Algebra Collection

ZIXI LI

Qiuzhen College, Tsinghua University

2023

目录

0.1 非交换代数

定理 0.1.1 (Wedderburn 小定理). 有限除环都是域。

证明. 设 D 是有限除环，F 是乘法群的中心，那么 F 是有限域。设 $q=|F|$，D 是 F 上的线性空间，记 $n=\dim_F D, |D|=q^n$，于是只需证明 $n=1$。

对于任何 $x\in D$：

$$C_D(x)=\{y\in D|xy=yx\}$$

是除环，并且 $F\subseteq C_D(x)\subseteq D$，因此它作为 F 上的线性空间元素个数必定形如 q^d，另一方面作 $C_D(x)$ 作为 $D^\times$ 的子群，一定满足 $q^d-1|q^n-1$，于是简单的数论讨论说明 $d|n$。

现在写出 $D^\times$ 类方程：

$$q^n-1=q-1+\sum\frac{q^n-1}{q^{d_x}-1}$$

其中求和对非平凡的共轭类进行。现在考虑分圆多项式 $\Phi_n(T)$,对于 $d|n, d<n$ 就有 $\Phi_n(T)|\dfrac{T^n-1}{T^d-1}$，于是代入 $T=q$ 就有 $\Phi_n(q)|\dfrac{q^n-1}{q^d-1}$，从而再次代入类方程就有 $\Phi_n(q)|q-1$。

但是计算模长知 $n>1$ 时这是不可能的，因此只有 $n=1$，这就完成了证明。 □

定理 0.1.2 (Artin-Wedderburn 定理). 如果 R 是半单环（作为自身的左模是半单的：即子模一定存在直和补），那么存在正整数 $n, d_1, \cdots, d_n$，以及除环 $D_1, \cdots, D_n$ 使得

$$R\cong\prod_{i=1}^{n}M_{d_i}(D_i)$$

其中 $M_n(D)$ 是除环上的矩阵代数。

证明. 首先我们指出 Schur 引理：单模之间的同态要么是同构，要么是零态射。作为推论，单模的自同态代数是除环。

由于 R 作为左 R-模半单，那么存在一族单左理想 L_i 使得 $R=\oplus_{i\in I}L_i$。

设 1 在 L_i 中的投影为 e_i，那么 r 在 L_i 中的投影是 re_i，即 $L_i=\{r|re_i=r\}$，从而 e_i 非零（否则 $L_i=0$，这与 L_i 是单模矛盾）。因此 1 拆解成为了若干个非零的 e_i 的和，于是 L_i 个数有限。依同构分类有

$$R\cong\oplus_{i=1}^{n}L_i^{d_i}$$

现在由 Schur 引理：

$$End_R(R)=\prod_{i=1}^{n}End_R(L_i^{d_i})=\prod_{i=1}^{n}M_{d_i}(End_R(L_i))$$

由 Schur 引理，$End_R(L_i)$ 是除环，D_i 是它的反还，$End_R(R)=R^{op}$，于是

$$R\cong\prod_{i=1}^{n}M_{d_i}(D_i)$$

□

推论 0.1.3. 左半单环和右半单环相同。

0.2 $PSL_n(F)$ 的单性

0.2.1 Iwasawa 定理

定义 0.2.1 (双传递). 称 G 在 X 上的作用是双传递的，如果 $|X| \geq 2$，并且对于任何 $x_1, x_2, y_1, y_2 \in X$，$x_1 \neq x_2, y_1 \neq y_2$，就有 $\exists g \in G, g(x_1) = y_1, g(x_2) = y_2$。

定理 0.2.2. *如果 G 在 X 上的作用是双传递的，那么对于任何 $x \in X, Stab_x$ 是 G 的极大真子群。*

证明. 固定 $H_x = Stab_x$，以及 $g \notin H_x$，我们来证明 $G = H_x \cup H_x g H_x$。

这是因为如果 $g' \notin H_x$，$gx, g'x \neq x$。那么考虑偶对 $(x, gx); (x, g'x)$，存在 $g'' \in G, s.t. g''x = x, g''gx = g'x$。因此 $g'' \in H_x$。进一步 $g''gx = g'x$ 说明 $g' \in g''gH_x \subseteq H_x g H_x$。

现在 H_x 不可能是 G，否则 $|X| = 1$。如果 $H_x < K < G$，取 $g \in K - H_x$，那么 $K \supseteq H_x \cup H_x g H_x = G$，矛盾。

□

定理 0.2.3. *如果 G 在 X 上的作用是双传递的，那么任何正规子群 $N \trianglelefteq G$ 在 X 上的作用要么是平凡的，要么是传递的。*

证明. 如果 N 的作用不是平凡的，那么 $\exists x \in X, n \in N, nx \neq x$。那么对于任何 $y \neq y', y, y' \in X$：考虑偶对 $(x, nx), (y, y')$，存在 $g \in G$ 使得 $gx = y, gnx = y'$。

因此 $y' = (gng^{-1})y$，并且 $gng^{-1} \in N$，从而是传递的作用。 □

定理 0.2.4 (Iwasawa). *如果 G 在 X 上的作用是双传递的，并且：*

- *存在 $x \in X$，使得 $Stab_x$ 包含一个 $Stab_x$ 的 Abel 正规子群 U，并且 U 在 G 中的全体共轭子群生成了 G。*
- $[G, G] = G$。

那么 G/K 是单群，其中 K 是群作用的核。

证明. 假定 $K \leq N \leq G$，并且 $N \trianglelefteq G$。现在取 $H = Stab_x$，那么 $NH = HN$ 是 G 的包含 H 的子群，由定理 0.2.2$NH = H$ *or* G。由定理 0.2.3 N 在 X 上的作用是平凡或者传递的。

如果 $NH = H$，那么 N 固定 x，从而在 X 上作用不是传递的。因此 N 在 X 上的作用是平凡的，于是 $N \subseteq K$，从而只能有 $N = K$。

如果 $NH = G$，那么取 U 为满足要求的 Abel 子群，$U \trianglelefteq H$。从而 $NU \trianglelefteq NH = G$。对于任何 $g \in G$，$gUg^{-1} \subseteq g(NU)g^{-1} = NU$。因此由 U 的假定，$NU = G$。

因此 $G/N = NU/N \cong U/(N \cap U)$，$U$ 的 Abelian 性说明 G/N 也是如此，因此 $N \supseteq [G, G] = G$，从而 $N = G$。

□

0.2.2 $PSL_2(F)$

定理 0.2.5. *对于域 $|F| \geq 4$，$PSL_2(F)$ 是单群。*

使用 Iwasawa 定理 0.2.4，考虑 $SL_2(F)$ 在 $P^1(F)$ 上的作用。

命题 0.2.6. $SL_2(F) \curvearrowright P^1(F)$ 的作用是双传递的。

这是简单的，将两条不同的 1 维子空间对应地拉至目标子空间即可，再调整系数使之落入 SL。

命题 0.2.7. 这个作用的核 K 是 $SL_2(F)$ 的中心。

它一定是纯量阵 rI 和 SL_2 的交。（这一事实对于 $n > 2$ 也成立：因为 $GL_n(F)$ 的中心是纯量阵 rI：只需观察 $I_n + c \cdot E_{ij}$ 的中心化子即可。）

命题 0.2.8. $\begin{pmatrix}1\\0\end{pmatrix} \cdot F$ 的稳定化子包含一个满足 *Iwasawa* 定理要求的 *Abel* 正规子群。

证明. 计算知稳定化子群为：

$$\{\begin{pmatrix}a & b\\0 & 1/a\end{pmatrix} | a \in F^\times, b \in F\}$$

那么计算知 $U = \{\begin{pmatrix}1 & b\\0 & 1\end{pmatrix} | b \in F\}$ 满足要求。

正规性和 Abel 都是简单的，其共轭子群生成 $SL_2(F)$ 是因为

$$\begin{pmatrix}1 & 0\\-\lambda & 1\end{pmatrix} = \begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & \lambda\\0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}^{-1}$$

并且 $\begin{pmatrix}1 & 0\\ & 1\end{pmatrix}, \begin{pmatrix}1 & *\\0 & 1\end{pmatrix}$ 生成了 $SL_2(F)$。 □

定理 0.2.9. 对于 $|F| \geq 4$，$[SL_2(F), SL_2(F)] = SL_2(F)$。

证明.

$$\begin{pmatrix}a & 0\\0 & 1/a\end{pmatrix}\begin{pmatrix}1 & b\\0 & 1\end{pmatrix}\begin{pmatrix}1/a & 0\\0 & a\end{pmatrix}\begin{pmatrix}1 & -b\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & b(a^2-1)\\0 & 1\end{pmatrix}$$

由于 $|F| \geq 4$，存在 $a^2 - 1 \neq 0$ 的情况，于是这说明 $U \subseteq [SL_2(F), SL_2(F)]$。由于交换子群是正规的，它包含 U 在 $SL_2(F)$ 中的所有共轭子群，这说明了 $[SL_2(F), SL_2(F)] = SL_2(F)$。 □

0.2.3 $SL_n(F)$

定理 0.2.10. 对于任何域 F，$n > 2$，$PSL_n(F)$ 是单群。

命题 0.2.11. $SL_n(F) \curvearrowright P^{n-1}(F)$ 的作用是双传递的，并且作用的核是 $SL_n(F)$ 的中心。

这和 $n = 2$ 的情况没有任何本质区别。

命题 0.2.12. $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} \cdot F$ 的稳定化子包含一个满足 *Iwasawa* 定理要求的 *Abel* 正规子群。

证明. 计算知稳定化子群为：

$$\{\begin{pmatrix} a & * \\ 0 & M \end{pmatrix} | a \cdot \det M = 1\}$$

考虑子群 $U = \{\begin{pmatrix} 1 & * \\ 0 & I_{n-1} \end{pmatrix}\}$，这是 $Stab$ 的正规子群：考虑到 $(1,1)$ 分量的投影。

同时它是 Abel 的，因为它同构于 F^{n-1}。

Claim 1. $n > 2$，每个 $I_n + \lambda E_{ij}, i \neq j$ 在 $SL_n(F)$ 中和 $I_n + E_{12}$ 共轭，其中 $\lambda \in F^\times$。

取出 F^n 的一组标准基 e_k，设 T 是矩阵 $I_n + \lambda E_{ij}$ 表示的线性变换。记 $f_1 = \lambda e_i, f_2 = e_j, f_3, \cdots, f_n$ 是 $e_1, \cdots, e_{i-1}, e_{i+1}, \cdots, e_{j-1}, e_{j+1}, \cdots, e_n$ 的一组排列。

那么 T 在 $\{f_i\}$ 下的表示是 $I_n + E_{12}$。即在 $GL_n(F)$ 中，$I_n + \lambda E_{ij} = A(I_n + E_{12})A^{-1}$。

现在我们对 A 进行一些调整使之成为 $SL_n(F)$ 中的元素。由于 $A(e_k) = f_k$，现在定义

$$A_c(e_k) = \begin{cases} f_k & k < n \\ cf_n, k = n \end{cases}$$

现在观察知这也是满足要求的 A_c（注意 $n \geq 3$，所以变换 cf_n 时不会受到 E_{12} 的影响）那么调整 A_c 的系数 c 即可使之落入 $SL_n(F)$ 中。

Claim 2. $I_n + \lambda E_{ij}, i \neq j, \lambda \in F^\times$ 生成了 $SL_n(F)$。

只需考虑行变换和列变换总能将 $SL_n(F)$ 变为标准型 I_n。 □

定理 0.2.13. $[SL_n(F), SL_n(F)] = SL_n(F)$

证明. 首先说明 $I_n + E_{12} \in SL_n(F)$，这是因为将左上角 2×2 分块，右下角 $(n-2) \times (n-2)$ 保持 I_n，这个问题和 $SL_2(F)$ 的构造没有差别。

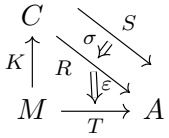
现在由于换位子群是正规的。因此 $I_n + \lambda E_{ij}$ 都在换位子群里，进而 $SL_n(F)$ 也是。 □

0.3 Kan 扩张

0.3.1 Kan 扩张

定义 0.3.1 (右 Kan 扩张). 给定函子 $K : M \to C, T : M \to A$，称 T 沿 K 的右 Kan 扩张是偶对 $(R, \varepsilon : RK \to T)$，其中 $R \in A^C$，$\varepsilon : RK \to T$ 是自然变换，并且满足偶对在函子 $A^K : A^C \to A^M$ 到 $T \in A^M$ 的自然变换中是万有的。

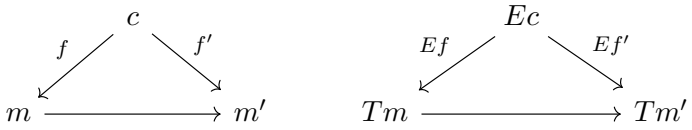
注记. 这里万有性的意思是对于任何 $(S, \alpha : SK \to T)$，存在唯一的自然变换 $\sigma : S \to R$ 使得，$\alpha = \varepsilon \cdot \sigma K : SK \to T$，即：



因此：$Nat(S, Ran_K T) \cong Nat(SK, T)$，并且这个双射关于 S 是自然的。这实际上说明 $Ran : A^M \to A^C$ 是 $A^K : A^C \to A^M$ 的右伴随。同时万有性保证了 $Ran_K T$ 在自然同构意义下唯一。

例子. M 是 C 的子范畴，并且 $K : M \to C$ 是嵌入函子时：A^K 是指将 $C \to A$ 限制成为 $M \to A$。我们现在考虑给定 $T : M \to A$ 的延拓 $E : C \to A$。

那么 $Ec \in A$ 总是应当满足：



因此当然可以选取 Ec 为右侧图表的极限锥。

这一结果可以推广到任何 $K : M \to C$ 上：

定理 0.3.2 (右 Kan 扩张的逐点极限构造)**.** 考虑逗号范畴 $(c \downarrow K)$：这里的记号是指 $\mathbf{1} \xrightarrow{\mapsto c} C \xleftarrow{K} M$。

如果 $K : M \to C, T : M \to A$ 满足

$$(c \downarrow K) \xrightarrow{pr} M \xrightarrow{T} A$$

对每个 c 都在 A 中有极限，记极限锥为 λ，

$$Rc = \varprojlim((c \downarrow K) \to M \to A)$$

并且 $g : c \to c'$ 诱导了唯一的态射 $Rg : \varprojlim TQ_c \to \varprojlim TQ_{c'}$（这里 $Q_c = pr_c$）使得它和诸极限锥交换。

因此这定义出了一个函子 $R : C \to A$，对于每个 $m \in M$，$\lambda_{1_{Km}} = \varepsilon_m$ 诱导了自然变换 $\varepsilon : RK \to T$，这里 1_{Km} 是 $(Km \downarrow K)$ 中的元素，于是 Km 对应的极限锥中有一个分量 $RKm \to Tm$。

(R, ε) 是 T 沿 K 的右 *Kan* 扩张。

推论 0.3.3. M 是小范畴，A 完备，那么 $T : M \to A, K : M \to C$ 总有右 *Kan* 扩张。

推论 0.3.4. 如果 K 是全忠实函子，$\varepsilon : RK \to T$ 是一个自然同构。

证明. 我们只需说明 $RKm = Tm$，这是因为考虑 $Cone(TQ)$，每个 $Km \to Km'$ 由 $m \to m'$ 给出，于是给出了 $Tm \to Tm'$。这就说明了 Tm 是一个顶点。 □

推论 0.3.5. M 是 C 的全子范畴，函子 $T : M \to A$ 沿嵌入 $M \to C$ 的扩张 K 的确满足 $RK = T$，并且 $1 : RK \to T$ 使得 R 成为右 *Kan* 扩张。

类似地，定义左 Kan 扩张，它满足 Lan 是 A^k 的左伴随。自然也有逐点极限构造：

$$Lc = \varinjlim((K \downarrow c) \to M \to A)$$

0.3.2 Kan 扩张的 Coend 公式

第一部分

P.Morandi - Field and Galois Theory

第一章　域扩张

1.1　结论

命题 1.1.1 (维数控制). $[F(a_1,\cdots,a_n):F]\leq\prod[F(a_i):F]$

证明. 归纳：只需注意对于 L/F，$[L(a):L]\leq[F(a):F]$（观察极小多项式）。 □

这一不等式有如下推广：

命题 1.1.2 (Morandi 1.17,19). *K 是 F 的有限扩域，L_1,L_2 是 K 的子域且都包含 F，那么*

$$[L_1L_2:F]\leq[L_1:F]\cdot[L_2:F]$$

进一步如果 $\gcd([L_1:F],[L_2:F])=1$，上述不等式取等。

存在使得上述不等式严格成立的例子。

证明. 假定 $L_1=F(a_1,\cdots,a_n);L_2=F(b_1,\cdots,b_m)$。仿照前述，只需说明：

对于 L/F，$[L(a_1,\cdots,a_n):L]\leq[F(a_1,\cdots,a_n):F]$。

$n=1$ 时已证。对 n 归纳，假定 $n-1$ 成立，那么：

$$\begin{aligned}[L(a_1,\cdots,a_n):L]&=[L(a_1,\cdots,a_{n-1})(a_n):L(a_1,\cdots,a_{n-1})]\cdot[L(a_1,\cdots,a_{n-1}):L]\\&\leq[F(a_1,\cdots,a_{n-1})(a_n):F(a_1,\cdots,a_{n-1})]\cdot[F(a_1,\cdots,a_{n-1}):F]\\&=[F(a_1,\cdots,a_n:F)]\end{aligned}$$

这就说明了结果。现在对于 L_1,L_2 直接运用上述结果得证。

如果 $\gcd([L_1:F],[L_2:F])=1$，注意到 $[L_1L_2:F]=[L_1:F]\cdot[L_1L_2:L_1]$，于是 $[L_1:F]|[L_1L_2:F]$，对 L_2 同理。于是结合前述不等式得证。

取 $L_1=L_2$，$[L_1:F]=2$ 时上述不等式严格成立：因为 $L_1L_2=L_1$。 □

定理 1.1.3 (代数扩张的传递性). *如果 $L/F,K/L$ 是代数的，那么 K/F 也是。*

证明. 给定 $\alpha\in K$，$f(x)=\min(\alpha,L)$，设诸系数为 $c_{n-1},\cdots,c_0$。现在由于 L/F 是代数的，那么 $L_0=F(c_{n-1},\cdots,c_0)$ 是有限扩张。

于是 α 在 L_0 上是代数的。然而

$$[F(\alpha):F]\leq[L_0(\alpha):F]=[L_0(\alpha):L_0]\cdot[L_0:F]$$

两部分都是有限的，因此 α 在 F 上是代数的。 □

1.2 例子

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

证明. 由于 $4=[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]$ 是 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{3}):\mathbb{Q}]$ 的因子，并且前述不等式保证了 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{3}):\mathbb{Q}]\leq 8$，于是 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{3}):\mathbb{Q}]=4$ 或 8。

如果 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{3}):\mathbb{Q}]=4$，那么 $[\mathbb{Q}(\sqrt[4]{2},\sqrt{3}):\mathbb{Q}(\sqrt[4]{2})]=1$，即两个域相同：$\sqrt{3}\in\mathbb{Q}(\sqrt[4]{2})$。

但是初等计算知 $\sqrt{3}$ 不可能写成 $1,\sqrt[4]{2},\sqrt{2},\sqrt[4]{8}$ 的 $\mathbb{Q}-$ 线性组合，从而完成证明。 □

例子. *$K=k(t)$ 为域 k 的有理函数域，选定 $u\in K-k$，设 $u=f(t)/g(t)$，其中 $f,g\in k[t]$ 并且 f,g 互素。取 $F=k(u)$。那么*

$$[K:F]=\max\{\deg f,\deg g\}$$

证明. 由于 $K=k(t)=k(u)(t)=F(t)$，因此只需计算 $\min(F,t)$。

考虑 $p(x)=ug(x)-f(x)\in F[x]$，那么 t 是 $p(x)$ 的根，并且 $\deg p=\max\{\deg f,\deg g\}$。（唯一使这个结果不成立的可能是 $m=n$ 并且首项系数消去：但是此时首项系数是 ub_n-a_n，$u\notin K$，于是首项系数非零）

现在只需说明 $p(x)$ 在 F 上不可约。首先 u 不是 k 上的代数元，否则 $[K:k]=[K:F]\cdot[F:k]$，第二项有限，第一项由前述 t 的零化多项式知有限，于是 $[k(t):k]<+\infty$，这是不可能的。

因此 u 在 k 上超越，从而 $k[u]\cong k[x]$。现在将 p 视为 u 的多项式：$p\in k[x][u]\subseteq k(x)[u]$，$p$ 关于 u 的次数是 1，于是它在 $k(x)$ 上不可约。

由于 $\gcd(f,g)=1$，那么 p 在 $k[x][u]$ 中是本原的。于是 p 在 $k[x]$ 上是不可约的。

因此如果 p 在 $k[u]$ 上是可约的，那么将两个因子 $qr=p$ 分别整理成关于 u 的多项式，就给出了 $k[x]$ 上的分解，与前述矛盾。从而 p 在 $k(u)=F$ 上不可约，这就说明了结果。 □

