第五章　复数域和多项式

1.5　多项式的根

定义 1.22 设 F 和 K 是域, 且 F 是 K 的子域. 设 $f \in F[x]$ 且 $\alpha \in K$. 如果 $f(\alpha) = 0$, 则称 α 是 f 在 K 中的一个根*(root)*, 即 α 是方程 $f(x) = 0$ 在 K 中的一个解.

例 1.23 多项式 $x^2 - 2 \in \mathbb{Q}[x]$ 在 $\mathbb{R}$ 中有根 $\pm\sqrt{2}$. 但它在 $\mathbb{Q}$ 中无根.

命题 1.24 设 F 是域, $f \in F[x]$ 且 $\deg(f) = n > 0$. 则 $\alpha \in F$ 是 f 的根当且仅当 $\mathrm{rem}(f, x - \alpha) = 0$;

证明. 由余式定理可知,

$$f(\alpha) = 0 \iff \mathrm{rem}(f, x - \alpha) = 0. \quad \square$$

定理 1.25 设 F 是域, $f \in F[x]$ 且 $\deg(f) = n > 0$. 则 f 在域 F 中至多有 n 个互不相同的根.

证明. (法 1). 对 n 归纳. 当 $n = 1$ 时, $f = f_1 x + f_0$, $f_1, f_0 \in F$ 且 $f_1 \neq 0$. 则 f 的唯一的根是 $-f_1^{-1} f_0$. 结论成立.

设 $n > 1$ 且结论对 $n - 1$ 成立. 如果 f 在 F 中没有根, 则结论显然成立. 否则, 设 $\alpha \in F$ 是 f 的一个根. 根据命题

1.24, $f(x)=g(x)(x-\alpha)$, 其中 $g\in F[x]$ 且 $\deg(g)=n-1$. 再设 β 是 f 的一个不同于 α 的根. 则

$$0=f(\beta)=g(\beta)(\beta-\alpha).$$

故 $g(\beta)=0$. 由归纳假设可知, g 至多有 $n-1$ 个互不相同的根. 故 f 至多有 n 个互不相同的根.

(法 2) 假设 f 有 n 个互不相同的根, $\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1}\in F$. 再令

$$f(x)=f_nx^n+\cdots+f_1x+f_0,\quad f_k\in F.$$

则

$$f_n\alpha_i^n+\cdots+f_1\alpha_i+f_0=0,\quad i=1,2,\ldots,n+1.$$

故

$$\underbrace{\begin{pmatrix}1&\alpha_1&\ldots&\alpha_1^n\\1&\alpha_2&\ldots&\alpha_2^n\\\vdots&\vdots&\ddots&\vdots\\1&\alpha_n&\ldots&\alpha_n^n\end{pmatrix}\begin{pmatrix}f_0\\f_1\\\vdots\\f_n\end{pmatrix}}_{A}=\mathbf{0}_{n+1}$$

注意到 A 是 $n+1$ 阶范德蒙德矩阵且其行列式非零, 故 $f_n=f_{n-1}=\cdots=f_0=0$. 与 $\deg(f)>0$ 矛盾. □

例 1.26 对任意 $a\in\mathbb{R}$, 矩阵 $\begin{pmatrix}0&a\\0&0\end{pmatrix}$ 都是 $f(x)=x^2$ 的根.

期末小结

矩阵部分

设 F 是域.

1. 方阵

   (a) $(\mathrm{M}_n(F), +, O, \cdot, E)$ 是非交换环且对任意 $\lambda \in F$, $A, B \in \mathrm{M}_n(F)$,

   $$\lambda(A+B) = \lambda A+\lambda B, \quad \lambda(AB) = (\lambda A)B = A(\lambda B).$$

   (b) A 可逆当且仅当 A 满秩;

   (c) A 是左(右)零因子当且仅当 A 亏秩且 $A \neq O$;

   (d) A 是中心元当且仅当 A 是数乘矩阵(证明不要求);

   (e) $(\mathrm{M}_n(F), +, O, \cdot, E)$ 所有可逆矩阵对于乘法构成群 $\mathrm{GL}_n(F)$, 称为 F 上的一般线性群. 特别有: 对于任意 $A, B \in \mathrm{GL}_n(F)$ $\left(A^{-1}\right)^{-1} = A$ 和 $(AB)^{-1} = B^{-1}A^{-1}$.

