环的算术性质(二)

张起帆

四川大学数学学院

email: qifanzhang@scu.edu.cn

2020 年 3 月 30 日

内容提要

追溯历史—理想的产生

先看一个不定方程的例子. 在整数范围内解方程:

$$y^2 + 5 = x^3.$$

分析 从前的经验告诉我们应该利用环$\mathbb{Z}[\sqrt{-5}]$, 遗憾(或幸运)的是它不再是唯一分解环. 看

$$2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \qquad (1).$$

但Kummer(在研究Fermat大定理时)认为上式不应推翻唯一分解性, 就像

$$(2 \times 3) \times (5 \times 7) = (2 \times 7) \times (3 \times 5)$$

并未推翻$\mathbb{Z}$的唯一分解性一样.

追溯历史—理想的产生

为此需将**(1)**的两端继续分解为**4**个量

$$(2, 1+\sqrt{-5}), (2, 1-\sqrt{-5}), (3, 1+\sqrt{-5}), (3, 1-\sqrt{-5})$$

相乘. 上述**4**个元被**(Kummer)**称为“理想数”，环上的元素被视为“正宗”数. 当然, 他引进了形如

$$(a_1, ..., a_n)$$

的理想数**(**强行当作最大公约数**)**以及它们之间的乘法规则从而恢复了唯一分解性. 其实, 那就是今天说的理想, 只要把理想作为子集合而不作为数就不难理解了.

追溯历史—理想的产生

为能解这个方程，我们列出关于这个环的两个基本事实(它蕴含在未来的定理中).

- **事实1** 环$\mathbb{Z}[\sqrt{-5}]$的任意非零理想可唯一分解为素理想之积.
- **事实2** 对环$\mathbb{Z}[\sqrt{-5}]$的理想I，若I^3为主理想，则I为主理想.

追溯历史—理想的产生

下面我们解上述方程．首先通过简单分析知x为奇，y为偶，将原方程变为一个关于理想的等式

$$(y+\sqrt{-5})(y-\sqrt{-5})=(x)^3.$$

易知理想$(y+\sqrt{-5})$与$(y-\sqrt{-5})$无公因子(作为练习)，即理想$(y+\sqrt{-5}, y-\sqrt{-5})$为单位理想，故由事实**1**知存在理想$I$使

$$(y+\sqrt{-5})=I^3.$$

追溯历史—理想的产生

再由事实2知I亦为主理想，可设$I=(a+b\sqrt{-5})$,代入前面的理想方程得

$$(y+\sqrt{-5})=(a+b\sqrt{-5})^3.$$

从而有

$$y+\sqrt{-5}=u(a+b\sqrt{-5})^3.$$

这里u为环$\mathbb{Z}[\sqrt{-5}]$的单位，必然$u=\pm 1$.可设

$$y+\sqrt{-5}=(a+b\sqrt{-5})^3,$$

简单比较虚部知上式不可能成立，从而，原方程无解.

理想的运算

对交换环R的理想I, J，可定义以下运算：

1. $I + J := \{x + y | x \in I, y \in J\}$
2. $I \cap J$
3. $IJ :=$ 由集合$\{xy | x \in I, y \in J\}$生成的理想.

对主理想整环(比如$\mathbb{Z}$)，有

- $(a) + (b) = (\gcd(a, b))$.
- $(a) \cap (b) = (\mathrm{lcm}(a, b))$.
- $(a)(b) = (ab)$.

理想的运算

对交换环R的理想I, J，可定义以下运算：

1. $I + J := \{x + y | x \in I, y \in J\}$
2. $I \cap J$
3. $IJ :=$ 由集合$\{xy | x \in I, y \in J\}$生成的理想.

对主理想整环(比如$\mathbb{Z}$)，有

- $(a) + (b) = (\gcd(a, b))$.
- $(a) \cap (b) = (\operatorname{lcm}(a, b))$.
- $(a)(b) = (ab)$.