例子. *对于一个有理数组成的有限集 $\{p_1,\cdots,p_n\}$，如果任何 $\{\sqrt{p_1},\cdots,\sqrt{p_n}\}$ 的子集元素乘积都不在 $\mathbb{Q}$ 中，那么 $[\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n}):\mathbb{Q}]=2^n$*

证明. 对 n 归纳，$n=0,1$ 已证。

由于 $[\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n}):\mathbb{Q}]=2^{n-2}$，只需证明 $\{1,\sqrt{p_1},\sqrt{p_2},\sqrt{p_1p_2}\}$ 在其上线性无关。

有归纳假设 $[\mathbb{Q}(\sqrt{p_1},\sqrt{p_3},\cdots):\mathbb{Q}]=\cdots=2^{n-1}$，因此 $\sqrt{p_1},\sqrt{p_2},\sqrt{p_1p_2}\notin\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n})$。假定有 $\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n})$ 上线性组合：

$$a+b\sqrt{p_1p_2}=c\sqrt{p_1}+d\sqrt{p_2}$$

其中 $a,b,c,d\in\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n})$

那么平方后即得

$$a^2+b^2p_1p_2-c^2p_1-d^2p_2=2(cd-ab)\sqrt{p_1p_2}$$

由于 $\sqrt{p_1p_2}\notin\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n})$，只能有 $cd=ab$。

同样对 $a-d\sqrt{p_2}=c\sqrt{p_1}-b\sqrt{p_1p_2}$ 平方得到 $ad=bcp_1$。于是 $a^2d=abcp_1=c^2dp_1$，因此 $c^2d=0$（否则 $\sqrt{p_1}\in\mathbb{Q}(\sqrt{p_3},\cdots,\sqrt{p_n})$）

如果 $d \neq 0$。那么 $a + b\sqrt{p_1p_2} = d\sqrt{p_2}$，因此 $a^2 + 2ab\sqrt{p_1p_2} + b^2p_1p_2 = d^2p_2$。于是 $ab = 0$，容易验证这不可能发生；同样可以检验 $c \neq 0$ 的情况。

因此这就说明了 $\{1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}\}$ 在 $\mathbb{Q}(\sqrt{p_3}, \cdots, \sqrt{p_n})$ 上线性无关，从而完成了证明。

□

1.3 习题

练习 1.1 (Morandi 1.8). *$K = F(a)$ 是 F 的有限扩张。对 $\alpha \in K$，定义 $L_\alpha : K \to K$ 为 $L_\alpha(x) = \alpha x$。这是 F 线性变换，证明 $\det(xI - L_a)$ 是 a 的极小多项式 $\min(F, a)$。另外对于何种 α 有 $\det(xI - L_\alpha) = \min(F, \alpha)$?*

证明. 由有限单扩张的结构：设 $\deg \min(F, a) = n$，那么 $1, a, \cdots, a^{n-1}$ 是 K 在 F 上的一组基，观察 L_a 在其上的作用是 $\min(F, a)$ 对应的友矩阵，那么结果成立。

如果 $\det(xI - L_\alpha) = \min(F, \alpha)$，那么 $\min(F, \alpha)$ 也是 n 次多项式，于是 $1, \alpha, \cdots, \alpha^{n-1}$ 是 $F-$ 线性无关的 n 个元素，从而张成了 K，于是 $K = F(\alpha)$。

因此满足要求的 α 恰好是使得 $K = F(\alpha)$ 成立的那些 α。 □

练习 1.2 (Morandi 1.10). *K 是 F 的扩域，$a \in K$ 使得 $[F(a) : F]$ 是奇数，那么 $F(a) = F(a^2)$，举例说明结果对 $[F(a) : F]$ 是偶数不成立。*

证明. 有扩域 $F \subseteq F(a^2) \subseteq F(a)$。注意 $F(a) = F(a^2)(a)$，因此 $[F(a) : F(a^2)] = \min(F(a^2), a)$。

如果 $a \in F(a^2)$，那么结论已成立。若否：明显 $x^2 - a^2$ 是一个 $F(a^2)[x]$ 中的零化多项式，并且是次数最低者（1 次则意味着 $a \in F(a^2)$。因此 $[F(a) : F(a^2)] = 2$。

然而 $[F(a) : F] = [F(a) : F(a^2)] \cdot [F(a^2) : F]$，矛盾。

当 $a = \sqrt[4]{2}$ 时 $F(a) \neq F(a^2)$。 □

练习 1.3 (Morandi 1.11: 中间扩环就是扩域). *K 是 F 的代数扩张，R 是 K 的子环使得 $F \subseteq R \subseteq K$，那么 R 是域。*

证明. 对于 $r \in R$，假定

$$r^n + c_{n-1}r^{n-1} + \cdots + c_0 = 0, c_i \in F$$

那么

$$r^{-1} = \frac{1}{c_0}[-r^{n-1} - \cdots - c_1] \in R$$

□

练习 1.4 (Morandi 1.14,15: 域的合成的有限性、代数性). *假定 L_1, L_2 是 F 的扩域，并且包含于某个共同的域内：那么 L_1L_2 是 F 的有限扩域 $\iff$ L_1, L_2 都是；L_1L_2 是 F 的代数扩域 $\iff$ L_1, L_2 都是。*

证明. L_1L_2/F 有限 $\implies$ L_1, L_2 有限：因为 $[L_i : F] \leq [L_1L_2 : F] < +\infty$

L_1, L_2 是 F 的有限扩域，于是可设 $L_1 = F(a_1, \cdots, a_n); L_2 = F(b_1, \cdots, b_m)$。那么 $L_1L_2 = F(a_1, \cdots, a_n, b_1, \cdots, b_m)$。

于是

$$[L_1L_2:F]=[F(a_1,\cdots,a_n,b_1,\cdots,b_m):F]\leq\prod[F(a_i):F]\prod[F(b_i):F]$$

由于有限扩域是代数的，那么上式右侧诸因子都是有限的。

L_1L_2/F 是代数扩域 $\Longrightarrow$ L_1,L_2 是。

如果 L_1,L_2 都是 F 的代数扩域：考虑 L_1L_2 中在 F 上整的元素（于是等价地就是代数的元素），由交换代数结果知这些元素构成了包含 L_1,L_2 的 F 的扩环。

这个环一定是域，因为如果 r 在 F 上是代数的，$1/r$ 也一定如此（倒根方程）。因此这是一个包含 L_1,L_2 的域，于是只能是 L_1L_2。 □

练习 1.5 (Morandi 1.16: 代数整数不是有限扩张). $\mathbb{A}$ 是 $\mathbb{Q}$ 在 $\mathbb{C}$ 中的代数闭包，那么 $[\mathbb{A}:\mathbb{Q}]=\infty$。

证明. 假定 $[\mathbb{A}:\mathbb{Q}]=n$，那么对于任何 $\alpha\in\mathbb{A}$，其极小多项式次数不超过 n。但是考虑 $\sqrt[n+1]{2}$ 即得矛盾：因为 $x^{n+1}-2$ 是不可约多项式，从而其极小多项式次数为 $n+1$。 □

第二章　自同构

2.1　结论

定义 2.1.1. 域扩张 K/F 的 Galois 群定义为全体保持 F 不动的域自同构 $K \to K$ 构成的群。

2.1.1　Galois 对应

定理 2.1.2. 对于域扩张 K/F，$L \mapsto Gal(K/L)$ 和 $H \mapsto \mathcal{F}(H)$ 给出了 $Gal(K/F)$ 的形如 $Gal(K/L)$ 的子群（L 是中间域）和形如 $\mathcal{F}(S)$ 的中间域（$S \subseteq Aut(K)$）之间的一一对应。

我们有更一般的 Galois 对应：

命题 2.1.3 (Morandi 2.12:Galois 联络)**.** S, T 是两个偏序集，如果 $f : S \to T, g : T \to S$ 分别逆转偏序（即 $s_1 \leq_S s_2 \implies f(s_2) \leq_T f(s_1), etc.$），并且 $s \leq_S g(f(s)), t \leq f(g(t))$。那么 $\operatorname{Im} g$ 和 $\operatorname{Im} f$ 之间有一一对应，这个对应由 $s \mapsto f(s)$ 和 $t \mapsto g(t)$ 给出。

注记. 将偏序集看成范畴，这实际上给出了 S, T^{op} 之间的一对伴随函子。

2.1.2　Galois 群大小的控制

命题 2.1.4 (有限扩张的 Galois 群有限)**.** 如果 $[K : F] < +\infty$，那么 $|Gal(K/F)| < +\infty$。

证明. 假定 $K = F(a_1, \cdots, a_n)$，Galois 群中的元素将每个 a_i 映到其极小多项式在 K 中的根，这样的选择个数总是有限的。 □

现在有更精细的控制：

定义 2.1.5 (特征)**.** 一个特征是指群 G 到域 K 的乘法群 K^* 的一个群同态。

注记. 取 $G = K^*$ 后，K 的 F 自同构诱导了 $G \to K^*$ 的特征。

引理 2.1.6 (Dedekind's Lemma)**.** 给定不同的特征 $\tau_1, \cdots \tau_n : G \to K^*$，那么它们在 K 上线性无关。即

$$\sum_i c_i \tau_i(g) = 0, \forall g \in G$$

其中 $c_i \in K$，那么 $\forall i, c_i = 0$。

证明. 若否，选择最小的 k 使得存在 k 个特征线性无关并且系数 c_i 不全是 0. 由 k 的极小性 $\forall c_i \neq 0$。

由于 $\tau_1 \neq \tau_2$，取 $h \in G$ 使得 $\tau_1(h) \neq \tau_2(h)$。那么：

$$\sum_{i=1}^{k}(c_i\tau_1(h))\tau_i(g) = 0$$

并且

$$\sum_{i=1}^{k}(c_i\tau_i(h))\tau_i(g) = \sum_{i=1}^{k} c_i\tau_i(hg) = 0$$

两式相减：

$$\sum_{i=1}^{k}(c_i(tau_1(h) - \tau_i(h)))\tau_i(g) = 0$$

对所有 g 成立。由于首项系数为 0，我们给出了 $k-1$ 个特征的线性组合使得系数不全为零（$c_2(\tau_1(h) - \tau_2(h))$，这和 k 的极小性矛盾。 □

命题 2.1.7 (有限扩张的 Galois 群大小不超扩张次数). *K/F 是有限扩张，那么 $|Gal(K/F)| \leq [K:F]$。*

证明. 假设 $Gal(K/F) = \{\tau_1, \cdots, \tau_n\}$，但是 $m = [K:F] < n$。取 K 的 $F-$ 基 $\alpha_1, \cdots, \alpha_m$，那么 K 上的矩阵

$$A = (\tau_i(\alpha_j))_{\substack{1\leq i\leq n \\ 1\leq j\leq m}}$$

的秩满足 $\text{rank}(A) \leq m < n$。

因此 A 的行向量是线性相关的，即 $\sum_i c_i\tau_i(\alpha_i) = 0, \forall j$，并且 c_i 不全为 0。

现在考虑域自同构诱导的 $G = K^* \to K^*$ 的特征，容易验证在生成元上作用得到的行向量线性相关说明了这些特征线性相关：

假定 $g = \sum_j a_j\alpha_j$，那么

$$\sum_i c_i\tau_i(g) = \sum_i c_i\tau_i(\sum_j a_j\alpha_j) = \sum_j a_j(\sum c_i\tau_j\alpha_j) = 0$$

那么由 Dedekind 引理，$c_i = 0, \forall i$，矛盾。 □

定义 2.1.8. 称代数扩张 K/F 是 Galois 的，如果 $F = \mathcal{F}(Gal(K/F))$

命题 2.1.9 (Galois 扩张时取等). *G 是 K 的一些自同构构成的有限群，$F = \mathcal{F}(G)$，那么 $|G| = [K:F]$，于是 $G = Gal(K/F)$。*

反过来，有限扩张 K/F 是 Galois 的如果 $|Gal(K/F)| = [K:F]$

证明. 由于 $G \subseteq Gal(K/F)$，$|G| \leq |Gal(K/F)| \leq [K:F]$。假定 $|G| < [K:F]$，取 $n = |G|$，$\alpha_1, \cdots, \alpha_{n+1} \in K$ 在 F 上线性无关，$G = \{\tau_1, \cdots, \tau_n\}$。

再次考虑矩阵

$$A = (\tau_i(\alpha_j))_{\substack{1\leq i\leq n \\ 1\leq j\leq n+1}}$$

那么 A 的列向量是 $K-$ 线性相关的。无妨选取最小的 k 使得存在 k 列（无妨为前 k 列）使得：

$$\sum_{i=1}^{k} c_i \tau_j(\alpha_i) = 0, \forall j$$

这里 $c_i \in K$。k 的极小性说明 $\forall i, c_i \neq 0$。

进一步假定 $c_1 = 1$。现在选出一个 $\sigma \in G$，作用到前述式子上，由于 $\sigma \circ \tau_j$ 只是对全体 τ_j 进行重排，就有：

$$\sum_{i=1}^{k} \sigma(c_i) \tau_j(\alpha_i) = 0, \forall j$$

由于 $c_1 = 1$，将两式相减就有

$$\sum_{i=2}^{k} (c_i - \sigma(c_i)) \tau_j(\alpha_i) = 0$$

极小性说明 $\forall i, c_i - \sigma(c_i) = 0$。因此每个 G 中的元素都固定了 c_i，从而 $c_i \in \mathcal{F}(G) = F$。

然而如果每个 c_i 都是 F 中元素，那么 $0 = \tau_j(\sum_{i=1}^{k} c_i \alpha_i)$，于是 $\sum_{i=1}^{k} c_i \alpha_i = 0$，这和 α_i 的选取矛盾。

因此这说明只能有 $|G| = [K : F]$，从而 $G = Gal(K/F)$。

反过来如果 $|Gal(K/F)| = [K : F]$，那么考虑 $L = \mathcal{F}(Gal(K/F))$，则 $F \subseteq L$。上一半命题说明 $Gal(K/F) = Gal(K/L)$。

于是有

$$[K : F] = |Gal(K/F)| = |Gal(K/L)| = [K : L] \leq [K : F]$$

，这说明 $[K : F] = [K : L]$，从而 $L = F$。 □

2.2 例子

命题 2.2.1 (单扩张是 Galois 扩张的条件). *K/F 是域扩张，$a \in K$ 是 F 上的代数元，那么 $|Gal(F(a)/F)$ 为 $\min(F, a)$ 在 $F(a)$ 中的不同根的个数。从而 $F(a)/F$ 是 Galois 的 $\iff$ $\min(F, a)$ 在 $F(a)$ 中有 n 个不同的根，$n = \deg \min(F, a)$。*

证明. $F-$ 自同构完全由其在 a 上的作用决定，于是 $|Gal(F(a)/F)| \leq n$：因为它将 a 映到 $\min(F, a)$ 在 $F(a)$ 中的根（这不会超过 n 个选择）

反过来对于 $\min(F, a)$ 在 $F(a)$ 中的另一个根 b，将 a 映到 b 确实直接诱导了一个 $F-$ 自同构。因此这就说明了 $|Gal(F(a)/F)$ 为 $\min(F, a)$ 在 $F(a)$ 中的不同根的个数。

现在 $[F(a) : F] = \deg \min(F, a)$，由命题 2.1.9知这等价于 $\min(F, a)$ 在 $F(a)$ 中有 n 个不同的根。 □

例子 (对称多项式，Galois 反问题). *取 $K = k(x_1, \cdots, x_n)$，那么有 S_n 在 K 上的自同构：对 x 的下指标做置换。现在考虑 $F = \mathcal{F}(S_n)$，那么 K/F 是 Galois 扩张，并且 $Gal(K/F) = S_n$。由于每个群 G 都是某个 S_n 的子群，再次考虑 $\mathcal{F}(G)$ 即可得到以 G 为 Galois 群的 Galois 扩张。*

考虑初等对称多项式：

$$s_1 = x_1 + \cdots + x_n, \cdots, s_n = x_1 x_2, \cdots, x_n$$

。那么 $k(s_1, \cdots, s_n) \subseteq F$，我们将会说明实际上它就是 F。

例子 (Morandi 2.8: 置换不可约多项式的根). 假定 $a \in \mathbb{C}$ 并且是 $\mathbb{Q}$ 上的代数元，$p(x) = \min(\mathbb{Q}, a)$，$b$ 是 p 在 $\mathbb{C}$ 中的根。那么 $\sigma : \mathbb{Q}(a) \to \mathbb{C}$ 是一个 $\mathbb{Q}-$ 同态。

例子 (Morandi 2.9: 并不总能任意置换多项式的根). 考虑 $f(x) = x^4 - 2x^3 + 7x^2 - 6x + 12$ 的两根 $i\sqrt{3}, 1 + i\sqrt{3}$，K 是 f 的全体根在 $\mathbb{Q}$ 上生成的扩域。不存在 K 的自同构将 $i\sqrt{3}$ 映为 $1 + i\sqrt{3}$。

证明. 假设存在，那么 $-3 = \sigma(-3) = -2 + 2i\sqrt{3}$，矛盾。 □

注记. 这实际上是因为 $i\sqrt{3}, 1 + i\sqrt{3}$ 位于 f 的两个不可约分支内。现在结合前一例子就说明了 f 不可约（前一例中那样的 σ 会导出这里的矛盾）。

例子 (Morandi 2.10). 判断下列扩域是否是 *Galois* 的：

1. $\mathbb{Q}(\omega)/\mathbb{Q}$，$\omega$ 是三次单位根
2. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$
3. $\mathbb{Q}(\sqrt{5}, \sqrt{7})$

证明.

1. 是，因为 $\min(\mathbb{Q}, \omega) = x^3 - 1$，$1, \omega, \omega^2$ 是 $\mathbb{Q}(\omega)$ 中的三个不同的根。
2. 不是，因为 $\min(\mathbb{Q}, \sqrt[4]{2}) = x^4 - 2$，但是 $\mathbb{Q}(\sqrt[4]{2})$ 中只有 $\pm\sqrt[4]{2}$ 两个不同的根。
3. 是，因为 $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5}+\sqrt{7})$，而 $\sqrt{5}+\sqrt{7}$ 在 $\mathbb{Q}$ 上的极小多项式是 $x^4 - 24x^2 + 109$。它在 $\mathbb{Q}$ 上不可约，于是确实是极小多项式。

   它的其他根为 $\pm\sqrt{5} \pm \sqrt{7}$，都落在 $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ 中。

□

例子 (Morandi 2.13). $K = k(x)$ 是 k 上有理函数域，定义 K 的自同构 σ, τ 为：

$$\sigma(f(x)/g(x)) = f(1/x)/g(1/x)$$

$$\tau(f(x)/g(x)) = f(1-x)/g(1-x)$$

计算 $\{\sigma, \tau\}$ 的不动域 F，$Gal(K/F)$，并找到 h 使得 $F = k(h)$

证明. 注意到 $\{\sigma, \tau\}$ 在 $Aut(K)$ 中生成的子群为

$$\{\mathrm{id}, \sigma, \tau, \sigma\tau, \tau\sigma, \sigma\tau\sigma\} \cong S_3$$

那么由命题 2.1.9知 K/F 是 Galois 的，并且 $[K : F] = 6, Gal(K/F) = S_3$

现在计算 F：注意 $Gal(K/F)$ 的 6 个元素作用到 x 上分别是：

$$x, \frac{1}{x}, 1-x, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}$$

设它们分别为 $s_1, \cdots, s_6$，那么 $Gal(K/F)$ 的作用只不过是对 $s_1, \cdots, s_6$ 进行置换。

现在考虑初等对称多项式 $t_2 = s_1s_2 + s_1s_3 + \cdots + s_5s_6$：经计算它是

$$\frac{(x^2-x-1)(x^4-2x^3+5x^2-4x+1)}{(x-1)^2x^2}$$

于是由第 1.2 节知 $[K : k(t_2)] = 6$，但是另一方面 $k(t_2) \subseteq F$，于是只有 $k(t_2) = F$。 □

- $k(x)/k$ **的 Galois 群**

例子 (Morandi 2.14,15). $K = k(x)$ 是 k 上有理函数域，对于 $u \in K$ 证明 $K = k(u)$ 当且仅当 $u = (ax+b)/(cx+d)$，$a, b, c, d \in K$ 并且 $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$

进一步，每一个 k 上的可逆 2×2 矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 都决定了 $Gal(k(x)/k)$ 的一个元素 $x \mapsto (ax+b)/(cx+d)$。反过来，证明每个 $Gal(k(x)/k)$ 中的元素都具有如上形式。

因此作为推论就得到

$$Gal(k(x)/k) \cong PGL_2(k)$$

。

证明. 假定 $K = k(u)$，那么 $[k(x) : k(u)] = 1$，从而 u 一定能写成两个不超过一次的多项式的比（第 1.2 节），因此直接验证即得到结果。

现在对于 $\tau \in Gal(k(x)/k)$，由于 x 在 k 上生成了 $k(x)$，那么 $\tau(x)$ 也能在 k 上生成 $k(x)$，从而 $\tau(x)$ 一定具有前述形式，这就完成了证明。 □

