我们已经知道，域上的多项式环是唯一分解整环，

即域 F 上的多项式可以表示成 F[x]中不可约元的乘积，

特别地，若 f(x)是 F[x]中的不可约元，则必有 deg f(x)＞0，

但是，在一般整环 R 上的多项式环中，零次多项式有可能是 R[x]中的不可约元

基于此，我们有必要考虑整环上多项式环的不可约元及因子分解等问题，

令 R 是唯一分解整环，f(x)属于 R[x]，

若 deg f(x)=0，则属于 R 的 f(x)的因子分解问题已经解决，

若 deg f(x)＞0，我们取 r 为 f(x)所有系数的最大公因子，则 f(x)=rg(x)，

其中 g(x)的系数的最大公因子为 1，

此时，f(x)的因子分解问题转化为 r 和 g(x)的因子分解问题，

而属于 R 的 r 的因子分解问题已经解决，

因此，我们仅需要考虑 g(x)的因子分解，

定义 9.1 令 R 是唯一分解整环，$f(x)=a_nx^n+\cdots+a_1x+a_0$ 属于 R[x]，且 deg f(x)＞0，

若 1 是 f(x)所有系数的最大公因子，则称 f(x)是 R[x]中的本原多项式，

R[x]中次数大于零的不可约元一定是本原多项式，

一般地，若 f(x)是 R[x]中的不可约元，且 deg f(x)=n，

则称 f(x)是 R[x]中的 n 次不可约元，

引理 9.1 令 R 是唯一分解整环，属于 R[x]的 f(x)，g(x)是本原多项式，

若 af(x)=bg(x)，其中 a，b 属于 R，a，b≠0，

则存在属于 U(R)的 u，使得 f(x)=ug(x)

证: 因为等式 af(x)=bg(x)的左右两端多项式系数的最大公因子分别为 a 和 b，

因此 a 和 b 相伴，即存在属于 U(R)的 u，使得 b=au，从而 f(x)=ug(x)，

引理 9.2(高斯引理)设 R 是唯一分解整环 ，

则 R[x]中两个本原多项式的乘积仍然是本原多项式 ，

证: 若属于 R[x]的 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, $g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0$ 是两个本原多项式 ，

则 $f(x)g(x)=c_{n+m}x^{n+m}+\cdots+c_{i+j}x^{i+j}+\cdots+c_1x+c_0$ ，

其中 $c_{i+j}=a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_ib_j+\cdots+a_{i+j}b$, $0\leqslant i+j\leqslant n+m$ ，

下面我们用反证法证明 ，

如果 f(x)g(x)不是本原多项式 ，

那么存在属于 R 的不可约元 p，使得 $p|c_{n+m}$, $\cdots$, $p|c_{i+j}$, $\cdots$, $p|c_1$, $p|c_0$ ，

但是 f(x) , g(x)是本原的 ，所以 p 不能整除所有的 a_i 和 b_j ，

于是 ，不妨假设 $p|a_0$, $p|a_1$, $\cdots$, $p|a_{i-1}$, $p\nmid a_i\cdots$, $p|b_0$, $p|b_1$, $\cdots$, $p|b_{j-1}$, $p\nmid b_j$ ，

现在考察 f(x)g(x)中 x^{i+j} 的系数 $c_{i+j}=a_0b_{i+j}+a_1b_{i+j-1}+\cdots+a_ib_j+\cdots+a_{i+j}b_0$ ，