2. 初等等价

   (a) 第 I、II、III 类初等矩阵的定义、意义和它们的逆都是同类初等矩阵;

(b) 打洞引理;

(c) 可逆矩阵是初等矩阵之积，等价地说法, $\mathrm{GL}_n(F)$ 的一组生成元是所有 F 上的 $n \times n$ 初等矩阵.

3. 矩阵求逆

(a) 行变换法,

(b) 多项式法: 设 $A \in \mathrm{M}_n(F)$. 则存在 $f \in F[A] \setminus 0$ 使得 $f(A) = 0$. 设 f 是满足上述条件的次数最小的多项式. 则 A 可逆当且仅当 $f(0) \neq 0$. 此时, 通过 f 可以求出 $g \in F[x]$ 使得 $A^{-1} = g(A)$.

4. 矩阵分块(不专门考, 利用矩阵分块证明秩的不等式不考)

行列式部分

1. 定义与性质:

(a) 行列式定义只需要加法和乘法;

$$\det((a_{i,j})_{n\times n}) = \sum_{\sigma \in S_n} \epsilon_\sigma a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

(b) 行列式多重线性斜对称, 且如果有两行或两列相同, 则行列式的值等于零;

(c) 转置保持行列式的值;

(d) 行列式乘积定理.

推论: (i) 设 $A \in \mathrm{GL}_n(F)$. 则 $\det(A^{-1}) = \det(A)^{-1}$.

(ii) $\det : \mathrm{GL}_n(F) \to (F^*, \cdot, 1)$ 是群同态.

2. 行列式的计算

(a) 利用初等行列变换化为上(下)三角形;

(b) 利用按一行一列展开找递归公式, 并用归纳法证明该公式;

(c) 利用分块矩阵计算行列式.

3. 行列式的应用

(a) 伴随矩阵和原矩阵的逆的关系. 习题

$$(AB)^\vee = B^\vee A^\vee$$

不考;

(b) Cramer 法则不专门考;

(c) 矩阵的秩和它子式的关系. 它说明秩的概念只和加法乘法有关.

群、环、域

1. 二元运算不专门考. 同余运算必考.

2. 群

    (a) 群、同态、同构、子群的定义, 子群的判别法;
    (b) 最低阶的非循环群，最低阶的非交换群;
    (c) 群和子群的生成元;
    (d) 群中元素的阶的计算;
    (e) 循环群的分类, 确定循环群的所有子群.
    (f) Lagrange 定理和 Cayley 定理不考.

3. 环

    (a) 环、同态、同构、子环, 整环的定义, 环的特征;
    (b) 广义分配律;
    (c) 子环的验证, 例如 $\mathbb{R}[A]$, $\mathbb{Z}[\sqrt{2}]$;
    (d) 环中的左和右零因子和可逆元, 环中所有可逆元组成的乘法群, 剩余环和 $F[A]$ 中的零因子和可逆元的确定;
    (e) 环中的消去律;
    (f) 同态(单同态)与特征的关系;
    (g) 幂零元和幂零矩阵不考.

4. 域

(a) 域、同态、同构、子域, 域的特征,

(b) 子域的验证(交换子环和非零元可逆),

(c) 整环的分式域(不要求证明),

(d) 域的嵌入,

(e) 域上的线性代数.

一元多项式

1. 未定元的引入不考.

2. 在 $R[x]$ 中

   (a) 次数、首项系数

   (b) 加法、乘法

   (c) 赋值同态(证明不要求)

3. 在 $F[x]$ 中, F 是域

   (a) $F[x]$ 是整环,

   (b) $F[x]$ 中的除法,

   (c) 设 $f \in F[x]$ 和 $A \in \mathrm{M}_n(F)$. 计算 $f(A)$.

2 多元多项式

把 $R[x]$ 看作系数环, $R[x][y]$ 是 $R[x]$ 上的关于 y 的一元多项式环.

例 2.1 设

$$\begin{aligned} f &= (x^2+1)y^3 - (x+1)y^2 - x^5 + 2x \in \mathbb{Z}[x][y] \\ &= x^2y^3 + y^3 - xy^2 - y^2 - x^5 + 2x \quad \textit{(分配律)} \\ &= -x^5 + y^3x^2 + (2-y^2)x + y^3 - y^2 \in \mathbb{Z}[y][x]. \end{aligned}$$

由此可知, $\mathbb{Z}[x][y] = \mathbb{Z}[y][x] =: \mathbb{Z}[x,y]$ 并称之为 $\mathbb{Z}$ 上的二元多项式环.

