2023年12月21日 6:48

多元多项式和定数

回忆：在 $R[x_1, \cdots x_n]$ 中，$X_n = \{x_1^{d_1} \cdots x_n^{d_n} \mid d_1, \cdots d_n \in \mathbb{N}\}$

设 $f = \alpha_1 M_1 + \cdots + \alpha_k M_k = \beta_1 N_1 + \cdots + \beta_l N_l$

其中 $\alpha_1, \cdots \alpha_k, \beta_1, \cdots \beta_l \in R \setminus \{0\}$

$M_1, \cdots, M_k \in X_n$ 两两不同

$N_1, \cdots N_l \in X_n$ 两两不同

则 $k = l$，且适当调整下标后

$\alpha_i = \beta_i, \quad M_i = N_i, \quad i = 1, 2, \cdots k$

证：设 $M_1 = N_1, \cdots M_i = N_i$

$M_{i+1}, \cdots M_k \notin \{N_1, \cdots N_l\}$

$N_{i+1}, \cdots N_l \notin \{M_1, \cdots M_k\}$

由 $\alpha_1 M_1 + \cdots + \alpha_k M_k = \beta_1 N_1 + \cdots + \beta_k N_k$

$\Rightarrow (\alpha_1 - \beta_1) M_1 + \cdots + (\alpha_i - \beta_i) M_i$

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

$+ (-\beta_{i+1}) N_{i+1} + \cdots + (-\beta_l) N_l = 0$

$\because M_1, \cdots M_i, M_{i+1}, \cdots M_k, N_{i+1}, \cdots N_l$

是两两之不相同的多项式

$\therefore$ 由引理可知

$\alpha_{i+1} = \cdots = \alpha_k = 0, \quad \beta_{i+1} = \cdots = \beta_l = 0$

于是 $k=l=\bar{z}$

且 $\alpha_1=\beta_1, \cdots \alpha_k=\beta_k$ 因

定义：设 $p\in R[x_1,\cdots x_n]\setminus\{0\}$

其分布式为

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

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

$$\deg p := \max(\deg(M_1),\cdots \deg M_k)$$

$$\text{规定 } \deg 0 := -\infty.$$

p $\deg_{x_i} p$ $i=1,2\cdots n$

$\deg p$

例 $f=2(x-y)(x+y)+3y^2-5xyz+(y+z)^2-2y^3$

$\in \mathbb{Z}[x,y,z]$

求：$\deg_x(f)$, $\deg_y(f)$, $\deg_z(f)$

$\deg(f)$

解：$f=2x^2-(5yz)x-2yz-z^2-2y^3$

$=-2y^3-(2xz+2z)y+2x^2-z^2$

$=-z^2-(5xy+2y)z+2x^2-2y^3$

$=-(2y^3+5xyz)+(2x^2-2yz-z^2)$

$\deg_x f = 2, \quad \deg_y f = 3, \quad \deg_z f = 2$

$\deg(f) = 3$.

§2.2 齐次多项式

定义：设 $h \in R[x_1, \dots x_n] \setminus \{0\}$

若其分布式为

$$h = \alpha_1 M_1 + \dots + \alpha_k M_k$$

且有 $\deg M_1 = \dots = \deg M_k = d$

则称 h 是齐 d 次

齐次的. 0 认为是齐任何次

注：$\forall \varphi \in R[x_1, \dots x_n] \setminus \{0\}$

$$\varphi = h_d + h_{d-1} + \dots + h_0$$

其中 h_i 是齐 i 次的，

$h_d \neq 0$

$$f = \underbrace{-(2y^3 + 5xyz)}_{h_3} + \underbrace{(2x^2 - 2yz - z^2)}_{h_2} + \underbrace{0}_{h_1} + \underbrace{0}_{h_0}$$

引理 设 h_d, h_e 分别是齐 d 次和

引理 设 h_d, h_e 分别是齐 d 次和 e 次齐(非零)

则 (i) $\deg(h_d + h_e) \leq \max(d, e)$

且如果 $d \neq e$, 则"="成立

(ii) $\deg(h_d h_e) \leq d + e$

且如果 R 是整环, 则"="成立

证: (i) 注意到合并同类项产生对消只可能在次数相同的单项式之间进行

(ii) 同(i)类系数相乘为零.

