期末考试复习提纲

于品教授放过我

2025 年 12 月 26 日

A 域的扩张理论基本梳理

这一部分我们对一些重要的 (我们希望研究的) 扩张进行归类, 并梳理他们的基本性质, 我们对这一类扩张能够实施的基本操作:

A1) 代数扩张和超越扩张

A1-1 定义

先定义代数元, 若所有元都是代数元, 那么扩张就是代数的, 一个特例是有限扩张; 否则, 扩张就是超越扩张

A1-2 代数扩张基本性质

1. 代数闭包的存在性: 我们可以将它视作最大的代数扩张, 这是对代数闭包的态射描述
2. 传递性
3. 代数运算封闭性
4. 扩张的代数部分是一个域:L^{alg}, 指的是扩张和代数闭包的交集
5. 嵌入的可延拓性, 基域到闭包的嵌入一定能延拓到扩域上

A1-3 代数扩张的基本操作

1. 取正规闭包, 在态射意义下, 我们认为正规闭包是嵌入态射 $\sigma \in Hom_K(L, \Omega)$ 诱导的所有 $\sigma(L)$ 的合成域,(因为正规扩张本身就应该视为对嵌入态射不变的扩张)
2. 取可分闭包, 在态射意义下, 我们可以这样理解可分闭包: 如果
3. 需要注意的是, 正规闭包往往需要" 添加" 元素, 而可分闭包需要" 减少" 元素.

A2) 分裂域和正规扩张

A2-1 分裂域的性质

为简略期间, 不再写定义

分裂域是唯一的, 这是因为 K 嵌入本身也保持 K-系数多项式

我们留意到扩张 $K(\alpha) \simeq K[X]/(m_\alpha(X))$ 中未必包含所有根

假设极小多项式的另一个根 $\beta \notin K(\alpha)$, 那么 $K(\beta) \simeq K(\alpha) \in \overline{K}$, 这就是说,$K$ 的嵌入, 延拓到 $K(\alpha)$ 上, 可以不保持 $K(\alpha)$

我们自然猜测以下两个性质具有一定的关联:

域扩张包含了一个不可约多项式的所有根 $\leftrightarrow$ 基域嵌入的延拓一定保持扩域

事实上, 两个性质就是等价的, 我们称之为正规性, 据此我们定义正规扩张

A2-2 正规扩张的定义

1. 存在一个 (一族)K-系数多项式,L 是它的分裂域
2. 任意一个 (一族)K-系数多项式, 它要么在 L 上没有根, 要么在 L 上分裂
3. 存在代数封闭域 Ω, 任意给定一个 K-嵌入的延拓, 它都保持 L
4. 任意代数封闭域 Ω, 任意给定一个 K-嵌入的延拓, 它都保持 L

A2-3 正规扩张的基本性质

1. 正规扩域的复合域也是正规扩域

2. 正规扩域相对于中间域也是正规的扩域

   (从根的角度来看存在一族 K-系数多项式, 它的分裂域是 L, 将它们视为 M-系数多项式即可, 从态射的角度来看, 所有 M-嵌入也必须是 K-嵌入)

3. 正规扩张没有传递性

4. 2 次扩张都是正规扩张 (我们可以这样背过这个结论: 指数为 2 的子群都是正规子群), 并且利用这个结论, 很容易构造不传递的正规扩张链

5. 给定 $\sigma \in \mathbf{Gal}(L/K)$ 和一个元素 α 的零化多项式 $P(X)$, 那么 $\sigma(\alpha)$ 也被 $P(X)$ 零化, 这是定义非常自然的推论, 它也非常好用

A3) 可分扩张

除了下面例子以外, 任何扩张都是可分的, 这一节的讨论是平凡的.