我们来考虑一些特例：

练习 2.1 (Morandi 2.16). $k = \mathbb{R}$，A 为旋转 $2\pi/3$ 给出的 2×2 矩阵。那么 A 在 $Gal(k(x)/k)$ 中生成了一个 3 阶子群 G。F 是 G 的不动域，于是 $k(x)/F$ 是 *Galois* 的。

现在考虑 $u = x + Ax + A^2x = \dfrac{3x^3 - 9x}{3x^2 - 1}$，由第 1.2 节知 $[k(x) : k(u)] = 3$，但是 $k(u) \subseteq F$，因此 $F = k(u)$。

练习 2.2 (Morandi 2.17). $k = \mathbb{F}_p$，$\varphi : k(x) \to k(x) : x \mapsto x+1$，于是这生成了 $Gal(k(x)/k)$ 的 p 阶子群。F 是这个子群的不动域，于是 $k(x)/F$ 是 *Galois* 的。

现在考虑 $u = x(x+1)\cdots(x+p-1) = x^p - x$，那么 $[k(x) : k(u)] = p$，而 $k(u) \subseteq F$，于是 $F = k(u)$。

更一般地，对于特征 p 域 k，$a \in k$，$\varphi : k(x) \to k(x) : x \mapsto x+a$。同样地取 $u = x^p - a^{p-1}x$，那么不动域 $F = k(u)$。

2.3 习题

练习 2.3 (Morandi 2.2). $\mathbb{R}$ 的域自同构只有恒等。

证明. 首先自同构 σ 满足 $\sigma|_{\mathbb{Q}} = \mathrm{id}$。对于 $a > 0$，设 $a = b^2, b \neq 0$。那么 $\sigma(a) = \sigma(b)^2 > 0$。因此 σ 是单调增的 $\mathbb{R} \to \mathbb{R}$ 的映射。

由于 $\mathbb{Q}$ 在 $\mathbb{R}$ 中稠密，这直接说明了 $\sigma = \mathrm{id}$。 □

练习 2.4 (Morandi 2.6). *charF* $\neq 2$，扩域 K 满足 $[K:F]=2$。证明 $K=F(\sqrt{a})$，并且这个扩张是 *Galois* 的。

证明. 假定 $\{1,\alpha\}$ 是 K 在 F 上的一组基，那么 $\alpha^2=c_1+c_2\alpha, c_i\in F$。

因此 $(\alpha-c_2/2)^2=c_1+c_2^2/4$，并且 $\{1,\alpha-c_2/2\}$ 仍然是 K 在 F 上的一组基，这就说明了结果。

现在假定 $K=F(\sqrt{a})$，$\min(F,\sqrt{a})=x^2-a$，但是 $-\sqrt{a}$ 也在 $F(\sqrt{})$ 中并且 $\sqrt{a}\neq-\sqrt{a}$，因此由单扩张是 Galois 扩张的判别，知它确实是 Galois 的。 □

练习 2.5 (Galois 扩张不具有合成性). $F\subseteq L\subseteq K$。如果 K/L，L/F 是 *Galois* 的，那么 K/F 不一定是 *Galois* 的。

反过来如果 K/F 是 *Galois* 的，那么即使 K/L 是 *Galois* 的，我们也不能推出另一部分扩域 L/F 是 *Galois* 的。

然而 K/F 是 *Galois* 的能说明对于任何中间域 L，K/L 是 *Galois* 的：这实际上是 *Galois* 基本定理的一部分，这里先不证明。

证明. 考虑 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$。注意：

$$\mathbb{Q}(\sqrt[4]{2})=\mathbb{Q}(\sqrt{2})(\sqrt[4]{2})$$

而 $\min(\mathbb{Q}(\sqrt{2}),\sqrt[4]{2})=x^2-\sqrt{2}$，因此 $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]=2$，另一方面 $x^2-\sqrt{2}$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 中恰好有两个不同的根 $\pm\sqrt[4]{2}$，因此这个扩张是 Galois 的。

但是 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是 Galois 扩张。

反过来，考虑 $K=\mathbb{Q}(\sqrt[3]{2},\omega)$，这里 ω 是三次单位根，则 $K/\mathbb{Q}$ 是 Galois 扩张。并且：$\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\sqrt[3]{2})$ 是 Galois 扩张，但是 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是。 □

第三章　正规扩张

3.1　结论

定义 3.1.1 (分裂). 给定扩域 K/F，$f \in F[x]$。称 f 在 K 上分裂如果 f 可以分解为 $K[x]$ 中若干一次因式的乘积，即可以写成 $a\prod(x-\alpha_i)$ 的形式，其中 $a \in F, \alpha_i \in K$。

定义 3.1.2 (分裂域). 扩域 K/F，$f \in F[x]$. 称 K 是 f 的分裂域，如果 f 在 K 上分裂并且 $K = F(\alpha_1, \cdots, \alpha_n)$，这里 α_i 是 f 的根。更一般地给定非常值 $F-$ 多项式的集合 S，称 K 是 S 的分裂域，如果每个 $f \in S$ 都在 K 上分裂，并且 $K = F(X)$。这里 X 是全体 f 的所有根。

3.1.1　分裂域的存在性、代数闭包

容易观察到只要能找到一个扩域使得多项式 f 分裂，那我们选取其根生成的子域就得到了分裂域。前者存在是因为：

定理 3.1.3 (单个多项式分裂域存在). *$f(x) \in F[x], \deg f = n$，那么存在 K/F 使得 $[K:F] \leq n$，并且 K 包含 f 的一个根。因此存在 L/F 使得 $[L:F] \leq n!$，并且 f 在 L 上分裂*

证明. 取 K 为 $F[x]/(p(x))$ 即可。 □

推论 3.1.4. *当 S 是有限集时，分裂域存在。*

对于一般的情况，我们采用类似的思路：找到一个代数扩张的最大者（这样所有多项式都分裂），然后再选好子域得到分裂域。前者就是代数闭域。

引理 3.1.5. *对于一个域 K，如下等价：*

1. *不存在除 K 自身以外的代数扩张*
2. *不存在除 K 自身以外的有限扩张*
3. *对于域扩张 L/K，K 在 L 中的代数闭包是自身*
4. *每个 $f \in K[x]$ 在 K 上分裂*
5. *每个 $f \in K[x]$ 在 K 中有根*
6. *K 上的每个不可约多项式次数均为 1。*

满足这样性质的域称为代数闭域。

证明. $1 \implies 2$ 显然。

$2 \implies 3$：如果 a 是 K 上的代数元，那么 $K(a)/K$ 是有限扩张。于是 $K(a) = K, a \in K$。

$3 \implies 4$：$f \in K[x]$，L 是 f 在 K 上的分裂域。那么 L/K 是有限扩张，从而是代数扩张，从而 $L = K$，从而 f 在 K 上分裂。

$4 \implies 5$ 显然。

$5 \implies 6$ 显然。

$6 \implies 1$ 给定代数扩张 L/K，$a \in L$，$p(x) = \min(K, a)$，那么 $\deg p = 1$，于是 $a \in K$，从而 $L = K$。 □

我们来证明代数闭域的存在性，很容易意识到应该使用 Zorn 引理，但这里有一些集合论上的小技巧。

引理 3.1.6. 如果 K/F 是代数扩张，那么 $|K| \leq \max\{|F|, |\mathbb{N}|\}$。

证明. 对多项式根直接计数即可。 □

定理 3.1.7. 域 F 存在代数闭包。

证明. 选择一个包含 F 的集合 S 使得 $|S| > \max\{|F|, |\mathbb{N}|\}$。$\mathcal{A}$ 为全体 F 在 S 中的代数扩张依包含关系构成的偏序集。

由 Zorn 引理选出极大元 M。假定有代数扩张 L/M，那么

$$|L| \leq \max\{|M|, |\mathbb{N}|\} \leq \max\{|F|, |\mathbb{N}|\} < |S|$$

因此存在单射 $f : L \to S$，并且 $f|_M = \mathrm{id}$，于是通过 f 将 L 的域结构诱导到 $f(L)$ 上，这就给出了扩域 $f(L)/M$，并且 $f(L)$ 是 M 的代数扩张。而 M 是 F 的代数扩张，从而 $f(L)$ 是 F 的代数扩张（定理 1.1.3）。

M 的极大性说明 $f(L) = M$，由于 $f|_M = \mathrm{id}$，因此 $L = M$。从而 M 满足要求。 □

于是分裂域的存在性立刻得证：在代数闭包中将根添加进 F。特别地：

推论 3.1.8. 全体 F 上非常值多项式生成的分裂域是 F 的代数闭包：因为 F 的代数闭包是极大的代数扩张，只能通过把所有根添加进去得到。

3.1.2 分裂域的唯一性、扩张同构定理

引理 3.1.9 (单根之间的转移). 给定域同构 $\sigma : F \to F'$，$f(x)$ 不可约，α 是 f 在某个扩张 K/F 的根，α' 是 $\sigma(f)$ 在某个扩张 K'/F' 中的根，那么存在同构 $\tau : F(\alpha) \to F'(\alpha')$，使得 $\tau(\alpha) = \alpha'$，$\tau|_F = \sigma$。

证明. 这是因为单扩张有着明确的结构 $F[x]/(f)$，直接考虑 $F[x]/(f) \to F'[x]/(f')$ 即可。 □

引理 3.1.10 (分裂域之间的转移). 给定域同构 $\sigma : F \to F'$，K/F 是 $\{f_i\}$ 在 F 上的分裂域。域同态 $\tau : K \to K'$ 满足 $\tau|_F = \sigma$。那么 $\tau(K)$ 是 $\{\tau(f_i')\}$ 在 F' 上的分裂域。

证明. 直接验证：$\tau(f_i')$ 的分裂性显然，生成是因为 $\tau(K)$ 当然由 K 在 F 上的生成元的像决定。 □

定理 3.1.11 (扩张同构定理). 给定域同构 $\sigma : F \to F'$，S 是一族 F 的多项式，$S' = \sigma(S)$。

K, K' 分别为 S, S' 在 F, F' 上的分裂域，那么存在域同构 $\tau : K \to K'$，使得 $\tau|_F = \sigma$。更进一步对于 $\alpha \in K$，以及任意一个 $\sigma(\min(F, \alpha))$ 在 K' 中的根，都可以选取 τ 满足 $\tau(\alpha) = \alpha'$。

证明. 取 $\mathcal{S}$ 为全体 (L, φ) 满足 L 是 K 的子域，$\varphi : L \to K'$ 是 σ 的延拓，偏序关系由域的包含和 φ 的限制相同给出。

$\mathcal{S}$ 是非空的，并且满足 Zorn 引理条件，选出极大元 (M, τ)。如果 $M \neq K$，那么存在 $f \in S$ 使得它不在 M 上分裂。选出这个 f 对应的不在 M 中的根 α，$p(x) = \min(F, a)$。再取 $p' = \sigma(p) \in F'[x]$，α' 为 f' 的某个根（这个根存在因为 p' 整除 f'，并且 f' 在 K' 上分裂）

由引理 3.1.9，存在 $\rho : M(\alpha) \to \tau(M)(\alpha')$ 是 τ 的延拓。那么这和 (M, τ) 的极大性矛盾。

因此 $M = K$，从而引理 3.1.10说明 $\tau(K) \subseteq K'$ 是 S' 的分裂域，于是 $\tau(K) = K'$。但是满域同态是同构，因此这就完成了证明，我们这样构造出的更大 τ 也的确是满足 $\tau(\alpha) = \alpha'$ 的。 □

推论 3.1.12. 给定域 F 上的一族多项式 S，其任何两个分裂域都是 $F-$ 同构的，特别地，代数闭包总是 $F-$ 同构的。

推论 3.1.13. 任何 F 的代数扩张 K 都 $F-$ 同构于某个代数闭包 N 的子域。

证明. 考虑 K 的代数闭包 M，由定理 1.1.3它也是 F 的代数扩张，从而 M 是 F 的代数闭包。考虑 $F-$ 同构 $f : M \to N$，那么 $K \to f(K)$ 即为所求。 □

3.1.3 正规扩张

定义 3.1.14 (正规扩张). 称 K/F 是正规的，如果 K 是 F 上某些多项式的分裂域。

命题 3.1.15 (正规扩张的几种看法). 给定代数扩张 K/F，以下等价：

1. K/F 是正规的
2. 如果 M 是 K 的代数闭包，$\tau : K \to M$ 是 $F-$ 同态，那么 $\tau(K) = K$
3. 如果 $F \subseteq L \subseteq K \subseteq N$，$\sigma : L \to N$ 是 $F-$ 同态，那么 $\sigma(L) \subseteq K$，并且存在 $\tau \in Gal(K/F)$ 使得 $\tau|_L = \sigma$
4. 对于任何不可约 $f(x) \in F[x]$，只要 f 在 K 中有根，f 就一定在 K 上分裂。

证明. $1 \implies 2$：由引理 3.1.10，$\tau(K) \subseteq M$ 也是分裂域。于是 $K, \tau(K)$ 是由相同的元素在 F 上生成的（全体多项式的根）。

$2 \implies 3$：假定 $F \subseteq L \subseteq K \subseteq N$，以及 $F-$ 同态 $\sigma : L \to N$。由于 $L \subseteq K$，于是 L/F 是代数扩张，从而 $\sigma(L) \subseteq N$ 在 F 上是代数的。

令 M' 是 F 在 N 中的代数闭包，M 是 M' 的代数闭包（于是由定理 1.1.3也是 K 的代数闭包）。现在由定理 3.1.11，存在 $\rho : M \to M$，使得 $\rho|_L = \sigma$。

再取 $\tau = \rho|_K$，那么由条件 2，$\tau(K) = K$。因此 $\sigma(L) = \tau(L) \subseteq \tau(K) = K$，并且 $\tau \in Gal(K/F)$。

$3 \implies 4$：假定 f 在 F 上不可约，$\alpha \in K$ 是根。取 $L = F(\alpha) \subseteq K$，$N$ 是 K 的代数闭包。对于任何 f 的根 $\beta \in N$，由引理 3.1.9存在 $F-$ 同态 $\sigma : L \to M : \alpha \to \beta$。由条件 3，$\sigma(L) \subseteq K$，因此 $\beta \in K$。从而 f 的根都在 K 中，即 f 在 K 上分裂。

$4 \implies 1$：K 是全体 $\{\min(F, a)|a \in K\}$ 的分裂域。 □

作为推论：

推论 3.1.16. *如果 K/F 是正规扩张，那么它是 $\{\min(F, a)|a \in K\}$ 的分裂域。*

下面给出正规扩张的一个性质：

命题 3.1.17 (Morandi 3.13: 正规扩张中多项式的各个不可约因子次数相同). *K/F 是正规扩张，f 是 $F[x]$ 中的不可约多项式，$g_1(x), g_2(x)$ 是 $K[x]$ 的任意两个首一不可约因子，那么存在 $\sigma \in Gal(K/F)$ 使得 $\sigma(g_1) = g_2$。*

于是自然它的各个不可约因子次数相同。

证明. 取 K 的代数闭包 M，假设 $\alpha_1, \alpha_2 \in M$ 分别从属于两个（K 中的）不可约因子 g_1, g_2，那么由扩张同构定理存在 $F-$ 自同构 $\sigma : M \to M$ 使得 $\sigma(\alpha_1) = \alpha_2$。

现在考虑 $\tau = \sigma|_K : K \to M$ 是 $F-$ 同态，那么 $\tau(K) = K$，于是 $\sigma(g_1) \in K[x]$，并且 $x - \alpha_2|\sigma(g_1)$，从而 $g_2|\sigma(g_1)$（因为 g_2 是 α_2 在 $K[x]$ 中的极小多项式）。

然而 g_1 在 $K[x]$ 中是不可约的，σ 是 K 的自同构，于是 $\sigma(g_1)$ 也在 $K[x]$ 中不可约，因此 $\sigma(g_1) = g_2$。 □

3.2 例子

例子 (Morandi 3.8). *计算 $x^6 + 1$ 在 $\mathbb{Q}$ 和 $\mathbb{F}_2$ 上的分裂域的次数。*

证明. $\mathbb{Q}$：$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$。其在 $\mathbb{C}$ 中的所有根是 $\pm i$ 和 $\pm\sqrt{\frac{1 \pm \sqrt{3}i}{2}}$。

计算知 $L = \mathbb{Q}(\sqrt{\frac{1 + \sqrt{3}i}{2}})$ 包含了所有的根：因此这是分裂域。生成元 $\sqrt{\frac{1 + \sqrt{3}i}{2}}$ 的极小多项式是 $x^4 - x^2 + 1$，因此次数为 4.

$\mathbb{F}_2$：$x^6 + 1 = (x + 1)^2(x^2 + x + 1)^2$，于是其分裂域是 $\mathbb{F}_2$ 的唯一的二次扩域。 □

例子 (Morandi 3.9). *计算 $x^4 - 7$ 在 $\mathbb{Q}$，$\mathbb{F}_5$ 和 $\mathbb{F}_{11}$ 上的分裂域。*

证明. $\mathbb{Q}$：明显 $\mathbb{Q}(\sqrt[4]{7}, i)$ 即为所求。

$\mathbb{F}_5$：考虑 $\mathbb{F}_5[t]/(t^4 - 7)$，由于 $x^4 - 7$ 不可约因此它生成了极大理想，从而上述的确是域。

在这个域中 $x^4 - 7 = (x - t)(x - 2t)(x - 3t)(x - 4t)$：因为 $(kt)^4 - 7 = k^4t^4 - 7 \equiv t^4 - 7 \mod 5$，从而的确是分裂域。

$\mathbb{F}_{11}$：$x^4 - 7 = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$，考虑 $\mathbb{F}_{11}[t]/(t^2 + 1)$，那么在这个域中 $x^4 - 7 = (x - t - 1)(x - t + 1)(x + t - 1)(x + t + 1)$，从而的确是分裂域。 □

例子 (Morandi 3.17: 对称多项式是初等对称多项式的多项式). *$K = k(x_1, \cdots, x_n)$，S_n 作用在 K 上。给定对称多项式 $f \in k[x_1, \cdots, x_n]$（即 $\sigma(f) = f, \forall \sigma \in S_n$），证明 $f \in k[s_1, \cdots, s_n]$。*

证明. 取不动域 $F=\mathcal{F}(S_n)$，考虑扩环 $k[s_1,\cdots,s_n]\subseteq F\cap k[x_1,\cdots,x_n]$。

这是整扩张，因为每个 x_i 都在 $k[s_1,\cdots,s_n]$ 上整：$(t-x_1)\cdots(t-x_n)=t^n-s_1t^{n-1}+\cdots+(-1)^ns_n$，从而 x_i 是右侧这个多项式的根。

我们来说明诸 s_i 在 k 上是代数独立的：假定 $g(s_1,\cdots,s_n)=0$，但 g 不是零多项式。对单项式（或更准确地说：全体 $n-$ 数组）定义 $S-$ 序：$x_1^{a_1}\cdots x_n^{a_n}>_S x_1^{b_1}\cdots x_n^{b_n}\iff a_j+\cdots+a_n>b_j+\cdots+b_n$，其中 j 是最小使得 $a_j+\cdots+a_n\neq b_j+\cdots b_n$ 的 j。

假定 $g(t_1,\cdots,t_n)$ 中 $t_1^{a_1-a_2}t_2^{a_2-a_3}\cdots t_n^{a_n}$ 是在 $S-$ 序下的第一项，那么直接验证知 $x_1^{a_1}\cdots x_n^{a_n}$ 是将 $g(e_1,\cdots,e_n)$ 展开为 x_i 的多项式后按字典序排序的第一项，于是我们证明了 g 在 $S-$ 序的首项是 0，以此类推我们说明了所有项都必须是 0，从而就说明了 g 是零多项式。

因此 $k[s_1,\cdots,s_n]\cong k[t_1,\cdots,t_n]$：然而域上多项式环是 UFD，从而是整闭的，因此 $F\cap k[x_1,\cdots,x_n]=k[s_1,\cdots,s_n]$，从而完成了证明。

□

3.3 习题

练习 3.1 (Morandi 3.1: 有限个多项式分裂域等价于单个多项式分裂域). *K 是 $\{f_1,\cdots,f_n\}$ 在 F 上的分裂域 $\iff$ 它是 $f_1\cdots f_n$ 在 F 上的分裂域：这是由定义直接验证的。*

练习 3.2 (Morandi 3.2,3: 分裂域是最小使得 S 分裂的域). *K 是多项式族 $S\subseteq F[x]$ 在 F 上的分裂域。如果 L 是 K/F 的中间域，并且每个 $f\in S$ 都分裂，那么 $L=K$。*

更进一步对于任何中间域 L，K 都是 S 在 L 上的分裂域。这是由定义直接验证的。

练习 3.3 (Morandi 3.5: 正规扩张不具有合成性). *$F\subseteq L\subseteq K$，K/L 和 L/F 都正规，但是 K/F 可以不正规。*

证明. 再一次考虑 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$：$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是正规的：因为它是 x^2-2 在 $\mathbb{Q}$ 上的分裂域；同理 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ 是 $x^2-\sqrt{2}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的分裂域。

但是 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规的，因为不可约多项式 x^4-2 在 $\mathbb{Q}(\sqrt[4]{2})$ 中有根，但是不分裂。 □

