抽象代数学(XXII)

设R是含幺交换环，上一讲已得带余除法：$\forall f(x), g(x) \neq 0 \in R[x]$，且$g(x)$首项系数是$R$中单位，则存在唯一多项式$q(x), r(x) \in R[x]$，使得

$$f(x) = q(x)g(x) + r(x)，且 \deg r(x) < \deg g(x)$$

推论 设R如上，$f(x) \in R[x]$，$\forall c \in R$，存在唯一$q(x) \in R[x]$，$f(x) = q(x)(x-c) + f(c)$.

定义 设R是交换环S的子环，$f(x_1, \cdots, x_n) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \in R[x_1, \cdots, x_n]$，$c_1, \cdots, c_n \in S$ 使得$f(c_1, \cdots, c_n) = 0$，则$(c_1, \cdots, c_n)$称为f的根(或零点)

定理 设D是唯一分解整区，其分式域为$\mathbb{F}$，设$f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$，若$u = \frac{c}{d} \in \mathbb{F}$，$c, d \overset{\neq 0}{\in} D$，$(c,d)=1$且$u$是$f(x)$的根，则$c | a_0$且$d | a_n$.

证明：$f(u) = 0 \Rightarrow \sum_{i=0}^{n} a_i \left(\frac{c}{d}\right)^n = 0 \Rightarrow a_0 d^n + a_1 c d^{n-1} + \cdots + a_n c^n = 0$

$\Rightarrow c | a_0 d^n$，$d | a_n c^n$，因为$(c,d)=1 \Rightarrow c | a_0$，$d | a_n$

例 $D = \mathbb{Z}$，$\mathbb{F} = \mathbb{Q}$，$f(x) = 3x^4 - 6x^3 - 21x^2 - 11x - 4 \in \mathbb{Z}[x]$

设$\frac{c}{d}$是一个根，则c可能$\pm 1, \pm 2, \pm 4$，d可能$\pm 1, \pm 3$

以下目标：D唯一分解整区 $\Rightarrow$ $D[x]$唯一分解整区

定义 设D是唯一分解整区，对 $f(x)=\sum_{i=0}^{n}a_ix^i\in D[x]$，设 $(a_0,a_1,\cdots,a_n)$ 为D中单位，则 $f(x)$ 是本原多项式.

显然，$\forall f(x)\neq 0\in D[x]$，$f(x)=cf_1(x)$，$c\in D$，$f_1(x)$ 是本原多项式.

定理（Gauss）本原多项式乘积是本原多项式.

证明：设 $f(x)=\sum_{i=0}^{m}a_ix^i$，$g(x)=\sum_{j=0}^{n}b_jx^j$ 均是 $D[x]$ 上本原多项式.

$f(x)g(x)=\sum_{k=0}^{n+m}c_kx^k$，$c_k=\sum_{i+j=k}a_ib_j$，若 $f(x)g(x)$ 非本原，

则存在不可约元 p（也是素元）$\in D$，$p\mid c_k$，$k=0,\cdots,n+m$

因为 $f(x)$，$g(x)$ 均本原，存在 s,t 使得 $p\mid a_i$，$(i<s)$

$p\nmid a_s$，$p\mid b_j$ $(j<t)$，$p\nmid b_t$

$$c_{s+t}=a_0b_{s+t}+a_1b_{s+t-1}+\cdots+a_{s-1}b_{t+1}+a_sb_t+a_{s+1}b_{t-1}+\cdots+a_{s+t}b_0$$

（若 $s+t>m$，则 $a_{m+1}=\cdots=a_{s+t}=0$，同理对于 $b_{n+1},\cdots,b_{s+t}$）

$p\mid c_{s+t}$，但 $p\nmid a_sb_t$（p是素元）矛盾！

推论. 设D是唯一分解整区，分式域为 $\mathbb{F}$，$f\in D[x]$，是本原多项式，$\deg f(x)>0$，则 $f(x)$ 在 $D[x]$ 中不可约 $\Leftrightarrow$

$f(x)$ 在 $\mathbb{F}[x]$ 中不可约

注：若 $f(x)$ 非本原，结论不对，例如 $2x+2\in\mathbb{Z}[x]$ 可约

$2x+2$ 在 $\mathbb{Q}[x]$ 中不可约.

证明：设 $f(x)\in D[x]$ 不可约且 $f(x)=g(x)h(x)$，$g(x),h(x)\in\mathbb{F}[x]$，$\deg g(x)\geq 1$，$\deg h(x)\geq 1$.

