Field

颜成子游

2022 年 5 月 11 日

目录

经过了群，环，模，线性代数的学习，我们开始研讨代数性质最丰富的结构——域。

1 域的基本概念

域的概念在学习环的时候就已经有介绍过。我们再重复一遍

定义 1.1 交换的除环是域。即在域中，除零外的其他元素都有逆元，并且他们之间的乘法运算封闭。

对于域，有如下比较明显的事实：

定理 1.0.1

1. 设 R 是交换幺环，M 是 R 的极大理想，那么 R/M 是一个域。

2. 有限的整环是域。

3. R 是无零因子环，并且只有有限个理想（包括左，右，双边理想）。则 R 是除环。（可以用这个定理说明域中除的性质。）

2 域的代数闭包

前面我们讨论了多项式 $f(x) \in F[x]$ 在 F 中的分裂域。我们证明了它一定存在，并且在保 F 同构的意义下唯一。自同构群的阶有限，$|Aut(E)| \leq [E:F]$. 并且 $[E:F]|n!$。

我们考虑下列三个问题：

1. 取 $\{f_k\}_{k=1}^n$，是否存在域扩张 E 使得每个 f_k 都分裂?
2. 取 S 为多项式集合，并且为无限集合。是否存在域扩张 E 使得每个 $f \in S$ 都分裂?
3. $\forall f \in F[x]$，是否存在一个域扩张 E 使得 f 分裂?

第一个问题，只需要取 g 为 n 个多项式的积即可。

我们先讨论第三个问题，这引出了“代数闭包”的概念：

2.1 代数闭包的概念，等价形式

定义 2.1 称 E 是 F 的代数闭包，如果 E 是 F 的代数扩张，并且任意 $F[x]$ 中的多项式都在 E 中分裂。

代数闭包的名字让人联想到代数闭域。值得庆幸的是，代数闭包确实是代数闭域。

定义 2.2 称 E 是 F 的代数闭包，如果 E 是 F 的代数扩张，并且 E 代数封闭。

我们验证这两个定义等价：

命题 2.1.1 两个定义等价。

证明 定义 2 推导定义 1：

显然 F 上多项式都是 E 上的多项式。由于 E 封闭，从而只要一步步去掉一次因式，就有 F 分裂。

定义 1 推导定义 2：

如果有 $g \in E[x]$ 在 E 上没有根，取其分裂域 K，根据代数扩张传递性，则 K 是 F 的代数扩张。取 $\alpha \in K$，则 $f_\alpha \in F[x]$ 是 α 最小多项式。从而 f_α 分裂于 E，于是 $\alpha \in E$。矛盾！从而任意多项式都有根。 □

因此我们意识到，如果 $K/E/F$，E 是代数闭包，那么 $K = E$。这某种意义上说明 E 是“最大的代数扩张”。我们还可以从另外一个意义上说明这件事：

定理 2.1.1 (代数闭包是最大的代数扩张) *设 E 是 F 的代数闭包，那么任取 K 是 F 的代数扩张，存在嵌入映射：*

$$i : K \to E, \quad i|_F = id_F$$

如果 $K/E/F$，K 也是代数扩张，那么 $K = E$。

证明 考虑集合 $S = \{(L, i_L)|L \subset K\}$。$i_L$ 表示从 L 到 E 存在嵌入映射，为代数扩张。

显然集合 S 不是空集。

定义偏序关系：$<$, 若 $L_1 \subset L_2$ 且 $i_{L_2}|_{L_1} = i_{L_1}$.

