回忆 设 F 是域，$f,g\in F[x]\setminus\{0\}$

如果 $\gcd(f,g)=1$，则称 f 和 g 互素

定理2.8. 设 F 是域，$f,g\in F[x]\setminus\{0\}$

则 f 和 g 互素 $\Leftrightarrow \exists u,v\in F[x]$ 使得

$$uf+vg=1$$

证："$\Rightarrow$" 由定理2.7和上述定义直接可得

"$\Leftarrow$" 显然1是 f 和 g 的公因子. 由引理2.1(ii)

f 和 g 的任何公因子都整除1，于是

f 和 g 互素 ☐

记号：给定 $f\in F[x]$，$A\in M_n(F)$.

K_f 记系数矩阵为 $f(A)$ 的齐次

线性方程组的解空间 $V_{f(A)}$.

按核分解

定理2.9 设 $f,g\in F[x]\setminus\{0\}$，互素

$A\in M_n(F)$. $fg(A)=O_{n\times n}$

则 $F^n=K_f\oplus K_g$ ①

证：先证：$K_f\cap K_g=\{\vec{0}\}$.

设 $\vec{x}\in K_f\cap K_g$. ⊕ $\because f,g$ 互素

$\exists u,v\in F[x]$ 使得

$$u(x)f(x)+v(x)g(x)=1$$

代入 A 得

$$u(A)f(A)+v(A)g(A)=E \quad (*)$$

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

$$u(A)[f(A)\vec{x}]+v(A)[g(A)\vec{x}]=\vec{x}$$

$\because \vec{x}\in K_f\cap K_g \quad \therefore f(A)\vec{x}=g(A)\vec{x}=\vec{0}$

$\Rightarrow \vec{x}=\vec{0}$

$\Rightarrow K_f\cap K_g=\{\vec{0}\}$

再证：$F^n=K_f+K_g$

设 $\vec{x}\in F^n$. 由 (*)

$$\vec{x}=\underbrace{u(A)f(A)\vec{x}}_{\vec{y}}+\underbrace{v(A)g(A)\vec{x}}_{\vec{z}}$$

$g(A)\vec{y} = g(A)u(A)f(A)\vec{x}$

$= u(A)f(A)g(A)\vec{x}$ [$\because F[A]$ 是交换环]

$= u(A)[(fg)(A)\vec{x}]$ [$\because$ 对试值是同态

$= u(A)\vec{0}$ [$\because K_{fg} = F^n$

$= \vec{0}$

$\Rightarrow \vec{y} \in K_g$ 同理 $\vec{z} \in K_f$

于是 $\vec{x} = \vec{y} + \vec{z} \in K_g + K_f$

$\Rightarrow F^n = K_f \oplus K_g$ ☒

例：设 $A \in M_n(F)$，$A^2 = E$

证明：当 $\mathrm{char}(F) \neq 2$ 时

$V_{A+E} \oplus V_{A-E} = F^n$

并说明当 $\mathrm{char}(F) = 2$ 时

上述结论不成立.

证：设 $p(x) = x^2 - 1$

$p(A) = A^2 - E = O$

$p(x) = \underbrace{(x+1)}_{f}\underbrace{(x-1)}_{g}$

当 $\mathrm{char}(F) \neq 2$ 时 $1 \neq -1 \Rightarrow f, g$ 互素

$fg(A) = O$. 于是

$F^n = K_f \oplus K_g$ (定理2.9)

$= V_{A-E} \oplus V_{A+E}$

设 $F = \mathbb{Z}_2$ $A = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$, $A^2 = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$

$A+E = A-E = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix}$

$V_{A+E} = V_{A-E} = \langle \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix} \rangle$ $V_{A+E} + V_{A-E} = V_{A+E}$

和不直，也不是整个空间.