定理 设 $f, g \in R[x_1, \ldots x_n]$

则 (i) $\deg(f+g) \leq \max(\deg(f), \deg(g))$

且如果 $\deg(f) \neq \deg(g)$

则等号成立

(ii) $\deg(fg) \leq \deg(f) + \deg(g)$

且如果 R 是整环, 则

"="成立

证: 把 f 和 g 分解为齐次分量

$$f = a_d + a_{d-1} + \cdots + a_0$$

$$g = b_e + b_{e-1} + \cdots + b_0$$

其中 a_i 是 x 次项

b_j 是 y 次项

如果 f 式 g 为零. 定理显然

否则 $a_\delta \neq 0$, $b_e \neq 0$

则定理由上述引理用于

a_δ, b_e 即可

例 $f = (x+y)z^2 - z$

$lc_z(f) = (x+y)$. $lc_x(f) = z^2$

---

§2.3 赋值同态

定理 设 R 和 S 是两个交换环,

$\varphi: R \to S$ 是环同态

取 $s_1, \cdots s_n \in S$. 则存在唯一

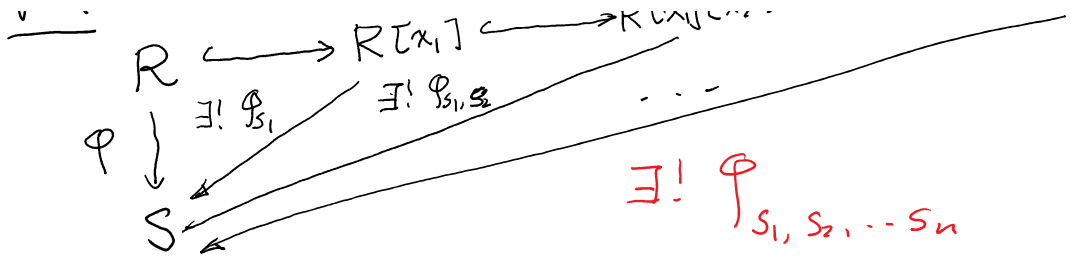
环同态 $\varphi_{s_1,\cdots s_n}: R[x_1 \cdots x_n] \to S$

满足 $\varphi_{s_1,\cdots s_n}|_R = \varphi$

且 $\varphi_{s_1,\cdots s_n}(x_i) = s_i$, $i = 1, 2 \cdots n$

证:

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



由上图和之前n归纳可以:

$$M = x_1^{d_1} \cdots x_n^{d_n}$$

$$\varphi_{s_1, s_2 \cdots s_n}(M) = s_1^{d_1} \cdots s_n^{d_n}$$

$\alpha \in R$, $\varphi_{s_1, s_2 \cdots s_n}(\alpha M) = \varphi(\alpha) s_1^{d_1} \cdots s_n^{d_n}$

多项式按作用的定义.

