抽象代数笔记

主讲教师：邱德荣　　记录人：马明扬(1.1-1.4),李航(1.5-2.3)

目录

1 域的代数扩张

1.1 代数闭包

K/F是一个数域扩张，$F \overset{\sigma}{\hookrightarrow} K$ 嵌入，对于多项式$F[x]$中多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

定义$\sigma f(x)$为

$$\sigma f(x) \triangleq f^{\sigma}(x) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_1)x + \sigma(a_0) \in \sigma(F)[x] \subset K[x].$$

设有$\alpha \in F$ 使得 $f(\alpha) = 0$, 则

$$\begin{aligned} f^{\sigma}(\sigma(\alpha)) &= \sigma(a_n)\sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\ &= a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\ &= 0. \end{aligned}$$

即$\sigma(\alpha)$是f^{σ}上的一个根.

如下图

$$\begin{tikzcd} K \arrow[rr, "\sigma"] & & K \\ & F, \arrow[ul] \arrow[ur, "id"'] & \end{tikzcd}$$

$F \subset K, \sigma : K \longrightarrow K$是一个$F\check{}$嵌入, 且$\sigma|_F = id$.设$f(x) \in F[x], \alpha \in K$。若$f(\alpha) = 0$, 则由于$\sigma(f(x)) = f^{\sigma}(x) = f(x)$(因为$\sigma|_F = id_F$)，故

$$0 = \sigma(0) = \sigma(f(\alpha)) = f^{\sigma}(\alpha) = f(\sigma(\alpha)),$$

即$f(\sigma(\alpha)) = 0$. 从而$\sigma(\alpha)$也是$f(x)$的一个根。

$\sigma(f(\alpha)) = f(\sigma(\alpha))$, 考虑

$$\sigma(\frac{f(\alpha)}{g(\alpha)}) = \frac{f^{\sigma}(\sigma(\alpha))}{g^{\sigma}(\sigma(\alpha))},$$

从而得到

$$\sigma(\frac{f(\alpha)}{g(\alpha)}) = \frac{f(\sigma(\alpha))}{g(\sigma(\alpha))}.$$

问：F是一个域，$f(x) \in F[x], degf > 0$是否有F的扩域E，使得f在E中有根？

由于$F[x]$是PID，则任意一个多项式

$$f(x) = P_1(x)^{e_1} \cdots P_r(x)^{e_r}$$

其中$P_i(x)$在F上不可约. 不妨设f在F上不可约，$f(x) \in F[x]$.令$m =< f > \lhd F[x]$，则m是极大理想

$$\begin{tikzcd} F[x] \arrow[rr, "\sigma"] & & F[x]/m \triangleq E \\ & F \arrow[ul, "\eta"] \arrow[ur] & \end{tikzcd}$$

显然σ为满射,此时E为域，F直接看作E的子域，从而可把E看作F的扩域, 由于$f(x) \in m$，故在$E = F[x]/m$中$\overline{f(x)} = \overline{0}$. 将$f(x)$展开如下：

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[X],$$

于是我们有：

$$\begin{aligned} \overline{0} = \overline{f(x)} &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{a_n x}^n + \cdots + \overline{a_1 x} + \overline{a_0} \end{aligned}$$

即在E中（注意到$\overline{a_i} = a_i, i = 1 \cdots n, F \hookrightarrow E$ ）

继而得到：

$$\overline{0} = a_n \overline{x}^n + \cdots + a_1 \overline{x} + \overline{a_0}$$

此时$\overline{x} \in E$,即$f(\overline{x}) = \overline{0}$,也即$f$在$E$中有根.

定理　设F是一个域，$f(x) \in F[X]$,且$degf > 0$,则存在一个F扩域E,使得f在E中有根.(证明上面已给出)

推论　设F是一个域，$f_1(x) \cdots f_n(x) \in F[X]$,且$degf_i > 0, i = 1 \cdots n$,则存在一个$F$扩域$E$,使得$f_1(x) \cdots f_n(x)$在$E$中均有根.

证明. 由上述定理，存在一个F扩域E_1,使得$f_1(x)$在E_1中有根，此时

$$f_2(x) \in F[X] \subset E_1[X],$$

又由上述定理，存在E_1扩域E_2,使得$f_2(x)$在E_2中有根.依次下去，得到E_{n-1}扩域E_n,使得$f_n(x)$在E_n中有根.

即$f_1(x) \cdots f_n(x)$在E_n中有根. □

定义　代数封闭域（$algebraically\ field$）

设K是一个域,如果K上任意一个次数大于0的多项式，均在K中有根，则称K是一个代数封闭域.

事实　设K是一个代数封闭域,$f(x) \in K[X]$,且$n = degf > 0$,则$f(x)$在K中有且只有n个根.(重根按重数计算)

证明. 由所设，$f(x)$在K中有根，取其一为α_1,即$\alpha_1 \in K$,,满足$f(\alpha) = 0$,此时由带余除法可知，

$$(x - \alpha_1) | f(x),$$

即:

$$f(x) = (x - \alpha_1) \cdot g(x),$$

其中$g(x)\in K[X]$,且次数为$n-1$.

(1)若$n-1=0$,则$f(x)$在K中有一个根，结论显然成立.

(2)若$n-1>0$,此时$g(x)$在K中有一个根α_2,此时有：

$$g(x)=(x-\alpha_2)\cdot h(x),$$

其中$h(x)\in K[X]$,且次数为$n-2$,即:

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdot h(x)$$

依次做下去，得到：

$$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

故$f(x)$在K中有且只有n个根.(重根按重数计算)　□

定理　任一个域均包含于一个代数封闭域 .

证明. (Artin)

设k是一个域,令：

$$S_0=\{f(x)\in k[X],degf>0\},$$

对每个$f\in S_0$,都给f对应于一个未定元，记之为X_f,记

$$S=\{X_f:f\in S_0\}.$$

令$A=K[S]$是k上关于未定元集S的多项式环.注意到，对每个$f\in S_0$,都有$f(X_f)\in A$,令：

$$I=<f(X_f):f\in S_0>,$$

为A中由所有$f(X_f)(f\in S_0)$生成的理想.

下证：I是A的真理想，即证$1\notin I$,

反证，若$1\in I$,就有

$$1=g_1f_1(X_{f_1})+\cdots+g_nf_n(X_{f_n}) \tag{1}$$

其中$g_1\cdots g_n\in A,f_1\cdots f_n\in S_0,g_1\cdots g_n\in A$是$\{X_f\}_{f\in S_0}$中有限个变量的多项式.(虽然$A$中的变量个数是无限的，但每个多项式$g_i$的变量个数是有限的)

对于$f_i(X_{f_i})\in k[X_f],i=1\cdots n$,由上述定理可知，存在$k$的扩域$E_1$,使得$f_i(X_{f_i})$在$E_1$中均有根，不妨取其根为$\alpha_i\in E$,(即$f_i(\alpha_i)=0$),将$\alpha_i$代入（1）中,得到：

$$1=g_1(\alpha_1)f_1(\alpha_1)+\cdots+g_n(\alpha_n)f_n(\alpha_n)=0,$$

矛盾！

因此I是A的真理想，故有A的一个极大理想m,使得$I\subset m$.令$K_1=A/m$,则K_1是一个域，从而如下图所示：

$$\begin{tikzcd} A=K[S] \arrow[rr, "\sigma"] & & K_1=A/m \\ & k \arrow[ul] \arrow[ur] & \end{tikzcd}$$

其中σ显然为满射，K_1可看作是k的一个扩域.任取$f \in S_0, f(X_f) \in I \subset m$. 从而有$\overline{f(X_f)} = \overline{0} \in A/m = K_1$,即$f(\overline{X_f}) = \overline{0}$,也即$\overline{X_f}$是$f$在$K_1$中的一个根.

对于K_1按上述步骤，可构造K_1的一个扩域K_2，使得K_1中的任一次数≥ 0的多项式，在K_2中均有根.依此类推，可得到域的扩张链如下：

$$k \subset K_1 \subset \cdots \subset K_n \subset \cdots,$$

其中K_n中次数大于0的多项式均在K_n-1中有根.令$K = \bigcup\sum_{i=1}^{\infty} K_i$,则显然$K$是一个域，且$k \subset K$.

下证：K是代数封闭域.

为此任取$f(x) \in K[X]$,且$degf > 0$,则由上述构造可知，存在$n \in Z_{\geq 0}$,使得$f(x) \in K_n[X]$,于是$f(x)$在$K_{n+1}[X](\subset K)$中与根，故K是代数封闭域. □

定理　设k是一个域，则存在域K,使得K是代数封闭域，且K/k是代数扩张，称K是k的一个代数闭包.

证明. 由前面的定理可知，k包含于一个代数封闭域E中，令$K = \{\alpha \in E, \alpha是一个k—代数元\}$,则$K$是一个域，且$K/k$是一个代数扩张.

下证：K是代数封闭域.

为此任取$f(x) \in K[X]$,且$degf > 0$,则$f(x) \in E[X]$,由于E是代数封闭域，故f在E中有根，取其一为α,即$\alpha \in E, f(\alpha) = 0$

显然α是一个K—代数元,即$K[\alpha]/K$是一个代数扩张，又由于K/k是一个代数扩张，进而可知$K[\alpha]/k$是一个代数扩张.即α是一个k—代数元,从而可知$\alpha \in K$,因此K是代数封闭域，K是k的一个代数闭包（同构意义下） □

E是代数封闭域,K/k是一个代数扩张,$\sigma : k \to E$,问是否存在$\tau; K \to E$,使得$\tau|_k = \sigma$.正如下图所示：

$$\begin{tikzcd} K \arrow[rr, "\tau"] & & E \\ & k \arrow[ul] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

简化模型　$K = k(\alpha)$是k上的单代数扩张，设α在k上的极小多项式为$P_\alpha(x) \in k[X]$,从而有$P_\alpha^\sigma(x) \in \sigma(k)[X] \subset E[X]$,且有$P_\alpha^\tau(x) \in E[X]$.

由$P_\alpha(\alpha) = 0$推出$0 = \tau(P_\alpha(\alpha)) = P_\alpha^\tau(\tau(\alpha)) = P_\alpha^\sigma(\tau(\alpha))$,即$\tau(\alpha)$是$P_\alpha^\sigma$在$E$中的一个根.

反之，$\beta \in E$,且$P_\alpha^\sigma(\beta) = 0$,令

$$\tau; k(\alpha) \to E, \quad \alpha \longmapsto \beta$$

从而有对应

$$g(\alpha) \longmapsto g^\sigma(\tau(\alpha)) = g^\sigma(\beta)$$

继而下图成立：

$$\begin{tikzcd} K=k(\alpha) \arrow[rr, "\tau"] & & E \\ & k \arrow[ul] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

命题 设E是代数封闭域,$k \subset$E,α是一个k—代数元,$P_\alpha(x) \in k[X]$是k上的极小多项式，则$k(\alpha)$到E中的k-嵌入的个数=$P_\alpha(x)$中全部互异根的个数$\leq degP_\alpha(x)$

命题 设K/k是一个代数扩张，E是一个代数封闭域，$\sigma; k \to E$是一个域嵌入，则σ可延拓到K上，即有域嵌入

$$\tau; K \to E$$

,使得$\tau|_k = \sigma$.

1.2 分裂域 正规扩张

回顾：设k是代数封闭域，,$f(x) \in k[X]$,且$n = degf > 0$,,则$f(x)$在k中有根，从而就有n个根.(重根按重数计算)

设F是一个域，$f(x) \in F[X]$,且$n = degf > 0$,,则$f(x)$在F中至多有n个根.

代数闭包：K/k是一个域扩张（1）K/k是代数扩张；（2）K是代数封闭的，则称K是k的一个代数闭包.

取E为代数封闭域，且$k \subset E$,令： $k^\alpha = \{\alpha \in E, \alpha$是一个$k$—代数的$\}$,则$k^\alpha$是$k$的一个代数闭包.

