

从根式公式到五次障碍：我的证明框架笔记

第三版 · 2026-10-06。保留前两版正文，在第 11 章末尾加入我的整体理解、必要条件与限制映射两次用途的对照，第 1 章增加简短导航。先看框架，再沿着框架读完整证明。HTML 是主要阅读文件，Markdown 是配套源文件。

原始材料：《五次方程伽罗瓦群推导》分享对话。本篇覆盖其中七轮数学问答，编号 A01—A07；另收录本聊天三轮追问及一段整体理解，编号 B01—B04。按逻辑依赖重排并重写解释，原问题保留在对应位置；补充的证明与校正明确标出。

我已经学过群、域、分裂域、单位根和可解群，但在最后一步仍觉得几套构造没有接上：一边是由五个根和五个系数得到的域扩张，一边是从系数开始逐步开根的域塔。这份笔记的目标，是看清它们为什么必须联系到同一个分裂域的同一个 Galois 群。

全文固定特征零。所有有限代数扩张放在同一个代数闭包中讨论；通用模型中的不定元先构造有理函数域，再取系数域的代数闭包。域的包含用 $\subseteq$ ，允许某一步没有真正扩大；重复层可删去。

两种阅读方式

先掌握框架：第 1 章 → 第 4 章 → 第 6 章章首 → 第 8 章 → 第 11 章。逐步核对证明：按第 1—12 章顺序阅读。每章先交代任务，再给结论、证明和回到主线的连接。

目录

- 第 1 章：两条路线，在同一个群上相遇
- 第 2 章：通用五次方程，为什么仍是系数域到分裂域

- 第 3 章：把根式表达式逐步翻译成域塔
- 第 4 章：分裂域的位置，是中间域而不必是列出的层
- 第 5 章：补单位根，单个根式层才有阿贝尔群
- 第 6 章：逐层补共轭，构造对原基础域 Galois 的大域
- 第 7 章：域塔怎样变成可解群的正规列
- 第 8 章：限制映射，把大群的可解性传给分裂域
- 第 9 章：不相邻层可以吗？先检查使用条件
- 第 10 章：为什么 S_5 不可解，完整补上群论障碍
- 第 11 章：把所有桥梁合起来，完成反证
- 第 12 章：复习地图、原问题索引与校正记录

对象与符号速查

符号	本篇中的固定角色
t	一元多项式的变量；与五个形式根 x_i 区分
$x_1, \dots, x_5$	在 $\mathbb{Q}$ 上代数独立的不定元，用来构造通用模型
e_j	五个 x_i 的第 j 个基本对称多项式
$F = \mathbb{Q}(e_1, \dots, e_5)$	原基础域，也是通用方程的系数域；加入单位根以后仍然叫 F
$E = F(x_1, \dots, x_5)$	通用方程的分裂域，由方程自身决定
$R_i; R = R_m$	假想根式公式给出的原始根式塔各层与塔顶
$q; \mu_q; \zeta_q$	所需根式指数的最小公倍数；全部 q 次单位根；一个本原单位根
$M_0, \dots, M_m = N$	补单位根、逐层补共轭构造的大域塔；每层对 F 都 Galois
Ω	F 的一个代数闭包，容纳 E, R, N

符号	本篇中的固定角色
$G = \text{Gal}(N/F)$	用来容纳根式运算的“大”Galois 群
$H_i = \text{Gal}(N/M_i)$	G 中固定 M_i 的子群
$\text{res}; \sigma _E$	限制映射；只让自同构 σ 在 E 上作用
$\ker \varphi; \text{im } \varphi$	群同态的核与像；核中映到目标群的单位元
$\triangleleft; \cong; \hookrightarrow$	正规子群；同构；单射同态
$S_5; A_5$	五个对象上的全部置换；其中的偶置换

“可解”用于群时指存在阿贝尔商的正规列；“根式可解”用于多项式时指所有根可由基础域元素经过有限次四则运算和开根得到。它们的联系需要证明，不能仅凭名字认定。

第 1 章：两条路线，在同一个群上相遇

1.1 我的疑问究竟在哪里

原问题 A01：最后从5次方程推出无根式解，是直接从5个根和5个系数的域扩张来推出Galois群之类的，貌似和之前构建的方式不一样

原问题 A06：所以在5次方程那个证明中域塔以及矛盾是怎么来的来着

这两个问题都在问：方程本身的分裂域，与假想公式制造的根式塔，到底是什么关系？先把对象的来源分开，后面才能看清它们如何合流。

路线一：方程自身的对称性

五个独立形式根 $\rightarrow$ 基本对称式作为系数
 $\rightarrow$ 系数域 F 与分裂域 $E \rightarrow$
 $\text{Gal}(E/F) \cong S_5 \rightarrow$ 这个群不可解。

看第 2、10 章的证明

路线二：假想公式能制造什么

假设存在根式公式 $\rightarrow$ 原始根式塔，顶层
 R 包含全部根 $\rightarrow E \subseteq R \rightarrow$ 补成大域
 $N \rightarrow \text{Gal}(N/F)$ 可解 $\rightarrow \text{Gal}(E/F)$
可解。

看第 3—8 章的证明

路线一不依赖根式公式的存在。路线二从一个反证假设出发。最后，它们分别说同一个 $\text{Gal}(E/F)$ 不可解与可解，矛盾才成立。

1.2 四个域，四个角色

域	怎样得到	在证明中的任务
F	从方程系数生成	固定可使用的初始信息
E	在 F 中加入方程的全部根	承载方程自身的 Galois 群
R	从 F 按假想公式逐步加入根式	保证所有根都可由这些运算得到
N	扩大 R ，补单位根与所需共轭	提供对 F Galois、群可解的容器

核心包含关系是

$$F \subseteq E \subseteq R \subseteq N.$$

与此同时，另有一张“建造记录”

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_m = R.$$

两张图共同描述同一批域；第一张只说明包含，第二张还记录每次根式运算。不能从第一张图推断 E 等于某个 R_i 。

1.3 为什么根式塔之后仍有工作

原问题 A07：换言之域塔之后还要做一些工作

是的。原始根式塔证明的是“运算能够造出什么元素”，而 Galois 理论还需要“所有共轭都在域内”“限制映射可用于商群”等条件。第 5—7 章负责把前一个对象加工成后一个对象。

公式 $\Rightarrow$ 原根式塔 $\Rightarrow$ 包含它的可解 Galois 大域 $\Rightarrow$ 分裂域的群可解

理解框架时，先记每个箭头的任务；核对证明时，再逐一检查它的条件与构造。

简短导航：原始根式塔 $\rightarrow$ 补单位根与所需共轭 $\rightarrow$ 构造可解的 Galois 大群 $\rightarrow$ 通过限制商群得到原分裂域的群可解。读完总反证后，可在第 11.7—11.8 节回看我的整体理解和两次限制映射的不同用途。

第 2 章：通用五次方程，为什么仍是系数域到分裂域

本章任务：证明“先造根，再造系数”仍然得到一个有限 Galois 分裂域，并完整证明它的群是 S_5 。

2.1 “五个独立的根”是什么意思

取不定元 $x_1, \dots, x_5$ 。说它们在 $\mathbb{Q}$ 上代数独立，是说不存在非零多元多项式 $P \in \mathbb{Q}[X_1, \dots, X_5]$ 使

$$P(x_1, \dots, x_5) = 0.$$

这不是概率上的独立。它意味着没有额外代数关系，可以自由重命名变量。

先构造有理函数域

$$E = \mathbb{Q}(x_1, \dots, x_5).$$

其元素是多项式的分式 $P(x_1, \dots, x_5)/Q(x_1, \dots, x_5)$ ，其中 $Q \neq 0$ 。定义

$$e_j = \sum_{1 \leq i_1 < \dots < i_j \leq 5} x_{i_1} \cdots x_{i_j}, \quad 1 \leq j \leq 5,$$

并令

$$F = \mathbb{Q}(e_1, e_2, e_3, e_4, e_5) \subseteq E.$$

每个 e_j 已经属于 E ，所以 $F \subseteq E$ 是由生成域的定义直接得到的。

2.2 同一个多项式，同时看见系数与根

展开乘积得到

$$f(t) = \prod_{i=1}^5 (t - x_i) = t^5 - e_1 t^4 + e_2 t^3 - e_3 t^2 + e_4 t - e_5 \in F[t].$$

所有 x_i 都是这个多项式的根，而且

$$F(x_1, \dots, x_5) = \mathbb{Q}(x_1, \dots, x_5) = E.$$

第一项包含 $\mathbb{Q}$ 和全部 x_i ，所以包含右边；反方向由 $F \subseteq E$ 得到。因此 E 正是 f 在 F 上的分裂域。

补充证明：为什么这个扩张有限？ 虽然 x_i 对 $\mathbb{Q}$ 是超越元，但它们对 F 都满足上面的五次多项式，因而对 F 代数。逐个加入它们，每步次数有限（至多 5），塔式定理给出 $[E : F] < \infty$ 。于是“ $E/\mathbb{Q}$ 超越”与“ E/F 有限代数”完全兼容，因为基础域不同。

各 x_i 不相等，否则有非零关系 $x_i - x_j = 0$ 。因此 f 没有重根。有限可分分裂域是 Galois 扩张；下面第 6、8 章还会直接证明所用的嵌入稳定与延拓事实。

2.3 为什么这些系数确实代表“一般系数”

仅说“根很独立”还不够：要证明 $e_1, \dots, e_5$ 也代数独立。

补充证明。在单项式上使用按 $x_1 > x_2 > \dots > x_5$ 的字典序。 e_j 的最高单项式是 $x_1 \cdots x_j$ ，系数为 1。因此

$$e_1^{a_1} \cdots e_5^{a_5}$$

的最高单项式是

$$x_1^{a_1+a_2+a_3+a_4+a_5} x_2^{a_2+a_3+a_4+a_5} x_3^{a_3+a_4+a_5} x_4^{a_4+a_5} x_5^{a_5}.$$

字典序与乘法相容，所以最高单项式的乘积就是乘积的最高单项式。设上述五个指数为 $b_1, \dots, b_5$ ，便可恢复

$$a_1 = b_1 - b_2, \quad a_2 = b_2 - b_3, \quad a_3 = b_3 - b_4, \quad a_4 = b_4 - b_5, \quad a_5 = b_5.$$

