域上一元多项式环

域是特殊的整环. 整环中无零因子，对多项式 $f(x),g(x)$，有以下性质.

性质 1. $f(x)\cdot g(x)\neq 0 \iff f(x)\neq 0, g(x)\neq 0$.

性质 2. $\deg(f(x)g(x))=\deg f(x)+\deg g(x)$.

性质 3. 若 R 是整环，则 $R[x]$ 也是整环，且二者的单位相同.

证明. 对前者，证明 $R[x]$ 是无零因子的交换幺环即可，交换是因为 R 是交换的，又含有幺元 1，假设存在零因子 $f(x)$，则对非零多项式 $g(x)$，有 $f(x),g(x)\neq 0$，推出 $f(x)\cdot g(x)\neq 0$，这与 $f(x)$ 是零因子矛盾.

对后者，R 的单位是 $R[x]$ 的单位是显然的，因为 $R\subset R[x]$. 反之，设 $f(x),g(x)\in R^*[x]$ 满足 $f(x)g(x)=1$，则

$$\deg(f(x)g(x))=\deg f(x)+\deg g(x)=\deg 1=0,$$

于是 $\deg f(x)=\deg g(x)=0$，$f(x),g(x)\in R^*$. □

注. 可以推广到 n 元多项式环.

定理 1. 设 $F[x]$ 是域 F 上的一元多项式环，则对任意 $f(x),g(x)\in F[x]$，$g(x)\neq 0$，存在唯一的 $q(x),r(x)\in F[x]$ 使得

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

证明. 首先证明 $q(x),r(x)$ 的存在性. 设 $\deg g(x)=m$，由于 $\deg g(x)\neq 0$，故 $m\geqslant 0$. 当 $\deg f(x)<m$ 时可取 $q(x)=0$，$r(x)=f(x)$. 对 $f(x)$ 的次数作归纳，设 $\deg f(x)<n$ 时，$q(x)$ 与 $r(x)$ 已存在.

当 $\deg f(x)=n$ 时，不妨设 $n\geqslant m$. 设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0,$$

由于 $\deg g(x)=m$，于是 $b_m\neq 0$. 取 $q_0(x)=a_nb_m^{-1}x^{n-m}$，令

$$f_1(x)=f(x)-q_0(x)g(x)=(a_{n-1}-a_nb_m^{-1}b_{m-1})x^{n-1}+\cdots,$$

故 $\deg f_1\leqslant n-1<n$. 由归纳假设，存在 $q_1(x),r_1(x)$ 使得

$$f_1(x)=q_1(x)g(x)+r_1(x),$$

于是

$$f(x)=q_0g(x)+q_1g(x)+r_1(x)=(q_0(x)+q_1(x))g(x)+r_1(x).$$

于是 $q(x)=(q_0(x)+q_1(x))$，$r(x)=r_1(x)$.

然后证明 $q(x),r(x)$ 的唯一性. 假设另有 $q'(x),r'(x)$ 使得

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

则

$$(q(x)-q'(x))g(x)=r'(x)-r(x),$$

若 $q(x)-q'(x)\neq 0$，则

$$\deg(q(x)-q'(x))g(x)=\deg(q(x)-q'(x))+\deg g(x)=\deg(r'(x)-r(x)).$$

而

$$\deg(r'(x)-r(x))=\max\{\deg r(x),\deg r'(x)\}<\deg g(x),$$

导出矛盾，于是 $q'(x)=q(x)$，$r'(x)=r(x)$. □

注. 分别称 $q(x),r(x)$ 为 $f(x)$ 除以 $g(x)$ 的**商式**和**余式**. 若 $f_1(x)$ 与 $f_2(x)$ 除以 $g(x)$ 的余式相同，则称 $f_1(x)$ 与 $f_2(x)$ **同余**，记作 $f_1(x)\equiv f_2(x) \pmod{g(x)}$.

推论 1. 域上一元多项式环是 Euclid 环.

证明. 令 $\delta(f(x))=2^{\deg f(x)}$，则

$$\delta(r(x))<\delta(g(x)),$$

于是 $F[x]$ 为 Euclid 环. □

推论 2. 设 $F[x]$ 是域 F 上一元多项式环，$f_1(x),f_2(x),g(x)\in F[x]$ 且 $g(x)\neq 0$，则

$$f_1(x)\equiv f_2(x)\pmod{g(x)} \iff g(x)\mid(f_1(x)-f_2(x)).$$

而且 $f_1(x)\equiv f_2(x) \pmod{g(x)}$ 对 $F[x]$ 的加法和乘法都是同余关系.

