第 8 章 域

有理数域，实数域，复数域是三个最常见的域. 在本章中，我们将从环出发，介绍域的基本概念，进而讨论域的代数扩张，而后的正规扩张与可分扩张是域扩张的重要内容. 然后，作为本章乃至近世代数学的核心内容，我们将介绍著名的 Galois 基本定理，解释域扩张与自同构群之间的紧密联系. 最后，我们简要介绍有限域的相关内容.

8.1 域上的多项式

域的概念产生于方程求解，特别是多项式方程求解. 在本节，我们首先介绍域上多项式的相关性质.

定义 8.1.1 F 是一个域，若$a_n,\cdots,a_0\in F, a_n\neq 0$,则称 $f(x)=a_nx^n+\cdots+a_1x+a_0$为**域 F 上的一元多项式**或**多项式**，称n为该多项式的**次数**，记为 $\deg f=n$.

显然，若记$F[x]=\{a_nx^n+\cdots+a_1x+a_0|a_n,\cdots,a_0\in F\}$，则$F[x]$构成环，我们称之为 **$F$ 上的一元多项式环**或**多项式环**.

例 8.1.1 F 是一个域，则$F[x]$是交换整环.

定义 8.1.2 若 F 上的多项式 $f(x)$等于 F 上其它两个非零次多项式 $g(x),h(x)$的乘积，即 $f(x)=g(x)h(x)$，且 $\deg h$, $\deg h$ 均不为 0，则称多项式 $f(x)$是**可约的**, $g(x),h(x)$称为 $f(x)$的**因式**或 $g(x)$,$h(x)$整除 $f(x)$；否则，称之为**不可约的**.

例 8.1.2 在有理数域$\mathbf{Q}$，实数域$\mathbf{R}$下，x^2+1是不可约的，但在复数域$\mathbf{C}$下，$x^2+1=(x+i)(x-i)$是可约的；在有限域$\mathbf{Z}_2$下，$x^2+1=(x+1)^2$是可约的.

定理 8.1.1（带余除法） F 是一个域，$F[x]$是 F 上的一元多项式环，

(1)设 $f(x),g(x)\in K[x]$， $f(x)\neq 0$，则存在唯一的 $q(x),r(x)\in K[x]$，使

$$g(x)=q(x)f(x)+r(x),$$

其中 $r(x)=0$ 或 $\deg r(x)<\deg f(x)$. $q(x)$和 $r(x)$分别称为用 $f(x)$去除 $g(x)$所得的**商式**和**余式**.

(2) $F[x]$是 Euclid 环.

证明 (1) 存在性. 设

$$f(x)=a_nx^n+a_1x^{n-1}+\cdots+a_0\quad(a_0\neq 0).$$

如果 $n=0$，则 $f(x)=a_0$，取 $q(x)=\dfrac{1}{a_0}g(x)$, $r(x)=0$ 即可.

下面假定 $n>0$. 对 $g(x)$的次数做数学归纳法.

如果 $g(x)=0$ 或 $\deg g(x)<n$，则令 $q(x)=0$, $r(x)=g(x)$即满足要求. 设 $\deg g(x)<m$ 时，命题正确，则当 $\deg g(x)=m$ 时，有

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_m\quad(b_0\neq 0).$$

令

$$g_1(x)=g(x)-\frac{b_0}{a_0}x^{m-n}f(x).$$

若 $g_1(x)=0$，则取 $q(x)=\frac{b_0}{a_0}x^{m-n}$，$r(x)=0$. 否则，因 $\deg g_1(x)<m$，按归纳假设，存在 $q_1(x),r_1(x)\in K[x]$，使得

$$g_1(x)=q_1(x)f(x)+r_1(x),$$

这里 $r_1(x)=0$ 或 $\deg r_1(x)<\deg f(x)$. 现令

$$q(x)=\frac{b_0}{a_0}x^{m-n}+q_1(x),\ r(x)=r_1(x),$$

则显然有 $g(x)=q(x)f(x)+r(x)$.

唯一性. 设 $\tilde{q}(x),\tilde{r}(x)$ 也满足命题要求，那么

$$q(x)f(x)+r(x)=\tilde{q}(x)f(x)+\tilde{r}(x),$$
$$[q(x)-\tilde{q}(x)]f(x)=\tilde{r}(x)-r(x).$$

比较两边的次数，即可知 $\tilde{r}(x)-r(x)=0$，$q(x)-\tilde{q}(x)=0$.

(2)令 $\delta(f(x))=2^{\deg f(x)}$，由于 $\deg r(x)<\deg f(x)$，则 $\delta(r(x))<\delta(f(x))$，故 $F[x]$ 是 Euclid 环.

推论 F 是一个域，$F[x]$ 是主理想整环，因而也是唯一析因环.

证明：因 $F[x]$ 是 Euclid 环，结合 7.3 节相应结论可得.

定理 8.1.1 相当于初等数论中的整数的带余除法，又称为多项式的欧几里得除法. 我们知道，在初等数论中可以用辗转相除法求两个整数的最大公因子，这种方法同样可以用于求两个多项式的最大公因子.

这种求两个多项式最大公因式的方法称为**多项式的辗转相除法**或**广义欧几里得除法**. 类似于整数中的辗转相除法，我们可以利用回代过程将 $(f(x),g(x))$ 表达成 $f(x)$ 和 $g(x)$ 的线性组合，即如下定理.

定理 8.1.2 给定不全为零的两个多项式 $f(x),g(x)\in F[x]$，则一定存在 $a(x),b(x)\in F[x]$ 使得，$(f(x),g(x))=a(x)f(x)+b(x)g(x)$.

由于域上的一元多项式环 $F[x]$ 本身就是交换幺环，所以交换环中理想的概念仍然适用于 $F[x]$ 中的理想. 对任意 $f(x)\in F[x]$，知

$$\langle f(x)\rangle=\{u(x)f(x)\mid u(x)\in F[x]\}$$

是由 $f(x)$ 生成的主理想.

我们已经指出 $F[x]$ 是主理想整环，即的任一理想都由某个多项式 $f(x)$ 生成. 容易证明对任意 $c\in F\backslash\{0\}$，有 $\langle f(x)\rangle=\langle cf(x)\rangle$，我们指定 $f(x)$ 为最高次数项系数为 1 的多项式，简称**首 1 多项式**.

定理 8.1.3 主理想的简单性质：

(1) $\langle f(x)\rangle\subseteq\langle g(x)\rangle$ 且 $g(x)\neq0\Leftrightarrow g(x)\mid f(x)$.

(2) $\langle f(x)\rangle=\langle g(x)\rangle\Leftrightarrow g(x)=cf(x)$，其中 $c\in F$, $c\neq0$.

证明 (1) 如果 $g(x)\mid f(x)$，则 $f(x)$ 的倍式必然也是 $g(x)$ 的倍式，即 $\langle f(x)\rangle$ 的元素必然是 $\langle g(x)\rangle$ 的元素，得到 $\langle f(x)\rangle\subseteq\langle g(x)\rangle$.

反过来，设 $f(x)=q(x)g(x)+r(x)$，其中 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$. 由理想的性质可知，$r(x)\in\langle g(x)\rangle$，所以只能 $r(x)=0$，即 $f(x)=q(x)g(x)$，因此 $g(x)\mid f(x)$.

(2) 由(1)可知，$\langle f(x)\rangle=\langle g(x)\rangle$ 的充要条件是 $g(x)\mid f(x)$ 且 $f(x)\mid g(x)$，即 $g(x)=cf(x)$，其中 $c\in K$, $c\neq0$.

定理 8.1.4 $\langle f(x)\rangle$ 为 $F[x]$ 的极大理想，当且仅当 $f(x)$ 为不可约多项式.

证明： 由 $F[x]$ 是 Euclid 环以及定理 8.1.3 易证.

定理 8.1.5 设 $p(x)\in F[x]$ 且为不可约多项式，则商环 $F[x]/\langle p(x)\rangle$ 构成一个域.

证明一：由商环的讨论可知，显然 $F[x]/\langle p(x)\rangle$ 是一个交换环，有幺元[1]，所以我们只要证明 $F[x]/\langle p(x)\rangle$ 中的非零元在 $F[x]/\langle p(x)\rangle$ 中都有乘法逆元即可. 因为 $p(x)$ 是不可约多项式，

所以对任意$[f(x)]\in F[x]/<p(x)>$且$[f(x)]\neq 0$，都有$(f(x),p(x))=1$. 进而存在多项式 $s(x),t(x)\in F[x]$使得

$$s(x)\,f(x)+t(x)\,p(x)=1,$$

即 $s(x)f(x)\equiv 1(\mathrm{mod}\ p(x))$，这说明$[f(x)]$为可逆元素，$[s(x)]$为其逆元，从而$F[x]/<p(x)>$中的任意非零元素都为可逆元素，即$F[x]/<p(x)>$构成一个域.

证明二：由于$<p(x)>$是极大理想，由定理 8.1.4 和定理 7.4.3 知，$F[x]/<p(x)>$是域.

例 8.1.3 设 $K=\mathbf{Z}_p$,其中 p 是素数. 设 $p(x)$是$F[x]$中的 n 次不可约多项式，则

$$F[x]/<p(x)>=\{[a_{n-1}x^{n-1}+\cdots a_1x+a_0]\,|\,a_i\in F\},$$

我们可以将这个集合看作由所有次数小于 n，系数在 K 内的多项式组成. 这是一个元素个数有限的域，其元素个数为 p^n.

定义 8.1.3(理想的和) 设 I_1 与 I_2 是 $F[x]$的理想，令

$$I_1+I_2=\{\,f(x)+g(x)|\,f(x)\in I_1,\,g(x)\in I_2\},$$

则 I_1+I_2 也是 $F[x]$的一个理想(读者自证)，称为 I_1 与 I_2 的**和**.

定理 8.1.6 域 F 上的一元多项式环 $F[x]$中的两个理想$<f(x)>$与$<g(x)>$的和等于由 $f(x)$与 $g(x)$的最大公因子生成的理想.

证明 不妨设 $f(x), g(x)$不全为零，则

$$<f(x))+(g(x)>\neq<0>,$$

故可设

$$<f(x)>+<g(x)>=<d(x)>,$$

$d(x)$为首一多项式. 因$<f(x)>\subseteq<d(x)>$，故 $d(x)|\,f(x)$，同理 $d(x)|\,g(x)$，即 $d(x)$为 $f(x), g(x)$的一个公因式. 若 $d_1(x)$为 $f(x)$和 $g(x)$的任一公因式，则由 $d_1(x)|\,f(x)$推知$<f(x)>\subseteq<d_1(x)>$，同理$<g(x)>\subseteq<d_1(x)>$，于是

$$<d(x)>=<f(x)>+<g(x)>\subseteq<d_1(x)>,$$

而这表明 $d_1(x)|\,d(x)$，所以 $d(x)=(f(x),g(x))$.

