

从多项式到分圆域：我的 Galois 理论补充笔记

第一版（2026-10-06）：参照本地 v4-2026-10-05 的章节、符号速查、完整证明、追问和公式复制格式整理。HTML 是主要阅读文件，Markdown 是配套源文件。

原始材料：《介绍多项式与分圆域》分享对话。正文覆盖 49 段可见数学回答；**A01—A49** 是核对用的原回答编号，不表示本篇阅读顺序。

这份笔记接在伽罗瓦理论主线之后，补上我在多项式、单位根和分圆域上反复追问的基础。这里“整式”沿用原对话的理解，指多项式；代数整数尚未系统展开。

按知识依赖调整阅读顺序，把后补的解释移到需要它的位置。正文保留原解释的证明和具体例子；“原问题”摘出我的实际请求，选中的上下文仍保存在原材料。标为“补充证明”的内容是本版新增的推导。原解释中的“你”“我们”不代表我已经独立完成证明；其中回顾或预告的结果，以本篇相应证明章节为准。

先抓住五个观念

核心观念	需要时去哪里找
不可约与最小多项式必须说明基础域；加入代数元后，最小多项式次数等于扩张次数	第 1 章
本原 n 次单位根就是阶恰为 n ；阶是第一次回到 1 的幂次数	第 2—3 章
Φ_n 把阶恰为 n 的根收集起来， $\varphi(n)$ 数这些根；编号 n 不等于多项式次数	第 4—5 章

核心观念	需要时去哪里找
整数系数与有理数域上的不可约性分别要证明；二者成立后， Φ_n 才成为本原单位根的最小多项式	第 6—9 章
分圆域包含全部单位根；自同构由生成元的像决定，复合对应指数相乘	第 10—11 章

忘记阶公式时，回到 $(\zeta_n^a)^d = 1 \iff n \mid ad$ ，再找最小正整数 d 。这比把每个公式单独背下来更方便。

目录

- 第 1 章：多项式、最小多项式与域扩张
- 第 2 章：复指数与全部单位根
- 第 3 章：本原单位根、阶与互素
- 第 4 章：分圆多项式：按阶收集根
- 第 5 章：欧拉函数的计数与两个恒等式
- 第 6 章：整数系数：首一除法与强归纳法
- 第 7 章：域的特征、有限域与 Frobenius
- 第 8 章：导数、重根与可分性
- 第 9 章：完整证明分圆多项式在有理数域上不可约
- 第 10 章：分裂域、正规性与 Galois 扩张
- 第 11 章：分圆域的自同构与模 n 可逆元群
- 第 12 章：复习重点与后续学习边界

常用符号速查

记号	对象、含义与读法
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	整数环、有理数域、实数域、复数域
$F[x]; F[\alpha]; F(\alpha)$	多项式环; 代入 α 生成的环; 加入 α 生成的域
$m_{\alpha, F}; [E : F]$	相对于 F 的首一最小多项式; 向量空间维数, 不是除法
ζ_n	zeta 下标 n ; 固定取 $e^{2\pi i/n}$, 是一个本原 n 次单位根
$\mu_n; \text{ord}(\alpha)$	全部 n 次单位根; 元素的乘法阶
$\Phi_n(x); \varphi(n)$	大写 Phi: 第 n 个分圆多项式; 小写 phi: 欧拉函数, 两个不同对象
$\gcd(a, n); d \mid n; p \nmid n$	正的最大公因数; 整除; 不整除
$\mathbb{F}_p; \mathbb{F}_p[x]$	模素数 p 的有限域; 该域上的多项式环
$\bar{f}; f'$	系数逐项模 p 后的多项式; 形式导数。上横线用于复数时也可表示复共轭, 依局部语境区别
$\text{char } F$	域的特征: 多少个单位元相加首次得到零, 或特征零
$\mathbb{F}_p(t); \overline{F}$	有理函数域, t 是不定元; 代数闭包
$[a] \in \mathbb{Z}/n\mathbb{Z}$	模 n 的剩余类; 方括号不是扩张次数
$(\mathbb{Z}/n\mathbb{Z})^\times$	剩余类环中可逆元组成的乘法群; 上标 $\times$ 表示可逆元集合
$\sigma_a; \Psi$	域自同构 $\zeta_n \mapsto \zeta_n^a$; 从可逆剩余类到自同构的群同构

记号	对象、含义与读法
$C_m; C_2 \times C_2$	m 阶循环群；四元 Klein 群

基本约定： $n \geq 1$, p 是素数；“首一”指最高次项系数为 1。本原单位根的“本原”指阶，本原整数多项式的“本原”指系数最大公因数为 1。两者不可混用。

第 1 章：多项式、最小多项式与域扩张

本章对象： F 是基础域， $F[x]$ 是多项式环； α 是扩域中的代数元， $m_{\alpha,F}$ 是首一最小多项式。

1.1 多项式环、基础域、不可约性与加入一个根

原问题：一步步向我介绍整式相关和分圆域相关的数学知识吧，我在学习Galois理论的时候遇到了一些相关知识，但是感觉我理解的不是很充分

整理提示：本段末尾预告的分圆结论将在第 4—11 章证明。

我们把这部分重新搭一遍，而且我会尽量把它和你正在学的 **Galois 理论** 连接起来，而不是孤立地讲“多项式技巧”。

我先把路线给你看清楚，然后今天只走第一步。这里我先把你说的“整式”理解成 **多项式 (polynomial) 相关知识**；以后如果你还想补“代数整数 algebraic integers”，我们可以另开一条线。

我们要走的路线

整体上可以分成三层：

1. 多项式本身

$F[x]$, 整除、最大公因式、不可约多项式

↓

2. 多项式如何制造域扩张

$F[x]/(f(x))$, $F(\alpha)$, 最小多项式、分裂域

↓

3. 单位根与分圆域

$x^n - 1$, $\Phi_n(x)$, $\mathbb{Q}(\zeta_n)$, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$

最后你会看到一个非常漂亮的闭环：

多项式 $\rightarrow$ 根 $\rightarrow$ 域扩张 $\rightarrow$ 自同构 $\rightarrow$ Galois 群
--

而分圆域其实是这个闭环里最重要、最好算的一类具体例子。

第一步：为什么 Galois 理论一开始就离不开 $F[x]$?

先不要管分圆域。

假设我们研究一个多项式：

$$f(x) = x^2 - 2.$$

如果我们的基础域是

$$F = \mathbb{Q},$$

那么：

$$f(x) \in \mathbb{Q}[x].$$

这里

$$\mathbb{Q}[x]$$

是什么意思？

就是：

系数都在 $\mathbb{Q}$ 里的所有多项式组成的集合。

例如：

$$x^2 - 2,$$

$$3x^5 + \frac{1}{2}x - 7,$$

$$x^{100} + 1$$

都属于 $\mathbb{Q}[x]$ 。

1. 为什么强调“系数在哪个域里”？

这是以后 Galois 理论里极其重要的一件事。

例如：

$$x^2 - 2$$

在

$$\mathbb{Q}[x]$$

里不能分解成一次因子。

但在

$$\mathbb{R}[x]$$

里：

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

所以：

一个多项式是否不可约，必须说明是在哪个域上。

不能单独说：

$x^2 - 2$ 是不可约的。

严格说应该是：

$x^2 - 2$ 在 $\mathbb{Q}[x]$ 中不可约。

而在 $\mathbb{R}[x]$ 中可约。

这件事以后会不断出现。

2. 为什么 $F[x]$ 特别好?

因为如果 F 是一个域, 那么 $F[x]$ 中可以做一种类似整数除法的操作。

例如整数中:

$$17 = 5 \times 3 + 2.$$

多项式中也是一样。

如果

$$f(x), g(x) \in F[x], \quad g(x) \neq 0,$$

那么一定存在唯一的

$$q(x), r(x) \in F[x]$$

使得:

$$\boxed{f(x) = q(x)g(x) + r(x)}$$

并且

$$\deg r < \deg g.$$

这就是多项式除法算法。

这一点非常重要, 因为它使 $F[x]$ 的行为非常像整数 $\mathbb{Z}$ 。

3. 多项式和整数之间有一个很深的类比

你可以先建立这张心理对应表:

整数 $\mathbb{Z}$	多项式 $F[x]$
2,3,5,7 是素数	不可约多项式
$12 = 2^2 \cdot 3$	多项式分解成不可约因子
$\gcd(a, b)$	$\gcd(f, g)$
Euclidean algorithm	多项式 Euclidean algorithm

例如：

$$x^2 - 1 = (x - 1)(x + 1).$$

类似于：

$$6 = 2 \cdot 3.$$

而：

$$x^2 + 1$$

在 $\mathbb{R}[x]$ 中：

$$x^2 + 1$$

不可约吗？

是，因为：

$$x^2 + 1$$

在 $\mathbb{R}[x]$ 中其实没有实根，因此对二次多项式来说不可约。

但在：

$$\mathbb{C}[x]$$

中：

$$x^2 + 1 = (x - i)(x + i).$$

所以再次说明：

“不可约”永远是相对于基础域而言的。

4. “不可约”为什么对域扩张这么重要？

这是第一个真正和 Galois 理论连起来的地方。

还是考虑：

$$f(x) = x^2 - 2.$$

它在 $\mathbb{Q}[x]$ 不可约。

但我们想要一个世界，其中：

$$x^2 - 2$$

真的有一个根。

我们把这个根叫：

$$\alpha.$$

要求：

$$\alpha^2 = 2.$$

于是得到一个更大的域：

$$\mathbb{Q}(\alpha).$$

因为 $\alpha^2 = 2$ ，所以任意高次幂都可以降下来。

例如：

$$\alpha^3 = 2\alpha,$$

$$\alpha^4 = 4.$$

因此这个域里的任意元素其实都长成：

$$\boxed{a + b\alpha, \quad a, b \in \mathbb{Q}.}$$

当：

$$\alpha = \sqrt{2}$$

时：

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

5. 这里出现一个极其重要的思想

我们原本只有：

$$\mathbb{Q}.$$

但是有一个多项式：

$$x^2 - 2$$

在这里没有根。

于是我们人为扩大这个域，把一个根放进去：

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

这就是：

域扩张

最基本的来源。

所以从概念上说：

多项式没有根

促使我们：

加入一个根

从而：

产生域扩张。

这就是 Galois 理论的起点。

6. 还有一个更抽象但更漂亮的写法

我们甚至不必预先知道 $\sqrt{2}$ 是什么。

直接写：

$$\boxed{\mathbb{Q}[x]/(x^2 - 2)}$$

这个商环里，把 $x^2 - 2$ 当成 0。

所以：

$$x^2 = 2.$$

也就是说，商掉以后， x 自动变成一个满足：

$$x^2 = 2$$

的元素。

因此：

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}).$$

这其实是代数学里一个非常核心的思想：

想创造一个满足某个方程的元素，就让那个方程等于 0。

例如想创造：

$$i^2 = -1,$$

就可以写：

$$\mathbb{R}[x]/(x^2 + 1).$$

这和：

$$\mathbb{C}$$

本质上一样。

7. 为什么这里要求 $f(x)$ 不可约？

这是下一步最关键的问题。

如果：

$$f(x)$$

在 $F[x]$ 中不可约，那么：

$$\boxed{F[x]/(f)}$$

是一个域。

例如：

$$\mathbb{Q}[x]/(x^2 - 2)$$

是域。

但是如果：

$$f(x) = x^2 - 1 = (x - 1)(x + 1),$$

那么：

$$\mathbb{Q}[x]/(x^2 - 1)$$

就不是域。

原因很直观。

在商环里：

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

因此：

$$(x - 1)(x + 1) = 0.$$

可是：

$$x - 1 \neq 0, \quad x + 1 \neq 0.$$

所以出现了两个非零元素相乘等于零：

$$(x - 1)(x + 1) = 0.$$

这叫做**零因子**。

而域里不可能有零因子。

因此：

$$f \text{ 不可约} \iff F[x]/(f) \text{ 是域}$$

对于 $F[x]$ 来说，这是一个非常重要的定理。

先停在这里

你现在最值得真正抓住的是下面这条链，而不是记很多定义：

不可约多项式 $\longrightarrow$ 加入它的一个根 $\longrightarrow$ 得到新的域

例如：

$$x^2 - 2$$

对应：

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

以后我们会把：

$$x^n - 1$$

拿出来研究。

它的根就是：

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1},$$

也就是 n 次单位根。

然后再把它分解成：

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

这里的：

$$\Phi_n(x)$$

就是第 n 个分圆多项式。

再取它的一个根 ζ_n ，就会得到：

$$\mathbb{Q}(\zeta_n)$$

也就是第 n 个分圆域。

所以你刚才在 Galois 理论里遇到的“单位根到底要不要固定”“为什么加单位根”“为什么自同构把 ζ_n 送到另一个单位根”，其实都建立在今天这套框架上。

下一步我建议专门讲“不可约多项式、最小多项式和 $F(\alpha)$ 为什么本质上是同一件事”。这个弄懂以后，再进入单位根和分圆多项式会顺很多。

1.2 补充证明：除法、Bézout 等式与不可约商环

设 F 为域， $g \neq 0$ 。若当前被除式最高次项是 ax^r ，除式最高次项是 bx^m ，且 $r \geq m$ ，减去 $(a/b)x^{r-m}g$ 即降低次数。域中 $b \neq 0$ 可逆，有限次操作后得到 $f = qg + r$ ，其中 $r = 0$ 或 $\deg r < \deg g$ 。若还有 $f = q_1g + r_1$ ，相减后 $(q - q_1)g = r_1 - r$ ；左边非零时次数至少为 $\deg g$ ，右边非零时次数小于它，故商、余数唯一。

对两个多项式反复做带余除法，余数次数严格下降，最后一个非零余数（调成首一）就是最大公因式。逐次倒代给出多项式版 Bézout 等式： $uf + vg = \gcd(f, g)$ 。

设 m 非常数且不可约。商环 $F[x]/(m)$ 中的非零元素 $[h]$ 满足 $m \nmid h$ 。不可约性给出 $\gcd(h, m) = 1$ ，于是存在 $u, v \in F[x]$ 使 $uh + vm = 1$ 。进入商环后 $[u][h] = [1]$ ，故每个非零元素有逆元，商环是域。

反过来，若 $m = ab$ ，其中 a, b 都非常数且次数小于 $\deg m$ ，则 $[a], [b]$ 非零而 $[a][b] = [0]$ 。域无零因子，所以商环不是域。这里需要 m 非零且非常数。

1.3 最小多项式、商环和扩张次数

整理提示：本节先建立代数元的一般模板；末尾把分圆多项式认作最小多项式的结论，以第 9 章不可约性证明为依据。

我们现在就把上一节最关键的三个对象彻底连起来：

不可约多项式	$\leftrightarrow$	最小多项式	$\leftrightarrow$	$F(\alpha)$
--------	-------------------	-------	-------------------	-------------

这一步如果真正理解了，后面分圆多项式 $\Phi_n(x)$ 、单位根 ζ_n 、分圆域 $\mathbb{Q}(\zeta_n)$ 会顺很多。

第二步：什么是最小多项式？

先从一个具体例子开始。

设

$$\alpha = \sqrt{2}.$$

显然：

$$\alpha^2 - 2 = 0.$$

所以 α 是多项式

$$x^2 - 2$$

的根。

但它其实也是很多其他多项式的根，比如：

$$x^4 - 4$$

因为

$$(\sqrt{2})^4 - 4 = 0.$$

还可以有：

$$x^3 - 2x,$$

因为

$$(\sqrt{2})^3 - 2\sqrt{2} = 0.$$

于是自然出现一个问题：

这么多多项式都以 α 为根，哪个最重要？

答案就是：

最小多项式

1. 最小多项式的定义

设 F 是一个域， α 是某个扩域中的元素。

如果存在非零多项式

$$f(x) \in F[x]$$

使得

$$f(\alpha) = 0,$$

那么称 α 在 F 上是代数的。

这时存在唯一一个首一不可约多项式

$$m_{\alpha,F}(x) \in F[x]$$

满足：

$$m_{\alpha,F}(\alpha) = 0.$$

它就叫做 α 在 F 上的最小多项式。

记作：

$$\boxed{m_{\alpha,F}(x)}$$

2. 为什么叫“最小”？

因为它是所有满足

$$f(\alpha) = 0$$

的非零多项式中次数最低的那个首一多项式。

例如：

$$\alpha = \sqrt{2}.$$

在 $\mathbb{Q}$ 上：

$$x^2 - 2$$

不可约，所以：

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

而像：

$$x^4 - 4 = (x^2 - 2)(x^2 + 2)$$

虽然也以 $\sqrt{2}$ 为根，但次数更高。

3. 一个非常重要的定理

如果

$$f(\alpha) = 0, \quad f(x) \in F[x],$$

那么：

$$\boxed{m_{\alpha, F}(x) \mid f(x)}$$

也就是说：

α 的最小多项式整除所有以 α 为根的 F -系数多项式。

这个结论以后会频繁使用。

4. 为什么？

这是一个很漂亮的多项式除法证明。

设：

$$m(x) = m_{\alpha, F}(x).$$

对任意满足 $f(\alpha) = 0$ 的 $f(x)$, 做除法:

$$f(x) = q(x)m(x) + r(x),$$

其中:

$$\deg r < \deg m.$$

把 $x = \alpha$ 代进去:

$$f(\alpha) = q(\alpha)m(\alpha) + r(\alpha).$$

但:

$$f(\alpha) = 0, \quad m(\alpha) = 0,$$

所以:

$$r(\alpha) = 0.$$

如果 $r \neq 0$, 那 r 就是一个次数比 m 还低、但仍然以 α 为根的多项式。

这和 m 的最小性矛盾。

所以:

$$r = 0.$$

因此:

$$m \mid f.$$

5. 为什么最小多项式一定不可约?

这个也很重要。

假设最小多项式：

$$m(x)$$

可以分解：

$$m(x) = g(x)h(x)$$

其中：

$$\deg g, \deg h < \deg m.$$

因为：

$$m(\alpha) = 0,$$

所以：

$$g(\alpha)h(\alpha) = 0.$$

现在注意：

$$g(\alpha), h(\alpha)$$

是在一个域里。

域没有零因子，所以：

$$g(\alpha) = 0$$

或者：

$$h(\alpha) = 0.$$

但 g, h 的次数都小于 m ，这就和 m 是最低次数矛盾。

所以：

$$m_{\alpha, F}(x) \text{ 必不可约}$$

6. 反过来也成立

这一点你最好记住。

如果：

$$f(x) \in F[x]$$

是首一不可约多项式，并且：

$$f(\alpha) = 0,$$

那么：

$$f(x) = m_{\alpha, F}(x)$$

因为最小多项式必须整除 f ，但 f 已不可约。

所以只能相同。

7. 最小多项式依赖基础域

这是以后 Galois 理论里非常容易混淆的地方。

考虑：

$$\alpha = \sqrt{2}.$$

在：

$$\mathbb{Q}$$

上：

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

但是如果基础域已经是：

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

那么 $\sqrt{2}$ 本身已经属于基础域。

此时：

$$x - \sqrt{2}$$

就是它的最小多项式。

所以：

$$m_{\sqrt{2}, \mathbb{Q}(\sqrt{2})}(x) = x - \sqrt{2}.$$

因此必须始终记得：

最小多项式一定是“相对于哪个基础域”而言的。

8. 最小多项式与扩张次数

现在进入最漂亮的联系。

如果：

$$m_{\alpha, F}(x)$$

的次数是：

$$n,$$

那么：

$$[F(\alpha) : F] = n$$

也就是：

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

这是一个非常重要的公式。

9. 为什么？

假设：

$$\deg m = n.$$

那么：

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

构成 $F(\alpha)$ 在 F 上的一组基。

所以任意元素都能唯一写成：

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

其中：

$$a_i \in F.$$

为什么高次幂可以降下来？

因为最小多项式：

$$m(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$$

满足：

$$m(\alpha) = 0.$$

所以：

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

因此任何：

$$\alpha^k, \quad k \geq n$$

都能不断降到：

$$1, \alpha, \dots, \alpha^{n-1}$$

的线性组合。

10. 例如 $\sqrt{2}$

因为：

$$m_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2,$$

次数是 2。

所以：

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

并且：

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

是一组基。

因此：

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

11. 再看一个三次例子

设：

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

它满足：

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

而：

$$x^3 - 2$$

在 $\mathbb{Q}[x]$ 中不可约。

所以：

$$m_{\alpha, \mathbb{Q}}(x) = x^3 - 2.$$

因此：

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

而每个元素唯一写成：

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}.$$

也就是：

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

12. 现在把商环也接上

上一节我们写过：

$$F[x]/(f).$$

现在可以更精确地说：

如果：

$$m(x) = m_{\alpha, F}(x),$$

那么：

$$F(\alpha) \cong F[x]/(m(x))$$

这是非常核心的结构定理。

意思是：

“往 F 中加入一个满足 $m(\alpha) = 0$ 的元素”，本质上就等于“在 $F[x]$ 中规定 $m(x) = 0$ ”。

13. 这个同构到底是怎么来的？

定义映射：

$$\varphi : F[x] \rightarrow F(\alpha)$$

为：

$$f(x) \mapsto f(\alpha).$$

这叫evaluation map，即代入映射。

例如：

$$3x^2 + x + 1 \mapsto 3\alpha^2 + \alpha + 1.$$

它的核是什么？

就是所有满足：

$$f(\alpha) = 0$$

的多项式。

刚刚我们已经证明：

$$f(\alpha) = 0 \iff m_{\alpha, F} \mid f.$$

因此：

$$\ker \varphi = (m_{\alpha, F}).$$

而像：

$$\varphi(F[x])$$

正好就是：

$$F[\alpha].$$

由于 α 是代数元，这时：

$$F[\alpha] = F(\alpha).$$

于是第一同构定理给出：

$$\boxed{F[x]/(m_{\alpha, F}) \cong F(\alpha)}$$

这个结果非常值得你熟悉。

14. 为什么代数元时 $F[\alpha] = F(\alpha)$?