Example 1 (不可分扩张)**.** 考虑有限域上面的有理函数域 (就是多项式环的分式域)$\mathbb{F}_p(t)$, 在里面添加 $t^{\frac{1}{p}}$, 得到的扩张是不可分扩张

A4) 可分扩张的定义

1. 某个元素极小多项式无重根, 就被称为可分元素, 如果扩域中全体元素都是可分的, 扩张就是可分的;

2. 取定代数封闭域 Ω, 考虑所有 K-嵌入映射的延拓, 如果延拓的个数就等于扩张次数, 那么就是可分的. 考虑特例: 单代数扩张, 这个定义和上面定义 1 的等价性非常显然, 对于有限扩张, 我们可以考虑单代数扩张的链.

3. 还有一种刻画方式, 任给不同的 K-嵌入,L 的像也不同 (也就是说不同的态射可以被区分), 这可能是可分这一称呼的来由

我们不再过多考虑扩张是否可分, 所以断言一切扩张都是可分的.

A5) Galois 扩张

正规且可分的扩张就是 Galois 扩张, 所有 Galois 扩张都是有限的

Remark. 实际上, 无限的 Galois 扩张是存在的, 但是据于品老师的描述, 这种扩张的研究思路是 naïve 的:

做如下的回顾: 对于无限的结构, 我们往往研究与之相关的有限结构, 并且定义一种极限, 用有限结构的极限来逼近无限. 在这里我们使用所谓的 Krull 拓扑来描述收敛性

Krull 拓扑的动机是这样的:

我们在 Galois 群 $\mathbf{Gal}(L/K)$ 上面定义拓扑

给定一个 Galois 扩张 L/K, 那么 L 是所有有限中间域 M 的并集, 并且 $\mathbf{Gal}(L/M)$ 落在 $\mathbf{Gal}(L/K)$ 的内部. 因此, 直观上 Galois 群单位元的邻域应该是 $\mathbf{Gal}(L/M)$, 所以我们就这样定义单位元的邻域基, 再利用群的平移性质可以定义出所有元素的邻域基

对于无限的情况, 我们还要修正 Galois 对应定理

注意到给定子群 H, 回顾课本对于 Galois 对应定理的证明, 我们只证明了 $\mathbf{Gal}(L/L^H)$ 是一系列包含 H 的闭集的交, 所以 $\mathbf{Gal}(L/L^H)$ 至少包含 (实际上等于) $\overline{H}$, 有限的情况下 $\overline{H} = H$, 所以 Galois 对应定理对于所有子群成立, 然而对于无限的情况,H 未必是一个闭集, 因此我们需要修改对应定理, 新的命题是: 闭子群和中间域一一对应.

据于品老师说, 这一部分是 naïve 的, 而且我们不会考, 所以不再赘述, 并且将重点放在几种特殊的扩张中:

A5-1 Abel 扩张

Abel 扩张指的是 Galois 群是交换群的扩张, 它最重要的性质可能是这个

Proposition 2 (有限生成 Abel 群分类定理)**.** *任给 Abel 扩张, 我们都能找到一个域塔, 使得 K_{i+1}/K_i 是循环扩张*

它的逆命题不成立:$\mathbb{Q} - \mathbb{Q}(\sqrt{2}) - \mathbb{Q}(\sqrt[4]{2})$

另一个重要的结论: 添加根式得到的扩张是 Abel 扩张

Remark. 于品老师最爱的例子之一, 将 K 上带有复乘的椭圆曲线的所有 n-torsion 点添加到 K 上面可以得到一个 Abel 扩张

A5-2 循环扩张,Hilbert 90, Kummer 理论

我们不再叙述定义与证明, 只考虑定理和相关的例子:

Theorem 3 (Hilbert 90)**.** *给定 n 次循环扩张和 Galois 群生成元 σ, 某个元素 x 范数为 1 的等价条件是: 不动点方程 $x \cdot \sigma(y) = y$ 有解*

某个元素的迹为 0 的条件是不动点方程 $x + \sigma(y) = y$ 有解

Remark. 实际上, 迹为 0 的元素都可以表示成不动点方程的解可以被形式化为 $\mathrm{Ker}(\mathrm{Tr}) = \mathrm{Im}(\sigma - 1)$, 范数的命题亦然, 据此我们可以发展上同调理论来推广 Hilbert 90

