第三章　域　论

§1　子域与扩域

1. 证明子域的交仍是子域.

证明　设 $\{F_i\}_{i\in I}$ 是域 F 的一族子域. 显然 $1\in\bigcap_{i\in I}F_i$. 其次, 设 $a,b\in\bigcap_{i\in I}F_i$. 于是, $a,b\in F_i$, $\forall i\in I$, 从而, $a-b,ab\in F_i$, $\forall i\in I$; 当 $a\neq 0$ 时, $a^{-1}\in F_i$, $\forall i\in I$. 因此 $a-b,ab\in\bigcap_{i\in I}F_i$; 当 $a\neq 0$ 时, $a^{-1}\in\bigcap_{i\in I}F_i$. 所以 $\bigcap_{i\in I}F_i$ 是域 F 的子域.

2. 设域 F 的特征为 p, 对于任意的 $a,b\in F$, 证明:

(1) $(a+b)^{p^n}=a^{p^n}+b^{p^n}$;

(2) $(a-b)^{p-1}=\sum_{i=0}^{p-1}a^ib^{p-1-i}$.

证明 (1) 由于域是整环, 根据第二章§5 习题第 12 题, 我们有

$$(a+b)^{p^n}=a^p+b^p=a^{p^n}+b^{p^n}.$$

(2) 当 $a=b$ 时, 我们有

$$\sum_{i=0}^{p-1}a^ib^{p-1-i}=pa^{p-1}=0.$$

因此 $(a-b)^{p-1}=\sum_{i=0}^{p-1}a^ib^{p-1-i}$. 当 $a\neq b$ 时, 我们有

$$(a-b)\sum_{i=0}^{p-1}a^ib^{p-1-i}=a^p-b^p=(a-b)^p.$$

因为 $a-b\neq 0$, 根据消去律, 由上式可得 $(a-b)^{p-1}=\sum_{i=0}^{p-1}a^ib^{p-1-i}$.

3. 证明 $\mathbb{Q}$ 和 $\mathbb{Z}_p$ (p 是素数) 都是素域.

证明　设 F 是 $\mathbb{Q}$ 的子域. 于是, $1\in F$, 从而, $\mathbb{Z}\subseteq F$. 由于 F 是域, 因此当 $m,n\in\mathbb{Z}$ 且 $n\neq 0$ 时, $\dfrac{m}{n}\in F$, 从而, $F=\mathbb{Q}$. 这就表明 $\mathbb{Q}$ 是素域.

设 F 是 $\mathbb{Z}_p$ 的子域. 于是, 加群 F 是加群 $\mathbb{Z}_p$ 的子群, 从而, $|F|\,|\,p$. 由 F 是域可知, $|F|\geq 2$. 因为 p 是素数, 所以 $|F|=p$, 从而, $F=\mathbb{Z}_p$. 这就表明 $\mathbb{Z}_p$ 是素域.

4. 在 $\mathbb{Q}(\sqrt[3]{2})$ 中, 求 $1+\sqrt[3]{2}+\sqrt[3]{4}$ (关于乘法) 的逆元.

证明　由于 $(1+\sqrt[3]{2}+\sqrt[3]{4})(\sqrt[3]{2}-1)=(\sqrt[3]{2})^3-1=1$, 因此 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆元为 $\sqrt[3]{2}-1$.

5. 证明 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

证明　显然 $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, 因此 $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$. 另一方面, 由于 $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})=1$, 因此 $\sqrt{3}-\sqrt{2}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 这样一来, 注意到

$$\sqrt{3}=\frac{1}{2}((\sqrt{3}+\sqrt{2})+(\sqrt{3}-\sqrt{2})),\ \sqrt{2}=\frac{1}{2}((\sqrt{3}+\sqrt{2})-(\sqrt{3}-\sqrt{2})),$$

可以断言 $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, 从而, $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 所以

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

6. 设 E 是域 F 的扩域且 $[E:F]$ 是素数, 证明: F 与 E 之间没有非平凡的中间域.

