多项式环是数学中重要的研究对象之一

在高等代数中，我们讨论了数域上多项式的性质，

本节我们不仅将数域上多项式的概念推广到环上，

而且推广了数域上多项式的带余除法，

假定本节涉及的环都是有 1 的非零交换环，

若$\overline{R}$是 R 的扩环，则假定$\overline{R}$与 R 有相同的单位元，

定义 8.1 设 R 是环$\overline{R}$的子环，

若存在属于$\overline{R}$的 x，使得对属于 N 的任意的 n 及属于 R 的 $a_0, a_1, \cdots, a_n$，

当 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0$ 时，必有 $a_0=a_1=\cdots=a_n=0$，

则称 x 是环 R 的未定元，

我们知道，Z[i]是 Z 的扩环，

但对属于 Z[i]任意$\alpha=a+bi$，有$\alpha^2+(-2a)\alpha+(a^2+b^2)=0$，

即 Z[i]的任意元素都不是 Z 的未定元，

那么，在有 1 的交换环上是否有未定元呢?

定理 8.1 若 R 是环，

则存在 R 的某个扩环$\overline{R}$及属于$\overline{R}$的 x，使得 x 是环 R 的未定元

证: 我们采用构造的方法来证明本定理，

(1)构造有单位元的交换环$\overline{R}$，

为此令$\overline{R}=\{(a_0, a_1, \cdots, a_n, \cdots) | a_i \in R, i=0, 1, \cdots\}$其中只有有限个 a_i 不为 0，

并且在$\overline{R}$中规定:

$(a_0, a_1, \cdots, a_n, \cdots)=(b_0, b_1, \cdots, b_n, \cdots) \Leftrightarrow a_i=b_i, i=0, 1, \cdots, n, \cdots$

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

$(a_0, a_1, \cdots, a_n, \cdots)\bullet(b_0, b_1, \cdots, b_n, \cdots)=(c_0, c_1, \cdots, c_n, \cdots)$，

其中 $c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0, k=0, 1, \cdots, n, \cdots$

则容易验证，$\{R;+, \bullet\}$是有单位元的交换环，而且单位元为$(1, 0, 0, \cdots, 0, \cdots)$

(2)$\overline{R}$是 R 的扩环，

事实上，若令φ: $R\to\overline{R}$，$a\to(a, 0, 0, \cdots, 0, \cdots)$，则易知$\varphi$是 R 到$\overline{R}$的单同态，

从而，我们可以视$\overline{R}$是 R 的扩环，

当然，我们可以把 R 中的元素 a 等同于$\overline{R}$中的元素$(a, 0, 0, \cdots, 0, \cdots)$，

因此，$\overline{R}$与 R 有相同的单位元，

(3)$\overline{R}$中的元素$(0, 1, 0, \cdots, 0, \cdots)$是环 R 的未定元，

事实上，若令 $x=(0, 1, 0, \cdots, 0, \cdots)$，则 $x^k=(\overbrace{0, \cdots, 0}^{k\text{个}}, 1, 0, \cdots, 0, \cdots)$

$a_kx^k=(a_k, 0, \cdots, 0, \cdots)(0, \cdots, 0, 1, 0, \cdots, 0, \cdots)=(\overbrace{0, \cdots, 0}^{k\text{个}}, a_k, 0, \cdots, 0, \cdots)$，

因此，$a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n=(a_1, a_2, \cdots, a_n, 0, \cdots)$，

那么若 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0$，则$(a_1, a_2, \cdots, a_n, 0, \cdots)=0$，

从而 $a_0=a_1=\cdots=a_n=0$，即 x 是 R 的未定元，

定理 8.2 设 R 是环，$\overline{R}$是 R 的扩环，

若属于$\overline{R}$的 x 是 R 的未定元，

则 $R[x]=\{a_0+a_1x+\cdots+a_nx^n|a_0, a_1, \cdots, a_n \in R, n \in N\}$

是包含 R 和 x 的环$\overline{R}$的最小子环，

证: 由子环的判定定理可知，R[x]是$\overline{R}$的子环，

事实上，令 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$ 属于 R[x]