则除了 a_ib_j 项外 , p 整除上式中的所有项 ，所以 , $p|a_ib_j$ ，

又因为 R 是唯一分解整环 ，不可约元 p 也是素元 ，因此 , $p|a_i$ 或 $p|b_j$, 矛盾 ，

定理 9.1 令 R 是唯一分解整环，F 是 R 的分式域，

若 f(x)属于 R[x]，

则当且仅当 f(x)可以分解成 F[x]中两个次数大于零的多项式乘积时，

f(x)可以分解成 R[x]中两个次数大于零的多项式乘积

证: 因为 $R[x] \subseteq F[x]$，

所以若 f(x)可以分解成 R[x]中两个次数大于零的多项式乘积，

则 f(x)可以分解成 F[x]中两个次数大于零的多项式乘积，

反之，若 f(x)可以分解成 F[x]中两个次数大于零的多项式乘积，

则不妨设 f(x)是本原多项式

且 $f(x)=g(x)h(x)$，$g(x)$，$h(x)$属于 $F[x]$，$\deg g(x)$，$\deg h(x) \geqslant 1$，

进而，可令 $f(x)=\frac{s}{t} g_0(x)h_0(x)$，$s$，$t$ 属于 R，$(s, 1) \sim 1$，

其中属于 R[x]的 $g_0(x)$，$h_0(x)$是本原多项式，

由引理 9.2 和引理 9.1，可知，

$g_0(x)h_0(x)$仍是本原多项式且存在属于 U(R)的 u，使得 $f(x)=ug_0(x)h_0(x)$，

即 f(x)可以分解成 R[x]中两个次数大于零的多项式乘积，

上述定理告诉我们，在考虑因子分解问题时，

唯一分解整环上本原多项式的分解问题等价于其分式域上多项式的分解问题，

命题 9.1 设 R 是唯一分解整环 ，则多项式环 R[x]也是唯一分解整环 ，

证: 设 f(x)是 R[x]中非零、不可逆元 ，F 是 R 的分式域 ，

首先 ，证明 f(x)在 R[x]中有唯一分解 ，

若 deg f(x)=0，则由 R 是唯一分解整环可知 f(x)有唯一分解 ，

若 deg f(x)＞0，不妨设 f(x)=rg(x)，其中 r 属于 R，g(x)是 R[x]中的本原多项式 ，

从而 g(x)是 F[x]中的非零、不可逆元 ，

由于域上的多项式环 F[x]是唯一分解整环 ，所以 g(x)在 F[x]中有唯一分解 ，

令 $g(x)=g_1(x)g_2(x)\cdots g_m(x)$，其中 $g(x)，g_2(x)，\cdots，g_m(x)$是 F[x]中的不可约元 ，

另外 $g_i(x)$可以表示为 $g_i(x)=\frac{s_i}{t_i}h_i(x)$，其中 $s_i，t_i$属于 R，

$h_i(x)$是 R[x]中的本原多项式

由本章命题 7.3 可知 $h_i(x)$是 F[x]中的不可约元 ，

再由定理 9.1 可知 $h_i(x)$是 R[x]中的不可约元 ，

令 $t=t_1\cdots t_m，s=s_1\cdots s_m$，则 $tg(x)=sh_1(x)h_2(x)\cdots h_m(x)$，

由引理 9.2 和引理 9.1 可知 ，$h_1(x)h_2(x)\cdots h_m(x)$是本原多项式 ，

且存在属于 U(R)的 u，使得 $g(x)=uh_1(x)h_2(x)\cdots h_m(x)$，

若 r 是 R 中的可逆元 ，则 f(x)在 R[x]中有唯一分解 $f(x)=ruh_1(x)h_2(x)\cdots h_m(x)$，

若 r 不是 R 中的可逆元 ，则 r 有唯一分解 $r=p_1p_2\cdots p_n$，

其中 $p_1，p_2，\cdots，p_n$是 R 中的不可约元 ，

从而 f(x)在 R[x]中有唯一分解 $f(x)=up_1p_2\cdots p_nh_1(x)h_2(x)\cdots h_m(x)$，

其次 ，我们来证明分解的唯一性 ，

设 $f(x)=p_1p_2\cdots p_sh_1(x)h_2(x)\cdots h_m(x)=q_1q_2\cdots q_tg_1(x)g_2(x)\cdots g_n(x)$，

其中 $p_1，\cdots，p_s，q_1，\cdots，q_t$是 R 中的不可约元 ，

$h_1(x)，\cdots，h_m(x)，g_1(x)，\cdots，g_n(x)$是 R[x]中次数大于零的不可约元 ，

从而 $h_1(x)，\cdots，h_m(x)，g_1(x)，\cdots，g_n(x)$是本原多项式 ，

根据引理 9.1 及引理 9.2 可知 ，

存在属于 U(R)的 u，使得 $h_1(x)，\cdots，h_m(x)=g_1(x)，\cdots，g_n(x)$，

因为 F[x]是唯一分解整环 ，所以 $m=n，h_i(x)\sim g_i(x)(i=1，2，\cdots，n)$，

将 $h_1(x)\cdots h_m(x)=ug_1(x)\cdots g_n(x)$代入 f(x)，则有 $p_1\cdots p_s\,u=q_1\cdots q_t$

又由 R 是唯一分解整环可知 ，$s=t，p_i\sim q_i，1\leqslant i\leqslant s$

利用命题 9.1，我们可以证明在第 7 节中提出的结论:

唯一分解整环不一定是主理想整环，

例 9.1 试证明 Z[x]是唯一分解整环，但不是主理想整环，

证: 由命题 9.1 可知，Z[x]是唯一分解整环，

但是其中的⟨{2，x}⟩却不是 Z[x]的主理想，

若不然，⟨{2，x}⟩是 Z[x]的主理想，则不妨令⟨{2，x}⟩=⟨f(x)⟩，

因为 2，x 属于⟨f(x)⟩，

所以存在属于 Z[x]的 g(x)，h(x)，使得 2=f(x)g(x)，x=f(x)h(x)，

因而 f(x)=±1，⟨f(x)⟩=Z[x]，

而理想⟨{2，x}⟩={2g(x)+xh(x) | g(x)，h(x)属于 Z[x]}中的多项式的常数项为偶数

因此，⟨{2，x}⟩≠⟨f(x)⟩，

所以，⟨{2，x}⟩不是 Z[x]的主理想，即 Z[x]不是主理想整环，

下面介绍一个判断唯一分解整环上的多项式是不可约元的常用的判别法:

艾森斯坦判别法，

定理 9.2(艾森斯坦)令 R 是唯一分解整环，

$f(x)=a_nx^n+\cdots+a_1x+a_0(a_n\neq 0)$是 R[x]中次数大于零的本原多项式，

若存在属于 R 的不可约元 p，使得 $p\nmid a_n$，$p^2\nmid a_0$，$p|a_i$，$0\leqslant i\leqslant n-1$，

则 f(x)是 R[x]中的不可约元，

证: 用反证法，若 f(x)有真因子 g(x)，则存在 h(x)，使得 $f(x)=g(x)h(x)$，

因为 f(x)是本原多项式，所以 $\deg g(x)\geqslant 1$，$\deg h(x)\geqslant 1$，

令 $g(x)=b_kx^k+\cdots+b_1x+b_0$，$h(x)=c_lx^l+\cdots+c_1x+c_0$，这里 $b_k\neq 0$，$c_l\neq 0$，k，$l<n$

因为 $a_0=b_0c_0$，$p|a_0$，$p^2\nmid a_0$，所以只能存在 b_0，c_0 之一被 p 整除，可令 $p|c_0$，$p\nmid b_0$

又因 $a_n=b_kc_l$，$p\nmid a_n$，所以 $p\nmid c_l$，

而 $p|c_0$，所以，我们可以取到最小的下标 $r>0$，使得 $p\nmid c_r$，$0<r\leqslant l<n$，

于是，我们考察 $a_r=b_0c_r+b_1c_{r-1}+\cdots+b_rc_0$

在上式右端中 $p\nmid b_0c_r$，而 p 整除其余各项，因此 $p\nmid a_r$

这与已知假设 $p|a_i$，$0\leqslant i\leqslant n-1$ 矛盾，因此，f(x)是 R[x]中的不可约元，

例 9.2 令 p 是素数，证明属于 Z[x]的多项式 $f(x)=\frac{x^p-1}{x-1}=x^{p-1}+\cdots+x+1$ 是不可约元

证: 因为多项式 f(x)的不可约性等价于 f(x+1)的不可约性，

所以，我们考察属于 Z[x]的 $f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+C_p^1x^{p-2}+C_p^2x^{p-3}+\cdots+p$，

利用艾森斯坦判别法(Z 中的不可约元取为素数 p)，f(x+1)是 Z[x]中的不可约元，

因此 f(x)是 Z[X]中的不可约元，

例 9.3 证明属于 Q[x]的多项式 $f(x)=\frac{3}{2}x^5-18x^3+3x+3$ 是 Q[x]中不可约元

证: 因为 $f(x)=\frac{3}{2}(x^5-12x^3+2x+2)$，

所以若令 $g(x)=x^5-12x^3+2x+2$，则 g(x)是 Z[x]中的本原多项式，

由定理 9.1 可知，g(x)在 Q[x]中的不可约性等价于 g(x)在 Z[x]中的不可约性，

利用艾森斯坦判别法(Z 中的不可约元取为 2)可知，g(x)是 Z[x]中的不可约元，

从而 g(x)是 Q[x]中的不可约元，进而 f(x)是 Q[x]中的不可约元，

我们知道有理数域上的多项式不一定能分解成一次因子的乘积，
但是，复数域上的多项式可以分解成一次因子的乘积，
那么对于一般域上的多项式，是否可以找到一个扩域，
使该多项式在此扩域上能分解成一次因子的乘积呢?

命题 9.2 设 F 是一个域，如果属于 F[x]的 f(x)是次数大于零的多项式，
则存在 F 的一个扩域，使得 f(x)在此扩域中有根，
证: 因为 F[x]是唯一分解整环，所以 f(x)有不可约因子，设为 p(x)，
又因为 F[x]是主理想整环，所以 p(x)生成的理想是极大理想，
因此 $F[x]/\langle p(x)\rangle$是域，
考虑自然同态$\pi: F[x]\to F[x]/\langle p(x)\rangle$，$g(x)\to g(x)+\langle p(x)\rangle=\overline{g(x)}$
因为对属于 F 的 a，当$\pi(a)=0$时，有 a 属于$\langle p(x)\rangle$，从而 $a=0$，
即可以将 F 视为$F[x]/\langle p(x)\rangle$的一个子域，
从而 $p(\overline{x})=\overline{p(x)}=0$，即$\overline{x}$是 p(x)的一个根，也是 f(x)的根，

推论 9.1 设 F 是一个域，如果属于 F[x]的 f(x)是次数大于零的多项式，
则存在 F 的扩域 E，使得 f(x)可以表示为 E 中一次因子的乘积，

既然，在 F 的某个扩域上，f(x)有一次因子，那么一次因子能出现多少次呢?

