伽罗瓦理论

Galois theory

作者：Galois 爱求五次根

时间：2022/10/9

宗旨：执象而求，咫尺千里

我们必须知道，我们终将知道

目录

第 1 章 Galois 理论 **1**

1.1 群论初步 . . . 1

1.1.1 群与子群 . . . 1

1.1.2 陪集与商集 . . . 1

1.1.3 群同态 . . . 2

1.2 域论初步：域与域的扩张 . . . 3

1.2.1 域 . . . 3

1.2.2 域扩张 . . . 3

1.2.3 代数扩张 . . . 4

1.2.4 分裂域 . . . 6

1.2.5 正规扩张 . . . 6

1.2.6 可分扩张 . . . 6

1.3 伽罗瓦群和伽罗瓦扩张 . . . 7

1.3.1 伽罗瓦群 . . . 7

1.3.2 伽罗瓦扩张 . . . 8

1.4 伽罗瓦理论基本定理 . . . 9

1.4.1 子群和中间域之间的双射 . . . 9

1.4.2 正规子群和正规扩张一一对应 . . . 10

1.5 二次、双二次和三次多项式 . . . 11

1.5.1 二次和双二次扩张 . . . 11

1.6 三次扩张 . . . 11

第 1 章 Galois 理论

1.1 群论初步

1.1.1 群与子群

一个**群**是一个集合和一个二元运算 (binary operation) 的组合，此二元运算满足几个运算规律

定义 1.1 (群/group)

对于一个非空集合 G 和一个二元运算

$$\because G \times G \to G, (a,b) \mapsto a \cdot b$$

若它们满足以下几个定律：

1. （结合律）对于任意 $a,b,c \in G$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. （单位元）存在 $e \in G$，使得对于任意 $a \in G$，有 $a \cdot e = e \cdot a = a$。$e$ 就叫作单位元 (identity element)
3. （逆）对于任意 $a \in G$，存在 $a^{-1} \in G$，使得 $a \cdot a^{-1} = a^{-1} \cdot a = e$。这里的 a^{-1} 叫作 a 的逆 (inverse)

那么具有满足上述三个性质的二元运算的非空集合构成一个群

♣

注 为了表示的简洁，将 $a \cdot b$ 写作 ab，而且通常将单位元 e 写作 1

性质 很容易看出，在一个群中，单位元 e 是唯一的，一个元素的逆也是唯一的，一个元素的逆的逆是这个元素本身，且 $(ab)^{-1} = b^{-1}a^{-1}$

接下来介绍**子群**的概念

定义 1.2 (子群/subgroup)

对于一个群 G 的非空子集 H，若任意 $a,b \in H$ 都满足 $ab \in H$，且 H 和 $\cdot$ 的限制 (restriction) 构成一个群，那么 H 叫作 G 的一个子群

♣

例题 1.1 $(\mathbb{Z}, +)$ 是群 $(\mathbb{R}, +)$ 的一个子群

1.1.2 陪集与商集

一个子群 H 可以定义一个在群 G 上的**等价关系** (equivalence relation)，因而可以将 G 分解为叫作**陪集**的**等价类** (equivalence class)

定义 1.3 (子群诱导的同余关系/congruent)

令 G 为一个群，并令 H 为 G 的一个子群。对于 $a,b \in G$，若存在 $h \in H$ 使得 $a = bh$，则称 a 和 b 模 H 同余，写作 $a \equiv b \bmod H$

♣

性质 容易证明，模 H 同余是一个等价关系，即满足自反性 (reflexivity)，对称性 (symmetry) 和传递性 (transitivity)

与同余关系相联的等价类叫作**陪集**

定义 1.4 (陪集/coset)

定义 1.4 令 H 为群 G 的一个子群。对于每个 $a \in G$

$$aH = \{ah : h \in H\}$$

叫作 H 在 G 中的陪集

♣

根据定义可知，陪集 aH 就是等价类 $[a]=\{x\in G:a\equiv b \bmod H\}$ 。对于一个集合 A ，其上的不同的等价类构成一个将 A 分成不交 (disjoint) 子集的分解。因此，H 引出了一个将 G 分为不交等价类的分解

定义 1.5 (子群的商集及其指数)

令 H 为群 G 的一个子群。H 在 G 中的商集 (quotient set) G/H 是 H 的所有陪集的集合。H 在 G 中的指数 (index) 是 $[G:H]=|G/H|$ ，即商集的阶 (order)，它代表 H 在 G 中的🄵集的数量。若 G/H 是无限的，则 $[G:H]=\infty$

♣

例题 1.2 $k\mathbb{Z}=\{kn:n\in\mathbb{Z}\}$ 是 $\mathbb{Z}$ 的一个子群。那么，$\mathbb{Z}/k\mathbb{Z}=\{[0],\cdots,[k-1]\}$ ，故 $[\mathbb{Z}:k\mathbb{Z}]=k$ 。由于 G 是 $[G:H]$ 个不同的陪集的并集，其中每个陪集的阶是 $|H|$

根据例1.2，很自然地得到了**拉格朗日定理**的结论

定义 1.6 (拉格朗日定理/Langrange's theorem)

令 G 为一个有限群，并令 H 为 G 的一个子群。那么 $|H|$ 整除 $|G|$。更准确地说

$$|G|=[G:H]|H|$$

♣

接下来介绍一个重要的概念，即**正规子群**的概念

定义 1.7 (正规子群/normal subgroup)

令 H 为群 G 的一个子群。若对于所有 $g\in G$ 和所有 $h\in H$ ，都有 $ghg^{-1}\in H$ ，则称 H 是 G 的一个正规子群

♣

注 由于正规子群在共轭 (conjugation) 下是不变的，所以又叫不变子群 (invariant subgroup) 。正规子群的重要性在于，它可以用来构造商群 (quotient group)。正规子群还构成群同态 (homomorphism) 的核 (kernel) 。不难通过正规子群的定义得出，若 H 是群 G 的一个正规子集，商集 G/H 和乘积 $(aH)(bH)=abH$ 构成一个群。在后面介绍的伽罗瓦理论的时候，正规子群将会和域的正规扩张对应起来

1.1.3 群同态

另一个需要介绍的概念是群同态，它们是两个群之间的一类映射，满足乘积的映射等于映射的乘积。这样的性质保证在群同态下，群的结构是相容的

定义 1.8 (群同态及其核)

