可視化高斯整數

Timo Chang
timo65537@protonmail.com
譯者: 仙女仙女

最後編輯: 2025 年 12 月 26 日

二次體 (二次域) $\mathbb{Q}(i)$ 具有多種優美的結構, 比如說它是一個範數-歐幾里德體, 亦即, $\mathbb{Q}(i)$ 在 $\mathbb{Q}$ 上的體範數在其整數環 $\mathbb{Z}[i]$——高斯整數環 $\mathbb{Z}[i]$ 上誘導出一個歐幾里德函數. 特別地, 這個歐幾里德函數恰與複數的模一致, 因而使我們得以在複平面上直觀地呈現 $\mathbb{Z}[i]$ 的若干性質. 本文將藉由這一幾何圖像, 探討其中的幾項性質.

1 歐幾里德整環 $\Longrightarrow$ 主理想整環

定義 1.1 所謂整環 D 上的**歐幾里德函數** (**範數**) 是滿足下列兩條件的函數 $\nu : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$:

- 對任何 $a, b \in D$, $b \neq 0$, 存在 $q, r \in D$ 使得 $a = bq + r$, 其中或者 $r = 0$, 或者 $\nu(r) < \nu(b)$;
- 對任何非零元 $a, b \in D$, 均有 $\nu(a) \leq \nu(ab)$.

稱有歐幾里德函數的整環爲**歐幾里德整環**.

定義 1.2 若整環 D 的每個理想 I 均爲主理想, 即存在 $\alpha \in I$ 使得 $I = (\alpha) = \alpha \cdot D$, 則稱 D 爲**主理想整環**.

我們有以下基本事實.

定理 1.3 所有歐幾里德整環均爲主理想整環.

證明 設 D 爲具有歐幾里德函數 ν 的歐幾里德整環, I 爲 D 的非零理想. 在 I 的所有非零元之中選取歐幾里德範數最小的 $b \in I$, 並斷言 b 生成理想 I. 假設存在 $a \in I \setminus (b)$. 令 $q, r \in D$ 滿足 $a = bq + r$, 其中或者 $r = 0$, 或者 $\nu(r) < \nu(b)$. 不難看出 $r \neq 0$, 否則 $a = bq \in (b)$, 但要是 $\nu(r) < \nu(b)$, 便有 $r = a - bq \in I$, 與 b 的選取矛盾. 因此, $I = (b)$. □

此論證脈絡分明, 理解起來並不困難, 現在我們將以高斯整數 $\mathbb{Z}[i]$ 爲例, 嘗試對其加以視覺化的理解.

例 1.4 首先, 注意到 $\mathbb{Z}[i]$ 上一個自然的歐幾里德函數由 $\mathbb{Q}(i)$ 在 $\mathbb{Q}$ 上的體範數 (見 [Fra03, Theorem 47.4]), 即 $N(u+vi) := u^2+v^2$, 其中 $u, v \in \mathbb{Z}$. 不難看出, 對任意 $z \in \mathbb{Z}[i]$, 有 $N(z) = z \cdot \bar{z} = |z|^2$, 其中 $\bar{\cdot}$ 表示複共軛, $|\cdot|$ 表示 $\mathbb{C}$ 上的絕對值. 所以, $N(z)$ 測量複平面上從 z 至 0 的距離. 範數 $N(z)$ 越小, z 離原點就越近.

根據定理 1.3 的證明, $\mathbb{Z}[i]$ 的各非零理想由某個 $b \in I$ 生成, 其中在 I 的所有非零元之中, $N(b)$ 是最小的, 亦即 b 在 I 的所有非零元之中距離原點最近. 另一方面, 注意到

$$(b) = \{n \cdot b + m \cdot ib \mid n, m \in \mathbb{Z}\}$$

含一切 b 和 ib 的 $\mathbb{Z}$-線性組合. 運算「$+(n \cdot b)$」(相應地, 「$+(m \cdot ib)$」) 表示將複平面上一點沿方向 $\vec{v}_1$ 方向 (見圖 1) (相應地, $\vec{v}_2$) n 步 (相應地, m 步), 其中各步之長爲 $|b|$. 於是, 任一個線性組合 $n \cdot b + m \cdot ib$ 表示移動 $n \cdot \vec{v}_1 + m \cdot \vec{v}_2$. 因此, 當 n, m 遍及一切整數對時, (b) 的元素在複平面上形成格子點, 如圖 1 所示. 換言之, 理想 $(b) \subseteq I$ 含每個方形的所有頂點 (圖 1 以 $b = 1 - 2i$ 的情形爲例, 其它情形類似).