这个命题的直接推论如下.

推论 1 设 $f(x)$与 $g(x)$是域 F 上的一元多项式环 $F[x]$中的二多项式, $f(x)$与 $g(x)$的最大公因子为 $d(x)$，则存在 $u(x),v(x)\in F[x]$，使得 $d(x)=u(x)\,f(x)+v(x)\,g(x)$.

基于这个推论，我们还可以得到两个重要的推论.

推论 2 设 $f(x), g(x)$是 $F[x]$内两个不全为零的多项式，则下列命题等价：

(1) $f(x)$与 $g(x)$互素;

(2) 存在 $u(x),v(x)\in F[x]$，使 $u(x)\,f(x)+v(x)\,g(x)=1$;

(3) $<f(x)>+<g(x)>=F[x]$.

推论 3 设 $f(x), g(x), h(x)\in F[x]$,并且 $f(x)\neq 0$，如果 $f(x)|g(x)h(x)$且$(f(x),g(x))=1$，则 $f(x)|\,h(x)$.

根据上面定理 8.1.6 推论 3，可得下面的引理.

引理 8.1.7 设 $p(x)$为 $F[x]$内不可约多项式， $f_1(x), f_2(x),..., f_k(x)\in F[x]$.若 $p(x)\,|\prod_{i=1}^{k}f_i(x)$，则 $p(x)$整除某个 $f_j(x)$.

我们已经证明了 $F[x]$是唯一析因环，下面给出更为详细的证明.

定理 8.1.8(因式分解唯一定理) 设 F 是一个域，给定多项式

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\quad（a_i\in F,\quad a_0\neq 0）,$$

则 $f(x)$可以分解为

$$f(x)=a_0(p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}\quad（k_i>0,\quad i=1,2,\cdots,r）,$$

其中 $p_1(x),\cdots,p_r(x)$ 是 $K[x]$内首项系数为1且两两不同的不可约多项式. 而且, 除了不可约多项式的排列次序外, 上面的分解式是由 $f(x)$唯一决定的.

证明 先证存在性, 对 deg $f(x)$做数学归纳法. 当 deg $f(x)$=0 时, 命题显然成立.

设命题对 deg $f(x)<n$ 的多项式 $f(x)$成立. 下面考察 deg $f(x)=n$ 时的情况.

如果 $f(x)$本身是不可约的, 则 $p_1(x)=\dfrac{1}{a_0}f(x)$ 仍为不可约多项式, 而 $f(x)=a_0p_1(x)$, 故命题成立.

如果 $f(x)$可约, 那么它有一个非平凡因式 $g(x)$, 故有分解式 $f(x)=g(x)h(x)$, 这里 $0<\deg g(x)<\deg f(x)$, $0<\deg h(x)<\deg f(x)$, 按照归纳假设, $g(x)$与 $h(x)$均可分解为互不相同的不可约多项式的幂的乘积, 这样, $f(x)$显然也有这样的分解式.

再证唯一性. 对 deg$f(x)$做数学归纳法. deg$f(x)$= 0 时命题显然成立.

设命题对 deg $f(x)<n$ 的多项式 $f(x)$成立. 现考察 deg $f(x)=n$ 的情形. 设其有两个分解式. 因为 $a_0\neq 0$, 约去 a_0 后得到

$$(p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}=(q_1(x))^{l_1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s},\tag{8.3.1}$$

从上式知 $p_1(x)\mid(q_1(x))^{l_1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}$, 因为 $p_1(x)$ 是不可约多项式, 根据引理, $p_1(x)$ 整除某个 $q_i(x)$, 不妨设 $p_1(x)\mid q_1(x)$. 但 $q_1(x)$ 也是不可约多项式, 故只能有

$$p_1(x)=aq_1(x)\ (a\in K).$$

又因为 $p_1(x)$ 与 $q_1(x)$ 首项系数都是 1, 故 $a=1$, 即 $p_1(x)=q_1(x)$, 从式(8.3.1)两边消去 $p_1(x)$, 得

$$g(x)=(p_1(x))^{k_1-1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}=(q_1(x))^{l_1-1}(q_2(x))^{l_2}\cdots(q_s(x))^{l_s}.$$

现在 $\deg g(x)=\deg f(x)-\deg p_1(x)<n$, 按照归纳法, 应有 $r=s$, 且适当排列不可约多项式次序后, 有 $p_i(x)=q_i(x)$, $k_i=l_i$ （$i=1,2,\cdots,r$）. 由此可知, $f(x)$的分解式是唯一的.

习题 8.1

A 组

1. 域上的一元多项式环[x]是主理想环, 即如果 I 是 $K[x]$的一个非零理想, 则存在 $K[x]$内的首一多项式 $f(x)$, 使 $I=\langle f(x)\rangle$.
2. 试在 $\mathbf{Q},\mathbf{R},\mathbf{C},\mathbf{Z}_5$ 内分解多项式: (1) x^2+1;(2) x^2+x+1
3. 求x^5-3x^3+2x在 $\mathbf{Z}_5$ 内的根.
4. 设 F 是一个域, $f(x)\in F[x]$, 证明：存在非平凡 $g(x)\in F[x]$使得$g^2(x)\mid f(x)$当且仅当 $F[x]/\langle f(x)\rangle$含有非零的幂零元.

B 组

5. 设 p 是素数, $a_n\neq 0\ (\mathrm{mod}\ p)$, $a_nx^n+\cdots+a_1x+a_0=0\ (\mathrm{mod}\ p)$在 $\mathbf{Z}_p$ 中最多有n个非同余的解.
6. 设 F 是一个域, 只有 q 个元素$\alpha_1,\cdots,\alpha_q$, 证明在$F[x]$中有$x^q-x=(x-\alpha_1)\cdots(x-\alpha_q)$.

7. 证明 Wilson 定理：$(p-1)! \equiv -1 (\bmod p)$.

8.2 域的代数扩张

给定域上多项式求根，实际上就是域的扩张. 我们这里简要介绍域的代数扩张的概念.

定义 8.2.1 域 F,K 满足 $F \subset K$，则称 F 为 K 的**子域**, K 为 F 的**扩张**或**扩域**.

定义 8.2.2 不包含任何非平凡子域的域称为**素域**.

定理 8.2.1 设Π为一个素域，则或$\Pi \cong \mathbf{Z}_p$ 或$\Pi \cong \mathbf{Q}$.

证明: 设e是Π的单位元，则$\mathbf{Z}e = \{ne \mid n \in \mathbf{Z}\}$为$\Pi$ 的子环. 作$\mathbf{Z}\epsilon$到$\mathbf{Z}e$ 的同态π，由于π是满同态，则有 $\mathbf{Z}e \cong \mathbf{Z}/\ker\pi$. 由于 $\mathbf{Z}$ 为主理想环，故存在 $p \in \mathbf{Z}$ 使得 $\ker\pi = <p>$. 由于 p 为整环$\mathbf{Z}e$ 的特征，故p为素数或 0.

若p为素数，则$\mathbf{Z}e \cong \mathbf{Z}/<p> = \mathbf{Z}_p$ 为域，注意到Π 为素域，且$\mathbf{Z}_p \subseteq \Pi$，故$\Pi \cong \mathbf{Z}_p$.

若$p = 0$，则$\mathbf{Z}e \cong \mathbf{Z}$，故$\mathbf{Z}e$ 的分式域 K 同构于$\mathbf{Z}\epsilon$的分式域$\mathbf{Q}$，即$K \subseteq \Pi$，又因Π 为素域，故$\Pi \cong \mathbf{Q}$.

定理 8.2.2 设 F 为一个域, p 为素数，则

(1) F 的特征为 p 当且仅当对$\forall a \in F$，有 pa=0;

(2) F 的特征为 0 当且仅当对$\forall a \in F^*, \forall n \in \mathbf{Z}e^*$，有 $na \neq 0$.

证明 : (1)若 F 的特征为 p，则其素域$\Pi \cong \mathbf{Z}_p$，因而 pe=0，故 pa=pea=0，$\forall a \in F$.

反之，若 pa =0，$\forall a \in F$，则 pe=0，因此由定理 8.2.1 知$\Pi \cong \mathbf{Z}_p$，故 Ch F=p.

(2)若F的特征为0，则$\Pi \cong \mathbf{Q}$，因而$\mathbf{Z}e \cong \mathbf{Z}$，故$na \neq 0, ne \neq 0$. 又因域$F$是整环，无零因子，故有$\forall a \in F^*, na \neq 0$.

反之，若$\forall a \in F^*, \forall n \in \mathbf{Z}e^*$，有 $na \neq 0$，于是$ne \neq 0$，即由定理 8.2.1 知$\Pi \cong \mathbf{Q}$，因此 Ch F=0.

我们现在知道，任何一个域包含唯一一个素域，且该素域由其特征唯一确定. 我们可以从较为简单的素域得到其扩域. 下面，类似于群、环同构的概念，我们定义域同构.

定义 8.2.3 设F_1, F_2为域，F_1到F_2的映射σ：$F_1 \longrightarrow F_2$满足，对$\forall a, b \in F_1$,有$\sigma(a+b) = \sigma(a) + \sigma(b), \sigma(ab) = \sigma(a)\sigma(b)$，则称$\sigma$为$F_1$到$F_2$的**同构**，若$F_1$=$F_2$，则称$\sigma$为**自同构**.

例 8.2.1 证明域之间的同态为单同态，进而，域与其同态像同构. 这也就是为何我们通常对群和环讨论同态，而对域只讨论同构.

定义 8.2.4 设 K 为域 F 的扩域, S 为 K 的子集. K 中所有包含$F \cup S$的子域的交，即有 F 与 S 生成的子域，称为 F 上添加 S 所得的域，记为$F(S)$.

如果以$F[S]$表示以下形式的所有的有限和：

$$\sum_{i_1,\cdots,i_n \geq 0} \alpha_{i_1,\cdots i_n} a_1^{i_1}, \cdots, a_n^{i_n}$$

(其中$a_j \in S$, j=1, ⋯,n, $\alpha_{i_1,\cdots i_n} \in F$)所构成的集合. 显然$F[S]$是 K 的子环，其分式域恰为$F(S)$. 当S为有限集$\{a_1, \ldots, a_n\}$时，记

$$F[S]=F[a_1,\dots,a_n],F(S)=F(a_1\ \dots,a_n).$$

定理 8.2.3 设 K 为域 F 的扩域, $S\subseteq K$, 则：

(1) $F(S)=\bigcup_{S'\subseteq S}F(S')$, 此处$S'$为遍历$S$的所有有限子集;

(2)若$S=S_1\cup S_2$, 则$F(S)=F(S_1)(S_2)$.

