0.1 多项式环

定理 0.1

设 $\widetilde{R}$ 是一个交换幺环,R 是 $\widetilde{R}$ 的子环且 $1 \in R$. 又设 $u \in \widetilde{R}$,$\widetilde{R}$ 中由 R 与 u 生成的子环, 即包含 R 与 u 的最小子环记为 $R[u]$. 则

$$R[u] = \{a_0 + a_1 u + \cdots + a_n u^n \mid a_i \in R, n \in \mathbf{N} \cup \{0\}\},$$

也称 $R[u]$ 为R **上添加** u **生成的子环**.

证明 记 $S = \{a_0 + a_1 u + \cdots + a_n u^n \mid a_i \in R,\ n \in \mathbf{N} \cup \{0\}\}$. 首先证明 $S \subseteq R[u]$. 由于 $R[u]$ 是包含 R 和 u 的子环, 而 S 中的所有元素都可以通过有限次运算 (加法、乘法、取逆) 从 R 和 u 得到, 因此 $S \subseteq R[u]$.

接下来证明 $R[u] \subseteq S$. 设 $f(u) = a_0 + a_1 u + \cdots + a_m u^m \in S$,$g(u) = b_0 + b_1 u + \cdots + b_n u^n \in S$, 不妨设 $m \leqslant n$, 再令 $a_{m+1} = \cdots = a_n = 0$, 则

$$f(u) + g(u) = \sum_{i=0}^{n} (a_i + b_i) u^i \in S.$$

令 $-f(u) \triangleq (-a_0) + (-a_1)u + \cdots + (-a_m)u^m \in S$, 则 $f(u) + (-f(u)) = 0$. 因此 S 对加法封闭且有加法逆元. 又 $\widetilde{R}$ 是交换幺环且 $S \subseteq \widetilde{R}$, 故 S 对加法满足结合律和交换律. 于是 S 对加法构成 R 的 Abel 群.

由于 $\widetilde{R}$ 是交换环, 故

$$f(u) g(u) = \left(\sum_{i=1}^{n} a_i u^i \right) \left(\sum_{i=1}^{n} b_i u^i \right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) u^k \in S.$$

令 $a_0 = 1, n = 0$, 则有 $1 \in S$. 因此 S 对乘法封闭且含幺元 1. 又 $\widetilde{R}$ 是交换幺环且 $S \subseteq \widetilde{R}$, 故 S 对乘法满足结合律. 于是 S 对乘法构成 R 的幺半群. 故 S 是交换幺环 $\widetilde{R}$ 的子环.

对于任意 $r \in R$, 可取 $r = r + 0 \cdot u + 0 \cdot u^2 + \cdots \in S$, 故 $R \subseteq S$. 同时 $u = 0 + 1 \cdot u + 0 \cdot u^2 + \cdots \in S$. 再设 T 是 $\widetilde{R}$ 的任一包含 R 和 u 的子环, 则 T 必然包含所有的 $a_i u^i$ $(a_i \in R)$ 以及它们的有限和, 即 $S \subseteq T$. 因此 S 是包含 R 和 u 的最小子环.

综上可知 $R[u] = S$.

□

定义 0.1

如果在 R 中存在有限多个元素 $a_0, a_1, \cdots, a_n$ 且 $a_n \neq 0$, 使得

$$a_0 + a_1 u + \cdots + a_n u^n = 0,$$

那么称 u 为 R 上的**代数元**, 使上述关系成立的最小正整数 n 称为代数元 u 的**次数**, 记为 $\deg(u, R)$.

例题 0.1 令 $\widetilde{R} = \mathbf{C}$, 则 $\sqrt{-1}$ 为 $\mathbf{Z}$ 上的代数元,

$$\mathbf{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} \mid m, n \in \mathbf{Z}\}$$

称为 **Gauss 的整数环**,$\deg(\sqrt{-1}, \mathbf{Z}) = 2$. 同样 $\sqrt{-1}$ 为 $\mathbf{Q}$ 上的代数元,$\deg(\sqrt{-1}, \mathbf{Q}) = 2$.