理想的运算

定义

称理想I和J互素，如果$I+J=(1)$.

命题

若I和J互素，则$I\cap J=IJ$.

Proof.

由定义知总有$I\cap J\supset IJ$. 现证反包含

$$I\cap J=(I\cap J)(I+J)=(I\cap J)I+(I\cap J)J\subset IJ+IJ=IJ.$$

理想的运算

定义

称理想I和J互素，如果$I+J=(1)$.

命题

若I和J互素，则$I\cap J=IJ$.

Proof.

由定义知总有$I\cap J\supset IJ$. 现证反包含

$$I\cap J=(I\cap J)(I+J)=(I\cap J)I+(I\cap J)J\subset IJ+IJ=IJ.$$

□

理想的运算

定义

称理想I和J互素，如果$I+J=(1)$.

命题

若I和J互素，则$I\cap J=IJ$.

Proof.

由定义知总有$I\cap J\supset IJ$. 现证反包含

$$I\cap J=(I\cap J)(I+J)=(I\cap J)I+(I\cap J)J\subset IJ+IJ=IJ.$$

$\square$

理想的运算

定理

设R的理想$I_1, ..., I_n$两两互素，则$R/I_1 \cap \cdots \cap I_n \cong R/I_1 \times \cdots \times R/I_n$.

证明：做映射$\phi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$

$$\phi(a) = (\overline{a} \bmod I_1, ..., \overline{a} \bmod I_n)$$

它显然是同态，Ker$\phi = I_1 \cap \cdots \cap I_n$.

理想的运算

定理

设R的理想$I_1, ..., I_n$两两互素，则$R/I_1 \cap \cdots \cap I_n \cong R/I_1 \times \cdots \times R/I_n$.

证明：做映射$\phi : R \longrightarrow R/I_1 \times \cdots \times R/I_n$

$$\phi(a) = (\overline{a} \bmod I_1, ..., \overline{a} \bmod I_n)$$

它显然是同态，Ker$\phi = I_1 \cap \cdots \cap I_n$.

理想的运算

剩下只需证明它是满的，进一步只需证$(\overline{1},\overline{0},...,\overline{0})$在像中，即需找到$a\in R$满足对每个$j>1$，

$$a\equiv 1 \pmod{I_1}, a\equiv 0 \pmod{I_j} \qquad *$$

由于$I_1+I_j=(1)$，故存在$a_1\in I_1, a_j\in I_j$有$a_1+a_j=1$. 即

$$\begin{cases} a_j\equiv 1 \pmod{I_1} \\ a_j\equiv 0 \pmod{I_j} \end{cases}$$

取$a=a_2\cdots a_n$，则a满足$*$式. 证毕.

理想的运算

注记：对唯一分解整环R，可以定义两个元a, b的最大公约元和最小公倍元(在相伴的意义下唯一确定)，分别记为$\gcd(a, b)$和$\mathrm{lcm}(a, b)$.

当R是PID 时，有

$$(a) + (b) = (\gcd(a, b)).$$

在R非PID时，上式却未必成立．例如：

$R = \mathbb{Z}[X], g.c.d.(2, X) = 1$，但$(2) + (x) \neq (1)$.

整环的分式域

对任意整环R, 会有一个包含它的最小的域K, "最小"的意思是下列范性：对任意域L和单同态$\phi : R \longrightarrow L$, ϕ可唯一地扩充到K上.

下面具体构造这样的K如下. 令$S = R^* \times R$, 在S上定义关系$\sim$,

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

容易验证它是一等价关系.

整环的分式域

对任意整环R, 会有一个包含它的最小的域K, “最小”的意思是下列范性：对任意域L和单同态$\phi : R \longrightarrow L$, ϕ可唯一地扩充到K上.

下面具体构造这样的K如下. 令$S = R^* \times R$, 在S上定义关系$\sim$,

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

容易验证它是一等价关系.

