环的算术性质(一)

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

环的基本知识

这里强调几个关于交换环的概念和事实：

- 零环即只含有一个元素的环.
- 极大理想：(非零)交换环R的理想I称为极大理想，如果包含I的理想恰好是两个(I自己和R);R也称为单位理想，因为一个理想含有单位当且仅当它是R.
- 素理想：交换环R的理想$I \neq R$称为素理想，如果$ab \in I \Longrightarrow a \in I$或$b \in I$.

环的基本知识

这里强调几个关于交换环的概念和事实：

- 零环即只含有一个元素的环.
- 极大理想: (非零)交换环R的理想I称为极大理想，如果包含I的理想恰好是两个(I自己和R);R也称为单位理想，因为一个理想含有单位当且仅当它是R.
- 素理想: 交换环R的理想$I \neq R$称为素理想，如果$ab \in I \Longrightarrow a \in I$或$b \in I$.

环的基本知识

这里强调几个关于交换环的概念和事实：

- 零环即只含有一个元素的环.
- 极大理想：(非零)交换环R的理想I称为极大理想，如果包含I的理想恰好是两个(I自己和R);R也称为单位理想，因为一个理想含有单位当且仅当它是R.
- 素理想：交换环R的理想$I \neq R$称为素理想，如果$ab \in I \implies a \in I$或$b \in I$.

环的基本知识

基本事实:

- 一个交换环R是域当且仅当R恰好有两个理想，即零理想和单位理想，统称平凡理想.
- R是整环$\Longrightarrow R[X]$是整环. 这是因为对任意两个非0多项式，积的首项(即最高次项)=首项的积，当然非0.

环的基本知识

基本事实:

- 一个交换环R是域当且仅当R恰好有两个理想，即零理想和单位理想，统称平凡理想.
- R是整环$\Longrightarrow R[X]$是整环. 这是因为对任意两个非**0**多项式，积的首项(即最高次项)=首项的积，当然非**0**.

环的基本知识

定理

设R是交换环，I是R的理想，则有

1) I是极大理想当且仅当R/I是域.

2) I是素理想当且仅当R/I是整环.

证明：1)由同态第二基本定理立得：

$$I\text{极大} \Longleftrightarrow R\text{的包含}I\text{的理想恰好是两个} \Longleftrightarrow$$

$$R/I\text{恰好有两个理想} \Longleftrightarrow R/I\text{是域}$$

2) 对$a \in R$，用$\bar{a}$表$a + I$，由于$a \in I \Longleftrightarrow \bar{a} = 0$，因此把素理想定义翻译成商环语言就是2).

环的基本知识

定理

设R是交换环，I是R的理想，则有

1) I是极大理想当且仅当R/I是域.

2) I是素理想当且仅当R/I是整环.

证明：1)由同态第二基本定理立得：

$$I\text{极大} \Longleftrightarrow R\text{的包含}I\text{的理想恰好是两个} \Longleftrightarrow$$
$$R/I\text{恰好有两个理想} \Longleftrightarrow R/I\text{是域}$$

2) 对$a \in R$，用$\bar{a}$表$a+I$，由于$a \in I \Longleftrightarrow \bar{a}=0$，因此把素理想定义翻译成商环语言就是2).

环的基本知识

定理

设R是交换环，I是R的理想，则有

1) I是极大理想当且仅当R/I是域.

2) I是素理想当且仅当R/I是整环.

证明：1)由同态第二基本定理立得：

$$I\text{极大} \Longleftrightarrow R\text{的包含}I\text{的理想恰好是两个} \Longleftrightarrow$$
$$R/I\text{恰好有两个理想} \Longleftrightarrow R/I\text{是域}$$

2) 对$a \in R$，用$\bar{a}$表$a+I$，由于$a \in I \Longleftrightarrow \bar{a}=0$，因此把素理想定义翻译成商环语言就是2).

环的基本知识

推论

极大理想是素理想.