证明

□

例题 0.2 令 $\widetilde{R} = \mathbf{Q}$, 则 $\frac{1}{2}$ 是 $\mathbf{Z}$ 上代数元且 $\mathbf{Z} \subset \mathbf{Z}\left[\frac{1}{2}\right] \subset \mathbf{Q}$,$\deg\left(\frac{1}{2}, \mathbf{Z}\right) = 1$.

证明

□

定义 0.2

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环,$u \in \widetilde{R}$,$R[u]$ 为 R 添加 u 生成的 $\widetilde{R}$ 的子环, 若满足 $a_0, a_1, \cdots, a_n$ 不全为 0 时,

$$a_0 + a_1 u + \cdots + a_n u^n \neq 0,$$

则称 u 为 R 上的**超越元**或**不定元**.$R[u]$ 中的一个元素 $f(u) = a_0 + a_1 u + \cdots + a_n u^n$ 称为 u 的 (系数在 R 中的) 一个**多项式**. 若 $a_n \neq 0$, 则称 n 为 $f(u)$ 的次数, 记为 $\deg f(u)$.$R[u]$ 称为 R 上的一个**一元多项式环**. ♣

例题 0.3 设 $\mathbf{P}$ 是一个数域,x 是一个文字, 则 $\mathbf{P}[x]$ 是 $\mathbf{P}$ 上的一个一元多项式环,x 是 $\mathbf{P}$ 上的超越元.

证明

□

定理 0.2

交换幺环 R 上的一元多项式环一定存在. ♡

证明 令

$$\widetilde{R} = \{(a_0, a_1, \cdots) \mid a_i \in R \text{ 且仅有有限个} a_i \neq 0\}.$$

自然 $\widetilde{R}$ 中元素 $(a_0, a_1, \cdots) = (b_0, b_1, \cdots)$ 当且仅当 $a_i = b_i (i = 0, 1, \cdots)$. 在 $\widetilde{R}$ 中定义加法与乘法

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots), \tag{1}$$

$$(a_0, a_1, \cdots) \cdot (b_0, b_1, \cdots) = (c_0, c_1, \cdots). \tag{2}$$

其中,

$$\begin{aligned} c_n &= a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 \\ &= \sum_{i+j=n} a_i b_j, \quad n = 0, 1, \cdots. \end{aligned} \tag{3}$$

由于 $(a_0, a_1, \cdots), (b_0, b_1, \cdots) \in \widetilde{R}$, 故 $\exists m \in \mathbf{N}$, 使 $n > m$ 时,$a_n = b_n = 0$. 于是 $a_n + b_n = 0$, 故 $(a_0 + b_0, a_1 + b_1, \cdots) \in \widetilde{R}$. 而当 $n > 2m$ 时,$c_n = \sum\limits_{i+j=n} a_i b_j = 0$, 故 $(c_0, c_1, \cdots) \in \widetilde{R}$. 由此知上面定义的加法与乘法是良定义的.

容易验证 $\widetilde{R}$ 对加法为 Abel 群, 它的零元素为 $0 = (0, 0, \cdots)$ 且 $-(a_0, a_1, \cdots) = (-a_0, -a_1, \cdots)$. 同样容易验证 $\widetilde{R}$ 对乘法是可交换的且有幺元 $(1, 0, \cdots)$. 下面验证乘法的结合律. 设

$$f = (a_0, a_1, \cdots), \quad g = (b_0, b_1, \cdots), \quad h = (c_0, c_1, \cdots),$$

则 $(fg)h$ 的第 k 个元素为

$$\sum_{s+r=k} \left(\sum_{i+j=s} a_i b_j \right) c_r = \sum_{i+j+r=k} a_i b_j c_r = \sum_{i+t=k} a_i \left(\sum_{j+r=t} b_j c_r \right),$$

这也是 $f(gh)$ 的第 k 个元素. 故 $\widetilde{R}$ 对乘法为交换幺半群. 又注意到 $(f+g)h$ 的 k 个元素为

$$\sum_{i+j=k} (a_i + b_i) c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j,$$

这也是 $fh + gh$ 的第 k 个元素.$h(f+g)$ 的 k 个元素为

$$\sum_{i+j=k} c_i \left(a_j + b_j \right) = \sum_{i+j=k} c_i a_j + \sum_{i+j=k} c_i b_j,$$

这也是 $hf + hg$ 的第 k 个元素. 因此 $\widetilde{R}$ 中加法与乘法间的分配律成立, 故 $\widetilde{R}$ 为交换幺环.