证明 ：(1)显然$F(S')\subseteq F(S)$, 故$\bigcup_{S'\subseteq S}F(S')\subseteq F(S)$. 反之, 对$\forall a\in F(S)$有$a=\frac{f}{g}$其中 $f,g\in F[S]$. 由于 f,g 的表达式均为有限和形式, 因而存在S的子集$S_0{}'$, 使得 $f,g\in F[S_0{}']$, 于是 $a=\frac{f}{g}\in F[S_0{}']\subseteq\bigcup_{S'\subseteq S}F(S')$, 故结论(1)成立.

(2)由于$F(S_1\cup S_2)$是 K 中同时包含$S_1\cup S_2$与F的最小子域, 而$F,S_1,S_2\subseteq F(S_1)(S_2)$, 故有$F(S_1\cup S_2)\subseteq F(S_1)(S_2)$. 反之, $F(S_1)(S_2)$是包含$F(S_1)$与S_2的最小子域, 而$F(S_1)\subseteq F(S_1\cup S_2),S_2\subseteq F(S_1\cup S_2)$, 故$F(S_1)(S_2)\subseteq F(S_1\cup S_2)$, 因而结论(2)成立.

推论 $F(\alpha_1,\cdots,\alpha_n)=F(\alpha_1)\cdots(\alpha_n)$.

为了论述接下来的域扩张, 我们下面将环上代数元的概念引入域中.

定义 8.2.5 设 K 为域 F 的扩域, $\alpha\in K$, 若存在域上的非零多项式 $f(x)$满足 $f(\alpha)=0$, 则称α为 ***F* 上的代数元**, 否则称α为 ***F* 上的超越元**. K 包含的 F 上的代数元的集合, 称之 ***F* 在 *K* 中的代数闭包**. F 上所有的代数元的集合称为 F 的**代数闭包**, 记为$\overline{F}$.

此外, 若域 K 是本身的代数闭包, 即 K 上多项式的根均在 K 中, 则称 K 为**代数闭域**.

定义 8.2.6 设K为域F的扩域且存在$\alpha\in K$使得$K=F(\alpha)$, 则称K为F的**单扩张**. 若α为 F 上的代数元, 则称 K 为F的**单代数扩张**, 若α为 F 上的超越元, 则称 K 为F的**单超越扩张**.

定理 8.2.4 设 K 为域 F 的扩域, $S\subseteq K$, 则：

(1)若α为 F 上的超越元, 则$F(\alpha)\simeq F(x)$, 其中$F(x)$为F上多项式环$F[x]$的分式域;

(2)若α为 F 上的代数元, 则$F(\alpha)\simeq F[x]/<p(x)>$, 其中$p(x)$为$F[x]$中一个首一的、由以$\alpha$为根的不可约多项式, 即$p(\alpha)=0$.

证明 ：$F(\alpha)$是$F[\alpha]$ 的分式域, 作$F[x]$到$F[\alpha]$的映射π:

$\pi(a_nx^n+\cdots+a_1x+a_0)$=$a_n\alpha^n+\cdots+a_1\alpha+a_0$

易知π是满同态.

(1) 若α为F上的超越元, 则$\ker\pi=\{0\}$, 因此π是$F[x]$到$F[\alpha]$的同构, 进而可将π作用到$F[x]$的分式域$F(x)$上, 使得π是$F(x)$到$F(\alpha)$的同构, 进而$F(\alpha)\simeq F(x)$.

(2) 若α为 F 上的代数元, $\ker\pi$是$F[x]$的非零理想, 由于$F[x]$是主理想环, 故 $\ker\pi$=$<p(x)>$, 其中$p(x)$为$F[x]$中一个非零多项式. 若限定$p(x)$是首一的多项式, 则$p(x)$唯一.

若$p(x)$是可约多项式, 则可设$p(x)$=$g(x)\ h(x)$, $\deg g>0$,$\deg h>0$. 因$p(\alpha)=0$且$F[x]$是整环, 则 $g(\alpha)=0$ 或 $h(\alpha)=0$, 进而$p(x)\mid g(x)$或$p(x)\mid h(x)$. 故 $\deg g\geq\deg p$ 或 $\deg h\geq\deg p$, 矛盾.

由定理 7.4.6 知, $<p(x)>$是极大理想, $F[x]/<p(x)>$是域. 由环的同态基本定理知, $F[\alpha]\simeq F[x]/<p(x)>$是域, 而$F[\alpha]$作为域的分式域即为$F[\alpha]$本身, 故$F(\alpha)\simeq F[x]/<p(x)>$.

定理 8.2.5 设 K 为域 F 的扩域, K_0为 K 在 F 上的代数闭包, 则K_0是含于 K 的 F 的最大代数扩张, 且对$\forall\delta\in K\backslash K_0,\delta$在$K_0$上是超越的.

证明：只需证K_0为 F 的扩域, 则可由定义知K_0是含于 K 的 F 的最大代数扩张. 显然, $F\subseteq K_0$. 设$\alpha,\beta\in K_0$且$\beta\neq 0$, 于是有$\alpha\pm\beta,\alpha\beta^{\pm1}\in F(\alpha,\beta)$=$F(\alpha)(\beta)$, 而易知 $F(\alpha)(\beta)$是 F 的代数扩张, 因而$\alpha\pm\beta,\alpha\beta^{\pm1}$均为 F 上的代数元, 即$\alpha\pm\beta,\alpha\beta^{\pm1}\in K_0$, 故$K_0$为 F 的扩域.

定义 8.2.7 设 K 为域 F 的扩域, $\alpha\in K$为 F 上的代数元, $F[x]$中以α为根的不可约的首一多项式称为α在 F 上的不可约多项式, 记为 $\mathrm{Irr}(\alpha, F)$, 其次数称为α在 F 上的次数, 记为

$\deg(\alpha, F)$.

由以上定理知，若α为 F 上的代数元，则 $\ker\pi =< \mathrm{Irr}(\alpha,F) >$ 且

$$F(\alpha) \simeq F[x]/< \mathrm{Irr}(\alpha,F) >.$$

例 8.2.2 $\mathrm{Irr}(\sqrt{2},\mathbf{Q}) = x^2-2$，请读者说明$\mathbf{Q}(\sqrt{2}) \cong \mathbf{Q}[x]/<x^2-2>$.

若 K 为域 F 的扩域，则 K 可作为 F 上的线性空间，进而有一下结论.

定理 8.2.6 设$F(\alpha)$是 F 的单代数扩张，$\deg(\alpha, F)=n$，则$F(\alpha)$是 F 上的 n 维线性空间，$1,\cdots,\alpha^{n-1}$构成$F(\alpha)$的一组基.

证明 ：由Euclid 环$F[x]$上的带余除法知，设$\forall f(x)\in F[x]$，$f(x)\neq 0$，则存在唯一的 $q(x)$,$r(x)\in K[x]$，使

$$f(x)=q(x)\,\mathrm{Irr}(\alpha,F)+r(x),\ r(x)=0 \text{ 或 } \deg r(x)<\deg f(x)$$

故 $f(\alpha)=r(\alpha)$，于是$1,\cdots,\alpha^{n-1}$可以生成 F 上的线性空间$F(\alpha)$. 我们只需要证线性$1,\cdots,\alpha^{n-1}$无关.

若 $1,\cdots,\alpha^{n-1}$ 线性相关，则存在 $a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0=0, a_i$ 不全为 0. 设$h(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0$则$h(\alpha)=0, \mathrm{Irr}(\alpha,F)|h(x)$，从而 $\deg h \geq n$，矛盾.

定义 8.2.8 设K_1、K_2为域 F 的扩域，若存在K_1到K_2的同构ϕ使得$\phi|_F=\mathrm{id}_F$，则称K_1、K_2为 F 的**等价扩张**，称ϕ为 ***F*-同构**，若K_1=K_2时，ϕ为 ***F*-自同构**.

定理 8.2.7 (1)设$F(\alpha_1)$、$F(\alpha_2)$是 F 的单超越扩张，则$F(\alpha_1)$、$F(\alpha_2)$是 F 的等价扩张.

(2)若对于$F[x]$上的首一不可约多项式$p(x)$，存在F的单代数扩张$F(\beta)$使得$\mathrm{Irr}(\beta,F)=p(x)$，且满足这个条件的任何两个代数扩张一定是 F 的等价扩张.

证明 ：(1)若$F(\alpha_1)$、$F(\alpha_2)$是 F 的单超越扩张，则$F(\alpha_1)\simeq F(x), F(\alpha_2)\simeq F(x)$因而$\phi$：$F(\alpha_1)\simeq F(\alpha_2)$，且易知$\phi|_F=\mathrm{id}_F$.

(2)对任意使得$\mathrm{Irr}(\beta,F)=p(x)$的$F$的单代数扩张$F(\beta)$，有$F(\beta)\simeq F[x]/<p(x)>$，故满足该条件的扩张均与$F[x]/<p(x)>$同构. 此外，该映射将$F$中元素 a 映射为 $a+<p(x)>$因而该同构作用于F上为恒等变换.

定义 8.2.9 设 K 为域 F 的扩域，若 K 中每个元素都是 F 上的代数元，则称 K 为 F 的**代数扩张**.

定义 8.2.10 若 K 为 F 的扩域, K 作为 F 上的线性空间是有限维的，则称 K 为 F 的**有限扩张**，该维数称 K 为在 F 上的**维数**，记为$[K:F]$；若 K 作为 F 上的线性空间是无限维的，则称 K 为 F 的**无限扩张**.

定理 8.2.8 设$F(\alpha)$为F的单扩张，则以下三个条件等价：

(1) $F(\alpha)$为F的代数扩张;

(2) α是F上的代数元;

(3) $F(\alpha)$为F的有限扩张.

证明 ：(1)⟹(2)显然;

(2) ⟹(3) 由于α是F上的代数元，故存在$F[x]$中多项式$p(x)$，使得$p(\alpha)=0, F(\alpha)$为F的上的线性空间，维数小于$p(x)$次数，故(3)成立.

(3) ⟹(1) 设$[F(\alpha):F]=n$，则$\forall\beta\in F(\alpha), 1,\beta,\cdots,\beta^n$线性相关，存在不全为 0 的$a_0,a_1,\cdots,a_n\in F$使得$a_0+a_1\beta\cdots+a_n\beta^n=0$，因而$\beta$是$F$上的代数元，进而$F(\alpha)$为$F$的代数扩张.