例 $f(x_1, x_2) = x_1^2 + x_2^2 - 1 \in R[x_1, x_2]$

$\alpha, \beta \in R$ $\quad f(\alpha, \beta) = 0$

$\Leftrightarrow$ $\varphi_{\alpha,\beta}(f)$

等价于

在微积分中. 函数

$f(x_1, \cdots x_n)$ 是 d 齐次的

如果 $\forall t \in R$

$f(tx_1, \cdots tx_n) = t^d f(x_1, \cdots x_n)$

---

§3. 复数

§3. 代数

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

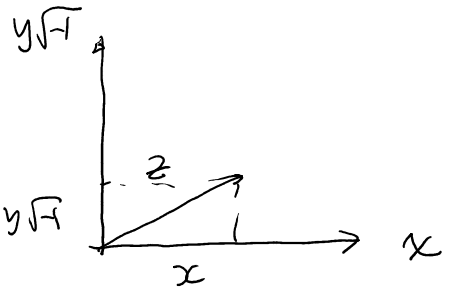
$z^2 + 1 = 0$ 无实根

设 $z = x + y\sqrt{-1}$ $x, y \in \mathbb{R}$

x 称为 z 的实部 记为 $\mathrm{Re}(z)$

y 称为 z 的虚部 记为 $\mathrm{Im}(z)$

$\sqrt{-1}$ 称为虚单位



设 $z_1 = x_1 + y_1\sqrt{-1}$

$z_2 = x_2 + y_2\sqrt{-1}$

$x_1, x_2, y_1, y_2 \in \mathbb{R}$

$$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)\sqrt{-1}$$

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)\sqrt{-1}$$

可直接验证

$(\mathbb{C}, +, 0)$ 为交换群

$(\mathbb{C}, \cdot, 1)$ 为交换幺

含幺半群

设 $z = x + y\sqrt{-1}$. x, y 不全为零

要证 z 可逆

$\bar{z} := x - y\sqrt{-1}$ 称为 z 的共轭

$z \cdot \bar{z} = (x + y\sqrt{-1})(x - y\sqrt{-1})$

$= x^2 + y^2$

当 x, y 不全为零时 $x^2 + y^2 \neq 0$

$z \cdot \frac{\bar{z}}{x^2+y^2} = 1 \Rightarrow z^{-1} = \frac{\bar{z}}{x^2+y^2}$

分配律易直接验证.

于是

$(\mathbb{C}, +, 0, \cdot, 1)$ 是域

称为复数域 (field of complex numbers)

complex $x + y\sqrt{-1}$

例 设

$F = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \middle| \ x, y \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$

验证 F 是域

验证: 设 $A = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, $B = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$

其中 $A, B \in F$

$A - B = \begin{pmatrix} x-u & y-v \\ -(y-v) & x-u \end{pmatrix} \in F$

$\Rightarrow (F, +, 0)$ 是 $(M_2(\mathbb{R}), +, 0)$

$\Rightarrow (F, +, 0)$ 是 $(M_2(\mathbb{R}), +, 0)$ 的子群

$$AB = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}\begin{pmatrix} u & v \\ -v & u \end{pmatrix}$$

$$= \begin{pmatrix} xu-yv & xv+yu \\ -yu-xv & xu-yv \end{pmatrix} \in F$$

乘法封闭

$$BA = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

$$= \begin{pmatrix} xu-yv & xv+yu \\ -xv-yu & xu-yv \end{pmatrix} = BA$$

乘法交换

$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in F$

其在运算规律与 $M_2(\mathbb{R})$ 中为一致

于是 $(F, +, 0, \cdot, E)$

是 $(M_2(\mathbb{R}), +, 0, \cdot, E)$

的交换子环.

设 $A \neq 0$ 即 $x \neq 0$ 或 $y \neq 0$

$\| $

$(x \quad y)$

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

$\det(A) = x^2 + y^2 \neq 0$

于是 A 在 $M_2(\mathbb{R})$ 中可逆

$$A^{-1} = \begin{pmatrix} \frac{x}{x^2+y^2} & \frac{-y}{x^2+y^2} \\ \frac{y}{x^2+y^2} & \frac{x}{x^2+y^2} \end{pmatrix} \in F$$

于是 F 是域

考虑: $\varphi: \mathbb{C} \longrightarrow F$

$$z = x + y\sqrt{-1} \longmapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

