15.8 设 $p(x)=x^3+3x-2, u=x+(p(x))\in Q[x]/p(x))$, 试将 $(u+4)^{-1}$写成u的二阶多项式。

解：同上题，设 $(u+4)^{-1}=ax^2+bx+c$

由 $(u+4)(ax^2+bx+c)=1$

$$\Rightarrow a=1/78, b=-2/39, c=19/78$$

$$\therefore (u+4)^{-1}=1/78\,x^2-2/39\,x+19/78$$

15.9判定下述元素是不是给定域上的代数元。

（1）$e^{i\frac{2\pi h}{k}}$ 关于Q和R,其中k,h为正整数，且h<k;

令

$$x = e^{i\frac{2\pi h}{k}} = \cos\frac{2\pi h}{k} + i\sin\frac{2\pi h}{k}$$

$$x^k = 1$$

$$\therefore e^{i\frac{2\pi h}{k}}\text{是}x^k - 1 = 0\text{的根}$$

$$\therefore e^{i\frac{2\pi h}{k}}\text{是}Q, R\text{上的代数元。}$$

(2) $\sqrt{3}+\sqrt{2}$关于Q;

令$x = \sqrt{3} + \sqrt{2}$

等式两边平方得$x^2 = 5 + 2\sqrt{6}$

移项再平方得（$x^2 - 5)^2 = (2\sqrt{6})^2$

即$x^4 - 10x^2 + 1 = 0$

$\therefore \sqrt{3}+\sqrt{2}$为$x^4 - 10x^2 + 1 = 0$的根

(3) $2\pi+1$关于Q,其中π为圆周率。

采用反证法，设$2\pi+1$为关于Q的代数元

$$\therefore \exists f(x)=\sum_{i=1}^{n}a_i x^i \in Q[x],\text{满足} f(2\pi+1)=0,$$

$$\therefore \sum_{i=0}^{n}a_i(2\pi+1)^i=0 \Longrightarrow \sum_{i=0}^{n}k_i\pi^i=0$$

这与π为超越元矛盾。$\therefore 2\pi+1$为超越元。

15.11　找出下述元素在所指定域上的极小多项式：

(1) $3+\sqrt{2}$ 关于Q；

(2) 7＋5i关于Q，R。

解：1）记$x=3+\sqrt{2}$，可得$x^2-6x+7=0$。$x^2-6x+7\in Q[x]$，首项系数为1，且在Q[x]上不可约，即为所求极小多项式。

2）记$x=7+5i$，可得$x^2-14x+74=0$。$x^2-14x+74$为7＋5i关于Q，R的极小多项式。

15.13　$x^3-\alpha \in Q[x]$是不可约的，β是$x^3-\alpha$的一个根，证明：$Q(\beta)$不是$x^3-\alpha$的根域。

证明：假设$Q(\beta)$是$x^3-\alpha$的根域。

∵β是$x^3-\alpha$的一个根

∴ $\beta^3-\alpha=0$

∴ $x^3-\alpha= x^3-\beta^3=(x-\beta)(x^2+\beta x+\beta^2)$

由假设可知$(x^2+\beta x+\beta^2)$在$Q(\beta)$内可分解。

∵任何$a\in Q(\beta)$可表示为$a_0+a_1\beta+a_2\beta^2$(a_0, a_1, $a_2\in Q$)

∴存在$a,b\in Q(\beta)$满足 $x^2+\beta x+\beta^2=(x-a)(x-b)=(x-(a_0+a_1\beta+a_2\beta^2))(x-(b_0+b_1\beta+b_2\beta^2))$ 由等式两边x的系数对应相等可得

