从置换到五次方程：我的伽罗瓦理论笔记

> 第四版（2026-10-05）：保留第二版的完整证明与追问，统一数学排版；HTML 为主要阅读文件，Markdown 为配套源文件。
>
> 原始材料：《介绍抽象代数》分享对话。正文覆盖其中 92 段数学回答；4 段关于文档工具与使用方式的讨论另留在原材料中。$A01$—$A96$ 是原回答编号，用于核对覆盖情况，不表示本篇阅读顺序。

我的目标是一步步理解一般五次及以上方程为什么没有根式通解。后面问到的基础问题已移到第一次需要它的位置；“原问题”保留我的实际提问，“补充证明”是本版加入的推导。段落中保留的“你”或“我们”来自原解释，它们不被当作我已经独立完成的思考。

阅读顺序是：置换与群 → 陪集与商群 → 同态与可解群 → A_5 的障碍 → 域与嵌入 → Galois 群与限制映射 → 根式塔的正规化 → 一般方程的群 → 无根式通解。根的重命名、自同构允许的根置换以及一般形式根的任意置换，是不同阶段的概念，正文分别证明它们的联系。

目录

- 第 1 章：目标：从问题出发，而不是提前背结论
- 第 2 章：置换与群：循环、复合和换位
- 第 3 章：奇偶性、交错群与子群
- 第 4 章：陪集与 Lagrange 定理
- 第 5 章：正规子群和商群：让陪集乘法没有歧义
- 第 6 章：群同态、核、像和第一同构定理
- 第 7 章：可解群：定义、例子及保持可解的三个引理

- 第 8 章：A_5 的结构：完整证明五次的群论障碍
- 第 9 章：域、理想、代数元与扩张次数
- 第 10 章：域同态、嵌入、自同构和 Galois 群
- 第 11 章：分裂域、正规性与嵌入的延拓
- 第 12 章：完整例子：三次分裂域的群为什么是 S_3
- 第 13 章：中间域、限制映射和商群公式
- 第 14 章：根式塔：单位根、共轭与正规闭包
- 第 15 章：完整搭桥：根式可解 ⇒ Galois 群可解
- 第 16 章：一般方程的群与 Abel–Ruffini 定理

常用符号速查

有理数域记为 $\mathbb{Q}$，实数域记为 $\mathbb{R}$。这些双线体大写字母表示数域，不是普通的小写字母。正文中的数学对象与公式均采用统一的数学字体。

记号	类型与含义
$F \subseteq E \subseteq K$	域的包含关系；当前小节声明哪一个是基础域
$F[x]$；$F(\alpha)$	多项式环；加入 α 后生成的最小域
$[K : F]$	K 作为 F 向量空间的维数，不是除法
G；$H \leq G$；$N \triangleleft G$	群；子群；正规子群
e；id（恒等映射）	群的单位元；E 上恒等自同构
σ、τ、φ	映射；每次使用时要核对定义域和值域
$\mathrm{Gal}(K/F)$	由 $K \to K$、逐点固定 F 的域自同构组成的群
res；$\sigma\|_E$	限制映射；把 σ 的输入范围限制到 E

记号	类型与含义
$\ker \varphi$；$\operatorname{im} \varphi$	同态的核；实际达到的像；核的单位元取决于目标结构
S_n；A_n；C_n；V_4	对称群；交错群；循环群；Klein 四元群
ζ_n；μ_n	本原 n 次单位根；全体 n 次单位根组成的群
e_j	基本对称式，与群单位元 e 不同
$\overline{F}$ 或 Ω	代数闭包，给嵌入与多项式根提供共同容器
$\leq$；$\lhd$；$\cong$；$\hookrightarrow$	子群；正规子群；同构；单射嵌入

这张表用于查阅，不代替局部定义。a、α、σ 等字母在不同例子中重新声明；本节的对象约定写在章首。涉及正规、可分、单位根、满射的条件会在应用时再次指出。

第 1 章：目标：从问题出发，而不是提前背结论

本章对象：r_i 表示第 i 个根；此处先讨论根的重命名，不认定任意重命名都是域自同构。

1.1 从韦达关系发现根的置换

我们可以完全按照你前面学多元微积分的方式：**一次只推进一个核心概念，每一步都说明“为什么现在需要它”，直到最后真正看懂 Abel–Ruffini 定理背后的 Galois 理论。**

先把最终目标说准确一点：

> **不是“所有五次及以上方程都没有根式解”。**
>
> 正确说法是：**不存在一个像二次公式那样，仅用系数、四则运算和有限次开方，就能解所有一般五次方程的公式。**

> 某些五次方程当然有根式解，例如
>
> $$x^5 - 1 = 0.$$

我们最终要理解的逻辑链大致是：

方程的根 → 根之间的置换 → 群 → 子群/正规子群 → 域 → 域扩张 → Galois 群 → 可解群 → 根式扩张 → S_5 不可解 → 一般五次方程无根式通解。

但现在先不碰“域”“Galois 群”。

第一步：为什么解方程会突然和“置换”有关？

假设一个三次方程有三个根：

$$r_1, r_2, r_3.$$

例如

$$(x-1)(x-2)(x-3) = 0.$$

根就是

$$1, 2, 3.$$

你写方程时，并没有规定谁必须叫 r_1、谁必须叫 r_2。

所以：

$$(r_1, r_2, r_3)$$

和

$$(r_2, r_1, r_3)$$

其实描述的是**同一组根**。

也就是说，我们可以把三个根重新排列。

例如：

$$r_1 \to r_2, \qquad r_2 \to r_1, \qquad r_3 \to r_3.$$

这叫一个 **permutation（置换）**。

三个东西有多少种置换?

如果有三个根：

$$1, 2, 3$$

可能排列成：

$$123, \quad 132, \quad 213, \quad 231, \quad 312, \quad 321.$$

一共

$$3! = 6$$

种。

这些置换的全体叫

$$S_3,$$

读作：

> symmetric group on 3 letters
> **三个对象上的对称群（S_3 的阶是 6）**

这里的“对称”不是几何上的镜像对称，而是说：

> 对三个对象进行所有可能重新排列所形成的结构。

为什么这和方程有关系？

这才是最关键的地方。

考虑一个一般三次方程：

$$x^3 + ax^2 + bx + c = 0$$

三个根是

$$r_1, r_2, r_3.$$

根据韦达定理：

$$r_1 + r_2 + r_3 = -a,$$

$$r_1r_2 + r_1r_3 + r_2r_3 = b,$$

$$r_1r_2r_3 = -c.$$

注意一个非常重要的现象。

如果交换 r_1, r_2：

$$r_1 \leftrightarrow r_2,$$

那么

$$r_1 + r_2 + r_3$$

完全不变。

同样，

$$r_1 r_2 + r_1 r_3 + r_2 r_3$$

也不变。

以及

$$r_1 r_2 r_3$$

也不变。

所以：

> **方程的系数只能“看到”根的某些对称组合，却不能区分每一个根是谁。**

这其实就是整个 Galois 理论的种子。

例如：

$$(x - r_1)(x - r_2)(x - r_3)$$

展开为

$$x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3.$$

你把 r_1, r_2, r_3 随便交换，展开结果完全一样。

因此：

方程的系数天然具有“根的置换对称性”

Galois 最伟大的想法之一就是：

> **不要直接问“根长什么样”，而要问“在保持已有代数关系不变的情况下，这些根允许怎样互相置换？”**

最终，“哪些置换允许发生”就会形成一个**群**。

而这个群竟然能够告诉我们：

这个方程能不能用根式解

下一步我们就正式解释：

什么叫“群”？

而且我不会直接扔四条公理，而是先从“连续做两个置换”开始，让你看到为什么群的定义几乎是被迫出现的。

第 2 章：置换与群：循环、复合和换位

本章对象：S_n 是 n 个对象上的置换群；e 是恒等置换，$\sigma\tau$ 先作用 τ 再作用 σ。

2.1 置换的复合、单位元和逆：群的定义

我们现在正式进入抽象代数的第一个核心概念：**群（group）**。

但先不背定义。先看为什么“群”会自然出现。

第二步：为什么置换会形成“群”？

上一节我们有三个根：

$$r_1, r_2, r_3.$$

考虑两个操作。

第一个操作 σ：

$$r_1 \leftrightarrow r_2, \qquad r_3 \text{ 不动.}$$

也就是

$$\sigma : \begin{cases} r_1 \mapsto r_2 \\ r_2 \mapsto r_1 \\ r_3 \mapsto r_3 \end{cases}$$

再考虑另一个操作 τ：

$$r_2 \leftrightarrow r_3, \qquad r_1 \text{ 不动.}$$

即

$$\tau : \begin{cases} r_1 \mapsto r_1 \\ r_2 \mapsto r_3 \\ r_3 \mapsto r_2 \end{cases}$$

现在问题来了：

> 如果我先做 τ，再做 σ，结果是什么？

这就是“两个置换的复合”。

---

1. 先做 τ，再做 σ

我们逐个跟踪。

对 r_1

先做 τ：

$$r_1 \mapsto r_1.$$

再做 σ：

$$r_1 \mapsto r_2.$$

所以最终：

$$r_1 \mapsto r_2.$$

对 r_2

先做 τ：

$$r_2 \mapsto r_3.$$

再做 σ：

$$r_3 \mapsto r_3.$$

所以：

$$r_2 \mapsto r_3.$$

对 r_3

先做 τ：

$$r_3 \mapsto r_2.$$

再做 σ：

$$r_2 \mapsto r_1.$$

所以：

$$r_3 \mapsto r_1.$$

最终得到：

$$r_1 \mapsto r_2, \qquad r_2 \mapsto r_3, \qquad r_3 \mapsto r_1.$$

这是一个新的置换。

可以写成：

$$\sigma\tau.$$

注意传统约定：

$$\sigma\tau$$

通常表示：

> **先做 τ，再做 σ。**

和函数复合一样：

$$(\sigma \circ \tau)(x) = \sigma(\tau(x)).$$

第一个重要现象：做完还是置换

我们从两个置换出发：

$$\sigma, \tau.$$

把它们连续做，得到的东西仍然是一个置换。

不会突然得到“半个置换”或者某种不在系统里的对象。

这叫：

封闭性

英文：

> closure

也就是：

如果

$$a, b \in G,$$

那么

$$ab \in G.$$

第二个现象：有一个“什么都不做”的操作

考虑一个置换 e：

$$r_1 \mapsto r_1, \qquad r_2 \mapsto r_2, \qquad r_3 \mapsto r_3.$$

什么都没变。

这叫：

恒等置换

英文：

> identity permutation

记作：

$$e.$$

它满足：

$$e\sigma = \sigma e = \sigma.$$

就像普通数字里：

$$1 \times a = a \times 1 = a.$$

所以群里也需要一个“1”一样的东西。

这叫：

单位元

或

恒等元

英文：

> identity element

第三个现象：每个操作都能撤销

比如：

$$\sigma : r_1 \leftrightarrow r_2.$$

做一次以后 r_1, r_2 换了。

再做一次：

$$r_1 \leftrightarrow r_2$$

又换回来。

所以：

$$\sigma\sigma = e.$$

因此：

$$\sigma^{-1} = \sigma.$$

这里的

$$\sigma^{-1}$$

叫 σ 的逆。

它满足：

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = e.$$

这叫：

逆元

英文：

> inverse

不过不是所有置换都等于自己的逆。

例如：

$$\rho : r_1 \mapsto r_2, \quad r_2 \mapsto r_3, \quad r_3 \mapsto r_1.$$

这是一个三循环。

做一次：

$$1 \to 2 \to 3 \to 1.$$

它的逆就是反方向：

$$1 \to 3 \to 2 \to 1.$$

所以：

$$\rho^{-1} \neq \rho.$$

第四个现象：三个操作连续做时，括号怎么放不重要

假设有三个置换：

$$\sigma, \tau, \rho.$$

那么：

$$(\sigma\tau)\rho$$

和

$$\sigma(\tau\rho)$$

结果一样。

为什么？

因为它们本质上都是：

> 先做 ρ，再做 τ，最后做 σ。

区别只在于你“先把哪两个看成一组”。

数学上写成：

$$(\sigma\tau)\rho = \sigma(\tau\rho).$$

这叫：

结合律

英文：

> associativity

现在群的定义自然出现了

一个集合 G，如果里面的元素有一种运算，满足：

$$\boxed{\begin{array}{l}\textbf{1.}\ \text{封闭}\\ \textbf{2.}\ \text{结合律}\\ \textbf{3.}\ \text{有单位元}\\ \textbf{4.}\ \text{每个元素都有逆元}\end{array}}$$

那么 G 就叫一个：

$$\boxed{\text{群}}$$

英文：

$$\boxed{\textbf{group}}$$

所以并不是数学家凭空发明了四条奇怪公理。

恰恰相反：

> 这四条性质正是“可组合、可撤销的对称操作”天然具有的性质。

S_3 就是一个群

三个对象所有置换组成：

$$S_3.$$

共有：

$$3! = 6$$

个元素。

我们可以写成：

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

这些括号是什么意思，我们下一步会仔细讲。

例如：

$$(12)$$

表示：

$$1 \leftrightarrow 2,$$

而 3 不动。

$$(123)$$

表示：

$$1 \to 2, \qquad 2 \to 3, \qquad 3 \to 1.$$

这里先记住一个非常重要的思想：

> 群研究的不是“东西本身”，而是“允许怎样操作这些东西”

这就是为什么群会在 Galois 理论里出现。

对于一个方程，我们最终不主要研究：

$$r_1, r_2, \ldots, r_n$$

本身长什么样，而研究：

> 哪些根可以互换，而所有已知代数关系仍保持不变

这些允许的交换会形成一个群。

而这个群，就是后来所谓的 **Galois 群**。

不过现在还没资格定义它。

下一步我建议先讲一个非常具体而重要的东西：

> 置换的循环记号，以及怎样计算两个置换的乘积

因为如果连 S_3、S_4、S_5 里的元素都不会算，后面“S_5 为什么不可解”会完全失去直觉。

2.2 置换群这个具体模型

> 原问题：现在讨论的都是这种置换群对吧

对，**目前我们讲的群，全部都是从“置换”这个具体例子出发的**。

更准确地说：

$$S_n$$

本身就是一个**置换群**，因为它的元素都是对 n 个对象的置换。

而

$$A_n$$

也是置换群，因为它只是从 S_n 中挑出了所有偶置换。

但要注意：

> **“群”这个概念远远不只包括置换群。**

比如整数在加法下：

$$(\mathbb{Z}, +)$$

也是群。

因为有封闭性、结合律、单位元 0、每个整数 a 都有逆元 $-a$。

还有非零实数在乘法下：

$$(\mathbb{R}^\times, \cdot)$$

也是群。

所以现在的学习顺序其实是：

具体的置换 $\rightarrow$ 发现群的四条规律 $\rightarrow$ 抽象出“群”

我们暂时一直用置换群，是因为它和后面的方程根最直接相关，而且最容易看见“对称性”。

以后讲到 Galois 群时，仍然会回到置换：

$$\boxed{\text{Galois 群本质上就是根之间允许发生的某些置换}}$$

只是到那时，这些置换会受到“必须保持代数关系”的限制。

所以目前你可以先把：

群

理解成一个更抽象的大概念，而

置换群

是群里面特别重要的一类。

2.3 循环记号、乘法顺序与非交换性

第三步：置换的循环记号到底是什么意思？

我们还是从三个对象开始：

$$1, 2, 3.$$

假设有一个置换：

$$1 \mapsto 2, \qquad 2 \mapsto 3, \qquad 3 \mapsto 1.$$

我们把它写成：

$$(123).$$

这个记号的意思不是一个三位数，而是：

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 1.$$

因为最后 3 又回到 1，所以叫一个 cycle，**循环**。

1. 为什么 (123) 和 (231) 是同一个置换?

看:

$$(123) : 1 \to 2,\ 2 \to 3,\ 3 \to 1.$$

而

$$(231) : 2 \to 3,\ 3 \to 1,\ 1 \to 2.$$

完全一样。

所以:

$$(123) = (231) = (312).$$

只是从循环里的不同位置开始写。

但是:

$$(132)$$

就不同了。

它表示:

$$1 \to 3, \quad 3 \to 2, \quad 2 \to 1.$$

它恰好是 (123) 的反方向。

因此:

$$(123)^{-1} = (132).$$

---

2. 二循环：(12)

$$(12)$$

表示：

$$1 \to 2, \qquad 2 \to 1,$$

其他元素不动。

这种只交换两个元素的置换叫：

$$\boxed{\textbf{transposition}，\text{换位}}$$

所以：

$$(12),\ (13),\ (23)$$

都是换位。

而且换位有一个简单性质：

$$(12)^2 = e.$$

因为交换两次就回去了。

---

3. 为什么一个置换可以拆成几个循环?

考虑四个元素：

$$1, 2, 3, 4.$$

假设某个置换是：

$$1 \leftrightarrow 2,$$

同时：

$$3 \leftrightarrow 4.$$

我们就写成：

$$(12)(34).$$

这表示：

$$1 \to 2, \quad 2 \to 1,$$

以及：

$$3 \to 4, \quad 4 \to 3.$$

因为这两个循环涉及的元素完全不同，所以叫：

$$\boxed{\text{不相交循环}}$$

disjoint cycles。

---

4. 不相交循环为什么可以交换顺序？

比如：

$$(12)(34).$$

你可以先做 (34)，再做 (12)。

也可以先做 (12)，再做 (34)。

因为它们操作的是不同元素，所以：

$$(12)(34) = (34)(12).$$

这是一个很特殊的现象。

注意：

> 一般来说，置换乘法并不满足交换律。

也就是说通常：

$$\sigma\tau \neq \tau\sigma.$$

---

5. 来算一个真正的例子

考虑：

$$(12)(23).$$

按照约定：

$$(12)(23)$$

表示：

> 先做右边的 (23)，再做左边的 (12)。

逐个追踪。

对 1：

先做 (23)：

$$1 \to 1.$$

再做 (12)：

$$1 \to 2.$$

所以：

$$1 \to 2.$$

对 2：

先做 (23)：

$$2 \to 3.$$

再做 (12)：

$$3 \to 3.$$

所以：

$$2 \to 3.$$

对 3：

先做 (23)：

$$3 \to 2.$$

再做 (12)：

$$2 \to 1.$$

所以：

$$3 \to 1.$$

因此：

$$(12)(23) = (123).$$

---

6. 反过来算

现在算：

$$(23)(12).$$

还是先做右边的 (12)。

对 1：

$$1 \to 2 \to 3.$$

所以：

$$1 \to 3.$$

对 3：

$$3 \to 3 \to 2.$$

所以：

$$3 \to 2.$$

对 2：

$$2 \to 1 \to 1.$$

所以：

$$2 \to 1.$$

因此：

$$(23)(12) = (132).$$

于是：

$$(12)(23) \neq (23)(12).$$

具体就是：

$$(123) \neq (132).$$

这说明：

$$\boxed{S_3\text{不是交换群}}$$

---

7. 什么叫交换群?

如果一个群 G 中对所有 a, b 都有：

$$ab = ba,$$

那么这个群叫：

$$\boxed{\textbf{Abelian group}，\text{阿贝尔群}}$$

中文也叫：

$$\boxed{\text{交换群}}$$

例如整数加法：

$$3+5=5+3.$$

所以：

$$(\mathbb{Z},+)$$

是阿贝尔群。

但：

$$S_3$$

不是。

---

8. 为什么“非交换”以后会非常重要？

因为一般五次方程的障碍，最终就和某些群的复杂非交换结构有关。

但不是简单地说：

$$\text{非交换} \Rightarrow \text{不能根式解}.$$

这不对。

因为三次、四次方程的 Galois 群也可能非交换，但仍然有根式公式。

真正关键的是更精细的概念：

$$\boxed{\text{可解群 solvable group}}$$

后面我们会看到：

- S_2 可解；
- S_3 可解；
- S_4 可解；
- S_5 不可解。

而“一般 n 次方程能否根式求解”最终就跟这个有关。

---

9. 还差一个重要事实：所有置换都可以拆成换位

例如：

$$(123)$$

可以写成：

$$(123) = (12)(23).$$

一个更长的循环：

$$(1234)$$

可以写成：

$$(14)(13)(12),$$

或者用另一套等价分解。

一般地：

$$(a_1 a_2 \cdots a_k)$$

总能拆成若干个换位。

这意味着：

所有置换都可以由“交换两个元素”构造出来

这个事实之后会引出一个非常重要的概念：

奇置换和偶置换

然后会自然得到：

$$A_n$$

也就是**交错群 alternating group**。

而最终五次方程理论中最核心的怪物之一就是：

$$A_5.$$

因为：

A_5是最小的非交换单群

这正是 S_5 不可解的核心原因之一。

所以，下一步我们就讲：

为什么“换位个数的奇偶性”居然是一个不变量

这一步非常关键，因为它会第一次把我们带到 A_5。

2.4 为什么任意置换都可写成不相交循环

> 原问题：置换群为什么都可以写成括号形式貌似没解释

对，这一块前面确实跳过去了。更准确地说，不是“置换群本身写成括号”，而是：

置换群里的每一个置换，都可以写成若干个循环的乘积

这些循环就是我们一直写的：

$$(123),\quad (12)(34)$$

这种括号形式。

关键问题就是：**为什么任意置换都一定能这么写？**

先看一个具体置换。假设对集合

$$\{1,2,3,4,5,6\}$$

有置换 σ：

$$1\mapsto 3,\quad 3\mapsto 5,\quad 5\mapsto 1,$$

同时

$$2\mapsto 4,\quad 4\mapsto 2,$$

以及

$$6 \mapsto 6.$$

我们从 1 开始追踪：

$$1 \to 3 \to 5 \to 1.$$

它回到了起点，所以这一部分可以写成：

$$(135).$$

再找一个还没出现过的元素，比如 2：

$$2 \to 4 \to 2.$$

所以：

$$(24).$$

最后：

$$6 \to 6.$$

理论上可以写成：

$$(6),$$

但长度为 1 的循环通常省略。

因此整个置换写成：

$$\boxed{\sigma = (135)(24)}.$$

这里其实已经透露了证明的方法。

为什么一定会“绕回来”？

设我们有有限集合：

$$\{1, 2, \dots, n\}$$

和一个置换 σ。

所谓置换，本质上是这个集合到自身的**双射**：

$$\sigma : \{1, \dots, n\} \to \{1, \dots, n\}.$$

现在任选一个元素，比如 a，不断作用 σ：

$$a, \quad \sigma(a), \quad \sigma^2(a), \quad \sigma^3(a), \dots$$

因为一共只有有限个元素，所以这个序列不可能永远出现全新的元素。

迟早会有重复。

假设第一次发生重复时：

$$\sigma^r(a) = \sigma^s(a), \qquad r < s.$$

由于 σ 是双射，所以有逆：

$$\sigma^{-r}.$$

两边同时作用 σ^{-r}，得到：

$$a = \sigma^{s-r}(a).$$

所以从 a 一直追踪，最终一定回到 a。

于是得到一个循环：

$$a \to \sigma(a) \to \sigma^2(a) \to \cdots \to a.$$

因此可以写成：

$$\boxed{(a, \sigma(a), \sigma^2(a), \ldots)}.$$

这就是循环为什么必然出现。

还有一个问题：

> 会不会从另一个元素出发，追踪一会儿，然后“撞进”刚才那个循环？

例如已经有：

$$1 \to 3 \to 5 \to 1.$$

有没有可能另一个元素 2 满足：

$$2 \to 3?$$

不可能。

因为如果：

$$1 \to 3$$

同时：

$$2 \to 3,$$

那就有两个不同元素都映到 3。

这违反了置换是**一一对应（injective）**。

所以：

$$\boxed{\text{不同的循环要么完全相同，要么完全不相交}}$$

因此，我们可以这样构造任意置换的循环分解：

先随便取一个元素，比如 1，不断作用 σ，直到回到 1，得到第一个循环。

然后找一个没出现在第一个循环里的元素，再重复，得到第二个循环。

继续下去。

因为元素只有有限多个，这个过程最终结束。

于是任意置换都可以写成：

$$\boxed{\sigma = C_1 C_2 \cdots C_k}$$

其中每个 C_i 都是一个循环，而且这些循环彼此不相交。

举一个完整例子。

假设：

$$\sigma : \begin{cases} 1 \mapsto 4 \\ 4 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 6 \\ 6 \mapsto 3 \\ 5 \mapsto 5 \end{cases}$$

从 1 开始：

$$1 \to 4 \to 2 \to 1,$$

所以得到：

$$(142).$$

再取还没用过的 3：

$$3 \to 6 \to 3,$$

得到：

$$(36).$$

5 不动：

$$5 \to 5.$$

所以整个置换：

$$\boxed{\sigma = (142)(36)}$$

固定点 5 被省略了。

如果你愿意完整写，也可以写：

$$(142)(36)(5),$$

只是数学上通常不这么写。

这里还有一个很重要的结论：

任意置换的“不相交循环分解”在循环顺序意义下是唯一的

例如：

$$(142)(36)$$

和

$$(36)(142)$$

是同一个置换，因为两个循环不相交。

而：

$$(142) = (421) = (214)$$

也是同一个循环，因为只是换了起点。

除了这些写法上的变化，循环结构本身是确定的。

所以我们才可以很自然地讨论一个置换“有一个 3-循环、一个 2-循环”等结构。

最后再补一句，避免一个常见混淆：

$$(123)(45)$$

不是说“先把整个群拆成括号”。

而是说某一个具体置换 σ 的作用可以描述为：

$$1 \to 2 \to 3 \to 1$$

以及

$$4 \leftrightarrow 5.$$

所以：

括号记号描述的是单个置换的循环结构

而一个置换群，则是很多这样的置换组成的集合。

比如：

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

下一步如果继续，我建议顺着这里再证明一个前面用过但还没有真正证明的结论：

为什么每一个循环都能拆成换位

从而得到：

任意置换都能拆成换位

这样之前“奇置换/偶置换”的基础就彻底补齐了。

2.5 把循环拆成换位：原问题所需的连接

下一步我建议先把前面一个基础缺口彻底补上：

为什么任意一个循环都能拆成若干个换位

也就是证明

$$(a_1 a_2 \cdots a_k)$$

一定可以写成 $k-1$ 个二循环（换位）的乘积。

例如：

$$(1234)$$

为什么可以写成

$$(14)(13)(12).$$

这一步补完以后，我们就能严密串起：

任意置换 → 不相交循环分解 → 每个循环拆成换位 → 任意置换拆成换位 → 奇偶置换 → A_n.

这样之前关于 A_n 的基础就完整了，然后再回到：

正规子群 → 商群 → 可解群.

所以**下一步就只证明“一个循环为什么可以拆成换位”**，不再往后跳。

补充证明：循环分解与换位分解

本节的元素是有限集合 $1,\dots,n$ 上的双射；乘积 $\sigma\tau$ 表示先做 τ，再做 σ。

任选尚未处理的元素 a_1，反复作用 σ。由于集合有限，一定会重复。第一次重复必然回到 a_1：若先重复在 a_j，且 j>1，σ 的单射性会让它前面的两个元素也相同，与“第一次重复”矛盾。因此得到一个循环。再从这个循环外选元素重复操作；这些循环彼此不相交，且最终覆盖所有元素。这证明任意置换都能分解为不相交循环。若两个循环不相交，则对任意元素，至多一个循环改变它，故两循环复合的先后顺序无关。

对 $k \geq 2$，换位分解为

$$(a_1a_2\cdots a_k) = (a_1a_k)(a_1a_{k-1})\cdots(a_1a_2).$$

逐个检查：a_1 先被最右换位送到 a_2，其余换位不动 a_2；对 $2 \le j<k$，先做的换位不动 a_j，随后 $(a_1 a_j)$ 把它送到 a_1，紧接着 $(a_1 a_{j+1})$ 把它送到 a_{j+1}，余下换位不动它；a_k 最后被 $(a_1 a_k)$ 送到 a_1。循环外的元素都不动。这与左端对每个元素的作用完全一致，故等式成立。结合不相交循环分解，任意置换都能拆成换位。原对话提出了这个证明任务，但没有把上述逐元素验证写完，这里补齐。

第 3 章：奇偶性、交错群与子群

本章对象：inv 表示一行排列的逆序数；$\mathbf{sgn}$ 是取值为 ±1 的符号映射；A_n 是偶置换组成的交错群。

3.1 换位个数的奇偶性为何定义良好

现在进入一个非常关键的概念：**置换的奇偶性**。它会自然产生 A_n，而 A_5 正是最后“五次方程为什么出问题”的核心对象。

第四步：为什么置换有“奇”和“偶”？

上一节我们知道：

> 任意置换都可以拆成若干个换位。

比如

$$(123) = (12)(23)$$

用了两个换位。

于是很自然会问：

> 一个置换能不能既拆成 2 个换位，又拆成 3 个换位?

如果可以，那么“用了奇数个还是偶数个换位”就没有意义。

神奇的地方就在这里：

$$\boxed{\text{不可能}}$$

同一个置换可能有很多不同的换位分解，但所有分解中换位个数的**奇偶性一定相同**。

所以我们可以定义：

- 能拆成偶数个换位 $\rightarrow$ **偶置换**
- 能拆成奇数个换位 $\rightarrow$ **奇置换**

---

1. 先看例子

$$(12)$$

它本身就是一个换位：

$$(12).$$

用了 1 个。

所以它是：

$$\boxed{\text{奇置换}}$$

---

(123)

我们刚才有：

$$(123) = (12)(23).$$

用了 2 个换位。

所以：

$$\boxed{(123) \text{ 是偶置换}}$$

(1234)

例如：

$$(1234) = (14)(13)(12).$$

用了 3 个换位。

所以：

$$\boxed{(1234) \text{ 是奇置换}}$$

---

2. 一个 k–循环是什么奇偶性?

一般来说：

$$(a_1 a_2 \cdots a_k)$$

可以拆成：

$$(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2).$$

总共用了：

$$k-1$$

个换位。

所以：

$$\boxed{k\text{-循环的奇偶性由 } k-1 \text{ 决定}}$$

例如：

$$2\text{-循环：}1\text{ 个换位} \Rightarrow \text{奇}$$

$$3\text{-循环：}2\text{ 个换位} \Rightarrow \text{偶}$$

$$4\text{-循环：}3\text{ 个换位} \Rightarrow \text{奇}$$

---

3. 可是为什么奇偶性不会因为换一种拆法而改变？

这才是真正需要解释的地方。

我们先引入一个非常直观的量：

$$\boxed{\text{逆序数}}$$

英文叫：

> inversion number

假设有排列：

$$2, 3, 1.$$

我们问：

> 有多少对数字的大小顺序被“颠倒”了？

正常顺序应该是：

$$1 < 2 < 3.$$

现在排列为：

$$2, 3, 1.$$

看每一对。

$$(2, 3)$$

顺序正常，因为：

$$2 < 3.$$

不算逆序。

但：

$$(2,1)$$

反了，因为：

$$2>1.$$

算一个。

还有：

$$(3,1)$$

也反了。

所以总共有：

$$2$$

个逆序。

于是：

$$\mathrm{inv}(231)=2.$$

这是偶数。

而 231 对应的正是置换：

$$(123).$$

所以它是偶置换。

---

4. 再看一个

排列：

$$2,1,3.$$

只有：

$$(2,1)$$

发生逆序。

所以：

$$\mathrm{inv}=1.$$

是奇数。

对应：

$$(12),$$

正好是奇置换。

---

5. 为什么交换两个元素一定改变奇偶性?

先看最简单的：交换两个**相邻**元素。

比如：

$$1,2,3$$

交换 $2,3$：

$$1, 3, 2.$$

逆序数从：

$$0$$

变成：

$$1.$$

奇偶性翻转。

再交换一次：

$$1, 2, 3$$

又从奇变偶。

所以：

相邻交换每做一次，逆序数奇偶性翻转一次

那如果交换两个不相邻元素呢?

例如：

$$1, 2, 3, 4$$

交换 1 和 4：

$$4, 2, 3, 1.$$

这种交换其实可以拆成奇数个相邻交换。

比如把 1 一步步移到右边：

$$1234$$

$$2134$$

$$2314$$

$$2341$$

然后把 4 往左移：

$$2431$$

$$4231$$

总共：

$$5$$

次。

也就是奇数次。

一般交换位置 i, j，需要：

$$2(j-i)-1$$

次相邻交换。

它永远是奇数。

因此：

任意一个换位都会让逆序数奇偶性翻转

---

6. 现在证明关键结论

从恒等排列：

$$1, 2, \ldots, n$$

开始。

它的逆序数是：

$$0,$$

所以是偶数。

如果一个置换由 m 个换位得到，那么每做一次换位，逆序数的奇偶性就翻转一次。

因此：

- m 为偶数 $\rightarrow$ 最终逆序数为偶数；
- m 为奇数 $\rightarrow$ 最终逆序数为奇数。

但一个确定的排列，它的逆序数是确定的。

所以不可能同一个排列同时由：

偶数个换位

和

奇数个换位

得到。

于是：

$$\boxed{\text{置换的奇偶性是定义良好的}}$$

这就是我们需要的结论。

---

7. 偶置换自己形成一个群

现在考虑 S_n 中的所有偶置换。

把它们收集起来：

$$A_n.$$

这个群叫：

$$\boxed{\textbf{alternating group}}$$

中文：

$$\boxed{\text{交错群}}$$

所以：

$$A_n \subset S_n.$$

为什么它是一个群？

因为：

- 偶 × 偶 = 偶；
- 单位元是偶置换；
- 偶置换的逆仍然是偶置换。

所以：

$$A_n$$

本身就是一个群。

---

8. A_3 是什么？

S_3 有 6 个元素：

$$e,\ (12),\ (13),\ (23),\ (123),\ (132).$$

其中：

$$e$$

是偶置换。

三个换位：

$$(12), (13), (23)$$

都是奇置换。

两个三循环：

$$(123), (132)$$

都是偶置换。

所以：

$$A_3 = \{e, (123), (132)\}.$$

一共三个元素。

正好是 S_3 的一半。

实际上：

$$|A_n| = \frac{n!}{2} \qquad (n \geq 2).$$

因此：

$$|A_5| = \frac{5!}{2} = 60.$$

而这 60 个偶置换组成的：

$$\boxed{A_5}$$

以后会成为整个故事的关键。

原因是：

$$\boxed{A_5 \text{ 是非交换的}}$$

而且比“不交换”更严重：

$$\boxed{A_5 \text{ 没有合适的非平凡正规子群}}$$

换句话说，它是一个：

$$\boxed{\text{非交换单群}}$$

而这正是一般五次方程无法通过一层层根式“拆开”的根本障碍。

不过现在“正规子群”和“单群”都还没学。

所以下一步我们应该先讲：

什么是子群?

然后再讲：

陪集 → 正规子群 → 商群

这条线很重要，因为“可解群”的定义就是建立在一层层正规子群和商群之上的。

3.2 把循环写成一行排列，再计算逆序数

> 原问题：逆序数在括号的形式不好数吧

对，**逆序数不是直接对循环括号记号来数的**。它最自然是对“一行排列”来数。

比如置换

$$(123)$$

循环记号表示

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 1.$$

如果要数逆序数，先把它写成一行形式：

$$[\sigma(1), \sigma(2), \sigma(3)] = [2, 3, 1].$$

然后看

$$2, 3, 1$$

里面有多少逆序对。

有：

$$(2,1),\quad (3,1),$$

所以逆序数是

$$2.$$

因此 (123) 是偶置换。

再比如

$$(12).$$

它对应

$$1\to 2,\quad 2\to 1,\quad 3\to 3,$$

所以一行形式是

$$[2,1,3].$$

只有一个逆序：

$$(2,1),$$

所以逆序数是 1，是奇置换。

因此你可以区分三种常见表示法：

$$\boxed{\text{循环记号 } (123)}$$

适合看“元素怎么绕圈走”；

$$\boxed{\text{一行记号 } [2,3,1]}$$

适合数逆序数；

还有一种两行记号：

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

它直接表示

$$1 \mapsto 2, \quad 2 \mapsto 3, \quad 3 \mapsto 1.$$

所以前面说“用逆序数证明奇偶性良定义”时，其实默认是把置换先转换成一行排列，再数逆序数。

而实际判断一个循环的奇偶性时，通常根本不会去数逆序数，而是直接用：

$$(a_1 a_2 \cdots a_k)$$

可以拆成 $k-1$ 个换位，因此

$$\boxed{k\text{-循环的符号是 } (-1)^{k-1}}.$$

所以例如：

$$(12345)$$

是一个 5–循环，

$$5 - 1 = 4$$

是偶数，因此它是偶置换。

你这个问题非常重要，因为它说明了**循环记号和逆序数其实是两套不同用途的表示工具**。

补充证明：逆序数、符号同态与交错群的大小

一行记号 $[\sigma(1),\dots,\sigma(n)]$ 的逆序数，是满足 $i<j$ 且 $\sigma(i)>\sigma(j)$ 的数对 (i,j) 的数量。交换两个相邻位置时，只有这两个数彼此的大小次序改变；其他数字与它们产生的逆序总数不变，所以逆序数恰好改变 1。交换相距 $j-i$ 的两个位置可以用 $2(j-i)-1$ 次相邻交换完成：先把左边的数向右移，再把原来右边的数向左移。这是奇数，故任何换位都改变逆序数的奇偶性。

从恒等排列开始做 m 次换位，最终逆序数模 2 就是 m 模 2。因此同一置换不可能有奇偶性不同的换位分解。若 σ、τ 分别拆成 p、q 个换位，把两串分解接起来就是 $\sigma\tau$ 的分解，所以

$$\operatorname{sgn}(\sigma\tau)=(-1)^{p+q}=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

这说明 sgn 是到乘法群 {1,−1} 的群同态。对 $n\geq 2$，固定一个换位 t，映射 $\sigma\mapsto t\sigma$ 给出偶置换与奇置换之间的双射，逆映射也是乘以 t。因此两者数量相同，$|A_n|=n!/2$。$n=1$ 时不适用这个一半公式，$A_1=S_1$ 都只有一个元素。

3.4 逐条检查偶置换确实构成群

> 原问题：太快了，为什么偶置换自己就成为一个群了

对，这里确实跳得太快了。我们先只回答一个问题：

> 为什么所有偶置换放在一起，仍然满足“群”的四条要求？

我们一点一点检查。

假设我们把 S_n 中所有偶置换拿出来，组成集合

$$A_n.$$

要证明它是一个群，就必须检查群的四条性质。

先看第一条：封闭性

我们需要证明：

如果

$$\sigma, \tau \in A_n,$$

那么

$$\sigma\tau \in A_n.$$

因为 σ 是偶置换，所以它可以写成偶数个换位：

$$\sigma = t_1 t_2 \cdots t_{2k}.$$

同理，

$$\tau = s_1 s_2 \cdots s_{2m}.$$

那么：

$$\sigma\tau = t_1 t_2 \cdots t_{2k} s_1 s_2 \cdots s_{2m}.$$

总共用了：

$$2k + 2m = 2(k + m)$$

个换位。

仍然是偶数。

所以：

$$\boxed{\text{偶} \times \text{偶} = \text{偶}}$$

于是：

$$\sigma\tau \in A_n.$$

所以封闭性成立。

第二条：结合律

这一条甚至不用重新证明。

因为 A_n 里的运算，和 S_n 里的运算完全一样，都是“置换复合”。

而我们已经知道所有置换的复合满足：

$$(\sigma\tau)\rho = \sigma(\tau\rho).$$

既然这在整个 S_n 里成立，那么当然在 A_n 这个更小的集合里也成立。

所以结合律自动继承下来。

第三条：单位元在不在里面?

群必须有一个单位元：

$$e.$$

它什么都不做。

现在要问：

$$e$$

是不是偶置换？

是。

因为我们可以认为它由：

$$0$$

个换位组成。

而

$$0$$

是偶数。

所以：

$$e \in A_n.$$

因此单位元也有。

第四条：逆元还在不在 A_n 里面？

这是最值得仔细看的。

假设：

$$\sigma = t_1 t_2 \cdots t_{2k}.$$

也就是 σ 由偶数个换位组成。

那么逆置换：

$$\sigma^{-1}$$

是什么？

利用：

$$(ab)^{-1} = b^{-1}a^{-1},$$

得到：

$$\sigma^{-1} = t_{2k}^{-1} \cdots t_2^{-1} t_1^{-1}.$$

但每个换位都等于自己的逆。

例如：

$$(12)^{-1} = (12).$$

所以：

$$\sigma^{-1} = t_{2k} \cdots t_2 t_1.$$

你会发现：

仍然有：

$$2k$$

个换位。

所以：

$$\sigma^{-1}$$

仍然是偶置换。

因此：

$$\boxed{\text{偶置换的逆仍然是偶置换}}$$

所以逆元条件也满足。

于是四条全部成立：

1. 偶置换复合后仍是偶置换
2. 结合律成立
3. e 是偶置换
4. 偶置换的逆仍是偶置换

因此：

$$\boxed{A_n \text{ 是一个群}}$$

更准确地说：

$$\boxed{A_n \text{ 是 } S_n \text{ 的一个子群}}$$

你可以先把这里理解成一个非常朴素的原则：

> 从一个大群里挑出一部分元素，如果这部分元素在“做运算、找单位元、找逆元”时都不会跑出去，那么它自己也组成一个小群。

这就是“子群”的直觉。

下一步最好就只讲这个：

$$\boxed{\text{什么叫子群，以及为什么有时只检查两三件事就够了}}$$

先不碰陪集、正规子群。

3.5 交错群作为对称群的子群

我们就沿着“偶置换群 A_n”继续，而且慢一点。

下一步先把一个概念讲清楚：

$$\boxed{A_n \text{ 为什么叫 } S_n \text{ 的子群}}$$

1. 什么是子群?