2.1 多元多项式环

定义 2.2 设 R 是交换环. 交换环 $R[x_1][x_2]\cdots[x_n]$ 称为 R 上的 n 元多项式环, 记为 $R[x_1,\ldots,x_n]$.

定理 2.3 当 R 是整环时, $R[x_1,\ldots,x_n]$ 是整环.

证明. 设 R 是整环. 当 $n=1$ 时 $R[x_1]$ 是整环(第十六讲定理 1.8). 对 n 归纳可直接得出 $R[x_1,\ldots,x_n]$ 也是整环. □

定义 2.4 设 $R[x_1,\ldots,x_n]$ 是交换环 R 上的多项式环. 令

$$X_n = \left\{ x_1^{d_1}\cdots x_n^{d_n} \mid d_1,\ldots,d_n \in \mathbb{N} \right\},$$

其中元素 $M = x_1^{d_1} \cdots x_n^{d_n}$ 称为 单项式, $d_1 + \cdots + d_n$ 称为 M 的*(总)*次数, 记为 $\deg(M)$. 而 d_i 称为 M 关于 x_i 的次数, 记为 $\deg_{x_i}(M)$, $i = 1, \ldots, n$.

注解 2.5 设 $M, N \in X_n$, 则$MN \in X_n$ 且

$$\deg(MN) = \deg(M) + \deg(N).$$

下面我们研究如何用单项式表示多项式. 由例 2.1 可知, 通过 $R[x_1, \ldots, x_n]$ 中的运算, $R[x_1, \ldots, x_n]$ 中的任何元素 f 可以写成

$$f = \alpha_1 M_1 + \cdots + \alpha_k M_k, \tag{1}$$

其中 $k \in \mathbb{Z}^+$, $\alpha_1, \ldots, \alpha_k \in R$, $M_1, \ldots, M_k \in X_n$. 通过合并同类项, 我们可进一步假设上式中 $M_1, \ldots, M_k$ 两两不同.

引理 2.6 设 (1) 中 $M_1, \ldots, M_k$ 两两不同且 $f = 0$. 则 $\alpha_1 = \cdots = \alpha_k = 0$.

证明. 对 n 归纳. 当 $n = 1$ 时, 结论成立(见定理 2.1 (i)). 设 $n > 1$ 且结论在 $n - 1$ 时成立. 设

$$d = \max(\deg_{x_n}(M_1), \ldots, \deg_{x_n}(M_k)).$$

如果 $d = 0$, 则 x_n 在 $M_1, \ldots, M_k$ 中都不出现. 由归纳假设 $\alpha_1 = \cdots = \alpha_k = 0$.

现在考虑 $d>0$ 的情形. 假设 $\alpha_1,\dots,\alpha_k$ 都不等于零. 再设 $i\in\{1,\dots,n\}$ 使得 $M_1,\dots,M_{i-1}$ 关于 x_n 的次数都小于 d, 而 $\deg_{x_n}(M_i)=\deg_{x_n}(M_{i+1})=\cdots=\deg_{x_n}(M_k)=d$. 则 $M_i=N_ix_n^d,\dots,M_k=N_kx_n^d$, 其中 $N_i,\dots,N_k\in X_{n-1}$. 于是

$$0=\underbrace{\alpha_1M_1+\cdots+\alpha_{i-1}M_{i-1}}_{P}+\underbrace{(\alpha_iN_i+\cdots+\alpha_kN_k)}_{Q}x_n^d.$$

注意到 P 作为关于 x_n 的多项式有 $\deg_{x_n}(P)<d$. 根据定理 2.1, $Q=0$. 再由归纳假设可知, $\alpha_i=\cdots=\alpha_k=0$, 矛盾. □

定理 2.7 设 $p\in R[x_1,\dots,x_n]$ 且 $p\neq 0$. 则存在唯一的 $k\in\mathbb{Z}^+$, $\alpha_1,\dots,\alpha_k\in R\setminus\{0\}$ 和两两不同的单项式 $M_1,\dots,M_k\in X_n$ 使得

$$p=\alpha_1M_1+\cdots+\alpha_kM_k. \tag{2}$$

(有时称上述表达式为 p 的“分布式”.)