那么 S 中的全序集合有上界。因为把这个全序集合中的所有 L 取并，定义 i，i 作用在并集上，每个元素的像就是在这个全序集合中的像。(映射是保持子集不变的)。

根据 Zorn 引理，S 也有最大值。即有一个 K' 满足：

$$\forall (L, i_L) \in S, L \subset K', i_{K'}|_L = i_L$$

下面证明 $K' = K$。

我们假设 $\alpha \in K \setminus K'$, 那么 α 在 K' 中有最小多项式 f_α。从而 $K'(\alpha)$ 满足：

$$j : K'(\alpha) \to E$$

(这是容易验证的) 这就与 K' 的最大性矛盾了。于是 α 是不存在的。

于是 $K' = K$ □

由这种“最大”性，我们不难想到，代数闭包一定是唯一的：

定理 2.1.2 (代数闭包唯一性) *任何一个域 K 的代数闭包，在同构意义下（保持 F）一定是唯一的。*

证明 取 K 的代数闭包 F,$\overline{F}$。我们有：

$$i_1 : F \to \overline{F}$$

$$i_2 : \overline{F} \to F$$

于是：

$$i : F \to F, i = i_2 \circ i_1$$

是一个嵌入映射。

假如这个嵌入映射不是满射，那么有：$\alpha \in F \setminus i(F)$. $i(F)$ 包含 K, 从而 α 是 $i(F)$ 上的代数元。取最小多项式 $f_\alpha \in i(F)[x]$，定义：

$$i^{-1} : i(F) \to F$$

则 $i^{-1}(f_\alpha)$ 在 F 中必须分裂（代数闭包）。从而 i 映射回去后，f_α 也分裂。于是 $\alpha \in i(F)$ 矛盾!

于是有 F 与 $\overline{F}$ 同构。 □

2.2 代数闭包的存在性

接下来要解决的问题是，代数闭包一定存在。这一点是比较困难的，需要巧妙地构造：

定理 2.2.1 *任意一个域 K 的代数闭包一定存在。*

证明 我们定义多项式环：

$$K[\ldots, x_f, x_g, \ldots]$$

其中 x_f 的指标集是 K 中所有不可约多项式。

考虑由 $\{f(x_f)\}$ 生成的理想 I。我们证明 $1 \notin I$。

事实上，如果 $1 \in I$，那么 1 被 $f(x_f)$ 有限生成。

我们取 $f(x)$（这是有限个多项式）的分裂域，那么带入 x_f 为 f 的根，在这个分裂域上，$1 = 0$，显然这是矛盾的。于是 $1 \notin I$。

根据 Zorn 引理，存在一个极大理想 m：$I \subset m$。

考虑 $K_0 = K[\ldots, x_f, \ldots]/m$。那么 K_0 是由 $F \cup \{x_f + m\}$ 生成。

我们证明这是一个代数扩张：由

$$f(x_f + m) = f(x_f) + m = 0$$

从而生成元都是代数元，于是 K_0 是一个代数扩张。并且在这个代数扩张中，每个 K 上的不可约多项式都有一个根：$x_f + m$。从而我们一直把这个操作进行下去：

$$K \to K_0 \to K_1 \to K_2 \ldots$$

取 $F = \bigcup_{n \geq 0} K_n$,$F$ 中的元素都是代数元，并且对于每个 f 不可约，都能把所有的根给逐步包进去。从而 F 是代数闭包。 □

3 域的正规扩张

这是一种介于“分裂域”和代数闭包之间的域扩张。

定义 3.1 *E/F 是代数扩张，称 E/F 是**正规扩张**，若 $\forall f(x) \in F[x]$ ，若 f 不可约且在 E 中有根，则 f 在 E 中分裂。*

