抽象代数学

设R是一个环，$a\in R$，由a生成的子环

$\langle a\rangle=\{b_1a+b_2a^2+\cdots+b_ma^m \mid b_i\in\mathbb{Z}, m\in\mathbb{N}\}$

由a生成的理想

$(a)=\{x_1ay_1+\cdots+x_may_m+xa+ay+na \mid x_i, y_i, x, y\in R, n\in\mathbb{Z}\}$

这种理想称为主理想(principal ideal)

若R是含幺交换环 则$(a)=\{ra \mid r\in R\}$

定义 若R是一个整环，且每个理想均是主理想，则R称为主理想整环(principal ideal domain，简称PID)

若R是整区且满足定义条件，则R是主理想整区.

例1 $\mathbb{Z}$是一个主理想整区

证明：设I是$\mathbb{Z}$的一个理想，若$I=\{0\}$ 则$I=(0)$

若$I\neq\{0\}$，存在最小正整数$a\in I$. 则$(a)\subseteq I$ $\forall b\in I$

由带余除法，$b=qa+r$，$q,r\in\mathbb{Z}$，$0\le r<a$. 则

$r=b-qa\in I$，这与条件：a是I中最小正整数 可得$r=0$

$b\in(a)$ 因此$I=(a)$.

例2 一个域F是一个主理想整区，它的理想只有(0)，(1)

例3 若$\mathbb{F}$是一个域，则$\mathbb{F}[x]$是一个主理想整区.

证明：设I是$\mathbb{F}[x]$的一个理想 且$I\neq(0)$. 设$p(x)\neq 0\in I$ 满足对于$\forall q(x)\neq 0\in I$ $\deg p(x)\leq \deg q(x)$. 正如例1，

由带余除法，$q(x)=p(x)t(x)+r(x)$, $0\leq\deg r(x)<\deg p(x)$

但是$r(x)\in I$，则$r(x)=0$ $q(x)\in(p(x))\Rightarrow I=(p(x))$

注：(1) $\mathbb{Z}[x]$不是一个PID. 例如$(2,x)$不是一个主理想.

否则$(2,x)=(p(x))\Rightarrow 2=p(x)q(x)\Rightarrow p(x)=\pm1$或$\pm2$.

若$p(x)=2$ $x\notin(2)$

(2) 设R是一个整区，$R[x]$是一个主理想整环$\Leftrightarrow R$是个域.

定理 主理想整区是唯一分解整环.

我们分解如下几步证明这个定理.

引理1 设R是一个主理想整区，$a\in R$是不可约元$\Leftrightarrow$ $(a)\neq(0)$, (a)是极大理想，即若I是R的理想，$(a)\subsetneq I$，则 $I=R$

证明："$\Rightarrow$" 设$a\in R$不可约，则$(a)\neq(0)$. 若I是R的理想，且$(a)\subsetneq I$，因为R是一个PID，则$I=(b)$，$(a)\subsetneq(b)$ $\exists c\in R$，$a=bc$，由a不可约，且$(a)\subsetneq(b)$ 则b可逆

"$\Leftarrow$" 设$(a)\neq 0$，(a)极大，设$a=bc$，则$(a)\subset($

由极大性，$(b)=(a)$ 或 $(b)=R$. 若 $(b)=(a)$ 则 $a\sim b$

$\Rightarrow c$ 可逆.

引理2. 设 R 是主理想整区，则它的不可约元是素元.

证明：设 $a\neq 0\in R$ 是不可约元，且 $a\mid bc$，若 $a\nmid b$

则 $b\notin(a)\Rightarrow(a)\subsetneq(a,b)$，由 (a) 的极大性，$(a,b)=R$

$\exists x,y\in R$ $\quad xa+yb=1$，$\Rightarrow c=xac+ybc$，因为右边

被 a 整除，得 $a\mid c\Rightarrow a$ 是素元.

引理3. 设 R 是主理想整区，则它满足因子链条件，即

$\forall a\neq 0\in R$ $\quad a$ 不可逆，则 a 可写成有限个不可约元乘积

证明：设 $a\neq 0\in R$ 且非单位. 若 a 不可约，则已得结论.