令 $g(x)=\sum_{i=0}^{n}\left(\frac{a_i}{b_i}\right)x^i$，$h(x)=\sum_{j=0}^{m}\left(\frac{c_j}{d_j}\right)x^j$，$a_i,b_i,c_j,d_j\in D$

且 $b_i,d_j\neq 0$　令 $b=b_0b_1\cdots b_n$　$\hat{b}_i=b_0b_1\cdots b_{i-1}b_{i+1}\cdots b_n$

$g_1(x)=\sum_{i=0}^{n}a_i\hat{b}_ix^i\in D[x]$，$\exists\, c\in D$，$g_1(x)=c\,g_2(x)$，$g_2(x)\in D[x]$ 是本原多项式，$g=\frac{1}{b}g_1=\frac{c}{b}g_2$，$\deg g(x)=\deg g_2(x)$

同理 $h(x)=\frac{e}{d}h_2(x)$，$h_2(x)\in D[x]$ 本原，$d,e\in D$.

$\Rightarrow f(x)=\left(\frac{c}{b}\right)\cdot\left(\frac{e}{d}\right)g_2(x)h_2(x)\Rightarrow(bd)f(x)=(ce)g_2(x)h_2(x)$

因为 $f(x)$，$g_2(x)h_2(x)$ 均本原，bd 和 ce 在 D 中相伴.

即 $f(x)$ 和 $g_2(x)h_2(x)$ 在 $D[x]$ 中相伴，从而和 $f(x)$ 不可约矛盾.

反之，若 $f(x)$ 在 $\mathbb{F}[x]$ 中不可约且 $f(x)=g(x)h(x)$，$g(x),h(x)\in D[x]$，$g(x),h(x)$ 可看成 $\mathbb{F}[x]$ 中多项式，必有一个为 $\mathbb{F}$ 中单位，设为 $g(x)$，$g(x)$ 在 $D[x]$ 中是一个常数 $g_0\in D$.（$\deg g(x)=0$）

因为 $f(x)$ 是本原的，g_0 是 D 中单位.

定理 若D是唯一分解整区，则$D[x]$也是.

证明：若$f(x)\in D[x]$ $\deg f(x)>0$，则$f(x)=cf_1(x)$，$c\in D$，

$f_1(x)$本原多项式，设$\mathbb{F}$是D的分式域，则$\mathbb{F}[x]$是欧氏整区，从而是唯一分解整区，且包含$D[x]$，设$f_1(x)=p_1^*(x)\cdots p_n^*(x)$

$p_i^*(x)\in\mathbb{F}[x]$不可约，由上一推论证明，$p_i^*(x)=\left(\frac{a_i}{b_i}\right)p_i(x)$，

$a_i,b_i\in D$，$b_i\neq 0$，$\frac{a_i}{b_i}\in\mathbb{F}$，$p_i(x)\in D[x]$，$p_i(x)$是本原的，

$p_i(x)$在$\mathbb{F}[x]$中不可约，从而在$D[x]$中不可约. 令$a=a_1\cdots a_n$，$b=b_1\cdots b_n$，则$f_1(x)=\left(\frac{a}{b}\right)p_1(x)\cdots p_n(x)$，$f_1(x)$和

$p_1(x)\cdots p_n(x)$均本原，从而$a\sim b$（在D中）$\frac{a}{b}=u$单位.

$f(x)=c_1\cdots c_l(up_1)p_2\cdots p_n$ $\quad c_1\cdots c_l=c$，c_i不可约（在D中）

即$f(x)$写成有限个不可约元（$D[x]$中）乘积.

（唯一性）设$f(x)=c_1\cdots c_m p_1\cdots p_n=d_1\cdots d_r q_1\cdots q_s$

其中$c_1,\cdots,c_m,d_1,\cdots,d_r\in D$不可约，

$p_1,\cdots,p_n,q_1\cdots q_s\in D[x]$正次数不可约多项式（也是本原的），则$c_1\cdots c_m$和$d_1\cdots d_r$相伴，因为D唯一分解，

$m=r$. 重排后，$c_i\sim d_i\Rightarrow p_1\cdots p_n$和$q_1\cdots q_s$在$D[x]$中

相伴$\Rightarrow$在$\mathbb{F}[x]$中相伴，但$\mathbb{F}[x]$是唯一分解，则$n=s$，

重排后，p_i和q_i在$\mathbb{F}[x]$中相伴. 存在$\frac{u}{v}\in\mathbb{F}$; $u,v\in D$

$$p_i=\frac{u}{v}q_i \qquad p_i, q_i\text{本原} \Rightarrow u\sim v\text{(在}D\text{中)}$$

$\Rightarrow p_i, q_i$在$D[x]$中相伴.