证明. 存在性由交换环的运算规律直接可得.

下面证明唯一性. 设

$$p=\beta_1N_1+\cdots+\beta_\ell N_\ell,$$

其中 $\beta_1,\dots,\beta_\ell\in R\setminus\{0\}$ and $N_1,\dots,N_\ell\in X_n$ 两两不同. 再设 $i\in\{1,2,\dots,\min(k,\ell)\}$ 使得 $M_1=N_1,\dots,M_i=N_i$,

且对任意的 $s,t\in\{i+1,\ldots,\max(s,t)\}$, $M_s\neq N_t$. 则:

$$
\begin{aligned}
p-p=&(\alpha_1-\beta_1)M_1+\cdots+(\alpha_i-\beta_i)M_i\\
&+\alpha_{i+1}M_{i+1}+\cdots+\alpha_kM_k+(-\beta_{i+1})N_{i+1}+\cdots+(-\beta_\ell)N_\ell=0.
\end{aligned}
$$

根据引理 2.6, $i=k=\ell$ 且 $\alpha_1=\beta_1$, $\ldots$, $\alpha_k=\beta_k$. □

定义 2.8 设 $p\in R[x_1,\ldots,x_n]\setminus\{0\}$ 的分布式表示为 (2). 多项式 p 的*(总)*次数定义为

$$
\max(\deg(M_1),\ldots,\deg(M_k)),
$$

记为 $\deg(p)$. 此外, 0 的次数定义为 $-\infty$.

注解 2.9 设 $p\in R[x_1,\ldots,x_n]$ 和 $i\in\{1,\ldots,n\}$. 我们把看成 p 在系数环 $R[x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n]$ 上关于 x_i 的元多项式. 多项式 p 关于 x_i 的次数记为 $\deg_{x_i}(p)$.

例 2.10 设: $f=2(x-y)(x+y)+3y^2-5xyz-(y+z)^2-2y^3\in\mathbb{Z}[x,y,z]$. 求 $\deg_x(f)$, $\deg_y(f)$, $\deg_z(f)$ 和 $\deg(f)$.

解. 利用交换环中的计算规则可知

$$
\begin{aligned}
f&=2x^2-(5yz)x-2yz-z^2-2y^3 &&\text{(看成关于 x 的元多项式)}\\
&=-2y^3-(2xz+2z)y+2x^2-z^2 &&\text{(看成关于 y 的元多项式)}\\
&=-z^2-(5xy+2y)z+2x^2-2y^3 &&\text{(看成关于 z 的元多项式)}\\
&=-(2y^3+5xyz)+(2x^2-2yz-z^2) &&\text{(分布表示)}.
\end{aligned}
$$

于是$\deg_x(p)=2$, $\deg_y(p)=3$, $\deg_z(p)=2$ 和 $\deg(p)=3$.

2.2 齐次(homogeneous)多项式

为了研究多元多项式的加法和乘法, 我们引入齐次多项式的概念.

定义 2.11 设 $h \in R[x_1, \ldots, x_n]$. 如果存在 $\beta_1, \ldots, \beta_\ell \in R$ 和 d 次的单项式 $N_1, \ldots, N_\ell \in X_n$ 使得

$$h = \beta_1 N_1 + \cdots + \beta_\ell N_\ell,$$

则称 h 是齐 d 次的. 特别地, 0 认为是齐任意次的多项式.

如果多项式 h 非零, 则它是齐 d 次的当且仅当在它的分布表达式中出现的单项式都是 d 次的. 任何一个非零的 d 次多项式 p 都可以唯一地写成

$$p = h_d + h_{d-1} + \cdots + h_0,$$

其中 h_i 是齐 i 次的多项式且 $h_d \neq 0$. 我们称上式为 p 的齐次（加法）分解.

例 2.12 例 *2.10* 中的多项式 $f = h_3 + h_2 + h_1 + h_0$, 其中

$$h_3 = -(3y^3 + 5xyz),\ h_2 = 2x^2 - 2yz - z^2,\ h_1 = h_0 = 0.$$

引理 2.13 设 h_d 和 h_e 分别是 $R[x_1, \ldots, x_n]$ 中齐 d 次和齐 e 次多项式. 则

(i) $\deg(h_d + h_e) \leq \max(d, e)$, 且当 $d \neq e$ 时等式成立.

