\ A_1A_2 \in F$.

且 $A_1A_2=A_2A_1$, 当 $A_1\neq\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 时, A_1可逆

习题课证明了 F 是域

$$\varphi:\ F \longrightarrow \mathbb{C}$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a+bi$$

$$\varphi\Big[\underbrace{\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}}_{A_1}+\underbrace{\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}}_{A_2}\Big]=\varphi\left(\begin{pmatrix} a_1+a_2 & b_1+b_2 \\ -b_1-b_2 & a_1+a_2 \end{pmatrix}\right)$$
$$=(a_1+a_2)+(b_1+b_2)i=(a_1+b_1i)+(a_2+b_2i)$$
$$=\varphi(A_1)+\varphi(A_2)$$

$$\varphi(A_1A_2)=\varphi\begin{pmatrix} a_1a_2-b_1b_2 & a_1b_2+b_1a_2 \\ -b_1a_2-a_1b_2 & a_1a_2-b_1b_2 \end{pmatrix}$$
$$=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i$$
$$=(a_1+b_1i)(a_2+b_2i)=\varphi(A_1A_2)$$

$$\varphi(E)=\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)=1.$$

且 φ 是满射

$\because$ φ 必是单射 (第4章 命题4.12)

于是 φ 是同构, 其中

$$\varphi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)=i$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$=-E.$$

§3 多元多项式

§3.1 多元多项式环

设 R 是交换环,

$R[x]$ 是 R 上关于未定元 x 的一元多项式环

$R[x][y]$ 是 $R[x]$ 上关于 y 一元多项式环

例 $R=\mathbb{Z}$，$f\in\mathbb{Z}[x][y]$ 为

$$f=(2x^2+1)y^2-(x^2+1)y+5x$$ 递归式

$$=2x^2y^2+y^2-x^2y-y+5x\in\mathbb{Z}[x,y]$$

分布式

定义：设 R 是交换环，R 上的 n 元多项式环是指 $R[x_1][x_2]\cdots[x_n]$，也记为 $R[x_1,\cdots x_n]$.

定义：设 $X_n=\{x_1^{i_1}\cdots x_n^{i_n}\mid i_1,\cdots i_n\in\mathbb{N}\}$

称 X_n 中元素为单项式 (monomial)

设 $x_1^0\cdots x_n^0=1$.

~~注：当 $(i_1,\cdots i_n)\neq(j_1,\cdots j_n)$ 时~~

引理3.1. 设 $\alpha_1,\cdots\alpha_k\in R\setminus\{0\}$，$M_1,\cdots M_k\in X_n$ 两两不同

则 $\alpha_1M_1+\cdots+\alpha_kM_k\neq0$

证：对 n 归纳，当 $n=1$ 时

$$X_1=\{1,x_1,x_1^2,\cdots\}$$

由引理2.2. 引理成立. 当 n 时

设 $n-1$ 时引理成立.

不妨设

$$\deg_{x_n}(M_1)\leq\cdots\leq\deg_{x_n}(M_k)$$

若 $\deg_{x_n}(M_k)=0$. 则由归纳假设引理成立.

设 $d=\deg_{x_n}(M_k)>0$ 且

$$\deg_{x_n}(M_l)=\cdots=\deg_{x_n}(M_{k-1})=\deg_{x_n}(M_k)=d$$

而 $\deg_{x_n}(M_1)=\cdots=\deg_{x_n}(M_{l-1})<d$

对 $j\in\{l,l+1,\cdots k\}$. 把

$$M_j=N_jx_n^d,\ \text{其中 } N_j\in X_{n-1}$$

$\because$ M_j 两两不同

$\therefore$ N_j 两两不同 $j=l,l+1,\cdots k$.

假设 $P=\alpha_1 M_1+\cdots+\alpha_k M_k=0$

$P=(\alpha_l N_l+\cdots+\alpha_k N_k)x_n^d$

$+\quad P_{d-1}x_n^{d-1}+\cdots+P_0$

其中 $P_0,\cdots,P_{d-1}\in R[x_1,\cdots x_{n-1}]$

则 $\alpha_l N_l+\cdots+\alpha_k N_k=0$

$\Rightarrow \alpha_l=\cdots=\alpha_k=0$ （归纳假设）

$\rightarrow\leftarrow$

命题3.1 设 $f\in R[x_1,\cdots x_n]\setminus\{0\}$

则 $\exists!$ $\alpha_1,\cdots\alpha_k\in R\setminus\{0\}$, $M_1,\cdots M_k\in\Sigma_n$

两两不同. 使得

$$f=\alpha_1 M_1+\cdots+\alpha_k M_k$$

证: 存在性. 由分配律直接导出.

唯一性

设 $f=\alpha_1 M_1+\cdots+\alpha_k M_k$

且 $f=\beta_1 N_1+\cdots+\beta_l N_l$ $\beta_1,\cdots\beta_l\in R\setminus\{0\}$

其中 $\alpha_1,\cdots\alpha_k$, $\beta_1,\cdots\beta_l$

$M_1,\cdots,M_k\in\Sigma_n$ 两两不同

$N_1,\cdots N_l\in\Sigma_n$ 也两两不同

不妨设: $M_1=N_1,\cdots M_s=N_s$

$M_{s+1},\cdots M_k$ $N_{s+1},\cdots N_l$ 两两不同

则 $(\alpha_1-\beta_1)M_1+\cdots+(\alpha_s-\beta_s)M_s$ $-\beta_{s+1}N_{s+1}-\cdots-\beta_l N_l$

$+\alpha_{s+1}M_{s+1}+\cdots+\alpha_k M_k$

$=0$

由引理3.1. $\alpha_{s+1}=\cdots=\alpha_k=0$ $\beta_{s+1}=\cdots=\beta_l=0$

即 ~~$l=k$~~ $s=k=l$

且 $(\alpha_1-\beta_1)M_1+\cdots+(\alpha_k-\beta_k)M_k=0$

$\Rightarrow \alpha_1=\beta_1\ \cdots\ \alpha_k=\beta_k$.

定义：单项式 $M=x_1^{i_1}\cdots x_n^{i_n}$ 的全次数

定义为 $i_1+\cdots+i_n$，记为 $\deg(M)$

设 $f\in R[x_1,\cdots,x_n]\setminus\{0\}$

$$f=\alpha_1M_1+\cdots+\alpha_kM_k$$

$\alpha_1,\cdots,\alpha_k\in R\setminus\{0\}$，$M_1,\cdots,M_k\in \Sigma_n$（两两不同）

则 $\deg(f)=\max\limits_{1\le i\le k}(\deg(M_i))$

f 关于 x_i 的次数 记为 $\deg_{x_i}(f)$，$i=1\cdots n$

例：$f=x_1x_2x_3+2x_1x_2^2+x_1x_3+5x_2x_3^4$

$\deg(f)=5$ $\quad\deg_{x_1}(f)=1$，$\deg_{x_2}(f)=2$

$\deg_{x_3}(f)=4$.