这个有点微妙。

定义上：

$$F[\alpha]$$

是所有：

$$f(\alpha)$$

构成的集合，也就是只允许做加法和乘法。

而：

$$F(\alpha)$$

则是包含 F 和 α 的最小的域，所以还必须允许除法。

乍一看：

$$F[\alpha]$$

可能比：

$$F(\alpha)$$

小。

但如果 α 是代数的，那么：

$$F[\alpha]$$

本身已经是一个域。

因此：

$$\boxed{F[\alpha] = F(\alpha)}$$

15. 为什么 $F[\alpha]$ 已经有逆元?

例如:

$$\mathbb{Q}[\sqrt{2}].$$

取:

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

它的逆:

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

看起来不一定还是 $a + b\sqrt{2}$ 。

但有理化:

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

还是在:

$$\mathbb{Q}[\sqrt{2}]$$

里。

一般情况也是如此。

更抽象地说:

$$F[\alpha] \cong F[x]/(m)$$

而 m 不可约, 因此右边是域。

所以左边也是域。

16. 到这里可以形成一张非常重要的图

如果：

$$\alpha$$

在 F 上代数，那么：

$$m_{\alpha, F}(x)$$

是不可约多项式。

它决定：

$$F(\alpha)$$

而且：

$$F(\alpha) \cong F[x]/(m_{\alpha, F})$$

同时：

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

所以可以画成：

$$m_{\alpha, F}(x) \longleftrightarrow F[x]/(m_{\alpha, F}) \longleftrightarrow F(\alpha)$$

这是你以后学 Galois 理论时反复出现的基本模板。

17. 这和分圆域马上就会连接

以后我们取：

$$\alpha = \zeta_n,$$

其中：

$$\zeta_n = e^{2\pi i/n}$$

是一个本原 n 次单位根。

它满足：

$$\zeta_n^n = 1,$$

所以它当然是：

$$x^n - 1$$

的根。

但：

$$x^n - 1$$

通常不是 ζ_n 的最小多项式。

它真正的最小多项式是：

$$\boxed{\Phi_n(x)}$$

也就是第 n 个分圆多项式。

于是：

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x))$$

而且：

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$$

这里的 $\varphi(n)$ 是 Euler ϕ 函数。

你现在应该已经隐约看到：

分圆多项式其实就是“本原单位根的最小多项式”。

这就是为什么它在 Galois 理论里那么重要。

下一步我们最好先不直接上 Φ_n ，而是先把 $x^n - 1$ 的所有根、单位根、本原单位根到底是什么彻底搞清楚。这样之后分圆多项式就会自然出现，而不是突然冒出来。

1.4 补充证明：不借循环论证，补齐逆元与基

原回答给出了降幂的想法。还要证明逆元仍在 $F[\alpha]$ ，以及降幂后的表示唯一。

设 $m = m_{\alpha, F}$ 。若 $h(\alpha) \neq 0$ ，则 $m \nmid h$ ，由不可约性及多项式 Bézout 等式，有 $uh + vm = 1$ 。代入 α 得到 $u(\alpha)h(\alpha) = 1$ 。因此 $F[\alpha]$ 本身就是域，等于 $F(\alpha)$ 。

设 $d = \deg m$ 。把任意 h 除以 m 可得 $h(\alpha) = r(\alpha)$ ，其中 $\deg r < d$ ，所以 $1, \alpha, \dots, \alpha^{d-1}$ 张成 $F(\alpha)$ 。若它们有非零线性关系，就存在次数小于 d 的非零多项式以 α 为根，与最小次数矛盾。故这组元素线性无关，是一组基， $[F(\alpha) : F] = d$ 。

代入映射 $F[x] \rightarrow F[\alpha]$ 的核是 (m) ，于是 $[h] \mapsto h(\alpha)$ 给出 $F[x]/(m) \cong F(\alpha)$ 。

例子中的 $\sqrt{2} \notin \mathbb{Q}$ 可由互素分数的奇偶性反证。 $x^3 - 2$ 若在 $\mathbb{Q}[x]$ 可约，三次多项式必有有理根；有理根定理只允许 $\pm 1, \pm 2$ ，逐一代入皆非根，故不可约。

第 2 章：复指数与全部单位根

本章对象： $i^2 = -1$ ； n 是正整数， $\zeta_n = e^{2\pi i/n}$ ； μ_n 表示全部 n 次单位根。

2.1 欧拉公式的幂级数推导与旋转意义

原问题：欧拉公式是怎么来的

整理提示：原对话曾把“欧拉函数”的追问理解成“欧拉公式”。这段推导仍有数学内容，移到单位根所用的复指数之前；欧拉函数在第 5 章另讲。

欧拉公式

$$e^{i\theta} = \cos \theta + i \sin \theta$$

不是凭空猜出来的。最自然的推导之一，是从指数函数、正弦、余弦的幂级数出发。我们一步一步来。

先从实指数函数开始。微积分里可以证明：

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

这个展开式不仅对实数 x 有效，也可以把 x 换成复数。

于是令

$$x = i\theta.$$

得到

$$e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \dots$$

现在利用：

$$i^2 = -1, \quad i^3 = -i, \quad i^4 = 1,$$

然后每四次循环一次。

所以：

$$e^{i\theta} = 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \dots$$

现在把“没有 i ”的项和“带 i ”的项分别收集起来：

$$\begin{aligned} e^{i\theta} &= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \dots\right) \\ &\quad + i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \dots\right). \end{aligned}$$

关键来了。

微积分里：

$$\cos \theta = 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \dots$$

而：

$$\sin \theta = \theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \dots$$

所以前面两大坨正好就是：

$$\cos \theta$$

和

$$\sin \theta.$$

因此：

$$e^{i\theta} = \cos \theta + i \sin \theta$$

这就是欧拉公式。

但这里有一个更深、也更值得理解的地方：

为什么指数函数碰到 i 以后，突然和“旋转”发生关系？

因为指数函数满足：

$$\frac{d}{d\theta} e^{i\theta} = i e^{i\theta}.$$

而在复平面里，乘以 i 恰好代表逆时针旋转 90° 。

例如：

$$1 \mapsto i,$$

$$i \mapsto -1,$$

$$-1 \mapsto -i.$$

所以

$$\frac{dz}{d\theta} = iz$$

的意思可以直观理解成：

z 的瞬时运动方向永远是把 z 本身旋转 90° 后的方向。

如果 z 是从

$$z(0) = 1$$

开始，那么它就会沿单位圆不停旋转。

于是自然有：

$$z(\theta) = \cos \theta + i \sin \theta.$$

所以欧拉公式背后的几何本质其实是：

$$e^{i\theta} = \text{复平面上“旋转 } \theta \text{”}$$

这也是为什么单位根会自然写成：

$$\zeta_n = e^{2\pi i/n}.$$

因为这就是从 1 出发，在单位圆上旋转：

$$\frac{2\pi}{n}$$

的角度。

然后：

$$\zeta_n^k = e^{2\pi i k/n}$$

就是旋转 k 次。

所以你前面学单位根时出现的指数表达式，其实全都来自欧拉公式的这个“复指数 = 旋转”的几何意义。

下一步如果你愿意，我们可以继续追问一个更基础的问题：为什么 $e^x, \sin x, \cos x$ 会有刚才那些幂级数展开？这样欧拉公式就可以从最底层完全推出来。

2.2 为什么复指数等于 1 恰好对应整圈旋转

原问题：这是为什么

这一步来自 Euler 公式：

$$e^{i\theta} = \cos \theta + i \sin \theta$$

所以如果要求

$$e^{i\theta} = 1,$$

注意右边的实数 1 在复数里其实是

$$1 + 0i.$$

因此必须同时满足

$$\cos \theta = 1, \quad \sin \theta = 0.$$

在单位圆上， $(\cos \theta, \sin \theta)$ 表示从正实轴出发转过 θ 后到达的点。要得到

$$(1, 0),$$

也就是回到单位圆最右端，只能转完整圈：

$$0, \quad 2\pi, \quad -2\pi, \quad 4\pi, \quad -4\pi, \dots$$

因此

$$\theta = 2\pi m, \quad m \in \mathbb{Z}.$$

换句话说，

$$e^{i\theta} = 1 \iff \theta \equiv 0 \pmod{2\pi}$$

这同时体现了复指数函数一个特别重要的性质：

$$e^{i(\theta+2\pi)} = e^{i\theta}$$

因为

$$\cos(\theta + 2\pi) = \cos \theta, \quad \sin(\theta + 2\pi) = \sin \theta.$$

所以复指数在虚方向上是周期性的。

例如：

$$e^{i0} = 1,$$

$$e^{i2\pi} = 1,$$

$$e^{i4\pi} = 1,$$

以及

$$e^{-i2\pi} = 1.$$

但

$$e^{i\pi} = -1,$$

$$e^{i\pi/2} = i,$$

都不是 1。

而且你刚才那一步现在就可以完全展开：

假设

$$\zeta_n^a = \zeta_n^b,$$

由于

$$\zeta_n = e^{2\pi i/n},$$

所以

$$e^{2\pi ia/n} = e^{2\pi ib/n}.$$

两边相除：

$$e^{2\pi i(a-b)/n} = 1.$$

根据我们刚刚证明的结论：

$$\frac{2\pi(a-b)}{n} = 2\pi m$$

其中 $m \in \mathbb{Z}$ 。

约去 2π ：

$$\frac{a-b}{n} = m.$$

所以

$$a-b = mn,$$

也就是

$$\boxed{n \mid (a-b)}.$$

这其实就是以后单位根里经常出现的一个核心原则：

$$\boxed{\zeta_n^a = \zeta_n^b \iff a \equiv b \pmod{n}}$$

也就是说， ζ_n 的指数只需要看模 n 的余数。

下一步如果继续往深一点，其实很值得解释：**Euler 公式 $e^{i\theta} = \cos \theta + i \sin \theta$ 本身为什么成立。这会把这个这里最后一个“默认接受的公式”也补上。

2.3 全部 n 次单位根：互异性与穷尽性

原问题：这一步也得说明一下吧

对，这一步不能直接跳过去。我们从

$$x^n = 1$$

为什么恰好有

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$$

这 n 个根开始。

先设

$$\zeta_n = e^{2\pi i/n}.$$

那么显然：

$$\zeta_n^n = e^{2\pi i} = 1.$$

所以 ζ_n 是 $x^n - 1$ 的一个根。

更一般地，对任意整数 k ：

$$(\zeta_n^k)^n = \zeta_n^{kn} = (\zeta_n^n)^k = 1.$$

因此：

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$$

全都是 $x^n - 1$ 的根。

但这里还要证明两件事：它们彼此不同，而且没有别的根。

第一件事，为什么它们彼此不同？假设

$$\zeta_n^a = \zeta_n^b.$$

那么

$$\zeta_n^{a-b} = 1.$$

写成指数形式：

$$e^{2\pi i(a-b)/n} = 1.$$

而

$$e^{i\theta} = 1$$

当且仅当

$$\theta = 2\pi m, \quad m \in \mathbb{Z}.$$

所以

$$\frac{a-b}{n} \in \mathbb{Z},$$

即

$$n \mid (a-b).$$

如果

$$0 \leq a, b \leq n-1,$$

那么唯一可能就是

$$a = b.$$

所以这 n 个根互不相同。

第二件事，为什么没有别的根？这里有两种理解。

最简单的是代数基本定理： $x^n - 1$ 是 n 次多项式，所以在复数中按重数计算一共有 n 个根。我们已经找到了 n 个互不相同的根，因此不可能再有别的。

也可以直接从复数极坐标看。假设

$$z^n = 1.$$

把 z 写成

$$z = re^{i\theta}.$$

那么

$$z^n = r^n e^{in\theta} = 1.$$

右边的模长是 1，所以

$$r^n = 1.$$

由于 $r \geq 0$ ，所以

$$r = 1.$$

而辐角必须满足

$$n\theta = 2\pi k, \quad k \in \mathbb{Z}.$$

所以

$$\theta = \frac{2\pi k}{n}.$$

于是

$$z = e^{2\pi i k/n}.$$

也就是

$$z = \zeta_n^k.$$

而因为

$$\zeta_n^{k+n} = \zeta_n^k,$$

所以只需要取

$$k = 0, 1, \dots, n-1.$$

因此所有根恰好是

$$\boxed{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}}.$$

几何上，这 n 个根就是单位圆上等间隔分布的 n 个点，每两个相邻点的夹角都是

$$\frac{2\pi}{n}.$$

如果你愿意，下一步我可以继续解释一个很关键的问题：为什么这些根里只有一部分是“本原 n 次单位根”。

第 3 章：本原单位根、阶与互素

本章对象： $\text{ord}(\alpha)$ 是使 $\alpha^d = 1$ 的最小正整数 d ； $\text{gcd}(a, n)$ 是正的最大公因数。

3.1 补充证明：互素时为什么可以约掉一个整数因子

整数 Euclidean 算法从 $a = qn + r$ 开始，不断用除数除余数，直到余数为零。公因数在每一步保持不变，最后一个非零余数是 $g = \gcd(a, n)$ ；倒代得到整数 u, v 使 $ua + vn = g$ 。负整数可先取绝对值再调整符号。

若 $\gcd(a, n) = 1$ 且 $n \mid ad$ ，取 $ua + vn = 1$ 并乘 d ，得 $d = uad + vnd$ 。右边两项均被 n 整除，因此 $n \mid d$ 。这正是阶公式中“约掉互素部分”的理由。

3.2 本原单位根、阶与互素指数

原问题：从这里继续

我们就从这里继续，而且把“本原 n 次单位根”这件事一步一步彻底讲清楚。

前面我们已经知道：

$$x^n - 1 = 0$$

的全部复根是

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1},$$

其中

$$\zeta_n = e^{2\pi i/n}.$$

现在的问题是：

为什么这些根里只有一部分是“本原 n 次单位根”？

关键在于一个概念：阶 (order)。

一个单位根 α 的阶，定义为最小的正整数 m ，使得

$$\alpha^m = 1.$$

例如：

$$1^1 = 1,$$

所以 **1** 的阶是 **1**。

再看

$$-1.$$

有：

$$(-1)^1 = -1 \neq 1,$$

但

$$(-1)^2 = 1.$$

所以 **-1** 的阶是 **2**。

现在看

$$\zeta_6 = e^{2\pi i/6}.$$

我们有

$$\zeta_6^6 = 1.$$

但更小的正整数 $1, 2, 3, 4, 5$ 都不能让它变成 1 ，所以它的阶是 6 。

因此：

ζ_6 是本原 6 次单位根

所谓“本原 n 次单位根”，就是：

阶恰好等于 n 的单位根

这比“它满足 $z^n = 1$ ”更强。

因为满足

$$z^n = 1$$

只说明：

$$\text{ord}(z) \mid n,$$

并不说明它的阶一定就是 n 。

例如：

$$-1$$

满足

$$(-1)^6 = 1,$$

所以它当然是一个 6 次单位根。

但是它的阶只有 2 ，所以它不是本原 6 次单位根。

这就是最容易混淆的地方：

n 次单位根 $\neq$ 本原 n 次单位根

前者只要求

$$z^n = 1,$$

后者要求

$$z^n = 1$$

且没有任何更小的正整数 $m < n$ 使

$$z^m = 1.$$

现在我们看 $n = 6$ 的全部根：

$$1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5.$$

分别判断它们的阶。

$$1$$

的阶是 1。

$$\zeta_6$$

的阶是 6。

$$\zeta_6^2$$

满足

$$(\zeta_6^2)^3 = \zeta_6^6 = 1,$$

所以它的阶至多是 3。实际上就是 3。

$$\zeta_6^3$$

满足

$$(\zeta_6^3)^2 = \zeta_6^6 = 1,$$

所以它的阶是 2。

$$\zeta_6^4$$

和 ζ_6^2 一样，阶是 3。

而

$$\zeta_6^5$$

的阶又是 6。

所以：

本原 6 次单位根只有 ζ_6, ζ_6^5

这时你可能会问：

为什么偏偏是指数 1 和 5？

因为

$$\gcd(1, 6) = 1,$$

$$\gcd(5, 6) = 1.$$

而：

$$\gcd(2, 6) = 2,$$

$$\gcd(3, 6) = 3,$$

$$\gcd(4, 6) = 2.$$

所以会得到一个非常重要的结论：

$$\boxed{\zeta_n^k \text{ 是本原 } n \text{ 次单位根} \iff \gcd(k, n) = 1}$$

为什么？

因为：

$$(\zeta_n^k)^m = 1$$

等价于

$$\zeta_n^{km} = 1.$$

而前面已经知道：

$$\zeta_n^r = 1 \iff n \mid r.$$

所以：

$$(\zeta_n^k)^m = 1 \iff n \mid km.$$

我们要找最小的正整数 m 。

设：

$$d = \gcd(n, k).$$

写成：

$$n = dn', \quad k = dk',$$

其中：

$$\gcd(n', k') = 1.$$

条件

$$n \mid km$$

变成：

$$dn' \mid dk'm.$$

约掉 d ：

$$n' \mid k'm.$$

由于

$$\gcd(n', k') = 1,$$

所以必须：

$$n' \mid m.$$

最小这样的 m 就是：

$$m = n' = \frac{n}{d}.$$

因此：

$$\boxed{\text{ord}(\zeta_n^k) = \frac{n}{\gcd(n, k)}}$$

于是：

$$\text{ord}(\zeta_n^k) = n$$

当且仅当

$$\gcd(n, k) = 1.$$

所以“本原”本质上对应“指数和 n 互素”。

这一步一旦明白，欧拉函数就会非常自然：

$$\varphi(n)$$

定义为 $1, \dots, n$ 中和 n 互素的整数个数。

所以本原 n 次单位根的个数就是：

$$\boxed{\varphi(n)}$$

比如 $n = 8$ ，与 8 互素的是

$$1, 3, 5, 7,$$

所以本原 8 次单位根是：

$$\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7,$$

一共

$$\varphi(8) = 4$$

个。

而这四个根正好就是

$$\Phi_8(x)$$

的全部根。

所以：

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

并且：

$$\deg \Phi_n = \varphi(n)$$

这里整条逻辑链是：

$$\zeta_n^k$$

的阶为

$$\frac{n}{\gcd(n, k)}$$

所以阶恰好为 n

$$\iff \gcd(n, k) = 1,$$

于是本原 n 次单位根有

$$\varphi(n)$$

个，于是第 n 个分圆多项式有

$$\varphi(n)$$

个根，于是

$$\deg \Phi_n = \varphi(n).$$

下一步最自然的是讲：

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

为什么成立。这个公式正好把“所有 n 次单位根”和“按阶分类的本原单位根”完全连接起来。

3.3 普通单位根与本原单位根怎样区分

原问题：本原几次和阶数很容易搞反吧

对，非常容易混，尤其“ n 次单位根”和“本原 n 次单位根”长得太像。

最稳妥的办法是始终把“本原 n 次”翻译成一句话：

$$\boxed{\text{本原 } n \text{ 次单位根} = \text{阶恰好等于 } n}$$

而普通的“ n 次单位根”只要求：

$$\alpha^n = 1.$$

它的阶可以是 n 的任何约数，不一定是 n 。

比如 -1 ：

$$(-1)^6 = 1,$$

所以它是 6 次单位根；但

$$(-1)^2 = 1,$$

而且 2 是最小的，所以它的阶是 2。因此它不是本原 6 次单位根，而是：

$$\boxed{\text{本原 } 2 \text{ 次单位根}}$$

你可以记成：

$$\boxed{\text{“几次单位根”看它满足哪个 } x^n = 1; \text{ “本原几次”看它的最小指数，也就是阶。}}$$

再举一个：

$$\zeta_6^2.$$

它当然满足

$$(\zeta_6^2)^6 = 1,$$

所以是 6 次单位根。

但实际上：

$$(\zeta_6^2)^3 = 1,$$

而 3 是最小的，所以

$$\text{ord}(\zeta_6^2) = 3.$$

因此它是：

本原 3 次单位根

不是本原 6 次单位根。

所以最关键的一句话就是：

$$\alpha \text{ 是本原 } n \text{ 次单位根} \iff \text{ord}(\alpha) = n$$

这两个概念其实不是两个独立概念：“本原 n 次”就是“阶为 n ”的另一种说法。

3.4 忘记阶公式时，从整除条件重新推导

原问题：这个怎么来的，我突然忘记了

这个公式就是我们前面证明过的：

$$\text{ord}(\zeta_n^a) = \frac{n}{\gcd(a, n)}$$

重新推一遍就清楚了。

设

$$d = \text{ord}(\zeta_n^a),$$

意思是 d 是最小正整数，使得

$$(\zeta_n^a)^d = 1.$$

于是：

$$\zeta_n^{ad} = 1.$$

而 ζ_n 本身的阶是 n ，所以：

$$\zeta_n^m = 1 \iff n \mid m.$$

因此这里等价于：

$$\boxed{n \mid ad}.$$

现在问题就变成：

最小的正整数 d 是多少，才能让 $n \mid ad$ ？

设

$$g = \gcd(a, n).$$

把它们写成：

$$a = ga', \quad n = gn',$$

并且：

$$\gcd(a', n') = 1.$$

条件

$$n \mid ad$$

就变成：

$$gn' \mid ga'd.$$

约去 g ：

$$n' \mid a'd.$$

但因为：

$$\gcd(a', n') = 1,$$

所以 a' 不能帮 d 提供任何 n' 的因子，因此必须：

$$n' \mid d.$$

最小的正整数 d 就是：

$$d = n'.$$

而：

$$n' = \frac{n}{g} = \frac{n}{\gcd(a, n)}.$$

所以：

$$\text{ord}(\zeta_n^a) = \frac{n}{\gcd(a, n)}$$

例如：

$$\zeta_{12}^8.$$

因为

$$\gcd(8, 12) = 4,$$

所以：

$$\text{ord}(\zeta_{12}^8) = \frac{12}{4} = 3.$$

你也可以直接验证：

$$(\zeta_{12}^8)^3 = \zeta_{12}^{24} = 1,$$

而 1、2 次幂都还不是 1。

最好记住背后的核心句子：

$$\text{ord}(\zeta_n^a) = \text{使 } n \mid ad \text{ 的最小正整数 } d$$

公式只是从这句话算出来的。

3.5 本原单位根的数量不是一，恰好是欧拉函数

原问题：但是一个本原n次根有几个不一定对吧

对，你理解得对。

“本原 n 次单位根”不是唯一的。满足

$$\text{ord}(\alpha) = n$$

的元素通常有多个，它们的个数正好是

$$\boxed{\varphi(n)}$$

其中 φ 是欧拉函数。

例如 $n = 5$ 。全部 5 次单位根是

$$1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4.$$

因为

$$1, 2, 3, 4$$

都和 5 互素，所以

$$\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$$

全都是本原 5 次单位根。因此有

$$\varphi(5) = 4$$

个。

再比如 $n = 6$ 。只有指数与 6 互素的那些：

$$1, 5.$$

所以本原 6 次单位根只有

$$\zeta_6, \zeta_6^5,$$

共

$$\varphi(6) = 2$$

个。

所以要区分这两句话：

“一个本原 n 次单位根”