定理 8.2.9 设 E 为 F 的有限扩张, K 为 E 的有限扩张，则 K 为 F 的有限扩张，且

$$[K:F]=[K:E]\,[E:F]$$

证明 ：设$[K:E]=n$, $[E:F]=m$，取 K 作为 E 上线性空间的一组基$\alpha_1,\cdots,\alpha_n$，取 E 作为 F 上线性空间的一组基$\beta_1,\cdots,\beta_m$. 我们可以证明$S=\{\alpha_i\beta_j|1\leq i\leq n, 1\leq j\leq m\}$为 K 作为 F 上线

性空间的一组基，且各个元素是线性无关的．具体证明留习题.

习题 8.2

A 组

1. 求下列域扩张的次数

   (1) $[\mathbf{Q}(\sqrt{3},\sqrt{5}):\mathbf{Q}]$;

   (2) $[\mathbf{Q}(\sqrt{3}+\sqrt{5}):\mathbf{Q}]$;

   (3) $[\mathbf{Q}(\sqrt[3]{2},\sqrt{5}):\mathbf{Q}]$;

   (4) $[\mathbf{Q}(\sqrt{3},\sqrt{5}):\mathbf{Q}(\sqrt{3}+\sqrt{5})]$

2. 若 K 为 F 的扩域, $[K:F]=p$ 是素数，则对于$\forall\ \alpha\in K\backslash F$，有 $K=F(\alpha)$.
3. 证明(1)例题 8.2.2, (2)定理 8.2.9
4. 证明：若 $a,b\in\mathbf{Q}$，$\sqrt{a}+\sqrt{b}\neq 0$，则 $\mathbf{Q}(\sqrt{3},\sqrt{5})=\mathbf{Q}(\sqrt{3}+\sqrt{5})$.

B 组

5. 若 K 为 F 的扩域，α，$\beta\in K\backslash F$，$\deg(\alpha,F)$与 $\deg(\beta,F)$互素，求证: $\mathrm{Irr}(\alpha,F)$是$F(\beta)[x]$上的不可约多项式，从而$[F(\alpha,\beta):F]=\deg(\alpha,F)\deg(\beta,F)$.
6. 试证明：对任意有限域 F，均存在素数 p 以及正整数 n，使得 F 由p^n个元素构成.
7. （1）证明：$\mathbf{Q}(\sqrt{3})$ 和 $\mathbf{Q}(\sqrt{5})$ 作为上的线性空间是同构的，但作为域不是同构的.

   （2）若 $K=F(\alpha)$为 F 的扩域，证明L_α：$x\to\alpha x,\forall x\in K$ 是 K 到自身的线性变换，并说明 $\det(xI-L_\alpha)=\mathrm{Irr}(\alpha,F)$.

8.3 分裂域与自同构

我们在本节中，将进一步讨论域上多项式的根的求解问题.

定义 8.3.1 设 F 为域，$f(x)\in F[x]$, E 为 F 的扩域，如果

(1) $f(x)$在$E[x]$上可以分解为一次因式的乘积：

$$f(x)=a(x-\alpha_1)\cdots(x-\alpha_n),a\in F,\alpha_i\in E,i=1,\cdots,n$$

(2) $E=F(\alpha_1,\cdots,\alpha_n)$

则称E为$f(x)$在 F 上的**分裂域**.

定理 8.3.1 $f(x)$是 F 上多项式，且 $\deg f>0$，则$f(x)$在 F 上的分裂域存在.

证明：我们对 $\deg f$运用数学归纳法进行证明．若 $\deg f=1$，则$f(x)=ax+b=a(x-a^{-1}b),a,b\in F$，故$F$是$f(x)$分裂域．设结论对 $\deg f=k$成立，当 $\deg f=k+1$时，设$p(x)$是$f(x)$的一个不可约因式，令$F_1=F[x]/<p(x)>$，则由定理 7.4.7 以及上节结论知，F_1是F的单代数扩张，且$F_1=F(\alpha_1)$，其中$\alpha_1=x+<p(x)>$．于是$p(\alpha_1)=0$，故在F_1上有$f(\alpha_1)=0$. $f(x)$作为$F_1[x]$中的多项式，有分解

$$f(x)=(x-\alpha_1)f_1(x),f_1(x)\in F_1[x],\deg f_1=k$$

由归纳假设，存$f_1(x)$在F_1上的分裂域$E=F_1(\alpha_2,\cdots,\alpha_{k+1})$，于是$f(x)$在$E$上有分解

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{k+1}).$$

另一方面$E=F_1(\alpha_2,\cdots,\alpha_{k+1})=F(\alpha_1)(\alpha_2,\cdots,\alpha_{k+1})=F(\alpha_1,\cdots,\alpha_{k+1})$，故$E$是$f(x)$在$F$上的

分裂域.

例 8.3.1 求 x^3-2在$\mathbf{Q}$上的分裂域.

易知x^3-2是$\mathbf{Q}$上的不可约因式，且$\sqrt[3]{2}$是$x^3-2=0$的一个根，$[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}]$=3且.
$x^3-2=(\mathrm{x}-\sqrt[3]{2})(x^2+\sqrt[3]{2}\mathrm{x}+\sqrt[3]{4})$，设$\alpha$是$x^2+\sqrt[3]{2}\mathrm{x}+\sqrt[3]{4}$的一个根.

若记$\omega=\alpha/\sqrt[3]{2}$则容易验证: $\omega^2+\omega+1=(\alpha/\sqrt[3]{2})^2+\alpha/\sqrt[3]{2}+1=(\alpha^2+\sqrt[3]{2}\alpha+\sqrt[3]{4})/\sqrt[3]{4}=0$.
故ω是$x^2+x+1=0$ 的根，进而$[\mathbf{Q}(\omega):\mathbf{Q}]=2$. 所以$x^3-2$在$\mathbf{Q}$上的分裂域为$\mathbf{Q}(\sqrt[3]{2},\omega)$，且$[\mathbf{Q}(\sqrt[3]{2},\omega):\mathbf{Q}]=6$.

值得注意的是，x^3-2的其它根$\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$并不都在$\mathbf{Q}(\sqrt[3]{2})$之中（其中$\omega=e^{\frac{2\pi i}{3}}$）.

定理 8.3.2 设F_1,F_2为域，映射σ：$F_1\longrightarrow F_2$为F_1到F_2的同构. $p_1(x)\in F_1[x]$，相应的$p_2(x)=\sigma(p_1(x))\in F_2[x]$. E_1,E_2分别为$p_1(x),p_2(x)$在F_1,F_2上的分裂域，则σ可以扩充为$E_1\longrightarrow E_2$的同构.

证明： 我们这里仅给出简略证明. 设$p_1(x)$在E_1内有分解$p_1(x)=(x-\alpha_1)\cdots(x-\alpha_n)$，其中$\alpha_i\in E_1,i=1,\cdots,$; 设$p_2(x)$在$E_2$内有分解$p_2(x)=(x-\beta_1)\cdots(x-\beta_n)$，其中$\beta_i\in E_2,i=1,\cdots,$, 从而有$E_1=F_1(\alpha_1,\cdots,\alpha_n)$. 同时，由于σ为$F_1$到$F_2$的同构，我们可将σ取作$\{\alpha_1,\ldots,\alpha_n\}$到$\{\beta_1,\ldots,\beta_n\}$之间的一一映射，从而有

$$p_2(x)=(x-\beta_1)\cdots(x-\beta_n)=(x-\sigma(\alpha_1))\cdots(x-\sigma(\alpha_n)),$$

从而$E_2=F_2(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))=\sigma(F_1)(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))$，而σ扩充为$F_1(\alpha_1,\cdots,\alpha_n)$到$\sigma(F_1)(\sigma(\alpha_1),\cdots,\sigma(\alpha_n))$的同构.

推论 $f(x)$在F上的分裂域在同构的意义下唯一.

证明： 令F_1=F_2，由以上定理可得.

下面我们介绍群在域扩张中的作用,我们先来介绍群的特征.

定义 8.3.2 设$(G,\cdot)$为群，$(F,+,\cdot)$为域，σ为$(G,\cdot)$到$(F,\cdot)$的同态映射，即对$\forall\alpha,\beta\in G,\sigma(\alpha)\sigma(\beta)=\sigma(\alpha\beta),\sigma(\alpha)\neq 0$，则称σ为**群 *G* 在 *F* 中的特征**.

值得指出的是，我们这里需要规定：对$\forall\alpha\in G$，有$\sigma(\alpha)\neq 0$. 否则，若存在$\sigma(\alpha)=0$，则对$\forall\beta\in G,\sigma(\beta)=\sigma(\alpha)\sigma(\alpha^{-1}\beta)=0$

定义 8.3.3 设$\sigma_1,\cdots,\sigma_n$为G在F中的特征，若存在不全为 0 的$a_1,\cdots,a_n\in F$使得对$\forall x\in G$，有$a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)=0$，则称特征$\sigma_1,\cdots,\sigma_n$是**相关的**; 否则称特征$\sigma_1,\cdots,\sigma_n$是**无关的**.

定理 8.3.3 G是群，$\sigma_1,\cdots,\sigma_n$为G在F中互异的特征，则$\sigma_1,\cdots,\sigma_n$是无关的.

证明： 由我们对n进行归纳.

首先，对于$n=1$时的σ_1，因为$\forall\alpha\in G$，有$\sigma_1(\alpha)\neq 0$，故根据定义，是σ_1无关的. 现假设对结论对所有小于$n-1$的整数成立. 设

$$a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)=0 \qquad (*)$$

是$\sigma_1,\cdots,\sigma_n$的非平凡的相关. 若有$a_i=0\in F$，则与假设矛盾，故$a_1,\cdots,a_n$均不为 0.