验证: φ 是双射同构

验证: 设 $z_1 = x_1 + y_1\sqrt{-1}$, $x_1, x_2, y_1, y_2 \in \mathbb{R}$
$z_2 = x_2 + y_2\sqrt{-1}$,

$$\varphi(z_1+z_2) = \varphi((x_1+x_2) + (y_1+y_2)\sqrt{-1})$$

$$= \begin{pmatrix} x_1+x_2 & y_1+y_2 \\ -(y_1+y_2) & x_1+x_2 \end{pmatrix}$$

$$= \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix} + \begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix}$$

$$= \varphi(z_1) + \varphi(z_2)$$

$$\varphi(z_1 z_2) = \varphi\left((x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{-1}\right)$$

$$= \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -(x_1y_2 + x_2y_1) & x_1x_2 - y_1y_2 \end{pmatrix}$$

$$\varphi(z_1)\varphi(z_2) = \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix}$$

$$= \begin{pmatrix} x_1x_2 - y_1y_2 & x_1y_2 + y_1x_2 \\ -y_1x_2 - y_2x_1 & x_1x_2 - y_1y_2 \end{pmatrix}$$

$$\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$$

$$\varphi(1) = \varphi(1 + 0\sqrt{-1}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$

于是 φ 是环同态

设 $\varphi(x + y\sqrt{-1}) = 0 = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$

$\Rightarrow x = y = 0 \Rightarrow$

$x + y\sqrt{-1} = 0$

φ 单

设 $A = \begin{pmatrix} u & v \\ -v & u \end{pmatrix}$

$\varphi(u + v\sqrt{-1}) = A$ 满

于是 $F \cong \mathbb{C}$

$$\varphi(\sqrt{-1}) = \varphi(0 + \sqrt{-1}) = \boxed{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

$$= -E$$

命题: $-: \mathbb{C} \longrightarrow \mathbb{C}$

$$z \longmapsto \bar{z}$$

$$\| \qquad\qquad \|$$

$$x+y\sqrt{-1} \longmapsto x-y\sqrt{-1}, \quad x, y \in \mathbb{R}$$

(i) $-\circ- = id_{\mathbb{C}}$ [一是双射]

(ii) $\bar{z} = z \iff z \in \mathbb{R}$

(iii) $-$: 是同构

证: i) $\overline{\overline{x+y\sqrt{-1}}} = \overline{x-y\sqrt{-1}} = x+y\sqrt{-1}$ √

ii) $\bar{z} = z \iff x+y\sqrt{-1} = x-y\sqrt{-1}$

$\iff y\sqrt{-1} = -y\sqrt{-1}$

$\iff y = -y$

$\iff 2y = 0 \iff y = 0.$

(char(ℝ) = 0)

iii) 设 $z_1 = x_1 + y_1\sqrt{-1}$, $z_2 = x_2 + y_2\sqrt{-1}$

$$\overline{z_1+z_2} = \overline{(x_1+x_2)+(y_1+y_2)\sqrt{-1}}$$

$$= (x_1+y_2)-(y_1+y_2)\sqrt{-1}$$

$$= \left(x_1 - y_1\sqrt{-1}\right) + \left(x_2 - y_2\sqrt{-1}\right)$$

$$= \bar{z}_1 + \bar{z}_2$$

$$\overline{z_1 z_2} = \overline{(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{-1}}$$

$$= (x_1x_2 - y_1y_2) - (x_1y_2 + x_2y_1)\sqrt{-1}$$

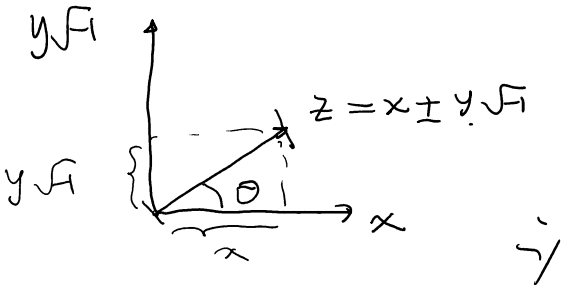
$$\overline{z_1}\,\overline{z_2} = (x_1 - y_1\sqrt{-1})(x_2 - y_2\sqrt{-1})$$
$$= (x_1x_2 - y_1y_2) + (-y_1x_2 - y_2x_1)\sqrt{-1}$$
$$= \overline{z_1 z_2}.$$