令 G,H 为群，并令 $f:G\to H$ 为一个映射。若对于任意 $a,b\in G$ ，都有

$$f(ab)=f(a)f(b)$$

则称 f 是一个群同态，集合 $\ker(f)=\{a\in G:f(a)=1\}$ 叫作群同态 f 的核

♣

注 根据群同态的定义，可以得知 $f\left(g^{-1}\right)=f(g)^{-1}\forall g\in G$ ，并可以进一步得到 $\ker(f)$ 是 G 的一个正规子群

定义 1.9 (群同构/isomorphism)

若一个群同态是双射的 (bijective)，那么它叫作一个群同构

♣

注 显然，同构是一个关于群的等价关系，同构群作为群有着完全相同的性质。从一个群到其自身的群同态叫作群自同态 (endomorphism)，而从从一个群到其自身的同构叫作群自同构 (endomorphism)。将一个群 G 的同态的集合 $S(G)$ 加上群同态的复合 (composition) 。视作一个群，我们可以得到，群的自同态的集合 $\mathrm{Aut}(G)$ 构成 $S(G)$ 的一个子群

1.2 域论初步：域与域的扩张

1.2.1 域

在一个 (ring) 中，有加法核乘法两种二元运算，而非像在群中那样只有一种，且环中的元素满足分配律 (distributive law)。除环 (division ring) 的概念是通过在环的基础上加上乘法逆的存在性得到的，而域的概念是通过在除环的基础上加上乘法交换律得到的

定义 1.10 (环/ring)

一个集合 R 和定义在其上的两种二元运算 $+$（加法）和 $\cdot$（乘法），构成一个环，若它们满足：

1. $(R,+)$ 是一个阿贝尔群 (abelian group)，即
- $(a+b)+c=a+(b+c)\forall a,b,c\in R$ ，即加法满足加法结合律
- $a+b=b+a\forall a,b\in R$ ，即加法满足加法交换律
- 存在元萦 $0\in R$ 使得 $a+0=a\forall a\in R$ ，即 0 为一个加法单位元
- $\forall a\in R,\exists -a\in R,a+(-a)=0$ ，即 $-a$ 是 a 的加法逆

2. $(R,\cdot)$ 是一个么半群 (monoid)，即
- $(a\cdot b)\cdot c=a\cdot(b\cdot c)\forall a,b,c\in R$ ，即加法满足乘法结合律
- 存在元素 $\mathrm{L}\in R$ 使得 $a\cdot 1=1\cdot a=a\forall a\in R$ ，即为一个乘法单位元.

3. 乘法关于加法满足分配律，即
- $a\cdot(b+c)=a\cdot b+a\cdot c\forall a,b,c\in R$
- $(a+b)\cdot c=a\cdot c+b\cdot c\forall a,b,c\in R$

对于一个环 R ，若 $\forall a\in R\backslash\{0\},\exists a^{-1}\in R,a\cdot a^{-1}=a^{-1}\cdot a=1$ ，即 a^{-1} 是 a 的乘法逆，那它是一个除环。对于一个除环 R ，若 $a\cdot b=b\cdot a\forall a,b\in R$ ，即乘法满足乘法交换律，那它是一个域 ♣

定义 1.11 (域的特征/characteristic)

一个域 k 的特征是最小的正整数 n ，使得在 k 中 $n\cdot 1=0$ ，写作 $\mathrm{char}(k)$ 。若这样的 n 不存在，则 $\mathrm{char}(k)=0$ 。若 k 是域 K 的一个子域，由于 K 中的 1 也是 k 中的 1 ，有 $\mathrm{char}(k)=\mathrm{char}(K)$ ♣

1.2.2 域扩张

域扩张的概念和群论中子群的概念类似

定义 1.12 (域扩张/field extension)

若一个环 R 的子集 A 是一个环，那么 A 叫作 R 的一个子环 (subring)。若一个域 K 的子环 k 是一个域，那么 k 叫作 K 的一个子域 (subfield)，且 K/k 叫作一个域扩张、若 K/k 是一个域扩张，且 K 的子域 L 包含 k ，则称 L 是 K/k 的一个中间域 (intermediate field) ♣

一个相关概念是域扩张的**度数**，它可以类比子群的指数

定义 1.13 (域扩张的度数/degree)

定义 2.3 一个域扩张 K/k 的度数 $[K:k]$ 是 K 作为一个 k-向量空间的维度 (dimension). 若此向量空间是无限维的，则 $[K:k]=\infty$ ♣

性质 由于 $[K:k]=1$ 等价于 1 是 K 的一个 k-基底 (basis)，即 $K=k\cdot 1=kmathrm$ $[K:k]=1$ 等价于 $K=k$ 。域扩张的度数具有乘法关系

定理 1.1 (度数定理)

若 L 是域扩张 K/k 的一个中间域，则

$$[K:k]=[K:L][L:k]$$

其中 $n\infty=\infty n=\infty\forall n\in\mathbb{N}$。特别地，当且仅当 $[K:L]$ 和 $[L:k]$ 是有限扩张，$[K:k]$ 是一个有限扩张 ♡

注 此定理可以通过线性代数中构造基底的方法来证明

1.2.3 代数扩张

若要引入正规扩张 (normal extension) 的概念，我们先要引入一些相关概念，包括多项式环 (polynomial ring)，代数扩张 (algebraic extension) 和分裂域 (splitting field)

定义 1.14 (多项式环)

令 R 为一个环，一个系数在 R 中的多项式 f 形如 $f=\sum_{i=0}^{n}a_ix^i$，其中 $a_i\in R$，$n\in\mathbb{N}$。若 $a_n\neq 0$，则 n 叫作 f 的度数 (degree)。令 $R[x]$ 为系数在 R 中的多项式的集合。若对于 $f=\sum_{i=0}^{n}a_ix^i$ 和 $g=\sum_{i=0}^{m}b_ix^i$，这里 $n\geq m$，定义

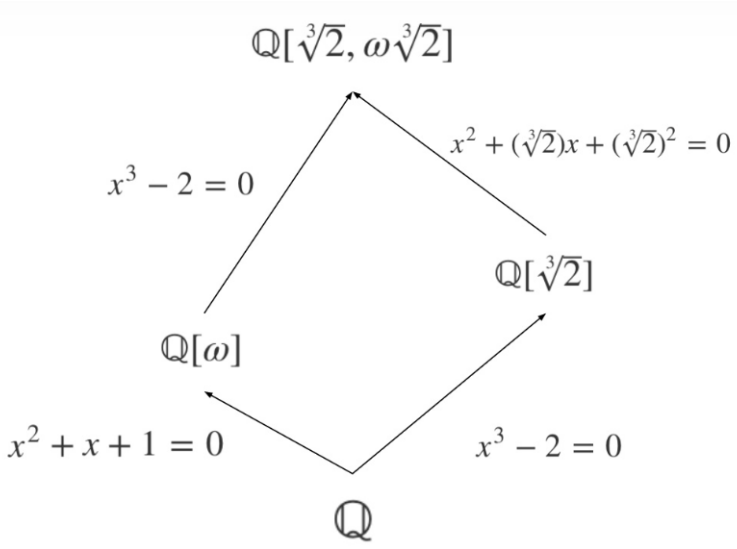
$$f+g=\sum_{i=0}^{n}(a_i+b_i)\,x^i, fg=\sum_{k=0}^{n+m}\sum_{i+j=m}a_ib_jx^{i+j}$$