命题 设k是代数封闭域，且K/k是一个代数扩张，则$K = k$.(代数闭域只有平凡的代数扩张)

证明. 任取$\alpha \in K, \alpha$是一个k—代数元，α在k上的极小多项式为,$P_\alpha(x) \in k[X]$,则$degP_\alpha(x) > 0$,于是$P_\alpha(x)$在k中完全分解.特别地，$\alpha \in k$ □

命题 设E为代数封闭域，k是一个域，则k到E的任何一个嵌入，$\sigma; k \to E$均可延拓到k的任何一个代数扩域K上，即对于任意代数扩张K/k,存在嵌入：

$$\tau; K \to E,$$

使得$\tau|_k = \sigma$.

证明. 取$S = \{(F, \tau) : F$是K/k的中间域,$\tau; F \to E$,且$\tau|_k = \sigma$显然$(k, \sigma) \in S, S \neq \phi$.

在S中引入如下关系：对于$(F_1, \tau_1), (F_2, \tau_2) \in S$，定义$(F_1, \tau_1) \leq (F_2, \tau_2)$，如果$F_1 \subset F_2$，且满足$\tau_2|_{F_1} = \tau_1$.

易验证，“$\leq$”是S上的一个偏序关系，即$(S, \leq)$是一个非空偏序集.

如下图：

$$\begin{tikzcd}
K \arrow[r] & E \\
F_2 \arrow[u] \arrow[ur, "\tau_2"] & \\
F_1 \arrow[u] \arrow[uur, "\tau_1"] & \\
k \arrow[u] \arrow[uuur, "\sigma"] &
\end{tikzcd}$$

任取S上的一个全序子集$\{(F_i,\tau_i)\}_{i\in I}$,令$L=\bigcup_{i\in I}F_i$,则$L$是$K/k$的一个中间域，此时我们令：

$$\tau; L\to E \quad \alpha\longmapsto\tau_i(\alpha)$$

其中$\alpha\in F_i$,对任意的$\alpha\in L$,则τ是一个嵌入.

证明思路如下图：

$$\begin{tikzcd}
K \arrow[r] & E \\
K_0(\alpha) \arrow[u] \arrow[ur, "\tau"] & \\
K_0 \arrow[u] \arrow[uur, "\tau_0"] & \\
k \arrow[u] \arrow[uuur, "\sigma"] &
\end{tikzcd}$$

该嵌入是良好定义的.如果$\alpha\in F_i$,且$\alpha\in F_j$,则不妨设$F_i\subset F_j$,此时$\tau_i=\tau_j|_{F_i}$,从而有$\tau(\alpha)=\tau_i(\alpha)=\tau_j|_{F_i}(\alpha)=\tau_j(\alpha)$.且对任意的$\alpha\in K$,有$\alpha\in F_i$（对于任意的$i\in I$)进而有

$$\tau(\alpha)=\tau_i(\alpha)=\sigma(\alpha),$$

即$\tau|_k=\sigma$.可以推出$(L,\tau)\in S$,且显然有$\tau|_{F_i}=\tau_i$,即$(F_i,\tau_i)\leq(L,\tau)(i\in I)$成立.也即$(L,\tau)$是$\{(F_i,\tau_i)\}_{i\in I}$在$S$中的一个上界.

因此由$Zorn$引理可知，S中有极大元，设其中的一个极大元为(K_0,τ_0).

下证：$K=K_0$.

假若不然，则有$\alpha\in K,\alpha\notin K_0$,由所设$\alpha$是一个$k$—代数元,从而$\alpha$也是一个$K_0$—代数元,故$K_0(\alpha)/K_0$是一个单代数扩张.

由前面的定理得τ_0可延拓到$K_0(\alpha)$上,即有嵌入

$$\tau':K_0(\alpha)\to E,$$

使得$\tau'|_{K_0=\tau_0}$.显然有$\tau'|_k=\tau_0|_k=\sigma$,故$(K_0(\alpha),\tau')\in S$.但$(K_0,\tau_0)\leq(K_0(\alpha),\tau')$,但$K_0\neq K_0(\alpha)$与$K_0$的极大性矛盾.

因此$K=K_0$. □

取E为代数封闭域，且$k \subset E$,令$k^a = \{\alpha \in E, \alpha$是一个$k$—代数元$\}$,则$k^a$是$k$的一个代数闭包.

设k, k'是域，$\sigma : k \to k'$为同态应射同态映射；$\eta : k \to k^a$为恒等嵌入；$\eta' : k' \to k'^a$为恒等嵌入.如图所示：

$$\begin{tikzcd} k^a \arrow[r, "\tau"] & k'^a \\ k \arrow[u, "\eta"] \arrow[r, "\sigma"'] & k' \arrow[u, "\eta'"'] \end{tikzcd}$$

则σ可延拓到k^a上，即有域嵌入$\tau : k^a \to k'^a$,使得$\tau|_k = \sigma$.即有：

$$\begin{tikzcd} k^a \arrow[r, "\tau"] & k'^a \\ k \arrow[u] \arrow[ur] & \end{tikzcd}$$

推论　任一个域k的代数闭包在k—同构下是唯一的，即对于k的两个的代数闭包K_1与K_2,都有域同构：

$$\sigma : K_1 \to K_2,$$

使得$\sigma|_k = id$.(即K_1与K_2是k—同构的)

命题　域F的任一个有限乘法子群都是循环的.

证明. 设$G \subset F^*$是一个有限群，且$|G| > 1$，由有限$Able$群结构定理可知，只需证G是一个P群的情形.（P是素数）此时记$|G| = p^n (n \in Z_{\geq 1})$,令$S = \{m \in Z_{\geq 0}$:存在$a \in G$,使得$\sigma(a) = p^m\}$,则$S \neq \phi$,且对于任意$m \in S$,有$m \leq n$.由S是一个有限集合，故S中有最大整数，记之为r,且有$b \in G$,使得$\circ(b) = p^r$,显然$r \leq n$.

于是对任意的$\alpha \in G$,记$\circ(\alpha) = p^s, s \in Z_{\geq 0}$,则$s \leq r$.于是就有$\alpha^{p^r} = (\alpha^{p^s})^{p^{r-s}} = 1^{p^{r-s}} = 1$.因此，$G$中元素均是$X^{p^r} - 1$的根.

因为$G \subset F^*$,而$X^{p^r} - 1$在F中至多有p^r个根，可以推出$|G| \leq p^r$,即$p^n \leq p^r \leq p^n$,从而得到$r = n$,进而得到$\circ(b) = p^n$.

故$G =< b >$.　□

分裂域　正规扩张

设k是一个域，$f(x) \in k[X]$,且$n =, degf > 0$,取k^a为k的一个代数闭包，则$f(x)$在k^a中可完全分解为：

$$f(x) = a(x - \alpha_1) + \cdots + (x - \alpha_n)$$

令$K = k(\alpha_1 \cdots \alpha_n) \subset k^a$.

事实:上述K是k^a/k中使得$f(x)$在其中可完全分解的最小中间域.若$\alpha_1 \cdots \alpha_n \in K'$,则可以得到$K = k(\alpha_1 \cdots \alpha_n) \subset K'$,称$K$为$f$在$k$上的一个分裂域.我们有：

$$K = k(\alpha_1 \cdots \alpha_n) \to K^\sigma = k\{\sigma(\alpha_1) \cdots \sigma(\alpha_n)\}$$

从而我们有对应：

$$\{\alpha_1\cdots\alpha_n\}\longmapsto\{\sigma(\alpha_1)\cdots\sigma(\alpha_n)\}$$

从而我们有下图：

$$\begin{tikzcd}
K=k(\alpha_1\cdots\alpha_n) \arrow[rr, "\sigma"] & & K^\sigma=k\{\sigma(\alpha_1)\cdots\sigma(\alpha_n)\} \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

分裂域是在k—同构意义下是唯一的.

对于两个多项式的分裂域，$f_1,f_2\in k(x)$,f_1的根为$\alpha_1\cdots\alpha_m$；f_2的根为$\beta_1\cdots\beta_n$；我们得到$E_1=k(\alpha_1\cdots\alpha_m),E_2=k(\beta_1\cdots\beta_n)$,则有：

$$\begin{aligned}E&=E_1E_2=E_1(E_2)=E_2(E_1)\\&=k(\alpha_1\cdots\alpha_m)k(\beta_1\cdots\beta_n)\\&=k(\alpha_1\cdots\alpha_m\beta_1\cdots\beta_n)\end{aligned}$$

定义(分裂域) 设K是一个域,$\{f_i\}_{i\in I}$是k上的一簇多项式，取定k^a为k的一个代数闭包,$\{f_i\}_{i\in I}$在k^a/k中的分裂域是指K:$k\subset K\subset k^a$,且满足：

（1）每个$f_1,(i=1\cdots n)$在K中完全分解；

（2）对k^a/k的任一个中间域E,如果k^a/k在E中完全分解，有$K\subset E$；

具体地,令$S=\{\alpha\in k^a$:存在$i\in I$,使得$f_i(\alpha)=0$,则有$K=k(S)$.注意到：分裂域是在k—同构意义下是唯一的.

考虑不可约多项式，设k是一个域,$f(x)\in k[X]$,且f在k上不可约，从而有：

$$f(x)=a(x-\alpha_1)+\cdots+(x-\alpha_n)$$

$\alpha_1\cdots\alpha_n\in k^a$,令$S=\{\alpha_1\cdots\alpha_n\}$, 我们有映射：

$$\sigma:k(\alpha)\to k^a\quad\alpha\longmapsto\sigma(\alpha),$$

由$f(\sigma(\alpha))=0$,可知：$\sigma(\alpha)\in\{\alpha_1\cdots\alpha_n\}$我们有下图：

$$\begin{tikzcd}
k(\alpha) \arrow[r, "\sigma"] & K^a \\
k \arrow[u] \arrow[ur, "id"'] &
\end{tikzcd}$$

进而我们考虑下图：

$$\begin{tikzcd}
K=k(\alpha_1\cdots\alpha_n) \arrow[r] & k^a \\
k(\alpha) \arrow[u] \arrow[ur] & \\
k \arrow[u] \arrow[uur] &
\end{tikzcd}$$

取$K=k(\alpha_1\cdots\alpha_n)$为$f$在$k^a/k$中的分裂域，对于映射

$$\tau:K\to\tau(K)\quad \tau|_k=id,$$

我们有:$f^\tau(x)=f(x)$,推出$0=\tau(0)=\tau(f(\alpha_i))=f(\tau(\alpha_i))$,从而推出$\tau(\alpha_i)\in S$,进而有$\tau(K)\subset k(S)=K$,即$\tau(K)=K$.

又由于K/k是代数扩张，故τ是满的，从而$\tau\in Aut_k(K)$为K到自身的一个k-嵌入. 即有下图：

$$\tau:K\to K\quad \tau|_k=id.$$

定义（正规扩张）　设K/k是一个域的代数扩张，k^a为k的一个代数闭包,如果K到自身的k-自同构，则称K/k是一个正规扩张.

定义　设k是一个域, $\alpha\beta\in k^a$.如果在k上的不可约多项式，$P(x)\in k[X]$,使得$P(\alpha)=P(\beta)=0$,则称α与β是k-共轭的.(极小多项式相同，即多项式的根之间为k-共轭元.)

定义　$\alpha\sim\beta\in k^a\iff$ 极小多项式相同,(固定一个代数闭包的情形下，给一个$\alpha\in k$,则就对应于一个极小多项式.)则"$\sim$"是一个等价关系.

$k^a/\sim=\{k-$共轭类$\}$

1.3　正规扩张　可分扩张

定理　设K/k是一个域的代数扩张，k^a是k的包含K一个代数闭包,则下列陈述等价：

（1）K到k^a的任一个k-嵌入均是K的一个k-自同构，即$\sigma(K)=K$.

（2）$k[X]$中的任一不可约多项式f如果在K中有一个根，则f在K中完全分解.（即K包含$\alpha\in k^a$的同时也包含α的在k^a中的全部共轭元.）

（3）K是k上一簇多项式在k上的分裂域.

证明.（1）$\Longrightarrow$（2）证明思路如下图：

$$\begin{tikzcd}
K \arrow[r, "\tau"] & k^a \\
k(\alpha) \arrow[u] \arrow[r] \arrow[ur, "\sigma"] & k(\beta) \arrow[u] \\
k \arrow[u] \arrow[ur, "id"] &
\end{tikzcd}$$

设$f(x)\in k[X]$为k上的一个不可约多项式，且有$\alpha\in K$.使得$f(\alpha)=0$

下证：$f(x)$在k^a中的任一个根β都必在K中.