假设有一个群 G。

如果我们从里面挑出一部分元素，形成一个集合 H，并且 H 自己在同样的运算下也构成一个群，那么就说：

$$\boxed{H \leq G}$$

意思是：

$$H \text{ 是 } G \text{ 的子群}$$

英文叫：

> subgroup

例如：

$$A_n \subset S_n.$$

因为 A_n 里的元素本来就是 S_n 的置换，只不过我们只挑出了偶置换。

而且刚才已经证明了：

- 偶置换乘偶置换还是偶置换；
- 单位元是偶置换；
- 偶置换的逆还是偶置换。

所以：

$$\boxed{A_n \leq S_n}$$

---

2. 用 S_3 看最清楚

我们知道：

$$S_3 = \{e, (12), (13), (23), (123), (132)\}.$$

其中偶置换是：

$$e, \quad (123), \quad (132).$$

所以：

$$A_3 = \{e, (123), (132)\}.$$

现在你可以把它理解成：

$$S_3$$

是一个有 6 个元素的大群，

而

$$A_3$$

是它里面一个有 3 个元素的小群。

---

3. 为什么 A_3 自己真的“关起门来”就能运算？

我们随便算。

例如：

$$(123)(123).$$

做两次 (123)。

第一次：

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 1.$$

再做一次：

$$1 \to 3, \quad 2 \to 1, \quad 3 \to 2.$$

所以：

$$(123)^2 = (132).$$

而：

$$(132) \in A_3.$$

再算：

$$(123)(132) = e.$$

也还在 A_3。

再算：

$$(132)^2 = (123).$$

仍然在 A_3。

所以你会发现：

$$\{e, (123), (132)\}$$

无论怎么复合，都不会跑到：

$$(12), (13), (23)$$

这些奇置换里面去。

这就是“封闭”的直观意义。

---

4. 为什么 A_n 恰好有 S_n 一半那么多元素？

这个结论很重要：

$$|A_n| = \frac{n!}{2}.$$

我们先别急着证明一般情况，先看 S_3。

S_3 一共有：

$$6$$

个置换。

其中：

$$3$$

个偶置换，

$$3$$

个奇置换。

刚好一半一半。

再看一个非常巧妙的对应。

假设 σ 是偶置换。

我们固定拿一个奇置换，比如：

$$(12).$$

然后做：

$$(12)\sigma.$$

因为：

$$\text{奇} \times \text{偶} = \text{奇},$$

所以结果一定是奇置换。

反过来，如果 τ 是奇置换，那么：

$$(12)\tau$$

就是：

$$\text{奇} \times \text{奇} = \text{偶}.$$

所以固定乘一个换位 (12)，会在：

$$\text{偶置换}$$

和

$$\text{奇置换}$$

之间建立一一对应。

因此两边数量必然相同。

而：

$$|S_n| = n!.$$

所以：

$$\boxed{|A_n| = \frac{n!}{2}}.$$

例如：

$$|A_3| = 3,$$

$$|A_4| = 12,$$

$$|A_5| = 60.$$

---

5. 现在先记住一个结构

我们目前有：

$$A_n \leq S_n.$$

可以想象成：

$$\boxed{\text{所有置换 } S_n}$$

里面分成两半：

$$\boxed{\text{偶置换 } A_n}$$

和

$$\boxed{\text{奇置换}}$$

但这里有个很重要的不对称：

> 偶置换自己构成一个群，而奇置换自己不构成群。

为什么？

因为两个奇置换相乘：

$$\text{奇} \times \text{奇} = \text{偶}.$$

所以奇置换集合不封闭。

比如：

$$(12)(23) = (123).$$

左边两个都是奇置换，

右边：

$$(123)$$

却是偶置换。

所以奇置换不能自己组成群。

到这里先停一下。

下一步最自然的是继续讲：

$$\boxed{\text{为什么 } A_n \text{ 不只是子群，而是一个“正规子群”}}$$

但“正规子群”不能直接定义，否则又会跳太快。

所以更合理的下一步是先引入：

$$\boxed{\text{左陪集和右陪集}}$$

因为“正规子群”本质上就是：

$$\text{左陪集} = \text{右陪集}.$$

而且从 $A_n \subset S_n$ 这个例子出发，陪集会非常直观。

第 4 章：陪集与 Lagrange 定理

本章对象：G 是群，$H \leq G$；gH 是左陪集，Hg 是右陪集；$|G|$ 表示群的元素个数，称为阶。

4.1 左陪集与分组的含义

现在我们只讲一个新概念：**陪集（coset）**。先不急着讲正规子群。

第五步：什么是陪集?

我们继续用最熟悉的例子：

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

以及它的子群

$$A_3 = \{e, (123), (132)\}.$$

现在假设我拿出 S_3 中一个元素，例如

$$(12).$$

然后让它分别乘 A_3 里的每一个元素：

$$(12)e,$$

$$(12)(123),$$

$$(12)(132).$$

把得到的所有结果收集起来。

这个集合就叫：

$$(12)A_3.$$

它是 A_3 的一个**左陪集**。

---

1. 一般定义是什么？

如果：

$$H \leq G$$

是一个子群，取任意

$$g \in G,$$

那么：

$$gH$$

定义为：

$$gH = \{gh \mid h \in H\}.$$

意思就是：

> 固定 g，然后把 H 里面每个元素都放到 g 的右边去乘。

这叫：

$$\boxed{\text{左陪集}}$$

注意虽然叫“左陪集”，其实是因为固定的 g 放在左边：

$$gH.$$

---

2. 具体算 $(12)A_3$

我们有：

$$A_3 = \{e, (123), (132)\}.$$

所以：

$$(12)A_3 = \{(12)e,\ (12)(123),\ (12)(132)\}.$$

第一个很简单：

$$(12)e = (12).$$

现在算第二个：

$$(12)(123).$$

按照我们的约定，先做右边的 (123)，再做左边的 (12)。

逐个跟踪：

$$1 \to 2 \to 1,$$

所以：

$$1 \to 1.$$

再看 2：

$$2 \to 3 \to 3,$$

所以：

$$2 \to 3.$$

再看 3：

$$3 \to 1 \to 2.$$

所以：

$$3 \to 2.$$

因此：

$$(12)(123) = (23).$$

再算：

$$(12)(132).$$

对 1：

$$1 \to 3 \to 3.$$

所以：

$$1 \to 3.$$

对 3：

$$3 \to 2 \to 1.$$

所以：

$$3 \to 1.$$

对 2：

$$2 \to 1 \to 2.$$

所以：

$$2 \to 2.$$

因此：

$$(12)(132) = (13).$$

所以：

$$\boxed{(12)A_3 = \{(12), (23), (13)\}}$$

你会发现：

$$(12)A_3$$

正好就是三个奇置换。

---

3. 这件事为什么很有意思？

因为原来的：

$$A_3 = \{e, (123), (132)\}$$

是三个偶置换。

而：

$$(12)A_3 = \{(12), (23), (13)\}$$

是三个奇置换。

所以整个 S_3 被分成了两块：

$$S_3 = A_3 \cup (12)A_3.$$

而且这两块没有重叠。

也就是说：

$$\boxed{S_3 = \text{偶置换那一块} + \text{奇置换那一块}}$$

这正是陪集开始发挥作用的地方。

---

4. 为什么陪集大小和原子群一样？

你可能已经看到了：

$$|A_3| = 3$$

而：

$$|(12)A_3| = 3.$$

这不是巧合。

一般来说：

$$|gH| = |H|.$$

为什么？

因为：

$$h \mapsto gh$$

不会把两个不同的 h 变成同一个结果。

假设：

$$gh_1 = gh_2.$$

左边同时乘：

$$g^{-1}.$$

得到：

$$h_1 = h_2.$$

所以不同的 h 一定得到不同的 gh。

因此：

$$H$$

里有多少元素，

$$gH$$

就有多少元素。

---

5. 还有一个很容易忽略的点

如果我们取：

$$g = e,$$

那么：

$$eH = H.$$

所以：

$$H$$

自己其实也是自己的一个陪集。

比如：

$$eA_3 = A_3.$$

甚至如果 $g \in H$，例如：

$$g = (123),$$

那么：

$$(123)A_3 = A_3.$$

原因是：

> 子群里的一个元素去乘整个子群，只是在子群内部重新排列元素，不会产生新的元素。

所以对于 A_3 来说，左陪集实际上只有两种：

$$A_3$$

和

$$(12)A_3.$$

也就是：

偶置换

和

奇置换.

这里先停在这个程度。

下一步我们再讲一个几乎一模一样、但非常关键的新东西：

$$\boxed{Hg}$$

也就是**右陪集**。

然后你会看到一个非常重要的问题：

> 为什么有时候 $gH = Hg$，有时候却不相等？

“正规子群”就是从这个问题里自然长出来的。

4.2 不同陪集为什么相同或不相交

因为只要两个左陪集有哪怕一个共同元素，就能证明它们其实整个集合完全一样。

设两个左陪集是

$$gH, \qquad kH.$$

假设它们不是完全不相交，也就是说存在某个元素 x，同时属于二者：

$$x \in gH \cap kH.$$

那么根据陪集定义，一定存在

$$h_1, h_2 \in H$$

使得

$$x = gh_1 = kh_2.$$

于是：

$$gh_1 = kh_2.$$

右边乘 h_1^{-1}，得到

$$g = kh_2h_1^{-1}.$$

因为 H 是群，所以

$$h_2h_1^{-1} \in H.$$

记

$$h_0 = h_2h_1^{-1} \in H.$$

于是：

$$g = kh_0.$$

现在看整个陪集：

$$gH = (kh_0)H.$$

由于 $h_0 \in H$，而“用 H 自己的一个元素乘整个 H”不会改变 H：

$$h_0H = H.$$

因此：

$$gH = k(h_0H) = kH.$$

所以我们得到：

$$\boxed{gH \cap kH \neq \varnothing \quad \Longrightarrow \quad gH = kH}$$

换句话说，如果两个陪集不相等，那么它们就一个共同元素都不能有：

$$\boxed{gH = kH \quad \text{或者} \quad gH \cap kH = \varnothing}$$

这就是为什么陪集能够把整个群 G 切成一块一块、互不重叠的部分。

例如在 S_3 中：

$$A_3 = \{e, (123), (132)\}$$

和

$$(12)A_3 = \{(12), (13), (23)\}$$

完全不相交，而且合起来正好是整个 S_3。

4.3 用陪集证明 Lagrange 定理

这里我前面那句话写错了，应该是：

$$\boxed{\text{子群的大小必须整除有限群的大小}}$$

这就是 **Lagrange 定理（拉格朗日定理）**。

而且我们其实已经有足够工具证明它了，因为前面已经学过陪集。

假设有限群 G 有一个子群 $H \leq G$。

每一个左陪集：

$$gH$$

和 H 本身有完全一样多的元素，因为映射

$$h \mapsto gh$$

是一一对应。

所以每个陪集大小都是：

$$|H|.$$

另一方面，不同的陪集要么完全相同，要么完全不相交。

因此整个群 G 可以被这些陪集完整地分成若干块：

$$G = g_1H \sqcup g_2H \sqcup \cdots \sqcup g_kH.$$

每一块都有：

$$|H|$$

个元素。

所以：

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{k\text{ 次}} = k|H|.$$

于是：

$$\boxed{|H| \mid |G|}$$

也就是：

$$\boxed{\text{子群阶整除群阶}}.$$

这里的“阶”就是元素个数。

所以刚才那个 3 元群的例子里，如果存在一个 2 元子群 H，就必须有：

$$2 \mid 3.$$

但显然不成立。

因此一个 3 阶群不可能有 2 阶子群。

这就是为什么假设

$$a^2 = e$$

会出问题：因为如果 $a \neq e$ 且

$$a^2 = e,$$

那么

$$\{e, a\}$$

就是一个有 2 个元素的子群，可是 2 不整除 3，矛盾。

所以在一个 3 阶群中，任取非单位元 a，必然有：

$$a^3 = e,$$

并且

$$G = \{e, a, a^2\}.$$

因此它是循环群，也就一定是阿贝尔群。

第 5 章：正规子群和商群：让陪集乘法没有歧义

本章对象：$H \triangleleft G$ 表示 H 在 G 的共轭下稳定。G/H 的元素是陪集；单位元是陪集 H，不是 G 中的单个元素 e。

补充证明：正规性的等价条件，以及商群乘法为何要求正规性

本节 G 是群，$H \leq G$ 是子群，g 是 G 中元素。由集合等式两边右乘 g^{-1}，得到

$$gH = Hg \quad \Longleftrightarrow \quad gHg^{-1} = H.$$

若对所有 g 都只有 $gHg^{-1} \subseteq H$，用 g^{-1} 代入再左右乘 g、g^{-1}，会得到反向包含，因此实际也是等号。这就是共轭形式的正规性。它表示整个子群作为集合稳定，并不要求 g 与每个 h 交换。

商群乘法的充分性由原证明的代表元计算给出。必要性也可以证明：假设陪集乘法按代表元定义且良定义。$h \in H$ 与 $e \in H$ 是同一陪集的代表元，则 $(hH)(gH) = (eH)(gH)$，故 $hgH = gH$，进而 $g^{-1}hg \in H$。这对所有 g, h 成立，故 H 正规。于是这个条件正好解决代表元歧义。

5.2 右陪集与正规子群

现在只加一个新概念：**右陪集**。

前面我们有：

$$gH = \{gh \mid h \in H\},$$

这叫左陪集。

那么同样地，也可以把固定元素 g 放在右边：

$$Hg = \{hg \mid h \in H\}.$$

这就叫：

右陪集

还是用：

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

和

$$A_3 = \{e, (123), (132)\}.$$

现在取：

$$g = (12).$$

我们前面已经算过左陪集：

$$(12)A_3.$$

现在算右陪集：

$$A_3(12).$$

也就是：

$$A_3(12) = \{e(12), (123)(12), (132)(12)\}.$$

第一个：

$$e(12) = (12).$$

再算：

$$(123)(12).$$

按照我们的约定，先做右边的：

$$(12),$$

再做左边的：

$$(123).$$

对 1：

$$1 \to 2 \to 3,$$

所以：

$$1 \to 3.$$

对 3：

$$3 \to 3 \to 1,$$

所以：

$$3 \to 1.$$

对 2：

$$2 \to 1 \to 2.$$

所以：

$$2 \to 2.$$

因此：

$$(123)(12) = (13).$$

再算：

$$(132)(12).$$

对 1：

$$1 \to 2 \to 1,$$

所以：

$$1 \to 1.$$

对 2：

$$2 \to 1 \to 3,$$

所以：

$$2 \to 3.$$

对 3：

$$3 \to 3 \to 2.$$

所以：

$$3 \to 2.$$

因此：

$$(132)(12) = (23).$$

所以：

$$\boxed{A_3(12) = \{(12), (13), (23)\}}$$

而前面：

$$(12)A_3 = \{(12), (13), (23)\}.$$

于是：

$$\boxed{(12)A_3 = A_3(12)}$$

这说明什么？

说明对于这个子群 A_3：

左边乘整个 A_3

和

右边乘整个 A_3

最后得到的是同一个集合。

这不是所有子群都有的性质。

如果一个子群 $H \leq G$ 满足：

$$gH = Hg$$

对所有

$$g \in G$$

都成立，那么我们就称：

$$\boxed{H \text{ 是 } G \text{ 的正规子群}}$$

英文：

$$\boxed{\textbf{normal subgroup}}$$

记作：

$$H \triangleleft G.$$

所以：

$$\boxed{A_3 \triangleleft S_3}$$

但这里最容易产生一个误解。

正规子群并不是说：

$$gh = hg$$

对每一个 $h \in H$ 都成立。

不是这个意思。

要求的是：

$$gH = Hg$$

这两个**集合**相同。

也就是说，左边乘以后得到的那一堆元素，和右边乘以后得到的那一堆元素一样。

具体某个 h 不一定和 g 交换。

例如：

$$(12)(123) \neq (123)(12).$$

实际上：

$$(12)(123) = (23),$$

而：

$$(123)(12) = (13).$$

二者不相等。

但整个集合仍然相等：

$$(12)A_3 = A_3(12).$$

所以：

$$\boxed{\text{正规} \neq \text{每个元素都交换}}$$

这是非常重要的一点。

下一步最值得解释的是：

为什么我们非要关心正规子群?

答案是：因为只有对子群“足够正规”，我们才能把整个群按这些陪集压缩成一个新的群，也就是**商群**。而“可解群”最终正是靠一层一层的商群来定义的。

5.3 商群的元素为什么是陪集

现在进入一个很关键、也很容易第一次看懵的概念：**商群（quotient group）**。

这一步我们慢一点，因为“正规子群为什么重要”就在这里。

先继续用：

$$A_3 \triangleleft S_3.$$

我们已经知道 S_3 被 A_3 的陪集分成两块：

$$A_3$$

和

$$(12)A_3.$$

其中：

$$A_3 = \{\text{所有偶置换}\},$$

而

$$(12)A_3 = \{\text{所有奇置换}\}.$$

现在做一个思想实验：

> 我不再关心每一个具体置换是谁，我只关心它属于“偶的那一块”还是“奇的那一块”。

也就是说，把整个 A_3 看成一个“大元素”：

$$[A_3],$$

把所有奇置换那一块也看成另一个“大元素”：

$$[(12)A_3].$$

这样，原来有 6 个元素的 S_3，就被压缩成了只有 2 个“大元素”的东西。

也就是：

$$\boxed{S_3/A_3}$$

它的元素是：

$$A_3, \qquad (12)A_3.$$

现在最关键的问题来了：

这些“块”之间能不能像群元素一样相乘？

我们希望定义：

$$(gA_3)(hA_3) = (gh)A_3.$$

例如：

$$[(12)A_3]\cdot[(23)A_3].$$

因为 (12) 和 (23) 都是奇置换，所以它们都属于同一个陪集：

$$(12)A_3=(23)A_3.$$

那么“奇那一块 × 奇那一块”应该等于什么？

算：

$$(12)(23)=(123).$$

而 (123) 是偶置换，所以：

$$(123)\in A_3.$$

于是：

$$\boxed{\text{奇块}\times\text{奇块}=\text{偶块}}$$

同理：

$$\text{偶块}\times\text{偶块}=\text{偶块},$$

$$\text{偶块}\times\text{奇块}=\text{奇块},$$

$$\text{奇块}\times\text{偶块}=\text{奇块}.$$

你应该会发现，这和：

$$(+1)(+1)=+1,$$

$$(-1)(-1) = +1$$

很像。

所以：

$$S_3/A_3$$

本质上就是一个只有两个元素的群。

但这里藏着一个非常严重的问题。

假设我说：

$$(gH)(kH) = (gk)H.$$

问题是：

一个陪集 gH 往往可以用很多不同的 g 来表示。

比如在这里：

$$(12)A_3 = (13)A_3 = (23)A_3.$$

它们其实是同一块。

那么如果我选择不同的代表元，比如用 (12) 或 (13)，最后乘出来的陪集会不会不同？

如果会不同，那么这个“乘法”就根本没有定义好。

我们希望：

$$gH = g'H, \qquad kH = k'H$$

时，一定有：

$$(gk)H = (g'k')H.$$

只有这样，陪集之间的乘法才是**良定义的**。

而这正是正规子群最重要的作用：

$$\boxed{H \triangleleft G}$$

恰好保证了：

$$\boxed{(gH)(kH) = (gk)H}$$

不会因为你选了不同代表元而产生歧义。

所以你可以把“正规子群”先理解成：

> 一个子群如果足够规则，使得“把它压成一个点以后”，剩下的块还能正常做群运算，那么它就是正规子群。

于是我们终于知道为什么普通子群还不够，而需要“正规子群”。

整个逻辑是：

子群

不一定能拿来“压缩”原群。

但：

正规子群

可以。

压缩之后得到：

商群

记作：

$$G/H.$$

在我们的例子里：

$$S_3/A_3$$

就是把：

所有偶置换看成一个元素，

把：

所有奇置换看成另一个元素.

最后只剩两个元素。

下一步最适合讲的是：

为什么“商群”可以理解为把一个群中的某部分结构忽略掉

这层直觉非常重要，因为以后“可解群”本质上就是：不断找正规子群、不断取商群，把一个复杂群一层层剥简单。

5.4 代表元计算：陪集乘法的良定义

关键就在这里。我们把它严格证明出来，不跳步。

假设

$$gH = g'H, \qquad kH = k'H.$$

这句话分别意味着什么？

因为 g' 属于 $g'H$，而 $g'H = gH$，所以

$$g' \in gH.$$

因此一定存在某个

$$h_1 \in H$$

使得

$$g' = gh_1.$$

同理，因为

$$kH = k'H,$$

所以存在

$$h_2 \in H$$

使得

$$k' = kh_2.$$

于是

$$g'k' = (gh_1)(kh_2) = gh_1kh_2.$$

现在真正的问题是：

$$gh_1kh_2$$

能不能写成

$$gk(\text{某个 } H \text{ 中的元素})?$$

因为如果能，那么它就属于

$$gkH.$$

难点就是中间这个：

$$h_1k.$$

我们想把 k 移到 h_1 左边。

在普通交换群里可以直接写成：

$$h_1k = kh_1,$$

但这里当然不能这么做。

正规性就是在这里起作用。

因为

$$H \triangleleft G,$$

等价地，对任意 $k \in G$ 和任意 $h_1 \in H$，都有

$$k^{-1}h_1k \in H.$$

先把这个新元素记成：

$$h_3 = k^{-1} h_1 k.$$

于是：

$$h_3 \in H.$$

而且从

$$h_3 = k^{-1} h_1 k$$

两边左乘 k，得到：

$$k h_3 = h_1 k.$$

所以：

$$h_1 k = k h_3.$$

代回刚才：

$$g' k' = g h_1 k h_2$$

就变成

$$g' k' = g k h_3 h_2.$$

因为：

$$h_3, h_2 \in H$$

而 H 是群，所以封闭：

$$h_3h_2 \in H.$$

记

$$h_4 = h_3h_2 \in H.$$

于是：

$$g'k' = gkh_4.$$

所以：

$$g'k' \in gkH.$$

也就是说：

$$g'k'H = gkH.$$

因此，无论你选择 gH 的代表元 g 还是 g'，选择 kH 的代表元 k 还是 k'，最终得到的陪集都是：

$$\boxed{gkH}.$$

所以定义

$$\boxed{(gH)(kH) = (gk)H}$$

是没有歧义的。

你可以把整个证明压缩成最关键的一步：

$$gh_1kh_2$$

之所以能够变成

$$gk(\text{某个 } H \text{ 中的元素}),$$

就是因为正规性允许我们把

$$h_1k$$

改写成

$$kh_3, \qquad h_3 \in H.$$

也就是：

> 正规性允许 H 中的元素“穿过”外面的群元素，但穿过去后可能变成另一个 H 中的元素。

注意它不是说

$$h_1k = kh_1,$$

而是说：

$$\boxed{h_1k = kh_3}$$

其中 h_3 仍然属于 H。

这其实就是“正规子群”最值得建立的直觉。

5.5 检查商群的全部群公理

既然刚才已经证明了“陪集乘法”在正规子群时是良定义的，下一步就该把最重要的一件事补完整：

> 为什么 G/H 真的构成一个群?

设

$$H \triangleleft G.$$

我们定义商集

$$G/H = \{gH \mid g \in G\},$$

并定义乘法

$$(gH)(kH) = (gk)H.$$

现在逐条检查群公理。

先看**封闭性**。两个元素

$$gH,\ kH \in G/H$$

相乘得到

$$(gH)(kH) = (gk)H.$$

而 $gk \in G$，所以

$$(gk)H$$

还是 G/H 中的一个陪集。因此封闭。

再看**结合律**。

取三个陪集：

$$gH,\quad kH,\quad lH.$$

左边：

$$[(gH)(kH)](lH)$$

先算：

$$(gH)(kH)=(gk)H,$$

所以

$$[(gH)(kH)](lH)=((gk)H)(lH)=((gk)l)H.$$

另一种括号：

$$(gH)[(kH)(lH)]$$

得到：

$$(gH)((kl)H)=(g(kl))H.$$

因为原群 G 中满足结合律：

$$(gk)l=g(kl),$$

所以：

$$((gk)l)H=(g(kl))H.$$

因此商群也满足结合律。

这里你可以看到一个常见规律：

> 商群很多性质，是从原群 G 继承下来的。

第三个，**单位元是什么？**

原群的单位元记作 e。

商群里面对应的陪集是：

$$eH.$$

但

$$eH = H.$$

所以商群的单位元其实就是：

$$\boxed{H}.$$

验证：

$$H \cdot gH = (eH)(gH) = (eg)H = gH.$$

同样：

$$(gH)H = gH.$$

所以：

$$\boxed{\text{商群中，整个 } H \text{ 被当成了单位元}}$$

这句话非常重要。

它其实揭示了“取商”的本质。

比如我们有

$$S_3/A_3.$$

在这里，原来 A_3 中有三个元素：

$$e,(123),(132).$$

但是取商以后，这三个元素全部被压成：

$$A_3.$$

而这个“大元素”就是商群的单位元。

所以从商群的角度来看：

$$e,\ (123),\ (132)$$

之间的区别被**彻底忽略了**。

这就是为什么我前面说：

> 取商群，可以理解为“把 H 内部的区别抹掉”。

最后看**逆元**。

商群中有一个元素：

$$gH.$$

它的逆是什么?

应该是:

$$g^{-1}H.$$

因为:

$$(gH)(g^{-1}H) = (gg^{-1})H = eH = H.$$

而 H 正是商群的单位元。

所以:

$$\boxed{(gH)^{-1} = g^{-1}H}.$$

四条全部成立,因此:

$$\boxed{G/H \text{ 是一个群}}$$

前提就是:

$$\boxed{H \triangleleft G}.$$

现在我们已经有了一个很有力量的操作:

$$G \longrightarrow G/H.$$

它做的事情是:

> 把 H 中的所有变化都视为“不重要”，只看不同陪集之间的区别。

例如：

$$S_3$$

有 6 个元素，但取

$$S_3/A_3$$

以后，只剩：

$$\boxed{2}$$

个元素。

因为它只区分：

偶置换

和

奇置换.

于是：

$$|S_3/A_3| = 2.$$

而：

$$|S_3| = 6, \qquad |A_3| = 3.$$

你会看到：

$$\boxed{|S_3/A_3| = \frac{|S_3|}{|A_3|}}$$

一般有限群中，如果 $H \triangleleft G$，也有：

$$\boxed{|G/H| = \frac{|G|}{|H|}}.$$

到这里，我们终于已经有足够工具开始接近“**可解群**”了。

但下一步我不会直接给定义。

我们先拿 S_3 做一件非常具体的事情：

$$\boxed{\{e\} \triangleleft A_3 \triangleleft S_3}$$

然后看看把 S_3 一层一层“剥掉”以后，会剩下什么。

这正是以后所谓“可解”的核心直觉。

第 6 章：群同态、核、像和第一同构定理

本章对象：$\varphi : G \to H$ 是群同态；e_G、e_H 是不同群的单位元；$N = \ker \varphi$。这里的核属于群论。

本节先定义：群同态、核、像和同构

设 G、H 是群，其单位元分别为 e_G、e_H。群同态 $\varphi : G \to H$ 满足 $\varphi(ab) = \varphi(a)\varphi(b)$。由 $\varphi(e_G) = \varphi(e_G)^2$ 可得 $\varphi(e_G) = e_H$；再由 $\varphi(a)\varphi(a^{-1}) = e_H$，得到 $\varphi(a^{-1}) = \varphi(a)^{-1}$。

核 $\ker\varphi$ 是映到 e_H 的元素组成的集合，像 $\operatorname{im}\varphi$ 是实际可以达到的元素组成的集合。两者都是子群：核内两元素的 ab^{-1} 仍映到 e_H；像内 $\varphi(a)\varphi(b)^{-1}=\varphi(ab^{-1})$ 仍在像中。对 $n\in\ker\varphi$、$g\in G$，

$$\varphi(gng^{-1})=\varphi(g)e_H\varphi(g)^{-1}=e_H,$$

所以 $\ker\varphi\triangleleft G$。单射表示不同输入得到不同输出，满射表示每个目标元素都能达到；双射的群同态称为群同构。符号 $\cong$ 表示结构同构，不要求两个群的元素是同一种对象。

补充证明：第一同构定理的完整检查

令 $N=\ker\varphi$。原映射 $\varphi:G\to H$ 的输入是群元素；下面的新映射 Φ 的输入是陪集。核已经证明为正规子群，所以商群 G/N 有定义。

第一步：定义新映射。

$$\Phi:G/N\longrightarrow\operatorname{im}\varphi,\qquad \Phi(gN)=\varphi(g).$$

第二步：检查良定义。 若 $gN=g'N$，则存在 $n\in N$ 使 $g'=gn$。因为 $\varphi(n)=e_H$，有

$$\varphi(g')=\varphi(g)\varphi(n)=\varphi(g).$$

所以同一陪集选用不同代表元时，得到同一个像。

第三步：检查单射。 若 $\varphi(g)=\varphi(g')$，则

$$\varphi(g^{-1}g')=\varphi(g)^{-1}\varphi(g')=e_H.$$

因此 $g^{-1}g'\in N$，从而 $gN=g'N$。也就是说，相同输出只能来自同一陪集。

第四步：检查满射。 目标取为 $\operatorname{im}\varphi$。其中任一元素都可以写成 $\varphi(g)$，它正是 gN 在 Φ 下的像。

第五步：检查保持乘法。

$$\Phi((gN)(kN)) = \varphi(gk) = \varphi(g)\varphi(k) = \Phi(gN)\Phi(kN).$$

因此 Φ 是双射的群同态。原对话详细解释了“相同像恰好对应相同陪集”；这里同时补上核的正规性及新映射保持乘法的检查。

6.2 核这个集合记号逐个符号拆解

> 原问题：这是什么意思

这个式子是在定义“核（kernel）”。

$$N = \{g \in G : \varphi(g) = e_H\}.$$

逐个拆开看。

$$G$$

是原来的群。

$$H$$

是映射到的另一个群。

$$\varphi : G \to H$$

表示一个群同态。

而

$$e_H$$

表示群 H 里的单位元。

所以：

$$\{g \in G : \varphi(g) = e_H\}$$

的意思就是：

> 把 G 里面所有经过 φ 后变成 H 的单位元的元素 g 全部收集起来。

这个集合就叫：

$$\ker \varphi.$$

也就是：

$$\boxed{\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}}$$

这里冒号

$$:$$

或者竖线

$$\mid$$

都可以读成：

> “满足……”

所以：

$$g \in G : \varphi(g) = e_H$$

就是：

> g 属于 G，并且满足 $\varphi(g) = e_H$。

比如：

$$\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

表示“取奇偶性”。

那么目标群的单位元是“偶”这一类，也就是

$$0 \pmod 2.$$

因此：

$$\ker \varphi = \{n \in \mathbb{Z} : n \equiv 0 \pmod 2\}.$$

也就是所有偶数。

放回我们刚才的 Galois 情形：

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F),$$

那么

$$\ker(\mathrm{res})$$

就是那些限制到 E 后变成恒等映射的自同构，也就是：

$$\boxed{\text{所有固定 } E \text{ 的自同构}}$$

因此：

$$\ker(\mathrm{res}) = \mathrm{Gal}(K/E).$$

你这里主要是卡在集合构造符号

$$\{g \in G : \cdots\}$$

而不是“核”本身。

6.3 像是实际能够到达的目标元素

> 原问题：这里突然出现imfi是指什么

这里的

$$\mathrm{im}\,\varphi$$

是 image *of* φ，中文叫：

$$\boxed{\varphi \text{ 的像}}$$

意思是：

> G 里的元素经过 φ 映射之后，实际上能够到达 H 里的哪些元素。

如果

$$\varphi : G \to H,$$

那么定义：

$$\boxed{\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\}}$$

也就是把所有

$$g \in G$$

都丢进 φ，收集所有输出。

注意它不一定等于整个 H。

比如：

$$\varphi : \mathbb{Z} \to \mathbb{Z}, \qquad \varphi(n) = 2n.$$

那么虽然目标群是整个 $\mathbb{Z}$，但实际上只能得到偶数：

$$\operatorname{im}\varphi = 2\mathbb{Z}.$$

所以：

$$\boxed{\operatorname{im}\varphi \subseteq H}$$

但未必：

$$\operatorname{im}\varphi = H.$$

刚才那个式子

$$G/N \longrightarrow \operatorname{im}\varphi$$

意思就是：

> 把 G 按照核 $N = \ker\varphi$ 的陪集压缩以后，得到的商群 G/N，可以和 φ 真正能到达的那部分 $\operatorname{im}\varphi$ 一一对应。

最终第一同构定理说的是：

$$\boxed{G/\ker\varphi \cong \operatorname{im}\varphi}$$

所以这里的 `im` 就是 image 的缩写。

6.4 第一同构定理的陪集证明

第一同构定理描述群同态怎样通过核的陪集形成同构。先在群论中证明，再在第 13 章应用于限制映射。

我们现在有一个群映射：

$$\varphi : G \to H.$$

这里不是任意映射，而是**群同态**，意思是它保持群运算：

$$\boxed{\varphi(ab) = \varphi(a)\varphi(b)}$$

现在设：

$$N = \ker \varphi.$$

也就是说：

$$N = \{g \in G : \varphi(g) = e_H\}.$$

我们想知道：

> 如果两个元素 $g_1, g_2 \in G$ 经过 φ 后得到同一个东西，它们之间是什么关系？

假设：

$$\varphi(g_1) = \varphi(g_2).$$

两边左乘：

$$\varphi(g_2)^{-1}.$$

得到：

$$\varphi(g_2)^{-1}\varphi(g_1) = e_H.$$

因为 φ 是同态，

$$\varphi(g_2^{-1}) = \varphi(g_2)^{-1},$$

所以：

$$\varphi(g_2^{-1}g_1) = e_H.$$

因此：

$$g_2^{-1}g_1 \in \ker\varphi = N.$$

于是存在某个 $n \in N$，使：

$$g_2^{-1}g_1 = n.$$

所以：

$$g_1 = g_2 n.$$

也就是说：

$$g_1 \in g_2 N.$$

因此：

$$\boxed{\varphi(g_1) = \varphi(g_2) \iff g_1 N = g_2 N}$$

这个结论非常重要。

它的意思是：

> φ 无法区分的元素，恰好就是落在同一个核的陪集里的元素。

举个非常简单的例子。

假设：

$$\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

把整数按奇偶性分类：

$$\varphi(n) = n \bmod 2.$$

那么：

$$\ker \varphi = \{\text{所有偶数}\} = 2\mathbb{Z}.$$

比如：

$$1, 3, 5, 7, \dots$$

虽然是不同整数，但经过 φ 后全部变成：

$$1.$$

因为它们互相只差一个偶数：

$$3 - 1 = 2, \qquad 5 - 1 = 4, \dots$$

所以它们其实都属于同一个陪集：

$$1 + 2\mathbb{Z}.$$

同样所有偶数属于：

$$0 + 2\mathbb{Z}.$$

所以 φ 真正在区分的并不是每个整数，而只是：

$$\boxed{\text{核的不同陪集}}$$

因此，与其让 φ 作用在每个 g 上，我们完全可以直接让它作用在陪集上：

$$gN \longmapsto \varphi(g).$$

这就得到：

$$G/N \longrightarrow \operatorname{im}\varphi.$$

而刚才已经证明：

$$g_1N = g_2N$$

当且仅当

$$\varphi(g_1) = \varphi(g_2).$$

所以这个新映射既不会把两个不同陪集错误地压成一个，也不会遗漏 φ 真正能达到的元素。

因此：

$$\boxed{G/\ker\varphi \cong \operatorname{im}\varphi}$$

这就是**群的第一同构定理**。

第 7 章：可解群：定义、例子及保持可解的三个引理

本章对象：C_m 是 m 阶循环群；V_4 是四元 Klein 群。可解列只要求相邻项正规，不要求每项正规于整个 G。

7.1 可解群的定义与 S_3 的可解列

> 原问题：直接回到这里吧

可以，我们直接回到这里。

前面已经讲过：

$$\text{正规子群} \to \text{商群}$$

所以现在下一步就是开始理解：

$$\boxed{\text{什么叫“可解群”（solvable group）}}$$

但先不下抽象定义，先拿 S_3 做例子。

考虑这条链：

$$\{e\} \triangleleft A_3 \triangleleft S_3.$$

这里：

$$A_3 = \{e, (123), (132)\}.$$

我们来看这条链到底有什么特殊之处。

首先看最上面这一层：

$$S_3/A_3.$$

前面已经知道，它只有两个元素：

$$A_3, \qquad (12)A_3.$$

因此：

$$|S_3/A_3| = 2.$$

一个只有两个元素的群一定是交换群，所以：

$$\boxed{S_3/A_3 \text{ 是阿贝尔群}}$$

然后再看下一层：

$$A_3/\{e\}.$$

因为除以最小子群 $\{e\}$ 基本什么都没压掉，所以：

$$A_3/\{e\} \cong A_3.$$

而 A_3 有三个元素：

$$e, (123), (132).$$

并且：

$$(123)(132) = (132)(123) = e,$$

整个 A_3 是交换群。

所以：

$$\boxed{A_3/\{e\} \text{ 也是阿贝尔群}}$$

现在你会看到：

$$S_3$$

虽然自己不是交换群，但我们能找到一条正规子群链：

$$\boxed{\{e\} \triangleleft A_3 \triangleleft S_3}$$

使得每一层相邻两群做商之后：

$$A_3/\{e\}$$

和

$$S_3/A_3$$

全都是阿贝尔群。

这就是“可解群”的核心思想：

> 一个群本身可以很复杂、可以不交换；但如果能把它通过正规子群一层一层拆开，而每一层剩下的商群都是交换群，那么这个群就叫可解群。

所以：

$$\boxed{S_3 \text{ 是可解群}}$$

正式定义就是：

如果存在一条链

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G$$

使得每一个商群

$$G_{i+1}/G_i$$

都是阿贝尔群，那么：

$$\boxed{G \text{ 是可解群}}$$

英文：

$$\boxed{\textbf{solvable group}}$$

这里的“可解”这个名字现在看起来非常奇怪：

> 群又没有方程，为什么叫“可解”？

这不是巧合。

这个名称正是因为 Galois 理论最后证明：

$$\boxed{\text{多项式可以用根式求解} \iff \text{它的 Galois 群是可解群}}$$

所以“solvable group”中的 solvable，确实和我们最终要研究的“方程能不能用根式解”直接相关。

不过现在还不要跳到 Galois 理论。

下一步最重要的是弄懂：

$$\boxed{\text{为什么“每一层商群是阿贝尔群”代表群被逐层简化了}}$$

然后我们再看 S_4 为什么也可解，而到了 S_5 为什么这套拆法会卡在 A_5。

7.2 阿贝尔商群如何逐层消去非交换部分

现在我们只解释一个问题：

> 为什么“每一层商群都是阿贝尔群”可以理解成把非交换性逐层消掉？

这其实是“可解群”定义背后的核心直觉。

先看一个群 G。如果 G 本身是阿贝尔群，那么最简单，因为所有元素都满足

$$ab = ba.$$

这时候你甚至不需要很多层，直接有：

$$\{e\} \triangleleft G,$$

而

$$G/\{e\} \cong G$$

本身就是阿贝尔群。

所以所有阿贝尔群当然都是可解群。

但 S_3 本身不是阿贝尔群。比如：

$$(12)(23) \neq (23)(12).$$

那为什么它还是“可解”？

因为我们找到：

$$\{e\} \triangleleft A_3 \triangleleft S_3.$$

现在看：

$$S_3/A_3.$$

在这个商群里，我们已经不再区分 A_3 里面的元素。

也就是说：

$$e,\ (123),\ (132)$$

全部被视为同一个“大元素”：

$$A_3.$$

而所有奇置换则被视为另一个“大元素”。

于是原来 S_3 中很多复杂的非交换行为，被压进了 A_3 里面。

外面剩下的结构：

$$S_3/A_3$$

只有两个元素，因此是交换的。

所以可以这样理解：

> S_3 的“非交换复杂性”并没有遍布整个群，而是可以被集中到较小的子群 A_3 里。

然后我们继续进入 A_3。

但 A_3 本身已经是交换群了。

于是复杂性到这里就结束了。

所以：

$$S_3 \supset A_3 \supset \{e\}$$

就是一种“一层一层剥掉非交换结构”的过程。

你也可以把它画成：

$$S_3$$

先忽略掉 A_3 内部的区别，得到

$$S_3/A_3,$$

这是阿贝尔群。

然后再看被我们刚才“藏起来”的 A_3。

它自己也是阿贝尔的。

所以整个 S_3 虽然不是阿贝尔群，但它是由若干层阿贝尔结构搭起来的。

这就是：

可解群

的直觉。

这里还有一个更精确的说法。

如果

$$G/N$$

是阿贝尔群，那么在商群里：

$$(gN)(hN) = (hN)(gN).$$

也就是说：

$$ghN = hgN.$$

这等价于说：

$$(gh)^{-1}hg \in N$$

或者更常见地写成：

$$ghg^{-1}h^{-1} \in N.$$

这个元素：

$$\boxed{ghg^{-1}h^{-1}}$$

叫做 g, h 的**交换子**，英文：

> commutator

记作：

$$[g, h].$$

如果 g, h 真正交换，那么：

$$gh = hg,$$

于是：

$$ghg^{-1}h^{-1} = e.$$

所以交换子是在测量：

$$\boxed{\text{两个元素“不交换了多少”}}$$

如果 G/N 是阿贝尔群，那么所有交换子都落进 N：

$$[g,h] \in N.$$

因此可以理解成：

> 把 N 压成单位元以后，所有“不交换的误差”都消失了。

这就是为什么阿贝尔商群代表“非交换性被压进更小的子群里”。

所以一条可解链：

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

满足每个：

$$G_{i+1}/G_i$$

都是阿贝尔群，本质上是在说：

$$\boxed{\text{每走下一层，剩余的非交换性都可以继续塞进更小的子群}}$$

最后一直塞到：

$$\{e\}.$$

于是所有非交换复杂性都被一层层消解掉了。

这就是“solvable”的群论意义。

下一步就很自然了：

$$\boxed{\text{看 } S_4 \text{ 为什么也能这样一层层拆}}$$

然后再对比 S_5，看它为什么最终卡在 A_5。

7.3 S_4 的可解列

现在我们看：

$$\boxed{S_4 \text{ 为什么仍然是可解群}}$$

但这一步会比 S_3 多一层，所以我们慢慢来。

对 S_4，一个很有用的正规子群链是：

$$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

这里新出现了一个东西：

$$\boxed{V_4}$$

它叫 Klein four group，**克莱因四元群**。

先只搞清楚 V_4 是什么。

S_4 是对

$$\{1,2,3,4\}$$

的所有置换。

其中有三个很特别的偶置换：

$$(12)(34),$$

$$(13)(24),$$

$$(14)(23).$$

再加上单位元：

$$e.$$

于是定义：

$$\boxed{V_4 = \{e, (12)(34), (13)(24), (14)(23)\}}$$

为什么这些都是偶置换?