练习 3.4 (Morandi 3.6,7). *K/F 满足 $[K:F]=m$，以及 F 上的不可约多项式 f 满足 $\deg f=n$，并且 $\gcd(m,n)=1$。那么 f 在 K 上也不可约。*

例子：$x^5-9x^3+15x+6$ 在 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上不可约。

证明. 假设 K 的某个扩域 N 包含 f 的一个根 α，那么考虑

$$[K(\alpha):F]=[K(\alpha):K]\cdot[K:F]=[K(\alpha):F(\alpha)]\cdot[F(\alpha):F]$$

故 $mn|[K(\alpha):F]$。

另一方面

$$[K(\alpha):F]=[K(\alpha):K]\cdot[K:F]\leq[F(\alpha):F]\cdot[K:F]=mn$$

于是 $[K(\alpha):K]=n$，即 α 在 K 上的极小多项式也是 n 次的，从而还是 f。故 f 在 K 上也不可约。 □

练习 3.5 (Morandi 3.10,11). f 是素数次的 F 上多项式，如果对每个扩张 K/F，f 在 K 中有根 $\Longrightarrow$ f 在 K 上分裂，那么要么 f 在 F 上不可约，要么 f 在 F 中有根（于是由条件分裂）。

作为特例：

1. $f(x)=x^p-a$，$char(F)=p, a\in F$
2. $f(x)=x^p-x-a$，$char(F)=p, a\in F$
3. $f(x)=x^p-a$，$char(F)\neq p$，F 包含 ω 使得 $\omega^p=1, \omega\neq 1$。

都满足前述条件。

证明. 假设 f 在 F 中没有根，那么考虑 f 在 F 上的分裂域 $K=F(a_1,\cdots,a_p)$，这里 a_i 是 f 的根。

那么由条件 $F(a_i)=F(a_1,\cdots,a_p)$，于是 f 在 F 上的每个不可约因子次数都相同：它们都是 $[F(a_i):F]=[F(a_1,\cdots,a_p):F]$。但是 $\deg f=p$，于是这些不可约因子要么全为 1（于是分裂），要么是 p（于是不可约）。

我们来验证三种情况

1. 如果 x^p-a 在 K 中有根 r，那么 $x^p-a=(x-r)^p$ 从而分裂。
2. 如果 x^p-x-a 在 K 中有根 r，那么 $r, r+1,\cdots,r+p-1$ 都是根从而分裂。
3. 如果 x^p-a 在 K 中有根，那么 $r,\omega r,\cdots,\omega^{p-1}r$ 都是根从而分裂。

□

练习 3.6 (Morandi 3.12). K 是域，$\sigma\in Aut(K)$ 并且阶无限，F 是 σ 的固定域。如果 K/F 是代数的，那么它是正规扩张。

证明. 对于任何 F 上的不可约多项式 f，如果它在 K 中有根 α，考虑 $\sigma^i(\alpha)$：它们都是 f 的根。

由于 $\alpha\notin F$，假定直到 $n-1$ 我们都得到互异的根（即最小的 n 非零使得 $\sigma^n(\alpha)=\alpha$）：$\{\alpha,\sigma(\alpha),\cdots,\sigma^{n-1}(\alpha)\}$。那么考虑 $(x-\alpha)\cdots(x-\sigma^{n-1}(\alpha))$，注意到 $p(x)$ 在 σ 作用下不动，于是 $p\in F[x]$。

因此在 $F[x]$ 中 $p|f$（这是因为考虑带余除法 $f=pq+r$，那么 r 作为 $K[x]$ 有超过自身次数个数的根，于是 $r=0$），从而 f 的不可约性要求 $p=f$，于是 f 分裂。 □

练习 3.7 (Morandi 3.15: 合成域保持正规). 如果 $K/F, L/F$ 正规，那么 KL/F 也正规。反过来不正确。

证明. 取 KL 的代数闭包，那么它也是 K, L, F 的代数闭包。对于任何 $F-$ 同态 $\tau: KL\to M$，$\tau(KL)=\tau(K)\tau(L)$。

但是 $\tau|_K, \tau|_L$ 仍然都是到代数闭包的 $F-$ 同态，于是由正规扩张知 $\tau(K)=K, \tau(L)=L$，从而 $\tau(KL)=KL$，故 KL/F 正规、

反过来不正确：$F=\mathbb{Q}, K=\mathbb{Q}(\sqrt[3]{2}), L=\mathbb{Q}(i)$ 即为例子。 □

第四章　可分扩张

4.1　结论

4.1.1　可分多项式和可分扩张、Galois 扩张的判别

定义 4.1.1 (可分多项式). 称 F 上的不可约多项式在 F 上是可分的，如果它在分裂域中不含重根。对于一般的 F 上多项式，称它是可分的如果它的所有不可约因子都是可分的。

利用形式导数，有非常简单的可分性判别：

命题 4.1.2 (可分性判别). *$f \in F[x]$ 是非常数多项式，那么 f 在分裂域中没有重根 $\iff$ 在 $F[x]$ 中 $\gcd(f, f') = 1$，这里 f' 是形式导数。*

证明. 首先互素在扩域 K/F 下是保持的：假设在 $F[x]$ 中 $\gcd(f, g) = 1$，那么存在 F 中多项式使得 $fm + gn = 1$，从而在 $K[x]$ 中也是如此，于是在 $K[x]$ 中 (f, g) 生成了 $K[x]$，从而互素；反过来如果在 $K[x]$ 中 $\gcd(f, g) = 1$，那么其在 $F[x]$ 中的 gcd 整除在 K 中的 $\gcd(= 1)$，因此在 $F[x]$ 中互素。

现在我们知道了互素在扩域下是保持的，因此直接在 F 的代数闭包计算即可直接得到结果。 □

我们使用上述结果：

命题 4.1.3 (不可约多项式的可分性). *给定不可约多项式 $f(x) \in F[x]$：*

1. *$char(F) = 0$，则 f 可分；$char(F) = p > 0$，则 f 可分 $\iff$ $f'(x) \neq 0$，这当且仅当 $f \notin F[x^p]$*
2. *$char(F) = p > 0$，则存在 $m \geq 0$，使得 $f(x) = g(x^{p^m})$，并且 $g(x) \in F[x]$ 是不可约且可分的。*

证明. 第一段是显然的；对于第二段选取 m 为最大的使得 $f(x) \in F[x^{p^m}]$ 的 m。那么 $g(x) \notin F[x^p]$（否则可以选 $m+1$），因此 g 可分。g 显然不可约：因为它的分解直接诱导了不可约多项式 f 的分解。 □

定义 4.1.4 (可分扩张). 给定域扩张 K/F，$\alpha \in K$ 称为可分元如果 $\min(F, \alpha)$ 在 F 上可分。如果每个 $\alpha \in K$ 都是可分的，称 K/F 是可分扩张。

定理 4.1.5 (Galois 扩张的刻画). *K/F 是代数扩张，下列等价：*

1. K/F 是 Galois 的

2. K/F 是正规且可分的

3. K 是 F 上一族可分多项式的分裂域

证明. 1 $\Longrightarrow$ 2. 假定 K/F 是 Galois 的，$\alpha \in K$。取 $\alpha_1, \cdots, \alpha_n$ 为全体互异的 $\sigma(\alpha), \sigma \in Gal(K/F)$。这是有限集，因为它们都是 $\min(F, \alpha)$ 的根。

取 $f(x) = \prod(x - \alpha_i)$。于是对于任何 $Gal(K/F)$ 的元素 τ，$\tau(f) = f$（因为它诱导了 $\{\alpha_i\}$ 到自身的单射，从而是双射），于是 $f \in F[x]$。从而 $\min(F, \alpha)|f$，因此 $\min(F, \alpha)$ 在 K 上分裂，并且无重根。于是 K 是全体 K 中元素极小多项式的分裂域，并且都可分，因此 K/F 正规可分。

2 $\Longrightarrow$ 3. 如果 K/F 正规可分，由推论 3.1.16，K 是 $\{\min(F, a)|a \in K\}$ 的分裂域：由定义这些多项式都是可分的。

3 $\Longrightarrow$ 1. 首先证明 $[K : F] < +\infty$ 的情况：对 $n = [K : F]$ 归纳。$n = 1$ 时平凡，假定结果对扩张次数小于 n 的所有扩域都成立，K 是可分多项式 $\{f_i\}$ 的分裂域。

由于 $n > 1$，存在 f_i 的根 α 不在 F 中，取 $L = F(\alpha)$，那么 $[L : F] > 1$，$[K : L] < n$。由于 K 也是 $\{f_i\}$ 在 L 上的分裂域，并且 $\{f_i\}$ 在 L 上也可分（回忆互素和扩域无关），那么归纳假设说明了 K/L 是 Galois 的。

考虑 $H = Gal(K/L)$，它是 $Gal(K/F)$ 的子群。$\alpha_1, \cdots, \alpha_r$ 是 $\min(F, \alpha)$ 在分裂域里的根。由于 f_i 可分，那么 $\min(F, \alpha)$ 也可分。因此 $[L : F] = r$。由同构扩张定理，存在 $\tau_i \in Gal(K/F)$ 使得 $\tau_i(\alpha) = \alpha_i$。陪集 $\tau_i H$ 两两不交：因为 $\tau_i^{-1}\tau_j$ 如果是 H 中的元素，那它保持 $\alpha \in L$：但是这相当于要求 $\alpha_i = \alpha_j$，这不可能发生。

于是

$$|Gal(K/F)| \geq r \cdot |H| = [L : F] \cdot [K : L] = [K : F]$$

（倒数第二个等号是因为归纳假设以及 Galois 扩张时不等式取等）

再结合 $|G| \leq [K : F]$，就得到了 $|G| = [K : F]$，从而 K/F 是 Galois 的。

现在考虑一般的 K/F：K 是一族可分多项式 S 的分裂域，X 为这些多项式的全体根，那么 $K = F(X)$。对于 $a \in \mathcal{F}(Gal(K/F))$，我们需要说明 $a \in F$。存在 X 的有限子集 $\{\alpha_1, \cdots, \alpha_n\} \subseteq X$，使得 $a \in F(\alpha_1, \cdots, \alpha_n)$。取 $L \subseteq K$ 为 $\{\min(F, \alpha_i)\}$ 的分裂域，自然这些 $\min(F, \alpha_i)$ 都是可分的。那么由前文对有限扩张的讨论知 L/F 是有限 Galois 扩张。

由命题 3.1.15，任何一个 $F-$ 自同构 $L \to L$（从而天然是 $F-$ 同态 $L \to K$）都是由 $Gal(K/F)$ 的某个元素限制得到的。反过来，将 $Gal(K/F)$ 的元素视作 K 到代数闭包 M 的 $F-$ 同态，那么它限制到 L 上就是 $F-$ 同态 $L \to M$：由命题 3.1.15，这个同态的像是 L（因为 L/F 也是正规扩张）。

因此：

$$Gal(L/F) = \{\sigma|_L|\sigma \in Gal(K/F)\}$$

从而 $a \in \mathcal{F}(Gal(L/F))$（因为 a 在 $Gal(K/F)$ 的不动域里，而 $Gal(L/F)$ 的元素全都是由前者限制得到），但 L/F 是 Galois 的，于是 $a \in F$，从而 $\mathcal{F}(Gal(K/F)) = F$，即 K/F 是 Galois 的。 □

推论 4.1.6. *L/F 是有限扩张：*

1. *L/F 是可分的 $\iff$ L 包含在 F 的某个 Galois 扩张里。*
2. *$L = F(\alpha_1, \cdots, \alpha_n)$，$L/F$ 是可分的 $\iff$ 每个 α_i 是可分元。*

证明.

1. 如果 $L \subseteq K$，K/F 是 Galois 的，那么 K/F 可分，从而 L/F 可分。反过来如果 L/F 可分，设 $L = F(\alpha_1, \cdots, \alpha_n)$，取 K 为 $\{\min(F, \alpha_i)\}$ 的分裂域：这是一族可分多项式的分裂域，从而 K/F 是 Galois 的。
2. 取 K 为 $\{\min(F, \alpha_i)\}$ 的分裂域，那么 K/F 是 Galois 的，由前一命题得证。

□

4.1.2 完美域、纯不可分扩张

定义 4.1.7 (完美域). *F 是完美域，如果 F 的代数扩张都可分。*

定理 4.1.8 (完美域的刻画). *特征 p 域 F 是完美域 $\iff$ $F^p = F$。*

作为推论：有限域都是完美的：因为 $\varphi(a) = a^p$ 是一个域同态，从而是单的，从而是满的。

证明. 如果 F 完美，考虑单扩张 $K = F(\alpha)$，α 是 $x^p - a$ 的根，那么 $x^p - a = (x - \alpha)^p$。然而 K/F 是可分的，于是只能有 $\alpha \in F$，从而 $a \in F^p$。

如果 $F^p = F$，K/F 是代数扩张。取 $\alpha \in K, p = \min(F, \alpha)$，那么存在 m 使得 $p(x) = g(x^{p^m})$，g 是不可约且可分的。如果 $g = x^r + \cdots + a_1 x + a_0$，存在 $b_i^p = a_i, b_i \in F$，于是 $p(x) = (\sum_i b_i x^{p^{m-1} i})^p$。但是 p 不可约，于是 $m = 1$。从而 $p = g$ 是可分的，因此 α 可分，K/F 可分。 □

定义 4.1.9 (纯不可分). 给定代数扩张 K/F，称 $\alpha \in K$ 是纯不可分的，如果 $\min(F, \alpha)$ 在其分裂域中有且仅有一个根（不计重数），称扩域 K/F 是纯不可分的，如果 K 的元素都是纯不可分的。

对于特征 p 域 F，$\alpha \in K$ 是纯不可分的 $\iff$ $\exists n, \alpha^{p^n} \in F$：此时 $\min(F, \alpha) = (x - \alpha)^{p^n}$。

证明. 假如 $\alpha^{p^n} \in F$，结论自明。反过来考虑 $f(x) = \min(F, \alpha)$，那么存在可分不可约多项式 $g(x^{p^m}) = f(x)$：于是在分裂域中 $g(x) = (x - b_1) \cdots (x - b_r)$，从而 $f(x) = (x^{p^m} - b_1) \cdots (x^{p^m} - b_r)$。如果 $r > 1$：由 g 的可分性诸 b_i 应当不同；但是由纯不可分性这是不可能的。于是只能有 $f(x) = x^{p^m} - b_1$，那么这就说明了结果。 □

引理 4.1.10 (纯不可分性质). *K/F 是代数扩张*

1. *$\alpha \in K$ 同时是可分和纯不可分元，那么 $\alpha \in F$*
2. *如果 K/F 是纯不可分扩张，那么 K/F 是正规的并且 $Gal(K/F) = \{\mathrm{id}\}$。特别地如果 $[K : F] < +\infty$，$p = char(F)$，那么 $[K : F] = p^n$*

3. $K=F(X)$，每个 X 都是纯不可分的，那么 K 也是纯不可分的。

4. $F\subseteq L\subseteq K$：K/F 是纯不可分的 $\iff$ $K/L, L/F$ 都是纯不可分的。

证明. 1. 显然：因为 $\min(\alpha,F)$ 无重根并且只有一个根，于是只能是 $x-\alpha$

2. 正规性显然：因为每个 $\min(F,\alpha)$ 都在 K 上分裂。同样每个自同构也只能将 α 映到 α，于是 Galois 群平凡。如果 $[K:F]<+\infty$，设 $K=F(\alpha_1,\cdots,\alpha_n)$：注意到 $K/L/F$ 中如果 K/F 纯不可分，那么 $K/L, L/F$ 都是：因此我们只需对单扩张证明，这个情况是显然的。

3. 对于任何 K 中元素 a，存在有限的 $\alpha_i\in X$ 使得 $a\in F(\alpha_1,\cdots,\alpha_n)$。它是 α_i 的多项式之商：因此充分大的 m 一定能使得 $a^{p^m}\in F$，从而也是纯不可分的。

4. 显然。

□

定义 4.1.11 (可分闭包和纯不可分闭包). 给定域扩张 K/F：定义全体可分元构成的集合为可分闭包；全体纯不可分元构成的集合为纯不可分闭包。

注记. 它们都是域：因为推论 4.1.6说明 a,b 可分 $\implies$ $F(a,b)$ 可分，从而可分闭包是域。而上一命题的证明过程说明了纯不可分闭包是域。

命题 4.1.12 (代数扩张 = 先可分扩张再纯不可分扩张). 给定域扩张 K/F，S,I 分别是可分和纯不可分闭包，自然它们都是 F 的扩域：S/F 可分，I/F 纯不可分，$S\cap I=F$。如果 K/F 是代数扩张，那么 K/S 纯不可分。

证明. 如果 $\alpha\in K$，那么 $\min(F,\alpha)=g(x^{p^n})$，$g$ 可分，不可约。于是 $a=\alpha^{p^n}$ 是可分的，从而说明 K/S 是纯不可分的。 □

推论 4.1.13 (可分具有合成性). $F\subseteq L\subseteq K$，$L/F, K/L$ 都可分，那么 K/F 也可分。

证明. 取 F 在 K 中的可分闭包，那么 $L\subseteq S$。由于 K/L 可分，K/S 也可分。但是 K/S 还是纯不可分的，于是 $K=S$，从而得证。 □

一般情况下，我们不能将代数扩张拆成先纯不可分扩张再可分扩张，但是在正规的情况下这是可以做到的。

定理 4.1.14. K/F 正规，S,I 同上。那么 S/F 是 $Galois$ 的，$I=\mathcal{F}(Gal(K/F))$，并且 $Gal(S/F)\cong Gal(K/I)$。因此 K/I 是 $Galois$ 的，进一步 $K=SI$。

证明. $a\in S$，$f=\min(F,a)$：那么它在 K 上分裂。由于 a 在 F 上可分，它没有重根。于是 f 的所有根都是可分的，从而都在 S 中。因此 S/F 正规，从而 Galois。

定义同态 $\theta: Gal(K/F)\to Gal(S/F):\sigma\mapsto\sigma|_S$：因为命题 3.1.15的第二点：（$S/F$ 是正规的，于是 $\sigma|_S$ 作为 $S\to K(\hookrightarrow\bar{K})$ 满足 $\sigma(S)=S$）θ 的核是 $Gal(K/S)$：这是纯不可分扩张，于是核是平凡的。θ 是满的：因为命题 3.1.15的第三点。因此 θ 是同构。

下面说明 $I=\mathcal{F}(Gal(K/F))$：如果 $a\in I$，$a^{p^n}\in F$：那么 $a^{p^n}=\sigma(a)^{p^n}$：而 $x^{p^n}-y^{p^n}=(x-y)^{p^n}$，因此 $a=\sigma(a)$。反过来如果 $b\in\mathcal{F}(Gal(K/F))$：由于 K/S 是纯不可分的，存在 n

使得 $b^{p^n} \in S$。选定 $\tau \in Gal(S/F)$，存在 $\sigma \in Gal(K/F)$ 使得 $\tau = \sigma|_S$（θ 是同构），那么 $\tau(b^{p^n}) = \sigma(b^{p^n})$，而这件事对每个 τ 都成立，于是 $b^{p^n} \in \mathcal{F}(Gal(S/F)) = F$。于是 b 在 F 上纯不可分，从而 $I = \mathcal{F}(Gal(K/F))$。

因此 $Gal(K/F) = Gal(K/I)$。作为推论：K/I 是 Galois 的，于是可分。K 在 SI 上可分：因为 $I \subseteq SI$；K 在 SI 上纯不可分，因为 $S \subseteq SI$，从而 $K = SI$。 □

定义 4.1.15 (可分次数和不可分次数). 有限扩张 $[K : F]$ 的可分次数 $[K : F]_s := [S : F]$；不可分次数 $[K : F]_i := [K : S]$。

注记. 不可分次数的如此定义是因为我们发现即使 K/F 不可分，仍然有可能 $I = F$：这说明 $[I : F]$ 并不是一个好的衡量不可分程度的值——归根结底这源于一般的代数扩张只能拆成先可分扩张再纯不可分扩张。

命题 4.1.16 (乘法公式). 可分次数和不可分次数也满足乘法公式：即如果 $F \subseteq L \subseteq K$，那么 $[K : F]_s = [K : L]_s[L : F]_s; [K : F]_i = [K : L]_i[L : F]_i$

证明. 引理 8.1.6 □

定义 4.1.17 (纯不可分扩张的 $p-$ 维数). F 是特征 p 域，K 是 F 的有限扩张。假定 $K^p \subseteq F$，那么这是一个纯不可分扩张。

称 $\{a_1, \cdots, a_n\} \subseteq K$ 是 $p-$ 基，如果如下是真扩张链：$F \subset F(a_1) \subset F(a_1, a_2) \subset \cdots \subset F(a_1, \cdots, a_n) = K$

证明：对于 $K^p \subseteq F$ 的扩张 K/F，如果 $\{a_1, \cdots, a_n\}$ 是 $p-$ 基，那么 $[K : F] = p^n$。

进一步证明：对于任何纯不可分扩张 K/F，都存在一族前述形式的升链使得相邻两个域扩张次数为 p：这样的 $\{a_i\}$ 称为纯不可分扩张的 $p-$ 基。

证明. 通过归纳，只需证明 $[F(a_1, \cdots, a_{i+1}) : F(a_1, \cdots, a_i)] = p$。由于这是真扩张，于是次数 > 1。