$a+b=\beta$

$ab=\beta^2$

由上面两式可得

$a_1+b_1=1$

$a_1b_1=1$

a_1,b_1在Q内无解，与$a_1,b_1\in Q$矛盾。

∴假设不成立

$Q(\beta)$不是$x^3-\alpha$的根域

15.16 F为域， $f(x)$， $g(x) \in F[x]$， 已知$f(x)$是不可约的， K为F的扩域， 在K中$f(x)$ 与$g(x)$有公共零点， 证明： $f(x) \mid g(x)$。

证明：记$f(x)$首项系数为$a \in F^*$, α为$f(x)$ 和$g(x)$的公共零点。则$f(x)/a$为α在$F[x]$中极小多项式。

$\because g(\alpha)=0$

$\therefore f(x)/a \mid g(x)$

$\because a \in F^*$

$\therefore f(x) \mid g(x)$

15.18证明$f(x)=x^4+1\in Q[x]$，α为$f(x)$的根，
 则$Q(\alpha)$为$f(x)$的根域。

证明：∵ α为$f(x)$的根

∴ $\alpha^4+1=0$

∴ $f(x)= x^4-\alpha^4=(x-\alpha)(x+\alpha)(x^2+\alpha^2)$

∵ $\alpha^2=-(-1)\alpha^2=-\alpha^6$

∴ $x2+\alpha^2=(x-\alpha^3)(x+\alpha^3)$

即$f(x)=(x-\alpha)(x+\alpha)(x-\alpha^3)(x+\alpha^3)$

∴ $f(x)$能在$Q(\alpha)$上分解为一次因子的乘积

∵ $f(x)$的根域是包含α的Q的最小扩域，而 $Q(\alpha)$为包含α和Q的最小域。

∴$Q(\alpha)$为$f(x)$的根域

15.20　F为域，char $F=p$, α是$x^p-\alpha \in F[x]$的一个根，问$F[\alpha]$是否是$x^p-\alpha$的根域？

解：　$F[\alpha]$是$x^p-\alpha$的根域。

∵ α是$x^p-\alpha \in F[x]$的一个根

∴ $\alpha^p-\alpha=0$

即$\alpha^p ＝ \alpha$

∵ F为域且char F=p

∴p为素数或0

当p=0时， $f(x)=x^p-\alpha=1-\alpha$， 与题意矛盾

∴ p为素数

则$(x-\alpha)^p=x^p-\alpha^p=x^p-\alpha$

即$x^p-\alpha$可在$F(\alpha)$内分解为一次因子的乘积，而$F(\alpha)$为包含α的F的最小扩域，所以$F(\alpha)$为$x^p-\alpha$的根域。

15.22 求下列多项式的根域及扩张次数：

1）Q上多项式x^6-6;

2）Z_5上多项式x^3+4x+3

解：1） x^6-6为Q上不可约多项式，

由 $x^6-6＝0$得

$x=\sqrt[6]{6}(\cos\frac{k\pi}{3}+i\sin\frac{k\pi}{3})$ k=0,1,2,3,4,5

∴ x^6-6的根域为Q（$\sqrt[6]{6},\sqrt{3}i$)。

且[Q（$\sqrt[6]{6},\sqrt{3}i$)：Q]=6×2=12

2)根域为$Z_5[x]/x^3+4x+3$,扩张次数为3。

∵ x^3+4x+3在Z_5 [x]上不可约。

∴记Z_5 [x] /x^3+4x+3 为K， 则x^3+4x+3 在K上有根， x^3+4x+3 的根域包含K。记x^3+4x+3在K中的根为α。

则$\alpha^{125}-\alpha=0$， 由前面16题结论可得

$x^3+4x+3 \mid x^{125}-x$

而$x^{125}-x$的所有解构成域K

∴ x^3+4x+3的所有解都在K内

∴K为x^3+4x+3的根域

15.24（2）解：$GF(9)=GF(3^2)=Z3x/(x2+1)=\{ax+b|a,b\epsilon Z3\}$

+	0	1	2	X	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	X	X+1	X+2	2x	2x+1	2x+2
1	1	2	0	X+1	X+2	X	2x+1	2x+2	2x
2	2	0	1	X+2	X	X+1	2x+2	2x	2x+1
x	X	X+1	X+2	2x	2x+1	2x+2	0	1	2
x+1	X+1	X+2	X	2x+1	2x+2	2x	1	2	0
x+2	X+2	X	X+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	X	X+1	X+2
2x+1	2x+1	2x+2	2x	1	2	0	X+1	X+2	x
2x+2	2x+2	2x	2x+1	2	0	1	X+2	x	X+1

*	0	1	2	X	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	X	X+1	X+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	X+2	X+1
x	0	X	2x	2	X+2	2x+2	1	X+1	2x+1
x+1	0	X+1	2X+2	X+2	2x	1	2x+1	2	x
x+2	0	X+2	2X+1	2x+2	1	x	X+1	2x	2
2x	0	2x	x	1	2x+1	X+1	2	2X+2	X+2
2x+1	0	2x+1	X+2	X+1	2	2x	2X+2	X	1
2x+2	0	2x+2	x+1	2X+1	x	2	X+2	1	2x

(3) 解： GF(8)=GF(2^3)= Z2x/(x3+x2+1)=ax2+bx+ca,b,cϵZ2}

+	0	1	x	X+1	X^2	X^2+1	X^2+x	X^2+x+1
0	0	1	x	X+1	X^2	X^2+1	X^2+x	X^2+x+1
1	1	0	X+1	x	X^2+1	X^2	X^2+x+1	X^2+x
x	x	X+1	0	1	X^2+x	X^2+x+1	X^2	X^2+1
X+1	X+1	x	1	0	X^2+x+1	X^2+x	X^2+1	X^2
X^2	X^2	X^2+1	X^2+x	X^2+x+1	0	1	x	X+1
X^2+1	X^2+1	X^2	X^2+x+1	X^2+x	1	0	X+1	x
X^2+x	X^2+x	X^2+x+1	X^2	X^2+1	X+1	X+1	0	1
X^2+x+1	X^2+x+1	X^2+x	X^2+1	X^2	x	x	1	0

*	0	1	x	X+1	X^2	X^2+1	X^2+x	X^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	X+1	X^2	X^2+1	X^2+x	X^2+x+1
x	0	x	X^2	X^2+x	X^2+1	X^2+x+1	1	X+1
X+1	0	X+1	X^2+x	X^2+1	1	x	X^2+x+1	X^2
X^2	0	X^2	X^2+1	1	X^2+x+1	X+1	x	X^2+x
X^2+1	0	X^2+1	X^2+x+1	x	X+1	X^2+x	X^2	1
X^2+x	0	X^2+x	1	X^2+x+1	x	X^2	X+1	X^2+1
X^2+x+1	0	X^2+x+1	X+1	X^2	X^2+x	1	X^2+1	x