其中 $b_i=0\forall i>m$，则 $R[x]$ 和这两个运算构成一个多项式环 ♣

定义 1.15 (超越元与代数扩张)

若 $a\in K$ 是 $f=\sum_i b_ix^i\in k[x]$ 的一个根 (root)，即 $f(a)=\sum_i b_ia^i=0$，则 a 在 k 上为代数的 (algebraic)，否则 a 在 k 上为超越的 (transcendental)。若 K 中的所有元素在 k 上都是代数的，则 K/k 叫作一个代数扩张。令 $a_1,\cdots,a_l\in K$，K 的所有包含 k 和 $a_1,\cdots,a_l$ 的子域的交集 $k(a_1,\cdots,a_l)$ 叫作由 $a_1,\cdots,a_l$ 生成的 k 的扩张。若 $a\in K$ 在 k 上是代数的，则 $k(a)$ 叫作 k 的一个简单代数扩张 ♣

例题 1.3 由于 $\sqrt{2}\in\mathbb{R}$ 是多项式 x^2-2 的一个根，$\sqrt{2}$ 在 $\mathbb{Q}$ 上是代数的，故 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是一个简单代数扩张。简单代数扩张的重要性在于，所有的有限代数扩张本质上都是简单代数扩张。一个简单代数扩张可以由 a 的所谓的最小多项式 (minimal polynomial) 来表示



定义 1.16 (首一多项式与主理想)

若多项式 f 的首项系数为 1，则 f 被称作首一的 (monic)。注意，对于任意 $f \in k[x]\backslash\{0\}$，存在唯一的首一多项式 g，使得由 f 生成的主理想 (principal ideal) 等于由 g 生成的主理想，即 $\langle f\rangle = \{fh : h \in k\} = \{gh : h \in k\} = \langle g\rangle$. 令 a 在 k 上为代数的，并令 $\mathrm{ev}_a : k[x] \to K, g \mapsto g(a)$ 为赋值同态 (evaluation homomorphism)。注意 a 是代数的等价于 $\ker(\mathrm{ev}_a) \neq \{0\}$.$a$ 在 k 上的最小多项式是唯一的首一多项式 f_a，使得 $\ker(\mathrm{ev}_a) = \langle f_a\rangle$

定义 1.17 (理想/ideal)

设 R 是环，I 是 R 的子环，如果对于 $\forall i \in I, \forall r \in R$ 有 $ir, ri \in I$ 成立，则称 I 是 R 的理想子环 (ideal subring)，简称理想，这样的规律称为吸收律 (absorption property)。如果只成立 $ra \in I$，则称为左理想；如果只成立 $ar \in I$，则称为右理想

可以证明，最小多项式 f_a 是 $k[x]$ 中使得 $f(a) = 0$ 的唯一的不可约 (irreducible) 首一多项式，这里不可约是指不可被分解为非常数多项式的乘积，而唯一性是因为 $k[x]$ 是一个主整环 (principal integral domain)，即所有理想都是主理想的、不存在带零因子 (zero divisor) 的交换环 (commutative ring)

例题 1.4 根据艾森斯坦判别法 (criterion of Eisenstein)，对于任意质数 (prime number) p 和正整数 n，$x^n - p \in \mathbb{Q}[x]$ 都是不可约的，所以 $x^n - p$ 是 $\sqrt[n]{p}$ 在 $\mathbb{Q}$ 上的最小多项式

定义 1.18 (商环)

如果 I 是环 R 的理想，那么 $(I,+) \lhd (R,+)$，因为环对于加法是交换的，交换群的子群又是正规子群，从而可以定义商群 R/I，其中的元素是 I 的陪集 $r + I$，并且对于 $\forall a, b \in R$ 定义了这样的加法 $(a + I) + (b + I) = (a + b) + I$。希望能够定义乘法 $(a + I)(b + I) = ab + I$ 使得 R/I 是环。可以验证，这样的乘法是良定义、满足结合律而且封闭的

设 I 是环 R 的理想，如果按照上述加法和乘法进行定义，则 R/I 是环，称为商环 (quotient ring or factor ring)

定义 1.19 (环同态与环同构)

如果 R 和 S 是两个环，存在一个映射 $\varphi : R \to S : r \mapsto \varphi(r)$ 使得其对于 $\forall r_1, r_2 \in R$ 有 $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2), \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ 都成立，则称 φ 是 R 到 S 的一个环同态 (ring homomorphism)。如果 φ 是双射，则称 φ 是 R 到 S 的一个环同构 (ring isomorphism)，此时称两个环是同构的，记为 $R \cong S$。如果这个映射 $\varphi : R \to R$ 是同构映射，即 $R \cong R$，则称 φ 是一个 R 到 R 的自同构 (automorphism)

通过**环同态**理论，可以证明下面的结论

定理 1.2

若 $a \in K$ 在 k 上是代数的，且 f_a 是相应的最小多项式，则 $k(a) \cong k[x]/\langle f_a\rangle$，且 $[k(a) : k] = \deg(f_a)$

注 因此，一个最小多项式可以界定一个简单代数扩张。此外，最小多项式还可以定义一个域同构的扩张。若 $\phi : k \to k'$ 和 $\Phi : K \to K'$ 是域同构，且 K/k 和 K'/k' 为域扩张，且 $\Phi|_k = \phi$，那么 Φ 叫作 ϕ 的扩张。通过由同构 $\phi : k \to k'$ 定义的另一个同构

$$\phi^* : k[x] \to k'[x], \quad \sum_i a_i x^i \mapsto \sum_i \phi(a_i) x^i$$

定理 1.3

对于具有相同的最小多项式的、在 k 上为代数的 $a, a' \in K$，存在一个唯一的 k-同构 $\phi : k(a) \to k(a')$，使得 $\phi(a) = a'$