Example 4. 勾股定理和 Pell 方程都是 Hilbert 90 的特例, 他们分别对应扩张 $\mathbb{Q}(i)/\mathbb{Q}$ 和 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$

Theorem 5 (Kummer)**.** *假设 K 包含了所有 n 次单位根, 那么有限扩张 L/K 的两个命题等价:*

(i)L/K 是 n 次循环扩张;

(ii)L 是某个 $K[X]$ 中多项式 $X^n - a$ 的分裂域, 且 $a \notin (K^\times)^d (d|n)$

证明的核心是观察到 ξ^{-1} 是一个范数为 1 的元素, 设定不动点方程的某个解为 α, 那么就有 $\sigma(\alpha) = \xi\alpha$

我们可以用这个定理来刻画任意一个域 (未必包含所有单位根) 上 $X^n - a$ 的分裂域的 Galois 群

Proposition 6. *对于任意的域 K, 某个 $K[X]$ 中多项式 $X^n - a$ 的分裂域 L 一定有*

$$\mathbf{Gal}(L/K) < \mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z})$$

因为分裂域就是 $K(\alpha, \xi)$, 同态必须把本原单位根映射到本原单位根, 将 α 映射到 $P(X)$ 的根

B 对称多项式基本理论

B1) 补充: 多项式基本理论

B1-1 有理系数多项式

1. 本原多项式的 Gauss 引理
2. 整系数多项式和有理系数多项式环可约是等价的
3. 不可约判则:Eisenstein, Mod p 法
4. (整系数多项式) 有理根定理

B1-2 其他的一般多项式

1. 根的性质: 代数基本定理 (据此可以定义所谓的代数封闭域),Vieta 定理

B2) 对称多项式的重要定理

对称多项式说的是变量置换下保持不变的多项式

Theorem 7 (对称多项式基本定理)**.** 对称多项式可以表示为初等多项式的多项式*:*

用环论的语言来说, 我们认为 $\mathbb{Z}[X_1, X_2, \ldots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[e_1, e_2, \ldots, e_n]$

证明是基于归纳法的, 我们只要给出多元多项式的序 *(*一般来说是字典序*)*, 再找到合适的方式消去最高次项, 就可以归纳 *(*递降*)*

Theorem 8 (Newton)**.** 作为一种特殊的对称多项式, 幂和多项式有基于初等对称多项式的递推关系

B3) 结式和判别式

B3-1 结式的定义和等价定义

结式是用于判别多项式是否有公共根的工具:

1. Sylvester 矩阵定义
2. 用根的关系定义 (我们需要用到分裂域)
3. 将 f 的根代入 g 定义 (和第二个定义几乎一样)

B3-2 判别式的定义和等价定义

判别式就是一个多项式所有根两两作差, 平方之后得到的结果, 如果无重根, 那么它就非 0, 注意到, 它也能用结式来定义 (因为根的重数可以用导数来判断):

$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2}\mathrm{Res}(f, f')$

B3-3 结式和判别式的重要性质

注意到 Δ 总是被 $\mathbf{Gal}(L/K)$ 保持, 我们就知道它总是属于基域 K 这里是目标内容注意到 $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$ 是判别式的一个平方根, 并且所有保持这个元素的 Galois 群作用恰好是偶置换, 据此, 我们断言

$$\delta \in K \Leftrightarrow \mathbf{Gal}(L/K) \subseteq \mathfrak{A}_n$$

据此可以计算一个简单的例子:

Example 9. 不可约多项式 $P(X) = X^3 - 2$ 的分裂域是 $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, 此时 $\mathbf{Gal}(L/Q) = \mathfrak{S}_3$

