伽罗瓦理论是域论中最重要的内容，它将域的扩张与群联系起来，本节主要介绍伽罗瓦基本定理(定理 6.2)，我们先引入几个常用的概念和符号，设 E, F 是域，若令 $\text{Aut}(E)=\{\varphi|\varphi \text{ 是 } E \text{ 的自同构}\}$ ，则按映射的合成运算， $\text{Aut}(E)$ 构成群，称其为 E 的自同构群，如果 E 包含 F ，那么在自同构群 $\text{Aut}(E)$ 中，有一个子群是我们非常关心的，即其中的 F -同构组成的群 $\text{Aut}_F(E)=\{\varphi \in \text{Aut}E|\varphi(a)=a, \forall a \in F\}$ ，称其为 E 关于 F 的伽罗瓦群或包含 F 的扩张 E 的伽罗瓦群，若 K 是包含 F 的 E 的中间域，即 $E \supseteq K \supseteq F$ ，则 $\text{Aut}_K(E)$ 是伽罗瓦群 $\text{Aut}_F(E)$ 的子群，并记 $\text{Aut}_K(E)$ 为 K' ，那么 $F'=\text{Aut}_F(E)$ ， $E'=\{\text{id}_E\}$ 若 H 是伽罗瓦群 $\text{Aut}_F(E)$ 的子群，则易知 $H'=\{x \in E|\sigma(x)=x, \forall \sigma \in H\}$ 是 E 的子域且 H' 包含 F ，称 H' 为群 H 的固定域，若 K 是包含 F 的 E 的中间域，则 K' 是伽罗瓦群 $\text{Aut}_F(E)$ 的子群，那么 K' 的固定域为 $(K')'$ ，简记为 K'' 同样地，若 H 是伽罗瓦群 $\text{Aut}_F(E)$ 的子群，则 $(H')'=H''$ 是 $\text{Aut}_F(E)$ 的子群，后面我们将会看到 K 包含于 K'' ， H 包含于 H'' ，

例 6.1 试确定复数域 C 关于实数域 R 的伽罗瓦群，

解: 显然， $C=R(i)=\{a+bi|a, b \in R\}$ ，

若 φ 属于 $\text{Aut}_R(C)$ ，则 $\varphi(a+bi)=a+b\varphi(i)$ ，即 φ 是由 $\varphi(i)$ 决定的，

而 $(\varphi(i))^2=\varphi(i^2)=\varphi(-1)=-1$ ，即属于 C 的 $\varphi(i)=\pm i$ ，因此 $\text{Aut}_R(C)=\{\varphi_0, \varphi_1\}$ ，

其中 $\varphi_0(a+bi)=a+bi$ ， $\varphi_1(a+bi)=a-bi$ ， a, b 属于 R ，

例 6.2 试确定包含 Q 的扩张 $Q(\sqrt[3]{2})$ 的伽罗瓦群，

解: $\sqrt[3]{2}$ 在 Q 上的极小多项式为 $f(x)=x^3-2$ ，则 $Q(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}|a, b, c \in Q\}$ ，

那么对属于 $\text{Aut}_Q(\sqrt[3]{2})$ 的任意 φ ， φ 由 $\varphi(\sqrt[3]{2})$ 决定，

因为 $\sqrt[3]{2}$ 是 $f(x)$ 的根，所以 $\varphi(\sqrt[3]{2})$ 是 $f(x)$ 的根，

因此， $\varphi(\sqrt[3]{2})=\sqrt[3]{2}$ ， $\sqrt[3]{2}\omega$ 或 $\sqrt[3]{2}\omega^2$ ，其中 $\omega=\frac{-1+\sqrt{3}i}{2}$

但是， $\sqrt[3]{2}\omega$ 和 $\sqrt[3]{2}\omega^2$ 不属于 $Q(\sqrt[3]{2})$ ，

因此 $\varphi(\sqrt[3]{2})$ 只能等于 $\sqrt[3]{2}$ ，即 $\varphi(a+b\sqrt[3]{2}+c\sqrt[3]{4})=a+b\sqrt[3]{2}+c\sqrt[3]{4}$ ， $\text{Aut}_Q(\sqrt[3]{2})=\{\text{id}\}$ ，

注意，对包含 F 的任意扩张 E ，有 $E'=\{\text{id}_E\}$ ，从而 $E''=E$ ，

但是，一般情况下 $F'' \neq F$ ，

例如，在例 6.1 中，有 $R'=\text{Aut}_R(C)$ ， $R''=R$ ，

但是，在例 6.2 中， $Q'=\{\text{id}\}$ ， $Q''=Q(\sqrt[3]{2}) \neq Q$ ，

定义 6.1 令包含 F 的 E 是域的扩张，如果 $F''=F$ ，那么称 E 是 F 的伽罗瓦扩张

命题 6.1 令包含 F 的 E 是域的扩张， K, L 是 E 的中间域， H, J 是 $\text{Aut}_F(E)$ 的子群

(1) 若 L 包含于 K ，则 K' 包含于 L'