1.2.4 分裂域

接下来是分裂域的概念。对于一个非常数多项式 $f \in k[x]$，我们想找到一个有限域扩张，使得 f 在 K 中有根 (root)，甚至在 K 上分裂为线性因式 (linear factor)。对于一个 $k[x]$ 中的不可约多项式，我们总可以找到一个简单代数扩张 K/k，使得 $[K:k]=\deg(f)$，且 f 在 K 中有根。这里的 K 是由给 k 连接 (adjoin) f 的根得到，并且可以不断地给 k 连接 f 的根，直到 f 在 K 中可以分解为线性因式。最小的这样的域叫作 f 在 k 上的**分裂域**，它在同构的意义下是唯一的

定义 1.20 (分裂域)

令多项式 $f \in k[x]$ 的度数为 $n>0$。若一个有限域扩张 K/k 使得 f 在 K 上分裂为线性因式，即存在 $a_1,\cdots,a_n,b \in K$ 使得

$$f = b(x-a_1)\cdots(x-a_n)$$

且 f 不再任何中间域 $k \subseteq L \subsetneq K$ 上分裂，则 K 叫作 f 在 k 上的分裂域.

♣

注 可以证明，多项式的分裂域总是存在的，且若 K 是 f 在 k 上的分裂域，则 K 是 f 在任意中间域 L 上的分裂域

此外，分裂域也可以应用于域同构的扩张

定理 1.4

若 K 和 K' 是 f 在 k 上的分裂域，则存在同构 $\Phi: K \to K'$，它是自同构 $\phi: k \to k$ 的扩张

♡

例题 1.5 若 r 是 x^4+1 在 $\mathbb{Q}$ 的一个扩张里的一个根，那么 $-r, \frac{1}{r}, -\frac{1}{r}$ 也是 x^4+1 的根，且这些根是不同的；那么，我们在 $\mathbb{Q}(r)$ 上就得到了一个分裂 $x^4+1=(x-r)(x+r)\left(x-\frac{1}{r}\right)\left(x+\frac{1}{r}\right)$，即 $\mathbb{Q}(r)$ 是 $\mathbb{Q}$ 的一个分裂域

1.2.5 正规扩张

正规域扩张是由分裂域得到的

定义 1.21 (正规扩张)

若一个域扩张 K/k 是代数的，且任意在 K 中有根的不可约多项式 $f \in k[x]$ 在 K 中分裂为线性因式，则称 K/k 是一个正规扩张

♣

注 正规域扩张由分裂域得到的结论可以通过域同构的扩张和最小多项式来证明

命题 1.1

若一个域扩张 K/k 是有限的，那么，当且仅当 K 是 $k[x]$ 中的一个多项式的分裂域，K/k 是正规的

♠

例题 1.6 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不是一个正规扩张 ($\mathbb{Q}(\sqrt[3]{2})$ 不是 $\mathbb{Q}$ 的一个分裂域)，而 $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)/\mathbb{Q}$ 是一个正规扩张 ($\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)$ 是 $\mathbb{Q}$ 的一个分裂域)

1.2.6 可分扩张

另一个非常重要的扩张是**可分扩张** (separable extension)，这个概念是为了避免多重根而提出的。一个正规可分扩张就是后面要介绍的伽罗瓦扩张

定义 1.22

令 $f \in k[x]$，并令

$$f = b(x-a_1)^{m_1}\cdots(x-a_l)^{m_l}, m_i>0, a_1,\cdots,a_l \in K \text{ 互不相同}$$

为 f 在域扩张 K/k 上的一个分为线性因式的分裂。若 $m_i=1$，则 a_i 叫作一个单根。若 $m_i>1$，则 a_i 叫作一个阶为 m_i 的多重根。若对于一个代数域扩张 K/k，所有在 K 中有根的不可约多项式 $f\in k[x]$ 在它们的分裂域中只有单根，则 K/k 叫作一个可分扩张。若 k 的所有代数扩张 K/k 都是可分的，则 k 叫作完美的 (perfect)

注 判断多重根的标准是：如果一个根既是多项式 $f=\sum_{i=0}^{n}a_ix^i\in k[x]$ 的根，又是其导数 (derivative) $f'=\sum_{i=1}^{n}ia_ix^{i-1}\in k[x]$ 的根，则它是 f 的一个多重根，反之亦然。因此，可以得到，对于一个不可约多项式 $f\in k[x]$，当且仅当 $f'\neq 0f$ 在其分裂域中没有多重根

注 任意特征为 0 的域都是完美的，即它的所有代数域扩张都是可约的

下面要证明的**本原元定理**是一个非常重要的定理，它在 Galois 理论中有重要的应用。此定理说，任意有限的可约域扩张 K/k 都是简单的，即 $K=k(a)$，这里 $a\in K$。特别地，任意特征为 0 的有限扩张都是简单的

定理 1.5 (本原元定理/theorem of the primitive element)

若 K/k 是一个有限可分域扩张，那么存在 $a\in K$，使得 $K=k(a)$。这个元素 a 叫作一个本原元

证明 为简化讨论，假设 k 是无限的，比如 k 是一个特征为 0 的域。此结论对有限的 k 也成立，但证明会更复杂一些

由于 $[K:k]$ 是有限的，$K=k(a_1,\cdots,a_n)$，这里 $a_1,\cdots,a_n\in K$。现在对 n 进行归纳：$n=1$ 的基本情况无需证明。对于 $n>2$，根据级纳假设，$k(a_1,\cdots,a_{n-1})=k(a)$，这里 $a\in K$，故 $K=k(a,a_n)$. 因此，我们可以假设 $n=2$，且 $K=k(a,b)$。接下来证明，$K=k(c)$，这里 $c=a+zb$，其中 $z\in k$

令 f 和 g 分别为 a 和 b 在 k 上的最小多项式。令 L/K 为一个域扩张，使得 f,g 在 L 上分裂为线性因式。令 $x_1=a,x_2,\cdots,x_n$ 为 f 的根，并令 $y_1=b,y_2,\cdots,y_m$ 为 g 的根。由于 K/k 是可分的，$b\neq y_j\forall j\neq 1$。对于 $1=1\cdots,n$ 和 $j=2,\cdots,mz_{ij}=\frac{x_i-a}{b-y_j}$ 使得 $a+z_{ij}b=x_i+z_{ij}y_j$，且在 L 中是唯一的。由于 k 是无限的，可以选择 z，使得它和所有 z_{ij} 都不同，故 $a+zb\neq x_i+zy_j$ 除非 $i=j=1$