不同的 a 向量给出不同的最高单项式。在任意有限非零线性组合中，选择最高单项式最大的那一项；其最高项不可能被其他项抵消。因此任何非零 $P \in \mathbb{Q}[Y_1, \dots, Y_5]$ 都有 $P(e_1, \dots, e_5) \neq 0$ 。

这证明 e_j 代数独立。令一般首一五次式的系数 $a_{5-j} = (-1)^j e_j$ ，就得到通常写法

$$t^5 + a_4 t^4 + a_3 t^3 + a_2 t^2 + a_1 t + a_0.$$

具体系数可能产生额外关系，因此不能把通用模型的 S_5 结论直接套给每一个具体五次方程。

2.4 每个置换都确实给出域自同构

取 $\pi \in S_5$ ，定义变量替换

$$T_\pi(x_i) = x_{\pi(i)}.$$

它先给出多项式环的自同构：保持加法乘法，逆映射是 $T_{\pi^{-1}}$ 。因此非零多项式仍然非零。
定义

$$T_\pi\left(\frac{P}{Q}\right) = \frac{T_\pi(P)}{T_\pi(Q)}.$$

良定义检查。若 $P/Q = P'/Q'$ ，则 $PQ' = P'Q$ 。应用多项式自同构得到 $T_\pi(P)T_\pi(Q') = T_\pi(P')T_\pi(Q)$ ，故结果不依赖分式表示。分母非零；运算保持；逆置换给出逆。因此这是 E 的域自同构。

置换只重排 e_j 求和中的项，所以固定全部 e_j ，进而固定整个 F 。这就构造了 $5!$ 个不同的 F 自同构，而不是仅仅构造根的标签变化。

2.5 反方向：自同构没有其他自由度

若 $\sigma \in \text{Gal}(E/F)$ ，因 σ 固定 f 的系数，

$$f(\sigma(x_i)) = \sigma(f(x_i)) = 0.$$

所以每个 x_i 被送到某个 x_j 。自同构单射，使不同根的像不同，因此得到五个根的置换。又因 E 由 F 和这些根生成，其作用被根的像完全确定。

于是根作用

$$\rho : \text{Gal}(E/F) \longrightarrow S_5$$

是单射群同态；第 2.4 节构造了它的每一个可能输出，所以它也满射。故

$$\boxed{\text{Gal}(E/F) \cong S_5.}$$

回到主线：至此只用了方程的通用模型。根式公式还没有进入证明。

第 3 章：把根式表达式逐步翻译成域塔

原问题 A02：但是这样貌似都没有构建其根式可解和这两个域扩张的Galois群可解的联系吧，还是说，只要是根式域其实就是我们之前一步步构建的那种域塔

本章任务：把“从系数有限次四则运算和开根”落实为一座有限根式塔，证明所有公式输出都在塔顶。

3.1 四则运算与开根，为什么待遇不同

设当前已经得到一个域 K 。在 K 中做加减乘除（除数非零）仍然留在 K ，不必增加新层。遇到开根运算时，若被开方数 a 已经在 K ，选取代数闭包中的一个 α 满足

$$\alpha^n = a,$$

则将当前域扩大成 $K(\alpha)$ 。此时 α 满足 $t^n - a$ ，所以是代数元；即使该多项式可约，也有 $[K(\alpha) : K] \leq n$ 。

根式表达式有限，按运算依赖顺序处理所有开根节点：先处理内层，再处理外层。就得到

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_m = R, \quad R_i = R_{i-1}(\alpha_i), \quad \alpha_i^{n_i} = a_i \in R_{i-1}.$$

所谓“根式塔”记录的就是这些开根节点。

3.2 新追问：为什么每层都是某次幂等于前层元素

新问题 B01：根式表达式有限，按运算依赖顺序处理所有开根节点：先处理内层，再处理外层。就得到

所谓“根式塔”记录的就是这些开根节点。这一步为什么还会是那种n次直接就是等于一个值的情况，有没有可能是一个n次的多项式而不只是一个最高次

有可能满足含有其他项的多项式。这里需要先区分：当前的一次开根操作产生的中间量，与原方程要求的根。

如果计算过程中当前出现的是

$$\alpha_i = \sqrt[n_i]{a_i}, \quad a_i \in R_{i-1},$$

那么“选择一个 n_i 次根”的含义本来就是选择满足

$$\alpha_i^{n_i} = a_i$$

的元素。这个关系来自**该操作的定义**，并非从任意一个一般多项式方程强行整理得到。

原方程的根可以通过这些中间量继续做四则运算得到。它自己的方程可以含有一次项、二次项等；我们没有要求它本人就是每一步加入的 α_i 。

本段的逻辑起点是已经假设存在根式公式。有了公式，才能沿着它的开根节点选取生成元。不能只知道某元素满足一个一般多项式，就声称它有这种根式构造；否则恰好把五次证明要否定的事情当成了前提。

3.3 仍觉得差一点：沿着一个完整公式实际建塔

新问题 B02：大概理解了，但是还是差点意思

这里最容易混淆的是：原方程有很多项，为什么建塔时却只写最高次幂的关系？原因在于，塔选择公式中的开根中间量作为生成元，不要求选择原方程的根本人。

取原方程

$$x^2 + x - 1 = 0.$$

它的一个根是

$$x = \frac{-1 + \sqrt{5}}{2}.$$

现在不跳过中间步骤，按公式依次操作：

当前操作	得到的元素	对域的影响
从有理数计算被开方数	$5 \in \mathbb{Q}$	留在原域
开平方	$\beta = \sqrt{5}$	加入 β ，得到 $\mathbb{Q}(\beta)$
减去 1，再除以 2	$x = (\beta - 1)/2$	留在 $\mathbb{Q}(\beta)$ ，无需新增层

因此公式对应的根式塔是

$$\mathbb{Q} \subseteq \mathbb{Q}(\beta), \quad \beta^2 = 5.$$

此处两种方程分别描述两个元素：

$$\underbrace{x^2 + x - 1 = 0}_{\text{原方程的根 } x}, \quad \underbrace{\beta^2 = 5}_{\text{开根产生的中间量 } \beta}.$$

它们可以在同一个域内存在，毫不冲突。甚至

$$x = \frac{\beta - 1}{2}, \quad \beta = 2x + 1 \implies \mathbb{Q}(x) = \mathbb{Q}(\beta).$$

同一个域，可以有不同的生成元。用 x 生成时，它满足含一次项的多项式；用公式中的 β 生成时，就能直接记录 $\beta^2 = 5$ 。根式塔是在选择后一种生成方式，并没有把原方程改成另一个方程。

原方程另一个根 $x_- = (-1 - \beta)/2$ 也在这个域中，因此两根的分裂域就是 $\mathbb{Q}(\beta)$ 。这也展示了“加入中间根式，最后得到所有方程根”的具体过程。

为什么把低次项挪到右边还不够

由原方程可以写出

$$x^2 = 1 - x.$$

但这里右端含有尚未得到的 x 。若当前域是 $\mathbb{Q}$ ，并不能据此把 $1 - x$ 当成前层已经有的被开方数。事实上 $x \notin \mathbb{Q}$ ：否则 $\beta = 2x + 1$ 将使 $\sqrt{5}$ 为有理数。若 $1 - x \in \mathbb{Q}$ ，也会得到 $x \in \mathbb{Q}$ ，同样矛盾。

一般地，若某根 u 满足

$$c_n u^n + c_{n-1} u^{n-1} + \cdots + c_1 u + c_0 = 0, \quad c_n \neq 0,$$

把低次项移到右边虽然得到

$$u^n = -\frac{c_{n-1} u^{n-1} + \cdots + c_1 u + c_0}{c_n},$$

却没有保证右边属于前一层域，因为它还依赖正在试图求出的 u 。根式塔要求的正是 $a_i \in R_{i-1}$ ，而不仅仅是等式外形像“某次幂等于一个值”。

3.4 多项式仍可能有其他项：基础域与最小多项式都要分清

换回原基础域以后，方程可以有多项

考虑嵌套根式，令

$$\alpha = \sqrt{2}, \quad \beta = \sqrt{1 + \alpha}.$$

它给出两步塔

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta), \quad \alpha^2 = 2, \quad \beta^2 = 1 + \alpha.$$

对第二步的**当前基础域** $\mathbb{Q}(\alpha)$ ，被开方数 $1 + \alpha$ 已经存在，所以这一层仍然是开平方。若要消去 α ，直接描述 β 对**原基础域** $\mathbb{Q}$ 的关系，则有

$$\beta^2 - 1 = \alpha \implies (\beta^2 - 1)^2 = 2 \implies \beta^4 - 2\beta^2 - 1 = 0.$$

所以“对前一层有纯开根关系”与“对原基础域满足有多项的方程”可以同时成立。这里先只声称四次式是一个满足的方程；不能仅凭这个计算就自动认定它是最小多项式。

即使不换基础域，开根方程也未必就是最小多项式

若 $\alpha^n = a \in K$ ，则 α 满足 $t^n - a$ 。其首一最小多项式 $m_{\alpha, K}$ 只需满足

$$m_{\alpha, K}(t) \mid t^n - a.$$

补充证明。将 $t^n - a$ 除以 $m_{\alpha, K}$ ，所得余式在 α 处也为零；余式次数更低，由最小性只能为零。因此得到整除关系。该因子可能含有其他次数项，所以并未要求最小多项式本身只有最高次项与常数项。

例如本原三次单位根 ω 满足 $\omega^3 = 1$ ，而

$$t^3 - 1 = (t - 1)(t^2 + t + 1).$$

它不是 1，故满足 $t^2 + t + 1$ 。该二次式在 $\mathbb{Q}$ 上没有根（判别式为 -3 ），所以不可约，正是其最小多项式。这里开根关系的指数为 3，最小多项式次数却为 2。

