# 域

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

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

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.

**解**:

$\mathbb{Q}[x]$: $x^3+2x+3=(x^3+1)+2(x+1)=(x+1)(x^2-x+1)+2(x+1)=(x+1)(x^2-x+3)$.

$\mathbb{Z}_5[x]$: $x^3-2x+3=(x+1)(x^2-x+3)=(x+1)(x^2+4x+3)=(x+1)^2(x+3)$

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

**解**:

(1) $\mathbb{Q},\mathbb{R}$上无法分解, $\mathbb{C}$上分解为$(x+i)(x-i)$, $\mathbb{Z}_5$上分解为$(x+2)(x+3)$.

(2) $\mathbb{Q},\mathbb{R},\mathbb{Z}_5$上无法分解, $\mathbb{Q}$上分解为$\left(x+\frac{1+\sqrt{-3}}{2}\right)\left(x+\frac{1-\sqrt{-3}}{2}\right)$

4. 求$x^5-3x^3+2x$在$\mathbb{Z}_5$内的根.

**解**: 把0,1,2,3,4依次代入, 计算得0,1,4是根.

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.

**证明**: $\forall a\in\mathbb{Z}_p, a^p=a$, 所以$x^p+a=x^p+a^p=(x+p)^a$.

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

**解**: 设$f(x)=x^4+x^3+x^2-x+1$. $x+2\mid f(x)$说明$x=-2$是$f(x)$在$\mathbb{Z}_p$上的根. $f(-2)=15\pmod p=0$, 于是$p|15$, 所以$p=3$或5.

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$\mathrm{deg}f(x)\neq\mathrm{deg}g(x), N\neq F[x]$, 则$f(x),g(x)$至少有一个是可约的.

**证明**: $\forall u_1(x),u_2(x),v_1(x),v_2(x),h(x)\in F[x]$, 有

$$(u_1f+v_1g)\pm(u_2f+v_2g)=(u_1\pm u_2)f+(v_1\pm v_2)g$$
$$h(u_1f+v_1g)=(hu_1)f+(hv_1)g$$

所以$N$是$F[x]$的理想.

若$f(x),g(x)$均不可约, 由$\mathrm{deg}f(x)\neq\mathrm{deg}g(x)$可知$(f(x),g(x))=1$. 于是$\exists u_0(x),v_0(x)\in$

$F[x]$使得$1=u_0(x)f(x)+v_0(x)g(x)\in N$, 此时$N=F[x]$, 矛盾. 因此$f(x),g(x)$至少有一个可约.

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.

**证明**: 若$f(x)$在$\mathbb{Q}[x]$中可约, 那么在$\mathbb{Z}[x]$中可约, 那么在$\mathbb{Z}_p[x]$中也可约.

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

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

**证明**: $\forall a\in F, a^q=a$即$a^q-a=0$, 于是任意$a\in F$都是方程$x^q-x=0$的解, 即$x^q-x=0$至少有$q$个解; 而$x^q-x=0$ 至多有$q$个解, 因此$x^q-x=0$恰好有$q$个解, 且这$q$个解就是$F$中的所有元素$a_i$.

10. 验证$x^3-x$在$\mathbb{Z}_6$中有6个根.

**证明**: 分别验证0,1,2,3,4,5.

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

**解**: 1次: $x,\quad x+1$;

2次: $x^2+x+1$;

3次: $x^3+x^2+1, \quad x^3+x+1$;

4次: $x^4+x+1, \quad x^4+x^3+1, \quad x^4+x^3+x^2+x+1$.

12. 列出$\mathbb{Z}_3[x]$中所有2次不可约多项式.

**解**: $\pm(x^2+1), \quad \pm(x^2+x-1), \quad \pm(x^2-x-1)$

13*. 设$R$是无零因子环且只有有限个元素. 证明$R$是域.

**解**: 无零因子⇒乘法满足消去律. $R* = R \setminus \{0\}$对乘法构成满足消去律的有限半群, 根据群习题2可知, $R^*$对乘法构成群, 因此$R$是有限体.

★ Wedderburn定理: 有限体是域.

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

**证明**: $p=2$时, $x^4+1=(x+1)^4$;

$p \equiv 1 \pmod 4$时, $\left(\frac{1}{p}\right) = 1$, 即$\exists \alpha \in \mathbb{Z}_p$使得$\alpha^2 = 1 \pmod p$, 此时$x^4+1 = x^4-\alpha^2 = (x^2+\alpha)(x^2-\alpha)$;

$p \equiv 3 \pmod 4$时, $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = -\left(\frac{2}{p}\right)$, 说明2不是$p$的二次剩余时, -2一定是$p$的二次剩余; -2不是$p$的二次剩余时, 2一定是$p$的二次剩余.

2是$p$的二次剩余时, $\exists \beta \in \mathbb{Z}_p$使得$\beta^2 = 2 \pmod p$, 此时$x^4+1 = (x^2+1)-2x^2 = (x^2+\beta x+1)(x^2-\beta x+1)$;

-2是$p$的二次剩余时, $\exists \gamma \in \mathbb{Z}_p$使得$\gamma^2 = -2 \pmod p$, 此时$x^4+1 = (x^2-1)+$

$2x^2 = (x^2 + \gamma x - 1)(x^2 - \gamma x - 1)$;

综上, $p$为素数时$f(x) \in \mathbb{Z}_p[x]$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).

**证明**: 易证构成非交换群, $a, b, c$取值各有$p$个, 故集合中有$p^3$个矩阵.

16. 构造4阶有限域.

**解**: $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

17. 构造9阶有限域.

**解**: $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$. (答案不唯一, 可取$\mathbb{Z}_3[x]$中其他的2次不可约多项式)

18. 构造16阶有限域.

**解**: $\mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$. (答案不唯一, 可取$\mathbb{Z}_2[x]$中其他的4次不可约多项式)

19. 设有限域$F$的特征为$p$($p$为素数), 证明$\forall a,b\in F$, 恒有$(a+b)^{p^n}=a^{p^n}+b^{p^n}$.
**证明**: 交叉项的系数均可被$p$整除.

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)

**解**: '3A'=$(00111010)_2=x^5+x^4+x^4+x$, 'D6'=$(11010110)_2=x^7+x^6+x^4+x^2+x$.

$(x^5+x^4+x^4+x)(x^7+x^6+x^4+x^2+x) \pmod 2 = x^{12}+x^7+x^5+x^4+x^3+x^2$,

$$\begin{aligned}
&x^{12}+x^7+x^5+x^4+x^3+x^2 \pmod{x^8+x^4+x^3+x+1} \pmod 2\\
=&x^{12}+x^7+x^5+x^4+x^3+x^2-(x^4+1)(x^8+x^4+x^3+x+1) \pmod 2\\
=&x^4+x^2+x+1.
\end{aligned}$$

$x^4+x^2+x+1=(00010111)_2=$'17'.