计算的细节: 显然判别式小于 0 所以不存在有理数平方根, 因此 Galois 群至少包含一个对换, 此外,Galois 群必须是传递的, 因此它逐个检验 $\mathfrak{S}_3$ 的子群就能得到这个证明

除此之外, 我们知道有限可分扩张都是单扩张, 利用结式, 我们可以计算这个单扩张的本原元的零化多项式, 进一步说明这个扩张是一个多项式的分裂域, 以下是一个具体的例子:

Example 10. 注意到 $\sqrt{2}+\sqrt{3}$ 是 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 的本原元素, 求解它的极小多项式:
我们需要利用这样的事实, 结式为 0 $\Leftrightarrow$ 两个多项式有公共根
基于这个事实: 我们假设 $P(X)=X^2-2$,$Q(X)=X^2-3$, 那么考虑结式 $R(Y)=\mathrm{Res}_X(P(X),Q(Y-X))$
此时 $R(Y)=0 \Leftrightarrow P(X),Q(Y-X)$有公共的根 $\Leftrightarrow$ Y 是 P 的某个根和 Q 的某个根的和
我们可以用结式的第三个定义来计算, 假设 $P(X)$ 全体根为 $\{\alpha_i\}_{1\le i\le n}$
我们就知道

$$R(Y)=a_m^{degQ}prod_{i=1}^{m}Q(\alpha_i)=Q(Y-\sqrt{2})Q(Y+\sqrt{2})$$

从而 $R(Y)=Y^4-10Y^2+1$

C Dedekind 定理

我们不加证明地给出以下用于计算分裂域 Galois 群中元素的定理

Theorem 11. *给定首一不可约的整系数多项式 $P(X)$, 考虑它在有理数域上的分裂域 $L/\mathbb{Q}$*
如果 $P(X)$ 在 $mod\ p$ 意义下的不可约分解包含的次数为 $(n_1,n_2,\ldots,n_d)$, 那么 **Gal**$(L/\mathbb{Q})$ *包含一个型为 $(n_1,n_2,\ldots,n_d)$ 的元素*
特别的, 一个不可约多项式分裂域的 Galois 群中一定包含一个 n-循环.

Example 12. 取多项式 $P(X)=X^4+4X^3+2X^2+3X-5$

mod2 之后不可约, 自然不可约, 自然分裂域的 Galois 群包含一个 4-循环
mod3 之后 $\overline{P}(X)=X^4+X^3+2X^2+1=(X-1)(X^3-X+1)$, 从而包含一个 (1,3)

置换

此时, 我们考虑到 $\mathbf{Gal}(L/\mathbb{Q})$ 是一个至少 12 个元素的, 包含 4-循环的 $\mathfrak{S}_4$ 的子群, 从而它是 $\mathfrak{S}_4$.

下面考虑一个更复杂的命题, 它需要一个引理

Lemma 13. *给定一个群 $G \subseteq \mathfrak{S}_n$,$G$ 在 n 元集上的作用传递, 并且它包含一个对换和一个 n-1 循环, 那么 $G = \mathfrak{S}_n$*

从群论角度上来看, 它非常容易证明但是看起来非常无聊. 据此我们从 Galois 理论的角度来考察:

传递作用给出多项式的不可约性,n-1 循环对应着多项式有 modp 根, 对换使得 Galois 群不落在 $\mathfrak{A}_n$ 中未必包含所有根

Example 14. 令 K 为 $P(X) = X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}(K/\mathbb{Q})$ 。

显然这个例子中多项式不可约, 而且有 mod3 是 (1,5) 的,mod5 是 (1,1,1,1,2) 的, 就得到了这个证明

D Kummer 理论

Example 15. $P(X) = (X^5 - 2)(X^5 - 3) \in \mathbb{Q}$ 的分裂域的 Galois 群 $\mathbf{Gal}(L/\mathbb{Q})$

我们先做一个简单的情形: 记中间域 K 是 $X^5 - 2$ 的分裂域, 它应该恰好是 20 次扩张 (因为 5 次单位根对应一个 4 次扩张,$\sqrt[5]{2}$ 对应一个 5 次扩张)