指的是“任选其中一个”，比如我们常常记作

$$\zeta_n.$$

而

“所有本原 n 次单位根”

则有

$$\varphi(n)$$

个，具体就是

$$\zeta_n^k, \quad \gcd(k, n) = 1.$$

这也是为什么记号 ζ_n 容易让人误以为“本原 n 次单位根只有一个”：其实 ζ_n 只是我们挑选并固定的一个代表。

第 4 章：分圆多项式：按阶收集根

本章对象： $\Phi_n(x)$ 收集阶恰为 n 的单位根； $d \mid n$ 中的 d 始终遍历正约数。

4.1 分圆多项式的 Phi 记号怎样读

原问题：不是我是指哪个本源 n 次的那个

你指的是这个：

$$\Phi_n(x)$$

这里的 Φ 是希腊字母 Phi（大写 Φ ，小写 ϕ ）。

所以：

$$\Phi_n(x)$$

英文通常读作：

“phi sub n of x ”

中文可以念：

“Phi 下标 n 的 x ”，或者直接说“第 n 个分圆多项式”。

而

$$\varphi(n)$$

这里的 φ 也是 phi 的一种小写字形，表示欧拉函数，通常读作：

“phi of n ”。

所以这两个虽然都念 phi，但含义不同：

$\Phi_n(x)$ 是分圆多项式

$\varphi(n)$ 是欧拉函数。

4.2 分圆多项式的编号为什么是 n ，次数为什么是欧拉函数

原问题：重点解释为什么是第 n 个，以及为什么是欧拉函数

对，这里真正要搞清楚的是两个问题：

为什么叫“第 n 个”分圆多项式？

以及

$\deg \Phi_n(x) = \varphi(n)$ 为什么？

这两个其实来自同一件事：按照单位根的“阶”来分类。

第一步：先看 $x^n - 1$ 的根

方程

$$x^n = 1$$

在复数中一共有 n 个根：

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1},$$

其中可以取

$$\zeta_n = e^{2\pi i/n}.$$

例如 $n = 6$:

$$\zeta_6 = e^{2\pi i/6}.$$

那么 $x^6 - 1$ 的六个根就是

$$1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5.$$

但是，这六个根其实不是“同一种”单位根。

比如：

$$1^1 = 1,$$

所以 1 的阶是 1 。

而

$$(\zeta_6^3)^2 = 1,$$

因为

$$\zeta_6^3 = -1.$$

所以 ζ_6^3 的阶其实是 2 ，不是 6 。

再比如：

$$(\zeta_6^2)^3 = 1,$$

所以 ζ_6^2 的阶是 3。

因此：

$$x^6 - 1$$

的根里面混着：

1 阶、2 阶、3 阶、6 阶单位根

第二步：什么叫“本原 n 次单位根”？

如果一个单位根 α 满足：

$$\alpha^n = 1,$$

而且对任何

$$1 \leq k < n$$

都有

$$\alpha^k \neq 1,$$

那么就说它的阶正好是 n 。

这就叫：

本原 n 次单位根

primitive n -th root of unity。

例如：

$$\zeta_6 = e^{2\pi i/6}$$

本身的阶是 6，所以它是本原 6 次单位根。

而：

$$\zeta_6^2$$

不是，因为它的阶只有 3。

第三步：“第 n 个分圆多项式”的“第 n 个”到底是什么意思？

这里非常容易产生误解。

它不是说：

按次数排序的第 n 个多项式。

而是说：

对应“阶恰好等于 n ”的单位根。

定义：

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

也就是说：

$$\Phi_n(x)$$

的根恰好就是所有本原 n 次单位根。

因此它被编号为 n 。

用 $n = 6$ 看最清楚

$x^6 - 1$ 的根有：

$$\zeta_6^0, \zeta_6^1, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5.$$

分别看它们的阶：

$$\zeta_6^0 = 1$$

阶为 **1**。

$$\zeta_6^3 = -1$$

阶为 **2**。

$$\zeta_6^2, \zeta_6^4$$

阶为 **3**。

而：

$$\zeta_6, \zeta_6^5$$

阶才真正是 **6**。

所以：

$$\Phi_6(x) = (x - \zeta_6)(x - \zeta_6^5).$$

算出来就是：

$$\Phi_6(x) = x^2 - x + 1.$$

所以这里的“6”表示：

它收集的是阶恰好为 6 的单位根

第四步：为什么突然出现 $\gcd(k, n) = 1$?

这是核心。

我们研究：

$$\zeta_n^k.$$

它的阶是多少？

一般公式是：

$$\text{ord}(\zeta_n^k) = \frac{n}{\gcd(n, k)}$$

所以：

$$\zeta_n^k$$

的阶等于 n ，当且仅当：

$$\frac{n}{\gcd(n, k)} = n.$$

这等价于：

$$\gcd(n, k) = 1.$$

因此：

$$\boxed{\zeta_n^k \text{ 是本原 } n \text{ 次单位根} \iff \gcd(k, n) = 1.}$$

这就是为什么“互素”突然出现。

第五步：为什么阶公式是

$$\text{ord}(\zeta_n^k) = \frac{n}{\gcd(n, k)}?$$

我们一步一步看。

假设：

$$(\zeta_n^k)^m = 1.$$

那么：

$$\zeta_n^{km} = 1.$$

而 ζ_n 的阶是 n ，所以必须有：

$$n \mid km.$$

现在我们要找最小的正整数 m ，使：

$$n \mid km.$$

设：

$$d = \gcd(n, k).$$

写成：

$$n = dn', \quad k = dk',$$

其中：

$$\gcd(n', k') = 1.$$

条件：

$$n \mid km$$

变成：

$$dn' \mid dk'm.$$

约掉 d ：

$$n' \mid k'm.$$

因为：

$$\gcd(n', k') = 1,$$

所以：

$$n' \mid m.$$

最小的正整数 m 就是：

$$m = n' = \frac{n}{d}.$$

因此：

$$\text{ord}(\zeta_n^k) = \frac{n}{\gcd(n, k)}$$

第六步：现在欧拉函数自然出现了

Euler ϕ 函数定义就是：

$$\varphi(n) = \#\{1 \leq k \leq n : \gcd(k, n) = 1\}$$

也就是说：

$1, \dots, n$ 中，与 n 互素的整数有多少个。

而我们刚才证明：

$$\zeta_n^k$$

是本原 n 次单位根，当且仅当：

$$\gcd(k, n) = 1.$$

所以本原 n 次单位根的数量就是：

$$\varphi(n)$$

而：

$$\Phi_n(x)$$

每一个本原 n 次单位根对应一个一次因子：

$$x - \zeta_n^k.$$

所以：

$$\deg \Phi_n(x) = \varphi(n).$$

例如 $n = 8$

看：

$$1, 2, 3, 4, 5, 6, 7, 8.$$

与 8 互素的是：

$$1, 3, 5, 7.$$

所以：

$$\varphi(8) = 4.$$

因此本原 8 次单位根是：

$$\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7.$$

所以：

$$\Phi_8(x) = \prod_{k=1,3,5,7} (x - \zeta_8^k).$$

最终：

$$\Phi_8(x) = x^4 + 1$$

而它的次数：

$$4 = \varphi(8).$$

第七步：为什么 $x^n - 1$ 会分成所有 Φ_d ？

现在你甚至可以理解这个公式了：

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

因为：

$$x^n - 1$$

的每个根，其阶一定整除 n 。

也就是说， $x^n - 1$ 的根可以按照“阶”分组：

阶 1, 阶 d_1 , 阶 d_2 , ..., 阶 n ,

其中这些阶全部都是 n 的约数。

而：

$$\Phi_d(x)$$

恰好收集“阶正好等于 d ”的那些根。

所以自然得到：

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

比如：

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

分别是：

$$\Phi_1(x) = x - 1,$$

$$\Phi_2(x) = x + 1,$$

$$\Phi_3(x) = x^2 + x + 1,$$

$$\Phi_6(x) = x^2 - x + 1.$$

次数也刚好满足：

$$1 + 1 + 2 + 2 = 6.$$

也就是著名恒等式：

$$\boxed{\sum_{d|n} \varphi(d) = n.}$$

现在你应该能看到这个恒等式为什么“不是巧合”：

n

个 n 次单位根，被按照各自的阶分组。

阶为 d 的有：

$$\varphi(d)$$

个。

所以：

$$n = \sum_{d|n} \varphi(d).$$

最后把最重要的一条链压缩成一句话：

$$\Phi_n \text{ 之所以编号为 } n \iff \text{它的根是阶恰为 } n \text{ 的单位根}$$

而

$$\deg \Phi_n = \varphi(n)$$

是因为：

$$\zeta_n^k \text{ 的阶为 } n \iff \gcd(k, n) = 1,$$

而这样的 k 恰好有 $\varphi(n)$ 个。

下一步最值得讲的是一个更深的问题：为什么 $\Phi_n(x)$ 明明用复数根定义，最后系数却落在 $\mathbb{Z}$ ，而且还在 $\mathbb{Q}[x]$ 中不可约？这一步正好会直接接到 Galois 理论。

4.3 按阶分类，证明分圆乘积恒等式

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

而且重点不是先记公式，而是理解它为什么必然成立。

先回忆前面已经知道的两件事：

$$x^n - 1 = 0$$

的所有根，就是全部 n 次单位根。

而

$$\Phi_d(x)$$

的根，是全部本原 d 次单位根，也就是阶恰好为 d 的单位根。

现在关键问题来了：

一个 n 次单位根，它的阶可能是多少？

设 α 是 n 次单位根，也就是

$$\alpha^n = 1.$$

假设 α 的阶是 d ，即

$$d = \text{ord}(\alpha).$$

那么一定有：

$$\boxed{d \mid n}.$$

为什么？

因为 $\alpha^d = 1$ ，而 d 是最小正整数。

对 n 用 d 做整数除法：

$$n = qd + r, \quad 0 \leq r < d.$$

于是

$$1 = \alpha^n = \alpha^{qd+r} = (\alpha^d)^q \alpha^r = \alpha^r.$$

但 d 是使 $\alpha^d = 1$ 的最小正整数。

如果 $r > 0$ ，就会出现一个比 d 更小的正整数 r 满足

$$\alpha^r = 1,$$

矛盾。

所以只能：

$$r = 0.$$

因此：

$$\boxed{d \mid n}.$$

这一步非常重要：

$$\boxed{\alpha^n = 1 \implies \text{ord}(\alpha) \mid n}$$

现在我们就把 $x^n - 1$ 的所有根按“阶”分类。

比如 $n = 12$ 。

12 的正约数是：

$$1, 2, 3, 4, 6, 12.$$

所以任何满足

$$\alpha^{12} = 1$$

的根，它的阶只能是：

$$1, 2, 3, 4, 6, 12.$$

不可能出现阶为 5、7、8、9 的根。

于是全部 12 次单位根可以分成几组：

$$\boxed{\text{阶 } 1 \cup \text{阶 } 2 \cup \text{阶 } 3 \cup \text{阶 } 4 \cup \text{阶 } 6 \cup \text{阶 } 12}$$

而这些组分别就是：

$$\Phi_1(x), \Phi_2(x), \Phi_3(x), \Phi_4(x), \Phi_6(x), \Phi_{12}(x)$$

的根。

所以所有 $x^{12} - 1$ 的根，恰好就是这些分圆多项式的全部根。

因此：

$$\boxed{x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)}$$

一般地：

$$\boxed{x^n - 1 = \prod_{d|n} \Phi_d(x)}$$

还有一个细节：为什么前面没有差一个常数倍？

因为两边都是首一多项式。

左边：

$$x^n - 1$$

最高次项系数是 1。

右边每个 $\Phi_d(x)$ 也是首一多项式，所以乘积也是首一。

而且两边有完全相同的一组根，没有重根。

所以它们必须完全相等。

为什么 $x^n - 1$ 没有重根？这个也可以顺便证明。

设

$$f(x) = x^n - 1.$$

那么导数是

$$f'(x) = nx^{n-1}.$$

如果 α 是重根，那么必须同时满足：

$$f(\alpha) = 0$$

和

$$f'(\alpha) = 0.$$

第一式给出：

$$\alpha^n = 1,$$

所以

$$\alpha \neq 0.$$

但第二式要求：

$$n\alpha^{n-1} = 0.$$

在特征 0 的域，比如 $\mathbb{C}$ ，而 $n \neq 0$ 、 $\alpha \neq 0$ 保证 $n\alpha^{n-1} \neq 0$ ，与第二式矛盾（ $n = 1$ 时导数直接为 1）。

所以所有 n 次单位根都是单根。

现在我们可以看一个具体例子，比如 $n = 6$ 。

6 的约数是：

$$1, 2, 3, 6.$$

所以：

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

逐个写：

$$\Phi_1(x) = x - 1,$$

$$\Phi_2(x) = x + 1,$$

$$\Phi_3(x) = x^2 + x + 1,$$

$$\Phi_6(x) = x^2 - x + 1.$$

因此：

$$x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1).$$

你可以检查次数：

$$1 + 1 + 2 + 2 = 6.$$

这正好又对应：

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6.$$

所以我们得到：

$$\boxed{\sum_{d|n} \varphi(d) = n}$$

这不是一个偶然的数论恒等式，而是因为：

$$\boxed{n \text{ 个 } n \text{ 次单位根}}$$

被按阶分成了：

$$\boxed{\varphi(d) \text{ 个阶为 } d \text{ 的根}}$$

其中 $d \mid n$ 。

所以：

$$n = \sum_{d|n} \varphi(d).$$

下一步最自然的是继续解释：

$\Phi_n(x)$ 为什么系数居然在 $\mathbb{Z}$

以及更重要的：

$\Phi_n(x)$ 为什么在 $\mathbb{Q}[x]$ 中不可约

这一步会真正开始和 Galois 理论正面接轨。

第 5 章：欧拉函数的计数与两个恒等式

本章对象： $\varphi(n)$ 数 $1, \dots, n$ 中与 n 互素的整数； $p \mid n$ 的乘积仅遍历不同素因子。

5.1 欧拉函数：数互素整数，也数可逆剩余类

原问题：我是指那个公因子的

对，你指的是前面那个和“公因子/互素”有关的 **欧拉函数** (Euler totient function)，不是欧拉公式。

它记作

$\varphi(n)$

定义是：

$$\varphi(n) = \#\{1 \leq k \leq n : \gcd(k, n) = 1\}$$

也就是：从 1 到 n 里，有多少个数和 n 没有大于 1 的公因子。

例如 $n = 6$:

1, 2, 3, 4, 5, 6

其中与 6 互素的是

1, 5.

所以

$$\varphi(6) = 2.$$

为什么会有这样一个函数？本质上是数论里经常需要问：

模 n 意义下，哪些数有乘法逆元？

答案恰好就是那些满足

$$\gcd(k, n) = 1$$

的数，所以 $\varphi(n)$ 其实是在数：

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

里有多少个元素。

而在你现在学的单位根里，它又自然出现，因为：

$$\zeta_n^k$$

是本原 n 次单位根，当且仅当

$$\gcd(k, n) = 1.$$

所以本原 n 次单位根的个数就是

$$\varphi(n).$$

更进一步，欧拉函数有一个很重要的计算公式：

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

其中 p 遍历 n 的不同素因子。

比如

$$12 = 2^2 \cdot 3.$$

所以

$$\varphi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4.$$

因为 $1, \dots, 12$ 中与 12 互素的是：

$$1, 5, 7, 11.$$

这个公式其实就是“把所有与 n 有公共素因子的数删掉”。

例如 $n = 12$ 。先有 12 个数。

删掉 2 的倍数，占一半：

$$12 \left(1 - \frac{1}{2}\right) = 6.$$

再删掉剩下那些 3 的倍数，相当于再乘：

$$1 - \frac{1}{3}.$$

于是：

$$12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

所以

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

本质上来自“排除所有与 n 共享素因子的数”。

你现在先记住最核心的两层就够了：

$$\varphi(n) = \text{与 } n \text{ 互素的余数类数量}$$

而在分圆域里：

$$\varphi(n) = \text{本原 } n \text{ 次单位根的数量}$$

所以最终才得到

$$\deg \Phi_n = \varphi(n).$$

下一步我可以专门一步一步证明为什么

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

而不是只给这个公式。

5.2 用容斥原理证明欧拉函数的乘积公式

我们就把这个公式从最直观的“删掉有公共素因子的数”一步一步推出来：

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

其中 $p \mid n$ 表示 p 遍历 n 的所有不同素因子。

先看一个具体例子， $n = 12$ 。

$$12 = 2^2 \cdot 3.$$

要找和 12 互素的数，就是在

$$1, 2, \dots, 12$$

中，排除所有和 12 有公共素因子的数。

因为 12 的素因子只有 2 和 3，所以只需要排除：

2 的倍数

以及

3 的倍数。

一开始有 12 个数。

2 的倍数有：

$$2, 4, 6, 8, 10, 12$$

共

$$\frac{12}{2} = 6$$

个。

所以删掉它们以后剩：

$$12 - \frac{12}{2} = 12 \left(1 - \frac{1}{2}\right) = 6.$$

但现在还要删掉 3 的倍数。

不能直接再减 $12/3$ ，因为 6 和 12 已经因为 2 的倍数被删过一次了。

这就是为什么需要“容斥原理”。

3 的倍数有

$$\frac{12}{3} = 4$$

个：

$$3, 6, 9, 12.$$

而同时是 2 和 3 的倍数，也就是 6 的倍数，有：

$$\frac{12}{6} = 2$$

个。

所以最终：

$$\varphi(12) = 12 - \frac{12}{2} - \frac{12}{3} + \frac{12}{6}.$$

算一下：

$$= 12 - 6 - 4 + 2 = 4.$$

整理：

$$\varphi(12) = 12 \left(1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6} \right).$$

注意括号里正好能因式分解：

$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6} = \left(1 - \frac{1}{2} \right) \left(1 - \frac{1}{3} \right).$$

所以：

$$\boxed{\varphi(12) = 12 \left(1 - \frac{1}{2} \right) \left(1 - \frac{1}{3} \right)}$$

现在推广到一般情况。

假设：

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

是 n 的素因数分解。

一个数 k 和 n 互素，当且仅当：

$$k$$

不被任何一个

$$p_1, p_2, \dots, p_r$$

整除。

所以从 $1, \dots, n$ 这 n 个数里，删掉所有 p_i 的倍数。

被 p_i 整除的数有：

$$\frac{n}{p_i}$$

个。

被 p_i, p_j 同时整除的数有：

$$\frac{n}{p_i p_j}$$

个。

被三个不同素数同时整除的数有：

$$\frac{n}{p_i p_j p_k}$$

个。

于是容斥原理给：

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i < j} \frac{n}{p_i p_j} - \sum_{i < j < k} \frac{n}{p_i p_j p_k} + \dots$$

把 n 提出来：

$$\varphi(n) = n \left[1 - \sum_i \frac{1}{p_i} + \sum_{i < j} \frac{1}{p_i p_j} - \dots \right].$$