§3 因式分解

在本节中 D 是整环，F 是域

$D^* = D \setminus \{0\}$, $F^* = F \setminus \{0\}$

§3.1 不可约元和素元

定义：设 $a \in D^*$ 且不可逆. 如果 a 不能写成两个不可逆元之积，则称 a 是不可约元（既约元）(irreducible element). 如果 $\forall b, c \in D^*$

$$a \mid (bc) \Longrightarrow a \mid b \text{ 或 } a \mid c$$

则称 a 是素元（prime element）

例. 在 $\mathbb{Z}$ 中的不可约元是素数（可正可负）. 它们也都是素元

（见第1章引理6.2）

例：$F[x]$ 中的不可约元称为 $F[x]$ 中的不可约多项式. 它们的次数必为正. 显然. 一次多项式都是不可约的.

例. $x^2 - 2$ 在 $\mathbb{Q}[x]$ 中不可约. 但在 $\mathbb{R}[x]$ 中可约

引理 3.1 设 F 是域. 则 $F[x]$ 中的不可约元是素元

证明：设 $p \in F[x]$ 不可约，$f, g \in F[x]$

$p \mid (fg)$. 再设 $p \nmid f$. 则

$\gcd(f, p) = 1$. [$\because p$ 不可约]

由 Bezout 定理，$\exists u, v \in F[x]$ 使得

$$uf + vp = 1$$

$$\Longrightarrow ufg + vpg = g$$

$\because p \mid (fg)$ 且 $p \mid pg$ $\therefore p \mid g$ [引理3.1(iii)]

□

命题3.1 设 $p \in D^*$ 是素元，则 p 是不可约元

证：假设 p 不是不可约元，则 $\exists a, b \in D^*$ 不可逆，使得 $p = ab$. 不妨设 $p \mid a$，则 $a = cp$，$c \in D^*$

$\Rightarrow p = cpb \Rightarrow p(1-cb) = 0$

$\Rightarrow$ 由消去律，$1 = cb \Rightarrow b$ 可逆 →←

定义：设 $a \in D^*$，如果存在可逆元 $\varepsilon \in D$ 和不可约元 $p_1, \cdots, p_s \in D^*$ 使得

$$a = p_1 \cdots p_s \quad (*)$$

则称 a 在 D 中有不可约分解，称 $p_1, \cdots, p_s$ 为 a 的不可约因子

注：

例：$\mathbb{Z}^*$ 中整数有不可约分解（见第一章定理6.4）

命题3.2 $F[x] \setminus \{0\}$ 中多项式都有不可约分解.

证：设 $f \in F[x]$，$\deg f = d$

$d = 0$ 和 $d = 1$ 时结论显然成立.

设 $d > 1$，且结论对次数小于 d 的多项式都成立.

如果 f 本身不可约，则结论成立.

再设 $f = gh$，其中 $g, h \in F[x] \setminus F$

由 $d = \deg(g) + \deg(h)$ [命题2.2(iii)]

$0 < \deg(g) < d$，$0 < \deg(h) < d$

由归纳假设，g, h 有不可约分解

把这两个不可约分解相乘得到 f 的不可约分解 □

§3.2 唯一因子分解整环

(Unique factorization domain, UFD)

定义：如果 D^* 中每个元素都有不可约分解

且 当

$$a = u p_1 \cdots p_m = v q_1 \cdots q_n$$

其中 u, v 可逆，$p_1, \cdots, p_m, q_1 \cdots q_n$ 不可约，都有

$m = n$，和适当调整下标后

$p_1 \sim q_1$，…，$p_m \sim q_m$

则称 D 是 UFD.

例：设 $f(x) = (x-1)(3x-1)(-6x-2)(-x+1)$

$24 = 2 \times 2 \times 2 \times 3 = 3 \times (-2) \times 2 \times (-2)$

$3 \sim 3$ $2 \sim -2$，$2 \sim (-2)$，$2 \sim 2$

定理 3.1 设 D^* 中每个元素都有不可约分解. 则

D 是 UFD $\Leftrightarrow$ D 中的每个不可约元都是素元

证："$\Rightarrow$" 设 p 是 D 中不可约元，$a, b \in D^*$

使得 $p \mid (ab)$，且 $p \nmid a$.

我们来证 $p \mid b$.