$a_{i+1}^p \in F \subseteq F(a_1, \cdots, a_i)$，于是 $\min(F(a_1, \cdots, a_i), a_{i+1}) = (x - a_{i+1})^p$（回忆对纯不可分元的刻画定义 4.1.9）。

因此 $[F(a_1, \cdots, a_{i+1}) : F(a_1, \cdots, a_i)] = p$。

下面来看一般的情况：对于 $\alpha_1 \in K - F$，存在极小的 n_1 使得 $\alpha_1^{p^{n_1}} \in F$，取 $a_1 = \alpha_1^{p^{n_1-1}}$。那么 $F \subset F(a_1)$，并且扩张次数为 p。假设我们直到 a_i 都已经选定，再一次选取 $\alpha_{i+1} \in K - F(a_1, \cdots, a_i)$，那么存在极小的 n_{i+1} 使得 $\alpha_{i+1}^{p^{n_{i+1}}} \in F(a_1, \cdots, a_i)$，那么取 $a_{i+1} = \alpha_{i+1}^{p^{n_{i+1}-1}}$ 即可。这样的操作一定会恰好终止到 K 上：因为纯不可分扩张 K/F 的扩张次数一定是 p 的幂。 □

4.2 例子

例子. 对于 $a \in F - F^p$，$x^p - a$ 在 F 上不可约，但是在 F 上不可分。

证明. 练习 3.5直接说明了结果；不可分是因为 α 是根 $\implies x^p - a = (x - \alpha)^p$。 □

例子. K/F 是有限扩张，$char(F)$ 不整除 $[K : F]$，那么 K/F 可分：（首先只用考虑正特征情况）观察纯不可分扩张的阶数一定是 p^n，将 K/F 拆分为 $K/S/F$ 即可得证。

例子 (Morandi 4.11). K 是特征 p 完美域 k 上的有理函数域 $k(x)$, $F=k(u), u=f(x)/g(x), f,g$ 互素。那么 K/F 可分 $\iff u\notin K^p$。

证明. 注意 $K=F(x)$, $\min(F,x)=ug(x)-f(x)$。因此 K/F 不可分 $\iff ug(x)-f(x)\in F[x^p]$。

这等价于 $f,g\in k[x^p]$。现在由于 k 是完美域，$k^p=k$，因此这进一步等价于 $f,g\in (k[x])^p$，于是这等价于 $u\in (k(x))^p=K^p$。 □

例子 (Morandi 4.13: 既不正规也不可分的扩张). $\mathbb{F}_2(x^{1/6})/\mathbb{F}_2(x)$ 不正规：因为 $\sqrt[3]{(}x)$ 的极小多项式是 t^3+x；但是它不分裂。

$\sqrt{x}$ 是纯不可分的：因为 $\sqrt{x}^2=x\in\mathbb{F}_2(x)$。

例子 (Morandi 4.14). k 是特征 p 域，$K=k(x,y), F=k(x^p,y^p)$。那么 K/F 是 p^2 阶的纯不可分扩张，并且不是单扩张。

证明. 注意任何 $k[x,y]$ 中的元素 f 都满足 $f^p\in k[x^p,y^p]$（交叉项系数由于形如组合数一定是 p 的倍数）。因此 $k(x,y)^p\subseteq F$，从而是纯不可分扩张。

由定义 4.1.17，$\{x,y\}$ 构成了一组 $p-$ 基，因此这个扩张次数是 p^2。

如果 K/F 是单扩张，设 $K=F(a)$。但是 $a^p\in F$，于是 $[K:F]\le p$，矛盾。 □

4.3 习题

练习 4.1 (Morandi 4.4). $F\subseteq L\subseteq K$，K/L 正规，L/F 纯不可分，证明 K/F 正规。

证明. 对于 $\alpha\in K$，$\min(L,\alpha)$ 分裂。由于 $\min(L,\alpha)$ 的系数在一个充分大的 p^m 幂次后变为 F 的元素，那么存在 m 使得：$\min(L,\alpha)^{p^m}\in F[x]$。

于是 $\min(F,\alpha)|\min(L,\alpha)^{p^m}$：但是后者在 K 上分裂，于是前者也是。 □

练习 4.2 (更精细的纯不可分扩张描述). F 是特征 p 域，K/F 是纯不可分扩张，$[K:F]=p^n$。那么对每个 $a\in K, a^{p^n}\in F$。

证明. 由于 $[K:F]=p^n$，任何 a 的极小多项式次数不超过 p^n 次。现在 a 是纯不可分元，于是 $a^{p^m}\in F$（选取 m 为最小满足这一条件者）。$m\le n$ 则结论已证，如果 $m>n$，那么 $\min(F,a)|a^{p^m}-f, f\in F$。

如果 $f\notin F^{p^m}$，那么 $x^{p^m}-f$ 不可约（再次使用练习 3.5：$x^{p^m}-a$ 满足条件是因为只要有一个根 α，那么 $x^{p^m}-a=(x-\alpha)^{p^m}$ 从而分裂）此时 $\min(F,a)=x^{p^m}-f$，这和极小多项式次数不超 p^n 矛盾。

因此 $f\in F^{p^m}$，即 $a^{p^m}\in F^{p^m}$。这说明 $a\in F$（$a^{p^m}-e^{p^m}=(a-e)^{p^m}$），从而这和 m 的极小性矛盾。 □

练习 4.3 (Morandi 4.7,8,9: 合成域保持可分/纯不可分/Galois). 如果 $K/F, L/F$ 可分，那么 KL/F 也可分。反过来也正确。

同样地：$K/F, L/F$ 纯不可分，那么 KL/F 也纯不可分。反过来也正确。

$K/F, L/F$ $Galois$，那么 KL/F 也 $Galois$。反过来不正确。

证明. 可分闭包是域，因此 KL/F 的可分闭包包含 K, L，于是只能是 KL。反过来也是正确的：因为 K, L 中元素天然是 KL 中元素，从而在 F 上可分。

对于纯不可分的命题同样考虑纯不可分闭包即可。反过来是正确的：因为 K, L 中元素天然是 KL 中元素，从而在 F 上纯不可分。

对于 Galois 的命题：结合练习 3.7和本命题即可。反过来不正确的例子已经在练习 3.7中给出。 □

因此我们给出合成域性质的总结：

推论 4.3.1 (Morandi 4.10). *K, L 共同包含在某个域内，且均包含 F：*

1. *$K = F(X)$，$X \subseteq K$，那么 $KL = L(X)$。*
2. *$[KL : F] \leq [K : F] \cdot [L : F]$，特别地右侧两个因子互素时等号成立：命题 1.1.2*
3. *$K/F, L/F$ 是代数/正规/可分/纯不可分/Galois 扩张时 KL/F 也是代数/正规/可分/纯不可分/Galois 扩张：练习 1.4、练习 3.7和前一命题。*

第五章　Galois 基本定理

5.1　结论

5.1.1　Galois 对应

定理 5.1.1 (Galois 基本定理). *K/F 是有限 Galois 扩张，$G = Gal(K/F)$。那么 K/F 的中间域和 G 的子群有一一对应：由 $L \mapsto Gal(K/L)$ 和 $H \mapsto \mathcal{F}(H)$ 给出。*

如果 $L \leftrightarrow H$，那么 $[K : L] = |H|, [L : F] = [G : H]$。$H$ 是 G 的正规子群 $\iff$ L/F 是 Galois 的，此时 $Gal(L/F) \cong G/H$。

证明. 由偏序集之间的 Galois 对应，我们已经知道了有形如 $\mathcal{F}(H)$ 的中间域和形如 $Gal(K/L)$ 的子群之间的一一对应。

现在对于任何一个中间域 L：由于 K/F 是 Galois 的，那么是正规可分的。于是 K/L 是正规可分（因为在 L 上的极小多项式整除在 F 上的，于是后者分裂说明前者分裂；后者可分说明前者可分），从而 K/L 是 Galois 的，即 $L = \mathcal{F}(Gal(K/L))$。

对于任何一个子群 $H \leq G$，H 是有限的。由命题 2.1.9，这说明 $H = Gal(K/\mathcal{F}(H))$。注意：这里有限性是必要的，这也暗示了无限 Galois 理论与有限 Galois 理论的不同。

上述两个结果证明了一一对应。$[K : L] = |Gal(K/L) = |H|$，于是 $[L : F] = [K : F]/[K : L] = |G|/|H| = [G : H]$。

如果 H 是 G 的正规子群，$L = \mathcal{F}(H)$。对于 $a \in L, b$ 是 $\min(F, a)$ 在 K 中的任何根。由同构扩张定理：存在 $\sigma \in G, \sigma(a) = b$。对于 $\tau \in H$，$\tau(b) = \sigma\sigma^{-1}\tau\sigma(a)$，由于 $\sigma^{-1}\tau\sigma \in H$，这说明 $\tau(b) = \sigma(a) = b$，即 $b \in \mathcal{F}(H) = L$。因此 $\min(F, a)$ 在 L 上分裂，从而 L/F 是正规的。它被 Galois 扩张包含于是自动是可分的，因此 L/F 是 Galois 的。

反过来，如果 L/F 是 Galois 的。考虑 $\theta : G \to Gal(L/F) : \theta(\sigma) = \sigma|_L$。命题 3.1.15说明了这是良定的（$\sigma|_L$ 可以看做 $L \to \bar{K}$ 的 $F-$ 同态，那么 $\sigma|_L(L) = L$，于是确实限制成了自同构）。

$\ker\theta = Gal(K/L) = H$，因此 $H \trianglelefteq G$。θ 还是满射：因为任何 $\tau \in Gal(L/F)$，都存在 $\sigma|_L = \tau$（同构扩张定理，当然也可以用命题 3.1.15的第三点），因此 $Gal(L/F) \cong G/H$。 □

定理 5.1.2 (Natural Irrationality). *K/F 是有限 Galois 扩张，L/F 是任一域扩张。那么 KL/L 是 Galois 的并且 $Gal(KL/L) \cong Gal(K/K \cap L)$。作为推论：$[KL : L] = [K : K \cap L]$。*

证明. 假设 K 是多项式族 S 在 F 上的分裂域，那么 KL 就是这些多项式在 L 上的分裂域。F 上的多项式在 F 中可分，自然也在 L 中可分，因此 KL/L 是 Galois 的。

定义 $\theta : Gal(KL/L) \to Gal(K/F) : \theta(\sigma) = \sigma|_K$，再一次地这是良定的（命题 3.1.15）。$\ker\theta = \{\sigma \in Gal(KL/L) | \sigma|_K = \mathrm{id}\}$，这说明 $\ker\theta$ 的元素同时固定 K 和 L，于是固定 KL，从而只能是 id。

因此 θ 是单射。$\mathrm{Im}\,\theta$ 是 $Gal(K/F)$ 的子群，由 Galois 基本定理一定形如 $Gal(K/E), E$ 是某个中间域。

如果 $a \in K \cap L$，那么 a 被 $\sigma|_K$ 固定，因此 $a \in E$。反过来如果 $a \in E$，那么 $a \in K$，并且对于任何 $\sigma \in Gal(KL/L), \sigma(a) = a$，从而 $a \in L$。这就说明 $E = K \cap L$。

于是 $Gal(KL/L) = \mathrm{Im}\,\theta = Gal(K/K \cap L)$。 □

命题 5.1.3. *1. $K \subseteq N$ 都是 F 的 Galois 扩张，那么 $\varphi : Gal(N/F) \to Gal(K/F) : \sigma \mapsto \sigma|_K$ 是良定的满同态，并且核是 $Gal(N/K)$*

2. L, L 都是 F 的 Galois 扩张，那么前述映射诱导了单同态 $Gal(KL/F) \to Gal(K/F) \oplus Gal(L/F)$，这是满同态 $\iff K \cap L = F$。

证明. 1. 命题 3.1.15和同构扩张定理的直接应用。

2. 诱导同态是泛性质，如果两个 $Gal(KL/F)$ 的元素诱导了相同的 $Gal(K/F) \oplus Gal(L/F)$ 的元素，那么它们在 K, L 上相同，因此也在 KL 上相同，从而是同一个元素：这就说明了是单同态。

   如果 φ 是满射，那么对于 $\alpha \in K \cap L$，β 是 α 极小多项式在 F 上的根。由于 K, L 正规，$\beta \in K \cap L$。同构扩张保证存在 $\tau \in Gal(K/F)$ 将 $\alpha \mapsto \beta$。

   由满射，存在 $\sigma \in Gal(KL/F)$，使得 $\sigma|_K = \tau, \sigma|_L = \mathrm{id}$。于是 $\alpha = \beta$，从而 $\alpha \in F$：因为 K, L 在 F 上可分。

   反过来的证明在有限 Galois 扩张时利用 Natural Irrationality 的维数计算即可。对于一般的 Galois 扩张需要用到无限 Galois 理论。

   参见https://math.stackexchange.com/questions/507671

   □

5.1.2 Primitive Element Theorem

定理 5.1.4 (单扩张判定：Primitive Element Theorem)**.** *有限扩张 K/F 是单扩张当且仅当存在有限个中间域。*

证明. 这里先假定 $|F| = \infty$。（有限域的情况见推论 6.1.2）如果 K/F 中间域有限，假定 $K = F(\alpha_1, \cdots, \alpha_n)$，我们对 n 归纳。$n = 1$ 显然，假定 $K = F(\alpha_1, \cdots, \alpha_{n-1})$，由条件 L/F 之间的中间域也是有限的，因此 $L = F(\beta)$。

现在 $K = F(\alpha_n, \beta)$。对于每个 $a \in F$，取 $M_a = F(\alpha_n + a\beta)$：它是 K/F 的中间域。由于仅有有限个中间域，但是 $a \in F$ 有无限个，那么存在 $a \neq b$ 使得 $M_a = M_b$。

于是 $\beta = \dfrac{(\alpha_n + b\beta) - (\alpha_n + a\beta)}{b - a} \in M_a = M_b$。那么 $\alpha_n = (\alpha_n + b\beta) - b\beta \in M_b$。于是 $K = F(\alpha_n, \beta) = M_b$，从而 K/F 是单扩张。

反过来如果 $K = F(\alpha)$ 是单扩张，对于任何中间域 M，有 $K = M(\alpha)$。那么在 $M[x]$ 中 $\min(M,\alpha)|\min(F,\alpha)$。

假定 $\min(M,\alpha)$ 的系数分别为 $a_0, a_1, \cdots, a_{r-1}$，$M_0 = F(a_0, \cdots, a_{r-1}) \subseteq M$，那么 $q \in M_0[x]$。于是：

$$[K:M] = \deg \min(M,\alpha) \geq \deg(\min(M_0,\alpha)) = [K:M_0] = [K:M]\cdot[M:M_0]$$

于是只能 $[M:M_0]=1$，即 $M = M_0$。从而中间域只被 $\min(M,\alpha)$ 决定：而这作为 p 的首一因子当然个数有限。 □

注记 (Morandi 5.21). Primitive Element Theorem 有如下另外的证明（仍然是对无限域）

对于基域 F 无限的有限维线性空间 K/F，它不可能是有限个真子空间的并。因此如果 K/F 只有有限个真中间域，设为 $\{K_i\}$，那么存在 $a \in K - \cup_i K_i$。此时 $K = F(a)$，否则 $F(a)$ 是某个真中间域 K_i，但是这和 a 的选择矛盾。

推论 5.1.5. *K/F 是有限可分扩张，那么它是单扩张。*

证明. 假定 $K = F(\alpha_1, \cdots, \alpha_n)$，那么 N 为 $\{\min(F,\alpha_i)\}$ 的分裂域，则 N/F 是 Galois 的。

N/F 的确是有限扩张：因为多项式集是有限集。那么由 Galois 对应：N/F 的中间域对应着有限群 $Gal(N/F)$ 的子群：这当然是有限的。于是 K/F 只有有限个中间域，那么 K 是单扩张。 □

5.1.3 正规闭包

定义 5.1.6. *K/F 是代数扩张，它的正规闭包定义为 $\{\min(F,a)|a \in K\}$ 在 F 上的分裂域。*

命题 5.1.7 (正规闭包是最小的正规扩张). *K/F 是代数扩张，N 是它的正规闭包*

1. *N/F 是包含 K 的正规扩张，并且如果 $K \subseteq M \subseteq N, M$ 是 F 的正规扩张，那么 $M = N$。*
2. *$K = F(a_1, \cdots, a_n)$ 时 N 是 $\min(F,a_1), \cdots, \min(F,a_n)$ 在 F 上的分裂域。*
3. *K/F 是有限扩张，则 N/F 也是。*
4. *K/F 可分，则 N/F 是 Galois 的。*

证明.

1. 给定 $K \subseteq M \subseteq N$，如果 $a \in K$，那么 $a \in M$，$\min(F,a)$ 在 M 上分裂。于是全体 $\min(F,a), a \in K$ 的根都在 M 里，从而由定义只能 $M = N$，因为 $N = F(X)$（X 是全体 $\min(F,a), a \in K$ 的根）
2. 取 L 为 $\{\min(F,a_i)\}$ 生成的分裂域，那么这是正规扩张，并且在正规闭包内。于是它只能是正规闭包。
3. 由前一命题：N/F 是有限个多项式的分裂域，于是也是有限扩张。
4. N/F 是一族可分多项式的分裂域，于是是 Galois 扩张。

□

推论 5.1.8 (任何正规扩张都包含一个正规闭包). *K/F 是代数扩张，N 是正规闭包。N' 是任何包含 K 的正规扩张，那么存在 $F-$ 同态 $N \to N'$。于是如果 N' 不含任何在 F 上正规的包含 K 的真子域，那么 N 和 N' 是 $F-$ 同构的。*

证明. $\min(F,a)$ 在 N' 上分裂，于是由同构扩张定理存在 $\sigma : N \to N'$ 是 $\mathrm{id} : F \to F$ 的延拓。那么 $\sigma(N)$ 是 $\{\min(F,a)|a \in K\}$ 的分裂域（在 N' 中），于是这就说明了结果。 □

我们自然好奇域扩张的正规闭包和反映到 Galois 群里的正规闭包是否相同：事实上确实如此。

命题 5.1.9 (域扩张正规闭包对应 Galois 群的正规闭包). *K/F 是 Galois 的，$G = Gal(K/F)$，L 是中间域。$N \subseteq K$ 是 L/F 的正规闭包（我们可以认为 $N \subseteq K$ 正是由于前一个推论），如果 $H = Gal(K/L)$，那么 $Gal(K/N) = \cap \sigma H \sigma^{-1}$*

证明. 这是因为 N 是正规闭包 $\iff$ N 是极小的使得 N/F 正规的扩张 $\iff$ $Gal(K/N)$ 是最大的 H 中的正规子群 $\iff$ $Gal(K/N) = \cap \sigma H \sigma^{-1}$。 □

5.1.4 后续结果

定理 5.1.10 (代数基本定理). *$\mathbb{C}$ 是代数闭的。*

证明. 给定 $\mathbb{C}$ 的有限扩张 L，这是可分扩张。并且 $L/\mathbb{R}$ 也是有限扩张。取 N 为 $L/\mathbb{R}$ 的正规闭包 N。那么 $\mathbb{C} \subseteq N$：因为任何 $\mathbb{C}$ 中元素在 $\mathbb{R}$ 上的不可约多项式的另一根只能是其共轭，从而分裂。

设 $G = Gal(N/\mathbb{R})$，那么 $|G| = 2[N : \mathbb{C}]$。取 H 为 G 的 2-Sylow 子群，E 是 H 的固定域。那么 $[G : H] = [E : \mathbb{R}]$ 是奇数。

但是 $E/\mathbb{R}$ 是奇数次扩张，对于任何 $a \in E - \mathbb{R}$，$\mathbb{R}(a)/\mathbb{R}$（作为中间域）也是奇数，于是 $\deg(\min(\mathbb{R}, a))$ 是奇数，那么这个多项式一定在 $\mathbb{R}$ 上有根。于是由不可约性它只能是 1 次的，因此 $a \in \mathbb{R}$。从而 $E = \mathbb{R}$。

因此 $G = H$，它一定是一个 $2-$ 群，于是 $Gal(N/\mathbb{C})$ 作为 G 的指数为 2 的子群也是一个 2-群。取 P 为 $Gal(N/\mathbb{C})$ 的极大真子群，那么 $[Gal(N/\mathbb{C}) : P] = 2$。

现在 $N/\mathbb{R}$ 是 Galois 的，于是 $N/\mathbb{C}$ 也是。那么 P 对应着不动域 T，并且 $[T : \mathbb{C}] = 2$。这是不可能的：因为任何复数域中的 2 次多项式都有解。

于是只能有 $|G| = 1$，从而 $N = \mathbb{C}$，于是 $L = \mathbb{C}$。 □

定理 5.1.11 (正规基定理). *K/F 是有限 Galois 扩张，那么存在 $a \in K$ 使得 $\{\sigma(a)|\sigma \in Gal(K/F)\}$ 是 K 的一组 $F-$ 基。*

