第一章 Galois 理论

我们在本章系统讨论 Galois 理论. 前四节是 Galois 理论的核心, 第 5 节给出 Galois 基本定理及其推论. 作为应用, 利用 Galois 理论与 Sylow 定理给出了代数基本定理的一个证明.

Galois 理论的主要思想是, 将每一个域扩张对应于一个群: Galois 群. 于是将域论问题转化为群论问题. 由于有限维扩张的 Galois 群总是有限的, 故可以利用有限群的数字信息来研究域扩张. 于是, 数学史上困扰了人们数个世纪的若干难题可以由域论解决. 作为域论的应用, 我们在第三章给出若干著名尺规作图不可能问题的证明, 同时也确定次数大于等于 5 的多项式方程为什么不能根式求解.

1. 域扩张

我们在本节研究域论, 将给出一些基本概念的定义, 同时给出大量的例子以帮助读者理解相关的概念, 我们假设读者熟悉环论与向量空间的一些基本事实.

域论主要研究域的扩张问题. 事实上, 经典的尺规作图问题与域上一元多项式方程的根式可解性都是通过分析适当的域扩张来解决的, 我们将在第三章给出这些问题的解答.

域是一个非零元构成乘法群的交换幺环, 且 $1\neq 0$. 如果域 F 含于域 K, 就称 K 是 F 的**扩域**, F 是**基础域**, K/F 为**域扩张**. 对域扩张 K/F, K 可视为域 F 上的向量空间, 简称 $F-$ 空间, 其**维数** $\dim_F K$ 也记为 $[K:F]$, 根据域扩张维数的有限性, 分为**有限扩张**与**无限扩张**.

本章主要讨论有限扩张.

例 1.1 常见的域. 有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$, 复数域 $\mathbb{C}$, 模素数 p 的剩余类域

$$\mathbb{F}_p=\{0,1,2,\cdots,p-1\}.$$

$\mathbb{Q}$ 与 $\mathbb{F}_p$ 是最常见的基础域. 有理数域上的有限维扩张称为**代数数域**, 它是代数数论中的主要研究对象, 如 $\mathbb{Q}\left(\sqrt{2}\right),\mathbb{Q}\left(\sqrt{3}+\mathrm{i}\sqrt[4]{5}\right)$ 等.

例 1.2 域 k 上单个不定元的有理函数域 $k(x)=\left\{\dfrac{f(x)}{g(x)}\middle| f(x),g(x)\in k[x],g(x)\neq 0\right\}$.

域 k 上 n 个不定元 $x_1,\cdots,x_n$ 的有理函数域

$$k(x_1,\cdots,x_n)=\left\{\frac{f(x_1,\cdots,x_n)}{g(x_1,\cdots,x_n)}\middle| f,g\in k[x_1,\cdots,x_n],g\neq 0\right\}.$$

例 1.3 域 k 上的 Laurent 级数: $k((x))=\left\{\sum\limits_{n=n_0}^{+\infty}a_nx^n\middle| n_0\in\mathbb{Z},a_n\in k\right\}$. 它是函数域 $k(x)$ 的一个扩域. 其中乘法是通常多项式乘法的推广:

$$\sum_{n=n_0}^{+\infty} a_n x^n \sum_{n=n_1}^{+\infty} b_n x^n = \sum_{n=n_0+n_1}^{\infty} \left(\sum_{k=n_0}^{n-n_1} a_k b_{n-k} \right) x^n = \sum_{n=n_0+n_1}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n .$$

习题: 证明如上定义的 $k((x))$ 是一个域.

提示: 对系数递归, 形如 $1+a_1 x+a_2 x^2+\cdots$ 的元可依次求得其逆元的系数 $b_0, b_1, b_2, \cdots$.

例 1.4 2 维域扩张 $\mathbb{C}/\mathbb{R}$, 复数域视为实数域上的向量空间, 具有基 $\{1, \mathrm{i}\}$.

复数域与实数域都可以视为有理数域的扩域.

若 $\alpha \in \mathbb{C}$, 我们将在命题 1.8 证明

$$\mathbb{Q}(\alpha) = \left\{ \left. \frac{\sum_i a_i \alpha^i}{\sum_i b_i \alpha^i} \right| a_i, b_i \in \mathbb{Q}, \sum_i b_i \alpha^i \neq 0 \right\}.$$

是有理数域的一个扩域. 域扩张 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 的有限性取决于 α 的选取.

例如, 若 $\alpha = \sqrt{-1} = \mathrm{i}$ 或 $\alpha = \exp(2\pi \mathrm{i}/3) = \cos(2\pi \mathrm{i}/3) + \mathrm{i}\sin(2\pi \mathrm{i}/3)$ 时, $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$, 这可以作为命题 1.15 的推论得到. 另一方面, 我们将在 14 节证明 $[\mathbb{Q}(\pi):\mathbb{Q}] = \infty$.

若 α 是某个有理数域上多项式 $f(x) \in \mathbb{Q}[x]$ 的根, 称 α 是**代数元**, 相应域扩张 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 称为**代数扩张**. 若 α 不是有理数域上任一非零多项式的根, 称 α 是**超越元**, 相应的域扩张 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 称为**超越扩张**. 如 $\mathbb{Q}(\pi)/\mathbb{Q}, \mathbb{Q}(x)/\mathbb{Q}$ 都是超越扩张.

例 1.5 设 k 是域, $K := k(t)$ 是不定元 t 的有理函数域, $f \in K$ 是非零元, 令

$$F = k(f) = \left\{ \left. \frac{\sum_i a_i f^i}{\sum_j b_j f^j} \right| a_i, b_j \in k, \sum_j b_j f^j \neq 0 \right\}.$$

比如 $f(t) = t^2$ 时, K/F 是 2 维域扩张, 具有一组基 $\{1, t\}$:

任一 t 的多项式均可唯一写成 $th(f) + h_1(f)$ 的形式, 其中 h, h_1 是多项式, 于是 K 中元均可写成 $\dfrac{th(f)+g_1(f)}{th(f)+h_1(f)}$ 的形式, 类似于带根号的分式有理化,有

$$\frac{th(f)+g_1(f)}{th(f)+h_1(f)} = \frac{(tg(f)+g_1(f))(th(f)-h_1(f))}{(th(f)+h_1(f))(th(f)-h_1(f))} = \frac{tm(f)+n(f)}{s(f)} = t\frac{m(f)}{s(f)} + \frac{n(f)}{s(f)} \cdots$$

在例 1.17 将证明, 如果 f 是非常数的多项式, 则 K/F 是有限维域扩张. 在第五章将证明 Luroth 定理: 如果域 L 是 K/k 的中间域, 即 $k \subseteq L \subseteq K$, 那么 L 必然形如 $k(f)$ 对某个 $f \in K$.

例 1.6 $K:=\mathbb{Q}[t]/(t^3-2)$，可将 $p(t)=t^3-2$ 换成有理数域上任一 n 次不可约多项式，此时将得到有理数域的一个 n 维扩域，该扩域包含给定多项式 $p(t)=t^3-2$ 的一个根.

定义 1.7 **生成子环** $F[X]=F[a_1,\cdots,a_n]$，**生成子域** $F(X)=F(a_1,\cdots,a_n)$.

直接验证知域的子域(子环)之交仍为子域(子环). 因此 $F(X)$ 是域 K 的包含域 F 与子集 X 的最小的子域.

设 K/F 是域扩张，$a\in K$，称

$$\mathrm{ev}_a: F[x]\to K, f(x)\mapsto f(a), \forall f(x)\in F[x]$$

为**取值同态(evaluation homomorphism)**，记 $\mathrm{ev}_a(f(x))$ 为 $f(a)$. 直接验证知 ev_a 既是环同态也是 $F-$ 线性映射.

命题 1.8 设 K/F 是域扩张，$a\in K$，则 $F[a]=\{f(a)\mid f(x)\in F[x]\}$，且

$$F(a)=\left\{\frac{f(a)}{g(a)}\middle| f,g\in F[x], g(a)\neq 0\right\}.$$

进而，$F(a)$ 是 $F[a]$ 的商域.

命题 1.9 设 K/F 是域扩张，$a_1,\cdots,a_n\in K$，则

$$F[a_1,\cdots,a_n]=\{f(a_1,\cdots,a_n)\mid f\in F[x_1,\cdots,x_n]\},$$

且

$$F(a_1,\cdots,a_n)=\left\{\frac{f(a_1,\cdots,a_n)}{g(a_1,\cdots,a_n)}\middle| f,g\in F[x_1,\cdots,x_n], g(a_1,\cdots,a_n)\neq 0\right\}.$$

进而，$F(a_1,\cdots,a_n)$ 是 $F[a_1,\cdots,a_n]$ 的商域.

命题 1.10 设 K/F 是域扩张，$X\subseteq K$，如果 $\alpha\in F[X]$，则 $\alpha\in F(a_1,\cdots,a_n)$ 对某些 $a_1,\cdots,a_n\in X$. 因此 $F(X)=\cup\{F(a_1,\cdots,a_n)\mid a_1,\cdots,a_n\in X\}$，对 X 的全部有限子集取并.

定义 1.11 设 K/F 是域扩张，$\alpha\in K$ 称为**在 F 上代数**是指存在非零多项式 $f(x)\in F[x]$ 使得 $f(\alpha)=0$. 若 $\alpha\in K$ 不在 F 上代数则称 a **在 F 上超越**. 如果 K 的每一个元都在 F 上代数，就称 **K 在 F 上代数**，称 K/F 是**代数扩张**.

定义 1.12 设 α 在域 F 上代数，α 在 F 上的**最小多项式**是指 $F[x]$ 中以 α 为根的次数最小的首 1 多项式，通常记为 $\min(F,\alpha)$. 事实上是取值同态 ev_α 之核的首 1 生成元.

$\min(F,\alpha)$ 是 F 上不可约的多项式.

例 1.13 虚单位 $\mathrm{i}=\sqrt{-1}$ 在有理数域上代数:

$$\min(\mathbb{Q},\mathrm{i})=x^2+1=\min(\mathbb{R},\mathrm{i}),\ \min(\mathbb{C},\mathrm{i})=x-\mathrm{i}.$$

若 $r\in\mathbb{Q}$，则 $\sqrt[n]{r}$ 是 x^n-r 的根从而在有理数域上代数. 一般来说，最小多项式与基础域相关.

$\omega=\exp\left(\frac{2\pi\mathrm{i}}{n}\right)=\cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}$ 满足 $\omega^n-1=0$，故 ω 在有理数域上代数，我们将在第 7 节确定 $\min(\mathbb{Q},\omega)$.

例 1.14 1873 年, Hermite 证明了 e 在有理数域上是超越元, 9 年后 Lindermann 证明了 π 在有理数域上的超越性. 不过 π 在 $\mathbb{Q}(\pi)$ 上代数，它是 $x-\pi\in\mathbb{Q}(\pi)[x]$ 的根. 人们目前还不知道 e 是否在 $\mathbb{Q}(\pi)$ 上超越. 我们将在 14 节证明 π 与 e 在有理数域上超越.

命题 1.15 设 K/F 是域扩张，$\alpha\in K$ 在 F 上代数. 则

(1) a 的最小多项式 $\min(F,\alpha)$ 在 F 上不可约;

(2) 设 $g(x)\in F[x]$，则: $g(\alpha)=0\Leftrightarrow\min(F,\alpha)\mid g(x)$;

(3) 令 $n=\deg(\min(F,\alpha))$，则 $[F(\alpha):F]=\deg(\min(F,\alpha))<\infty$，此时 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 是 $F(\alpha)$ 的一组 $F-$ 基，进而 $F(\alpha)=F[\alpha]$.

例 1.16 $\sqrt[3]{2}$ 是多项式 $x^3-2\in\mathbb{Q}[x]$ 的根，由 Eisenstein 判别法知该 x^3-2 在 $\mathbb{Q}$ 上不可约，所以 x^3-2 是 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的最小多项式. 所以 $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$.