例：对环$\mathbb{Z}[X]$，理想(X)是素理想、但非极大理想，因为$\mathbb{Z}[X]/(X)\cong\mathbb{Z}$是整环，但不是域；对素数$p$，理想$(p)$是素理想、但非极大理想，因为

$$\mathbb{Z}[X]/(p)\cong\mathbb{Z}/(p)[X]$$

是整环，但不是域.

环的基本知识

对素数p和多项式$f(X)\in\mathbb{Z}[X]$，理想(p,f)是否极大?

这里我们需要看$\mathbb{Z}[X]/(p,f)\cong\mathbb{Z}/(p)[X]/(\bar{f})$是否是域，这就需要$\bar{f}$是$\mathbb{Z}/(p)[X]$中的不可约多项式. 比如$p=3$, $f(X)=X^2+1$.

思考题: 刻画环$\mathbb{Z}[X]$的所有极大理想和素理想.

环的基本知识

对素数p和多项式$f(X) \in \mathbb{Z}[X]$，理想(p, f)是否极大？这里我们需要看$\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/(p)[X]/(\overline{f})$是否是域，这就需要$\overline{f}$是$\mathbb{Z}/(p)[X]$中的不可约多项式. 比如$p = 3$, $f(X) = X^2 + 1$.

思考题：刻画环$\mathbb{Z}[X]$的所有极大理想和素理想.

环的基本知识

对素数p和多项式$f(X) \in \mathbb{Z}[X]$，理想(p, f)是否极大？这里我们需要看$\mathbb{Z}[X]/(p, f) \cong \mathbb{Z}/(p)[X]/(\overline{f})$是否是域，这就需要$\overline{f}$是$\mathbb{Z}/(p)[X]$中的不可约多项式. 比如$p = 3$, $f(X) = X^2 + 1$.

思考题: 刻画环$\mathbb{Z}[X]$的所有极大理想和素理想.

唯一分解整环，主理想整环，Eulcilid环

环的概念起源于数论，第一个例子当然是$\mathbb{Z}$，平行地还有域上的一元多项式环，它们具有唯一分解性都是因为有带余除法．同样还有其它的具有带余除法的环，比如

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}, d = -1, \pm 2, 3.$$

特别需指出的是：借助这些环，可以更方便地研究环$\mathbb{Z}$的性质，比如下列问题：

1、什么素数p可表为两个整数的平方和或者更一般地表为整数的二元二次型？

2、方程$y^2 = x^3 + 2$如何在$\mathbb{Z}$中求解？

唯一分解整环，主理想整环，Eulcilid环

环的概念起源于数论，第一个例子当然是$\mathbb{Z}$，平行地还有域上的一元多项式环，它们具有唯一分解性都是因为有带余除法. 同样还有其它的具有带余除法的环，比如

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}, d = -1, \pm 2, 3.$$

特别需指出的是：借助这些环，可以更方便地研究环$\mathbb{Z}$的性质，比如下列问题：

1、什么素数p可表为两个整数的平方和或者更一般地表为整数的二元二次型？

2、方程$y^2 = x^3 + 2$如何在$\mathbb{Z}$中求解？

唯一分解整环，主理想整环，Eulcilid环

以下考虑的都是在整数的唯一分解定理的证明中抽象出的概念、方法和结论. 现在设R为(交换)整环.

定义

- 元素$a \in R$称为不可约的如果满足: $a = bc \Longrightarrow b$和c之一为单位.
- a称为素元如果满足: $a|bc \Longrightarrow a|b$或$a|c$.
- 元素a与b称为相伴，如果存在单位u满足$a = bu$.

唯一分解整环，主理想整环，Eulcilid环

以下考虑的都是在整数的唯一分解定理的证明中抽象出的概念、方法和结论. 现在设R为(交换)整环.

定义

- 元素$a \in R$称为不可约的如果满足: $a = bc \Longrightarrow b$和c之一为单位.
- a称为素元如果满足: $a|bc \Longrightarrow a|b$或$a|c$.
- 元素a与b称为相伴，如果存在单位u满足$a = bu$.