不妨设 $n \leqslant m$

(若 $n<m$，根据 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0 \bullet x^{n+1}+a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$

可设 $a_m=a_{m-1}=\cdots=a_{n+1}=0$)，

则 $f(x)-g(x)=(a_m-b_m)x^m+(a_{m-1}-b_{m-1})x^{m-1}+\cdots+(a_1-b_1)x+a_0-b_0$ 属于 R[x]，

$f(x)g(x)=c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\cdots+c_1x+c_0$ 属于 R[x]，

其中 $c_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0$, $k=0, 1, \cdots, m+n$，

因此，R[x]是$\overline{R}$的子环，

如果存在$\overline{R}$的子环 R_0 使关系 $R \subseteq R_0$ 成立，其中 x 属于 R_0，则有 R[x]包含于 R_0，

即 R[x]是包含 R 和 x 的环$\overline{R}$的最小子环，

由定理 8.1，我们知道，环 R 一定有未定元 x，

那么，若 R 还有另外一个未定元 y，则环 R[x]与 R[y]又有什么关系呢?

命题 8.1 设 x, y 是 R 的两个未定元，则环 R[x]与 R[y]同构，

证: 只需证明映射$\varphi: R[x] \to R[y]$, $\sum_{i=1}^{n} a_ix^i \to \sum_{i=1}^{n} a_iy^i$ 是环同构即可

命题 8.1 说明，环 R[x]与未定元的选取无关，

因此，我们在谈论多项式环时，不需要强调未定元所在的环，

定义 8.2 若 x 是环 R 的未定元，

则称 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，是 R 上(关于未定元 x)的一元多项式，

其中 n 属于 N，a_i 属于 R，$i=0,1,\cdots,n$，

称 $R[x]=\{a_0+a_1x+\cdots+a_nx^n|a_0,a_1,\cdots,a_n\in R,n\in N\}$是环 R 上的一元多项式环，

一般地，我们用符号 $f(x),g(x),\cdots$表示 R 上(关于未定元 x)的一元多项式，

若 $f(x)$属于 $R[x]$，若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，

则称 a_ix^i 是 $f(x)$的 i 次项，并称 a_i 是 i 次项的系数，

当 $a_n\neq 0$ 时，称 a_nx^n 是 $f(x)$的首项，n 是 $f(x)$的次数，并记为 $\deg f(x)=n$，

系数全为零的多项式称为零多项式，零多项式不规定次数，

在多项式环 $R[x]$中，通过比较首项系数易知:

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

$\deg(f(x)g(x))\leqslant\deg f(x)+\deg g(x)$，

并且若 R 是整环，则 $\deg(f(x)g(x))=\deg f(x)+\deg g(x)$，

此时，$R[x]$的单位群就是 $U(R)$，

实际上，一元多项式环的概念可以推广到多元多项式环，

设 R 是有 1 的交换环，则由于 R 有未定元 x_1，从而有一元多项式环 $R[x_1]$，

又因 $R[x_1]$是有 1 的交换环，所以 $R[x_1]$有未定元 x_2，

从而有二元多项式环 $R[x_1][x_2]=R[x_1,x_2],\cdots$

不断重复这个过程，

则可以得到一个 n 元多项式环 $R[x_1][x_2]\cdots[x_n]=R[x_1,x_1,\cdots,x_n]$，

命题 8.2 若 R 是整环，则多项式环 $R[x]$是整环，

证: 因为 $R[x]$是有 1 的交换环，且对属于 $R[x]$的任意 $f(x),g(x)$

若令 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0,g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$，