当 $z \neq 0$ 时

$$z^{-1} = \frac{\overline{z}}{(z\overline{z})}$$

[验证 $z \cdot \frac{\overline{z}}{(z\overline{z})} = \frac{z\cdot\overline{z}}{z\overline{z}} = 1$]

§3.2. 复数的极表示



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

称为 z 的模长

注 $|z| = \sqrt{z\overline{z}}$

$(z\overline{z} = (x+y\sqrt{-1})(x-y\sqrt{-1}) = x^2+y^2)$

$\theta \in [0, 2\pi)$ 称为 z 的幅角 (辐角)

记为 $\arg(z)$

则: $z = |z|(\cos\theta + \sqrt{-1}\sin\theta)$

称为 z 的极坐标表示.

引理 设 $z_1 = |z_1|(\cos\theta_1 + \sqrt{-1}\sin\theta_1)$

$z_2 = |z_2|(\cos\theta_2 + \sqrt{-1}\sin\theta_2)$

则 $z_1z_2 = |z_1||z_2|(\cos(\theta_1+\theta_2) + \sqrt{-1}\sin(\theta_1+\theta_2))$

证 $z_1z_2 = |z_1||z_2|(\cos\theta_1 + \sqrt{-1}\sin\theta_1)(\cos\theta_2 + \sqrt{-1}\sin\theta_2)$

$= |z_1||z_2| ((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + (\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1)\sqrt{-1})$

$= |z_1||z_2| (\cos(\theta_1+\theta_2) + \sqrt{-1}\sin(\theta_1+\theta_2))$

命题 设 $z = |z|(\cos\theta + \sqrt{-1}\sin\theta)$

则 (i) $\forall n \in \mathbb{N}$

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

(ii) 若 $z \neq 0$ 则

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

证: (i) 对 n 归纳. $n=0$ ✓

设 $n>0$. 且 z^{n-1} 结论成立

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

$|z|(\cos\theta + \sqrt{-1}\sin\theta)$

$= |z|^n(\cos(n\theta) + \sqrt{-1}\sin n\theta)$ ✓

$z \cdot \frac{1}{|z|}(\cos\theta - \sqrt{-1}\sin\theta)$

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

$= 1.$

欧拉公式:

$e^{i\theta} = \cos\theta + \sqrt{-1}\sin\theta, \quad \theta \in \mathbb{R}$

欧拉公式之证

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

$$e^{i\theta} = \sum_{n=0}^{\infty} \frac{(i\theta)^n}{n!} \qquad i = \sqrt{-1}$$

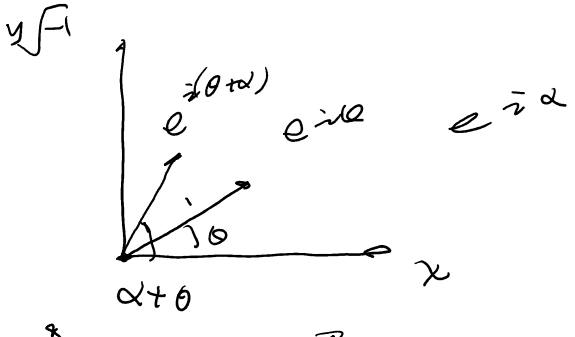
$$= \sum_{k=0}^{\infty} \frac{(i\theta)^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{(i\theta)^{2k+1}}{(2k+1)!}$$

$\cos\theta$ $\qquad$ $i\sin\theta$

$$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

$$(e^{i\theta})^{-1} = e^{-i\theta}$$

$$(e^{i\theta})^n = e^{in\theta}$$



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

§3.3 幂主根

设 $n \in \mathbb{Z}^+$, 方程

$z^n=1$ 在 $\mathbb{C}$ 中的解称为

n次单位根.

