抽象代数学

设$\mathbb{F}$是一个域，我们总结$\mathbb{F}[x]$的一些基本性质

规定 若 $f(x)=a_0\neq 0\in\mathbb{F}$ 则 $\deg f(x)=0$.

$f(x)=0$ 则 $\deg f(x)=-\infty$

性质：(1) $\mathbb{F}[x]$是欧氏整环，因而是唯一分解整环.

(2) 设 $f(x)\in\mathbb{F}[x]$不可约，则$(f(x))$是$\mathbb{F}[x]$的极大理想，反之亦然.

(3) $\dfrac{\mathbb{F}[x]}{(f(x))}$是一个域 $\Leftrightarrow f(x)\in\mathbb{F}[x]$不可约

证明：(3) 若$f(x)$不可约，则$(f(x))$是极大理想，$\forall g(x)\notin(f(x))$，则$(f(x),g(x))=\mathbb{F}[x]$，存在$u(x),v(x)\in\mathbb{F}[x]$

$u(x)f(x)+v(x)g(x)=1$ 在$\dfrac{\mathbb{F}[x]}{(f(x))}$中，$\overline{v(x)}\cdot\overline{g(x)}=\overline{1}$

反之，若$\dfrac{\mathbb{F}[x]}{(f(x))}$是一个域，考虑 $\mathbb{F}[x]\longrightarrow\dfrac{\mathbb{F}[x]}{(f(x))}$，则$\mathbb{F}[x]$中包含$(f(x))$的理想和$\dfrac{\mathbb{F}[x]}{(f(x))}$中理想一一对应，从而包含$(f(x))$的理想$=\mathbb{F}[x]$.

例 $\mathbb{F}=\mathbb{R}$，$f(x)=x^2+1$ $\quad\dfrac{\mathbb{R}[x]}{(x^2+1)}\cong\mathbb{C}$

设$\mathbb{F}\hookrightarrow S$ $\;S$是一个环，$\mathbb{F}$是其子环. 例如$S=\mathbb{F}[x]$

$\forall s\in S$，$\langle s\rangle=\{a_0+a_1s+\cdots+a_ns^n \mid a_i\in\mathbb{F},n\in\mathbb{N}\}\overset{\text{记作}}{=\!=}\mathbb{F}[s]$

定义 $\mathbb{F}[x] \xrightarrow{\eta} \mathbb{F}[s]$ 这是一个满的环同态

$$x \longmapsto s$$

$$\sum a_i x^i \longmapsto \sum a_i s^i$$

$\ker\eta$ 是 $\mathbb{F}[x]$ 的理想 则 $\ker\eta = (f(x))$ $\exists f(x) \in \mathbb{F}[x]$

(1) 若 $f(x)=0$，η 是同构，$\Leftrightarrow \mathbb{F}[s]$ 整环 S 称为超越元 (transcendental element)

(2) 若 $f(x) \neq 0$，则 $f(x)$ 不可约，否则 $f(x) = f_1(x) f_2(x)$

$\eta(f(x)) = \eta(f_1(x))\,\eta(f_2(x)) = f_1(s) f_2(s) = 0$

因为 $\mathbb{F}[s]$ 整环，$f_1(s)=0$ 或 $f_2(s)=0 \Rightarrow f_1(x)$ 或 $f_2(x) \in \ker\eta$

此时 s 称为代数元 (algebraic element)

例 $\mathbb{F}=\mathbb{Q}$ $\sqrt{2} \notin \mathbb{Q}$ $\mathbb{Q}[x] \xrightarrow{\eta} \mathbb{Q}[\sqrt{2}]$

$\ker\eta = (x^2-2)$ $\dfrac{\mathbb{Q}[x]}{\ker\eta} \cong \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

$\pi \notin \mathbb{Q}$ $\mathbb{Q}[x] \simeq \mathbb{Q}[\pi]$

$\mathbb{Q}[\sqrt{2}]$ 是一个域 因为 x^2-2 在 $\mathbb{Q}[x]$ 中不可约.