证明. 同样我们先只证明 F 是无限域的情况。K/F 是有限可分的，于是是单扩张，设 $K = F(a)$。取 $f = \min(F, a)$，$G = Gal(K/F) = \{\sigma_1, \cdots, \sigma_n\}.\sigma_1 = \mathrm{id}, \sigma_i(a) = a_i$。

定义

$$g_i(x) = \sigma_i(g_1(x)) = \frac{f(x)}{(x - a_i)f'(a_i)}$$

那么对于 $j \neq k, g_i(x)g_k(x) \equiv 0 \mod f(x)$。由于诸 a_i 不同，$\deg g_i = n - 1$，那么：

$$g_1(x) + \cdots + g_n(x) - 1 = 0$$

（每个 a_i 都是上式左侧的根，但左侧次数不超 $n-1$）

于是 $g_i^2(x)-g_i(x)\equiv g_i(x)(g_1(x)+\cdots+g_n(x)-1)=0 \mod f(x)$。

现在考虑行列式 $D(x)=\det(\sigma_j\sigma_k(g_1(x)))$，那么 $D(x)^2$ 是这个矩阵和其转置的乘积的行列式：经观察发现它的对角线是 $g_1^2(x)+\cdots+g_n^2(x)\equiv g_1(x)+\cdots+g_n(x)\equiv 1 \mod f(x)$，其余元素 $\equiv 0 \mod f(x)$，于是 $D^2(x)\equiv 1 \mod f(x)$，故 $D(x)\neq 0$。

由于 F 是无限的，存在 $\alpha\in F$ 使得 $D(\alpha)\neq 0$，那么取 $\theta=g_1(\alpha)$，从而 $\det(\sigma_j\sigma_k(\theta))\neq 0$。

如果有 $F-$ 线性组合 $x_1\sigma_1(\theta)+\cdots+x_n\sigma_n(\theta)=0$，那么作用上 σ_i 给出了一组线性方程组：

$$(\sigma_j\sigma_k(\theta))\mathbf{x}^T=0$$

这就说明了 $x=0$，于是 θ 就是满足要求的元。 □

定理 5.1.12 (可分次数是嵌入个数)**.** *有限扩张 K/F 的可分次数 $[K:F]_s$ 等于 K 到 F 的代数闭包的 $F-$ 同态个数。*

证明. 我们先考虑单扩张，如果 $K=F(a), f=\min(F,a), N$ 是 F 的代数闭包，$b\in N$ 是 f 的某个根。那么考虑 f 的分裂域 M，存在 $\sigma: M\to M: a\mapsto b$。限制到 K，然后嵌入到 N 中即得到一个 $F-$ 同态 $K\to N$，并且将 $a\mapsto b$。

现在对于任意的 K/F，取可分闭包 S/F：那么这是一个单扩张（有限可分）$S=F(b)$。由前述，我们总有 $F(b)\to N$，并将 b 映为另外的 $\min(F,b)$ 在 N 中的根：于是这有 $[S:F]=[K:F]_s$ 种可能。

现在对于任何 $a\in K-S$，一定有 $a^{p^n}\in S$：注意它纯不可分，于是极小多项式在 N 中的根也只有 a 自身。因此如果 $F(b)\to N$ 能够延拓到 $K\to N$，这样的延拓方式唯一。然而这样的延拓方式的确存在：因为对 $S\subseteq S\subseteq K\subseteq N$ 应用命题 3.1.15，注意到 K/S 是纯不可分扩张，从而是正规的：这就得到了结论。 □

5.2 例子

我们下面研究多项式分裂域的 Galois 群的计算。

练习 5.1 (Morandi 5.1: 可分不可约多项式分裂域的 Galois 群是传递的)**.** *S_n 的子群 G 称为传递的，如果对每个 $i,j\in\{1,\cdots,n\}$，存在 $\sigma\in G,\sigma(i)=j$。*

设 K 是 F 上可分不可约多项式 f 的分裂域，$\deg f=n$。那么 $|Gal(K/F)|$ 被 n 整除并且同构于 S_n 的传递子群。作为推论：$[K:F]|n!$。

证明. 首先 $Gal(K/F)$ 天然可以看做 S_n 的子群：观察其在分裂域中 f 的 n 个根上的作用。

由于 K/F 有中间域 $F(\alpha_1)$，这里 α_1 是 f 的一个根：$[F(\alpha_1):F]=n$，因此 $|Gal(K/F)|=[K:F]=[K:F(\alpha_1)]\cdot[F(\alpha_1):F]$ 是 n 的倍数。

由同构扩张定理，对于任何两根 α_i,α_j，都存在 $Gal(K/F)$ 中的元素将 α_i 映到 α_j。这就证明了传递子群。 □

推论 5.2.1. *S_n 的传递子群 G 的阶一定是 n 的倍数：考虑 G 在 $\{1,\cdots,n\}$ 上的作用。那么 $|G|=|Gx|\cdot|Stab(x)|=n|Stab(x)|$。*

1. S_3 的传递子群有 S_3 自身和 $<(123)>\cong \mathbb{Z}/3\mathbb{Z}$。它们是所有可能得 *3* 次可分不可约多项式的分裂域的 *Galois* 群。

2. S_4 的传递子群有 S_4 自身；*4-cycle* 生成的循环群 $\mathbb{Z}/4\mathbb{Z}$：$<(1234)>,<(1243)>,<(1324)>$；二面体群 D_4：$<(1234),(13)>,<(1243),(14)>,<(1324),(12)$；$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$：$<(12)(34),(13)(24)>$；交错群 A_4：$<(123),(12)(34)>$。

3. S_5 的传递子群有：

   (a) S_5：取 $f(t)=(t-x_1)\cdots(t-x_5)\in\mathbb{Q}(s_1,\cdots,s_5)[t]$（$s_i$ 是初等对称多项式）。f 的分裂域是 $K=\mathbb{Q}(x_1,\cdots,x_5)$，*Galois* 群是 S_5。

   (b) *5-cycle* 生成的子群 $\mathbb{Z}/5\mathbb{Z}$

   (c) *10* 阶子群 D_5（$\mathbb{Z}/10\mathbb{Z}$ 不可能出现：因为 S_5 没有 *10* 阶元）

   (d) *15* 阶子群不可能出现：因为他只能是循环群，但是 S_5 没有 *15* 阶元

   (e) *20* 阶子群：$\mathbb{F}_{20}=\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/5\mathbb{Z}$（它是全体 $\mathbb{F}_5$ 上的仿射变换群 $ax+b, a\in\mathbb{F}_5^\times, b\in\mathbb{F}_5$）。其它 *20* 阶群都包含 10 阶元，因此不可能出现。

   (f) *30* 阶子群：如有 $|G|=30$ 且 $G\leq A_5$，那么 $G\trianglelefteq A_5$，矛盾。因此 $|A_5\cap G|=|G||A_5|/|G\cdot A_5|=30\times 60/120=15$（$G\cdot A_5=S_5$），但是 S_5 不含 15 阶子群，从而不存在 *30* 阶子群。

   (g) *40* 阶子群：如有，一定只有 $G\cap A_5\cong\mathbb{F}_{20}$：但是它包含奇置换，从而不存在。

   (h) *60* 阶子群：交错群 A_5。

例子. 计算如下 F 中多项式 f 的分裂域 K 的 *Galois* 群：

1. $F=\mathbb{Q}, f(x)=x^4-7$
2. $F=\mathbb{F}_5, f(x)=x^4-7$
3. $F=\mathbb{Q}, f(x)=x^5-2$
4. $F=\mathbb{F}_2, f(x)=x^6+1$
5. $F=\mathbb{Q}, f(x)=x^8-1$

证明. 1. $K=\mathbb{Q}(\sqrt[4]{7},i)$，$Gal(K/F)$ 作用到分裂域的四个根上可以是对换（复共轭）；也可以是保持 i，然后将 $\sqrt[4]{7}\mapsto\sqrt[4]{7}i$，从而诱导了 4-cycle。注意 i 的像有两个选择，$\sqrt[4]{7}$ 的像则有 4 个，因此 Galois 群大小不超 8。但是前述两者已经生成了大小为 8 的二面体群 D_4，从而即为所求。

2. 由第三章例子，分裂域为单扩张 $\mathbb{F}_5(\alpha)$，$\alpha^4=7$。注意到 $\alpha\mapsto k\alpha$ 满足要求，于是 Galois 群为 $\mathbb{Z}/4\mathbb{Z}$

3. 分裂域为 $\mathbb{Q}(\sqrt[5]{2},\omega)$（$\omega$ 为 5 次单位根）。那么 $\sqrt[5]{2}$ 的像有 5 种，ω 的像也有 5 种：于是 Galois 群大小不超 25。它不是 $\mathbb{Z}/5\mathbb{Z}$，因为存在二阶元（复共轭）；它不是 D_5，因为存在四阶元（$\omega\mapsto\omega^2$）。于是只能是 $\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/5\mathbb{Z}$，即 $\mathbb{F}_5$ 上的仿射变换群）

4. 由第三章例子，分裂域为 $\mathbb{F}_2$ 的二次扩域，于是 Galois 群只能是 $\mathbb{Z}/2\mathbb{Z}$。

5. $f(x)=(x-1)(x+1)(x^2+1)(x^4+1)$。于是 Galois 群只能分别置换 $\pm i$ 和 $\{\omega,\omega^3,\omega^5,\omega^7\}$，分裂域是 $\mathbb{Q}(\omega)$：其中 ω 是八次（本原）单位根。经检验 $\omega\mapsto\omega^i(i=1,3,5,7)$ 都是 $Gal(K/F)$ 的元素，于是 $Gal(K/F)=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。

□

例子 (Morandi 5.12). *F 特征非 2，K/F 是 4 次的 Galois 扩张。如果 $Gal(K/F)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$，那么 $K=F(\sqrt{a},\sqrt{b})$。*

证明. 回忆 2 次扩张只能形如 $F(\sqrt{a})$，假设两个 $\mathbb{Z}/2\mathbb{Z}$ 的子群对应的中间域分别为 $F(\sqrt{a}),F(\sqrt{b})$。

那么如果 $\sqrt{b}\in F(\sqrt{a})$，那么容易验证 $F(\sqrt{b})=F(\sqrt{a})$：这和包含关系矛盾。于是 $[F(\sqrt{a},\sqrt{b}):F(\sqrt{a})]\geq 2$，于是只能是 $K=F(\sqrt{a},\sqrt{b})$。 □

例子 (Morandi 5.22). *$K=\mathbb{Q}(X),X=\{\sqrt{p},p\ primes\}$。那么 $K/\mathbb{Q}$ 是 Galois 的。如果 $\sigma\in Gal(K/\mathbb{Q})$，定义 $Y_\sigma=\{\sqrt{p}|\sigma(\sqrt{p})=-\sqrt{p}\}$。*

1. $Y_\sigma=Y_\tau\implies\sigma=\tau$
2. 对于任何 $Y\subseteq X$，存在 $\sigma\in Gal(K/\mathbb{Q})$ 使得 $Y_\sigma=Y$。
3. 作为推论说明 $|Gal(K/\mathbb{Q})=|2^X|$。但是 $[K:\mathbb{Q}]=|X|$，这就给出了无限情况下 $|Gal(K/\mathbb{Q})|>[K:\mathbb{Q}]$ 的例子。

证明. 唯一非平凡的部分是第二点。由于 $[\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n}):\mathbb{Q}]=2^n$，那么它的 Galois 群恰好对应着将每个 $\sqrt{p_i}$ 反号/不反号。

于是在每个 X 的有限子集 T 中，我们都有一个 Galois 群众的元素将 $T\cap Y$ 的元素反号，其余保持不动。因此对所有 T 取余极限即可。（这里隐隐展现出了无限 Galois 理论的一角） □

5.2.1 习题

练习 5.2 (Morandi 5.9:Galois 扩张中的共轭). *K/F 是有限 Galois 扩张，$n=[K:F],a\in K,r=[F(a):F],H=Gal(K/F(a))$。$\tau_1,\cdots,\tau_r$ 是 H 的左陪集代表元，那么 $\min(F,a)=\prod_{i=1}^r(x-\tau_i(a))$。作为推论：*

$$\prod_{\sigma\in Gal(K/F)}(x-\sigma(a))=\min(F,a)^{n/r}$$

证明. 首先对于任何 $\sigma\in Gal(K/F)$，作用到 $\prod_{i=1}^r(x-\tau_i(a))$ 都是不变的（因为不过是对 $\sigma_i(a)$ 进行了置换：注意 $\sigma_i(a)$ 和陪集代表元选取无关），于是 $\prod_{i=1}^r(x-\tau_i(a))$。

其次 $r=\deg\min(F,a)$，于是这就说明了 $\prod_{i=1}^r(x-\tau_i(a))=\min(F,a)$。 □

练习 5.3 (Morandi 5.10:Galois 扩张中平移的特征多项式). *K/F 是 Galois 的，有平移 $L_a:K\to K:b\mapsto ab$。那么 L_a 的特征多项式是 $\prod_{\sigma\in Gal(K/F)}(x-\tau_i(a))$，极小多项式是 $\min(F,a)$。*

证明. 注意 $K=\oplus^{[K:F(a)]}F(a)$，L_a 在每个 $F(a)$ 上的作用都如同它限制在 $F(a)$ 上，于是结合单扩张的情况结论和上一命题结论自明。 □

练习 5.4 (Morandi 5.15). K/F 是有限正规扩张，并且没有真中间域，那么 $[K:F]$ 是素数。这对非正规扩张不正确。

证明. 考虑 K/F 的可分闭包 S。如果 $S=K$，那么 K/FGalois，于是由 Sylow p 子群的存在性直接得到结果；如果 $S=F$，那么 K/F 纯不可分，由 p-基的存在得证。

取 Galois 扩张 L/F 使得 $Gal(L/F)=S_4$，$K=\mathcal{F}(S_3)$，那么 K/F 没有真中间域，因为 $S_3\leq S_4$ 是极大的。 □

练习 5.5 (Morandi 5.16). $K/\mathbb{Q}$ 是 *Galois* 扩张，将 K 视为 $\mathbb{C}$ 的子域。如果 $\sigma(K)$ 是复共轭，那么 $\sigma(K)=K$。于是 $\sigma|_K\in Gal(K/\mathbb{Q})$。

证明 $\mathcal{F}(\sigma|_K)=K\cap\mathbb{R}$，以及 $[K:K\cap\mathbb{R}]\leq 2$，并且说明这个扩张次数能取到 *1* 和 *2*.

证明. 由命题 3.1.15，$\sigma|_K$ 可视做 $K\to\bar{\mathbb{Q}}$ 的 $\mathbb{Q}$ 同态，那么 $\sigma(K)=K$。由于 $\mathcal{F}(\sigma)=\mathbb{R}$，自然 $\mathcal{F}(\sigma|_K)=K\cap\mathbb{R}$。

由于 $K/\mathbb{Q}$Galois，那么 $K/(K\cap\mathbb{R})$ 也是如此，并且它对应着 $<\sigma|_K>$ 生成的子群，这就说明了 $[K:K\cap\mathbb{R}]\leq 2$，因为 $\sigma|_K^2=\mathrm{id}$。

$K=\mathbb{Q},\mathbb{Q}(i)$ 即为例子。 □

练习 5.6 (Morandi 5.26). K/F 是正规扩张，L/F 是代数扩张。如果 $K/F, L/F$ 中存在一个是可分扩张，那么 $[KL:L]=[L:K\cap L]$。

证明. K/F 可分，则 Galois。【未完】 □

第六章　有限域

6.1　结论

定理 6.1.1. 域 K 的乘法群的有限子群 G 是循环群。作为推论，有限域的乘法群是循环群。

证明. 注意 G 是有限 Abel 群，$n = |G|, m = exp(G)$，则 $m|n$。$x^m - 1$ 至多在 K^* 中有 m 个根；然而 $|G|$ 的元素都是 $x^m - 1$ 的根, 从而 $n \leq m$。这说明 $n = m$，于是 G 是循环群。 □

推论 6.1.2 (Primitive Element Theorem: 有限域). K/F 是有限域之间的扩张，那么是单扩张。由于前文未证明的部分是有限域的有限扩张如果中间域有限,那么是单扩张,这完成了 *Primitive Element Theorem*。

证明. K^* 是循环群，设由 α 生成。那么 $K = F(\alpha)$。 □

定理 6.1.3 (有限域结构定理). F 是特征 p 有限域，$|F| = p^n$（因为它是 $\mathbb{F}_p$ 的扩域，从而是其上的有限维线性空间）。那么 F 是 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的分裂域，从而 $F/\mathbb{F}_p$ 是 *Galois* 的。更进一步 *Frobenius* 自同构 $\sigma : a \mapsto a^p$ 生成了 *Galois* 群 $Gal(F/\mathbb{F}_p)$，它是循环群。

证明. $|F^*| = p^n - 1$，于是 $a^{p^n-1} = 1, \forall a \in F^*$，从而 $a^{p^n} - a = 0, \forall a \in F$。即 F 的元素都满足 $x^{p^n} - x$，但是这个多项式至多 p^n 个根，从而 F 是 $x^{p^n} - x$ 的分裂域。

$\sigma : a \mapsto a^p$ 确实是 $\mathbb{F}_p-$ 同态，于是由 F 的有限性，非零自同态都是同构。固定域是 $\{a \in F : a^p = a\} \supseteq \mathbb{F}_p$，但是它至多也只有 p 个根，于是 $\mathbb{F}_p$ 恰为固定域。

注意 σ 在 $Aut(F)$ 是 n 阶元：因为存在一个元素 $a \in F^\times$ 在乘法群中的阶恰为 $p^n - 1$，于是 $\sigma^i, i < n$ 不是 id。从而 σ 阶为 n，但是 $|Gal(F/\mathbb{F}_p)| = [F : \mathbb{F}_p] = n$，因此 Galois 群就是由它生成的。 □

推论 6.1.4. K/F 是特征 p 有限域之间的扩张，那么 K/F 是 *Galois* 的，*Galois* 群是循环群。如果 $|F| = p^n$，那么 $Gal(K/F)$ 是由自同构 $\tau(a) = a^{p^n}$ 生成的。

证明. $K/F/\mathbb{F}_p$，因此 K/F 是 Galois 的。其 Galois 群对应着 $Gal(K/\mathbb{F}_p)$ 的 n 阶子群，因此也是循环群，并且由 σ^n 生成。 □

下面我们将所有有限域放入一个代数闭包中考虑：

定理 6.1.5. N 是 $\mathbb{F}_p$ 的代数闭包，对于任何 n，存在唯一的 N 的子域，使得 $|N| = p^n$。如果 K, L 是 N 的子域，阶分别为 p^m, p^n，那么 $K \subseteq L \iff m|n$。此时 L/K 的性质如同前文所描述。

证明. 由于 p^n 阶域都是 $x^{p^n}-x$ 的分裂域，因此自然唯一。后文推论都是自然的。 □

推论 6.1.6 (Morandi 6.12). *K,L 是 F 的 n 次和 m 次扩张，那么 KL 是 F 的 $lcm(n,m)$ 次扩张；$K\cap L$ 是 $\gcd(n,m)$ 次扩张。这是因为上一命题指出 F 的扩域构成的偏序集和整数集在整除下构成的偏序集同构。*

推论 6.1.7. *F 是有限域，$f(x)$ 是 $\deg n$ 的 F 上不可约多项式。*

1. *a 是 f 在 F 的某个扩域中的根，那么 $F(a)$ 就是 f 在 F 的分裂域。从而 K/F 如果是分裂域，那么 $[K:F]=n$*
2. *如果 $|F|=q$，那么 f 的根是 a^{q^r}。*

证明. 取 K/F 为 f 的分裂域，那么 $F(a)$ 是 F 的 n 次扩张，于是 $F(a)/F$ 是 Galois 的，从而 $f(x)=\min(F,a)$ 分裂。

对于后半部分，注意同构扩张定理说明分裂域中的所有根都能通过将 Galois 群作用在一个根上得到，那么结论自明。 □

推论 6.1.8. *有限域都是完美域。*

证明. 每个有限扩张都是 Galois 的，从而每个代数扩张都是可分的（对单个元考虑即回到有限扩张的情况）。 □

命题 6.1.9. *$x^{p^n}-x$ 是全体 $\mathbb{F}_p$ 上次数为 n 的因子且首一不可约多项式的乘积。*

证明. 取 F 为 p^n 阶域，它是 $x^{p^n}-x$ 的分裂域。令 $a\in F$，$m=[\mathbb{F}_p(a):\mathbb{F}_p]$，那么 $m|n$，并且 $\min(\mathbb{F}_p,a)|x^{p^n}-x$。

反过来对于不可约多项式 f，并且其次数 $m|n$，取 K 为 f 的分裂域，那么 $K=\mathbb{F}_p(a)$，因此 $[K:\mathbb{F}_p]=m$，从而 $K\subseteq F$。因此 $a\in F$，并且 a 的极小多项式就是 f。而 $x^{p^n}-x$ 无重根，这就将其分解成了不同的不可约因子，从而得证。 □

6.2 例子

例子. *在 $\mathbb{F}_3$ 上 $x^4+1=(x^2+x-1)(x^2-x-1)$：由于有限域上相同次数不可约多项式的分裂域都是在一个代数闭包里大小相同的有限域，于是它们一定相同。这说明 x^4+1 的分裂域就是 $\mathbb{F}_3$ 的二次扩域。*