我们考虑扩张 L/K, 我们希望说明 $X^5 - 3$ 在 K 上面没有根 (否则由正规性 $K = L$), 反设根存在, 那么 $\mathbb{Q}(\sqrt[5]{3})$ 是域扩张 $K/\mathbb{Q}$ 的一个中间域, 这又对应了 $\mathbf{Gal}(K/\mathbb{Q})$ 的一个 4 阶 (Sylow2) 子群, 利用 Sylow 定理, 这样的子群有 1 个或 5 个

更进一步,Sylow2 子群对应的中间域应该是 $\mathbb{Q}(\sqrt[5]{3} \cdot \xi^k)(k = 0, 1, 2, 3, 4)$

此时 $\mathbb{Q}(\sqrt[5]{2})$ 也是一个中间域, 考虑到这是 $\mathbb{R}$ 的子域, 我们就知道 $\mathbb{Q}(\sqrt[5]{3} = \mathbb{Q}(\sqrt[5]{2},$ 但是 (经过相当繁琐的计算) 我们知道不可能!

因此我们知道 X^5-3 在 K 上没有根, 我们还要证明它是不可约的:

我们希望利用 X^5-3 在 $\mathbb{Q}$ 上的不可约性证明在 K 上面的不可约性: 反设在 k 上可约, 因为它没有根, 可知不可约因子一个是二次多项式, 一个是三次多项式

任取 $\sigma \in \mathbf{Gal}(K/\mathbb{Q})$ 保持 X^5-3, 由分解的唯一性, 以及次数的的比较, 我们知道不可约因子也被 σ 保持, 从而这说明不可约因子也是 $\mathbb{Q}$ 的元素, 这给出了矛盾!

Example 16. 我们可以计算 $(\mathbf{Q}, X^6-2)$ 的 Galois 群.

E 练习题

EX.4 素谱和幂零元的关系

Proof.

先证明 $\mathfrak{Nil}(A) \subseteq \cap_{\mathfrak{p}\in \mathrm{Spec}(A)}\mathfrak{p}$: 任取素理想 $\mathfrak{p}$,$x \cdot x^{n-1} = x^n = 0 \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$

再证明 $\mathfrak{Nil}(A) \supseteq \cap_{\mathfrak{p}\in \mathrm{Spec}(A)}\mathfrak{p}$: 反设存在 $x \in \mathfrak{Nil}(A) - \cap_{\mathfrak{p}\in \mathrm{Spec}(A)}$, 那么存在 $\mathfrak{p}_0$, 使得 $x \notin \mathfrak{p}_0$, 这说明 $x^n \notin \mathfrak{p}_0$(这是因为 $A/\mathfrak{p}_0$ 是整环, 没有零因子)

这就说明 $\mathfrak{Nil}(A) - \cap_{\mathfrak{p}\in \mathrm{Spec}(A)} = \emptyset$, 矛盾!

Remark. 所谓 Scheme 理论就是从这里开始的, 在过去, 我们只认为多项式环中的理想能够决定一个几何对象 (例如经典的: 多项式 ax^2+by^2+1 生成的 (素) 理想定义出一个二次曲线). 但是这个命题告诉我们, 对任何交换环, 我们都可以定义一个几何结构 $\mathrm{Spec}(A)$

EX.5

Proof.