整环的分式域

在S上定义加法和乘法运算：

$$(a,b)+(c,d)=(ac,ad+bc),(a,b)(c,d)=(ac,bd).$$

易知这两种运算都是具有同余关系的，即

$$\alpha\sim\beta,\gamma\sim\delta\Longrightarrow\alpha+\gamma\sim\beta+\delta,\alpha\gamma\sim\beta\delta.$$

因此可将运算通过代表元定义到$S/\sim$上，再验证$S/\sim$按这样的加法和乘法运算构成环. **0**元是$\overline{(1,0)}$，**1**是$\overline{(1,1)}$. 最后记$\frac{b}{a}=\overline{(a,b)}$，于是

$$K:=S/\sim=\{\frac{b}{a}|a\in R^*,b\in R\}.$$

整环的分式域

显然K也是域，因为只要a,b都非零，则$\frac{a}{b}\frac{b}{a}=\frac{1}{1}$.
还需验证R是K的子环. 为此做同态

$$R \longrightarrow K, b \longmapsto \frac{b}{a}.$$

易知这是单同态. 沿着这个单同态，也称嵌入，可以把R看作K的子环，即把b和$\frac{b}{1}$等同起来.

最后证明前面说的范性. 若有单同态$\phi : R \longrightarrow L$，则可定义同态$\psi : R \longrightarrow L$，$\psi(\frac{b}{a}) = \frac{\phi(b)}{\phi(a)}$. 定义合理是因为$a \neq 0 \Longrightarrow \phi(a) \neq 0$. 显然$\psi|R = \phi$.

整环的分式域

显然K也是域，因为只要a,b都非零，则$\frac{a}{b}\frac{b}{a}=\frac{1}{1}$。还需验证$R$是$K$的子环．为此做同态

$$R \longrightarrow K, b \longmapsto \frac{b}{a}.$$

易知这是单同态．沿着这个单同态，也称嵌入，可以把R看作K的子环，即把b和$\frac{b}{1}$等同起来．

最后证明前面说的范性．若有单同态$\phi: R \longrightarrow L$，则可定义同态$\psi: R \longrightarrow L$，$\psi(\frac{b}{a})=\frac{\phi(b)}{\phi(a)}$．定义合理是因为$a\neq 0 \Longrightarrow \phi(a)\neq 0$．显然$\psi|R=\phi$．

Gauss定理

UFD未必是PID. 例如$\mathbb{Z}[X]$, 它不是PID, 理想$(2,x)$就不是主理想, 但从下一个定理知它是UFD.

Gauss定理

R**是UFD, 则**$R[X]$**也是.**

证明Gauss定理之前需要做一些准备.

定义

R上的多项式$\sum_{i=0}^{n} a_i X^i$称为本原多项式, 若系数$a_0, \ldots, a_n$的最大公约元是1, 即$d | a_0, \ldots, a_n \Longrightarrow d$是单位.

Gauss定理

UFD未必是PID. 例如$\mathbb{Z}[X]$, 它不是PID, 理想$(2,x)$就不是主理想, 但从下一个定理知它是UFD.

Gauss定理

R是UFD, 则$R[X]$也是.

证明Gauss定理之前需要做一些准备.

定义

R上的多项式$\sum_{i=0}^{n} a_i X^i$称为本原多项式, 若系数$a_0, \dots, a_n$的最大公约元是1, 即$d|a_0, \dots, a_n \Longrightarrow d$是单位.

