多项式环

定义 1 (生成的子环)**.** 设 $\tilde{R}$ 是交换幺环，$R < \tilde{R}$ 且 $1 \in R$. 设 $u \in \tilde{R}$，称包含 R 与 u 的最小子环为 R 与 u **生成的子环**，记作 $R[u]$，则对任意 $n \in \mathbb{N}$，有

$$R[u] = \{a_0 + a_1 u + \cdots + a_n u_n \mid a_i \in R\},$$

也称 $R[u]$ 为 R 上添加 u **生成的子环**.

定义 2 (代数元)**.** 如果 R 中存在有限多个元素 $a_0, a_1, \cdots, a_n$ 且 $a_n \neq 0$ 使得

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

则称 u 是 R 上的**代数元**. 称满足上述条件的最小的 n 为代数元的**次数**，记作 $\deg(u, R)$.

定义 3 (超越元)**.** 若对任意 $a_0, a_1, \cdots, a_n \in R$，$a_0 + a_1 u + \cdots + a_n u^n = 0$ 当且仅当 $a_0, a_1, \cdots, a_n$ 全为零，则称 u 是 R 上的**超越元**或**不定元**.

注. *不是代数元的元素就是超越元.*

定义 4 (一元多项式环)**.** 当 u 是交换幺环 R 上的超越元时，称 $R[u]$ 为**一元多项式环**，$R[u]$ 中的元素称为**一元多项式**.

定义 5. 设多项式 $f(u) = a_0 + a_1 u + \cdots + a_n u^n \in R[u]$，若 $a_n \neq 0$，则称 n 为 $f(u)$ 的**次数**，记作 $\deg f(u)$. 称 $a_i x^i$ 为 $f(x)$ 的第 i 项，a_i 称为第 i 项的**系数**，a_0 称为**常数项**，$a_n x^n$ 称为**首项**.

注. *规定非零元 $a_0 \in R$ 作为多项式的次数为 0，零元 0 的次数为 $-\infty$.*

性质 1. $\deg f(x) = 0 \iff f(x) \in R^*$.

性质 2. $\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$.

定义 6 (首一多项式)**.** 首项系数为 1 的非零多项式称为**首一多项式**.

性质 3. 首一多项式的乘积仍为首一多项式.

定理 1. 交换幺环上的一元多项式环存在.

证明. 令 $\tilde{R} = \{(a_0, a_1, \cdots) \mid a_i \in R\text{且仅有有限个}a_i \neq 0\}$. 定义加法与乘法如下.

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots),$$

$$(a_0, a_1, \cdots) \cdot (b_0, b_1, \cdots) = (c_0, c_1, \cdots),$$

其中，

$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 = \sum_{i+j=n} a_i b_j.$$

由于 $(a_1, a_2, \cdots), (b_1, b_2, \cdots) \in \tilde{R}$，于是存在 m，当 $n > m$ 时，$a_n = b_n = 0$. 于是 $a_n + b_n = 0$，$n > 2m$ 时，$c_n = \sum\limits_{i+j=n} a_i b_j = 0$. 于是上述加法与乘法是良定义的.

可以证明 $\tilde{R}$ 对加法作成 Abel 群，零元为 $(0, 0, \cdots)$，$-(a_1, a_2, \cdots) = (-a_1, -a_2, \cdots)$.

$\tilde{R}$ 对乘法可换且幺元为 $(1, 0, 0, \cdots)$. 对任意 $f = (a_0, a_1, \cdots)$，$g = (b_0, b_1, \cdots)$，$h = (c_0, c_1, \cdots)$，$(fg)h$ 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，于是 $\tilde{R}$ 对乘法是结合的，故 $\tilde{R}$ 为乘法幺半群.

而 $(a_n + b_n)c_n = a_n c_n + b_n c_n$，于是分配律满足，$\tilde{R}$ 是交换幺环.

令 $R_0 = (a_0, 0, 0, \cdots)$，其中 $a_0 \in R$. 可以验证 $\varphi : R_0 \to R, (a_0, 0, \cdots) \mapsto a_0$ 是同构，于是可将 R 看作 $\tilde{R}$ 的子环，且幺元就是 $\tilde{R}$ 的幺元.

令 $u = (0, 1, 0, \cdots)$，则有

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

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

若 $f = (a_0, a_1, \cdots) \in \tilde{R}$，则存在 n 使得 $a_{n+1} = a_{n+2} = \cdots = 0$，于是

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

故 $\tilde{R} = R_0\,[u] = R\,[u]$. 若

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

则 $(a_0, a_1, \cdots, a_n, 0, \cdots) = (0, \cdots, 0)$，于是 $a_0 = a_1 = \cdots = a_n = 0$. 于是 u 是 R 上的超越元，故 $\tilde{R} = R\,[u]$ 是 R 上的一元多项式环. □

定理 2. 设 R 和 S 都是交换幺环，幺元分别为 $1, 1'$，η 是 R 到 S 的同态且 $\eta(1) = 1'$，则对任意 $u \in S$，η 可唯一扩充为 $R\,[x]$ 到 S 的同态 η_u 使得 $\eta_u(x) = u$.