若 a 可约，设 $a=a_1a_1'$ $\quad a_1,a_1'$ 均非单位，$(a)\subsetneq(a_1)$
且 a_1 可约

继续上述讨论，若 a_1 可约，$a_1=a_2a_2'$，~~若 a_2,a_2' 均不可约~~，

$(a_1)\subsetneq(a_2)$，若 a 不能写成有限个不可约元乘积，则得

到无穷升链：$(a)\subsetneq(a_1)\subsetneq(a_2)\subsetneq\cdots$

令 $I=\bigcup_{i=1}^{\infty}(a_i)$ 它是 R 的理想：$\forall x,y\in I$，则 $\exists i\leq j$

$x\in(a_i),y\in(a_j)\Rightarrow x,y\in(a_j)\Rightarrow I$ 关于加法、乘法封闭.

$\forall r\in R, x\in I$ $\quad\exists k$，$x\in(a_k)\Rightarrow rx\in I$.

由于 R 是 PID，$\exists b\in R$，$I=(b)$，$b\in I\Rightarrow\exists l$，$b\in(a_l)$

即 $(b) \subseteq (a^l) \Rightarrow (a^l) = (a^{l+1}) = \cdots$ 与 a 不能写成有限个不可约元乘积矛盾.

定理是引理1, 2, 3的自然推论.

欧氏整环 (Euclidean domain)

定义 设 R 是一个整区且存在从 $R^* = R\setminus\{0\}$ 到 $\mathbb{N}$ (非负整数) 的一个映射 $\delta: R^* \longrightarrow \mathbb{N} = \{0, 1, 2, \cdots\}$ 满足

(1) 若 $a, b \in R$ 且 $b \neq 0$, 则存在 $q, r \in R$, $a = bq + r$, $r = 0$ 或 $\delta(r) < \delta(b)$;

(2) $\forall a, b \neq 0 \in R$, 有 $\delta(ab) \geq \delta(a)$. 则 R 称为欧氏整环

换句话说, 我们赋予 R 中非零元一个"长度", 可以比较大小, 从而使用带余除法.

例. $\mathbb{Z}$, $\mathbb{F}[x]$ ($\mathbb{F}$ 是一个域) 均有带余除法 $\Rightarrow$ 它们是欧氏整环, 其中 $\delta(n) = |n|$, $\delta(f(x)) = \deg f(x)$.

例 $\mathbb{Z}[\sqrt{-1}]$ 是欧氏整环, $\forall a \in \mathbb{Z}[\sqrt{-1}]$ $a = x + y\sqrt{-1}$, $\delta(a) = x^2 + y^2 \in \mathbb{N}$. $\forall a, b \neq 0 \in \mathbb{Z}[\sqrt{-1}]$, $a = x_1 + y_1\sqrt{-1}$, $b = x_2 + y_2\sqrt{-1}$, 显然 $\delta(ab) \geq \delta(a)$. 以下展示定义中 (1) 成立.

欲求 $q, r \Leftrightarrow ab^{-1} = q + rb^{-1}$ 即给定 $\mathbb{Q}(i)$ 中一元素 u, 找 $\mathbb{Z}[\sqrt{-1}]$ 中一元素 v, 使得 u, v 尽可能"接近".

设 $\frac{a}{b} = A+Bi$，$A, B \in \mathbb{Q}$，存在整数 C, D，使得

$$|A-C| \leq \frac{1}{2}, \quad |B-D| \leq \frac{1}{2} \quad (A, B\text{的四舍五入})$$

令 $q = C+Di \qquad r = a - bq = b(\frac{a}{b} - q)$

$$\delta(r) = \delta[b((A-C)+(B-D)i)]$$

$$= \delta(b)[(A-C)^2+(B-D)^2] \leq \delta(b)[(\tfrac{1}{2})^2+(\tfrac{1}{2})^2] < \delta(b)$$

（这里 δ 被扩充为 $\delta: \mathbb{Q}[i] = \{a+bi \mid a, b \in \mathbb{Q}\} \longrightarrow \mathbb{Q}_{\geq 0}$）

定理 欧氏整环是PID.

证明：设 R 是欧氏整环，I 为 R 的理想，若 $I \neq \{0\}$，存在 $b \in I$，$\delta(b)$ 最小．即 $\delta(b) = \min\{\delta(x) \mid x \in I, x \neq 0\}$ $\forall a \in I$ 则存在 q, r，$a = bq + r$，$r = 0$ 或 $\delta(r) < \delta(b)$，因为 $a, b \in I$ $r \in I$，于是 $r = 0$ 即 $a = bq \Rightarrow I = (b)$.

推论 欧氏整环是唯一分解整环.

注：存在主理想整环不是欧氏整环

例 $R = \{a + b(\frac{1+\sqrt{-19}}{2}) \mid a, b \in \mathbb{Z}\}$ 是PID，不是欧氏整环.

