Chapter 5

复数域

在中学我们就已经学习过复数了。这一章我们将介绍复数的更多性质。

5.1 复数的定义和运算

我们在数学分析课程中已经学习过实数 $\mathbb{R}$ 的严格定义，并且知道 $\mathbb{R}$ 是一个域。我们自然地可以考虑 $\mathbb{R}$ 的扩域。那么我们应该如何将 $\mathbb{R}$ 嵌入到一个更大的域中呢？一个容易想到的办法是往 $\mathbb{R}$ 里添加一些新元素，然后让新元素与原来的元素进行运算，从而得到一个关于加减乘除封闭的集合，这就是我们所需要的扩域。具体地说，我们有如下定义：

定义 5.1.1 令 $\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$，其中 i 满足 $i^2 = -1$(即 i 是 $x^2 + 1 = 0$ 的一个根)，在 $\mathbb{C}$ 上定义如下的加法和乘法：

$$\begin{aligned} + :& \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} \\ & (a + bi, c + di) \longmapsto (a + c) + (b + d)i \\ \times :& \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} \\ & (a + bi, c + di) \longmapsto (ac - bd) + (ad + bc)i \end{aligned}$$

则容易验证 $(\mathbb{C}, +, 0, \times, 1)$ 是域，并且 $a + bi(\neq 0)$ 的负元是 $-a - bi$，乘法逆元是 $\dfrac{a - bi}{a^2 + b^2}$，并且 $\mathbb{R} \to \mathbb{C}$, $x \mapsto x + 0_{\mathbb{R}} i$ 是域同态。我们称 $\mathbb{C}$ 是复数域，其中的元素称为复数 (complex number)。

我们称 i 为虚数单位；若 $z = x + yi \in \mathbb{C}$，则称 x 为 z 的实部，记作 $x = \Re(z)$；y 为 z 的虚部，记作 $y = \Im(z)$；如果 $\Re(z) = 0$，则称 z 为纯虚数；我们称 $\bar{z} = x - yi$ 是 z 的**共轭复数**。容易验证：$z + \bar{z} \in \mathbb{R}$, $z\bar{z} \in \mathbb{R}$, $\bar{\bar{z}} = z$。于是我们有：

命题 5.1.1 $\varphi : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ 是 $\mathbb{C}$ 的自同构，并且 $\varphi^2 = \mathrm{id}_{\mathbb{C}}$。[1]

由定义即可证明，留作练习。

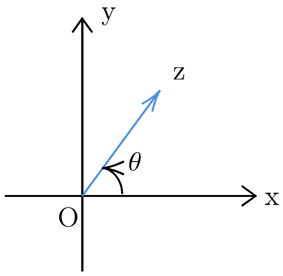
符号 i 的解释

我们知道，i 是实系数方程 $x^2 + 1 = 0$ 的一个根，然而，这样假设似乎并不是很自然，下面我们找到一个“实体”满足这个“方程”。

[1]还可以证明 φ 是 $\mathbb{C}$ 上的连续函数，这是分析学的内容。

注意到实数域 $\mathbb{R}$ 与二阶方阵环的子环 $\{\lambda E_2 \mid \lambda \in \mathbb{R}\}$ 同构，而我们可以找到矩阵 $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$，它满足 $J^2 + E = O$，于是我们可以考虑由 E, J 通过加法、实数乘法和矩阵乘法生成的子矩阵环 (代数)，即 $F = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$，很容易验证 F 是一个域 (练习：找出 F 中非零元的逆矩阵)。我们作映射 $\varphi : \mathbb{C} \to F$, $a + bi \mapsto aE + bJ$，容易验证 φ 是一个域同构。这样我们就给虚数单位 i 找到了一个合适的 "实体"：矩阵方程 $X^2 + E = O$ 的解。我们在下册复化与实化一节中会更深入地学习这一点。