因为σ_1,σ_n是互异的，故存在$\alpha\in G$使得$\sigma_1(\alpha)\neq\sigma_n(\alpha)$，对上述等式乘以${a_n}^{-1}$得到:

$$b_1\sigma_1(x)+\cdots+b_{n-1}\sigma_{n-1}(x)+\sigma_n(x)=0,\ \text{其中}b_i={a_n}^{-1}a_i\neq 0$$

用αx代替上式中的x，有:

$$b_1\sigma_1(\alpha)\sigma_1(x)+\cdots+b_{n-1}\sigma_{n-1}(\alpha)\sigma_{n-1}(x)+\sigma_n(\alpha)\sigma_n(x)=0$$

进而乘以$\sigma_n(\alpha)^{-1}$，有:

$$\sigma_n(\alpha)^{-1}\mathrm{b}_1\sigma_1(\alpha)\sigma_1(x)+\cdots+\sigma_n(\alpha)^{-1}b_{n-1}\sigma_{n-1}(\alpha)\sigma_{n-1}(x)+\sigma_n(x)=0$$

减去(*)式得:

$$(\mathrm{b}_1-\sigma_n(\alpha)^{-1}\mathrm{b}_1\sigma_1(\alpha))\sigma_1(x)+\cdots+c_{n-1}\sigma_{n-1}(x)=0$$

其中$\sigma_1(x)$系数不等于 0，否则有$b_1=\sigma_n(\alpha)^{-1}b_1\sigma_1(\alpha)$，从而$\sigma_n(\alpha)b_1=b_1\sigma_1(\alpha)=\sigma_1(\alpha)b_1$. 从而$\sigma_n(\alpha)=\sigma_1(\alpha)$，与α的选择矛盾. 因此，上式构成$\sigma_1,\cdots,\sigma_{n-1}$的相关关系，与假设矛盾.

推论 E_1,E_2为域，$\sigma_1,\cdots,\sigma_n$为E_1到E_2的n个互异的同构映射，则$\sigma_1,\cdots,\sigma_n$是无关的.

值得注意的是，这里的无关与定义 8.3.3 中一致，考虑的是E_1,E_2的乘法群.

定义 8.3.4 设$\sigma_1,\cdots,\sigma_n$为E_1到E_2的同构映射，若存在$\alpha\in E_1$使得$\sigma_1(\alpha)=\cdots=\sigma_n(\alpha)$，则$\alpha$称为$\sigma_1,\cdots,\sigma_n$的**不变元**，记为 $\mathrm{Inv}(\sigma_1,\cdots,\sigma_n)$.

引理 8.3.4 域E对于$\sigma_1,\cdots,\sigma_n$的不动点构成E的子域，称之为E对于$\sigma_1,\cdots,\sigma_n$的**不变域**.

证明： 设 a,b 是不变元，由$\sigma_i(a+b)=\sigma_i(a)+\sigma_i(b)$，$\sigma_j(ab)=\sigma_j(a)\sigma_j(b)$且

$\sigma_i(a)^{-1}=\sigma_j(a)^{-1}=\sigma_j(a^{-1})=\sigma_i(a^{-1})$易得.

定理 8.3.5 $\sigma_1,\cdots,\sigma_n$为域E_1到域E_2的n个互异的同构映射，F 为E_1对于$\sigma_1,\cdots,\sigma_n$的不变域，则有$[E_1{:}F]\geq n$.

证明： 设$[E{:}F]=r<n$，且$\omega_1,\cdots,\omega_r$为 E 作为 F 扩域的生成元. 考虑下列方程组：

$$\sigma_1(\omega_1)x_1+\cdots+\sigma_n(\omega_1)x_n=0$$
$$\vdots$$
$$\sigma_1(\omega_r)x_1+\cdots+\sigma_n(\omega_r)x_n=0$$

由于变量个数n大于方程个数 r，故存在非零解，仍记为$x_1,\cdots,x_n$.

对于$\forall\alpha\in E$，存在$a_1,\cdots,a_r\in F$ 使得$\alpha=a_1\omega_1+\cdots+a_r\omega_r$. 我们用$a_1$乘以第一个方程，$\cdots,a_r$乘以第 r 个方程，由于$a_i\in F$ 则$\sigma_1(a_i)=\sigma_j(a_i)$且$\sigma_j(a_i)\sigma_j(\omega_i)=\sigma_j(a_i\omega_i)$，得到：

$$\sigma_1(a_1\omega_1)x_1+\cdots+\sigma_n(a_1\omega_1)x_n=0$$
$$\vdots$$
$$\sigma_1(a_r\omega_r)x_1+\cdots+\sigma_n(a_r\omega_r)x_n=0$$

对上述方程相加，并利用$\sigma_i(a_1\omega_1)+\cdots+\sigma_i(a_r\omega_r)=\sigma_i(\alpha)$，得到：

$$\sigma_1(\alpha)x_1+\cdots+\sigma_n(\alpha)x_n=0$$

进而得到$\sigma_1,\cdots,\sigma_n$的相关关系，与定理 8.3.3 矛盾.

推论 $\sigma_1,\cdots,\sigma_n$为域E的n个互异的自同构，F 为E对于$\sigma_1,\cdots,\sigma_n$的不变子域，则有$[E{:}F]\geq n$.

定义 8.3.5 域 F 为E的子域，所有保持 F 不变的E的自同构，即所有E的 F-自同构，对映射的复合运算构成群 G，称之为***E*的 *F*-自同构群**，记 G 为 $\mathrm{Aut}(E/F)$.

显然, $\mathrm{Aut}(E/F)$的单位元为E到自身的恒等映射 id.

定义 8.3.6 域 F 为E的子域，G 为 $\mathrm{Aut}(E/F)$的子群，易证E中所有在 G 作用下保持不变的元素构成的集合: $\mathrm{Inv}(G)=\{\alpha\in E|\sigma(\alpha)=\alpha,\forall\sigma\in G\}$ 构成域，称之为E对于G的**不变域**.

值得说明的是，$\mathrm{Aut}(E/F)$的不变域不一定为 F，一般存在中间域$F_1,F\subset F_1\subset E$使得$\mathrm{Inv}(\mathrm{Aut}(E/F))=F_1$.

定义 8.3.7 域E为域 F 的扩张，$[E{:}F]$有限，如果E的 F-自同构群的不变域为F，即$\mathrm{Inv}(\mathrm{Aut}(E/F))=F$，则称$E$为 F 的**正规扩张**.

定理 8.3.6 $\sigma_1=\mathrm{id},\sigma_2,\cdots,\sigma_n$构成域$E$的自同构群 $G=\mathrm{Aut}(E/F)$，F 为 $\mathrm{Aut}(E/F)$的不变域，则有$[E{:}F]=n$.

证明： 不变域由所有满足$x\in E,\sigma_i(x)=x$, $i=1,\cdots,n$ 的x构成. 设$[E{:}F]>n$，则存在 E 中元素$\alpha_1,\cdots,\alpha_{n+1}$在 F 上无关. 考虑下列方程组：

$$x_1\sigma_1(\alpha_1)+\cdots+x_{n+1}\sigma_1(\alpha_{n+1})=0$$
$$\vdots$$
$$x_1\sigma_n(\alpha_1)+\cdots+x_{n+1}\sigma_n(\alpha_{n+1})=0$$

由于变量个数$n+1$大于方程个数n，故存在 E 中非零解. 但该解不能属于 F，否则上述第一

个等式为$\alpha_1,\cdots,\alpha_{n+1}$在 F 上相关（注意到$\sigma_1=\mathrm{id}$），矛盾.

在所有$x_1,\cdots,x_{n+1}$的非零解中，取含有非零元最少的解：$a_1,\cdots,a_r,0,\cdots,0$，其中前$r$个变量不为 0．显然，$r\neq 1$，否则$\sigma_1(\alpha_1)=\alpha_1=0$，矛盾．与此同时，由于对任意解同时作用$a_r{}^{-1}$仍为方程组的解，我们假设$a_r=1$．至此，我们得到：

$$a_1\sigma_i(\alpha_1)+\cdots+a_{r-1}\sigma_i(\alpha_{r-1})+\sigma_i(\alpha_r)=0,\ i=1,\cdots,n \qquad (*)$$

由于$a_1,\cdots,a_{r-1}$不能同时属于 F，我们假设$a_1\in E\backslash F$，故存在σ_k使得$\sigma_k(a_1)\neq a_1$．因为$\sigma_1=\mathrm{id},\sigma_2,\cdots,\sigma_n$ 构成域 E 的自同构群 Aut(E /F)，进而 $\sigma_k\sigma_1,\sigma_k\sigma_2,\cdots,\sigma_k\sigma_n$ 构成 $\sigma_1=\mathrm{id},\sigma_2,\cdots,\sigma_n$的置换．对(*)作用$\sigma_k$得到：

$$\sigma_k(a_1)\sigma_k\sigma_j(\alpha_1)+\cdots+\sigma_k(a_{r-1})\sigma_k\sigma_i(\alpha_{r-1})+\sigma_k\sigma_j(\alpha_r)=0,\ j=1,\cdots,n$$

假设$\sigma_k\sigma_j=\sigma_i$，进而得到：

$$\sigma_k(a_1)\sigma_i(\alpha_1)+\cdots+\sigma_k(a_{r-1})\sigma_i(\alpha_{r-1})+\sigma_i(\alpha_r)=0,\ i=1,\cdots,n \qquad (**)$$

(*)-(**)得到：

$$(a_1-\sigma_k(a_1))\sigma_i(\alpha_1)+\cdots+(a_{r-1}-\sigma_k(a_{r-1}))\sigma_i(\alpha_{r-1})=0,\ i=1,\cdots,n$$

得到$r-1$个变量不为 0 的非零解，与r的选取矛盾.

推论 1 如果域 F 为域E对于群G的不变域，则E的所有 F-自同构属于G.

证明： 设$[E{:}F]=n=|G|$，且σ为第$n+1$个E的 F-自同构，则 F 在$n+1$个E的 F-自同构下保持不变，与定理 8.3.5 的推论矛盾.

推论 2 具有相同不变域的自同构群是唯一的.

定义 8.3.8 $f(x)$为$F[x]$中的多项式，如果其在$F[x]$中的不可约因式没有重根，则称其为**可分的**．域E为域 F 的扩张，$\alpha\in E$，若α是$F[x]$中一个可分多项式$f(x)$的根，则称α是**可分的**，如果$\forall\alpha\in E$可分，则称E为**可分的**，或**可分扩张**.

定理 8.3.7 E为 F 的正规扩张当且仅当E为F上的一个可分多项式$p(x)$的分裂域.

证明： **充分性：**

设E为F上的一个可分多项式$p(x)$的分裂域．如果$p(x)$的所有根在F内，则E=F，则 Aut(E/F)=id，命题得证．现假设有至少有$n>1$个根在$E\backslash F$内，我们将通过对n的归纳完成证明，故设充分性命题对所有小于等于n个根在$E\backslash F$内时的$p(x)$成立.

设$p(x)=p_1(x)\cdots p_r(x)$为$p(x)$在$F[x]$内不可约因式的分解，假设至少一个不可约因式次数>1，否则$p(x)$的根均在F内．设 deg $p_1(x)$=$s>1,\alpha_1$是$p_1(x)$的一个根，则$[F(\alpha_1){:}F]$ =deg $p_1(x)=s$．现考虑$p(x)$在$F(\alpha_1)[x]$内的分解，则$p(x)$有小于n个根在$E\backslash F(\alpha_1)$中.