如果 p 是素数，则由 Eisenstein 判别法知 x^n-p 在 $\mathbb{Q}$ 上不可约，故 $\left[\mathbb{Q}\left(\sqrt[n]{p}\right):\mathbb{Q}\right]=n$.

复数 $\omega=\cos\frac{2}{3}\pi+\mathrm{i}\sin\frac{2}{3}\pi$ 是 $\mathbb{Q}$ 上多项式 x^3-1 的根，x^3-1 在 $\mathbb{Q}$ 上分解为

$$x^3-1=(x-1)\left(x^2+x+1\right),$$

注意到 x^2+x+1 以 ω 为根，在 $\mathbb{Q}$ 上无根从而在 $\mathbb{Q}$ 上不可约，它是 ω 在 $\mathbb{Q}$ 上的最小多项式. 所以 $[\mathbb{Q}(\omega):\mathbb{Q}]=2$.

设 p 是素数, 令 $\rho=\cos\frac{2}{p}\pi+\mathrm{i}\sin\frac{2}{p}\pi$, 则 ρ 满足 $\mathbb{Q}$ 上多项式 x^p-1, 且

$$x^p-1=(x-1)\left(x^{p-1}+x^{p-2}+\cdots+x+1\right),$$

而 $x^{p-1}+x^{p-2}+\cdots+x+1$ 以 ρ 为根, 做变换 $x=y+1$ 知其在 $\mathbb{Q}$ 上不可约(参见习题 22), 是 ρ 在 $\mathbb{Q}$ 上的最小多项式. 所以 $\left[\mathbb{Q}(\rho):\mathbb{Q}\right]=p-1$.

例 1.17 设 $K=k(t)$ 是域 k 上不定元 t 的有理函数域. 设 $u\in K-k$, 记 $u=\dfrac{f(t)}{g(t)}$, 其中 $f,g\in k[t]$ 且 $\left(f(t),g(t)\right)=1$, 令 $F=k(u)$, 断言

$$[K:F]=\max\left\{\deg\left(f(t)\right),\deg\left(g(t)\right)\right\},$$

这表明 K/F 是一个有限扩张.

例 1.18 设域 $K=F(a_1,\cdots,a_n)$ 是域 F 上的有限生成扩张, 令 $L_i=F(a_1,\cdots,a_i)$, 令 $L_0=F$, 则有子域升链

$$F=L_0\subseteq L_1\subseteq L_2\subseteq\cdots\subseteq L_n=K,$$

且 $L_{i+1}=L_i(\alpha_{i+1})$. 即, 将有限生成的域扩张 K/F 分解为一系列的由单个元生成的子扩张 L_{i+1}/L_i, 而命题 1.15 及类似的结论有助于研究子扩张 L_{i+1}/L_i. 为此, 需要证明若干传递性的结论.

K 是**域 F 上有限生成向量空间**: 若存在 $a_1,\cdots,a_n$ 使得任一 K 中元均可表为 $a_1,\cdots,a_n$ 的 $F-$线性组合, 即 K 作为 $F-$空间的维数有限, 或 $[K:F]<\infty$;

K 是**域 F 上有限生成环**: 若存在 $a_1,\cdots,a_n\in K$ 使得 $K=F[a_1,\cdots,a_n]$;

K 是**域 F 上有限生成扩域**: 若存在 $a_1,\cdots,a_n\in K$ 使得 $K=F(a_1,\cdots,a_n)$.

引理 1.19 设 K/F 是有限扩张, 则 K/F 是有限生成扩张与代数扩张.

证明 设 $\alpha_1,\cdots,\alpha_n$ 是 K 的一组 $F-$基. 则 K 中任一元均形如 $\sum\limits_{1\le i\le n}c_i\alpha_i$, 因此

$$K=F(\alpha_1,\cdots,\alpha_n),$$

所以 K 是 F 上有限生成的扩域.

任取 $a\in K$, 则 K 中 $n+1$ 个元 $1,a,a^2,\cdots,a^n$ $F-$线性相关, 故存在 $c_0,c_1,\cdots,c_n\in F$ 使得

$$c_0 1 + c_1 a + c_2 a^2 \cdots + c_n a^n = 0,$$

令 $f(x) = \sum_{0 \le i \le n} c_i x^i$，则 $f(x) \in F[x]$ 使得 $f(a) = 0$，故 a 在 F 上代数，即 K 在 F 上代数.■

命题 1.20(望远镜公式) 设 $F \subseteq L \subseteq K$ 都是域，则 $[K:F] = [K:L] \cdot [L:F]$.

命题 1.21 设 K/F 是域扩张. 如果每一个 $a_i \in K$ 都在 F 上代数，则 $F[a_1, \cdots, a_n]$ 是 F 上的有限维域扩张，且 $[F[a_1, \cdots, a_n]:F] \le \prod_{i=1}^{n} [F[\alpha_i]:F]$.

即：有限生成的代数扩张都是有限扩张.

证明 对 n 用归纳法.

$n = 1$ 时由命题 1.15 知单代数扩域 $F[a_1]$ 是有限维扩域，命题为真.

令 $L = F[a_1, \cdots, a_{n-1}]$，由归纳假设知 L 是域，且 $[L:F] \le \prod_{i=1}^{n-1} [F[\alpha_i]:F]$.

注意到 $\min(L, \alpha_n) \mid \min(F, \alpha_n)$，由命题 1.15 知 $[F[a_1, \cdots, a_n]:L] = [L[\alpha_n]:L] \le [F[\alpha_n]:L]$，所以

$$[F[a_1, \cdots, a_n]:F] = [F[a_1, \cdots, a_n]:L][L:F] \le [F[\alpha_n]:F] \prod_{i=1}^{n-1} [F[\alpha_i]:F] = \prod_{i=1}^{n} [F[\alpha_i]:F].■$$

例： $a = \sqrt[4]{2}, b = \sqrt[4]{18}$，则 $[\mathbb{Q}(a):\mathbb{Q}] = [\mathbb{Q}(b):\mathbb{Q}] = 4$，$[\mathbb{Q}(a,b):\mathbb{Q}] = 8$，即如上不等式取严格不等号.

对素数 2 用 Eisenstein 判别法知二者的零化多项式 $f(x) = x^4 - 2$ 与 $g(x) = x^4 - 18$ 在有理数域上是不可约的，这表明 $[\mathbb{Q}(a):\mathbb{Q}] = [\mathbb{Q}(b):\mathbb{Q}] = 4$.

另一方面，$\mathbb{Q}(a,b) = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2} \cdot \sqrt{3}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$.

下证 $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}):\mathbb{Q}] = 8$. 首先 $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}):\mathbb{Q}] \le [\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 8$.

其次，$\sqrt{3} \notin \mathbb{Q}(\sqrt[4]{2})$，否则，设 $\sqrt{3} = r + s\sqrt[4]{2} + u\sqrt[4]{4} + v\sqrt[4]{8}, r, s, u, v \in \mathbb{Q}$，则

$$3 = (r + s\sqrt[4]{2} + u\sqrt[4]{4} + v\sqrt[4]{8})(r + s\sqrt[4]{2} + u\sqrt[4]{4} + v\sqrt[4]{8})$$

$$= (r^2 + 4sv + 2u^2) + 2(rs + uv)\sqrt[4]{2} + 2(ru + sv)\sqrt[4]{4} + 2(rv + su)\sqrt[4]{8},$$

于是 $\begin{cases} r^2 + 4sv + 2u^2 = 3, & (1) \\ rs + uv = 0, \\ ru + sv = 0, \\ rv + su = 0, \end{cases}$ (*)，故 $\begin{cases} r^2 - 4ru + 2u^2 = 3, & (2) \\ (r-s)(u-v) = 0, \\ (r-u)(s-v) = 0, \\ (r-v)(s-u) = 0, \end{cases}$

由 $(r-u)(s-v) = 0$ 知 $r = u$ 或 $s = v$，若 $r = u$，代入(1)得 $-r^2 = 3$，这与 $r \in \mathbb{Q}$ 矛盾！所以 $r \ne u$ 且 $s = v$，此

时(*)变为$\begin{cases} r^2-4ru+2u^2=3, \\ s(r+u)=0, \\ ru+s^2=0, \end{cases}$.

若$r+u=0$，代入(2)得$6r^2=3$，于是$\sqrt{2}=\pm 2r\in\mathbb{Q}$，矛盾!

所以$r+u\neq 0$，于是由$s(r+u)=0$知$s=0$，代入$ru+s^2=0$得$ru=0$，所以$r=0$或$u=0$，代入(2)得$2u^2=3$或者$r^2=3$，得到$\sqrt{6}$或$\sqrt{3}\in\mathbb{Q}$，矛盾!

故$\left[\mathbb{Q}(a,b):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt[4]{2},\sqrt{3}\right):\mathbb{Q}\right]=8<\left[\mathbb{Q}(a):\mathbb{Q}\right]\cdot\left[\mathbb{Q}(b):\mathbb{Q}\right]$.■

推论 1.22 设K/F是域扩张. $a\in K$，则: a在F上代数$\Leftrightarrow\left[F(a):F\right]<\infty$.

进而，若$\left[K:F\right]<\infty$，则K/F是代数扩张. 即: 有限维扩张都是代数扩张.

代数扩张一般来说不一定是有限扩张. 如全体代数数所成数域K在$\mathbb{Q}$上代数，但$K/\mathbb{Q}$是代数扩张.

命题 1.23 设K/F是域扩张. K的子集X中元均在F上代数，则$F(X)$在F上代数. 如果$|X|<\infty$，则$\left[F(X):F\right]<\infty$.

证明 任取$a\in F(X)$. 由命题 1.10 知存在有限多个元$\alpha_1,\cdots,\alpha_n\in X$使得$a\in F(\alpha_1,\cdots,\alpha_n)$. 由命题 1.21 知$F(\alpha_1,\cdots,\alpha_n)$在$F$上代数，所以$a$在$F$上代数，故$F(X)$在$F$上代数.

若$|X|<\infty$，由命题 1.21 知$\left[F(X):F\right]<\infty$.■

下面来证明**代数扩张的传递性**.

定理 1.24 设$F\subseteq L\subseteq K$都是域. 若K/L与L/F都是代数扩张，则K/F也是代数扩张.

证明 任取$\alpha\in K$，由K/L代数，设$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in L[x]$是$\alpha$在$L$上的最小多项式. 由$L/F$代数知域$L_0:=F(a_0,a_1,\cdots,a_{n-1})$是$F$上的有限维扩张，由$f(x)\in L_0[x]$知$\alpha$在$L_0$上代数. 于是

$$\left[L_0(\alpha):F\right]=\left[L_0(\alpha):L_0\right]\cdot\left[L_0:F\right]<\infty.$$

由$F(\alpha)\subseteq L_0(\alpha)$知$\left[F(\alpha):F\right]\leq\left[L_0(\alpha):F\right]<\infty$，所以$\alpha$在$F$上代数. 由$\alpha$的任意性知$K/F$代数. ■

定义 1.25 设有域扩张K/F，K中在F上代数的元所成集称为F在K中的**代数闭包**.

推论 1.26 设K/F是域扩张，L是F在K中的代数闭包. 则L是域，且为F含于K中的最大代数扩张.

证明 设 $a,b\in L$，由命题 1.23 知 $F(a,b)/F$ 是代数扩张，故 $F(a,b)\subseteq L$，注意到 $a\pm b$，$ab, a/b\in F(a,b)\subseteq L$，故 L 对域运算封闭，是 K 的子域. K 中在 F 上代数的元均含于 L，故 L 是 F 的含于 K 中的最大代数扩张.■

域扩张的合成：设 K/F 是域扩张. L_1, L_2 是 K 的包含 F 的子域，K 的由 $L_1\bigcup L_2$ 生成的子域称为 L_1, L_2 的**合成域**，记为 L_1L_2，于是 $L_1L_2=L_1(L_2)=L_2(L_1)$.

引理 设 K/F 是域扩张，如果 $a\in K$ 在域 F 上代数，且 $F-$不可约首一多项式 $f(x)\in F[x]$ 使得 $f(a)=0$，则 $\min(F,a)=f(x)$.