(ii) $\deg(h_d h_e) \le d+e$, 且当 R 是整环时等式成立.

证明. (i) 当 $d > e$ 时, h_d 中出现的单项式不可能与 h_e 中的单项式相等. 由引理 2.6, $\deg(h_d + h_e) = d$. 当 $d = e$ 时, $\deg(h_d + h_e) = d$ 或 0. 结论成立.

(ii) 由注释 2.9 可知, $h_d h_e$ 或者等于零或者是齐 $d+e$ 次多项式. 当 R 整环时, $R[x_1, \ldots, x_n]$ 也是整环. 于是当 h_d 和 h_e 都非零时, $h_d h_e$ 也不等于零. 故 $\deg(h_d h_e) = d+e$. □

定理 2.14 设 p 和 q 分别是 $R[x_1, \ldots, x_n]$ 中 d 次和 e 次多项式. 则

(i) $\deg(p+q) \le \max(d,e)$, 且当 $d \ne e$ 时整等式成立.

(ii) $\deg(pq) \le d+e$, 且当 R 是整环时等式成立.

证明. 当 p 或 q 等于零时, 结论显然成立. 设 p 和 q 都不等于零. 令

$$p = g_d + \cdots + g_1 + g_0 \quad \text{和} \quad q = h_e + \cdots + h_1 + h_0,$$

其中 g_i 是齐 i 次的, h_j 是齐 j 次的, 且 h_d 和 g_e 都非零.

(i) 当 $d > e$ 时, g_d 是出现在 $p+q$ 的齐次加法分解中次数最高的齐次多项式, 于是 $\deg(p+q) = d$. 当 $d = e$ 时, 由引理 2.13 (i) 可知, $\deg(p+q) \le d$.

(ii) 由引理 2.13 (ii) 可知,

$$pq = g_d h_e + r,$$

其中 r 的齐次分解中出现的齐次多项式的次数小于 $d+e$. 于是, $\deg(pq) \leq d+e$. 当 R 是整环时. $\deg(g_d h_e) = d+e$. 这也是 pq 的次数. □

2.3 赋值同态

我们把关于一元多项式环的赋值同态定理推广到多元情形.

定理 2.15 设 R 和 S 是两个交换环, $\phi : R \longrightarrow S$ 是环同态. 对任意的 $s_1, \ldots, s_n \in S$, 存在唯一的环同态 $\phi_{s_1,\ldots,s_n} : R[x_1, \ldots, x_n] \longrightarrow S$ 使得

$$\phi_{s_1,\ldots,s_n}(x_i) = s_i,\ i = 1, \ldots, n \quad \text{且} \quad \phi_{s_1,\ldots,s_n}|_R = \phi.$$

证明. 对 n 归纳. 当 $n=1$ 时, 定理即为一元多项式的赋值同态定理(见定理 2.3). 设 $n-1$ 时定理成立. 即存在唯一的环同态 $\phi_{s_1,\ldots,s_{n-1}} : R[x_1, \ldots, x_{n-1}] \longrightarrow S$ 满足

$$\phi_{s_1,\ldots,s_{n-1}}(x_i) = x_i,\ i = 1, \ldots, n-1 \quad \text{且} \quad \phi_{s_1,\ldots,s_{n-1}}|_R = \phi.$$

令 $\psi = \phi_{s_1,\ldots,s_{n-1}}$. 对 ψ, $R[x_1, \ldots, x_{n-1}][x_n]$ 和 s_n 再次用定理 2.3 得到唯一的环同态: $\psi_{s_n} : R[x_1, \ldots, x_{n-1}][x_n] \longrightarrow S$ 满足 $\psi_{s_n}(x_n) = s_n$ 且 $\psi_{s_n}|_{R[x_1,\ldots,x_{n-1}]} = \psi$. 可直接看出 ψ_{s_n} 就是所要求的同态 $\phi_{s_1,\ldots,s_n}$. □

例 2.16 设 F 是域. $\phi: F\longrightarrow F$ 是恒同映射, $\alpha_1,\ldots,\alpha_n\in F$. 则存在唯一的赋值同态

$$\begin{array}{rccc}\phi_{\alpha_1,\ldots,\alpha_n}: & F[x_1,\ldots,x_n] & \longrightarrow & F \\ & p(x_1,\ldots,x_n) & \mapsto & p(\alpha_1,\ldots,\alpha_n).\end{array}$$

如果 $p(\alpha_1,\ldots,\alpha_n)=0$, 则称 $(\alpha_1,\ldots,\alpha_n)$ 是多项式 p 在 F 上的一个零点.

