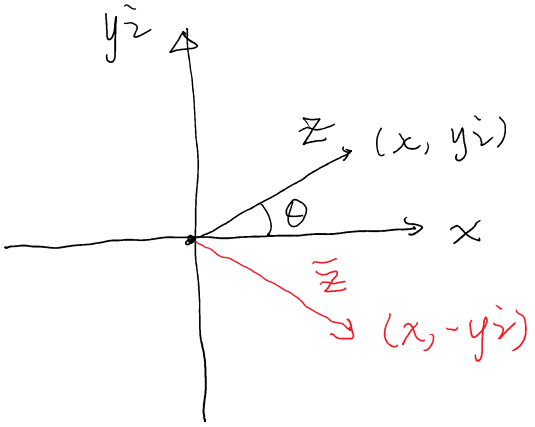
线性代数

2022年2月28日 7:28

回忆: $\mathbb{C}=\{x+yi \mid x,y\in\mathbb{R}\}$ $i^2=-1$

设 $z=x+yi$



$|z|=\sqrt{x^2+y^2}$

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

Euler: $e^{i\theta}=\cos\theta+i\sin\theta$

$z=|z|e^{i\theta}$

$\bar{z}=x-yi$: $\bar{\ }:\mathbb{C}\to\mathbb{C}$ isomorphism

$z\bar{z}=x^2+y^2 \Rightarrow |z|=\sqrt{z\bar{z}}$

$z=\bar{z} \Leftrightarrow z\in\mathbb{R}$

§4.3 单位根

$z\in\mathbb{C}$ 称为 n 次单位根 ($n\in\mathbb{Z}^+$)

如果 $z^n=1$

命题: 方程 $z^n=1$ 在 $\mathbb{C}$ 中有 n 个互不相同的根

$$\varepsilon_k=e^{\frac{2k\pi}{n}i},\quad k=0,1,\cdots,n-1$$

pf $\varepsilon_k^n=\left(e^{\frac{2k\pi}{n}i}\right)^n$

$n\cdot\frac{2k\pi}{n}i=e^{2k\pi i}$

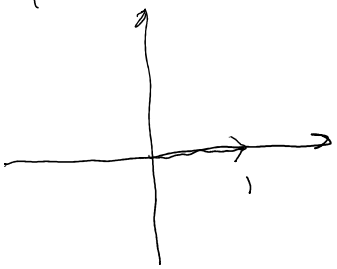
$$= e^{n \cdot \frac{2k\pi}{n} i} = e^{2k\pi i}$$