定义 3.2 *F 是域，$S \subset F[x] \setminus F$，若 E/F 满足：*

1.$\forall f \in S$，f 在 E 中分裂。

2. 若 E' 有：$E/E'/F$ 且 E' 也满足：$\forall f \in S$，f 在 E' 中分裂。那么 $E = E'$

则称 E 是 S 在 F 上的分裂域。

同构意义下，S 的分裂域是使其中所有多项式都分裂的最小代数扩张。若 S 有限，则回到之前的问题。

介绍 S 的分裂域的原因来源于下面这个让人感到愉快的定理：

定理 3.0.1 E/F 正规等价于存在 $S \subset F[x] \setminus F$，$E/F$ 是 S 的分裂域扩张。

推论 3.0.2 若 E/F 是正规扩张，则 $\forall E/K/F$，E/K 也是正规扩张。

证明 E/F 是正规扩张，则可以找到 S 使得 E/F 是 S 的分裂域扩张

记 E' 是 S 在 K 上的分裂扩张。由于 S 在 E 上分裂，$K \subset E$ 得：

$$E' \subset E$$

但 E/F 是 S 的分裂域扩张，于是：

$$E \subset E'$$

于是 $E = E'$

于是 E/K 分裂域扩张。 □

推论 3.0.3 E/F 是有限扩张，则：

则 E/F 正规 $\Longleftrightarrow \exists f(x) \in F[x]$，$E/F$ 是 f 的分裂域扩张。

定义 3.3 取 K/F 扩张，称 K 的一个扩张 E 为 F 关于 K/F 的正规闭包，若：

1.E/F 正规。

2.$\forall M, E/M/K, M/F$ 正规，则 $M = E$。

推论 3.0.4 若 K/F 有限，则 K 有一个有限次的正规闭包 E/K。

证明 若 K/F 有限，则有：

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

记 $f_i \in F[x]$ 为 α_i 的最小多项式，$g = f_1 \ldots f_n$ E/F 是 g 的分裂扩张。则 $E/K/F$,E/F 正规扩张。

下证 E 最小。

设 $\exists E/M/K/F$ 满足 M/F 正规。

由于 $\alpha_1, \ldots, \alpha_n \in K \subset M$,$g$ 在 M 有根，从而分裂（不可约因子都有根）。

从而 $E \subset M$。

引理 3.0.5 记 F 为域，$f(x) \in F[x]$ 不可约，E/F 为 f 的分裂域扩张。

记 f 的根为 $\alpha_1, \ldots, \alpha_n$。则：

$$\forall \alpha_i, \alpha_j \exists \varphi : E \to E$$

为同构：

$$\varphi|_F = id_F, \varphi(\alpha_i) = \alpha_j$$

什么时候正规扩张的中间域也能给出一个正规扩张呢?

定理 3.0.6 E/F 正规且有限，记 $K : E/K/F$, 以下叙述等价：

1. K/F 正规。

2. $\forall \sigma : E \to E, \sigma|_F = id_F$，则 $\sigma(K) = K$。

3. $\forall \sigma : E \to E, \sigma|_F = id_F$，则 $\sigma(K) = K$。

证明 $1 \Rightarrow 2$: $2 \Rightarrow 3$: $3 \Rightarrow 1$: □

4 域的可分扩张

4.1 可分扩张的基本概念

定义 4.1 F 是一个域，$f(x) \in F[x]$ 不可约，记 K/F 是 $f(x)$ 的分裂域扩张。称 $f(x)$ 可分，若 f 在 $K[x]$ 中可分解：

$$f(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

满足 α_j 各不相同。

$g \in F[x]$ 可分当且仅当其不可约因子都可分。

定义 4.2 F 域，E/F 为代数扩张。称 $\alpha \in E$ 为可分元，若 α 在 F 中的最小多项式可分。

定义 4.3 E/F 是可分扩张，若 $\forall \alpha \in E$,α 是 F 中的可分元。

注：并不要求 f_α 在 E 中可分。只要求其在自身的分裂域扩张中，根互不相同。

命题 4.1.1 可分扩张的中间域，与两头都可分：

E/F 可分，$E/K/F$，从而 $E/K, K/F$ 均可分。

证明 显然 K/F 是可分扩张。我们只证明 E/K 是可分扩张。

任取 $\alpha \in E$，考虑 $f_\alpha \in F[x]$ 是 α 在 F 上的最小多项式。$g_\alpha \in K[x]$ 是 α 在 K 上的最小多项式。

我们有：在 $K[x]$ 中，$g_\alpha | f_\alpha$。

记 f_α 的分裂域为 L，从而 f_α 没有重根。于是 g_α 在 L 上也没有重根，于是在其自己的分裂域也没有重根，于是 α 在 K 上可分。于是 E/K 可分。 □