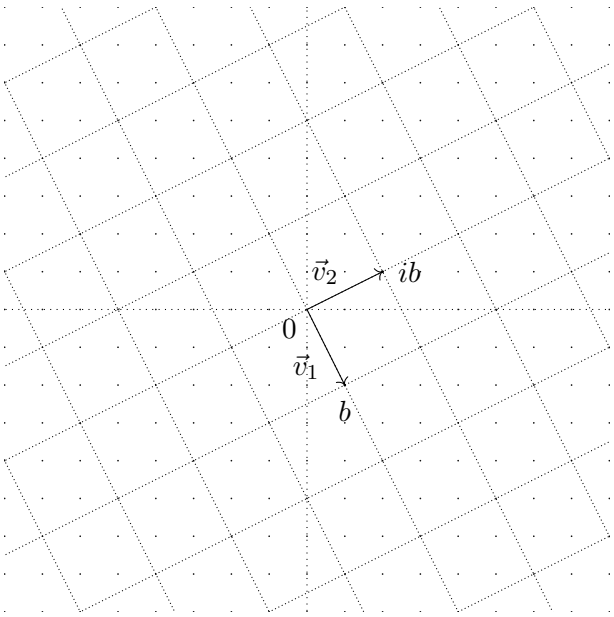

圖 1

現, 若 $(b) \subsetneq I$, 則存在 $a \in I$, $a \notin (b)$, 即 a 不爲任一個頂點 (如圖 2). 因 $\mathbb{Z}[i]$ 是具有歐幾里德函數 N 的歐幾里德整環, 故可取 $q, r \in \mathbb{Z}[i]$ 使得 $a = bq + r$, 其中或者 $r = 0$, 或者 $N(r) < N(b)$.

考慮不等式

$$N(r) = N(a - bq) < N(b),$$

其代數意義爲: 在對數 a 作運算 $-bq$ 後, 其歐幾里德範數 $N(a - bq) = N(r)$ 將變得小於 $N(b)$; 而其幾何意義爲: 在在複平面上沿著網格移動之後, 點 a 將抵達 r 且變得比 b 還更靠近原點, 即終點 r 將位於以原點爲圓心、半徑為 $|b|$ 的圓的內部, 如下圖 2.

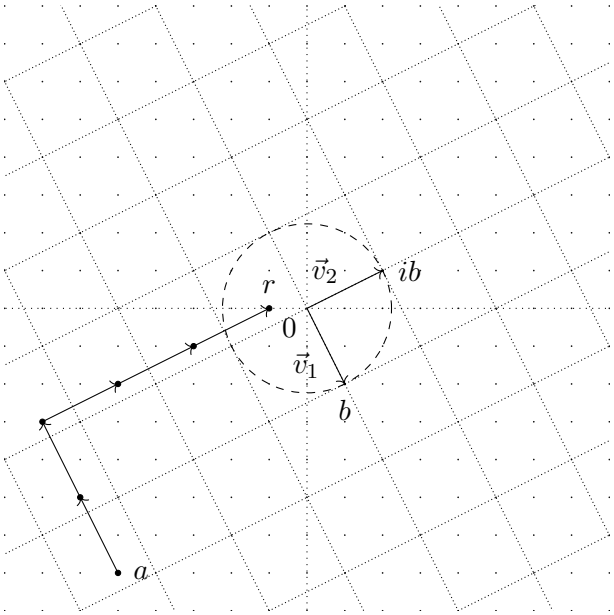

圖 2

注意到, 因 a 不是任何一個頂點, 故最終不會停在原點, 換言之, $r \neq 0$. 而且, 由於 $a \in I$ 沿著方向 $\vec{v}_1$ 和 $\vec{v}_2$ 移動, 故其停靠點 (圖 2 中的黑點) 仍在理想 I 中. 特別地, 我們有 $r \in I$ 且 $N(r) < N(b)$, 但這與 b 的選取矛盾. 因此, $I = (b)$.

註記 1.5 圖 2 中的點 $a, b \in \mathbb{Z}[i]$ 實際上分別是 $a = -5 - 7i$ 及 $b = 1 - 2i$, 故 a 的路徑也暗示了

$$a + (-2b + 3ib) = r = -1 \quad \text{且} \quad N(r) < N(b),$$

等價地, 可寫成

$$a = bq + r, \quad \text{其中} \quad q = 2 - 3i \quad \text{及} \quad r = -1,$$

這正是由歐幾里德函數 N 在 $\mathbb{Z}[i]$ 所誘導出的帶餘除法.

2 $\mathbb{Z}[i]$ 的有限商

根據以上提及的帶餘除法, 不難證明 $\mathbb{Z}[i]$ 對其任何理想的商是有限環 (見 [Fra03, Exercise 47.15]), 接下來我們將此性質呈現在複平面中.