我们也可以将复数 $x + yi$ 视作二维平面上的点 (x, y)，即将 $\mathbb{C}$ 视作向量空间 $\mathbb{R}^2$。于是，设 $z = x + yi$，我们定义 z 的**模长** $\|z\| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$，容易验证 $z \neq 0$ 时 $z^{-1} = \dfrac{\bar{z}}{\|z\|^2}$。我们称射线 Oz 与 x 轴正半轴的夹角 θ 为 z 的**辐角**，记作 $\theta = \arg(z)$，我们通常规定 $0 \leqslant \theta < 2\pi$。于是我们立刻有 $x = \|z\| \cos\theta$, $y = \|z\| \sin\theta$，那么 $z = x + yi = \|z\|(\cos\theta + i \sin\theta)$，我们把或者称为**复数的三角形式或极坐标形式**。



复数的三角形式的一个优点是方便我们做乘法。

命题 5.1.2 设 $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$, $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$，其中 $r_1, r_2 > 0$, $\theta_1, \theta_2 \in \mathbb{R}$。则 $z_1z_2 = r_1r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$。特别地，如果 $z = r(\cos\theta + i\sin\theta)$, $r > 0, \theta \in \mathbb{R}$，则 $z^n = r^n(\cos n\theta + i\sin n\theta)$(称为 De Moivre(棣莫弗) 公式)；如果 $z \neq 0$，则 $z^{-1} = \dfrac{1}{r}(\cos\theta - i\sin\theta)$。

证明是容易的，留作练习。

复数的指数形式

我们定义 $e^{i\theta} = \cos\theta + i\sin\theta$ $(\theta \in \mathbb{R})$，则我们可以将复数的三角形式 $z = r(\cos\theta + i\sin\theta)$ 写成更简单的 $z = re^{i\theta}$，并且将复数的乘法写成更简单的形式 $z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$。这个定义的合理性来自如下的 Taylor 级数形式推导 [1]：

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

于是

$$\begin{aligned} e^{i\theta} &= \sum_{k=0}^{\infty} \frac{(i\theta)^k}{k!} \\ &= \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!} + i \sum_{k=1}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!} \\ &= \cos\theta + i\sin\theta \end{aligned}$$

特别地，取 $\theta = \pi$ 即得到 $e^{i\pi} + 1 = 0$，这就是著名的欧拉公式。

[1] 我们会在复变函数课程中更严谨地定义复数域上的初等函数。

借助棣莫弗公式我们可以方便地对复数进行开方运算：设 $z == r(\cos\theta + i\sin\theta)$，如果 ω 满足 $\omega^n = z$，不妨设 $\omega = r_0(\cos\theta_0 + i\sin\theta_0)$，则 $\omega^n = r_0^n(\cos n\theta_0 + i\sin n\theta_0)$，对比 z 的形式可得 $r_0^n = r$，$n\theta_0 = \theta + 2k\pi, k \in \mathbb{Z}$，即 $r_0 = \sqrt[n]{r}$，$\theta_0 = \dfrac{\theta + 2k\pi}{n}, k \in \mathbb{Z}$。

特别地，我们关注 1 在 $\mathbb{C}$ 中的 n 次方根。

定义 5.1.2 设 $n \in \mathbb{Z}^+$，$\omega \in \mathbb{C}$，如果 $\omega^n = 1$，则称 ω 是一个 n 次单位根。

定理 5.1.1 设 $n \in \mathbb{Z}^+$，则 $\mathbb{C}$ 中有且仅有 n 个互不相同的 n 次单位根，并且它们在复数的乘法下构成 n 阶循环群。

证明: 由上面的复数开方法可知全部的 n 次单位根为 $e^{\frac{2k\pi i}{n}}, \forall k \in \mathbb{Z}$。实际上这些数有且只有 n 个，这是因为如果 $i \equiv j \mod n$，即 $i - j = mn, m \in \mathbb{Z}$，则

$$e^{\frac{2k\pi i}{n}} - e^{\frac{2k\pi j}{n}} = e^{\frac{2k\pi j}{n}}(e^{\frac{2k\pi(i-j)}{n}} - 1) = e^{\frac{2k\pi i}{n}}(e^{2km\pi} - 1) = 0$$

