1，试判断 $x^2+\overline{1}$是否是 $Z_5[x]$中的不可约元，

解: 由于$\overline{2}^2+\overline{1}=\overline{0}$，$\overline{3}^2+\overline{1}=\overline{0}$，从而$\overline{2}$，$\overline{3}$为 x^2+1 在 Z_5 中的根，

故 x^2+1 不是 $Z_5[x]$中的不可约元，

2，求 $Z_2[x]$中所有三次不可约元，

解: 令 $f(x)=ax^3+bx^2+cx+d$，a，b，c，d 属于 Z_2，若 $f(x)$可约，则(x)有根，

将$\overline{0}$，$\overline{1}$分别代入 $f(x)=0$，则有 $d=0$ 或 $a+b+c+d=0$，

因此，若 $f(x)$是 $Z_2[x]$中的不可约元，则 $d=1$ 且 $a+b+c=0$，

从而 $f(x)=x^3+x^2+1$ 或 $f(x)=x^3+x+1$，

3，将 x^5-x 和 x^8-x 分别表示成 $Z_2[x]$中不可约元的乘积，

解: $x^5-x=x(x^4-1)=x(x^2-1)(x^2+1)=x(x-1)^2(x+1)^2=x(x-1)^4$

$x^8-x=x(x-1)(x^3+x^2+1)(x^3+x+1)$，

4，求 $Z_3[x]$中所有二次不可约元，

解: 令 $f(x)=ax^2+bx+c$，a，b，c 属于 Z_3，若 $f(x)$可约，则 $f(x)$有根，

将$\overline{0}$，$\overline{1}$，$\overline{2}$分别代入 $f(x)=0$，则分别有 $c=0$，$a+b+c=0$，$a-b+c=0$

若 $f(x)$是 $Z_3[x]$中的不可约元，则 $c\neq0$，$a+b+c\neq0$，$a-b+c\neq0$

从而有 $c=\overline{1}$，$a=\overline{1}$，$b=\overline{0}$，或 $b=c=\overline{1}$，$a=\overline{2}$，或 $c=\overline{1}$，$a=b=\overline{2}$，

或 $a=b=\overline{1}$，$c=\overline{2}$，或 $a=\overline{1}$，$b=c=\overline{2}$，或 $b=\overline{0}$，$a=c=\overline{2}$

则 $f(x)=x^2+1$，或 $f(x)=\overline{2}x^2+x+1$，或 $f(x)=\overline{2}x^2+\overline{2}x+1$，或 $f(x)=x^2+x+\overline{2}$

或 $f(x)=x^2+\overline{2}x+\overline{2}$，或 $f(x)=\overline{2}x^2+\overline{2}$

5，证明 $f(x)=x^4-10x^2+1$ 是 $Q[x]$中的不可约元，

证明 1: ±1 不是 $f(x)$的根，若 $f(x)$可约，则 $f(x)=(x^2+ax+b)(x^2+cx+1/b)$，

因此

$$\begin{cases} a+c=0 \\ a+b^2c=0 \\ b^2+abc+10b+1=0 \end{cases}$$

上面方程组无有理解，所以(x)是 $Q[x]$中的不可约元，

证明 2: $f(x)$的四个根为$\pm(\sqrt{2}\pm\sqrt{3})$，

6，证明属于 $Q[x]$的多项式 $g(x)=x^p+px+1$ 是 $Q[x]$中的不可约元(p 是素数，$p\neq2$)

证明: $g(x-1)=x^p-C_p^1x^{p-1}+C_p^1x^{p-2}+\cdots+2px-p$，取素数 p，

则由艾森斯坦判别法得 $g(x-1)$是不可约元，从而 $g(x)$是不可约元，

7，设 R 是唯一分解整环，F 是 R 的分式域，$f(x)=a_nx^n+\cdots+a_1x+a_0$ 属于 $R[x]$，

若属于 F 的 $\frac{s}{r}$ 是 $f(x)$在 F 上的根，且$(s,r)\sim1$，则 $r|a_n, s|a_0$

证明: 由已知得 $f\left(\frac{s}{r}\right)=a_n\left(\frac{s}{r}\right)+\cdots+a_1\left(\frac{s}{r}\right)+a_0=0$