而括号里恰好就是乘积展开：

$$\prod_{i=1}^r \left(1 - \frac{1}{p_i} \right).$$

所以：

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

这就是公式的来源。

这里还有一个你很值得注意的点：

指数 a_i 为什么没有直接出现在乘积里？

因为判断

$$\gcd(k, n) = 1$$

时，只关心 k 是否被某个素因子 p_i 整除。

比如：

$$n = 2^5 \cdot 3^7.$$

一个 k 只要能被 2 整除，就已经和 n 不互素了；不需要继续区分它是否能被 $2^2, 2^3$ 整除。

所以乘积只遍历“不同素因子”。

例如：

$$\varphi(8) = 8 \left(1 - \frac{1}{2}\right) = 4.$$

虽然：

$$8 = 2^3,$$

但只出现一次素数 2。

同样：

$$\varphi(18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 6.$$

与 18 互素的数正好是：

$$1, 5, 7, 11, 13, 17.$$

现在把它重新接回你正在学的分圆域：

$$\deg \Phi_n = \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

所以例如：

$$[\mathbb{Q}(\zeta_{12}) : \mathbb{Q}] = \deg \Phi_{12} = \varphi(12) = 4.$$

也就是说，欧拉函数不仅是在数“互素整数”，同时直接告诉你第 n 个分圆域相对于 $\mathbb{Q}$ 的扩张次数。

5.3 为什么最大公因数一定整除 n

原问题：为什么整除

因为这里的 d 被定义成

$$d = \gcd(k, n).$$

而“最大公因数”首先得是一个公因数，所以它一定同时整除 k 和 n 。

也就是说：

$$d \mid k$$

并且

$$\boxed{d \mid n}.$$

例如如果

$$\gcd(8, 12) = 4,$$

那么 4 当然整除 8，也整除 12。

所以当我们把 $1, \dots, n$ 按照

$$\gcd(k, n) = d$$

分类时， d 不可能随便取，而只能取 n 的约数。

比如 $n = 12$ ，那么可能的 d 只能是

$$1, 2, 3, 4, 6, 12.$$

不可能有

$$\gcd(k, 12) = 5$$

因为 5 根本不整除 12。

所以前面写

$$\boxed{d \mid n}$$

不是额外假设，而是从

$$d = \gcd(k, n)$$

自动得到的。

5.4 欧拉函数的约数和：单位根计数证明

原问题：为什么这个成立

这个恒等式

$$n = \sum_{d|n} \varphi(d)$$

本质上是因为：把 $1, \dots, n$ 这 n 个整数按它们和 n 的最大公因数分类，每一类的数量恰好是某个 $\varphi(d)$ 。

先看最直观的单位根版本，因为和你现在学的内容最贴近。

$x^n - 1$ 一共有 n 个不同的复根。每一个根都有一个阶，而且这个阶一定整除 n 。

所以这 n 个根可以按“阶”分组：

$$\text{阶为 } d, \quad d \mid n.$$

而阶恰好为 d 的单位根有多少个？

就是：

$$\varphi(d).$$

因为本原 d 次单位根一共有 $\varphi(d)$ 个。

于是所有根的总数就是：

$$\sum_{d|n} \varphi(d).$$

但另一方面， $x^n - 1$ 本来就有 n 个不同的根。

所以：

$$n = \sum_{d|n} \varphi(d)$$

举个例子， $n = 6$ 。

6 的约数是：

$$1, 2, 3, 6.$$

各阶单位根的数量分别是：

$$\varphi(1) = 1,$$

$$\varphi(2) = 1,$$

$$\varphi(3) = 2,$$

$$\varphi(6) = 2.$$

加起来：

$$1 + 1 + 2 + 2 = 6.$$

这正好就是 $x^6 - 1$ 的 6 个根。

所以这个公式其实是在说：

$$\boxed{\text{所有 } n \text{ 次单位根} = \text{按阶分类后的所有本原 } d \text{ 次单位根}}$$

其中 d 遍历 n 的所有约数。

如果你愿意，我下一步可以继续给你讲这个恒等式的纯整数证明，不借助单位根。

5.5 欧拉函数的约数和：纯整数分类证明

我们不用单位根，只用整数和最大公因数来证明

$$\boxed{\sum_{d|n} \varphi(d) = n}.$$

核心思路是：把

$$1, 2, \dots, n$$

这 n 个整数按它们和 n 的最大公因数分类。

先看一个具体例子，取

$$n = 12.$$

把 $1, \dots, 12$ 按

$$\gcd(k, 12)$$

来分组。

可能出现的最大公因数一定是 12 的约数：

$$1, 2, 3, 4, 6, 12.$$

例如：

$$\gcd(k, 12) = 1$$

的有

$$1, 5, 7, 11,$$

共

$$4 = \varphi(12)$$

个。

再看

$$\gcd(k, 12) = 2.$$

这些 k 可以写成

$$k = 2m.$$

条件变成

$$\gcd(2m, 12) = 2.$$

把 2 提出来：

$$\gcd(m, 6) = 1.$$

所以 m 必须在 $1, \dots, 6$ 中与 6 互素。

这样的 m 有

$$\varphi(6) = 2$$

个。

所以满足

$$\gcd(k, 12) = 2$$

的 k 也有

$$\varphi(6)$$

个。

一般来说, 如果

$$\gcd(k, n) = d,$$

其中

$$d \mid n,$$

那么可以写

$$k = dm.$$

又因为

$$n = d \cdot \frac{n}{d},$$

所以

$$\gcd(k, n) = d$$

等价于

$$\gcd\left(dm, d\frac{n}{d}\right) = d.$$

提出 d :

$$d \gcd\left(m, \frac{n}{d}\right) = d.$$

于是

$$\boxed{\gcd\left(m, \frac{n}{d}\right) = 1}$$

所以这样的 m 有

$$\varphi\left(\frac{n}{d}\right)$$

个。

因此，满足

$$\gcd(k, n) = d$$

的整数 k 有

$$\boxed{\varphi\left(\frac{n}{d}\right)}$$

个。

现在把所有可能的 $d \mid n$ 加起来，因为每个

$$k = 1, \dots, n$$

都会且只会属于其中一类：

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

最后注意，当 d 遍历 n 的所有约数时，

$$\frac{n}{d}$$

也恰好遍历 n 的所有约数。

所以把变量换个名字，就得到

$$n = \sum_{d|n} \varphi(d).$$

这就是纯整数证明。

你可以把它记成一句话：

把 $1, \dots, n$ 按 $\gcd(k, n)$ 分类

每一类的大小就是某个欧拉函数值，所以总数相加必然等于 n 。

而你前面学的单位根证明，其实和这个证明结构非常像：一个是按“最大公因数”分类，一个是按“阶”分类。

第 6 章：整数系数：首一除法与强归纳法

本章对象： $\mathbb{Z}[x]$ 是整数系数多项式环； $G(x)$ 是真约数对应的分圆多项式之积。首一保证系数为整数，已知整除才保证余数为零。

6.1 整数系数与不可约性：接下来需要证明的两件事

原问题：可以了，我理解了这些，下一步是介绍什么

下一步最合适的是进入分圆多项式真正核心的两件事：

$$\Phi_n(x) \in \mathbb{Z}[x]$$

以及

$$\Phi_n(x) \text{ 在 } \mathbb{Q}[x] \text{ 中不可约}$$

这两步一旦弄懂，你就会真正明白为什么

$$\Phi_n(x)$$

会成为本原 n 次单位根 ζ_n 在 $\mathbb{Q}$ 上的最小多项式。

然后就能顺理成章得到：

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n),$$

再进一步进入：

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

我建议接下来的顺序是：

1. 先解释为什么 $\Phi_n(x)$ 明明由复数根定义，最后系数却全是整数；
2. 再证明它为什么在 $\mathbb{Q}[x]$ 中不可约；

3. 然后解释为什么每个 Galois 自同构都由

$$\zeta_n \mapsto \zeta_n^a, \quad \gcd(a, n) = 1$$

决定；

4. 最后把分圆域的 Galois 群和模 n 可逆元群联系起来。

我们现在就可以从第 1 步开始：

为什么 $\Phi_n(x)$ 的系数竟然是整数？

这个问题本身就很有意思，因为定义

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} (x - \zeta_n^k)$$

里面明明全是复数。

6.2 首一除数为什么不会制造分数

原问题：这一步其实也没有理解

关键点就在多项式长除法的每一步，都要做一件事：

“被除式最高次项系数” $\div$ “除式最高次项系数”

所以如果除式是**首一多项式**，也就是最高次项系数为 **1**，你每次实际上只是在“除以 1”，自然不会因为这一步产生分数。

比如先看：

$$x^4 + 2x^3 + 3x + 1$$

除以

$$x^2 + x + 1.$$

除式最高次项是

$$x^2.$$

被除式最高次项是

$$x^4.$$

为了消掉 x^4 ，第一步必须乘：

$$\frac{x^4}{x^2} = x^2.$$

所以商的第一项是 x^2 ，系数仍然是整数。

然后减去

$$x^2(x^2 + x + 1).$$

减法当然还是整数系数多项式。

接下来再看剩下多项式的最高次项，再重复完全同样的过程。

更一般地，假设除式是：

$$g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

其中所有 $b_i \in \mathbb{Z}$ 。

注意最高次项系数就是：

1.

现在被除式在某一步最高次项是：

$$ax^r, \quad a \in \mathbb{Z}.$$

为了把这一项消掉，我们应该拿 $g(x)$ 乘：

$$ax^{r-m}.$$

为什么？

因为：

$$ax^{r-m} \cdot x^m = ax^r.$$

所以正好把最高次项消掉。

而这个新加入商里的系数就是：

$$a,$$

它原本就是整数。

所以不会出现分数。

反过来看一个不是首一的例子，就很明显了。

例如：

$$x^2$$

除以

$$2x + 1.$$

第一步要消掉 x^2 。

除式最高次项是：

$$2x.$$

所以必须算：

$$\frac{x^2}{2x} = \frac{1}{2}x.$$

马上就出现：

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

所以商可能跑到

$$\mathbb{Q}[x]$$

里，而不再属于

$$\mathbb{Z}[x].$$

所以你可以把“首一”在这里的作用记成非常具体的一句话：

多项式长除法每一步都要除以除式的首项系数。

如果这个系数是：

1,

那么：

$$\text{整数} \div 1 = \text{整数},$$

因此从头到尾所有系数都保持整数。

于是：

$$f, g \in \mathbb{Z}[x], \quad g \text{ 首一} \implies f = qg + r$$

时得到的

$$q, r$$

仍然都在：

$$\mathbb{Z}[x].$$

这正是我们前面证明 $\Phi_n(x) \in \mathbb{Z}[x]$ 时需要的那一步。

6.3 长除法能进行，不等于一定除尽

原问题：但是本身不一定能除尽吧，这个时候除数就作为余数

对，你抓到关键区别了：“**做得出多项式长除法**”和“**能够除尽**”是两件不同的事。

一般情况下当然不一定除尽。对任意

$$f(x), g(x) \in \mathbb{Z}[x]$$

且 $g(x)$ 首一，我们只能保证存在

$$q(x), r(x) \in \mathbb{Z}[x]$$

使得

$$f(x) = q(x)g(x) + r(x)$$

并且

$$\deg r < \deg g.$$

这里 $r(x)$ 才叫余数，不是 $g(x)$ 。

比如：

$$x^2 + 1$$

除以

$$x + 1.$$

做长除法：

$$x^2 + 1 = (x - 1)(x + 1) + 2.$$

所以商是

$$x - 1,$$

余数是

$$2.$$

因为：

$$\deg 2 = 0 < 1 = \deg(x + 1).$$

所以不是“除数变成余数”，而是：

当剩下的那部分次数已经低于除式次数时，就不能继续除，那一部分才是余数。

而我们前面证明 $\Phi_n(x) \in \mathbb{Z}[x]$ 时，情况比一般长除法更强。

我们已经提前知道：

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d < n}} \Phi_d(x).$$

设

$$G(x) = \prod_{\substack{d|n \\ d < n}} \Phi_d(x).$$

那么：

$$x^n - 1 = G(x)\Phi_n(x).$$

这已经告诉我们：

$$\boxed{G(x) \text{ 确实整除 } x^n - 1}$$

所以用 $G(x)$ 去除 $x^n - 1$ 时，余数必然是：

$$\boxed{0}.$$

现在我们只是额外利用：

$$G(x) \in \mathbb{Z}[x]$$

而且 G 首一，

所以长除法算出来的商一定仍然属于

$$\mathbb{Z}[x].$$

而这个商又已经知道就是

$$\Phi_n(x).$$

所以最终得到：

$$\boxed{\Phi_n(x) \in \mathbb{Z}[x]}.$$

因此整个证明里实际上用了两个完全不同的事实：

- | | |
|-----------------------|----------------------------|
| 1. G 首一 | $\implies$ 长除法的商、余数保持整数系数； |
| 2. $G \mid (x^n - 1)$ | $\implies$ 余数其实等于 0. |

这两个条件不要混在一起。“首一”保证不产生分数；“已知整除”才保证没有余数。

6.4 强归纳法究竟假设了哪些已知命题

原问题：这一步的归纳我怎么没看懂

你这里卡住的点，主要是因为这里用的不是“只假设 $n - 1$ 成立”的普通归纳法，而是**强归纳法**。

我们把它拆开。

我们想证明的命题是：

$$P(n) : \Phi_n(x) \in \mathbb{Z}[x].$$

第一步：起点

先证明

$$P(1).$$

因为

$$\Phi_1(x) = x - 1,$$

所以显然

$$\Phi_1(x) \in \mathbb{Z}[x].$$

第二步：归纳假设到底是什么？

现在假设我们正在证明 $P(n)$ 。

强归纳法允许我们假设：

$$P(1), P(2), \dots, P(n-1) \text{ 全部已经成立}$$

也就是说，我们暂时假设：

$$\Phi_1, \Phi_2, \dots, \Phi_{n-1}$$

全都是整数系数多项式。

注意这里不是只假设

$$\Phi_{n-1} \in \mathbb{Z}[x].$$

而是把所有比 n 小的情况都作为已知。

为什么需要这么强的假设？

因为公式

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

涉及的不是只有 Φ_{n-1} ，而是涉及 n 的所有约数 d 。

第三步：为什么这些 Φ_d 都能用归纳假设？

把 $d = n$ 那一项单独拿出来：

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d < n}} \Phi_d(x).$$

现在看乘积里面的每一个 d ：

$$d \mid n, \quad d < n.$$

因为它们都满足

$$d < n,$$

所以根据强归纳假设：

$$\Phi_d(x) \in \mathbb{Z}[x].$$

于是这些东西全部都是整数系数多项式。

例如假设现在证明 $n = 12$ 。

12 的真约数是：

$$1, 2, 3, 4, 6.$$

我们需要用到：

$$\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_6.$$

而这些编号全部小于 12，所以归纳假设已经告诉我们：

$$\Phi_1, \Phi_2, \Phi_3, \Phi_4, \Phi_6 \in \mathbb{Z}[x].$$

于是

$$G(x) = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)$$

当然也属于

$$\mathbb{Z}[x].$$

这就是那一步的意思。

第四步：然后怎么得到 Φ_n ?

定义

$$G(x) = \prod_{\substack{d|n \\ d < n}} \Phi_d(x).$$

于是：

$$x^n - 1 = G(x)\Phi_n(x).$$

我们已经知道：

$$G(x) \in \mathbb{Z}[x].$$

而且 $G(x)$ 是首一的。

所以用 $G(x)$ 去除

$$x^n - 1$$

时，因为除数首项系数是 1，多项式长除法不会制造分数。

因此商也属于：

$$\mathbb{Z}[x].$$

而这个商正好就是：

$$\Phi_n(x).$$

于是：

$$\boxed{\Phi_n(x) \in \mathbb{Z}[x]}.$$

这样就从

$$P(1), \dots, P(n-1)$$

推出了

$$P(n).$$

强归纳法完成。

你可以把整个逻辑压缩成：

假设所有编号 $< n$ 的 Φ 都是整数系数

而

$$\Phi_n = \frac{x^n - 1}{\text{由若干编号 } < n \text{ 的 } \Phi_d \text{ 组成的乘积}}$$

因此就能推出 Φ_n 也是整数系数。

关键就是：

$$\boxed{d \mid n, d \neq n \implies d < n}$$

所以所有需要用到的 Φ_d 都已经落在归纳假设覆盖的范围里。

6.5 分圆多项式属于整数多项式环的完整证明

$\Phi_n(x)$ 为什么明明用复数根定义，却属于 $\mathbb{Z}[x]$?

这一步其实可以用我们刚刚得到的

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

非常漂亮地证明。

1. 先看看为什么这个结论并不显然

按照定义,

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (x - \zeta_n^k).$$

而

$$\zeta_n = e^{2\pi i/n}$$

通常是一个复杂的复数。

例如 $n = 3$:

$$\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

本原三次单位根是

$$\zeta_3, \zeta_3^2.$$

所以定义告诉我们:

$$\Phi_3(x) = (x - \zeta_3)(x - \zeta_3^2).$$

一展开，神奇地变成：

$$\Phi_3(x) = x^2 + x + 1.$$

所有复数和虚部都消失了。

这不是偶然。对每个 n ，最终都有：

$$\Phi_n(x) \in \mathbb{Z}[x].$$

2. 先看几个例子

最简单的：

$$x - 1 = \Phi_1(x),$$

所以

$$\Phi_1(x) = x - 1.$$

再看 $n = 2$ ：

$$x^2 - 1 = \Phi_1(x)\Phi_2(x).$$

所以：

$$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1.$$

再看 $n = 3$ ：

$$x^3 - 1 = \Phi_1(x)\Phi_3(x).$$

所以：

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

再看 $n = 4$ 。

4 的约数是：

$$1, 2, 4.$$

所以：

$$x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x).$$

于是：

$$\Phi_4(x) = \frac{x^4 - 1}{(x - 1)(x + 1)}.$$

因为

$$(x - 1)(x + 1) = x^2 - 1,$$

所以：

$$\Phi_4(x) = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.$$

还是整数系数。

3. 一般情况下也用同样的想法

我们已经知道：

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

把最后一个 $\Phi_n(x)$ 单独拿出来：

$$x^n - 1 = \Phi_n(x) \prod_{\substack{d|n \\ d < n}} \Phi_d(x).$$

于是：

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(x)}$$

这就给了我们一个递归构造。

意思是：

如果所有比 n 小的、对应于 n 的真约数 d 的 Φ_d 都已经是整数系数，那么 Φ_n 也能由整数多项式除法得到。

4. 但你可能马上会问

即使分子分母都是整数系数多项式：

$$\frac{f(x)}{g(x)},$$

为什么商一定还是整数系数？

一般当然不一定。

例如：

$$\frac{x}{2}$$

就不是整数系数多项式。

所以这里还有一个重要条件：

$$\prod_{d|n, d < n} \Phi_d(x) \text{ 是首一多项式}$$

也就是说最高次项系数是 1。

5. 首一为什么这么重要？

举一个多项式长除法。

假设我们拿整数系数多项式

$$f(x)$$

除以一个首一整数系数多项式

$$g(x) = x^m + \dots$$

因为最高次项系数是 1，每一步消掉最高次项时，不需要除以 2、3、5 之类的整数。

例如：

$$x^4 - 1$$

除以

$$x^2 - 1.$$

最高次项：

$$x^4/x^2 = x^2.$$

商的第一项还是整数系数。

减掉：

$$x^4 - x^2,$$

剩：

$$x^2 - 1.$$

然后：

$$x^2/x^2 = 1.$$

得到：

$$x^2 + 1.$$

整个过程中不会产生分数。

一般来说：

$$\boxed{f, g \in \mathbb{Z}[x], \quad g \text{ 首一}}$$

那么用 g 对 f 做长除法时，商和余数都仍然在：

$$\mathbb{Z}[x]$$

里面。

6. 用数学归纳法正式证明

从 $n = 1$ 开始：

$$\Phi_1(x) = x - 1 \in \mathbb{Z}[x].$$

现在假设对于所有：

$$d < n$$

都有：

$$\Phi_d(x) \in \mathbb{Z}[x].$$

那么：

$$G(x) = \prod_{\substack{d|n \\ d < n}} \Phi_d(x)$$

也是整数系数多项式。

而且每个 $\Phi_d(x)$ 都是首一的，所以 $G(x)$ 也是首一的。

又因为：

$$x^n - 1 = G(x)\Phi_n(x),$$

所以 $G(x)$ 完整地整除 $x^n - 1$ 。

对

$$x^n - 1$$

除以首一整数多项式 $G(x)$ ，得到的商仍然是整数系数多项式。

而这个商就是：

$$\Phi_n(x).$$

所以：

$$\boxed{\Phi_n(x) \in \mathbb{Z}[x]}.$$

归纳完成。

7. 你可以把这个证明理解成什么？

我们一开始从复数定义：

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k).$$

看起来系数应该很复杂。

但实际上所有单位根一起组成：

$$x^n - 1,$$

而：

$$x^n - 1$$

本身是整数系数。

再按照“阶”把这些根一层层拆成：

$$\Phi_d.$$

由于每一层都是通过**整数多项式的精确除法**得到，所以最后每一层仍然落在：

$$\mathbb{Z}[x].$$

也就是说，复数根虽然看起来复杂，但它们以一种高度对称的方式成组出现，最后所有复数部分都抵消了。

8. 一个很漂亮的例子： Φ_6

我们知道：

$$x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6.$$

前面已经有：

$$\Phi_1 = x - 1,$$

$$\Phi_2 = x + 1,$$

$$\Phi_3 = x^2 + x + 1.$$

所以：

$$\Phi_6(x) = \frac{x^6 - 1}{(x - 1)(x + 1)(x^2 + x + 1)}.$$

化简：

$$\boxed{\Phi_6(x) = x^2 - x + 1}.$$

而它的两个根其实是：

$$e^{i\pi/3}, \quad e^{5i\pi/3}.$$

也就是：

$$\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

两者互为共轭。

乘起来：

$$(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}.$$

其中：

$$\alpha + \bar{\alpha} = 1,$$

$$\alpha\bar{\alpha} = 1.$$

于是：

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

所以从具体例子上也能看到：这些复数根并不是胡乱组合，而是以非常对称的方式一起出现。

到这里我们已经知道：

$$\boxed{\Phi_n(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]}.$$

但这还不够。

因为我们想说：

$$\Phi_n(x)$$

是 ζ_n 在 $\mathbb{Q}$ 上的最小多项式。

那还必须证明：

$$\Phi_n(x) \text{ 在 } \mathbb{Q}[x] \text{ 中不可约.}$$

这才是下一步真正关键、也比刚才难一些的定理。它会直接解释为什么所有本原 n 次单位根都是彼此的 Galois 共轭。

第 7 章：域的特征、有限域与 Frobenius

本章对象： p 始终是素数； $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 是域。横线 $\bar{}$ 表示把整数系数逐个模 p 。

7.1 域的特征：从不断累加单位元开始

原问题：所以特征为0和可分到底是什么意思

这两个概念其实是两条不同的线，只是在 Galois 理论里碰到了一起。

先说域的特征 (characteristic)。

设 F 是一个域。我们不断把 1 相加：

$$1, \quad 1 + 1, \quad 1 + 1 + 1, \quad \dots$$

如果永远不可能得到 0，就说

$$\boxed{\text{char } F = 0}.$$

例如：

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

都是特征 0 ，因为对任意正整数 n ,

$$n \cdot 1 \neq 0.$$

如果存在最小正整数 p ，使得

$$\underbrace{1 + \cdots + 1}_{p \text{ 次}} = 0,$$

那么：

$$\text{char } F = p.$$

对于一个域，这个 p 一定是素数。

例如：

$$\mathbf{F}_5 = \mathbb{Z}/5\mathbb{Z}$$

里：

$$1 + 1 + 1 + 1 + 1 = 0,$$

所以

$$\text{char } \mathbf{F}_5 = 5.$$

7.2 补充证明：域的正特征为什么一定是素数

若最小正整数 c 满足 $c \cdot 1_F = 0$ ，而 $c = ab$ ， $1 < a, b < c$ ，则 $(a \cdot 1_F)(b \cdot 1_F) = 0$ 。由最小性两因子均非零，与域无零因子矛盾。因此 c 是素数。

当 p 是素数，任意 $1 \leq a < p$ 与 p 互素，整数 Bézout 等式给出模 p 的逆元，所以 $\mathbb{F}_p$ 确实是域。特征 p 只说明整数倍单位元组成的素子域是 $\mathbb{F}_p$ ，并不限制整个域的元素数。

Frobenius 的中间项消失，还用到 $p \mid \binom{p}{k}$ ($0 < k < p$)： $\binom{p}{k} = p!/(k!(p-k)!)$ 是整数，分母不含素因子 p ，而分子含 p ，故该整数被 p 整除。

7.3 特征 p 的域不一定只有 p 个元素

原问题：所以特征 p 就是模 p 吗

可以把它理解成“整数部分按模 p 运算”，但特征 p 的域不一定是 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 。