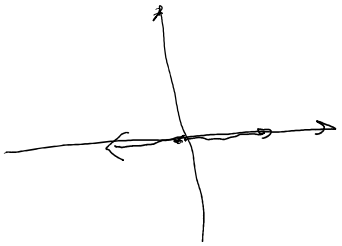
$$= \cos(2k\pi) + i\sin(2k\pi)$$

$$= 1$$

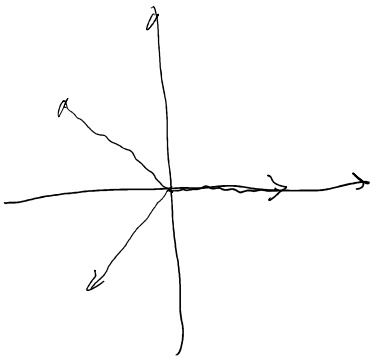
$n=2$ ± 1

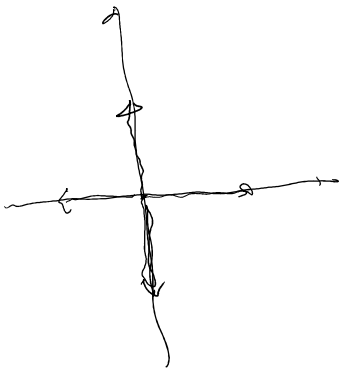
$n=1$





$n=3$ $\varepsilon_k = e^{\frac{2k\pi}{3} i}$ $k=0,1,2$





图

设 U_n 是所有 n 次单位根

的集合. $(U_n, \cdot, 1)$ 是群

$U_n \subset \mathbb{C}^*$ $(\mathbb{C}^*, \cdot, 1)$

是群

由上学期的知识,

验证 U_n 是群 只要验证

$\forall a, b \in U_n \quad ab^{-1} \in U_n$

$(ab^{-1})^n = a^n (b^n)^{-1}$

$= 1 \cdot (1)^{-1} = 1 \Rightarrow$

$ab^{-1} \in U_n$

U_n 是个循环群

$U_n = \langle \underset{\| }{e^{\frac{2\pi}{n} i}} \rangle$

ε_1

$(\because \varepsilon_k = \varepsilon_1^k, \quad k = 0, 1 \cdots n-1)$

$(\mathbb{Z}_n, +, 0)$

$U_n = \langle \varepsilon_\ell \rangle \iff gcd(n, \ell) = 1$

只要证 $ord(\varepsilon_\ell) = n$

$ord(\varepsilon_\ell) = ord(\varepsilon_1^\ell) = \frac{n}{gcd(n, \ell)}$

于是 $ord(\varepsilon_\ell) = n \iff gcd(n, \ell) = 1$

囧

命题：$(U_n, \cdot, 1)$ 是循环群

且 $U_n = \langle \varepsilon_l \rangle \Leftrightarrow \gcd(n, l) = 1$

如果 $U_n = \langle \varepsilon_l \rangle$，则称

ε_l 是本原单位根

例 设 $a_0, a_1, \cdots a_{n-1} \in \mathbb{C}$

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ \cdots & & & & \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{pmatrix}_{n \times n}$$

求 $\det(A)$. 并研究 A 何时可逆

回忆

$$B = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & 1 & \cdots & n-2 & n-1 \\ \cdots & & & & \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

求 B^{-1}

设 $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

设 $\varepsilon_0, \varepsilon_1 \cdots \varepsilon_{n-1}$ 是上述定义的等价根

$$f(\varepsilon_k) = a_0 + a_1\varepsilon_k + \cdots + a_{n-1}\varepsilon_k^{n-1}$$

$\varepsilon_k^n = 1$ $\quad \varepsilon_k f(\varepsilon_k) = a_0\varepsilon_k + a_1\varepsilon_k^2 + \cdots + a_{n-2}\varepsilon_k^{n-1} + a_{n-1}\varepsilon_k^n$

$$= a_{n-1} + a_0\varepsilon_k + a_1\varepsilon_k^2 + \cdots + a_{n-2}\varepsilon_k^{n-1}$$

$$\varepsilon_k^{n-1} f(\varepsilon_k) = a_0\varepsilon_k^{n-1} + a_1\varepsilon_k^n + a_2\varepsilon_k^{n+1} + \cdots + a_{n-1}\varepsilon_k^{2n-2}$$

$$= a_1 + a_2\varepsilon_k + \cdots + a_{n-1}\varepsilon_k^{n-2} + a_0\varepsilon_k^{n-1}$$

$$f(\varepsilon_k)\begin{pmatrix} 1 \\ \varepsilon_k \\ \vdots \\ \varepsilon_k^{n-1} \end{pmatrix} = A\begin{pmatrix} 1 \\ \varepsilon_k \\ \vdots \\ \varepsilon_k^{n-1} \end{pmatrix} \qquad k = 0, 1 \cdots n-1$$

$$\left[f(\varepsilon_0)\begin{pmatrix} 1 \\ \varepsilon_0 \\ \vdots \\ \varepsilon_0^{n-1} \end{pmatrix}, \cdots f(\varepsilon_{n-1})\begin{pmatrix} 1 \\ \varepsilon_{n-1} \\ \vdots \\ \varepsilon_{n-1}^{n-1} \end{pmatrix} \right]$$

$$= A\begin{pmatrix} 1 & \cdots & 1 \\ \varepsilon_0 & & \varepsilon_{n-1} \\ \vdots & & \vdots \\ \varepsilon_0^{n-1} & \cdots & \varepsilon_{n-1}^{n-1} \end{pmatrix}$$

$$\begin{pmatrix} \varepsilon_0^{n-1} & \varepsilon_1^{n-1} & \cdots & \varepsilon_{n-1}^{n-1} \end{pmatrix}$$

V 可逆

$$V \begin{pmatrix} f(\varepsilon_0) & & & \\ & f(\varepsilon_1) & & \\ & & \ddots & \\ & & & f(\varepsilon_{n-1}) \end{pmatrix} = AV$$

$$A = V \begin{pmatrix} f(\varepsilon_0) & & & \\ & f(\varepsilon_1) & & \\ & & \ddots & \\ & & & f(\varepsilon_{n-1}) \end{pmatrix} V^{-1}$$

$$\det(A) = \det(V)\det(C)\det(V^{-1})$$

$$= \det(C) = f(\varepsilon_0) f(\varepsilon_1) \cdots f(\varepsilon_{n-1})$$

A 可逆 $\Leftrightarrow$ $\det(A) \neq 0$

$\Leftrightarrow$ $f(\varepsilon_0) f(\varepsilon_1) \cdots f(\varepsilon_{n-1}) \neq 0$

$\Leftrightarrow$ $f(x)$ 和 $x^n - 1$ 在 $\mathbb{C}$ 中没有公共根

$\Leftrightarrow \gcd(f(x), x^n - 1) = 1$

$$\det(B) = \det \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \\ 2 & 3 & \cdots & 1 \end{pmatrix}$$