令 $c=a+zb$，显然 $k(c)\subseteq k(a,b)$。需要证明 $k(a,b)\subseteq k(c)$。定义 $h\in k(c)[x]$ 为 $h(x)=f(c-zx)$，那么 $h(b)=f(c-zb)=f(a)=0$。由于 b 是 g 在 L 中的一个根，$x-b$ 是 h 和 g 在 $L[x]$ 中的一个公因式。接下来想要证明，$x-b$ 是最大公因式 (greatest common divisor)。由于 g 在 L 上分裂为线性因式，最大公因式是 g 的某些线性因式的乘积。对于 $j\neq 1c-zy_j\neq x_i\forall i$，故 $h(y_j)=f(c-y_j)\neq 0$。因此，$x-y_j$ 不是 h 的因式，故 $x-b$ 是 h 和 g 的最大公因式

根据欧几里得算法 (Euclidean algorithm)，$h\in k(c)[x]$ 和 $g\in k[x]$ 的首一最大公因式在 $k(c)$ 中。因此，$x-b\in k(c)[x]$，即 $b\in k(c)$。又因为 $z\in ka=c+zb\in k(c)$，故 $k(a,b)\subseteq k(c)$

1.3 伽罗瓦群和伽罗瓦扩张

1.3.1 伽罗瓦群

伽罗瓦理论通过域的自同构的群将群论和域论连接起来。更准确地说，在伽罗瓦理论中，若想研究一个有限域扩张 K/k，可以通过研究由 K 的 k-自同构构成的**伽罗瓦群** $\mathrm{Gal}(K/k)$ 来完成。伽罗瓦群包含了有关域扩张的很多信息，也有人说现代数论不过是对伽罗瓦群 $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ 的研究

定义 1.23 (伽罗瓦群/Galois group)

令 K/k 为一个域扩张。K 在 k 上的伽罗瓦群 $\mathrm{Gal}(K/k)$ 是 k-自同构 $\phi:K\to K$ 的集合，即 $\phi(a)=a,\forall a\in k$。由于两个 k-自同构的复合是一个 k-自同构，这个集合和复合运算构成一个群

注 对于简单代数扩张 $k(a)/k$，它的伽罗瓦群可以由 a 的最小多项式的根的置换 (permutation) 群的子群来界定。此结论可以表述为下面这个定理

定理 1.6

若 $k(a)/k$ 是一个度数为 n 的简单代数扩张，f 为 a 在 k 上的最小多项式，R 为 f 在 $k(a)$ 中的根的集合，且 $S(R)=\{\sigma:R\to R \text{ 双射}\}$ 为 R 的置换群，那么它的伽罗瓦群 $\mathrm{Gal}(k(a)/k)$ 和 $S(R)$ 的一个阶为 $|R|\le n$ 的子群同构

♡

注 在这个定理的证明中，构造映射 $\mathrm{res}_R:\mathrm{Gal}(k(a)/k)\to S(R),\phi\mapsto\phi|_R$，并证明它是一个单射的群同态

例题 1.7 由于 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的最小多项式 x^2-2 有两个根 $\pm\sqrt{2}\,\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ 包含 id 和 $\pm\sqrt{2}\mapsto\mp\sqrt{2}$；由于 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的最小多项式 x^3-2 有一个根 $\sqrt[3]{2}\,\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 只包含 id

1.3.2 伽罗瓦扩张

伽罗瓦群是伽罗瓦理论中第一个重要概念，而第二个重要概念是伽罗瓦扩张，它是有限可分正规域扩张

定义 1.24 (伽罗瓦扩张)

若一个有限域扩张 K/k 是可分的且正规的，即任意在 K 中有根的不可约多项式 $f\in k[x]$ 在 K 中分裂为线性因式，且这样的多项式在其分裂域中只有单根，则 K/k 叫作一个伽罗瓦扩张

♣

借助本原元定理，可得推论

推论 1.1

若 K/k 为一个度数为 n 的伽罗瓦扩张，那么 $\mathrm{Gal}(K/k)$ 和 $\{1,\cdots,n\}$ 的置换群 S_n 的一个子群同构，且 $|\mathrm{Gal}(K/k)|=n$

♡

通过利用最小多项式构造的域同构的扩张，可以得出：对于一个伽罗瓦扩张 K/k 和 $a,b\in K$，当且仅当 a,b 有相同的最小多项式，存在 $\phi\in\mathrm{Gal}(K/k)$ 使得 $\phi(a)=b$。这样可以得到下面的结论，此结论对是伽罗瓦基本定理的证明的一部分

定理 1.7

若 K/k 是一个伽罗瓦扩张，则 $k=\{a\in K:\phi(a)=a\forall\phi\in\mathrm{Gal}(K/k)\}$

♡

证明 根据定义，若 $a\in k$ 且 $\phi\in\mathrm{Gal}(K/k)$，则 $\phi(a)=a$。现在假设 $\phi\in\mathrm{Gal}(K/k)$，并令 f 为 a 在 k 上的最小多项式。由于 K/k 是正规的，f 在 K 上分裂。令 b 为 f 的一个根，那么存在 $\phi\in\mathrm{Gal}(K/k)$ 使得 $\phi(a)=b$，故 $a=b$。由于 K/k 是可分的，f 没有多重根，故 $f=x-a\in k[x]$，即 $a\in k$

注 这个定理说的是，对于一个伽罗瓦扩张 K/kk 就是这个扩张中被伽罗瓦群 $\mathrm{Gal}(K/k)$ 的元素固定的元素的集合。因此，伽罗瓦群 $\mathrm{Gal}(K/k)$ 的子群与中间域 $K/L/k$ 被联系起来了。通常将域扩张视作多项式的分裂域，故我们将一个多项式 $f\in k[x]$ 的伽罗瓦群 $\mathrm{Gal}(f)$ 定义为其分裂域的伽罗瓦群。一个多项式的的伽罗瓦群也可以由它的根的置换群的一个子群界定

定义 1.25

令 $f\in k[x]$ 是一个非常数多项式，并令 K 为 f 在 k 上的分裂域，这里 K 在在 k 上是恒等映射的同构下是唯一的。那么，f 的伽罗瓦群是 $\mathrm{Gal}(f)=\mathrm{Gal}(K/k)$