设 $a = u p_1 \cdots p_m$ 其中，u, v 可逆

$b = v q_1 \cdots q_n$ $p_1, \cdots p_m, q_1 \cdots q_n$ 不可逆

因为 $p \in D$ 使得 $ab = cp$.

设 $c = w r_1 \cdots r_s$，其中 w 可逆. $r_1 \cdots r_s$ 可逆

则 $cwr_1 \cdots r_s p = uv p_1 \cdots p_m q_1 \cdots q_n$

$\because$ D 是 UFD 且 $p \nmid a$. $\therefore$

$\exists j \in \{1, \cdots n\}$ 使得

$p \sim q_j$

不妨设 $j=1$. 则 $p=\alpha q_1$，其中 α 可逆

$$b=u\alpha^{-1}(\alpha q_1)q_2\cdots q_n=u\alpha^{-1}p(q_2\cdots q_n)$$

$\Rightarrow p\mid b$

"$\Leftarrow$" 设 $a=up_1\cdots p_m=vq_1\cdots q_n$

其中 $u,v\in D$ 可逆. $p_1,\cdots p_m, q_1,\cdots,q_n\in D^*$

不可约. 不妨设 $m\le n$

$\because u,v$ 可逆 $\therefore p_1\mid(q_1\cdots q_n)$

$\because p_1$ 是素元 $\therefore \exists\, j\in\{1,2,\cdots n\}$ 使得

$$p_1\mid q_j$$

~~通过调整下标后~~. 不妨设 $j=1$.

$\because q_1$ 不可约 $\therefore p_1\sim q_1$.

于是 $\exists\,\beta_1\in D$ 可逆 使得 $q_1=\beta_1 p_1$

则 $up_1p_2\cdots p_m=v\alpha_1p_1q_2\cdots q_n$

由消去律 $up_2\cdots p_m=(v\alpha_1)q_2\cdots q_n$

对上式重复上述步骤 得到 ⑥

$q_2=\beta_2p_2$，其中 β_2 可逆

从而 $up_3\cdots p_m=(v\beta_1\beta_2)q_3\cdots q_n$.

重复有限次后得 $p_1\sim q_1, p_2\sim q_2,\cdots p_m\sim q_m$

且 $u=(v\beta_1\cdots\beta_m)q_{m+1}\cdots q_n$

$\Rightarrow 1=(u^{-1}v\beta_1\cdots\beta_m)q_{m+1}\cdots q_n$

$\Rightarrow q_{m+1},\cdots q_n$ 可逆. $\rightarrow\leftarrow$

$\Rightarrow m=n$ $1=(u^{-1}v\beta_1\cdots\beta_m)$. 证毕

推论 3.1. $\mathbb{Z}$ 和 $F[x]$ 都是 UFD

证: 由第一章引理 6.2 $\mathbb{Z}$ 中素元和不可约元相同. 由第一章定理 6.4 $\mathbb{Z}$ 中的非零元有不可约分解

由定理 3.1, $\mathbb{Z}$ 是 UFD

由引理 3.1 $F[x]$ 中不可约元是素元

由命题 3.2 $F[x]$ 非零元有不可约分解

由定理 3.2. $F[x]$ 是 UFD

注：$\mathbb{Z}$ 是 UFD 称为算术基本定理.

§3.3 重数

定义：设 D 是 UFD，p 是 D 中不可约元，$a \in D^*$，如果 $m \in \mathbb{N}$，满足 $p^m \mid a$ 但 $p^{m+1} \nmid a$，则称 m 是 p 在 a 中的重数

例：$24 = 2^3 \cdot 3$　　2 在 24 中重数是 3

3 在 24 中重数是 1，5 在 24 中重数是 0

$$f(x) = (x-1)(3x+1)^2(x^2+1) \in \mathbb{Q}[x]$$

$x-1$ 在 f 中重数是 1

$3x+1$ 在 f 中重数是 2

x^2+1 ------ 1

定义：设 $F \subset K$ 是两个域，$\alpha \in K$，$f \in F[x] \setminus F$（$f \in K[x]$），$f(\alpha)=0$，$(x-\alpha)$ 在 f 中的重数称为根 α 的重根，当重数为 1 时，α 称为 f 的单根，否则为重根

注：在上述例子中，1 是 f 单根

$-\frac{1}{3}$ 是 f 的二重根，$\pm i$ 是 f 的单根.