证明 由 $\min(F,a)$ 是 a 的最小多项式，$f(x)$ 是 a 的零化多项式，以及最小多项式整除零化多项式知 $\min(F,a)\big|f(x)$；再由 $f(x)$ 在 F 上不可约 $\min(F,a)$ 与 $f(x)$ 相伴，由二者均首一知 $\min(F,a)=f(x)$.■

如下涉及的域都是复数域的子域.

例 1.27 设 $\omega=e^{\frac{2\pi i}{3}}=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}$，求 $\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)$.

解 直接计算知 $\omega^3=1, \omega^2=-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{3}, \omega^2+\omega+1=0$.

先构造一个多项式 $g(x)\in\mathbb{Z}[x]$ 使得 $g\left(\omega+\sqrt[3]{2}\right)=0$.

计算知 $(x-\omega)^3-2=x^3-3\omega x^2+3\omega^2x-\omega^3-2=x^3-\frac{3}{2}x^2+\frac{3}{3}x-3-\frac{3\sqrt{3}}{2}\mathrm{i}\left(x^2+x\right)$，于是 $\omega+\sqrt[3]{2}$ 是多项式

$$\begin{aligned}g(x)&:=\left[\left(x^3+\tfrac{3}{2}x^2-\tfrac{3}{2}x-3\right)-\tfrac{3}{2}\mathrm{i}\sqrt{3}\left(x^2+x\right)\right]\left[\left(x^3+\tfrac{3}{2}x^2-\tfrac{3}{2}x-3\right)+\tfrac{3}{2}\mathrm{i}\sqrt{3}\left(x^2+x\right)\right]\\&=\left(x^3+\tfrac{3}{2}x^2-\tfrac{3}{2}x-3\right)^2+\tfrac{27}{4}\left(x^2+x\right)^2\\&=x^6+3x^5+\left(\tfrac{9}{4}-3+\tfrac{27}{4}\right)x^4+\left(-6-\tfrac{9}{2}+\tfrac{27}{2}\right)x^3+\left(\tfrac{9}{4}-9+\tfrac{27}{4}\right)x^2+9x+9\\&=x^6+3x^5+6x^4+3x^3+9x+9\end{aligned}$$

的一个根.

断言 $\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)=\mathbb{Q}\left(\omega+\sqrt[3]{2}\right)$. 显然 $\mathbb{Q}\left(\omega+\sqrt[3]{2}\right)\subseteq\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$.

令 $a=\omega+\sqrt[3]{2}$，则 $(a-\omega)^3=2$，展开得 $a^3-3a^2\omega+3a\omega^2-\omega^3=2$，利用 $\omega^2=-1-\omega$ 得 $\omega=\dfrac{a^3-3a-3}{3a^2+3a}$，因此 $\omega\in\mathbb{Q}(a)$，于是 $\sqrt[3]{2}=a-\omega\in\mathbb{Q}(a)$，所以 $\mathbb{Q}\left(\omega+\sqrt[3]{2}\right)\supseteq\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)$，故 $\mathbb{Q}\left(\omega,\sqrt[3]{2}\right)=\mathbb{Q}\left(\omega+\sqrt[3]{2}\right)$.

由 Eisenstein 判别法知 $x^3-2\in\mathbb{Q}[x]$ 是 $\mathbb{Q}-$ 不可约的，由引理知 $\min\left(\mathbb{Q},\sqrt[3]{2}\right)=x^3-2$，于是

$$\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=\deg\left(\min\left(\mathbb{Q},\sqrt[3]{2}\right)\right)=\deg\left(x^3-2\right)=3,$$

由望远镜公式知 $3\left|\left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}\right]\right.$.

由 Eisenstein 判别法知 $x^2+3\in\mathbb{Q}[x]$ 是 $\mathbb{Q}-$ 不可约的，由引理知 $\min\left(\mathbb{Q},\mathrm{i}\sqrt{3}\right)=x^2-3$，于是

$$\left[\mathbb{Q}(\omega):\mathbb{Q}\right]=\left[\mathbb{Q}\left(-\tfrac{1}{2}+\mathrm{i}\tfrac{\sqrt{3}}{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\mathrm{i}\sqrt{3}\right):\mathbb{Q}\right]=\deg\left(\min\left(\mathbb{Q},\mathrm{i}\sqrt{3}\right)\right)=\deg\left(x^2-3\right)=2,$$

由望远镜公式知 $2\left|\left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}\right]\right.$. 于是 $6\left|\left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}\right]\right.$，因而有

$$\deg\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)=\left[\mathbb{Q}\left(\omega+\sqrt[3]{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\omega,\sqrt[3]{2}\right):\mathbb{Q}\right]\geq 6.$$

由 $g\left(\omega+\sqrt[3]{2}\right)=0$ 与 $\deg g(x)=6$ 知 $\deg\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)\leq 6$，所以

$$\deg\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)=\deg\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)=6.$$

由 $g\left(\omega+\sqrt[3]{2}\right)=0$ 知 $\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)\left|g(x)\right.$，再由 $\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)$ 与 $g(x)$ 的次数均为 6 且首一知

$$\min\left(\mathbb{Q},\omega+\sqrt[3]{2}\right)=g(x)=x^6+3x^5+6x^4+3x^3+9x+9.\blacksquare$$

例 1.28 $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$：令 $a=\sqrt{2}+\sqrt{3}$，则 $\left(a-\sqrt{2}\right)^2=3$，于是得

$$\sqrt{2}=\frac{a^2-1}{2a},\sqrt{3}=a-\sqrt{2}=\frac{a^2+1}{2a}\in\mathbb{Q}(a).$$

故 $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)\subseteq\mathbb{Q}(a)\subseteq\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. 反包含是显然的. 若令

$$f(x)=\left(x-\sqrt{2}+\sqrt{3}\right)\left(x-\sqrt{2}-\sqrt{3}\right)\left(x+\sqrt{2}+\sqrt{3}\right)\left(x+\sqrt{2}-\sqrt{3}\right)=\left[\left(x-\sqrt{2}\right)^2-3\right]\left[\left(x+\sqrt{2}\right)^2-3\right]$$

$$=\left(x^2-1-2\sqrt{2}x\right)\left(x^2-1+2\sqrt{2}x\right)=x^4-10x^2+1,$$

则 $f(a)=0$，于是 $\min\left(\sqrt{2}+\sqrt{3},x\right)\left|f(x)\right.$.

下面证明 $f(x)$ 在有理数域上不可约.

多项式 $f(x)$ 可能的有理根为 ±1，但检验后发现都不是根，故 $f(x)$ 没有一次有理因式. 因此若 $f(x)$ 在有理数域上可约，则必然是分解为 $\mathbb{Q}$ 上两个二次不可约多项式的乘积，于是在整数环上有对应的分解. 由 $f(x)$ 首 1 可设两个二次不可约因式的首项系数为 1，此时

$$x^4-10x^2+1=\left(x^2+ax+b\right)\left(x^2+cx+d\right)=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd,$$

比较常数项知 $b=d=\pm1$，比较三次项系数知 $c=-a$，此时再比较二次项系数有 $-a^2\pm2=10$，可是不存在这样的整数 a，因此该多项式在 $\mathbb{Q}$ 上不可约.

由引理知 $\min\left(\mathbb{Q},\sqrt{2}+\sqrt{3}\right)=x^4-10x^2+1$.■

注记 更一般地，设 $m,n\in\mathbb{Z}$，且 $\sqrt{n}\notin\mathbb{Q}\left(\sqrt{m}\right)$，令

$$f(x)=\left(x-\sqrt{m}+\sqrt{n}\right)\left(x-\sqrt{m}-\sqrt{n}\right)\left(x+\sqrt{m}+\sqrt{n}\right)\left(x+\sqrt{m}-\sqrt{n}\right)=\left[\left(x-\sqrt{m}\right)^2-n\right]\left[\left(x+\sqrt{m}\right)^2-n\right]$$

$$=\left(x^2+(m-n)-2\sqrt{m}x\right)\left(x^2+(m-n)+2\sqrt{m}x\right)=x^4-2(m+n)x^2+(m-n)^2,$$

则 $\min\left(\mathbb{Q},\sqrt{m}+\sqrt{n}\right)=f(x)$.

例 1.29 求 $\sqrt{3}+\sqrt[3]{2}$ 在有理数域上的最小多项式 $\min\left(\mathbb{Q},\sqrt{3}+\sqrt[3]{2}\right)$.

解 直接计算知 $\left(x-\sqrt{3}\right)^3-2=x^3+9x-2-3\sqrt{3}\left(x^2+1\right)$，令

$$f(x)=\left[\left(x^3+9x-2\right)-3\sqrt{3}\left(x^2+1\right)\right]\left[\left(x^3+9x-2\right)+3\sqrt{3}\left(x^2+1\right)\right]$$

$$=\left(x^3+9x-2\right)^2-27\left(x^2+1\right)^2=x^6-9x^4-4x^3+27x^2-18x-23,$$

如上构造过程表明 $f\left(\sqrt{3}+\sqrt[3]{2}\right)=0$.

类似于例 1.27 的讨论可知 $\min\left(\mathbb{Q},\sqrt{3}+\sqrt[3]{2}\right)=f(x)=x^6-9x^4-4x^3+27x^2-18x-23$.■

我们在第 5 节将证明，**有理数域上的有限扩张都是单扩张.**

习题 1.1

1. 设 K/F 是域扩张. 对 $c\in F,\alpha\in K$ 规定数乘为 $c\cdot\alpha:=c\alpha$ 是 K 中的乘法运算，证明 K 是一个 $F-$空间.

2. 设 K/F 是域扩张. 证明 $[K:F]=1\Leftrightarrow K=F$.

3. 设 K/F 是域扩张，$\alpha\in K$. 证明取值映射

$$\mathrm{ev}_a:F[x]\to K,f(x)\mapsto f(a),\forall f(x)\in F[x]$$

既是一个环同态，也是一个 $F-$线性映射.

4. 证明命题 1.9.

5. 证明 $\mathbb{Q}\left(\sqrt{5},\sqrt{7}\right)=\mathbb{Q}\left(\sqrt{5}+\sqrt{7}\right)$.

6. 验证多项式环的如下泛性质:

(1) 设环 A 包含域 F. 若 $a_1,\cdots,a_n\in A$，证明存在唯一的环同态 $\varphi:F[x_1,\cdots,x_n]\to A$ 使得

$\varphi(x_i)=a_i, 1\le i\le n$.

(2) 进而, 设环 B 包含域 F, 映射 $f:\{x_1,\cdots,x_n\}\to B$ 满足性质: 对任一含域 F 的环 A 与元素 $a_1,\cdots,a_n\in A$, 存在唯一的环同态 $\varphi:B\to A$ 使得 $\varphi(f(x_i))=a_i, 1\le i\le n$. 证明环 B 同构于环 $F[x_1,\cdots,x_n]$.

7. 设 A 是环. 如果 A 还是一个 $F-$空间且满足

$$\alpha(ab)=(\alpha a)b=a(\alpha b), \forall \alpha\in F, a,b\in A,$$

则称 A 是一个 $F-$代数.

如果 A 是一个 $F-$代数, 证明 A 含有一个与 F 同构的拷贝.

证明如果 K 是域 F 的一个扩域, 则 K 是一个 $F-$代数.

8. 设 $K=F(a)$ 是域 F 的一个有限维扩张. 对 $\alpha\in K$, 规定从 K 到 K 的映射 L_α 为

$$L_\alpha: K\to K, x\mapsto \alpha x, \forall x\in K.$$

证明 L_α 是一个 $F-$线性变换. 证明 $\det(xI-L_a)$ 恰为 a 的最小多项式 $\min(F,a)$. 对什么样的 $\alpha\in K$ 成立 $\det(xI-L_\alpha)=\min(F,\alpha)$?

9. 设域扩张 K/F 的扩张维数 $[K:F]$ 是素数, 证明在 K 与 F 之间不存在其它中间域.

10. 设有域扩张 K/F. 如果 $a\in K$ 使得 $[F(a):F]$ 为奇数, 证明 $F(a)=F(a^2)$. 给出一个例子说明当 $[F(a):F]$ 为偶数时结论不再成立.