多项式 $x_1^2+x_2^2-1$ 在 $\mathbb{R}$ 上所有零点的集合是单位圆.

3 复数

3.1 复数域

设

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

设 $z=x+y\sqrt{-1}$, 其中 $x,y\in\mathbb{R}$. 则 x 称为 z 的实部, 记为 $\mathrm{Re}(z)$; y 称为 z 的虚部, 记为 $\mathrm{Im}(z)$. 注意到 $\mathbb{R}\subset\mathbb{C}$.

定义

$$\begin{array}{rccc}+: & \mathbb{C}\times\mathbb{C} & \longrightarrow & \mathbb{C} \\ & (x_1+y_1\sqrt{-1},x_2+y_2\sqrt{-1}) & \mapsto & (x_1+x_2)+(y_1+y_2)\sqrt{-1}.\end{array}$$

可直接验证 $(\mathbb{C},+,0)$ 是交换群. 定义

$$\begin{array}{rccc}\cdot: & \mathbb{C}\times\mathbb{C} & \longrightarrow & \mathbb{C} \\ & (x_1+y_1\sqrt{-1},x_2+y_2\sqrt{-1}) & \mapsto & (x_1x_2-y_1y_2)+(x_1y_2+y_1x_2)\sqrt{-1}.\end{array}$$

可直接验证 $(\mathbb{C},\cdot,1)$ 是交换含幺半群.

可直接验证分配律成立. 于是, $(\mathbb{C},+,0,\cdot,1)$ 是交换环.

设 $z=x+y\sqrt{-1}$, 其中 $x,y\in\mathbb{R}$. 则 $\bar{z}=x-y\sqrt{-1}$ 称为 z 的共轭. 注意到

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

当 $z\neq 0$ 时,

$$z\frac{\bar{z}}{x^2+y^2}=1.$$

故 $(\mathbb{C},+,0,\cdot,1)$ 是域, 称之为复数域. 它的元素称为复数.

例 3.1 设

$$F=\left\{\begin{pmatrix} x & y \\ -y & x\end{pmatrix} \;\middle|\; x,y\in\mathbb{R}\right\}.$$

则 F 是 $\mathrm{M}_2(\mathbb{R})$ 的交换子环, $(F,+,O,\cdot,E)$ 是域. 下面我们验证 F 和 $\mathbb{C}$ 是同构的.

定义

$$\begin{array}{rccc}\phi: & F & \longrightarrow & \mathbb{C} \\ & \begin{pmatrix} x & y \\ -y & x\end{pmatrix} & \mapsto & x+y\sqrt{-1}.\end{array}$$

可直接验证对任意 $A,B\in F$, $\phi(A+B)=\phi(A)+\phi(B)$. 设

$$A=\begin{pmatrix} x & y \\ -y & x\end{pmatrix} \quad \text{和} \quad B=\begin{pmatrix} u & v \\ -v & u\end{pmatrix}.$$

则

$$\begin{aligned}\phi(AB) &= \phi(\begin{pmatrix} xu-yv & xv+yu \\ -xv-yu & xu-yv \end{pmatrix}) \\ &= (xu-yv)+(xv+yu)\sqrt{-1} \\ &= (x+y\sqrt{-1})(u+v\sqrt{-1}) \\ &= \phi(A)\phi(B).\end{aligned}$$

进而, $\phi(E)=1$. 故 ϕ 是环同态. 显然 ϕ 是满射. 再根据命题第四章第三讲命题 *4.4*, ϕ 是同构.

注意到

$$\phi(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}) = \sqrt{-1}.$$

因为

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

所以 $\sqrt{-1}^2=-1$ 是合理的.

记 $\sqrt{-1}$ 为 $\mathbf{i}$, 称为虚单位.

命题 3.2 共轭映射 $z\mapsto \bar{z}$ 是从 $\mathbb{C}$ 到 $\mathbb{C}$ 的同构且 $\bar{\ }|_{\mathbb{R}}=\mathrm{id}_{\mathbb{R}}$.