命题 3.3. 设 $F \subset K$ 是两个域，$\alpha \in K$，$f \in F[x] \setminus F$，F 在 K 中互不相同的根为 $\alpha_1 \cdots \alpha_s$，其重数为 $m_1, \cdots m_s$

则 $m_1 + \cdots + m_s \leq \deg(f)$.

证：设 $d = \deg(f)$，对 d 归纳

$d=1$ 时 f 只有一个单根，结论成立

设结论对 $K[x]$ 中次数小于 d 的多项式都成立.

$f(x) = g(x)(x-\alpha_s)^{m_s}$，其中

$g(x) \in K[x]$，$g(\alpha_s) \neq 0$，$\deg g < \deg f$

$\forall i \in \{1,2,\cdots s-1\}$ $\because \alpha_i \neq \alpha_s$

$(x-\alpha_i)^{m_i}$ 与 $(x-\alpha_s)^{m_s}$ 互素

$\exists u, v \in K[x]$ 使得

$$u(x)(x-\alpha_i)^{m_i} + v(x)(x-\alpha_s)^{m_s} = 1$$

$$u(x)(x-\alpha_i)^{m_i} g(x) + v(x)(x-\alpha_s)^{m_s} g(x) = g(x)$$

$$u(x)(x-\alpha_i)^{m_i} g(x) + v(x) f(x) = g(x)$$

$\Rightarrow$ $(x-\alpha_i)^{m_i} \mid g(x)$，$i = 1,2,\cdots s-1$

$\Rightarrow$ $\deg(g) \geq m_1 + \cdots + m_{s-1}$ (归纳的假设)

$\Rightarrow$ $\deg(f) \geq m_1 + \cdots + m_{s-1} + m_s$ ▨

§3.4 $\mathbb{Q}[x]$ 中的因式分解

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

当 $m=1$，$\gcd(a_1, a_2, \cdots, a_m) = a_1$

当 $m>1$，时 $d \in \mathbb{Z}$ 称为 $a_1, \cdots a_m$ 的最大公因子，如果 d 是 $a_1, \cdots a_m$ 的公因子且 $a_1, \cdots a_m$ 的任意公因子的倍数.

记为 $\gcd(a_1, a_2, \cdots a_m)$

注：当 $m>1$ 时

$$\gcd(a_1, a_2, \cdots a_m) = \gcd(a_1, \gcd(a_2, \cdots a_m))$$

(自己验证)

证明：设 $a_1, a_2, \cdots, a_m \in \mathbb{Z}$，不全为零

$\gcd(a_1, a_2, \cdots a_m)$ 是 $a_1, a_2, \cdots a_m$ 中非零整数的最大公因子.

定义：设 $f \in \mathbb{Z}[x] \setminus \{0\}$ 写成

$$f = f_d x^d + f_{d-1} x^{d-1} + \cdots + f_0, \quad f_i \in \mathbb{Z}$$

f 的容度（content）是 $\gcd(f_d, f_{d-1}, \cdots f_0)$

记为 $\mathrm{cont}(f)$. 如果 $\mathrm{cont}(f)=1$, 则称 f 是本原的

例：设 $f = 2x^2+3x-2$, $g = 24x^3+3x-12$

$$\mathrm{cont}(f) = \gcd(2,3,2) = 1$$

$$\mathrm{cont}(g) = \gcd(24,3,-12) = 3$$

引理 3.2 设 p 是素数

(i) 令 ξ_p：$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$

$$f = \sum_{i=0}^{d} f_i x^i \mapsto \sum_{i=0}^{d} \bar{f}_i x^i$$

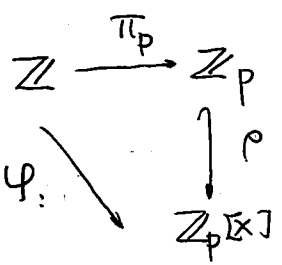
其中 $f_i \in \mathbb{Z}$, $\bar{f}_i$ 是 f_i 在 $\mathbb{Z}_p$ 中的同余类. 则 ξ_p 是环同态