由于$p(x)$在$F(\alpha_1)[x]$中，E为$p(x)$在$F(\alpha_1)$上的分裂域，根据归纳假设，E为$F(\alpha_1)$的正规扩张．所以，对于$\forall\alpha\in E\backslash F(\alpha_1)$，至少存在一个$E$的$F(\alpha_1)$-自同构$\sigma$使得$\sigma(\alpha)\neq\alpha$.

由于$p(x)$可分，则$p_1(x)$的根$\alpha_1,\cdots,\alpha_s$为E中互异元素．根据定理 8.3.2，存在同构$\sigma_1,\cdots,\sigma_s$将$F(\alpha_1)$映射为$F(\alpha_1),\ldots,F(\alpha_s)$，且保持$F$不变，将$\alpha_1$分别映射为$\alpha_1,\cdots,\alpha_s$．实际上，根据定理 8.3.2，$E$是$p(x)$在$F(\alpha_1)$上的分裂域，也是$p(x)$在$F(\alpha_1),\ldots,F(\alpha_s)$上的分裂域，所以上述任意的$\sigma_i$将$F(\alpha_1)$中的$p(x)$仍旧映射为$F(\alpha_1),\ldots,F(\alpha_s)$中$p(x)$的．我们现将$\sigma_1,\cdots,\sigma_s$扩充为$E$的自同构映射，仍记为$\sigma_1,\cdots,\sigma_s$，且保持$F$不变，将$\alpha_1$分别映射为$\alpha_1,\cdots,\alpha_s$.

设θ为任意一个在所有E的F-自同构下的不变元，则根据归纳假设，$\theta\in F(\alpha_1)$，因此具有如下形式：

$$\theta=c_0+c_1\alpha_1\cdots+c_{s-1}\alpha_1{}^{s-1},c_i\in F,i=1,\ldots,s$$

我们对上述等式作用σ_i，利用$\sigma_i(\theta)=\theta$得：

$$\theta=c_0+c_1\alpha_i\cdots+c_{s-1}\alpha_i{}^{s-1}$$

从而方程 $c_{s-1}x^{s-1}+\cdots+c_1x+c_0-\theta=0$有$s$个互异的根$\alpha_1,\cdots,\alpha_s$，大于方程的次数．故方程是平凡的，$c_0-\theta=0$，即$\theta=c_0\in F$.

必要性：

先来证明一个引理.

引理 E为 F 的正规扩张，则E为F上的可分扩张. 此外，E中任意元素，均为分裂域在E中的F上的多项式的根.

证明： 设$\sigma_1,\cdots,\sigma_s$构成的以F为不变域的E的自同构群$G.\alpha\in E,\alpha$在$\sigma_1,\cdots,\sigma_s$下的像为互异的 r 个元素：$\alpha_1=\alpha,\cdots,\alpha_r$ ($r\leqslant s$). 由于G为群,

$$\sigma_j(\alpha_i)=\sigma_j(\sigma_k(\alpha))=\sigma_j\sigma_k(\alpha)=\sigma_m(\alpha)=\alpha_n$$

因此，G在$\alpha_1=\alpha,\cdots,\alpha_r$的作用为置换，从而多项式$f(x)=(x-\alpha_1)\cdots(x-\alpha_s)$的系数是在$G$作用下的不变元. 因为$E$中在$G$作用下的不变元属于$F$，故$f(x)\in F[x]$.

若$g(x)\in F[x]$也以α为根，即$g(\alpha)=0$，将群G作用到$g(x)$可得$g(\alpha_i)=0$，进而$\deg g(x)>s, f(x)$为$F[x]$内不可约因式，引理得证.

下面回到定理必要性的证明. 设$\omega_1,\cdots,\omega_t$为E作为F扩域的生成元. 设$f_i(x)$为$F[x]$中以ω_i为根的可分多项式，则 E 是$p(x)=f_1(x)\cdots f_t(x)$的分裂域，完成证明.

定义 8.3.9 若 E 是$F[x]$内多项式$f(x)$的分裂域，我们称 G=Aut(E/F)为$f(x)$**的群**.

习题 8.3

A 组

1. 求$(x^2-3)(x^2-5)$在 $\mathbf{Q}$ 上的分裂域.
2. 求x^3-2在 $\mathbf{Q},\mathbf{Z}_5$ 上的分裂域以及 $\mathbf{Q},\mathbf{Z}_5$ 自同构群.
3. 求x^p-1在 $\mathbf{Q}$ 上的分裂域以及 $\mathbf{Q}$ 自同构群（p 为素数）.
4. 证明:(1)域的二次扩张是正规扩张; (2) $\mathbf{Q}(\sqrt[3]{2})$ 不是 $\mathbf{Q}$ 的正规扩张..

B 组

5. $F\subseteq B\subseteq E, E$为$F$的正规扩张，则 E为B的正规扩张.
6. 试给出定理 8.3.2 的完整证明**.**
7. 域$F\subseteq B\subseteq E, B$为$F$的正规扩张，$\sigma$为$E$的$F$同构，则$\sigma(B)=B$.
8. 设 **A** 为 **C** 在 **Q** 中的代数闭包，证明：**A** 是 **Q** 的正规扩张且$[\mathbf{A}:\mathbf{Q}]=\infty$.

8.4 伽罗瓦理论初步

这一节中，我们从一般的域扩张和自同构群出发，简要介绍法国数学家 Galois 在 19 世纪提出的 Galois 理论. 进而证明 Galois 基本定理的论述. 有兴趣的读者可以进一步阅读和学习关于 Galois 理论在高次方程根式解和尺规作图方面的应用.

定义 8.4.1 设域E为域 F 的扩张，则E的所有 F 自同构构成的集合构成群 Aut(E/F)，我们这里记为 **Gal(*E*/*F*)**，称为E在 F 上的**伽罗瓦（Galois）群**.

定义 8.4.2 设G是 Gal(E/F)的子群，则容易验证

$$\mathrm{Inv}_E G=\{a\in E\,|\,g(a)=a,\forall g\in G\}$$

是E的子域，定义为E**的**G**不变子域**. 在不致混淆时，记为Inv$G$.

定理 8.4.1 (1)若 $F\subseteq E_1\subseteq E_2$，则 Gal$(E_2/E_1)\subseteq$ Gal(E_2/F);

(2)若$G_1\subseteq G_2$，则Inv$G_2\subseteq$ InvG_1;

(3) $F\subseteq$ Inv(Gal(E/F));

(4) $G\subseteq$Gal(E/Inv$G$).

证明： 留作习题.

定义 8.4.3 设域E为域 F 的扩张，满足$F = \mathrm{Inv}(\mathrm{Gal}(E/F))$，则称$E$是$F$的 **Galois 扩张**.

定理 8.4.2 设域E为域 F 的有限扩张，则下列条件是等价的：

(1) E为F上的一个可分多项式$p(x)$的分裂域;

(2) E是F的 Galois 扩张，且$[E{:}F]$=| $\mathrm{Gal}(E/F)$|;

(3) E为F的正规扩张.

证明：(1)(3)等价我们已经在上一节证明过了，下面只证明(2) ⟹(3)和(3)⟹(2).

(2) ⟹(3) 对$\forall\alpha \in E$，设$G = \mathrm{Gal}(E/F)$，且 $\mathrm{Irr}(\alpha, F)$=$x^r + b_{r-1}x^r + \cdots + b_0$，其中$b_i \in F$. 于是对$\sigma \in G$有$\sigma(\alpha)^r + b_{r-1}\sigma(\alpha)^{r-1} + \cdots + b_0 = 0$，即$\sigma(\alpha)$是 $\mathrm{Irr}(\alpha, F)$的根，进而G有限. 设$\sigma_1(\alpha) = \alpha, \cdots, \sigma_s(\alpha)$为$\{\sigma(\alpha)^r | \sigma \in G\}$中不同元素.（注意到$\sigma_1 = \mathrm{id} \in G$）

令 $h(x)$=$\prod_{i=1}^{s}(x - \sigma_i(\alpha))$=$x^s + c_{s-1}x^s + \cdots + c_0$，其中显然$c_i$是$\sigma_1(\alpha), \cdots, \sigma_s(\alpha)$的对称多项式，且对$\forall\sigma \in G$，有$\sigma\sigma_1(\alpha), \cdots, \sigma\sigma_s(\alpha)$仍是$\sigma_1(\alpha), \cdots, \sigma_s(\alpha)$的一个排列，故$\sigma(c_i) = c_i$，进而$c_i \in F$, $h(x) \in F[x]$. 于是α是F上的可分元素，进而E是F的可分扩张，E为F的正规扩张.

(3)⟹(2) 由定理 8.3.6 知，$[E{:}F]$=| $\mathrm{Gal}(E/F)$|，设$F_1 = \mathrm{Inv}(\mathrm{Gal}(E/F))$，则由定理 8.4.1 有 $F \subseteq F_1$，$\mathrm{Gal}(E/F) \subseteq$ $\mathrm{Gal}(E/F_1)$，再利用 8.4.1(3)有 $\mathrm{Gal}(E/F_1) \subseteq$ $\mathrm{Gal}(E/F)$. 故 $\mathrm{Gal}(E/F)$= $\mathrm{Gal}(E/F_1)$.

又因$p(x)$也是F_1上的可分多项式，E也是$p(x)$在F_1中的分裂域，因而$[E{:}F_1]$=| $\mathrm{Gal}(E/F_1)$|，进而 $[E{:}F]$= $[E{:}F_1]$，从而$F_1 = \mathrm{Inv}\big(\mathrm{Gal}(E/F)\big) =\ F$，所以$E$是$F$的 Galois 扩张.

我们下面介绍 Galois 基本定理.

定理 8.4.2（**Galois 基本定理**）设$p(x)$为F上的一个可分多项式, G 为$p(x)$的群（定义 8.3.9），E是$p(x)$的分裂域，则：

(1)F, E任意的中间域 B（$F \subseteq B \subseteq E$）是 G 一个子群G_B的不变域，且不同的子群对应不同的中间域;

(2) 域B是F的正规扩张当且仅当G_B是G的正规子群，此时B的F自同构群与商群G/G_B同构;

(3) 对F, E任意的中间域 B我们有$[B{:}F]$=| G/G_B|, $[E{:}B]$=| G_B|.

证明：(1)对于F, E任意的中间域B, E均为$p(x)$作为 B上多项式的分裂域. 因此，E为B的正规扩张，所以B（$F \subseteq B \subseteq E$）是 G 一个子群G_B的不变域，该子群包含所有保持B不变的E自同构. 由定理 3.3.5 推论 2 可得，不同的子群对应不同的中间域. 下面，我们先证明 3 再证明 2.