素理想的逆像是素理想: 下面我们说明 $A/\varphi^{-1}(\mathfrak{q})$ 是一个整环

φ 诱导了 $A/\varphi^{-1}(\mathfrak{q})$ 到 $B/\mathfrak{q}$ 的一个同态 $\overline{\varphi}: a+\varphi^{-1}(\mathfrak{q}) \mapsto \varphi(a)+\mathfrak{q}$

这个映射是良定义的, 而且成为一个同态

反设 $A/\varphi^{-1}(\mathfrak{q})$ 不是一个整环, 假设 $A/\varphi^{-1}(\mathfrak{q})$ 有零因子 $a+\varphi^{-1}(\mathfrak{q}), b+\varphi^{-1}(\mathfrak{q})$, 那么他们被 $\overline{\varphi}$ 映射到 $\varphi(a)+\mathfrak{q}, \varphi(b)+\mathfrak{q}$

此时, 不妨设 $\varphi(a) \in \mathfrak{q}$, 就可知 $a \in \varphi^{-1}(\mathfrak{q})$, 但这和 a 是零因子相矛盾! 因此 $A/\varphi^{-1}(\mathfrak{q})$ 是一个整环, 也就是说素理想的逆象也是素理想.

极大理想的逆像未必是极大理想: 我们知道 $\mathbb{Q}$ 是一个域, 它的极大理想只有 $\{0\}$, 逆像自然也是 $\{0\}$, 但是 $\mathbb{Z}$ 中任意非平凡的理想都包含这个逆像, 所以逆像不是极大理想

EX.6

Proof. 利用归纳法来证明

归纳奠基是显然的, 归纳假设命题对于 $1, 2, ..., n$ 的情况都成立, 递推证明 $n+1$ 的情况:

此时, 利用反证法, 假设 $I \subseteq \cup_{1 \leq i \leq n+1} \mathfrak{p}_i$ 且 $I \not\subseteq \mathfrak{p}_j, \forall j$

根据归纳假设, 我们知道 $I \not\subseteq \cup_{i \neq j} \mathfrak{p}_i$, 从而, 我们可以取出元素 a_i, 满足 $a_i \notin \mathfrak{p}_j (\forall i \neq j)$, 此时, 取 $a = a_{n+1} + a_1 a_2 \cdots a_n$, 那么 $a \notin \mathfrak{p}_k, \forall k \in 1, 2, \ldots, n+1$, 就导出了矛盾.

Remark. 我们有以下几何直观:

EX.7

Proof. 由题设, 可以取出 $a \in I, b \in J$ 使得 $a+b=1$, 那么, 考虑 $(a+b)^{2n-1}$ 二项式展开, 并考虑里面 a 次数出现不少于 n 次的单项式 $w = b^{m_0} \cdot (a \cdot b^{m_1}) \cdot (a \cdot b^{m_2}) \cdots (a \cdot b^{m_l}) (l > n)$, 这个单项式的每一项都是 I 的元素, 因此乘积是 I^n 的元素. 因此, 所有这样的单项式的和也是 I^n 的元素

反过来, 剩下所有的单项式的和是 J^n 的元素, 从而我们就构造出了一对和为 1 元素, 他们分别属于 I^n, J^n

EX.8

由题意 $K(\alpha)/K, K(\beta)/K$ 分别是 $p = degP, q = degQ$ 次的扩张 (其中 p, q 互素), 那么他们均为 $K(\alpha, \beta)/K$ 的中间域, 从而 $[K(\alpha, \beta) : K] >= p \cdot q$, 从而 $[K(\alpha, \beta) : K(\beta)] >= p$, 又因为 $P(X)$ 给出了 $K(\beta)[X]$ 之中 α 的一个 p 次零化多项式, 从而极小多项式就是 $P(X)$

据此, 次数应该是 6

EX.9

下面记 $\xi \coloneqq e^{\frac{2\pi i}{n}}$, 那么记 $\alpha = \frac{\xi+\xi^{-1}}{2}$, 待求扩张就是 $\mathbb{Q}(\alpha)/\mathbb{Q}$

考虑 $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}(\alpha)$, 其中 $\beta = \frac{\xi-\xi^{-1}}{2}$

这是一个二次扩张, 因为 $\beta^2 + (1-\alpha^2) = 0$, 并且 $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ 就是分圆扩张, 其次数是 $p-1$, 从而 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 的次数是 $\frac{p-1}{2}$