11. 设有代数扩张 K/F, R 是 K 的子环使得 $F\subseteq R\subseteq K$, 证明 R 是域.

12. 证明 $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ 作为域是不同构的, 但是作为 $\mathbb{Q}$ 上的向量空间是同构的.

13. 设 $L_1=F(a_1,\cdots,a_n), L_2=F(b_1,\cdots,b_m)$. 证明合成域 $L_1L_2=F(a_1,\cdots,a_n,b_1,\cdots,b_m)$.

14. 设 L_1,L_2 都是域 F 的扩域且含于某个公共的域中, 证明 L_1L_2 是 F 上的有限维扩张当且仅当 L_1,L_2 均是 F 上的有限维扩张.

15. 设 L_1,L_2 都是域 F 的扩域且含于某个公共的域中, 证明 L_1L_2 在 F 上代数当且仅当 L_1,L_2 均在 F 上代数.

16. 设 $\mathbb{A}$ 是 $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包. 证明 $[\mathbb{A}:\mathbb{Q}]=\infty$.

17. 设 K 是域 F 的有限扩张. 如果 L_1,L_2 都是域 K 的包含 F 的子域, 证明:

$$[L_1L_2:F]\le[L_1:F]\cdot[L_2:F].$$

进而, 若$([L_1:F],[L_2:F])=1$, 证明$[L_1L_2:F]=[L_1:F]\cdot[L_2:F]$.

18. 证明$\left[\mathbb{Q}\left(\sqrt[4]{2},\sqrt{3}\right):\mathbb{Q}\right]=8$.

19. 试给出域 F 的扩域 L_1,L_2 的具体例子使得$[L_1L_2:F]<[L_1:F]\cdot[L_2:F]$.

20. 给出域扩张 K/F 的具体例子使得$[K:F]=3$但是 $K\neq F\left(\sqrt[3]{b}\right),\forall b\in F$.

21. 设$\alpha\in\mathbb{C}$是x^n-b的一个根, 其中$b\in\mathbb{C}$. 证明x^n-b分解为$\prod_{0\le i\le n-1}\left(x-\omega^i a\right)$, 其中$\omega=e^{2\pi i/n}$是 n 次单位根.

22. (1) 设 F 是域, $f(x)\in F[x]$. 若$f(x)=\sum_i a_i x^i,\alpha\in F$,令$f(x+\alpha)=\sum_i a_i(x+\alpha)^i$.

证明: f在 F 上不可约$\Leftrightarrow f(x+\alpha)$在 F 上不可约, $\forall\alpha\in F$.

(2) 若 p 是素数, 证明$x^{p-1}+x^{p-2}+\cdots+x+1$在$\mathbb{Q}$上不可约.

提示: 将 x 替换为$x+1$后再应用 Eisenstein 判别法.

23. 设 R 是环, 如果存在正整数 n 使得$n\cdot1=0$, 则满足$n\cdot1=0$的最小正整数 n 称为**环 R 的特征**, 否则规定环 R 的特征为 0. 设 R 是幺环, 定义$\varphi:\mathbb{Z}\to R,n\mapsto n\cdot1,\forall n\in\mathbb{Z}$. 证明$\varphi$是环同态且$\ker\varphi=m\mathbb{Z}$对某个唯一确定的非负整数, 进而证明 m 恰为环 R 的特征.

24. 对任一给定的正整数 n, 给出一个特征为 n 的环的例子.

25. 设 R 是整环, 证明$\operatorname{char}R=0$或素数.

26. 设 R 是交换幺环. 环 R 的全体子环(含幺元 1 的子环)的交称为 R 的**素子环**. 证明素子环是一个含于 R 所有子环中的一个子环. 进而证明 R 的素子环恰为$\{n\cdot1\mid n\in\mathbb{Z}\}$.

27. 设 F 是域. 如果$\operatorname{char}F=p>0$. 证明 F 的素子环同构于域$\mathbb{F}_p$. 如果$\operatorname{char}F=0$. 证明 F 的素子环同构于域$\mathbb{Z}$.

28. 设 F 是域. F 的全体子域的交称为 F 的**素子域**. 证明 F 的素子域是其素子环的商域, 它含于 F 的所有子域; 若$\operatorname{char}F=p>0$则同构于$\mathbb{F}_p$, 若$\operatorname{char}F=0$则同构于$\mathbb{Q}$.

2. 自同构

Galois 理论的主要思想是，将多项式 f 对应于其全部根所成集上的某个置换群，称为 f 的 Galois 群. 我们在本节将定义、研究且给出 Galois 群的一些数字信息. 我们这里对 Galois 群的描述并非源自 Galois 本人，而是源自 Artin 的等价描述.

从域 K 到其自身的**环同构**(保持加法与乘法的双射)称为域 K 的一个**自同构**. 记 K 的全体自同构关于映射合成所成群为 $\mathrm{Aut}(K)$. 即

$$\mathrm{Aut}(K)=\left\{\sigma: K\to K \text{ 是双射} \middle| \begin{array}{l}\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta),\\ \sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta),\forall \alpha,\beta\in K\end{array}\right\}.$$

在 $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$ 中令 $\alpha=\beta=1$，则 $\sigma(1)=\sigma(1)\sigma(1)$，于是 $\sigma(1)\big(1-\sigma(1)\big)=0$，所以 $\sigma(1)=1$ 或 0，由 σ 是双射知 $\sigma(1)=1$，即**域的自同构保持乘法幺元**，进而保持素子域中的元不变.

注记 (1) 更一般地，如果 R 是幺环，且 $\sigma: R\to S$ 是环的满同态，则 S 也是幺环，且 $\sigma(1_R)=1_S$:

任取 $s\in S$，由 σ 满知存在 $r\in R$ 使得 $s=\sigma(r)$，于是 $s\sigma(1_R)=\sigma(r)\sigma(1_R)=\sigma(r1_R)=\sigma(r)=s$，同理 $\sigma(1_R)s=s$，所以 $\sigma(1_R)=1_s$ 是 S 的乘法单位元.

特别地，幺环同构与域同构均保持乘法幺元.

(2) 显然 $\mathrm{Aut}(K)$ 包含 K 上的恒等变换 id_K 从而非空，直接验证知 $\mathrm{Aut}(K)$ 对乘积，求逆运算封闭，因此 $\mathrm{Aut}(K)$ 对映射的合成运算构成一个群.

为了研究域扩张，我们需要考虑扩域之间的映射.

设 K 与 L 都是域 F 的扩域，如果环同态 $\tau: K\to L$ 满足 $\tau(a)=a,\forall a\in F$，即 $\tau|_F=\mathrm{id}_F$，则称 τ 是一个 $F-$**同态**. 如果 τ 还是双射则称 τ 为 $F-$**同构**.

从域 K 到自身的 $F-$同构称为 $F-$**自同构**.

例. (1) 取复共轭 $\sigma:\mathbb{C}\to\mathbb{C}, z\mapsto\bar{z},\forall z\in\mathbb{C}$ 是复数域的一个 $\mathbb{R}-$自同构;

(2) $\tau:\mathbb{Q}(\sqrt{2})\to\mathbb{Q}(\sqrt{2}), a+b\sqrt{2}\mapsto a-b\sqrt{2},\forall a,b\in\mathbb{Q}$ 是数域 $\mathbb{Q}(\sqrt{2})$ 的一个 $\mathbb{Q}-$自同构.

下面给出 $F-$同态的一些性质.

如果 $\tau: K\to L$ 是 ***F* 的两个扩域间的** $F-$**同态**，注意到 K 与 L 都是 $F-$空间，此时 τ **也是** $F-$**空间之间的线性映射**:

$$\tau(c\alpha)=\tau(c)\tau(\alpha)=c\tau(\alpha),\tau(\alpha+\beta)=\tau(\alpha)+\tau(\beta),\forall\alpha,\beta\in K,c\in F.$$

由于域 K 只有平凡理想 K 或 0, 所以 $\ker\tau=K$ 或 0.

如果 $\ker\tau=K$, 则 τ 是零变换, 矛盾于 $\tau|_F=\mathrm{id}_F$!

所以 $\ker\tau=0$ 从而 τ 单, 于是可将 K 嵌入 L, 所以: **$F-$同态必为嵌入同态.**

若 $[K:F]=[L:F]=n$, 将 τ 视为同维数 $F-$空间 K 到 L 的线性映射, 由维数公式知:

$$\tau\text{是}F-\text{同态}\Rightarrow\tau|_F=\mathrm{id}_F\Rightarrow\tau\neq0\Rightarrow\ker\tau=0\Rightarrow\dim\ker\tau=0\Rightarrow\dim\mathrm{Im}\,\tau=n\Rightarrow\tau\text{满}.$$

特别地, **当 $[K:F]<\infty$ 时, 域 K 的 $F-$自同态一定是 $F-$自同构.**

定义 2.1 域扩张 K/F 的 **Galois 群** $\mathrm{Gal}(K/F)$ **定义为 K 的全体 $F-$自同构所成群.**

如何确定给定域扩张的 Galois 群? 如何计算? 我们先考虑如下特殊情形:

如果域 $K=F(X)$ 是由域 F 与 $X\subseteq K$ 生成, 那么域 K 的任一 $F-$自同构 σ 由其在 X 上的作用唯一确定. 例如, 若 F 的扩域 K 是由某个多项式 $f(x)\in F[x]$ 的根生成, 那么如下两个引理表明: 可以将 Galois 群 $\mathrm{Gal}(K/F)$ 解释为 f 的根集上的一个置换群. 这种在基础域上添加一个多项式的根得到的域扩张尤为重要, 将在第 3 节对其进行研究. 下面的两个引理有助于计算 Galois 群.

引理 2.2 设有 F 的扩域 $K=F(X)$, 其中 $X\subseteq K$. 若 $\sigma,\tau\in\mathrm{Gal}(K/F)$ 满足 $\sigma|_X=\tau|_X$, 则 $\sigma=\tau$. 即: 扩域 $K=F(X)$ 的 **$F-$自同构由其在生成集上的作用完全确定.**

证明 任取 $\alpha\in K$, 由 $K=F(X)$ 知存在有限子集 $\{\alpha_1,\cdots,\alpha_n\}\subseteq X$ 使得 $\alpha\in F(\alpha_1,\cdots,\alpha_n)$. 这意味着存在 $f,g\in F[x_1,\cdots,x_n]$ 使得 $\alpha=f(\alpha_1,\cdots,\alpha_n)/g(\alpha_1,\cdots,\alpha_n)$. 不妨设

$$f(x_1,\cdots,x_n)=\sum b_{i_1i_2\cdots i_n}x^{i_1}x^{i_2}\cdots x^{i_n},g(x_1,\cdots,x_n)=\sum c_{i_1i_2\cdots i_n}x^{i_1}x^{i_2}\cdots x^{i_n},$$

其中系数均属于 F. 注意到 $\sigma,\tau\in\mathrm{Gal}(K/F)$ 作为 $F-$自同构保持加法, 乘法, 且固定 F 中的元不变, 因此

$$\sigma(\alpha)=\frac{\sum b_{i_1i_2\cdots i_n}\sigma(\alpha_1)^{i_1}\sigma(\alpha_2)^{i_2}\cdots\sigma(\alpha_n)^{i_n}}{\sum c_{i_1i_2\cdots i_n}\sigma(\alpha_1)^{i_1}\sigma(\alpha_2)^{i_2}\cdots\sigma(\alpha_n)^{i_n}}=\frac{\sum b_{i_1i_2\cdots i_n}\tau(\alpha_1)^{i_1}\tau(\alpha_2)^{i_2}\cdots\tau(\alpha_n)^{i_n}}{\sum c_{i_1i_2\cdots i_n}\tau(\alpha_1)^{i_1}\tau(\alpha_2)^{i_2}\cdots\tau(\alpha_n)^{i_n}}=\tau(\alpha).$$

故 $\sigma=\tau$, 即任一 $F-$自同构由其在生成集上的作用唯一确定.■

引理 2.3 设 $\tau:K\to L$ 是 $F-$同态, $\alpha\in K$ 在 F 上代数.