(2) 若 H 包含于 J ，则 J' 包含于 H'

(3) K 包含于 K'' ， H 包含于 H''

至此，我们知道在包含 F 的扩张 E 的中间域

与 $\text{Aut}_F(E)$ 的子群之间有如下的对应关系：

$$\begin{array}{ccc}
 E \supseteq K \supseteq F & & E=E'' \supseteq H' \supseteq F'' \supseteq F \\
 \downarrow & \downarrow & \downarrow & & \uparrow & \uparrow & \uparrow \\
 E'=\{\text{id}_E\} \subseteq K' \subseteq F'=\text{Aut}_F(E) & & & & \{\text{id}_E\} \subseteq H \subseteq F'=\text{Aut}_F(E)
 \end{array}$$

定义 6.2 令 K 是包含 F 的扩张 E 的中间域，
若 $K=K''$ ，则称 K 为包含 F 的扩张 E 的闭域，
令 H 是域 E 关于域 F 的伽罗瓦群 $\text{Aut}_F(E)$ 的子群，
若 $H=H''$ ，则称 H 为包含 F 的扩张 E 的闭群，

命题 6.2 若包含 F 的 E 是域的扩张，

则在包含 F 的 E 的所有闭域和所有闭群之间存在一一对应

证: 若 K 是包含 F 的 E 的闭域，则 $(K')''=(K'')'=K'$ ，即 K' 是闭群，

因此我们可以给出闭域到闭群的映射 $\varphi: K \rightarrow K'$

设 K 和 L 都是闭域，若 $K'=L'$ ，则 $K''=L''$ ，

再由 K 和 L 都是闭域有 $K=L$ ，即 φ 是单射，

设 H 是包含 F 的 E 的闭群，则 $(H')''=(H'')'=H'$ ，即 H' 是闭域，且 $(H')'=H''=H$ ，

这说明 φ 是满射，因而 φ 是所有闭域到所有闭群的双射

既然域的扩张与其伽罗瓦群之间有对应关系，

那么域的扩张次数与群的指数之间又是什么关系呢？

引理 6.1 令 L, M 是包含 F 的扩张 E 的中间域，且 L 包含于 M ，

若 $|M':L|=n<\infty$ ，则 $|L:M|\leq n$ ，

证: 对扩张次数 n 用数学归纳法，当 $n=1$ 时，结论显然成立，

假设扩张次数小于 n 时，结论成立，考察扩张次数等于 n 的情况，

若存在包含 L 的 M 的中间域 K ，满足 $K\neq M, K\neq L$ ，则 $|M:K|<n, |K:L|<n$ ，

由归纳假设得 $|K':M'| |L':K'| \leq |M:K| |K:L|$ ，

再由本章定理 3.2 及第二章推论 3.2，不等式两端变为 $|L':M'| \leq |M:L|$ ，结论成立

若不存在包含 L 的 M 的中间域 K ，满足 $K\neq M, K\neq L$ ，

则对属于 $M-L$ 的任意 β ，必有 $M=L(\beta)$ ，

因为包含 L 的 M 是有限扩张，所以 β 是 L 上的代数元，

令 β 的属于 $L[x]$ 的极小多项式为 $f(x)$ ，则 $\deg f(x)=n$ ，

考虑 L' 关于 M 的陪集分解，令 $\tau M'$ 是一个左陪集，其中 τ 属于 L'

因为 β 是属于 $L[x]$ 的 $f(x)$ 的根，所以 $\tau(\beta)$ 也是 $f(x)$ 的根，

若 $\sigma M'$ (σ 属于 L') 是一个左陪集， $\sigma M' \neq \tau M'$ ，则 $\tau(\beta) \neq \sigma(\beta)$ ，

事实上，若 $\tau(\beta) = \sigma(\beta)$ ，则 $\beta = \tau^{-1}\sigma(\beta)$ ，

又因 $M=L(\beta)$ ， τ, σ 属于 L' ，所以 $\tau^{-1}\sigma$ 属于 M' ，从而， $\sigma M' = \tau M'$ ，矛盾，