证明 假设 L 是 F 与 E 的中间域. 根据定理 1.9, $[E:F]=[E:L][L:F]$. 由于 $[E:F]$

是素数, 因此$[E:L]=1$或$[L:F]=1$, $L=E$ 或$L=F$. 这就是说, F 与E之间没有非平凡的中间域.

7. 设E是域F的扩域且$[E:F]$是素数, $\alpha\in E\setminus F$, 证明: $E=F(\alpha)$.

证明 由$\alpha\in E\setminus F$可知, $F(\alpha)$是F与E的中间域且$F\neq F(\alpha)$. 因为$[E:F]$是素数, 根据上题, F 与E之间没有非平凡的中间域. 所以$E=F(\alpha)$.

§2 单扩域

1. 证明: $\mathbb{Q}(i)\cong\mathbb{Q}[x]/(x^2+1)$.

证明 这里给出两种证法.

证法一:定义$\mathbb{Q}[x]$到$\mathbb{Q}[i]$的映射φ如下:

$$\varphi(f(x))=f(i),\ \forall f(x)\in\mathbb{Q}[x].$$

显而易见, φ是环$\mathbb{Q}[x]$到环$\mathbb{Q}[i]$的满同态, 从而, $\mathbb{Q}(i)\cong\mathrm{Ker}(\varphi)$. 此外, 我们有

$$f(x)\in\mathrm{Ker}(\varphi)\Leftrightarrow f(i)=0\Leftrightarrow f(i)=f(-i)=0$$

$$\Leftrightarrow x^2+1\mid f(x)\Leftrightarrow f(x)\in(x^2+1),\ \forall f(x)\in\mathbb{Q}[x],$$

从而, $\mathrm{Ker}(\varphi)=(x^2+1)$. 所以$\mathbb{Q}(i)\cong\mathbb{Q}[x]/(x^2+1)$.

证法二:令$N=(x^2+1)$, 定义$\mathbb{Q}[i]$到$\mathbb{Q}[x]/(x^2+1)$的映射φ如下: 对于任意的$a+bi\in\mathbb{Q}[i]$(其中$a,b\in\mathbb{Q}$),

$$\varphi(a+bi)=a+bx+N.$$

显然, φ是域$\mathbb{Q}[i]$到域$\mathbb{Q}[x]/(x^2+1)$的单同态. 其次, 对于任意的$f(x)\in\mathbb{Q}[x]$, 根据带余出发, 存在$q(x),r(x)\in\mathbb{Q}[x]$, 使得

$$f(x)=q(x)(x^2+1)+r(x),$$

其中, $r(x)=0$或者$\deg(r(x))<2$. 不妨设$r(x)=c+dx$, 其中$c,d\in\mathbb{Q}$. 于是,

$$\varphi(c+di)=c+dx+N=f(x)+N.$$

因此φ是域$\mathbb{Q}[i]$到域$\mathbb{Q}[x]/(x^2+1)$的同构. 所以$\mathbb{Q}(i)\cong\mathbb{Q}[x]/(x^2+1)$.

2. 计算$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$.

解 根据命题 1.7, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$. 显而易见, $\sqrt{2}$是$\mathbb{Q}$上的代数元, 其极小多项式为x^2-2. 这样, 根据定理 2.6, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. 同理, $\sqrt{3}$是$\mathbb{Q}(\sqrt{2})$上的代数元, 其极小多项式为x^2-3. $[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$这样一来, 根据定理 1.9, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\times2=4$.

3. 设E是域F的扩域, $E=F(u)$, u在F上是代数的且其极小多项式的次数为奇数, 证明: $E=F(u^2)$.