即 $a_ns^n+\cdots+a_1r^{n-1}s+a_0r^n=0$，因此，$r|a_ns^n$

又因$(r,s)=1$，从而有 $r|a_n$，同理有 $s|a_0$

8，令 R 是唯一分解整环，F 是 R 的分式域，属于 R[x]的 f(x)是本原多项式，

试证明当且仅当 f(x)在 F[x]中不可约时，f(x)在 R[x]中不可约，

证明: 必要性，反证，

若 f(x)可以分解为 F[x]中两个次数大于零的多项式的乘积

则 f(x)可以分解为 R[x]中两个次数大于零的多项式的乘积，

这与 f(x)在 R[x]中不可约矛盾

充分性，因为 f(x)是本原多项式，所以 $f(x)\neq 0$ 且不可逆，

R[x]是唯一分解整环，令 $f(x)=a_1\cdots a_n p_1(x)\cdots p_m(x)$，

其中 $a_1,\cdots,a_n,p_1(x),\cdots,p_m(x)$是 R[x]中的不可约元，

由必要性可知 $p_1(x),\cdots,p_m(x)$是 F[x]中不可约元，

由于 f(x)是 F[x]中不可约元，所以 $f(x)=a_1\cdots a_n p_1(x)$

因为 f(x)是本原多项式，所以 $f(x)=p_1(x)$是 R[x]中不可约元，

习题 1 判断唯一分解整环 R 的同态像 R'是否一定是唯一分解整环，

解: 不一定，设 R=Z[x]，则 R 是唯一分解整环，

若 R'=Z[i]，$\varphi(f(x))=f(i)$是 R 到 Z[i]的满同态映射，此时 R'是唯一分解整环，

若 R'=Z[$\sqrt{-3}$]，则$\varphi(f(x))=f(\sqrt{-3})$是 R 到 Z[$\sqrt{-3}$]的满同态映射，

但是 R'不是唯一分解整环，

习题 2 设 F 是域，f(x)属于 F[x]，deg f(x)=n＞0，

试证明 f(x)在 F 中根的个数不可能大于 n，重根按重数计算，

证明: 因为 F[x]是唯一分解整环，将 f(x)分解成不可约多项式的乘积，

f(x)在 F 中根的个数等于分解式中一次因式的个数，这个个数不可能大于 n，

习题 3 设 f(x)是域 F 上不可约多项式，Char F=p(素数)，

如果 f(x)在 F 中有重根，证明 f(x)的每一个根的重数都相等

证明: 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

若 g(x)有重根，则 g(x)是关于 x^p 的多项式，不妨设 $f(x)=g(x^{p^k})$，

但是 f(x)不是$x^{p^{k+1}}$的多项式，显然 g(x)是不可约多项式，进而无重根，

令 g(x)在其分裂域内的分解式为 $g(x)=\prod_{i=1}^{m}(x-\alpha_i)$

则 $f(x)=\prod_{i=1}^{m}\left(x^{p^k}-\alpha_i\right)=\prod_{i=1}^{m}(x-\alpha_i)^{p^k}$

习题 4 设 F 是域，f(x)属于 F[x]，α为 f(x)的 k 重根，试证明

(1)若 Char F∤k，则α是 f'(x)的 k−1 重根;

(2)若 Char F|k，则α是 f'(x)的至少 k 重根

证明: 设 E 为 f(x)在 F 上的分裂域，则 $f(x)=(x-\alpha)^k g(x)$属于 E[x]，其中 $g(\alpha)\neq 0$，

故 $f'(x)=(x-\alpha)^{k-1}h(x)$，其中 $h(x)=kg(x)+(x-\alpha)g'(x)$，于是

(1)若 Char F∤k，则以 x=α代入 h(x)得 $kg(\alpha)\neq 0$，即 x−a 不是 h(x)的因式，

所以 f'(x)以α为 k−1 重根

(2)若 Char F|k，则 $f'(x)=(x-\alpha)^k g'(x)$，结论得证，

习题 5 求 $x^4-\overline{2}x^3-x+\overline{2}$在 Z_7 中所有的根

解: 设 $f(x)=x^4-\overline{2}x^3-x+\overline{2}$，易知$\overline{1}$，$\overline{2}$，$\overline{4}$都是 f(x)的根，