EX.10

任取 $\sigma \in \mathbf{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$，我们知道 $\sigma(\sqrt{2})^2 = 2, \sigma(\sqrt{3})^2 = 3, \sigma(\sqrt{5})^2 = 5$，从而 $\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{3}) = \pm\sqrt{3}, \sigma(\sqrt{5}) = \pm\sqrt{5}$，这说明 Galois 群是 $(\mathbb{Z}/2\mathbb{Z})^3$。

用归纳的方法方法说明 $\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_d})/\mathbb{Q}$（其中 $p_i(i=1,2,\ldots,d)$ 是互不相等的素数）是一个 2^d 次的扩张。

考虑域扩张 $\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_{d-1}},\sqrt{p_d})/\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_{d-1}})$，只要证明这个扩张是 2 次的。

将 $\mathbb{R}$ 视为 $\mathbb{Q}$-线性空间，$\{1,\sqrt{p_1},\sqrt{p_2},\ldots,\sqrt{p_d},\ldots,\sqrt{p_ip_j},\ldots,\sqrt{p_1p_2\cdots p_d}\}$ 是线性无关的，据此 $\sqrt{p_d} \notin \mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_{d-1}})$，从而极小多项式次数至少为 2，又因为 X^2-p_d 就是一个 2 次零化多项式，就可知极小多项式就是 X^2-p_d，递降就可以得到 $\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_d})/\mathbb{Q}$ 是一个 2^d 次扩张。

结合包含关系就可以得到 $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$。

EX.11

Proof. 由题意 $K/\mathbb{Q}$ 是一个正规扩张,$\mathbb{C}$ 是一个代数封闭域.

将复共轭映射限制在 K 上, 这是 K 的一个保持 $\mathbb{Q}$ 的嵌入, 由正规扩张的定义, 这个嵌入也保持 K, 这也就是说复共轭映射保持 K

EX.12

用 Galois 对应定理重新描述这个命题:

原命题等价于" 给定 $H \leq G$, 那么 $\cap_{g\in G} gHg^{-1}$ 是 G 的正规子群, 而且任意 $N <$

$H, N \triangleleft G$ 都满足 $N \leq \cap_{g\in G} gHg^{-1}$"

任取 $N \leq H, N \triangleleft G$, 任取 g,N 满足 $g^{-1}Ng \subseteq H$, 也就是 $N \leq gHg^{-1}$, 从而 N 落在 H 的正规核中

再证明正规核是正规子群, 据定义, 正规核中的元素在共轭映射下仍然落在正规核中, 所以正规核是正规子群

EX.13

Proof. 为了利用 Galois 对应定理, 我们只需要说明 L/M_0 是一个 Galois 扩张: 这是因为 L/K 是正规且可分的, 自然分别给出了 L/M_0 的正规性和可分性.

由 Galois 对应定理,$H \triangleleft N_G(H)$, 从而它对应的扩张 M/M_0 是正规扩张.

进一步, 如果 M/M' 是正规扩张, 那么 M' 一定对应了 G 中的一个子群, 它正规化 H, 我们知道 $N_G(H)$ 包含了所有正规化 H 的 G 的子群, 据此 $M' \supseteq M_0$.

EX.14

见B3.3 判别式的性质

进一步, 因为 Galois 群在根集的作用是传递的, 如果 Disc(P) 是完全平方数, 那么 Galois 群落在交错群中, 交错群能够传递作用在 $\{1, 2, 3\}$ 的子群只有它本身, 因此 Galois 群只能是交错群.

如果 Disc(P) 不是完全平方数, 那么它至少包含一个奇置换 (也就是对换), 因为它是传递的子群, 所以它只能是对称群.

EX.15

假如有一个 $P(X)$ 满足 $degP > 2$, 考虑 $P(X)$ 的分裂域 M, 那么 M 对应了一个指数为 $degP$ 的,$\mathfrak{S}_n$ 的子群, 考虑到任意 $\mathfrak{S}_n, (n \geq 5)$ 子群要么是交错群, 要么指数至少为 n, 就说明了 $degP$ 至少为 n.

