近世代数之九

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 唯一分解整环UFD
2. Gauss定理

UFD的定义

定义

整环R称为**UFD**，若满足以下两条：

1. 存在不可约分解：$a=c_1c_2\cdots c_r$，c_i不可约
2. 不可约分解唯一：$a=c_1'c_2'\cdots c_s'$，c_j'不可约，则$r=s$且相差置换，c_i与c_i'相伴。

命题

设R为UFD。则以下命题成立。

1. 不可约元=素元。
2. 标准分解$a=up_1^{n_1}\cdots p_r^{n_r}$，$p_i$素元，互补相伴；所有因子！
3. 存在gcd以及lcm
4. 分式域Frac(R)中元素的既约表达（唯一！）

Noether环

设$X \subseteq R$。则包含X的最小理想, 称为X生成的理想:

$$RX = \{\text{有限和} \sum_i a_i \cdot x_i, \text{ 其中} x_i \in X\}$$

若理想I由有限个元素生成，则I称为**有限生成理想**。

定义

环R称为**Noether环**,若任何理想均有限生成。

例如，PID是Noether环。事实上，我们研究的环绝大多数是Noether环。

定理 (Hilbert基定理1890)

设R为Noether环。则$R[x_1, \cdots, x_n]$以及其商环均为为Noether环。

Noether整环有不可约分解

不可约分解普遍存在！

命题

设R为Noether整环。则任何$a \in R$有不可约分解。

素分解总唯一！

命题

设R为整环。若a有素分解。则其不可约分解唯一。

特别地，Noether整环R是UFD当且仅当：不可约元=素元。

例如，PID是UFD。

虚二次域

定理 (Gauss 1801, Heegner 1952/ Baker 1966/ Stark 1967)

设d为*square-free*的正整数。则$\mathbb{Q}(\sqrt{-d})$中的代数整数环$\mathcal{O}$是*UFD*当且仅当是*PID*，当且仅当$d = 1, 2, 3, 7, 11, 19, 43, 67, 163$。

注：$\mathcal{O}$是ED当且仅当$d = 1, 2, 3, 7, 11$。

注：$\mathbb{Q}(\sqrt{d})$的情况更难; norm-ED完全分类[Hardy-Wright 1979]。

猜想(Gauss)：存在无穷个square-free的正整数d 使得$\mathbb{Q}[\sqrt{d}]$的代数整数环是PID。

Gauss定理

定理

设R为UFD。则$R[x]$亦为UFD。

特别地，$\mathbb{Z}[x]$为UFD，不为PID (其素理想(x)，不极大)。

证明：定义容量$c(f)$以及本原多项式。

引理 (Gauss引理)

设$f(x), g(x) \in R[x]$。则$c(f \cdot g) \sim c(f) \cdot c(g)$，其中$\sim$表示相伴。特别地，本原多项式之积仍是本原的。

考虑$R[x] \subseteq K[x]$，其中K为分式域；利用$K[x]$中已有的不可约分解。

得出$R[x]$的两类不可约元：$a \in R$以及本原不可约多项式$f(x) \in R[x]$。

两个有用的结论

相比于$K[x]$中，在$R[x]$判别不可约通常较容易些。

命题

设R为UFD，K为其分式域。设$f(x)\in R[x]$为本原多项式。则$f(x)\in R[x]$不可约元当且仅当$f(x)\in K[x]$为不可约多项式。

命题 (Eisentein判别法)

设R为UFD，$f(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$本原，$p\in R$素元。设$p\nmid a_n$，$p|a_{n-1},\cdots,p|a_1$，$p^2\nmid a_0$。则$f(x)\in K[x]$不可约多项式。

例如，$x^n-2\in\mathbb{Q}[x]$均不可约。