同样的方法可以证明如果 $i \not\equiv j \mod n$，则 $e^{\frac{2k\pi i}{n}} \neq e^{\frac{2k\pi j}{n}}$。于是 $U_n = \{e^{\frac{2k\pi i}{n}} \mid k = 0, 1, \ldots, n-1\}$ 是全部的 n 次单位根。下面说明 U_n 在复数乘法下成群。设 $a, b \in U_n$，则 $(ab^{-1})^n = \dfrac{a^n}{b^n} = 1$，所以 $ab^{-1} \in U_n$，即 U_n 是群。

最后我们说明 U_n 是循环群，这只需要在 U_n 中找到一个 n 阶元素即可。注意到 $(e^{\frac{2\pi i}{n}})^n = 1$，而对任意的 $l \in \{1, \ldots, n-1\}$，有 $(e^{\frac{2\pi i}{n}})^l = e^{\frac{2l\pi i}{n}} \neq 1$，即 $e^{\frac{2\pi i}{n}}$ 是 n 阶元，所以 $U_n =< e^{\frac{2\pi i}{n}} >$ 是循环群。 □

实际上，我们可以证明，任何域的有限阶乘法子群都是循环群。证明需要用到 Sylow 定理，我们会在抽象代数课程中学习。

我们把 n 次单位根群记作 U_n。U_n 的生成元称为 n 次本原单位根。下面我们考虑 n 次本原单位根的性质。

命题 5.1.3 $e^{\frac{2k\pi i}{n}}$ 是 n 次本原单位根 $\iff \gcd(k, n) = 1$。

证明: $(\Longrightarrow)$ 用反证法，如果 $\gcd(k, n) = r > 1$，那么令 $m = \dfrac{n}{r} < n$，有 $(e^{\frac{2k\pi i}{n}})^m = e^{2\frac{k}{r}\pi i}$，而 $\dfrac{k}{r}$ 是整数，故 $(e^{\frac{2k\pi i}{n}})^m = 1$，即 $e^{\frac{2k\pi i}{n}}$ 的阶小于 n，从而与 $e^{\frac{2k\pi i}{n}}$ 是 n 次本原单位根矛盾！
$(\Longleftarrow)\gcd(k, n) = 1 \Longrightarrow \exists a, b \in \mathbb{Z}$ 使得 $an + bk = 1$，于是

$$e^{\frac{2\pi i}{n}} = e^{\frac{2(an+bk)\pi i}{n}} = (e^{\frac{2k\pi i}{n}})^b$$

所以 $\forall l \in \{1, \ldots, n-1\}$，有

$$e^{\frac{2l\pi i}{n}} = (e^{\frac{2k\pi i}{n}})^{bl}$$

即 $e^{\frac{2k\pi i}{n}}$ 是生成元。

于是我们立刻有：

推论 5.1.1 $\mathbb{C}$ 中 n 次本原单位根有且只有 $\varphi(n)$ 个，其中 φ 是欧拉函数。

实际上，命题 5.1.3的结论可以推广到一般的循环群，证明方法类似，留作思考。

例 5.1.1 $\mathbb{C}$ 中 4 次单位根为 $\pm 1, \pm i$，其中本原单位根为 $\pm i$。

5.2 实数域的二次扩张

本节的主要结论是：复数域在同构意义下是唯一的，即下面的定理。

定理 5.2.1 设 F 是 $\mathbb{R}$ 上的 2 维向量空间，在 F 上有一个乘法使得 F 在自然的加法和该乘法下是整环，则 F 是域并且与 $\mathbb{C}$ 同构。

