域

1. $x^2+4\in\mathbb{Z}_5[x]$, 将其分解为不可约因式的积.

2. 试问x^3+2x+3是$\mathbb{Q}[x]$中的不可约多项式吗? 作为$\mathbb{Z}_5[x]$中的多项式是否不可约? 若可约, 试将它分解为不可约因式的积.

3. 试在$\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}_5$内分解多项式: (1) x^2+1; (2) x^2+x+1.

4. 求x^5-3x^3+2x在$\mathbb{Z}_5$内的根.

5. 证明$\forall a\in\mathbb{Z}_p$(p为素数), x^p+a在$\mathbb{Z}_p[x]$中都可约.

6. 求所有的奇素数p, 使得在$\mathbb{Z}_p[x]$中有$x+2\mid x^4+x^3+x^2-x+1$.

7*. 设F是一个域, $f(x),g(x)\in F[x]$. 证明

$$N=\{u(x)f(x)+v(x)g(x)|u(x),v(x)\in F[x]\}$$

是$F[x]$的理想. 又若deg$f(x)\neq$deg$g(x)$, $N\neq F[x]$, 则$f(x),g(x)$至少有一个是可约的.

8. 设$f(x)\in\mathbb{Z}[x]$. 证明若$f(x)$作为$\mathbb{Z}_p[x]$中多项式不可约, 则$f(x)$为$\mathbb{Q}[x]$中多项式也不可约.

9. 设域F中只有q个元素$a_1,a_2,\ldots,a_q$. 求证在$F[x]$中有

$$x^q-x=(x-a_1)(x-a_2)\cdots(x-a_q).$$

10. 验证x^3-x在$\mathbb{Z}_6$中有6个根.

11. 列出$\mathbb{Z}_2[x]$中次数不超过4的所有不可约多项式.

12. 列出$\mathbb{Z}_3[x]$中所有2次不可约多项式.

13. 设R是无零因子环且只有有限个元素. 证明R是域.

14. p为素数时, 证明$f(x)=x^4+1\in\mathbb{Z}_p[x]$是可约多项式.

15. 设p是素数, 证明:

$$\left\{\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}\middle|\, a,b,c\in\mathbb{Z}_p\right\}$$

是p^3阶非交换群(运算为矩阵乘法).

16. 构造4阶有限域.

17. 构造9阶有限域.

18. 构造16阶有限域.

19. 设有限域F的特征为p(p为素数), 证明$\forall a,b\in F$, 恒有$(a+b)^{p^n}=a^{p^n}+b^{p^n}$.

20. 设有限域GF(2^8)为$\mathbb{Z}_2[x]/\langle x^8+x^4+x^3+x+1\rangle$. 一个8比特的二进制数$b_7b_6b_5b_4b_3b_2b_1b_0$可以用GF($2^8$)中的元素$b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0$来表示. 请计算十六进制数'3A'和'D6'在GF(2^8)中的乘积. (结果用十六进制数表示)