定理 $\mathbb{F}[x]$ 上 n 次多项式 $f(x)$ 至多在 $\mathbb{F}$ 中有 n 个根 $(n>0)$

引理 若 $f(x) \in \mathbb{F}[x]$，$\deg f(x) > 0$，则 $\forall a \in \mathbb{F}$，$f(a)=0$

$\Longleftrightarrow (x-a) \mid f(x)$

证明：由带余除法 $f(x)=(x-a)q(x)+r(x)$

$\deg r(x)<\deg(x-a)=1$ 即 $r(x)=r\in\mathbb{F}$

$f(a)=0\Rightarrow r=f(a)=0\Rightarrow (x-a)\mid f(x)$

证明定理：关于 $f(x)$ 的次数归纳 $\deg f(x)=n$

$n=1$ $f(x)=ax+b$，$a\neq 0, b\in\mathbb{F}$ $f(x)=0\Rightarrow x=-\frac{b}{a}$

假设定理对于次数 $\leq d$ 的多项式成立.

当 $n=d+1$，若 $f(x)$ 在 $\mathbb{F}$ 中无根，则结论成立 $0\leq d+1$

否则，存在一个根 $a\in\mathbb{F}$，$f(a)=0$. 由引理，$f(x)=(x-a)g(x)$

$\deg g(x)=d$，使用归纳假设，$g(x)$ 在 $\mathbb{F}$ 中至多 d 个根.

若 $b\in\mathbb{F}$ $f(b)=0$ 则 $(b-a)g(b)=0\Rightarrow b=a$ 或 b 为 $g(x)=0$

在 $\mathbb{F}$ 中的根，因此 $f(x)=0$ 在 $\mathbb{F}$ 中至多 $d+1$ 个根.

注：对于一个群 G，$f(x)=e$ 在 G 中可能有 $>\deg f(x)$ 个根

例如 $x^2=e$ 在 S_3 中有3个根.

应用：

定理 任意域的乘法子群的有限子群是循环群.

证明：设 $\mathbb{F}$ 是一个域，$\mathbb{F}^*=\mathbb{F}\setminus\{0\}$ 是乘法群，$G\leq\mathbb{F}^*$，且

$|G|=n<\infty$ $\forall g\in G$，$g^n=e$，即 g 是 $x^n=1$ 的根，有

至少 n 个根，但 $x^n-1=0$ 在 $\mathbb{F}$ 中至多 n 个根，即 G 中元素是

它的全部根，设 $a\in G$ 有最大阶数 l_a，$l_a|n$，若 $b\notin\langle a\rangle$

b 的阶数为 l_b，则 $l_b\leq l_a$，~~因为 ab~~ 存在 c 的阶数为 $[l_a, l_b]$，

所以 $l_b|l_a$，即 G 中元素均满足 $x^{l_a}=1$，因此 $l_a=n$.

($x^{l_a}-1=0$ 只有 $\leq l_a$ 个根).

下面我们推广多项式到一般环上

R 是一个环，$x\notin R$ 不定元

$R[x]=\{f(x)=a_0+a_1x+\cdots+a_nx^n \mid a_i\in R, i=0,1,\cdots,n, n\geq 0\}$

$\deg f(x)=n$. 可以定义 $R[x]$ 上加法、乘法 $\Rightarrow R[x]$ R 上的多项式环　$R[x]$ 交换 $\Leftrightarrow R$ 交换，$R[x]$ 有幺元 $\Leftrightarrow R$ 有幺元.

定义　设 R 是 E 的子环，$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$

$\forall a\in E$，定义 $f(a)=a_0+a_1a+\cdots+a_na^n\in E$.