唯一分解整环，主理想整环，Eulcilid环

定义

R称为唯一分解整环(UFD)，如果R中每一个元都可唯一分解为不可约元的乘积.

注记 这里的唯一性指对两种分解$p_1 \cdots p_m = q_1 \cdots q_n$一定有$m = n$且经过适当排序，$p_i$与$q_i$相伴.

定义

由一个元素生成的理想$(a) = aR$称为主理想；如果R的所有理想都是主理想，则称R为主理想整环(PID).

唯一分解整环，主理想整环，Eulcilid环

定义

R称为唯一分解整环(UFD)，如果R中每一个元都可唯一分解为不可约元的乘积.

注记 这里的唯一性指对两种分解$p_1 \cdots p_m = q_1 \cdots q_n$一定有$m = n$且经过适当排序，$p_i$与$q_i$相伴.

定义

由一个元素生成的理想$(a) = aR$称为主理想；如果R的所有理想都是主理想，则称R为主理想整环(PID).

唯一分解整环，主理想整环，Eulcilid环

定义

R称为*Eulcid*环如果存在一个映射$\phi : R^* \longrightarrow \mathbb{Z}_{>0}$，使得对任意$a \in R, b \in R^*$,一定有$q, r \in R$使$a = bq + r$,
且$r = 0$或$\phi(r) < \phi(b)$.

注记 可理解为a可$\mathrm{mod}\, b$同余于一个比b小的元.

唯一分解整环，主理想整环，Eulcilid环

命题

R是唯一分解整环当且仅当满足如下两条：

(1)主理想升链稳定，即主理想序列

$$(a_1) \subset (a_2) \subset \cdots$$

只能有有限项.

(2)不可约元一定是素元.

注记 这个命题的证明是直截了当的，留作练习. 第一条管分解的存在性，第二条管唯一性.

唯一分解整环，主理想整环，Eulcilid环

定理

R是Eulcilid环$\Longrightarrow$ R是主理想整环$\Longrightarrow$ R是唯一分解整环.

证明：若R是Eulcid环，有标准映射$\phi: R^* \longrightarrow \mathbb{Z}_{\geq 0}$.
取R的一个理想$I \neq 0$，记a为I中满足$\phi(x)$最小的非零元，证明$I = aR$.

首先$aR \subset I$是显然的. 证反包含. 任取$b \in I$，若$b \notin I$，则b可表为$b = aq + r$，其中$q, r \in R$，且$\phi(r) < \phi(a)$.
但$r = b - aq \in I$，这与$\phi(a)$的最小性矛盾，从而$a \in I$，
即$aR \subset I$. 故$I = aR$. 因此R是**PID**.

唯一分解整环，主理想整环，Eulcilid环

定理

R是Eulcilid环$\Longrightarrow$ R是主理想整环$\Longrightarrow$ R是唯一分解整环.

证明：若R是**Eulcid**环，有标准映射$\phi : R^* \longrightarrow \mathbb{Z}_{\geq 0}$. 取$R$的一个理想$I \neq 0$，记$a$为$I$中满足$\phi(x)$最小的非零元，证明$I = aR$.

首先$aR \subset I$是显然的. 证反包含. 任取$b \in I$，若$b \notin I$，则b可表为$b = aq + r$，其中$q, r \in R$，且$\phi(r) < \phi(a)$. 但$r = b - aq \in I$，这与$\phi(a)$的最小性矛盾，从而$a \in I$，即$aR \subset I$. 故$I = aR$. 因此R是**PID**.

唯一分解整环，主理想整环，Eulcilid环

若R是PID，我们来证它满足UFD的两个基本条件.

1) 若有主理想升链$(a_1) \subset (a_2) \subset \cdots (a_n) \subset \cdots$,取

$$I = \cup_n (a_n),$$

容易检查I是理想，设$I = (a)$，存在N使得$a \in (a_N)$，那么对$n > N$,有

$$I = (a) \subset (a_N) \subset (a_n) \subset I,$$

即

$$I = (a_N) = \cdots = (a_n)$$

上述升链稳定.