(ii) 如果 $f \in \mathbb{Z}[x]$ 是本原的，则 $\xi_p(f) \neq 0$ ⑨

证：(i) π_p：$\mathbb{Z} \to \mathbb{Z}_p$（商映射）

ρ：$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p[x]$

$\bar{a} \mapsto \bar{a}$



（嵌入）

$\because$ π_p, ρ 是环同态

$\therefore$ $\varphi = \rho \circ \pi_p$ 是环同态

由赋值同态定理：

φ_x：$\mathbb{Z}[x] \to \mathbb{Z}[x]$ 是环同态

而 $\xi_p = \varphi_x$

(ii) ⊙ 若 $\xi_p(f) = 0$

则 $\bar{f}_0 = \bar{f}_1 = \cdots = \bar{f}_d = 0$

$\Rightarrow p \mid f_0, p \mid f_1, \cdots, p \mid f_d$

$\Rightarrow \mathrm{cont}(f) \neq 1$. $\to\leftarrow$ ☒

例：列出 $\mathbb{Z}_2[x]$ 中所有首一的二次多项式，并找出其中不可约元

证：$x^2+\alpha x+\beta$，$\alpha,\beta\in\mathbb{Z}_2$

x^2，x^2+x，$x^2+\bar{1}$，$x^2+x+\bar{1}$（不可约）

例：证明：$f=x^4+x+1$ 不能写成两个整系数的非零次多项式之积

解：假设

$$f=(a_2x^2+a_1x+a_0)(b_2x^2+b_1x+b_0)$$

$a_2b_2=1$．不妨设 $a_2=b_2=1$

类似当 f 是一个一次一个三次多项式之积时，这两个因子也可假设是首一的

设 $f=gh$，其中 $g,h\in\mathbb{Z}[x]$ 首一

$$\xi_2(f)=\xi_2(g)\xi_2(h)$$

$\xi_2(f)=x^4+x+\bar{1}$

∵ $\bar{0},\bar{1}$ 都不是 $\xi_2(f)$ 的根

∴ $\xi_2(g)$，$\xi_2(h)$ 次数是 2 且不可约

$\xi_2(f)=(x^2+x+\bar{1})^2=x^4+x^2+\bar{1}$ → ← ☒

Gauss 引理：设 $f,g\in\mathbb{Z}[x]$ 本原，则 fg 也是本原的

证：假设 fg 不是本原的，则存在素数 p 满足 $p\mid \mathrm{cont}(fg)$

于是 $\xi_p(fg)=\bar{0}$

$\Rightarrow$ $\xi_p(f)\xi_p(g)=\bar{0}$ [引理 3.2(i)]

∵ $\mathbb{Z}_p[x]$ 是整环

∴ $\xi_p(f)=\bar{0}$ 或 $\xi_p(g)=\bar{0}$

与引理 3.2(ii) 矛盾 ☒

注：$\forall f\in\mathbb{Z}[x]\setminus\{0\}$

$f=\mathrm{cont}(f)\tilde{f}$，其中 $\tilde{f}\in\mathbb{Z}[x]$ 本原

例：$f=-3x^3-6x+6=3(-x^3-2x+2)$

定理 3.2 设 $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ 如果 f 不能写成 $\mathbb{Z}[x]$ 中两个正次数的多项式之积，则 f 在 $\mathbb{Q}[x]$ 中不可约.