事实上，对于上述的$\beta\in k^a$,令

$$\sigma:k(\alpha)\to k^a\quad \alpha\longmapsto\beta,$$

则$\sigma: k(\alpha) \to k^a$是一个$k$-嵌入.

由于$K/k(\alpha)$是代数的，故σ可延拓为

$$\tau: K \to k^a,$$

即$\tau|_{k(\alpha)} = \sigma$.

显然τ也是一个k-嵌入，由所设，$\tau(K) = K$.特别地，$\beta = \sigma(\alpha) = \tau(\alpha) \in K$,故$K$包含$\alpha$的全部共轭元.

（2）$\Longrightarrow$（3）取$S = \{P(x) \in k[X], P(x)$是某个$\alpha \in K$在$k$上的不可约多项式$\}$,则$K$是$S$在$k$上的分裂域.

（3）$\Longrightarrow$（1）设K是多项式簇$\{f_i\}_{i \in I} \subset k[X]$在$k$上的分裂域.(其中$deg f_i > 0$)

任取K到k^a的任一个k-嵌入如下：

$$\begin{tikzcd} K \arrow[rr, "\sigma"] & & k^a \\ & k \arrow[ul] \arrow[ur, "id"'] & \end{tikzcd}$$

下证$\sigma(K) = K$.

下面只需证：$\sigma(K) \subset K$.

为此任取$\alpha \in K$，由所设，有$f_i \subset k[X]$，使得$f_i(\alpha) = 0$,从而有$\sigma(f_i(\alpha)) = 0$,即$f_i(\sigma(\alpha)) = 0 \Rightarrow \sigma(\alpha) \in K \Rightarrow \sigma(\alpha) \subset K$.故$\sigma(K) = K, \sigma$是$K \to K$的自同构. □

定理　（1）设K/k是一个域的正规扩张，对k的任一个扩域F，则FK/K也是正规的；

（2）设$k \subset E \subset K$,如果K/k是正规的，则K/E也是正规的；

（3）设K_1, K_2均是k的代数扩张，且$K_1, K_2 \subset L$，如果$K_1/k, K_2/k$均是正规的，则K_1K_2/k, $K_1 \cap K_2/k$均是正规的.

可分扩张　E/F是一个代数扩张，L, L'是F的两个代数封闭域，则有下图：

$$\begin{tikzcd} L' & E \arrow[l, "\tau^*"'] \arrow[r, "\sigma^*"] & L \\ & F \arrow[ul, "\tau"] \arrow[u] \arrow[ur, "\sigma"'] & \end{tikzcd}$$

设$\sigma: F \to L$是一个嵌入，$\tau: F \to L'$,令：$S(\sigma) = \{\sigma^*: E \to L$嵌入，且$\sigma^*|_F = \sigma\}$,$S(\tau) = \{\tau^*: E \to L'$嵌入，且$\tau^*|_F = \tau\}$.

事实：

$$S(\sigma) \longleftrightarrow S(\tau) \quad \sigma^* \longmapsto \tau^*$$

不妨令$\tau^* = \lambda \circ \sigma^*$，则有下图：

$$
\begin{tikzcd}
L' & & L \arrow[ll, "\lambda"'] \\
& E \arrow[ul, "\tau^*"'] \arrow[ur, "\sigma^*"] & \\
\tau(F) \arrow[uu] & F \arrow[l] \arrow[r] \arrow[uul, "\tau"] \arrow[uur, "\sigma"'] & \sigma(F) \arrow[uu]
\end{tikzcd}
$$

其中λ是$\tau \circ \sigma^{-1} : \sigma(F) \to L'$到$L'$上的延拓.

任取$\alpha \in F$,$\tau^*(\alpha) = \lambda\sigma^*(\alpha) = \lambda\sigma(\alpha) = \tau \circ \sigma^{-1}\sigma(\alpha) = \tau(\alpha)$,故$\tau^*|_F = \tau$.

定义　设E/F是一个代数扩张，F^a是F的一个代数闭包，任取一个F-嵌入$\sigma : F \to F^a$,令$S(\sigma) = \{\sigma^* : E \to F^a$嵌入，且$\sigma^*|_F = \sigma\}$.定义$E/F$的可分次数为$[E : F]_s \overset{\triangle}{=} \#\ S(\sigma)$.特别地$\sigma = id$

$$
\begin{aligned}
[E : F]_s &= \#S(id) \\
&= \#\{\sigma^* : E \to F^*, \sigma^*|_F = id\}
\end{aligned}
$$

即为$\#\{E$到F^*的全部F-嵌入$\}$.

例如：$E = F(\alpha)$为一个单代数扩张，$\alpha \in F^a$,则$[E : F]_s = \alpha$在F上的极小多项式全部互异根（根在F^a中）的个数.即有：

$$
\begin{tikzcd}
F(\alpha) \arrow[rr, "\sigma"] & & F^* \\
& F \arrow[ul] \arrow[ur, "id"'] &
\end{tikzcd}
$$

定理　设有域扩张$k \subset F \subset E$,则有$[E : k]_s = [E : F]_s[F : k]_s$.

证明. 令$S_E = \{\tau : E \to k^a$嵌入，且$\tau|_k = id\}$,$S_F = \{\sigma : F \to k^a$嵌入，且$\sigma|_k = id\}$,即有：

$$
\begin{tikzcd}
E \arrow[r, "\tau"] & k^a \\
F \arrow[u] \arrow[ur, "\sigma_i"] & \\
k \arrow[u] \arrow[uur, "id"'] &
\end{tikzcd}
$$

设$S_F = \{\sigma_1 \cdots \sigma_m\}$,对每一个$\sigma_i \in S_F$,记$S_{E/F}(\sigma_i) = \{\tau : E \to k^a$嵌入，且$\tau|_F = \sigma_i\}$,则$\#S_{E/F}(\sigma_i) = [E : F]_s$,且有$S_E \subset \{\tau : E \to k^a$嵌入，且$\tau|_F = \sigma_i$,对每个$i \in \{1 \cdots n\}\} \overset{\triangle}{=} T$

任取$\tau \in S_E$,则$\tau|_F$是F 到k^a的一个k-嵌入，$\tau|_F = \sigma_i$,对某个$i \in \{1 \cdots n\}$,从而得到$S_E \subset T$,因此$S_E = T$.

故我们得到：$[E : k]_s = \#S_E = \#T = m\#S_{E/F}(\sigma_i) = [E : F]_s[F : k]_s$.　□

定理　设K/k是一个域的有限扩张，则$[E : k]_s \leq [E : k]$.(即可分次数≤扩张次数)

证明. 由所设，$K=k(\alpha_1\cdots\alpha_n)$,其中$\alpha_1\cdots\alpha_n\in K$.于是有：

$$k\subset k(\alpha_1)\subset k(\alpha_1,\alpha_2)\subset\cdots\subset k(\alpha_1\cdots\alpha_n)=K,$$

其中 $k(\alpha_1\cdots\alpha_i)=k(\alpha_1\cdots\alpha_{i-1})(\alpha_i)$.

由前面的结果有：

$$\begin{aligned}[k(\alpha_1\cdots\alpha_i):k(\alpha_1\cdots\alpha_{i-1})]_s&=[k(\alpha_1\cdots\alpha_{i-1})(\alpha_i):k(\alpha_1\cdots\alpha_{i-1})]_s\\&\le[k(\alpha_1\cdots\alpha_i):k(\alpha_1\cdots\alpha_{i-1})].\end{aligned}$$

于是我们得到：

$$\begin{aligned}[K:k]_s&=[K:k(\alpha_1\cdots\alpha_{n-1})]_s\cdots[k(\alpha_1):k]_s\\&\le[K:k(\alpha_1\cdots\alpha_{n-1})]\cdots[k(\alpha_1):k]\\&=[K:k].\end{aligned}$$

□

命题　设$K=k(\alpha)$是k的单代数扩张，则K/k是可分的$\Longleftrightarrow$ α是可分代数元

证明. $[K:k]_s=[k(\alpha):k]_s=P_\alpha(x)$在$k^a$中互异根的个数.

故：K/k可分$\Longleftrightarrow$ $[K:k]_s=[K:k]=degP_\alpha(x)$=$P_\alpha(x)$在$k^a$中互异根的个数$\Longleftrightarrow$ $P_\alpha(x)$在k^a中无重根$\Longleftrightarrow$ $P_\alpha(x)$为可分的$\Longleftrightarrow$ α为k上的可分代数元. □

定义　设k是一个域，k_a是k的一个代数闭包，$\alpha\in k^a$,称α为k上的可分代数元.如果α在k上的极小多项式是可分的.

注：多项式可分$\Longleftrightarrow$它无重根；

命题　域的代数扩张K/k是可分的$\Longleftrightarrow$ K中的每个元素均是k上的可分代数元.特别地，对于有限扩张K/k有：K/k可分$\Longleftrightarrow$ $K=k(\alpha_1\cdots\alpha_n),\alpha_1\cdots\alpha_n\in K$为$k$上的可分代数元.

正规闭包

回忆一下正规扩张，$K/k,K=k(\alpha),\alpha\in K$单代数扩张，$\alpha$在$k$上的极小多项式为：

$$P_\alpha(x)=(x-\alpha_1)\cdots(x-\alpha_n),\quad\alpha_1=\alpha\in K$$

记E为$P_\alpha(x)$在k上的分裂域（$\subset k^a$）,则E是k^a中包含$k(\alpha)$的最小正规扩域,称E是$k(\alpha)/k$的一个正规闭包.

由于K/k是正规扩张，从而在K上完全分裂，$\tau(\alpha)\in E,E/k$正规，$\tau|_K=\sigma\Rightarrow\tau(\alpha)=\sigma(\alpha)=\alpha_i$,对某个$i\in\{1\cdots n\}$,即有下图：

$$\begin{tikzcd} E \arrow[r, "\tau"] & k^a \\ K=k(\alpha) \arrow[u] \arrow[ur, "\sigma"] & \\ k \arrow[u] \arrow[uur, "id"'] & \end{tikzcd}$$

一般地，任一个代数扩张K/k在k^a中均有一个正规闭包k',即：（1）k'/k是正规的（$k' \subset k^a$）;(2)设$E \subset k^a, E/k$是正规的，且$E \supset K$,则$E \supset K'$.

定理　本原元（*primtive　element*）

设K/k是域的有限扩张，则：K是k的单代数扩张$\Longleftrightarrow$ K/k只有有限个中间域.特别地,域的有限可分扩张必是单代数扩张，此时$K = k(\alpha), \alpha$称为K/k的一个本原元.

证明. (1)"$\Leftarrow$"(充分性)若k是有限域，则由K/k是有限扩张$\Rightarrow$ K是有限域，则K^*是循环群，记$K^* =< \alpha >, \alpha \in K, \alpha \neq \{0\}$,从而推出$K = k(\alpha)$.则$K$为单扩张.

若k是无限域，设K/k只有有限多个中间域，由于K/k是有限扩张，不妨$K = k(\alpha, \beta)$.对任意的$c \in k^*$,有中间域:

$$E_c = k(\alpha + c\beta),$$

由所设K/k只有有限个中间域，但$c \in k^*$是无限的，从而有$c_1, c_2 \in k^*, c_1 \neq c_2$,使得$k(\alpha + c_1\beta) = k(\alpha + c_2\beta) \overset{\triangle}{=} E$.于是$\alpha + c_1\beta, \alpha + c_2\beta \in E$,从而推出$(c_1 - c_2)\beta \in E$.又由于$c_1 \neq c_2 \Rightarrow c_1 - c_2 \neq 0 \Rightarrow \frac{1}{(c_1-c_2)}(c_1 - c_2)\beta \in E$.即$\beta \in E$,进而我们有$\alpha = (\alpha + c_1\beta) - c_1\beta \in E$.即

$$K = k(\alpha, \beta) \subset E \subset K,$$

故$K = E = k(\alpha + c\beta)$.