因为例如：

$$(12)(34)$$

是两个换位的乘积。

两个是偶数，所以它是偶置换。

因此：

$$V_4 \subset A_4.$$

现在先看它为什么自己是一个群。

设

$$a = (12)(34),$$

$$b = (13)(24),$$

$$c = (14)(23).$$

那么：

$$a^2 = b^2 = c^2 = e.$$

因为每个都只是交换两对元素，做两次就还原。

更有意思的是：

$$ab = c.$$

我们算一下。

$$(12)(34)(13)(24).$$

还是从右往左。

先追踪 1：

$$1 \xrightarrow{(13)(24)} 3 \xrightarrow{(12)(34)} 4.$$

所以：

$$1 \to 4.$$

再看 4：

$$4 \to 2 \to 1.$$

所以：

$$4 \to 1.$$

因此有：

$$(14).$$

再看 2：

$$2 \to 4 \to 3.$$

所以：

$$2 \to 3.$$

而：

$$3 \to 1 \to 2.$$

所以：

$$3 \to 2.$$

因此：

$$ab = (14)(23) = c.$$

同样：

$$bc = a,$$

$$ca = b.$$

所以这四个元素彼此相乘，永远不会跑出去。

因此：

$$V_4$$

确实是一个群。

而且这个群还是阿贝尔群。

例如：

$$ab = c,$$

同时：

$$ba = c.$$

所以：

$$ab = ba.$$

实际上 V_4 中任意两个元素都交换。

因此：

$$\boxed{V_4 \text{ 是阿贝尔群}}$$

这已经告诉我们最下面这一层：

$$V_4/\{e\}$$

是阿贝尔群。

现在看整个链：

$$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

为了证明 S_4 可解，我们需要逐层看：

$$V_4/\{e\},$$

$$A_4/V_4,$$

$$S_4/A_4.$$

其中第一层已经知道：

$$V_4/\{e\} \cong V_4$$

是阿贝尔群。

最后一层：

$$S_4/A_4$$

和前面 S_3/A_3 一样，只区分奇置换和偶置换，所以只有两个元素，也一定是阿贝尔群。

真正需要理解的是中间这一层：

$$\boxed{A_4/V_4}$$

为什么也是阿贝尔群。

这就是下一步最合适讲的内容。

7.4 V_4 的正规性与三阶商群为何循环

现在只解决中间这一层：

$$\boxed{A_4/V_4 \text{ 为什么是阿贝尔群}}$$

这里其实有两个问题：

1. V_4 为什么是 A_4 的**正规子群**，这样 A_4/V_4 才有资格成为商群？
2. 这个商群为什么是阿贝尔群？

我们一个一个来。

先看大小：

$$|A_4| = \frac{4!}{2} = 12.$$

而

$$|V_4| = 4.$$

所以如果能够取商，那么：

$$|A_4/V_4| = \frac{12}{4} = 3.$$

也就是说，商群只有 **3 个元素**。

但我们现在还不能直接宣布它是群，因为首先要证明：

$$V_4 \triangleleft A_4.$$

为什么 V_4 是正规子群?

我们有:

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

这里介绍一个非常有用的事实。

如果 σ 是一个置换，那么:

$$\sigma(a\,b)\sigma^{-1}$$

等于:

$$(\sigma(a)\,\sigma(b)).$$

直觉上就是:

> 左右用 σ 和 σ^{-1} 包起来，相当于把循环里的标签全部按照 σ 重新命名。

例如假设:

$$\sigma = (123).$$

那么:

$$\sigma(12)\sigma^{-1}$$

就是把 $1, 2$ 分别换成

$$\sigma(1) = 2, \qquad \sigma(2) = 3,$$

所以：

$$\sigma(12)\sigma^{-1} = (23).$$

同样：

$$\sigma(12)(34)\sigma^{-1}$$

就会变成

$$(\sigma(1)\sigma(2))(\sigma(3)\sigma(4)).$$

关键是：

> 两个不相交的换位，在这种“重新命名”之后，仍然是两个不相交的换位。

所以：

$$(12)(34)$$

经过任意置换共轭后，只可能变成：

$$(12)(34),\quad (13)(24),\quad (14)(23).$$

也就是说，它还是待在 V_4 里面。

单位元 e 当然也还是 e。

因此对任意：

$$\sigma \in A_4,$$

都有：

$$\sigma V_4 \sigma^{-1} = V_4.$$

这正是正规子群的另一个等价定义：

$$\boxed{V_4 \triangleleft A_4}.$$

现在我们终于可以形成商群：

$$A_4/V_4.$$

它有：

$$3$$

个元素。

接下来的问题是：

> 为什么任何只有 3 个元素的群一定是阿贝尔群?

设这个群是：

$$G = \{e, a, b\}.$$

取一个不是单位元的元素，比如：

$$a \neq e.$$

看：

$$a^2.$$

它只能是 e, a, b 之一。

它不可能等于 a，因为如果：

$$a^2 = a,$$

两边乘 a^{-1}，得到：

$$a = e,$$

矛盾。

所以只有两种可能：

$$a^2 = e$$

或者

$$a^2 = b.$$

但第一种其实也不可能。

如果：

$$a^2 = e,$$

那么集合

$$\{e, a\}$$

会形成一个 2 元子群。

而子群大小必须整除群大小；2 不能整除 3。

如果暂时不想用这个定理，也可以以后再补。

所以必然：

$$a^2 = b.$$

于是：

$$a^3 = ab.$$

而因为群只有三个元素，继续乘最终必须回到 e，事实上：

$$a^3 = e.$$

因此整个群其实就是：

$$\{e, a, a^2\}.$$

所有元素都是 a 的幂。

那么：

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i.$$

所以一定交换。

因此：

任何 3 阶群都是循环群，因此是阿贝尔群

于是：

$$\boxed{A_4/V_4 \text{ 是阿贝尔群}}.$$

现在三层全部打通：

$$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

对应商群：

$$V_4/\{e\}$$

阿贝尔；

$$A_4/V_4$$

3 阶群，阿贝尔；

$$S_4/A_4$$

2 阶群，阿贝尔。

所以：

$$\boxed{S_4 \text{ 是可解群}}.$$

到这里，你已经看到了为什么四次方程对应的对称群 S_4 还能够被“一层层拆成阿贝尔结构”。

下一步就轮到真正的分水岭：

$$\boxed{S_5}$$

我们会先看它最自然的第一层：

$$A_5 \triangleleft S_5,$$

然后发现问题全部集中到了 A_5。而 A_5 和之前的 A_3, A_4 会出现一个本质性的不同。

补充证明：可解群的子群仍可解

设 G 有可解列 $e = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_r = G$，$H \leq G$。令 $H_i = H \cap G_i$。对 $x \in H_{i+1}$、$y \in H_i$，xyx^{-1} 同时属于 H 与 G_i，故属于 H_i；所以 $H_i \triangleleft H_{i+1}$。映射

$$H_{i+1}/H_i \longrightarrow G_{i+1}/G_i, \qquad hH_i \longmapsto hG_i$$

良定义且保持乘法；若 $hG_i = G_i$，则 $h \in H \cap G_i = H_i$，因此单射。其目标群阿贝尔，所以定义域也阿贝尔。于是 $e = H_0 \triangleleft \dots \triangleleft H_r = H$ 是可解列；相邻项允许相等，重复项删去即可。这补上原对话推广到 $n \geq 5$ 时仅引用、尚未写出的证明。

补充证明：可解的核与可解的商群给出可解的整体

设 $N \triangleleft G$，且 N 与 $Q = G/N$ 都可解。取 N 的可解列 $e = N_0 \triangleleft \dots \triangleleft N_s = N$；取 Q 的可解列 $N = Q_0 \triangleleft \dots \triangleleft Q_t = Q$。令 $\pi : G \to Q$ 是商映射，$P_j = \pi^{-1}(Q_j)$。因 $Q_j \triangleleft Q_{j+1}$，共轭计算给出 $P_j \triangleleft P_{j+1}$，而且 $P_0 = N$、$P_t = G$。

把 π 限制到 P_{j+1}，再映到 Q_{j+1}/Q_j，其核恰好是 P_j，且满射。第一同构定理给出 $P_{j+1}/P_j \cong Q_{j+1}/Q_j$，因此这些商群阿贝尔。把两条链连接为

$$\{e\} = N_0 \triangleleft \cdots \triangleleft N_s = N = P_0 \triangleleft P_1 \triangleleft \cdots \triangleleft P_t = G,$$

得到 G 的可解列。特别地，阿贝尔核当然可解，所以“可解群的阿贝尔扩张仍可解”。这里的“扩张”是群论中的核与商群关系，不是说把两个群简单做直积。

补充定义与证明：交换子如何检测商群的交换性

交换子 $[a,b]=aba^{-1}b^{-1}$；它等于 e 当且仅当 $ab=ba$。若 $N\triangleleft G$，则 G/N 阿贝尔，当且仅当所有交换子都落在 N 中。事实上，$abN=baN$ 等价于 $(ba)^{-1}ab\in N$；该元素 $a^{-1}b^{-1}ab$ 与 $aba^{-1}b^{-1}$ 互为一个共轭，N 正规，所以两种条件等价。也可以直接在商群中计算 aN、bN 的交换子。后面的商群可解证明就用这个判别。

7.6 可解群的商群仍可解

现在证明：

$$\boxed{G\text{ 可解},\ N\triangleleft G\Longrightarrow G/N\text{ 可解}}$$

我们只用已经学过的“可解群”定义，不额外引入新定理。

假设 G 可解。那么存在一条正规子群链：

$$\{e\}=G_0\triangleleft G_1\triangleleft\cdots\triangleleft G_r=G$$

并且每一层：

$$\boxed{G_{i+1}/G_i\text{ 是阿贝尔群}}.$$

现在我们想研究：

$$G/N.$$

这里 $N\triangleleft G$，否则商群 G/N 都没有定义。

我们有自然的商映射：

$$\boxed{\pi:G\to G/N}$$

它把：

$$g \mapsto gN.$$

现在把原来每一个 G_i 都通过 π 映射过去。

定义：

$$\boxed{H_i = \pi(G_i)}$$

于是每个 H_i 都是 G/N 里的一个子群。

原来的链：

$$G_0 \subset G_1 \subset \cdots \subset G_r$$

经过 π 后变成：

$$H_0 \subset H_1 \subset \cdots \subset H_r.$$

最上面：

$$H_r = \pi(G) = G/N.$$

最下面呢?

因为：

$$G_0 = \{e\},$$

所以：

$$H_0 = \pi(\{e\}) = \{N\}.$$

注意在商群 G/N 中，单位元就是陪集：

$$N.$$

所以：

$$\boxed{\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N}$$

我们现在只需要证明每一个：

$$H_{i+1}/H_i$$

都是阿贝尔群。

为什么？

任取：

$$a, b \in G_{i+1}.$$

因为：

$$G_{i+1}/G_i$$

是阿贝尔群，所以在这个商群里：

$$(aG_i)(bG_i) = (bG_i)(aG_i).$$

也就是：

$$abG_i = baG_i.$$

这意味着“不交换产生的差别”落在 G_i 里面。也就是：

$$\boxed{aba^{-1}b^{-1} \in G_i}$$

现在对它作用商映射 π：

$$\pi(aba^{-1}b^{-1}) \in \pi(G_i) = H_i.$$

因为 π 是群同态：

$$\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1}.$$

所以：

$$\boxed{\pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} \in H_i}$$

这句话又意味着：

在商群

$$H_{i+1}/H_i$$

里面：

$$\pi(a)H_i$$

和

$$\pi(b)H_i$$

能够交换。

而 a, b 是任意的，所以：

$$\boxed{H_{i+1}/H_i \text{ 是阿贝尔群}}.$$

于是我们已经给 G/N 找到了一条：

$$\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N$$

并且每一层商群都是阿贝尔群。

按照可解群定义：

$$\boxed{G/N \text{ 可解}}.$$

7.7 逐元素证明群链的像仍形成正规链

> 原问题：为什么这个就成立了

这里要分成三件事证明，刚才我确实压得太快了。

我们定义了：

$$H_i = \pi(G_i),$$

其中

$$\pi : G \to G/N, \qquad \pi(g) = gN.$$

而原来有：

$$G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G.$$

现在为什么能得到：

$$\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N?$$

先看最下面。

因为

$$G_0 = \{e\},$$

所以：

$$H_0 = \pi(G_0) = \{\pi(e)\}.$$

而：

$$\pi(e) = eN = N.$$

所以：

$$\boxed{H_0 = \{N\}}.$$

注意这里 N 是商群 G/N 的单位元，因为：

$$N \cdot gN = gN.$$

所以 $\{N\}$ 就相当于普通群里的 $\{e\}$。

再看最上面。

因为：

$$G_r = G,$$

所以：

$$H_r = \pi(G_r) = \pi(G).$$

而商映射 π 会把所有 $g \in G$ 送成所有陪集 gN。

这些陪集正好构成整个：

$$G/N.$$

所以：

$$\boxed{H_r = G/N}.$$

第三件事最关键：

为什么：

$$H_i \triangleleft H_{i+1}?$$

我们知道原来：

$$G_i \triangleleft G_{i+1}.$$

现在取任意：

$$x \in H_{i+1}$$

和：

$$y \in H_i.$$

因为：

$$H_{i+1} = \pi(G_{i+1}),$$

所以存在：

$$a \in G_{i+1}$$

使：

$$x = \pi(a).$$

同理存在：

$$b \in G_i$$

使：

$$y = \pi(b).$$

现在看共轭：

$$xyx^{-1}.$$

代入：

$$xyx^{-1} = \pi(a)\pi(b)\pi(a)^{-1}.$$

因为 π 是群同态：

$$= \pi(aba^{-1}).$$

而原来：

$$G_i \triangleleft G_{i+1},$$

所以：

$$aba^{-1} \in G_i.$$

于是：

$$\pi(aba^{-1}) \in \pi(G_i) = H_i.$$

所以：

$$xyx^{-1} \in H_i.$$

这对任意 $x \in H_{i+1}$、$y \in H_i$ 都成立，因此：

$$\boxed{H_i \triangleleft H_{i+1}}.$$

所以整个链才真正成立：

$$\boxed{\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N}$$

核心就是一句：

> 正规子群经过群同态取像以后，仍然正规于对应的大群的像。

这里不是因为“把 G_i 映过去”就自动能写 $\triangleleft$，还需要上面这个共轭计算。

7.8 逐元素证明像链的相邻商群阿贝尔

刚才我们已经证明了：

$$H_i = \pi(G_i)$$

会形成一条正规的子群链：

$$\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N.$$

现在还差最后一件事：

$$\boxed{H_{i+1}/H_i \text{ 为什么是阿贝尔群?}}$$

原来的 G 是可解群，所以我们知道：

$$G_{i+1}/G_i$$

是阿贝尔群。

这句话意味着：任取

$$a, b \in G_{i+1},$$

它们在商群里交换：

$$(aG_i)(bG_i) = (bG_i)(aG_i).$$

也就是：

$$abG_i = baG_i.$$

这意味着 ab 和 ba 只差一个 G_i 中的元素。等价地：

$$aba^{-1}b^{-1} \in G_i.$$

现在把它通过

$$\pi : G \to G/N$$

映过去。

令

$$x = \pi(a), \qquad y = \pi(b).$$

因为 $a, b \in G_{i+1}$，所以：

$$x, y \in H_{i+1}.$$

而：

$$aba^{-1}b^{-1} \in G_i.$$

作用 π：

$$\pi(aba^{-1}b^{-1}) \in \pi(G_i) = H_i.$$

利用 π 是群同态：

$$\pi(aba^{-1}b^{-1}) = xyx^{-1}y^{-1}.$$

所以：

$$\boxed{xyx^{-1}y^{-1} \in H_i}.$$

这就意味着，在商群

$$H_{i+1}/H_i$$

里，x 和 y 的不交换部分已经被压进了单位元。

因此：

$$(xH_i)(yH_i) = (yH_i)(xH_i).$$

因为 x, y 任意，所以：

$$\boxed{H_{i+1}/H_i \text{ 是阿贝尔群}}.$$

于是我们有：

$$\{N\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G/N$$

而且每一个：

$$H_{i+1}/H_i$$

都是阿贝尔群。

这正是“可解群”的定义，所以：

$$\boxed{G/N \text{ 可解}}.$$

第 8 章：A_5 的结构：完整证明五次的群论障碍

本章对象：共轭类 $Cl_G(x)$ 是 $gxg^{-1} : g \in G$；中心化子 $C_G(x)$ 是与 x 交换的元素组成的子群；单群只有两个正规子群。

8.1 从 S_4 走到 S_5：单群障碍

好，我们现在正式进入分水岭：

$$\boxed{S_5}$$

前面对 S_4，我们找到：

$$\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

并且每一层商群都是阿贝尔群。

现在尝试对 S_5 做同样的事。

首先最自然的子群还是：

$$A_5 = \{\text{所有偶置换}\}.$$

而且和前面一样：

$$\boxed{A_5 \triangleleft S_5}.$$

为什么？

因为置换的奇偶性在共轭下不改变。

如果：

$$\sigma \in S_5, \qquad \tau \in A_5,$$

那么看：

$$\sigma\tau\sigma^{-1}.$$

如果用“奇偶性乘法”来算：

$$\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma^{-1}).$$

其中：

$$\operatorname{sgn}(\tau) = +1$$

因为 τ 是偶置换。

并且：

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma).$$

所以：

$$\operatorname{sgn}(\sigma\tau\sigma^{-1}) = \operatorname{sgn}(\sigma)^2 = 1.$$

因此：

$$\sigma\tau\sigma^{-1} \in A_5.$$

所以：

$$\boxed{A_5 \triangleleft S_5}.$$

然后看商群：

$$S_5/A_5.$$

因为：

$$|S_5| = 5! = 120,$$

而：

$$|A_5| = \frac{120}{2} = 60,$$

所以：

$$|S_5/A_5| = 2.$$

因此：

$$\boxed{S_5/A_5 \text{ 是阿贝尔群}}.$$

所以第一层完全没问题：

$$S_5 \longrightarrow S_5/A_5.$$

真正的问题全部被压进了：

$$\boxed{A_5}.$$

这和 S_4 很像。

但是 S_4 的时候，我们进入 A_4 后，还能继续找到：

$$V_4 \triangleleft A_4.$$

于是继续拆：

$$A_4/V_4.$$

但到了 A_5，奇怪的事情发生了：

$$\boxed{A_5 \text{ 没有类似 } V_4 \text{ 的非平凡正规子群。}}$$

准确地说：

$$A_5$$

的正规子群只有：

$$\{e\}$$

和

$$A_5$$

本身。

这种群就叫：

$$\boxed{\textbf{simple group}，\text{单群}}.$$

注意“单群”不是说它很简单。

恰恰相反，这里的 simple 意思是：

> **它已经不能通过正规子群继续拆开。**

而 A_5 更麻烦的是：

$$\boxed{A_5 \text{ 不是阿贝尔群}}.$$

所以如果我们尝试：

$$\{e\} \triangleleft A_5,$$

对应的商群就是：

$$A_5/\{e\} \cong A_5,$$

但 A_5 本身不是阿贝尔群。

因此这条链不满足“每一层商群都是阿贝尔群”。

而又因为 A_5 没有中间的非平凡正规子群，所以没法像：

$$A_4 \supset V_4 \supset \{e\}$$

那样绕过去。

这就是关键障碍：

$$\boxed{A_5 \text{ 是非阿贝尔单群}}$$

于是：

$$\boxed{A_5 \text{ 不可解}}$$

进而：

$$\boxed{S_5 \text{ 不可解}}.$$

但这里最难的一步我们还没有证明：

$$\boxed{\text{为什么 } A_5 \text{ 没有任何非平凡正规子群?}}$$

这一步不能一句话带过。

下一步我们应该先把 A_5 里的元素按循环类型全部分类，然后再看一个正规子群如果包含某种元素，会被“共轭”迫使包含哪些其他元素。这样才能真正看出为什么它最后只能是整个 A_5。

8.2 A_5 的循环类型及元素数目

下一步先**只做一件事：把 A_5 里面到底有哪些类型的置换弄清楚**。这一步是证明 A_5 是单群的准备。

A_5 是 S_5 里的所有偶置换，所以一共有

$$|A_5| = \frac{5!}{2} = 60$$

个元素。

我们要问：

> 一个作用在 $\{1,2,3,4,5\}$ 上的偶置换，它的不相交循环分解可能长什么样？

先从所有可能的循环类型开始。

---

1. 恒等置换

当然有

$$e.$$

它什么都不动。

共：

$$1$$

个。

---

2. 一个换位，例如 (12)

换位是奇置换，所以：

$$(12) \notin A_5.$$

因此这种类型全部排除。

---

3. 一个 3–循环，例如 (123)

一个 3–循环可以拆成两个换位：

$$(123) = (13)(12),$$

所以它是偶置换。

因此：

$$(123) \in A_5.$$

所以 A_5 中有所有 3–循环。

现在数一共有多少个。

先从 5 个元素里挑 3 个：

$$\binom{5}{3} = 10.$$

对于选定的三个元素，例如 $\{1,2,3\}$，可以形成几个不同的 3–循环？

有：

$$(123)$$

和

$$(132).$$

注意

$$(123) = (231) = (312)$$

只是同一个循环换了起点，不算新的。

所以每组三个元素产生：

$$2$$

个 3–循环。

因此一共有：

$$10 \times 2 = 20.$$

所以：

$$\boxed{3\text{-循环共有 } 20 \text{ 个}}$$

---

4. 两个不相交的换位

例如：

$$(12)(34).$$

这是两个换位的乘积，所以是偶置换。

因此也属于 A_5。

这种类型叫：

$$\boxed{\text{double transposition，双换位}}$$

例如：

$$(12)(34),\quad (13)(25),\quad (15)(24).$$

现在数有多少个。

首先，有 5 个元素，其中必然有一个元素不动。

先选那个不动的元素：

$$5$$

种选择。

剩下 4 个元素要分成两对。

例如剩下：

$$1,2,3,4.$$

可以配成：

$$(12)(34),$$

$$(13)(24),$$

$$(14)(23).$$

正好 3 种。

所以总数：

$$5 \times 3 = 15.$$

因此：

$$\boxed{\text{双换位共有 } 15 \text{ 个}}$$

---

5. 一个 4–循环

例如：

$$(1234).$$

4–循环需要：

$$4 - 1 = 3$$

个换位。

3 是奇数，所以它是奇置换。

因此：

$$(1234) \notin A_5.$$

全部排除。

---

6. 一个 5–循环

例如：

$$(12345).$$

5–循环需要：

$$5-1=4$$

个换位。

4 是偶数，所以：

$$(12345)\in A_5.$$

现在数有多少个 5–循环。

对于 5 个固定元素，一个 5–循环可以写成：

$$(a_1a_2a_3a_4a_5).$$

总共有：

$$5!$$

种排列方式。

但是同一个循环可以从任意位置开始写：

$$(12345)=(23451)=(34512)=(45123)=(51234).$$

所以每个循环被重复计算了 5 次。

因此：

$$\frac{5!}{5} = 4! = 24.$$

所以：

$$\boxed{5\text{-循环共有 } 24 \text{ 个}}$$

现在把所有偶置换类型加起来：

$$1 + 20 + 15 + 24 = 60.$$

正好：

$$|A_5| = 60.$$

因此我们没有遗漏任何元素。

所以 A_5 的元素只有四种类型：

类型	数量
e	1
3-循环	20
双换位	15
5-循环	24

这张表后面非常重要。

接下来我们要利用“正规子群在共轭下必须保持不变”。

直觉上，如果某个正规子群 $N \triangleleft A_5$ 含有一个元素，比如：

$$(123),$$

那么它不能只含这一个 3–循环。

因为对 A_5 中各种 σ 做

$$\sigma(123)\sigma^{-1},$$

会把标签重新排列，从而强迫 N 同时包含很多其他 3–循环。

下一步就是仔细讲：

$$\boxed{\text{共轭为什么等于“重新给循环里的数字贴标签”}}$$

以及它如何限制正规子群。

8.3 共轭就是重新给循环贴标签

本段先解释共轭的作用，并列出需要验证的共轭类数量。三循环、双换位及五循环的类大小将在紧接着的补充证明中计算，不能只由“重新贴标签”这句话直接认定。

现在我们只讲：

$$\boxed{\sigma\tau\sigma^{-1}}$$

为什么可以理解成“把 τ 里的数字重新命名”。

假设

$$\tau = (123).$$

它的意思是：

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 1.$$

现在取另一个置换 σ。比如

$$\sigma = (14)(25).$$

那么：

$$\sigma(1) = 4, \qquad \sigma(2) = 5, \qquad \sigma(3) = 3.$$

我们来看

$$\sigma(123)\sigma^{-1}.$$

结论是：

$$\boxed{\sigma(123)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3))}$$

所以这里就是：

$$\boxed{\sigma(123)\sigma^{-1} = (453)}$$

也就是

$$(453).$$

为什么？

我们直接跟踪一个元素。

比如先看 $\sigma(1) = 4$。

对 4 作用

$$\sigma(123)\sigma^{-1}.$$

第一步，最右边的 σ^{-1}：

$$4 \mapsto 1.$$

然后做 (123)：

$$1 \mapsto 2.$$

最后做 σ：

$$2 \mapsto 5.$$

所以：

$$4 \mapsto 5.$$

同理：

$$5 \mapsto 3,$$

$$3 \mapsto 4.$$

于是：

$$4 \to 5 \to 3 \to 4,$$

所以就是：

$$(453).$$

因此：

$$\boxed{\sigma(a_1 a_2 \cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))}$$

这就是“共轭就是重新贴标签”。

现在来看为什么这对正规子群重要。

假设：

$$N \triangleleft A_5.$$

正规意味着：

$$\sigma N \sigma^{-1} = N$$

对所有

$$\sigma \in A_5$$

都成立。

所以如果：

$$\tau \in N,$$

那么：

$$\sigma \tau \sigma^{-1} \in N.$$

换句话说：

> 只要 N 含有一个元素，它就必须同时包含这个元素在 A_5 中的所有共轭元素。

这就非常强。

例如如果：

$$(123) \in N,$$

那么所有形如：

$$\sigma(123)\sigma^{-1}$$

的元素也必须在 N 里。

而这些都是 3–循环。

事实上，在 A_5 中所有 20 个 3–循环彼此共轭。

所以：

$$\boxed{N \text{ 如果包含一个 } 3\text{-循环，就必须包含全部 } 20 \text{ 个 } 3\text{-循环}}$$

同理，15 个双换位也形成一个共轭类。

所以：

$$\boxed{N \text{ 如果包含一个双换位，就必须包含全部 } 15 \text{ 个双换位}}$$

但 5–循环这里稍微特殊一点：

> 在 S_5 中，24 个 5–循环全部彼此共轭； 但在 A_5 中，它们会裂成两个共轭类，每类 12 个。

这个细节后面证明 A_5 单群时很重要。

所以 A_5 的共轭类大小实际上是：

$$\boxed{1,\ 20,\ 15,\ 12,\ 12}$$

总和：

$$1+20+15+12+12=60.$$

下一步我们就利用这个事实：

> 正规子群必须是若干个共轭类的并，并且一定包含单位元。

然后看这些共轭类大小能不能拼出一个既整除 60、又严格介于 1 和 60 之间的正规子群大小。

补充证明：A_5 的共轭类为什么是 1、20、15、12、12

先定义中心化子 $C_G(x)=g\in G:gx=xg$，它是一个子群。共轭映射 $g\mapsto gxg^{-1}$ 的两个输入 g,h 得到同一个输出，当且仅当 $h^{-1}g\in C_G(x)$。因此共轭类与中心化子的左陪集一一对应，有限群中

$$|\mathrm{Cl}_G(x)|=|G|/|C_G(x)|.$$

这一步只用了已经证明的陪集计数，不需要提前调用其他群论定理。

对三循环 $c=(123)$，交换它的置换必须保持集合 {1,2,3}，在这个集合上只能是 e,c,c^2；在剩下的 {4,5} 上可选 e 或 (45)。S_5 中中心化子有 6 个元素，其中偶置换恰好 3 个。因此 A_5 中这个共轭类有 60/3=20 个元素，正好覆盖全部三循环。

对双换位 $d=(12)(34)$，交换它的置换必须固定唯一不动点 5。它可以决定把 {1,2} 送到两对中的哪一对（2 种），以及每对内的顺序（各 2 种），故 S_5 的中心化子有 8 个元素。奇置换 (12) 在该中心化子中，乘以它给出中心化子内偶、奇元素的双射，所以偶元素有 4 个。共轭类大小为 60/4=15，正好覆盖全部双换位。

对五循环 $c=(12345)$，与它交换的置换 g 一旦确定 $g(1)$，其余像由 $g(c^j(1))=c^j(g(1))$ 决定。因此中心化子恰好是 e,c,c^2,c^3,c^4，其中所有元素均为偶置换。每个 A_5 共轭类大小为 60/5=12。五循环总共有 24 个，所以分成恰好两个类。单位元独自一类，于是得到 1、20、15、12、12。

补充检查：非阿贝尔单群为什么不可解

令 $a=(123)$、$b=(345)$，乘积从右向左作用。ab 把 3 送到 4，ba 把 3 送到 1，因此 $ab\neq ba$。故 A_5 非阿贝尔。若它存在可解列，删除重复项后，最后一个真子群必须正规于 A_5。单群性迫使这个真子群为 e，于是最后的商群就是 A_5 本身，却不是阿贝尔群，矛盾。再利用已证明的“可解群的子群仍可解”，推出 S_5 不可解。

8.5 用共轭类并集与整除条件证明 A_5 单群

现在我们利用刚才得到的 A_5 共轭类大小

$$\boxed{1,\ 20,\ 15,\ 12,\ 12}$$

来证明：

$$\boxed{A_5 \text{ 没有非平凡正规子群}}$$

先只看第一个关键点。

如果

$$N \triangleleft A_5,$$

并且 $x\in N$，那么对任意 $\sigma\in A_5$，

$$\sigma x\sigma^{-1}\in N.$$

所以只要 N 含有一个 x，它就必须把 x 的**整个共轭类**都包含进去。

因此：

$$\boxed{\text{正规子群一定是若干个共轭类的并}}$$

并且因为任何子群都必须包含单位元 e，所以大小为 1 的共轭类

$$\{e\}$$

必然包含。

于是正规子群 N 的大小只能由下面这些数字拼出来：

$$1,\quad 20,\quad 15,\quad 12,\quad 12.$$

也就是说一定是

$$|N| = 1 + \text{若干个 } 20, 15, 12, 12.$$

现在第二个条件来自刚才学过的 Lagrange 定理。

因为

$$N \leq A_5$$

而

$$|A_5| = 60,$$

所以：

$$\boxed{|N| \mid 60}.$$

60 的正因数只有：

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.$$

所以我们只需要看看：

> 用 $1, 20, 15, 12, 12$ 中的若干项相加，能不能得到这些因数中的某一个？

我们逐渐加。

只取单位元：

$$1.$$

这对应：

$$N = \{e\}.$$

这是平凡正规子群。

如果再加入一个 12 元共轭类：

$$1 + 12 = 13.$$

但：

$$13 \nmid 60.$$

不行。

加入 15 元类：

$$1 + 15 = 16,$$

而

$$16 \nmid 60.$$

不行。

加入 20 元类：

$$1 + 20 = 21,$$

也不整除 60。

再尝试两个非平凡共轭类：

$$1 + 12 + 12 = 25,$$

$$1 + 12 + 15 = 28,$$

$$1 + 12 + 20 = 33,$$

$$1 + 15 + 20 = 36.$$

没有一个整除 60。

三个：

$$1 + 12 + 12 + 15 = 40,$$

$$1 + 12 + 12 + 20 = 45,$$

$$1 + 12 + 15 + 20 = 48.$$

也都不整除 60。

最后全部都要：

$$1 + 12 + 12 + 15 + 20 = 60.$$

这就是整个 A_5。

因此正规子群的大小只有两种可能：

$$|N| = 1$$

或者

$$|N| = 60.$$

所以：

$$\boxed{N = \{e\} \quad \text{或} \quad N = A_5}$$

不存在中间的非平凡正规子群。

因此：

$$\boxed{A_5 \text{ 是单群}}$$

但我们还需要另一半：

$$A_5$$

不是阿贝尔群。

这个很容易，例如：

$$(123), (345) \in A_5,$$

但一般有

$$(123)(345) \neq (345)(123).$$

所以 A_5 是：

$$\boxed{\text{非阿贝尔单群}}.$$

这就直接造成“可解”失败。

因为如果想构造：

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = A_5$$

而 A_5 没有任何中间正规子群，那么只能是：

$$\{e\} \triangleleft A_5.$$

对应唯一的非平凡商群：

$$A_5/\{e\} \cong A_5.$$

可是它不是阿贝尔群。

所以：

$$\boxed{A_5 \text{ 不可解}}$$

进而因为

$$A_5 \triangleleft S_5$$

且 A_5 已经是不可解的障碍，所以：

$$\boxed{S_5 \text{ 也不可解}}.$$

到这里，我们已经完成了纯群论这半边：

$$S_2, S_3, S_4 \text{ 可解}, \qquad S_5 \text{ 不可解}.$$

下一步就要开始真正搭桥到**方程**：

$$\boxed{\text{为什么“用根式解方程”竟然对应“Galois 群是可解群”？}}$$

在进入这个桥之前，我们首先必须学一个新对象：**域（field）**。因为“知道哪些数”和“加入一个平方根以后知道哪些新数”都要用域来精确描述。

第 9 章：域、理想、代数元与扩张次数

本章对象：$\mathbb{Q}$ 是有理数域；R 是含单位元的交换环；I 是理想；$F \subseteq E \subseteq K$ 是域塔。$F(\alpha)$ 是生成域，$[K:F]$ 是向量空间维数；span 表示所有给定域系数的线性组合。

9.1 域与域扩张：允许使用哪些数

现在开始进入和“根式解”真正连接的另一半：**域（field）**。

这一步先只回答一个问题：

> 我们怎样严格描述“目前允许使用哪些数，以及这些数之间允许做哪些运算”？

假设我们从有理数开始：

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z},\ q \neq 0 \right\}.$$

如果我们只允许做：

$$+, \quad -, \quad \times, \quad \div$$

而且除数不能是 0，那么从有理数出发，永远还是有理数。

例如：

$$\frac{2}{3} + \frac{5}{7} = \frac{29}{21} \in \mathbb{Q},$$

$$\frac{2}{3} \cdot \frac{5}{7} = \frac{10}{21} \in \mathbb{Q},$$

$$\frac{2/3}{5/7} = \frac{14}{15} \in \mathbb{Q}.$$

所以 $\mathbb{Q}$ 对四则运算是“封闭”的。

这就是域最核心的直觉：

一个域，是一个可以自由做四则运算而不会跑出去的数系

当然，正式定义稍微严格一些。

一个集合 F，如果有加法和乘法，并满足：

$$(F, +)$$

是一个阿贝尔群，

同时非零元素

$$F^\times = F \setminus \{0\}$$

在乘法下也是一个阿贝尔群，

再加上乘法对加法满足分配律：

$$a(b+c) = ab + ac,$$

那么 F 就叫一个域。

这里其实就是把我们前面学过的“群”用到了两次。

第一次是加法：

$$(F, +).$$

所以必须有：

$$0,$$

每个 a 有加法逆元：

$$-a.$$

第二次是乘法：

$$(F \setminus \{0\}, \times).$$

所以必须有：

$$1,$$

每个非零 a 有乘法逆元：

$$a^{-1}.$$

也就是可以除以 a。

因此：

域就是既能加减，又能乘除的代数系统

最典型的例子是：

$$\mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}.$$

它们都是域。

但整数：

$$\mathbb{Z}$$

不是域。

为什么？

因为：

$$2 \in \mathbb{Z},$$

但它的乘法逆元：

$$\frac{1}{2}$$

不在 $\mathbb{Z}$ 中。

所以整数不能在内部自由做除法。

现在这个概念为什么和方程有关?

考虑:

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

如果我们只在

$$\mathbb{Q}$$

里面工作，那么它没有根。

因为:

$$\sqrt{2} \notin \mathbb{Q}.$$

于是我们想做一件事:

> 在原来的有理数域里“加入”一个新数 $\sqrt{2}$。

加入以后，我们当然不能只拥有一个孤零零的 $\sqrt{2}$。

因为如果这是一个域，那就必须还能做加减乘除。

所以必须至少包含:

$$1 + \sqrt{2},$$

$$3 - 2\sqrt{2},$$

$$\frac{1}{1 + \sqrt{2}},$$

等等。

而：

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

最后会发现，这个新域里的每个元素都可以写成：

$$\boxed{a + b\sqrt{2}, \qquad a, b \in \mathbb{Q}}$$

这个新域记作：

$$\boxed{\mathbb{Q}(\sqrt{2})}.$$

读作：

> $\mathbb{Q}$ adjoining $\sqrt{2}$

中文通常说：

> 在 $\mathbb{Q}$ 上添加 $\sqrt{2}$ 得到的域。

这一步非常重要，因为以后所谓“用根式解方程”，本质上就是不断做：

$$F \subset F(\sqrt[n_1]{a_1}) \subset F(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \subset \cdots$$

也就是：

$$\boxed{\text{不断往已有的域里加入根式}}$$

所以“根式解”最终会变成一个关于**域扩张**的问题。

下一步最自然就是仔细讲：

$$\boxed{\mathbb{Q}(\sqrt{2}) \text{ 为什么恰好都是 } a+b\sqrt{2}，\text{不会需要更复杂的形式}}$$

这会正式引出“域扩张”的概念。

9.2 先定义环和理想，理解吸收性质

> 原问题：你得解释理想是什么吧

对，这里确实应该先把“理想（ideal）”讲清楚，不然前面那句话是悬空的。

先从我们已经熟悉的结构开始。

一个环 R 里有两种运算：

$$+, \qquad \times.$$

例如：

$$\mathbb{Z}$$

就是一个环。

现在我们想从 R 里面挑一个子集 I，希望它在某种意义上“对环运算很稳定”。

理想要求两件事。

第一，I 对加法本身要形成一个群。也就是如果

$$a, b \in I,$$

那么：

$$a - b \in I.$$

例如偶数集合：

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

满足这一点。

第二，这才是理想最特殊的地方：

$$\boxed{a \in I, \quad r \in R \Longrightarrow ra \in I}$$

如果是交换环，也等价于

$$ar \in I.$$

意思是：

> 理想里的一个元素，乘上整个环里的任意元素，都不能跑出理想。

例如在

$$R = \mathbb{Z}$$

里，

$$I = 2\mathbb{Z}$$

是一个理想。

因为如果

$$a = 2k$$

是偶数，而

$$r \in \mathbb{Z},$$

那么：

$$ra = r(2k) = 2(rk),$$

仍然是偶数。

所以：

$$2\mathbb{Z}$$

是 $\mathbb{Z}$ 的理想。

同理：

$$3\mathbb{Z}, \quad 5\mathbb{Z}, \quad 12\mathbb{Z}$$

都是理想。

为什么不能只说“子群”？

因为子群只管一种运算。

比如：

$$2\mathbb{Z}$$

是整数加法群

$$(\mathbb{Z}, +)$$

的子群。

但是“理想”还额外要求：

$$\boxed{\text{外面的环元素可以乘进来}}$$

所以理想比“加法子群”要求更强。

可以先记：

$$\boxed{\text{理想} = \text{加法子群} + \text{对整个环的乘法吸收}}$$

这里常说理想具有 **吸收性**。

因为：

$$r \in R, \quad a \in I$$

以后，

$$ra$$

被“吸”回 I 里面。

现在就能理解为什么域同态的核是理想。

假设：

$$\varphi : R \to S$$

是环同态。

它的核是：

$$\ker \varphi = \{a \in R : \varphi(a) = 0\}.$$

首先，如果

$$a, b \in \ker \varphi,$$

那么：

$$\varphi(a) = 0, \qquad \varphi(b) = 0.$$

于是：

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0.$$

所以：

$$a - b \in \ker \varphi.$$

这说明它是加法子群。

再看吸收性。

如果：

$$a \in \ker \varphi, \qquad r \in R,$$

那么：

$$\varphi(ra) = \varphi(r)\varphi(a).$$

因为：

$$\varphi(a) = 0,$$

所以：

$$\varphi(ra) = \varphi(r) \cdot 0 = 0.$$

因此：

$$ra \in \ker \varphi.$$

所以：

$$\boxed{\ker \varphi \text{ 是 } R \text{ 的理想}}$$

现在再回头看域 K。

假设：

$$I \subseteq K$$

是一个理想，而且里面有一个非零元素：

$$a \in I, \qquad a \neq 0.$$

因为 K 是域，所以：

$$a^{-1} \in K.$$

而理想有吸收性，所以既然

$$a \in I$$

且

$$a^{-1} \in K,$$

就必须有：

$$a^{-1}a \in I.$$

但：

$$a^{-1}a = 1.$$

所以：

$$1 \in I.$$

接下来任取：

$$x \in K.$$

因为：

$$1 \in I,$$

又因为 $x \in K$，利用理想的吸收性：

$$x \cdot 1 \in I.$$

于是：

$$x \in I.$$

所以整个 K 都在 I 里：

$$I = K.$$

因此域只有两个理想：

$$\boxed{\{0\}, \quad K}.$$

这就是前面那个结论的完整背景。

9.3 域的理想为什么只有零理想和整个域

这里是在解释：**为什么域 K 只有两个理想：$\{0\}$ 和整个 K**。

假设 I 是 K 的一个理想，而且 I 里有某个非零元素

$$a \in I, \qquad a \neq 0.$$

理想有一个关键性质：

$$\boxed{a \in I,\, r \in K \quad \Longrightarrow \quad ra \in I}$$

也就是说，**理想里的元素乘上环（这里是域）中的任意元素，结果还必须留在理想里**。

因为 K 是域，而 $a \neq 0$，所以 a 有逆元：

$$a^{-1} \in K.$$

现在在上面的理想性质里取

$$r = a^{-1}.$$

因为 $a \in I$，所以

$$a^{-1}a \in I.$$

但

$$a^{-1}a = 1.$$

所以：

$$\boxed{1 \in I}.$$

这一步就是你选中的那句话的意思。

然后一旦 $1 \in I$，事情就结束了。因为任取一个

$$x \in K,$$

利用理想的性质：

$$x \cdot 1 \in I.$$

而

$$x \cdot 1 = x.$$

所以任意 $x \in K$ 都属于 I。

因此：

$$I = K.$$

所以一个域里的理想只有两种可能：

$$\boxed{I = \{0\}}$$

或者，只要它含有任意一个非零元素，就立即变成：

$$\boxed{I = K}.$$

这也就是前面说“域同态的核只能是 $\{0\}$ 或整个域”的根本原因。

9.4 完整验证 $\mathbb{Q}(\sqrt{2})$ 的元素形式

现在就把这件事彻底讲清楚：

$$\boxed{\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}}$$

为什么正好是这种形式？

先从“加入 $\sqrt{2}$”是什么意思说起。

我们原来只有：

$$\mathbb{Q}.$$

现在要求新的域里还必须有：

$$\sqrt{2}.$$

既然它是域，就必须对四则运算封闭。

所以至少会产生：

$$1 + \sqrt{2}, \quad 3\sqrt{2}, \quad \frac{5}{2} - 7\sqrt{2}$$

等等。

这些显然都属于：

$$a + b\sqrt{2}.$$

关键问题是：

> 继续乘、除以后，会不会出现 $(\sqrt{2})^2, (\sqrt{2})^3$ 之类，从而需要更高次项？

先看乘法。

设

$$x = a + b\sqrt{2},$$

$$y = c + d\sqrt{2}.$$

那么：

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}).$$

展开：

$$= ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2.$$

但：

$$(\sqrt{2})^2 = 2.$$

所以：

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

仍然是：

$$\boxed{\text{有理数} + \text{有理数} \cdot \sqrt{2}}.$$

高次项自动被压回来了。

例如：

$$(\sqrt{2})^3 = 2\sqrt{2},$$

$$(\sqrt{2})^4 = 4.$$

所以根本不需要保留：

$$(\sqrt{2})^2, (\sqrt{2})^3, \dots$$

作为新的独立东西。

加减更简单：

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

仍然是同样形式。

取负号：

$$-(a + b\sqrt{2}) = -a - b\sqrt{2}.$$

也还是同样形式。

真正需要检查的是除法。

假设：

$$a+b\sqrt{2}\neq 0.$$

我们希望：

$$\frac{1}{a+b\sqrt{2}}$$

仍然写成：

$$c+d\sqrt{2}.$$

方法就是乘共轭：

$$\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}.$$

得到：

$$\frac{a-b\sqrt{2}}{a^2-2b^2}.$$

因为：

$$a,b\in\mathbb{Q},$$

所以：

$$a^2-2b^2\in\mathbb{Q}.$$

而且只要

$$a+b\sqrt{2}\neq 0,$$

这个分母不会为 0。

因此：

$$\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

两个系数仍然都是有理数。

所以逆元仍然属于这个集合。

于是：

$$\{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$$

确实是一个域。

而且它包含：

$$\mathbb{Q}$$

和

$$\sqrt{2}.$$

因此它就是“包含 $\mathbb{Q}$ 和 $\sqrt{2}$ 的最小域”：

$$\boxed{\mathbb{Q}(\sqrt{2})}.$$

这里“最小”很重要，意思不是数值大小，而是：

> 只加入为了保证域运算不得不加入的东西，不额外加入别的数。

比如：

$$\pi$$

当然也可以和 $\sqrt{2}$ 一起放进一个更大的域，但仅仅从 $\mathbb{Q}$ 加入 $\sqrt{2}$，并不会被迫得到 π。

现在再看一个很重要的结构。

$$\mathbb{Q}(\sqrt{2})$$

里的每个数都能唯一写成：

$$a + b\sqrt{2}.$$

这里实际上只有两个“基本方向”：

$$1, \qquad \sqrt{2}.$$

所以我们常写：

$$\mathbb{Q}(\sqrt{2}) = \mathrm{span}_{\mathbb{Q}}\{1, \sqrt{2}\}.$$

它作为一个 $\mathbb{Q}$–向量空间，维数是：

$$2.$$

于是定义：

$$\boxed{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2}$$

这个数字叫：

$$\boxed{\text{域扩张的次数 } \mathbf{degree}}$$

直觉上就是：

> 从 $\mathbb{Q}$ 扩张到 $\mathbb{Q}(\sqrt{2})$，需要两个基底方向 $1, \sqrt{2}$。

这一步非常关键，因为后面如果加入一个满足三次不可约方程的数，扩张次数可能是 3；加入五次根，次数也可能变化。

下一步最自然的是讲：

$$\boxed{\text{什么是代数元、最小多项式，以及为什么扩张次数等于最小多项式的次数}}$$

因为 $\sqrt{2}$ 之所以只需要 $1, \sqrt{2}$，根本原因就是它满足：

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

9.5 代数元、最小多项式、扩张次数

现在讲三个紧密相关的概念：

$$\boxed{\text{代数元}} \quad \to \quad \boxed{\text{最小多项式}} \quad \to \quad \boxed{\text{扩张次数}}$$

先用 $\sqrt{2}$ 这个最熟悉的例子。

我们知道：

$$\sqrt{2}$$

满足

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

而这个多项式的系数都在 $\mathbb{Q}$ 里。

所以我们说：

$$\boxed{\sqrt{2}\text{ 是 }\mathbb{Q}\text{ 上的代数元}}$$

更一般地，如果一个数 α 满足某个非零多项式方程

$$a_n\alpha^n+\cdots+a_1\alpha+a_0=0$$

其中

$$a_i\in F,$$

那么称：

$$\boxed{\alpha\text{ 是域 }F\text{ 上的代数元}}$$

英文是 algebraic element。

例如：

$$\sqrt{2}$$

是 $\mathbb{Q}$ 上的代数元；

$$\sqrt[3]{2}$$

也是，因为它满足

$$x^3-2=0.$$

而像 π,e 相对于 $\mathbb{Q}$ 则不是代数元，它们是超越数。

但一个数通常会满足很多多项式。

比如 $\sqrt{2}$ 满足：

$$x^2 - 2 = 0,$$

当然也满足：

$$(x^2 - 2)(x + 7) = 0,$$

即：

$$x^3 + 7x^2 - 2x - 14 = 0.$$

甚至还满足：

$$(x^2 - 2)^5 = 0.$$

所以仅仅说“它满足一个多项式”信息太多、太冗余。

我们真正想找的是：

> 最简单、最低次数的那个多项式。

对 $\sqrt{2}$，就是：

$$x^2 - 2.$$

这个多项式叫：

$$\boxed{\sqrt{2} \text{ 在 } \mathbb{Q} \text{ 上的最小多项式}}$$

英文：

> minimal polynomial

正式一点说，如果 α 是 F 上的代数元，那么它的最小多项式 $m_\alpha(x)$ 是：

$$\boxed{\text{系数在 } F \text{ 中、首一、次数最低，并且满足 } m_\alpha(\alpha)=0 \text{ 的多项式}}$$

“首一”就是最高次项系数取 1。

例如：

$$m_{\sqrt{2}}(x)=x^2-2.$$

为什么不能有一次多项式?