例子. *q 是 p 的幂，n 不被 p 整除。取 $\mathbb{F}_q$ 为 q 个元素的有限域，K 是 x^n-1 在其上的分裂域，那么 $K=\mathbb{F}_{q^{\varphi(n)}}$。*

证明. 取 σ 为 $K/\mathbb{F}_q$ 的 Frobenius 元（即生成了 Galois 群）。那么 $\sigma(a)=a^q$。于是直接计算知对于任何 x^n-1 的根 α，$\sigma^{\varphi(n)}(\alpha)=\alpha$，从而 $\sigma^{\varphi(n)}=\mathrm{id}$。

全体 x^n-1 的根构成了 K^* 的有限子群，于是是循环群，从而存在一个元素 β 使得其阶为 n。那么对于任何 $l<\varphi(n)$，$\sigma^l(\beta)\neq\beta$（直接计算）。因此 σ 的阶为 $\varphi(n)$，从而完成了证明。 □

6.3 习题

练习 6.1 (Morandi 6.3). *F 是有限域，对于任何 n 都存在 F 上的 n 次不可约多项式。*

证明. 取 F 的 n 次扩张 K，那么 K/F 是 Galois 的，从而有限可分，于是是单扩张 $K = F(a)$。那么 a 的极小多项式即为所求。 □

练习 6.2 (Morandi 6.8). *F 是特征 p 域。*

1. *F^p 是 F 的子域。*
2. *$F = \mathbb{F}_p(x)$，计算 F^p 和 $[F : F^p]$。*

证明. 1. 注意 $a \mapsto a^p$ 是域同态，那么 F^p 不过是 $^p : F \to F$ 的像。

2. $F^p = \mathbb{F}_p(x^p)$，从而 $[F : F^p] = p$。

□

练习 6.3 (Morandi 6.10). *有限域中的每个元素都可以写成两个元素的平方和。*

证明. char2 时显然：因为 $a = a^{2^n} = (a^{2^{n-1}})^2 + 0^2$。

对于特征 p 域（p 是奇素数），考虑群同态 $\varphi : K^\times \to K^\times : x \mapsto x^2$，那么 $\ker\varphi = \{\pm 1\}$（回忆 $K^\times$ 是乘法群）。

于是 φ 的像个数是 $(p^n-1)/2$，计算上 0 这就说明 F 中有 $(p^n+1)/2$ 个平方元。如果 $a \in F$ 不能表示为两个平方元的和，那么每个 $a - f^2$ 都不是平方元，说明非平方元至少有 $(p^n+1)/2$ 个。这说明 F 至少 p^n+1 个元素，矛盾。 □

练习 6.4 (Morandi 6.11). *有限域 F 满足 $|F| = q$，那么 F 上 p 次不可约多项式的个数为 $\dfrac{q^p - q}{p}$。*

证明. 这是显然的：因为 p 次不可约多项式的分裂域都是同一个域（阶为 q^p 者），$\mathbb{F}_{q^p}$ 的每个元素的极小多项式都应整除 p，于是只能是 1 和 p。将次数为 1（即 F 中）元素去掉，每个不可约多项式贡献了 p 个根，这就完成了证明。 □

练习 6.5. *k 是 $\mathbb{F}_p$ 的代数闭包，$\varphi \in Gal(k/\mathbb{F}_p)$ 是 Frobenius 自同构 $a \mapsto a^p$，那么 ϕ 无限阶，并且存在 $\sigma \in Gal(k/\mathbb{F}_p)$ 使得 $\sigma \notin <\varphi>$：这说明 $\mathbb{F}_p$ 的绝对 Galois 群不是循环群。*

证明. 假设 φ 有阶 m，那么 $a^{p^m} = a, \forall k$，于是每个 $|k| \le p^m$。但是 k 有 $|p^{n+1}|$ 阶子域，矛盾。

（我们知道了 $\mathbb{F}_p$ 的绝对 Galois 群实际上是 $\varprojlim \mathbb{Z}/n\mathbb{Z}$）遵循这个提示，我们可以给出构造：$\sigma := \cdots \circ \varphi^{3!} \circ \varphi^{2!} \circ \varphi^{1!}$。容易验证每个元素只会被作用有限次。

如果 $\sigma = \varphi^n$，观察其在子域 $\mathbb{F}_{p^{k!}}$ 的作用即知矛盾。 □

练习 6.6. *N 是有限域 F 的的代数闭包，证明 $Gal(N/F)$ 是 Abel 群，并且不含有有限阶元素。*

证明. 对于 Abel 性，只需注意到限制到每个 $\mathbb{F}_{p^n}$ 后得到的 Galois 群是交换的。

现在如果 $\sigma \in Gal(N/F)$ 是有限阶的，设阶为 m。取 $x \in N$ 使得 $[F(x) : F] = n$。假设 $\sigma|_{\mathbb{F}_{p^{mn}}}$ 阶为 k，那么 $k|m$，从而 $[\mathbb{F}_{p^{mn}} : \mathcal{F}(\sigma|_{\mathbb{F}_{p^{mn}}})]|m$。这说明了 $n|[\mathcal{F}(\sigma|_{\mathbb{F}_{p^{mn}}}) : F]$。而 $F(x)$ 是 F 的 n 次扩域，这说明 $F(x) \subseteq \mathcal{F}(\sigma|_{\mathbb{F}_p^{mn}})$，从而 $\sigma(x) = x$，进而 $\sigma = \mathrm{id}$。 □

第七章　分圆扩张

7.1　结论

7.1.1　分圆扩张

定义 7.1.1 (单位根、本原单位根和分圆扩张). $\omega \in F, \omega^n = 1$，则称 ω 为 n 次单位根。如果 ω（在乘法群中的）的阶是 n，那么称 ω 是本原的。对于任何单位根 ω，称扩域 $F(\omega)/F$ 是分圆扩张。

注记. 如果 ω 是 n 次本原单位根，那么 $\mathrm{char}(F)$ 不能是 n 的因子，否则 $(\omega^{n/p}-1)^p = \omega^n - 1 = 0$。

取 K 为 $x^n - 1$ 的分裂域，那么全体 $x^n - 1$ 的根构成了域的乘法群的有限子群，从而是循环群。这个时候循环群的生成元恰为本原单位根。

命题 7.1.2. *$char(F)$ 不是 n 的因子，K 是 $x^n - 1$ 在 F 上的分裂域。那么 K/F 是 Galois 的，并且 $K = F(\omega)$，这里 ω 是任何一个本原单位根，同时 $Gal(K/F)$ 同构于 $(\mathbb{Z}/n\mathbb{Z})^*$ 的子群。因此 $Gal(K/F)$ 是 Abel 的并且 $[K : F] | \varphi(n)$。*

证明. $x^n - 1$ 是可分的，于是 K/FGalois。如果 ω 是本原单位根，那么 ω^i 生成了 $x^n - 1$ 的所有解，从而生成了分裂域。

每个 $Gal(K/F)$ 都可以看做其在单位根构成的乘法子群 $\mathbb{Z}/n\mathbb{Z}$ 上的自同构，因此可以嵌入到 $Aut(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$，从而完成了证明。 □

7.1.2　$\mathbb{Q}$ 的分圆扩张

考虑 $\mathbb{Q}$ 上的本原单位根 $\{e^{2\pi i r/n} | \gcd(r, n) = 1\}$。

定义 7.1.3. n 次分圆多项式定义为 $\Psi_n(x) = \prod(x - \omega_i)$（乘法取遍本原单位根）。

引理 7.1.4.

$$x^n - 1 = \prod_{d|n} \Psi_d(x)$$

作为推论，$\Psi_n(x) \in \mathbb{Z}[x]$。

证明. 第一个等式是初等的。$\Psi_d(x), d|n, d < n$ 恰好取出的是那些与 n 的最大公因子为 d 的单位根。

作为推论，我们在 n 上归纳：注意 $x^n - 1 = \prod_{d<n, d|n} \Psi_d(x) \cdot \Psi_n(x)$，于是应用带余除法即证。 □

定理 7.1.5 (分圆多项式不可约). $\Psi_n(x)$ 在 $\mathbb{Q}$ 上不可约。

证明. 等价地，我们证明在 $\mathbb{Z}$ 上的不可约性：假设 $\Psi_n(x) = P(x)Q(x)$，其中 P, Q 为首一整系数多项式，P 不是常数并且在 $\mathbb{Z}$ 上不可约。

取 P 的一个根 z 以及和 n 互素的素数 p。那么 z^p 是 Ψ 的根，从而是 P 或 Q 的根。

如果 z^p 是 Q 的根，那么 z 是 $P(x), Q(x^p)$ 的公共根，从而 $P(x)|Q(x^p)$。设 $Q(x^p) = P(x)R(x)$，从而 $P(x)R(x) \equiv Q(x^p) \equiv Q(x)^p \equiv Q(x)(mod\ p)$。再设 $x^n - 1 = \Psi_n(x)S(x)$，那么 $(x^n - 1) \equiv P(x)Q(x)S(x) \equiv P^2(x)R(x)S(x)(mod\ p)$。

这说明 $x^n - 1$ 在 $\mathbb{F}_p$ 上的分裂域中有重根，但是观察形式导数和 $(n, p) = 1$ 知不可能。

因此 z^p 是 $P(x)$ 的根。现在对于任何与 n 互素的正整数 s，z^s 都是 $P(x)$ 的根，因为我们可以不断地往幂次上添加一个和 n 互素的素数（使用前述论证）。更进一步还可以嘉定这个 z 就是单位根 $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$。（在选取 P 的时候我们选 ω 的不可约分支即可）。

于是 $\Phi_n(x)$ 的根都是 $P(x)$ 的根，从而完成了证明。 □

推论 7.1.6. *K 是 $x^n - 1$ 在 $\mathbb{Q}$ 上的分裂域，那么 $[K : \mathbb{Q}] = \varphi(n)$，$Gal(K/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$。特别地，$\omega$ 是 K 中的本原单位根，则 $K = \mathbb{Q}(\omega), Gal(K/\mathbb{Q}) =< \sigma >$，并且 $\sigma_i(\omega) = \omega^i$。*

证明. 这是前述命题的综合。 □

7.2 例子

记 $\mathbb{Q}_n$ 为 n 次分圆扩张（即 $x^n - 1$ 的分裂域）。

例子. *给出 $\mathbb{Q}_{12}$ 的所有中间域：*

此时 Galois 群为 $(\mathbb{Z}/12\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$，其中两个直和因子的生成元分别为 $\omega \mapsto \omega^5, \omega \mapsto \omega^{-1}$。

于是真中间域为：$\mathbb{Q}(\omega+\omega^5), \mathbb{Q}(\omega+\omega^{-1})$（注意这两者都是 $\mathbb{Q}$ 的二次扩域，并且 $\omega+\omega^5, \omega+\omega^1 1$ 被固定，于是确实是要求的中间域。

练习 7.1. *$\mathbb{Q}(\cos(2k\pi/n)), \gcd(k, n) = 1$ 在 $\mathbb{Q}$ 上是 Galois 的，并且其扩张次数为 $\varphi(n)/2$。但是对于 $\sin(2k\pi/n)$ 这不正确、*

证明. 注意到 $\mathbb{Q}(\cos(2k\pi/n)) \subseteq \mathbb{Q}_n$，于是它是分圆扩张（从而是 Abel 扩张）的子扩张。注意 Abel 群的子群都正规，于是 $\mathbb{Q}(\cos(2k\pi/n))\mathbb{Q}$ 是 Galois 的。

现在由于 $\cos(2k\pi/n) = (\omega+\omega^{-1})/2$，这里 $\omega = e^{2k\pi/n}$ 从而是本原单位根，从而 $\mathbb{Q}_n = \mathbb{Q}(\omega)$。

$\omega^2 - 2\cos(2k\pi/n)\omega + 1 = 0$，于是 ω 的极小多项式次数不超过 2。然而 $\omega \notin \mathbb{Q}(\cos(2k\pi/n))$ 因为后者在实数内。这就说明这个扩张恰为 2 次扩张，从而 $[\mathbb{Q}(\cos(2k\pi/n)) : \mathbb{Q}] = \varphi(n)/2$。 □

7.3 习题

练习 7.2. *分圆域之间的包含关系与有限域类似：*

1. *$\mathbb{Q}_n \subseteq \mathbb{Q}_m \iff n|even(m)$，这里 $even(m)$ 在 m 是奇数时为 $2m$，偶数时为 m：这个复杂性源于 $\mathbb{Q}_m = \mathbb{Q}_{2m}(m\ odd)$。*

2. $\mathbb{Q}_n\mathbb{Q}_m = \mathbb{Q}_{lcm(n,m)}$

3. $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_{\gcd(n,m)}$

练习 7.3 (Morandi 7.15:Kronecker-Weber)**.** $d \in \mathbb{Q}, \mathbb{Q}(\sqrt{d})$ 包含在某个分圆扩张内。（更一般的 *Kronecker-Weber* 定理是任何 *Abel* 扩张都在某个分圆扩张内）

证明. 我们只需要考虑 d 是素数 $\pm p$ 的情况。对一般的情况只需将 d 的分子分母做素因数分解，然后把所有的素因子对应的分圆域取合成域得到所求的分圆扩张。

同样我们也无需考虑负数的情况，因为只需添加 $\mathbb{Q}_4 = \mathbb{Q}(i)$ 即可。

我们有 Gauss 和 $G_p \coloneqq \sum_{a=1}^{p-1} \left(\frac{r}{p}\right) \omega^a$，这里 ω 是 p 次单位根 $e^{2\pi i/p}$。Gauss 和的结果说明 $G_p^2 = \left(\frac{-1}{p}\right) p$，那么我们就得到了证明：因为 Gauss 和的左侧式子落在某个分圆扩张里，右侧则为 $\sqrt{p}$。 □

练习 7.4. *G 是有限 Abel 群，则存在一个 Galois 扩张 $K/\mathbb{Q}$ 使得 $Gal(K/\mathbb{Q}) = G$。*

证明. $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_k\mathbb{Z}$。取充分大的互不相同的素数 p_i 使得 $p_i \equiv 1 \mod n_i$（Dirichlet 定理），$r = \prod p_i$。那么 $Gal(\mathbb{Q}_r/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ 存在一个和 G 同构的商群，并且它是正规的。于是考虑对应的中间域即可。 □

第八章　范数和迹

8.1　结论

8.1.1　范数和迹

定义 8.1.1 (范数和迹). K/F 是有限扩张，那么范数、迹分别定义为

$$N_{K/F}(a) = \det L_a$$

$$T_{K/F}(a) = \mathrm{Tr} L_a$$

这里 L_a 是平移 $b \mapsto ab$。

命题 8.1.2. *K/F 是有限扩张，$n = [K : F]$。*

1. *$a \in K$，那么 $N_{K/F}(a), T_{K/F}(a) \in F$。*
2. *$T_{K/F} : K \to K$ 是 $F-$ 线性变换*
3. *$\alpha \in F$ 则 $T_{K/F}(\alpha) = n\alpha, N_{K/F}(\alpha) = \alpha^n$*
4. *$N_{K/F}$ 是积性的，即 $N_{K/F}(ab) = N_{K/F}(a)N_{K/F}(b)$*

命题 8.1.3 (通过极小多项式描述范数和迹). $[K : F] = n$，$a \in K, p(x) = x^m + \alpha_{m-1}x^{m-1} + \cdots + \alpha_0$ 是极小多项式，那么 $N_{K/F}(a) = (-1)^n \alpha_0^{n/m}, T_{K/F}(a) = -\dfrac{n}{m}\alpha_{m-1}$。

证明. 这是和练习 5.3一样的道理,在单扩张的情况下是已知的,那么再一次注意 $K = \oplus^{[K:F(a)]} F(a)$（这里每个直和项都是将 $F(a)$ 乘上 $K/F(a)$ 的一个基得到的，于是 L_a 作用在其上和在 $F(a)$ 上无异。 □

8.1.2　通过嵌入描述的范数和迹

首先回忆定理 5.1.12:

引理 8.1.4. *K/F 是有限扩张，那么 $[K : F]_s$ 等于 $K \to \bar{F}$ 的 $F-$ 同态个数（$\bar{F}$ 是代数闭包）。*

以及练习 4.2

引理 8.1.5. *K/F 是有限纯不可分扩张，$a \in K$ 则 $a^{K:F} \in F$。更进一步地，对于有限 Galois 扩张 N/F，$a \in KN$，则 $a^{[K:F]} \in N$，KN/N 也是纯不可分扩张。*

证明. 第一部分不过是练习 4.2，第二部分是因为 K 纯不可分，N 可分，于是 $N\cap K=F$。那么 $[NK:K]=[N:F]$，从而 $[NK:N]=[K:F]$。

注意每个 NK 中的元素都可以写为 $N(k_1,\cdots,k_n)$ 的形式：其分子分母都是 $N[k_1,\cdots,k_n]$ 中的元素。由于对于充分大的 p^n，$k_i^{p^n}\in F$，那么对于充分大的 p^n，$N[k_1,\cdots,k_n]$ 中元素的 p^n 次幂都称为 $N(F)=N$ 中的元素。

这说明 NK/N 纯不可分，那么由第一部分的命题就得到了结果。 □

引理 8.1.6 (乘法次数). $F\subseteq L\subseteq K$，$[K:F]<+\infty$。那么 $[K:F]_i=[K:L]_i\cdot[L:F]_i$

证明. S_1 是 F 在 L 中的可分闭包；S_2 是 L 在 K 中的可分闭包；S 是 F 在 K 中的可分闭包。

由于 K 中在 F 上可分的元素在 L 上也可分，于是 $S\subseteq S_2$，从而 $SL\subseteq S_2$，并且 S_2/SL 是可分的（因为在 L 上可分）；也是纯不可分的（因为 K/S 是纯不可分的，从而 S_2/S 也是，于是 S_2/SL 也是）。

因此 $S_2=SL$。我们接下来证明 $[S:S_1]=[S_2:L]$。由于 S/F 是可分的，S/S_1 也是可分的。那么 S/S_1 是单扩张，设 $S=S_1(a),f=\min(S_1,a),g=\min(L,a)$。那么在 $L[x]$ 中 $g|f$，然而 L/S_1 是纯不可分的，因此 g 的某次幂在 $S_1[x]$ 中，从而在 $S_1[x]$ 中 f 整除 g 的某次幂。这两个事实要求 f 是 g 的某次幂。然而 f 没有重根，因此只能 $f=g$。

从而 $[S:S_1]=[L(a):L]=[SL:L]=[S_2:L]$，于是这就说明了 $[S_2:S]=[L:S_1]$，利用乘积公式代入即得原结论。 □

现在我们得到计算范数和迹的主定理：

定理 8.1.7 (通过嵌入描述范数和迹). K/F 是有限扩张，$\sigma_1,\cdots,\sigma_r$ 是全体 $K\to\bar F$ 的 $F-$ 同态。如果 $a\in K$，那么：

$$N_{K/F}(a)=(\prod_j\sigma_j(a))^{[K:F]_i}$$

$$T_{K/F}(a)=[K:F]_i\sum_j\sigma_j(a)$$

证明. 取 $g(x)=(\prod_j(x-\sigma_j(a)))^{[K:F]_i}\in\bar F[x]$。由于定理 5.1.12，$r=[K:F]_s$，从而 $\deg g=[K:F]$。

记 $p(x)=\min(F,a)$。如果 $b\in\bar F$ 是 $p(x)$ 的根，那么由同构扩张定理存在 $\tau:M\to M$ 使得 $\tau(a)=b$。那么 $\tau|_K$ 是某个 σ_j，因此这就说明了 g,p 的根相同。

取 S 为可分闭包，N 为 S/F 的正规闭包，那么 N 是一组可分多项式的分裂域（回忆有限扩张正规闭包的构造是生成元的极小多项式分裂域），从而 N/F 是 Galois 的。那么由 Natrua Irrationality$[KN:K]=[N:K\cap N]|[N:S]$，从而 $[KN:N]|[K:S]=[K:F]_i$。由练习 4.2，KN/N 是纯不可分的，于是 $c^{[L:F]_i}\in N,\forall c\in KN$。

现在 KN 是 S 的 Galois 扩张和纯不可分扩张的合成，于是是两个正规扩张的合成，从而 KN/S 也是正规的。那么由命题 3.1.15知 $\sigma(K)\subseteq KN$。

因此 $g(x)\in N[x]$（这是因为 $(KN)^{[K:F]_i}\subseteq N$。现在对于任何 $Gal(\bar F/F)$ 中的元素 τ，$\{\tau\sigma_i|_K\}=\{\sigma_i\}$，于是 $\tau(g)=g$，从而 g 的系数在 $Gal(\bar F/F)$ 的不动域中。由定理 4.1.14，这正是 F 在代数闭包中的纯不可分闭包。于是 g 的系数同时在 N 中，由前文 N/F 是 Galois 的，从而是可分的，于是这就要求 $g\in F[x]$。

现在由 p 在 $F[x]$ 中的不可约性，这就要求 $g(x)=p(x)^{[K:F]/\deg p}$，那么由 8.6，$g(x)$ 就是 L_a 的特征多项式，那么结果得证。 □

