近世代数之七

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

欧式整环

考虑整环R，以及$R^\times = R \setminus \{0_R\}$。

定义

整环R称为**ED**，若存在*size function*

$$\phi\colon R^\times \longrightarrow \{0, 1, 2, \cdots\}$$

使得任给$a, b \in R^\times$，存在$q, r \in R$满足

$$a = qb + r$$

其中$r = 0_R$或$\phi(r) < \phi(b)$。

上表达式不唯一:$33 = 3 \cdot 9 + 6 = 4 \cdot 9 - 3$（第二个更好，因为$\phi(-3) = |-3|$更小）。

ED是PID

定理

ED 是PID。

注：size function给出辗转相除法。

Gauss整数环

回顾$\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} \mid m, n \in \mathbb{Z}\}$。

定理

$\mathbb{Z}[\sqrt{-1}]$是*ED*，从而是*PID*。

证明：The norm map

$$N \colon \mathbb{Q}[\sqrt{-1}]^{\times} \longrightarrow \mathbb{Q}_{+}, \quad z \mapsto z \cdot \bar{z}$$

是乘法映射，限制为size function。需分析余项$a + b\sqrt{-1}$, $|a|, |b| \leq \frac{1}{2}$。

证明：$U(\mathbb{Z}[\sqrt{-1}]) = \{\pm 1, \pm\sqrt{-1}\}$。

练习：记$i = \sqrt{-1}$。计算$\gcd(4 + 7i, 3 + 4i)$。

$\mathbb{Z}[\sqrt{-2}]$

回顾$\mathbb{Z}[\sqrt{-2}] = \{m + n\sqrt{-2} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-2})$。

定理

$\mathbb{Z}[\sqrt{-2}]$是*ED*，从而是*PID*。

证明：The norm map

$$N \colon \mathbb{Q}[\sqrt{-2}]^{\times} \longrightarrow \mathbb{Q}_{+}, \quad z \mapsto z \cdot \bar{z}$$

是乘法映射，限制为size function。

证明：$U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$。

$\mathbb{Z}[\sqrt{-3}]$不是PID

回顾$\mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-3})$。

命题

$\mathbb{Z}[\sqrt{-3}]$不是*PID*。

证明：$2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$，2不可约，但非素元。

Eisenstein整数环

考虑$\omega = e^{\frac{\pi i}{3}} = \frac{1+\sqrt{-3}}{2}$，满足$\omega^2 - \omega + 1 = 0$以及$\omega^6 = 1$。

注意$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega] = \{m + n\omega \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-3})$。

定理

$\mathbb{Z}[\omega]$是*ED*,从而是*PID*。

证明：还是用the norm map $N(z) = z \cdot \bar{z} \in \mathbb{Q}_+$，（根据$a, b$正负性,可能需要调整$a, b$）分析余项

$$a + b\omega = (a + \frac{b}{2}) + \frac{b}{2}\omega$$

(尽可能小)的长度。

证明：$U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$。

思考：为什么$\mathbb{Z}[\sqrt{-3}]$不，但扩大后却可以？？

展望：代数整数环，参考Atiyah-Macdonald

考虑$\mathbb{Z} \subseteq R \subseteq F = \mathrm{Frac}(R)$使得$\mathbb{Q} \subseteq F$是有限维空间。

定义 (E. Kummer 1847)

$\alpha \in F$成为**代数整数**，若α满足首一的整系数方程。记F中代数整数全体为$\mathcal{O}_F$。

重要事实：$\mathcal{O}_F$是子环，且$\mathrm{Frac}(\mathcal{O}_F) = F$。

命题

假设$R \subseteq \mathcal{O}_F$。若$R$是*PID*（或更弱点，为*UFD*）。则$R = \mathcal{O}_F$。

证明：R为UFD蕴含着R整闭。但，根据定义，我们看出$\mathcal{O}_F$为R的整闭包。

注意：$\mathcal{O}_F$总整闭（Dedekind整环），但不是UFD。

$\mathbb{Z}[\sqrt{2}]$是ED

回顾$\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$。

定理

$\mathbb{Z}[\sqrt{2}]$是*ED*，从而是*PID*。

证明：$m + n\sqrt{2} \mapsto |m^2 - 2n^2|$!

练习：$1 + \sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$，从而$U(\mathbb{Z}[\sqrt{2}])$为无限群。

练习：$\mathbb{Z}[\sqrt{3}]$? $\mathbb{Z}[\sqrt{5}]$?

链接：https://oeis.org/A048981