推论 3. 设 $F[x]$ 是域 F 上一元多项式环，$f(x)\in F[x]$，$c\in F$，则

$$f(x)\equiv f(c)\pmod{(x-c)}$$

且 $(x-c)\mid f(x)\iff f(c)=0$.

证明. 恒等映射 id_F 可以开拓为同态 $\eta: F[x] \to F$，使得 $\eta(x) = c$. 又因为 $\deg(x-c) = 1$，故存在 $q(x) \in F[x]$，$r \in F$ 使得

$$f(x) = q(x)(x-c) + r.$$

两边以 η 作用，得

$$f(c) = q(c)(c-c) + r = r.$$

于是

$$f(x) - f(c) = f(x) - r = q(x)(x-c),$$

得 $(x-c) \mid (f(x) - f(c))$，故

$$f(x) \equiv f(c) \pmod{(x-c)}.$$

特别地，$(x-c) \mid f(x) \iff f(x) \equiv 0 \pmod{(x-c)} \iff f(c) = 0$. □

定义 1 (根)**.** 设 $F[x]$ 是域 F 上一元多项式环，$c \in F$ 且使 $f(c) = 0$，则称 c 是 $f(x)$ 的一个**根**.

注. 由 $(x-c) \mid f(x) \iff f(c) = 0$ 可以看出，多项式的根与一次因式的关系是十分密切的.

推论 4. 若 $c_1, c_2, \cdots, c_k$ 是 $f(x)$ 的互不相同的根，则有 $\prod\limits_{i=1}^{k}(x-c_i) \mid f(x)$，从而 $k \leqslant \deg f(x)$.

证明. 因为 $x - c_i$ 的因子只能是 1 次的和 0 次的，而 0 次的因子即 F 中元素，为单位. 那么 $x - c_i$ 的一次因子不是真因子，所以 $x - c_i$ 是不可约元素. 对任意 $c_i \neq c_j$，有

$$\frac{1}{c_i - c_j}(x - c_j) - \frac{1}{c_i - c_j}(x - c_i) = 1,$$

则 $(x - c_i, x - c_j) = 1$.

对任意 c_i，$f(c_i) = 0$，于是 $(x - c_i) \mid f(x)$，又对任意 $c_i \neq c_j$ 有 $(x - c_i, x - c_j) = 1$，于是 $\prod\limits_{i=1}^{k}(x-c_i) \mid f(x)$，从而 $k \leqslant \deg f(x)$. □

推论 5. 设 S 是整环，R 是 S 的子环且 $1 \in R$，则 $f(x) \in R[x]$ 在 S 中不同根的个数不超过 $\deg f(x)$.

证明. 设 F 为 S 的分式域，则 $R[x] \subset S[x] \subset F[x]$，即 $f(x) \in F[x]$，由推论4可得. □

定理 2. 设 F 是域，G 是 $F^* = F \backslash \{0\}$ 的一个有限的乘法子群，则 G 为循环群.

证明. $|G|$ 有限，取 G 中阶最大的元素 g，设其阶为 m，则 $\langle g\rangle = \{1, g, g^2, \cdots, g^{m-1}\}$. 下证 $G = \langle g\rangle$.

一方面，G 是群，对运算封闭，于是 $\langle g\rangle \subset G$. 下证 $G \subset \langle g\rangle$.

对任意 $h \in G$，去证 h 是 $x^m - 1$ 的根，从而 $|G| \leqslant \deg(x^m - 1) = m$，而 $|\langle g\rangle| = m$，于是 $G \subset \langle g\rangle$ 即完成证明.

要证 h 是 $x^m - 1$ 的根，即证 $h^m - 1 = 0$，$h^m = 1$. 记 $|h| = m_1$，证明 $m_1 \mid m$ 即可.

反设 $m_1 \mid m$，则必有素数 p 满足 $m_1 = p^s l$，$m = p^r k$，其中 $(p, lk) = 1$，使 $s > r$. 由 $(p^s, l) = 1$，有 $|h^l| = p^s$，同理有 $|g^{p^r}| = k$，而 G 是 Abel 群，有

$$h^l \cdot g^{p^r} = g^{p^r} \cdot h^l,$$

且 $(p^s, k) = 1$，于是

$$|h^l \cdot g^{p^r}| = p^s k > p^r k = m,$$

这与 m 阶元素 g 是阶最大的元素矛盾. 故 $m_1 \mid m$. □

注. 这个定理的证明很有技巧性，值得进一步探究学习.

推论 6. 有限域 F 的非零元素集 F^* 对乘法作成循环群.