推论 8.1.8. *K/F 是 Galois 扩张时不可分次数是 1，正规性要求所有到代数闭包的嵌入都是 $Gal(K/F)$ 的元素。于是上述情况变为：*

$$N_{K/F}(a)=\prod_{\sigma\in Gal(K/F)}\sigma(a)$$

$$T_{K/F}(a)=\sigma_{\sigma\in Gal(K/F)}\sigma(a)$$

8.1.3 乘积公式

定理 8.1.9 (乘积公式). $F\subseteq L\subseteq K,[K:F]<+\infty$。那么

$$N_{K/F}(a)=N_{L/F}(N_{K/L}(a))$$

$$T_{K/F}(a)=T_{L/F}(T_{K/L}(a))$$

证明. 取 M 为 F 的代数闭包。σ_i 为 $L\to M$ 的 $F-$ 同态，τ_i 为 $K\to M$ 的 $L-$ 同态。同构扩张定理保证它们都延拓为 $M\to M$ 的自同构，仍然保持记号。于是每个 $\sigma_j\circ\tau_k$ 都是 $M\to M$ 的 $F-$ 自同构。

反过来对于任何 $\rho:K\to M$ 的 $F-$ 自同构，$\rho|_L$ 是某个 σ_j，于是 $\sigma_j^{-1}\circ\rho$ 是某个固定 L 的 $F-$ 自同构，于是 $\sigma_j^{-1}\circ\rho=\tau_k$，从而 $\rho=\sigma_j\circ\tau_k$。那么由前述公式结果显然。 □

推论 8.1.10 (可分的判定). *K/F 是可分的 $\iff$ $T_{K/F}$ 不是零映射，即存在 $a\in K,T_{K/F}(a)\neq 0$。*

证明. 如果 K/F 不可分，那么 $\mathrm{char}(F)=p>0$。取 S 为 K/F 的可分闭包，$S\neq K,K/S$ 纯不可分。

然而 $T_{K/S}(a)=[K:S]_i\sum\sigma_i(a)=p^n\sum\sigma_i(a)=0$，从而 $T_{K/F}=T_{S/F}\circ T_{K/S}=0$。

反过来如果 K/F 是可分的，取 N 为正规闭包，那么只需说明 $T_{N/F}$ 是非零映射。此时 $T_{N/F}(a)=\sum_i\sigma_i(a)$，那么由 Dedekind 引理，$\sum_j\sigma_j(a)$ 不能对所有 a 都取零，于是得证。 □

8.2 例子

练习 8.1. *对于有限域之间的扩张 K/F，范数映射 $N_{K/F}$ 是满射。*

证明. 假设 $|F|=p^n,[K:F]=m$，那么 $Gal(K/F)$ 由 $\sigma:a\mapsto a^{p^n}$ 生成。

此时

$$N_{K/F}(a)=a\cdot a^{p^n}\cdot a^{p^{2n}}\cdots a^{p^{(m-1)n}}=a^{1+p^n+\cdots+p^{(m-1)n}}=a^{(p^{mn}-1)/(p^n-1)}$$

注意 $|K|=p^{nm}$，$N_{K/F}$ 诱导了 $K^*\to K^*$ 的群同态，即循环群之间的同态 $\mathbb{Z}/(p^{nm}-1)\mathbb{Z}\to\mathbb{Z}/(p^{nm}-1):a\mapsto(p^{nm}-1)/(p^n-1)\cdot a$。

于是它的像恰为 $\mathbb{Z}/(p^{nm}-1)\mathbb{Z}$ 中 $(p^{nm}-1)/(p^n-1)$ 的整数倍，于是像大小为 $p^n-1=|F^*|$。从而这的确是满射。 □

练习 8.2. p 是奇素数，$K=\mathbb{Q}(\omega)$，ω 是本原 p 次单位根，$N_{K\mathbb{Q}}(1-\omega)=p$。

证明. $K/\mathbb{Q}$ 是 Galois 的，ω 在诸 Galois 自同构下的作用是 ω^i。于是 $N_{K/\mathbb{Q}}(1-\omega)=\prod_{i=1}^{p-1}(1-\omega^i)=p$。 □

练习 8.3. $n\geq 3,\omega$ 是 n 次本原单位根，$K=\mathbb{Q}(\omega),N_{K/\mathbb{Q}}(\omega)=1$。

证明. K 是 n 次分圆扩张，$K/\mathbb{Q}$ 是 Galois 的：

$$N_{K/\mathbb{Q}}(\omega)=\prod_{\gcd(r,n)=1}\omega^r=\omega^{\varphi(n)\cdot n/2}=1$$

□

8.3 习题

练习 8.4. K/F 是有限 $Galois$ 扩张，L 是中间域，那么 $L=F(\{T_{K/L}(a)|a\in K\})$。

证明. 由正规基定理，存在 $a\in K$ 使得 $\{\sigma(a)|\sigma\in Gal(K/F)\}$ 构成 K 的 $F-$ 基。取

$$\alpha=T_{K/L}(a)=\sum_{\sigma\in Gal(K/L)}\sigma(a)$$

那么 $\tau(\alpha)=\alpha,\forall\tau\in Gal(K/L)$。反过来如果 $\tau(\alpha)=\alpha,\exists\tau\in Gal(K/F)$，即

$$\sum_{\sigma\in Gal(K/L)}\tau\sigma(a)=\sum_{\sigma\in Gal(K/L)}\sigma(a)$$

那么由于 $\{\sigma(a)|\sigma\in Gal(K/F)\}$ 是一组基，每个 $\tau\sigma$ 都应在 $Gal(K/L)$ 内。

从而 τ 也在 $Gal(K/L)$ 那，因此这就说明了 $Gal(K/L)=Gal(K/F(\alpha))$。

于是 $L=F(\alpha)=F(\{T_{K/L}(a)|a\in K\})$。 □

练习 8.5. K/F 是有限 $Galois$ 扩张，L 是中间域，那么 $L=F(\{N_{K/L}(a)|a\in K\})$。

证明. 首先 F 是有限域的时候练习 8.1已经解决了问题。假定 F 是无限域。

由于 K/F 是有限 Galois 扩张，从而是单扩张，假定 $K=F(\alpha)$，$f(x)=\min(L,\alpha)=\prod_{\sigma\in Gal(K/L)}(x-\sigma(\alpha))$。假定 f 的系数分别为 $l_{n-1},\cdots,l_0$，我们证明 $L=F(l_0,\cdots,l_{n-1})$。

首先一侧的包含是简单的，于是 $Gal(K/L)\subseteq Gal(K/F(l_0,\cdots,l_{n-1}))$。对于 $\tau\in Gal(K/F(l_0,\cdots,l_{n-1}))$，$\tau$ 固定 $f(x)$，从而它置换了根 $\sigma(\alpha)$。这就说明 $\tau\sigma(\alpha)=\sigma'(\alpha),\exists\sigma,\sigma'\in Gal(K/L)$，于是这就说明了 $\tau\in Gal(K/L)$。

从而 $Gal(K/L)=Gal(K/F(l_0,\cdots,l_{n-1}))$，这就说明了两个域相同。

现在注意我们只需要证明 $l_0,\cdots,l_{n-1}\subseteq F(\{N_{K/L}(a)|a\in K\})$。

对于 $a\in F$,

$$f(a)=\prod_{\sigma\in Gal(K/L)}(a-\sigma(\alpha))=\prod_{\sigma\in Gal(K/L)}(\sigma(a)-\sigma(\alpha))$$

$$=\prod_{\sigma\in Gal(K/L)}\sigma(a-\alpha)=N_{K/L}(a-\alpha)$$

由于 $|F|$ 是无限的，可以选择不同的元素 $a_0, \cdots, a_{n-1} \in F$，使得有如下方程：

$$\begin{pmatrix} 1 & a_0 & \cdots & a_0^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & \cdots & a_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} l_0 \\ \vdots \\ l_{n-1} \end{pmatrix} = \begin{pmatrix} f(a_0) - a_0^n \\ \vdots \\ f(a_{n-1}) - a_{n-1}^n \end{pmatrix}$$

但是左侧矩阵行列式是 Vandermonde 行列式，我们的选取使得这个行列式非零，于是我们将 l_i 表示成 $f(a_i)$ 和 F 的元素的有理式。但是 $f(a_i)$ 是 $N_{K/L}(a_i - \alpha)$，这就完成了证明。 □

第九章　循环扩张

定义 9.0.1 (循环扩张). Galois 扩张 K/F 称为循环扩张，如果 $Gal(K/F)$ 是循环群。

9.0.1　包含本原单位根的循环扩张 ≈ 添加一个 n 次根

我们来说明一个循环扩张的结构定理：它指出包含原根的循环扩张一定是添加 n 次根得到的扩张。这也是我们能得到的最普遍的一个结构定理。

引理 9.0.2. *F 包含 n 次本原单位根 ω，K/F 是 n 次循环扩张，σ 是 $Gal(K/F)$ 的生成元，那么存在 $a \in K$ 使得 $\omega = \sigma(a)/a$。*

证明. 由于 σ 是 $F-$ 线性变换，这相当于证明 σ 有特征值 ω。

注意 $\sigma, \cdots, \sigma^{n-1}$ 是线性无关的（Dedekind 引理），于是 σ 的极小多项式恰好为 $x^n - 1$，从而是特征多项式的因子。但是 ω 是 $x^n - 1$ 的根，这就说明了结果。 □

定理 9.0.3. *F 包含 n 次本原单位根 ω，K/F 是 n 次循环 Galois 扩张，那么存在 $a \in K, K = F(a), a^n = b \in F$，即 $K = F(\sqrt[n]{b})$。*

证明. 存在 a 使得 $\sigma(a) = \omega a, \sigma^i(a) = \omega^i a$。于是 a 只被 id 固定，从而 $Gal(K/F(a)) =< \mathrm{id} >$，因此 $K = F(a)$。

$a^n = (\omega a)^n$，于是它被 σ 固定，从而 $a^n \in F$，这就说明了结果。 □

当然对于这一类添加 n 次根的扩张，我们也有如下描述：

命题 9.0.4. *F 包含 n 次本原单位根，$K = F(\sqrt[n]{b})$。那么 K/F 是循环 Galois 扩张，并且 $m = [K : F]$ 等于 $b(F^*)^n$ 在 $F^*/(F^*)^n$ 中的阶，并且 $\min(F, \sqrt[n]{b}) = x^m - d, \exists d \in F$。*

证明. 假定 $a \in K, a = \sqrt[n]{b}$，那么由于 F 有本原根，$x^n - b$ 分裂。计算形式导数知它可分，于是确实 Galois。

$\min(F, a)$ 的根形如 $\{\omega^j a\}$，并且 $\min(F, a) | x^n - b$。诶富哦 $\sigma \in Gal(K/F)$，那么 $\sigma(a) = \omega^i a$。现在取

$$\mathcal{S} = \{i \mod n | \sigma(a)/a = \omega^i \ for\ some\ \sigma \in Gal(K/F)\}$$

那么 $\mathcal{S}$ 是 $Gal(K/F) \to \mathbb{Z}/n\mathbb{Z}$ 的像（这个映射是 $\sigma \mapsto i \mod n, \omega^i = \sigma(a)/a$。

如果 $\sigma \mapsto 0 \mod n$，那么 $\sigma(a) = a$，于是 $\sigma = \mathrm{id}$，这说明上述同态是单同态。因此 $Gal(K/F) \cong \mathcal{S}$ 是 $\mathbb{Z}/n\mathbb{Z}$ 的子群，从而也是循环的。

假定 $Gal(K/F) =< \tau >$，$\tau(a) = \omega^t a$。取 $m = |Gal(K/F)|$，那么 m 是 ω^t 的阶。多项式 $\prod_{i=0}^{m-1}(x - \tau^i(a))$ 在 $F[x]$ 中（因为它被 τ 固定）。那么观察常数项知 $a^m \in F$，于是 $b^m = a^{mn} \in (F^*)^n$。

假设 m' 是 $b(F^*)^n$ 在 $F^*/(F^*)^n$ 中的阶，那么 $m'|m$。反过来由于 $b^{m'} \in (F^*)^n$，那么 $b^{m'} = c^b, \exists c \in F$。因此 $a^{m'n} = c^n$，从而 $a^{m'} = c\omega^i, \exists i$。因此 $a^{m'} \in F$。于是 $a^{m'} = \tau(a^{m'}) = \omega^{tm'}a^{m'}$，从而 $\omega^{tm'} = 1$，因此 $m|m'$。

这就说明了 $m = m'$，现在 $m = [K : F] = \deg(\min(F, a))$，并且 $x^m - a^m \in F[x]$，这就说明了 $\min(F, a) = x^m - a^m$。 □

现在这样的循环扩张结构使得我们能给出中间域的描述：

推论 9.0.5. *K/F 是 n 次循环扩张，F 包含 n 次本原单位根。如果 $K = F(\sqrt[n]{a})$，那么任何中间域都形如 $F(\sqrt[m]{a})$，其中 m 是 n 的因子。*

证明. σ 是 $Gal(K/F)$ 的生成元，那么每个子群都形如 $< \sigma^t >$。

假设 $n = tm$，$\alpha = \sqrt[n]{a}$，那么容易验证 α^t 被 σ^m 固定：$\sigma^m(\alpha^t) = \omega^{tm}\alpha^t = \alpha^t$。

然而 $a(F^*)^m$ 的阶等同于 $\alpha^t(F^*)^n$ 的阶，后者恰好是 m，因此 $F(\sqrt[m]{a})$ 的扩张就是 m 次的，从而计算次数知 $F(\sqrt[m]{a})$ 就是不动域，这就完成了证明。 □

9.0.2 特征 p 的 p 次循环扩张

定理 9.0.6. *$char(F) = p, K/F$ 是 p 次循环 Galois 扩张。那么 $K = F(\alpha), \alpha^p - \alpha - a = 0, \exists a \in F$。*

证明. 假设 σ 是 Galois 群的生成元，T 是 $F-$ 线性变换 $\sigma - \mathrm{id}$。那么 $\ker T = F, T^p = \sigma^p - \mathrm{id}^p = 0$，从而 $\mathrm{Im}\, T^{p-1} \subseteq \ker T = F$。但是像空间是 $F-$ 线性子空间，于是只能 $\mathrm{Im}\, T^{p-1} = \ker T = F$。

因此假定 $1 = T^{p-1}(c), \exists c \in K$，取 $\alpha = T^{p-2}(c)$，那么 $T(\alpha) = 1, \sigma(\alpha) - \alpha = 1$。由于 α 没有被 σ 固定，$\alpha \notin F$，于是 $F(\alpha) = K$，因为 $[K : F] = p$ 是素数（从而没有中间域）。

现在 $\sigma(\alpha^p - \alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$，因此 $a = \alpha^p - \alpha \in F$，从而完成了证明。 □

再一次地我们有反过来的结果：

定理 9.0.7. *F 是特征 p 域，$a \in F$ 并且不能写成 $b^p - b, b \in F$ 的形式。那么 $f(x) = x^p - x - a$ 在 F 上不可约，其分裂域是 F 的 p 次循环 Galois 扩张。*

证明. 取 α 为 f 的根，那么 $\alpha, \alpha + 1, \cdots, \alpha + p - 1$ 都是互异的 f 的根。条件保证了 $\alpha \notin F$，于是分裂域 $K = F(\alpha)$。

现在如果 f 可约，设不可约因子为 $g_1, \cdots, g_r$，对每个 i 选取 g_i 的根 β，那么都有 $K = F(\beta)$，于是 $\deg g_i = [K : F], \forall i$。从而 $\deg f = r \deg g_1$。于是只能有一个不可约因子，从而 f 不可约。

现在 $[K : F] = p$，由同构扩张定理存在 $\sigma(\alpha) = \alpha + 1, \sigma \in Gal(K/F)$，于是 σ 的阶为 p，从而 $Gal(K/F) =< \sigma >$。 □

9.1 问题

练习 9.1. *F 是包含 n 次本原单位根的域，$a \in F$。那么 $x^n - a$ 在 F 上不可约 $\iff$ 它不是某个 F 中元素的 m 次方，其中 $m > 1$ 是 n 的因子。*

证明. 考虑 x^n-a 的分裂域 K，设有一根 α，那么诸 $\omega^i\alpha$ 都是根，因此 $K=F(\alpha)$。

如果 x^n-a 不可约，那么 $[K:F]=n$。由命题 9.0.4，最小的使得 $a^k=b^n,\exists b\in F$ 是 n。然而如果 $a=c^m,c\in F,a^{n/m}=c^{m*(n/m)}=c^n$，矛盾。因此 a 不是这样的 m 次幂。

反过来如果 a 不是这样的 m 次幂，但是 x^n-a 可约，设 $x^n-a=\prod(x-\omega^i\alpha)=f(x)g(x)$。

那么 $f(x),g(x)$ 的常数项形如 $\omega^b\alpha^k,\omega^c\alpha^{n-k}$。于是由 Euclid 算法，$\alpha^{\gcd(k,n-k)}\in F$。从而 $a=[\alpha^{\gcd(k,n-k)}]^{n/\gcd(k,n-k)}$，由条件矛盾。 □

练习 9.2. *F 是域，ω 是 F 的怠忽必报中的一个本原 n 次单位根。如果 $a\in F$ 不是 $F(\omega)$ 中的某个元素的 m 次方，$m>1,m|n$，那么 x^n-a 在 F 上不可约。*

证明. 由前一命题 x^n-a 在 $F(\omega)$ 上不可约，于是在 F 上不可约。 □

练习 9.3. *始终假定 F 特征非 2，我们来考虑一个不包含本原 4 次单位根的域的 4 次循环扩张。F 不包含 4 次本原单位根，$L=F(\sqrt{a}),a\in F-F^2$，$K=L(\sqrt{b}),b\in L-L^2$。证明以下等价：*

1. *a 是 F 中元素的平方和*
2. *$-1=N_{L/F}(\alpha),\exists\alpha\in L$*
3. *$a=N_{L/F}(\alpha),\exists\alpha\in L$*
4. *$N_{L/F}(b)\equiv a \mod (F^*)^2,\exists b\in L$*
5. *K/F 是循环扩张（这里的 K 是由上一个条件的 b 决定的）*
6. *L 包含在 F 的某个 4 次循环扩张中。*

证明. 1 $\implies$ 2. 假设 $a=b^2+c^2$，那么取 $\alpha=b/c+1/c\cdot\sqrt{a}$ 则由于 L/F 是 Galois 扩张（可分性直接检验）：

$$N_{L/F}(\alpha)=b^2/c^2-a/c^2=-1$$

2 $\implies$ 3. 假设 $-1=N_{L/F}(\alpha)$。注意 $N_{L/F}(\sqrt{a})=-a$，那么 $N_{L/F}(\alpha\sqrt{a})=a$。

3 $\implies$ 4. 显然

4 $\implies$ 5. 假设 $b=k_1+k_2\sqrt{a}$。那么 $N_{L/F}(b)=k_1^2-ak_2^2$。由条件它是某个 $ak^2,k\in F$。

注意 $\sqrt{b}$ 满足多项式 $f(x)=(x-\sqrt{b})(x+\sqrt{b})(x-k\sqrt{a/b})(x+k\sqrt{a/b})=x^4-\frac{1}{b}(ak^2+b^2)+ak^2$。

如果 $k_2=0,a=(k_1/k)^2\in F^2$，矛盾。因此 $k_2\neq0$，从而 $K=F(\sqrt{b})$。现在 $[K:F]=[K:L]\cdot[L:F]=4$，并且 $K=F(\sqrt{b})$，那么 f 在 F 上不可约。直接验证知 f 的根各不相同，于是分裂，从而 K/F 是 Galois 的。

因此由同构扩张定理存在 $\sigma\in Gal(K/F)$ 使得 $\sigma(\sqrt{b})=k\sqrt{a/b}$，我们证明它的阶是 4.

首先 $\sigma^2(\sqrt{b})=\sqrt{b/a}\sigma(\sqrt{a})$，如果它是 $\sqrt{b}$，那么 $\sigma(\sqrt{a})=\sqrt{a}$。但是：

$$\sigma(\sqrt{b})=\sigma(\sqrt{k_1+k_2\sqrt{a}})=k\sqrt{a/b}=\sqrt{k_1-k_2\sqrt{a}}\implies\sigma(\sqrt{a})=-\sqrt{a}$$

矛盾，于是 σ 阶是 4.

5 $\implies$ 6. 显然

$6 \implies 1$. 假设 $[K:F]$ 是包含 L 的 4 次循环扩张，$[K:L]=2$，从而 $K=L(\sqrt{b}), b \in L-L^2$。如果 $b \in F$，那么 $[F(\sqrt{b}):F]=2$，从而 $F(\sqrt{b})=F(\sqrt{a})$（$\mathbb{Z}/4\mathbb{Z}$ 的二阶子群唯一）。但是这就说明 $K=L$ 了，矛盾。因此 $K=F(\sqrt{b})$。

假定 $b=k_1+k_2\sqrt{a}$，再一次地 $F(\sqrt{a}) \neq F(\sqrt{b})$ 说明 $k_1 \neq 0$，于是 $\min(F,\sqrt{b})=x^4-2k_1x^2+k_1^2-k_2^2a$。 □