证明. $R\,[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}$，定义 η_u:

$$\eta_u(a_0 + a_1 x + \cdots + a_n x^n) = \eta(a_0) + \eta(a_1) u + \cdots + \eta(a_n) u^n.$$

映射 η_u 是良定义的，$\eta_u(x)=\eta(1x)=1'u=u$，且 η_u 是同态映射.

若 η' 也是 η 的扩充且 $\eta'(x)=u$，于是

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

故 $\eta'=\eta_u$，即扩充是唯一的. □

推论 1. 设 R 是交换幺环，$R[x]$ 和 $R[y]$ 都是 R 上的一元多项式环，则 $R[x]$ 与 $R[y]$ 同构.

证明. 作 R 到 $R[y]$ 的嵌入映射 i，则 i 是同态. 由定理2，i 可唯一扩充为 i_y，使得

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

于是 i_y 是满同态，又 y 是 R 上超越元，于是 i_y 又是单同态，故 i_y 是同构. □

推论 2. 设 $\tilde{R}$ 是交换幺环，R 是 $\tilde{R}$ 的子环且 $1\in R$，$R[x]$ 是 R 上一元多项式环，设 $u\in\tilde{R}$，则存在 $R[x]$ 中的理想 I 满足

$$R\cap I=\{0\},\qquad R[u]\cong R[x]/I,$$

而且，当且仅当 $I\neq\{0\}$ 时，u 是代数元.

证明. 考虑 R 到 $\tilde{R}$ 的嵌入映射 i，则 i 是同态. 由定理2，i 可以唯一扩充为 i_u，满足 $i_u(R[x])=R[u]$. 记 $I=\ker i_u$，则 I 是 $R[x]$ 的理想，由同态基本定理，有

$$R[u]\cong R[x]/I.$$

对任意 $a\in R\cap I$，

$$a=i(a)=i_u(a)=0,$$

于是 $R\cap I=\{0\}$. 考虑不全为零的 $a_0,a_1,\cdots,a_n$，有

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

于是 $I\neq\{0\}$ 当且仅当 u 为代数元. □

推论 3. 设 R 是交换幺环，$R[x]$ 是 R 上一元多项式环，若 I 是 $R[x]$ 的理想，$R\cap I=\{0\}$ 且 $I\neq\{0\}$，则 $R[x]/I$ 是 R 添加一个代数元所得的环.

证明. 记 $\pi:R[x]\to R[x]/I$ 为自然同态，则 $\pi\big|_R:R\to\pi(R)$ 是满同态，而

$$\ker\pi\big|_R=I\cap R=\{0\},$$

于是 π 是单同态. 故 π 是同构. 于是 $R \cong \pi(R)$.

令 $u = \pi(x)$. 因为 $I \neq \{0\}$，于是存在不全为 0 的 $a_0, a_1, \cdots, a_n$ 使得

$$0 \neq \sum_{i=0}^{n} a_i x^n \in I,$$

而

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

同时 $\pi(a_0), \pi(a_1), \cdots, \pi(a_n)$ 不全为零，于是 u 是 R 上的代数元.

而

$$R[x]/I = \pi(R[x]) = \pi(R)[\pi(x)] = \pi(R)[u] \cong R[x],$$

正是 R 上添加 u 所得的环. □

多元多项式是一元多项式的推广.

定义 7 (生成的子环)**.** 设 $\tilde{R}$ 是交换幺环，$R < \tilde{R}$ 且 $1 \in R$. 设 $u_1, u_2, \cdots, u_n \in \tilde{R}$，称包含 R 与 $u_1, u_2, \cdots, u_n$ 的最小子环

$$R[u_1, u_2, \cdots, u_n] = \left\{ \sum a_{k_1 k_2 \cdots k_n} u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} \;\middle|\; a_{k_1 k_2 \cdots k_n} \in R \right\}$$

为 R 上添加 $u_1, u_2, \cdots, u_n$ **生成的子环**.(其中 $a_{k_1 k_2 \cdots k_n}$ 仅有有限个不为 0)

定义 8 (代数相关, 代数无关)**.** 如果 R 中存在有限多个 $a_{k_1 k_2 \cdots k_n} \neq 0$ 使

$$\sum a_{k_1 k_2 \cdots k_n} u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} = 0,$$

则称 $u_1, u_2, \cdots, u_n$ 在 R 上是**代数相关**的，否则称 $u_1, u_2, \cdots, u_n$ 在 R 上是**代数无关**的.