如果有：

$$x-a=0,\qquad a\in\mathbb{Q},$$

那么就意味着：

$$\sqrt{2}=a\in\mathbb{Q},$$

矛盾。

所以最低次数确实是 2。

现在看：

$$\sqrt[3]{2}.$$

它满足：

$$x^3 - 2 = 0.$$

如果这个多项式在 $\mathbb{Q}$ 上不可约，那么它就是最小多项式。

这里的“不可约”意思是：

> 不能在 $\mathbb{Q}[x]$ 里分解成两个次数都更低的非恒定多项式。

对于：

$$x^3 - 2,$$

如果它在 $\mathbb{Q}$ 上可约，因为它是三次多项式，就一定有一个有理根。

但有理根只能是：

$$\pm 1, \pm 2,$$

都不成立。

所以它不可约。

因此：

$$m_{\sqrt[3]{2}}(x) = x^3 - 2.$$

现在来到最重要的结论。

如果：

$$m_\alpha(x)$$

在 F 上的次数是：

$$n,$$

那么：

$$F(\alpha)$$

里的每个元素都可以唯一写成：

$$\boxed{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}$$

其中：

$$a_i \in F.$$

为什么只需要到 α^{n-1}？

因为最小多项式给了一个关系：

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0.$$

所以：

$$\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_0.$$

也就是说：

$$\boxed{\alpha^n \text{ 可以用更低次幂表示}}$$

于是：

$$\alpha^{n+1}, \alpha^{n+2}, \ldots$$

也都能不断降次。

例如 $\sqrt{2}$ 满足：

$$\alpha^2 = 2,$$

所以任何高次幂都只能化成：

$$a + b\alpha.$$

而 $\sqrt[3]{2}$ 满足：

$$\alpha^3 = 2.$$

所以任何元素都可以化成：

$$a + b\alpha + c\alpha^2.$$

也就是：

$$\boxed{\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}}$$

因此：

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

于是得到一个非常重要的定理：

$$\boxed{[F(\alpha) : F] = \deg m_\alpha(x)}$$

也就是：

> 加入一个代数元后，域扩张的次数，等于这个元素最小多项式的次数。

例如：

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2,$$

因为：

$$m_{\sqrt{2}}(x)=x^2-2.$$

而：

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3,$$

因为：

$$m_{\sqrt[3]{2}}(x)=x^3-2.$$

下一步最自然的是讲：

$$\boxed{\text{如果连续加入多个数，扩张次数怎样相乘}}$$

也就是塔式定理：

$$[K:F]=[K:E][E:F].$$

这会直接帮助我们理解“不断加入根式”的结构。

补充证明：最小多项式为什么不可约，为什么给出扩张次数

F 是域，α 是 F 上的代数元。存在非零多项式使它为零，因此在所有这类多项式中选次数最小的，并除以首项系数，得到首一多项式 m。若 $m = uv$，其中 u, v 都是正次数，则 $0 = m(\alpha) = u(\alpha)v(\alpha)$，在域中必有一个因子为零，违反最小次数。所以 m 不可约。

多项式除法表明：若 $p(\alpha) = 0$，把 p 除以 m 得 $p = qm + r$，$\deg r < \deg m$。代入 α 后 $r(\alpha) = 0$，最小性迫使 $r = 0$。因此所有在 α 处为零的多项式恰好是 m 的倍数，也证明首一最小多项式唯一。

设 $d = \deg m$。任何多项式表达式都能化简为 1、α、…、α^{d-1} 的 F 线性组合。还要检查除法不会跑出去：若 $q(\alpha) \neq 0$，则不可约的 m 与 q 互素；多项式 Euclid 算法给出 $u\,q + v\,m = 1$，所以 $q(\alpha)^{-1} = u(\alpha)$。于是这些多项式表达式已是一个域，即 $F[\alpha] = F(\alpha)$。

若这 d 个元素线性相关，就存在次数小于 d 的非零多项式使 α 为零，矛盾。因此它们是一组基，$[F(\alpha) : F] = d$。这也解释“生成元”不能直接当作向量空间的基。

这里用到的多项式 Euclid 算法：重复带余除法，余数次数严格下降，最后非零余数为最大公因式；从最后一步逆向代入，就把最大公因式写成两个原多项式的组合。互素时该组合可归一化为 1。

原例子的有理根定理也可以直接检查：若互素整数 p, q 的比 p/q 是整系数多项式 $a_d x^d + \ldots + a_0$ 的根，乘以 q^d 后，p 整除 $a_0 q^d$，q 整除 $a_d p^d$。因 p, q 互素，得到 $p \mid a_0$、$q \mid a_d$；首一时 $q = \pm 1$。因此 $x^3 - 2$ 的有理根只可能是 ±1、±2。

补充例子：$\sqrt{2}$ 不在 $\mathbb{Q}$，$\sqrt{3}$ 不在 $\mathbb{Q}(\sqrt{2})$

若 $\sqrt{2} = p/q$，取互素整数 p, q，则 $p^2 = 2q^2$，p 必为偶数；写 $p = 2r$ 后 $q^2 = 2r^2$，q 也为偶数，矛盾。

若 $\sqrt{3} = a + b\sqrt{2}$，$a, b \in \mathbb{Q}$，平方得 $3 = a^2 + 2b^2 + 2ab\sqrt{2}$。因 $\sqrt{2}$ 无理，$ab = 0$。若 $b = 0$，则 $a^2 = 3$；若 $a = 0$，则 $b^2 = 3/2$。两者都不可能是有理数的平方：一个有理数平方的约分分子和分母中，各素因子的指数都是偶数，而 3、3/2 不满足。因此 $\sqrt{3}$ 不在 $\mathbb{Q}(\sqrt{2})$，原塔式定理例子中的第二层确实是二次扩张。

9.7 塔式定理的乘积基构造

现在讲**塔式定理（tower law）**，它回答一个很自然的问题：

> 如果不是一次只加入一个数，而是连续扩张几次，最终扩张次数怎么计算？

假设有三层域：

$$F \subset E \subset K.$$

如果

$$[E : F] = m,$$

而

$$[K : E] = n,$$

那么：

$$\boxed{[K : F] = [K : E]\,[E : F] = nm}$$

这就是塔式定理。

先不急着证明，先看一个具体例子。

从

$$\mathbb{Q}$$

开始，先加入：

$$\sqrt{2}.$$

得到：

$$E = \mathbb{Q}(\sqrt{2}).$$

我们已经知道：

$$[E : \mathbb{Q}] = 2,$$

因为一个基可以取：

$$\{1, \sqrt{2}\}.$$

现在再加入：

$$\sqrt{3}.$$

得到：

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

现在我们把 K 看成是在 E 上加入 $\sqrt{3}$：

$$K = E(\sqrt{3}).$$

如果 $\sqrt{3} \notin E$，那么它在 E 上仍然满足：

$$x^2 - 3 = 0,$$

而且这个多项式在 E 上仍不可约，于是：

$$[K : E] = 2.$$

所以塔式定理告诉我们：

$$[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 2 \times 2 = 4.$$

因此：

$$\boxed{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4}$$

这和我们直接观察也一致。

因为这个域里的元素都可以写成：

$$(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3},$$

展开：

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

所以：

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}.$$

它在 $\mathbb{Q}$ 上有四个基本方向：

$$1, \quad \sqrt{2}, \quad \sqrt{3}, \quad \sqrt{6}.$$

因此维数确实是 4。

现在解释为什么塔式定理成立。

假设：

$$[E:F]=m,$$

取 E 在 F 上的一组基：

$$e_1,\dots,e_m.$$

也就是说，任意 $e\in E$ 都能唯一写成：

$$e=a_1e_1+\cdots+a_me_m,\qquad a_i\in F.$$

再假设：

$$[K:E]=n,$$

取 K 在 E 上的一组基：

$$k_1,\dots,k_n.$$

那么任意 $x\in K$ 可以写成：

$$x=b_1k_1+\cdots+b_nk_n,\qquad b_j\in E.$$

但每个 b_j 又能写成：

$$b_j=\sum_{i=1}^{m}a_{ij}e_i,\qquad a_{ij}\in F.$$

代回去：

$$x = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} e_i \right) k_j.$$

整理：

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} (e_i k_j).$$

所以从 F 的角度看，K 可以由这些元素张成：

$$e_i k_j.$$

一共有：

$$mn$$

个。

进一步可以证明它们线性无关，因此它们正好构成 K 在 F 上的一组基。

于是：

$$\boxed{[K : F] = mn}.$$

这件事为什么对“根式解”重要？

因为所谓根式解，本质上就是建立一座这样的塔：

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r,$$

每一步都通过加入一个根式：

$$F_{i+1} = F_i(\alpha_i),$$

其中：

$$\alpha_i^{n_i} \in F_i.$$

比如：

$$\alpha_i = \sqrt[n_i]{a_i}.$$

所以根式解不是一句模糊的“用了几次开方”，而是：

> 存在一串通过加入根式得到的域扩张，使方程的根最终落在最上面的域里。

这就是以后“根式可解”严格定义的基础。

下一步最自然的是进入另一个核心概念：

> 分裂域（splitting field）

因为一个多项式可能不止一个根，而 Galois 理论真正关心的是：

> **把这个多项式的所有根都加入以后得到的最小域。**

补充证明：塔式定理中乘积基的线性无关性

原对话证明了 $e_i k_j$ 张成 K，下面补齐线性无关。若

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij} e_i\right) k_j = 0, \qquad a_{ij} \in F,$$

由于 $k_1, \dots, k_n$ 在 E 上线性无关，每个括号均为 0；由于 $e_1, \dots, e_m$ 在 F 上线性无关，每个 $a_{ij} = 0$。所以乘积集合是一组基，$[K : F] = [K : E][E : F]$。

第 10 章：域同态、嵌入、自同构和 Galois 群

本章对象：本篇域同态要求把 1 映到 1。$\sigma : K \to L$ 是域映射；域同态的核映到 0，Galois 群同态的核映到恒等自同构。

10.1 嵌入的单射条件

> 原问题：所以嵌入就是要求是单射吗

对。

在域论里，**嵌入（embedding）通常就是指一个保持域结构的单射同态**。

也就是说，一个映射

$$\sigma : K \to L$$

如果满足：

$$\sigma(a+b) = \sigma(a) + \sigma(b),$$

$$\sigma(ab) = \sigma(a)\sigma(b),$$

$$\sigma(1) = 1,$$

并且还是**单射**，那它就是一个域嵌入。

所以你可以先记成：

$$\boxed{\text{域嵌入} = \text{保持加法乘法的单射}}$$

之所以强调“单射”，是因为它要把原来的域 K 原封不动地“放进”另一个域 L 里，不能把两个不同元素压成同一个。

其实对域来说，只要是非零的域同态，单射往往是自动的。因为如果

$$\sigma(a) = \sigma(b),$$

那么

$$\sigma(a - b) = 0.$$

而域同态的核只能是

$$\{0\}$$

或者整个域；但又因为

$$\sigma(1) = 1 \neq 0,$$

所以不可能整个域都进核，因此只能

$$a - b = 0,$$

也就是

$$a = b.$$

所以域同态天然几乎就是嵌入。

10.2 域同态的核与乘法群同态的核

> 原问题：为什么，此外域同态的核，指的是加法的还是乘法的

对，这里有两个容易混淆的“核”，你问得很关键。

这里说的**域同态的核**，指的是把域同态看成一个**加法群同态**时的核，也就是：

$$\boxed{\ker \varphi = \{a \in K : \varphi(a) = 0\}}$$

这里对应的是目标域的**加法单位元** 0，不是乘法单位元 1。

假设

$$\varphi : K \to L$$

是域同态。

为什么它的核只能是

$$\{0\}$$

或者整个 K？

先假设核里出现了某个非零元素：

$$a \neq 0, \qquad a \in \ker \varphi.$$

那么：

$$\varphi(a) = 0.$$

因为 K 是**域**，任何非零 a 都有乘法逆元：

$$a^{-1} \in K.$$

于是：

$$a^{-1}a = 1.$$

对两边作用 φ：

$$\varphi(a^{-1}a) = \varphi(1).$$

因为域同态保持乘法：

$$\varphi(a^{-1})\varphi(a) = 1.$$

但我们已经知道：

$$\varphi(a) = 0.$$

所以左边变成：

$$\varphi(a^{-1}) \cdot 0 = 0.$$

于是得到：

$$0 = 1.$$

矛盾。

因此，只要 φ 是正常的域同态（特别是 $\varphi(1) = 1$），就不可能有任何非零元素进入核。

所以：

$$\boxed{\ker \varphi = \{0\}}$$

因此域同态自动是单射。

你可能会问：

> 那为什么刚才还说“核只能是 $\{0\}$ 或整个域”？

这是从更一般的**环同态/理想**角度说的。

核有一个性质：如果

$$a \in \ker \varphi$$

而

$$r \in K,$$

那么：

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0.$$

所以：

$$ra \in \ker \varphi.$$

这种对子集的要求叫做**理想（ideal）**。

而一个域只有两个理想：

$$\boxed{\{0\} \quad \text{和} \quad K}.$$

原因也正是刚才那个逆元论证：如果一个理想里包含任何非零 a，因为 $a^{-1} \in K$，就有

$$a^{-1}a = 1$$

也在理想里；一旦理想包含 1，那么任意

$$x = x \cdot 1$$

都在理想里，因此它就是整个 K。

至于你问“有没有乘法的核”，确实也可以考虑：

$$K^\times \to L^\times$$

这个**乘法群同态**。

这时群论意义下的核是：

$$\{a \in K^\times : \varphi(a) = 1\}.$$

这是另一回事。

所以一定要区分：

$$\boxed{\text{域/环同态的核：}\ \varphi(a) = 0}$$

因为这里关注的是加法零元；

而

$$\boxed{\text{乘法群同态的核：}\ \varphi(a) = 1}$$

因为乘法群的单位元是 1。

我们刚才证明“域同态自动单射”时，用的是前一种：

$$\boxed{\ker \varphi = \{a : \varphi(a) = 0\}}.$$

10.3 域自同构与 Galois 群

现在进入 Galois 理论真正的核心概念：

$$\boxed{\text{域自同构（}\mathbf{field\ automorphism}\text{）}}$$

先不要急着碰 $x^3 - 2$。我们从最简单的

$$\mathbb{Q}(\sqrt{2})$$

开始。

一个“域自同构”可以先理解成：

> **把这个域里的元素重新对应到这个域里的元素，同时完全保持加法和乘法结构。**

也就是说，一个映射

$$\sigma : K \to K$$

如果满足

$$\sigma(a+b) = \sigma(a) + \sigma(b),$$

$$\sigma(ab) = \sigma(a)\sigma(b),$$

并且是双射，那么它就是 K 的一个域自同构。

但在 Galois 理论里我们通常还会指定一个基础域，比如 $\mathbb{Q}$，要求：

$$\boxed{\sigma(q) = q \qquad \forall q \in \mathbb{Q}}$$

也就是说，所有有理数必须原封不动。

这叫：

$$\boxed{\mathbb{Q}\text{-自同构}}$$

现在研究：

$$K = \mathbb{Q}(\sqrt{2}).$$

里面任何元素都是：

$$a + b\sqrt{2}, \qquad a, b \in \mathbb{Q}.$$

如果 σ 固定所有有理数，那么

$$\sigma(a) = a, \qquad \sigma(b) = b.$$

所以：

$$\sigma(a + b\sqrt{2}) = a + b\,\sigma(\sqrt{2}).$$

因此你会发现：

> 整个 σ 怎么作用，其实完全由它把 $\sqrt{2}$ 送到哪里决定。

那 $\sqrt{2}$ 能被送到哪里？

因为：

$$(\sqrt{2})^2 = 2.$$

自同构必须保持乘法，所以：

$$\sigma((\sqrt{2})^2) = \sigma(2).$$

左边：

$$\sigma((\sqrt{2})^2) = \sigma(\sqrt{2})^2.$$

右边因为 $2 \in \mathbb{Q}$，而 σ 固定 $\mathbb{Q}$，所以：

$$\sigma(2) = 2.$$

因此：

$$\sigma(\sqrt{2})^2 = 2.$$

所以：

$$\sigma(\sqrt{2})$$

只能是方程

$$x^2 - 2 = 0$$

的根。

也就是：

$$\boxed{\sigma(\sqrt{2}) = \sqrt{2} \quad \text{或} \quad -\sqrt{2}}$$

这很重要。

因此 $\mathbb{Q}(\sqrt{2})$ 有两个固定 $\mathbb{Q}$ 的自同构。

第一个是什么都不做：

$$\sigma_1(\sqrt{2}) = \sqrt{2}.$$

于是：

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}.$$

这就是恒等自同构：

$$e.$$

第二个把：

$$\sqrt{2} \mapsto -\sqrt{2}.$$

于是：

$$\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}.$$

比如：

$$3 + 5\sqrt{2}$$

被送到：

$$3 - 5\sqrt{2}.$$

这看起来很像我们熟悉的“共轭”。

所以：

$$\boxed{\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{e, \sigma\}}$$

其中：

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

这个群有两个元素。

而且：

$$\sigma^2 = e.$$

所以它和一个 2 元循环群本质上一样。

现在最关键的问题来了：

> 为什么自同构一定把一个多项式的根送到另一个根？

假设：

$$f(x) = a_n x^n + \cdots + a_0$$

其中所有：

$$a_i \in \mathbb{Q}.$$

假设：

$$f(\alpha) = 0.$$

也就是：

$$a_n\alpha^n + \cdots + a_0 = 0.$$

现在对两边作用 σ：

$$\sigma(a_n\alpha^n + \cdots + a_0) = \sigma(0).$$

因为 σ 保持加法和乘法，而且固定所有 $a_i \in \mathbb{Q}$，所以：

$$a_n\sigma(\alpha)^n + \cdots + a_0 = 0.$$

也就是：

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

因此：

$$\boxed{\alpha \text{ 是根} \Longrightarrow \sigma(\alpha) \text{ 仍然是根}}$$

这一步就是“域自同构”和“根的置换”之间真正的桥。

现在再回头看：

$$x^2 - 2.$$

它的两个根是：

$$\sqrt{2}, \quad -\sqrt{2}.$$

一个固定 $\mathbb{Q}$ 的自同构只能：

- 固定两个根；
- 或交换两个根。

所以这些自同构实际上就是在置换根。

这就是为什么 Galois 群天然是一个置换群。

接下来再看：

$$x^3 - 2.$$

它的分裂域是：

$$K = \mathbb{Q}(\alpha, \omega),$$

其中：

$$\alpha = \sqrt[3]{2},$$

三个根是：

$$\alpha, \quad \omega\alpha, \quad \omega^2\alpha.$$

如果 σ 是一个固定 $\mathbb{Q}$ 的 K 的自同构，那么因为

$$\alpha^3 = 2,$$

所以：

$$\sigma(\alpha)^3 = 2.$$

因此：

$$\sigma(\alpha)$$

只能是三个根之一：

$$\alpha, \quad \omega\alpha, \quad \omega^2\alpha.$$

所以自同构一定会重新排列这三个根。

于是终于得到定义：

$$\boxed{\mathrm{Gal}(K/F) = \{\text{所有固定 } F \text{ 的 } K \text{ 的域自同构}\}}$$

这就是：

$$\boxed{\text{Galois 群}}$$

它的元素不是“根本身”，而是：

$$\boxed{\text{保持基础域和所有代数运算不变时，对根允许进行的置换}}$$

下一步最适合具体算：

$$\boxed{\mathrm{Gal}(x^3 - 2/\mathbb{Q})}$$

到底为什么有 6 个元素，并且为什么它就是：

$$\boxed{S_3}.$$

这一步会把“域自同构”和我们最开始学的置换群真正合并起来。

第 11 章：分裂域、正规性与嵌入的延拓

本章对象：Ω 或 $\overline{F}$ 是包含所需代数元的代数闭包；$\tau : E \to \Omega$ 是固定 F 的嵌入，延拓 $\tilde{\tau} : K \to \Omega$ 要与 τ 在 E 上一致。

本节定义：特征、可分、正规与 Galois

特征 0 表示有限个 1 相加永远不等于 0；$\mathbb{Q}$ 及其所有扩张域都是特征 0。不可约多项式可分，表示它在代数闭包中没有重根。有限扩张 K/F 可分，表示其每个元素的最小多项式可分。K/F 正规，表示 $F[x]$ 中任何不可约多项式只要在 K 有一个根，就在 K 内完全分裂。有限扩张同时正规和可分，称为 Galois。

特征 0 中，正次数不可约多项式 p 的导数 p' 不为零，且次数更低。若 p 有重根，则 p 与 p' 有共同根，其最大公因式非平凡；p 不可约迫使 p 整除 p'，与次数矛盾。所以特征 0 下有限代数扩张自动可分。

补充证明：分裂域、正规性与嵌入稳定的关系

在代数闭包 Ω 中，若 K 是 F 上某多项式的分裂域，则任意固定 F 的嵌入 $\sigma : K \to \Omega$ 都把这些根送到同一多项式的根，所以 $\sigma(K) \subseteq K$。嵌入作为 F 线性映射保持维数，且 K/F 有限，因此 $\sigma(K) = K$。

反过来，若每个固定 F 的嵌入都把 K 映回自身，取 $\alpha \in K$ 及其最小多项式的任意根 $\beta \in \Omega$。映射 $\alpha \mapsto \beta$ 先给出 $F(\alpha) \to \Omega$ 的嵌入，再用下一节证明的延拓构造扩展到 K。因此 $\beta \in K$，最小多项式的全部根都在 K。故 K/F 正规。

因此，有限扩张的“正规”与“每个固定基础域的嵌入都把整个域映回自身”等价。上面的反向证明在延拓引理证明后即可逐步核查，正向用于分裂域时不依赖反向。

11.2 分裂域：把一个多项式的全部根加入

现在进入 **分裂域（splitting field）**。这个概念会第一次把“域”重新和前面讲过的“根的置换”接起来。

考虑一个多项式

$$f(x) \in F[x].$$

所谓它在 F 上的分裂域，就是：

> **从 F 出发，把 $f(x)$ 的所有根都加入以后得到的最小域。**

先看最简单的例子：

$$f(x) = x^2 - 2 \in \mathbb{Q}[x].$$

它的两个根是

$$\sqrt{2}, \qquad -\sqrt{2}.$$

加入 $\sqrt{2}$ 以后，我们得到

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

但是

$$-\sqrt{2}$$

本来就已经在这个域里，因为域对取负封闭。

所以：

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

已经能够在 $\mathbb{Q}(\sqrt{2})$ 中完全分解成一次因子。

因此：

$$\boxed{\mathbb{Q}(\sqrt{2}) \text{ 是 } x^2 - 2 \text{ 的分裂域}}$$

这里“splitting”就是“完全裂开成一次因子”的意思。

真正有意思的是三次方程：

$$x^3 - 2 = 0.$$

我们已经知道一个实根：

$$\alpha = \sqrt[3]{2}.$$

如果只加入它：

$$\mathbb{Q}(\alpha),$$

是不是就已经获得了三个根？

不是。

因为一个三次多项式在复数里有三个根。

我们来找另外两个。

方程：

$$x^3 = 2.$$

如果

$$\alpha^3 = 2,$$

那么只要找满足

$$\omega^3 = 1$$

的数，就有：

$$(\alpha\omega)^3 = \alpha^3\omega^3 = 2.$$

所以三个根实际上是：

$$\alpha, \qquad \alpha\omega, \qquad \alpha\omega^2,$$

其中

$$\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

而：

$$\omega^3 = 1, \qquad \omega \neq 1.$$

这就是一个三次单位根。

现在注意关键问题：

$$\mathbb{Q}(\sqrt[3]{2})$$

里的元素都是：

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}, \qquad a, b, c \in \mathbb{Q}.$$

这些全部都是**实数**。

所以：

$$\omega \notin \mathbb{Q}(\sqrt[3]{2}),$$

因为 ω 不是实数。

因此只加入一个根 $\sqrt[3]{2}$，并没有把另外两个根也自动带进来。

所以：

$$\boxed{\mathbb{Q}(\sqrt[3]{2}) \text{ 不是 } x^3-2 \text{ 的分裂域}}$$

我们还要加入：

$$\omega.$$

于是得到：

$$\boxed{K=\mathbb{Q}(\sqrt[3]{2},\omega)}$$

在这个域里，三个根：

$$\sqrt[3]{2}, \qquad \omega\sqrt[3]{2}, \qquad \omega^2\sqrt[3]{2}$$

全都存在。

因此：

$$x^3-2=(x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)$$

在 K 里完全分裂。

所以：

$$\boxed{\mathbb{Q}(\sqrt[3]{2},\omega) \text{ 是 } x^3-2 \text{ 的分裂域}}$$

这里有一个非常重要的区别。

加入**某一个根**得到：

$$F(\alpha).$$

但分裂域要求：

$$\boxed{\text{所有根都在里面}}$$

所以这两个东西不一定相同。

二次例子里恰好相同：

$$\mathbb{Q}(\sqrt{2})$$

既是“加入一个根的域”，也是分裂域。

三次例子里则不同：

$$\mathbb{Q}(\sqrt[3]{2}) \subsetneq \mathbb{Q}(\sqrt[3]{2}, \omega).$$

我们甚至可以算一下这个分裂域的次数。

首先：

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

然后加入 ω。

ω 满足：

$$\omega^2 + \omega + 1 = 0,$$

因为：

$$\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1) = 0$$

而 $\omega \neq 1$。

并且 $\omega \notin \mathbb{Q}(\sqrt[3]{2})$，所以它在这个实数域上仍然需要一个二次扩张。

因此：

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2.$$

根据塔式定理：

$$[K : \mathbb{Q}] = 2 \times 3 = 6.$$

所以：

$$\boxed{[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6}$$

这个数字 6 很快就会再次出现。

因为三个根有：

$$3! = 6$$

种可能置换。

而对于这个具体多项式，它的 Galois 群实际上正是：

$$S_3.$$

不过现在还差最后一个关键概念才能说清楚这句话：

$$\boxed{\text{域自同构 automorphism}}$$

也就是说：

> 在保持原来的有理数完全不动、同时保持加法和乘法关系的前提下，我们可以怎样重新排列这个分裂域里的元素？

一旦定义这个东西，“根的置换”就会从之前比较直观的想法，变成严格的 **Galois 群**。这就是下一步。

11.3 嵌入、代数闭包、延拓的对象类型

> 原问题：这一段都没看懂

可以，这一段确实一下子引入了太多新东西：**嵌入、代数闭包、延拓定理、$\tilde{\tau}$** 全挤在一起了。我们先全部拆开，而且暂时**不证明延拓定理**，只先弄懂它到底在说什么。

先回到最具体的场景：

$$F \subset E \subset K.$$

你可以把它想成：

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

这里：

$$F = \mathbb{Q},$$

$$E = \mathbb{Q}(\sqrt{2}),$$

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

现在在 E 上，我们有一个自同构：

$$\tau : E \to E$$

满足：

$$\tau(\sqrt{2}) = -\sqrt{2}.$$

这就是一个只定义在 E 上的“规则”。

也就是说，目前 τ 知道怎么处理：

$$a + b\sqrt{2},$$

因为：

$$\tau(a + b\sqrt{2}) = a - b\sqrt{2}.$$

但它还不知道怎么处理：

$$\sqrt{3},$$

因为：

$$\sqrt{3} \notin E.$$

所以目前：

$$\tau$$

只定义在小域 E 上。

我们现在想做的是：

> 能不能把这个规则扩展到整个更大的域 K？

也就是说，希望找到一个新映射：

$$\widetilde{\tau} : K \to K$$

满足：

$$\widetilde{\tau}|_E = \tau.$$

这里：

$$\widetilde{\tau}$$

读作“tau tilde”，可以理解成：

> τ 的扩展版。

而

$$\widetilde{\tau}|_E = \tau$$

意思是：

> 虽然 $\widetilde{\tau}$ 定义在整个 K 上，但如果只看它在 E 里的作用，它和原来的 τ 完全一样。

比如我们可以定义：

$$\tilde{\tau}(\sqrt{2}) = -\sqrt{2},$$

同时规定：

$$\tilde{\tau}(\sqrt{3}) = \sqrt{3}.$$

这样就把原本只会处理 $\sqrt{2}$ 的 τ，扩展成了一个还能处理 $\sqrt{3}$ 的映射。

这就是：

$$\boxed{\text{延拓 extension}}$$

最核心的意思。

那“嵌入 embedding”又是什么？

其实你现在可以先把它理解成：

> 一个保持加法、乘法，而且不会把两个不同元素压成同一个元素的域映射。

比如：

$$\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$

满足：

$$\sqrt{2} \mapsto -\sqrt{2}$$

就是一个嵌入。

因为它保持：

$$+, \times$$

这些代数结构。

“自同构”其实就是一种特殊的嵌入：

$$\boxed{\text{自同构} = \text{从一个域到它自己的双射嵌入}}$$

所以“嵌入”是更宽一点的概念。

那为什么前面突然写：

$$\widetilde{\tau} : K \to \overline{F}$$

而不是直接：

$$\widetilde{\tau} : K \to K?$$

因为一般的延拓定理，第一步只能保证：

> 可以把 τ 扩展成一个定义在 K 上的嵌入，但它的像暂时可能落到一个更大的世界里。

这个更大的世界就是：

$$\overline{F}.$$

这里的横线：

$$\overline{F}$$

表示：

$$\boxed{F \text{ 的代数闭包 } \textbf{algebraic closure}}$$

你现在不需要掌握正式定义，可以先把它理解成：

> 一个足够大的域，里面包含了所有在 F 上代数的数，也就是各种多项式的根。

比如：

$$F = \mathbb{Q}.$$

那么：

$$\overline{\mathbb{Q}}$$

里面会有：

$$\sqrt{2}, \quad \sqrt{3}, \quad i, \quad \sqrt[3]{2}, \quad \omega,$$

等等所有代数数。

所以它相当于提供一个“足够大的容器”，保证我们扩展映射时不会因为目标元素没地方放而卡住。

因此那句话：

$$\widetilde{\tau} : K \to \overline{F}$$

其实只是说：

> 原来只定义在 E 上的 τ，可以扩展成一个定义在整个 K 上的映射；为了保险，我们先允许它把 K 中的元素送到一个足够大的域 $\overline{F}$ 中。

而：

$$\widetilde{\tau}|_E = \tau$$

就是：

> 这个扩展不会改变原来已经规定好的行为。

比如原来：

$$\tau(\sqrt{2}) = -\sqrt{2},$$

那么延拓以后仍然必须有：

$$\widetilde{\tau}(\sqrt{2}) = -\sqrt{2}.$$

它不能突然反悔。

现在再看我们为什么最终还是希望：

$$\widetilde{\tau}(K) = K.$$

因为如果我们要让：

$$\widetilde{\tau}$$

成为 K 的**自同构**，那它必须把 K 映回 K 自己。

而不能出现：

$$K \longrightarrow \text{外面另一个域}.$$

这时候：

$$K/F \text{ 是 Galois}$$

就会发挥作用。

它保证这种固定 F 的嵌入实际上不会把整个 K 搬到外面去，而是：

$$\boxed{\widetilde{\tau}(K) = K}.$$

于是：

$$\widetilde{\tau} : K \to K$$

就真的成为 K 的自同构了。

所以把那整段压缩成一句直白的话：

$$\boxed{\text{一个只定义在中间域 } E \text{ 上的自同构，通常可以向上扩展到更大的 } K。}$$

第一步先允许它映到一个很大的容器：

$$\overline{F}.$$

如果：

$$K/F$$

是 Galois，那么扩展后的映射实际上还会把 K 留在 K 里面，于是变成：

$$K \text{ 的自同构.}$$

你现在最值得抓住的不是“代数闭包”的正式定义，而是这条逻辑：

$$\boxed{E \text{ 上的自同构} \to \text{扩展到 } K \to \text{Galois 保证最后仍落在 } K}$$

下一步如果继续，我建议先不讲一般的延拓定理证明，而是先解释：**为什么“K/F 是 Galois”会保证这些嵌入把 K 映回自己。** 这会更容易接上你现在的理解。

11.4 单个代数元上的嵌入延拓构造

下一步我建议**先不要继续往“根式塔 → 可解群”走**，而是把我们刚才留下的那个真正缺口补掉：

$$\boxed{\text{为什么一个 } E \text{ 上的嵌入能够继续延拓到 } K}$$

我们刚才只是把“延拓定理”当成现成结论用了，但你已经开始追问它为什么成立，所以最好把它拆开证明。

下一步会按这个顺序来：

$$E \subset E(\alpha)$$

假设已经有一个嵌入

$$\tau : E \to \overline{F}.$$

我们要研究：

> 如果再加入一个代数元 α，怎样把 τ 扩展到 $E(\alpha)$?

核心会发现：

如果 α 的最小多项式是

$$m_\alpha(x) \in E[x],$$

那么延拓后的映射必须把

$$\alpha$$

送到一个满足“系数已经经过 τ 变换后的多项式”的根。

也就是说，我们会第一次看到类似

$$m_\alpha(x) = a_0 + a_1 x + \cdots + a_n x^n$$

经过 τ 后变成

$$\tau(m_\alpha)(x) = \tau(a_0) + \tau(a_1)x + \cdots + \tau(a_n)x^n.$$

然后只要在代数闭包 $\overline{F}$ 里挑它的一个根 β，就可以定义

$$\widetilde{\tau}(\alpha) = \beta.$$

再由

$$E(\alpha)$$

里的每个元素都是由 E 和 α 生成的，就能把整个 $\widetilde{\tau}$ 定下来。

所以**下一步真正要学的是：**

“向一个代数元延拓嵌入”的具体构造

这比直接背“延拓定理”重要得多。学完这一小步，再把它重复有限次，就能理解为什么从 E 能一路延拓到整个有限扩张 K。

补充证明：嵌入怎样延拓到一个代数元，再延拓到有限扩张

Ω 是含 F 的代数闭包；E/F 是代数扩张，α 在 E 上代数。给定固定 F 的嵌入 $\tau : E \to \Omega$，设 $m(x)$ 是 α 在 E 上的首一最小多项式。$\tau(m)$ 表示只对系数作用 τ。它在 $\tau(E)[x]$ 中仍不可约：若分解，把系数用 τ 的逆映回 E，就得到 m 的分解，矛盾。

在 Ω 中选 $\tau(m)$ 的一个根 β。$E(\alpha)$ 的每个元素有唯一形式 $\sum_{j=0}^{d-1} c_j \alpha^j$，定义

$$\widetilde{\tau}\left(\sum_{j=0}^{d-1} c_j \alpha^j\right) = \sum_{j=0}^{d-1} \tau(c_j)\beta^j.$$

唯一表示保证没有表达式歧义。该映射保持加法。乘法时先把两多项式相乘，再除以 m 化简；在目标中对应除以 $\tau(m)$，因为 $\tau(m)(\beta) = 0$，得到同一个结果。因此保持乘法并把 1 送到 1。非零域同态自动单射，所以得到 $E(\alpha) \to \Omega$ 的嵌入，且限制到 E 等于 τ。

若 K/E 有限，选一组有限基 $b_1, \dots, b_s$，则 $K = E(b_1, \dots, b_s)$；逐次把嵌入延拓到这些代数元，就得到 $K \to \Omega$ 的嵌入。若 K/F 正规，嵌入像等于 K，因而是 K 的 F 自同构。这给出限制映射满射所需的完整证明，而不只是把“延拓定理”作为口号引用。

补充证明：为什么有限 Galois 群的元素个数等于扩张次数

若 $E \to \Omega$ 的嵌入已固定，加入可分代数元 α 时，上述延拓恰好由 $\tau(m)$ 的不同根决定，一共有 $\deg m = [E(\alpha) : E]$ 种。沿有限生成塔逐层计数，得到固定 F 的 $K \to \Omega$ 嵌入数等于各层次数的乘积，即 $[K : F]$。若 K/F 正规，每个这样的嵌入都变成 K 的自同构。因此 $|\mathrm{Gal}(K/F)| = [K : F]$。这说明通过维数计算群的大小需要可分、正规条件，而不能任意套到非正规扩张。

11.6 正规性为什么让嵌入变回自同构

关键是：**Galois 扩张里的“normal（正规）”性质，恰好保证所有共轭根都已经在 K 里面。**

我们一步一步看。

假设

$$K/F$$

是有限 Galois 扩张。这里真正起作用的是：

$$\boxed{K/F \text{ 是正规扩张}}$$

Galois = 正规 + 可分；这里暂时只需要“正规”。

假设 $\alpha \in K$。

因为 α 是 F 上的代数元，它有一个在 F 上的最小多项式：

$$m_\alpha(x) \in F[x].$$

而：

$$m_\alpha(\alpha) = 0.$$

现在有一个固定 F 的嵌入

$$\sigma : K \to \overline{F}.$$

因为 σ 固定 F 中的系数，所以和我们前面讨论 Galois 自同构时一样：

$$m_\alpha(\alpha)=0$$

经过 σ 后得到：

$$m_\alpha(\sigma(\alpha))=0.$$

所以：

$$\boxed{\sigma(\alpha)\text{ 必须是 }m_\alpha(x)\text{ 的另一个根}}$$

这一步很重要。

现在如果 K/F 不是正规扩张，就可能出问题。

例如：

$$K=\mathbb{Q}(\sqrt[3]{2}).$$

取：

$$\alpha=\sqrt[3]{2}.$$

它的最小多项式是：

$$x^3-2.$$

三个根：

$$\sqrt[3]{2},\qquad \omega\sqrt[3]{2},\qquad \omega^2\sqrt[3]{2}.$$

但是 K 只包含第一个。

因此可以有一个 $\mathbb{Q}$–嵌入：

$$\sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}.$$

于是：

$$\sigma(K) = \mathbb{Q}(\omega\sqrt[3]{2}).$$

这个域不等于原来的：

$$\mathbb{Q}(\sqrt[3]{2}).$$

所以这个嵌入真的把 K “搬到外面去了”。

现在换成正规扩张。

例如：

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

这是 $x^3 - 2$ 的分裂域。

因此它已经包含：

$$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2}.$$

所以如果一个固定 $\mathbb{Q}$ 的嵌入把

$$\sqrt[3]{2}$$

送成：

$$\omega\sqrt[3]{2},$$

没有关系，因为：

$$\omega\sqrt[3]{2} \in K.$$

它没有跑出 K。

这就是 normal 的核心：

$$\boxed{\alpha \in K \Longrightarrow \alpha \text{ 在 } F \text{ 上的所有共轭根也都在 } K}$$

更标准地说，对于正规扩张 K/F，如果一个不可约多项式

$$f(x) \in F[x]$$

在 K 里有一个根，那么它就在 K 里完全分裂。

于是对任意：

$$\alpha \in K,$$

我们已经知道：

$$\sigma(\alpha)$$

必须是 α 的某个共轭根。

但正规性又保证：

$$\text{这些共轭根全都在 } K.$$

所以：

$$\sigma(\alpha) \in K.$$

因为这对所有

$$\alpha \in K$$

都成立，因此：

$$\boxed{\sigma(K) \subseteq K}.$$

那为什么最后不是只有

$$\sigma(K) \subseteq K,$$

而是：

$$\sigma(K) = K?$$

因为 σ 是嵌入，所以它是一一的。

而且 K/F 是有限扩张，所以：

$$[\sigma(K) : F] = [K : F].$$

但我们又有：

$$\sigma(K) \subseteq K.$$

一个 K 的真子域如果作为 F–向量空间真地更小，就不可能和 K 有完全相同的有限维数。

因此只能：

$$\boxed{\sigma(K) = K}.$$

于是原本只是：

$$\sigma : K \to \overline{F}$$

的嵌入，实际上自动变成：

$$\boxed{\sigma : K \to K}$$

也就是 K 的自同构。

所以整条逻辑可以压缩成：

$$\alpha \in K$$

$$\Downarrow$$

$$\sigma(\alpha) \text{ 是 } \alpha \text{ 的某个共轭根}$$

$$\Downarrow \quad (K/F \text{ 正规})$$

$$\sigma(\alpha) \in K$$

$$\Downarrow$$

$$\sigma(K) \subseteq K$$

再利用有限维和单射：

$$\boxed{\sigma(K) = K}.$$

所以你之前那句话“Galois 保证映射不会把 K 送出去”，严格说真正负责这件事的是：

$$\boxed{\textbf{Galois 扩张中的 normality（正规性）}}$$

而不是“可分性”。

11.7 以 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 理解延拓和限制

我们先用具体例子看“延拓”是什么意思，再说一般情形。

设

$$F=\mathbb{Q},\qquad E=\mathbb{Q}(\sqrt{2}),\qquad K=\mathbb{Q}(\sqrt{2},\sqrt{3}).$$

我们有

$$F\subset E\subset K.$$

现在先看：

$$\mathrm{Gal}(E/\mathbb{Q}).$$

它有两个元素。

一个是恒等：

$$\sqrt{2}\mapsto\sqrt{2}.$$

另一个记作 τ：

$$\boxed{\tau(\sqrt{2})=-\sqrt{2}}.$$

现在问题是：

> 这个只定义在 E 上的 τ，能不能变成一个定义在整个 K 上的自同构？

可以。

因为 K 比 E 多出来的生成元就是：

$$\sqrt{3}.$$

所以我们只需要再决定：

$$\sqrt{3}\mapsto ?$$

一种最简单的选择就是：

$$\sqrt{3}\mapsto \sqrt{3}.$$

于是定义：

$$\sigma(\sqrt{2})=-\sqrt{2},\qquad \sigma(\sqrt{3})=\sqrt{3}.$$

那么任意

$$x\in K$$

都可以写成

$$x=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6},$$

所以 σ 自动被确定为：

$$\sigma(x)=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}.$$

这确实是 K 的一个自同构。

而且限制回 E：

$$\sigma|_E = \tau.$$

所以我们说：

$$\boxed{\sigma \text{ 是 } \tau \text{ 从 } E \text{ 到 } K \text{ 的一个延拓}}$$

其实我们还有另一种选择：

$$\sqrt{3} \mapsto -\sqrt{3}.$$

于是也可以定义：

$$\sigma'(\sqrt{2}) = -\sqrt{2}, \qquad \sigma'(\sqrt{3}) = -\sqrt{3}.$$

那么同样：

$$\sigma'|_E = \tau.$$

所以注意：

$$\boxed{\text{一个 } E \text{ 上的自同构，延拓到 } K \text{ 时不一定唯一}}$$

但我们现在只关心：

> 至少有没有一个延拓?