推论. 若$\mathbb{F}$是一个域，则$\mathbb{F}[x_1,\cdots,x_n]$是唯一分解整区.

素理想

以下R是含幺交换环

定义 I是R的理想且$I\neq R$，若$\forall a,b\in R$，$ab\in I$均可推断$a\in I$或$b\in I$. 则I称为素理想.

例. $\mathbb{Z}=R$，p是一个素数，(p)是素理想.

R整区，(0)是一个素理想.

定理 设R是整区，$p, c\neq 0\in R$

(1) p为素元$\Longleftrightarrow(p)$是非零素理想.

(2) c不可约元$\Longleftrightarrow(c)$是R的全体真主理想中极大理想.

证明: (1) p为素元，$\Rightarrow$ 若$ab\in(p)$，$p\mid ab$，$p\mid a$或$p\mid b$，

$\Rightarrow a\in(p)$或$b\in(p)$ 反之亦然.

(2) 设c不可约元，$(c)\neq R$，若$(c)\subset(d)$，则$c=dx$，$\Rightarrow$

d或x是单位，即$(d)=R$或$c\sim d$，$(c)=(d)$

反之，若(c)在真主理想中极大，则$c\neq 0$，c非单位，若$c=ab$，则$(c)\subset(a)$，$(c)\subset(b)$ 由极大性 $(c)=(a)$或$(a)=R$，$(c)=(a)\Rightarrow cx=a$，$ay=c\Rightarrow c=cxy\Rightarrow xy=1$

定理．若I是R的理想且$I\neq R$，则(1) I是素理想$\Leftrightarrow R/I$是整区，(2) I是极大理想$\Leftrightarrow R/I$是域．

证明：(1) "$\Rightarrow$" $\forall \bar{r}_1,\bar{r}_2\in R/I$，且$\bar{r}_1\cdot\bar{r}_2=\bar{0}$ 则$r_1r_2\in I$

$\Rightarrow r_1\in I$或$r_2\in I\Rightarrow \bar{r}_1=\bar{0}$或$\bar{r}_2=\bar{0}$

"$\Leftarrow$" 若R/I是整区，$ab\in I$，则$\bar{a}\cdot\bar{b}=\bar{0}\Rightarrow\bar{a}=\bar{0}$或$\bar{b}=\bar{0}$

$\Rightarrow a\in I$或$b\in I$．

例．$\mathbb{Z}[x]$，$f(x)$不可约$\in\mathbb{Z}[x]$ $(f(x))$是素理想

不是极大理想

则$\dfrac{\mathbb{Z}[x]}{(f(x))}$是整区．

定理 $\mathbb{Z}[x]$中素理想有以下三类：

(1) (0)；(2) $(f(x))$，$f(x)\in\mathbb{Z}[x]$不可约；(此时非极大理想)

(3) $(p,f(x))$，$p\in\mathbb{Z}$素数，$f(x)$在$\mathbb{Z}_p[x]$中不可约 (极大理想

证明：略．(参见《代数学引论》，153页)

素理想一个重要应用是代数几何

一般地，极大理想是素理想，反之不然 如 $\mathbb{Z}[x]$

设 R 是含幺交换环，I 是一个素理想，则 $S=R-I$ 是一个乘法闭集，即 $\forall s_1, s_2 \in S$，$s_1 s_2 \in S$

~~令 $R_S = \{ \frac{r}{s} \mid r\in R, s\in S \}$~~

令 $R\times S = \{(r,s) \mid r\in R, s\in S\}$ 定义"$\sim$"

$(r,s)\sim(r',s') \Longleftrightarrow s_1(rs'-r's)=0$，$\exists s_1\in S$

令 $R_S = \frac{R\times S}{\sim} = S^{-1}R = \{\frac{r}{s} \mid r\in R, s\in S\}$.

定理 R_S 是一个含幺交换环，有唯一极大理想 $J=\{\frac{a}{s} \mid a\in I, s\in S\}$

证明：$\forall \frac{r}{s} \notin J$，则 $r\notin I$，因此 $\frac{r}{s}$ 是单位，从而 J 极大.

例 $R=\frac{\mathbb{F}[x,y]}{(f(x,y))}$ $f(x,y)$ 不可约，$\forall (a,b)\in \mathbb{F}^2$

$\overline{(x-a,\ y-b)}$ 是 R 的极大理想. 记作 $I_{(a,b)}$

则令 $S=R-I_{(a,b)}$ $S^{-1}R$ 有唯一极大理想.

作业 Page 114-115 2, 3, 5, 7, 8, 9, 10