特征 p 的定义是：

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ 次}} = 0$$

而且 p 是最小的正整数满足这一点。

因此在这样的域里：

$$p = 0, \quad p + 1 = 1, \quad -1 = p - 1$$

这些整数系数的运算确实和“模 p ”完全一样。

例如特征 3 中：

$$3 = 0, \quad 4 = 1, \quad 5 = 2.$$

所以

$$3x^2 + 4x + 5$$

就等同于

$$x + 2.$$

但是域本身可以比 $\mathbf{F}_p$ 大得多。

例如：

$$\mathbf{F}_p$$

当然是特征 p 。

但

$$\mathbf{F}_p(t)$$

——系数在 $\mathbf{F}_p$ 中的有理函数域——也是特征 p 。

它里面除了

$$0, 1, \dots, p-1$$

还有

$$t, \quad \frac{1}{t}, \quad t^2 + 1, \quad \frac{t+1}{t^2+t+1}, \dots$$

很多元素。

所以更准确地说：

$$\text{char } F = p \implies F \text{ 内部的整数运算按照模 } p \text{ 发生}$$

而不是说：

$$F = \mathbb{Z}/p\mathbb{Z}.$$

事实上，每个特征 p 的域内部都会天然包含一个最小的子域：

$$\mathbb{F}_p$$

这叫它的**素子域** (prime subfield)。

这也解释了我们刚才为什么在特征 p 中有：

$$(x - \alpha)^p = x^p - \alpha^p.$$

因为二项式展开中的

$$\binom{p}{k}$$

对 $1 \leq k \leq p-1$ 都是 p 的倍数，而在特征 p 的域里：

$$p = 0,$$

所以这些中间项全部消失。

7.4 有限域上的多项式环怎样读、怎样运算

原问题：这个 finx 不知道怎么念

你应该是指我刚才写的

$$\mathbf{F}_p[x]$$

这个记号。

中文一般读作：

“ $\mathbf{F}$ 下标 p ，方括号 x ”

更有数学意义地说，就是：

“ $\mathbf{F}_p$ 上的多项式环”

英文通常说 “the polynomial ring over $\mathbf{F}$ sub p ”，或者直接读 “ $\mathbf{F}$ sub p bracket x ”。

这里：

$$\mathbf{F}_p$$

表示有 p 个元素的有限域（当 p 是素数时就是）

$$\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}.$$

而

$$\mathbf{F}_p[x]$$

就是系数来自 $\mathbf{F}_p$ 的所有多项式组成的环。

例如在

$$\mathbf{F}_3[x]$$

里,

$$5x^2 + 7x + 4$$

和

$$2x^2 + x + 1$$

其实是同一个多项式, 因为系数都对 3 取模:

$$5 \equiv 2, \quad 7 \equiv 1, \quad 4 \equiv 1 \pmod{3}.$$

所以你前面看到的“在模 p 下研究多项式”, 严格地说, 就是把多项式放进

$$\boxed{\mathbf{F}_p[x]}$$

里面研究。

7.5 费马小定理: 用非零剩余类的排列证明

原问题: 费马小定理呢

费马小定理是我们前面证明

$$g(x^p) \equiv g(x)^p \pmod{p}$$

时用到的一步。它本身也值得单独讲清楚。

费马小定理说:

$$\boxed{a^p \equiv a \pmod{p}}$$

对任意整数 a 和素数 p 都成立。

等价地，如果

$$p \nmid a,$$

那么：

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

这两个形式是等价的。

例如 $p = 5$ ，取 $a = 2$ ：

$$2^5 = 32 \equiv 2 \pmod{5}.$$

或者：

$$2^4 = 16 \equiv 1 \pmod{5}.$$

为什么成立？最漂亮的证明之一是看模 p 的非零余数：

$$1, 2, \dots, p-1.$$

假设 $p \nmid a$ 。把它们全部乘以 a ：

$$a, 2a, 3a, \dots, (p-1)a.$$

对 p 取模以后，这些仍然恰好只是

$$1, 2, \dots, p-1$$

的一个重新排列。

为什么不会重复？如果

$$ia \equiv ja \pmod{p},$$

那么

$$p \mid a(i - j).$$

因为 p 是素数且 $p \nmid a$ ，所以只能：

$$p \mid (i - j).$$

但 $1 \leq i, j \leq p - 1$ ，所以只能 $i = j$ 。

于是把这些数全部相乘：

$$a \cdot 2a \cdot 3a \cdots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p}.$$

左边是：

$$a^{p-1}(p - 1)!.$$

所以：

$$a^{p-1}(p - 1)! \equiv (p - 1)! \pmod{p}.$$

因为 p 不整除 $(p - 1)!$ ，所以它在模 p 下可逆，可以约掉：

$$\boxed{a^{p-1} \equiv 1 \pmod{p}.$$

再乘一个 a ，得到：

$$\boxed{a^p \equiv a \pmod{p}.$$

这正是我们前面需要的地方，因为

$$g(x)^p \equiv a_0^p + a_1^p x^p + \cdots + a_m^p x^{mp} \pmod{p},$$

再用费马小定理：

$$a_i^p \equiv a_i \pmod{p},$$

于是：

$$g(x)^p \equiv a_0 + a_1 x^p + \cdots + a_m x^{mp} = g(x^p).$$

所以你可以把那一步记成两层：

$$\boxed{(A + B)^p \equiv A^p + B^p \pmod{p}}$$

来自二项式系数被 p 整除；

而

$$\boxed{a^p \equiv a \pmod{p}}$$

来自费马小定理。

两者合起来才得到：

$$\boxed{g(x)^p \equiv g(x^p) \pmod{p}.$$

7.6 从互素情形补上被素数整除的情形

原问题：为什么在 a, p 互素的情况下很快就乘以 a 就得到了任一情况

对，这里其实省略了一个分类讨论，所以看起来像“突然从互素推广到了任意 a ”。

前面我们证明的是：

$$p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}.$$

这时候两边乘以 a ：

$$a^p \equiv a \pmod{p}.$$

所以对于所有满足 $p \nmid a$ 的整数 a ，结论成立。

那如果 $p \mid a$ 呢？

这时

$$a \equiv 0 \pmod{p}.$$

于是

$$a^p \equiv 0^p = 0 \pmod{p}.$$

所以同样有

$$a^p \equiv a \equiv 0 \pmod{p}.$$

因此实际上分成两种情况：

$$\boxed{\begin{cases} p \nmid a : & a^{p-1} \equiv 1 \Rightarrow a^p \equiv a; \\ p \mid a : & a \equiv 0, a^p \equiv 0. \end{cases}}$$

两种情况合起来，才得到对任意整数 a ：

$$\boxed{a^p \equiv a \pmod{p}}.$$

所以严格地说，不是“乘一个 a 就从互素情况推广到了任意情况”，而是：

互素情况靠费马小定理；不互素情况本身就是显然的。

7.7 Frobenius 恒等式：系数模素数后为什么成立

我们先把这一步讲透：

$$g(x^p) \equiv g(x)^p \pmod{p}$$

这里的“ $\text{mod } p$ ”是指：所有多项式系数都对 p 取模。

假设

$$g(x) = a_0 + a_1x + \cdots + a_mx^m$$

其中 $a_i \in \mathbb{Z}$ 。

那么

$$g(x)^p = (a_0 + a_1x + \cdots + a_mx^m)^p.$$

在模 p 意义下，有一个非常重要的现象：

$$(A + B)^p \equiv A^p + B^p \pmod{p}$$

因为二项式展开：

$$(A + B)^p = A^p + \binom{p}{1} A^{p-1} B + \cdots + \binom{p}{p-1} A B^{p-1} + B^p.$$

当 p 是素数时，

$$p \mid \binom{p}{k}, \quad 1 \leq k \leq p-1.$$

所以中间所有项模 p 都消失，只剩：

$$(A+B)^p \equiv A^p + B^p \pmod{p}.$$

同理推广到很多项：

$$(a_0 + a_1x + \cdots + a_mx^m)^p \equiv a_0^p + a_1^p x^p + \cdots + a_m^p x^{mp} \pmod{p}.$$

另一方面，费马小定理告诉我们：

$$a_i^p \equiv a_i \pmod{p}.$$

于是：

$$g(x)^p \equiv a_0 + a_1x^p + \cdots + a_mx^{mp}.$$

但右边正好就是：

$$g(x^p).$$

所以：

$$\boxed{g(x)^p \equiv g(x^p) \pmod{p}}$$

这有时叫 characteristic p 下的 Frobenius 现象。

第 8 章：导数、重根与可分性

本章对象： f' 是形式导数；可分多项式没有重根，可分代数元的最小多项式没有重根；本章的 t 是不定元。

8.1 导数、公因式与模素数后没有重因子

原问题：这一步跳了

整理提示：这里先独立建立导数与重因子判据。末尾回到分圆不可约性时所说的矛盾，将在第 9 章完整使用。

对，这里确实跳了两层。我们把它拆成两个完全独立的小命题：

有重因子 $\implies$ 多项式和它的导数有公因子

然后再证明

$x^n - 1$ 与它的导数在 $\mathbf{F}_p[x]$ 中互素

这样结论才出来。

先讲第一层。

假设一个多项式 $F(x)$ 有重因子。最简单的意思就是存在某个非常数多项式 $h(x)$ ，使得

$$h(x)^2 \mid F(x).$$

所以可以写成

$$F(x) = h(x)^2 q(x).$$

求导：

$$F'(x) = 2h(x)h'(x)q(x) + h(x)^2q'(x).$$

把 $h(x)$ 提出来：

$$F'(x) = h(x) (2h'(x)q(x) + h(x)q'(x)).$$

所以不仅

$$h \mid F,$$

而且

$$h \mid F'.$$

因此：

$$\boxed{F \text{ 有重因子} \implies \gcd(F, F') \neq 1.}$$

这就是“为什么看导数能够检查重因子”。

对普通的重根也很好理解。例如

$$F(x) = (x - a)^2 q(x).$$

那么求导之后仍然保留一个

$$x - a$$

因子，所以：

$$F(a) = 0, \quad F'(a) = 0.$$

因此一个根如果是重根，它也一定是导数的根。

现在第二层。

我们是在模 p 下工作，所以实际上考虑：

$$F(x) = x^n - 1 \in \mathbf{F}_p[x].$$

它的导数仍然是

$$F'(x) = nx^{n-1}.$$

这里有一个非常重要的条件：

$$p \nmid n.$$

因为在 $\mathbf{F}_p$ 中，整数 n 要对 p 取模。

如果 $p \nmid n$ ，那么

$$n \not\equiv 0 \pmod{p}.$$

所以 n 在 $\mathbf{F}_p$ 中是一个非零常数。

因此：

$$F'(x) = nx^{n-1}$$

与

$$x^{n-1}$$

只有一个非零常数倍的区别。

所以如果 F 和 F' 有公共的非常数因子，它最终必须来自 x 。

但：

$$x \nmid x^n - 1.$$

为什么？

因为 $x^n - 1$ 的常数项是

$$-1 \neq 0.$$

所以：

$$\gcd(x^n - 1, nx^{n-1}) = 1.$$

也就是：

$$\gcd(F, F') = 1.$$

而刚刚已经知道：

$$F \text{ 有重因子} \implies \gcd(F, F') \neq 1.$$

现在反过来：

$$\gcd(F, F') = 1 \implies F \text{ 没有重因子}.$$

因此：

$$p \nmid n \implies x^n - 1 \text{ 在 } \mathbf{F}_p[x] \text{ 中没有重因子}.$$

也可以从“根”的角度看同一件事，这可能更直观。

假设 α 是 $x^n - 1$ 的重根。

那么必须同时满足：

$$\alpha^n - 1 = 0$$

和

$$n\alpha^{n-1} = 0.$$

第一式：

$$\alpha^n = 1$$

说明

$$\alpha \neq 0.$$

第二式中，因为

$$p \nmid n,$$

所以在 $\mathbf{F}_p$ 中：

$$n \neq 0.$$

又因为：

$$\alpha \neq 0,$$

所以：

$$n\alpha^{n-1} \neq 0.$$

矛盾。

因此不存在重根。

这里你还值得看一下为什么条件

$$\boxed{p \nmid n}$$

必不可少。

假设反过来：

$$p \mid n.$$

最简单取

$$n = p.$$

那么在模 p 下，根据我们刚讲过的 Frobenius：

$$x^p - 1 = (x - 1)^p.$$

例如模 3：

$$x^3 - 1 = (x - 1)^3 \quad \text{在 } \mathbf{F}_3[x] \text{ 中.}$$

因为：

$$(x - 1)^3 = x^3 - 3x^2 + 3x - 1 \equiv x^3 - 1 \pmod{3}.$$

这时候 1 是一个三重根。

同时：

$$(x^p - 1)' = px^{p-1} = 0$$

因为在模 p 下：

$$p = 0.$$

所以你现在应该能看到为什么前面的证明特意要求：

$$\boxed{p \nmid n}.$$

它正是为了保证导数

$$nx^{n-1}$$

不会因为模 p 而整个变成零。

最后再把它接回我们正在证明的分圆多项式不可约性：

我们前一步假设 $f(\zeta^p) \neq 0$ ，推出了

$$\bar{\Phi}_n$$

在 $\mathbf{F}_p[x]$ 中有重因子。

由于

$$\bar{\Phi}_n \mid x^n - 1,$$

就会导致

$$x^n - 1$$

也有重因子。

可是刚刚证明：

$$p \nmid n \implies x^n - 1 \text{ 没有重因子.}$$

矛盾。

因此原来的假设只能是错的：

$$\boxed{f(\zeta^p) = 0}.$$

这就是那个“最后一击”中间缺失的完整逻辑。

8.2 可分的定义，以及特征零为什么保证代数扩张可分

原问题：所以特征为0和可分到底是什么意思

再说可分 (separable)。

先别急着讲“扩张可分”，先看一个多项式。

如果一个多项式在代数闭包中分解以后，所有根都互不相同，就叫它**可分多项式**。

例如：

$$f(x) = x^2 - 2$$

在 $\mathbb{C}$ 中分解：

$$(x - \sqrt{2})(x + \sqrt{2}).$$

两个根不同，所以它是可分的。

但如果：

$$f(x) = (x - 1)^2,$$

根 1 出现了两次，所以它不是可分的。

因此可以先简单理解为：

可分 = 没有重根

更准确地说，是“在分裂域中没有重复根”。

现在把它放到代数元上。

假设 α 在 F 上代数，它有最小多项式

$$m_{\alpha, F}(x).$$

如果这个最小多项式没有重根，就称：

α 在 F 上可分

如果一个代数扩张 E/F 中每一个元素都在 F 上可分，就称：

E/F 是可分扩张.

所以“扩张可分”最终仍然是在说：

这些代数元的最小多项式有没有重根。

现在才来到你问的关键：

$\text{char } F = 0 \implies$ 所有不可约多项式都是可分的

为什么？

这里要用你刚才已经学过的“导数检测重根”。

如果 $f(x)$ 有重根，那么：

$$\gcd(f, f') \neq 1.$$

现在假设

$$f(x) \in F[x]$$

是不可约多项式。

因为 f 不可约，如果

$$\gcd(f, f') \neq 1,$$

那么它们的公因子不可能只是一个小因子——由于 f 不可约，只能是：

$$\boxed{f \mid f'}.$$

可是如果 f 是非恒定多项式，

$$\deg f' < \deg f.$$

一个次数更高的非零多项式不可能整除一个次数更低的多项式。

所以只有一种可能：

$$f'(x) = 0.$$

因此我们得到一个非常关键的结论：

$$\boxed{\text{不可约多项式如果不可分} \implies f'(x) = 0.}$$

现在特征 0 就发挥作用了。

假设：

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

那么：

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

在特征 0 的域中：

$$1, 2, 3, \dots, n$$

这些整数作为域里的元素都不是 0。

因此只要 f 不是常数，就不可能所有导数项都消失：

$$\boxed{f' \neq 0}.$$

于是不可约多项式不可能有重根。

所以：

$$\boxed{\text{char } F = 0 \implies F \text{ 上每个不可约多项式都是可分的}.}$$

而代数元的最小多项式本来就是不可约的，所以所有代数元都是可分的。

最终：

$$\boxed{\text{char } F = 0 \implies \text{任何代数扩张 } E/F \text{ 都是可分的}.}$$

这也解释了为什么前面对于

$$\mathbb{Q}(\zeta_n)/\mathbb{Q}$$

我们几乎一句话就能处理“可分性”：

因为

$$\text{char } \mathbb{Q} = 0.$$

所以 ζ_n 的最小多项式

$$\Phi_n(x)$$

自动没有重根。

因此：

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是可分扩张.

而为什么正特征下会出问题，你看一个极端现象就明白了。

在特征 p 下：

$$(x^p)' = px^{p-1} = 0,$$

因为：

$$p = 0$$

在这个域里。

所以例如某些多项式可能长成

$$x^p - a$$

而导数竟然是：

$$0.$$

这在特征 **0** 中绝对不会发生，也正是不可约多项式或代数扩张的不可分现象只会出现在正**特征**里的根源。

所以你可以先把这三个层次记住：

$$\boxed{\text{char } F = 0}$$

意味着整数系数不会因为模 p 而消失；

因此：

$$\boxed{\text{非恒定不可约多项式的导数不为 } 0}$$

因此：

$$\boxed{\text{不可约多项式没有重根}}$$

因此：

$$\boxed{\text{代数扩张自动可分.}}$$

这就是“特征 **0**，所以自动可分”那句话背后的完整逻辑。

8.3 可分的字面意义：根分开，嵌入才有足够多的选择

原问题：但是这里的可分貌似没什么含义啊，我觉得可分必定有其字面的意义吧

对，你这个感觉是对的。“可分 (separable)”这个词不是随便起的，它确实有很直观的字面意义：根能够彼此“分开”。

最开始这个概念其实是针对多项式说的。设

$$f(x) \in F[x].$$

到了它的分裂域以后，我们把它写成一次因子的乘积。如果是

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

而且

$$\alpha_1, \alpha_2, \dots, \alpha_n$$

彼此不同，那么这些根就是“分开的”，因此称 f 可分：

separable $\approx$ roots are separable/distinguishable

反过来，如果出现：

$$f(x) = (x - \alpha)^p,$$

虽然次数是 p ，但所有根都“塌缩”成同一个 α ，你就没办法把 p 个根区分开来，所以称为不可分 (inseparable)。

一个普通例子：

$$f(x) = x^2 - 2.$$

在 $\mathbb{C}$ 中：

$$f(x) = (x - \sqrt{2})(x + \sqrt{2}).$$

两个根

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

是不同的，因此它们可以被“分开”：

$$\boxed{x^2 - 2 \text{ 是可分的}}.$$

但真正体现“不可分”含义的是正特征。

比如在特征 p 中考虑：

$$f(x) = x^p - a.$$

假设在代数闭包里存在 α ，满足

$$\alpha^p = a.$$

由于特征为 p ，二项式展开中间项全部消失：

$$(x - \alpha)^p = x^p - \alpha^p.$$

所以：

$$x^p - a = (x - \alpha)^p.$$

你会发现：

这是一个 p 次多项式，但它不是有 p 个不同的根，而是同一个根 α 重复了 p 次。

所以这些根没有办法“分开”：

inseparable

这个词的字面意义就非常明显了。

更重要的是，这个“分开”的含义到了 **Galois 理论**里会变得更深。

还记得我们说过，一个代数元 α 的最小多项式如果有多个根，那么不同的嵌入可能把

α

送到它的不同共轭根。

例如：

$$\alpha = \sqrt{2}.$$

最小多项式：

$$x^2 - 2$$

有两个不同的根：

$$\sqrt{2}, \quad -\sqrt{2}.$$

因此从

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

到 $\mathbb{C}$ 有两个固定 $\mathbb{Q}$ 的嵌入：

$$\sqrt{2} \mapsto \sqrt{2}$$

以及

$$\sqrt{2} \mapsto -\sqrt{2}.$$

所以：

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

同时恰好有两个不同的 $\mathbb{Q}$ -嵌入。

这不是巧合。

对于有限扩张 E/F ，如果它是可分的，那么：

$$\boxed{\#\{\text{固定 } F \text{ 的嵌入 } E \rightarrow \overline{F}\} = [E : F].}$$