定义 9.2 设 F 是一个域，α属于 F，f(x)属于 F[x]，
若$(x-\alpha)^k|f(x)$，$(x-\alpha)^{k+1}\nmid f(x)$，则称α是 f(x)的 k 重根，
特别地，当 $k=1$ 时，称α是 f(x)的单根，当 $k>1$ 时，称α是 f(x)的重根，

下面我们先规定形式导数，

然后，借用形式导数的性质来判断一个多项式是否有重根，

令 F 是域，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 属于 F[x]，

则定义其形式导数为 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$

容易验证，形式导数具有与导数一样的“加、减、乘”等性质，

即如果 f(x)，g(x)属于 F[x]，

那么 $(f(x)\pm g(x))'=f'(x)\pm g'(x)$，$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$

定理 9.3 设 F 是域，f(x)属于 F[x]

则 f(x)在 F 的某个扩域上有重根的充分必要条件是 f(x)，f'(x)在 F[x]中不互素，

证: 首先，如果属于 $E(\supseteq F)$的α是 f(x)的 k 重根$(k>1)$

则在 E[x]上有 $f(x)=(x-\alpha)^kg(x)$，$(x-\alpha)\nmid g(x)$，

所以，$f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^kg'(x)=(x-\alpha)^{k-1}-[kg(x)+(x-\alpha)g'(x)]$，

又因 $k>1$，于是 $x-\alpha$是 f(x)，f'(x)的公因子，

若属于 E[x]的 d(x)是 f(x)和 f'(x)的最大公因子，则 $\deg d(x)>0$，

另外，我们可以通过多项式的辗转相除法求出 f(x)和 f'(x)的最大公因子 $d_0(x)$，

那么 $d_0(x)\sim d(x)$，即 $\deg d_0(x)>0$，

而在辗转相除的过程中涉及的多项式的系数必定属于 F，所以，$d_0(x)$属于 F[x]，

即 f(x)与 f'(x)在 F[x]中不互素，

其次，如果 f(x)和 f'(x)在 F[x]中不互素，不妨令$(f(x),f'(x))=d(x)$属于 F[x]，

则由命题 9.2 可知，d(x)在某个扩域 E 上有根，

若设α属于 E，$d(\alpha)=0$，则α是 f(x)，f'(x)的根，

事实上，x 还是 f(x)的重根，如若不然，则 $f(x)=(x-\alpha)g(x)$，$(x-\alpha)\nmid g(x)$，

又因 $f'(x)=g(x)+(x-\alpha)g'(x)$，所以，$(x-\alpha)\nmid f'(x)$，即$\alpha$不是 f'(x)的根，矛盾，

因此，α一定是 f(x)的重根，

实际上，我们很容易知道;

如果属于 F[x]的 f(x)是不可约元，

则 f(x)在 F 的扩域上有重根的充分必要条件是 $f'(x)=0$,

事实上，若 $f'(x)\neq 0$，则 $\deg f'(x)<\deg f(x)$,

又因为 f(x)是不可约元，所以$(f(x), f'(x))\sim 1$，从而 ,f(x)没有重根，

若 $f'(x)=0$，则 f(x)和 f'(x)不互素，进而 ,f(x)有重根，

定理 9.4 设 F 是域，属于 F[x]的 f(x)是不可约元，则

(1)当 Char F=0，时 f(x)没有重根;

(2)当 Char F=p(素数)，当且仅当 f(x)是关于 x^p 的多项式，

即存在属于 F[x]的 g(x)，使得 $f(x)=g(x^p)$时 ,f(x)有重根，

证明: (1)的结论是显然的，

(2)令 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 属于 F[x],

则形式导数为 $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$,

因为 f(x)有重根的充分必要条件是 $f'(x)=0$,

所以的 $na_n=0, (n-1)a_{n-1}=0, \cdots, a_1=0$,

又因 Char F=p，所以由 $ia_i=0, 1\leqslant i\leqslant n$，可以知道 $p|i$ 或 $p|a_i$,

于是，不可约元 f(x)的形式为

$f(x)=a_{kp}x^{kp}+a_{(k-1)p}x^{(k-1)p}+\cdots+a_px^p+a_0=a_{kp}(x^p)^k+a_{(k-1)p}(x^p)^{k-1}+\cdots+a_p(x^p)+a_0$

若令 $g(x)=a_{kp}x^k+a_{(k-1)p}x^{k-1}+\cdots+a_px+a_0$，则当然有 $f(x)=g(x^p)$

反之，若 $f(x)=g(x^p)$，则 $f'(x)=0$，因此 f(x)有重根，