证明: 设 $\mathbf{1}$ 是 F 的乘法幺元，则 $\mathbb{R} \to \mathbb{R}\cdot\mathbf{1}$ 是环同构，即我们可以将 $\mathbb{R}$ 嵌入 F 中。由于 F 是 $\mathbb{R}$ 上的 2 维向量空间，故由基扩充定理可以找到 $\mathbf{e} \in F \setminus \mathbb{R}\cdot\mathbf{1}$ 使得 $\mathbf{1}, \mathbf{e}$ 是 F 的一组基。于是 $\forall a \in F,\ \exists \alpha, \beta \in \mathbb{R}$ 使得 $a = \alpha\mathbf{1} + 2\beta\mathbf{e}$，特别地，$\mathbf{e}^2 = \alpha\mathbf{1} + 2\beta\mathbf{e}$。[1] 于是可令 $\mathbf{f} = -\beta\mathbf{1} + \mathbf{e} \notin \mathbb{R}\cdot\mathbf{1}$，则

$$\mathbf{f}^2 = (-\beta\mathbf{1} + \mathbf{e})^2 = \mathbf{e}^2 - 2\beta\mathbf{e} + \beta^2\mathbf{1} = (\alpha + \beta^2)\mathbf{1}$$

注意到 $\mathbf{f} \notin \mathbb{R}\cdot\mathbf{1}$, 则 $\alpha+\beta^2 < 0$, 于是可以令 $\alpha+\beta^2 = -\delta,\ \delta > 0$, 则 $(\frac{1}{\sqrt{\delta}}\mathbf{f})^2 = -\mathbf{1}$, 取 $\mathbf{j} = \frac{1}{\sqrt{\delta}}\mathbf{f},\ \mathbf{j}^2 = -\mathbf{1}$, 容易验证 $\varphi : \mathbb{C} \to F,\ a + bi \mapsto a\mathbf{1} + b\mathbf{j}$ 是环同构，从而 F 是域并且同构于复数域。这样我们就完成了证明。 □

上面的定理告诉我们: $\mathbb{R}$ 的二次扩张在同构意义下是唯一的。那么, 有理数域的二次扩张是什么情况呢? 设 d 是一个整数 (可以是负数), 如果 $\sqrt{d}$ 不是有理数, 则 $\mathbb{Q}(\sqrt{d}) = \{\alpha + \beta\sqrt{d} \mid \alpha, \beta \in \mathbb{Q}\}$ 是有理数域上的二维向量空间, 并且是有理数域的一个扩域, 称为 $\mathbb{Q}$ 的二次扩域 (验证之), $d > 0$ 时 $\mathbb{Q}(\sqrt{d})$ 称为实二次扩域，$d < 0$ 时 $\mathbb{Q}(\sqrt{d})$ 称为虚二次扩域。显然 $\mathbb{Q}$ 的二次扩域不是唯一的 (思考：证明 $\mathbb{Q}(\sqrt{2})$ 与 $\mathbb{Q}(\sqrt{3})$ 之间不是域同构)。我们可以类似地定义 $\mathbb{Q}(\sqrt{d})$ 中元素的共轭和范数，感兴趣的读者可以自行推导它们的性质。二次扩域是数论的研究对象，有些问题至今尚未解决。

---

[1] 这样构造的原因是, 我们希望找到满足 $\mathbf{j}^2 = -\mathbf{1}$ 的元素, 如果这样的元素存在, 则可设 $\mathbf{e} = a\mathbf{1} + b\mathbf{j},\ b \neq 0$, 于是 $\mathbf{e}^2 = (a^2 - b^2)\mathbf{1} + 2ab\mathbf{j} = (-a^2 - b^2)\mathbf{1} + 2a(a\mathbf{1} + b\mathbf{j}) = (-a^2 - b^2)\mathbf{1} + 2a\mathbf{e}$，这启示了 $\mathbf{j}$ 的构造。

5.3 * 复数的初等几何

我们已经知道，复数可以视作 $\mathbb{R}$ 上的二维向量空间 (即复平面)，于是许多平面几何的问题可以化成复数运算的问题来解决。下面我们简单提供一些用复数来解决平面几何问题的例子。