则有 $f(x)g(x)=a_nb_mx^{n+m}+\cdots$，其中 $a_n\neq 0,b_m\neq 0$

因为 R 是整环，所以 $a_nb_m\neq 0$，即在 $R[x]$中没有零因子，从而，$R[x]$是整环

定理 8.3(带余除法)设 R 是有 1 的交换环，

令 $f(x)$, $g(x)$属于 $R[x]$，若 $g(x)\neq 0$，且 $g(x)$的首项系数为 R 中的可逆元，

则存在唯一的属于 $R[x]$的 $q(x)$, $r(x)$，使得 $f(x)=g(x)q(x)+r(x)$,

其中 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$,

证: 首先证明存在性，

当 $f(x)=0$ 或 $f(x)\neq 0$ 且 $\deg g(x)>\deg f(x)$时，令 $q(x)=0$, $r(x)=f(x)$即可，

当 $f(x)\neq 0$ 且 $\deg g(x)\leqslant\deg f(x)$时，对 $\deg f(x)$用数学归纳法，

不妨令 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$

其中 $m\leqslant n$, a_n , $b_m\neq 0$，而且 b_m 是可逆元，

易知，当 $\deg f(x)=0$ 时，结论成立，

假设存在性对次数小于 $\deg f(x)$的多项式成立，下面我们考虑多项式 $f(x)$,

因为 $f(x)-g(x)a_nb_m^{-1}x^{n-m}=(a_{n-1}x^{n-1}+\cdots+a_0)-(b_{m-1}x^{m-1}+\cdots+b_0)a_nb_m^{-1}x^{n-m}$

所以，若 $f(x)-g(x)a_nb_m^{-1}x^{n-m}=0$，则令 $q(x)=a_nb_m^{-1}x^{n-m}$, $r(x)=0$ 即可，

若 $f(x)-g(x)a_nb_m^{-1}x^{n-m}\neq 0$，则令 $f_1(x)=f(x)-g(x)a_nb'x^{n-m}$，有 $\deg f_1(x)<\deg f(x)$

由归纳假设可知，存在属于 $R[x]$的 $q_1(x)$, $r_1(x)$，使得 $f_1(x)=g(x)q_1(x)+r_1(x)$

其中 $r_1(x)=0$ 或 $\deg r_1(x)<\deg g(x)$,

进而，$f(x)=g(x)[a_nb_m^{-1}x^{n-m}+q_1(x)]+r_1(x)$,

故若令 $q(x)=a_nb_m^{-1}x^{n-m}+q_1(x)$, $r(x)=r_1(x)$，则 $f(x)=g(x)q(x)+r(x)$,

其中 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$，即存在性对 $f(x)$成立，

再证明唯一性，

若另外存在 $q_1(x)$, $r_1(x)$适合条件，并且 $q(x)\neq q_1(x)$, $r(x)\neq r_1(x)$,

则 $g(x)q(x)+r(x)=g(x)q_1(x)+r_1(x)$, $g(x)[q(x)-q_1(x)]=r_1(x)-r(x)$,

因为 $g(x)$的首项系数是可逆元，所以上式左边的次数为

$\deg\{g(x)[q(x)-q_1(x)]\}=\deg g(x)+\deg[q(x)-q_1(x)]=\deg g(x)$,

而右边的次数为 $\deg[r_1(x)-r(x)]<\deg g(x)$，矛盾，

因此，唯一性成立，

一般地，我们把上述定理中的 $q(x)$, $r(x)$分别叫做 $f(x)$除以 $g(x)$的商式和余式，

若将定理 8.3 的结果应用到域上，

则可知在数域上的多项式环中成立的带余除法，在一般域上同样成立，

特别地，若 F 是域，则我们可以在 F[x]中定义$\delta(f(x))=\deg f(x)$，

那么 F[x]是欧氏环，进而 F[x]是主理想整环，是唯一分解整环，

例 8.1 在 $Z_6[x]$中，$f(x)=\overline{2}x^2+\overline{3}x+1$，$g(x)=\overline{3}x+\overline{5}$，试计算 $f(x)g(x)$，