"$\Rightarrow$"(必要性)设$K = k(\alpha)$是k的一个单代数扩张，设$P_\alpha(x)$为α在k上的极小多项式，记$S = \{$中间域$E : k \subset E \subset K\}$,对每个$E \in S, \alpha$也是$E$上的代数元，记$\alpha$在$E$上的极小多项式为$P_{\alpha,E}(x)$，则显然有$P_{\alpha,E}(x)|P_\alpha(x)$,(因为$P_\alpha(x)$也是$E$上的多项式，且$P_\alpha(\alpha) = 0$.)

记$T = \{P_{\alpha,E}(x) : E \in S\}$,则$\#T < +\infty$.令：

$$\phi : S \to T \quad E \mapsto P_{\alpha,E}(x).$$

下证：ϕ是一个单射.

对于$P_{\alpha,E}(x) \in T, (E \in S)$,令$F$为$k$上添加$P_{\alpha,E}(x)$的全部系数所得的扩域，则$k \subset F \subset E$.此时$P_{\alpha,E}(x) \in F(X)$,且为$F$上不可约多项式.

又显然$K = k(\alpha) = E(\alpha) = F(\alpha) \Rightarrow [K : E] = degP_{\alpha,E}(x); [K : F] = degP_{\alpha,E}(x)$,从而推出$[K : E] = [K : F]$,又由于$F \subset E$,即可得到$E = F$.由此可知$\phi$是一个单射.

故有$\#S \leq \#T < +\infty$,即S是一个有限集，从而K/k中的中间域只有有限个. □

（2）下证：域的有限可分扩张必是单代数扩张，$\#k = +\infty$.

证明. 证法一（书上），设$[K : k] = n$,不妨设$K = k(\alpha, \beta), (\alpha, \beta \in K)$,由所设$[K : k]_s = n$,取$k$的代数闭包$k^a$,使得$k^a \subset K$.此时$K$到$k^a$共有$n$个不同的$k$-嵌入$\sigma_1 \cdots \sigma_n$.即：

$$\begin{tikzcd} K \arrow[r, "\sigma_i"] & k^a \\ k \arrow[u] \arrow[ur, "id"'] & \end{tikzcd}$$

令$f(x) = \prod_{1 \leq i \neq j \leq n}\{(\sigma_i\alpha + x\sigma_i\beta) - (\sigma_j\alpha + x\sigma_j\beta)\}$,则$f(x) \neq 0$.(不是零多项式)

假若不然，则有上述$i,j,i\neq j$,使得$\sigma_i\alpha+x\sigma_i\beta=\sigma_j\alpha+x\sigma_j\beta$,即满足$\sigma_i\alpha=\sigma_j\alpha,\sigma_i\beta=\sigma_j\beta$,从而对于$\sigma_i,\sigma_j:K\to k^a$,我们得到：$\sigma_i=\sigma_j$,与所设矛盾，故$f(x)\neq 0$.

设$f(x)$在k^a中至多有有限个根（零点），故在k中也只有有限个零点.但$\#k=+\infty$.，从而存在$c\in k^*$,使得$f(c)\neq 0$.于是$(\sigma_i\alpha+c\sigma_i\beta)-(\sigma_j\alpha+c\sigma_j\beta)\neq 0$,也即$\sigma_i\alpha+c\sigma_i\beta\neq\sigma_j\alpha+c\sigma_j\beta,(i\neq j)$.注意到$\sigma_i\alpha+c\sigma_i\beta=\sigma_i(\alpha+c\beta),(i=1\cdots n)$,而$\sigma_i$是$K$到$k^a$的$k$-嵌入，故$\sigma_i(\alpha+c\beta)$均是$\alpha+c\beta$的$k$-共轭元，从而推出$[k(\alpha+c\beta):k]_s\geq n$.

另一方面，$k(\alpha+c\beta)\subset K$,即有：

$$n=[K:k]=[K;k]_s\geq[k(\alpha+c\beta):k]=[k(\alpha+c\beta):k]_s\geq n,$$

故有，$K=k(\alpha+c\beta)$. □

证明. 证法二（构造法）把满足上面条件的c找出

不妨设$K=k(\alpha,\beta)$,取定k的一个代数闭包k^a,使得$k^a\subset K$,分别设α,β在k^a中的全部共轭元为$\alpha=\alpha_1\cdots\alpha_m,\beta=\beta_1\cdots\beta_n$,令

$$S=\{\frac{\alpha_i-\alpha_j}{\beta_l-\beta_k}|1\leq i\neq j\leq m,1\leq l\neq k\leq n\},$$

显然S是一个有限集.

由所设，k是一个无限域，故有$c\in k^*$,使得$c\notin S$,又设$f(x),g(x)\in k[X]$是α,β在k上的极小多项式，记$r=\alpha+c\beta=\alpha_1+c\beta_1\in K$,令$h(x)=f(r-cx)$,则$h(x)\in k[r][X]\subset K[X]$,则$h(\beta_1)=f(r-c\beta_1)=f(\alpha_1)=0$,可以推出$\beta_1$是$h(x)$的一个根，又$\beta_1$也是$g(x)$的一个根，而$h(\beta_j)\neq 0,(j=2\cdots n)$,若不然，$h(\beta_j)=0\Rightarrow f(r-c\beta_j)=0$,而$f(x)$的根为$\alpha_1\cdots\alpha_m$,进而有$r-c\beta_j=\alpha_i$,对某个$i=1\cdots m$,即

$$\alpha_1+c\beta_1-c\beta_j=\alpha_i\Rightarrow\alpha_1-\alpha_i=c(\beta_j-\beta_1)\Rightarrow c=\frac{\alpha_1-\alpha_i}{\beta_j-\beta_1}\Rightarrow c\in S,$$

矛盾！

由于$g(x),h(x)\in k[r][X]$,且由上述讨论可知，$g(x),h(x)$的最大公因式为$(x-\beta_1)$,即$(g(x),h(x))=x-\beta_1$,由辗转相除法可知：$x-\beta_1\in k[r][X]\Rightarrow\beta=\beta_1\in k[r]$,又由于$r=\alpha+c\beta\Rightarrow\alpha=r-c\beta\in k[r]\Rightarrow k(\alpha,\beta)=K\subset k[r]\subset K$,故

$$K=k(r)=k(\alpha,\beta).$$

□

例如：$K=Q(\sqrt{-1},\sqrt{-2})=Q(r)$,求$r$.

解：由于$K=Q(\sqrt{-1})(\sqrt{-2})$,而$\sqrt{-1}$的$Q$-共轭元为$\pm\sqrt{-1}$,$\sqrt{2}$的$Q$-共轭元为$\pm\sqrt{2}$,$[Q(\sqrt{-1}):Q]=2,[Q(\sqrt{-1})(\sqrt{-2}):Q(\sqrt{-1})]=2$.(这是由于$\sqrt{-2}\notin Q(\sqrt{-1})$,如若不然$\sqrt{-2}=a+b\sqrt{-1}$,$a,b\in Q\Rightarrow 2=a^2-b^2+2ab\sqrt{-1}$.左边属于$Q$,右边属于$C$,但不属于$Q$,从而矛盾,故$\sqrt{-2}\notin Q(\sqrt{-1})$,$\Rightarrow[Q(\sqrt{-1})(\sqrt{-2}):Q(\sqrt{-1})]=2$.)故有$[K:Q]=4$.

K/Q是有限可分，故有本原元,从而有：

$$S = \{\pm\frac{\sqrt{-1}-(-\sqrt{-1})}{\sqrt{2}-(-\sqrt{2})}\} = \{\pm\frac{\sqrt{-1}}{\sqrt{2}}\}.$$

取$c = 1$即满足条件.即有：

$$Q(\sqrt{-1})(\sqrt{-2}) = Q(\sqrt{-1}+\sqrt{2}).$$

1.4 有限域

设k是一个有限域，此时k的特征$char(k) = p$,(p为素数)即为p元域，$F_p \subset k$.换言之F_p是k的素子域,显然，k/F_p是有限扩张（即有限域的有限扩张）.

不妨设$[k;F_p] = n, \Rightarrow k = |F_p|^n = p^n$,记$k = F_q, F_q = p^n$.取$k$的一个代数闭包$k^a$,则$G = F_q^*$是一个$q-1$阶循环群，可以推出存在$\alpha \in F_q^*$,有$\alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha$(任意$\alpha \in F_q$).即$\alpha$是多项式$x^{q-1}-1$在$k^a$中的一个根.

$k = F_q \subset \{x^q - x$在$k^a$中的根$\}. \Rightarrow q = \#k \leq \#\{x^q - x$在$k^a$中的根$\} \leq q$,从而有$k = \{x^q - x$在$k^a$中的根$\}$,且$x^q - x$在$k$中是可分的，由于$f(x) = x^q - x \Rightarrow f'(x) = qx^{q-1} - 1 = -1, (f(x), f'(x)) = 1$.

设K, k均为有限域，且$k \subset K$,记$char(k) = p$,(p为素数)，由前述讨论可知：$\#k = p^m, \#K = p^n, (m, n \in Z_{\geq 1})$.记$[K;k] = r \in Z_{\geq 1}$,则$p^n = |K| = |k|^r = (p^m)^r \Rightarrow n = mr \Rightarrow m|n$.即若有限域有包含关系，其指数定有整除关系.

事实上，设K, k均为有限域，且$k \subset K$，则K/k是一个可分的单代数扩张.由于$|k| = p^m, |K| = p^n. \Rightarrow k = \{x^{p^m} - x$在$k^a$中的全部根$\} = x^{p^m} - x$在$F_q$上的分裂域,$\Rightarrow k/F_q$也是正规扩张$\Rightarrow K/k$也是正规扩张，即有：

$$\begin{tikzcd}
K \arrow[r] & k^a \\
k \arrow[u] \arrow[ur, "\sigma"] & \\
F_q \arrow[u] \arrow[uur, "id"'] &
\end{tikzcd}$$

设$char(k) = p$,(p为素数).令：

$$\phi : k \to k \quad \alpha \mapsto \alpha^p,$$

则$\phi \in Aut_{F_p}(k)$是k到自身的一个自同构.

由于任意$\alpha, \beta \in k$,有：

$$\phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \phi(\alpha) + \phi(\beta),$$

且满足：

$$\phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \phi(\alpha)\phi(\beta),$$

ϕ是一个域同态，又由于其是$x^{p^m} - x$在F_p上的分裂域，ϕ是自同构，即$\phi \in Aut(k)$.

定义：称上述映射$\phi : k \to k$为k上的$Frobenious$自同构，记为$Frob_k$.

事实：ϕ是k到自身的F_p-自同构，任意的$\alpha \in F_p \Rightarrow \phi(\alpha) = \alpha^p = \alpha$.易知$Aut_{F_p}(k)$关于映射的合成是一个群.

首先有$\#Aut_{F_p}(k) = [k : F_p] = m, \phi \in Aut_{F_p}(k) = \{\sigma : \sigma$是$k$到自身的$F_p$-自同构$\}$.任意的$\alpha \in k$,

$$\phi(\alpha) = \alpha^p,$$

$$\phi^2(\alpha) = \phi(\phi(\alpha)) = \phi(\alpha^p) = \phi(\alpha)^p = \alpha^{p^2},$$

即有:

$$\phi^r(\alpha) = \alpha^{p^r},$$

特别地，

$$\phi^m(\alpha) = \alpha^{p^m} = \alpha, (\alpha \in k)$$

即$\phi^m = id. \Rightarrow \circ(\phi)|m$.

又记$\circ(\phi) = r$,则$\phi^r = id$.于是任意的$\alpha \in k$,有$\phi^r = \alpha = id(\alpha) \Rightarrow \alpha^{p^r} = \alpha \Rightarrow k \subset \{x^{p^r} - x$在$k^a$中的全部根$\}$.

进而有$p^m \leq p^r \Rightarrow m \leq r|m \Rightarrow r = \circ(\phi) = m \Rightarrow Aut_{F_p}(k) =< \phi >=< Frob_{F_p} >$.

故$Aut_{F_p}(k)$是由$Frobenious$元生成的m阶循环群.

一般地，对于有限域扩张K/k,$char(k) = p$,(p为素数)，$Aut_k(K) =< Frob_K >=< \phi_K >$.

$$Frob_K : K \to K \quad \alpha \mapsto \alpha^{p^m} = \alpha^{|k|},$$

且有$\circ(\phi_K) = \#Aut_k(K) = [K : k] = \frac{n}{m}$.