(3) 对F, E任意的中间域 B，由于B是 G 子群G_B的不变域，根据定理 8.4.1 和 8.3.5 得$[E{:}B]$=| G_B|. 若记 $\mathrm{o}(G_B)$= | G_B|，$\mathrm{i}(G_B)$= $|G/G_B|$，则有 $\mathrm{o}(G)$= $\mathrm{o}(G_B)$ $\mathrm{i}(G_B)$. 但$[E{:}F]$= $\mathrm{o}(G)$, $[E{:}F]$= $[E{:}B]$ $[B{:}F]$，故$[B{:}F]$= $\mathrm{i}(G_B)$= $|G/G_B|$, (3)得证;

(2)易知 $\mathrm{i}(G_B)$为G_B的左陪集个数. G中元素为E的自同构，且将B同构地映射到E的其它子域，同时F在上仍为恒等映射 id.

此外，G_B的同一左陪集中的元素，在B上作用是相同的: 设$\sigma\sigma_1, \sigma\sigma_2$属于$G_B$的同一左陪集$\sigma G_B$，由于$\sigma_1, \sigma_2$保持$B$不变，对$\forall\ \alpha \in B$，我们有$\sigma\sigma_1(\alpha) = \sigma(\alpha) = \sigma\sigma_2(\alpha)$.

不同的陪集诱导不同的同构映射：若σ, τ诱导相同的同构，则对$\forall\ \alpha \in B$有 $\sigma(\alpha) = \tau(\alpha)$. 因此$\sigma^{-1}\,\tau$=$\sigma_1 \in G_B$. 但是$\tau = \sigma\sigma_1$且$\tau G_B =\ \sigma\sigma_1 G_B =\ \sigma G_B$，故$\sigma, \tau$属于$G_B$的同一左陪集.

任一B的F-同构由 G中的自同构导出. 设σ将B映射为B'且在F上为恒等映射 id, 则在σ作用下，$\sigma p(x) = p(x), E$是$p(x)$在B, B'中的分裂域. 根据定理 8.3.2，σ可以开拓为E的自同构σ'，又因为σ'保持F不变，故$\sigma' \in G$. 因此，B的自同构数与G_B的左陪集个数相同，进而等于$[B{:}F]$.

由于σB的元素在$\sigma G_B \sigma^{-1}$ 左作用下不变，因而域σB显然与$\sigma G_B \sigma^{-1}$相对应.

设B是F的正规扩张，由定理 8.3.6，B的F-自同构个数等于$[B{:}F]$. 与此同时，如果B的F-

自同构个数等于$[B:F]$，则B是F的正规扩张：若F'是所有这些同构的不变域，则$F \subseteq F' \subseteq B$，再由定理 8.3.6, $[B:F']$等于这个群中自同构的个数，因此$[B:F']=[B:F]$，进而$[F':F]=1$ 即$F=F'$. 所以，B是F的正规扩张当且仅当B的F-自同构个数等于$[B:F]$.

B是F的正规扩张当且仅当E中B的任意同构是B的自同构. 这是由于上述的结论以及同构、自同构数目相同，因此，对于$\forall\sigma, \sigma B = B$等价于$\sigma G_B \sigma^{-1} \subseteq G_B$，这样我们就得到：$B$是$F$的正规扩张当且仅当$G_B$是$G$的正规子群.

如上所述，每个B的同构可以由G_B的左陪集的作用所确定. 若B是F的正规扩张，这些同构均为自同构，但此时左陪集恰由商群 G/G_B的元素组成. 因此，每个B的自同构与G/G_B的唯一一个元素对应. 由于G/G_B的运算为映射的复合，所以上述对应是G/G_B域B的$F-$自同构群的同构关系. 至此，我们完成了定理的证明.

例 8.4.1 设$\omega = e^{\frac{2\pi i}{3}}$为 1 的 3 次单位根，易知$\mathbf{Q}(\sqrt[3]{2},\omega)$为$\mathbf{Q}$的关于$x^3-2=0$的扩张，进而$\mathbf{Q}(\sqrt[3]{2},\omega)$为$x^3-2$在$\mathbf{Q}$上的分裂域，又$x^3-2$为$\mathbf{Q}$上的可分多项式，进而$\mathbf{Q}(\sqrt[3]{2},\omega)$为$\mathbf{Q}$的 Galois 扩张.

$\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$的阶为 6. 但阶为 6 的群只有整环$\mathbf{Z}_6$和对称群$S_3$两个. 哪一个才是$G=\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$呢？ 由于$\mathbf{Q}(\sqrt[3]{2})$不是$\sqrt[3]{2}$的最小多项式$x^3-2$的分裂域，中间域$\mathbf{Q}(\sqrt[3]{2})$不是$\mathbf{Q}$的 Galois 扩张. 因此，对应的子群不是$G$的正规子群.

然而，交换群的子群均为正规子群，而G 的上述子群不是正规子群，所以G不是$\mathbf{Z}_6$，而是S_3. 下面我们进一步讨论G在$\mathbf{Q}(\sqrt[3]{2},\omega)$上的作用，以及$\mathbf{Q}(\sqrt[3]{2},\omega)$的$\mathbf{Q}$自同构群.

设

$$\sigma:\ \sqrt[3]{2} \to \sqrt[3]{2}\,\omega, \omega \to \omega$$

$$\tau:\ \sqrt[3]{2} \to \sqrt[3]{2}, \omega \to \omega^2$$

显然σ,τ为$\mathbf{Q}(\sqrt[3]{2},\omega)$的$\mathbf{Q}$自同构，$\sigma$的阶为 3，$\tau$的阶为 2，$\sigma\tau \neq \tau\sigma$. 从而$G$的子群为：

$$<\mathrm{id}>, <\sigma>, <\tau>, <\sigma\tau>, <\sigma^2\tau>,\ G.$$

相应$\mathbf{Q}(\sqrt[3]{2},\omega)$和$\mathbf{Q}$中间的不变域为：

$$\mathbf{Q}(\sqrt[3]{2},\omega), \mathbf{Q}(\omega), \mathbf{Q}(\sqrt[3]{2}), \mathbf{Q}(\omega^2\sqrt[3]{2}), \mathbf{Q}(\omega\sqrt[3]{2}), \mathbf{Q}.$$

我们可以通过求不变域、域扩张的维数证明上述子域恰对应于上述子群，这里留作习题.

例 8.4.2 设$K=\mathbf{Q}(\sqrt{3},\sqrt{5})$，容易验证$K$为$(x^2-3)(x^2-5)$在$\mathbf{Q}$上的分裂域，进而为$\mathbf{Q}$的 Galois 扩张，且$G=\mathrm{Gal}(K/\mathbf{Q})=\mathrm{Gal}(\mathbf{Q}(\sqrt{3},\sqrt{5})/\mathbf{Q})$的阶为 4. $\mathrm{Gal}(K/\mathbf{Q})$中的 4 个元素由下列构成：

$$\mathrm{id}:\ \sqrt{3} \to \sqrt{3}, \sqrt{5} \to \sqrt{5}$$

$$\sigma:\ \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to \sqrt{5}$$

$$\tau:\ \sqrt{3} \to \sqrt{3}, \sqrt{5} \to -\sqrt{5}$$

$$\sigma\tau:\ \sqrt{3} \to -\sqrt{3}, \sqrt{5} \to -\sqrt{5}$$

且$\sigma^2=\tau^2=\mathrm{id}$. 从而$\mathrm{Gal}(K/\mathbf{Q})=<\sigma><\tau>\cong \mathbf{Z}_2\times\mathbf{Z}_2$有如下的子群：

$$<\mathrm{id}>, <\sigma>, <\tau>, <\sigma\tau>,\ G$$

相应的中间域（作为不变子域）为：

$$K=\mathbf{Q}(\sqrt{5}), \mathbf{Q}(\sqrt{3}), \mathbf{Q}(\sqrt{15}), \mathbf{Q}.$$

例 8.4.3 设p为素数，$\omega=e^{2\pi i/p}$为 1 的p次单位根，$K=\mathbf{Q}(\omega)$，容易验证K为x^p-1在$\mathbf{Q}$上的分裂域，进而为$\mathbf{Q}$的 Galois 扩张，且$G=\mathrm{Gal}(K/\mathbf{Q})=\mathrm{Gal}(\mathbf{Q}(\omega))/\mathbf{Q})$的阶为$p$.

由定理 6.5.7 知，阶为p的群为循环群，故G为循环群$<\sigma>=\{\sigma,\sigma^2,\cdots,\sigma^{p-1},\sigma^p=\mathrm{id}\}$，其中$\sigma^k$满足：$\sigma^k(\omega)=\omega^k, 1\le k\le p$. 故$\mathrm{Gal}(K/\mathbf{Q})\cong\mathbf{Z}_p$.

习题 8.4

A 组

1. 证明定理 8.4.1.
2. 求 $K=\mathbf{Q}(\sqrt{3},\sqrt{5},\sqrt{7})$ 对于 $\mathbf{Q}$ 的 Galois 群，以及其所有子群和相应的不变子域.
3. 设 r 是$x^3+x^2-2x+1\in\mathbf{Q}[x]$的一个根，证明$r^2-2$也是一个根，$\mathbf{Q}(r)$是 $\mathbf{Q}$ 的正规扩张，求 $\mathrm{Gal}(\mathbf{Q}(r))/\mathbf{Q})$.
4. (1)设$\omega=e^{2\pi i/8}$，求 $K=\mathbf{Q}(\omega)$ 对于 $\mathbf{Q}$ 的 Galois 群，以及其所有子群和相应的不变子域.
   (2)设n为正整数，$\omega=e^{2\pi i/n}$，求 $K=\mathbf{Q}(\omega)$ 对于 $\mathbf{Q}$ 的 Galois 群，以及其所有子群和相应的不变子域.

B 组

5. 设$f(x)$为域F上无重根的首一多项式，K 是$f(x)$的分裂域，且 K 在上有分解$f(x)=\prod_{i=1}^{m}(x-\alpha_i)$，则
   (1) $\mathrm{Gal}(K/F)$ 与置换群$S_{\{\alpha_1,\cdots,\alpha_m\}}$的一个子群 G 同构;
   (2)对于任意α_i,α_j存在$\sigma\in G$使得$\sigma(\alpha_i)$=α_j当且仅当$f(x)$在域F上不可约.
6. (1) 设 $K\subseteq N$ 为域 F 的 Galois 扩张，说明下列映射φ：$\mathrm{Gal}(N/F)\to\mathrm{Gal}(K/F)$满足$\varphi(\sigma)=\sigma|_K$是群的满同态，因此，$\mathrm{Gal}(K/F)=\{\sigma|_K\mid\sigma\in\mathrm{Gal}(N/F)\}$，并由此说明 $\ker(\varphi)$= $\mathrm{Gal}(N/K)$.
   (3) 设 K、L 为域 F 的 Galois 扩张，说明上述映射可诱导群的单同态：
   $$\mathrm{Gal}(KL/F)\to\mathrm{Gal}(K/F)\oplus\mathrm{Gal}(L/F),$$
   并说明此映射为满射当且仅当 $K\cap L=F$.