(1) 若 $f(x)\in F[x]$ 使得 $f(\alpha)=0$, 则 $f(\tau(\alpha))=0$.

(2) τ 置换了 $\min(F,\alpha)$ 的根, 且 $\min(F,\alpha)=\min(F,\tau(\alpha))$.

(3) **$F-$自同构将 F 上代数的元 $\alpha\in K$ 变为其最小多项式 $\min(F,\alpha)$ 的根.**

证明 (1) 设 $f(x)=c_0+c_1x+\cdots+c_nx^n\in F[x]$，则

$$0=\tau(0)=\tau(f(\alpha))=\tau\left(\sum_i c_i\alpha^i\right)=\sum_i\tau(c_i)\tau(\alpha)^i=\sum_i c_i\tau(\alpha)^i=f(\tau(\alpha)).$$

(2) 令 $p(x)=\min(F,\alpha)$，由 $p(\alpha)=0$ 与(1)知 $p(\tau(\alpha))=0$，即 $\tau(\alpha)$ 也是 $\min(F,\alpha)$ 的根，故 τ 置换了 $\min(F,\alpha)$ 的根.

由 $p(\tau(\alpha))=0$ 知 $\min(F,\tau(\alpha))\mid p(x)$，再由 $p(x)=\min(F,\alpha)$ 与 $\min(F,\tau(\alpha))$ 均首 1 且 $F-$不可约，所以 $\min(F,\tau(\alpha))=\min(F,\alpha)$.

(3) 由(2)即得.■

推论 2.4 若 $[K:F]<\infty$，则 $|\mathrm{Gal}(K/F)|<\infty$. 即**有限维扩张的 Galois 群必然有限.**

证明 由 $[K:F]<\infty$ 可设 $K=F(\alpha_1,\cdots,\alpha_n)$ 且每一个 $\alpha_i\in K$ 在 F 上代数. 此时 K 的任一 $F-$自同构由其在诸 α_i 上的作用唯一确定. 由引理 2.3，每一 α_i 在 $F-$自同构下的像是 $\min(F,\alpha_i)$ 的根，仅有限多种可能，因此 K/F 仅有限多个自同构. ■

例 2.5 域扩张 $\mathbb{C}/\mathbb{R}$ 的 Galois 群为 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})=\{\mathrm{id},\sigma\}$，其中 σ 是复共轭.

显然恒等变换与复共轭都是 $\mathbb{C}$ 的 $\mathbb{R}-$自同构，故 $\{\mathrm{id},\sigma\}\subseteq\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

由 $\mathbb{C}=\mathbb{R}(\mathrm{i})$ 知 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ 中元由其在生成元 i 上的作用完全确定. 由引理 2.3 知，若 $\tau\in\mathrm{Gal}(\mathbb{C}/\mathbb{R})$，则 $\tau(\mathrm{i})$ 是 $\min(\mathbb{R},\mathrm{i})=x^2+1$ 的根，故 $\tau(\mathrm{i})=\mathrm{i}$ 或 $-\mathrm{i}$，所以 $\tau=\mathrm{id}$ 或者 $\tau=\sigma$.■

确定域扩张 K/F 的 Galois 群的方法:

(1) 找出域扩张的某个有限生成元集 $X\subseteq K$ 使得 $K=F(X)$;

(2) 分析每一个 $\tau\in\mathrm{Gal}(K/F)$ 在生成元集上的作用效果: $F-$自同构 τ 总是将 K 中元变为该元最小多项式的一个根，且该根还属于 K.

例 2.6 域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 的 Galois 群 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})=\{\mathrm{id}\}$.

设 σ 是 $\mathbb{Q}\left(\sqrt[3]{2}\right)$ 的 $\mathbb{Q}-$ 自同构，则 $\sigma\left(\sqrt[3]{2}\right)$ 是 $\min\left(\mathbb{Q},\sqrt[3]{2}\right)=x^3-2$ 的根，令 $\omega=e^{\frac{2\pi}{3}\mathrm{i}}$，则 x^3-2 的 3 个根为 $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$. 可是 x^3-2 在 $\mathbb{Q}\left(\sqrt[3]{2}\right)$ 中唯一的根为 $\sqrt[3]{2}$：如果还有其它根在域 $\mathbb{Q}\left(\sqrt[3]{2}\right)$ 中，则得到 $\omega\in\mathbb{Q}\left(\sqrt[3]{2}\right)$，于是 $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}(\omega)\right]=\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]\Big/\left[\mathbb{Q}(\omega):\mathbb{Q}\right]=3/2$，这是不可能的!

也可由 $\omega=\dfrac{-1+\mathrm{i}\sqrt{3}}{2}\in\mathbb{Q}\left(\sqrt[3]{2}\right)$ 导出 $\mathrm{i}\in\mathbb{Q}\left(\sqrt[3]{2}\right)\subseteq\mathbb{R}$ 得到矛盾!

所以 $\sigma\left(\sqrt[3]{2}\right)=\sqrt[3]{2}$，利用 σ 的作用由 $\sigma\left(\sqrt[3]{2}\right)$ 唯一确定即知 $\sigma=\mathrm{id}$.■

例 2.7 设 $K=\mathbb{F}_2(t)$ 是 2 元域 $\mathbb{F}_2$ 上不定元 t 的有理函数域，令 $F=\mathbb{F}_2\left(t^2\right)$. 则 K 是 F 上的 2 维扩域，K 具有一组 $F-$ 基 $\{1,t\}$ (参阅例 1.5).

$t\in K$ 满足多项式 $x^2-t^2\in F[x]$，由 $x^2-t^2=(x-t)^2$ 知 t 是 x^2-t^2 在 $K[x]$ 中唯一的根. 这表明若 $\sigma\in\mathrm{Gal}(K/F)$，则 $\sigma(t)=t$，故 $\sigma=\mathrm{id}$，即 $\mathrm{Gal}(K/F)=\{\mathrm{id}\}$.■

例 2.8 设 2 元域 $\mathbb{F}_2=\{0,1\}$，直接计算知 $f(x)=1+x+x^2$ 在 $\mathbb{F}_2$ 中没有根，故 $f(x)$ 在 $\mathbb{F}_2$ 上不可约. 令 $M=\left(1+x+x^2\right)$ 表示 $1+x+x^2$ 在 $\mathbb{F}_2[x]$ 中生成的极大理想，令

$$K=\mathbb{F}_2[x]/M=\left\{\bar{0},\bar{1},\bar{x},\overline{1+x}\right\},\ \text{其中}\ \overline{a+bx}=(a+bx)+M\in K,\forall a,b\in\mathbb{F}_2,$$

则 K 的子域 $\left\{\bar{0},\bar{1}\right\}$ 与 $\mathbb{F}_2$ 同构，将其等同于 $\mathbb{F}_2$，令 $\alpha=\bar{x}$，则 $K=\left\{a+b\alpha\middle|a,b\in\mathbb{F}_2\right\}$. 如果 $\sigma\in\mathrm{Gal}\left(K/\mathbb{F}_2\right)$，则 $\sigma(\alpha)$ 也是 $1+x+x^2$ 的根，将 $1+x+x^2$ 分解为 $(x+\alpha)(x+\beta)$，比较系数得 $1+x+x^2$ 的另一个根为 $\alpha+1$，因此 $\sigma(\alpha)=\alpha$ 或者 $\alpha+1$，故 $\mathrm{Gal}\left(K/\mathbb{F}_2\right)$ 最多有两个元. 直接验证知映射

$$\sigma:a+b\alpha\mapsto a+b(\alpha+1),\forall a,b\in\mathbb{F}_2$$

确实是 $\mathrm{Gal}\left(K/\mathbb{F}_2\right)$ 中元，此时 $\mathrm{Gal}\left(K/\mathbb{F}_2\right)=\{\mathrm{id},\sigma\}$.■

Galois 理论的基本思想是域的扩张可以回溯到域扩张的 Galois 群.

给定域扩张 K/F，则有域扩张的 Galois 群 $\mathrm{Gal}(K/F)$. 更一般地，如果 L 是**域扩张 K/F 的中间域**，即 $F\subseteq L\subseteq K$，还可得到**群 $\mathrm{Gal}(K/L)$，它是 $\mathrm{Gal}(K/F)$ 的子群：** 域 K 的保持中间域 L 不变的自同构当然保持更小的域 F 中的元不变.

反之，**给定 $\mathrm{Gal}(K/F)$ 的子群，也可得到域扩张 K/F 的一个中间域.** 事实上，对 $\mathrm{Aut}(K)$ 的任一子集 S 都可得到 K 的一个子域，令

$$\mathcal{F}(S)=\{a\in K\,|\,\tau(a)=a,\forall\tau\in S\}.$$

直接验证知 $\mathcal{F}(S)$ 是 K 的子域, 称为 ***S* 的固定域**, 也记为 $\mathrm{Inv}(S)$. 如果 $S\subseteq\mathrm{Gal}(K/F)$, 则 $\mathcal{F}(S)$ 是扩张 K/F 的中间域.

下面的引理给出了 Galois 群与固定域的一些简单性质.

引理 2.9 设 K 是域.

(1) 域 $L_1\subseteq L_2\subseteq K\Rightarrow\mathrm{Gal}(K/L_1)\geq\mathrm{Gal}(K/L_2)$; 固定大子域的自同构, 固定小子域.

(2) 域 $L\subseteq K\Rightarrow L\subseteq\mathcal{F}(\mathrm{Gal}(K/L))$; 固定子域 L 的自同构群的固定域当然含 L.

(3) $S_1\subseteq S_2\subseteq\mathrm{Aut}(K)\Rightarrow\mathcal{F}(S_1)\supseteq\mathcal{F}(S_2)$; 少元 S_1 固定的域比多元 S_2 固定的域更大.

(4) $S\subseteq\mathrm{Aut}(K)\Rightarrow S\subseteq\mathrm{Gal}(K/\mathcal{F}(S))$; 任一自同构均保持其固定域不动.

(5) $L=\mathcal{F}(S)$ 对某 $S\subseteq\mathrm{Aut}(K)\Rightarrow L=\mathcal{F}(\mathrm{Gal}(K/L))$;

(6) $H=\mathrm{Gal}(K/L)$ 对某子域 $L\subseteq K\Rightarrow H=\mathrm{Gal}(K/\mathcal{F}(H))$.

证明 前四个结论由定义即得.

(5) 由(4)知 $S\subseteq\mathrm{Gal}(K/\mathcal{F}(S))=\mathrm{Gal}(K/L)$, 由(3)知 $L=\mathcal{F}(S)\supseteq\mathcal{F}(\mathrm{Gal}(K/L))$.

另一方面, 由(2)知 $L\subseteq\mathcal{F}(\mathrm{Gal}(K/L))$, 故 $L=\mathcal{F}(\mathrm{Gal}(K/L))$.

(6) 由(2)知 $L\subseteq\mathcal{F}(\mathrm{Gal}(K/L))=\mathcal{F}(H)$, 由(1)知 $H=\mathrm{Gal}(K/L)\geq\mathrm{Gal}(K/\mathcal{F}(H))$.

另一方面, 由(4)知 $H\leq\mathrm{Gal}(K/\mathcal{F}(H))$, 故 $H=\mathrm{Gal}(K/\mathcal{F}(H))$.■

简易方便的记号: 加撇. 记 $L':=\mathrm{Gal}(K/L), H'=\mathcal{F}(H)$, 设

$$F\subseteq L_1,L_2\subseteq K,\ \ 1\leq H,J\leq\mathrm{Gal}(K/F)=G,$$

则如上结论可翻译为

(1) $L_1\subseteq L_2\Rightarrow L_1'\geq L_2'$; $H\leq J\Rightarrow H'\geq J'$;

(2) $L_1\subseteq L_1''$, $H\leq H''$;

(3) $H'=H'''$, $L'=L'''$;

(4) $F'=G,K'=1,1'=K,G'=\mathcal{F}(\mathrm{Gal}(K/F))\supseteq F$.