证明 显然$F(u^2)\subseteq E$. 设u在F上是代数的且其极小多项式的次数为$2n+1$(n为非负整数). 于是, $[E:F]=2n+1$. 若$n=0$, 则$[E:F]=1$, 从而, $E=F$. 由此可

见, $E=F(u^2)$. 不妨假设 $n>0$. 于是, $1,u,u^2,\cdots,u^{2n}$ 是 F 上的向量空间 E 的一个基. 显然 $1,u^2,,\cdots,u^{2n-2},u^{2n}$ 是 F 上的向量空间 $F(u^2)$ 中 $n+1$ 个线性无关的向量, 从而, $[F(u^2):F]\geq n+1$. 根据定理 1.9, $[E:F]=[E:F(u^2)][F(u^2):F]$. 这样, 由 $[E:F]=2n+1$ 和 $[F(u^2):F]\geq n+1$ 可知 $[E:F(u^2)]<2$, 从而, $[E:F(u^2)]=1$. 所以 $E=F(u^2)$.

总之, $E=F(u^2)$.

4. 证明: $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$ 上是代数的, 其极小多项式的次数为 4.

证明 根据 §1 习题第 5 题, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. 根据第 2 题, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$, 即 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$. 这样一来, 根据定理 2.6, $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$ 上是代数的, 其极小多项式的次数为 4.

注 $\sqrt{2}+\sqrt{3}$ **的极小多项式为** $m(x)=x^4-10x^2+1$.

5. 设 E 是域 F 的有限扩域, $\alpha\in E$ 是 F 上的代数元, 其极小多项式的次数为 n, 证明 $n\,|\,[E:F]$.

证明 由于 E 是域 F 的有限扩域, 因此 $[E;F]<\infty$. 根据定理 1.9, 我们有

$$[E:F]=[E:F(\alpha)][F(\alpha):F].$$

由于 α 的极小多项式的次数为 n, 根据定理 2.6, $[F(\alpha):F]=n$. 这样, 根据上式可以断言, $n\,|\,[E:F]$.

§3 代数扩域

1. 设 E 是域 F 的代数扩域, $\alpha\in E$, $\alpha\neq 0$, 证明: 存在 $f(x)\in F[x]$ 使 $\alpha^{-1}=f(\alpha)$.

证明 由于 E 是域 F 的代数扩域, 因此 α 在 F 上是代数的. 这样一来, 根据定理 2.6, $F(\alpha)=F[\alpha]$. 显然, $\alpha^{-1}\in F(\alpha)$. 所以存在 $f(x)\in F[x]$ 使 $\alpha^{-1}=f(\alpha)$.

2. 设 E 是域 F 的扩域, $\alpha,\beta\in E$ 是 F 上的代数元, 证明: $\alpha\pm\beta,\alpha\beta,\alpha\beta^{-1}$ ($\beta\neq 0$) 均为 F 上的代数元.

证明 由于 α 是 F 上的代数元, 因此 $[F(\alpha),F]<\infty$. 由于 β 是 F 上的代数元, 因此 β 是 $F(\alpha)$ 上的代数元, 从而, $[F(\alpha)(\beta),F(\alpha)]<\infty$. 这样一来, 根据定理 1.9, $[F(\alpha)(\beta),F]<\infty$. 此外, 根据命题 1.7, $F(\alpha,\beta)=F(\alpha)(\beta)$. 所以 $[F(\alpha,\beta),F]<\infty$. 由于 $\alpha\pm\beta,\alpha\beta\in F(\alpha,\beta)$, 根据定理 3.2, $\alpha\pm\beta$ 和 $\alpha\beta$ 为 F 上的代数元. 同理, 当 $\beta\neq 0$ 时, $\alpha\beta^{-1}\in F(\alpha,\beta)$, 因此 $\alpha\beta^{-1}$ 为 F 上的代数元..

3. 设 E 是域 F 的有限扩域, 证明: 存在 E 中有限多个元素 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 使得 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

证明 设 E 是域 F 的 n (n 为正整数) 次扩域 (参看定义 1.8). 于是 E 是域 F 上的 n 维向量空间. 任取 E 的一个基 $\alpha_1,\alpha_2,\cdots,\alpha_n$, 则 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

§4　分裂域

1. 证明: $\mathbb{Q}(\sqrt{2})$ 是多项式 x^2-2 在 $\mathbb{Q}$ 上的分裂域.