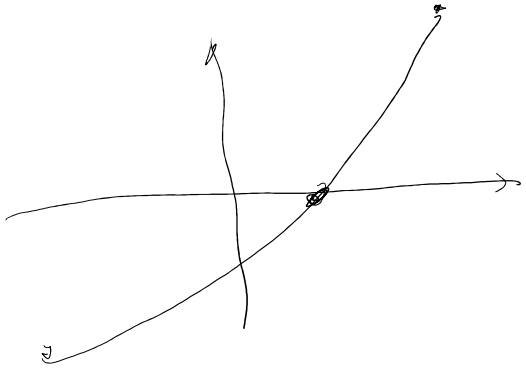
$f = 1 + 2X + \cdots + nX^{n-1}$

$= f(\varepsilon_0) f(\varepsilon_1) \cdots f(\varepsilon_{n-1})$

$$\det(B) = (-1)^{\frac{n+1}{2}} n^{n-1}$$

$$h(x) = x^3 + a_2 x^2 + a_1 x + a_0$$

$a_j \in \mathbb{R}$



$z^n = 1 \quad \forall \ u \in \mathbb{C}$

$$u = \frac{|u|}{\Delta} e^{i\theta}$$

$$\sqrt[n]{u} = \sqrt[n]{|u|}\, \varepsilon_k, \quad k = 0, 1, \cdots n-1$$

§4.4 代数学基本定理

(Fundamental Theorem of Algebra)

(FTA)

FTA 设 $f(x) \in \mathbb{C}[x]$, $\deg(f) > 0$

则 f 在 $\mathbb{C}$ 中有根

x^2+1 在 $\mathbb{R}$ 中无根

设 $i^2=-1$. $\mathbb{C}=\{x+yi \mid x,y\in\mathbb{R}\}$

推论1 $\mathbb{C}[x]$ 中的不可约元都是一次多项式

$F[x]$

F^{∞}

一次多项式都不可约

证 设 $f\in\mathbb{C}[x]$ 是不可约元

则 $\deg(f)>0$

由 FTA, $\exists \alpha\in\mathbb{C}$ 使得

$f(\alpha)=0$

由余式定理 $f(x)=(x-\alpha)g(x)$

其中 $g\in\mathbb{C}[x]$

$\because f$ 不可约 $\therefore \deg(g)=0$

$\Rightarrow \deg(f)=1$ ✓

★ 推论2 设 $f\in\mathbb{C}[x]$, $\deg(f)=n>0$

则 $\exists\ \alpha_1,\cdots\alpha_k\in\mathbb{C}$ 两两不同

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

$a \in \mathbb{C}$

使得 $f(x) = a(x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}$

证：利用UFD中的相伴不可约分解即可

注：$a = lc(f)$

推论3 $\mathbb{R}[x]$ 中不可约元的次数小于3

证：设 $f \in \mathbb{R}[x]$, $\deg(f) > 2$

假设 f 是 $\mathbb{R}[x]$ 中的不可约元

$\because f \in \mathbb{C}[x]$

$\therefore \exists \alpha \in \mathbb{C}$ 使得 $f(\alpha) = 0$ (FTA)

则 $f(x) = (x-\alpha)g(x)$

其中 $g \in \mathbb{C}[x]$

$$f(x) = f_n x^n + \cdots + f_1 x + f_0$$

$f_j \in \mathbb{R}$

$$0 = f_n \alpha^n + \cdots + f_1 \alpha + f_0$$

$$0 = \bar{0} = \overline{f_n \alpha^n + \cdots + f_1 \alpha + f_0}$$

$$= \overline{f_n} \, \bar{\alpha}^n + \cdots + \overline{f_1} \, \bar{\alpha} + \overline{f_0}$$

$$= f_n \bar{\alpha}^n + \cdots + f_1 \bar{\alpha} + f_0$$

于是 $\bar{\alpha}$ 也是 $f(x)$ 根

$\because f$ 在 $\mathbb{R}[x]$ 中不可约

$\therefore \alpha \in \mathbb{C} \setminus \mathbb{R}$

故 $\alpha \neq \bar{\alpha}$

由此可知 $f(x) = (x-\alpha)(x-\bar{\alpha})h(x)$

$h \in \mathbb{C}[x]$

$$(x-\alpha)(x-\bar{\alpha})$$

$$= x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}$$

($\alpha + \bar{\alpha} \in \mathbb{R}$, $\alpha\bar{\alpha} \in \mathbb{R}$)

(11 (个
IR 在

$f(x)$, $(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$

$(x-\alpha)(x-\bar{\alpha}) \mid f(x)$

$\Rightarrow h \in \mathbb{R}[x]$

$f(x) = p(x)h(x)$, 其中 $p=(x-\alpha)(x-\bar{\alpha}) \in \mathbb{R}[x]$

f 不可约 $\rightarrow\leftarrow$ 矛盾

推论4 $\mathbb{R}[x]$ 中次数为正的多项式

是一次式二次实系数多项式之积.