这说明根式塔中的 n_i 表示所选开根操作的指数，不必等于该层扩张次数；仍然有

$$[R_{i-1}(\alpha_i) : R_{i-1}] = \deg m_{\alpha_i, R_{i-1}} \leq n_i.$$

3.5 我的理解落点：每次新增一层，只处理一次开根

新问题 B03：换言之就是每次域扩张只处理开根号的事情，

对，在按根式公式构造原始根式塔时，每次新增一层，只负责加入一个开根得到的元素：

$$R_i = R_{i-1}(\alpha_i), \quad \alpha_i^{n_i} = a_i \in R_{i-1}.$$

此前的加减乘除用来准备 a_i ；开根操作把 α_i 加入；后续的加减乘除继续留在新域里。 a_i 可以由多个已有根式复杂组合得到的元素，不必只是原始系数中的某一个数。

最终的方程根也可以是多个中间量的组合，不必直接等于某个 α_i 。若这次开根得到的元素本来就在当前域中，则 $R_i = R_{i-1}$ ，这一步可以省去。

这里的表述限定于从公式建立原始塔的这种安排。一般域扩张可以加入任意代数元；而第 6 章的正规化塔，一个阶段还可能同时加入多个共轭根式。它们没有改变本章这个结论的适用范围。

回到五次反证的连接

先假设原方程的根有根式公式，再按公式的开根中间量建塔。每个中间量因其产生方式具有幂等于前层元素的关系；公式最后输出的五个根则都落在塔顶。我们并没有假设原方程的每个根，本人都满足这种单次开根关系。

3.6 补充证明：按表达式结构归纳

允许的表达式由基础域元素、加减乘除与取 n 次根递归构成。

基础情形：一个 F 元素已在塔底。归纳步骤：若两个子表达式已在当前域，四则运算的结果仍在其中；若对一个已得到的元素取根，加入选定的根就得到下一层。每次节点处理后，所有已处理子表达式的值都在当前域。因此最终输出在塔顶。

多个子表达式分别带有根式时，可以先处理第一个，再处理第二个；扩大基础域不会破坏此前的等式 $\alpha^n = a$ 。这保证表达式有多个分支也能排成一条塔。

3.7 五个根分别有公式，怎样合并成一座塔

不能只为一个根写塔，就直接说塔顶包含全部根。假设五个根各有一个有限根式表达式，把这些表达式的开根操作都列出，按每个表达式内部的依赖顺序处理，并把选定的根式值放在同一个 Ω 中。

处理完第一个表达式后，继续处理第二个，直到第五个；被开方数由此前已经加入的元素构成，所以仍在当前域中。最终得到同一座有限塔，并有

$$x_1, \dots, x_5 \in R.$$

共同出现的根式可以复用；不复用也只会造成可删除的重复层。因此根式可解所需的是存在某座塔，而不是某个唯一、最短的塔。

若“公式”通过不同根号选择给出所有根，只需把所需的有限多个选择也加入公共塔。若只给出一个根，对于不可约多项式，可在第 6 章的正规大域中补出它的全部共轭；本篇反证采用“全部根根式可解”的标准表述。

3.8 一个具体的运算例子

考虑

$$u = \sqrt{2} + \sqrt{1 + \sqrt{2}}.$$

先取 $\alpha = \sqrt{2}$ ，再取 $\beta = \sqrt{1 + \alpha}$ 。域塔是

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta), \quad \alpha^2 = 2, \quad \beta^2 = 1 + \alpha.$$

加法得到 $u = \alpha + \beta$ ，无需再添一层。这个例子也预示正规化的困难：当 α 被送到 $-\alpha$ 时， β^2 的右边变成 $1 - \alpha$ ；只补原来的 β 的负号未必够。

3.9 反方向也成立，但尚未涉及群

塔中加入的每个 α_i 都是前层元素的一个根式；而代数生成域 $K(\alpha)$ 的元素可写成 α 的多项式，系数在 K （由最小多项式与 Bézout 等式消去分母）。归纳得到塔顶每个元素都有根式表达式。

因此，对分裂域为 E 的多项式，

全部根根式可解 $\iff \exists$ 有限根式塔 R/F ，使 $E \subseteq R$.

这只是“表达式”与“域塔”的互译；“Galois 群可解”还需要后续证明。

第 4 章：分裂域的位置，是中间域而不必是列出的层

原问题 A03：还是感觉差点意思，我的意思是说，如何保证根的域和系数的域就是这个塔的一部分

本章任务：准确证明 $F \subseteq E \subseteq R$ ，并区分“包含在塔顶中”与“出现在塔的建造记录中”。

4.1 系数域为什么在塔底

“用系数表达根”表示以这些系数及有理常数作为初始元素。先允许所有四则运算，就得到它们生成的域 F 。之后才按第 3 章加入根式。因此从 F 起塔是公式语义的翻译。

即使一个公式只实际使用部分系数，从完整系数域 F 起塔仍然可行：扩大初始可用元素，只会允许更多运算，不会破坏公式。

4.2 分裂域为什么包含在塔顶

第 3 章得到 $F \subseteq R$ 与 $x_i \in R$ 。而

$$E = F(x_1, \dots, x_5)$$

的定义，是包含 F 和全部 x_i 的最小域。 R 本身就是这样一个域，所以

$$\boxed{F \subseteq E \subseteq R.}$$

这里“所有根都在 R ”使用反证假设；“由此它们生成的域也在 R ”使用生成域的最小性。这是两个明确的理由。

4.3 更正原对话例子：真正没列出的中间域

原对话取 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ 作例子，暗示它没被列在

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

中。然而令 $u = \sqrt{2} + \sqrt{3}$ ，就有 $u^{-1} = \sqrt{3} - \sqrt{2}$ ，故

$$\sqrt{2} = \frac{u - u^{-1}}{2}, \quad \sqrt{3} = \frac{u + u^{-1}}{2}.$$

所以 $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ，它恰好等于塔顶。原结论成立，例子应改为下面这个。

取 $f(t) = t^2 - 6$ ，其分裂域是

$$E = \mathbb{Q}(\sqrt{6}).$$

用 $\sqrt{6} = \sqrt{2}\sqrt{3}$ 表达根，可采用塔

$$\mathbb{Q} = R_0 \subset R_1 = \mathbb{Q}(\sqrt{2}) \subset R_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = R.$$

于是 $E \subseteq R$ ，但 E 不是这三层中的任何一层。

逐项证明。 $[E : \mathbb{Q}] = 2$ ，因为 6 不是有理数平方，故 $E \neq R_0$ 。若 $\sqrt{6} = a + b\sqrt{2}$ ，其中 $a, b \in \mathbb{Q}$ ，平方比较系数得到

$$a^2 + 2b^2 = 6, \quad 2ab = 0.$$

若 $b = 0$ ，有理数平方为 6，不可能；若 $a = 0$ ，有 $b^2 = 3$ ，也不可能。所以 $E \neq R_1$ 。类似地， $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ：平方后只能得到有理数平方为 3 或为 $3/2$ ，都不可能。因此 $[R : \mathbb{Q}] = 4$ ，而 $[E : \mathbb{Q}] = 2$ ，故 $E \neq R_2$ 。这些平方不可能性可由有理数既约分式中素因子指数的奇偶性直接验证。

4.4 在图里， E 与各 R_i 未必可比较

准确的图是：有一座从 F 到 R 的根式塔；另有从 F 到 R 的中间域 E 。一般并不知道对每个 i ，是 $E \subseteq R_i$ 还是 $R_i \subseteq E$ 。

上例中 $E = \mathbb{Q}(\sqrt{6})$ 与 $R_1 = \mathbb{Q}(\sqrt{2})$ 都是二次域且不相等，所以彼此不包含。只能确定它们都包含 F 、都包含在 R 中。

回到主线：后面使用 $E \subseteq N$ 和限制映射，将大群的信息传给 E 。完全不需要把 E 硬塞成原根式塔某一层。

第 5 章：补单位根，单个根式层才有阿贝尔群

本章任务：解释为什么原始塔未必 Galois，证明补单位根的基础层阿贝尔，并证明固定单位根后的单根式层是循环群的子群。

5.1 原始根式层缺少什么

令 $\alpha = \sqrt[3]{2}$ ，则 $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ 。多项式 $t^3 - 2$ 在 $\mathbb{Q}$ 上不可约：三次式可约必有有理根，而有理根只能是整数因子 $\pm 1, \pm 2$ ，逐个代入都不是根。

它另外两根 $\omega\alpha, \omega^2\alpha$ 为非实数，不在 $\mathbb{Q}(\alpha)$ 中。所以该扩张不正规，也不是 Galois。它的自同构群仍可以定义，而且这里只含恒等映射；但不能用“群阶等于扩张次数”的 Galois 结论。

5.2 补单位根，先处理对原基础域的那一层

对原始塔中的指数 $n_1, \dots, n_m$ ，取

$$q = \text{lcm}(n_1, \dots, n_m), \quad M_0 = F(\mu_q) = F(\zeta_q).$$

没有根式操作时约定 $q = 1$ 。 M_0 是 $t^q - 1$ 在 F 上的分裂域。特征零使该多项式可分，因为它与导数 qt^{q-1} 没有共同根，所以 M_0/F 是有限 Galois 扩张。

补充证明：这层群为什么阿贝尔。自同构保持元素的乘法阶： $\sigma(u)^d = 1$ 等价于 $u^d = 1$ ，反方向由逆自同构得到。因此 $\sigma(\zeta_q)$ 仍为本原 q 次单位根，可以唯一写为 ζ_q^a ，其中 $\gcd(a, q) = 1$ ，指数按模 q 取值。

由于 M_0 由 F 和 ζ_q 生成，指数决定整个自同构。又有

$$\sigma_a \sigma_b(\zeta_q) = \zeta_q^{ab}.$$

所以得到单射同态

$$\text{Gal}(M_0/F) \hookrightarrow (\mathbb{Z}/q\mathbb{Z})^\times.$$

右端乘法交换，左端便阿贝尔。 $q = 1$ 时扩张和群都平凡，单独处理即可。

这里对一般 F 只证明嵌入，没有声称是整个可逆剩余类群。例如 F 已含所有单位根时，左端平凡。已有分圆笔记证明了在 $\mathbb{Q}$ 上得到整个群；本篇只需要这个子群结论。