解: $f(x)g(x)=\overline{6}x^3+(\overline{4}+\overline{9})x^2+(\overline{3}+\overline{3})x+\overline{5}=\overline{1}x^2+5=x^2+\overline{5}$，

例 8.2 求整环 $Z_p[x]$的特征，其中 p 是素数，

解: 因为 Z_p 与 $Z_p[x]$的单位元相同，且 Z_p 的特征是 p，所以 $Z_p[x]$的特征也是 p

注意，Z_p 与 $Z_p[x]$的特征都是 p，但是 Z_p 是有限环，$Z_p[x]$是无限环，

例 8.3 设 $f(x)=x^3+x^2+\overline{1}$，$g(x)=x^2+x+\overline{1}$属于 $Z_2[x]$，

求 $Z_2[x]$中多项式 u(x)和 v(x)，使得 $f(x)u(x)+g(x)v(x)=(f(x),g(x))$，

解: 因为 Z_2 是域，所以 $Z_2[x]$中有带余除法，

利用带余除法可得 $f(x)=g(x)x+(\overline{1}-x)$，$g(x)=(\overline{1}-x)(-x)+\overline{1}$，

因此，$f(x)x+g(x)(x^2+\overline{1})=\overline{1}$，即 $u(x)=x$，$u(x)=x^2+\overline{1}$，

下面讨论多项式根的问题，

定义 8.3 设 R 是有 1 的交换环，若 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 属于 R[x]，r 属于 R

则称 $a_nr^n+\cdots+a_1r+a_0$ 为多项式 f(x)在 r 点处的值，记为 f(r)，

特别地，如果 $f(r)=0$，则称 r 为 f(x)在 R 上的一个根，

推论 8.1 设 R 是有 1 的交换环，若 f(x)属于 R[x]，r 属于 R，

则存在属于 R[x]的唯一的 q(x)，使得 $f(x)=(x-r)q(x)+f(r)$，

当且仅当存在属于 R[x]的 q(x)，使得 $f(x)=(x-r)q(x)$时，

属于 R 的 r 是 f(x)的根

例 8.4 证明整环 R 上 n 次多项式 $f(x)$在 R 上最多有 n 个不同的根，

证: 设 $a_1, a_2, \cdots, a_m$ 是 $f(x)$在 R 上的所有不同的根，

由 a_1 是 $f(x)$的根可知，存在属于 $R[x]$的 $q_1(x)$，使得 $f(x)=(x-a_1)q_1(x)$，

因为 R 是整环，

所以由 $0=f(a_2)=(a_2-a_1)q_1(a_2)$，可知 $q_1(a_2)=0$，即 a_2 是 $q_1(x)$的根，

进而，存在属于 $R[x]$的 $q_2(x)$，使得 $q_1(x)=(x-a_2)q_2(x)$，

那么 $f(x)=(x-a_1)(x-a_2)q_2(x)$，

如此继续下去⋯，可知 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_m)q_m(x)$，因此，$m\leqslant n$，

例 8.5 判断多项式 $f(x)=\overline{4}x^3-\overline{2}x^2+x+\overline{3}$在 Z_5 中是否有根，

解: 因为 $f(\overline{0})=\overline{3}$，$f(\overline{1})=f(\overline{3})=f(\overline{4})=\overline{1}$，$f(\overline{2})=\overline{4}$，所以 $f(x)$在 Z_5 中没有根

例 8.6 试求多项式 $f(x)=x^2+\overline{3}x+\overline{2}$在 Z_6 中的所有异根，

解: 因为 $f(\overline{0})=\overline{2}$，$f(\overline{1})=f(\overline{2})=f(\overline{4})=f(\overline{5})=\overline{0}$，$f(\overline{3})=\overline{2}$，

所以 $f(x)$在 Z_6 中有 4 个不同的根，