现在回到 restriction map：

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F).$$

它做的是：

$$\sigma \mapsto \sigma|_E.$$

如果 E 上的每一个自同构 τ 都至少能找到一个 K 上的 σ，使：

$$\sigma|_E = \tau,$$

那么就说明：

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

里的每个元素都能被 `res` 命中。

这就叫 `res` 是：

$$\boxed{\text{满射 surjective}}$$

也就是说：

$$\boxed{\mathrm{im}(\mathrm{res}) = \mathrm{Gal}(E/F)}$$

一般情况下为什么能延拓?

这里需要一个新的重要事实。

假设：

$$K/F$$

是有限 Galois 扩张，而且：

$$F \subset E \subset K.$$

取一个固定 F 的 E–自同构：

$$\tau : E \to E.$$

首先，τ 可以看成把 E 嵌入一个更大的代数闭包中的映射。

有一个基本的**延拓定理**告诉我们：

$$\boxed{\text{这样的 } F\text{-嵌入可以延拓到 } K \text{ 上}}$$

也就是说，可以找到：

$$\widetilde{\tau} : K \to \overline{F}$$

使得：

$$\widetilde{\tau}|_E = \tau.$$

这里暂时先把

$$\overline{F}$$

理解为“一个足够大的、包含所有相关代数根的域”。

但我们还需要：

$$\widetilde{\tau}(K) = K,$$

否则它只是把 K 映到外面的某个地方，还不能算 K 的自同构。

这时候就用到了：

$$\boxed{K/F \text{ 是 } \mathrm{Galois}}$$

特别是它的“正规性 normality”。

正规性保证：

> 固定 F 的任何这种嵌入，都不会把 K 整体送出 K。

所以：

$$\widetilde{\tau}(K) = K.$$

于是：

$$\widetilde{\tau} \in \mathrm{Gal}(K/F).$$

而：

$$\widetilde{\tau}|_E = \tau.$$

因此 E 上每个自同构都能从 K 上限制下来。

所以：

$$\boxed{\mathrm{im}(\mathrm{res}) = \mathrm{Gal}(E/F)}$$

前面第一同构定理已经给了：

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{im}(\mathrm{res}).$$

现在代入：

$$\boxed{\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)}$$

这就是我们一直想得到的关系。

你可以先把它读成一句话：

> **总 Galois 群除掉那些“在 E 上什么都不做”的自同构以后，剩下的正好就是 E/F 这一层能看到的 Galois 群。**

下一步就可以把这个公式真正用到**根式塔**上，从而构造出 Galois 群的正规子群链。

第 12 章：完整例子：三次分裂域的群为什么是 S_3

本章对象：$\alpha = \sqrt[3]{2}$ 取实根；ω 是本原三次单位根；$K = \mathbb{Q}(\alpha, \omega)$。$\alpha$、$\omega$ 是生成元，六个基元素另行证明。

12.1 Gal 记号的斜杠指基础域

> 原问题：这里还是不好理解符号，虽然我理解是在做自同构的群

这里确实容易误解，尤其是这个斜杠：

$$\mathrm{Gal}(x^3 - 2/\mathbb{Q})$$

看起来像“拿 $x^3 - 2$ 除以 $\mathbb{Q}$”，其实**完全不是除法**。

更严格的写法应该先定义它的分裂域：

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

然后写：

$$\boxed{\mathrm{Gal}(K/\mathbb{Q})}$$

这里的

$$K/\mathbb{Q}$$

意思是：

> **域扩张 K over $\mathbb{Q}$**

也就是：

$$\mathbb{Q} \subset K.$$

所以：

$$\mathrm{Gal}(K/\mathbb{Q})$$

完整意思是：

> 所有“把 K 映到自己、同时把 $\mathbb{Q}$ 中每个元素都固定不动”的域自同构所组成的群。

写成集合就是：

$$\boxed{\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma : K \to K \mid \sigma \text{ 是域自同构，且 } \sigma(q) = q,\ \forall q \in \mathbb{Q}\}}$$

所以这里可以逐个读：

$$\mathrm{Gal}$$

表示“Galois 群”；

$$K$$

表示我们正在操作的那个大域；

$$/$$

这里读作 over，不是除号；

$$\mathbb{Q}$$

表示要求自同构必须固定不动的基础域。

因此：

$$\boxed{\mathrm{Gal}(K/\mathbb{Q})}$$

可以直译成：

> **K 相对于 $\mathbb{Q}$ 的 Galois 群。**

而我前面写的

$$\mathrm{Gal}(x^3-2/\mathbb{Q})$$

是一种常见的简写，意思其实是：

> 取 x^3-2 在 $\mathbb{Q}$ 上的分裂域 K，然后研究
>
> $$\mathrm{Gal}(K/\mathbb{Q}).$$

更不容易混淆的写法是：

$$\boxed{f(x)=x^3-2,\qquad K=\text{它在 }\mathbb{Q}\text{ 上的分裂域}}$$

然后：

$$\boxed{\mathrm{Gal}(f/\mathbb{Q}):=\mathrm{Gal}(K/\mathbb{Q})}$$

所以以后看到

$$\mathrm{Gal}(f/F)$$

你就把它翻译成一句话：

> **“多项式 f 在基础域 F 上的 Galois 群。”**

而真正被做自同构的是它的**分裂域**，不是多项式本身。

12.2 生成域的四则运算规则

> 原问题：但是这里的生成有规则吧

有，而且规则非常明确。

$$\mathbb{Q}(\alpha,\omega)$$

里的“生成”不是随便组合，而是：

$$\boxed{\text{从 } \mathbb{Q},\alpha,\omega \text{ 出发，反复允许 } +,-,\times,\div}$$

其中除法当然要求分母不为 0。

所以更形式化地说：

$$\mathbb{Q}(\alpha,\omega)$$

就是**包含 $\mathbb{Q},\alpha,\omega$ 的最小域**。

也就是说，你一开始有

$$\mathbb{Q},\quad \alpha,\quad \omega,$$

然后因为域必须封闭，就必须把这些东西也收进去：

$$\alpha+\omega,$$

$$\alpha\omega,$$

$$\alpha^2,$$

$$\frac{1}{\alpha+\omega},$$

$$\frac{\alpha^2+3\omega}{2-\alpha\omega},$$

等等。

一般来说，域生成可以理解成所有形如

$$\boxed{\frac{P(\alpha,\omega)}{Q(\alpha,\omega)}}$$

的元素，其中

$$P,Q\in\mathbb{Q}[x,y],\qquad Q(\alpha,\omega)\neq 0.$$

也就是：

> 用有理数作为系数，对 α,ω 做有限次加减乘除所能得到的一切数。

但这个例子又有额外关系：

$$\alpha^3=2,$$

以及

$$\omega^2+\omega+1=0.$$

所以

$$\alpha^3$$

可以降成常数，

$$\omega^2$$

可以降成

$$-\omega - 1.$$

因此看似很复杂的表达式最终都能压缩成

$$a + b\alpha + c\alpha^2 + d\omega + e\alpha\omega + f\alpha^2\omega.$$

所以你说“生成有规则”是对的。最核心的规则就是：

取最小的、对四则运算封闭的集合

而如果生成元满足代数方程，就再利用这些代数关系不断化简。

你也可以把它和前面的“群生成”对比着理解：群生成允许不断做群运算和取逆；域生成则允许不断做

$$+, -, \times, \div.$$

12.3 生成元与向量空间的基

> 原问题：这个符号的意思就是基是1还有这两个，然后系数是有理数对吧

不完全是。这里最关键的是区分 **“生成元”** 和 **“基”**。

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

这个符号的意思是：

> 从 $\mathbb{Q}$ 出发，把 $\sqrt[3]{2}$ 和 ω 加进去，并且为了保持“域”对四则运算封闭，把所有被迫产生的元素也一起加入。

所以

$$\sqrt[3]{2},\ \omega$$

是**生成元（generators）**，不是说基就是

$$\{1, \sqrt[3]{2}, \omega\}.$$

令

$$\alpha = \sqrt[3]{2}.$$

因为

$$\alpha^3 = 2,$$

所以 α 的高次幂都能降到

$$1, \alpha, \alpha^2.$$

同时

$$\omega^2 + \omega + 1 = 0,$$

所以

$$\omega^2 = -\omega - 1,$$

因此 ω 的高次幂只需要保留 $1, \omega$。

把两者结合起来，就会产生：

$$1, \quad \alpha, \quad \alpha^2, \quad \omega, \quad \alpha\omega, \quad \alpha^2\omega.$$

而这个例子里，这 6 个元素恰好构成 K 在 $\mathbb{Q}$ 上的一组基：

$$\boxed{\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\}}$$

所以任意 $x \in K$ 都可以唯一写成：

$$\boxed{x = a + b\alpha + c\alpha^2 + d\omega + e\alpha\omega + f\alpha^2\omega}$$

其中：

$$a, b, c, d, e, f \in \mathbb{Q}.$$

也可以更紧凑地写成：

$$x = (a + b\alpha + c\alpha^2) + (d + e\alpha + f\alpha^2)\omega.$$

因此你可以把

$$\boxed{\mathbb{Q}(\alpha, \omega)}$$

理解为：

> **“由 $\mathbb{Q}$ 和 α, ω 生成的最小域。”**

而不是：

> “以 $1, \alpha, \omega$ 为基的向量空间。”

这两个概念要分开。这里 α, ω 是**生成域所需的生成元**；最终作为 $\mathbb{Q}$–向量空间的基有 6 个元素。

补充证明：三次例子的六种自同构确实全部存在

$\alpha = \sqrt[3]{2}$ 取实根，ω 是非实本原三次单位根。$x^3 - 2$ 在 $\mathbb{Q}$ 上不可约：三次多项式可约就有一次因子，因此有有理根；有理根定理只允许 ±1、±2，逐个代入都不是根。所以 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$。

α 的生成域完全在 $\mathbb{R}$ 中，而 ω 非实；ω 满足 $x^2 + x + 1$，所以 $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$，总次数为 6。另一方面 $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$，由塔式定理 $[K : \mathbb{Q}(\omega)] = 3$，因此 α 在 $\mathbb{Q}(\omega)$ 上的最小多项式仍是 $x^3 - 2$。

在 $\mathbb{Q}(\omega)$ 上用 $\alpha \mapsto \omega\alpha$ 延拓恒等嵌入，得到 $K \to K$ 的嵌入；由于像含 ω 与 $\omega\alpha$，也含 α，故它是自同构 r。复共轭 s 固定 α，把 ω 送到 ω^2。这给出了真实存在的两个映射，不是仅列出满足方程的候选像。

它们满足 $r^3 = s^2 = e$，并且 $srs = r^{-1}$。六个映射 $e, r, r^2, s, rs, r^2 s$ 对 α、ω 的作用各不相同。所有自同构最多只有 3×2 个候选，所以这六个就是全部。r、s 在三个根上分别诱导 (123)、(23)，且此作用忠实（根生成整个域），故 $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$。

12.5 计算三次分裂域的六个自同构

现在我们就具体算：

$$K = \mathbb{Q}(\alpha, \omega), \qquad \alpha = \sqrt[3]{2}, \qquad \omega^3 = 1,\ \omega \neq 1$$

的 Galois 群

$$\mathrm{Gal}(K/\mathbb{Q}).$$

目标是看清楚它为什么正好是 S_3。

先看一个固定 $\mathbb{Q}$ 的自同构 σ。因为

$$\alpha^3 = 2,$$

所以

$$\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2.$$

因此 $\sigma(\alpha)$ 必须仍然是 $x^3 - 2$ 的一个根。

三个根是：

$$\alpha, \qquad \omega\alpha, \qquad \omega^2\alpha.$$

所以：

$$\boxed{\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}}$$

一共有 3 种可能。

再看 ω。

它满足：

$$\omega^2 + \omega + 1 = 0.$$

所以：

$$\sigma(\omega)^2 + \sigma(\omega) + 1 = 0.$$

这个二次方程的两个根就是：

$$\omega, \qquad \omega^2.$$

因此：

$$\boxed{\sigma(\omega) \in \{\omega, \omega^2\}}$$

一共有 2 种可能。

于是看起来我们可能有：

$$3 \times 2 = 6$$

种自同构。

而且这个例子中，这 6 种确实全部都存在。

为什么只需要决定 α 和 ω 的去向？

因为：

$$K = \mathbb{Q}(\alpha, \omega).$$

也就是说整个 K 都是由有理数、α、ω 通过四则运算生成的。

而 σ 已经要求固定所有有理数。

所以一旦知道：

$$\sigma(\alpha), \qquad \sigma(\omega),$$

那么整个 σ 的作用就完全被决定了。

例如：

$$x = 3 + 2\alpha - \alpha^2\omega.$$

那么：

$$\sigma(x) = 3 + 2\sigma(\alpha) - \sigma(\alpha)^2\sigma(\omega).$$

没有其他自由度。

现在我们把这 6 种可能列出来：

$\sigma(\alpha)$	$\sigma(\omega)$
α	ω
α	ω^2
$\omega\alpha$	ω
$\omega\alpha$	ω^2
$\omega^2\alpha$	ω
$\omega^2\alpha$	ω^2

所以：

$$\boxed{|\mathrm{Gal}(K/\mathbb{Q})| = 6}.$$

接下来关键不是“6”这个数字本身，而是：

> 这 6 个自同构实际上就是对三个根的 6 种置换。

把三个根记作：

$$r_1 = \alpha,$$

$$r_2 = \omega\alpha,$$

$$r_3 = \omega^2\alpha.$$

任意 σ 都会把它们重新排列。

例如先取一个自同构 r：

$$r(\alpha) = \omega\alpha, \qquad r(\omega) = \omega.$$

看看它对三个根怎么作用。

首先：

$$r(r_1) = r(\alpha) = \omega\alpha = r_2.$$

再看：

$$r(r_2) = r(\omega\alpha) = r(\omega)r(\alpha) = \omega \cdot \omega\alpha = \omega^2\alpha = r_3.$$

最后：

$$r(r_3) = r(\omega^2\alpha) = \omega^2 \cdot \omega\alpha = \omega^3\alpha = \alpha = r_1.$$

所以它对根的作用就是：

$$r_1 \to r_2 \to r_3 \to r_1.$$

也就是一个 3-循环：

$$\boxed{(123)}.$$

现在再取另一个自同构 s：

$$s(\alpha) = \alpha, \qquad s(\omega) = \omega^2.$$

它其实就是复共轭。

对第一个根：

$$s(r_1) = s(\alpha) = \alpha = r_1.$$

对第二个：

$$s(r_2) = s(\omega\alpha) = \omega^2\alpha = r_3.$$

对第三个：

$$s(r_3) = s(\omega^2\alpha) = \omega\alpha = r_2.$$

所以：

$$r_2 \leftrightarrow r_3,$$

而 r_1 不动。

也就是：

$$\boxed{(23)}.$$

于是我们的 Galois 群里已经有：

$$(123)$$

和

$$(23).$$

而这两个置换可以生成整个 S_3。

因此：

$$\boxed{\mathrm{Gal}(K/\mathbb{Q}) \cong S_3}$$

这里的

$$\cong$$

不是“严格等于”，而是：

$$\boxed{\text{同构}}$$

意思是：

> 这两个群的元素虽然表面上不是同一种对象，一个是域自同构，一个是置换，但它们的群运算结构完全一样。

所以终于把我们最开始的两条线接起来了：

$$\text{域自同构} \longrightarrow \text{根的置换} \longrightarrow \text{置换群}.$$

而 Galois 群就是：

$$\boxed{\text{这些允许的根置换所形成的群}}$$

下一步就该进入真正关键的一桥：

$$\boxed{\text{为什么“加入一个根式”会让 Galois 群只增加一种很受限制的阿贝尔结构}}$$

也就是开始解释为什么：

$$\text{根式可解} \Rightarrow \text{Galois 群可解}.$$

12.6 系数固定的自同构为何把根送到根

> 原问题：这一步不是很理解

这一步其实就是我们前面讲过的“自同构保持多项式关系”，只是这里应用到**原方程的根**上。

设

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$$

而 K 是它的分裂域。取

$$\sigma \in \mathrm{Gal}(K/F).$$

这句话的意思是：

$$\sigma : K \to K$$

是域自同构，并且固定 F 中的所有元素。

现在假设

$$r_1$$

是 $f(x)$ 的一个根，所以：

$$f(r_1) = 0.$$

也就是：

$$a_n r_1^n + \cdots + a_1 r_1 + a_0 = 0.$$

对整个等式作用 σ：

$$\sigma(a_n r_1^n + \cdots + a_0) = \sigma(0).$$

因为 σ 保持加法、乘法，而且每个系数

$$a_i \in F$$

都被固定，所以：

$$a_n \sigma(r_1)^n + \cdots + a_1 \sigma(r_1) + a_0 = 0.$$

也就是：

$$\boxed{f(\sigma(r_1)) = 0}.$$

因此：

$$\boxed{\sigma(r_1) \text{ 也必须是 } f(x) \text{ 的根}}.$$

如果 f 的根是

$$r_1, r_2, \ldots, r_n,$$

那么：

$$\sigma(r_1)$$

一定是其中某一个：

$$r_j.$$

同样：

$$\sigma(r_2), \ldots, \sigma(r_n)$$

也全部还在这组根里面。

所以 σ 对根集做的事情一定是：

$$\{r_1, \ldots, r_n\} \longrightarrow \{r_1, \ldots, r_n\}.$$

而且因为 σ 是自同构，所以是双射，不可能把两个不同根都压成同一个根。

因此它实际上就是对这些根进行一个**置换**：

$$\boxed{\sigma \leftrightarrow \text{某个 } \pi \in S_n}.$$

但注意一个关键区别：

$$\boxed{\textbf{Galois 自同构一定给出根的置换}}$$

并不意味着：

$$\boxed{\text{任意根的置换都一定是 Galois 自同构}}.$$

一般具体多项式只允许其中一部分置换。

例如 $x^3 - 2$ 的分裂域里确实允许全部 S_3；但有的方程可能只允许一个更小的子群。

最后还有一步：为什么一个 Galois 自同构一旦知道它怎么置换所有根，就完全确定了？

因为分裂域本身就是：

$$\boxed{K = F(r_1, \dots, r_n)}$$

也就是说，K 是由基础域 F 和这些根生成的。

σ 已经固定 F，再告诉你每个

$$r_i \mapsto r_{\pi(i)},$$

那么 K 里所有通过这些根做四则运算得到的元素怎么变化，也全部被确定了。

所以我们得到一个非常重要的包含关系：

$$\boxed{\mathrm{Gal}(K/F) \hookrightarrow S_n}$$

意思是：**Galois 群可以看成 S_n 的一个子群。**

这比我上一条直接说“Galois 自同构必须把根重新排列”完整得多。

第 13 章：中间域、限制映射和商群公式

本章对象：默认 K/F 有限 Galois；只有额外满足 E/F 正规时，$\mathbf{res}$ 才以 $\mathrm{Gal}(E/F)$ 为目标群。$\mathbf{res}$ 是群映射，σ 是它的输入，$\sigma|E$ 是它的输出。

13.1 域越大，固定它的自同构越少

现在我们要把“域的一层层扩张”翻译成“群的一层层子群”。

这一步的核心是一个非常漂亮的反向关系：

$$\boxed{\text{域越大，对应的 } \mathbf{Galois} \text{ 子群反而越小}}$$

先不要记定理，我们用一个具体例子理解。

假设有：

$$F \subset E \subset K$$

其中 K/F 是一个 Galois 扩张。

我们考虑总的 Galois 群：

$$G = \mathrm{Gal}(K/F).$$

也就是所有“固定 F”的 K 的自同构。

现在因为 E 比 F 更大，如果我要求一个自同构不仅固定 F，还必须固定整个 E，那它受到的限制就更多。

于是得到一个更小的群：

$$H = \mathrm{Gal}(K/E).$$

注意：

$$H \subset G.$$

为什么？

因为如果一个自同构把 E 里的所有元素都固定，那当然也会把 $F \subset E$ 里的所有元素固定。

所以：

$$\boxed{F \subset E \Longrightarrow \mathrm{Gal}(K/E) \subset \mathrm{Gal}(K/F)}$$

这就是“反向”。

域越大：

$$F \subset E,$$

要固定的东西越多，

所以允许的自同构越少。

举个很简单的例子。

还是：

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

整个 K 相对于 $\mathbb{Q}$ 的自同构，可以独立决定：

$$\sqrt{2} \mapsto \pm\sqrt{2},$$

$$\sqrt{3} \mapsto \pm\sqrt{3}.$$

所以一共有 4 个：

$$|\mathrm{Gal}(K/\mathbb{Q})| = 4.$$

现在取中间域：

$$E = \mathbb{Q}(\sqrt{2}).$$

如果一个自同构必须固定 E，那它就必须固定：

$$\sqrt{2}.$$

所以原来关于 $\sqrt{2}$ 的“正负自由度”消失了。

它只能决定：

$$\sqrt{3} \mapsto \pm\sqrt{3}.$$

于是：

$$|\mathrm{Gal}(K/E)| = 2.$$

所以你看到：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K$$

对应的是：

$$\mathrm{Gal}(K/\mathbb{Q}) \supset \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \supset \{e\}.$$

域链方向是：

$$\boxed{\text{越往上越大}}$$

群链方向是：

$$\boxed{\text{越往下越小}}$$

这就是 Galois 对应最核心的直觉。

更一般地，如果：

$$F \subset E_1 \subset E_2 \subset K,$$

那么：

$$\mathrm{Gal}(K/F) \supset \mathrm{Gal}(K/E_1) \supset \mathrm{Gal}(K/E_2) \supset \mathrm{Gal}(K/K) = \{e\}.$$

也就是：

$$\boxed{F \subset E_1 \subset E_2 \subset K}$$

反向对应：

$$\boxed{G \supset H_1 \supset H_2 \supset \{e\}}$$

其中

$$H_i = \mathrm{Gal}(K/E_i).$$

但现在还差一个很关键的问题：

> 这些 H_i 为什么会是正规子群？
> 以及为什么商群
>
> $$H_i/H_{i+1}$$
>
> 会对应某一层域扩张的 Galois 群？

这就是 Galois 基本定理真正有力量的地方。

下一步我们就只讲第一件事：

$$\boxed{\text{为什么“中间域本身对基础域是 Galois 的”时，对应子群就是正规子群}}$$

这正好会把我们前面学过的“正规子群”和现在的“中间域”连接起来。

13.2 中间域正规时，对应子群为何正规

现在只讲这一件事：

$$\boxed{\text{为什么中间域 } E/F \text{ 是 Galois 时，} \mathrm{Gal}(K/E) \text{ 会成为 } \mathrm{Gal}(K/F) \text{ 的正规子群}}$$

先设：

$$F \subset E \subset K,$$

并令

$$G = \mathrm{Gal}(K/F),$$

$$H = \mathrm{Gal}(K/E).$$

我们已经知道：

$$H \le G.$$

现在要证明：

$$\boxed{H \triangleleft G}$$

也就是对任意

$$\sigma \in G,$$

都有：

$$\sigma H \sigma^{-1} = H.$$

先取一个：

$$\tau \in H.$$

因为 $\tau \in H$，所以 τ 的定义是：

> τ 固定 E 中的每个元素。

也就是：

$$\tau(x) = x, \qquad \forall x \in E.$$

现在我们看共轭：

$$\sigma\tau\sigma^{-1}.$$

我们要证明它仍然属于 H。

也就是说，需要证明：

$$\sigma\tau\sigma^{-1}$$

仍然固定 E。

任取：

$$x \in E.$$

看：

$$(\sigma\tau\sigma^{-1})(x).$$

从右往左作用。

第一步：

$$x \overset{\sigma^{-1}}{\longmapsto} \sigma^{-1}(x).$$

这里问题来了：

> $\sigma^{-1}(x)$ 还一定在 E 里面吗？

这正是关键。

如果：

$$\sigma^{-1}(E) = E,$$

那么当然：

$$\sigma^{-1}(x) \in E.$$

于是因为 τ 固定 E：

$$\tau(\sigma^{-1}(x)) = \sigma^{-1}(x).$$

最后再作用 σ：

$$\sigma(\sigma^{-1}(x)) = x.$$

所以：

$$(\sigma\tau\sigma^{-1})(x) = x.$$

于是：

$$\sigma\tau\sigma^{-1} \in H.$$

因此：

$$\sigma H\sigma^{-1} = H.$$

也就是：

$$\boxed{H \triangleleft G}.$$

所以整个证明实际上卡在一句话：

$$\boxed{\sigma(E) = E}$$

为什么成立？

这就是为什么需要 E/F 是 Galois。

如果 E/F 是 Galois，那么 E 可以理解为某个多项式在 F 上的分裂域。

而 $\sigma \in \mathrm{Gal}(K/F)$ 固定 F，所以它把这个多项式的根仍然送到这个多项式的根。

因为 E 是由这些根生成的，所以：

$$\sigma(E) = E.$$

也就是说：

> E 作为一个整体，在所有固定 F 的自同构作用下不会被送到别的地方去。

于是对应的：

$$H = \mathrm{Gal}(K/E)$$

就是正规子群。

你可以把这件事和前面的正规子群直觉对应起来：

在群论里：

$$H \triangleleft G$$

意思是 H 在共轭作用下保持不变。

在域论里，对应的是：

$$E$$

在 G 的作用下作为一个整体保持不变。

所以：

$$\boxed{E/F \text{ Galois} \iff \mathrm{Gal}(K/E) \triangleleft \mathrm{Gal}(K/F)}$$

这就是 Galois 基本定理里最漂亮的一条对应关系之一。

下一步就可以继续讲：

$$\boxed{G/H \cong \mathrm{Gal}(E/F)}$$

也就是为什么“商群”恰好对应“中间那一层域扩张的 Galois 群”。

13.3 域的整体稳定不等于固定每个单位根

> 原问题：这个得保证单位根也是固定的吧

对，你抓到了一个很关键的区别：**“E 在所有固定 F 的自同构下保持不变”本身，不要求额外加入单位根；它要求的是 E/F 是 Galois。** 单位根是在我们前面构造“根式扩张的每一层都是 Galois 且阿贝尔”时需要的。

这两个条件要分开看。

比如

$$F \subset E \subset K,$$

且

$$\sigma \in \mathrm{Gal}(K/F).$$

如果 E/F 是 Galois，那么 σ 会把 E 送回自身：

$$\sigma(E) = E.$$

这里不需要专门说“单位根固定”。

为什么？因为 E/F 是 Galois 意味着，粗略说，E 已经包含了定义它所需多项式的**全部共轭根**。因此 σ 虽然可能把这些根互相交换，但它们仍然都在 E 里面，于是整个 E 不会跑出去。

反过来看我们之前的例子就很清楚。

设

$$\alpha = \sqrt[3]{2}$$

并考虑：

$$E = \mathbb{Q}(\alpha).$$

它不是 $x^3 - 2$ 的分裂域，因为另外两个根

$$\omega\alpha, \qquad \omega^2\alpha$$

不在 E 里。

放进更大的分裂域

$$K = \mathbb{Q}(\alpha, \omega)$$

后，有某个

$$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$$

满足：

$$\sigma(\alpha) = \omega\alpha.$$

于是：

$$\sigma(E) = \sigma(\mathbb{Q}(\alpha)) = \mathbb{Q}(\omega\alpha).$$

而：

$$\mathbb{Q}(\omega\alpha) \neq \mathbb{Q}(\alpha).$$

所以：

$$\boxed{\sigma(E) \neq E}.$$

问题的本质不是单独因为“ω 没固定”，而是：

$$\boxed{E/\mathbb{Q} \text{ 不是 Galois}}$$

因此 E 没有包含自己所有的共轭。

那我们之前为什么反复强调：

$$\boxed{\text{把 } \omega \text{ 加入基础域}}$$

呢？

那是在解决另一个问题。

我们希望一层根式扩张

$$F \subset F(\alpha), \qquad \alpha^n = a \in F$$

不但成为 Galois 扩张，而且其 Galois 群还是**阿贝尔群**。

如果：

$$\zeta_n \in F,$$

那么所有根

$$\alpha, \zeta_n\alpha, \dots, \zeta_n^{n-1}\alpha$$

都自动在

$$F(\alpha)$$

里，所以这一层成为分裂扩张。

同时，因为：

$$\zeta_n \in F,$$

所有固定 F 的自同构必须满足：

$$\sigma(\zeta_n) = \zeta_n.$$

于是自同构只能：

$$\alpha \mapsto \zeta_n^k \alpha,$$

从而产生阿贝尔结构。

所以单位根实际上同时帮了我们两件事：

$$\boxed{\zeta_n \in F}$$

使得加入一个根 α 后，其他

$$\zeta_n^k \alpha$$

也自动进入扩张域——帮助这一层成为**分裂/Galois 扩张**；

同时它又让所有自同构固定 ζ_n——帮助这一层的 Galois 群成为**阿贝尔群**。

所以你可以这样区分：

$$\boxed{E/F \text{ Galois} \Rightarrow E \text{ 作为整体在固定 } F \text{ 的自同构下保持不变}}$$

而

$$\boxed{\text{单位根已在 } F}$$

是我们构造**特殊的根式 Galois 层**时用来保证这一条件、并进一步保证“阿贝尔”的工具。

你刚才这个疑问其实正好触及了后面证明里一个非常容易混淆的点：**“Galois”负责稳定中间域，“含单位根”负责让根式层变成特别简单的 Galois 扩张。**

13.4 限制映射连接域层和群层

下一步最自然的是把刚才的“中间域 ↔ 正规子群”继续推进一步，证明：

$$\boxed{\mathrm{Gal}(K/F)\big/\mathrm{Gal}(K/E)\cong\mathrm{Gal}(E/F)}$$

但我们不会直接上这个公式。先只做第一步：

$$\boxed{\text{什么叫把 } K \text{ 上的自同构“限制”到 } E}$$

假设

$$F\subset E\subset K,$$

并且 E/F 是 Galois。

取一个

$$\sigma\in\mathrm{Gal}(K/F).$$

因为刚才已经知道：

$$\sigma(E)=E,$$

所以虽然 σ 原本是

$$\sigma : K \to K,$$

我们完全可以只观察它在 E 中的作用：

$$\sigma|_E : E \to E.$$

这个符号

$$\boxed{\sigma|_E}$$

读作：

> σ restricted to E，即“σ 限制在 E 上”。

例如假设

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \qquad E = \mathbb{Q}(\sqrt{2}).$$

某个自同构 σ 可能满足

$$\sigma(\sqrt{2}) = -\sqrt{2}, \qquad \sigma(\sqrt{3}) = -\sqrt{3}.$$

但如果我们只看 $E = \mathbb{Q}(\sqrt{2})$，那么 $\sqrt{3}$ 根本不属于 E，所以我们不关心它怎么变。

在 E 上，

$$\sigma|_E$$

就只是：

$$\sqrt{2} \mapsto -\sqrt{2}.$$

因此我们得到一个映射：

$$\boxed{\mathrm{res} : \mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(E/F)}$$

定义为：

$$\mathrm{res}(\sigma) = \sigma|_E.$$

这里 `res` 就是 restriction 的缩写。

这一步非常重要，因为接下来我们会问：

> 哪些 K 上不同的自同构，限制到 E 后会变成同一个自同构？

答案正好是：它们的差别来自那些**完全固定 E** 的自同构，也就是

$$\mathrm{Gal}(K/E).$$

于是商群

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$$

就会自然出现。

所以**下一步就应该证明这个 restriction map 的核为什么恰好是**

$$\boxed{\mathrm{Gal}(K/E)}.$$

这一步讲清楚以后，商群和中间域那一层 Galois 群的关系就几乎出来了。

13.5 限制映射的核

这里我们先不急着上同构定理，只把一个新概念讲清楚：

$$\boxed{\textbf{restriction map}\text{ 的核是什么}}$$

我们已经有：

$$F \subset E \subset K$$

并定义：

$$G = \mathrm{Gal}(K/F).$$

如果 E/F 是 Galois，那么每个

$$\sigma \in G$$

都会把 E 映回 E，所以可以限制：

$$\sigma|_E : E \to E.$$

于是有映射：

$$\mathrm{res} : G \to \mathrm{Gal}(E/F),$$

定义为：

$$\mathrm{res}(\sigma) = \sigma|_E.$$

现在问：

> 哪些 $\sigma \in G$ 经过这个映射以后，变成 $\mathrm{Gal}(E/F)$ 里的单位元?

先看 $\mathrm{Gal}(E/F)$ 的单位元是什么。

它就是：

$$\mathrm{id}_E,$$

也就是在 E 上什么都不做：

$$x \mapsto x, \qquad \forall x \in E.$$

因此：

$$\mathrm{res}(\sigma) = \mathrm{id}_E$$

意味着：

$$\sigma|_E = \mathrm{id}_E.$$

翻译成人话就是：

$$\boxed{\sigma(x) = x, \qquad \forall x \in E}$$

也就是说：

> σ 固定整个 E。

但“所有固定 E 的 K 的自同构”正是：

$$\mathrm{Gal}(K/E).$$

因此：

$$\boxed{\ker(\mathrm{res}) = \mathrm{Gal}(K/E)}$$

这里新出现了：

$$\boxed{\ker}$$

叫做 **kernel，核**。

一般来说，如果有群同态：

$$\varphi : G \to H,$$

那么它的核定义为：

$$\boxed{\ker \varphi = \{g \in G : \varphi(g) = e_H\}}$$

也就是说：

> 在映射以后“看起来什么都没做”的那些元素。

所以在我们的例子里：

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F),$$

一个 σ 如果属于核，就说明：

$$\sigma|_E = \mathrm{id}_E.$$

虽然它在整个 K 上可能不是单位元，但只看 E 时，它完全看不出来。

用具体例子会很清楚。

设：

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

$$E = \mathbb{Q}(\sqrt{2}),$$

$$F = \mathbb{Q}.$$

考虑自同构：

$$\sigma : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

它在整个 K 上不是恒等，因为：

$$\sqrt{3} \mapsto -\sqrt{3}.$$

但是限制到 E：

$$E = \mathbb{Q}(\sqrt{2}),$$

里面没有 $\sqrt{3}$。

而且它固定：

$$\sqrt{2}.$$

所以对任何：

$$a+b\sqrt{2}\in E,$$

都有：

$$\sigma(a+b\sqrt{2})=a+b\sqrt{2}.$$

因此：

$$\sigma|_E=\mathrm{id}_E.$$

所以这个 σ 属于：

$$\ker(\mathrm{res}).$$

而它也确实属于：

$$\mathrm{Gal}(K/E),$$

因为它固定整个 E。

于是得到：

$$\boxed{\ker(\mathrm{res})=\mathrm{Gal}(K/E)}$$

这个结果非常漂亮，因为“核”在群论里天然是正规子群。

所以我们立刻得到：

$$\boxed{\mathrm{Gal}(K/E)\triangleleft\mathrm{Gal}(K/F)}$$

这其实又给出了“为什么它是正规子群”的另一种证明方式。

下一步就是利用群论里的**第一同构定理**：

$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

代入这里，就会得到：

$$\operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \cong \operatorname{im}(\mathrm{res}).$$

然后我们再解释为什么这个像正好是：

$$\operatorname{Gal}(E/F).$$

这样就得到我们真正想要的：

$$\boxed{\operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \cong \operatorname{Gal}(E/F)}$$

13.6 从定义再次验证限制映射的核

> 原问题：这一步是怎么来的来着

这一步其实非常直接，只是符号容易遮住意思。

我们有：

$$\mathrm{res} : \operatorname{Gal}(K/F) \to \operatorname{Gal}(E/F),$$

定义为：

$$\mathrm{res}(\sigma) = \sigma|_E.$$

现在“核”的定义是：

$$\ker(\mathrm{res}) = \{\sigma \in \mathrm{Gal}(K/F) : \mathrm{res}(\sigma) = \mathrm{id}_E\}.$$

也就是那些经过限制以后，在 E 上变成恒等映射的 σ。

而

$$\mathrm{res}(\sigma) = \sigma|_E,$$

所以条件

$$\mathrm{res}(\sigma) = \mathrm{id}_E$$

等价于：

$$\sigma|_E = \mathrm{id}_E.$$

再展开，就是：

$$\sigma(x) = x, \qquad \forall x \in E.$$

也就是说：

> σ 固定 E 中每一个元素。

但“所有固定 E 的 K–自同构”按定义就是：

$$\mathrm{Gal}(K/E).$$

因此：

$$\boxed{\ker(\mathrm{res}) = \mathrm{Gal}(K/E)}$$

所以这一步本质上只是把两个定义接起来：

$$\boxed{\text{核} = \text{限制后变成恒等的那些元素}}$$

而

$$\boxed{\mathrm{Gal}(K/E) = \text{固定整个 } E \text{ 的 } K\text{-自同构}}$$

两者描述的是同一批自同构。

13.7 映射的输入元素本身也是映射

> 原问题：但是这个映射本身是不同同构之间的映射啊

对，你理解得对。这里最容易混的就是“映射的元素本身也是映射”。

我们把层次分开：

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

这是一个**群**。它的“元素”不是普通数字，而是一个个 K 上的域自同构：

$$\sigma : K \to K.$$

同样，

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

也是一个群，它的元素是：

$$\tau : E \to E$$

这样的域自同构。

现在 `res` 是一个**群同态**：

$$\boxed{\mathbf{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)}$$

它输入一个“映射” σ，输出另一个“映射”：

$$\boxed{\sigma \mapsto \sigma|_E}$$

所以确实是：

$$\text{映射} \longmapsto \text{映射}.$$

而“核”是针对这个**群同态 res** 来定义的。

群同态的核，就是所有被送到**目标群单位元**的元素。

这里目标群是：

$$\mathrm{Gal}(E/F).$$

它的单位元是什么？

不是数字 0 或 1，而是：

$$\boxed{\mathrm{id}_E}$$

也就是在 E 上什么都不做的恒等自同构：

$$x \mapsto x.$$

所以：

$$\ker(\mathrm{res}) = \{\sigma \in \mathrm{Gal}(K/F) : \mathrm{res}(\sigma) = \mathrm{id}_E\}.$$

而：

$$\mathrm{res}(\sigma) = \sigma|_E.$$

因此：

$$\sigma|_E = \mathrm{id}_E$$

意思就是：

$$\sigma(x) = x, \qquad \forall x \in E.$$

这恰好就是：

$$\sigma \in \mathrm{Gal}(K/E).$$

所以：

$$\boxed{\ker(\mathrm{res}) = \mathrm{Gal}(K/E)}$$

你可以把它理解成两层：

$$\boxed{\text{第一层：}\sigma\text{ 是域之间的映射}}$$

$$\boxed{\text{第二层：}\mathrm{res}\text{ 是“这些映射之间”的群同态}}$$

而 `res` 的核，就是那些被它送到“恒等映射” id_E 的 σ。

13.8 同态、嵌入、同构、自同构及两层映射

> 原问题：这里主要是几个概念和符号，一会儿用的是同态一会儿又变成了同构，虽然我理解这些意思，但是有的你说的比较快，就不知道你到底在指称什么

这里集中回看已经建立的几种映射类型；群论定义、域映射定义及延拓过程在前文各自出现，本段用于在限制映射上辨认它们。

对，你现在真正卡的不是数学思想，而是**“同一个字母到底代表什么对象、这个映射此刻是什么类型”切换得太快**。后面 Galois 理论里如果不严格区分，确实非常容易乱。

我们先暂停主线，把目前会反复出现的几个词彻底固定下来。以后我第一次引入一个映射时，会先写清楚“从哪里到哪里、是什么类型”，不再直接跳符号。

1. 同态 homomorphism：保持运算的映射

这是最宽泛的概念。

群之间：

$$\varphi : G \to H$$

如果满足

$$\varphi(ab) = \varphi(a)\varphi(b),$$

就是群同态。

此时**不要求单射，也不要求满射**。

例如：

$$\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

把整数映成奇偶类，就是群同态，但显然不是单射。

---

2. 同构 isomorphism：双射的同态

如果

$$\varphi : G \to H$$

既保持结构，又是双射，那么叫：

$$\boxed{\text{同构}}$$

于是写：

$$G \cong H.$$

所以逻辑关系是：

$$\boxed{\text{同构} = \text{同态} + \text{双射}}$$

例如：

$$G/\ker\varphi \cong \operatorname{im}\varphi$$

这里的 $\cong$ 是说这两个**群的结构完全一样**，并不是说它们是同一个集合。

---

3. 嵌入 embedding：单射的同态

如果

$$\varphi : E \to K$$

保持域的加法、乘法，又是单射，就叫域嵌入。

所以：

$$\boxed{\text{嵌入} = \text{同态} + \text{单射}}$$

它不要求像覆盖整个目标域 K。

例如可以有：

$$\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{C}.$$

它只是把小域“完整地放进”大域。

而我们前面讲过，对于保持 1 的域同态，单射其实自动成立，所以域论里“域同态”和“域嵌入”的距离比群论里小很多。

---

4. 自同构 automorphism：从自己到自己的同构

如果

$$\sigma : K \to K$$

既是域同态，又是双射，那么叫：

域自同构

所以：

自同构 = 从一个对象到它自己的同构

例如：

$$\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}),$$

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

这就是自同构。

现在把它们放在一张关系图里最清楚：

同态

加上“单射”：

⇓

嵌入

加上“满射”：

⇓

同构

如果这个同构恰好还是：

$$K \to K,$$

就叫：

自同构.