为了找到 $n = 4$ 情况下的反例, 我们只需要考虑 $\mathfrak{S}_4$ 的 8 阶子群 (之一)$\langle(13), (1234)\rangle$

例如: 我们假设 $X^4 - X - 1$ 在 $\mathbb{Q}$ 上的分裂域, 并假设四个根为 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$,

那么我们可以构造出元素:

$$\theta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \theta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \theta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

其中 θ_2 是被 D_4 保持的元素, 而 θ_1, θ_3 则是 θ_2 在 Galois 群中映射下的像:

下面我们计算 $(X-\theta_1)(X-\theta_2)(X-\theta_3)$

其中 $X^4 - X - 1$ 的二次项为 0 说明 $\theta_1 + \theta_2 + \theta_3 = 0$

$\theta_1\theta_2 + \theta_2\theta_3 + \theta_1\theta_3 = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)(\alpha_1\alpha_2\alpha_3 + \alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha 4 + \alpha_1\alpha_3\alpha_4) - 4\alpha_1\alpha_2\alpha_3\alpha_4 = -4$

$\theta_1\theta_2\theta_3 = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) + \sum_{i<j<k}(\alpha_i\alpha_j\alpha_k)^2$

从而这个极小多项式是 $X^3 + 4X - 1$

EX.16

考虑域塔 $L - K(x) - K$, 和对应的 Galois 群子群链 $\mathbf{1} < H \leq \mathbf{Gal}(L/K)$

交换群的子群都是正规的,H 也是正规的, 对应地 $K(x)/K$ 是正规扩张.

此时 $P(X) \in K[X]$ 在 $K(x)$ 上有一个根, 据正规扩张的性质,$K(x)$ 是 $P(X)$ 的分裂域, 也就是 $L = K(x)$

EX.17

为证明它是 Galois 扩张, 只需要证明:

1. 扩张是可分的: 这是因为 $\mathbb{Q}$ 特征为 0;

2. 扩张是正规的: 显然, 这个域是一族 $\mathbb{Q}[X]$ 中多项式 $\{P_i(X) = X^2 - p_i\}_{i\in 1,2,3,\ldots,d}$ 在 $\mathbb{Q}$ 上的分裂域, 从而它是正规的.

Ex.10中已经证明了它是一个 2^d 次扩张, 并且考虑到形如 $\sigma : \sqrt{p_i} \mapsto \varepsilon_i\sqrt{p_i}(\varepsilon_i \in \{\pm 1\})$ 的元素已经给出了 $\mathbf{Gal}(L/\mathbb{Q})$ 中两两不等的 2^d 个元素, 因此直接观察群元素的性质可知

$$\mathbf{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^d$$

如果 $\sqrt{15} \in \mathbb{Q}(\sqrt{10}, \sqrt{42})$

那么我们有如下的域塔:

(i) $\mathbb{Q} - \mathbb{Q}(\sqrt{15}) - \mathbb{Q}(\sqrt{10}, \sqrt{42})$

(ii) $\mathbb{Q} - \mathbb{Q}(\sqrt{10}) - \mathbb{Q}(\sqrt{10}, \sqrt{42})$

(iii)$\mathbb{Q} - \mathbb{Q}(\sqrt{42}) - \mathbb{Q}(\sqrt{10}, \sqrt{42})$

(iv) $\mathbb{Q} - \mathbb{Q}(\sqrt{105}) - \mathbb{Q}(\sqrt{10}, \sqrt{42})$

并且这些域塔中相邻的域扩张都是 2 次的, 我们知道 4 阶群的 2 阶子群至多 3 个, 而且 (ii)(iii)(iv) 给出的域塔是两两不同的, 所以 (i) 必须等于这三者之中的某一个.

显然 $\sqrt{15} \notin \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{42}), \mathbb{Q}(\sqrt{105})$, 就给出了证明.

F 没有这一节

F 不存在.