证明　我们已经知道, $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{Q}$ 的一个扩域, $\pm\sqrt{2}$ 是多项式 x^2-2 的仅有的两个根, 并且 $\pm\sqrt{2}\in\mathbb{Q}(\sqrt{2})$. 显然还有 $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(\sqrt{2},-\sqrt{2})$, 所以 $\mathbb{Q}(\sqrt{2})$ 是多项式 x^2-2 在 $\mathbb{Q}$ 上的分裂域.

2. 证明: 多项式 x^4+1 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}$ 的单扩域 $\mathbb{Q}(\alpha)$, 其中 α 是 x^4+1 的一个根.

证明　我们有

$$x^4+1=(x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(1-i))(x-\frac{\sqrt{2}}{2}(-1+i))(x-\frac{\sqrt{2}}{2}(-1-i)),$$

其中 i 表示 -1 的一个平方根. 令

$$\alpha=\frac{\sqrt{2}}{2}(1+i),\ \alpha_2=\frac{\sqrt{2}}{2}(1-i)),\ \alpha_3=\frac{\sqrt{2}}{2}(-1+i),\ \alpha_4=\frac{\sqrt{2}}{2}(-1-i).$$

于是, α 是 $\mathbb{Q}$ 上的代数元. 显而易见, x^4+1 是 α 在 $\mathbb{Q}$ 上的极小多项式. 因此 $\mathbb{Q}(\alpha)$ 是 $\mathbb{Q}$ 上的四维向量空间, 并且 $1,\alpha,\alpha^2,\alpha^3$ 是 $\mathbb{Q}(\alpha)$ 的基. 由于

$$\alpha_2=-\alpha^3\in\mathbb{Q}(\alpha),\ \alpha_3=\alpha^3\in\mathbb{Q}(\alpha),\ \alpha_4=-\alpha\in\mathbb{Q}(\alpha),$$

因此 $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha,\alpha_2,\alpha_3,\alpha_4)$. 所以多项式 x^4+1 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}$ 的单扩域 $\mathbb{Q}(\alpha)$.

3. 设 $f(x)$ 是域 F 上的 n（>0）次多项式, E 是 $f(x)$ 在域 F 上的分裂域, 证明: $[E:F]\le n!$.

证明　不妨设 $f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. 对于每一个 $i\in\{1,2,\cdots,n-1\}$, 令

$$q_i(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_i),\ f_i(x)=(x-\alpha_{i+1})(x-\alpha_{i+2})\cdots(x-\alpha_n).$$

于是, $f(x)=q_i(x)f_i(x)$, $1\le i\le n-1$. 显然, 对于每一个 $i\in\{1,2,\cdots,n-1\}$, $f(x)$ 和 $q_i(x)$ 都是 $F(\alpha_1,\alpha_2,\cdots,\alpha_i)$ 上的多项式. 这样, 由 $f(x)=q_i(x)f_i(x)$ 可知 $f_i(x)$ 也是 $F(\alpha_1,\alpha_2,\cdots,\alpha_i)$ 上的多项式. 将 α_{i+1} 在 $F(\alpha_1,\alpha_2,\cdots,\alpha_i)$ 上的极小多项式记做 $m_{i+1}(x)$. 由 $f_i(\alpha_{i+1})=0$ 可知 $\deg(m_{i+1}(x))\le n-i$. 再将 α_1 在 F 上的极小多项式记做 $m_1(x)$. 由 $f(\alpha_1)=0$ 可知, $\deg(m_1(x))\le n$. 这样一来, 根据定理 1. 9, 我们有

$$\begin{aligned}&[E;F]=[F(\alpha_1,\alpha_2,\cdots,\alpha_n):F]\\&=[F(\alpha_1):F]\cdot[F(\alpha_1,\alpha_2):F(\alpha_1)]\cdot\cdots\cdot[F(\alpha_1,\alpha_2,\cdots\alpha_n):F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})]\\&=\deg(m_1(x))\cdot\deg(m_2(x))\cdot\cdots\cdot\deg(m_n(x))\\&\le n\cdot(n-1)\cdot\cdots\cdot2\cdot1=n!.\end{aligned}$$

§5　有限域

1. 证明: 四元域不能同构于八元域的子域.