5.3 单个根式层的完整群论计算

设 K 特征零，且 $\mu_n \subseteq K$ 。取 $a \in K$ ， $\alpha^n = a$ ，令 $L = K(\alpha)$ 。

若 $a = 0$ ，则 $\alpha = 0$ ， $L = K$ ，群平凡。以下设 $a \neq 0$ 。 $t^n - a$ 的根恰为 $\zeta\alpha$ ，其中 $\zeta \in \mu_n$ ；它们都在 L ，而且互不相同。因此 L/K 是有限可分分裂域，也就是 Galois 扩张。

对 $\sigma \in \text{Gal}(L/K)$ ，定义

$$\chi(\sigma) = \frac{\sigma(\alpha)}{\alpha} \in \mu_n.$$

若 $\chi(\sigma) = 1$ ，则 σ 固定 K 与生成元 α ，故为恒等。因此 χ 单射。因为 $\tau(\alpha)/\alpha \in K$ ， σ 固定它，所以

$$\begin{aligned}
\chi(\sigma\tau) &= \frac{\sigma(\tau(\alpha))}{\alpha} \\
&= \frac{\sigma((\tau(\alpha)/\alpha)\alpha)}{\alpha} \\
&= \frac{\tau(\alpha)}{\alpha} \frac{\sigma(\alpha)}{\alpha} = \chi(\sigma)\chi(\tau).
\end{aligned}$$

所以它是单射群同态。 $\mu_n = \langle \zeta_n \rangle$ 是循环群，故

$\text{Gal}(L/K)$ 是循环群的子群，因而阿贝尔。

循环群的子群仍循环：取子群中最小正指数 d ，对任何其他指数作除法，余数若非零会违反 d 的最小性，故所有元素都是 ζ_n^d 的幂。平凡子群也循环。

5.4 为什么必须逐点固定单位根

上面的同态验证真正用到 $\sigma(\zeta) = \zeta$ 。只知道域里含有单位根，或自同构把单位根集合送回自身，都不够；单位根必须属于被逐点固定的基础域 K 。

例如 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega)$ 的群是 C_3 ，而它对 $\mathbb{Q}$ 的群是 S_3 。后者允许复共轭把 ω 送到 ω^2 。同一个顶层域，换基础域，得到的群就不同。

例子的次数与群核对。 令 $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 。三次不可约性给出 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ；该域为实域，不含非实的 ω ，而 ω 满足二次式 $t^2 + t + 1$ ，所以 $[L : \mathbb{Q}] = 6$ 。 L 是 $t^3 - 2$ 的可分分裂域，群忠实作用于三个根。有限可分扩张的嵌入数等于次数：逐个加入代数元，每一个已有嵌入都恰有该步最小多项式次数个延拓，因为该多项式可分；次数与选择数都沿塔相乘。正规性使这些嵌入全是自同构。因此该群有 6 个元素，嵌入 S_3 后只能等于 S_3 。又 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ ，故 $[L : \mathbb{Q}(\omega)] = 3$ ；固定单位根后的群由第 5.3 节是循环群，且阶为 3，故为 C_3 。

5.5 同时加入多个根式，群仍阿贝尔

设 $\mu_n \subseteq K$ ，且有限个 β_j 满足 $\beta_j^n = b_j \in K$ ， $b_j \neq 0$ 。取

$$L = K(\beta_1, \dots, \beta_s).$$

它包含所有 $t^n - b_j$ 的全部根，是这些多项式的共同分裂域，因此 L/K Galois。将第 5.3 节的计算对每个生成元做一遍，得到

$$\text{Gal}(L/K) \hookrightarrow \mu_n^s, \quad \sigma \mapsto \left(\frac{\sigma(\beta_1)}{\beta_1}, \dots, \frac{\sigma(\beta_s)}{\beta_s} \right).$$

比值决定生成元的像，故单射；固定各比值保证同态。有限直积 μ_n^s 阿贝尔，所以左端阿贝尔。它未必循环，这是正规化后“一个阶段加入很多共轭根式”需要的准确结论。

回到主线：补单位根解决单层的群结构；还没有证明整座塔对原基础域 F 正规。下一章解决这件事。

第 6 章：逐层补共轭，构造对原基础域 Galois 的大域

本章任务：实际构造 $R \subseteq N$ ，同时保证 N/F Galois，并保留可解性所需的阿贝尔层。不能只写“取正规闭包”就跳到“群可解”。

6.1 先看为什么只补各层负号不够

第 3.8 节中的塔满足 $\alpha^2 = 2$ 、 $\beta^2 = 1 + \alpha$ 。若一个固定 $\mathbb{Q}$ 的嵌入把 α 送到 $-\alpha$ ，它必须把 β 送到某个满足

$$\gamma^2 = 1 - \alpha$$

的元素。只把 β 换成 $-\beta$ ，其平方仍是 $1 + \alpha$ ，并没有补出这次嵌入需要的像。

因此要补的对象包括被开方数在基础域自同构下的所有像，再对它们开根。第 5 章处理的单位根倍数，只是固定某一个被开方数时的根。

6.2 本章将证明的构造结论

原始塔为

$$F = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_m = R, \quad R_i = R_{i-1}(\alpha_i), \quad \alpha_i^{n_i} = a_i \in R_{i-1}.$$

将构造

$$F \subseteq M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = N,$$

满足下表。

条件	为什么需要
$R_i \subseteq M_i$	新塔保留原公式的全部运算结果
每个 M_i/F 有限 Galois	每层对原基础域稳定，方便使用限制映射
$\text{Gal}(M_0/F)$ 阿贝尔	加单位根的那一层也纳入证明
每个 $\text{Gal}(M_i/M_{i-1})$ 阿贝尔	将新塔翻译为可解群的正规列

注意 F 始终不变。不能先把底层扩大到 $F(\mu_q)$ ，最后却忘记证明回到原 F 时的群仍可解。

6.3 两个域论事实及其理由

特征零保证代数扩张可分。首一不可约多项式 p 的导数 p' 非零且次数更低。若 p 有重根，便有 $\gcd(p, p') \neq 1$ ；不可约性会迫使 $p \mid p'$ ，与次数矛盾。因此不可约多项式的根互异。

有限可分扩张的正规性，可用嵌入稳定来检验。若有限扩张 L/K 中每个有根的不可约 K 多项式都分裂，那么固定 K 的嵌入把每个生成元送到其最小多项式的另一个根，也在 L ，所以像包含在 L ；有限维数给出像等于 L 。反方向：任一最小多项式的任一根都定义一个简单扩张的嵌入，再按第 7.2 节的延拓构造延到 L ；若所有嵌入都稳定 L ，这些根便全在 L 。该延拓证明独立于本章，不以正规性或可解性为前提。

特别地，共同分裂域的生成元是已加入的多项式根，任何固定系数域的嵌入仍把它们送到已加入的根；因此共同分裂域正规。

6.4 从第一层开始归纳

设 $M_0 = F(\mu_q)$ ，其中 q 为全部 n_i 的最小公倍数。第 5.2 节已证明 M_0/F 有限 Galois，群阿贝尔；并且 $R_0 = F \subseteq M_0$ 。

归纳假设已经构造 M_{i-1} ，使其对 F 有限 Galois，且 $R_{i-1} \subseteq M_{i-1}$ 。定义有限集合

$$\mathcal{A}_i = \{\sigma(a_i) : \sigma \in \text{Gal}(M_{i-1}/F)\}.$$

群有限，因为有限扩张的嵌入个数不超过扩张次数：逐个加入代数生成元，每次像只能从有限个最小多项式的根中选择。故上面的集合也有限。

令 M_i 是在 M_{i-1} 上加入所有多项式

$$t^{n_i} - b, \quad b \in \mathcal{A}_i$$

的全部根所得的域。由于多项式和根的数目有限，这一步是有限扩张。

6.5 它为什么仍包含原始塔的这一层

恒等自同构属于 $\text{Gal}(M_{i-1}/F)$ ，所以 $a_i \in \mathcal{A}_i$ 。我们加入 $t^{n_i} - a_i$ 的所有根，当然包括原先选定的 α_i 。又有 $R_{i-1} \subseteq M_{i-1}$ ，于是

$$R_i = R_{i-1}(\alpha_i) \subseteq M_i.$$

这个包含关系逐层归纳，最后得到 $R \subseteq N$ 。

6.6 这一阶段的群为什么阿贝尔

因为 $n_i \mid q$ ，所有 n_i 次单位根属于 M_0 ，因而属于 M_{i-1} 。对每个非零 $b \in \mathcal{A}_i$ ，选一个根 β_b ；其他根均为单位根倍数。 $b = 0$ 时只有根 0，不增加扩张。

所以

$$M_i = M_{i-1}(\beta_b : b \in \mathcal{A}_i, b \neq 0),$$

且第 5.5 节给出

$$\text{Gal}(M_i/M_{i-1}) \hookrightarrow \prod_{b \in \mathcal{A}_i, b \neq 0} \mu_{n_i}.$$

这既证明该层 Galois，也证明其群阿贝尔。一个阶段可能加入多个根式，所以群是循环群有限直积的子群，不能一律说它循环。

6.7 最关键的补充证明：为什么 M_i 对原 F 也正规

任取固定 F 的嵌入 $\tau : M_i \rightarrow \Omega$ 。归纳假设使

$$\tau(M_{i-1}) = M_{i-1}, \quad \eta = \tau|_{M_{i-1}} \in \text{Gal}(M_{i-1}/F).$$

对 $b = \sigma(a_i) \in \mathcal{A}_i$ ，有

$$\tau(b) = \eta\sigma(a_i) \in \mathcal{A}_i.$$

因此 τ 把被开方数集合送回自身； η^{-1} 也如此，故实际上置换这个集合。

若 $\beta^{n_i} = b \in \mathcal{A}_i$ ，则

$$\tau(\beta)^{n_i} = \tau(b) \in \mathcal{A}_i.$$

所有这样的多项式的根已经加入 M_i ，所以 $\tau(\beta) \in M_i$ 。 M_i 由 M_{i-1} 和这些根生成，因此 $\tau(M_i) \subseteq M_i$ 。