故$Aut_k(K)$是一个$[K : k]$阶循环群.

1.5 不可分扩张

设 $K|k$ 是单代数扩张, $K = k(\alpha)$, α在k上极小多项式为$f(x) \in k[x]$. 设$deg(f) = n$,则$\{1, \alpha, \cdots, \alpha^{n-1}\}$ 是K的一组$k-$基,$K = k(\alpha) = k[\alpha]$.

取定k的代数闭包k^a,设$\alpha_1, \cdots, \alpha_m$是$f(x)$在$k^a$中的全部互异根，$\alpha_i$的重数记为$r_i$, 则在$k^a$中，有

$$f(x) = (x - \alpha_1)^{r_1} \cdots (x - \alpha_m)^{r_m},$$

其中$m = [K : k]_s$(可分次数)。K到k^a的$k-$嵌入共有m个，分别记为$\sigma_1, \cdots, \sigma_m$,取定$\alpha = \alpha_1$,不妨设$\sigma_i(\alpha) = \alpha_i$,将$\sigma_i$延拓为$k^a$上的一个$k-$自同构，记之为$\tau_i$,于是有 $\tau_i|_K = \sigma_i$,

$$\tau_i(f(x)) = (x - \tau_i(\alpha_1))^{r_1} \cdots (x - \tau_i(\alpha_m))^{r_m},$$

即

$$\begin{aligned}(x - \alpha_1)^{r_1} \cdots (x - \alpha_i)^{r_i} \cdots (x - \alpha_m)^{r_m} \\ = (x - \alpha_i)^{r_1} \cdots (x - \tau_i(\alpha_m))^{r_m}\end{aligned}$$

由此可得$r_i = r_1(i = 1, \cdots, m)$.即极小多项式的所有根在代数闭包$k^a$中有相同的重数。特征为零的域上不可约多项式无重根.因此若f有重根，则$char(k) = p$，其中p为某一素数。同时注意到由于f有重根，故$(f, f^{'}) \neq 1$,但由于f不可约且 $deg(f^{'}) < deg(f)$,$f^{'}$只能为零，这就说明f是形如$f(x) = g(x^p)$的多项式(其中$g(x) \in k[x]$,且由于$f(x)$为$k[x]$中不可约多项式，$g(x)$也是$k[x]$中不可约多项式.). 于是α^p是$g(x)$的一个根。重复上述过程，最终，我们可以找到最小的整数$r \geq 0$，使得α^{p^r}是$k[x]$中一个可分不可约多项式$h(x)$的根，且

$$f(x) = h(x^{p^r}).$$

设$h(x)$在k^a中的分解为$h(x) = (x - \beta_1)\cdots(x - \beta_s)$, 令$\gamma_i \in k^a(i = 1, \cdots, s)$使得$\gamma_i^{p^r} = \beta_i$, 设$t = r_1 = \cdots = r_m$ 则

$$\begin{aligned} f(x) &= (x - \alpha_1)^t \cdots (x - \alpha_m)^t \\ &= (x^{p^r} - \gamma_1^{p^r}) \cdots (x^{p^r} - \gamma_s^{p^r}) \\ &= (x - \gamma_1)^{p^r} \cdots (x - \gamma_s)^{p^r} \end{aligned}$$

由一元多项式分解的唯一性知$m = s, t = p^r$.
于是

$$f(x) = (x - \alpha_1)^{p^r} \cdots (x - \alpha_s)^{p^r}.$$

由

$$[k(\alpha) : k] = deg(f) = s \cdot p^r = [k(\alpha) : k]_s \cdot p^r$$

知$[k(\alpha) : k]_s | [k(\alpha) : k]$,它们的商$\frac{[k(\alpha):k]}{[k(\alpha):k]_s} = p^r$称为$k(\alpha)|k$的**不可分次数**,记之为$[k(\alpha) : k]_i$.
令$\beta = \alpha^{p^r}$,则$h(\beta) = h(\alpha^{p^r}) = f(\alpha) = 0$,由于$h(x)$是首一不可约多项式，于是$h(x)$是$\beta$在$k[x]$上的极小多项式.因$h(x)$无重根， $[k(\alpha^{p^r}) : k] = [k(\alpha^{p^r}) : k]_s = deg(h(x)) = s$. 由域扩张的次数传递公式知$[k(\alpha) : k(\alpha^{p^r})] = \frac{n}{[k(\alpha^{p^r}):k]} = \frac{n}{s} = p^r$.同样可得到

$$[k(\alpha) : k(\alpha^{p^r})]_s = \frac{[k(\alpha) : k]_s}{[k(\alpha^{p^r}) : k]_s} = \frac{s}{s} = 1.$$

于是$[k(\alpha) : k(\alpha^{p^r})]_i = p^r$. 注意到$k(\alpha) = k(\alpha^{p^r})(\alpha)$,令$a = \alpha^{p^r} \in k(\alpha^{p^r})$, 则$x^{p^r} - a$是$\alpha$在$k(\alpha^{p^r})$上的极小多项式，该极小多项式只有一个根$\alpha$且重数为$p^r$.
定义：设k是域，$char(k) = p > 0$, k^a是k的一个代数闭包，设$\alpha \in k^a$,如果有$r \in \mathbb{Z}_{\geq 0}$使得 $\alpha^{p^r} \in k$,则称α为k上的一个**纯不可分元**。
命题：设K/k是一个代数扩张，$char(k) = p > 0$,则下列陈述等价：
(i)$[K : k]_s = 1$.
(ii)K中任一元素均是k上纯不可分元。
(iii)对$\forall \alpha \in K$, α在k上的极小多项式均形如$x^{p^r} - a, a \in k, r \in \mathbb{Z}_{\geq 0}$.
(iv)K是在k上添加若干个纯不可分元生成。
称满足上述命题中等价条件的域扩张K/k为一个**纯不可分扩张**。

证明. $(i) \Rightarrow (ii)$任取$\alpha \in K$,由$[k(\alpha):k]_s|[K:k]_s = 1$知 $[k(\alpha):k]_s = 1$,由此知α在k上极小多项式必形如 $x^{p^r} - a \in k[x]$,由此$\alpha^{p^r} \in k$,即α是k上纯不可分元。
$(ii) \Rightarrow (iii)$设$\alpha \in K$是k上的纯不可分元，即有$\exists r \in \mathbb{Z}_{\geq 0}, x^{p^r} - a \in k[x]$,使得$\alpha^{p^r} = a \in k$,不妨设$r$是满足该条件的最小的非负整数，令$f(x) = Irr(\alpha, k, x)$为$\alpha$在$k$上的不可约多项式(极小多项式)，则$f(x)|x^{p^r} - a$. 由于

$$x^{p^r} - a = x^{p^r} - \alpha^{p^r} = (x-\alpha)^{p^r},$$

$f(x) = (x-\alpha)^m$,其中$m = p^s t \leq p^r, s \leq r, p \nmid t$.对$f(x)$进行二项式展开，

$$\begin{aligned} f(x) &= (x-\alpha)^{p^s t} \\ &= (x^{p^s} - \alpha^{p^s})^t \\ &= x^{p^s t} - t \cdot \alpha^{p^s} x^{p^s(t-1)} + \cdots + (-1)^t \alpha^{p^s t} \in k[x], \end{aligned}$$

因此$t \cdot \alpha^{p^s} \in k$,由$p \nmid t$,而$char(k) = p$得到$t$在$k$中可逆，于是$\alpha^{p^s} = b \in k$.由$r$的极小性得到$r \leq s$.又由上面知$s \leq r$,因此$r = s, t = 1$.即 $f(x) = x^{p^r} - a$.即$x^{p^r} - a$是α在k上的不可约多项式。
$(iii) \Rightarrow (iv)$显然地.
$(iv) \Rightarrow (i)$任取K到k的某一代数闭包$\bar{F}$的 $k-$嵌入，设K由在k上纯不可分元$\{\alpha_i\}_{i\in I}$生成，则

$$f_i(X) = Irr(\alpha_i, k, X)$$

是α_i在k上的极小多项式，由于α_i是纯不可分元, 存在$r \in \mathbb{Z}_{\geq 0}, a \in k$使得$\alpha_i^{p^r} = a_i \in k$，因此$f_i(X)|(X^{p^r} - a_i)$,即$f(X)$只有唯一根$\alpha_i$,任意$K$到$\bar{F}$的$k$嵌入$\tau$把元素映到其共轭元，但任意$\alpha_i$的共轭元只有自身,于是$\tau$是恒等映射,即$[K:k]_s = 1$. □

命题：设$K|k$是一个代数扩张，K_0为K中所有在k上可分的代数扩张的合，则$K_0|k$是可分扩张，$K|K_0$是纯不可分的。也称K_0为k在K中的可分闭包。

证明. $K|k$的可分子扩张的复合仍是可分扩张，于是$K_0|k$是可分扩张；若$char(k) = 0$,则显然$K_0 = K$,若$char(k) = p$,则任给$\alpha \in K$,存在非负整数n使得α^{p^n}在k上可分的，于是$\alpha^{p^n} \in K_0$,即$K|K_0$是纯不可分扩张。 □

推论:对于上述命题中$K|k$为有限扩张的情形,有

$$[K:k]_s = [K_0:k],$$
$$[K:k]_i = [K:K_0].$$

证明.

$$\begin{aligned} [K:k]_s &= [K:K_0]_s \cdot [K_0:k]_s \\ &= 1 \cdot [K_0:k]_s \\ &= [K_0:k]. \end{aligned}$$

$$\begin{aligned}[K:k]_i &= [K:K_0]_i\cdot[K_0:k]_i\\ &= [K:K_0]_i\cdot 1\\ &= [K:K_0].\end{aligned}$$

□

推论:设$K|k$是域的正规扩张，K_0是k在K中的可分闭包，则$K_0|k$也是正规扩张。

证明. 设k^a是k的一个代数闭包，任取K_0到k^a的一个$k-$嵌入σ,下面证明$\sigma(K_0)=K_0$,从而$K^0|k$是正规扩张.

σ可延拓到K上，记为$\tau:K\to k^a$.由于$K|k$是正规扩张，$\tau(K)=K$.任取$\alpha\in K_0$, α在k上极小多项式$P_\alpha(X)\in k[X]$无重根,而$\tau(\alpha)=\sigma(\alpha)$在$k$上极小多项式也是$P_\alpha(X)$，于是$\tau(\alpha)$在$k$上也可分，从而$\tau(\alpha)\in K_0$,即$\tau(K_0)\subseteq K_0\Rightarrow\sigma(K_0)=K_0$. □

推论:设$E|k$是域的一个有限扩张，$p=char(k)>0$,若$E^p\cdot k=E$,则$E|k$是可分的。反之，如果$E|k$是可分，则$E^{p^r}k=E(\forall r\in\mathbb{Z}_{\geq 1})$.

证明. $\Rightarrow$:设E_0是k在E中的极大可分扩张，$E|k$是有限扩张，因此对$\forall\alpha\in E$,存在固定的$m\in\mathbb{Z}_{\geq 1}$使得$\alpha^{p^m}\in E_0$,于是$E^{p^m}\subseteq E_0$.

另一方面，

$$\begin{aligned}&E^pk=E\\ &\quad\Rightarrow E^p=(E^pk)^p=E^{p^2}k^p\\ &\quad\Rightarrow E^{p^2}k^{p+1}=E^pk=E\\ &\quad\Rightarrow E^{p^2}k\supseteq E^{p^2}k^{p+1}=E\supseteq E^{p^2}k\\ &\quad\Rightarrow E=E^{p^2}k\end{aligned}$$

如此归纳下去便得到$E=E^{p^n}k(n\in\mathbb{Z}_{\geq 1})$, 但$E^{p^m}k\subseteq E_0k=E_0$,于是$E\subseteq E_0\subseteq E$,即$E_0=E$, $E|k$是可分的。

$\Leftarrow$:设$E|k$可分，则$E|E^pk$是可分.又对任意$\alpha\in E$,有$\alpha^p\in E^p\subseteq E^pk$，于是$E|E^pk$是纯不可分的.故$E=E^pk$.由上面证明可得对任意$r\in\mathbb{Z}_{\geq 1}, E^{p^r}\cdot k=E$. □

命题：设$K|k$是域的一个正规扩张，令$G=Aut_k(K)$是K到自身的$k-$自同构，又记

$$K^G=\{\alpha\in K|\sigma(\alpha)=\alpha,\forall\sigma\in G\}.$$

则K^G是$K|k$的中间域，且$K^G|k$是纯不可分的，$K|K^G$是可分的。又设K_0是k在K中的可分闭包，则$K_0K^G=K, K_0\cap K^G=k$.