例 2.1 先來考慮如例 1.4 中的理想 $(b) = (1 - 2i)$, 我們想要計算 $\mathbb{Z}[i]/(1 - 2i)$ 的基數. 考察圖 3.

在將商環 $\mathbb{Z}[i]/(1-2i)$ 加以視覺化時, 可把圖 3 中具有相同相對位置的點視爲「同一個點」, 舉例來說, 紅色的點應視爲同一個元素, 橘色以及其他顏色的點亦然. 由此可見, $\#(\mathbb{Z}[i]/(1-2i)) = 5$. (練習: 試透過這些點來看出 $\mathbb{Z}[i]/(1 - 2i)$ 上的加運算及乘運算.)

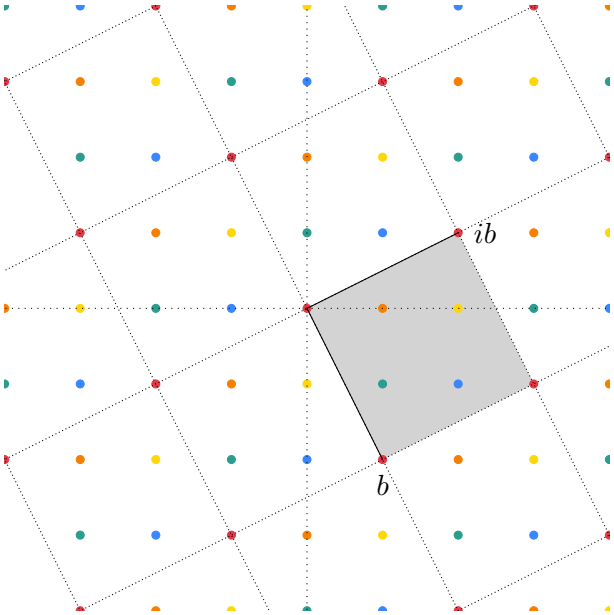

圖 3

例 2.2 更一般地, 斷言: 若 $\gcd(u,v)=1$, 則 $\mathbb{Z}[i]/(u+vi)$ 的基數爲 u^2+v^2. 設 $z:=u+vi\neq 0$, 不妨假設 u 和 v 同不爲 0, 否則 z 爲可逆元, 結論顯然成立. 而且只要選取適當的生成元, 便可假設 $u,v\in\mathbb{N}$, 即 z 在第一象限中 (對例 2.1 來說, 這相當於改以 $ib=2+i$ 作爲生成元, 而非原先的 $b-2i$; 參見 3).

不難檢查, 以 0 和 $z=u+vi$ 爲端點的線段上只有端點是 $\mathbb{Z}[i]$ 中的點. 的確, 若存在 $m+ni\in\mathbb{Z}[i]$, $0<m<u$, 使得 $un=vm$, 則由 $\gcd(u,v)=1$, 可得 u 整除 m, 矛盾. 因 $\mathbb{Z}[i]$ 在乘以 i 的運算 (即, 將點繞原點逆時針旋轉 90 度) 之下封閉, 故上述觀察對於以 0 和 iz 爲端點的線段亦成立.

以上論證了在由 z 與 iz 所張成矩形的邊界上, 恰有 $\mathbb{Z}[i]$ 的四個點, 而在商環 $\mathbb{Z}[i]/(z)$ 中, 這四個點表示同一個元素. 取 $A=u^2+v^2$ 該矩形的面積, $B=4$ 爲邊界點數, I 爲內點數, 則依皮克定理[1], 有

$$A=I+\frac{B}{2}-1,$$

因此

$$\#(\mathbb{Z}[i]/(z))=I+1=A=u^2+v^2.$$

註記 2.3 設 d 爲無平方因子的整數, 其二次體 $\mathbb{Q}(\sqrt{d})$ 爲範數-歐幾里德體 (即 $\mathbb{Q}(\sqrt{d})$ 在 $\mathbb{Q}$ 上

[1]給定以整數座標爲頂點的多邊形, 其面積爲 A, 其整數座標的邊界點數爲 B, 其整數座標的內點數爲 I, 則有

$$A=I+\frac{B}{2}-1.$$

的體範數在其整數環上引出歐幾里德函數) 者已完全確定有[2]

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

因此, 非常歡迎讀者嘗試爲其它環給出類似於例 1.4, 2.1 及 2.2 的幾何詮釋, 例如艾森斯坦整數環 $\mathbb{Z}[\omega]$, 其中 $\omega := (-1 + \sqrt{-3})/2$.

參考資料

[Fra03] John B. Fraleigh. *A First Course in Abstract Algebra*. 7th. Addison-Wesley, 2003.

[2] 整數數列線上百科 (OEIS): 使 $\mathbb{Q}(\sqrt{n})$ 爲範數-歐幾里德體的那些無平方因子的 n