且其中二次多项式无实根.

$\int \frac{c}{(ax+b)^m} dx$ ✓ $\int \frac{ux+v}{(ax^2+bx+c)^m} dx$

注:

$f, g \in \mathbb{C}[x]$

$f = a(x-\alpha_1)^{m_1} \cdots (x-\alpha_k)^{m_k}$

$g = b(x-\beta_1)^{n_1} \cdots (x-\beta_q)^{n_q}$

$gcd(f,g)=1 \Leftrightarrow \{\alpha_1 \cdots \alpha_k\} \cap \{\beta_1 \cdots \beta_s\} = \varnothing$

---

§4.5 两个例子

例 $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}] = \{x+y\sqrt{-5} \mid x,y \in \mathbb{Z}\} \subset \mathbb{C}$

注. $\sqrt{-5} = \sqrt{5}\,i$

$\mathbb{Z}[\sqrt{-5}]$ 是整环，但不是UFD

$a,b,c,d \in \mathbb{Z}$

$$(a+b\sqrt{-5})(c+d\sqrt{-5})$$
$$= (ac-5bd) + (ad+bc)\sqrt{-5}$$
$$\in \mathbb{Z}[\sqrt{-5}]$$

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

$\mathbb{Z}[\sqrt{-5}]$ 中的可逆元是 ± 1

下面说 3，$2+\sqrt{-5}$，$2-\sqrt{-5}$

都是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元

假设 $3=(a+b\sqrt{-5})(c+d\sqrt{-5})$

取共轭 $3=(a-b\sqrt{-5})(c-d\sqrt{-5})$

$$9=(a+b\sqrt{-5})(a-b\sqrt{-5})(c+d\sqrt{-5})(c-d\sqrt{-5})$$

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

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

$$a^2+5b^2=\begin{cases}\pm1 & \Rightarrow a=\pm1,\ b=0\\ \pm3 & \Rightarrow \text{不可能}\\ \pm9 & \Rightarrow c=\pm1,\ d=0\end{cases}$$

于是 $a+b\sqrt{-5}$ 是可逆元

或 $c+d\sqrt{-5}$ 是可逆元

$\Rightarrow$ 3 是不可约的

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

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

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

类似推论可知

$a+b\sqrt{-5}$ 或 $c+d\sqrt{-5}$

是 ± 1

$\Rightarrow$ $2+\sqrt{-5}$ 不可约

同理 $2-\sqrt{-5}$ 不可约

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

$3 \nmid 2+\sqrt{-5} \Rightarrow \mathbb{Z}[\sqrt{-5}]$

$3 \nmid 2-\sqrt{-5}$ 不是UFD

例 Hamilton 四元数

令 $H = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \middle| u, v \in \mathbb{C} \right\}$

则 $H \subset M_2(\mathbb{C})$

可以证明：

1. $H \subseteq M_2(\mathbb{C})$ 的子环

2. H 是非交换的

3. 设 $A \in H$ 不是零矩阵

则 $\exists B \in H$ 使得

$$AB = BA = E$$

这是人类发现的第一个

skew-field

---

1. $\mathbb{C}$ 上运算 $+, \cdot, -$

封闭，交换

2. $\mathbb{C}$ 中多项式可以分解为

一次多项式之积

3. 验证 H 满足上述三条

---

4. $\mathbb{R}[x]$ 多项式可以分解为

一次和二次多项式之积

§5 多元多项式

设 $(R,+,0,\cdot,1)$ 是一个交换环

$R[x]$ 是 R 上关于未定元 x 的一元多项式环

$R[x][y]$ 是 R 上关于未定元 x,y 的二元多项式环

例

$$f=(x^2+1)y^3-(x+1)y^2-x^5+2x \in Z[x][y]$$

$$=x^2y^3+y^3-xy^2-y^2-x^5+2x$$

$$=-x^5+y^3x^2+(2-y^2)x+y^3-y^2 \in Z[y][x]$$

§5-1 多元多项式环

设 R 是交换环. 则

交换环 $R[x_1][x_2]\cdots[x_n]$

称为R上关于未定元 $x_1, x_2, \cdots x_n$ 的 n 元多项式环。记为

$$R[x_1, x_2, \cdots x_n]$$

定理：(i) 当 R 是整环时

$R[x_1, x_2, \cdots x_n]$ 也是整环

(ii) 当 R 是 UFD 时，

$R[x_1, x_2, \cdots x_n]$ 也是 UFD

证：(i) R 整环 $\Rightarrow R[x]$ 是整环

由归纳法直接可得

(ii) 见讲义

$\mathbb{C}[x, y]$ 因式分解是唯一的。