推论 2.10 设 K/F 是域扩张. 则

$\mathcal{A}=\{\mathrm{Gal}(K/F)$ 形如 $\mathrm{Gal}(K/L)$ 的子群 $|\ L$ 是中间域$\}$，**闭子群集**

$\mathcal{B}=\{K/F$ 形如 $\mathcal{F}(S)$ 的中间域 $|\ S\subseteq \mathrm{Aut}(K)\}$，**闭子域集**

之间存在反包含的双射关系，且 $\mathrm{Gal}:\mathcal{A}\to\mathcal{B}, L\mapsto \mathrm{Gal}(K/L)$ 与 $\mathcal{F}:\mathcal{A}\to\mathcal{B}, H\mapsto \mathcal{F}(H)$ 是一对互逆双射.

证明 由引理 2.9(5)与(6)即得. ■

即：对加了撇的闭子群集与闭子域集，加撇运算是一对互逆的双射.

如果 K/F 是有限扩张，何时 $L\mapsto \mathrm{Gal}(K/L)$ 是 K/F 的中间域集到 $\mathrm{Gal}(K/F)$ 的子群集的双射？由引理 2.9(5)知其成立的必要条件是 $F=\mathcal{F}(\mathrm{Gal}(K/F))$. 我们将在第 5 节证明这也是一个充分条件.

定义 2.11 从群 G 到域 K 的非零元乘法群 K^* 的群同态称为群 G 的 **$K-$线性特征标**.

注记 (1) 根据定义，**$\mathrm{Gal}(K/F)$ 中元可视为群 $G=K^*$ 的 $K-$线性特征标**.

(2) 群 G 的全部 $K-$值函数关于函数的加法与 $K-$数乘构成一个 $K-$空间.

(3) 在群 G 中每个元处取值均为 1_K 的函数：$\mathbf{1}:G\to K^*, g\mapsto 1_K, \forall g\in G$ 是 G 的一个 $K-$线性特征标.

下面的三个结论针对有限扩张，给出了 Galois 群阶更精确的一些数字信息.

引理 2.12(Dedekind 引理) 设 $\tau_1,\cdots,\tau_n$ 是**群 G 的互异 $K-$线性特征标**，则 $\tau_1,\cdots,\tau_n$ **在 K 上线性无关**.

即，若 $c_1,\cdots,c_n\in K$ 使得 $c_1\tau_1(g)+\cdots+c_n\tau_n(g)=0, \forall g\in G$，则所有 $c_i=0$.

证明 反证. 设命题不成立，则 $\tau_1,\cdots,\tau_n$ 中存在数量最少的 k 个 $K-$线性相关元，由线性特征在 1_G 处取值恒为 1_K 知 $k\geq 2$，适当重排 τ_i 后不妨设 $\tau_1,\cdots,\tau_k$ 在 K 上线性相关，由 k 的最小性知有**全不为 0** 的系数 $c_1,\cdots,c_k\in K$ 使得

$$c_1\tau_1(g)+\cdots+c_k\tau_k(g)=0, \forall g\in G. \tag{1}$$

由 $\tau_1\neq\tau_2$ 知存在 $h\in G$ 使得 $\tau_1(h)\neq\tau_2(h)$，(1)式两端同乘 $\tau_1(h)$ 得

$$c_1\tau_1(h)\tau_1(g)+c_2\tau_1(h)\tau_2(g)+\cdots+c_k\tau_1(h)\tau_k(g)=0, \forall g\in G, \tag{2}$$

由 g 的任意性，将(1)式中的 g 换成 hg，再由 $\tau_i(hg)=\tau_i(h)\tau_i(g)$ 得

$$c_1\tau_1(h)\tau_1(g)+c_2\tau_2(h)\tau_2(g)+\cdots+c_k\tau_k(h)\tau_k(g)=0, \forall g\in G, \tag{3}$$

(2)式减去(3)式，得

$$c_2[\tau_1(h)-\tau_2(h)]\tau_2(g)+\cdots+c_k[\tau_1(h)-\tau_k(h)]\tau_k(g)=0, \forall g\in G,$$

由 $c_2\left[\tau_1(h)-\tau_2(h)\right]\neq 0$ 知 $\tau_2,\cdots,\tau_k$ 在 K 上线性相关, 与 k 的最小性矛盾!■

注记 设域扩张 K/F 的 Galois 群 $\mathrm{Gal}(K/F)=\{\tau_1,\cdots,\tau_n\}$, 将 $\mathrm{Gal}(K/F)$ 的元素视为 $K-$线性特征标, 则 Dedekind 引理表明 $\mathrm{Gal}(K/F)$ 中的元是 $K-$线性无关的.

命题 2.13(Artin) 若 K/F 是有限扩张, 则 $\left|\mathrm{Gal}(K/F)\right|\leq[K:F]$.

即: **有限扩张的 Galois 群阶不超过扩张维数.**

证明 因为 K/F 是有限扩张, 由推论 2.4 知 $\mathrm{Gal}(K/F)$ 有限.

(1) 反证. 设 $\mathrm{Gal}(K/F)=\{\tau_1,\cdots,\tau_n\}$ 且 $[K:F]=m<n$, 取 K 的一组 $F-$基 $\alpha_1,\cdots,\alpha_m$. 令 $A=\left(\tau_i(\alpha_j)\right)_{n\times m}$, 则秩 $R(A)\leq m<n$, 故 A 的行向量组 $K-$线性相关, 于是存在不全为 0 的 $c_i\in K$ 使得

$$\sum_{1\leq i\leq n}c_i\tau_i(\alpha_j)=0=0,1\leq j\leq n.$$

令 G 为域 K 的非零元乘法群 K^*, 任取 $g\in G$, 由 $\alpha_1,\cdots,\alpha_m$ 是 K 的一组 $F-$基知存在 $d_i\in F$ 使得 $g=\sum_{1\leq j\leq m}d_j\alpha_j$, 此时

$$\sum_{1\leq i\leq n}c_i\tau_i(g)=\sum_{1\leq i\leq n}c_i\tau_i\left(\sum_{1\leq j\leq m}d_j\alpha_j\right)=\sum_{1\leq j\leq m}d_j\sum_{1\leq i\leq n}c_i\tau_i(\alpha_j)=\sum_{1\leq j\leq m}d_j\cdot 0=0,$$

将 τ_i 视为群 K^* 上的 $K-$线性特征标, 由 Dedekind 引理知所有 c_i 均为 0, 矛盾!■

(2) 我们下面用矩阵的语言来描述如上证明:

反证. 设 $\mathrm{Gal}(K/F)=\{\tau_1,\cdots,\tau_n\}$ 且 $[K:F]=m<n$, 选取 K 的一组 $F-$基 $\alpha_1,\cdots,\alpha_m$. 令

$$A=\begin{pmatrix}\tau_1(\alpha_1) & \cdots & \tau_1(\alpha_m)\\ \vdots & & \vdots\\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_m)\end{pmatrix},$$

则秩 $R(A)\leq m<n$, 于是 $XA=\mathbf{0}$ 有非零解 $(c_1,\cdots,c_n)\in K^n$.

任取 $g\in K^*$, 由 $\alpha_1,\cdots,\alpha_m$ 是 K 的一组 $F-$基可设 $g=d_1\alpha_1+\cdots+d_m\alpha_m$, 则

$$(c_1\tau_1+\cdots+c_n\tau_n)(g)=(c_1,\cdots,c_n)\begin{pmatrix}\tau_1(g)\\ \vdots\\ \tau_n(g)\end{pmatrix}=(c_1,\cdots,c_n)\begin{pmatrix}\tau_1(d_1\alpha_1+d_2\alpha_2+\cdots+d_m\alpha_m)\\ \vdots\\ \tau_n(d_1\alpha_1+d_2\alpha_2+\cdots+d_m\alpha_m)\end{pmatrix}$$

$$=(c_1,\cdots,c_n)\begin{pmatrix}\tau_1(\alpha_1) & \cdots & \tau_1(\alpha_m)\\ \vdots & & \vdots\\ \tau_n(\alpha_1) & \cdots & \tau_n(\alpha_m)\end{pmatrix}\begin{pmatrix}d_1\\ \vdots\\ d_m\end{pmatrix}=\mathbf{0},$$

即 $(c_1\tau_1+\cdots+c_n\tau_n)(g)=0,\forall g\in G$. 将 τ_i 视为群 K^* 上的 $K-$线性特征标, 由 Dedekind 引理知所有 c_i 均为 0, 矛盾!■

(3) 直观证明: $\tau_1,\cdots,\tau_n$ 由其在 K 的 $F-$基 $\alpha_1,\cdots,\alpha_m$ 上的作用唯一确定, Dedekind 引理表明 $\tau_1,\cdots,\tau_n$ 线性无关, 等价于向量组 $(\tau_i(\alpha_1),\cdots,\tau_i(\alpha_m)),1\le i\le n$ 线性无关, 故 $n\le m$.■

注意有可能成立 $|\mathrm{Gal}(K/F)|<[K:F]$, 如例 2.6 与 2.7. 人们自然地提出如下问题:

对什么样的域扩张 K/F 有 $|\mathrm{Gal}(K/F)|=[K:F]$?

下面的命题给出了 $|\mathrm{Gal}(K/F)|=[K:F]$ 的一个充分条件.

命题 2.14 设 G 是域 K 的自同构群 $\mathrm{Aut}(K)$ 的有限子群, G 的固定域为 $F=\mathcal{F}(G)$, 则 $|G|=[K:F]$ 且 $G=\mathrm{Gal}(K/F)$, 特别地 K/F 是有限扩张.

证明(1) 因为 F 是 G 的固定域, 所以 $G\le\mathrm{Gal}(K/F)$.

如果 K/F 是有限扩张, 则由 Artin 引理知 $|\mathrm{Gal}(K/F)|\le[K:F]$, 再由 $G\le\mathrm{Gal}(K/F)$ 知 $|G|\le[K:F]$.

如果 K/F 是无限扩张, 由 G 有限知 $|G|\le[K:F]$. 所以恒成立 $|G|\le[K:F]$.

(2) 下证 $|G|=[K:F]$, **反证.**

若 $|G|<[K:F]$. 设 $G=\{\tau_1=\mathrm{id}_K,\cdots,\tau_n\}$, 由 $n=|G|<[K:F]$ 知 K 中存在 $n+1$ 个 $F-$线性无关元 $\alpha_1,\cdots,\alpha_{n+1}$, 令 $A=(\tau_i(\alpha_j))_{n\times(n+1)}$, 则 A 的列向量组 $K-$线性相关, 选取 A 中列数最少的 k 个 $K-$线性相关的列向量, 适当调整 α_i 的顺序后不妨设 A 的前 k 列 $K-$线性相关, 由 k 的最小性知存在**全不为 0** 的 $c_1,\cdots,c_k\in K$ 使得

$$\sum_{1\le j\le k}c_j\tau_i(\alpha_j)=0,1\le i\le n,(n\text{ 个分量})\qquad(1)$$

两端同乘 c_1^{-1} 后不妨设 $c_1=1\in F$.

(目标: 证明所有 $c_j\in F$, 在(1)中令 $i=1$ 知 $\alpha_1,\cdots,\alpha_k$ 是 $F-$线性相关的, 矛盾!)

任取$\sigma\in G$，注意到σ左乘导出集合G上的置换，于是当τ_i跑遍G时，$\sigma\tau_i$也跑遍G，故用σ左乘(1)中的n个式子时，得到的n个式子适当调整顺序后为

$$\sum_{1\le j\le k}\sigma\left(c_j\right)\tau_i\left(\alpha_j\right)=0,1\le i\le n. \tag{2}$$

注意到$1=c_1=\sigma\left(c_1\right)$，(1)中$n$个式子分别减去(2)中对应的$n$个式子后得

$$\sum_{2\le j\le k}\left(c_j-\sigma\left(c_j\right)\right)\tau_i\left(\alpha_j\right)=0,1\le i\le n,$$

由k的最小性知$c_j-\sigma\left(c_j\right)=0,2\le j\le k$，这表明每一$c_j$均被所有$\sigma\in G$固定，于是$c_j$含于$G$的固定域$F$，在(1)中令$i=1$，注意到$\tau_1=\mathrm{id}_K$，则

$$0=\sum_{1\le j\le k}c_j\tau_1\left(\alpha_j\right)=\sum_{1\le j\le k}c_j\,\mathrm{id}_K\left(\alpha_j\right)=\sum_{1\le j\le k}c_j\alpha_j,$$

于是$\alpha_1,\cdots,\alpha_k$是$F-$线性相关的，与$\alpha_1,\cdots,\alpha_{n+1}$是$F-$线性无关的矛盾!