♣

例题 1.8 令 $f=x^3-2\in\mathbb{Q}[x]$，那么 $\mathrm{Gal}(f)$ 是 S_3 的一个子群；令 K 为 $\mathbb{Q}$ 的分裂域，这里 $K/\mathbb{Q}$ 是一个伽罗瓦扩张；那么 $K=\mathbb{Q}\left(\sqrt[3]{2},e^{2\pi i/3}\right)$，且 $[K:\mathbb{Q}]=3\cdot2=6$，故 $|\mathrm{Gal}(f)|=6$；又因为 $\mathrm{Gal}(f)$ 是 S_3 的一个子群，$\mathrm{Gal}(f)=S_3$

1.4 伽罗瓦理论基本定理

1.4.1 子群和中间域之间的双射

伽罗瓦理论基本定理将伽罗瓦扩张 K/k 的中间域和域扩张的伽罗瓦群 $\mathrm{Gal}(K/k)$ 联系在一起，因此它可以将域论中的问题转化为群论的问题，使得它们更容易解决。在介绍伽罗瓦理论基本定理的证明之前，需要引入**固定域**的概念

定义 1.26 (固定域/fixed field)

若 K/k 是一个域扩张，那么对于其伽罗瓦群的子群 $H \subseteq \mathrm{Gal}(K/k)$，$H$ 的固定域是

$$\mathrm{Fix}(H) = \{\phi(a) = a \forall \phi \in H\}$$

♣

注 $\mathrm{Fix}(H)$ 显然是 K 的一个子域。此外已经在定理1.7中证明，对于一个伽罗瓦扩张 K/k $\mathrm{Fix}(\mathrm{Gal}(K/k)) = k$ 。还有，对于 K/k 的一个中间域 L ，$\mathrm{Gal}(K/L) = \{\phi \in \mathrm{Gal}(K/k) : \phi|_L = \mathrm{id}\}$ 是 $\mathrm{Gal}(K/k)$ 的一个子群

下面的定理就是伽罗瓦理论基本定理，由三部分构成

定理 1.8 (伽罗瓦理论基本定理)

令 K/k 为一个伽罗瓦扩张，L 为 K/k 的一个中间域，并令 H 为 $\mathrm{Gal}(K/k)$ 的一个子群：

1. 映射 $H \mapsto \mathrm{Fix}(H)$ 和 $L \mapsto \mathrm{Gal}(K/L)$ 是 $\{\mathrm{Gal}(K/k)$ 的子群 $\} \longleftrightarrow \{K/k$ 的中间域 $\}$ 之间互为逆的双射. 换句话说，$\mathrm{Fix}(\mathrm{Gal}(K/L)) = L$ ，且 $\mathrm{Gal}(K/\mathrm{Fix}(H)) = H$
2. 对于 $\mathrm{Gal}(K/k)$ 的子群 $H [K : \mathrm{Fix}(H)] = |H|$ ，且 $[\mathrm{Fix}(H) : k] = [\mathrm{Gal}(K/k) : H]$
3. 对于中间域 $k \subseteq L \subseteq K [K : L] = |\mathrm{Gal}(K/L)|$ ，且 $[L : k] = [\mathrm{Gal}(K/k) : \mathrm{Gal}(K/L)]$

♡

证明 第一部分是主要的，而第二和第三部分都是简单推论

1. 令 L 为 K/k 的一个中间域，则 K/L 是一个伽罗瓦扩张。由于 K 是一个多项式在 k 上的分裂域，故也是在 L 上的分裂域，因此 K/L 是一个正规扩张。令 f 为 a 在 L 上的最小多项式，并令 g 为 a 在 k 上的最小多项式。由于 K/k 是可分的，g 在其分裂域中没有多重根。由于 f 是 g 的因式，f 在其分裂域中没有多重根，故 K/L 是可分的。根据定理1.7，$\mathrm{Fix}(\mathrm{Gal}(K/L)) = L$

令 H 为 $\mathrm{Gal}(K/k)$ 的一个子群。想要证明 $\mathrm{Gal}(K/\mathrm{Fix}(H)) = H$。根据本原元定理，$K = k(a)$ ，其中 $a \in K$. 定义 $f = \prod_{h \in H}(x - h(a))$ ，故 $\deg(f) = |H|$。由于 $k(a)/k$ 是一个简单扩张，$h_1(a) = h_2(a)$ 意味着 $h_1 = h_2$ ，故 f 的根是不同的。将 f 写作 $f = \sum_i b_i x^i$ ，其中 $b_i \in k(a)$。接下来要证明 $b_i \in \mathrm{Fix}(H)$。对于 $l \in H$ ，令 $l_*(f) = \sum_i l(b_i)\, x^i$。由于 $l, h \in H$ ，$l_*(f) = \prod_{h \in H}(x - l(h(a))) = \prod_{h \in H}(x - h(a)) = f$。因此，$b_i \in \mathrm{Fix}(H)$ ，即 $f \in \mathrm{Fix}(H)[x]$。这样，$f(a) = 0$ ，故 a 在 $\mathrm{Fix}(H)$ 上的最小多项式 g 是 f 的因式。由于 $K = k(a) = F(a)$ ，有

$$|\mathrm{Gal}(K/\mathrm{Fix}(H))| = [K : \mathrm{Fix}(H)] = \deg(g) \leq \deg(f) = |H|$$

由于 H 是 $\mathrm{Gal}(K/\mathrm{Fix}(H))$ 的一个子群，我们有 $|\mathrm{Gal}(K/\mathrm{Fix}(H))| = |H|$ ，即 $\mathrm{Gal}(K/\mathrm{Fix}(H)) = H$

2. 由于 $\mathrm{Fix}(H)$ 是 K/k 的一个中间域，$K/\mathrm{Fix}(H)$ 是一个伽罗瓦扩张。因此，$[K : \mathrm{Fix}(H)] = |\mathrm{Gal}(\mathrm{K}/\mathrm{Fix}(\mathrm{H}))| = |H|$. 根据度数定理和朗格朗日定理，

$$[\mathrm{Fix}(H) : k] = [K : k]/[\mathrm{Fix}(H) : k] = |\mathrm{Gal}(K/k)|/|H| = [\mathrm{Gal}(K/k) : H]$$

3. 由于 K/L 是一个伽罗瓦扩张，$[K : L] = |\mathrm{Gal}(K/L)|$。那么

$$[L : k] = [K : k]/[K : L] = |\mathrm{Gal}(K/k)|/|\mathrm{Gal}(K/L)| = [\mathrm{Gal}(K/k) : \mathrm{Gal}(K/L)]$$