证: 假设 f 在 $\mathbb{Q}[x]$ 中可约. 则

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

通过适当系数的公因子得

$$uf = v\, g_1 h_1.$$

其中, $u, v \in \mathbb{Z}$, 互素, $g_1, h_1 \in \mathbb{Z}[x] \setminus \mathbb{Z}$

本原

如果 $u > 1$. 则 $\exists$ 素数 $p \mid u$

$$\xi_p(uf) = \xi_p(v g_1 h_1)$$

$$\xi_p(u)\, \xi_p(f) = \xi_p(v)\, \xi_p(g_1)\, \xi_p(h_1)$$

$\|$ $\neq$ 由引理 3.2 (ii)

$\overline{0}$ $\overline{0}$

□

定理 3.3 (Eisenstein 判别法) ⑪

设 $n > 1$, $f = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0 \in \mathbb{Z}[x]$, 其中 $f_i \in \mathbb{Z}$. 设 p 是素数. 如果 $p \mid f_{n-1}, \cdots, p \mid f_1, p \mid f_0$ 但 $p^2 \nmid f_0$.

则, f 在 $\mathbb{Q}[x]$ 中不可约

证: 假设 f 在 $\mathbb{Q}[x]$ 中可约

则 $f = gh$, $g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$ 首一

$\deg(g) = d < n$, $\deg h = e < n$

[∵ 定理 3.2 和 f 首一]

设 $g = x^d + g_{d-1}x^{d-1} + \cdots + g_0$

$h = x^e + h_{e-1}x^{e-1} + \cdots + h_0$

由 $f = gh$ 可得 $f_0 = g_0 h_0$

$$\xi_p(f) = \xi_p(g)\, \xi_p(h)$$

$$x^n = (x^d + \overline{g}_{d-1}x^{d-1} + \cdots + \overline{g}_0)(x^e + \overline{h}_{e-1}x^{e-1} + \cdots + \overline{h}_0)$$

∵ $\mathbb{Z}_p[x]$ 是 UFD 由唯一因式分解环

∴ 因 $\overline{g}_0 = \overline{0}$, $\overline{h}_0 = \overline{0}$ $\Rightarrow p \mid g_0, p \mid h_0$

$\Rightarrow p^2 \mid f_0$ ✗

□

例：证明：x^n+2x+2 在 $\mathbb{Q}[x]$ 中不可约。$(n\geq 2)$

证：取 $p=2$，$p\mid 2$，$p^2\nmid 2$，后项

由 Eisenstein 判别法，x^n+2x+2 在 $\mathbb{Q}[x]$ 中不可约。

例：设 p 是素数，证明 $x^{p-1}+x^{p-2}+\cdots+1$ 在 $\mathbb{Q}[x]$ 中不可约

证：$\sigma:\mathbb{Z}[x]\longrightarrow\mathbb{Z}[x]$

$\sum_{i=0}^{d} f_i x^i \longmapsto \sum_{i=0}^{d} f_i(x+1)^i$，$f_i\in\mathbb{Z}$

是环同态 [对于 $\mathbb{Z}\hookrightarrow\mathbb{Z}[x]$ 在 $x+1$ 处的赋值同态]

同理 $\tau:\mathbb{Z}[x]\to\mathbb{Z}[x]$

$\sum_{i=0}^{d} f_i x^i \mapsto \sum_{i=0}^{d} f_i(x-1)^i$

也是同态

$\sigma\tau(f(x))=\sigma(f(x-1))=f(x-1+1)=f(x)$ (12)

$\sigma\circ\tau=id_{\mathbb{Z}[x]}$，同理 $\tau\circ\sigma=id_{\mathbb{Z}[x]}$

设 $h(x)=x^{p-1}+x^{p-2}+\cdots+1$

$\sigma(h)=h(x+1)=\dfrac{(x+1)^p-1}{x+1-1}$

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

$\because p\mid\binom{p}{k}$，$k=1,2,\cdots p-1$，$p^2\nmid\binom{p}{p-1}=p$

$\Rightarrow h(x+1)$ 在 $\mathbb{Z}[x]$ 中不可约

$\Rightarrow h(x)$ 在 $\mathbb{Z}[x]$ 中也不可约

[$\because\sigma$ 是同构]