证明. 设 $z=x+y\mathbf{i}$, $x,y\in\mathbb{R}$. 则 $\bar{z}=x-y\mathbf{i}$. 于是, 当 $y=0$ 时, $\bar{z}=z$. 故 $\bar{\ }|_{\mathbb{R}}=\mathrm{id}_{\mathbb{R}}$. 进而,

$$\bar{\bar{z}}=\overline{x-y\mathbf{i}}=x+y\mathbf{i}=z.$$

故共轭映射的逆是它自身, 从而是双射. 下面只需证明共轭映射是同态. 再设 $z' = x' + y'\mathbf{i}$, 其中 $x', y' \in \mathbb{R}$. 则

$$\begin{aligned}\overline{z+z'} &= \overline{(x+x')+(y+y')\mathbf{i}} = (x+x')-(y+y')\mathbf{i}\\ &= (x-y\mathbf{i})+(x'-y'\mathbf{i}) = \bar{z}+\bar{z}'. \quad \square\end{aligned}$$

3.2 复数的极表示

设 $z = x + y\mathbf{i}$, 其中 $x, y \in \mathbb{R}$ 不全为零. 则

$$z = \sqrt{x^2+y^2}\left(\frac{x}{\sqrt{x^2+y^2}} + \frac{y}{\sqrt{x^2+y^2}}\mathbf{i}\right).$$

则存在唯一的 $\theta \in [0, 2\pi)$ 使得,

$$\cos\theta = \frac{x}{\sqrt{x^2+y^2}} \quad \text{和} \quad \sin\theta = \frac{y}{\sqrt{x^2+y^2}}.$$

称 $\sqrt{x^2+y^2}$ 为 z 的模长, 记为 $|z|$. 称 θ 为 z 的幅角, 记为 $\arg z$. 再设 0 的模长为零, 幅角任意. 则对任意 $z \in \mathbb{C}$,

$$z = |z|(\cos(\theta) + \sin(\theta)\mathbf{i}).$$

称之为 z 的极化公式.

引理 3.3 设复数

$$z_1 = |z_1|(\cos(\theta_1) + \sin(\theta_1)\mathbf{i}),\ \ z_2 = |z_2|(\cos(\theta_2) + \sin(\theta_2)\mathbf{i}).$$

则

$$z_1 z_2 = |z_1||z_2|(\cos(\theta_1+\theta_2) + \sin(\theta_1+\theta_2)\mathbf{i}).$$

证明. 直接计算得

$$
\begin{aligned}
z_1z_2 &= |z_1||z_2| \\
&\quad (\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)) + (\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2))\mathbf{i} \\
&= |z_1||z_2|(\cos(\theta_1+\theta_2) + \sin(\theta_1+\theta_2)\mathbf{i}). \quad \square
\end{aligned}
$$

命题 3.4 设 $z = |z|(\cos(\theta) + \sin(\theta)\mathbf{i})$.

(i) 对任意 $n \in \mathbb{N}$, $z^n = |z|^n(\cos(n\theta) + \sin(n\theta)\mathbf{i})$.

(ii) 如果 $z \neq 0$, 则 $z^{-1} = |z|^{-1}(\cos(\theta) - \sin(\theta)\mathbf{i})$.

证明. (i) 对 n 归纳. 当 $n = 0$ 时, 结论显然成立. 设 $n > 0$ 且结论对 $n-1$ 时成立.

$$
\begin{aligned}
z^n &= zz^{n-1} \\
&= |z|(\cos(\theta) + \sin(\theta)\mathbf{i})|z|^{n-1}(\cos((n-1)\theta) + \sin((n-1)\theta)\mathbf{i}) \\
&\quad \text{(归纳假设)} \\
&= |z|^n(\cos(n\theta) + \sin(n\theta)\mathbf{i}) \quad \text{(引理 3.3)}.
\end{aligned}
$$

(ii) 直接计算得

$$
\begin{aligned}
& z|z|^{-1}(\cos(\theta) - \sin(\theta)\mathbf{i}) \\
&= |z|(\cos(\theta) + \sin(\theta)\mathbf{i})|z|^{-1}(\cos(-\theta) + \sin(-\theta)\mathbf{i}) \\
&= 1 \quad \text{(引理 3.3)}. \quad \square
\end{aligned}
$$

