近世代数之八

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. Gauss素数
2. 平方和问题

PID的极大理想

定义

整环R中非零元a, b称为**相伴的**，若存在$u \in U(R)$使得$a = bu$。这等价于$(a) = (b)$。

相伴是等价关系。

命题

设R为PID。则存在双射

$$\{a \in R \mid \text{素元}\}/\text{相伴关系} \longleftrightarrow \mathrm{Max}(R), \quad a \mapsto (a).$$

回顾，此时$\mathrm{Spec}(R) = \{0\} \cup \mathrm{Max}(R)$。

Gauss素数

Gauss整数环$\mathbb{Z}[i]$中的素元称为**Gauss素数**。

回顾：$N(m+ni)=m^2+n^2$, 且$N(m+ni)=1$当且仅当$m+ni\in U(\mathbb{Z}[i])$。

故，$U(\mathbb{Z}[i])=\{\pm 1,\pm i\}$。

于是，$m+ni$相伴于$-m-ni$, $n-mi$,以及$-n+mi$。

例子

$$2=(1+i)(1-i)=(-i)\cdot(1+i)^2$$

故，2不是*Gauss*素*(*相伴于“平方数”*)*。

练习：$1+i$是*Gauss*素数。（考虑*Norm*）

引理

引理

设$z \in \mathbb{Z}[i]$。若$N(z) = p$为素数（这样p只能是2或$4k+1$），则z是Gauss素数。

引理

考虑奇素数p。若$p = 4k+3$。则p是Gauss素数。

证明：p不可约：$p = x \cdot y$，利用norm map。

Fermat 二平方和定理1640

定理

设p为奇素数。则$p = 4k+1$当且仅当$p = a^2 + b^2$。此时，这样的a, b唯一。

证明：“当”很容易。反过来，设$p = 4k+1$。则Euler判别法，$-\bar{1}$是模p二次剩余（或，利于循环群$\mathbb{F}_p^\times$以及$4|(p-1)$）。考虑环同构

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[x]/(x^2 + \bar{1})$$

故，p非素，故，$z|p$。则$N(z) = p$且$p = z \cdot \bar{z}$，z素（a,b的唯一性可由$\mathbb{Z}[i]$唯一分解得出）。

$p = 4k + 1$情况

如上，$p = 4k + 1$。则$p = (a + bi)(a - bi)$，且因子不相伴。

例如：$5 = 1^2 + 2^2$。故，素元$1 + 2i$以及$1 - 2i$!

例如：$13 = 2^2 + 3^2$。故，素元$2 + 3i$以及$2 - 3i$!

练习：研究商域$\mathbb{Z}[i]/(a + bi)$。

Gauss素数分类

定理

在相伴的意义下，*Gauss*素数为以下：

1. $1+i$
2. 素数$p>0$，其中$p=4k+3$
3. $a\pm bi$，其中$p=a^2+b^2$为$4k+1$的素数，$0<a<b$

注：$4k+3$以及$4k+1$的素数均无穷个（直接证，或，Dirichlet定理1837）。

$\mathrm{Spec}(\mathbb{Z}[i])$

回顾：$\mathrm{Spec}(\mathbb{Z}) = \{0\} \cup \{p\mathbb{Z} \mid p = 2, 3, 5, \ldots\}$

任环同态$\theta\colon R \to S$诱导$\mathrm{Spec}(S) \to \mathrm{Spec}(R), \quad \mathfrak{q} \mapsto \theta^{-1}(\mathfrak{q})$

例子

研究$\mathrm{Spec}(\mathbb{Z}[i]) \to \mathrm{Spec}(\mathbb{Z})$的图像。

这是满射，研究其*fibers!*

二平方和定理

定理

设$n \geq 2$。则n可写成二平方和当且仅当有标准分解$n = 2^r p_1^{m_1} \cdots p_t^{m_t}$，其中，若$p_i = 4k+3$，相应的$m_i$为偶数

证明：“当”比较容易（Fermat二平方和定理）。

反过来，$n = N(z)$，对z在Guass整数环中做素因子分解（为什么可以做？用Norm归纳！）。