7. 设 K 为域 F 的有限 Galois 扩张，证明：存在 $a\in K$ 使得$\{\sigma(a)|\ \sigma\in\mathrm{Gal}(K/F)\}$构成 K 作为 F 上线性空间的一组基.

8.5 有限域

我们将元素个数有限的域称为有限域. 在这节中，我们简要介绍有限域的结构和若干代数性质.

定义 8.5.1 包含元素个数有限的域称为**有限域**，或者**伽罗瓦域**.

在本章第二节中,我们知道有限域的特征必为素数. 通过前面的学习我们已经知道，对于任一素数 p，一定存在特征为 p 的有限域$\mathbf{Z}/p\mathbf{Z}=\mathbf{Z}_p$. 事实上，$\mathbf{Z}_p$是最简单的有限域，它含有$p$个元素，但是，有限域不仅仅包含这种形式. 我们在 7.4 节介绍过环与其极大理想的商环构成域，构造$\mathbf{Z}_p[x]/<f(x)>$，其中$f(x)$为$\mathbf{Z}_p[x]$上 n 次不可约多项式，即可得到造元素个数为p^n的有限域.

例 8.5.1 构造元素个数为p^n的有限域.

解: 取$f(x)$为$\mathbf{Z}_p[x]$上的n次不可约多项式，则容易证明$<f(x)>$为环$\mathbf{Z}_p[x]$的极大理想，进而$\mathbf{Z}_p[x]/<f(x)>$构成域.

此外，显然$\mathbf{Z}_p[x]/<f(x)>$由所有系数在$\mathbf{Z}_p$上的，次数小于等于 n-1 的多项式构成. 由

于满足上述多项式有p^n，则$\mathbf{Z}_p[x]/<f(x)>$为元素个数为p^n的有限域.

值得指出的是，若取α为上述$f(x)$的根，则$\mathbf{Z}_p(\alpha)$为$\mathbf{Z}_p$的 n 次扩张，进而$\mathbf{Z}_p(\alpha)$为元素个数为p^n的有限域.

实际上，由定理 8.2.4 可知，上述构造的两个域是同构的.

定理 8.5.1 设 F 是一有限域，具有 q 个元素，则有以下结论:

(1) 存在素数 p 使得 $\mathbf{Z}_p \subseteq F$;

(2) 存在正整数 n 使得 $q=p^n$;

(3) $\forall \alpha \in F$ 有$\alpha^q = \alpha$.

证明： (1)因为 F 有限，所以其特征 ch$F$ 必为一素数p，故包含素域$\mathbf{Z}_p$作为其子域;

(2)将 F 视为$\mathbf{Z}_p$上的线性空间，因为 F 有限，故存在正整数 n 使得$\dim_{\mathbf{Z}_p}(F)=n$，因而存在中的一组基$\alpha_1,\cdots,\alpha_n$，使得 F 上的元素可以被其唯一的线性表出为$a_1\alpha_1+\cdots+a_n\alpha_n$，其中$a_1,\cdots,a_n \in \mathbf{Z}_p$.

(3) $F^*=F\backslash\{0\}$构成循环群，$\alpha^{q-1}=1$，进而$\alpha^q=\alpha$.

至此，我们得出结论：所有有限域都是由素数的幂（p^n）个元素构成的，记为F_{p^n}.

下面给出F_{2^3}的例子.

例 4.4.1 求F_{2^3}的元素和以不可约多项式 x^3+x+1 为生成多项式的加法表与乘法表.

解 设F_{2^3}中的元素为$a_2x^2+a_1x+a_0\,(a_2,a_1,a_0\in\mathbf{Z}_2)$，根据$a_2,a_1,a_0$的不同取值，可得

a_2	a_1	a_0	$a_2x^2+a_1x+a_0$
0	0	0	0
0	0	1	1
0	1	0	x
0	1	1	$x+1$
1	0	0	x^2
1	0	1	x^2+1
1	1	0	x^2+x
1	1	1	x^2+x+1

所以F_{2^3}的元素为

$$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1.$$

其加法群的群表与乘法群的群表分别如表 8.5.1 和表 8.5.2 所示.

表 8.5.1 F_{2^3}的加法表

+	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	x+1	0	1

x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

表 8.5.2 GF (2^3)的乘法表

×	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	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

例 8.5.3 给素域 $\mathbf{Z}/5\mathbf{Z}$ 添加一个 2 的平方根，可以构造有限域 $\mathbf{Z}_5[x]/((x^2-2))$.

首先注意到在 $\mathbf{Z}/5\mathbf{Z}$ 中 2 不是二次剩余(不存在 2 的平方根)，因此二次多项式 x^2-2 在 $\mathbf{Z}_5$ 上是不可约多项式，于是 $\mathbf{Z}_5[x]/(x^2-2)$ 构成有限域，它实际上就是F_{5^2}. F_{5^2}的 25 个元素为$[ax+b]$,$0\le a\le 4$，$0\le b\le 4$. $\mathbf{Z}_5$ 是 $\mathbf{Z}_5[x]/(x^2-2)$ 的子域，并且有 $x^2\equiv 2 \bmod (x^2-2)$，所以$[x]$就是 2 的平方根.

定理 8.5.2 对于任一素数 p 和任一正整数 n，必然存在阶为 p^n 的有限域，并且在同构意义下，这样的有限域是唯一的.

证明： 作 $\mathbf{Z}_p$ 上的多项式$f(x)=x^{p^n}-x$，由上一定理知，元素个数为p^n的有限域，满足对$\forall\alpha\in F$ 有 $f(\alpha)=\alpha^{p^n}-\alpha=0$. 故该有限域为$f(x)$在 $\mathbf{Z}_p$ 上的分裂域，进而由定理 8.3.2 推论知，元素个数为p^n的有限域在同构意义下唯一.

定理 8.5.3 p 是素数，n 是正整数，则$\mathrm{Gal}(F_{p^n}/F_p)$是 n 阶循环群.

证明： 我们在前面已经证明F_{p^n}中任意元素α满足$\alpha^{p^n}-\alpha=0$，于是由使得$\sigma(\alpha)=\alpha^p$定义的 $\sigma\in\mathrm{Gal}(K/F)$满足$\sigma^n=\mathrm{id}$,$\sigma$生成一个 n 阶循环群.

由于 $F_{p^n}=\mathbf{Z}_p(\theta)=\{\theta^i|1\le i\le p^n-1\}\cup\{0\}$，多项式$f(x)=\prod_{i=1}^{n}(x-\theta^{p^i})$的系数是$\theta^{p^i}(1\le i\le n-1)$的对称多项式.

设$f(x)$的一单项式系数为$g=g(\theta,\theta^p,\cdots,\theta^{p^{n-1}})$，注意到这里涉及的所有域的特征均为 p，我们有$g^p=g(\theta^p,\theta^{p^2},\cdots,\theta)=g\left(\theta,\theta^p,\cdots,\theta^{p^{n-1}}\right)=g$. 又$x^p-x=0$ 有 p 个根，则$g\in\mathbf{Z}_p$，进而$f(x)\in\mathbf{Z}_p[x]$.

对任意$\varphi\in\mathrm{Gal}(F_{p^n}/F_p)$，有$\varphi f(x)=f(x)=\prod_{i=1}^{n}(x-\varphi(\theta)^{p^i})$，进而$\varphi(\theta)=\theta^{p^i},\varphi=\sigma^i$，定理得证.

定理 8.5.3 p 是素数，n 是正整数，q=p^n,F_q是 q 元有限域，则

(1) 映射σ：$a\to a^p$ 为F_q的F_p-自同构群，且$\sigma^n=\mathrm{id}$, ;

(2) 上述σ为 n 阶循环群$\mathrm{Gal}(F_{p^n}/F_p)$的生成元. 进一步地，$k$ 是任意正整数，则σ：$a\to a^q$为 k 阶循环群$\mathrm{Gal}(F_{q^k}/F_q)$的生成元.

我们称上述σ：$a\to a^q$为 **Frobenius 自同构**.

证明： 留做习题.

定理 8.5.4　F_{p^n}的乘法群${F_{p^n}}^*$是循环群.

证明： 设 $t \leq q-1$为乘法群${F_{p^n}}^*$中元素最大的阶. 根据交换群的性质，我们有${F_{p^n}}^*$中任意元素的阶均为 t 的因子，所以F_{p^n}中任意元素为$x^{t+1}-x$=0 的根，进而 $t \geq q-1$，故 $t = q-1$.

定义 8.5.2　乘法群${F_{p^n}}^*$的生成元称为F_{p^n}的初始元.

定理 8.5.5　设 g 是F_{p^n}的初始元，则F_{p^n}的初始元恰为集合$\{g^m | m \in Z, 1 \leq m \leq p^n - 1$ 且$(m, p^n - 1) = 1\}$.

证明： 即证阶数为p^n −1 的循环群的生成元，根据第 3 章既约剩余系的概念可易得.

推论　F_{p^n}有$\varphi(p^n - 1)$个初始元，其中φ为欧拉函数.

下面我们给出F_{p^n}的扩张与分裂域的结论.

定理 8.5.6　q=p^n，$\bigcup_{i=1}^{\infty} F_{q^i}$为$F_q$的代数闭包.

证明：参考文献[9].

习题 8.5

A 组

1. 求$\mathbf{Z}_2[x]$所有次数不大于 4 的不可约多项式.
2. 求$\mathbf{Z}_3[x]$所有二次不可约多项式.
3. p 是素数, k 是正整数, q=p^k，则F_{q^n}是F_{q^n}子域当且仅当 n 整除 m.
4. 对于任一正整数 n，证明: $\mathbf{Z}_p[x]$中存在 n 次不可约多项式.
5. 证明: $\mathbf{Z}_p[x]$中有无穷多个不可约多项式.

B 组

6. 证明定理 8.5.3.
7. 给定有限域$F_q, a \in F_q$，则存在$b \in F_q$使得 a=b^k当且仅当 gcd(k,q-1)=1.