也就是说，扩张的不同“方向”真的都能通过不同嵌入区分出来。

而不可分扩张就会发生“塌缩”。

假设一个代数元 α 的最小多项式次数是 p ，但在代数闭包中却只有一个不同的根：

$$m_\alpha(x) = (x - \alpha)^p.$$

虽然：

$$[F(\alpha) : F] = p,$$

但是你没有 p 个不同的共轭根可以把 α 送过去。

不同嵌入的数量就小于扩张次数。

极端情况下可能只有：

$$\alpha \mapsto \alpha$$

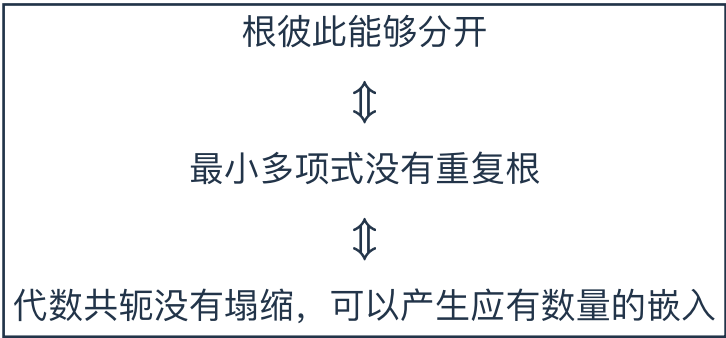
这一种选择。

所以“不可分”还可以理解成：

本应该由次数代表的多个代数共轭，发生了重合

这其实比单纯说“有重根”更能体现它为什么在 Galois 理论里重要。

所以你可以把 **separable** 理解成三个逐渐深入、但本质相同的说法：



第三层其实最能解释为什么 Galois 理论如此在意“可分”。

因为 Galois 理论本质上研究的是：

域的不同嵌入/自同构如何置换多项式的根

如果一个 p 次不可约多项式的 p 个根全塌成一个，根根本无法被置换，那么自同构就会严重减少。

这也解释了 Galois 扩张为什么要求同时满足：

可以粗略理解成：

- **正规**：某个根进来了以后，它的所有共轭根都在这个域里；
- **可分**：这些共轭根本身确实是彼此不同的。

这两个条件放在一起，Galois 群才能“完整地置换这些根”。

8.4 不可分例子的最小多项式为什么仍是 p 次

原问题：这个怎么看最小多项式都是一次的吧

对，你抓到了这里最容易产生误解的地方。关键是：“**最小多项式**”必须要求系数在基础域 F 里。

如果 $\alpha \notin F$ ，那么

$$x - \alpha$$

虽然当然以 α 为根，但它不属于

$$F[x],$$

因为它的系数 $-\alpha$ 不在 F 里面。

所以它**没有资格**成为 α 在 F 上的最小多项式。

举一个真正的不可分例子。取特征 p 的域

$$F = \mathbf{F}_p(t),$$

这里 t 可以理解成一个不定元。取 α 满足

$$\alpha^p = t.$$

那么 $\alpha \notin F$ ，而它满足

$$f(x) = x^p - t = 0.$$

事实上 $x^p - t$ 在 $F[x]$ 中不可约，因此：

$$\boxed{m_{\alpha, F}(x) = x^p - t}$$

它的次数是 p 。

但是到了代数闭包 $\overline{F}$ 里，因为特征是 p ，有

$$(x - \alpha)^p = x^p - \alpha^p$$

——中间的二项式系数全部在模 p 下消失。

又因为

$$\alpha^p = t,$$

所以

$$\boxed{x^p - t = (x - \alpha)^p}$$

是在 $\overline{F}[x]$ 里的分解。

所以同一个最小多项式：

$$m_{\alpha, F}(x) = x^p - t$$

在基础域 F 看，是一个 p 次不可约多项式；

但到了代数闭包里，它分裂成

$$(x - \alpha)^p,$$

只有一个不同的根 α ，重复了 p 次。

你刚才说“那最小多项式不是应该是 $x - \alpha$ 吗？”——如果基础域已经包含 α ，那完全正确：

$$m_{\alpha, F(\alpha)}(x) = x - \alpha.$$

但我们讨论的是 α 相对于原来的基础域 F 的最小多项式，而此时

$$x - \alpha \notin F[x].$$

所以这里一定要区分：

在 $F[x]$ 中：	$m_{\alpha, F}(x) = x^p - t;$
在 $\overline{F}[x]$ 中分解：	$m_{\alpha, F}(x) = (x - \alpha)^p.$

这也正是“不可分”最典型的样子：最小多项式在基础域上不可约、次数是 p ，但进入代数闭包以后， p 个根全部塌缩成同一个根。

8.5 补充证明：为什么 $x^p - t$ 在 $\mathbb{F}_p(t)[x]$ 不可约

先说明 t 不是有理函数的 p 次幂。若 $(A(t)/B(t))^p = t$ ，其中 $A, B \in \mathbb{F}_p[t]$ 非零，则 $A^p = tB^p$ 。比较两边被 t 整除的次数，左边为 $pv_t(A)$ ，右边为 $1 + pv_t(B)$ ，二者模 p 分别为 0 和 1 ，不可能相等。因此满足 $\alpha^p = t$ 的 α 不在 $F = \mathbb{F}_p(t)$ 中。

在代数闭包中， $x^p - t = (x - \alpha)^p$ 。若它在 $F[x]$ 可约，取首一真因子 h ，次数 r 满足 $1 \leq r < p$ 。由于只有一个不同的根， $h = (x - \alpha)^r$ ，其 x^{r-1} 的系数是 $-r\alpha$ 。该系数属于 F ，而 $r \neq 0$ 在特征 p 的域中可逆，故 $\alpha \in F$ ，矛盾。

因此 $x^p - t$ 不可约，确实是 α 在 F 上的最小多项式，扩张次数为 p 。它在代数闭包里仍只有一个不同的根；每个固定 F 的嵌入都只能把 α 送到自己。

原回答提到有限可分扩张的嵌入数等于扩张次数：对于简单扩张，嵌入与最小多项式不同根一一对应；一般有限可分扩张可分步加入有限个生成元，每一步把当前嵌入延拓的方法数等于该层最小多项式次数，乘起来由塔式定理得到总次数。

第 9 章：完整证明分圆多项式在有理数域上不可约

本章对象： $f = m_{\zeta_n, \mathbb{Q}}$, $\Phi_n = fg$ ；由 Gauss 引理知 f, g 首一且为整数系数。模 p 后不假设 $\bar{f}$ 仍不可约。

9.1 不可约性的目标：把分圆多项式认作最小多项式

原问题：好的，那下一步你要介绍什么

下一步最自然、也是这条线里最关键的一步，就是证明：

$$\Phi_n(x) \text{ 在 } \mathbb{Q}[x] \text{ 中不可约}$$

因为我们现在已经知道：

$$\Phi_n(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x].$$

而且 ζ_n 是它的一个根。

如果再证明 $\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约，那么根据最小多项式的定义，就立刻得到：

$$m_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x)$$

于是：

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n).$$

这一步非常重要，因为它把我们前面所有内容真正串起来了：

$$\boxed{\text{本原 } n \text{ 次单位根} \rightarrow \Phi_n(x) \rightarrow \text{最小多项式} \rightarrow \text{分圆域次数}}$$

然后再下一步就会进入 Galois 理论真正精彩的部分：

$$\sigma(\zeta_n) = \zeta_n^a, \quad \gcd(a, n) = 1,$$

进而得到

$$\boxed{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.}$$

所以我建议下一节就专门讲：为什么 $\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约。

这个证明比前面稍难，我会把它拆成几步，先讲证明策略，再逐步证明每一步。

9.2 不可约、首一且以指定元素为根，才是它的最小多项式

原问题：这里是怎么来的来着，是因为不可约直接就最小了吗

对，核心就是这个逻辑，但要加上一个条件：它不仅不可约，而且 ζ_n 确实是它的根。

我们已经知道：

$$\Phi_n(\zeta_n) = 0,$$

所以 $\Phi_n(x)$ 是一个在 $\mathbb{Q}[x]$ 中以 ζ_n 为根的多项式。

而 ζ_n 的最小多项式

$$m_{\zeta_n, \mathbb{Q}}(x)$$

有一个基本性质：

$$m_{\zeta_n, \mathbb{Q}}(x) \mid f(x)$$

对所有满足

$$f(\zeta_n) = 0, \quad f(x) \in \mathbb{Q}[x]$$

的多项式都成立。

所以特别地：

$$m_{\zeta_n, \mathbb{Q}}(x) \mid \Phi_n(x).$$

现在如果我们要再证明

$$\Phi_n(x)$$

在 $\mathbb{Q}[x]$ 中不可约，那么它的非平凡因子只有常数和它自己。

而最小多项式不是常数，所以只能：

$$m_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x)$$

因为两者还都是首一多项式。

所以你可以记成：

$$f(\alpha) = 0 + f \text{ 在 } F[x] \text{ 中首一不可约} \implies f = m_{\alpha, F}.$$

这里不是“只要不可约就自动是最小多项式”，而是要同时满足：

不可约 + 确实以 α 为根

才行。

9.3 不可约性证明策略：先处理不整除 n 的素数指数

下一步就开始证明：

$\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可约

这个证明比前面的内容明显难一层，所以我们先把证明目标和路线看明白，不急着一口气走完。

设

$$\zeta = \zeta_n$$

是我们固定的一个本原 n 次单位根。令它在 $\mathbb{Q}$ 上的最小多项式为

$$f(x) = m_{\zeta, \mathbb{Q}}(x).$$

因为

$$\Phi_n(\zeta) = 0,$$

所以前面已经证明过：

$$f(x) \mid \Phi_n(x).$$

现在我们来证明：

$$f(x) = \Phi_n(x).$$

也就是说，我们要证明：

f 不仅包含 ζ 这个根，而且实际上把 所有本原 n 次单位根都包含进去了。

为什么这样就够了？

因为

$$\Phi_n(x) = \prod_{\substack{1 \leq a \leq n \\ \gcd(a, n) = 1}} (x - \zeta^a).$$

所以如果我们能证明：

$$f(\zeta^a) = 0 \quad \text{对所有 } \gcd(a, n) = 1$$

那么 Φ_n 的所有根都是 f 的根。

而我们本来又知道：

$$f \mid \Phi_n.$$

两边都是首一多项式，因此只能：

$$f = \Phi_n.$$

这就是整个证明真正的核心。

现在问题变成：

$$\zeta \text{ 是 } f \text{ 的根} \implies \zeta^a \text{ 也都是 } f \text{ 的根吗?}$$

其中要求

$$\gcd(a, n) = 1.$$

我们不会直接证明任意 a ，而是先证明一个关键步骤：

$$p \nmid n, p \text{ 是素数} \implies f(\zeta^p) = 0.$$

也就是说：

如果 p 是一个不整除 n 的素数，那么从根 ζ 出发，把它变成 ζ^p ，仍然不会离开同一个最小多项式 f 的根集合。

为什么只证明素数 p 就够了？

因为如果

$$\gcd(a, n) = 1,$$

把 a 分解成素数：

$$a = p_1 p_2 \cdots p_r.$$

由于 a 和 n 互素，所以每个 p_i 都不整除 n 。

如果我们知道每一次

$$\alpha \mapsto \alpha^{p_i}$$

都仍然留在 f 的根中，那么就可以一步步得到：

$$\zeta \rightarrow \zeta^{p_1} \rightarrow \zeta^{p_1 p_2} \rightarrow \cdots \rightarrow \zeta^a.$$

于是所有

$$\zeta^a, \quad \gcd(a, n) = 1$$

都会成为 f 的根。

所以整个不可约性证明可以压缩成：

$$\boxed{\text{只要证明 } p \nmid n \implies \zeta^p \text{ 与 } \zeta \text{ 有同一个最小多项式}}$$

接下来就进入真正技术性的那一步：假设 ζ^p 不是 f 的根，然后利用模 p 多项式和 $x^n - 1$ 没有重根制造矛盾。

这一步会首次用到一个非常漂亮的恒等式：

$$\boxed{g(x^p) \equiv g(x)^p \pmod{p}}$$

它其实来自二项式系数

$$\binom{p}{k}$$

在 $0 < k < p$ 时都被 p 整除。下一步我们就先把这个恒等式讲透，再把它放进不可约性的证明里。

9.4 补充证明：Gauss 引理，以及首一有理因子为什么是整数系数

这是原对话只引用、未展开的关键步骤。整数多项式的各系数最大公因数为 1 时，称它为本原多项式。这里的“本原多项式”是系数条件，与“本原单位根”的阶条件不同。

第一步，本原多项式的乘积仍本原。 若本原的 $A, B \in \mathbb{Z}[x]$ 的乘积不本原，则存在素数 p 整除乘积的所有系数。模 p 后 $\bar{A}\bar{B} = 0$ ，但 $\bar{A}, \bar{B}$ 都非零，而 $\mathbb{F}_p[x]$ 是整环，矛盾。整环性直接来自非零多项式乘积的首项系数非零。

第二步，首一整系数多项式的首一有理因子仍为整数系数。设 $H \in \mathbb{Z}[x]$ 首一， $H = fg$ ， $f, g \in \mathbb{Q}[x]$ 首一。清分母并除去各系数公因数后，可写 $f = A/a$ 、 $g = B/b$ ，其中 A, B 本原， a, b 是它们的正首项系数。于是 $AB = abH$ 。左边由第一步本原，右边因 H 首一而其系数公因数恰好是 ab ，故 $ab = 1$ ，即 $a = b = 1$ 。因此 $f, g \in \mathbb{Z}[x]$ 。

应用到 $\Phi_n = fg$ ，因 Φ_n 首一且整数系数、最小多项式 f 首一，商 g 也首一，所以两者都是整数系数。

还需检查 $f \mid g(x^p)$ 能否模 p ：先在 $\mathbb{Q}[x]$ 得到整除，再在 $\mathbb{Z}[x]$ 用首一 f 做长除法。商和余数均为整数系数，而除法唯一性保证余数为零。因此整除关系本身在 $\mathbb{Z}[x]$ 中成立，取模后才合法地得到 $\bar{f} \mid \bar{g}(x^p)$ 。

9.5 不可约性关键矛盾：取模后产生重因子

现在把它放回分圆多项式的不可约性证明。

我们设：

$$f(x) = m_{\zeta, \mathbb{Q}}(x)$$

是本原 n 次单位根 ζ 的最小多项式。

因为

$$f \mid \Phi_n,$$

写成：

$$\boxed{\Phi_n(x) = f(x)g(x).}$$

这里 f, g 都可以取成整数系数首一多项式。这个结论来自 Gauss 引理；本章前面的补充证明已给出完整推导。

现在取一个素数 p ，满足：

$$p \nmid n.$$

我们想证明：

$$\zeta^p$$

也一定是 f 的根。

假设反过来：

$$\boxed{f(\zeta^p) \neq 0.}$$

因为

$$p \nmid n,$$

所以

$$\gcd(p, n) = 1.$$

因此前面已经证明过：

$$\zeta^p$$

仍然是一个本原 n 次单位根。

所以：

$$\Phi_n(\zeta^p) = 0.$$

而：

$$\Phi_n = fg.$$

于是：

$$f(\zeta^p)g(\zeta^p) = 0.$$

我们假设：

$$f(\zeta^p) \neq 0,$$

所以只能：

$$\boxed{g(\zeta^p) = 0.}$$

换一种写法：

$$g(\zeta^p) = 0 \iff g(x^p) \Big|_{x=\zeta} = 0.$$

所以：

$$\boxed{\zeta \text{ 是 } g(x^p) \text{ 的根.}}$$

但 f 是 ζ 的最小多项式。

因此：

$$\boxed{f(x) \mid g(x^p).}$$

这一步就是我们前面反复用过的：

最小多项式整除所有以该代数元为根的多项式。

现在才轮到刚刚证明的模 p 恒等式：

$$g(x^p) \equiv g(x)^p \pmod{p}.$$

因为：

$$f(x) \mid g(x^p),$$

模 p 以后仍然得到：

$$\boxed{\bar{f}(x) \mid \bar{g}(x^p)}$$

而：

$$\bar{g}(x^p) = \bar{g}(x)^p.$$

因此：

$$\boxed{\bar{f}(x) \mid \bar{g}(x)^p.}$$

这里上面的横线只是表示：

“把整数系数对 p 取模”。

例如：

$$2x^2 + 5x + 7$$

模 3 后变成：

$$2x^2 + 2x + 1.$$

现在最关键的事情发生了。

我们原本有：

$$\Phi_n = fg.$$

模 p 后：

$$\bar{\Phi}_n = \bar{f}\bar{g}.$$

与此同时：

$$\bar{f} \mid \bar{g}^p.$$

这意味着 $\bar{f}$ 和 $\bar{g}$ 不可能完全没有公共因子。更准确地说， $\bar{f}$ 的某个不可约因子也一定出现在 $\bar{g}$ 里面。

于是：

$$\bar{f}\bar{g}$$

里面这个因子至少出现两次。

也就是说：

$\bar{\Phi}_n(x)$ 在模 p 下出现了重因子。

而：

$$\Phi_n(x) \mid x^n - 1.$$

所以如果 Φ_n 模 p 有重因子，那么：

$$x^n - 1$$

模 p 也会有重因子。

接下来就是整个证明最后漂亮的一击：

$$p \nmid n \implies x^n - 1 \text{ 在模 } p \text{ 下根本不可能有重因子.}$$

为什么？因为它的导数是

$$nx^{n-1},$$

而在模 p 下由于 $p \nmid n$ ，这个导数不是零多项式，而且和 $x^n - 1$ 没有公共根。

这一点我们下一步可以仔细证明。证明完就产生矛盾，从而得到：

$$f(\zeta^p) = 0.$$

然后再从素数 p 推广到所有

$$\gcd(a, n) = 1$$

的 a ，最终得到

$$f = \Phi_n.$$

9.6 补充检查：模 p 后没有暗中假设不可约

从 $\bar{f} \mid \bar{g}^p$ 不能推出 $\bar{f} \mid \bar{g}$ ，因为 $\bar{f}$ 未必不可约。正确做法是： f 首一且次数至少为 1，所以模 p 后次数不变， $\bar{f}$ 有一个不可约因子 h 。域上的多项式 Euclidean 算法说明不可约因子有素性：若 $h \nmid A$ ，则 $uh + vA = 1$ ；若 $h \mid AB$ ，乘 B 即得 $h \mid B$ 。

故 $h \mid \bar{g}^p$ 推出 $h \mid \bar{g}$ 。于是 $h^2 \mid \bar{f}\bar{g} = \bar{\Phi}_n$ ，继而 $h^2 \mid x^n - 1$ ，与 $p \nmid n$ 时没有重因子矛盾。

此论证同样适用于 f 的任意根 α : f 不可约, $f(\alpha) = 0$ 就说明 f 是 α 的最小多项式; $f \mid \Phi_n$ 又保证 α 是本原 n 次单位根。因此“乘一个不整除 n 的素数指数”可以逐次重用, 并非只对最初选定的 ζ_n 成立。任意互素指数先取正的剩余类代表; 指数 1 无需任何步骤。

9.7 为何可以对每个素因子重复同一个步骤

原问题：这个是重复之前的步骤就可以吗

对，本质上就是重复使用前面那个“乘一个素数指数”的步骤。不过有一个小细节值得说清楚。

前面我们证明的是：

α 是 f 的一个本原 n 次单位根, 且 $p \nmid n \implies \alpha^p$ 仍然是 f 的根

一开始取

$$\alpha = \zeta_n.$$

若

$$a = p_1 p_2 \cdots p_r, \quad \gcd(a, n) = 1,$$

那么每个 p_i 都不整除 n 。

第一次用结论：

$$\zeta_n \longmapsto \zeta_n^{p_1},$$

得到

$$f(\zeta_n^{p_1}) = 0.$$

而且由于

$$\gcd(p_1, n) = 1,$$

所以

$$\zeta_n^{p_1}$$

仍然是本原 n 次单位根。

因此可以把它当成新的 α ，再对 p_2 使用同一个结论：

$$\zeta_n^{p_1} \longmapsto (\zeta_n^{p_1})^{p_2} = \zeta_n^{p_1 p_2}.$$

于是

$$f(\zeta_n^{p_1 p_2}) = 0.$$

再重复：

$$\zeta_n^{p_1 p_2} \longmapsto \zeta_n^{p_1 p_2 p_3}$$

.....

最后得到：

$$\boxed{f(\zeta_n^a) = 0.}$$

所以你说的“重复之前的步骤”完全正确。严格地说，这是对素因子个数做一次小归纳。

关键保证是：每一步得到的元素都仍然是本原 n 次单位根，因为累计指数始终与 n 互素。

9.8 从素数指数到所有互素指数，完成不可约性证明

原问题：下一步是要介绍什么了

下一步最自然的是把刚才已经铺好的证明收尾，真正得到：

$$\Phi_n(x) \text{ 在 } \mathbb{Q}[x] \text{ 中不可约}$$

其实我们已经完成了大部分困难步骤，现在还剩两个连接点。

第一，我们已经证明：如果

$$f(x) = m_{\zeta_n, \mathbb{Q}}(x)$$

而 p 是满足

$$p \nmid n$$

的素数，那么

$$\zeta_n^p \text{ 也一定是 } f(x) \text{ 的根}$$

否则会推出 $x^n - 1$ 在模 p 下有重因子，产生矛盾。

第二，我们接下来要把这个结论从“指数是一个素数 p ”推广到任意

$$\gcd(a, n) = 1.$$

因为如果

$$a = p_1 p_2 \cdots p_r$$

是素因数分解，而 $\gcd(a, n) = 1$ ，那么每个 p_i 都不整除 n 。

于是从

$$\zeta_n$$

开始：

$$\zeta_n \longmapsto \zeta_n^{p_1} \longmapsto \zeta_n^{p_1 p_2} \longmapsto \cdots \longmapsto \zeta_n^a.$$

每一步得到的仍然是 f 的根，所以最终：

$$f(\zeta_n^a) = 0 \quad \forall \gcd(a, n) = 1$$

而这些

$$\zeta_n^a$$

恰好就是所有本原 n 次单位根。

所以 f 包含了 Φ_n 的全部根。

另一方面，我们早就知道：

$$f \mid \Phi_n.$$

于是只能有：

$$f = \Phi_n.$$

因此：

$$\Phi_n(x) \text{ 在 } \mathbb{Q}[x] \text{ 中不可约.}$$

这样我们就真正得到：

$$m_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x)$$

以及：

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$$

到这里，“分圆多项式”这一部分基本就闭环了。

再下一步就该正式进入分圆域：

$$\mathbb{Q}(\zeta_n)$$

然后回答一个非常 Galois 理论的问题：

一个固定 $\mathbb{Q}$ 的自同构 σ ，能够把 ζ_n 送到哪里？

最后会得到非常漂亮的结论：

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

我建议下一步就从“为什么一个自同构必须把 ζ_n 送到另一个本原 n 次单位根”开始。

9.9 任意本原 n 次单位根在有理数域上都有同一个最小多项式

原问题：换言之分圆多项式就是在 $\mathbb{Q}$ 域中，本原 n 次根的最小的多项式，对于任何一个本原 n 次根都是

对，完全可以这样理解，但把表述稍微说严谨一点：

$\Phi_n(x)$ 是任意一个本原 n 次单位根在 $\mathbb{Q}$ 上的最小多项式

也就是说，如果 ζ_n 是一个本原 n 次单位根，那么

$$m_{\zeta_n, \mathbb{Q}}(x) = \Phi_n(x).$$

而且不只是你固定选的那个 ζ_n 。对于任何

$$\zeta_n^a, \quad \gcd(a, n) = 1,$$

它也是本原 n 次单位根，并且都有：

$$m_{\zeta_n^a, \mathbb{Q}}(x) = \Phi_n(x)$$

所以所有本原 n 次单位根，在 $\mathbb{Q}$ 看来都是“同一类代数元”，它们互为共轭。

例如 $n = 5$ ：

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

四个本原 5 次单位根

$$\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$$

在 $\mathbb{Q}$ 上的最小多项式全都是同一个：

$$x^4 + x^3 + x^2 + x + 1.$$

所以你可以把分圆多项式理解成：

“把所有本原 n 次单位根作为共轭根收集起来的那个最小多项式”