所以：

术语	额外要求
同态	保持结构
嵌入	同态+单射
同构	同态+双射
自同构	一个对象到自身的同构

再把目前 Galois 理论里的“角色”固定下来

我们目前讨论：

$$F \subset E \subset K.$$

这三个都是**域**。

这里 F 是最底层基础域，E 是中间域，K 是大域。

然后：

$$\mathrm{Gal}(K/F)$$

不是一个域，而是一个**群**。它的元素 σ 是：

$$\sigma : K \to K$$

这样的**域自同构**，并额外要求：

$$\sigma(a) = a, \qquad \forall a \in F.$$

所以每次看到

$$\sigma \in \mathrm{Gal}(K/F),$$

你脑子里应该自动展开成：

$$\boxed{\sigma : K \to K \text{ 是域自同构，并且逐点固定 } F}$$

然后我们有：

$$\mathrm{Gal}(K/E).$$

它也是一个群，它的元素仍然是：

$$\sigma : K \to K,$$

只是要求更严格：

$$\sigma(a) = a, \qquad \forall a \in E.$$

因为：

$$F \subset E,$$

固定整个 E 当然也固定 F，所以：

$$\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F).$$

再看刚才的 restriction：

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F).$$

注意这里 **res 本身是一个群同态**。

它输入的是一个：

$$\sigma : K \to K$$

然后输出：

$$\sigma|_E : E \to E.$$

所以这里实际上存在“两层映射”：

$$\boxed{\sigma \text{ 本身是域自同构}}$$

而

$$\boxed{\mathrm{res} \text{ 是把一个自同构送到另一个自同构的群同态}}$$

这个尤其容易混。

例如：

$$\mathrm{res}(\sigma) = \sigma|_E.$$

左边的 `res` 是**群之间的映射**；

右边的 σ 是**域之间的映射**。

这两个不是同一层次的东西。

还有我们刚才讲延拓时：

$$\tau : E \to E$$

原本是 E 的自同构。

为了延拓，我们暂时把它看成：

$$\tau : E \hookrightarrow \overline{F}.$$

这时候我们强调的是它作为一个**域嵌入**的身份。

然后延拓得到：

$$\widetilde{\tau} : K \hookrightarrow \overline{F}.$$

最开始只能称为**嵌入**。

等利用 K/F 的正规性证明：

$$\widetilde{\tau}(K) = K$$

以后，它实际上变成：

$$\widetilde{\tau} : K \to K$$

而且是双射。

这时候才能升级称为：

$$\boxed{\text{自同构}}$$

所以这里不是我把“嵌入突然叫成了自同构”，而是我们**证明了它的像恰好等于 K**，所以它从“单射同态”升级成了“到自身的双射同态”。

这个过程以后我会明确写成：

$$\text{先得到域嵌入 } \tilde{\tau}: K \hookrightarrow \overline{F}$$

然后证明：

$$\tilde{\tau}(K) = K$$

所以：

$$\text{因此 } \tilde{\tau} \in \mathrm{Gal}(K/F).$$

这样就不会突然换称呼。

从现在开始，我会在出现新映射时优先给你写成这种格式：

$$\boxed{\mathrm{res}: \underbrace{\mathrm{Gal}(K/F)}_{\text{群}} \longrightarrow \underbrace{\mathrm{Gal}(E/F)}_{\text{群}}, \qquad \sigma \longmapsto \sigma|_E}$$

并明确说 **res 是群同态，σ 是域自同构**。这样后面进入 Galois 基本定理时会清楚很多。

下一步也先不继续证明延拓定理，而应该先把 **“同态、核、像、单射、满射、同构”在 restriction map 这一个具体例子里全部对应起来**。这样第一同构定理那一段就不会再有符号漂移。

13.9 哪些对象属于群层，哪些属于域层

> 原问题：哪些是群的概念，哪些是域的概念

可以这样分最清楚：

概念	主要属于哪一层	在我们这里怎么用
群 group	群论	$G, H, \mathrm{Gal}(K/F)$
子群 subgroup	群论	$\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F)$
正规子群 normal subgroup	群论	$\mathrm{Gal}(K/E) \triangleleft \mathrm{Gal}(K/F)$
商群 quotient group	群论	G/H
群同态 homomorphism	群论	$\mathrm{res} : G \to H$
核 kernel	群论里常用，也可用于环/域同态	$\ker(\mathrm{res})$
像 image	一般映射/代数结构都可用	$\mathrm{im}(\mathrm{res})$
同构 isomorphism	群、域等结构都有	$G/H \cong \mathrm{Gal}(E/F)$
域 field	域论	$F, E, K, \mathbb{Q}$
域扩张 field extension	域论	$F \subset E \subset K$
代数元	域论	$\alpha = \sqrt[3]{2}$
最小多项式	域论	$m_\alpha(x)$
分裂域	域论	K 包含某多项式全部根
域嵌入 embedding	域论	$\tau : E \hookrightarrow \overline{F}$
域自同构 automorphism	域论	$\sigma : K \to K$
Galois 群	两者交界	“一群域自同构”组成的群

最容易混的是这几个：

$$\boxed{\mathrm{Gal}(K/F)}$$

本身是一个**群**；

但它里面的元素

$$\sigma \in \mathrm{Gal}(K/F)$$

是一个**域自同构**。

再比如

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$$

这里：

- `res` 是**群同态**；
- 输入的 σ 是**域自同构**；
- 输出的 $\sigma|_E$ 也是**域自同构**。

所以这里同时有“群层”和“域层”两层结构。

你可以把整个 Galois 理论暂时看成一句话：

$$\boxed{\text{用群论研究域自同构}}$$

也就是：

$$\text{域} \longrightarrow \text{域自同构} \longrightarrow \text{这些自同构组成群.}$$

这样以后看到符号时就先问：**现在是在谈域本身，还是在谈这些域自同构组成的群？**

13.10 限制映射、核、像与商群的角色逐一对应

好，我们继续，而且我会把“谁是群、谁是域、哪个符号在做什么”摆得更清楚。

现在我们有三层域：

$$F \subset E \subset K$$

并且假设：

$$K/F \text{ 是 Galois}, \qquad E/F \text{ 也是 Galois}.$$

我们定义两个群：

$$G = \mathrm{Gal}(K/F),$$

$$H = \mathrm{Gal}(K/E).$$

这里 $H \subset G$。

然后定义限制映射：

$$\boxed{\mathrm{res} : G \longrightarrow \mathrm{Gal}(E/F)}$$

规则是：

$$\boxed{\sigma \longmapsto \sigma|_E}$$

意思就是：原本 σ 作用在整个 K 上，现在只看它在 E 上做了什么。

前面我们已经知道：

$$\ker(\mathrm{res}) = H = \mathrm{Gal}(K/E).$$

也就是说：

> 那些限制到 E 后什么都不做的 K–自同构，恰好就是固定整个 E 的自同构。

现在只剩一个问题：

$$\boxed{\text{res 是不是满射?}}$$

也就是：

> $\mathrm{Gal}(E/F)$ 里的每一个自同构，能不能都从 K 上某个自同构限制下来?

答案是：

$$\boxed{\text{能}}$$

因为我们刚才讨论的延拓定理告诉我们：任取

$$\tau \in \mathrm{Gal}(E/F),$$

可以把它延拓成某个

$$\widetilde{\tau} \in \mathrm{Gal}(K/F)$$

并且满足：

$$\widetilde{\tau}|_E = \tau.$$

所以每个 τ 都能被 `res` 命中。

因此：

$$\boxed{\mathrm{im}(\mathrm{res}) = \mathrm{Gal}(E/F)}$$

于是第一同构定理给出：

$$G/\ker(\mathrm{res}) \cong \mathrm{im}(\mathrm{res}).$$

把具体对象代进去：

$$\boxed{\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F)}$$

这个式子非常重要。

它可以读成：

> 总的 Galois 群，除掉那些“在 E 上完全看不见的变化”，剩下的正好就是 E/F 这一层的 Galois 群。

所以现在“商群”和“中间域的一层扩张”终于完全对应起来了。

下一步就可以把它用在根式塔：

$$F_0 \subset F_1 \subset \cdots \subset F_r$$

上，得到反向的群链：

$$G_0 \supset G_1 \supset \cdots \supset G_r,$$

然后证明每个商群

$$G_i/G_{i+1}$$

都是阿贝尔群。

这一步完成以后，我们就真正得到：

$$\boxed{\text{根式可解} \Rightarrow \text{Galois 群可解}}$$

而且不是靠口号，而是可以看见每一层为什么对应。

13.11 限制映射满射的准确问题

下一步就该解决刚才留下的唯一缺口：

$$\boxed{\mathrm{im}(\mathrm{res}) = \mathrm{Gal}(E/F)}$$

也就是解释：

> E 上每一个固定 F 的自同构，为什么都能“延拓”成 K 上的自同构？

先不要直接上一般定理，我们会先用具体例子：

$$F = \mathbb{Q}, \qquad E = \mathbb{Q}(\sqrt{2}), \qquad K = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

在 E 上有一个非平凡自同构：

$$\sqrt{2} \mapsto -\sqrt{2}.$$

我们会先问：

> 能不能把它扩展到整个 K？

答案是可以，比如定义：

$$\sqrt{2} \mapsto -\sqrt{2}, \qquad \sqrt{3} \mapsto \sqrt{3}.$$

这样就得到 K 上的一个自同构。

然后再理解一般情形里为什么这种“延拓”成立。

一旦这一步完成，我们就得到：

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F).$$

这就是把**商群**和**中间域那一层扩张**真正对应起来的关键公式。

13.12 第一同构定理的陪集证明

例如我们刚才的限制映射

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$$

就是群同态。

为什么？

因为先复合两个自同构再限制到 E，和先分别限制到 E 再复合，效果相同：

$$(\sigma\tau)|_E = (\sigma|_E)(\tau|_E).$$

所以：

$$\mathrm{res}(\sigma\tau) = \mathrm{res}(\sigma)\mathrm{res}(\tau).$$

现在立刻代回 Galois 的情况。

我们有：

$$\mathrm{res} : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F).$$

已经知道：

$$\ker(\mathrm{res}) = \mathrm{Gal}(K/E).$$

所以第一同构定理直接给：

$$\boxed{\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{im}(\mathrm{res})}$$

现在只剩最后一个问题：

$$\boxed{\mathrm{im}(\mathrm{res}) \overset{?}{=} \mathrm{Gal}(E/F)}$$

也就是：

> E 上每一个固定 F 的自同构，能不能都从 K 上某个固定 F 的自同构限制下来？

这就是下一步。它涉及**“自同构能否从中间域延拓到整个分裂域”**。这一步讲清楚以后，我们才真正得到

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F).$$

第 14 章：根式塔：单位根、共轭与正规闭包

本章对象：$F_{i+1} = F_i(\alpha_i)$，α_i 的 n_i 次幂等于 $a_i \in F_i$；各层指数、元素均可不同。ζ_n 是本原 n 次单位根，μ_n 是全部 n 次单位根组成的群。

14.1 进入根式塔前回顾两条主线

进入根式塔前，已有的两条主线是：

$$\mathbb{Q} \to \text{域扩张} \to \text{分裂域} \to \text{域自同构} \to \textbf{Galois 群}$$

然后进一步讨论了“根式解”如何翻译成一层一层的域扩张：

$$F_i \subset F_{i+1} = F_i(\alpha), \qquad \alpha^n \in F_i.$$

最后停在一个很关键的技术点：

> 如果这一层的基础域 F 已经包含相应的 n 次单位根 ζ_n，那么自同构只能把
>
> $$\alpha$$
>
> 送到
>
> $$\zeta_n^k \alpha.$$

原讨论确认了以下需要的条件：

$$\boxed{\text{所以要先把单位根加入基础域}}$$

这样 ζ_n 就被固定，不会再被 Galois 自同构移动。

现在下一步就应该证明：

$$\boxed{\text{为什么这种“一层根式扩张”的 Galois 群一定是阿贝尔群}}$$

我们继续慢慢来。

假设：

$$F \subset K = F(\alpha),$$

并且

$$\alpha^n = a \in F.$$

同时假设：

$$\zeta_n \in F.$$

那么固定 F 的任何自同构 σ 都只能满足：

$$\sigma(\alpha) = \zeta_n^k \alpha.$$

另一个自同构 τ 则可能满足：

$$\tau(\alpha) = \zeta_n^l \alpha.$$

现在比较：

$$\sigma\tau$$

和

$$\tau\sigma.$$

先算：

$$\sigma\tau(\alpha).$$

因为：

$$\tau(\alpha) = \zeta_n^l \alpha,$$

所以：

$$\sigma\tau(\alpha) = \sigma(\zeta_n^l \alpha).$$

由于 $\zeta_n \in F$，而 σ 固定整个 F，所以：

$$\sigma(\zeta_n^l) = \zeta_n^l.$$

因此：

$$\sigma\tau(\alpha) = \zeta_n^l \sigma(\alpha).$$

又因为：

$$\sigma(\alpha) = \zeta_n^k \alpha,$$

所以：

$$\sigma\tau(\alpha) = \zeta_n^l \zeta_n^k \alpha = \zeta_n^{k+l} \alpha.$$

反过来：

$$\tau\sigma(\alpha) = \zeta_n^{k+l} \alpha.$$

因此：

$$\sigma\tau(\alpha) = \tau\sigma(\alpha).$$

而整个 K 是由 F 和 α 生成的。

两者都固定 F，而且在 α 上作用相同，所以它们在整个 K 上作用都相同。

因此：

$$\boxed{\sigma\tau = \tau\sigma}.$$

所以：

$$\boxed{\mathrm{Gal}(K/F) \text{ 是阿贝尔群}}$$

更直观地说，这些自同构本质上只是：

$$\alpha \mapsto \zeta_n^k \alpha.$$

做一次 k，再做一次 l，结果就是：

$$k + l.$$

而：

$$k + l = l + k.$$

所以自然交换。

这就是我们现在终于得到的关键结论：

$$\boxed{\text{单层根式扩张} + \text{基础域含相应单位根} \Longrightarrow \text{这一层的 Galois 群是阿贝尔的}}$$

接下来真正重要的一步，就是解释：

> 如果我们有一整座根式塔
>
> $$F_0 \subset F_1 \subset \cdots \subset F_r,$$
>
> 为什么这些“一层一层的阿贝尔群”会对应到总 Galois 群中的一条正规子群链?

这里就会第一次正式进入 **Galois 基本定理：中间域和子群之间的反向对应**。这一步是把“根式塔”真正变成“可解群”的桥。

14.2 把一个根式表达式拆成逐次开根

> 原问题：太快了没太理解为什么就加入了一个根式

对，刚才这里跳太快了。关键不是“为什么突然只加入一个根式”，而是：

> **所谓“能用根式解”，本来就可以拆成很多个“每次加入一个根式”的步骤。**

我们先把“根式表达式”看成一个实际公式。

比如：

$$\sqrt{2+\sqrt{3}}.$$

这个数看起来是一次写出来的，但它其实可以分两步构造。

先从

$$\mathbb{Q}$$

开始。

第一步加入：

$$\sqrt{3}.$$

得到：

$$F_1 = \mathbb{Q}(\sqrt{3}).$$

现在注意：

$$2 + \sqrt{3} \in F_1.$$

然后第二步再加入：

$$\sqrt{2 + \sqrt{3}}.$$

记

$$\alpha = \sqrt{2 + \sqrt{3}}.$$

那么：

$$\alpha^2 = 2 + \sqrt{3} \in F_1.$$

于是得到：

$$F_2 = F_1(\alpha).$$

也就是：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2+\sqrt{3}}).$$

所以一个嵌套根式：

$$\sqrt{2+\sqrt{3}}$$

实际上就是连续两次“加入一个根式”。

再看复杂一点的：

$$\sqrt[3]{2+\sqrt{5}}.$$

也一样。

第一步：

$$F_0 = \mathbb{Q}.$$

加入：

$$\sqrt{5},$$

得到：

$$F_1 = \mathbb{Q}(\sqrt{5}).$$

然后：

$$2+\sqrt{5} \in F_1.$$

再加入一个新元素 α，满足：

$$\alpha^3 = 2 + \sqrt{5}.$$

于是：

$$F_2 = F_1(\alpha).$$

所以：

$$\alpha = \sqrt[3]{2 + \sqrt{5}}.$$

因此，“每一步加入一个根式”的一般形式是：

已有一个域：

$$F_i.$$

然后选择一个：

$$a_i \in F_i.$$

再加入某个 α_i，使：

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

于是：

$$\boxed{F_{i+1} = F_i(\alpha_i)}.$$

这一步就叫一次**根式扩张**。

为什么这样就足够描述一般的“根式公式”？

因为根式公式只允许有限次：

$$+, -, \times, \div, \sqrt[n]{\ }.$$

而四则运算本来就已经被“域”自动包含了。

例如，如果你现在已经在 F_i 里，那么：

$$a+b, \quad a-b, \quad ab, \quad \frac{a}{b}$$

仍然都在 F_i 里。

所以四则运算根本不需要新扩张。

真正会把你带出当前域的，只有：

$$\boxed{\text{开根}}$$

比如：

$$\sqrt[n]{a}$$

可能不在当前域中。

这时候才需要扩张：

$$F_i \longrightarrow F_i(\sqrt[n]{a}).$$

所以从域的角度看，一个根式公式的构造过程，就是：

$$\boxed{F_0 \subset F_1 \subset \cdots \subset F_r}$$

其中每一步都是：

$$F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} \in F_i.$$

这不是人为规定出来的，而是把“有限次四则运算和开根”逐步翻译成域语言以后自然得到的。

比如一个更复杂的表达式：

$$x = \frac{1 + \sqrt{2 + \sqrt[3]{7}}}{3 - \sqrt{5}}.$$

可以按顺序构造：

$$\mathbb{Q}$$

先加入

$$\sqrt[3]{7},$$

得到 F_1；

再加入

$$\sqrt{2 + \sqrt[3]{7}},$$

得到 F_2；

再加入

$$\sqrt{5},$$

得到 F_3。

最后那个除法

$$\frac{1+\sqrt{2+\sqrt[3]{7}}}{3-\sqrt{5}}$$

不需要再扩张，因为 F_3 已经是域，自动允许除法。

所以最终这个数就在 F_3 中。

因此，“方程可以用根式解”的精确含义，最终就是：

> 存在这样一座有限的根式扩张塔，使方程的所有根都落在最顶层。

刚才我说“一次根式扩张的 Galois 结构比较简单”，讲的是这座塔里的**某一层**，不是说整个方程只需要开一次根。

下一步应该继续只研究一层：

$$F \subset F(\alpha), \qquad \alpha^n \in F,$$

看看为什么这一层的自同构只能把

$$\alpha$$

送成

$$\zeta_n^k \alpha.$$

这样会更顺。

14.3 根式公式与根式塔的逐步对应

> 原问题：为什么能用根式解就推出了根式塔

因为“能用根式解”本身，严格翻译成域语言后，几乎就是“存在一座根式塔”。

关键在于：一个根式公式只允许有限次做

$$+,\ -,\ \times,\ \div,\ \sqrt[n]{\ }.$$

而域已经自动对前四种运算封闭，所以真正会让你离开当前域的，只有“开根”。

假设基础域是

$$F_0 = F$$

，比如一般多项式系数所在的域。

如果公式第一步需要

$$\sqrt{a_0}, \qquad a_0 \in F_0,$$

我们就把这个新数记成

$$\alpha_0 = \sqrt{a_0}.$$

于是

$$\alpha_0^2 = a_0 \in F_0,$$

并扩张成

$$F_1 = F_0(\alpha_0).$$

现在因为 F_1 是域，所以任何由 F_0 和 α_0 做四则运算得到的东西都已经自动在 F_1 里，不需要再扩张。

假如下一步公式出现

$$\sqrt[3]{2+\alpha_0}\,,$$

因为

$$2+\alpha_0 \in F_1,$$

记

$$\alpha_1 = \sqrt[3]{2+\alpha_0},$$

那么

$$\alpha_1^3 = 2+\alpha_0 \in F_1.$$

再定义

$$F_2 = F_1(\alpha_1).$$

继续这样做。

所以任何有限的根式表达式都可以逐步翻译成：

$$F_0 \subset F_1 \subset \cdots \subset F_r$$

其中每一步都是

$$\boxed{F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} \in F_i.}$$

这就是根式塔。

例如一个很丑的表达式：

$$x = \frac{1+\sqrt{3+\sqrt[3]{2}}}{2-\sqrt{5}}.$$

可以拆成：

$$F_0 = \mathbb{Q},$$

先加入

$$\alpha_0 = \sqrt[3]{2}, \qquad \alpha_0^3 = 2,$$

得到

$$F_1 = \mathbb{Q}(\alpha_0).$$

再加入

$$\alpha_1 = \sqrt{3+\alpha_0}, \qquad \alpha_1^2 = 3+\alpha_0 \in F_1,$$

得到

$$F_2 = F_1(\alpha_1).$$

再加入

$$\alpha_2 = \sqrt{5}, \qquad \alpha_2^2 = 5,$$

得到

$$F_3 = F_2(\alpha_2).$$

那么最终

$$x = \frac{1+\alpha_1}{2-\alpha_2}$$

已经自动属于 F_3，因为 F_3 是域，允许四则运算。

所以核心就是：

四则运算不需要扩张域；每出现一次新的开根，扩张一次域。

于是：

有限根式表达式 $\Longrightarrow$ 有限根式塔

反过来也一样：如果有一座这样的根式塔，那么塔顶里的元素就是由有限次四则运算和开根逐步构造出来的。

因此在 Galois 理论里，“solvable ***by*** radicals”的严格定义本来就是：

> 存在一个根式扩张塔，使多项式的分裂域包含在塔顶域中。

所以这一步不是一个额外深奥定理，更多是在把“根式公式”精确地翻译成“域扩张语言”。

14.4 各层用的是同一个模板，而非同一个多项式

> 原问题：为什么每一步都要用相同的这个多项式来扩张域

不是每一步都用“同一个多项式”。你看到的

$$F_{i+1} = F_i(\alpha), \qquad \alpha^n = a \in F_i$$

只是我在描述**任意一层根式扩张的通用模板**，这里把下标省略了，所以容易看成每一步都一样。

真正的根式塔应该写成：

$$F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r$$

其中第 i 步是

$$\boxed{F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} = a_i, \quad a_i \in F_i}$$

这里：

$$\alpha_i, \quad n_i, \quad a_i$$

每一步都可以不同。

比如：

$$F_0 = \mathbb{Q}.$$

第一步加入平方根：

$$\alpha_0 = \sqrt{2}, \qquad \alpha_0^2 = 2.$$

所以

$$F_1 = \mathbb{Q}(\sqrt{2}).$$

第二步可能加入三次根：

$$\alpha_1 = \sqrt[3]{1+\sqrt{2}}.$$

那么：

$$\alpha_1^3 = 1 + \sqrt{2} \in F_1.$$

所以：

$$F_2 = F_1(\alpha_1).$$

第三步还可以加入五次根：

$$\alpha_2^5 = 3 + \alpha_1 \in F_2.$$

所以整个过程可能是：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}\right) \subset \cdots$$

对应的多项式分别可能是：

$$x^2 - 2,$$

$$x^3 - (1 + \sqrt{2}),$$

$$x^5 - (3 + \alpha_1),$$

完全不是同一个多项式。

还有一个更细的点值得现在就区分：

我们知道

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

所以 α_i 一定是

$$x^{n_i} - a_i$$

的一个根。

但：

$$\boxed{x^{n_i} - a_i \text{ 不一定是 } \alpha_i \text{ 的最小多项式}}$$

它的最小多项式只需要**整除** $x^{n_i} - a_i$。

例如如果已经在某个域里有 $\sqrt{2}$，然后你说加入

$$\alpha = \sqrt[4]{4},$$

那么

$$\alpha^4 = 4,$$

所以它满足

$$x^4 - 4 = 0.$$

但实际上

$$\alpha = \sqrt{2}$$

早就在域里了，而且最小多项式只有

$$x^2 - 2.$$

所以以后看到

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

你应该把它理解为：

> “第 i 层新加入的元素是某个当前域元素的 n_i 次根。”

而不是：

> “每一层都用同一个 $x^n - a$ 来扩张。”

接下来我们再看“对这一层做共轭/嵌入以后，为什么 $\sigma(\alpha_i)$ 仍然是一个根式”，就会清楚很多。

14.5 单层根式的生成元可能被送到哪里

好，我们就只研究一层：

$$F \subset F(\alpha), \qquad \alpha^n = a \in F.$$

先暂时不谈整座根式塔，也不谈五次方程，只问：

> 如果 σ 是一个固定 F 的自同构，那么它可以把 α 送到哪里？

因为

$$\alpha^n = a,$$

对两边作用 σ：

$$\sigma(\alpha^n) = \sigma(a).$$

由于 σ 保持乘法，

$$\sigma(\alpha^n) = \sigma(\alpha)^n.$$

而因为 σ 固定 F，且 $a \in F$，所以

$$\sigma(a) = a.$$

因此：

$$\boxed{\sigma(\alpha)^n = a}.$$

也就是说：

$$\boxed{\sigma(\alpha) \text{ 也必须是 } x^n - a \text{ 的根}}.$$

这一步最核心。

例如平方根：

$$\alpha^2 = 2.$$

那么 $\sigma(\alpha)$ 也必须满足：

$$x^2 = 2.$$

所以只能是：

$$\sqrt{2}$$

或者

$$-\sqrt{2}.$$

于是：

$$\sqrt{2} \mapsto \sqrt{2}$$

或

$$\sqrt{2} \mapsto -\sqrt{2}.$$

没有第三种可能。

再看三次根：

$$\alpha^3 = 2.$$

那么 $\sigma(\alpha)$ 必须满足：

$$x^3 = 2.$$

在复数中三个根是：

$$\alpha, \qquad \omega\alpha, \qquad \omega^2\alpha,$$

其中

$$\omega^3 = 1.$$

所以：

$$\boxed{\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}}$$

换句话说，它只能把 α 乘上一个三次单位根。

一般地，$x^n = a$ 的根如果取其中一个为 α，那么其余根都是：

$$\alpha, \quad \zeta_n\alpha, \quad \zeta_n^2\alpha, \ldots, \zeta_n^{n-1}\alpha,$$

其中

$$\zeta_n^n = 1.$$

所以：

$$\boxed{\sigma(\alpha) = \zeta_n^k\alpha}$$

对某个 k。

但这里有一个很重要的细节。

如果我们只有：

$$F(\alpha),$$

那么这些别的根未必都在这个域里面。

例如：

$$\mathbb{Q}(\sqrt[3]{2})$$

全部是实数，但

$$\omega\sqrt[3]{2}$$

不是实数。

所以：

$$\omega\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}).$$

因此在这个域内部，根本不存在把

$$\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$$

的自同构，因为目标元素都不在域里。

这也是为什么前面我们后来需要考虑更大的分裂域：

$$\mathbb{Q}(\sqrt[3]{2}, \omega).$$

所以“加入一个根式之后，自同构就是乘单位根”这句话要理解得稍微精确一点：

> 只要我们处在一个包含这些相关根的合适域里，那么固定基础域的自同构对 α 的作用，只能是
>
> $$\alpha \mapsto \zeta_n^k \alpha.$$

而这种变化很特殊，因为它不像任意置换那样乱来。

它只有：

$$\text{乘 } 1,\ \zeta_n,\ \zeta_n^2, \dots$$

这些可能。

这就是为什么根式扩张最终会和“阿贝尔结构”联系起来。下一步可以继续解释：**为什么这些“乘单位根”的操作彼此可交换。**

14.6 方程的全部根与最小多项式的共轭不相同

> 原问题：问题是不一定每一个解都满足这种形式吧

对，你这个质疑是对的。**我刚才那句话说得太强了。**

如果已知

$$\alpha_j^n = a_j$$

那么 α_j 是多项式

$$x^n - a_j$$

的一个根。假设 $\alpha_j \neq 0$，并且 ζ_n 是原始 n 次单位根，那么这个多项式的**所有根**确实都是

$$\boxed{\alpha_j,\ \zeta_n\alpha_j,\ \zeta_n^2\alpha_j, \dots, \zeta_n^{n-1}\alpha_j}$$

因为如果 $\beta^n = a_j$，那么

$$\left(\frac{\beta}{\alpha_j}\right)^n = \frac{\beta^n}{\alpha_j^n} = 1,$$

所以

$$\frac{\beta}{\alpha_j}$$

一定是某个 n 次单位根：

$$\frac{\beta}{\alpha_j} = \zeta_n^k.$$

于是

$$\beta = \zeta_n^k \alpha_j.$$

所以对于方程

$$x^n - a_j = 0,$$

这句话没问题。

但问题在于：

$$\boxed{\alpha_j \text{ 的“代数共轭”未必等于 } x^n - a_j \text{ 的所有根}}$$

因为 α_j 的真正共轭，是它的**最小多项式**的其他根。

而最小多项式只满足：

$$m_{\alpha_j}(x) \mid x^n - a_j.$$

所以共轭根只是上述

$$\zeta_n^k \alpha_j$$

中的**一部分**。

例如取：

$$\alpha = \sqrt{2}.$$

你完全可以说：

$$\alpha^4 = 4.$$

所以 α 满足：

$$x^4 - 4 = 0.$$

如果基础域里有 $i = \zeta_4$，那么 $x^4 - 4$ 的四个根是：

$$\sqrt{2}, \quad i\sqrt{2}, \quad -\sqrt{2}, \quad -i\sqrt{2}.$$

但是 $\sqrt{2}$ 的最小多项式（例如在 $\mathbb{Q}(i)$ 上）仍然是：

$$x^2 - 2,$$

所以它真正的共轭只有：

$$\sqrt{2}, \quad -\sqrt{2}.$$

而：

$$i\sqrt{2}, \quad -i\sqrt{2}$$

虽然是 $x^4 - 4$ 的根，却**不是 $\sqrt{2}$ 的共轭**。

因此刚才那句话应该改成：

> 每一个 α_j 的共轭都必定具有 $\zeta_n^k \alpha_j$ 的形式，但反过来未必全部都是共轭。

这已经足够支持后面的论证，因为一个固定基础域的自同构如果把 α_j 移动了，它只能把它送到它的某个共轭，因此必然仍是：

$$\boxed{\sigma(\alpha_j) = \zeta_n^{k_j}\alpha_j}$$

只是**允许的 k_j 可能只有一部分**，而不是 $0, \dots, n-1$ 全部都能出现。

而“一部分”也没有问题：它仍然落在由单位根乘法形成的阿贝尔结构里面。

14.7 单位根倍数形式仅适用于 $x^n - a$

> 原问题：我是指一个方程的根不一定是这种单位根的形式吧

对，你说得对。**一般多项式方程的根当然不一定是“某个根乘单位根”的形式。**

这种形式只对我们当前这一类特殊方程成立：

$$\boxed{x^n - a = 0}$$

因为如果 $\alpha^n = a$，另一个根 β 也满足

$$\beta^n = a,$$

那么

$$\left(\frac{\beta}{\alpha}\right)^n = 1,$$

所以

$$\frac{\beta}{\alpha}$$

一定是某个 n 次单位根，于是：

$$\beta = \zeta_n^k \alpha.$$

因此：

$$\boxed{x^n - a \text{ 的根一定是 } \zeta_n^k \alpha \text{ 这种形式}}$$

但比如一般三次方程

$$x^3 + x + 1 = 0$$

的三个根，就没有理由满足

$$r_2 = \omega r_1, \qquad r_3 = \omega^2 r_1.$$

一般完全不是这样。

这里之所以一直出现

$$\alpha, \zeta_n \alpha, \zeta_n^2 \alpha, \dots$$

是因为我们现在不是在讨论“原始待解多项式的根长什么样”，而是在讨论**根式公式构造过程中的某一步**。

根式塔的一步是：

$$F_i \subset F_i(\alpha_i),$$

并且特意满足

$$\alpha_i^{n_i} = a_i \in F_i.$$

所以这一层对应的特殊多项式就是：

$$x^{n_i} - a_i.$$

因此这一层才有：

$$\alpha_i \mapsto \zeta_{n_i}^k \alpha_i.$$

这和最终原方程

$$f(x) = 0$$

的根没有直接说成同一种形式。

整个思路其实是：

$$\boxed{\text{一般多项式的根}}$$

如果“能用根式表示”，那么这些根可以通过很多层：

$$+, -, \times, \div, \sqrt[n]{}$$

逐步构造出来。

而我们把每一次“开根”单独拿出来：

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

于是**每一个单独的开根步骤**都有单位根结构。

然后这些简单的阿贝尔结构一层层叠起来，最终限制原多项式的 Galois 群。

所以非常关键的区分是：

$$\boxed{\begin{array}{c}\text{一般方程 } f(x) = 0 \text{ 的根：不一定彼此相差单位根；} \\ \text{一次根式步骤 } x^n - a = 0 \text{ 的根：一定彼此相差 } n \text{ 次单位根.}\end{array}}$$

而 Galois 理论最巧妙的地方就在这里：**原方程可以很一般，但如果它能由一系列这种特殊的“开根步骤”造出来，那么它的 Galois 群就必须继承一种可逐层拆成阿贝尔群的结构。**

14.8 分裂域与阿贝尔性是两个不同条件

> 原问题：换言之得是分裂域是吧

对，基本可以这么理解，但再精确一点：

如果希望 α 的所有共轭根都能作为自同构的像出现，那么我们需要所在的扩张包含这些根。

最自然的做法就是取相关多项式的**分裂域**。

比如

$$\alpha = \sqrt[3]{2}.$$

只看

$$\mathbb{Q}(\alpha)$$

时，另外两个根

$$\omega\alpha, \qquad \omega^2\alpha$$

根本不在这个域里，所以不可能存在域自同构

$$\alpha \mapsto \omega\alpha.$$

而进入分裂域

$$K = \mathbb{Q}(\alpha, \omega)$$

以后，三个根全都在 K 中，于是自同构才有可能在它们之间进行置换。

不过还有一个非常关键的细节：**“是分裂域”本身还不足以保证 Galois 群是阿贝尔的。**

例如

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

确实是 $x^3 - 2$ 的分裂域，但：

$$\mathrm{Gal}(K/\mathbb{Q}) \cong S_3,$$

它反而**不是**阿贝尔群。

为什么？因为自同构不仅可以改变

$$\alpha,$$

还可以改变

$$\omega \leftrightarrow \omega^2.$$

所以真正让“一次根式扩张”对应阿贝尔结构的关键是：**基础域里已经包含相应的单位根。**

例如改成基础域

$$F = \mathbb{Q}(\omega),$$

再加入

$$\alpha = \sqrt[3]{2}.$$

得到：

$$K = F(\alpha) = \mathbb{Q}(\omega, \sqrt[3]{2}).$$

这时 $x^3 - 2$ 已经在 K 中完全分裂：

$$(x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha),$$

而且所有固定 F 的自同构都必须固定 ω。

因此只能有：

$$\alpha \mapsto \alpha,$$

$$\alpha \mapsto \omega\alpha,$$

$$\alpha \mapsto \omega^2\alpha.$$

这三个操作组成：

$$C_3,$$

是阿贝尔群。

所以后面真正要用的是这种结构：

$$\boxed{F \text{ 已含 } \zeta_n, \quad \alpha^n \in F, \quad K = F(\alpha) \text{ 是相应的分裂扩张}}$$

于是自同构只能：

$$\alpha \mapsto \zeta_n^k \alpha,$$

从而这一层的 Galois 群是循环群的子群，因此是阿贝尔的。

这也是为什么严格证明“根式可解 ⇒ Galois 群可解”时，会特意先把需要的**单位根**加入进来。

14.9 单位根必须进入该层的基础域

> 原问题：所以要把单位根加进去

对，准确说是：**要把相应的 n 次单位根加到基础域里。**

如果我们这一层加入的是

$$\alpha = \sqrt[n]{a}, \qquad \alpha^n = a,$$

那么方程

$$x^n - a = 0$$

的所有根都是

$$\alpha,\ \zeta_n\alpha,\ \zeta_n^2\alpha,\ \dots,\ \zeta_n^{n-1}\alpha,$$

其中 ζ_n 是一个原始 n 次单位根：

$$\zeta_n^n = 1.$$

所以如果基础域 F 已经包含 ζ_n，那么一旦加入 α，所有根就自动都进来了：

$$\zeta_n^k\alpha \in F(\alpha).$$

于是

$$F(\alpha)$$

就是 $x^n - a$ 的分裂域。

例如三次根时，先把

$$\omega = e^{2\pi i/3}$$

加入基础域：

$$F = \mathbb{Q}(\omega).$$

再加入

$$\alpha = \sqrt[3]{2}.$$

那么

$$F(\alpha) = \mathbb{Q}(\omega, \sqrt[3]{2})$$

里自动有三个根：

$$\alpha, \quad \omega\alpha, \quad \omega^2\alpha.$$

更重要的是，因为 $\omega \in F$，固定 F 的自同构**不能再动** ω。

因此它只能：

$$\alpha \mapsto \alpha, \quad \alpha \mapsto \omega\alpha, \quad \alpha \mapsto \omega^2\alpha.$$

这就比从 $\mathbb{Q}$ 出发简单很多。

所以这里的关键操作确实是：

先把需要的单位根加入基础域，再逐层加入根式。

而且不需要把每个单位根分别加进去；加入一个**原始 n 次单位根 ζ_n**，它的幂

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$$

就已经给出了全部 n 次单位根。

下一步就可以非常具体地证明：在这种情况下，为什么这一层的自同构群一定是阿贝尔群。

补充证明：单个根式层的群是循环群的子群

设特征为 0，基础域 B 已含全部 n 次单位根 μ_n，$\alpha^n = a \in B$。若 $a = 0$，则 $\alpha = 0$、$B(\alpha) = B$，是平凡扩张。下面设 $a \neq 0$。多项式 $x^n - a$ 的全部根是 $\zeta\alpha$（$\zeta \in \mu_n$），都在 $B(\alpha)$，且无重根；因此 $B(\alpha)/B$ 是 Galois。

对 $\sigma \in \mathrm{Gal}(B(\alpha)/B)$，定义 $\chi(\sigma) = \sigma(\alpha)/\alpha \in \mu_n$。$\alpha$ 的像确定整个自同构，所以 χ 单射。由于 σ 固定 μ_n，

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

所以 χ 是群同态，Galois 群同构于 μ_n 的一个子群。μ_n 由本原单位根 ζ_n 生成，是 n 阶循环群；循环群的子群仍循环：若子群非平凡，取生成元幂中最小正指数 d，用带余除法可知子群所有幂指数都是 d 的倍数。故该层群循环，特别地阿贝尔。χ 不一定满射，不能认定 n 种根像都能出现。

多个根式 $\beta_j^n = a_j \in B$ 的情形类似：令 $E = B(\beta_1, \dots, \beta_m)$，零生成元删去。映射 $\sigma \mapsto (\sigma(\beta_j)/\beta_j)_j$ 给出 $\mathrm{Gal}(E/B) \to \mu_n^m$ 的单射群同态，所以群阿贝尔。各坐标可能受生成元间的代数关系约束，因此不一定等于整个直积，也不能把“每个根式各自的全部倍数根”都叫作其最小多项式的全部共轭。

14.11 固定 $\mathbb{Q}$ 与固定 $\mathbb{Q}(\omega)$ 为什么得到不同的群

> 原问题：对解释为什么不固定omiga就不是固定就是

对，核心就在“**固定基础域**”这几个字。

假设

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega), \qquad \omega^2 + \omega + 1 = 0.$$