§1 复数

$x^2+1=0$ 没有实根

令 $i^2=-1$. 则 $i, -i$ 是上述方程的解

§1.1 复数域

设 $\mathbb{C}=\{x+yi \mid x, y\in\mathbb{R}\}$

$+:\ \mathbb{C}\times\mathbb{C}\longrightarrow\mathbb{C}$

$(x+yi, a+bi)\longmapsto (x+a)+(y+b)i$

$\cdot:\ \mathbb{C}\times\mathbb{C}\longrightarrow\mathbb{C}$

$(x+yi, a+bi)\longmapsto (xa-yb)+(xb+ya)i$

验证: $(\mathbb{C}, +, 0)$ 是交换 group 类群

其中 $0=0_{\mathbb{R}}+0_{\mathbb{R}}i$

验证过程与 $\mathbb{R}^2$ 中加法 $(\mathbb{R}^2, +, \vec{0})$ 是交换群类似

验证:

$(\mathbb{R}, \cdot, 1)$ 是含幺交换半群

其中 $1=1_{\mathbb{R}}+0\cdot i$

设 $z_1=x_1+y_1i$, $z_2=x_2+y_2i$

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

$=z_2z_1$ ($\because$ $\mathbb{R}$ 中乘法交换)

交换律成立

再设 $z_3=x_3+y_3i$

$(z_1z_2)z_3=(x_1x_2x_3-y_1y_2x_3-x_1y_2y_3-x_2y_1y_3)$

$+(x_1x_3y_2+x_3x_2y_1+x_1x_2y_3-y_1y_2y_3)i$

$z_1(z_2z_3)=(x_1+y_1i)[(x_2x_3-y_2y_3)+(x_2y_3+x_3y_2)i]$

$=(x_1x_2x_3-x_1y_2y_3-y_1x_2y_3-y_1x_3y_2)$

$+(x_1x_2y_3+x_1x_3y_2+y_1x_2x_3-y_1y_2y_3)i$

结合律成立

$(x_1+y_1i)(1_{\mathbb{R}}+0i)=x_1+y_1i$.

验证完

分配律.

$$z_1(z_2+z_3) = (x_1+y_1\mathrm{i})[(x_2+y_2\mathrm{i})+(x_3+y_3\mathrm{i})]$$
$$= (x_1+y_1\mathrm{i})[(x_2+x_3)+(y_2+y_3)\mathrm{i}]$$
$$= (x_1x_2+x_1x_3-y_1y_2-y_1y_3)+$$
$$(x_1y_2+x_1y_3+y_1x_2+y_1x_3)\mathrm{i}$$

$$z_1z_2+z_1z_3 = (x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)\mathrm{i}$$
$$+(x_1x_3-y_1y_3)+(x_1y_3+x_3y_1)\mathrm{i}$$

$$= (x_1x_2+x_1x_3-y_1y_2-y_1y_3)+(x_1y_2+x_2y_1+x_1y_3+x_3y_1)\mathrm{i}$$

分配律成立

于是 $(\mathbb{C}, +, 0, \cdot, 1)$ 是交换环

设 $z = x+y\mathrm{i}$, $x \neq 0_{\mathbb{R}}$ 或 $y \neq 0_{\mathbb{R}}$

$$z(x-y\mathrm{i}) = (x+y\mathrm{i})(x-y\mathrm{i}) = x^2+y^2.$$

$$w = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}\mathrm{i}$$

$zw = 1$ $(\mathbb{C}, +, 0, \cdot, 1)$ 是域

注: $\varphi: \mathbb{R} \longrightarrow \mathbb{C}$

$$x \longmapsto x+0_{\mathbb{R}}\mathrm{i}$$

是域同态.

通过嵌用符号 可以为 $\mathbb{R} \subset \mathbb{C}$

$\forall r \in \mathbb{R}$, $z = x+y\mathrm{i} \in \mathbb{C}$

$$rz = rx+ry\mathrm{i}$$

当 $x=0$ 时 $z = 0+y\mathrm{i} = y\mathrm{i}$

$$\mathrm{i}^2 = (0+1\mathrm{i})(0+1\mathrm{i}) = -1.$$

注: $\mathbb{C}$ 中的元素称为复数.

i 是虚单位

$z = x+y\mathrm{i} \in \mathbb{C}$, $x, y \in \mathbb{R}$

x 称为 z 的实部. 记为 $\mathrm{Re}(z)$

y 称为 z 的虚部. 记为 $\mathrm{Im}(z)$.