即在 Z_7 中有三个不同的根

而$\overline{2}$是 $f'(x)=\overline{4}x^3+x^2-1$ 的根，即$\overline{2}$是 f(x)的重根

又因 f(x)在 Z_7 中最多有 4 个根，所以 f(x)在 Z_7 中的根为$\overline{1}$，$\overline{2}$，$\overline{2}$，$\overline{4}$

习题 6 将 $Z_5[x]$中多项式 $x^3+x^2+\overline{3}$分解为不可约因式的乘积 ，

解: 令 $f(x)=x^3+x^2+\overline{3}$ ，则 $f(x)$有根$\overline{1}$ ，$\overline{2}$ ，而 $f'(x)=\overline{3}x^2+\overline{2}x$ 有根$\overline{1}$ ，

因此$\overline{1}$是重根 ，$f(x)=(x-\overline{1})^2(x-\overline{2})$ ，

习题 7 将 $Z[x]$中多项式 $3x^2+12x+9$ 分解为不可约因子的乘积 ，

解: $f(x)=3x^2+12x+9=3(x+1)(x+3)$ ，

习题 8 证明 x^2+1 在四元数体 H 中有无穷多个根

证明: 在 H 中记 E_2 为 1 ，$i=\begin{pmatrix}\sqrt{-1} & 0\\ 0 & \sqrt{-1}\end{pmatrix}$ $j=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ $k=\begin{pmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}$

则有 $i^2=j^2=k^2=-1$ ，$ij=-ji$ ，$jk=-kj=i$ ，$ki=-ik=j$

且 H 中每个元素可以唯一地表示为 $a+bi+cj+dk(a,b,c,d\in R)$

由此可见

$(a+bi+cj+dk)^2=a^2+2a(bi+cj+dk)-(b^2+c^2+d^2)=-1\Leftrightarrow a=0,b^2+c^2+d^2=1$

因而 x^2+1 在四元数体 H 中有无穷多个根

习题 9 设 R 是整环 ，$R[x]$是主理想整环 ，试证明 R 是域 ，

证明: 对属于 R 且不为 0 的 a，由 $R[x]$是主理想整环知 ，

存在属于 $R[x]$的 $f(x)$，使$\langle f(x)\rangle=\langle a,x\rangle$ ，

从而 $f(x)|a$ ，$f(x)|x$，由 $f(x)|a$ 知 ，$f(x)=b$ 属于 $R(b\neq 0)$;

再由 $f(x)=b$ 整除 x 知 b 必是可逆元 ，于是$\langle a,x\rangle=\langle 1\rangle$ ，

从而存在属于 $R[x]$的 $u(x)$ ，$v(x)$ ，使 $1=u(x)a+v(x)x$ ，

取 $x=0$ 得 $u(0)a=1$ ，即 a 是可逆元 ，

由 a 的任意性知 R 是域 ，

习题 10 证明域的乘法群的任何有限阶子群是循环群 ，

证明: 设 G 是域 F 的乘法群 F^*的有限子群 ，

由习题 2 知多项式 $f(x)=x^m-1$ 在 F 中最多有 m 个根 ，从而在 G 中最多有 m 个解 ，

根据第二章第 5 节典型题习题 35 知 G 是循环群 ，

习题 11 p 是大于 2 的素数，p∤a，

试证明当且仅当$a^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\ p)$时，$x^2\equiv a(\mathrm{mod}\ p)$在 Z 中有解，

证明: 必要性，

若设 b 是$x^2\equiv a(\mathrm{mod}\ p)$在 Z 中的一个解

则$b^2\equiv a(\mathrm{mod}\ p)$，从而$a^{\frac{p-1}{2}}\equiv b^{p-1}\equiv 1(\mathrm{mod}\ p)$，