(3) 由(2)知$\left|G\right|=\left[K:F\right]$，由$G$有限知$K/F$是有限扩张. 由 Artin 引理 2.13 知

$$\left|\mathrm{Gal}\left(K/F\right)\right|\le\left[K:F\right]=\left|G\right|<\infty.$$

再由$G\le\mathrm{Gal}\left(K/F\right)$知$G=\mathrm{Gal}\left(K/F\right)$.■

注记: (1) 若某个域K的自同构群为S_n，如上命题表明S_n的任一子群G均为 Galois 扩张$K/\mathcal{F}\left(G\right)$的 Galois 群.

(2) 对有限扩张K/F_1，由 Artin 引理 2.13，$\mathrm{Gal}\left(K/F_1\right)$的群阶不超过扩张次数$\left[K:F_1\right]$，此时$K'=1,F_1'=\mathrm{Gal}\left(K/F_1\right),1'=K$，但只能得到$F_1\subseteq\mathrm{Gal}\left(K/F_1\right)'$，未必成立$F_1=\mathrm{Gal}\left(K/F_1\right)'$.

如果令$G:=\mathrm{Gal}\left(K/F_1\right),F=\mathcal{F}\left(\mathrm{Gal}\left(K/F_1\right)\right)=G'$，则如上命题表明$G=\mathrm{Gal}\left(K/F\right)$，此时不仅有$K'=1,F'=\mathrm{Gal}\left(K/F\right),1'=K$，而且有

$$\mathrm{Gal}\left(K/F\right)'=G'=\mathrm{Gal}\left(K/F_1\right)'=\mathcal{F}\left(\mathrm{Gal}\left(K/F_1\right)\right)=F.$$

即有限扩张K/F_1不一定 Galois，但是域扩张K/F总是 Galois 的.

一般来说$F_1\ne F$，但$\left|\mathrm{Gal}\left(K/F_1\right)\right|=\left|G\right|=\left[K:F\right]$是$\left[K:F_1\right]$的因子，即

有限扩张的 Galois 群阶整除扩张次数.

定义 2.15 代数扩张扩张K/F称为 **Galois 扩张**，若$\mathcal{F}\left(\mathrm{Gal}\left(K/F\right)\right)=F$，也称 ***K* 在 *F* 上是 Galois 的**.

由命题 2.14 知，对任一有限扩张K/F_1，令$F=\mathcal{F}\left(\mathrm{Gal}\left(K/F_1\right)\right)$，则$K/F$是 Galois 的.

推论 2.16 设 K/F 是有限扩张. 则: **K/F 是 Galois 扩张** $\Leftrightarrow \left|\mathrm{Gal}(K/F)\right| = [K:F]$.

证 1 若 K/F 是 Galois 扩张, 则 $\mathcal{F}(\mathrm{Gal}(K/F)) = F$, 令 $G := \mathrm{Gal}(K/F) \le \mathrm{Aut}(K)$, 则由 Artin 引理 2.13 知 G 有限, 再由命题 2.14 知 $\left|\mathrm{Gal}(K/F)\right| = [K:F]$.

反之, 设 $\left|\mathrm{Gal}(K/F)\right| = [K:F]$, 令 $G := \mathrm{Gal}(K/F), L := \mathcal{F}(G) \subseteq K$, 由命题 2.14 知

$$\mathrm{Gal}(K/F) = G = \mathrm{Gal}(K/L) \text{ 且 } \left|\mathrm{Gal}(K/L)\right| = |G| = [K:L],$$

故 $[K:F] = \left|\mathrm{Gal}(K/F)\right| = [K:L] = [L:K][K:F]$, 所以 $[L:F] = 1$ 从而有 $L = F$.

证 2 因为 K/F 是有限扩张, 由 Artin 引理 2.13 知 $G := \mathrm{Gal}(K/F)$ 有限, 令

$$L := \mathcal{F}(G) = \mathcal{F}(\mathrm{Gal}(K/F)),$$

由命题 2.14 知 $G = \mathrm{Gal}(K/L)$ 且 $|G| = [K:L]$. 此时

$$K/F \text{ 是 Galois 扩张} \Leftrightarrow \mathcal{F}(\mathrm{Gal}(K/F)) = F \Leftrightarrow L = F \Leftrightarrow [L:F] = 1 \qquad \text{子域包含关系 } F \subseteq L \subseteq K$$

$$\Leftrightarrow [K:L] = [K:F] \Leftrightarrow |G| = [K:F]. \blacksquare$$

如上推论给出了扩张是否 Galois 的一个数字判别准则, 缺点是需要知道域扩张的 Galois 群阶, 而确定 Galois 群较困难. 不过可以较简单地判别单代数扩张 $F(\alpha)/F$ 是否 Galois.

推论 2.17 设有域扩张 K/F, $\alpha \in K$ 在 F 上代数, 最小多项式 $\min(\alpha, F)$ 的次数为 n. 则

(1) $\left|\mathrm{Gal}(F(\alpha)/F)\right| = \min(\alpha, F)$ 在 $F(\alpha)$ 中不同的根数;

(2) $F(\alpha)/F$ 是 Galois 扩张 $\Leftrightarrow$ $\min(\alpha, F)$ 在 $F(\alpha)$ 中有 n 个根.

证明 (1) 若 $\tau \in \mathrm{Gal}(F(\alpha)/F)$, 由引理 2.3 知 $\tau(\alpha)$ 是 $\min(\alpha, F)$ 的根. 进而, $F(\alpha)$ 的 $F-$ 自同构由其在 α 上作用唯一确定, 故 $\sigma \ne \tau \in \mathrm{Gal}(F(\alpha)/F)$, 则 $\sigma(\alpha) \ne \tau(\alpha)$. 故

$$\left|\mathrm{Gal}(F(\alpha)/F)\right| \le \min(\alpha, F) \text{ 在 } F(\alpha) \text{ 中不同的根数.}$$

反之, 设 $\beta \in F(\alpha)$ 是 $\min(\alpha, F)$ 的一个根, 规定

$$\tau : F(\alpha) \to F(\beta), f(\alpha) \mapsto f(\beta), \forall f(x) \in F[x],$$

由 β 是 $\min(\alpha, F)$ 的根知映射良定, 直接验证知其是一个 $F-$ 自同构, 且 $\tau(\alpha) = \beta$.

所以 Galois 群 $\mathrm{Gal}(F(\alpha)/F)$ 的阶恰为 α 的最小多项式在 $F(\alpha)$ 中不同的根数.

事实上, 这里表明单代数扩张 $F(\alpha)/F$ 的 Galois 群恰由形如 τ 的自同构构成.

(2) 注意到 $[F(\alpha):F]=\deg(\min(\alpha,F))$, 故

$F(\alpha)/F$ 是 Galois 扩张

$\Leftrightarrow [F(\alpha):F]=|\mathrm{Gal}(F(\alpha)/F)|$　　2.16

$\Leftrightarrow \deg(\min(\alpha,F))=|\mathrm{Gal}(F(\alpha)/F)|$　　$[F(\alpha):F]=\deg(\min(\alpha,F))=n$

$\Leftrightarrow \deg(\min(\alpha,F))=\min(\alpha,F)$ 在 $F(\alpha)$ 中不同的根数　　由(1)

$\Leftrightarrow \min(\alpha,F)$ 在 $F(\alpha)$ 中有 $\deg(\min(\alpha,F))=n$ 个根.■

记 $p(x):=\min(\alpha,F)$, 如下两种情形下域扩张 $F(\alpha)/F$ 不是 Galois 的:

(1) 在 $F(\alpha)$ 中不包含 $p(x)$ 的所有根.　　(2) $p(x)$ 可能有重根.

接下来两节将主要讨论这两种情形.

下面给出一些域扩张的例子, 并且确定这些域扩张是否为 Galois 扩张.

例 2.18 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ **不是 Galois 扩张:**因为 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, 而 $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})|=1$. 也可由 $\min(\sqrt[3]{2},\mathbb{Q})=x^3-2$ 在 $\mathbb{Q}(\sqrt[3]{2})$ 中仅有 1 个根 $\sqrt[3]{2}$.■

例 2.19 设 k 是特征为素数 p 的域, $k(t)$ 是 k 上不定元 t 的有理函数域. 考虑域扩张 $k(t)/k(t^p)$, 则 t 满足多项式 $x^p-t^p\in k(t^p)[x]$. 在 $k(t)$ 有分解式 $x^p-t^p=(x-t)^p$, 故 t 在 $k(t^p)$ 上的最小多项式仅有 1 个根, 所以 $\mathrm{Gal}(k(t)/k(t^p))=\{\mathrm{id}\}$, 所以 $k(t)/k(t^p)$ 不是 Galois 扩张.■

例 2.20 设域 F 的特征 $\mathrm{char}\,F\neq 2$, $\alpha\in F$ 不是 F 中某个元平方. 令 $K:=F[x]/(x^2-\alpha)$, 由 $x^2-\alpha$ 在 F 上不可约知 K 是域. 将 F 中元 a 等同于 K 中的元 $a+(x^2-\alpha)$, 则 F 可视为 K 的一个子域. 在此等同之下, K 中每一个元均形如 $a+bx+(x^2-\alpha)$, 都是元 $1+(x^2-\alpha)$ 与 $x+(x^2-\alpha)$ 的一个线性组合, 因此元 $1,u:=x+(x^2-\alpha)$ 构成 $F-$ 空间 K 的一组基, 所以 $[K:F]=2$. 定义 $\sigma:K\to K,a+bu\mapsto a-bu,\forall a,b\in F$, 由 u 与 $-u$ 是 $x^2-\alpha$ 在 K 中的两个根容易验证 $\sigma\in\mathrm{Aut}(K)$. 故 $\mathrm{id},\sigma\in\mathrm{Gal}(K/F)$ 得 $|\mathrm{Gal}(K/F)|\geq 2$.

再由 $|\mathrm{Gal}(K/F)|\leq[K:F]=2$ 知 $|\mathrm{Gal}(K/F)|=2=[K:F]$, 故 K/F 是 Galois 扩张.■

扩域 $K=F(u)$ 由满足 $x^2-\alpha$ 的元 u 生成. 我们通常将此域记为 $F\left(\sqrt{\alpha}\right)$.

例 2.21 $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}$ 是 Galois 扩张, 其中 $\omega=e^{\mathrm{i}\frac{2\pi}{3}}$. 事实上, 域 $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ 是由 x^3-2 的 3 个根 $\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上生成的域, 由 ω 满足 $x^2+x+1\in\mathbb{Q}[x]$ 及 $\omega\notin\mathbb{Q}\left(\sqrt[3]{2}\right)$ 知 $\left[\mathbb{Q}\left(\sqrt[3]{2},\omega\right):\mathbb{Q}\right]=6$. 易见(参阅习题 3 题)如下 6 个函数

$$\mathrm{id}:\sqrt[3]{2}\mapsto\sqrt[3]{2},\omega\mapsto\omega,\qquad \sigma_1:\sqrt[3]{2}\mapsto\omega\sqrt[3]{2},\omega\mapsto\omega,$$

$$\sigma_2:\sqrt[3]{2}\mapsto\sqrt[3]{2},\omega\mapsto\omega^2,\qquad \sigma_3:\sqrt[3]{2}\mapsto\omega\sqrt[3]{2},\omega\mapsto\omega^2,$$

$$\sigma_4:\sqrt[3]{2}\mapsto\omega^2\sqrt[3]{2},\omega\mapsto\omega,\qquad \sigma_5:\sqrt[3]{2}\mapsto\omega^2\sqrt[3]{2},\omega\mapsto\omega^2$$

均可扩充为均为 $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ 的自同构. 故

$$\left|\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}\right)\right|=6=\left[\mathbb{Q}\left(\sqrt[3]{2},\omega\right):\mathbb{Q}\right],$$

所以域扩张 $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}$ 是 Galois 扩张.■

例 2.22 下面的例子表明任一有限群均可成为某个 Galois 扩张的 Galois 群.