是 $f(x)$ 在 a 处取值，若 $f(a)=0$，则 a 是 $f(x)$ 的一个根（在 E 中）

注：一般地，若 $f_1(x), f_2(x)\in R[x]$　$\underset{\displaystyle f_1(x)\cdot f_2(x)}{\overset{f(x)}{\parallel}}$ 使用了 x 和 R 中元素交换，所以当代入 a，$f(a)$ 未必等于 $f_1(a)\cdot f_2(a)$

以下<u>假设 R 是含幺交换环</u>.

性质：(1) 若 R 是整区，则 $R[x]$ 是整区

证明：设 $f(x)=\sum_{i=0}^{n}a_ix^i$ $g(x)=\sum_{j=0}^{m}b_jx^j$ $a_i,b_j\in R$

$a_n,b_m\neq 0$, $m,n\geqslant 0$

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

R 整区 $\Rightarrow a_nb_m=c_{n+m}\neq 0 \Rightarrow f(x)g(x)\neq 0$

推论 R 整区，则 $R[x_1,x_2,\cdots,x_n]$ 均是整区.

(2) 设 R 为整区，则 $R[x]$ 中单位就是 R 中单位.

证明：设 $f(x)\in R[x]$，且存在 $g(x)\in R[x]$，$f(x)g(x)=1$

由(1)的证明，$f(x)=a_0$，$g(x)=b_0\in R$ $a_0b_0=1$

定理(带余除法) 设 R 为含幺环，$f(x),g(x)\in R[x]$，且 $g(x)$ 的首项系数是 R 中单位，则存在唯一 $q(x),r(x)\in R[x]$，使得 $f(x)=q(x)g(x)+r(x)$，且 $\deg r(x)<\deg g(x)$.

证明：(1) 存在性

设 $\deg g(x)>\deg f$ 则令 $q(x)=0$，$r(x)=f(x)$

设 $\deg g(x)\leq\deg f(x)$ 令 $f(x)=\sum_{i=0}^{n}a_ix^i$ $g(x)=\sum_{j=0}^{m}b_jx^j$

$m\leq n$，因为 b_m 是单位. 可对 $\deg f(x)=n$ 归纳

$n=0$, $m=0$ ✓

假设次数 $\leq n-1$ 的 f 有带余除法，当 $\deg f=n$.

$f(x)-a_nb_m^{-1}x^{n-m}g(x)=h(x)$ 是次数 $\leq n-1$ 的多项式

则存在 $q'(x), r(x)$ $\quad \deg r(x) < \deg g(x)$

$$h(x) = q'(x)g(x) + r(x)$$

$$\Rightarrow f(x) = \left(a_n b_m^{-1} x^{n-m} + q'(x)\right) g(x) + r(x)$$

(2) 唯一性

设 $f = q_1 g + r_1 = q_2 g + r_2$ $\quad \deg r_1, \deg r_2 < \deg g$

$\Rightarrow (q_1 - q_2) g = r_2 - r_1$ 比较次数，$q_1 - q_2 = 0 \Rightarrow r_1 - r_2 = 0$

注：定理"任意域的乘法子群的有限子群是循环群"证明也可以直接使用有限Abel群结构" 设 $\mathbb{F}$ 域，$\mathbb{F}^* = \mathbb{F}\setminus\{0\}$，$G \leq \mathbb{F}^\times$，则 $|G| < \infty$，则 G 是有限Abel群，设 $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ $\quad n = |G| = m_1 \cdots m_r$，$\mathbb{Z}_{m_1} = \langle a \rangle$，$\mathbb{Z}_{m_2} = \langle b \rangle$ 设 $l = [m_1, m_2]$，则 $\forall (x, y) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ 满足 $(x, y)^l = (0, 0) = e$，即 $x^l - e = 0$ 有至少 $m_1 m_2$ 个根，$l \geq m_1 m_2 \Rightarrow l = m_1 m_2$ 即 $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} = \mathbb{Z}_{m_1 m_2}$，由 m_i 的任意性，

$G \cong \mathbb{Z}_{m_1 \cdots m_r}$.

作业. Page110 $\quad$ 1, 4, 6, 8, 10, 11, 12.