定义 9 (n 元多项式环)**.** 若 $u_1, u_2, \cdots, u_n$ 在 R 上是代数无关的，则称 $R[u_1, u_2, \cdots, u_n]$ 是 R 上的 $\boldsymbol{n}$ **元多项式环**，$R[u_1, u_2, \cdots, u_n]$ 中的元素称为 $\boldsymbol{n}$ **元多项式**.

定义 10. 多项式环 $R[u_1, u_2, \cdots, u_n]$ 中，形如 $a x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} (a \in R, a \neq 0)$ 的元素称为**单项式**，a 称为单项式的**系数**，$k_1 + k_2 + \cdots + k_n$ 称为该单项式的**次数**，称多项式中所含单项式的最高次数为多项式的**次数**. 特别的，非零常数项的次数为 0，规定 0 的次数为 $-\infty$.

定理 3. 交换幺环 R 上的 n 元多项式环一定存在.

证明. 对 n 用数学归纳法. 现已证 $n = 1$ 时命题成立，假设 $n - 1$ 时命题成立，则存在 $R[x_1, x_2, \cdots, x_{n-1}]$ 为多项式环，且为交换幺环. 那么交换幺环 $R[x_1, x_2, \cdots, x_{n-1}]$ 上的一元多项式环也存在，即 $R[x_1, x_2, \cdots, x_{n-1}][x_n]$ 存在. 由于 $R[x_1, x_2, \cdots, x_n]$ 是包含 R 与 $x_1, x_2, \cdots, x_n$ 的最小的环，于是有

$$1 \in R \subset R[x_1, x_2, \cdots, x_n] \subset R[x_1, x_2, \cdots, x_{n-1}][x_n].$$

对任意 $f \in R[x_1, x_2, \cdots, x_{n-1}][x_n]$，存在 $f_0, f_1, \cdots, f_k$ 使得

$$f = f_0 + f_1 x_n + \cdots + f_k x_n^k,$$

于是 $R[x_1, x_2, \cdots, x_{n-1}][x_n] \subset R[x_1, x_2, \cdots, x_n]$，故

$$R[x_1, x_2, \cdots, x_n] = R[x_1, x_2, \cdots, x_{n-1}][x_n].$$

已知 $x_1, x_2, \cdots, x_{n-1}$ 代数无关，下证 $x_1, x_2, \cdots, x_n$ 代数无关. 设

$$\sum a_{k_1 k_2 \cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} = 0,$$

即证 $a_{k_1 k_2 \cdots k_n} = 0$. 令

$$f_i = \sum a_{k_1 k_2 \cdots k_{n-1} i} x_1^{k_1} x_2^{k_2} \cdots x_{n-1}^{k_{n-1}},$$

则 $f_i \in R[x_1, x_2, \cdots x_{n-1}]$ 且 $\sum\limits_i f_i x_n^i = 0$. 由于 x_n 是 $R[x_1, x_2, \cdots x_{n-1}]$ 上的超越元，于是 $f_i = 0$，故 $a_{k_1 k_2 \cdots k_{n-1} i} = 0$. □

定理 4. 设 R 和 S 都是交换幺环，幺元分别为 $1, 1'$，η 是 R 到 S 的同态且 $\eta(1) = 1'$，则对任意 $u_1, u_2, \cdots, u_n \in S$，$\eta$ 可唯一扩充为 $R[x_1, x_2, \cdots, x_n]$ 到 S 的同态 η_u 使得 $\eta_u(x_i) = u_i$，$i = 1, 2, \cdots, n$.

推论 4. 交换幺环上任意两个 n 元多项式同构.

推论 5. 设 $\tilde{R}$ 是交换幺环，R 是 $\tilde{R}$ 的子环且 $1 \in R$，$R[x_1, x_2, \cdots, x_n]$ 是 R 上 n 元多项式环，设 $u_1, u_2, \cdots, u_n \in \tilde{R}$，则存在 $R[x_1, x_2, \cdots, x_n]$ 中的理想 I 满足

$$R \cap I = \{0\}, \qquad R[u_1, u_2, \cdots, u_n] \cong R[x_1, x_2, \cdots, x_n]/I,$$

而且，当且仅当 $I \neq \{0\}$ 时，$u_1, u_2, \cdots, u_n$ 是代数相关的.

推论 6. 设 R 是交换幺环，$R[x_1, x_2, \cdots, x_n]$ 是 R 上 n 元多项式环，若 I 是 $R[x_1, x_2, \cdots, x_n]$ 的理想，$R \cap I = \{0\}$ 且 $I \neq \{0\}$，则 $R[x_1, x_2, \cdots, x_n]/I$ 是 R 添加 n 个代数相关元所得的环.