Gauss定理

引理1

本原多项式的乘积仍是本原多项式

证明：设$f, g \in R[X]$满足fg不是本原多项式，则必有R的某一素元p是fg的所有系数的公约元，当然pR为R的素理想，作自然同态$\pi : R \longrightarrow R/pR$，扩充到相应的多项式环上，仍记为$\pi$．于是

$$\pi(f)\pi(g) = \pi(fg) = 0.$$

而整环R/pR上的多项式环仍是整环，故$\pi(f) = 0$或$\pi(g) = 0$，即p是f或g的所有系数的公因子．那么f或g不是本原的．

Gauss定理

引理1

本原多项式的乘积仍是本原多项式

证明：设$f, g \in R[X]$满足fg不是本原多项式，则必有R的某一素元p是fg的所有系数的公约元，当然pR为R的素理想，作自然同态$\pi : R \longrightarrow R/pR$，扩充到相应的多项式环上，仍记为$\pi$．于是

$$\pi(f)\pi(g) = \pi(fg) = 0.$$

而整环R/pR上的多项式环仍是整环，
故$\pi(f) = 0$或$\pi(g) = 0$，即p是f或g的所有系数的公因子．那么f或g不是本原的．

Gauss定理

引理2

设f是R上的本原多项式且非常数，K为R的分式域，则f在R上不可约$\Longleftrightarrow$ f在K上不可约.

证明：“$\Longleftarrow$”是显然的，因为$R[X]$上的真分解也给出$F[X]$上的真分解.

Gauss定理

引理2

设f是R上的本原多项式且非常数，K为R的分式域，则f在R上不可约$\Longleftrightarrow$ f在K上不可约.

证明：“$\Longleftarrow$”是显然的，因为$R[X]$上的真分解也给出$F[X]$上的真分解.

Gauss定理

现证“$\Longrightarrow$”：设f为$R[X]$的本原多项式，若f在$F[X]$上可分解为$f = f_1 f_2 = (a_1 g_1)(a_2 g_2) = a g_1 g_2$，这里$a_1, a_2, a \in F$，$g_1, g_2$为$R[X]$中的本原多项式，从而存在$b, c \in R$有

$$bf = c g_1 g_2$$

由引理1知$g_1 g_2$为本原多项式，故对上式两端取系数的最大公因子得$b = cu, u \in R^{\times}$，于是$f = u g_1 g_2$，与f不可约矛盾. 证毕.

Gauss定理的证明

Gauss定理的证明需证明$R[x]$满足那两个基本条件.

首先证明每个元都能分解. 任意$f \in R[X]$都可表为$d \in R$与一为本原多项式之积, 同时显然有R的不可约元一定也是$R[x]$的不可约元, 故只需对本原多项式证明可分解即可.

不妨设f为本原多项式, 设$f = af_1 \cdots f_n$, $a \in R$, $f_1, ..., f_n$为$F[X]$中的首1不可约多项式.

Gauss定理的证明

取适当的$a_1, ..., a_n \in R$使

$$a_1 f_1 = g_1, ..., a_n f_n = g_n$$

为$R[X]$的本原多项式. 那么

$$a_1 \cdots a_n f = a g_1 \cdots g_n.$$

两端取系数的最大公因子得$a_1 \cdots a_n = au, u \in R^\times$, 于是$f = u g_1 \cdots g_n$, 另外由引理2知$g_1, ..., g_n$在$R[X]$中不可约.

Gauss定理的证明

最后证明$R[X]$的不可约元都是素元.

设$f(X)$是$R[X]$的不可约元. 若$f \in R$, 则可记$f = p$为R中的素元, 用引理1 的证明方法可得它也是$R[X]$的素元.

若$f \notin R$, 即f是本原多项式且在$F[X]$中不可约, 设有$g, h \in R[X]$, 使得$f|gh$, 由$F[X]$是UFD, 可知$f|g$或$f|h$.

Gauss定理的证明

不妨取前者，即存在$f_1 \in F[X]$使得

$$g = ff_1 \qquad (1).$$

取$a \in F$，使得$f_1 = af_2$，f_2为$R[X]$中的本原多项式于是$g = aff_2$. 由于ff_2为本原多项式，$g \in R[X]$，故$a \in R$，那么$f_1 \in R[X]$. 再看**(1)**式知在$R[X]$中有$f|g$，故f是$R[X]$的素元. 证毕.