这也正是后面 Galois 自同构为什么会在这些本原单位根之间互相置换的根本原因。

第 10 章：分裂域、正规性与 Galois 扩张

本章对象： $K = \mathbb{Q}(\zeta_n)$ ；正规性针对所有在扩域中有根的基础域不可约多项式，不能只检查一个例子。

10.1 把正规与可分接回分圆域

原问题：好吧，那下一步要介绍什么

下一步最合适的是把“可分”接回到你真正关心的 Galois 理论主线：

为什么 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是 Galois 扩张？

这一步会把两个条件彻底串起来：

Galois = 正规 + 可分

你刚刚已经基本理解了“可分”：

$\text{char } \mathbb{Q} = 0 \implies \mathbb{Q}(\zeta_n)/\mathbb{Q}$ 自动可分。

所以现在剩下真正值得讲的是：

为什么它正规？

而这里正好会解释你之前问过的“正规性和分裂域到底是什么关系”。

核心思路是：

ζ_n

是 $x^n - 1$ 的一个根，但

$$\mathbb{Q}(\zeta_n)$$

实际上不只是包含这一个根。

因为所有 n 次单位根都是：

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1},$$

它们全部都已经属于

$$\mathbb{Q}(\zeta_n).$$

因此：

$$x^n - 1 = \prod_{k=0}^{n-1} (x - \zeta_n^k)$$

在 $\mathbb{Q}(\zeta_n)$ 里完全分裂。

所以：

$\mathbb{Q}(\zeta_n)$ 是 $x^n - 1$ 在 $\mathbb{Q}$ 上的分裂域
--

而有限扩张有一个非常重要的定理：

E/F 正规 $\iff E$ 是某个 $F[x]$ 中多项式族的分裂域
--

所以：

$$\mathbb{Q}(\zeta_n)/\mathbb{Q}$$

正规。

再加上刚才的可分：

$$\mathbb{Q}(\zeta_n)/\mathbb{Q} \text{ 是 Galois 扩张.}$$

接下来我建议就专门讲这件事：**为什么“分裂域”会推出“正规”，以及正规到底是什么意思。**这会比直接背“正规 = 分裂域”更有帮助。

10.2 分裂域为什么正规，分圆域为什么是 Galois 扩张

我们就从“正规到底是什么意思”开始，而不是先背结论。

先设

$$E/F$$

是一个代数扩张。

“正规 (normal)”最常用的定义是：

如果 $f(x) \in F[x]$ 是不可约多项式，且它在 E 中有一个根，

那么：

$f(x)$ 在 E 中必须完全分裂。

这句话很值得慢慢看。

比如：

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

$\sqrt{2}$ 的最小多项式是

$$x^2 - 2.$$

它的另一个根是

$$-\sqrt{2},$$

也同样属于 $\mathbb{Q}(\sqrt{2})$ 。

所以这个不可约多项式一旦有一个根进入 E ，它的另一个共轭根也一起进来了。

这就是“正规”想表达的核心：

不能只收进某个不可约多项式的一部分根。

反过来看一个不正规的例子：

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

$\sqrt[3]{2}$ 的最小多项式是

$$x^3 - 2.$$

它在 $\mathbb{C}$ 中有三个根：

$$\sqrt[3]{2}, \quad \omega\sqrt[3]{2}, \quad \omega^2\sqrt[3]{2},$$

其中

$$\omega = e^{2\pi i/3}.$$

但是

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

只包含那个实根

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

并不包含另外两个复根。

所以：

$$\boxed{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \text{ 不正规.}}$$

因为它“只拿进来了一个根，没有把同一个不可约多项式的所有根都拿进来”。

现在你就能看懂为什么“分裂域”天然和正规有关。

假设

$$E$$

是某个多项式 $f(x) \in F[x]$ 的分裂域。

意思是：

$$E$$

是让

$$f(x)$$

完全分裂所需的最小域。

所以 E 是由 f 的全部根生成的。

直觉上，它不会偏爱其中某一个根。

如果一个 F -嵌入

$$\sigma : E \rightarrow \overline{F}$$

固定 F ，那么 σ 会把 f 的根送到 f 的根。

因为若

$$f(\alpha) = 0,$$

那么：

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

这里用了 σ 固定 F ，所以 f 的系数不变。

因此：

σ 只是重新排列 f 的根

而这些根本来全都已经在 E 里面。

所以：

$$\sigma(E) = E.$$

这就是正规性的另一个非常重要的等价刻画：

E/F 正规 $\iff$ 每个固定 F 的嵌入 $E \rightarrow \overline{F}$ 都把 E 映回自己

你可以把它理解成：

从外面看这个扩域，无论你怎么把它的共轭根重新排列，都不会跑出这个域。

这就是“正规”的几何/对称意义。

现在回到分圆域：

$$E = \mathbb{Q}(\zeta_n).$$

我们知道 $x^n - 1$ 的所有根都是：

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}.$$

而因为 E 已经包含 ζ_n ，所以它当然包含所有幂：

$$\zeta_n^k.$$

因此 $x^n - 1$ 在 E 中完全分裂。

而 E 又显然是由这些根生成的最小域，所以：

$$\boxed{\mathbb{Q}(\zeta_n) \text{ 是 } x^n - 1 \text{ 的分裂域}}$$

于是：

$$\boxed{\mathbb{Q}(\zeta_n)/\mathbb{Q} \text{ 正规.}}$$

再加上：

$$\text{char } \mathbb{Q} = 0$$

所以可分。

因此：

$$\boxed{\mathbb{Q}(\zeta_n)/\mathbb{Q} \text{ 是 Galois 扩张.}}$$

最值得记住的是这三个层次：

$$\boxed{\text{分裂域} \Rightarrow \text{所有共轭根都在里面} \Rightarrow \text{正规}}$$

而：

$$\boxed{\text{正规} + \text{可分} = \text{Galois}}$$

下一步最值得讲的是：为什么 $\mathbb{Q}(\sqrt[3]{2})$ 不正规，而它的分裂域

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

却正规。这个例子能把“只加一个根”和“加入全部根”的区别看得特别清楚。

10.3 补充证明：从嵌入稳定性到定义中的所有不可约多项式

原回答解释了嵌入如何置换用于生成分裂域的那些根。要推出正规性的定义，还必须处理任意 $h \in F[x]$ 不可约且在 E 中有根的情况。

有限代数扩张的嵌入延拓。 设 $\tau: L \rightarrow \Omega$ 为域嵌入， Ω 代数闭。加入一个代数元 β ，把它在 L 上的最小多项式 m 的系数逐个用 τ 映过去，得到 m^τ ；选它在 Ω 中的根 γ 。 m^τ 在 $\tau(L)[x]$ 中仍不可约（否则逆映系数会分解 m ），所以 $u(\beta) \mapsto u^\tau(\gamma)$ 给出 $L(\beta) \rightarrow \Omega$ 的嵌入。良定义与单射由最小多项式整除性质保证。有限扩张只需依次加入有限个生成元，故可逐层延拓。

现在设 E 是 $f \in F[x]$ 的分裂域。它由 f 的全部不同根生成。每个固定 F 的嵌入 $\sigma: E \rightarrow \Omega$ 都把这些根送到同一有限根集，并因单射而形成该根集的排列，所以 $\sigma(E) = E$ 。

若不可约 $h \in F[x]$ 有根 $\alpha \in E$ ，任取它在 Ω 中的另一根 β 。由相同最小多项式得到嵌入 $F(\alpha) \rightarrow \Omega$ ， $\alpha \mapsto \beta$ 。把它延拓到 E 后，刚证明的稳定性给出 $\beta \in E$ 。因此 h 的所有不同根都在 E ，按重数也完全分裂，故 E/F 正规。

反方向对有限扩张也成立：若 E/F 正规，选有限个生成元，把它们的最小多项式相乘。正规性保证该乘积在 E 中分裂，且它的根生成的域既包含全部生成元，又包含于 E ，因此恰为 E 。

10.4 单位根取幂后生成的域仍然正规

原问题：但是这个不知道怎么读的指数加一下就不一定是正规了吧

整理提示：原问题对“指数加一下”的意思并不完全明确，原解释按“取整数幂”作答。这里的结论只针对取幂；随意改变生成元没有统一的正规性结论。

对，你这里问得很关键。你看到的

$$\zeta_n$$

读作“zeta 下标 n ”（ ζ 是希腊字母 zeta）。

如果你的意思是：把生成元从 ζ_n 换成它的某个幂

$$\mathbb{Q}(\zeta_n^a),$$

那有意思的是：它依然是正规扩张，只是可能变成一个更小的分圆域。

原因是 ζ_n^a 的阶为

$$d = \frac{n}{\gcd(a, n)}.$$

所以 ζ_n^a 实际上是一个本原 d 次单位根。因此

$$\boxed{\mathbb{Q}(\zeta_n^a) = \mathbb{Q}(\zeta_d)}$$

其中

$$d = \frac{n}{\gcd(a, n)}.$$

而 $\mathbb{Q}(\zeta_d)$ 又是 $x^d - 1$ 的分裂域，所以依然正规。

特别地，如果

$$\gcd(a, n) = 1,$$

那么 $d = n$ ，于是

$$\zeta_n^a$$

仍然是本原 n 次单位根，而且实际上

$$\boxed{\mathbb{Q}(\zeta_n^a) = \mathbb{Q}(\zeta_n)}.$$

例如

$$\mathbb{Q}(\zeta_5^2) = \mathbb{Q}(\zeta_5).$$

因为 **2** 和 **5** 互素。

但如果取

$$\zeta_6^2,$$

它的阶是

$$\frac{6}{\gcd(6, 2)} = 3,$$

所以

$$\boxed{\mathbb{Q}(\zeta_6^2) = \mathbb{Q}(\zeta_3)}.$$

在这个例子里， $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ ，所以阶降低了，生成域却没有变小；它仍然正规。具体等式在本章补充证明中验证。

所以这里要修正一下直觉：**对单位根来说，取 ζ_n 的任意整数次幂并不会制造一个“不正规”的例子。它只会得到另一个分圆域。真正典型的不正规例子仍然是像

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$$

这种“只加入不可约多项式的一个根，却没有加入其他共轭根”的扩张。

10.5 补充证明与校正：取幂后的阶变小，生成域却未必变小

设 $a \in \mathbb{Z}$, $g = \gcd(a, n) > 0$, $d = n/g$, 写 $a = ga'$ 。按固定选择 $\zeta_m = e^{2\pi i/m}$, 有 $\zeta_n^a = \zeta_d^{a'}$, 且 $\gcd(a', d) = 1$ 。取整数 b 使 $a'b \equiv 1 \pmod{d}$, 则 $(\zeta_n^a)^b = \zeta_d$ 。两个方向的包含都成立，故 $\mathbb{Q}(\zeta_n^a) = \mathbb{Q}(\zeta_d)$ 。

这里的 d 变小只说明单位根的阶变小。域可以相同，例如 $\zeta_6^2 = \zeta_3$ ，同时 $\zeta_6 = 1 + \zeta_3$ ，所以 $\mathbb{Q}(\zeta_6^2) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ 。原回答把这个例子说成更小的域，本版已校正。

严格变小的例子是 $\mathbb{Q}(\zeta_8^2) = \mathbb{Q}(i)$ ：前者对应阶 4，相对于 $\mathbb{Q}$ 次数为 2； $\mathbb{Q}(\zeta_8)$ 次数为 4。取任意整数幂后得到的仍是分圆域，因此仍正规。

第 11 章：分圆域的同构与模 n 可逆元群

本章对象： $\sigma_a : K \rightarrow K$ 固定 $\mathbb{Q}$ ，把 ζ_n 送到 ζ_n^a ； Ψ 的输入是剩余类，输出是域自同构。

11.1 自同构必须把生成元送到另一个本原单位根

我们现在正式进入分圆域的 Galois 群。

设

$$K = \mathbb{Q}(\zeta_n),$$

其中 ζ_n 是一个固定的本原 n 次单位根。

我们要研究：

$$\text{Gal}(K/\mathbb{Q}),$$

也就是所有固定 $\mathbb{Q}$ 的域自同构

$$\sigma : K \rightarrow K.$$

关键问题是：

$$\sigma(\zeta_n) \text{ 可以是什么?}$$

先从一个最基本的事实开始。因为

$$\zeta_n^n = 1,$$

对两边作用 σ ：

$$\sigma(\zeta_n^n) = \sigma(1).$$

自同构保持乘法，而且固定 1 ，所以：

$$\sigma(\zeta_n)^n = 1.$$

因此：

$$\sigma(\zeta_n) \text{ 一定还是一个 } n \text{ 次单位根}$$

但这还不够。我们还要证明它其实是本原 n 次单位根。

假设

$$\sigma(\zeta_n)$$

的阶是 $d < n$ 。

那就有：

$$\sigma(\zeta_n)^d = 1.$$

于是：

$$\sigma(\zeta_n^d) = 1.$$

也就是：

$$\sigma(\zeta_n^d) = \sigma(1).$$

因为 σ 是单射，所以：

$$\zeta_n^d = 1.$$

但 ζ_n 的阶是 n ，这与 $d < n$ 矛盾。

因此：

$$\boxed{\text{ord}(\sigma(\zeta_n)) = n}.$$

也就是说：

$$\boxed{\sigma(\zeta_n) \text{ 必须是另一个本原 } n \text{ 次单位根}}$$

而所有本原 n 次单位根都长成：

$$\zeta_n^a, \quad \gcd(a, n) = 1.$$

所以：

$$\sigma(\zeta_n) = \zeta_n^a \quad \text{其中 } \gcd(a, n) = 1$$

这就是第一步。

而且因为

$$K = \mathbb{Q}(\zeta_n),$$

整个域里的元素都是由 $\mathbb{Q}$ 和 ζ_n 生成的，所以一个自同构一旦知道

$$\sigma(\zeta_n)$$

是什么，就完全确定了。

例如：

$$\sigma(a_0 + a_1\zeta_n + \cdots + a_m\zeta_n^m) = a_0 + a_1\sigma(\zeta_n) + \cdots + a_m\sigma(\zeta_n)^m,$$

因为所有 $a_i \in \mathbb{Q}$ 都被固定。

所以：

$$\text{一个 Galois 自同构完全由 } \zeta_n \text{ 的像决定}$$

现在自然出现一个映射：

$$\sigma \longmapsto a \pmod{n},$$

其中

$$\sigma(\zeta_n) = \zeta_n^a.$$

而 a 必须满足：

$$\gcd(a, n) = 1.$$

所以这些 a 正好构成：

$$(\mathbb{Z}/n\mathbb{Z})^\times.$$

下一步就要证明两件事：

每个 $\gcd(a, n) = 1$ 的 a 都真的对应一个自同构

以及：

$$\sigma_a \circ \sigma_b = \sigma_{ab}$$

这样才能真正得到：

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

这一步也正好能解释你之前问过的“Galois 自同构到底要不要固定单位根”：它固定的是基础域 $\mathbb{Q}$ ，并不固定 ζ_n ；相反，它可以在所有本原 n 次单位根之间置换。

11.2 追问：在哪里证明了自同构保持本原性

原问题：什么时候证明了

就是在你刚才说“那就继续吧”之后那一步证明的。核心分成两段。

先设

$$K = \mathbb{Q}(\zeta_n), \quad \sigma \in \text{Gal}(K/\mathbb{Q}).$$

因为

$$\zeta_n^n = 1,$$

对两边作用 σ :

$$\sigma(\zeta_n^n) = \sigma(1).$$

由于 σ 保持乘法且 $\sigma(1) = 1$, 得到

$$\sigma(\zeta_n)^n = 1.$$

所以

$$\boxed{\sigma(\zeta_n) \text{ 是一个 } n \text{ 次单位根.}}$$

然后还证明了它不能只是普通的 n 次单位根, 而必须仍然是**本原的**。

假设

$$\text{ord}(\sigma(\zeta_n)) = d < n.$$

那么

$$\sigma(\zeta_n)^d = 1.$$

于是

$$\sigma(\zeta_n^d) = \sigma(1).$$

因为 σ 是自同构，所以特别是单射，因此

$$\zeta_n^d = 1.$$

但 ζ_n 本身的阶是 n ，不可能存在 $d < n$ 使

$$\zeta_n^d = 1.$$

矛盾。

所以：

$$\boxed{\text{ord}(\sigma(\zeta_n)) = n.}$$

也就是说，

$$\sigma(\zeta_n)$$

一定是一个本原 n 次单位根。

而我们前面已经证明所有本原 n 次单位根恰好是：

$$\zeta_n^a, \quad \gcd(a, n) = 1.$$

所以自然得到：

$$\boxed{\sigma(\zeta_n) = \zeta_n^a \quad \text{for some } a \text{ with } \gcd(a, n) = 1.}$$

所以这里的逻辑是：

$$\sigma \text{ 保持方程} \Rightarrow \sigma(\zeta_n) \text{ 仍是 } n \text{ 次单位根}$$

再加上

σ 是单射 $\Rightarrow$ 阶不会下降

因此

$\sigma(\zeta_n)$ 仍然是本原 n 次单位根,

最后才写成

$$\zeta_n^a, \quad (a, n) = 1.$$

而我们现在正在证明的是反方向：每一个这样的 ζ_n^a ，是否真的都能作为某个自同构下 ζ_n 的像。

11.3 模 n 剩余类环中的可逆元乘法群

原问题：这个是模 n 同余的乘法群是吧

对，准确地说是：

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

表示 模 n 的剩余类环 $\mathbb{Z}/n\mathbb{Z}$ 里所有可逆元组成的乘法群。

也可以通俗地说成：

模 n 意义下“能做乘法逆元”的那些数构成的群

1. 先说 $\mathbb{Z}/n\mathbb{Z}$ 是什么

它是所有模 n 的同余类：

$$[0], [1], [2], \dots, [n-1].$$

其中

$$[a] = [b] \iff a \equiv b \pmod{n}.$$

这里面可以做加法和乘法：

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

所以它是一个环。

2. 为什么上面有个 $\times$?

这个 $\times$ 表示“取可逆元”。

也就是说，只保留那些存在乘法逆元的元素。

一个类

$$[a] \in \mathbb{Z}/n\mathbb{Z}$$

可逆，当且仅当存在

$$[b]$$

使得

$$[a][b] = [1].$$

也就是：

$$ab \equiv 1 \pmod{n}.$$

而这又等价于：

$$\gcd(a, n) = 1.$$

所以：

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$$

3. 例子

例 1: $n = 5$

$$\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}.$$

因为 5 是素数，所以除了 $[0]$ 以外全都可逆。

因此：

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{[1], [2], [3], [4]\}.$$

这是一个 4 元乘法群。

例如：

$$[2][3] = [6] = [1].$$

所以 $[2]$ 的逆元是 $[3]$ 。

例 2: $n = 6$

$$\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}.$$

与 6 互素的只有：

$$1, 5.$$

所以：

$$(\mathbb{Z}/6\mathbb{Z})^\times = \{[1], [5]\}.$$

这里：

$$[5][5] = [25] = [1].$$

所以 $[5]$ 是自己的逆元。

例 3: $n = 8$

与 8 互素的是：

$$1, 3, 5, 7.$$

所以：

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}.$$

4. 它为什么和分圆域的 Galois 群对应？

因为我们已经证明：

每个自同构都由

$$\zeta_n \mapsto \zeta_n^a$$

决定，而要保持“本原 n 次单位根”不变，就必须：

$$\gcd(a, n) = 1.$$

所以允许的指数恰好就是：

$$[a] \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

而且复合满足：

$$\sigma_a \circ \sigma_b = \sigma_{ab}.$$

这正对应于

$$[a] \cdot [b] = [ab]$$

的乘法。

所以：

$$\boxed{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.}$$

所以你那句“模 n 同余的乘法群”大体是对的，但更准确是：

因为不是所有模 n 的同余类都能进这个群，只有可逆的那些才行。

11.4 Bézout 等式证明可逆当且仅当互素

原问题：所以上面是怎么证明是乘法可逆元的

对，这一步就是证明：

$$[a] \in \mathbb{Z}/n\mathbb{Z} \text{ 可逆} \iff \gcd(a, n) = 1$$

这是一个很重要的基本结论。

先证明“如果互素，那么可逆”。

假设

$$\gcd(a, n) = 1.$$

根据 Bézout 等式，存在整数 x, y ，使得

$$ax + ny = 1.$$

两边对 n 取模：

$$ax + ny \equiv 1 \pmod{n}.$$

因为

$$ny \equiv 0 \pmod{n},$$

所以：

$$ax \equiv 1 \pmod{n}.$$

这就说明在 $\mathbb{Z}/n\mathbb{Z}$ 里：

$$[a][x] = [1].$$

因此 $[x]$ 就是 $[a]$ 的乘法逆元。

所以：

$$\boxed{\gcd(a, n) = 1 \implies [a] \text{ 可逆.}}$$

例如模 7：

$$\gcd(3, 7) = 1.$$

Bézout 可以写成：

$$3 \cdot 5 + 7 \cdot (-2) = 1.$$

所以：

$$3 \cdot 5 \equiv 1 \pmod{7}.$$

于是：

$$[3]^{-1} = [5].$$

再证明反方向。

假设 $[a]$ 在 $\mathbb{Z}/n\mathbb{Z}$ 中可逆。

那么存在某个整数 b ，使得：

$$ab \equiv 1 \pmod{n}.$$

这意味着：

$$n \mid (ab - 1).$$

所以存在整数 k ，使：

$$ab - 1 = kn.$$

也就是：

$$ab - kn = 1.$$

现在设

$$d = \gcd(a, n).$$

因为 $d \mid a$ ，所以：

$$d \mid ab.$$

又因为 $d \mid n$ ，所以：

$$d \mid kn.$$

因此 d 也整除它们的差：

$$d \mid (ab - kn).$$

但：

$$ab - kn = 1.$$

所以：

$$d \mid 1.$$

正的最大公因数只能是：

$$d = 1.$$

所以：

$$[a] \text{ 可逆} \implies \gcd(a, n) = 1.$$

两边合起来：

$$[a] \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \gcd(a, n) = 1.$$

你也可以把它记成一句非常有用的话：

$$\text{模 } n \text{ 下，能“约掉”的数，恰好就是和 } n \text{ 互素的数。}$$

这也是为什么前面 $\zeta_n \mapsto \zeta_n^a$ 中要求 $\gcd(a, n) = 1$ ：这些指数恰好就是模 n 下的乘法可逆元。

11.5 构造每个自同构：良定义、保持运算与逆映射

下一步就是证明：每一个与 n 互素的 a ，真的都能产生一个 $\mathbb{Q}$ -自同构。

前面我们只证明了：

$$\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

如果存在，那么一定满足

$$\sigma(\zeta_n) = \zeta_n^a, \quad \gcd(a, n) = 1.$$

现在要证明反方向：

$$\boxed{\gcd(a, n) = 1 \implies \text{确实存在一个 } \sigma_a \text{ 使 } \sigma_a(\zeta_n) = \zeta_n^a}$$