证明. 任取$\sigma \in Aut_k(K), \sigma|_k = id$,于是$k \subseteq K^G$,即$K^G$是$K|k$的中间域。

(1)下证$K^G|k$是纯不可分的。

为此，任取$\alpha \in K^G$,取定k的一个代数闭包k^a，使得$k^a \supseteq k$. 任取$k(\alpha)$到k^a的$k-$嵌入$\sigma : k(\alpha) \to k^a$，将$\sigma$延拓到$K$上，记之为$\tau : K \to k^a$.由所设$K|k$是正规扩张，则$\tau(K) = K$.即$\tau$是一个$K$到自身的$k-$嵌入，于是$\tau \in G$, $\sigma(\alpha) = \tau(\alpha) = \alpha(\forall \alpha \in K^G)$. 这就说明$\sigma = id$,即$k(\alpha)$到自身的$k-$嵌入只有唯一的恒等映射。从而$[k(\alpha) : k]_s = 1$，$\alpha$是$k$上的纯不可分元，令$\alpha$跑遍$K^G$可得$K^G|k$是纯不可分扩张。

(2)证明$K|K^G$是可分的，方法用$Serge\ Lang : Algebra.P_{264}$Artin定理的证明。

(3)若K_0是k在K中的可分闭包，则$K_0|k$是可分的，于是 $K_0 \cap K^G|k$是可分的，又由于$K^G|k$是纯不可分的，于是 $K_0 \cap K^G|k$是纯不可分的.综上，$K_0 \cap K^G = k$.

(4)由$K|K^G$是可分的，$K|(K^G \cdot K_0)$也是可分的，又因 K_0是k在K中的可分闭包，故$K|(K^G K_0)$是纯不可分的，于是 $K = K^G K_0$. □

例:(1)设p是素数，p元域$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$中，任意$\alpha \in \mathbb{F}_p, \alpha^p = \alpha$,于是$\mathbb{F}_p^p = \mathbb{F}_p$.

(2)$F = \mathbb{F}_p[x]$中，因x不能表示出某个多项式的p 次方,故$F^p \neq F$.

定义:设k是一个域，

(1)当$char(k) = 0$时，称k是一个perfect域。

(2)当$char(k) = p > 0$时，如果$k^p = k$,则称k是一个perfect域。

推论:设k是一个perfect 域，则k的任意代数扩张都是可分扩张，k的任意代数扩张都是$perfect$.

证明. 设$K|k$是域的代数扩张，任取$\alpha \in K$,设E是$k(\alpha)|k$在K中的正规闭包，记$G = Aut_k(E)$,则$E^G|k$是纯不可分的.

对于任意$\beta \in E^G$有$\beta^{p^r} \in k$，即$\beta^{p^r} = a \in k$. 由于k是perfect,有$b \in k$使得$a = b^p$,于是$\beta^{p^{r-1}} = b \in k$,继续下去可得到$\beta \in k$,于是$E^G \subseteq k$，但又因 $E^G \supseteq k$,故$E^G = k$。这就得到$E|k$是可分的，α 在k上是可分的，由于α是任意的，于是$K|k$是可分扩张.

□

2 Galois理论

2.1 有限Galois理论

设$K|k$是域的一个代数扩张，令$G = Gal(K|k) = Aut_k(K)$,则G是一个群，称为$K|k$的Galois群。任取$H \leq G$(子群),令

$$K^H = \{\alpha \in K | \sigma(\alpha) = \alpha, \forall \sigma \in H\},$$

结论:$k \subseteq K^H \subseteq K, K^H$是一个域。

证:任取$\alpha,\beta\in K^H$,对任意$\sigma\in H,\sigma(\alpha)=\alpha,\sigma(\beta)=\beta$,于是

$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)=\alpha+\beta\Longrightarrow\alpha+\beta\in K^H$$
$$\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)=\alpha\beta\Longrightarrow\alpha\beta\in K^H$$

若$\alpha\in K^H$,设$\beta=\alpha^{-1}\in K$, 由$\alpha\beta=1$,得$\sigma(\alpha)\sigma(\beta)=\alpha\beta=1$.于是$\sigma(\beta)=\beta$，即$\beta\in K^H$.综上，$K^H$是一个域。

定义:设$K|k$是一个域的代数扩张，如果$K|k$既是可分的，也同时是正规的，则称$K|k$是一个$Galois$**扩张**。

设$K|k$是一个n次$Galois$扩张，$n=[K:k]$.则$|Gal(K|k)|=[K:k]_s=[K:k]$.

定理(Artin)设k是一个域，$G\subseteq Aut(K)$是一个有限子群，令$k=K^G$,则$K|k$是一个$Galois$扩张，且其$Galois$群为$Gal(K|k)=G$.

证明. 任取$\alpha\in K$,设α的$G-$轨道为

$$G\cdot\alpha=\{\sigma_1\alpha,\sigma_2\alpha,\cdots,\sigma_r\alpha\}.$$

不妨设$\sigma_1=id$,显然,对任意$\tau\in G,\tau G\alpha=G\alpha$,即

$$\{\tau\sigma_1\alpha,\tau\sigma_2\alpha,\cdots,\tau\sigma_r\alpha\}.$$

令$f(x)=(x-\sigma_1\alpha)\cdots(x-\sigma_r\alpha)$, 则

$$\begin{aligned}f^\tau(x)&=(x-\tau\sigma_1\alpha)\cdots(x-\tau\sigma_r\alpha)\\&=f(x)\end{aligned}$$

这就说明$f(x)\in K^G[x]=k[x]$.显然，由于$\sigma_1=id,f(\alpha)=0$. 而$\sigma_1\alpha,\cdots,\sigma_r\alpha$两两不同，故$f(x)$无重根，即可分。从而$\alpha$是$k$上的可分元，由$\alpha$的任意性，$K|k$是可分的。

又设α在k上的极小多项式为$P_\alpha(x)$,则$P_\alpha|f(x)$,于是α的$k-$共轭元必属于$\{\sigma_1\alpha,\cdots,\sigma_r\alpha\}\subseteq K$,于是$\sigma(K)\subseteq K$,即$K|k$是正规扩张.综上，$K|k$是$Galois$扩张.

下证$Gal(K|k)=G$.设$|G|=n$,首先由定义易知$G\subseteq Gal(K|k)$. 又由上述证明可知，对任意$\alpha\in K$,有

$$[k(\alpha):k]=degP_\alpha(x)\le degf(x)\le|G|=n,$$

由此下述引理可证得$[K:k]\le n$.于是$|Gal(K|k)|\le n$.综上，$Gal(K|k)=G$. □

引理:设$E|k$是可分代数扩张，若存在固定地正整数n使得对任意 $\alpha\in E,[k(\alpha):k]\le n$.则$E|k$是有限扩张，且$[E:k]\le n$.

证明. 不妨设m是k的单代数扩张的最大次数，即有$\alpha\in K$,使得 $[k(\alpha):k]=m$,且$\forall\beta\in K,[k(\beta):k]\leq m$. 下面说明$K=k(\alpha)$。
若不然，存在$\beta\in K-k(\alpha)$,由本原元定理，存在$\gamma\in K$使得$k(\alpha,\beta)=k(\gamma)$.于是

$$k\subseteq k(\alpha)\subsetneqq k(\alpha)(\beta)=k(\gamma).$$

由$k(\gamma)|k$是单代数扩张，$[k(\gamma):k]\leq m$,这与$k(\alpha)\subsetneqq k(\gamma)$矛盾！故$K=k(\alpha)$,进而$[K:k]=m\leq n$. □

引理:设$K|k$是Galois扩张，$G=Gal(K|k)$,则$K^G=k$.

证明. 显然，$k\subseteq K^G$.下证$K^G\subseteq k$.

对任意$\alpha\in K^G$,任取$k(\alpha)$到K的一个$k-$嵌入，则σ可延拓为$k-$嵌入$\tau:K\to K$, 即$\tau\in G,\tau|_{k(\alpha)}=\sigma$.由所设 $\sigma(\alpha)=\tau(\alpha)=\alpha(\forall\alpha)\in K^G$.于是$\sigma=id$.由$k(\alpha)|k$是可分扩张，$[k(\alpha):k]=[k(\alpha):k]_s=1$.即$k(\alpha)=k$,由于$\alpha\in K^G$是任意，故$K^G\subseteq k$.综上，$K^G=k$. □

Galois理论基本定理(有限扩张情形).设$K|k$是域的n次$Galois$扩张,其$Galois$群为$G=Gal(K|k)$,用S表示所有k和K的中间域组成的集合，J表示G的所有子群组成的集合。令

$$\begin{aligned}\phi:&S\to J\\ &E\mapsto Gal(K|E)\end{aligned}$$

则(1)ϕ是一个双射，特别地，$K^{Gal(K|k)}=k$.
(2)设$k\subseteq E_1\subseteq E_2\subseteq K$,则对应地，有$\phi(E_1)\supseteq\phi(E_2)$.反之，如果 $1\leq H_1\leq H_2\leq G$,则$\phi^{-1}(H_1)\supseteq\phi^{-1}(H_2)$,
(3)对于中间域E,$k\subseteq E\subseteq K$, $E|k$是$Galois$扩张当且仅当$\phi(E)\triangleleft G$,此时

$$Gal(E|k)\cong G/\phi(E)\cong G/Gal(K|E).$$

(4)设有中间域$k\subseteq E_i\subseteq K(i=1,2)$，则

$$\phi(E_1\cap E_2)=<\phi_(E_1)\cup\phi(E_2)>$$
$$\phi(E_1E_2)=\phi(E_1)\cap\phi(E_2)$$

(5)设中间域$k\subseteq E_1\subseteq E_2\subseteq K$,则 $E_2|E_1$是$Galois$的当且仅当$\phi(E_2)\triangleleft\phi(E_1)$.此时有

$$Gal(E_2|E_1)\cong\phi(E_1)/\phi(E_2)=Gal(K|E_1)/Gal(K|E_1).$$

证明. (1)任取$E\in S$,由于$K|k$是Galois扩张，$K|E$是Galois扩张，即$Gal(K|E)\in J$，从而ϕ是良定义的。

下证ϕ是单射。设对于中间域$k\subseteq E_i\subseteq bK(i=1,2)$,若有$\phi(E_1)=\phi(E_2)$,即

$$Gal(K|E_1)=Gal(K|E_2).$$

由上一引理得,$E_1=K^{Gal(K|E_1)},E_2=K^{Gal(K|E_2)}$.由此$E_1=E_2$,即$\phi$是单射.

下证ϕ是满射。任取$H \leq G$,令$E = K^H$,此时由$Artin$定理，$K|E$是Galois扩张，且$Gal(K|E) = H$,显然E是中间域，且$\phi(E) = H$.故ϕ是满射.

综上，ϕ是双射。

(2)若$k \subseteq E_1 \subseteq E_2 \subseteq K$, $\phi(E_1) = Gal(K|E_1), \phi(E_2) = Gal(K|E_2)$. 任取$\sigma \in Gal(K|E_2)$, 则$\sigma|_{E_2} = id$,从而$\sigma|_{E_1} = id$.于是$\sigma \in Gal(K|E_1)$.这便是$\phi(E_1) \supseteq \phi(E_2)$.

同样可得:若$1 \leq H_1 \leq H_2 \leq G$,则$\phi^{-1}(H_1) \supseteq \phi^{-1}(H_2)$.