设 k 是域, $K=k\left(x_1,x_2,\cdots,x_n\right)$ 是 k 上 n 个不定元的有理函数域. 对任一置换 $\sigma\in S_n$, 规定 $\sigma\left(x_i\right)=x_{\sigma(i)}$, 则 σ 可自然延拓为 K 上的一个自同构:

$$\sigma\left(\frac{f\left(x_1,\cdots,x_n\right)}{g\left(x_1,\cdots,x_n\right)}\right)=\frac{f\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)}.$$

习题 5 表明这确实定义了 K 上的一个自同构. 我们可以视 $S_n\subseteq\mathrm{Aut}(K)$. 令 $F=\mathcal{F}\left(S_n\right)$, 由 2.14 知 K/F 是 Galois 扩张, 且 $\mathrm{Gal}(K/F)=S_n$. 域 F 称为 x_i 的对称函数域. 其命名缘由在于, 若 $f\left(x_1,\cdots,x_n\right)/g\left(x_1,\cdots,x_n\right)\in F$, 则

$$f\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)/g\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)=f\left(x_1,\cdots,x_n\right)/g\left(x_1,\cdots,x_n\right)$$

对所有的 $\sigma\in S_n$. 令

$$s_1=x_1+\cdots+x_n,\quad s_2=\sum_{1\le i\ne j\le n}x_ix_j,\cdots,s_n=x_1\cdots x_n.$$

多项式 s_i 称为 i 次初等对称函数. 则每一个 $s_i\in F$, 于是 $k\left(s_1,\cdots,s_n\right)\subseteq F$. 注意到

$$\left(t-x_1\right)\cdots\left(t-x_n\right)=t^n-s_1t^{n-1}+s_2t^{n-2}-\cdots+\left(-1\right)^n s_n.$$

据此, 我们在第 3 节得到 $F=k\left(s_1,\cdots,s_n\right)$. 这表明, 每一个 x_i 的对称函数都是初等对称函数的有理函数.■

小结

域的自同构群 $\mathrm{Aut}(K)$，域的自同构保持乘法幺元.

$F-$同态，$F-$同构，$F-$自同构;

F 的两个扩域间的 $F-$同态，则 τ 也可视为 $F-$空间之间的线性映射;

当 $[K:F]<\infty$ 时，K 的 $F-$自同态一定是 $F-$自同构.

域扩张 K/F 的 Galois 群 $\mathrm{Gal}(K/F)$ 定义为 K 的全体 $F-$自同构所成群.

引理 2.2 $K=F(X)$，若 $\sigma,\tau\in\mathrm{Gal}(K/F)$ 满足 $\sigma|_X=\tau|_X$，则 $\sigma=\tau$.

即：扩域 $K=F(X)$ 的 $F-$**自同构由其在生成集上的作用完全确定.**

引理 2.3 设 $\tau:K\to L$ 是 $F-$同态，$\alpha\in K$ 在 F 上代数.

(1) 若 $f(x)\in F[x]$ 使得 $f(\alpha)=0$，则 $f(\tau(\alpha))=0$.

(2) τ 置换了 $\min(F,\alpha)$ 的根，且 $\min(F,\alpha)=\min(F,\tau(\alpha))$.

(3) $F-$自同构将 F 上的代数元变为其最小多项式的根.

推论 2.4 有限维扩张的 Galois 群有限.

例 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})=\{\mathrm{id},\sigma\}$，**其中** σ **是复共轭.**　　$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}\right)=\{\mathrm{id}\}$.

域扩张 K/F 的**中间域**，$S\subseteq\mathrm{Aut}(K)$ 的**固定域** $\mathcal{F}(S)$.　　加撇运算的性质.

推论 2.10 域扩张的**闭子群集与闭子域集**之间存在反包含的双射:

$$\mathrm{Gal}:\mathcal{A}\to\mathcal{B},L\mapsto\mathrm{Gal}(K/L)\text{ 与 }\mathcal{F}:\mathcal{A}\to\mathcal{B},H\mapsto\mathcal{F}(H).$$

群 G 的 $K-$**线性特征标.**

Dedekind 引理 2.12 ***群 G 的互异 K−线性特征标在 K 上线性无关.***

$\mathrm{Gal}(K/F)$ 中的元是 $K-$线性无关的.

Atin 命题 2.13 若 K/F 是有限扩张，则 $|\mathrm{Gal}(K/F)|\le[K:F]$.

即：**有限扩张的 Galois 群阶不超过扩张维数.**

命题 2.14 $\mathrm{Aut}(K)$ 的有限子群 G 的固定域为 $F=\mathcal{F}(G)$，则 $|G|=[K:F]$ 有限且 $G=\mathrm{Gal}(K/F)$.

代数扩张扩张 K/F 若满足 $\mathcal{F}(\mathrm{Gal}(K/F))=F$ 则称为 **Galois 扩张**.

给定有限扩张 K/F_1 未必 Galois，令 $F=\mathcal{F}(\mathrm{Gal}(K/F_1))$，则 K/F 总是 Galois 的.

有限扩张的 Galois 群阶整除扩张次数.

推论 2.16 有限扩张 K/F 是 Galois 扩张 $\Leftrightarrow \left|\mathrm{Gal}\left(K/F\right)\right|=\left[K:F\right]$.

推论 2.17 设有域扩张 K/F，$\alpha\in K$ 在 F 上代数，最小多项式 $\min\left(\alpha,F\right)$ 的次数为 n. 则

(1) $\left|\mathrm{Gal}\left(F\left(\alpha\right)/F\right)\right|=\min\left(\alpha,F\right)$ 在 $F\left(\alpha\right)$ 中不同的根数;

(2) $F\left(\alpha\right)/F$ 是 Galois 扩张 $\Leftrightarrow \min\left(\alpha,F\right)$ 在 $F\left(\alpha\right)$ 中有 n 个根.

例 $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ **不是 Galois 扩张**.　　$\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}$ 是 Galois 扩张

任一有限群均可成为某个 Galois 扩张的 Galois 群. ·

习题 1.2

1. 证明恒等自同构是 $\mathbb{Q}$ 唯一的自同构.

2. 证明实数域 $\mathbb{R}$ 唯一的自同构是恒等自同构.

提示: 如果 σ 是自同构, 证明 $\sigma\big|_{\mathbb{Q}}=\mathrm{id}$，如果 $a>0$，则 $\sigma\left(a\right)>0$. 比较有意思的是, 尽管 $\left[\mathbb{C}:\mathbb{R}\right]=2$，可是有无穷多个 $\mathbb{C}$ 的自同构. 为什么这一事实与我们本题中的结论不矛盾?

3. 证明例 2.21 给出的 6 个函数都可以延拓为 $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ 的 $\mathbb{Q}-$ 自同构.

4. 设整环 B 的商域为 F. 如果 $\sigma:B\to B$ 是环同构, 证明 σ 诱导出环同构

$$\sigma':F\to F,a/b\mapsto\sigma\left(a\right)/\sigma\left(b\right),\forall 0\neq b,a\in B\,.$$

5. 设 $K=k\left(x_1,\cdots,x_n\right)$ 是域 k 上 n 个不定元的有理函数域. 证明如下定义

$$\sigma\left(\frac{f\left(x_1,\cdots,x_n\right)}{g\left(x_1,\cdots,x_n\right)}\right):=\frac{f\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)},\cdots,x_{\sigma(n)}\right)}$$

将每一个置换 $\sigma\in S_n$ 映射为域 K 的一个自同构.

提示: 第 4 题域习题 1.6 有助于本题求解.

6. 设 F 是特征不为 2 的域, K 是 F 的一个扩域使得 $\left[K:F\right]=2$. 证明 $K=F\left(\sqrt{a}\right)$ 对某个 $a\in F$; 此即, 证明 $K=F\left(\alpha\right)$, 其中 $\alpha^2=a\in F$. 进而证明域 K 在 F 上是 Galois 的.

7. 设 $F=\mathbb{F}_2,K=F\left(\alpha\right)$, 其中 α 是 $1+x+x^2$ 的一个根. 证明函数

$$\sigma:K\to K,a+b\alpha\mapsto a+b+b\alpha,\forall a,b\in F$$

是域 K 的一个 $F-$ 自同构.

8. 设 $\alpha\in\mathbb{C}$ 在 $\mathbb{Q}$ 上代数且 $p(x)=\min(\mathbb{Q},\alpha)$，设 b 是 $p(x)$ 的任一复根. 证明映射

$$\sigma:\mathbb{Q}(a)\to\mathbb{C},\ f(a)\mapsto f(b),\ \forall f(x)\in\mathbb{Q}[x]$$

是一个良定的 $\mathbb{Q}-$同态.

9. 证明复数 $\mathrm{i}\sqrt{3},1+\mathrm{i}\sqrt{3}$ 都是 $f(x)=x^4-2x^3+7x^2-6x+12$ 的根. 设 K 是有理数域 $\mathbb{Q}$ 与 $f(x)$ 的根生成的域. 时候存在 K 的自同构 σ 使得 $\sigma\left(\mathrm{i}\sqrt{3}\right)=1+\mathrm{i}\sqrt{3}$？

10. 确定如下域是否在有理数域上 Galois.

(1) $\mathbb{Q}(\omega)$，其中 $\omega=\exp(2\pi\mathrm{i}/3)$；　(2) $\mathbb{Q}\left(\sqrt[4]{2}\right)$；　(3) $\mathbb{Q}\left(\sqrt{5},\sqrt{7}\right)$.

提示：上一节的某个习题.

11. 证明或者否定如下断言及其逆：设有域的包含关系 $F\subseteq L\subseteq K$，如果 K/L 与 L/F Galois，则 K/F Galois.

3. 正规扩张

在上一节我们发现，单代数扩张 $F(\alpha)/F$ 不是 Galois 扩张源于两种情形：$\min(F,\alpha)$ 的某些根不在 $F(\alpha)$ 中，或 $\min(F,\alpha)$ 有重根. 本节主要讨论：何时 $F(\alpha)$ 包含 $\min(F,\alpha)$ 的所有根？这对一般代数扩张的意义何在?

我们首先给出实数域上多项式一个熟悉的结论.

引理 3.1 设 $f(x)\in F[x],\alpha\in F$，则：α 是 $f(x)$ 的根 $\Leftrightarrow x-\alpha\mid f(x)$.

进而，f 在 F 的任一扩域中最多有 $\deg(f)$ 个根.

证明 (1) 由多项式的带余除法，设 $f(x)=q(x)(x-a)+r(x)$，其中 $q(x),r(x)\in F[x]$ 且 $\deg(r(x))<1$，即 $r(x)=r$ 是常数. 在 $f(x)=q(x)(x-a)+r$ 中令 $x=\alpha$，则 $r=f(\alpha)$，故:

$$\alpha\text{ 是 }f(x)\text{ 的根}\Leftrightarrow 0=f(\alpha)=r\Leftrightarrow x-\alpha\mid f(x).$$

(2) 对 f 的次数用归纳法. ■

定义 3.2 设有域扩张 K/F，$f(x)\in F[x]$. 如果存在 $\alpha_1,\cdots,\alpha_n\in K,c\in F$ 使得

$$f(x)=c\prod_{i=1}^{n}(x-\alpha_i),$$

就称 $f(x)$ ***在 K 上分裂***. 即:f 在 K 上分裂 $\Leftrightarrow f$ 完全分解为 $K[x]$ 中一次因子之积.

为了讨论某给定多项式的根，需要一个扩域使其包含多项式的根. 下一定理表明对任一多项式