令 $R_0 = \{(a_0, 0, 0, \cdots) : a_0 \in R\}$, 则 R_0 显然是 R 的子环. 由

$$(a_0, 0, \cdots) + (b_0, 0, \cdots) = (a_0 + b_0, 0, \cdots),$$

$$(a_0, 0, \cdots) \cdot (b_0, 0, \cdots) = (a_0 b_0, 0, \cdots)$$

知 $a_0 \to (a_0, 0, \cdots)$ 是 R 到 R_0 上的同构映射. 为方便计, 将 R_0 中元素 $(a_0, 0, \cdots)$ 记为 a_0, 即可将 R 视为 $\widetilde{R}$ 的子环. R 的幺元 1 恰为 $\widetilde{R}$ 的幺元 $(1, 0, \cdots)$.

最后证明 $\widetilde{R}$ 是 R 上的一元多项式环. 令

$$u = (0, 1, 0, \cdots),$$

则不难验证

$$u^k = (\underbrace{0, \cdots, 0}_{k}, 1, 0, \cdots),$$

$$a_k u^k = (\underbrace{0, \cdots, 0}_{k}, a_k, 0, \cdots), \quad a_k \in R = R_0.$$

若 $f = (a_0, a_1, \cdots) \in \widetilde{R}$, 则有 n, 使 $a_{n+1} = a_{n+2} = \cdots = 0$. 于是

$$f = a_0 + a_1 u + \cdots + a_n u^n,$$

因而有 $\widetilde{R} = R_0[u] = R[u]$. 又若

$$a_0 + a_1 u + \cdots + a_n u^n = 0,$$

即

$$(a_0, a_1, \cdots, a_n, 0, \cdots) = (0, 0, \cdots),$$

则 $a_0 = a_1 = \cdots = a_n = 0$, 即 u 是 R 上的超越元, 因而 $\widetilde{R} = R[u]$ 是 R 上的一元多项式环.

□

定理 0.3

设 R, S 都是交换幺环, 它们的幺元分别是 $1, 1'$. 又若 η 是 R 到 S 的同态且 $\eta(1) = 1'$, 则 $\forall u \in S$,η 可唯一地扩充为 R 上的一元多项式环 $R[x]$ 到 S 的同态 η_u, 使得

$$\eta_u(x) = u.$$

即对 $\forall u \in S$,η 存在唯一的在 R 上的开拓 $\eta_u : R[x] \to S$ 满足

$$\eta_u|_R = \eta, \quad \eta_u(x) = u. \tag{4}$$

证明 因 $R[x]$ 为 R 上的一元多项式环, 故 $R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}$. 定义 η_u,

$$\eta_u(a_0 + a_1 x + \cdots + a_n x^n) = \eta(a_0) + \eta(a_1) u + \cdots + \eta(a_n) u^n \tag{5}$$

于是 η_u 是 $R[x]$ 到 S 的映射. 直接计算可知 η_u 为满足式(4)的扩充, 并为同态映射.

现设 η' 也是 η 的扩充且 $\eta'(x) = u$, 于是

$$\eta' \left(\sum_{i=0}^{n} a_i x^i \right) = \sum_{i=0}^{n} \eta'(a_i) u^i = \sum_{i=0}^{n} \eta(a_i) u^i = \eta_u \left(\sum_{i=0}^{n} a_i x^i \right),$$

故 $\eta' = \eta_u$, 即 η_u 是满足条件的唯一扩充.