证明　设 E 是八元域, F 是 E 的子域. 若 F 同构于四元域, 则 F 也是四元域, 并且

$[E:F]\geq 2$. 任取 $\alpha\in E\setminus F$, 则 $1,\alpha$ 线性无关. 令 $S=\{a+b\alpha\mid a,b\in F\}$. 于是, 一方面, 由于 $S\subseteq E$, 因此 S 至多有 8 个不同元素; 另一方面, 显然 S 有 16 个不同元素. 这个矛盾表明, 四元域不能同构于八元域的子域.

2. 设 F 是元素个数为 p^n 的有限域, 证明: F 中每个元素都有唯一的 p 次根.

证明 将 F 的素子域记做 K. 于是, $K\cong\mathbb{Z}_p$. 根据定理 5.3 和定理 5.4, F 就是多项式 $f(x)=x^{p^n}-x\in K[x]$ 的所有的根组成的集合. 因此 $(\alpha^{p^{n-1}})^p=\alpha$, $\forall\alpha\in F$. 这就是说, F 中每个元素 α 都以 $\alpha^{p^{n-1}}$ 为自己的 p 次根. 假设 β 也是 α 的 p 次根, 则

$$(\beta-\alpha^{p^{n-1}})^p=\beta^p-(\alpha^{p^{n-1}})^p=0,$$

从而, $\beta=\alpha^{p^{n-1}}$. 所以 α 的 p 次根是唯一的.

3. 设有限域 F 的特征为 p 且对于任意的 $a\in F$ 都有 $a^p=a$, 证明: $F\cong\mathbb{Z}_p$.

证明 将 F 的素子域记做 K. 于是, $K\cong\mathbb{Z}_p$, 并且 $|F|=p^n$, 其中 n 为正整数. 考察多项式 $f(x)=x^p-x\in K[x]$: 由命题 5.2 的证明可知, $f(x)$ 在 K 上的分裂域是 p 元域. 由于对于任意的 $a\in F$ 都有 $a^p=a$, 因此任意的 $a\in F$ 都是 $f(x)$ 的根, 从而, $n=1$. 所以 $F=K$, 从而, $F\cong\mathbb{Z}_p$.

4. 设 F 是元素个数为 q 的有限域, $f(x)\in F[x]$, 证明: $(f(x))^q=f(x^q)$.

证明 不妨设 F 的特征为 p, $q=p^m$, $f(x)=\sum_{k=0}^{n}a_kx^k$. 于是, $a^q=a$, $\forall a\in F$. 下面我们对 n 施行数学归纳法.

当 $n=0$ 时, 显然有 $(f(x))^q=f(x^q)$.

假设当 $n=r-1$ (r 为正整数) 时有 $(f(x))^q=f(x^q)$. 现在设 $n=r$. 根据二项式定理 (即第二章 §1 命题 1.3(7)), 我们有

$$(f(x))^q=((\sum_{k=0}^{r-1}a_kx^k)+a_rx^r)^q=\sum_{j=0}^{q}C_q^j(\sum_{k=0}^{r-1}a_kx^k)^{q-j}(a_rx^r)^j.$$

显然, 当 $0<j<q$ 时, $p\mid C_q^j$, 从而, $C_q^j(\sum_{k=0}^{r-1}a_kx^k)^{q-j}(a_rx^r)^j=0$. 这样一来, 根据归纳假设, 我们有

$$\begin{aligned}(f(x))^q&=(\sum_{k=0}^{r-1}a_kx^k)^q+(a_rx^r)^q=\sum_{k=0}^{r-1}a_k(x^q)^k+a_r^q(x^q)^r\\&=\sum_{k=0}^{r-1}a_k(x^k)^q+a_r(x^q)^r=f(x^q).\end{aligned}$$