充分性，分两种情况证明

当 p=4n+3(n 属于 Z)时，$a^{\frac{p-1}{2}}\equiv a^{2n+1}\equiv l(\mathrm{mod}\ p)$，则$a^{2n+2}\equiv a(\mathrm{mod}\ p)$，

即$x^2\equiv a(\mathrm{mod}\ p)$在 Z 中有解$a^{n+1}$

当 p=4n+1 时，因为Z_p的乘法群是 p−1 阶循环群，故可设$\bar{c}$是其生成元

令$\bar{a}=\bar{c}^m$，则$a^{2n}\equiv c^{2nm}(\mathrm{mod}\ p)$，又因$a^{2n}=a^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\ p)$，所以$\bar{c}^{2nm}=\bar{1}$

而$\bar{c}$的阶为 p−1=4n，因此，4n|2nm，2|m

今 m=2t，则$a\equiv c^{2t}(\mathrm{mod}\ p)$，即$c^t$是$x^2\equiv a(\mathrm{mod}\ p)$在 Z 中的解

习题 12 证明当 p 是形如 4n+1(n 属于Z^+)的素数时，p 不是 Z[i]的素元

证明: 因为$(-1)^{\frac{p-1}{2}}=(-1)^{2n}=1(\mathrm{mod}\ p)$

所以由上题知$x^2\equiv -1(\mathrm{mod}\ p)$在 Z 中有解，记为 b

则$b^2+1=(b+i)(b-i)$能被 p 整除，但是 p∤b±i，所以 p 不是 Z[i]中的素元

习题 13 高斯整环 Z[i]的不可约元(在相伴意义下)有且仅有以下三种:

(l)1+i

(2)a+bi，其中 a，b 属于 Z，$a^2+b^2\equiv1(\mathrm{mod}\ 4)$且为素数

(3)素数 $p\equiv3(\mathrm{mod}\ 4)$

证明: 由第 7 节典型题习题 9 知，

找 Z[i]中的不可约元即找属于 Z 的素数 p 的不可约因子，

(1)若 p=2，由于 2 的不可约因子有±(1±i)，因此，1±i 是 Z[i]中的不可约元，

(2)若 $p\equiv1(\mathrm{mod}\ 4)$，由上题知 p 不是 Z[i]中的素元，即 p 有非平凡因子α=a+bi，

由第 7 节典型题习题 8 知 $p=a^2+b^2$，a+bi 是 Z[i]的不可约元，

(3)若 $p\equiv3(\mathrm{mod}\ 4)$，假如 p=(a+bi)(a−bi)，

则 $p=a^2+b^2\equiv0,1,2$ 与 $p\equiv3(\mathrm{mod}\ 4)$矛盾

故 p 没有非平凡因子，p 在 Z[i]中不可约，

习题 14 判断多项式 f(x)在 Q(i)[x]中是否可约，$f(x)=x^{p-1}+x^{p-2}+\cdots+1$，

其中 p 为素数，

解: (1)若 p=2，显然 f(x)=x+1 不可约，

(2)设 p＞2，因为 Q(i)是 Z[i]的分式域，所以要证明 f(x)在 Q(i)[x]中不可约，

只需要证明 f(x)在 Z[i][x]中不可约，

考虑多项式 $f(y+1)=\sum_{i=1}^{p}C_p^i y^{i-1}$

当 $p\equiv1(\mathrm{mod}4)$时，p 有非平凡因子α=a+bi，且α=a+tbi 是 Z[i]中的不可约元，

根据艾森斯坦判别法得 f(x)不可约，

当 $p\equiv3(\mathrm{mod}\ 4)$时，是 Z[i]中的不可约元，

根据艾森斯坦判别法得知 f(x)不可约，

习题 15 设 $f(x)=3x^3-x+1$，判断 $f(x)$在 $Z[x]$中是否可约，

解: 这是一个 3 次本原多项式，

若 $f(x)$可约，则 $f(x)$必能分解为一个一次因式与一个二次因式之积，

因而必有一个有理根，而 $f(x)$的有理根只可能为$\pm 1, \pm \frac{1}{3}$

分别代入 $f(x)$检验，可知都不是 $f(x)$的根

所以 $f(x)$无有理根，因而 $f(x)$在 $Q[x]$不可约，进而在 $Z[x]$中不可约，

习题 16 证明 x^4+1 是环 $Z[x]$中的不可约元，

证明: 令 $x=y+1$，则 $x^4+1=y^4+4y^3+6y^2+4y+2$，取 $p=2$，

则由艾森斯坦判别方法知$(y+1)^4+1$ 是 $Z[x]$中的不可约元，

从而 x^4+1 是 $Z[x]$中的不可约元

习题 17 设 $f(x)=x^5-5x+1$，判断 $f(x)$在 $Z[x]$中是否可约，

解: 令 $x=t-1$，则 $f(x)=f(t-1)=t^5-5t^4+10t^3-10t^2+5$，取 $p=5$，

由艾森斯坦判别方法知 $f(t-1)$在 $Z[x]$中不可约，所以 $f(x)$在 $Z[x]$中也不可约，

习题 18 证明 $f(x)=x^4-10x^2+2x+1$ 是 $Q[x]$中的不可约元，

证明: $f(x+1)=x^4+4x^3-4x^2-14x-6$，取 $p=2$，

则由艾森斯坦判别方法知 $f(x+1)$是 $Z[x]$中的不可约元，

从而 $f(x)$是 $Q[x]$中的不可约元，

习题 19 证明 x^4-x^3-2x+1 是环 $Z[x]$中的不可约元，

证明: 易知± 1 不是 x^4-x^3-2x+1 的根，即在 $Q[x]$中，x^4-x^3-2x+1 没有一次因式

若在 $Q[x]$中 x^4-x^3-2x+1 可约，则应有 $x^4-x^3-2x+1=(x^2+ax\pm 1)(x^2+bx\pm 1)$，

比较 x^3 的系数，得 $a+b=-1$，比较 x 的系数，得$\pm(a+b)=-2$，这是不可能的，

于是 x^4-x^3-2x+1 在 $Q[x]$中不可约，从而在 $Z[x]$中不可约，

习题 20 判断多项式 $x^5+x^3-3x-x+1$ 在 $Q[x]$中是否可约 ，

解: 令 $f(x)=x^5+x^3-3x-x+1$，显然 $f(x)$在 Z 中无根 ，

即 $f(x)$不能分解为 $Z[x]$中一次因式和四次因式的乘积 ，

若 $f(x)=(x^2+\alpha x+\beta)(x^3+ax^2+bx+c)$，则$\beta=c=\pm1$，$a=-\alpha$，

从而 $f(x)=(x^2+\alpha x+\beta)(x^3-\alpha x^2+bx+\beta)$，

进一步有$\begin{cases} b-\alpha^2=1-\beta \\ \alpha b-\beta\alpha=-3-\beta \\ \alpha\beta+\beta b=-1 \end{cases}$ 但是它在 Z 中无解 ，

因此 ，$f(x)$在 $Z[x]$中不可约 ，从而 $f(x)$在 $Q[x]$中不可约

习题 21 判断 $Q(i)[x]$中多项式 $x^4+(8+i)x^3+(3-4i)x+1+2i$ 是否可约 ，

解: 因为$\alpha=1+2i$ 是唯一分解整环 $Z[i]$中的不可约元 ，而$\alpha|8+i$，$\alpha|3-4i$，$\alpha^2|\alpha$，

根据艾森斯坦判别方法知

$f(x)=x^4+(8+i)x^3+(3-4i)x+1+2i$ 是 $Z[i][x]$中的不可约元 ，

因为 $Q(i)$是 $Z[i]$的分式域 ，因此 $f(x)$是 $Q(i)[x]$中的不可约多项式

习题 22 设 R 是主理想整环 ，且 R 是无限集 ，

试证明若 R 中只有有限个可逆元 ，则 R 中有无限多个素理想 ，

证明: 反证 ，设$\langle p_1\rangle$，$\langle p_2\rangle$，$\cdots$，$\langle p_k\rangle$为 R 的所有素理想 ，