唯一分解整环，主理想整环，Eulcilid环

2) 对任意非0元$p \in R$，对定义做语言上的翻译有

$$p\text{是素元} \Longleftrightarrow (p)\text{是素理想}$$

$$p\text{是不可约元} \Longleftrightarrow \text{包含}(p)\text{的主理想只有两个}.$$

当R是PID时，上述第二条变成

$$p\text{是不可约元} \Longleftrightarrow \text{包含}(p)\text{的理想只有两个} \Longleftrightarrow (p)\text{是极大理想}.$$

由于极大理想是素理想，故不可约元是素元.

通过上述1)和2)得R是UFD.

唯一分解整环，主理想整环，Eulcilid环

例、Gauss整数环$\mathbb{Z}[i]$是Eulcid环，因而是PID和UFD.

证明：作映射$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^+$:

$$N(a+bi) = a^2 + b^2,$$

现证明N符合Eucilid环的要求.

对任意$\alpha, \beta \in \mathbb{Z}[i]$，若$\frac{\alpha}{\beta} \notin \mathbb{Z}[i]$,则可设

$$\frac{\alpha}{\beta} = \gamma + (a+bi),$$

这里$\gamma \in \mathbb{Z}[i]$,$a, b \in \mathbb{Z}$，且$a, b \in (-\frac{1}{2}, \frac{1}{2}]$. 于是

$$\alpha = \beta\gamma + \beta(a+bi).$$

唯一分解整环，主理想整环，Eulcilid环

例、Gauss整数环$\mathbb{Z}[i]$是Eulcid环，因而是PID和UFD.

证明：作映射$N:\mathbb{Z}[i]\longrightarrow\mathbb{Z}^{+}$:

$$N(a+bi)=a^2+b^2,$$

现证明N符合Eucilid环的要求.

对任意$\alpha,\beta\in\mathbb{Z}[i]$，若$\frac{\alpha}{\beta}\notin\mathbb{Z}[i]$,则可设

$$\frac{\alpha}{\beta}=\gamma+(a+bi),$$

这里$\gamma\in\mathbb{Z}[i]$,$a,b\in\mathbb{Z}$，且$a,b\in(-\frac{1}{2},\frac{1}{2}]$. 于是

$$\alpha=\beta\gamma+\beta(a+bi).$$

唯一分解整环，主理想整环，Eulcilid环

一方面，$\beta(a+bi)=\alpha-\beta\gamma\in\mathbb{Z}[i]$. 另一方面

$$N(\beta(a+bi))=N(\beta)N(a+bi)=(a^2+b^2)N(\beta)\leq\frac{1}{2}N(\beta)<N(\beta).$$

综上，我们证明了环$\mathbb{Z}[i]$是Eucilid环.

Euclid环的数论应用

先列出Gauss整数环$\mathbb{Z}[i]$的基本性质:

1. $\mathbb{Z}[i]$是Euclid环，也是PID和UFD.
2. 单位是$\pm 1, \pm i$.
3. 素元一定相伴于一个素数p或一个本原的元素$a + bi$, $(a, b) = 1$, 但什么样的p或一个本原的元素$a + bi$是素元则需进一步考察.

Euclid环的数论应用

定理

设p是奇素数，则

$$p\text{可表为二平方和} \iff p \equiv 1 \pmod 4.$$

证明：只需证“$\Longleftarrow$”(另一半是平凡的). 由于$p \equiv 1 \pmod 4$，即4是$p-1$的因子. 而乘法群$(\mathbb{Z}/p\mathbb{Z})^*$是$p-1$阶循环群，故有4阶元存在. 即存在整数$a$满足

$$a^4 \equiv 1 \pmod p, a^2 \not\equiv 1 \pmod p.$$

Euclid环的数论应用

定理

设p是奇素数，则

$$p\text{可表为二平方和} \iff p \equiv 1 \pmod 4.$$

证明：只需证“$\Longleftarrow$”(另一半是平凡的)．由于$p \equiv 1 \pmod 4$，即4是$p-1$的因子．而乘法群$(\mathbb{Z}/p\mathbb{Z})^*$是$p-1$阶循环群，故有4阶元存在．即存在整数$a$满足