给出一个引理：

引理 4.1.1 记 $i : F \to F'$ 是域的同构，$f(x) \in F[x]$ 可分，则 $i(f) \in F'[x]$ 也可分。

证明 同构的域诱导的分裂域扩张也是同构的。从而只要一个没有重根，则另一个也没有重根。

定理 4.1.2 $F(\alpha)$ 是单代数扩张，且 $[F(\alpha) : F] = n$。记 f_α 是 α 的最小多项式，设 $\varphi : F \to E$ 域同态，则有：

1. 若 α 可分，且 $\varphi(f_\alpha) \in E[x]$ 在 E 中分裂，则有且仅有 n 个：

$$\tilde{\varphi} : F(\alpha) \to E, \tilde{\varphi}|_F = \varphi$$

2. 否则，这样的 $\tilde{\varphi}$ 的个数小于 n。

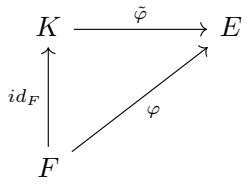
证明

定理 4.1.3 K/F 域扩张，$[K:F]=n$。$\forall\alpha\in K$，记 $f_\alpha\in F[x]$ 是 α 上的最小多项式。记 $\varphi:F\to E$:

1. 若 $\forall\alpha\in K$，α 可分，且 $\varphi(f_\alpha)$ 在 E 上分裂，则有且仅有 n 个:

$$\tilde{\varphi}:K\to E,\tilde{\varphi}|_F=\varphi$$

2. 否则，这样的 $\tilde{\varphi}:K\to E$ 的个数小于 n



证明 由于是有限扩张，从而只扩张了有限个代数元:

$$K=F(\alpha_1,\alpha_2,\dots,\alpha_n)$$

$$[K:F]=[k:F(\alpha_1,\dots,\alpha_{n-1})]:\cdots:[F(\alpha_1):F]=n$$

从而我们注意到，每一步扩张中，α_k 在 F 可分，那么在更大的域上也可分。并且其最小多项式也分裂。于是每一步都有几个选择。乘起来就是 n。若有满足条件的，那么第一步扩张就不满足。从而小于 n。□

推论 4.1.4 单代数扩张是可分扩张，当且仅当 α 是可分元。

证明 记 $f_\alpha\in F[x]$ 是 α 的最小多项式，扩张次数 n。
记 E/F 是 f_α 的分裂域扩张，从而 E/F 正规。
任取 $\beta\in E$,β 在 $F[x]$ 的最小多项式 f_β 分裂。
记 $i:F\to E$。
若 α 可分，那么就存在 n 个: $\tilde{i}:F(\alpha)\to E$。
由于 $\forall\beta\in F(\alpha)$，有 $\beta_1=\beta,\beta_2,\dots,\beta_n$ 使得:

$$F(\beta_1,\dots,\beta_n)=F(\alpha)$$

第一次扩张中，必须有 $[F(\beta):F]$ 个映射。从而 β 可分。 □

推论 4.1.5 设 $L=F(\alpha_1,\dots,\alpha_n)$ 是有限扩张。L/F 可分等价于 $\alpha_1,\dots,\alpha_n$ 在 F 中可分。

相比于可分不可约多项式，不可分的不可约多项式反而要少很多。接下来我们做这样的研究:

定义 4.4 如同 $\mathbb{C}[x]$ 的形式微商，我们也定义一般多项式的形式微商。不再赘述定义。

命题 4.1.2 F 是域，$f(x)\in F[x]$,$degf>0$。E/F 是分裂域扩张，下面叙述等价:

1.f 有重根。

2. 存在 $\alpha\in E$,$f(\alpha)=Df(\alpha)=0$。

3.$\exists g(x)\in F[x]$, 有 $deg\ g>0$, 满足 $g|f$, 且 $g|Df$。

证明 $1 \Rightarrow 2$: 设出重根, 求导即可得到答案。

$2 \Rightarrow 3$: g 设为 α 在 F 中的最小多项式。

$3 \Rightarrow 1$:

$g|f$ 意味着 g 在 E 中分裂。设 α 是 g 的一个根:

$$g = (x-\alpha)g_1(x), f = (x-\alpha)f_1(x)$$

求导即可得到完整的证明。 □

我们可以得出下面的结论:

定理 4.1.6 *F 是一个域, $f(x) \in F[x]$ 不可约。那么:*

$f(x)$ 不可分 $\Leftrightarrow \exists p$ 为素数, 使得 $Ch(F) = p$, 且存在 $a_k(k = 0, 1, \ldots, n)$, 使:

$$f(x) = \sum_{k=0}^{n} a_k x^{kp}$$

证明 若 f 不可分, 那么存在 α 使得:$f(\alpha) = Df(\alpha) = 0$。由于 f 不可约, 那么 f 是 α 在 F 上的最小多项式。

由于求导后多项式的次数必然降低, 而 $Df(\alpha) = 0$, 于是我们得到 f 求导后必然是零多项式。

于是我们有 $n_k * a_k = 0$ 对于每个 k 都成立。从而有质数 p 作为域的特征。并且 $n_k = pk$.

若 f 有如下的形式且不可约, 那么在 f 的分裂域上的 f 的根 α 都是重根。则 f 不可分。 □

例 4.1 *记 $F = \mathbb{F}_p(t)$ 是 $\mathbb{F}_p[t]$ 的分式域。证明 $x^p - t \in \mathbb{F}_p(t)[x]$ 不可分。*

证明

推论 4.1.7 *若 $Ch(F) = 0$, 则:*

1. 任何 $f(x) \in F[x] \setminus F$,$f$ 可分。

2.E/F 代数扩张, 则 E/F 可分。

定义 4.5 *完备域: 若 F 上的所有多项式都可分。*

设 F 是域, $F[x]$ 中的不可约多项式:

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

设 p 为素数, 考虑 $d = \gcd(k|a_k \neq 0)$ 的素数分解:

$$d = p^m d_1, p \nmid d_1$$

则有: $\exists g(x) \in F[x]$,

$$f(x) = g(x^{p^m})$$

我们给出以下命题:

命题 4.1.3 *若 $Ch(F) = p$, 则 $g(x)$ 不可约, 且可分。*

证明 不可约显然（因为 f 是不可约的）。

若 g 不可分，则有：

$$g = \sum_{k=0}^{n} a_k x^{kp}$$

$$f = \sum_{k=0}^{n} a_k x^{kp^{m+1}}$$

从而 $p^{m+1}|d$ 矛盾！ □

命题 4.1.4 *设 $Ch(F) = p$, 记 E/F 为 f 的分裂域扩张，则 f 在 E 中所有根的重数都为 p^m*

4.2 Frobenius 同态

定义 4.6 *F 是域，$Ch(F) = p$ 为素数。定义：*

$$Fr : F \to F \quad Fr(a) = a^p$$

命题 4.2.1 *F 是域，$Ch(F) = p$，则*

$$Fix(Fr) = \{a \in F | a^p = a\}$$

是 F 的素域 $\mathbb{F}_p$

证明 因为方程 $x^p - x = 0$ 的根只有 p 个，并且我们找到了 p 个：

$$0, 1, \ldots, p-1$$

命题 4.2.2 *F 是特征为 p 的域。若 F 是其素域的代数扩张，那么 Frobenius 同态是自同构。*

在证明这个命题前，我们给出两个引理：

引理 4.2.1 *E/F 是有限扩张，则 $End_F(E) = Aut_F(E)$。*

证明 比次数。 □

引理 4.2.2 *E/F 是代数扩张，则 $End_F(E) = Aut_F(E)$。*

证明 给出 $\varphi : E \to E, \varphi|_F = id_F$. 任给 $\alpha \in E$, 考虑 α 的最小多项式 $f_\alpha \in F[x]$。

记 $R = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ 是 E 中 f_α 所有根。

由于 $\varphi(f_\alpha) = f_\alpha$, 从而 $\varphi(R) \subset R$.