命题: 方程 $z^n=1$ 在 $\mathbb{C}$ 中

有 n 个互不相同的单位根

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

$(i=\sqrt{-1})$

证明:

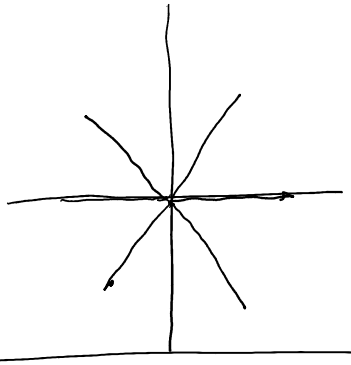
$$\varepsilon_k^n = \left(e^{\frac{2k\pi i}{n}}\right)^n$$

$$= e^{2k\pi i} = \cos 2k\pi + i \sin 2k\pi$$

$$=1$$

于是 $\varepsilon_0, \varepsilon_1, \cdots \varepsilon_{n-1}$ 是 $z^n=1$

的 n 个根.



于是 $\varepsilon_0, \varepsilon_1, \cdots \varepsilon_{n-1}$

互不相同

设 U_n 是 $\mathbb{C}$ 中所有 n 次单位根的集合

设 U_n 是 $\mathbb{C}$ 中所有 n 次单位根的集合

命题 $(U_n, \cdot 1)$ 是循环群

且 ε_k 是 U_n 的生成元

$\Leftrightarrow \gcd(k, n) = 1$

证：设 $\varepsilon_k, \varepsilon_m \in U_n$

$$(\varepsilon_k \varepsilon_m^{-1})^n = \varepsilon_k^n (\varepsilon_m^n)^{-1}$$
$$= 1 \cdot 1 = 1$$

$\Rightarrow (\varepsilon_k \varepsilon_m^{-1}) \in U_n$

由子群判别法可知 U_n 是 $(\mathbb{C}^*, \cdot 1)$ 的子群，其中 $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$$U_n = \{\varepsilon_0, \varepsilon_1, \varepsilon_2, \cdots \varepsilon_{n-1}\}$$
$$\varepsilon_k^k = \varepsilon_k, \quad k = 0, 1, 2, \cdots n-1.$$

于是 $U_n = \langle \varepsilon_1 \rangle$.

设 $k \in \{1, \cdots n-1\}$ 使得 $k \in \{0, 1, \cdots n\}$

$\gcd(k, n) = 1$

由 Bezout 关系

$\exists u, v \in \mathbb{Z}$ $uk + vn = k$

$$\varepsilon_1^k = \varepsilon_1^{uk+vn} = (\varepsilon_1^k)^u (\varepsilon_1^n)^v = (\varepsilon_k)^u$$

$$\varepsilon_k = \varepsilon_1^k = \varepsilon_1^{ul+vn} = (\varepsilon_1^l)^u (\varepsilon_1^n)^v = (\varepsilon_l)^u$$

$$\Rightarrow \varepsilon_k \in \langle \varepsilon_l \rangle$$

$$\Rightarrow U_n \subset \langle \varepsilon_l \rangle$$

$$\Rightarrow U_n = \langle \varepsilon_l \rangle$$

设 $U_n = \langle \varepsilon_l \rangle$

则 $\exists u \in \mathbb{Z}$, 使得

$$\varepsilon_l^u = \varepsilon_1$$

$$\Rightarrow \varepsilon_1^{lu} = \varepsilon_1 \Rightarrow \varepsilon_1^{lu-1} = 1$$

$\because \operatorname{ord}(\varepsilon_1) = n$

$\therefore n \mid (lu-1) \Rightarrow \exists v \in \mathbb{Z}$

$$lu - 1 = nv \Rightarrow lu + (-v)n = 1$$

$$\Rightarrow \gcd(l, n) = 1.$$

定义: 如果 $U_n = \langle \varepsilon_l \rangle$, 则称 ε_l 是单原始根