最后， τ 是固定 F 的单射线性映射，有限维数给出

$$[\tau(M_i) : F] = [M_i : F],$$

结合像的包含得到 $\tau(M_i) = M_i$ 。所以 M_i/F 正规；特征零保证可分，故是有限 Galois 扩张。归纳完成。

6.8 最终得到的是怎样的大域

设 $N = M_m$ 。我们已经证明

$$R \subseteq N, \quad N/F \text{ 有限 Galois,} \quad \text{新塔每个阶段的相对群都阿贝尔。}$$

这是一种明确的正规化构造，不要求 N 恰好是 R/F 的最小正规闭包。加入额外单位根后， N 可能更大。证明只需要它有限、包含 R 、对 F Galois，且拥有这些阿贝尔层。

如果只知道某个根 u 在 R 中，那么 $u \in N$ ；因 N/F 正规，它包含 u 的全部 F 共轭。对于不可约的原多项式，这些共轭就是它的全部根。这个补充情形也说明正规化究竟补了什么。

回到主线：域的构造已经完成。接下来要把“每层的群阿贝尔”翻译为“大群存在阿贝尔商的正规列”。

第 7 章：域塔怎样变成可解群的正规列

本章任务：证明 $\text{Gal}(N/F)$ 可解，并补齐限制映射与商群识别所需的域论工具。

7.1 可解群定义要求的是相邻正规与阿贝尔商

群 G 可解，是指存在有限列

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

每个 G_{j+1} 正规于 G_j ，且每个 G_j/G_{j+1} 阿贝尔。相邻项可以相等，重复项删去即可。不要求各 G_j 都正规于整个 G ；第 6 章的构造碰巧满足更强的条件。

要从域塔得到这样的群列，需要解释：这些子群是什么、正规性为什么成立、商群为什么等于相邻域层的群。

7.2 补充证明：嵌入可以逐个代数元延拓

设 $K \subseteq L$ 有限代数，已有域嵌入 $\varphi: K \rightarrow \Omega$ ， Ω 代数闭。先加入一个 $u \in L$ ，设其最小多项式是 $p(t) \in K[t]$ 。

将系数逐项应用 φ ，得到 $p^\varphi(t) \in \varphi(K)[t]$ 。系数域同构保持不可约性：若新多项式可约，逆向传回系数就会分解 p 。在 Ω 中取 p^φ 的一个根 v ，定义

$$\tilde{\varphi} \left(\sum_{j=0}^{d-1} c_j u^j \right) = \sum_{j=0}^{d-1} \varphi(c_j) v^j, \quad d = \deg p.$$

为何良定义并保持运算？ 求值映射的核是 (p) ：对任意多项式先除以 p ，若余式在 u 处为零，余式次数更低，只能为零。故 $K(u) \cong K[t]/(p)$ 。同理， $\varphi(K)[t]/(p^\varphi)$ 是域，并可嵌入 Ω ，把 t 的类送到 v 。上述映射正是这两个商域之间的系数同构加求值，因而良定义、保加法乘法，并且单射。它显然延拓 φ 。

有限扩张可以由有限个代数元生成：例如取一组有限基，其元素生成整个域。逐个重复这个构造，就将 φ 延拓到整个 L 。

这个引理只保证像在代数闭包中。若 L/K 正规，并且原嵌入固定 K ，才进一步保证像等于 L ，使延拓成为自同构。

7.3 补充证明：限制映射与商群的一般模板

设

$$B \subseteq C \subseteq D, \quad D/B \text{ 有限 Galois}, \quad C/B \text{ Galois}.$$

定义

$$\text{res} : \text{Gal}(D/B) \longrightarrow \text{Gal}(C/B), \quad \sigma \longmapsto \sigma|_C.$$

逐项检查如下。

- **值域正确**：\$C/B\$ 正规，使固定 \$B\$ 的嵌入把 \$C\$ 送回 \$C\$；因此 \$\sigma|_C\$ 确实是 \$C\$ 的自同构。
- **同态**：对 \$c \in C\$，\$\text{res}(\sigma\tau)(c) = \sigma(\tau(c)) = (\sigma|_C)(\tau|_C)(c)\$。
- **核**：映到恒等自同构，恰好表示逐点固定 \$C\$，故核为 \$\text{Gal}(D/C)\$。
- **满射**：任取 \$\tau \in \text{Gal}(C/B)\$，用第 7.2 节延拓到 \$D \rightarrow \Omega\$；延拓仍固定 \$B\$，而 \$D/B\$ 正规使其像为 \$D\$。它于是属于 \$\text{Gal}(D/B)\$，限制回 \$C\$ 就是原 \$\tau\$。

核总正规：若 \$h\$ 在核中，\$\text{res}(ghg^{-1}) = \text{res}(g)1\text{res}(g)^{-1} = 1\$。因此令 \$K = \text{Gal}(D/C)\$，可以定义

$$\overline{\text{res}} : \text{Gal}(D/B)/K \longrightarrow \text{Gal}(C/B), \quad \sigma K \longmapsto \sigma|_C.$$

若换代表元 \$\sigma h\$，其中 \$h \in K\$，限制的结果不变，所以良定义。若两代表元限制相同，则 \$\sigma^{-1}\tau \in K\$，故为同一陪集，得到单射；限制满射给出满射；乘法由限制同态得到。因此

$$\boxed{\text{Gal}(D/B)/\text{Gal}(D/C) \cong \text{Gal}(C/B).}$$

这就是本篇真正用到的商群公式，已经直接证明，无需把“Galois 对应”当作省略整段论证的理由。

7.4 把模板用于正规化的塔

第 6 章有

$$F \subseteq M_0 \subseteq \cdots \subseteq M_m = N.$$

令

$$G = \text{Gal}(N/F), \quad H_i = \text{Gal}(N/M_i).$$

固定的域越大，允许的自同构越少，所以

$$G \supseteq H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}.$$

各 M_i/F Galois，限制到 M_i 的映射以 H_i 为核，故 $H_i \triangleleft G$ ；特别有相邻正规性。

将第 7.3 节模板用于 $F \subseteq M_0 \subseteq N$ ，得到

$$G/H_0 \cong \text{Gal}(M_0/F).$$

再用于 $M_{i-1} \subseteq M_i \subseteq N$ ，得到

$$H_{i-1}/H_i \cong \text{Gal}(M_i/M_{i-1}), \quad 1 \leq i \leq m.$$

为何 N/M_{i-1} Galois？任意固定 M_{i-1} 的嵌入也固定 F ，由 N/F 正规得到像为 N ；可分性由特征零保证。 M_i/M_{i-1} 已在第 6 章证明 Galois。

7.5 商群阿贝尔，定义便真正满足了

第 5 章证明 $\text{Gal}(M_0/F)$ 阿贝尔，第 6 章证明各 $\text{Gal}(M_i/M_{i-1})$ 阿贝尔。所以

$$G \triangleright H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = \{1\}$$

的所有相邻商都阿贝尔，正好满足可解定义。因此

$\text{Gal}(N/F)$ 可解。

回到主线：得到的是包含原根式塔的大域 N 的群可解。还需要把这个结论传给方程自身的分裂域 E 。

第 8 章：限制映射，把大群的可解性传给分裂域

本章任务：证明 $\text{Gal}(E/F)$ 是可解大群的商群，并完整补齐可解群关于子群、商群与扩张的三个引理。

8.1 同一个 E ，已经落在 N 中

第 4 章由根式公式假设得到 $E \subseteq R$ ，第 6 章得到 $R \subseteq N$ ，所以

$$F \subseteq E \subseteq N.$$

第 2 章证明 E/F Galois，第 6 章证明 N/F Galois。第 7.3 节的全部条件已满足，于是限制映射给出

$$\text{res} : \text{Gal}(N/F) \rightarrow \text{Gal}(E/F), \quad \ker \text{res} = \text{Gal}(N/E),$$

因此

$$\boxed{\text{Gal}(E/F) \cong \frac{\text{Gal}(N/F)}{\text{Gal}(N/E)}}.$$

大群的元素是 N 上的自同构，目标群的元素是 E 上的自同构；限制不是把这些映射当作完全相同的对象，而是改变它们作用的输入范围。

8.2 为什么是商群，而不是直接当作子群

一个 E 的自同构可能有多个延拓到 N 。若两个 N 自同构在 E 上相同，则它们之差 $\sigma^{-1}\tau$ 逐点固定 E ，属于 $\text{Gal}(N/E)$ 。因此“它们在 E 上产生相同作用”对应一个核的陪集。

把同一个陪集内的延拓认作一类，才得到 E 上的一个自同构。这就是商群在这里出现的原因。一般没有一个自然、保持复合的“任选延拓”方式把 $\text{Gal}(E/F)$ 直接嵌入大群。

8.3 补充完整证明：可解群子群仍可解

原问题 A05：可解群的子群和商群都是可解的是吗

设 $G = G_0 \triangleright \cdots \triangleright G_r = \{1\}$ 是可解列， $H \leq G$ 。令 $H_i = H \cap G_i$ 。

对 $h \in H_i$ 、 $u \in H_{i+1}$ ， huh^{-1} 同时属于 H 与 G_{i+1} ：前者由 H 封闭，后者由 $G_{i+1} \triangleleft G_i$ 。故 $H_{i+1} \triangleleft H_i$ 。

定义

$$H_i/H_{i+1} \longrightarrow G_i/G_{i+1}, \quad hH_{i+1} \longmapsto hG_{i+1}.$$

换代表元只差一个 $H_{i+1} \subseteq G_{i+1}$ 的元素，所以良定义；陪集乘法表明它保持运算。核中满足 $h \in G_{i+1}$ ，又 $h \in H$ ，故 $h \in H_{i+1}$ ，所以单射。

目标阿贝尔，定义域也阿贝尔。于是

$$H = H_0 \triangleright \cdots \triangleright H_r = \{1\}$$

是一条可解列， H 可解。相邻交集若相等，删去重复项即可。

8.4 补充完整证明：可解群的商群仍可解

设 $K \triangleleft G$ ， $\pi: G \rightarrow G/K$ 是投影。记 $Q_i = \pi(G_i)$ 。像保持包含，因此

$$G/K = Q_0 \supseteq \cdots \supseteq Q_r = \{1\}.$$

若 $a \in G_i$ 、 $b \in G_{i+1}$ ，则

$$\pi(a)\pi(b)\pi(a)^{-1} = \pi(aba^{-1}) \in Q_{i+1}.$$

所以 $Q_{i+1} \triangleleft Q_i$ 。因 G_i/G_{i+1} 阿贝尔，任意 $a, b \in G_i$ 的交换子 $aba^{-1}b^{-1} \in G_{i+1}$ 。应用 π ，便知 Q_i/Q_{i+1} 中的交换子都是单位元，即该商阿贝尔。