(3)若$k \subseteq E \subseteq K$,且$E|k$是正规的，令

$$\psi : Gal(K|k) \to Gal(E|k)$$

$$\sigma \mapsto \sigma|_E,$$

则显然ψ是群同态，下证ψ是满射.任取$\sigma \in Gal(E|k)$,将σ延拓为K到k的代数闭包k^a的$k-$嵌入τ,由于$K|k$是正规扩张，故$\tau(K) = K$,从而$\tau \in Gal(K|k)$,于是$\psi(\tau) = \sigma$,即ψ是满射。

另一方面,

$$ker(\psi) = \{\sigma \in Gal(K|k) | \psi(\sigma) = id\} \subseteq Gal(K|E).$$

又$\forall \sigma \in Gal(K|E)$,则$\psi(\sigma) = \sigma|_E = id$,于是$Gal(K|E) \subseteq Ker\psi$.故$Gal(K|E) = ker\psi$.此时，$Gal(K|E)$是$Gal(K|k)$的正规子群，且由群同态基本定理得

$$Gal(K|k)/Gal(K|E) \cong Gal(E|k).$$

反过来，若$E|k$不是正规扩张，则存在E到K的$k-$嵌入λ使得$\lambda E \neq E$,将λ延拓成K的$k-$子同构,仍记为λ(因$K|k$是正规扩张,$\lambda(K) = K$),于是

$$Gal(K|\lambda E) = \lambda Gal(K|E)\lambda^{-1}.$$

$Gal(K|\lambda E)$与$Gal(K|E)$共轭但不相同(因对应的中间域不同)，这就说明$Gal(K|E)$不是$Gal(K|k)$的正规子群。

(4)若中间域$k \subseteq E_i \subseteq K(i = 1, 2)$，则

$$\begin{aligned}
&E_1 \supseteq E_1 \cap E_2, E_2 \supseteq E_1 \cap E_2 \\
\Rightarrow &\psi(E_1) \subseteq \psi(E_1 \cap E_2), \psi(E_2) \subseteq \psi(E_1 \cap E_2) \\
\Rightarrow &< \psi(E_1) \cup \psi(E_2) > \subseteq \psi(E_1 \cap E_2)
\end{aligned}$$

下证

$$\psi(E_1 \cap E_2) \subseteq \psi(E_1) \cup \psi(E_2) := H_0 = H_1 \cup H_2.$$

由于$H_0 \supseteq H_1, H_0 \supseteq H_2$,

$$\begin{aligned}
&K^{H_0} \subseteq K^{H_1}, K^{H_0} \subseteq K^{H_1} \\
&\Rightarrow H_0 \subseteq K^{H_1} \cap K^{H_2} = E_1 \cap E_2 \\
&\Rightarrow H_0 \supseteq Gal(K|E_1 \cap E_2) = \psi(E_1 \cap E_2) \\
&\Rightarrow < \psi(E_1) \cup \psi(E_2) > \supseteq \psi(E_1 \cap E_2) \\
&\Rightarrow \psi(E_1 \cap E_2) =< \psi(E_1) \cup \psi(E_2) >
\end{aligned}$$

(5)这是(3)的直接推论：运用(3)于域扩张$E_1 \subseteq E_2 \subseteq K$. □

2.2 Galois理论的若干应用

2.2.1 关于多项式根式解的Galois定理

例.$f(x) = x^4 - 6x^2 + 7 \in \mathbb{Q}[x]$.
令$t = x^2$, $f(x) = 0 \Rightarrow t = \frac{6 \pm \sqrt{8}}{2} = 3 \pm \sqrt{2} \Rightarrow x = \pm\sqrt{3 \pm \sqrt{2}}$.考虑下列域扩张

$$k := \mathbb{Q} \subseteq k_1 := \mathbb{Q}(\sqrt{2}) \subseteq k_2 := \mathbb{Q}(\sqrt{2})(\sqrt{3+\sqrt{2}}) \subseteq k_3 := \mathbb{Q}(\sqrt{2})(\sqrt{3+\sqrt{2}})(\sqrt{3-\sqrt{2}})$$

则

$$k_3 = k_2(\sqrt{3-\sqrt{2}}), k_2 = k_2(\sqrt{3+\sqrt{2}}), k_1 = k(\sqrt{2}),$$
$$(\sqrt{3-\sqrt{2}})^2 \in k_2, (\sqrt{3+\sqrt{2}})^2 \in k_1, (\sqrt{2})^2 \in k = \mathbb{Q}.$$

定义:设k是一个域，$f(x) \in k[x]$,称f在k上**可根式解**：如果存在k的扩域序列

$$k \subseteq k_1 \subseteq \cdots \subseteq k_r$$

使得k_r包含f的分裂域，且k_r是k的一个根式扩张，即有

$$k_r = k(\alpha_1, \cdots, \alpha_r), k_i = k_{i-1}(\alpha_i),$$

且$\alpha_i^{n_i} \in k_{i-1}$对某一正整数$n_i$成立.
定义：设$K|k$是一个域扩张.如果有域扩张序列

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = K$$

及$n_1, \cdots, n_r \in \mathbb{Z}_{>0}$使得 $K = k(\alpha_1, \cdots, \alpha_r), k_i = k_{i-1}(\alpha_i)$且$\alpha_i^{n_i} \in k_{i-1} (i = 1, \cdots, r)$,则称$K$是$k$的一个根式扩张。若记$n = n_1 \cdots n_r$,则 $\alpha_i^n \in k_{i-1}$,此时称K是k的$n-$**根式扩张**(n不是唯一的).

性质:设$K|E$和$E|k$均是根式扩张，则$K|k$也是根式扩张。

证明. 由$K|E$和$E|k$是根式扩张，有

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = E,$$

满足$k_i = k_{i-1}(\alpha_i), \alpha_i^n \in k_{i-1}$.

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = K,$$

满足$E_i = E_{i-1}(\beta_i), \beta_i^m \in E_{i-1}$.于是

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_r = E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_s = K$$

就满足$K|k$的根式扩张的条件。即$K|k$是根式扩张。 □

定理:设$K|k$是域的有限扩张，且L是$K|k$的一个正规闭包(选定k的一个代数闭包k^a).如果$K|k$是根式扩张，则$L|k$也是根式扩张.

证明. 由$K|k$是有限扩张，则设$K=k(\alpha_1,\cdots,\alpha_r)$.对$r$用归纳法。

当$r=1$时，简记$K=k(\alpha)$,因为L是$K|k$的正规闭包，故$L=k(\alpha_1,\cdots,\alpha_s)$,其中$\alpha_1,\cdots,\alpha_s$是$\alpha$的全部$k-$共轭元。由所设，$K|k$是一个$n-$根式扩张，于是$\alpha^n=a\in k$(对某个$a\in k$),即$\alpha$是$k$上多项式$x^n-a$的一个根，于是$P_\alpha(x)|(x^n-a)$,故$\alpha_1,\cdots,\alpha_s$都是$x^n-a$的根，即$\alpha_i^n=a\in k$. $L|k$是$n-$根式扩张。

现对于$K=k(\alpha_1,\cdots,\alpha_r)$,记$E=k(\alpha_1,\cdots,\alpha_{r-1})$,并设$E|k$的正规闭包为$L_1$,则由$E$是$k$的根式扩张，及归纳假设$L_1|k$也是根式扩张，又设$L$是$K|k$的正规闭包，则$L=L_1(\beta_1,\cdots,\beta_s)$,其中$\beta_1=\alpha_r,\beta_1,\cdots,\beta_s$是$\alpha_r$的全部$k-$共轭元。

任取β_i,令

$$\sigma_i:k(\alpha_r)\to k^a$$
$$\alpha_r\mapsto\beta_i$$

则σ_i是$k(\alpha_r)$到k^a的一个$k-$嵌入，σ可延拓成L到k^a的一个$k-$嵌入τ_i，由所设$K|k$是根式扩张，而$K=E(\alpha_r)$,于是 $\alpha_r^n=\gamma\in E$对于某一$n\in\mathbb{Z}_{>0}$成立。由于$E\subseteq L_1$，而L_1是一正规闭包，故

$$(\tau_i(\alpha_r))^n=\tau_i(\alpha_r^n)=\tau(\gamma)=\tau_i|_{L_1}(\gamma)\in L_1.$$

于是$\beta_i^n\in L_1(i=1,\cdots,s)$. 即$L|L_1$是根式扩张，又$L_1|k$是根式扩张，故$L|k$是根式扩张。 □

定义:设G是群，若存在G的子群列

$$G=G_0\supseteq G_1\supseteq\cdots\supseteq G_r=\{1\},$$

使得$G_{i+1}\trianglelefteq G_i$,且$G_i/G_{i-1}$是Abel群，则称$G$是可解群.

定理:(Galois)设k是一个域，$char(k)=0, f(x)\in k[x]$，K是$f(x)$在k上的分裂域。则f可根式解当且仅当$Gal(K|k)$是可解群.

证明. $\Rightarrow$)由f可根式解，K包含于某个k的根式扩域E中，又取$E|k$的正规闭包$L|k$,由前述定理可知$L|k$也是根式扩张。
不妨设$L|k,E|k$均是$n-$次根式扩张。即有域的扩张序列

$$k=k_0\subseteq k_1\subseteq\cdots\subseteq k_r=E\subseteq L,$$

其中$k_i=k_{i-1}(\alpha_i),\alpha_i^n\in k_{i-1}(i=1,\cdots,r),L=E(\alpha),\alpha^n\in E.$
记$G=Gal(L|k)$为$L|k$的Galois群，且记$H_i=Gal(L|k_i)(i=1,\cdots,r)$,即有子群序列

$$\{1\}\subseteq H_r\subseteq H_{r-1}\subseteq\cdots\subseteq H_1\subseteq H_0=G.$$

为简记，设k包含n次本原单位根ξ_n。

考虑扩张k_i/k_{i-1},由于$k_i=k_{i-1}(\alpha_i),\alpha_i^n\in k_{i-1}$,又$\xi_n\in k\in k_{i-1}$. 则由$Kummer$扩张结果可知,$k_i/k_{i-1}$是一个循环扩张(即$Gal(k_i|k_{i-1})$是循环群)。由$Galois$理论知$H_i\triangleleft H_{i-1}$(正规子群),且

$$H_{i-1}/H_i\cong Gal(k_i|k_{i-1})$$

是循环群。即$G=Gal(L|k)$是一个可解群，G的商群$Gal(K|k)$也是可解群($Gal(K|k)\cong G/Gal(L|K)$).

$\Leftarrow$)设$Gal(K|k)$是一个可解群，则有子群序列

$$G=Gal(K|k)=G_0\supseteq G_1\supseteq\cdots\supseteq G_r=\{e\}.$$

其中$G_{i+1}\lhd G_i$,且$G_i/G_{i+1}(i=0,\cdots,r-1)$是Abel群. 记$n=[K:k]$,且设$k$包含一个$n$次本原单位根$\xi_n$. 记$k_i=K^{G_i}$,则由$Galois$理论，可得$K$的子群序列

$$k=k_0\subseteq k_1\subseteq\cdots\subseteq k_r=k,$$

且$k_i|k_{i-1}$是Abel扩张(因为$Gal(k_i|k_{i-1})\cong G_{i-1}/G_i$是Abel群). 又由所设$\sigma^n=id(\forall\sigma\in G)$,故每个$k_i/k_{i-1}$均为指数为$n$的Abel扩张， 由Kummer理论可知$k_i|k_{i-1}(i=1,2,\cdots,r)$是一个根式扩张,从而$K|k$是根式扩张，即$f$可根式解。 □

Kummer理论：若有根式扩张$k(\sqrt[n]{\alpha})(\alpha\in k)$(Kummer扩张)，且$\xi_n\in k$,则Kummer扩张一定是循环扩张。

2.2.2 古希腊四大数学难题

1.化圆为方。 2.倍立方。 3.三等分角。 4.正多边形的作图问题。

方法：作图工具只有直尺与圆规.

(1)直线相交:l_1与l_2相交，

$$\begin{cases}a_1x+b_1y+c_1=0\\a_2x+b_2y+c_2=0\end{cases}$$

其中$a_i,b_i,c_i\in\mathbb{Q},i=1,2$.若有交点$P$,则$P\in\mathbb{Q}\times\mathbb{Q}$.

(2)直线与圆相交:

$$\begin{cases}a_1x+b_1y+c_1=0\\x^2+y^2+cx+dy+e=0\end{cases}$$

其中$a_1,b_1,c_1,c,d,e\in\mathbb{Q}$. 若有交点$P$,则$P=(x_0,y_0)\in\mathbb{Q}(\sqrt{\Delta})\times\mathbb{Q}(\sqrt{\Delta}),0\le\Delta\in\mathbb{Q}$.