1.4.2 正规子群和正规扩张一一对应

通过伽罗瓦理论基本定理，可以知道，通过伽罗瓦群和固定域，可以在伽罗瓦扩张 K/k 的中间域和此域扩张的伽罗瓦群的子群之间构造一个双射一一中间域 L/k 对应 $\mathrm{Gal}(K/k)$ 的子群 $\mathrm{Gal}(K/L)$ 。另外一个重要结论是，当且仅当 L/k 是一个正规扩张，$\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群，且

$$\mathrm{Gal}(L/k) = \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$$

这个结论是伽罗瓦理论基本定理的第二部分

定理 1.9

令 K/k 为一个伽罗瓦扩张，并令 L 为 K/k 的一个中间域。令 $\alpha \in \mathrm{Gal}(K/k)$ ，并令 $\alpha(L) = \{\alpha(a) : a \in L\}$。显然 $\alpha(L)$ 是 K/k 的一个中间域。那么，下面的陈述是等价的：

1. L/k 是一个正规扩张
2. $\alpha(L) = L \forall \alpha \in \mathrm{Gal}(K/k)$
3. $\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群

♡

证明 $(1 \Rightarrow 2)$ 令 $a \in L$ 并令 f 为 a 在 k 上的最小多项式. 由于 L/k 是一个正规扩张，f 的所有根都在 L 中。令 $\alpha \in \mathrm{Gal}(K/k)$. 由于 $f(\alpha(a)) = \alpha(f(a)) = 0\alpha(a) \in L$ ，故 $\alpha(L) \subseteq L$。类似地，可以证明 $\alpha(L)^{-1} \subseteq L$ ，即 $L \subseteq \alpha(L)$

$(2 \Rightarrow 3)$ 令 $\alpha, \beta \in \mathrm{Gal}(K/k)$，$\beta \in \mathrm{Gal}(K/\alpha(L))$ 等价于 $\beta(\alpha(a)) = \alpha(a) \forall a \in L$。这等价于 $\alpha^{-1}(\beta(\alpha(a))) = a \forall a \in L$, 而这等价于 $\alpha^{-1}\beta\alpha \in \mathrm{Gal}(K/L)$ ，即 $\beta \in \alpha\,\mathrm{Gal}(K/L)\alpha^{-1}$。那么，

$$\mathrm{Gal}(K/L) = \mathrm{Gal}(K/\alpha(L)) = \alpha\,\mathrm{Gal}(K/L)\alpha^{-1}$$

因此，$\mathrm{Gal}(K/L)$ 是 $\mathrm{Gal}(K/k)$ 的一个正规子群

$(3 \Rightarrow 1)$ 令 $\alpha \in \mathrm{Gal}(K/k)$. 由于 $\mathrm{Gal}(K/L) = \alpha\,\mathrm{Gal}(K/L)\alpha^{-1} = \mathrm{Gal}(K/\alpha(L))$ ，根据伽罗瓦理论基本定理，$L = \alpha(L)$。令 $f \in k[x]$ 为有根 $a \in L$ 的不可约多项式，并令 b 为 f 在 K 中的另一个根。由于 a, b 在 k 上的最小多项式都是 f ，又根据定理1.3，存在 $\alpha \in \mathrm{Gal}(K/k)$ 使得 $\alpha(a) = b$。那么，$b \in \alpha(L) = L$ ，故 K/k 是一个正规扩张

推论 1.2

可以用 K/L 和 K/L 的伽罗瓦群的商群来界定中 L/k 的伽罗瓦群，即

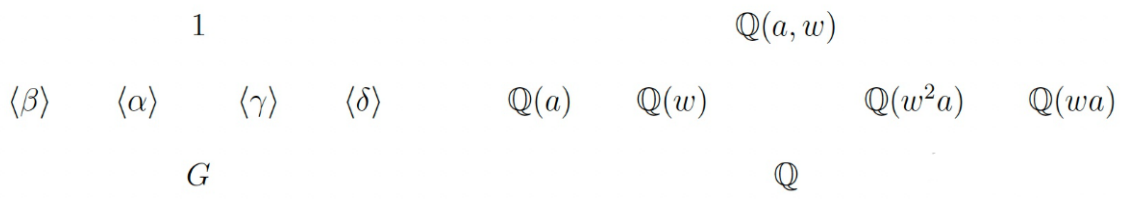
$$\mathrm{Gal}(L/k) \cong \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$$

这是因为 $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$ 和 $\mathrm{Gal}(L/k)$ 的一个子群，且 $|\mathrm{Gal}(L/k)| = |\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)|$

♡

例题 1.9 令 $\mathbb{Q}(a, w)$ 为 $x^3 - 2 \in \mathbb{Q}[x]$ 的一个分裂域，这里 $a = \sqrt[3]{2}$ ，且 $w = e^{2\pi i/3}$ 。已知，$G = \mathrm{Gal}(\mathbb{Q}(a, w)/\mathbb{Q}) = S_3$ 。S_3 的 6 个子群和对应的中间域如图??所示

其中 $\alpha(a) = wa, \alpha(w) = w\beta(a) = a, \beta(w) = w^2\gamma(a) = wa, \gamma(w) = w^2$ ，$\delta(a) = w^2 a, \delta(w) = w^2$ 。G 的正规子群 $1, \langle\alpha\rangle, G$ 对应正规扩张 $\mathbb{Q}(a, w), \mathbb{Q}(w), \mathbb{Q}$



1.5 二次、双二次和三次多项式

二次 (quadratic)、双二次 (biquadratic) 和三次 (cubic) 多项式的分裂域是特征为 0 的域 k 的伽罗瓦扩张的最简单的例子，有助于更好地理解伽罗瓦理论基本定理

1.5.1 二次和双二次扩张

二次多项式的情况是最简单的。令 $f=x^2+px+q\in k[x]$ 为一个不可约多项式，则根据二次多项式求根公式，它的两个根是 $-\frac{p}{2}\pm\sqrt{\frac{p^2}{4}-q}$ 。令 $\alpha=\sqrt{\frac{p^2}{4}-q}$ ，则 $k(\alpha)/k$ 是一个伽罗瓦扩张。此外，$[k(\alpha):k]=2$ ，且伽罗瓦群 $\mathrm{Gal}(k(\alpha)/k)$ 是由 $\alpha\mapsto-\alpha$ 生成的 $\mathbb{Z}/2\mathbb{Z}$ 。显然，$k(\alpha)$ 和 k 之间没有中间域