也就是说，不同左陪集的个数不会超过 $f(x)$ 不同根的个数，所以， $|L':M'| \leq n$

推论 6.1 若包含 F 的 E 是域的有限扩张，则 $|E:F| \geq |\text{Aut}_F E|$ ，

即 E 关于 F 的伽罗瓦群是有限群，

当然对于 $\tau_j(1 \leq j \leq n)$ 有 $\tau_j(a) = a_i, i = 1, 2, \dots, r,$

因此, $\tau_i(u_1 + u_2 a_2 + \dots + u_r a_r) = \tau_i(u_1) + \tau_i(u_2) a_2 + \dots + \tau_i(u_r) a_r = 0$

因为 τ_i 是双射, 所以 $u_1 + u_2 a_2 + \dots + u_r a_r = 0$

即属于 H' 的 $u_1, u_2, \dots, u_{n+1}$ 在 J' 上是线性相关的, 矛盾

因此, $|H' : J'| \leq |J : H|,$

定理 6.1 若包含 F 的 E 是域的扩张, 包含于 K 的 L 是 E, F 的中间域,

令 H, J 是 $\text{Aut}_F(E)$ 的子群, 且 H 包含于 J , 则

(1) 如果 L 是包含 F 的 E 的闭域, 且 $|K : L| < \infty$, 那么 K 是闭域, 且 $|L' : K'| = |K : L|$

(2) 如果 H 是包含 F 的 E 的闭群, 且 $|J : H| < \infty$, 那么 J 是闭群, 且 $|H' : J'| = |J : H|$

证: (1) 因为 $L = L'', K$ 包含于 $K'', |K : L| < \infty$,

所以 $|K : L| \geq |L' : K'| \geq |K'' : L''| \geq |K : L''| = |K : L|,$

因此, $|L' : K'| = |K : L|, |K'' : L''| = |K : L''|,$ 进而有 $K = K'', K$ 是闭域,

(2) 使用与(1)同样的方法可证。”

令包含 F 的 E 是域的有限扩张,

若包含 F 的 E 是伽罗瓦扩张, 则简称包含 F 的 E 是有限伽罗瓦扩张,

引理 6.3 设 E 是 F 的扩域, H 是 E 关于 F 的伽罗瓦群的子群,

试证明对属于 $\text{Aut}_F(E)$ 的任意 σ , 有 $(\sigma H \sigma^{-1})' = \sigma(H'),$

证: 显然, $\sigma H \sigma^{-1}$ 是 $\text{Aut}_F(E)$ 的子群,

若 a 属于 $(\sigma H \sigma^{-1})'$, 则对属于 H 的任意 $h, h \sigma^{-1}(a) = \sigma^{-1}(a),$

进而, $\sigma^{-1}(a)$ 属于 H', a 属于 $\sigma(H'),$ 这表明 $(\sigma H \sigma^{-1})'$ 包含于 $\sigma(H')$

反之, 若 a 属于 $H',$ 则对属于 H 的任意 $h, h(a) = a,$

进而, $\sigma h \sigma^{-1}(\sigma(a)) = \sigma h(a) = \sigma(a),$ 即 $\sigma(a)$ 属于 $(\sigma H \sigma^{-1})'$

因此, $\sigma(H')$ 包含于 $(\sigma H \sigma^{-1})',$ 综上, $(\sigma H \sigma^{-1})' = \sigma(H')$

命题 6.3 有限伽罗瓦扩张是正规扩张，

证： 设包含 F 的 E 是有限伽罗瓦扩张，

属于 $F[x]$ 的 $p(x)$ 是不可约元，属于 E 的 α 是 $p(x)$ 的根，

因为包含 F 的 E 是有限扩张，所以 $\text{Aut}_F(E)$ 是有限群，

设 $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r\}$ 是 α 在 $\text{Aut}_F(E)$ 作用下的全部像的集合

(注意， $\alpha_1, \alpha_2, \dots, \alpha_r$ 两两不同且属于 E)，

构造多项式 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$

对属于 $\text{Aut}_F(E)$ 的任意 σ ，有 $\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_r)$ 是 $\alpha_1, \alpha_2, \dots, \alpha_r$ 的一个排列

因而 $f(x)$ 的系数在 σ 作用下不变，即 $f(x)$ 属于 $F''[x]$ ，

因为包含 F 的 E 是伽罗瓦扩张，所以 $F = F''$ ，即 $f(x)$ 属于 $F[x]$ ，

对属于 $\text{Aut}_F(E)$ 的任意 σ ，由 $\sigma(\alpha)$ 也是 $p(x)$ 的根可知， $\alpha_1, \alpha_2, \dots, \alpha_r$ 都是 $p(x)$ 的根