□

推论 0.1

设 R 是交换幺环,$R[x]$ 与 $R[y]$ 都是 R 上的一元多项式环, 则 $R[x]$ 与 $R[y]$ 是同构的.

笔记 这个推论说明: 任何交换幺环上的一元多项式环在同构意义下唯一.

证明 事实上, 容易验证 R 到 $R[y]$ 的嵌入映射 $i(a) = a(\forall a \in R)$ 是 R 到 $R[y]$ 的环同态, 于是由定理 0.3知有 $R[x]$ 到 $R[y]$ 的同态 i_y 满足

$$i_y|_R = i, \quad i_y(x) = y.$$

从而任取 $a_0+a_1y+\cdots+a_ny^n\in R[y]$, 都有

$$i_y(a_0+a_1x+\cdots+a_nx^n)=a_0+a_1y+\cdots+a_ny^n,$$

故 i_y 是满同态. 由 y 是 R 上超越元知 $\ker i_y=\{0\}$, 因此由命题**??**知 i_y 是单同态. 故 i_y 是同构映射.

□

推论 0.2

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环,$R[x]$ 为 R 上的一元多项式环, 又设 $u\in\widetilde{R}$, 则有 $R[x]$ 中的理想 I 满足 $R\cap I=\{0\}$,$R[u]\cong R[x]/I$, 并且当且仅当 $I\neq\{0\}$ 时,u 为代数元.

证明 考虑 R 到 $R[u]$ 的嵌入映射 i, 则不难验证 i 是 R 到 $R[u]$ 上的同态. 于是由定理 0.3知可将 i 扩充为环同态 $i_u:R[x]\to R[u]$ 满足

$$i_u|_R=i,\quad i_u(x)=u.$$

注意到 $i_u(R[x])=R[u]$, 故 i_u 是满同态. 于是由环的同态基本定理知 $I=\ker i_u$ 为 $R[x]$ 中理想,$R[u]\cong R[x]/I$. 又若 $a\in R\cap I$, 则 $0=i_u(a)=i(a)=a$, 故 $R\cap I=\{0\}$. 由于 u 为 R 上代数元当且仅当存在 $a_n\neq 0$, 使得 $\sum\limits_{i=0}^{n}a_iu^i=0$. 这也当且仅当

$$i_u\left(\sum_{i=0}^{n}a_ix^i\right)=\sum_{i=0}^{n}a_iu^i=0\iff 0\neq\sum_{i=0}^{n}a_ix^i\in I\iff I\neq\{0\}.$$

□

推论 0.3

设 R 是交换幺环,$R[x]$ 是 R 上一元多项式环. 又若 I 是 $R[x]$ 的理想且 $R\cap I=\{0\}$,$I\neq\{0\}$, 则 $\widetilde{R}=R[x]/I$ 是 R 添加一个代数元所得的环.

证明 设 π 是 $R[x]$ 到 $R[x]/I$ 的自然同态, 于是 $\pi(R)$ 是 $\widetilde{R}$ 中的子环. 由定理**????**知

$$\pi(R)=R/I=(R+I)/I\cong R/(R\bigcap I)=R/\{0\}=R+0=R,$$

故可将 R 视为 $\widetilde{R}$ 的子环, 令 $u=\pi(x)$, 于是

$$\pi(a_0+a_1x+\cdots+a_nx^n)=\pi(a_0)+\pi(a_1)u+\cdots+\pi(a_n)u^n,$$

故 $\widetilde{R}=\pi(R[x])\subseteq R[u]\subseteq\widetilde{R}$, 即 $\widetilde{R}=R[u]$. 又由 $I\neq\{0\}$, 故 I 中有非零元素 $a_0+a_1x+\cdots+a_nx^n$, 其中 $a_n\neq 0$, 又因为 $\pi(R)\cong R$, 所以 $\pi(a_n)\neq 0$. 而

$$\pi(a_0+a_1x+\cdots+a_nx^n)=\pi(a_0)+\pi(a_1)u+\cdots+\pi(a_n)u^n=0,$$

故 u 为 R 上的代数元.

□