因为

$$K = \mathbb{Q}(\zeta_n),$$

我们很自然地想定义：

$$\boxed{\sigma_a(f(\zeta_n)) = f(\zeta_n^a)}$$

其中

$$f(x) \in \mathbb{Q}[x].$$

例如：

$$3 + 2\zeta_n - \zeta_n^2$$

就送到

$$3 + 2\zeta_n^a - \zeta_n^{2a}.$$

看起来非常自然。

但这里马上有一个需要证明的问题：

同一个域元素可能有不同的多项式表达式，这个定义会不会产生矛盾？

比如如果

$$f(\zeta_n) = g(\zeta_n),$$

我们必须保证：

$$f(\zeta_n^a) = g(\zeta_n^a).$$

否则这个映射就没有良定义。

这正是刚才证明“所有本原 n 次单位根都有同一个最小多项式”发挥作用的地方。

因为：

$$f(\zeta_n) = g(\zeta_n)$$

意味着

$$(f - g)(\zeta_n) = 0.$$

而 ζ_n 在 $\mathbb{Q}$ 上的最小多项式是：

$$\Phi_n(x).$$

所以：

$$\boxed{\Phi_n(x) \mid f(x) - g(x)}$$

于是可以写：

$$f(x) - g(x) = \Phi_n(x)h(x).$$

现在因为

$$\gcd(a, n) = 1,$$

所以

$$\zeta_n^a$$

也是本原 n 次单位根，因此：

$$\Phi_n(\zeta_n^a) = 0.$$

把 $x = \zeta_n^a$ 代进去：

$$f(\zeta_n^a) - g(\zeta_n^a) = \Phi_n(\zeta_n^a)h(\zeta_n^a) = 0.$$

所以：

$$f(\zeta_n^a) = g(\zeta_n^a).$$

因此这个定义没有歧义：

$$\boxed{\sigma_a(f(\zeta_n)) = f(\zeta_n^a)}$$

是良定义的。

这一步其实非常重要：因为 ζ_n 和 ζ_n^a 满足同一个最小多项式，所以可以把一个替换成另一个，而不会破坏原有的代数关系。

接下来，加法和乘法也自动保持。

例如：

$$\sigma_a(f(\zeta_n) + g(\zeta_n)) = (f + g)(\zeta_n^a)$$

等于：

$$f(\zeta_n^a) + g(\zeta_n^a).$$

所以：

$$\sigma_a(x + y) = \sigma_a(x) + \sigma_a(y).$$

乘法同理：

$$\sigma_a(xy) = \sigma_a(x)\sigma_a(y).$$

而且对任何

$$q \in \mathbb{Q},$$

有：

$$\sigma_a(q) = q.$$

所以它是一个固定 $\mathbb{Q}$ 的域同态。

现在还剩一个问题：它真的是**自同构**吗？也就是它能不能反过来。

因为

$$\gcd(a, n) = 1,$$

所以 a 在模 n 下有乘法逆元。

存在 b 使：

$$ab \equiv 1 \pmod{n}.$$

也就是：

$$ab = 1 + kn$$

某个 $k \in \mathbb{Z}$ 。

于是：

$$(\zeta_n^a)^b = \zeta_n^{ab} = \zeta_n^{1+kn} = \zeta_n (\zeta_n^n)^k = \zeta_n.$$

所以 σ_b 可以把 ζ_n^a 再送回来：

$$\zeta_n^a \xrightarrow{\sigma_b} \zeta_n.$$

因此：

$$\sigma_b = \sigma_a^{-1}.$$

所以 σ_a 确实是一个自同构。

于是我们终于得到：

$$\boxed{\forall a, \gcd(a, n) = 1, \quad \sigma_a : \zeta_n \mapsto \zeta_n^a}$$

都给出了一个元素

$$\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

下一步只差最后一件事：看两个这种自同构复合以后发生什么。你会发现：

$$\sigma_a \circ \sigma_b = \sigma_{ab}$$

于是 Galois 群的群运算就和“模 n 的可逆整数相乘”完全一致，这才最终得到

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

11.6 这一步到底要证明什么：集合对应还要保持运算

原问题：没太看懂你这下一步到底在证明什么

你这里不是某个公式没看懂，而是我刚才没有先把“现在到底要证明什么”说清楚。

我们前面已经做到两件事。

第一件：

$$\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

时，一定有

$$\sigma(\zeta_n) = \zeta_n^a$$

而且

$$\gcd(a, n) = 1.$$

也就是说，每个 Galois 自同构都会对应一个模 n 的可逆数 a 。

第二件：

对每个满足

$$\gcd(a, n) = 1$$

的 a ，我们也确实可以构造一个自同构

$$\sigma_a$$

使

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

所以现在其实已经知道：

$$\text{Galois 自同构} \longleftrightarrow \text{模 } n \text{ 的可逆数}$$

接下来还差最后一点：这个对应不仅是一一对应，而且还保持“群运算”。

为什么要证明这个？

因为我们不是只想说：

两边元素个数一样。

我们想证明的是更强的：

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

这里的 $\cong$ 是“群同构”，所以必须证明两边的运算也对应。

左边的群运算是什么？

是自同构的复合：

$$\sigma_a \circ \sigma_b.$$

右边的群运算是什麼？

是模 n 的乘法：

$$[a][b] = [ab].$$

所以我们刚才真正要证明的是：

$$\boxed{\sigma_a \circ \sigma_b = \sigma_{ab}}$$

这句话就是在说：

左边“先做 σ_b ，再做 σ_a ”
对应右边“把 b 和 a 相乘”。

为什么成立？

因为从生成元 ζ_n 看：

$$\zeta_n \xrightarrow{\sigma_b} \zeta_n^b \xrightarrow{\sigma_a} (\zeta_n^a)^b = \zeta_n^{ab}.$$

所以复合以后：

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

而 σ_{ab} 本来就是定义成：

$$\sigma_{ab}(\zeta_n) = \zeta_n^{ab}.$$

所以：

$$\sigma_a \circ \sigma_b = \sigma_{ab}.$$

这一步的目的就是证明：

“自同构复合”对应“指数相乘”

因此这个对应不仅是集合上的一一对应，而真的是群结构完全一样。

你可以把前面整个分圆域部分压缩成三步：

1. $\sigma(\zeta_n)$ 必须是 ζ_n^a , $(a, n) = 1$;
2. 每个这样的 a 都真的给出一个 σ_a ;
3. $\sigma_a \circ \sigma_b = \sigma_{ab}$.

第三步就是我刚才在证明的东西。

11.7 复合对应指数相乘，逐项验证群同构

那就把最后这一步完整做完。

我们现在已经知道：对每个满足

$$\gcd(a, n) = 1$$

的整数 a ，都有一个自同构

$$\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

满足

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

现在要看这些自同构之间怎么复合。

取两个：

$$\sigma_a, \quad \sigma_b.$$

先作用 σ_b ：

$$\zeta_n \xrightarrow{\sigma_b} \zeta_n^b.$$

再作用 σ_a ：

$$\sigma_a(\zeta_n^b).$$

因为自同构保持乘法，

$$\sigma_a(\zeta_n^b) = \sigma_a(\zeta_n)^b.$$

而

$$\sigma_a(\zeta_n) = \zeta_n^a,$$

所以：

$$\sigma_a(\zeta_n^b) = (\zeta_n^a)^b = \zeta_n^{ab}.$$

因此：

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

而 σ_{ab} 的定义就是：

$$\sigma_{ab}(\zeta_n) = \zeta_n^{ab}.$$

因为一个自同构完全由 ζ_n 的像决定，所以：

$$\sigma_a \circ \sigma_b = \sigma_{ab}.$$

注意这里 ab 实际上只需要看模 n 。

因为：

$$a \equiv a' \pmod{n}$$

就有

$$\zeta_n^a = \zeta_n^{a'}.$$

所以：

$$\sigma_a = \sigma_{a'}$$

当且仅当

$$a \equiv a' \pmod{n}.$$

因此真正对应的不是整数 a ，而是模 n 的剩余类：

$$[a] \in \mathbb{Z}/n\mathbb{Z}.$$

而且必须满足：

$$\gcd(a, n) = 1,$$

也就是 $[a]$ 在模 n 下可逆。

这些元素组成群：

$$(\mathbb{Z}/n\mathbb{Z})^\times.$$

现在定义映射：

$$\Psi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

为：

$$\boxed{[a] \longmapsto \sigma_a.}$$

刚才已经证明：

$$\sigma_a \circ \sigma_b = \sigma_{ab},$$

所以：

$$\Psi([a][b]) = \Psi([ab]) = \sigma_{ab} = \sigma_a \circ \sigma_b.$$

因此 Ψ 是群同态。

接下来检查它是一一对应。

如果：

$$\sigma_a = \sigma_b,$$

那么特别地：

$$\sigma_a(\zeta_n) = \sigma_b(\zeta_n).$$

所以：

$$\zeta_n^a = \zeta_n^b.$$

前面已经证明：

$$\zeta_n^a = \zeta_n^b \iff a \equiv b \pmod{n}.$$

所以：

$$[a] = [b].$$

因此 Ψ 是单射。

另一方面，我们前面已经证明：任何

$$\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

都必须满足：

$$\sigma(\zeta_n) = \zeta_n^a$$

其中

$$\gcd(a, n) = 1.$$

所以这个 σ 就是：

$$\sigma_a.$$

因此 Ψ 又是满射。

最终：

$$\boxed{\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.}$$

这就是分圆域最核心的 Galois 群结论。

它立刻给出两个重要推论。

第一：

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n).$$

这和我们之前得到的

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

完全吻合。

第二：

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

是交换群，因为模 n 的乘法满足：

$$ab \equiv ba \pmod{n}.$$

所以：

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \text{ 是 Abel 群.}$$

这个结论以后在“根式可解”里特别重要，因为分圆扩张提供的是非常典型的 Abel 扩张。

11.8 边界检查： $n = 1, 2$ 也成立

$\zeta_1 = 1$ 、 $\zeta_2 = -1$ 都在 $\mathbb{Q}$ 中，所以两个分圆域都等于 $\mathbb{Q}$ ，Galois 群为平凡群，次数均为 $\varphi(n) = 1$ 。对于 $n = 1$ ，模 1 只有一个剩余类，单位群按通常约定也是平凡群。

复共轭对应 $[-1]$ 。当 $n \geq 3$ 时它不是恒等映射； $n = 1, 2$ 时它是恒等映射。因此后续学习最大实子域时，指数 2 的公式必须限定 $n \geq 3$ 。

第 12 章：复习重点与后续学习边界

本章对象：先用已有定义重建公式。中间域、最大实子域和根式可解的进一步推导是后续主题；本章保留原对话的学习建议。

12.1 公式太多时，先记五个核心观念

原问题：好吧，还有什么要学的吗，我感觉公式太多我都记不住了

有，但我建议你**现在先别继续堆公式**。你已经走过了分圆域这条线最关键的一大段，接下来更重要的是把“结构”压缩成少数几个核心观念。

你现在真正需要记住的，其实只有这些：

1. ζ_n 是本原 n 次单位根，意思就是

$$\text{ord}(\zeta_n) = n.$$

2. 第 n 个分圆多项式 $\Phi_n(x)$ 的根，就是所有本原 n 次单位根；因此

$$\deg \Phi_n = \varphi(n).$$

3. $\Phi_n(x)$ 是任意本原 n 次单位根在 $\mathbb{Q}$ 上的最小多项式，因此

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

4. $\mathbb{Q}(\zeta_n)$ 包含全部 n 次单位根，所以它是 $x^n - 1$ 的分裂域；在特征 0 下又自动可分，因此它是 Galois 扩张。

5. 它的 Galois 自同构就是

$$\zeta_n \mapsto \zeta_n^a, \quad \gcd(a, n) = 1,$$

所以

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

你不需要死记像

$$\text{ord}(\zeta_n^a) = \frac{n}{\gcd(a, n)}$$

这种公式。忘了完全没关系，因为只要记得“阶就是最小的 $d > 0$ 使 $(\zeta_n^a)^d = 1$ ”：

$$(\zeta_n^a)^d = 1 \iff n \mid ad,$$

公式两三步就能重新推出。

接下来如果继续，我更建议不再讲新的公式，而是做一个完整具体例子，比如从头到尾研究

$$\boxed{\mathbb{Q}(\zeta_5)/\mathbb{Q}}$$

把 Φ_5 、扩张次数、四个自同构、Galois 群 C_4 、中间域 $\mathbb{Q}(\sqrt{5})$ 全部放在同一个例子里。这样前面那些公式会从“需要背”变成“自然看出来”。

我觉得这会比继续抽象推进更适合你现在的阶段。

12.2 后续学习路线：具体例子、中间域、实子域与根式

原问题：好的那我理解了，下一步还有什么知识吗

整理提示：本段是原对话的后续学习路线。群结构例子使用已证结论；Galois 对应、二次中间域、最大实子域及“可解群推出根式可解”的完整推导仍属下一阶段。

有，而且现在正好可以从“分圆域的基本结构”继续往 Galois 理论更深一层走。你目前已经把最核心的基础链条基本打通了：

$$x^n - 1 \rightarrow \text{单位根} \rightarrow \Phi_n(x) \rightarrow \mathbb{Q}(\zeta_n) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

接下来我建议按这个顺序继续。

第一步先讲 **为什么分圆域是 Galois 扩张**。这里会把你之前学过的两个关键词真正落地：

正规性 **normality**

可分性 **separability**

我们会看到

$$\mathbb{Q}(\zeta_n)$$

其实就是

$$x^n - 1$$

在 $\mathbb{Q}$ 上的分裂域，因此正规；而特征为 0，所以自动可分。因此：

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是 Galois 扩张。

这一步也正好能回答你之前曾经困惑的那个问题：“正规性和分裂域到底是什么关系？”

然后第二步做几个具体例子。比如 $n = 5$ ：

$$\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times.$$

右边是

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

在乘法下组成的群，而且

$$[2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [3], \quad [2]^4 = [1],$$

所以：

$$(\mathbb{Z}/5\mathbb{Z})^\times \cong C_4.$$

于是分圆域的 Galois 群就是一个四阶循环群。

再比如 $n = 8$ ：

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{[1], [3], [5], [7]\}.$$

但是：

$$3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

所以它不是 C_4 ，而是：

$$\boxed{C_2 \times C_2}.$$

这样你会开始真正体会：

不同 n

产生不同的 Galois 群结构。

第三步就是非常重要的 Galois 对应。既然

$$G = \text{Gal}(K/\mathbb{Q})$$

已经知道，那么：

$$G \text{ 的子群 } \longleftrightarrow K/\mathbb{Q} \text{ 的中间域}$$

例如 $\mathbb{Q}(\zeta_5)$ 的 Galois 群是 C_4 ，它有唯一一个二阶子群，因此分圆域中存在唯一一个二次中间域。最终可以算出：

$$\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$$

这会是一个非常漂亮的具体 Galois 对应例子。

第四步再讲**复共轭**。在分圆域中：

$$\overline{\zeta_n} = \zeta_n^{-1}.$$

所以复共轭这个 Galois 自同构对应：

$$[-1] \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

它的固定域就是所谓的**最大实子域**：

$$\mathbb{Q}(\zeta_n + \zeta_n^{-1})$$

而且当 $n \geq 3$ 时：

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2.$$

这个例子会让“固定域”这个概念变得非常具体。

再往后，就可以接回你之前学的“根式可解”：

$$(\mathbb{Z}/n\mathbb{Z})^\times$$

是 Abel 群，所以当然是可解群。因此分圆扩张的 Galois 群是可解的。这里最终会连接到：

单位根可以用根式表达

以及为什么在一般根式解理论中，经常需要“加入单位根”。

所以我建议下一步先讲：为什么 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 是 Galois 扩张，以及为什么它是 $x^n - 1$ 的分裂域。

这个顺序最适合你现在的进度，因为它会把你之前关于“正规、分裂域、自同构”的几个疑问重新串起来。

证明依赖与复习检查

把整条链连起来：多项式除法与最小多项式（第 1 章）提供代数关系；单位根的阶与互素指数（第 2—3 章）提供分类；分圆多项式与欧拉函数（第 4—5 章）提供根的计数；首一除法（第 6 章）保证整数系数；特征与 Frobenius（第 7 章）、导数与重因子（第 8 章）、Gauss 引理（第 9 章）一起证明不可约性；分裂域与可分性（第 10 章）保证 Galois 扩张；逐个构造自同构并检查复合（第 11 章）给出群结构。

复习时先问：当前基础域是什么？这个符号是数、域、多项式还是映射？“阶”是最小的哪一个正整数？为什么“首一”不等于“除尽”？模 p 后哪一步保持了次数，哪一步使用了不可约因子的素性？自同构的候选像为什么真的能定义一个映射？得到一一对应后，群运算是否也已经验证？

本版校正与整理边界

原分享页面与原对话段落保留在资料目录。本版改正 $x^2 + 1$ 在实数域上不可约的答句笔误；明确 $\mathbb{Q}(\zeta_6^2) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_6)$ ，取幂使阶降低未必使域变小；为 $n = 1$ 补齐导数判据的表述；把分圆多项式乘积的指数写成有限代表范围；把最大实子域的指数 2 预告限定

为 $n \geq 3$ 。

补充证明集中在原主线需要却未展开的地方，包括多项式商环、基的线性无关、Bézout 约分、特征为素数、不可分例子的不可约性、Gauss 引理、模 p 后的不可约因子论证及嵌入延拓与正规性。幂级数推导使用指数、正弦和余弦的标准展开；这些微积分基础在本篇作为已知。

原对话已完整走到分圆域的 Galois 群。第 12 章提及的中间域、实子域及根式理论是学习方向；本篇没有把那些尚未展开的证明写成已经完成的学习步骤。

原对话覆盖索引

所有 49 段可见数学回答均有正文落点。**A24** 拆成 Frobenius 恒等式与不可约性应用，**A41** 拆成域的特征与可分性；两个部分均保留。下表便于回到原材料核对。

原回答	本篇位置	内容
A01	第 1 章	多项式环、基础域、不可约性与加入一个根
A02	第 1 章	最小多项式、商环和扩张次数
A03	第 4 章	分圆多项式的编号为什么是 n ，次数为什么是欧拉函数
A04	第 2 章	全部 n 次单位根：互异性与穷尽性
A05	第 2 章	为什么复指数等于 1 恰好对应整圈旋转
A06	第 3 章	本原单位根、阶与互素指数
A07	第 4 章	按阶分类，证明分圆乘积恒等式
A08	第 3 章	普通单位根与本原单位根怎样区分
A09	第 3 章	本原单位根的数量不是一，恰好是欧拉函数

原回答	本篇位置	内容
A10	第 2 章	欧拉公式的幂级数推导与旋转意义
A11	第 5 章	欧拉函数：数互素整数，也数可逆剩余类
A12	第 5 章	用容斥原理证明欧拉函数的乘积公式
A13	第 5 章	欧拉函数的约数和：单位根计数证明
A14	第 5 章	欧拉函数的约数和：纯整数分类证明
A15	第 5 章	为什么最大公因数一定整除 n
A16	第 6 章	整数系数与不可约性：接下来需要证明的两件事
A17	第 6 章	分圆多项式属于整数多项式环的完整证明
A18	第 6 章	强归纳法究竟假设了哪些已知命题
A19	第 6 章	首一除数为什么不会制造分数
A20	第 6 章	长除法能进行，不等于一定除尽
A21	第 9 章	不可约性的目标：把分圆多项式认作最小多项式
A22	第 9 章	不可约、首一且以指定元素为根，才是它的最小多项式
A23	第 9 章	不可约性证明策略：先处理不整除 n 的素数指数
A24	第 7 章、第 9 章	Frobenius 恒等式与模素数的矛盾
A25	第 8 章	导数、公因式与模素数后没有重因子
A26	第 7 章	费马小定理：用非零剩余类的排列证明
A27	第 7 章	从互素情形补上被素数整除的情形

原回答	本篇位置	内容
A28	第 7 章	有限域上的多项式环怎样读、怎样运算
A29	第 4 章	分圆多项式的 Φ 记号怎样读
A30	第 9 章	任意本原 n 次单位根在有理数域上都有同一个最小多项式
A31	第 9 章	从素数指数到所有互素指数，完成不可约性证明
A32	第 11 章	自同构必须把生成元送到另一个本原单位根
A33	第 9 章	为何可以对每个素因子重复同一个步骤
A34	第 11 章	构造每个自同构：良定义、保持运算与逆映射
A35	第 11 章	追问：在哪里证明了自同构保持本原性
A36	第 11 章	复合对应指数相乘，逐项验证群同构
A37	第 11 章	这一步到底要证明什么：集合对应还要保持运算
A38	第 11 章	模 n 剩余类环中的可逆元乘法群
A39	第 11 章	Bézout 等式证明可逆当且仅当互素
A40	第 12 章	后续学习路线：具体例子、中间域、实子域与根式
A41	第 7 章、第 8 章	域的特征、可分性与特征零的作用
A42	第 8 章	可分的字面意义：根分开，嵌入才有足够多的选择
A43	第 8 章	不可分例子的最小多项式为什么仍是 p 次
A44	第 7 章	特征 p 的域不一定只有 p 个元素
A45	第 10 章	把正规与可分接回分圆域

原回答	本篇位置	内容
A46	第 10 章	分裂域为什么正规，分圆域为什么是 Galois 扩张
A47	第 10 章	单位根取幂后生成的域仍然正规
A48	第 3 章	忘记阶公式时，从整除条件重新推导
A49	第 12 章	公式太多时，先记五个核心观念