但是 R 是有限的，因此单射 φ 也是同构：$\exists \alpha_i, \varphi(\alpha_i) = \alpha$。

因此 φ 是满射，得到了同构。 □

从而命题的证明是显然的。

于是我们有推论：

推论 4.2.3 *F 是域，$Ch(F) = p$ 是素数，F 是其素域代数扩张。则 F 是完备的。*

证明 不妨设 $F/\mathbb{F}_p$。考虑 $Fr : F \to F$ 同构。

任取

$$f(x) = \sum_{k=0}^{n} a_k x^{kp}$$

只需说明 f 可约。但由于 Fr 同构，于是就有：$b_k^p = a_k$。

于是 $f(x) = (b_0 + b_1 x + \cdots + b_n x^n)^p$ 从而 f 可分。 □

若扩张不是代数的，我们不能说 F 一定不完备。但是如果 Fr 不同构，则一定不完备：因为 $x^p - a$ 不可约，不可分。

推论 4.2.4 *F 是特征为 p 的域。E/F 是代数扩张。则 F 完备可以导出 E 扩张。*

证明

5 Galois 理论

5.1 域的自同构及其不变子域

定义 5.1 *E/F 是扩张，E 上的 F 自同构的全体构成一个群，被称为 E/F 的 Galois 群，记为：$\mathrm{Gal}(E/F)$。*

由于代数扩张的域自同态全部为自同构，从而：

$$End_F(E) = \mathrm{Gal}(E/F)$$

定义 5.2 *取 $\varphi \in \mathrm{Gal}(E/F)$，$E/F$ 是扩张。记：*

$$\mathcal{K}(\varphi) := \{a \in E | \varphi(a) = a\}$$

为 φ 的不变子域。

命题 5.1.1 *φ 的不变子域是 E/F 的中间域。*

证明 $F \subset \mathcal{K}(\varphi)$。容易验证 $\mathcal{K}(\varphi)$ 是一个域。 □

类似地，我们可以考虑 $S \subset \mathrm{Gal}(E/F)$，定义 S 的不变子域为：

定义 5.3 *$S \subset \mathrm{Gal}(E/F)$，则：*

$$\mathcal{K}(S) : \{a \in E | \forall \varphi \in S, \varphi(a) = a\}$$

定义为 S 的不变子域。

命题 5.1.2 *$\mathcal{K}(S) = \bigcap_{\varphi \in S} \mathcal{K}(\varphi)$*

根据域的相交也是域的性质，我们不难得出，$\mathcal{K}(S)$ 也是 E/F 的中间域。

并且 $S_1 \subset S_2 \Longrightarrow \mathcal{S}_{\in} \subset \mathcal{S}_{\infty}$

从而，$\mathrm{Gal}(E/F)$ 中的子集似乎就能对应 E/F 中的一个中间域。

定义 5.4 K 是 E/F 的中间域。定义：

$$\Gamma(K) = \{\varphi \in \mathrm{Gal}(E/F) | \varphi|_K = id_K\}$$

必须验证 $\Gamma(K) < \mathrm{Gal}(E/F)$。但是验证的工作我们略去。

命题 5.1.3 $\Gamma(K) < \mathrm{Gal}(E/F)$。

命题 5.1.4 设 E/F 扩张，K_1, K_2 是 E/F 的中间域。则：

$$K_2 \subset K_1 \Longrightarrow \Gamma(K_1) < \Gamma(K_2)$$

但是反过来是不成立的。

例 5.1 记 $\mathbb{F}_p(t)$ 是 $\mathbb{F}_p$ 上多项式的分式域，考虑 $x^p - t$。假设 $\mathbb{F}_p(t)(\alpha)/\mathbb{F}_p(t)$ 是 $x^p - t$ 的分裂域扩张，$\alpha^p = t$。

此时 $\mathrm{Gal}(E/F)$ 是一个平凡群

现在对于集合 $\mathrm{Gal}(E/F)$ 和 $\{E/F\}$ 的中间域之间建立了两个映射：

$$\mathcal{K}, \quad \Gamma$$

一个很自然的问题是，这两个映射到底有什么关系?