因此， $f(x) | p(x)$ ，这表明 $f(x)$ 与 $p(x)$ 相差一个系数，

即存在属于 F 的 a ，使得 $p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$ ，即 $p(x)$ 的根都在 E 中

从而包含 F 的 E 是正规扩张，

定理 6.2(伽罗瓦基本定理)令包含 F 的 E 是有限伽罗瓦扩张, 则

(1)在包含 F 的 E 的中间域和群 $\text{Aut}_F(E)$ 的子群之间存在一一对应,

(2)若包含 L 的 K 是包含 F 的 E 的中间域, 则 $|K:L|=|L':K'|$,

若包含于 J 的 H 是 $\text{Aut}_F(E)$ 的子群, 则 $|J:H|=|H':J'|$,

(3)若 K 是包含 F 的 E 的中间域, 则当且仅当 $\text{Aut}_K(E)$ 是 $\text{Aut}_F(E)$ 的正规子群, 并且 $\text{Aut}_F(E)/\text{Aut}_K(E) \cong \text{Aut}_F(K)$ 时, 包含 F 的 K 是正规扩张

证: (1), (2)的证明留作习题, 这里仅给出(3)的证明,

设包含 F 的 K 是正规扩张,

首先, 我们说明对属于 $\text{Aut}_F(E)$ 的任意 σ , 必有 $\sigma|_K$ 属于 $\text{Aut}_F(K)$,

即对属于 K 的任意 k , 有 $\sigma(k)$ 属于 K ,

因为正规扩张是有限扩张, 所以属于 K 的 k 有极小多项式, 设为 $f(x)$,

因为 k 是 $f(x)$ 的一个根, 所以, $\sigma(k)$ 也是 $f(x)$ 的一个根,

又由包含 F 的 K 是正规扩张可知 $\sigma(k)$ 属于 K ,

因此, 我们有映射 $\varphi: F' \rightarrow \text{Aut}_F(K), \sigma \rightarrow \sigma|_K$ 易知, φ 是群同态, 其中 $F' = \text{Aut}_F(E)$

由群同态基本定理得 $F'/\text{Ker } \varphi \cong \varphi(F) \subseteq \text{Aut}_F(K)$,

因为 $\text{Ker } \varphi = \{\sigma \in F' | \sigma|_K = \text{id}_K\} = \text{Aut}_K(E) = K'$, 所以, $\text{Aut}_K(E)$ 是 $\text{Aut}_F(E)$ 的正规子群

由(2)的结论和推论 6.1 可知 $|F':K'| = |K:F| \geq |\text{Aut}_F(K)|$,

从而, $|\text{Aut}_F(K)| \geq |\varphi(F')| = |F'/K'| = |F':K'| \geq |\text{Aut}_F(K)|$

因此, $\varphi(F') = \text{Aut}_F(K), F'/K' = \text{Aut}_F(E)/\text{Aut}_K(E) \cong \text{Aut}_F(K)$,

反之, 若 $K' = \text{Aut}_F(E)$ 是 F' 的正规子群, 则对属于 F' 的任意 σ , 有 $\sigma K' \sigma^{-1} = K'$

再由引理 6.3 得 $(\sigma K' \sigma^{-1}) = \sigma(K'')$, 即 $K'' = \sigma(K'')$,

因为包含 F 的 E 是有限伽罗瓦扩张,

所以由定理 6.1(1)可知 K 是闭域, 即 $K = K''$, 从而 $\sigma(K) = K$,

此时我们可以定义映射 $\varphi: \text{Aut}_F(E) \rightarrow \text{Aut}_F(K), \sigma \rightarrow \sigma|_K$, 易知 φ 是群同态,

在包含于 K 的扩张 F 中,

由 $\varphi(\text{Aut}_F(E))$ 包含于 $\text{Aut}_F(K)$ 可知, F 包含于 $(\text{Aut}_F(K))'$ 包含于 $(\varphi(\text{Aut}_F(E)))'$

观察集合 $(\varphi(\text{Aut}_F(E)))' = \{a \in K | \sigma(a) = a, \forall \sigma \in \varphi(\text{Aut}_F(E))\}$

和 $(\text{Aut}_F(E))' = \{a \in E | \sigma(a) = a, \forall \sigma \in \text{Aut}_F(E)\}$

可得, $\varphi(\text{Aut}_F(E))'$ 包含于 $(\text{Aut}_F(E))'$

从而, F 包含于 $(\text{Aut}_F(K))'$ 包含于 $(\text{Aut}_F(E))' = F$, $F = (\text{Aut}_F(K))'$

即包含 F 的 K 是伽罗瓦扩张,

再由命题 6.3 可知, 包含 F 的 K 是正规扩张,