如果我们研究

$$\mathrm{Gal}(K/\mathbb{Q}),$$

定义只要求自同构 σ 对所有

$$q \in \mathbb{Q}$$

满足

$$\sigma(q) = q.$$

但是

$$\omega \notin \mathbb{Q},$$

所以定义**没有要求**

$$\sigma(\omega) = \omega.$$

那它能把 ω 送到哪里？

因为

$$\omega^2+\omega+1=0,$$

作用 σ 后：

$$\sigma(\omega)^2+\sigma(\omega)+1=0.$$

所以 $\sigma(\omega)$ 必须仍然是

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

的根，也就是：

$$\boxed{\sigma(\omega)=\omega \quad \text{或} \quad \omega^2}.$$

也就是说，如果基础域只有 $\mathbb{Q}$，自同构可以交换：

$$\omega \leftrightarrow \omega^2.$$

但如果我们把基础域改成

$$F=\mathbb{Q}(\omega),$$

再研究

$$\mathrm{Gal}(K/F),$$

那么定义要求：

$$\sigma(x)=x, \qquad \forall x\in\mathbb{Q}(\omega).$$

而：

$$\omega \in \mathbb{Q}(\omega),$$

所以立即得到：

$$\boxed{\sigma(\omega) = \omega}.$$

这就是为什么“把 ω 加进基础域”以后，它就被固定住了。

更重要的是，不固定 ω 为什么会让群变得不交换。

设

$$r: \quad \alpha \mapsto \omega\alpha, \quad \omega \mapsto \omega,$$

其中

$$\alpha = \sqrt[3]{2}.$$

再设

$$s: \quad \alpha \mapsto \alpha, \quad \omega \mapsto \omega^2.$$

看看先 s 后 r：

$$rs(\alpha) = r(\alpha) = \omega\alpha.$$

而先 r 后 s：

$$sr(\alpha) = s(\omega\alpha) = s(\omega)s(\alpha) = \omega^2\alpha.$$

所以：

$$\boxed{rs(\alpha) \neq sr(\alpha)}$$

因此：

$$\boxed{rs \neq sr}.$$

这正是非交换性出现的来源：一个操作在转动

$$\alpha \to \omega\alpha,$$

另一个操作却还可以把用于“转动”的 ω 本身变成 ω^2。

如果把 ω 放进基础域，第二种自由度就被禁止了，只剩：

$$\alpha \mapsto \omega^k\alpha,$$

这些操作就是指数相加，因此彼此交换。

所以可以把关键区别记成：

$$\boxed{\omega \notin F \Rightarrow \omega \text{ 可能被自同构移动}}$$

而

$$\boxed{\omega \in F \Rightarrow \omega \text{ 必须被所有 } F\text{-自同构固定}}$$

这就是“先加入单位根”在后面证明中的真正作用。

14.12 固定单位根后，单个根式层为什么阿贝尔

现在我们进入整个证明里最关键、也最容易被一句话糊弄过去的地方：

$$\boxed{\text{为什么“加入一个根式”对应的 Galois 结构是阿贝尔的?}}$$

这一步不能直接说“因为开方很简单”，我们从一个最简单的根式扩张开始。

假设基础域是 F，并且我们加入一个元素 α，满足

$$\alpha^n = a, \qquad a \in F.$$

于是得到

$$F(\alpha).$$

这就是一次典型的**根式扩张**。

先问：如果 σ 是一个固定 F 的自同构，那么 α 可以被送到哪里？

因为

$$\alpha^n = a,$$

所以

$$\sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(a) = a.$$

因此

$$\sigma(\alpha)$$

也必须是方程

$$x^n - a = 0$$

的一个根。

现在假设 α 是其中一个根。那么其他根是什么？

就是

$$\alpha,\quad \zeta_n\alpha,\quad \zeta_n^2\alpha,\quad \dots,\quad \zeta_n^{n-1}\alpha,$$

其中

$$\zeta_n = e^{2\pi i/n}$$

是一个 n 次单位根，满足

$$\zeta_n^n = 1.$$

所以任何自同构只能把

$$\alpha$$

送成

$$\boxed{\sigma(\alpha) = \zeta_n^k \alpha}$$

其中某个

$$k \in \{0, 1, \dots, n-1\}.$$

这已经非常受限制了。

先看平方根。

假设

$$\alpha^2 = a.$$

那么二次单位根只有

$$1,\ -1.$$

所以：

$$\sigma(\alpha)=\alpha$$

或者

$$\sigma(\alpha)=-\alpha.$$

因此这种自同构最多就像：

$$\{1,-1\}$$

一样运作。

它当然是阿贝尔的。

再看三次根。

假设

$$\alpha^3=a.$$

三个根：

$$\alpha,\quad \omega\alpha,\quad \omega^2\alpha.$$

如果基础域中已经包含 ω，那么固定基础域的自同构必须固定 ω。

于是自同构只能是：

$$\alpha\mapsto\alpha,$$

$$\alpha \mapsto \omega\alpha,$$

$$\alpha \mapsto \omega^2\alpha.$$

假设定义：

$$\sigma_k(\alpha) = \omega^k\alpha.$$

那么两个这种自同构复合：

$$\sigma_k\sigma_l(\alpha) = \sigma_k(\omega^l\alpha).$$

因为 ω 在基础域里，所以被固定：

$$= \omega^l\sigma_k(\alpha) = \omega^l\omega^k\alpha = \omega^{k+l}\alpha.$$

于是：

$$\sigma_k\sigma_l = \sigma_{k+l}.$$

而加法满足：

$$k + l = l + k.$$

所以：

$$\sigma_k\sigma_l = \sigma_l\sigma_k.$$

因此这个自同构群是阿贝尔的。

更准确地说，它是循环群的一个子群：

$$\boxed{\mathrm{Gal}(F(\alpha)/F) \hookrightarrow C_n}$$

前提是这里的扩张确实是 Galois，并且 F 已经包含所需的 n 次单位根。

这里你可能已经看到最重要的直觉了：

> 加入一个 n 次根式以后，自同构没有办法随意乱排很多根；它基本只能给这个根式乘上一个 n 次单位根。

即：

$$\alpha \mapsto \zeta_n^k \alpha.$$

而这些变化之间本质上就是“指数相加”：

$$k + l.$$

因此它们自然形成一个阿贝尔结构。

所以：

$$\boxed{\text{一次根式扩张产生的 Galois 层，本质上是阿贝尔的}}$$

但这里有一个非常重要的技术细节：

$$\boxed{\text{基础域里必须先有相应的单位根}}$$

否则事情会复杂一点。

例如我们刚才研究

$$x^3-2$$

时，仅有

$$\mathbb{Q}(\sqrt[3]{2})$$

是不够的。

我们还必须加入

$$\omega.$$

所以严格证明“根式可解 $\Rightarrow$ Galois 群可解”时，会先把必要的单位根也加入进来。

加入单位根本身不会破坏“可解性”，因为单位根对应的 Galois 群也是阿贝尔群。

所以最终会得到一座域塔：

$$F=F_0\subset F_1\subset F_2\subset\cdots\subset F_r$$

每一步都是：

$$F_{i+1}=F_i(\alpha_i),\qquad \alpha_i^{n_i}\in F_i,$$

并且把必要的单位根也准备好。

于是每一层对应的 Galois 群商：

$$G_i/G_{i+1}$$

都是阿贝尔群。

于是整个 Galois 群就存在一条：

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{e\}$$

使得：

$$G_i/G_{i+1}$$

全部阿贝尔。

这正好就是：

$$\boxed{\text{可解群}}$$

的定义。

所以现在我们终于得到核心桥梁的一半：

$$\boxed{\text{方程可以用根式解} \Longrightarrow \text{它的 Galois 群是可解群}}$$

下一步最适合做的，不是马上跳到五次方程，而是把这里的**域塔为什么会反过来产生一条 Galois 群的正规子群链**讲清楚。那一步就是 Galois 理论里真正的“域和群反向对应”。

14.13 对整个塔的嵌入使根式关系怎样变化

现在就看这一层：

$$F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} = a_i \in F_i.$$

假设我们有一个固定最底层 F_0 的域嵌入

$$\sigma : F_{i+1} \to \overline{F_0}.$$

我们先只问：α_i 被 σ 送到哪里？

因为

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

对两边作用 σ：

$$\sigma(\alpha_i^{n_i}) = \sigma(a_i).$$

由于 σ 保持乘法：

$$\sigma(\alpha_i)^{n_i} = \sigma(a_i).$$

所以：

$$\boxed{\sigma(\alpha_i) \text{ 是 } x^{n_i} - \sigma(a_i) \text{ 的一个根}}$$

也就是说：

$$\boxed{\sigma(\alpha_i) = \sqrt[n_i]{\sigma(a_i)}}$$

这里的“$= \sqrt[n_i]{\cdots}$”只是表示它是某一个 n_i 次根，不是在指定唯一的主值。

关键是：

$$a_i \in F_i.$$

因此 $\sigma(a_i)$ 属于：

$$\sigma(F_i).$$

于是我们得到：

$$\boxed{\sigma(\alpha_i)^{n_i} \in \sigma(F_i)}$$

这说明什么？

说明原来这一层：

$$F_i \subset F_i(\alpha_i)$$

是通过“加入一个根式”构造的。

做完 σ 以后，对应的共轭版本：

$$\sigma(F_i) \subset \sigma(F_{i+1})$$

仍然是通过加入一个根式构造的：

$$\boxed{\sigma(F_{i+1}) = \sigma(F_i)\big(\sigma(\alpha_i)\big)}$$

而且：

$$\sigma(\alpha_i)^{n_i} = \sigma(a_i) \in \sigma(F_i).$$

所以共轭后的这一层仍然是根式扩张。

这就是前面那句话的真正含义：

$$\boxed{\text{根式扩张在做代数共轭后，仍然是根式扩张}}$$

例如原来：

$$F_1 = \mathbb{Q}(\sqrt{2}),$$

满足：

$$(\sqrt{2})^2 = 2.$$

如果某个嵌入把：

$$\sqrt{2} \mapsto -\sqrt{2},$$

那么共轭后的生成元满足：

$$(-\sqrt{2})^2 = 2.$$

仍然是平方根式。

再比如：

$$\alpha^3 = 1 + \sqrt{2}.$$

如果某个嵌入把：

$$\sqrt{2} \mapsto -\sqrt{2},$$

那么：

$$\sigma(\alpha)^3 = 1 - \sqrt{2}.$$

所以共轭版本仍然只是：

$$\sqrt[3]{1 - \sqrt{2}}$$

这样一个根式。

因此，把原来的根式塔所有共轭版本都一起加入，并不会突然引入某种“超出根式”的神秘元素；每个新生成元仍然满足某个：

$$x^{n_i} - b = 0$$

其中 b 已经在前面的域里。

这就是为什么我们可以把根式塔补成一个更大的、对共轭稳定的 Galois 扩张，同时仍然保持“由根式逐层生成”的性质。

14.14 用 $\sqrt{2}$ 与 $\sqrt{(1+\sqrt{2})}$ 跟踪整座塔的像

> 原问题：这一整套还是不好理解

可以，这里不要再从一般的 F_i, α_i, σ 开始。我们先用一个完整的具体例子，把“为什么要对整座根式塔做嵌入”看明白。

假设我们有这座根式塔：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}\right).$$

先给它们起名字：

$$F_0 = \mathbb{Q},$$

$$F_1 = \mathbb{Q}(\sqrt{2}),$$

$$F_2 = \mathbb{Q}(\sqrt{2}, \alpha),$$

其中

$$\alpha = \sqrt[3]{1+\sqrt{2}},$$

所以

$$\boxed{\alpha^3 = 1+\sqrt{2}}.$$

现在暂时不要想什么“正规闭包”。只问一个问题：

> 如果把第一层里的 $\sqrt{2}$ 换成它的另一个共轭根 $-\sqrt{2}$，第二层会发生什么？

在第一层，

$$F_1 = \mathbb{Q}(\sqrt{2})$$

有一个熟悉的映射：

$$\sigma : \sqrt{2} \mapsto -\sqrt{2}.$$

同时所有有理数保持不动。

所以：

$$1 + \sqrt{2}$$

就会被送成：

$$1 - \sqrt{2}.$$

现在关键来了。

原来的 α 满足：

$$\alpha^3 = 1 + \sqrt{2}.$$

如果我们想把整个代数关系一起搬过去，那么新来的 $\sigma(\alpha)$ 必须满足什么？

因为映射必须保持乘法，所以：

$$\sigma(\alpha^3) = \sigma(\alpha)^3.$$

而原来：

$$\alpha^3 = 1 + \sqrt{2}.$$

所以：

$$\sigma(\alpha)^3 = \sigma(1+\sqrt{2}) = 1 - \sqrt{2}.$$

因此：

$$\boxed{\sigma(\alpha) \text{ 必须是 } 1-\sqrt{2} \text{ 的某个三次根}}$$

比如我们可以把其中一个写成：

$$\sqrt[3]{1-\sqrt{2}}.$$

所以原来的塔：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{1+\sqrt{2}})$$

会产生一个“共轭版本”：

$$\mathbb{Q} \subset \mathbb{Q}(-\sqrt{2}) \subset \mathbb{Q}\left(-\sqrt{2}, \sqrt[3]{1-\sqrt{2}}\right).$$

当然：

$$\mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}),$$

但第二层新出现的三次根可能不在原来的 F_2 中。

这就是我们为什么会说：

> 为了把最终大域做成 Galois 的，我们可能需要把这些“共轭版本”里的根也一起补进来。

而最关键的一点是：

原来第二层是通过开三次根得到的：

$$\alpha^3 = 1 + \sqrt{2}.$$

共轭以后仍然只是开三次根：

$$\sigma(\alpha)^3 = 1 - \sqrt{2}.$$

所以：

做共轭不会把“根式”变成某种更复杂的操作

它仍然是根式。

现在再回头看刚才那个抽象公式就容易很多了。

原来：

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

这句话只是抽象版的：

$$\alpha^3 = 1 + \sqrt{2}.$$

对整个关系做 σ：

$$\sigma(\alpha_i^{n_i}) = \sigma(a_i).$$

因为 σ 保持乘法：

$$\boxed{\sigma(\alpha_i)^{n_i} = \sigma(a_i)}.$$

这只是抽象版的：

$$\sigma(\alpha)^3 = 1 - \sqrt{2}.$$

所以那一大串符号真正想表达的其实只有一句话：

> 如果 α 原来是 a 的 n 次根，那么做共轭以后，$\sigma(\alpha)$ 就是 $\sigma(a)$ 的 n 次根。

这就是这一整套论证真正的核心。

14.15 代数共轭与群共轭的区别

> 原问题：这里的共轭和群元素的共轭到底是不是一个东西

不是一个东西，但**它们有很深的联系**。这里确实要分清楚“代数共轭”和“群共轭”。

你刚选中的“共轭版本”，这里说的是**域论/代数数里的共轭（conjugates）**。

比如

$$\alpha = \sqrt[3]{2}$$

在 $\mathbb{Q}$ 上的最小多项式是

$$x^3 - 2.$$

它的三个根

$$\sqrt[3]{2},\quad \omega\sqrt[3]{2},\quad \omega^2\sqrt[3]{2}$$

叫做 α 在 $\mathbb{Q}$ 上的**共轭元**。

所以这里的“共轭版本”大致是：

$$\boxed{\text{把生成元替换成它们的代数共轭后得到的那些域}}$$

例如：

$$\mathbb{Q}(\sqrt[3]{2})$$

的一个共轭域会是

$$\mathbb{Q}(\omega\sqrt[3]{2}).$$

而你前面群论里学的“共轭”是：

$$\boxed{ghg^{-1}}$$

其中 g,h 是群元素。

这是**群元素之间的一种操作**。

例如在置换群里：

$$\sigma(123)\sigma^{-1}$$

相当于重新给 $1,2,3$ 贴标签。

所以这两个“共轭”形式上完全不同：

代数共轭：同一个最小多项式的不同根

$vs.$

群共轭：$ghg^{-1}.$

但为什么都叫 conjugate?

因为在 Galois 理论里，它们会被自同构联系起来。

如果

$$\sigma \in \mathrm{Gal}(K/F)$$

而 $\alpha \in K$，那么

$$\sigma(\alpha)$$

就是 α 的一个 F–共轭。

也就是说，Galois 群通过自己的群元素 σ，把一个代数元送到它的代数共轭：

$$\alpha \mapsto \sigma(\alpha).$$

所以：

$$\boxed{\text{代数共轭，是 Galois 群作用在元素上得到的不同像}}$$

而群共轭

$$\sigma\tau\sigma^{-1}$$

则是 Galois 群内部不同自同构之间的关系。

所以最好这样记：

$$\boxed{\begin{array}{l}\alpha,\beta \text{ 共轭} \Rightarrow \text{它们是同一最小多项式的根} \\ \sigma,\tau \text{ 共轭} \Rightarrow \tau = g\sigma g^{-1} \text{ 之类}\end{array}}$$

一个是“域里的元素之间”，一个是“群里的元素之间”。

但 Galois 理论把两者桥接起来了。

14.16 共轭补在上层，原基础域保持固定

> 原问题：换言之有了一列之后，要保证最底层的域加入了所有的各种共轭的根

差一点，但关键不是“把所有共轭根都加入最底层域”，而是：

$$\boxed{\text{最底层域 } F_0 \text{ 通常保持不变；我们把所有需要的共轭根加入到上面的扩张域里。}}$$

比如原来有根式塔

$$F_0 \subset F_1 \subset F_2.$$

假设

$$F_0 = \mathbb{Q},$$

$$F_1 = \mathbb{Q}(\sqrt{2}),$$

$$F_2 = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}\right).$$

做共轭以后可能还需要加入

$$\sqrt[3]{1-\sqrt{2}}.$$

我们不是把它塞进最底层：

$$\mathbb{Q}$$

里。

否则基础域就变了。

而是把顶部扩大，例如变成某个更大的域 M：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{1+\sqrt{2}}, \sqrt[3]{1-\sqrt{2}}, \dots\right) = M.$$

目的就是让最终的 M 对所有这些共轭操作都“封闭”，最终能够成为：

$$\boxed{M/F_0 \text{ 的 Galois 扩张}}.$$

所以更准确的图是：

$$\boxed{F_0 \text{ 保持在底部}}$$

然后：

$$\boxed{\text{把原来根式塔缺少的共轭根不断补到上层的大域中}}$$

直到最上面的域对 F_0 的所有共轭都稳定。

只有一个东西我们前面确实有时会“先加到底层附近”，就是**单位根**。比如要处理三次根，我们可能先把

$$\omega$$

加入基础域，得到：

$$F_0' = F_0(\omega).$$

但这和“把所有代数共轭根都放进最底层”是两回事。

所以可以记成：

单位根：为了让每一层根式扩张变成简单的阿贝尔 Galois 层 各个共轭根：主要补到上层，最终把整座塔补成 Galois 大域

你现在这一步如果理解了，下一步就可以解释：**为什么“补齐所有共轭根”以后，最上面的域就会对 F_0 成为正规/Galois 扩张。**

14.17 每层 Galois，顶层仍可能不正规

这里要补的技术缺口是：

> **根式塔的每一层可以很简单，但最顶层对最底层未必是 Galois。**

先看一个很具体的例子。

设

$$F_0 = \mathbb{Q}.$$

第一步加入

$$\sqrt{2},$$

得到

$$F_1 = \mathbb{Q}(\sqrt{2}).$$

第二步再加入

$$\sqrt[4]{2}.$$

因为

$$(\sqrt[4]{2})^2 = \sqrt{2} \in F_1,$$

所以

$$F_2 = F_1(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}).$$

于是我们有根式塔：

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}).$$

而且每一步都是二次扩张。

但是现在看最顶层：

$$F_2/\mathbb{Q}.$$

$\sqrt[4]{2}$ 的最小多项式是

$$x^4 - 2.$$

它的四个根是

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}.$$

可

$$F_2 = \mathbb{Q}(\sqrt[4]{2})$$

完全由实数构成，所以：

$$i\sqrt[4]{2} \notin F_2.$$

因此 $x^4 - 2$ 没有在 F_2 中完全分裂。

所以：

$$\boxed{F_2/\mathbb{Q} \text{ 不是 } \mathbf{Galois}}$$

这说明：

$$\boxed{\text{逐层都很好的扩张，合起来未必对最底层 } \mathbf{Galois}}$$

那为什么这会影响我们前面的证明？

因为我们之前希望统一选一个大域 K，然后定义：

$$G_i = \mathrm{Gal}(K/F_i).$$

最好最终得到：

$$G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}.$$

如果直接取：

$$K = F_r,$$

那确实最后

$$\mathrm{Gal}(K/K) = \{e\}.$$

但问题是：

$$K/F_0$$

未必 Galois。

那么前面我们使用的 Galois 对应、restriction map 等工具就不能这么干净地全部使用。

所以一个自然办法是：

> 把 F_r 再扩大一点，让它变成 F_0 上的 Galois 扩张。

例如刚才：

$$F_2 = \mathbb{Q}(\sqrt[4]{2})$$

缺的是 i。

加入 i：

$$K = \mathbb{Q}(\sqrt[4]{2}, i).$$

那么四个根：

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}$$

就全在 K 中。

所以 K 是

$$x^4 - 2$$

的分裂域，从而：

$$K/\mathbb{Q}$$

是 Galois。

这种“把一个扩张补全到包含所有共轭根”的操作叫做取：

$$\boxed{\text{正规闭包 / normal closure}}$$

可以先把它理解为：

> 原来的域缺哪些共轭根，就把它们都补进来，直到整个域对基础域的共轭操作稳定。

但这里还有第二个问题。

假设原来的根式塔顶层是 F_r，我们把它扩大到一个 Galois 域 K。

那么：

$$F_r \subset K.$$

此时群链是：

$$G_0 \supset G_1 \supset \cdots \supset G_r,$$

其中

$$G_r = \mathrm{Gal}(K/F_r).$$

可是现在一般：

$$G_r \neq \{e\}.$$

因为：

$$F_r \neq K.$$

所以仅仅说“取正规闭包”还不够，我们还没把群链真正降到单位群。

这就是严格证明里真正需要再处理的一步。

解决办法不是随便取一个正规闭包，而是：

> 把原来的根式塔和它所有的共轭版本一起加入

并同时加入必要的单位根。

最后得到一个更大的域 M，满足两件事：

第一：

$$M/F_0$$

本身是 Galois。

第二，M 仍然可以通过一层层根式扩张构造出来。

也就是说我们可以安排成：

$$F_0' \subset F_1' \subset \cdots \subset F_s' = M,$$

每一步：

$$F'_{j+1} = F'_j(\beta_j), \qquad \beta_j^{n_j} \in F'_j,$$

并且相应单位根已经在下面的域里。

这样最顶层真的就是：

$$M.$$

于是定义：

$$G_j = \mathrm{Gal}(M/F'_j).$$

最后：

$$G_s = \mathrm{Gal}(M/M) = \{e\}.$$

现在才真正得到完整链：

$$G_0 \supset G_1 \supset \cdots \supset G_s = \{e\}.$$

而每一层：

$$G_j/G_{j+1} \cong \mathrm{Gal}(F'_{j+1}/F'_j)$$

都是阿贝尔群。

因此：

$$G_0$$

可解。

所以目前你只需要抓住两个层次：

原始的“根式解”给我们：

$$\boxed{\text{一座根式塔}}$$

但这座塔的顶层未必对底层 Galois。

于是严格证明会把它**补大**：

$$\boxed{\text{加入单位根和必要的共轭根}}$$

得到一座更大的：

$$\boxed{\textbf{Galois 根式塔}}$$

这样我们才能从顶到底完整地反向得到：

$$\boxed{\text{正规子群链} + \text{阿贝尔商群}}$$

从而证明 Galois 群可解。

这里“把所有共轭根加入后，为什么仍然能够保持为根式扩张”还有一些技术内容。下一步最好就专门解释这个，而不是直接宣布证明完成。

14.18 所有共轭加入后，为什么得到正规扩张

现在就解释：

$$\boxed{\text{为什么把所有共轭根补齐以后，最上面的域会对 } F_0 \text{ 变成正规扩张}}$$

先用最熟悉的例子。

假设最底层是：

$$F_0 = \mathbb{Q}.$$

原来只有：

$$K = \mathbb{Q}(\sqrt[3]{2}).$$

这里：

$$\alpha = \sqrt[3]{2}$$

的最小多项式是：

$$x^3 - 2.$$

它的三个共轭根是：

$$\alpha, \qquad \omega\alpha, \qquad \omega^2\alpha.$$

可是 K 只有第一个，所以 $K/\mathbb{Q}$ 不正规。

现在把另外两个共轭根也补进来：

$$M = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha).$$

实际上这和

$$\mathbb{Q}(\alpha, \omega)$$

是同一个域。

此时 $x^3 - 2$ 的三个根全部都在 M 里面：

$$x^3 - 2 = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha).$$

所以至少对这个多项式来说，任何把一个根换成另一个共轭根的操作，都不会把我们带出 M。

现在把这个想法推广。

假设最终的大域 M 是由一些代数元生成的：

$$M = F_0(\alpha_1, \alpha_2, \dots, \alpha_r).$$

我们把每一个 α_i 在 F_0 上的所有共轭都加入 M。

也就是说，如果

$$m_i(x) \in F_0[x]$$

是 α_i 的最小多项式，那么我们要求：

$$\boxed{m_i(x) \text{ 的所有根都在 } M}$$

对每个 i 都成立。

现在取一个固定 F_0 的嵌入：

$$\sigma : M \hookrightarrow \overline{F_0}.$$

因为 σ 固定 F_0，所以：

$$\sigma(\alpha_i)$$

必须仍然是 α_i 的最小多项式 $m_i(x)$ 的某个根。

但我们已经把 $m_i(x)$ 的所有根都加入了 M。

所以：

$$\boxed{\sigma(\alpha_i) \in M}$$

对每个生成元都成立。

而整个 M 是由：

$$F_0, \alpha_1, \dots, \alpha_r$$

生成的。

所以只要这些生成元都被送回 M，整个域都会被送回 M：

$$\sigma(M) \subseteq M.$$

再利用有限扩张下嵌入是单射且维数不变，就得到：

$$\boxed{\sigma(M) = M}.$$

这正是正规扩张的核心性质：

> 所有固定基础域 F_0 的嵌入，都把 M 映回 M 自己。

因此：

$$\boxed{M/F_0 \text{ 是正规扩张}}.$$

你也可以从“多项式分裂”的角度理解。

正规扩张的一个等价表述是：

> 如果一个在 $F_0[x]$ 中不可约的多项式，在 M 里有一个根，那么它的所有根都在 M 里。

而我们刚才做的事情正是：

$$\boxed{\text{只要出现一个代数元，就把它所有 } F_0\text{-共轭一起补进来}}$$

所以自然就满足了这个条件。

然后为什么我们敢进一步说“Galois”？

因为在我们现在最终关心的情形里，基础域通常是：

$$\mathbb{Q}$$

或者特征 0 的域。

特征 0 的域上的有限代数扩张自动是**可分的**。

所以：

$$\text{正规} + \text{可分}$$

得到：

$$\boxed{\text{Galois}}.$$

因此在我们这条五次方程的主线上，可以简单理解为：

$$\boxed{\text{补齐所有相关共轭根} \Rightarrow \text{正规} \Rightarrow \text{在特征 } 0 \text{ 下就是 Galois}}$$

下一步就该把这一整套重新接回根式塔，看看：**为什么补齐这些共轭根以后，每一层仍然可以安排成根式扩张，而且最终对应的群链每个商群都是阿贝尔群。**

14.19 再次任取嵌入是检验稳定性

> 原问题：不是很理解为什么要专门又做一个嵌入

这里“再取一个嵌入”不是为了额外构造什么东西，而是为了**检验 M/F_0 是否正规**。

正规扩张的一个很重要的判别方式就是：

$$\boxed{\text{任意固定 } F_0 \text{ 的嵌入 } \sigma : M \hookrightarrow \overline{F_0} \text{ 都必须把 } M \text{ 映回 } M}$$

所以我们必须“随便拿一个这样的 σ”来检查。

你可以把逻辑理解成：

> 我们想证明“无论怎么做，都不会跑出 M”；
>
> 那就必须先任取一种允许的做法 σ，然后证明它确实不会跑出去。

这和证明一个集合对某个操作封闭很像。比如要证明：

$$A \text{ 对加法封闭}$$

你会写：

$$\text{任取 } a, b \in A,$$

然后证明：

$$a + b \in A.$$

这里完全一样。

我们要证明：

$$M/F_0 \text{ 正规},$$

于是就：

$$\text{任取固定 } F_0 \text{ 的嵌入 } \sigma : M \hookrightarrow \overline{F_0},$$

然后证明：

$$\sigma(M) = M.$$

所以这个 σ 是一个“测试者”。

不是说原来没有映射，现在人为又加一个映射进去；而是：

正规性的定义/判别本身就要求考虑所有这样的嵌入

为什么这种嵌入能检测“共轭根是否都补齐”？

因为如果

$$\alpha_i \in M,$$

那么任何固定 F_0 的嵌入都会把 α_i 送到它的某个 F_0–共轭：

$$\alpha_i \mapsto \sigma(\alpha_i).$$

所以如果 M 漏掉了某个共轭根，就可能有一个嵌入把：

$$\alpha_i$$

送到那个漏掉的根，于是：

$$\sigma(M) \not\subseteq M.$$

例如：

$$M = \mathbb{Q}(\sqrt[3]{2}).$$

有嵌入：

$$\sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}.$$

但是：

$$\omega\sqrt[3]{2} \notin M.$$

所以立刻看出：

$$M/\mathbb{Q}$$

不正规。

反过来，如果我们已经把所有共轭根都补进去了，那么无论你取哪个 σ：

$$\sigma(\alpha_i)$$

都还在 M 里。

于是整个 M 都被送回 M。

所以这一段的核心可以压成：

> 引入 σ 是为了测试：所有可能的共轭变化会不会把 M 带出去。

如果不会，M/F_0 就具有正规性。

14.20 需要证明补齐共轭后仍保持根式结构

下一步就该把刚才留下的技术缺口补上：

为什么把根式塔的所有代数共轭一起加入后，仍然可以保持“根式扩张”的结构

这一步很重要，因为我们前面只是说“把原来的根式塔补成一个 Galois 的大域”，但还没证明这个补大的过程不会把“根式可解”这件事破坏掉。

具体来说，假设原来某一层是

$$F_{i+1} = F_i(\alpha), \qquad \alpha^n = a \in F_i.$$

如果我们对整个结构做一个 F_0–嵌入 σ，那么这一关系会变成

$$\sigma(\alpha)^n = \sigma(a).$$

因此新的代数共轭 $\sigma(\alpha)$ 仍然是某个元素 $\sigma(a)$ 的 n 次根。

也就是说，**共轭后的生成元仍然是通过开根得到的**。

于是把所有这些共轭生成元逐个加入，仍然可以写成一连串根式扩张。

这一步讲清楚后，我们就能得到一个真正严密的结论：

根式可解的多项式可以嵌入一个 Galois 的根式扩张中

然后再把这个 Galois 根式塔反向变成群链，最终推出：

根式可解 $\Rightarrow$ Galois 群可解

所以接下来最合适的就是从

$$\alpha^n = a$$

出发，具体看为什么做域嵌入以后会自动得到

$$\sigma(\alpha)^n = \sigma(a),$$

以及这为什么保证“共轭版本仍然是根式”。

14.21 同时加入多个根式时，群仍然阿贝尔

下一步就要把刚才“补齐共轭根”这件事，重新接回**根式塔 → 阿贝尔商群**。而且这里要比前面更精确一点：补齐共轭以后，一层里可能不再只加入一个根式，而是同时加入若干个同次数根式。

先看原来某一层：

$$F_i \subset F_{i+1} = F_i(\alpha), \qquad \alpha^n = a \in F_i.$$

如果为了让整个大域对最底层正规，我们把 α 的各种共轭版本也补进来，那么可能需要同时加入：

$$\alpha_1, \alpha_2, \dots, \alpha_m,$$

它们分别满足：

$$\alpha_1^n = a_1, \qquad \alpha_2^n = a_2, \qquad \dots, \qquad \alpha_m^n = a_m,$$

其中这些

$$a_j$$

都已经在前一层的大域中。

于是补大后的这一层更像：

$$\boxed{E_{i+1} = E_i(\alpha_1, \ldots, \alpha_m)}$$

而不是简单的

$$E_i(\alpha).$$

现在假设相关的 n 次单位根

$$\zeta_n$$

已经在 E_i 里。

那么对每个 α_j，方程 $x^n - a_j$ 的所有根都有下面的形式；实际的代数共轭可能只占其中一部分：

$$\alpha_j, \quad \zeta_n \alpha_j, \quad \zeta_n^2 \alpha_j, \ldots$$

所以一个固定 E_i 的自同构 σ，对每一个 α_j 都只能做：

$$\boxed{\sigma(\alpha_j) = \zeta_n^{k_j} \alpha_j}$$

这里不同的 j 可以对应不同的指数 k_j。

因此一个自同构大致可以用这一串指数描述：

$$(k_1, k_2, \ldots, k_m).$$

如果再有另一个自同构对应：

$$(l_1, l_2, \ldots, l_m),$$

那么两者复合，对每个生成元都是：

$$\alpha_j \mapsto \zeta_n^{k_j+l_j}\alpha_j.$$

所以整体上就是：

$$(k_1,\dots,k_m)+(l_1,\dots,l_m)$$

按坐标相加。

而坐标相加满足：

$$k_j+l_j=l_j+k_j.$$

因此这些自同构彼此交换。

所以即使补齐共轭以后，一层需要同时加入很多根式，这一层的 Galois 群仍然是：

$$\boxed{\text{阿贝尔群}}$$

更准确地说，它可以嵌入到若干循环群的直积中，例如：

$$C_n \times C_n \times \cdots \times C_n.$$

这一步非常关键，因为它解决了你刚才可能隐约担心的问题：

> “原来一个根式的 Galois 群是阿贝尔的，但为了补成正规扩张加入了一堆共轭根以后，会不会又变复杂？”

答案是：**不会变成非阿贝尔的那种复杂性**。只要单位根已经固定，每个根式仍然只能独立地“乘一个单位根”，这些操作仍然交换。

所以现在我们可以把补大的根式塔写成：

$$E_0 \subset E_1 \subset \cdots \subset E_r = M,$$

其中：

- M/E_0 是 Galois；
- 每一层 E_{i+1}/E_i 也是 Galois；
- 并且每一层的 Galois 群都是阿贝尔群。

下一步就可以非常干净地定义：

$$G_i = \mathrm{Gal}(M/E_i),$$

得到反向群链

$$G_0 \supset G_1 \supset \cdots \supset G_r = \{e\},$$

然后逐层证明：

$$\boxed{G_i/G_{i+1} \cong \mathrm{Gal}(E_{i+1}/E_i)}$$

所以每个商群都是阿贝尔群。到那一步，“为什么根式可解会推出 Galois 群可解”就真正闭环了。

第 15 章：完整搭桥：根式可解 $\Rightarrow$ Galois 群可解

本章对象：F 始终是原基础域；M_i 是补大的域，M 是最终的 Galois 大域，L 是原方程的分裂域；返回原方程要用 $\mathrm{Gal}(M/F)$，不能漏掉加入单位根的一层。

15.1 为什么要把限制映射用于根式塔

下一步就是把刚才这个 restriction map 用到**根式塔**上。

我们已经有：

$$F_0 \subset F_1 \subset \cdots \subset F_r$$

并且每一步都是一种根式扩张，理想情况下写成：

$$F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} \in F_i,$$

同时相关的单位根已经放进基础层，使每一步都成为 Galois 且其 Galois 群是阿贝尔的。

然后我们取一个足够大的最终 Galois 扩张 K/F_0，把这些 F_i 都放在 K 里面。

接着定义：

$$G_i = \mathrm{Gal}(K/F_i).$$

由于域越大，固定它的自同构越少，所以得到反向链：

$$\boxed{G_0 \supset G_1 \supset \cdots \supset G_r}$$

然后利用刚才得到的公式：

$$\mathrm{Gal}(K/F_i)/\,\mathrm{Gal}(K/F_{i+1}) \cong \mathrm{Gal}(F_{i+1}/F_i),$$

也就是：

$$\boxed{G_i/G_{i+1} \cong \mathrm{Gal}(F_{i+1}/F_i)}$$

右边因为这一层是根式扩张并且单位根已固定，所以是阿贝尔群。

于是：

$$G_i/G_{i+1}$$

也是阿贝尔群。

这样就得到一条正规子群链，每一层商群都阿贝尔，于是：

$$\boxed{G_0 \text{ 是可解群}}$$

也就是：

$$\boxed{\text{根式可解} \Rightarrow \textbf{Galois 群可解}}$$

所以下一步就是**具体把这一条“域塔反向变成群链”的过程写出来并逐层解释**。

15.2 条件充分时，把域塔反向翻译为群链

我们先在一个**结构最干净的情形**下把“域塔 $\to$ 群链”真正看懂；等这一步理解后，再处理一般根式塔里那个技术细节。

假设我们有一串域：

$$F_0 \subset F_1 \subset F_2 \subset K$$

并且暂时假设：

$$K/F_0$$

是 Galois 扩张，而且每一层

$$F_{i+1}/F_i$$

也都是 Galois 扩张。

现在定义三个群：

$$G_0 = \mathrm{Gal}(K/F_0),$$

$$G_1 = \mathrm{Gal}(K/F_1),$$

$$G_2 = \mathrm{Gal}(K/F_2).$$

注意这些群里的自同构，**作用的对象始终都是同一个大域 K**。

区别只在于“要求固定多少东西”。

对于 G_0，只要求固定：

$$F_0.$$

对于 G_1，要求固定更大的：

$$F_1.$$

所以限制更严格，允许的自同构更少：

$$G_1 \subseteq G_0.$$

同理：

$$G_2 \subseteq G_1.$$

所以域链：

$$F_0 \subset F_1 \subset F_2$$

会反向变成：

$$\boxed{G_0 \supset G_1 \supset G_2}$$

这一步应该比较直观。

现在真正关键的是：

$$G_0/G_1$$

代表什么？

我们刚才已经证明过一般公式：

如果

$$F \subset E \subset K$$

并且条件合适，那么：

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong \mathrm{Gal}(E/F).$$

现在把：

$$F = F_0, \qquad E = F_1$$

代进去。

左边就是：

$$\mathrm{Gal}(K/F_0)/\mathrm{Gal}(K/F_1).$$

也就是：

$$G_0/G_1.$$

所以：

$$\boxed{G_0/G_1 \cong \mathrm{Gal}(F_1/F_0)}$$

这个式子的直觉是：

> G_0 包含所有固定 F_0 的变化；
>
> G_1 是其中那些连 F_1 都完全固定的变化。
>
> 把 G_1 这种“在 F_1 上看不见的变化”除掉以后，剩下来的正好就是 F_1/F_0 这一层能够发生的变化。

再看第二层。

同样：

$$G_1/G_2 = \mathrm{Gal}(K/F_1)/\,\mathrm{Gal}(K/F_2).$$

所以：

$$\boxed{G_1/G_2 \cong \mathrm{Gal}(F_2/F_1)}$$

因此：

$$\boxed{\begin{array}{ccc} F_0 & \subset & F_1 \subset F_2 \\ \\ G_0 & \supset & G_1 \supset G_2 \end{array}}$$

而且相邻两层满足：

$$\boxed{G_i/G_{i+1} \cong \mathrm{Gal}(F_{i+1}/F_i)}$$

这就是整个桥。

现在把“根式”放进来。

假设第一层是：

$$F_1 = F_0(\alpha_0),$$

其中

$$\alpha_0^{n_0} \in F_0,$$

并且 F_0 已经含有相应的 n_0 次单位根。

我们前面已经知道，这时候：

$$\mathrm{Gal}(F_1/F_0)$$

是阿贝尔群。

于是根据：

$$G_0/G_1 \cong \mathrm{Gal}(F_1/F_0),$$

立即得到：

$$\boxed{G_0/G_1 \text{ 是阿贝尔群}}.$$

同理，如果：

$$F_2 = F_1(\alpha_1), \qquad \alpha_1^{n_1} \in F_1,$$

并且需要的单位根已经在 F_1 中，那么：

$$\mathrm{Gal}(F_2/F_1)$$

也是阿贝尔群。

于是：

$$\boxed{G_1/G_2 \text{ 是阿贝尔群}}.$$

继续下去就得到：

$$G_0 \supset G_1 \supset G_2 \supset \cdots$$

其中：

$$\boxed{G_i/G_{i+1} \text{ 全部是阿贝尔群}}$$

而这正是“可解群”所要求的结构。

所以现在已经能看到整个证明的骨架：

$$\boxed{\text{根式塔中的每一层是阿贝尔 Galois 扩张}}$$

通过 Galois 对应变成：

$$\boxed{\text{Galois 群的一层层正规子群，且相邻商群阿贝尔}}$$

于是总 Galois 群可解。

不过这里我刚才特意说了“**结构最干净的情形**”。因为一般的根式表达式产生的最顶层域，未必自动就是 F_0 上的 Galois 扩张，所以不能不加说明就直接把它叫作 K。

下一步应该补这个技术缺口：为什么证明一般的“根式可解 $\Rightarrow$ Galois 群可解”时，要把根式塔适当扩大成一个 Galois 的大域。 这一步补完以后，这个方向的证明才真正严密。

补充完整构造：从原根式塔到对原基础域 Galois 的大域

这是证明中不能略过的部分。把原基础域始终记为 F，不因加入单位根而改名。原塔为 $F = F_0 \subseteq \ldots \subseteq F_r$，其中 $F_{i+1} = F_i(\alpha_i)$，$\alpha_i^{n_i} = a_i \in F_i$。取 N 为所有 n_i 的最小公倍数，在同一个代数闭包内取 $M_0 = F(\mu_N)$。

M_0 是 x^N-1 在 F 上的分裂域，所以 M_0/F 是 Galois。任意 F 自同构把 ζ_N 送到某个同阶根 ζ_N^k，其中 k 与 N 互素。自同构由 ζ_N 的像决定；复合对应指数相乘模 N，所以

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

右端是模 N 的可逆剩余类在乘法下组成的群，乘法交换，故左端阿贝尔。$N = 1$ 的情形 $M_0 = F$，群平凡。于是“加入单位根”这一层也被纳入对原基础域的可解性证明。

归纳假设 M_i/F 是有限 Galois 扩张，且 $F_i \subseteq M_i$。令 $A_i = \sigma(a_i) : \sigma \in \mathrm{Gal}(M_i/F)$，这是一个有限集合。定义 M_{i+1} 为在 M_i 上加入所有 $x^{n_i} - b$（$b \in A_i$）的全部根所得的域。恒等自同构给出 $b = a_i$，因此原先的 α_i 也在其中，$F_{i+1} \subseteq M_{i+1}$。

由于 $\mu_{n_i} \subseteq M_0 \subseteq M_i$，对每个非零 b 只需选一个根 β_b，其他根都是单位根倍数；M_{i+1}/M_i 是这些多项式的分裂域，所以 Galois，且其群嵌入 μ_{n_i} 的有限直积，因此阿贝尔。