命题:设$\alpha\in R$,则α可尺规构作当且仅当有域扩张序列

$$\mathbb{Q}=k_0\subseteq k_1\subseteq\cdots\subseteq k_r,$$

使得$[k_i:k_{i-1}]\le 2(i=1,\cdots,r)$,且$\alpha\in k_r$.特别地,$\alpha\in k_r$且$[k_r:\mathbb{Q}]=2^s(s\in\mathbb{Z}_{\ge0})$,即$\alpha$必为代数数。

问题1:化圆为方(π=正方形的面积?)

解：无解.原因:π是超越数。如若不然，则有$\mathbb{Q}$的某个2^s次扩域k,使得$\pi\in k$,由此得到π是代数数，矛盾!

问题2：倍立方(2=正方形的体积?)

解：无解.问题等价于$\sqrt[3]{2}$是否尺规构作.由于$\sqrt[3]{2}$是3次代数数，$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$,而3不是2的幂，从而$\sqrt[3]{2}$不可尺规构作。

问题3：三等分角。

首先，θ可尺规构作当且仅当$cos\theta, sin\theta$均可尺规构作.

解：一般情况下无解。例$\beta = 60^0, \theta = \frac{\beta}{3} = 20^0$.

$$\begin{aligned}\frac{1}{2} &= cos60^0 = cos(3\theta) = cos(2\theta+\theta)\\ &= cos2\theta cos\theta - sin2\theta sin\theta\\ &= (2cos^2\theta - 1)cos\theta - 2sin^2\theta cos\theta\\ &= 2cos^3\theta - cos\theta - 2cos\theta + 2cos^3\theta\\ &= 4cos^3\theta - 3cos(\theta)\end{aligned}$$

即$cos\theta$是多项式$f(x) = 8x^3 - 3x - 1$的根，而$f(x)$在$\mathbb{Q}$上不可约，于是$[\mathbb{Q}(cos\theta) : \mathbb{Q}] = 3$,但3不是2的方幂，故$cos\theta$不可尺规作出。

问题4：正多边形作图问题。

解:正n边形可尺规作出当且仅当$\frac{2\pi}{n}$可尺规作出，又等价于 $cos\frac{2\pi}{n}, sin\frac{2\pi}{n}$可尺规作出。

令$\xi_n = e^{\frac{2\pi i}{n}} = cos\frac{2\pi}{n} + isin\frac{2\pi}{n}(n > 2)$,则$\xi_n^{-1} = cos\frac{2\pi}{n} - isin\frac{2\pi}{n}$.于是

$$cos\frac{2\pi}{n} = \frac{\xi_n + \xi_n^{-1}}{2} \in \mathbb{Q}(\xi_n + \xi_n^{-1}) \subseteq R.$$

由$\xi_n \notin \mathbb{Q}(\xi_n + \xi_n^{-1})$得$\mathbb{Q}(\xi_n) \supsetneqq \mathbb{Q}(\xi_n + \xi_n^{-1})$,于是

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n + \xi_n^{-1})] \geq 2.$$

又因ξ_n是多项式$f(x) = x^2 - (\xi_n + \xi_n^{-1})x + 1 \in \mathbb{Q}(\xi_n + \xi_n^{-1})[x]$的根，故

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n + \xi_n^{-1})] \leq 2.$$

综上，

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

定理:正n边形可尺规构作当且仅当$\phi(n)$(欧拉函数)是2的幂。

证明. 正n边形可尺规构作$\Leftrightarrow \frac{2\pi}{n}$可尺规作出$\Leftrightarrow$ $cos\frac{2\pi}{n}, sin\frac{2\pi}{n}$可尺规作出 $\Leftrightarrow$ $[\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}]$是2的幂。而

$$\begin{aligned}\phi(n) &= [\mathbb{Q}(\xi_n) : \mathbb{Q}]\\ &= [\mathbb{Q}(\xi_n) : \mathbb{Q}(cos\frac{2\pi}{n})][\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}]\\ &= 2[\mathbb{Q}(cos\frac{2\pi}{n}) : \mathbb{Q}].\end{aligned}$$

由此即知命题成立。 □

2.3　域的无限Galois扩张

设$K|k$是无限Galois扩张，一般我们就取K是k的代数闭包。记$G=Gal(K|k)$,对于中间域$k\subset E\subset K$记$H_E=Gal(K|E)$.定义集合 $\mathcal{I}=\{E: E$是$K|k$的中间域，且$E|k$是有限Galois扩张$\}$. $\mathcal{N}=\{H:H=Gal(K|E),E\in\mathcal{I}\}$.

命题1： (1) $\cap_{H\in\mathcal{N}} H=\{e\}$.(2) $\cap_{H\in\mathcal{N}}\sigma H=\{\sigma\}(\forall\sigma\in G)$.

证明：(1)任取$\sigma\in\cap_{H\in\mathcal{N}}H$,对任意$\alpha\in K$，设$E$是$k(\alpha)|k$在$K|k$中的正规闭包，则$E\in\mathcal{I},H_E=Gal(K|E)\in\mathcal{N}$,特别地$\sigma\in H_E$,对$\alpha\in E,\sigma(\alpha)=\alpha$,由$\alpha$的任意性，$\sigma=id$,即$\sigma$在$K$是恒等映射.

(2)

$$\begin{aligned}\forall\tau\in\cap_{H\in\mathcal{N}}\sigma H &\Rightarrow\tau\in\sigma H(\forall H\in\mathcal{N})\\ &\Rightarrow\sigma^{-1}\tau\in H(\forall H\in\mathcal{N})\\ &\Rightarrow\sigma^{-1}\tau\in\cap_{H\in\mathcal{N}}=e\\ &\Rightarrow\sigma=\tau\\ &\Rightarrow\cap_{H\in\mathcal{N}}\sigma H=\{\sigma\}(\forall\sigma\in G).\end{aligned}$$

命题2： 设$H_1,H_2\in\mathcal{N}$,则$H_1\cap H_2\in\mathcal{N}$.

证明：由$\mathcal{N}$的定义，存在$E_1,E_2\in\mathcal{I}$使得$H_1=Gal(K|E_1),H_2=Gal(K|E_2)$.由于$E_1E_2|k$是有限Galois扩张$E_1E_2\in\mathcal{I}$.由Galois理论知$H_1\cap H_2=Gal(K|E_1E_2)$于是$H_1\cap H_2\in\mathcal{N}$.

定义G上的$Krull$拓扑：规定$\{\sigma H:\sigma\in G,H\in\mathcal{N}\}$为$G$上的一个拓扑基。即$G$中子集$H^{'}$为开集当且仅当$H^{'}$为上述拓扑基元素之并。

定理:G在上述拓扑基下为Hausdorff,紧致且完全不连通的拓扑群。

证明:(i)完全不连通(能写成两个非空开子集的不交并，连通子集只有单点集)。

设$X\subset G$,且$|X|\geq 2$,取$\sigma,\tau\in X$,且$\sigma\neq\tau$. 由$\cap_{H\in\mathcal{N}}\sigma H=\{\sigma\}$知$\tau\notin\cap_{H\in\mathcal{N}}\sigma H$,从而$\exists H_0\in\mathcal{N}$使得$\tau\notin\sigma H_0$,即 $\tau\in G-\sigma H_0$ 注意到

$$X=X\cap G=X\cap(\sigma H_0\cup(G-\sigma H_0))=(X\cap\sigma H_0)\cup(X\cap(G-\sigma H_0))$$

G关于子群H有陪集分解$G=\cup_{i\in I}\sigma_iH$,由此知若H是开集，由于G是拓扑群，对任意$\sigma\in G$,σH为开集，从而H为其所有非平凡陪集的补集，为闭集。注意到$\sigma\in X\cap\sigma H_0,\tau\in X\cap(G-\sigma H_0)$,且$\sigma H_0,G-\sigma H_0$均为开集，这就得到$X$是完全不连通的。特别地，$G$是完全不连通的，此处还可以看出, G是hausdorff空间。

另证:若$\sigma,\tau\in G$且$\sigma\neq\tau$,则存在有限Galois子扩张$E|k$使得$\sigma|_E\neq\tau|_E$(注意到任取$x\in K$,必存在包含x的$K|k$的有限Galois子扩张$E|k$,例如E取$k(x)|k$在$K|k$中的代数闭包。若对任意有限Galois子扩张$E|k$有$\sigma|_E=\tau|_E$,则对任意$x\in K,\sigma(x)=\tau(x)$.矛盾！)因此$\sigma Gal(K|E)\neq\tau Gal(K|E)$,因此$\sigma Gal(K|E)\cap\tau Gal(K|E)=\emptyset$.

对于G的紧性,这里先省略证明。

注:设G关于闭子群H有陪集分解$G=\cup_{i\in I}\sigma_iH$，则由G的紧致性,H是G的开子集当且仅当$(G:H)$有限。

定理： 设$H\leq G$,记$H^{'}=Gal(K|K^H)$,则$H^{'}=\bar{H}$(H在G中的闭包.)

证明:显然，$H\leq H^{'}$.下证$H^{'}$为G中的闭集,只需证$G-H^{'}$为开集.

任取$\sigma \in G - H^{'}$,必有$\alpha \in K^{H}$使得$\sigma(\alpha) \neq \alpha$.对于$\alpha \in K$,有$E \in \mathcal{I}$使得$\alpha \in E$,于是取$H_0 = Gal(K|E) \in \mathcal{N}$.对于$\forall \tau \in H_0$,有$\tau\alpha = \alpha$,于是$\sigma(\tau\alpha) = \sigma\alpha \neq \alpha$,即

$$\sigma\tau(\alpha) \neq \alpha \Rightarrow \sigma\tau \in G - H^{'} \Rightarrow \sigma H_0 \in G - H^{'} \Rightarrow G - H \quad is \quad open \Rightarrow H^{'} is \quad closed.$$

下证$\bar{H} = H^{'}$.需证$\forall \sigma \in H^{'}, N \in \mathcal{N}$.都有$\sigma N \cap H \neq \emptyset$.
由定义，取$E \in \mathcal{I}$使得$N = Gal(K|E)$,令$H_0 = \{\rho|_E : \rho \in H\}$,于是$K^{H_0} = K^H \cap E$,由有限Galois基本定理到$H_0 = Gal(E|K^H \cap E)$,由$\sigma \in H^{'}, \sigma|_{K^H} = id$,因此$\sigma|_E \in H_0$.存在$\rho \in H$使得$\rho|_E = \sigma|_E$.于是$\sigma^{-1}\rho \in Gal(K|E) = N$，即$\rho \in \sigma N \cap H.\sigma N \cap H \neq \emptyset$.

命题：设$K|k$是无限Galois扩张，任取$K|k$的一个中间域，则$H_E = Gal(K|E)$是G的一个闭子群。
证：$H_E \leq G$,则$K^{Gal(K|E)} = E \Rightarrow H_E = Gal(K|E) = Gal(K|K^{H_E}) = \bar{H}_E$.
无限Galois扩张基本定理:设$K|k$是无限Galois扩张，令$G = Gal(K|k)$, $\mathcal{I}_0 = \{E : E$是$K|k$的中间域$\}$, $\mathcal{N}_0 = \{H|H$是G的子群$\}$.定义映射

$$\begin{aligned} \varphi :& \mathcal{I}_0 \to \mathcal{N}_0 \\ & E \mapsto Gal(K|E) \end{aligned}$$

则φ是一个双射。
(1)$E|k$是Galois$\Leftrightarrow H_E = Gal(K|E) \triangleleft G$.
(2)对于$E \in \mathcal{I}_0, [E : k] \leq +\infty \Leftrightarrow H_E = Gal(K|E)$是$G$的开子群。(若$H$是开子群，则任意$\sigma \in G$,$\sigma H$也是开子群，从而由陪集分解 $G = \cup_{i \in I} \sigma_i H$,知$H$也是闭子群.此时再由$G$的紧致性知$[G : H] \leq +\infty$.反之，若已知$H$是闭集，则由$[G : H] \leq +\infty$知$H$是开集)。

例F_p(p是素数)。