$(\mathbb{C}, +, 0, \cdot, 1)$ 称为复数域

注：$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

定义：设 $z = x+yi \in \mathbb{C}$，$x, y \in \mathbb{R}$

则 $x-yi$ 称为 z 的共轭，记作 $\bar{z}$

命题1.1. $\varphi: \mathbb{C} \longrightarrow \mathbb{C}$ 是同构
$z \longmapsto \bar{z}$

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

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

$$\varphi(z_1 z_2) = \varphi\big((x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)i\big)$$
$$= x_1x_2-y_1y_2-(x_1y_2+x_2y_1)i$$

$$\varphi(z_1)\varphi(z_2) = (x_1-y_1 i)(x_2-y_2 i)$$
$$= (x_1x_2-y_1y_2)+(-x_1y_2-x_2y_1)i$$

$$\Rightarrow \quad \varphi(z_1z_2) = \varphi(z_1)\varphi(z_2)$$

$$\varphi(1) = 1-0i = 1.$$

φ 是双射. $\because \varphi \circ \varphi = id_{\mathbb{C}} \Rightarrow \varphi$ 是对合

φ 是双同态. □

注：利用上述命题，$\forall z_1, z_2 \in \mathbb{R}$

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

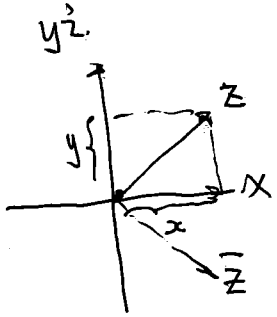
$z = x+yi$，$x, y \in \mathbb{R}$

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

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

§1.2 复数的几何意义

$z = x+yi$，$x, y \in \mathbb{R}$



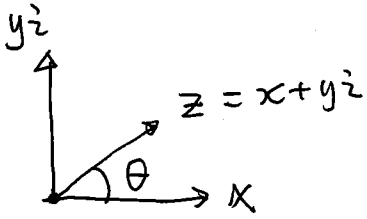
$\sqrt{z\bar{z}}$ 是 z 的"长度"

记为 $\|z\|$.

$\|z\| = 0 \Leftrightarrow x = y = 0 \Leftrightarrow z = 0$

当 $z \neq 0$ 时 $z^{-1} = \dfrac{\bar{z}}{\|z\|^2}$

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



θ 称为 z 的幅角

记为 $\arg(z)$

通常 $\theta \in [0, 2\pi)$

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

↓ 坐标表示　　↓ 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 $z_1 z_2 = \|z_1\|\|z_2\|(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))$

(ii) 设 $z = \|z\|(\cos\theta + i\sin\theta)$, $n \in \mathbb{N}$

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

(iii) 若 $z \neq 0$

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

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

$= \|z_1\|\|z_2\|\left[(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + (\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1)i\right]$

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

(ii) $n=0, 1$. 显然. 设 $n-1$ 时结论成立

$z^n = z^{n-1}z = \|z\|^{n-1}[\cos(n-1)\theta + i\sin[(n-1)\theta]](\cos\theta + i\sin\theta)$ [归纳]

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

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

$= 1$.

注: 由 (ii) 与 (iii) 可知: 当 $z \neq 0$ 时

$\forall n \in \mathbb{N}$　　$z^n = \|z\|^n(\cos n\theta - i\sin n\theta)$

§1.3 Euler 公式

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

$\theta \in \mathbb{R}$

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

$e^{ix} = \sum_{n=0}^{\infty} \frac{(ix)^n}{n!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} i^n$

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

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

$$\cos x \qquad\qquad \sin x$$

$$\Rightarrow \forall x \in \mathbb{R} \quad e^{ix} := \cos x + i \sin x$$

$$\forall x = \pi \quad e^{i\pi} = -1 \iff e^{i\pi} + 1 = 0$$

$$\forall z = \|z\| (\cos\theta + i \sin\theta) = \|z\| e^{i\theta}.$$