还必须证明 M_{i+1}/F 整体正规。任取固定 F 的嵌入 $\tau : M_{i+1} \to \Omega$。因 M_i/F 正规，$\tau(M_i) = M_i$，且 $\tau|_{M_i}$ 是 M_i 的 F 自同构。它把集合 A_i 置换回自身；若 $\beta^{n_i} = b \in A_i$，则 $\tau(\beta)^{n_i} = \tau(b) \in A_i$，所以 $\tau(\beta)$ 也是已经加入的根。这使所有生成元都回到 M_{i+1}，故 $\tau(M_{i+1}) \subseteq M_{i+1}$；有限维数给出等号。于是 M_{i+1}/F 正规，特征 0 保证可分，故 Galois。归纳完成。

最后得到 $F \subseteq M_0 \subseteq \ldots \subseteq M_r = M$，$M/F$ Galois，M_0/F 的群阿贝尔，且每层 M_{i+1}/M_i 的群阿贝尔。令 $H_{-1} = \mathrm{Gal}(M/F)$，$H_i = \mathrm{Gal}(M/M_i)$，则

$$H_{-1} \triangleright H_0 \triangleright H_1 \triangleright \cdots \triangleright H_r = \{e\}, \quad H_{-1}/H_0 \cong \mathrm{Gal}(M_0/F), \quad H_i/H_{i+1} \cong \mathrm{Gal}(M_{i+1}/M_i).$$

限制映射与第一同构定理使每个相邻商群阿贝尔，所以 $\mathrm{Gal}(M/F)$ 可解。这里始终固定原来的 F，已经避免了原对话中“把底层扩大成 E_0，然后直接返回原 F_0 的群”的缺口。

若 L 是原多项式的分裂域且 $L \subseteq F_r \subseteq M$，则 L/F Galois，限制映射 $\mathrm{Gal}(M/F) \to \mathrm{Gal}(L/F)$ 满射，核是 $\mathrm{Gal}(M/L)$。所以 $\mathrm{Gal}(L/F)$ 是可解群的商群，仍可解。即使只知道一个根在根式塔中，正规的大域 M 也包含该根的所有 F 共轭；对不可约原多项式，这就包含全部根。

15.4 根式可解推出群可解：主链合流

> 原问题：好吧，那继续吧

现在我们把前面已经建立的东西真正拼起来，证明这个方向：

$$\boxed{\text{根式可解} \Longrightarrow \text{Galois 群可解}}$$

先把原方程记成

$$f(x) \in F_0[x].$$

假设它可以用根式求解。意思是：存在一座根式塔，最终能够容纳 $f(x)$ 的全部根。

经过我们前面讨论的“加入必要单位根、补齐共轭”的处理，可以把它整理成一座更大的塔：

$$E_0 \subset E_1 \subset \cdots \subset E_r = M,$$

其中 M/E_0 是 Galois，并且每一步仍然由根式产生。

现在对这座塔反向定义：

$$G_i = \mathrm{Gal}(M/E_i).$$

于是：

$$G_0 = \mathrm{Gal}(M/E_0),$$

而最顶部因为

$$E_r = M,$$

所以

$$G_r = \mathrm{Gal}(M/M) = \{e\}.$$

因此得到群链：

$$\boxed{G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}}$$

注意方向反过来了：域越大，需要固定的东西越多，因此允许的自同构越少。

现在看相邻两层：

$$E_i \subset E_{i+1}.$$

前面已经建立过：

$$\boxed{G_i/G_{i+1} \cong \mathrm{Gal}(E_{i+1}/E_i)}$$

在我们整理好的根式塔中，每一层都是由若干根式产生，而且相关单位根已经在 E_i 里面。

所以这一层的自同构只能对这些新加入的根式做类似

$$\alpha \mapsto \zeta_n^k \alpha$$

的变化。

因此：

$$\mathrm{Gal}(E_{i+1}/E_i)$$

是阿贝尔群。

于是通过上面的同构：

$$\boxed{G_i/G_{i+1} \text{ 也是阿贝尔群}}$$

对每个 i 都成立。

所以我们得到了：

$$G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{e\},$$

而且：

$$G_i/G_{i+1}$$

每一层都是阿贝尔群。

这恰好就是“可解群”的定义。

因此：

$$\boxed{G_0 \text{ 是可解群}}.$$

但这里还有最后一个小问题。

我们真正关心的并不一定是这个较大的

$$G_0 = \mathrm{Gal}(M/E_0),$$

而是原方程 $f(x)$ 的 Galois 群。

设 L 是 $f(x)$ 的分裂域，那么：

$$L \subset M.$$

原方程的 Galois 群是：

$$\mathrm{Gal}(L/F_0).$$

这里必须使用固定原基础域 F_0 的大群 $\mathrm{Gal}(M/F_0)$。如果 E_0 已加入单位根，不能直接把原方程的群当作 $\mathrm{Gal}(M/E_0)$ 的商群。上一节完整构造已证明 $\mathrm{Gal}(M/F_0)$ 可解；限制到 L 后，原方程的群才是它的商群。

而：

$$\boxed{\text{可解群的商群仍然可解}}$$

所以原方程的 Galois 群也必须可解。

最终得到：

$$\boxed{f(x) \text{ 可以用根式求解} \Longrightarrow \mathrm{Gal}(f/F_0) \text{ 是可解群}}$$

这就是我们真正需要的方向。

现在距离“五次方程为什么没有一般根式公式”已经很近了。

接下来最自然的是把这个结论应用到**一般五次方程**：

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0.$$

我们需要理解为什么它的“通用 Galois 群”是

$$\boxed{S_5},$$

然后利用我们之前已经证明的：

$$S_5 \text{ 不可解},$$

推出：

$$\boxed{\text{一般五次方程不可能有根式通解}}.$$

这一步会把前面学的所有东西真正合流。

15.5 追问证明在哪里建立：核查当时的两处缺口

> 原问题：这是哪里建立的

这段追问保留了我检查证明是否真正成立的过程。原讨论发现的缺口在本版前文已经补证，下面的检查用于辨认哪些步骤不能一句话带过。

我们是在刚才“根式塔 $\to$ 群链”那几步里建立的，不过严格说，**我们已经把证明骨架搭出来了，但还有两个技术性小结论没有完全证明**，所以我刚才说“已经建立”稍微快了一点。

完整逻辑是这样的：

$$\boxed{\text{方程能用根式解}}$$

首先被翻译成存在一座根式塔：

$$F_0 \subset F_1 \subset \cdots \subset F_r,$$

其中每一步

$$F_{i+1} = F_i(\alpha_i), \qquad \alpha_i^{n_i} \in F_i.$$

也就是每一步只增加一次“开根”。

然后我们讨论了为什么要加入必要的单位根，并把塔补大，使最终可以放进一个 Galois 的根式扩张：

$$E_0 \subset E_1 \subset \cdots \subset E_r = M.$$

对于整理好的每一层：

$$E_{i+1}/E_i,$$

因为相应单位根已经固定，所以自同构只能类似于

$$\alpha \mapsto \zeta_n^k \alpha.$$

于是这一层的 Galois 群是阿贝尔群：

$$\boxed{\mathrm{Gal}(E_{i+1}/E_i) \text{ 阿贝尔}}.$$

然后我们定义：

$$G_i = \mathrm{Gal}(M/E_i).$$

域越大，固定它的自同构越少，所以得到反向链：

$$G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}.$$

接着利用我们之前讲的 restriction map + 第一同构定理：

$$\boxed{G_i/G_{i+1} \cong \mathrm{Gal}(E_{i+1}/E_i)}$$

所以每一个商群

$$G_i/G_{i+1}$$

都是阿贝尔群。

因此：

$$G_0 \supset G_1 \supset \cdots \supset \{e\}$$

就是一条“相邻商群全是阿贝尔群”的正规子群链。

而这正是：

$$\boxed{G_0 \text{ 是可解群}}$$

的定义。

最后，原多项式的分裂域 L 包含在这个更大的 M 中，因此原多项式的 Galois 群

$$\mathrm{Gal}(L/F_0)$$

可以从这个较大的可解 Galois 群得到；于是它也可解。

所以整条链是：

$$
\boxed{
\begin{aligned}
&\text{根式可解} \Rightarrow \text{存在根式塔} \\
&\qquad\quad \Rightarrow \text{可补成 Galois 根式塔} \\
&\qquad\quad \Rightarrow \text{每一层 Galois 群阿贝尔} \\
&\qquad\quad \Rightarrow \text{总 Galois 群有阿贝尔商群链} \\
&\qquad\quad \Rightarrow \text{总 Galois 群可解} \\
&\qquad\quad \Rightarrow \text{原方程的 Galois 群可解.}
\end{aligned}
}
$$

原对话在这个阶段发现了两处尚缺的证明（本版已在第 7 章和第 15 章补齐）：

$$
\boxed{\text{① 根式塔补成 Galois 大域后，仍能保持合适的根式塔结构}}
$$

以及

$$
\boxed{\text{② 可解群的商群仍然可解}}
$$

所以更严谨的说法应该是：

> **只理解骨架还不够，必须分别验证正规化根式塔的构造和商群的可解性。本版已经把这两个验证写在主结论之前。**

我建议下一步就先补 ② **可解群的商群为什么仍然可解**，因为非常短；然后再回头确认整个 Abel–Ruffini 证明链有没有遗漏。

15.6 原方程的群为什么是大群的商群

下一步最合适的是补上这条：

$$
\boxed{\text{可解群的商群仍然是可解群}}
$$

因为我们刚才得到的通常是一个较大的 Galois 扩张 M/F，并证明

$$G = \mathrm{Gal}(M/F)$$

可解；但原方程真正的分裂域可能只是

$$L \subset M.$$

我们最终要从 G 推到原方程的

$$\mathrm{Gal}(L/F).$$

而这个群会是 G 的一个商群。因此必须知道：

$$G \text{ 可解} \quad \Longrightarrow \quad G/N \text{ 可解}.$$

这一步其实很短，而且正好把前面的证明链补完整。

证明时我们会从 G 的可解链

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

出发，然后看它经过商映射

$$G \to G/N$$

以后，会变成怎样的一条子群链，并解释为什么每一层商群仍然是阿贝尔群。

把这一点补完之后，我们就可以比较严谨地宣布：

$$\boxed{\text{根式可解} \Rightarrow \text{原方程的 Galois 群可解}}$$

然后再回到 S_5 和一般五次方程。

15.7 可解群的商群仍可解

现在就可以把它放回我们的 Galois 问题。

我们之前构造了一个较大的 Galois 根式扩张：

$$M/F,$$

并得到：

$$G = \mathrm{Gal}(M/F)$$

是可解群。

而原多项式的分裂域记作：

$$L, \qquad F \subset L \subset M.$$

考虑限制映射：

$$\mathrm{Gal}(M/F) \longrightarrow \mathrm{Gal}(L/F).$$

它的核是：

$$\mathrm{Gal}(M/L).$$

因此第一同构定理给：

$$\boxed{\mathrm{Gal}(M/F)/\,\mathrm{Gal}(M/L) \cong \mathrm{Gal}(L/F)}$$

所以原方程的 Galois 群是较大的可解群的一个**商群**。

而我们刚刚证明：

可解群的商群仍然可解.

因此：

$$\boxed{\text{方程可用根式解} \Longrightarrow \mathrm{Gal}(L/F) \text{ 可解}}$$

到这里，这个方向的核心证明链已经真正接上了。

下一步最合适的是回到一般五次方程，仔细补上另一个关键点：**为什么“一般五次方程”的 Galois 群确实是 S_5，而不仅仅是 S_5 的某个子群。**

15.8 逐元素证明像链的相邻商群阿贝尔

现在这个结论终于可以放回 Galois 理论。

如果我们通过根式塔构造出了一个较大的 Galois 扩张

$$M/F$$

并证明：

$$G = \mathrm{Gal}(M/F)$$

是可解群。

而原方程的分裂域是：

$$F \subset L \subset M,$$

那么限制映射给出：

$$\mathrm{Gal}(M/F) \longrightarrow \mathrm{Gal}(L/F).$$

其核是：

$$\mathrm{Gal}(M/L).$$

所以：

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(M/F)/\mathrm{Gal}(M/L).$$

左边就是**原方程真正的 Galois 群**。

右边是一个可解群的商群，因此也是可解群。

于是我们现在可以比较完整地写出：

$$\boxed{\text{方程可以用根式解} \Longrightarrow \text{方程的 Galois 群是可解群}}$$

下一步就该回到五次方程，仔细解决我们此前略快的一点：

$$\boxed{\text{为什么“一般五次方程”的 Galois 群不是仅仅 } S_5 \text{ 的子群，而确实是整个 } S_5\text{。}}$$

这一步完成后，S_5 不可解和“五次无根式通解”就能真正接上。

第 16 章：一般方程的群与 Abel–Ruffini 定理

本章对象：$r_1, \dots, r_n$ 是代数独立不定元；e_j 是 j 阶基本对称式，区别于群单位元 e；系数域 $F = \mathbb{Q}(e_1, \dots, e_n)$，分裂域 $K = \mathbb{Q}(r_1, \dots, r_n)$。

16.1 一般五次方程的形式根与对称系数

现在进入最后这条主线里最关键的一步：

$$\boxed{\text{为什么“一般五次方程”的 Galois 群是 } S_5}$$

这里我们先把“一般五次方程”说清楚。不是某个具体的

$$x^5 - 2 = 0,$$

而是系数代数独立的一般首一多项式：

$$\boxed{x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0}$$

我们现在假设它有五个根：

$$r_1, r_2, r_3, r_4, r_5.$$

根据韦达定理，系数由根的**对称组合**决定：

$$r_1 + r_2 + r_3 + r_4 + r_5 = -a_4,$$

$$\sum_{i<j} r_i r_j = a_3,$$

一直到

$$r_1 r_2 r_3 r_4 r_5 = -a_0.$$

关键就在“对称”两个字。

假设我们交换：

$$r_1 \leftrightarrow r_2.$$

那么：

$$r_1 + r_2 + r_3 + r_4 + r_5$$

不会改变。

所有两两乘积的和也不会改变。

所有三三乘积的和也不会改变。

……

所以所有系数：

$$a_0, \dots, a_4$$

全部不变。

其实不只是交换 r_1, r_2。

对五个根进行**任意置换**

$$\sigma \in S_5$$

都会保持这些系数不变。

所以从“系数能看到的信息”来看：

$$r_1, r_2, r_3, r_4, r_5$$

一开始是完全对称的。

这已经提示：

> 一般情形下，五个根的全部 $5!$ 种置换都可能成为 Galois 自同构

也就是：

$$S_5.$$

不过这还只是直觉。我们可以把它说得更精确。

不要先写具体数字系数，而是假设五个根

$$r_1, \dots, r_5$$

是“完全独立的一般变量”。

先构造一个大域：

$$K = \mathbb{Q}(r_1, r_2, r_3, r_4, r_5).$$

然后定义五个基本对称多项式：

$$e_1 = r_1 + \cdots + r_5,$$

$$e_2 = \sum_{i<j} r_i r_j,$$

一直到：

$$e_5 = r_1 r_2 r_3 r_4 r_5.$$

再定义基础域：

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

这个 F 可以理解成：

> “只知道一般五次方程系数时，我们拥有的信息”。

因为一般五次方程就是：

$$(x - r_1) \cdots (x - r_5)$$

展开以后得到：

$$x^5 - e_1 x^4 + e_2 x^3 - e_3 x^2 + e_4 x - e_5.$$

也就是说，系数全部属于 F。

现在任取：

$$\sigma \in S_5.$$

例如：

$$\sigma = (123).$$

它把：

$$r_1 \to r_2, \quad r_2 \to r_3, \quad r_3 \to r_1$$

而其他根不动。

这个置换自然诱导一个 K 的自同构：

$$r_i \mapsto r_{\sigma(i)}.$$

但是因为：

$$e_1, \dots, e_5$$

都是**对称的**，任意根置换之后它们完全不变。

例如：

$$\sigma(e_1) = e_1,$$

$$\sigma(e_2) = e_2,$$

等等。

所以这个自同构固定整个：

$$F.$$

因此：

$$\sigma \in \mathrm{Gal}(K/F).$$

而这对每一个：

$$\sigma \in S_5$$

都成立。

所以至少：

$$S_5 \subseteq \mathrm{Gal}(K/F).$$

另一方面，Galois 自同构必须把多项式的根重新排列，所以它不可能做出比“五个根的置换”更多的事情。

因此：

$$\mathrm{Gal}(K/F) \subseteq S_5.$$

两边合起来：

$$\boxed{\mathrm{Gal}(K/F) \cong S_5}$$

这就是所谓：

$$\boxed{\text{一般五次方程的 Galois 群是 } S_5}$$

现在前面所有东西终于可以接起来。

我们已经证明过：

$$A_5$$

是非阿贝尔单群。

因此：

$$S_5$$

不可解。

另一方面，我们刚刚建立：

$$\boxed{\text{如果一个方程能用根式解} \Longrightarrow \text{它的 Galois 群可解}}$$

但是一般五次方程：

$$\mathrm{Gal} = S_5$$

而：

$$S_5 \text{ 不可解.}$$

矛盾。

所以：

$$\boxed{\text{一般五次方程不存在根式通解}}$$

这已经是 Abel–Ruffini 定理背后的核心逻辑。

但这里还有一个非常重要的措辞必须再次强调：

不是“所有五次方程都不能用根式解”

而是：

不存在一个能够解决所有一般五次方程的根式公式

某些具体五次方程的 Galois 群是可解群，因此当然仍然可以根式求解。

下一步最值得做的是补最后一个细节：**为什么“一般 n 次方程”在 $n \geq 5$ 时都没有根式通解，而不只是五次。** 这一步会非常短，因为一旦 S_5 已经出现，S_n（$n \geq 5$）的障碍基本就已经确定了。

补充证明：“一般变量”与“任意置换给出自同构”的准确含义

称 $r_1, \ldots, r_n$ 在 $\mathbb{Q}$ 上代数独立，是指任意非零多元多项式 $P \in \mathbb{Q}[X_1, \ldots, X_n]$ 都满足 $P(r_1, \ldots, r_n) \neq 0$。可以直接取 r_i 为不定元；$K = \mathbb{Q}(r_1, \ldots, r_n)$ 就是有理函数域，元素为多项式之比，分母非零。

$\pi \in S_n$ 对多项式环的作用是把每个 r_i 换为 $r_{\pi(i)}$。这保持加法乘法，逆置换给出逆映射，因此非零多项式不会变成零，非零分母不会消失。故该作用延伸为 K 的域自同构，也不存在选取不同分式表示造成的歧义。e_j 是 j 个不同变量乘积的总和；置换只重新排列这些求和项，所以固定每个 e_j，也固定 $F = \mathbb{Q}(e_1, \ldots, e_n)$。

还要确认这些系数没有额外代数关系。对变量按 $r_1 > r_2 > \ldots > r_n$ 的字典序排列单项式，e_j 的最高单项式是 $r_1 \ldots r_j$。因此 $e_1^{a_1} \cdots e_n^{a_n}$ 的最高单项式中，r_i 的指数为 $a_i + \ldots + a_n$。这个指数向量唯一确定 $a_1, \ldots, a_n$（相邻指数相减即可）。于是不同的 e 单项式有不同最高单项式；任何非零多项式 $P(e_1, \ldots, e_n)$ 的最高项都不能被抵消，故不为零。这证明 $e_1, \ldots, e_n$ 代数独立，可以作为一般系数。

多项式 $\Pi(x-r_i)$ 的系数在 F，所有根是互不相同的 r_i，且 K 由这些根生成。因此 K/F 是有限可分分裂域。自同构 σ 固定系数，故把每个 r_i 送到某个 r_j；生成元的像唯一确定 σ，这给出忠实的群作用 $\mathrm{Gal}(K/F)\to S_n$。上面的变量置换给出了该作用的每个可能输出，因此是同构。这里不是仅凭“两边可以嵌入”猜测相等，而是直接证明同一个根作用既单射又满射。

对一般首一多项式 $x^n+a_{n-1}x^{n-1}+\ldots+a_0$，令 $a_{n-j}=(-1)^j e_j$，就得到同一个系数域。因此这确实是通用多项式的模型；特化为具体系数后可能产生额外关系，不能把 S_n 的结论不加条件地套到每个具体多项式。

16.3 任意形式根置换确实产生系数固定的自同构

现在我们把“**一般五次方程为什么真的得到整个 S_5**”这一步讲严谨一点。先只证明其中一半：

五个根的任意置换，确实都产生一个固定系数的自同构

这里最重要的是，“一般五次方程”不能先取某个具体的五次方程。我们要把五个根先当成**彼此独立的形式变量**：

$$r_1,r_2,r_3,r_4,r_5.$$

你可以暂时把它们理解成五个没有额外代数关系的“抽象根”。

然后考虑包含它们的域：

$$K=\mathbb{Q}(r_1,r_2,r_3,r_4,r_5).$$

这个记号表示：从 $\mathbb{Q}$ 出发，把五个 r_i 加进来，然后允许四则运算。

接下来定义基本对称式：

$$e_1=r_1+r_2+r_3+r_4+r_5,$$

$$e_2 = \sum_{i<j} r_i r_j,$$

$$e_3 = \sum_{i<j<k} r_i r_j r_k,$$

$$e_4 = \sum_{i<j<k<l} r_i r_j r_k r_l,$$

$$e_5 = r_1 r_2 r_3 r_4 r_5.$$

于是：

$$(x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5)$$

展开以后就是：

$$x^5 - e_1 x^4 + e_2 x^3 - e_3 x^2 + e_4 x - e_5.$$

所以我们把：

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

看成“只知道一般五次方程系数时所知道的域”。

现在取一个具体置换，比如：

$$\sigma = (12).$$

我们规定：

$$r_1 \mapsto r_2, \qquad r_2 \mapsto r_1,$$

其余：

$$r_3, r_4, r_5$$

不动。

因为整个 K 都是由这些 r_i 和有理数通过四则运算生成的，所以这个规则会自然决定 K 中其他元素怎么变化。

例如：

$$\frac{r_1 + r_3}{r_2 - r_5}$$

就被送成：

$$\frac{r_2 + r_3}{r_1 - r_5}.$$

所以这确实给出了一个：

$$\sigma : K \to K.$$

而且交换两次就回来，所以显然是双射。

因此它是 K 的域自同构。

关键来了：它固定不固定 F？

看：

$$e_1 = r_1 + r_2 + r_3 + r_4 + r_5.$$

交换 r_1, r_2：

$$\sigma(e_1) = r_2 + r_1 + r_3 + r_4 + r_5 = e_1.$$

再看：

$$e_2 = \sum_{i<j} r_i r_j.$$

因为它把**所有两两乘积全部加起来**，交换两个根只会重新排列这些项，不会改变总和。

所以：

$$\sigma(e_2) = e_2.$$

同理：

$$\sigma(e_3) = e_3,$$

$$\sigma(e_4) = e_4,$$

$$\sigma(e_5) = e_5.$$

因此：

$$\sigma$$

固定：

$$e_1, \dots, e_5.$$

而 F 就是由这些 e_i 和 $\mathbb{Q}$ 生成的，所以：

$$\boxed{\sigma(x) = x, \qquad \forall x \in F}.$$

因此：

$$\sigma \in \mathrm{Gal}(K/F).$$

而这里完全没有用到 (12) 的特殊性。

任意：

$$\pi \in S_5$$

都可以定义：

$$r_i \mapsto r_{\pi(i)}.$$

所有 e_i 都是对称式，所以全部保持不变。

因此：

$$\boxed{\text{每一个 } \pi \in S_5 \text{ 都给出一个固定 } F \text{ 的 } K\text{-自同构}}$$

所以：

$$\boxed{S_5 \subseteq \mathrm{Gal}(K/F)}$$

这里的意思不是字面上两个集合一定相同，而是 S_5 可以自然嵌入这个 Galois 群。

接下来还要证明反方向：

$$\boxed{\mathrm{Gal}(K/F) \subseteq S_5}$$

也就是：**固定这些系数的自同构除了重新排列五个根以外，不可能再做别的事情。**

这一半其实正好用到你刚才问过的“Galois 自同构为什么必须把根送到根”。我们下一步把它在这个“一般五次方程”的具体构造里完整写出来。

16.4 根的作用忠实：Galois 群没有其他自由度

现在证明另一边：

$$\boxed{\mathrm{Gal}(K/F) \subseteq S_5}$$

我们仍然保持刚才的记号：

$$K = \mathbb{Q}(r_1, r_2, r_3, r_4, r_5),$$

而

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

对应的一般五次多项式是

$$f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5)$$

也就是

$$f(x) = x^5 - e_1 x^4 + e_2 x^3 - e_3 x^2 + e_4 x - e_5.$$

现在任取一个

$$\sigma \in \mathrm{Gal}(K/F).$$

这句话具体意味着：

$$\sigma : K \to K$$

是域自同构，并且固定 F 中所有元素。

尤其固定：

$$e_1, e_2, e_3, e_4, e_5.$$

考虑根 r_1。

因为

$$f(r_1) = 0,$$

对这个等式作用 σ：

$$\sigma(f(r_1)) = 0.$$

由于 $f(x)$ 的所有系数都属于 F，而 σ 固定 F，所以这些系数完全不动。

因此：

$$f(\sigma(r_1)) = 0.$$

也就是说：

$$\boxed{\sigma(r_1) \text{ 仍然是 } f(x) \text{ 的根}}$$

而 $f(x)$ 的根正好只有：

$$r_1, r_2, r_3, r_4, r_5.$$

所以：

$$\sigma(r_1) \in \{r_1, r_2, r_3, r_4, r_5\}.$$

同理：

$$\sigma(r_2), \dots, \sigma(r_5)$$

也全都属于这五个根。

现在还需要注意：σ 不可能把两个不同根送到同一个根。

例如不可能同时有：

$$\sigma(r_1) = r_3, \qquad \sigma(r_2) = r_3.$$

因为 σ 是自同构，所以一定是单射。

如果

$$\sigma(r_1) = \sigma(r_2),$$

单射就推出：

$$r_1 = r_2,$$

与这五个一般根彼此不同矛盾。

因此：

$$r_1, \dots, r_5$$

经过 σ 后仍然是一一对应地重新排列。

所以每一个 Galois 自同构都对应一个置换：

$$\boxed{\sigma \longmapsto \pi_\sigma \in S_5}$$

例如某个 σ 可能满足：

$$r_1 \mapsto r_3, \quad r_2 \mapsto r_1, \quad r_3 \mapsto r_2, \quad r_4 \mapsto r_4, \quad r_5 \mapsto r_5,$$

那它对应的置换就是：

$$(132)$$

之类。

而且一旦知道 σ 怎么处理这五个根，整个 σ 就完全确定。

因为：

$$K = \mathbb{Q}(r_1, \dots, r_5).$$

K 中任意元素都是由有理数和这些 r_i 通过四则运算构造出来的。

例如：

$$x = \frac{r_1 r_3 + r_5}{r_2 - r_4}.$$

只要知道每个 r_i 被送到哪里，就自动知道：

$$\sigma(x) = \frac{\sigma(r_1)\sigma(r_3) + \sigma(r_5)}{\sigma(r_2) - \sigma(r_4)}.$$

所以两个不同的 Galois 自同构不可能对应同一个根置换。

因此：

$$\boxed{\mathrm{Gal}(K/F) \hookrightarrow S_5}$$

也就是：

$$\boxed{\mathrm{Gal}(K/F) \text{ 可以看成 } S_5 \text{ 的一个子群}}$$

而上一节我们已经证明反方向：

$$\boxed{S_5 \hookrightarrow \mathrm{Gal}(K/F)}$$

因为五个一般根的**任意置换**都会保持所有对称系数 $e_1, \ldots, e_5$ 不变。

所以两边合起来：

$$\boxed{\mathrm{Gal}(K/F) \cong S_5}$$

这才是真正说明：

> **一般五次方程具有完整的 S_5 对称性，而不是某个更小的置换群。**

还有一个细节很值得你现在注意：这里的 $r_1, \ldots, r_5$ 一开始被当作彼此独立的“形式根”；它们虽然不是普通具体数字，但相对于系数域 F，每个 r_i 又都是代数的，因为都满足这个五次方程 $f(x) = 0$。

下一步就可以把这个结论和前面的

$$S_5 \text{ 不可解}$$

以及

$$\text{根式可解} \Rightarrow \text{Galois 群可解}$$

真正合起来，完整写出 Abel–Ruffini 的最后推理。

16.5 把群的不可解性转化为无根式通解

现在终于可以把前面的链条合起来。

我们已经有三个结论：

$$\boxed{1.\ \text{一般五次方程的 Galois 群是 } S_5}$$

$$\boxed{2.\ S_5 \text{ 不可解}}$$

$$\boxed{3.\ \text{如果一个方程能用根式解，那么它的 Galois 群必须可解}}$$

现在假设“一般五次方程”存在一个根式通解。

也就是说，我们可以只利用它的系数，通过有限次

$$+, -, \times, \div, \sqrt[n]{\ }$$

写出它的根。

根据第 3 条，这就会推出：

$$\mathrm{Gal}(K/F)$$

是可解群。

但一般五次方程的 Galois 群我们刚证明是：

$$\mathrm{Gal}(K/F) \cong S_5.$$

于是推出：

$$S_5 \text{ 可解.}$$

可我们前面已经证明：

$$S_5 \text{ 不可解.}$$

矛盾。

所以最初假设错误：

$$\boxed{\text{一般五次方程不存在根式通解}}$$

这就是 Abel–Ruffini 定理的核心结论。

但这里有一个非常重要的逻辑点。

我们证明的是：

$$\boxed{\text{不存在一个适用于所有五次方程的根式公式}}$$

并不是：

$$\boxed{\text{每一个具体五次方程都不能用根式解}}$$

比如：

$$x^5 - 1 = 0$$

当然可以解。

甚至一些结构更复杂的五次方程，只要其具体 Galois 群是可解群，也仍然可以用根式解。

真正的问题是：

> 一般五次方程具有完整的 S_5 对称性，而 S_5 太“复杂”，无法通过一层层阿贝尔的根式扩张构造出来。

这句话其实就是整套理论的直观核心：

$$\boxed{\text{根式只能逐层制造“可解的对称性”，}}$$

而一般五次方程需要：

$$\boxed{S_5}$$

这种不可解的对称性。

下一步最值得讲的是：**为什么四次及以下却可以有根式通解**。这样你就会看到“5”为什么恰好是分界点。

16.6 推广到高次需要可解群的子群引理

下一步就是把“五次”推广到所有

$$n \geq 5.$$

这里用到第 7 章已经补证的群论结论：

$$\boxed{\text{可解群的子群仍然是可解群}}$$

为什么这个结论有用？因为当

$$n \geq 5$$

时，

$$S_n$$

里面天然包含一个 S_5。

例如在 S_7 里，我们只允许置换

$$1, 2, 3, 4, 5$$

而让

$$6, 7$$

始终不动。

这些置换本身就组成一个子群：

$$H \leq S_7,$$

而且

$$H \cong S_5.$$

一般地：

$$\boxed{S_5 \leq S_n \qquad (n \geq 5)}$$

这里的意思就是：S_n 里面有一个结构完全等同于 S_5 的子群。

我们前面已经知道：

$$S_5 \text{ 不可解.}$$

假如反过来假设：

$$S_n \text{ 可解},$$

那么因为“可解群的子群仍然可解”，它里面的这个 S_5 子群也必须可解。

于是得到：

$$S_5 \text{ 可解},$$

和前面的结果矛盾。

因此：

$$\boxed{S_n \text{ 在所有 } n \geq 5 \text{ 时都不可解}}$$

于是对一般 n 次方程：

$$\mathrm{Gal} \cong S_n,$$

当

$$n \geq 5$$

时这个 Galois 群不可解，而根式可解又要求 Galois 群可解，所以：

$$\boxed{\text{一般 } n \text{ 次方程在 } n \geq 5 \text{ 时没有根式通解}}$$

这里依赖的结论已在第 7 章逐元素证明：

$$\boxed{\text{可解群的子群仍然可解}}$$

所以下一步最合适的就是把这个证明掉。这样从 S_5 推到所有 S_n，$n \geq 5$ 就完全没有缺口了。

16.7 为什么所有 $n \geq 5$ 的一般方程都受同一障碍限制

> 原问题：那为什么6次及以上也不行

因为对“一般 n 次方程”，它的 Galois 群是

$$S_n.$$

所以关键变成：

$$\boxed{\text{为什么}n \geq 5\text{时，}S_n\text{都不可解？}}$$

原因很简单：当 $n \geq 5$ 时，S_n 里面都包含一个和 S_5 完全一样的子群。

例如在 S_6 里，只置换前五个元素：

$$1, 2, 3, 4, 5$$

而始终固定 6。

这些置换组成一个子群：

$$H = \{\sigma \in S_6 : \sigma(6) = 6\}.$$

这个 H 和 S_5 完全同构：

$$H \cong S_5.$$

同样，对任意 $n \geq 5$，只置换前五个元素、固定剩下的元素，就得到：

$$S_5 \leq S_n.$$

而我们已经知道：

$$S_5 \text{ 不可解.}$$

另一方面有一个群论结论：

$$\boxed{\text{可解群的任何子群也都是可解群}}$$

所以如果 S_n 可解，那么它里面的这个 S_5 子群也必须可解。

但这与

$$S_5 \text{ 不可解}$$

矛盾。

因此：

$$\boxed{S_n \text{ 对所有 } n \geq 5 \text{ 都不可解}}$$

再结合一般 n 次方程：

$$\mathrm{Gal} \cong S_n,$$

以及

$$\text{根式可解} \Rightarrow \mathrm{Galois} \text{ 群可解},$$

就得到：

$$\boxed{\text{一般 } n \text{ 次方程在所有 } n \geq 5 \text{ 时都没有根式通解}}$$

所以“五次”之所以是分界点，不是因为 6、7、8 次出现了什么全新的障碍，而是因为：

S_5 这个不可解结构从 $n = 5$ 开始就已经出现，并且一直嵌在所有 S_n 里。

下一步如果继续，最自然的是证明刚才用到的：

可解群的子群为什么仍然可解

这个证明也不长。

最后检查：本篇证明了哪个方向

正文证明的是根式可解 $\Rightarrow$ Galois 群可解，并用其逆否命题得到 Galois 群不可解 $\Rightarrow$ 不能根式求解。这已经足够证明 Abel–Ruffini。原对话中提到的完整判别“根式可解 $\Longleftrightarrow$ Galois 群可解”还包含反方向；反方向不是本篇上述论证的结果，不能把它当成已由正方向自动证明。某些具体五次方程可根式求解，例如 $x^5 - 2$ 的根是 $\sqrt[5]{2}$ 乘五次单位根；这里把根式记作五次根，正文正式公式写为 $\sqrt[5]{2}\zeta_5^k$。

推广到 $n \geq 5$ 时，只需“子群保持可解”及前五个对象上的 S_5 子群，不需要提前证明 A_n 对所有 $n \geq 5$ 都是单群。一般 n 次方程的群为 S_n 已在上一节对任意 n 证明，所以推广没有额外的“群等于 S_n”缺口。

证明依赖与复习检查

本篇到无根式通解的每个必要连接都有明确落点：循环到换位及奇偶性在第 2—3 章；陪集计数和商群良定义在第 4—5 章；第一同构定理在第 6 章；可解性的子群、商群、扩张引理在第 7 章；A_5 的类型计数、共轭类计数、单群性及不可解性在第 8 章；最小多项式和塔式定理在第 9 章；域嵌入延拓及正规性在第 10—11 章；具体根作用在第 12 章；限制映射的良定义、核与满射在第 13 章；单位根与根式层在第 14 章；整个塔的正规化及返回原基础域在第 15 章；一般系数模型和 $n \geq 5$ 的结论在第 16 章。

复习时我可以逐项自问：这个符号是什么对象？映射的输入和输出是什么？此处固定的是哪一个域？为什么能构成群或商群？为什么该映射单射或满射？这一步的正规性是相邻层的，还是整个顶层对最底层的？最终返回原方程时有没有漏掉加入单位根的一层？

原对话覆盖索引

下表用于确认原有证明和解释均有去处。顺序已经重排；部分回答的群论证明和域论应用拆到不同章，原式与论证分别保留。$A42$—$A45$ 是文档工具讨论，不含本篇所需的数学证明；完整原回答仍保存在资料文件中。

原回答	本篇位置	内容
$A01$	第 1 章	从韦达关系发现根的置换
$A02$	第 2 章	置换的复合、单位元和逆：群的定义
$A03$	第 2 章	循环记号、乘法顺序与非交换性
$A04$	第 3 章	换位个数的奇偶性为何定义良好
$A05$	第 3 章	逐条检查偶置换确实构成群
$A06$	第 2 章	置换群这个具体模型
$A07$	第 3 章	交错群作为对称群的子群
$A08$	第 4 章	左陪集与分组的含义
$A09$	第 5 章	右陪集与正规子群
$A10$	第 5 章	商群的元素为什么是陪集
$A11$	第 5 章	代表元计算：陪集乘法的良定义

原回答	本篇位置	内容
$A12$	第 5 章	检查商群的全部群公理
$A13$	第 2 章	为什么任意置换都可写成不相交循环
$A14$	第 3 章	把循环写成一行排列，再计算逆序数
$A15$	第 2 章	把循环拆成换位：原问题所需的连接
$A16$	第 7 章	可解群的定义与 S_3 的可解列
$A17$	第 7 章	阿贝尔商群如何逐层消去非交换部分
$A18$	第 7 章	S_4 的可解列
$A19$	第 7 章	V_4 的正规性与三阶商群为何循环
$A20$	第 4 章	用陪集证明 Lagrange 定理
$A21$	第 4 章	不同陪集为什么相同或不相交
$A22$	第 8 章	从 S_4 走到 S_5：单群障碍
$A23$	第 8 章	A_5 的循环类型及元素数目
$A24$	第 8 章	共轭就是重新给循环贴标签
$A25$	第 8 章	用共轭类并集与整除条件证明 A_5 单群
$A26$	第 9 章	域与域扩张：允许使用哪些数
$A27$	第 9 章	完整验证 $\mathbb{Q}(\sqrt{2})$ 的元素形式
$A28$	第 9 章	代数元、最小多项式、扩张次数
$A29$	第 9 章	塔式定理的乘积基构造

原回答	本篇位置	内容
$A30$	第 11 章	分裂域：把一个多项式的全部根加入
$A31$	第 10 章	域自同构与 Galois 群
$A32$	第 12 章	$\mathbf{Gal}$ 记号的斜杠指基础域
$A33$	第 12 章	生成元与向量空间的基
$A34$	第 12 章	生成域的四则运算规则
$A35$	第 12 章	计算三次分裂域的六个自同构
$A36$	第 14 章	固定单位根后，单个根式层为什么阿贝尔
$A37$	第 14 章	把一个根式表达式拆成逐次开根
$A38$	第 14 章	单层根式的生成元可能被送到哪里
$A39$	第 14 章	分裂域与阿贝尔性是两个不同条件
$A40$	第 14 章	单位根必须进入该层的基础域
$A41$	第 14 章	固定 $\mathbb{Q}$ 与固定 $\mathbb{Q}(\omega)$ 为什么得到不同的群
$A46$	第 14 章	进入根式塔前回顾两条主线
$A47$	第 13 章	域越大，固定它的自同构越少
$A48$	第 13 章	中间域正规时，对应子群为何正规
$A49$	第 13 章	域的整体稳定不等于固定每个单位根
$A50$	第 13 章	限制映射连接域层和群层
$A51$	第 13 章	限制映射的核

原回答	本篇位置	内容
$A52$	第 6 章、第 13 章	第一同构定理的陪集证明
$A53$	第 6 章	核这个集合记号逐个符号拆解
$A54$	第 6 章	像是实际能够到达的目标元素
$A55$	第 13 章	限制映射满射的准确问题
$A56$	第 11 章	以 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 理解延拓和限制
$A57$	第 11 章	嵌入、代数闭包、延拓的对象类型
$A58$	第 11 章	正规性为什么让嵌入变回自同构
$A59$	第 10 章	嵌入的单射条件
$A60$	第 10 章	域同态的核与乘法群同态的核
$A61$	第 9 章	域的理想为什么只有零理想和整个域
$A62$	第 9 章	先定义环和理想，理解吸收性质
$A63$	第 11 章	单个代数元上的嵌入延拓构造
$A64$	第 13 章	同态、嵌入、同构、自同构及两层映射
$A65$	第 13 章	哪些对象属于群层，哪些属于域层
$A66$	第 13 章	限制映射、核、像与商群的角色逐一对应
$A67$	第 13 章	从定义再次验证限制映射的核
$A68$	第 13 章	映射的输入元素本身也是映射
$A69$	第 15 章	为什么要把限制映射用于根式塔

原回答	本篇位置	内容
$A70$	第 15 章	条件充分时，把域塔反向翻译为群链
$A71$	第 14 章	每层 Galois，顶层仍可能不正规
$A72$	第 14 章	代数共轭与群共轭的区别
$A73$	第 14 章	需要证明补齐共轭后仍保持根式结构
$A74$	第 14 章	各层用的是同一个模板，而非同一个多项式
$A75$	第 14 章	对整个塔的嵌入使根式关系怎样变化
$A76$	第 14 章	用 $\sqrt{2}$ 与 $\sqrt{(1+\sqrt{2})}$ 跟踪整座塔的像
$A77$	第 14 章	共轭补在上层，原基础域保持固定
$A78$	第 14 章	所有共轭加入后，为什么得到正规扩张
$A79$	第 14 章	再次任取嵌入是检验稳定性
$A80$	第 14 章	同时加入多个根式时，群仍然阿贝尔
$A81$	第 14 章	方程的全部根与最小多项式的共轭不相同
$A82$	第 14 章	单位根倍数形式仅适用于 $x^n - a$
$A83$	第 15 章	根式可解推出群可解：主链合流
$A84$	第 16 章	一般五次方程的形式根与对称系数
$A85$	第 12 章	系数固定的自同构为何把根送到根
$A86$	第 16 章	推广到高次需要可解群的子群引理
$A87$	第 15 章	追问证明在哪里建立：核查当时的两处缺口

原回答	本篇位置	内容
$A88$	第 14 章	根式公式与根式塔的逐步对应
$A89$	第 15 章	原方程的群为什么是大群的商群
$A90$	第 7 章、第 15 章	可解群的商群仍可解
$A91$	第 7 章	逐元素证明群链的像仍形成正规链
$A92$	第 7 章、第 15 章	逐元素证明像链的相邻商群阿贝尔
$A93$	第 16 章	任意形式根置换确实产生系数固定的自同构
$A94$	第 16 章	根的作用忠实：Galois 群没有其他自由度
$A95$	第 16 章	把群的不可解性转化为无根式通解
$A96$	第 16 章	为什么所有 $n \geq 5$ 的一般方程都受同一障碍限制