命题 5.1.5 S 是 $\mathrm{Gal}(E/F)$ 的非空子集，K 是 E/F 的中间域。

1. $S \subset \Gamma(\mathcal{K}(S))$
2. $K \subset \mathcal{K}(\Gamma(K))$
3. $\mathcal{K}(S) = \mathcal{K}(\Gamma(\mathcal{K}(S)))$
4. $\Gamma(K) = \Gamma(\mathcal{K}(\Gamma(K)))$

证明略。

对于 $\mathrm{Gal}(E/F)$ 中的非空子集 S，考虑其生成的子群 $< S >$。我们验证两个集合的不变子域是相同的：

$$\mathcal{K}(S) = \mathcal{K}(< S >)$$

5.2 Galois 扩张

定义 5.5 设 E/F 扩张，称 E/F 是一个 ***Galois* 扩张**，如果 E/F 正规可分。

例 5.2

1. $\mathbb{Q}[\sqrt[3]{2}, \omega]/Q$ 是正规的可分扩张，是 *Galois* 扩张。
2. $\mathbb{Q}$ 的代数闭包是正规可分的扩张。
3. $\mathbb{F}_p(t)(\alpha)/F_p(t)(p \neq 2)$ 是 $x^2 - t$ 的分裂域。则是 *Galois* 扩张。

例 5.3

1. $\mathbb{Q}(\sqrt[3]{(2)})/Q$ 不正规，但可分。
2. $\mathbb{F}_p(t)(\alpha)/F_p(t)$ 是 $x^p - t$ 的分裂域。正规但不可分。

Galois 扩张继承了两种扩张的性质：

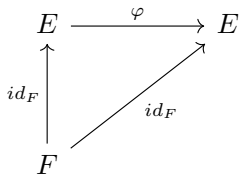
定理 5.2.1 *E/F 有限，以下叙述等价：*

1. *E/F Galois 扩张。*
2. $|\mathrm{Gal}(E/F)| = [E : F]$
3. *有 Galois 子群 G 使得 $\mathcal{K}(G) = F$*
4. $\mathcal{K}(\mathrm{Gal}(E/F)) = F$

证明 $1 \to 2$: 若 E/F 是 Galois 扩张

那么任取 $\alpha \in E$,$f_\alpha \in F[x]$ 分裂且没有重根。

我们要寻找满足如下交换图的 φ:



根据定理**??**，此时每个 α 都可分，f_α 分裂，于是有 n 个这样的 φ。

$2 \to 1$: 定理**??**有逆命题。

$3 \to 4, 4 \to 3$:

$$F = \mathcal{K}(G) \supset \mathcal{K}(\mathrm{Gal}(E/F)) \supset F$$

$2 \to 4$:

记 $K = \mathcal{K}(\mathrm{Gal}(E/F))$ 是中间域。于是:

$$[E : F] = |\mathrm{Gal}(E/F)| = |Gal(E/K)| = [E : K]$$

从而 $K = F$.

在上述等式中，需要注意,Galois 扩张具有对中间域的传递性。即 $E/K/F$，则 E/K 也是 Galois 扩张。另一方面，由于 $K = \mathcal{K}(\mathrm{Gal}(E/F))$，从而任何保持 F 的同构也保持 K 的同构。于是 $|\mathrm{Gal}(E/F)| = |Gal(E/K)$。根据 12 等价，上述等式就连起来了。

$4 \to 2$:

反证法，假设：$[E : F] = n$,$|\mathrm{Gal}(E/F)| = s + 1$，$s + 1 < n$:

$$a_1, a_2, a_3, \ldots, a_n$$

是基。

$$id = \varphi_0, \varphi_1, \ldots, \varphi_s$$

是 Galois 群。于是我们有方程组：

$$\sum_{j=1}^{n} \varphi_k(a_j)x_j = 0, k = 0, 1, 2, \ldots, s$$

这个方程有非零解。取其中零元素最多的解 $(1, b_2, \ldots, b_n)$：我们断言，$b_2, b_3 \ldots, b_n$ 是 F 中的元素：