一个双二次多项式是两个二次多项式的乘积，这样的多项式的情况也比较简单。令 α 为一个不可约首一二次多项式 $f\in k[x]$ 的根，并令 β 为另一个不可约首一二次多项式 $g\in k[x]$ 的根，且 g 在 $k(\alpha)$ 上也不可约。那么，$[k(\alpha,\beta):k(\alpha)]=2=[k(\alpha):k]$ ，故 $[k(\alpha,\beta):k(\beta)]=[k(\alpha,\beta):k(\alpha)][k(\alpha):k]/[k(\beta):k]=2$ 。由于 $k(\alpha,\beta)$ 是 fg 在 k 上的分裂域，$k(\alpha,\beta)/k$ 是一个伽罗瓦扩张。令 α' 为 f 在 $k(\alpha)$ 中的另一个根，β' 为 g 在 $k(\beta)$ 中的另一个根，并令 $a=\alpha-\alpha' b=\beta-\beta'$ 。那么，$k(a)=k(\alpha)$ ，$k(b)=k(\beta)$ ，且 $k(a,b)=k(\alpha,\beta)$

由于 $k(\alpha,\beta)/k(\beta)$ 是一个简单扩张，在 $k(\alpha,\beta)$ 上存在一个唯一的 $k(\beta)$-自同构 ϕ ，使得 $\phi(\alpha)=\alpha'$ ，即 $\phi(a)=-a$ 。显然 $\phi^2=\mathrm{id}$ 。同理，在 $k(a,b)$ 上存在一个唯一的 $k(a)$-自同构 ψ ，使得 $\psi(b)=-b$ ，且 $\phi^2=\mathrm{id}$ 。此外，$\phi\psi=\psi\phi$ 。因此，$\mathrm{Gal}(k(\alpha,\beta)/k)$ 和 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 同构。此群的三个真子集 $H_1=\{\mathrm{id},\phi\},H_2=\{\mathrm{id},\psi\},H_1=\{\mathrm{id},\phi\psi\}$ 分别对应中间域 $L_1=k(a),L_2=k(b),L_3=k(ab)$

1.6 三次扩张

令 $f=y^3+a_2y^2+a_1y+a_0\in k[y]$ 。通过变量变换 $y=x-\frac{a_2}{3}$ ，可以假设二次项为 0 ，即 $f=x^3+px+q\in k[x]$ 。通过变量变换 $x=u-v$ ，得

$$f(u-v)=u^3-v^3-(3uv-p)(u-v)+q$$

为了使 $f(u-v)=0$ ，需要 $u^3-v^3+q=0$ ，且 $3uv-p=0$ 。将第二个等式 $v=\frac{p}{3u}$ 代入第一个等式，有

$$27u^6-p^3+27u^3q=0$$

通过变量变换 $y=u^3$ ，解关于 y 的二次方程，和 $u=\sqrt[3]{y}$ 和 $v=\sqrt[3]{u^3+q}$ ，得到三次多项式的一个根

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

下面介绍**关于不可约三次首一多项式 $f=x^3+px+q\in k[x]$ 的伽罗瓦理论**。令 K 为 f 在 k 上的分裂域。将 f 写作 $f=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ ，我们有 $\alpha_1+\alpha_2+\alpha_3=0$ ，$\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=p$ ，以及 $\alpha_1\alpha_2\alpha_3=-q$ 。第一个等式说明 $\alpha_3\in k(\alpha_1,\alpha_2)$ 。得到一个域的链 $k\subseteq L=k(\alpha_1)\subseteq K=k(\alpha_1,\alpha_2)$ 。那么，有 $L=K$ 和 $L\subsetneq K$ 两种可能性

若想搞清楚这两种情况何时发生，需要考察 f 在 $L[x]$ 中是如何分解的。由于 f 在 k 上不可约，$[L:k]=3$ 。在 $L[x]$ 中可将 f 写作 $f=(x-\alpha_1)g$ ，其中 $g=(x-\alpha_1)(x-\alpha_2)\in K[x]$ 。因此，若 g 在 $L[x]$ 中是可约的，则 $L=K$ ，且 $[K:k]=3$ ；若 g 在 $L[x]$ 中是不可约的，则 $[K:L]=2$ ，且 $[K:k]=6$

若 $L=K$ ，则 K/k 是一个简单代数扩张。那么，$\mathrm{Gal}(K/k)$ 是一个对 $\{\alpha_1,\alpha_2,\alpha_3\}$ 有简单可递的 (simply transitive) 群作用 (group action) 的 S_3 的子群。因此，$\mathrm{Gal}(K/k)$ 是由 $\{\alpha_1,\alpha_2,\alpha_3\}$ 的循环置换 (cyclic permutation) 构成的群。由于这个群没有非平凡 (nontrivial) 子群，K/k 没有中间域。若 $L\subsetneq K$ ，则 $\mathrm{Gal}(K/k)$ 是对称群 (symmetric group) S_3

可以用判别式 (discriminant) 来判断这两种情况的哪一种会发生。

定义 1.27

令 $f \in k[x]$ 为一个度数为 n 的不可约多项式。令 K 为 f 在 k 上的分裂域，并令 $\alpha_1, \cdots, \alpha_n$ 为 f 在 K 中的根。那么判别式被定义为

$$D = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

定义 $\delta = \sqrt{D} = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$

♣

由于 D 在 $\alpha_1 \cdots, \alpha_n$ 的任意置换下是不变的，D 被 $\mathrm{Gal}(K/k)$ 固定，故 $D \in k$ 。对于 $f = x^3 + px + qD = -4p^3 - 27q^2$ 。由判别式可知 $\mathrm{Gal}(K/k)$ 是否只包含偶置换 (even permutation)

命题 1.2

当且仅当 D 在 k 中是一个平方，即 $\delta \in k$ 时，$\mathrm{Gal}(K/k)$ 只包含偶置换

♠

证明 令 $\sigma \in S_n$ ，则 $\sigma(\delta) = (-1)^m \delta$ ，其中 m 是 $i < j$ 且 $\sigma(i) > \sigma(j)$ 的数对数。因此，$\sigma(\delta) = \mathrm{sign}(\sigma)\delta$. 那么，当且仅当 $\mathrm{Gal}(K/k)$ 只包含偶置换，δ 被所有 $\sigma \in \mathrm{Gal}(K/k)$ 固定

已知，S_3 有 3 个阶为 2 的、由长度为 1 的轮换 (transposition) 生成的子群，还有一个阶为 3 的、由循环置换生成的子群，这个子群只包含偶置换。那么，K/k 的中间域 $k(\alpha_1), k(\alpha_2), k(\alpha_3)$ 分别是轮换 $\alpha_2 \mapsto \alpha_3, \alpha_1 \mapsto \alpha_3, \alpha_1 \mapsto \alpha_2$ 的固定域，而 $k(\delta)$ 是F环置换的固定域