于是投影后的列是一条可解列， G/K 可解。这里仅需相邻正规性，没有暗中要求所有 G_i 正规于整个 G 。

8.5 补充完整证明：可解的核与商能拼出可解的整体

设 $K \triangleleft G$ ， K 可解， G/K 可解。令 $\pi: G \rightarrow G/K$ ，取商群的一条可解列

$$G/K = Q_0 \triangleright Q_1 \triangleright \cdots \triangleright Q_s = \{1\}.$$

取逆像 $L_i = \pi^{-1}(Q_i)$ ，有 $L_0 = G$ 、 $L_s = K$ 。若 $a \in L_i$ 、 $b \in L_{i+1}$ ，其像的共轭仍在 Q_{i+1} ，故 $aba^{-1} \in L_{i+1}$ 。因此 $L_{i+1} \triangleleft L_i$ 。

映射 $L_i \rightarrow Q_i/Q_{i+1}$ 由 π 再投影得到，满射且核为 L_{i+1} ；第 7.3 节同样的陪集验证给出

$$L_i/L_{i+1} \cong Q_i/Q_{i+1},$$

所以这些商都阿贝尔。把 K 自己的可解列接在 $L_s = K$ 后面，得到 G 的可解列。因此

$$\boxed{K \text{ 可解且 } G/K \text{ 可解} \implies G \text{ 可解。}}$$

不要求 G 由核与商群的直积构成；这个引理处理的正是一般的群扩张。

8.6 现在才把结论传给原方程

第 7 章给出 $\text{Gal}(N/F)$ 可解；第 8.1 节给出 $\text{Gal}(E/F)$ 是其商群；第 8.4 节给出可解性在商群下保持。于是

假设全部根有根式表达式 $\implies \text{Gal}(E/F)$ 可解。

这才完整接上“根式可解”与“Galois 群可解”。三个可解性引理中，这一步具体使用**商群引理**；子群引理稍后用于 S_5 的障碍，扩张引理解释跨层拼接。

第 9 章：不相邻层可以吗？先检查使用条件

原问题 A04：然后就是相邻域之间的glaos群之间的可解，我突然想起来不相邻可以吗

本章任务：把“可解性能够跨层”与“Galois 性不自动跨层”区分，并给出能够直接使用的条件。

9.1 三层拼接的准确陈述

设 $B \subseteq C \subseteq D$ ， D/B 有限 Galois，且 C/B Galois。第 7.3 节给出正合结构

$$1 \longrightarrow \text{Gal}(D/C) \longrightarrow \text{Gal}(D/B) \xrightarrow{\text{res}} \text{Gal}(C/B) \longrightarrow 1.$$

此处“正合”只是在压缩我们已经证明的事情：左侧是核，右侧限制满射。若两端群可解，第 8.5 节便给出中间群可解。这是跨层拼接的依据。

9.2 相邻两步 Galois，不保证总扩张 Galois

令 $a = \sqrt[4]{2}$ ，取

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(a).$$

第一步二次 Galois。第二步由 $a^2 = \sqrt{2}$ 得到，另一根 $-a$ 已在域内，且确实为二次：若 $\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 中某个 $(u + v\sqrt{2})^2$ ，比较系数将给出

$$u^2 + 2v^2 = 0, \quad 2uv = 1,$$

其中 $u, v \in \mathbb{Q}$ 。第一式迫使 $u = v = 0$ ，与第二式矛盾。因此第二步也是二次 Galois。

塔式定理给出 $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ ，所以 $t^4 - 2$ 是 a 的最小多项式。其根 $ia, -ia$ 不在实域 $\mathbb{Q}(a)$ 中，故总扩张不正规，也不是 Galois。

因此

$$D/C \text{ Galois}, C/B \text{ Galois} \not\Rightarrow D/B \text{ Galois}.$$

仍可定义 $\text{Aut}_B(D)$ ，通常也记作 $\text{Gal}(D/B)$ ；缺少的是 Galois 扩张的性质及相应商群模板，不是“自同构群无法存在”。本篇说“该层 Galois 群”时，涉及群阶、限制满射与商群公式，都会先检查扩张条件。

9.3 在本篇加工后的塔中，跨层为什么安全

第 6 章故意保证每个 M_i/F 都 Galois。因此任取 $i < j$ ， M_j/M_i 也是 Galois：固定 M_i 的嵌入固定 F ，所以保持 M_j ；特征零保证可分。

每个 $\text{Gal}(M_j/F)$ 也是 $G = \text{Gal}(N/F)$ 的商群，所以可解。其子群 $\text{Gal}(M_j/M_i)$ 因而可解。于是

在构造好的 M 塔中，任意不相邻的相对群都可解。

也可以固定一段 $M_i \subseteq \cdots \subseteq M_j$ ，把它反向译成群列；相邻商仍阿贝尔，所以整段的群可解。

9.4 条件表：实际应用时检查哪一条

已知条件	可得结论
D/B 有限 Galois, C/B Galois	限制到 C 满射, 核为 $\text{Gal}(D/C)$, 得到商群公式
再知两个相对群 $\text{Gal}(D/C)$ 、 $\text{Gal}(C/B)$ 可解	由扩张引理, $\text{Gal}(D/B)$ 可解
只知 D/C 与 C/B 都 Galois	总扩张 D/B 未必 Galois; 不能直接套上一行的公式
N/F 有限 Galois, 群可解; $F \subseteq K \subseteq L \subseteq N$, 且 L/K Galois	$\text{Gal}(L/K)$ 是可解群 $\text{Gal}(N/K)$ 的商群, 故可解

最后一行中 N/K Galois, 因为它是 Galois 顶层向中间基础域的扩张; $\text{Gal}(N/K)$ 是 $\text{Gal}(N/F)$ 的子群。然后把第 7.3 节用于 $K \subseteq L \subseteq N$ 。

回到主线：可解性可以跨很多层。使用正规子群与商群翻译之前，域论条件必须已经成立；这就是第 6 章逐层正规化的用途。

第 10 章：为什么 S_5 不可解，完整补上群论障碍

本章任务：为框架中的“ S_5 不可解”提供一份可独立核对的证明。已熟悉 A_5 的读者，可以先读第 10.1、10.6 节。

10.1 真正要证明的是不存在任何可解列

找到一条 $S_5 \triangleright A_5 \triangleright \{1\}$ 的链，并发现它有一个非阿贝尔商，只能说明这条链不满足可解定义；尚未排除别的可解列。

严谨路线是：证明 A_5 是非阿贝尔单群，从而它不可能有可解列；再由“可解群的任意子群仍可解”推出包含它的 S_5 不可解。

所谓**单群**，是只有平凡子群与自身这两个正规子群的非平凡群。

10.2 奇偶性与 A_5 的大小

一个 k 循环可写成 $k - 1$ 个换位，所以其符号为 $(-1)^{k-1}$ 。奇偶性良定义，可用如下短证明核对：令

$$\Delta(X_1, \dots, X_5) = \prod_{i < j} (X_i - X_j).$$

重排变量后，各无序对的因子仍出现一次，只可能改变符号，所以 $T_\pi(\Delta) = \varepsilon_\pi \Delta$ ，其中 $\varepsilon_\pi \in \{1, -1\}$ 。任意换位使该乘积变号：被交换那对的因子变号，其余涉及它们的因子成对重排。复合变量置换给出 $\varepsilon_{\pi\tau} = \varepsilon_\pi \varepsilon_\tau$ 。因此不论把置换写成哪种换位分解，换位个数的奇偶性都相同。

符号映射 $S_5 \rightarrow \{1, -1\}$ 满射，其核是 A_5 。乘以一个固定换位给出偶置换与奇置换的双射，故

$$|S_5| = 5! = 120, \quad |A_5| = 60.$$

A_5 作为符号同态的核正规于 S_5 ，并有 $S_5/A_5 \cong C_2$ 。但这个阿贝尔商本身不能消除 A_5 内部的障碍。

10.3 偶置换的全部循环类型与数量

把五个对象的置换分解成不相交循环。枚举 5 的分拆并检查符号，得到偶置换仅有以下四种类型。

类型	数量	计数理由
恒等置换	1	全部不动
三循环	20	选三对象有 $\binom{5}{3} = 10$ 种，每组三对象有 2 个三循环

类型	数量	计数理由
两个不相交换位	15	选不动对象有 5 种，其余四对象有 3 种配对
五循环	24	固定循环开头后排列其余对象，有 $4! = 24$ 种

总数 $1 + 20 + 15 + 24 = 60$ ，恰好覆盖 A_5 。

10.4 补充完整证明：共轭类大小是 1、20、15、12、12

对群 G 的元素 c ，其中心化子为

$$C_G(c) = \{g \in G : gc = cg\}.$$

两个元素 g, h 给出同一共轭 $gcg^{-1} = hch^{-1}$ ，当且仅当 $h^{-1}g \in C_G(c)$ 。所以共轭类与中心化子的左陪集一一对应，类大小为 $|G|/|C_G(c)|$ 。

三循环。取 $c = (123)$ 。与它交换的置换必须保持支撑集 $\{1, 2, 3\}$ ；在这三点上只能是 c 的三个幂，在 $\{4, 5\}$ 上可以恒等或交换。这使 $C_{S_5}(c)$ 有 6 个元素。 c 的幂均为偶置换，而 (45) 是奇置换，故 $C_{A_5}(c)$ 有 3 个元素。类大小 $60/3 = 20$ ，所有三循环形成一个类。

双换位。取 $c = (12)(34)$ 。交换者必须固定唯一不动点 5。可把 1 送到四个支撑点中的任意一点，其像一确定，2 的像便由 $g(2) = c(g(1))$ 确定；3 的像有剩下的两个选择，4 的像随之确定。恰有 $4 \cdot 2 = 8$ 个交换者。这些选择都保持 c 的两点轨道，确实满足交换。中心化子含奇置换 (12) ，乘以它给出奇偶元素的双射，因此偶交换者有 4 个。类大小 $60/4 = 15$ ，所有双换位形成一个类。