令 $q=p_1p_2\cdots p_k$，$\langle q\rangle=I$，则 I 包含于$\langle p_i\rangle$，

由于 R 是无限集 ，故 I 也是无限集 ，

对属于 I 的任意 x，$1\leqslant i\leqslant k$，$1+x$ 不属于$\langle p_i\rangle$，因此是可逆元 ，

这与 R 中只有有限个可逆元矛盾 ，

故 R 中有无限多个素理想 ，

习题 23 试证明 $Z_p[x]$中有无限多个不可约元 ，

证明: 因为 $Z_p[x]$是无限主理想整环 ，只有 $p-1$ 个可逆元 ，

于是由前一个习题知有无限多个素理想 ，

而 $Z_p[x]$的素理想由不可约元生成 ，故 $Z_p[x]$有无限多个不可约元 ，

习题 24 设 $p_1, p_2, \cdots, p_r$ 是 r 个不同素数，$m>1$，证明 $(p_1p_2\cdots p_r)^{\frac{1}{m}}$ 是无理数

证明: 因为 $(p_1p_2\cdots p_r)^{\frac{1}{m}}$ 是 $x^m-p_1p_2\cdots p_r$ 的根，

而 $p_1 | p_1p_2\cdots p_r$，$p_1^2 \nmid p_1p_2\cdots p_r$，$p_1 \nmid 1$，

根据艾森斯坦判别方法知 $x^m-p_1p_2\cdots p_r$ 是 $Q[x]$ 中的不可约多项式，

所以 $(p_1p_2\cdots p_r)^{\frac{1}{m}}$ 是无理数，

习题 25 设 $a_1, a_2, \cdots, a_n$，是不同的整数，

试证明 $(x-a_1)(x-a_2)\cdots(x-a_n)-1$ 是 $Q[x]$ 中不可约多项式

证明: 反证，因为 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$ 为 $Z[x]$ 中本原多项式，

故若在 $Q[x]$ 中 $f(x)$ 可约，则在 $Z[x]$ 中有

$f(x)=f_1(x)f_2(x)$，$f_1(x), f_2(x)$ 属于 $Z[x]$，$\deg f_1(x), \deg f_2(x)<n$，

因而 $f_1(a_i)f_2(a_i)=f(a_i)=-1$，$1\leqslant i\leqslant n$，故 $f_1(a_i)=-f_2(a_i)$，$1\leqslant i\leqslant n$，

又因为 $\deg f_1(x)<n$，$\deg f_2(x)<n$，所以 $f_1(x)=-f_2(x)$，

于是 $f(x)=-[f_1(x)]^2$ 是首项系数为 -1 的多项式，与其首项系数为 1 矛盾，

故 $f(x)$ 不可约

习题 26 设 F 是域，如果属于 $F[x]$ 的 x^n-a 不可约，

试证明对于 n 的任一正因子 m，x^m-a 在 $F[x]$ 中不可约，

证明: 设 $n=mk$，假若 $x^m-a=g(x)h(x)$ 属于 $F[x]$，

则 $x^n-a=(x^k)^m-a=g(x^k)h(x^k)$，矛盾，

习题 27 设 R 是唯一分解整环，P 是 R 的分式域，

f(x)是 R[x]中首项系数为 1 的多项式，

如果 g(x)是 f(x)在 P[x]中首项系数为 1 的因子，试证明 g(x)属于 R[x]，

证明: 令 $f(x)=g(x)h(x)$，显然 h(x)属于 P[x]且首项系数为 1，

因为 P 是 R 的分式域，所以 $g(x)=\frac{1}{s}\overline{g}(x)$，$h(x)=\frac{1}{t}\overline{h}(x)$，

其中 s，t 属于 R，$\overline{g}(x)$，$\overline{h}(x)$是 R[x]中的本原多项式，

那么 $stf(x)=\overline{g}(x)\overline{h}(x)$也是本原多项式，从而 st~1，s，t 是 R 的可逆元，

即 g(x)属于 R[x]，