事实上，容易验证 $\varphi(1, b_2, \ldots, b_n)$ 也是方程组的解。取 φ 使得 $\varphi(b_2) \neq b_2$

于是，$(0, b_2 - \varphi(b_2), \ldots, \varphi(b_n) - b_n)$ 也是一组解，从而矛盾于零元素最多。

但是，若每个 b_j 都属于 F，就与 $a_1, \ldots, a_n$ 为基矛盾！

从而最初的假设错误，从而证明结果。

引理 5.2.2 (Artin 引理) *E 是一个域，且 $G < Aut(E)$,$|G| < \infty$。记 F 是 G 的不变子域，那么 $[E : F] < \infty$，且 $[E : F] < |G|$。*

利用定义证明：

证明 和上述的定理证明思路一样。 □

推论 5.2.3 *$G < Aut(E)$ 且为有限群，$F = \mathcal{K})(G)$，$\mathcal{B}$ 是 E 中的一组向量，那么下面叙述等价：*

1. *$a_1, a_2, \ldots, a_m$ F-线性无关。*
2. *向量组：$\vec{\varphi}(a_i)$ E 线性无关。*
3. *向量组：$\vec{\varphi}(a_i)$ F 线性无关*

推论 5.2.4 *E/F 是有限扩张,$H < \mathrm{Gal}(E/F)$，则 $/\mathcal{K}(H)$ 是 Galois 扩张。且：*

$$H = (\Gamma \circ \mathcal{K})(H)$$

推论 5.2.5 *E/F 是有限扩张，则：*

$$\Gamma \circ \mathcal{K}$$

从 Galois 群的子群到 Galois 群的子群是一个恒等映射。

推论 5.2.6 *E/F 是有限扩张，H_1,H_2 是 Galois 群的子群。如果：*

$$\mathcal{K}(H)_1 \supset \mathcal{K}(H)_2$$

则：$H_1 < H_2$。

5.3 Galois 基本定理

接触了以上概念后，我们将给出 Galois 理论中最基本的定理：

定理 5.3.1 *设 E/F 有限且是 Galois 扩张。那么有：*

1. *$\mathcal{K}$ 和 Γ 都是双射。并且互为逆运算。*

2. 任意 $H < \mathrm{Gal}(E/F)$，则有：

$$[\mathrm{Gal}(E/F) : H] = [\mathcal{K}(H) : F]$$

3. $H \lhd \mathrm{Gal}(E/F) \Leftrightarrow \mathcal{K}(H)/F$ 是正规扩张，从而是 Galois 扩张。

4. $H \lhd \mathrm{Gal}(E/F)$，那么：

$$\frac{\mathrm{Gal}(E/F)}{H} \backsimeq Gal(\mathcal{K}(H)/F)$$

定理给出了 Galois 群与中间域之间密切的关系。在 Galois 理论中起到了密切的作用。

证明 1. 结合之前的定理，已经显然。

2. 记 $K = \mathcal{K}(H)$,$H = Gal(E/K)$.

$$|\mathrm{Gal}(E/F)| = [E : F] = [E : K] \times [K : F] = |Gal(E/K)|[K : F] = |H|[K : F]$$

从而：$[\mathrm{Gal}(E/F) : H] = [K : F]$.

3. 假设 H 是正规子群，则 $\forall \varphi \in Gal(E/F)$:

$$\varphi H \varphi^{-1} = H$$

记 $K = \mathcal{K}(H)$,$\phi \in H = Gal(E/K)$.

从而：$\varphi\phi\varphi^{-1} \in Gal(E/\varphi(K))$。

于是 $Gal(E/\varphi(K)) = \varphi H \varphi^{-1} = H$，从而 $\varphi(K) = K$。K 是正规扩张。

假设 $K = \mathcal{K}(H)/F$ 是正规扩张， □

$\forall g(x) \in \mathbb{Q}[x]$,$\exists f(x) \in Q[x]$:

$$f(g(\alpha)) = \alpha$$