五循环。取 $c = (12345)$ 。若 g 与 c 交换， $g(1)$ 一确定， $g(c^j(1)) = c^j(g(1))$ 决定其余全部像。五个选择分别给出 c 的五个幂，因此中心化子是 $\langle c \rangle$ 。它们全为偶置换，故在 A_5 中的中心化子大小为 5，类大小 $60/5 = 12$ 。共有 24 个五循环，每个类都大小 12，所以分成两个类。

因此 A_5 的共轭类大小恰为

$$1, 20, 15, 12, 12.$$

10.5 正规子群只能是共轭类并集，推出单群性

若 $K \triangleleft A_5$ ，且 $c \in K$ ，则对每个 $g \in A_5$ 都有 $gcg^{-1} \in K$ 。因此 K 是若干完整共轭类的并集，且必须包含恒等类。

所以 $|K|$ 是 1 加上 20, 15, 12, 12 中某些数的和。全部不同的可能值为

$$1, 13, 16, 21, 25, 28, 33, 36, 40, 45, 48, 60.$$

另一方面，Lagrange 定理要求 $|K| \mid 60$ ：左陪集相交则相等，各陪集都与 K 等大，而它们分割 A_5 ，故 60 是 $|K|$ 的整数倍。在上述名单中，仅 1 和 60 整除 60。于是 K 只能平凡或等于整个 A_5 ，证明 A_5 单。

10.6 非阿贝尔单群不可解，所以 S_5 不可解

取 $a = (123)$ 、 $b = (345)$ ，乘积从右向左作用，则

$$ab(3) = 4, \quad ba(3) = 1.$$

所以 $ab \neq ba$ ， A_5 非阿贝尔。

若 A_5 存在可解列，删除重复项后，紧邻 A_5 的下一个真子群必须正规于 A_5 。单群性迫使它为 $\{1\}$ ，于是第一层商群就是 A_5 本身，却非阿贝尔，矛盾。因此 A_5 不可解。

若 S_5 可解，其子群 A_5 应由第 8.3 节也可解，矛盾。所以

$$S_5 \text{ 不可解。}$$

回到主线：结合第 2 章，已经独立证明通用五次方程的 $\text{Gal}(E/F)$ 不可解。

第 11 章：把所有桥梁合起来，完成反证

本章任务：将已经证明的结论按用途连接，明确矛盾落在何处，以及最终结论的边界。

11.1 方程自身给出的结论

取代数独立的形式根，构造

$$F = \mathbb{Q}(e_1, \dots, e_5), \quad E = \mathbb{Q}(x_1, \dots, x_5), \quad f(t) = \prod_{i=1}^5 (t - x_i) \in F[t].$$

第 2 章完整证明 E/F 是有限 Galois 分裂域，且 $\text{Gal}(E/F) \cong S_5$ 。第 10 章证明 S_5 不可解。因此

$\text{Gal}(E/F)$ 不可解。

到这里还没有假设根式公式。

11.2 反证假设制造的对象

假设这个通用五次方程的全部根，都能从 F 出发用有限次四则运算和开根得到。

第 3 章把所有表达式合并成一座根式塔 R/F ，其塔顶包含所有 x_i ；第 4 章用生成域的最小性得到 $E \subseteq R$ 。

第 5、6 章补单位根并逐层补被开方数的共轭，构造 N ，满足

$$F \subseteq E \subseteq R \subseteq N, \quad N/F \text{ 有限 Galois}.$$

第 7 章把新域塔翻译成阿贝尔商的正规列，证明 $\text{Gal}(N/F)$ 可解。

第 8 章通过限制满射与商群引理推出

$\text{Gal}(E/F)$ 可解。

11.3 矛盾准确落在同一个群上

由通用方程的结构： $\text{Gal}(E/F)$ 不可解。

由假设存在根式公式： $\text{Gal}(E/F)$ 可解。

两条路线的基础域都是原来的 F ，分裂域都是原来的 E 。因此结论互相矛盾，根式公式假设必须否定。

得到

通用五次方程在其系数域上不能由根式解。

按通常的“通用根式公式”含义，公式由一般系数和有理常数，通过有限四则运算与开根构成；将一般系数作为代数独立变量使用，它就会给出通用模型中的根式表达式。所以通用模型的障碍排除了这样的公式。

这不是对某个具体数字五次式一概下结论，也没有声称所有五次式的群都是 S_5 。若允许公式中固定的其他常数作为基础常数，可在相应特征零常数域 k 上重新取代数独立的 x_i ，同样构造 $k(e_1, \dots, e_5) \subseteq k(x_1, \dots, x_5)$ ；本篇的变量置换与正规化证明仍成立。

11.4 为什么“具体五次可能可解”不矛盾

例如 $t^5 - 2$ 的根为

$$\sqrt[5]{2} \zeta_5^j, \quad 0 \leq j \leq 4.$$

这是有额外结构的具体方程。在 $\mathbb{Q}$ 上，先加入 ζ_5 的群是阿贝尔，再加入 $\sqrt[5]{2}$ 的相对群也是阿贝尔；整个分裂域对 $\mathbb{Q}$ Galois，扩张引理使其群可解。它并不是通用五次模型。

要把“全部根都有根式表达式”落实到 $\mathbb{Q}$ ，还需确认 ζ_5 也是根式：令

$u = \zeta_5 + \zeta_5^{-1} = 2 \cos(2\pi/5)$ 。由 $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$ ，除以 ζ_5^2 得到

$$(u^2 - 2) + u + 1 = 0, \quad u^2 + u - 1 = 0.$$

取 $u = (-1 + \sqrt{5})/2$ ，再由 $\zeta_5^2 - u\zeta_5 + 1 = 0$ 得到

$$\zeta_5 = \frac{u + \sqrt{u^2 - 4}}{2},$$

其中选择正虚部的平方根，即得到 $e^{2\pi i/5}$ 。所以所需单位根确实是有理常数的根式。这个例子直接展示了某些具体五次式可解。

11.5 本篇证明了哪个方向

本篇完整使用并证明

根式可解 $\implies$ 分裂域的 **Galois** 群可解。

再结合一般五次的群不可解，得到它不根式可解。无需先证明逆方向“群可解 $\implies$ 根式可解”。逆方向是完整 Galois 根式判据的另一半，涉及从群列重新构造根式层，本篇没有把它当作已证明的结论使用。

11.6 推广到一般高次，只增加一个子群观察

对 $n \geq 5$ ，同样取 n 个独立形式根与其基本对称式，第 2 章的论证逐字推广，得到通用 n 次方程的群是 S_n 。

S_n 含有固定第 6 到第 n 个对象、只置换前五个对象的子群，同构于 S_5 。若 S_n 可解，该子群也应可解，矛盾。因此所有 S_n ($n \geq 5$) 都不可解，同样排除一般 n 次方程的根式通解。

11.7 我现在对整条路线的理解

我的理解 B04：所以原始的域扩张无法保证构建出伽罗瓦群，也无法保证可解，需要做单位根的补充和共轭根的补充，然后再借助限制映射，商群和各种同构保证 e/f 的 Galois 群也是可解的

这段理解已经把“公式的原始根式塔”和“方程自身的分裂域群”连接起来。为了以后复习时不把几个条件混在一起，下面保留这条主线，并把措辞和每一步的职责说准确。

原始塔缺少的是使用 Galois 理论的条件

原始根式塔记录每次开根操作，未必保证每层或总扩张 R/F 是 Galois 扩张。它的 F 自同构群 $\text{Aut}_F(R)$ 仍然存在；不能把“扩张不是 Galois”写成“没有自同构群”。

例如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 不正规，但其自同构群存在，而且是平凡群，当然可解。这个例子说明，“原始塔无法保证可解”在当前理解中应读作：此时还不能直接从原始塔套用 Galois 对应、限制满射和商群公式，得到原方程分裂域的群可解。不应据此认定原始塔的自同构群可能不可解，也不能把它直接当成目标群 $\text{Gal}(E/F)$ 。

补单位根与补共轭，解决不同的事情

补单位根，处理每个根式阶段的群结构。把所需单位根放入当前基础层，并逐点固定它们，自同构作用于一个根式生成元时只能乘上单位根。这使单根式层的群嵌入循环群；一个阶段同时加入多个根式时，群嵌入循环群的有限直积，因而阿贝尔。

补所需共轭，处理对原基础域的正规性。下层自同构可能改变被开方数，所以不只是给某一个根乘上单位根，还要把这些变化后的被开方数的全部根加入。第 6 章逐层证明所有固定 F 的嵌入都把新域送回自身，特征零再保证可分。

两项工作要同时兼顾：构造出的域对原 F 正规，同时仍有阿贝尔的相对层。“成为 Galois 扩张”与“它的群可解”是两个需要分别证明的结论。第 2 章的通用五次分裂域本来就是 Galois 扩张，其群却是不可解的 S_5 ，所以正规、可分本身并不保证可解。

得到大域后，还要证明它的群确实可解

构造得到

$$F \subseteq M_0 \subseteq \cdots \subseteq M_m = N, \quad R \subseteq N.$$

每个 M_i/F 都有限 Galois；加单位根的第一层群阿贝尔，各根式阶段的相对群也阿贝尔。第 7 章再用限制映射把这些域层翻译为一个大群的正规列，证明其相邻商群都阿贝尔，才得到 $\text{Gal}(N/F)$ 可解。