作业：Page105，2，3，4，5，6，8，9.

二次代数整数环

定义 一个二次环是 $\mathbb{Z}[\nu]$ 其中 ν 是 $x^2+ax+b\in\mathbb{Z}[x]$ 的根。若 ν 是实根，则 $\mathbb{Z}[\nu]$ 是实二次环，否则是虚二次环 (imaginary quadratic ring)

例如：$\mathbb{Z}[\sqrt{-1}]$，$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

因为 $\nu^2=-a\nu-b\in\mathbb{Z}+\mathbb{Z}\nu \Rightarrow \mathbb{Z}[\nu]=\mathbb{Z}+\mathbb{Z}\nu$

ν 的共轭 (conjugate) 是 $\bar{\nu}=-a-\nu$ ($x^2+ax+b=0$ 的另一根)

$\forall\, x+y\nu\in\mathbb{Z}[\nu]$ 　共轭是 $x+y\bar{\nu}=(x-ay)-y\nu$

定义 $\delta:\mathbb{Z}[\nu]\longrightarrow\mathbb{Z}_{\geq 0}$ 称为范数 (norm)

$$\alpha=x+y\nu\longmapsto\alpha\bar{\alpha}=x^2-axy+by^2$$

(1) $\delta(\alpha)=0\Leftrightarrow\alpha=0$ 　(2) $\delta(\alpha\beta)=\delta(\alpha)\delta(\beta)$

例 $\nu=\sqrt{2}$ 　$\delta(x+y\nu)=x^2-2y^2$

$\nu=\frac{1+\sqrt{5}}{2}$ 　$\delta(x+y\nu)=x^2+xy-y^2$

定理 $\mathbb{Z}[\nu]$ 中单位是范数 $=\pm1$ 的元素

证明：设 $\alpha\in\mathbb{Z}[\nu]$ 是单位 $\Leftrightarrow\exists\,\beta\in\mathbb{Z}[\nu]$，$\alpha\beta=1\Rightarrow$
$\delta(\alpha)\cdot\delta(\beta)=1\Rightarrow\delta(\alpha)=\pm1$，反之 $\delta(\alpha)=\pm1\Rightarrow\alpha\bar{\alpha}=\pm1\Rightarrow\alpha$ 是单位.

例 $\mathbb{Z}[\sqrt{3}]$ 　$\delta(x+y\nu)=x^2-3y^2$

$\delta(\alpha)=\pm1\Longrightarrow\alpha=\pm1,\ \pm2\pm\sqrt{3}$

定理 令 $\xi = \frac{-1+\sqrt{-3}}{2}$，$\mathbb{Z}[\xi]$是唯一分解整环

证明：我们展示它是欧氏整环，定义 $\mathbb{Z}[\xi] \xrightarrow{\delta} \mathbb{Z}_{\geq 0}$

$\delta(a+b\xi) = a^2 - ab + b^2$（因为$\xi$满足$x^2+x+1=0$）

这可扩充为 $\mathbb{Q}[\xi] \xrightarrow{\delta} \mathbb{Z}_{\geq 0}$

$\forall \alpha, \beta \neq 0$ $\frac{\alpha}{\beta} = a + b\xi$，$a, b \in \mathbb{Q}$，$a, b$ 取整得

$a = a' + x$，$b = b' + y$ $0 \leq x, y < 1$，$a', b' \in \mathbb{Z}$

令 $q = a' + b'\xi \in \mathbb{Z}[\xi]$，$r = \alpha - \beta q = \beta(\frac{\alpha}{\beta} - q)$

$\delta(r) = \delta(\beta)\delta(x+y\xi) = \delta(\beta)(x^2 - xy + y^2) < \delta(\beta)$

（注：$x^2 - xy + y^2 = (x-y)^2 + xy < (x-y)^2 + y^2 < x^2 < 1$）

设$x<y$

$\mathbb{Z}[\xi]$的同余性质：(1) 单位：$\pm 1, \pm \xi, \pm \xi^2 = \pm(1+\xi)$

(2) $1-\xi \mid a+b\xi \Leftrightarrow 3 \mid a+b$ $a, b \in \mathbb{Z}$

(3) $1-\xi \nmid a+b\xi \Rightarrow (a+b\xi)^3 \equiv \pm 1 \pmod 9$

(4) 若$\delta(\alpha) = p$素数，则α是一个不可约元（也是素元）

因此 $1-\xi$是一个素元.