$$a^4 \equiv 1 \pmod p, a^2 \not\equiv 1 \pmod p.$$

Euclid环的数论应用

即$a^2 \equiv -1 \pmod p$，那么

$$p|a^2+1=(a+i)(a-i)$$

但$p|a+i$和$p|a-i$都不成立．说明p在$\mathbb{Z}[i]$上不是“素”的，即有$\mathbb{Z}[i]$上的非单位的元素$a+bi$和$c+di$，使得

$$p=(a+bi)(c+di)$$

即

$$p^2=(a^2+b^2)(c^2+d^2)$$

利用$\mathbb{Z}$的唯一分解性知

$$p=a^2+b^2.$$

Euclid环的数论应用

由该定理可得$\mathbb{Z}[i]$的其它基本性质如下:

- 素数p是$\mathbb{Z}[i]$的素元$\Longleftrightarrow p \equiv 3 \pmod 4$
- 对互素的整数a, b，$a + bi$是$\mathbb{Z}[i]$的素元$\Longleftrightarrow a^2 + b^2$是素数.

Euclid环的数论应用

通过对环$\mathbb{Z}[\sqrt{-2}]$的研究可得类似的定理.

定理

设p是奇素数，则

$$p = a^2 + 2b^2 \Longrightarrow (\frac{-2}{p}) = 1 \Longleftrightarrow p \equiv 1, 3 \pmod 8.$$

Euclid环的数论应用

下面再看解不定方程的问题.

例1、求方程$y^2+1=x^3$的整数解.

解：对方程模4可知y是偶数，$(y+i,y-i)=1$. 将原方程变形为

$$(y+i)(y-i)=x^3.$$

由$\mathbb{Z}[i]$的唯一分解性知

$$y+i=u(a+bi)^3, u\text{是单位}.$$

由于u只能取$\pm1,\pm i$，也是3次幂，故上式可简写为

$$y+i=(a+bi)^3$$

比较虚部知原方程解为$x=0,y=\pm1$.

Euclid环的数论应用

下面再看解不定方程的问题.

例1、求方程$y^2+1=x^3$的整数解.

解：对方程模4可知y是偶数，$(y+i, y-i)=1$. 将原方程变形为

$$(y+i)(y-i)=x^3.$$

由$\mathbb{Z}[i]$的唯一分解性知

$$y+i=u(a+bi)^3, u\text{是单位}.$$

由于u只能取$\pm 1, \pm i$，也是3次幂，故上式可简写为

$$y+i=(a+bi)^3$$

比较虚部知原方程解为$x=0, y=\pm 1$.

Euclid环的数论应用

例2、求方程$y^2+2=x^3$的整数解.

解：对方程模4可知y是奇数，$(y+\sqrt{-2}, y-\sqrt{-2})=1$. 将原方程变形为

$$(y+\sqrt{-2})(y-\sqrt{-2})=x^3.$$

由$\mathbb{Z}[\sqrt{-2}]$的唯一分解性知

$$y+\sqrt{-2}=u(a+b\sqrt{-2})^3, u\text{是单位}.$$

由于u只能取±1，也是3次幂，故上式可简写为

$$y+\sqrt{-2}=(a+b\sqrt{-2})^3$$

比较虚部知原方程无解.

Euclid环的数论应用

例2、求方程$y^2+2=x^3$的整数解.

解：对方程模4可知y是奇数，$(y+\sqrt{-2}, y-\sqrt{-2})=1$. 将原方程变形为

$$(y+\sqrt{-2})(y-\sqrt{-2})=x^3.$$

由$\mathbb{Z}[\sqrt{-2}]$的唯一分解性知

$$y+\sqrt{-2}=u(a+b\sqrt{-2})^3, u\text{是单位}.$$

由于u只能取± 1，也是3次幂，故上式可简写为

$$y+\sqrt{-2}=(a+b\sqrt{-2})^3$$

比较虚部知原方程无解.