这一步不是把“几个阿贝尔群拼起来”作为口头理由，而是实际找出大群中的子群、正规关系与商群同构。

最后才把可解性传给方程自身的群

原分裂域由根式公式假设落在 R 中，所以

$$F \subseteq E \subseteq R \subseteq N.$$

E/F 已由方程的可分分裂域结构保证 Galois， N/F 已由正规化构造保证 Galois。限制到 E 的映射因此有正确的目标，并且满射，核是 $\text{Gal}(N/E)$ 。第一同构定理给出

$$\text{Gal}(E/F) \cong \frac{\text{Gal}(N/F)}{\text{Gal}(N/E)}.$$

目标群于是成为可解大群的商群。由“可解群的商群仍可解”，得到 $\text{Gal}(E/F)$ 可解。

这里 F 始终是原基础域。加入单位根得到的是 $M_0 = F(\mu_q)$ ，并没有把原来的 F 改名或替换；加单位根的那一层也必须纳入可解群列。

11.8 限制映射的两次用途：先证明大群，再传给小域

用在什么地方	映射、核与商群	在整条证明中的任务
加工后的塔内部， $M_{i-1} \subseteq M_i \subseteq N$	限制 $\text{Gal}(N/M_{i-1}) \rightarrow \text{Gal}(M_i/M_{i-1})$ ；核为 $\text{Gal}(N/M_i)$ ；故 $H_{i-1}/H_i \cong \text{Gal}(M_i/M_{i-1})$	识别正规列的相邻商，证明大群可解
大域与原分裂域之间， $F \subseteq E \subseteq N$	限制 $\text{Gal}(N/F) \rightarrow \text{Gal}(E/F)$ ；核为 $\text{Gal}(N/E)$ ；故目标是大群的商群	把已经证明的大群可解性传给原方程的群

表中的 $H_i = \text{Gal}(N/M_i)$ ；加单位根的阶段还给出 $\text{Gal}(N/F)/H_0 \cong \text{Gal}(M_0/F)$ ，这一阿贝尔商也计入正规列。

两次使用的模板相同，任务不同。每次都核对三个条件：被限制到的中间域稳定、限制映射满射、核为逐点固定该中间域的同构。在最后一次中， E/F 正规保证稳定；嵌入延拓与 N/F 正规保证满射；核由定义得到。具体证明已经在第 7.3 节展开。

我的整体理解，精确整理版

原始根式塔记录公式的开根步骤，但未必满足直接使用 Galois 理论的条件。补单位根并逐层补齐所需共轭，构造包含原塔的有限 Galois 大域；再通过限制映射与相邻商群，证明它的群可解。最后，原分裂域包含在这个大域中，限制映射使原分裂域的群成为大群的商群，因而也可解。整个过程始终固定原基础域 F 。

回看第 11.3 节：这条路线由“存在根式公式”的假设推出 $\text{Gal}(E/F)$ 可解；而方程自身的通用结构已独立给出该群同构于不可解的 S_5 。两条路线在同一个群上相遇，矛盾才最终成立。

第 12 章：复习地图、原问题索引与校正记录

12.1 每个箭头依靠哪一个理由

推进	所需理由	对应位置
形式根 $\rightarrow$ 一般系数	基本对称式代数独立；系数符号替换	第 2.3 节
$F \subseteq E \rightarrow$ 群为 S_5	每个变量置换确实定义自同构；自同构由根的像决定	第 2.4—2.5 节
根式公式 $\rightarrow$ 有限塔	按表达式依赖顺序处理开根；四则运算留在域中	第 3 章
各根有表达式 $\rightarrow$ 同一塔包含全部根	在同一代数闭包中合并有限多个表达式	第 3.7 节
根在塔顶 $\rightarrow E \subseteq R$	生成域是包含基础域和生成元的最小域	第 4 章
加单位根 $\rightarrow$ 单层群阿贝尔	固定单位根使根的像之比定义单射同态	第 5 章
原塔 $\rightarrow$ 对 F Galois 的大域	对所有共轭被开方数补全部根，归纳证明嵌入稳定	第 6 章
阿贝尔域层 $\rightarrow$ 大群可解	限制满射、核与商群，构造正规列	第 7 章
大群可解 $\rightarrow$ 原分裂域群可解	E/F 与 N/F Galois；限制满射；商群保持可解	第 8 章

推进	所需理由	对应位置
非阿贝尔单群 $A_5 \rightarrow S_5$ 不可解	排除 A_5 所有可解列；使用子群引理	第 10 章
两条路线 $\rightarrow$ 否定根式假设	同一个 $\text{Gal}(E/F)$ 不能同时可解与不可解	第 11 章

12.2 三个群论工具，各自在哪里用

工具	主线中的具体用途
可解群的子群仍可解	从 A_5 不可解推出 S_5 不可解；也用于跨层相对群
可解群的商群仍可解	从 $\text{Gal}(N/F)$ 传给 $\text{Gal}(E/F)$
可解的核与商给出可解的整群	解释相邻域层怎样拼成跨层可解群；也可替代第 7 章的整群论证

三个工具已在第 8 章证明。它们不是同一条结论的不同说法，分别处理取小群、压缩群和拼接群。

12.3 十一个复习问题

1. x_i 对 $\mathbb{Q}$ 超越，为什么仍能对 F 代数？——它们满足系数在 F 中的 $f(t)$ 。
2. 假设公式存在，为什么 $E \subseteq R$ ？——全部根在 R ，再使用生成域的最小性。
3. E 必须等于某个 R_i 吗？——不必；第 4 章给出真正的反例。
4. 为什么只补单位根还不够？——基础层的共轭会改变被开方数，必须把变化后的根也加入。
5. 为什么大域的群可解？——域塔反向变成正规列，相邻商都阿贝尔。

6. 为什么目标群是商群？——限制相同的延拓构成核的陪集；延拓引理保证限制满射。
7. 矛盾落在哪个群？——原来的 $\text{Gal}(E/F)$ ，不是 $\text{Gal}(R/F)$ ，也不是换了基础域以后的群。
8. 为什么每层写成幂等于前层元素，而原方程仍有很多项？——塔选择公式中的开根中间量，不必选择原方程根本人。
9. 把低次项移到右边，是否就算根式步骤？——不算，必须额外保证右端已经属于前层；其中含未知根时不能自动保证。
10. 开根指数一定等于最小多项式次数吗？——不一定，最小多项式只需整除开根方程，扩张次数可能更小。
11. 限制映射在哪两处使用？——先在正规化塔中识别相邻商，证明大群可解；再限制到原分裂域，把可解性传给目标群。

12.4 原对话覆盖索引

原回答编号	原问题的核心	本篇去向与补充
A01	最后用五个根与系数构造的域，看起来与此前不同	第 1、2、10、11 章；补代数独立、有限性、置换自同构与群论障碍
A02	根式可解与两个域的 Galois 群，怎样连接	第 3、5—8 章；补公共塔、单位根层、逐层正规化及完整商群证明
A03	如何保证根域与系数域是塔的一部分	第 4 章；完整证明包含关系，校正并替换原例子
A04	不相邻域层是否也能讨论可解性	第 9 章；给出准确条件、非传递例子及跨层证明

原回答编号	原问题的核心	本篇去向与补充
A05	子群、商群是否保持可解	第 8.3—8.5 节；补两个保持引理及拼接引理
A06	域塔与最后的矛盾怎样得到	第 1、11 章；把两条路线和四个域固定在同一记号体系中
A07	得到域塔以后还需做什么	第 1.3、5—8 章；完整落实补单位根、补共轭、大群与限制商群
B01	为什么每层是纯开根关系，可否满足一般多项式	第 3.2、3.4 节；区分操作定义、基础域和最小多项式
B02	初步理解后仍觉得缺少连接	第 3.3 节；完整演示二次公式的中间量与输出，证明不能仅移项认作开根步骤
B03	每次扩张是不是只处理开根操作	第 3.5 节；确认原始塔的构造方式，说明四则运算、重复层与正规化塔的范围
B04	原塔、补单位根和共轭，再经限制商群得到目标群可解的整体理解	第 11.7—11.8 节；保留我的原话，澄清自同构群与 Galois 扩张、正规与可解、两次限制及原基础域不变

重排后的正文保留分享对话中的七个数学问题、本聊天三轮新增追问及一段整体理解，回答内容按用途重新组织，删除重复结尾和后续建议。原回答完整保存在项目的资料目录中，便于核对；本篇不把重写内容当作对话原文引用。

12.5 本篇校正与补齐记录

第三版新增：完整总结放在第 11.7—11.8 节，位于总反证之后、复习地图之前；保留我的整体理解原文，并补上条件区分和限制映射的两次用途。第 1 章只增加一段简短导航。前两版原有证明保留。

第二版新增：第 3.2—3.5 节完整纳入本聊天的三轮理解过程，新增计算步骤表、移项不能保证右端在前层的说明、嵌套根式对不同基础域的方程，以及开根指数与最小多项式次数的区别。第一版原有正文均保留，第 3 章原小节顺延，相关引用同步更新。

- 原对话的 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ 例子实际上等于塔顶，替换为 $\mathbb{Q}(\sqrt{6})$ ，并给出完整次数与不相等证明。
- “独立根”明确为代数独立不定元，补上对系数域的有限代数性，以及基本对称式的代数独立性。
- “所有根在某根式塔”补上多表达式合并与表达式结构归纳。
- “补单位根后取正规闭包，群就可解”展开成逐层构造，每层对原 F 的正规性分别证明。
- 正规化阶段可能加入多个根式，群只保证是循环群直积的子群、因而阿贝尔，未必循环。
- 加单位根对原 F 的那一层也计入阿贝尔商列；对一般 F 只声称嵌入可逆剩余类群。
- 分裂域在特征零可分，从而 Galois；没有把“任意特征下的分裂域”一概说成 Galois。
- 非 Galois 扩张仍有自同构群，修正“不能讨论群”的笼统说法，明确不能自动套用的结论。
- 补上嵌入延拓、限制满射、核与第一同构定理，以及可解性的三个群论工具。
- S_5 的不可解性排除所有可解列，补上 A_5 共轭类与单群性证明。

12.6 与前两份笔记的衔接

这份笔记围绕最后证明的连接来读；需要重新熟悉基础定义时，可回到已有文件：

- [伽罗瓦理论主笔记 · 第四版](#)：群论基础见第 2—8 章；域与嵌入见第 9—13 章；根式塔和通用方程见第 14—16 章。
- [多项式与分圆域补充笔记 · 第一版](#)：最小多项式见第 1 章；单位根与阶见第 2—5 章；可分性见第 8 章；分圆域自同构见第 10—11 章。

本篇已把最后反证直接需要的构造与证明写在正文，以上链接用于补基础和进一步阅读。

[保留的第一版阅读文件。](#) · [保留的第二版阅读文件。](#)