令

$$e^{\mathbf{i}\theta} = \cos(\theta) + \sin(\theta)\mathbf{i}.$$

则, $z=|z|(\cos(\theta)+\sin(\theta)\mathbf{i})$ 可简记为 $z=|z|e^{\mathbf{i}\theta}$. 上述引理和命题中的结论可写为

$$z_1=|z_1|e^{\mathbf{i}\theta_1}, z_2=|z_2|e^{\mathbf{i}\theta_2} \Longrightarrow z_1z_2=|z_1||z_2|e^{\mathbf{i}(\theta_1+\theta_2)}.$$

当 $z=|z|e^{\mathbf{i}\theta}\neq 0$ 时, 对任意 $n\in\mathbb{Z}$, $z^n=|z|^n e^{\mathbf{i}n\theta}$, 和 $\bar{z}=|z|e^{-\mathbf{i}\theta}$.

Euler "公式"

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

3.3 单位根

设 $n\in\mathbb{Z}^+$. 方程 $z^n=1$ 在 $\mathbb{C}$ 中的根称为 n 次单位根.

命题 3.5 方程 $z^n=1$ 在 $\mathbb{C}$ 中有 n 个互不相同的根

$$\epsilon_k=e^{\frac{2k\pi\mathbf{i}}{n}},\quad k=0,1,\ldots,n-1.$$

证明. 直接计算得

$$\epsilon_k^n=e^{2k\pi\mathbf{i}}=1.$$

故 $\epsilon_0,\epsilon_1,\ldots,\epsilon_{n-1}$ 都是单位根. 设 $k,m\in\{0,1,\ldots,n-1\}$ 且 $k\leq m$. 如果 $\epsilon_k=\epsilon_m$, 则

$$1=\epsilon_m\epsilon_k^{-1}=e^{\frac{2(m-k)\pi\mathbf{i}}{n}}.$$

因为 $m-k\in\{0,1,\ldots,n-1\}$, 所以 $m=k$. 故 $\epsilon_0,\epsilon_1,\ldots,\epsilon_{n-1}$ 两两不同. □

根据第五章第二讲定理 3.19, 方程 $z^n = 1$ 在 $\mathbb{C}$ 中的至多有 n 个根. 于是, $\mathbb{C}$ 中恰有 n 个互不相同的单位根. 记 U_n 是这些单位根的集合.

命题 3.6 三元组 $(U_n, \cdot, 1)$ 是循环群. $U_n = \langle \epsilon_\ell \rangle$ 当且仅当 $\gcd(\ell, n) = 1$.

证明. 设 $\epsilon_k, \epsilon_m \in U_n$. 则 $(\epsilon_k \epsilon_m^{-1})^n = \epsilon_k^n (\epsilon_m^n)^{-1} = 1$. 故 $\epsilon_k \epsilon_m^{-1} \in U_n$. 故 $(U_n, \cdot, 1)$ 是 $(\mathbb{C}^*, \cdot, 1)$ 的子群(第四章第一讲命题 2.24).

对任意 $k \in \{0, 1, \ldots, n-1\}$, $\epsilon_k = \epsilon_1^k$. 于是, $U_n = \langle \epsilon_1 \rangle$.

设 $\ell \in \{0, 1, \ldots, n\}$ 使得 $\gcd(\ell, n) = 1$. 对任意 $k \in \mathbb{Z}$, 存在 $u, v \in \mathbb{Z}$ 使得 $u\ell + vn = k$. (Bezout 关系的直接推论). 于是,

$$\epsilon_k = \epsilon_1^k = \epsilon_1^{u\ell + vn} = \left(\epsilon_1^\ell\right)^u (\epsilon_1^n)^v = \epsilon_\ell^u.$$

故 $U_n = \langle \epsilon_\ell \rangle$.

设 $U_n = \langle \epsilon_\ell \rangle$. 则存在 $u \in \mathbb{Z}$ 使得 $\epsilon_\ell^u = \epsilon_1$. 故 $\epsilon_1^{\ell u - 1} = 1$. 因为 $\operatorname{ord}(\epsilon_1) = n$, 所以 $n | (\ell u - 1)$. 故存在 $v \in \mathbb{Z}$ 使得 $\ell u - 1 = vn$ (第四章第二讲命题 2.38 (ii)), 即 $\ell u + vn = 1$. 根据第一章第四讲定理 7.8, $\gcd(\ell, n) = 1$. □

当 $U_n = \langle \epsilon_\ell \rangle$ 时, ϵ_ℓ 称为 n 次本原单位根.