设 $z_1 = x_1 + y_1 i$，$z_2 = x_2 + y_2 i$，我们定义内积 $< z_1, z_2 >= x_1x_2 + y_1y_2 = \Re(z_1\overline{z_2})$，则内积满足：
(1) 双线性性：$\forall \lambda_1, \lambda_2 \in \mathbb{C}$，$< \lambda_1 z_1 + \lambda_2 z_2, z_3 >= \lambda_1 < z_1, z_3 > + \lambda_2 < z_2, z_3 >$，$< z_3, \lambda_1 z_1 + \lambda_2 z_2 >= \lambda_1 < z_3, z_1 > + \lambda_2 < z_3, z_2 >$。
(2) 对称性：$< z_1, z_2 >=< z_2, z_1 >$。
(3) 正定性：对任意 $z \in \mathbb{C}$，$< z, z > \geqslant 0$，并且等号当且仅当 $z = 0$ 时成立。

于是显然有 $\|z\| = \sqrt{< z, z >}$，并且我们可以定义两个非零复数的夹角 θ：

$$\cos\theta = \frac{< z_1, z_2 >}{\|z_1\|\|z_2\|}$$

(一般规定 $0 \leqslant \theta < \pi$)。特别地，如果 $< z_1, z_2 >= 0$，则称 z_1, z_2 正交 (规定 0 与任意复数正交)。

于是，复平面上过两个点 $u, v \in \mathbb{C}$ 的直线可以用参数方程 $\overline{uv} : w = u + (v - u)t$，$t \in \mathbb{R}$ 表示 (w 是直线上任意一点对应的复数，t 为参数)。于是我们立刻有：
(1) 三个不同的点共线 $\Longleftrightarrow$ 它们对应的复数 z_1, z_2, z_3 满足 $z_3 = z_1 + (z_1 - z_2)t$，$t \in \mathbb{R}$，即 $\dfrac{z_3 - z_2}{z_1 - z_2} \in \mathbb{R}$。
(2) 两条直线 $\overline{z_1z_2}$，$\overline{z_3z_4}$ 垂直 $\Longleftrightarrow < z_2 - z_1, z_4 - z_3 >= 0$。

定理 5.3.1 *不共线的四点 z_1, z_2, z_3, z_4 共圆 $\Longleftrightarrow$ 其交比 $[z_1, z_2, z_3, z_4] = \dfrac{(z_1 - z_2)(z_3 - z_4)}{(z_1 - z_4)(z_3 - z_2)} \in \mathbb{R}$。*

证明: 注意到交比在任意一个平移 $z \mapsto z + a$，$\forall a \in \mathbb{C}$ 下保持不变 (验证留作练习)，则可以将坐标原点平移到 z_1, z_2, z_3 这个三角形的外心处，此时四点共圆 $\Longleftrightarrow \|z_1\| = \|z_2\| = \|z_3\| = \|z_4\|$，而后者等价于交比是实数 (验证留作练习)。 □

最后我们关注一下三大古典作图难题：三等分角、倍立方体、化圆为方。它们的结论都是不能用尺规作图的方法做出。为了证明这一点，我们需要讨论尺规作图可以作出哪些对象。

平面上的点与复数一一对应，给定单位长度 1，则我们可以用无刻度的直尺和圆规完成加、减、乘、取倒数、开平方的操作，于是我们通过尺规作图可以得到的数构成一个域 CS，称为**可构造数域**。显然 $\mathbb{Q} \subset CS \subset \mathbb{C}$。并且可以证明如下的结论：

定理 5.3.2 *$\alpha \in CS \Longleftrightarrow$ 存在二次扩张序列 $\mathbb{Q} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_n$ 使得 $\alpha \in \mathbb{K}_n$，其中每个 $\mathbb{K}_i/\mathbb{K}_{i-1}$ 都是二次扩张[1]。*

证明细节可以参考 Algebra, Thomas.W.Hungerford,GTM73 的 *ChapterV,Appendix*。我们可以证明，三等分任意角和倍立方体都需要构造 $\mathbb{Q}$ 的三次扩张，化圆为方需要 $\mathbb{Q}$ 的超越扩张，于是它们都不能由尺规作图得到。

[1]即 $\mathbb{K}_i$ 是 $\mathbb{K}_{i-1}$ 的 2 维向量空间。