

# 代数 (algebra) 知识大纲

本文另参考视频《群论之美宣传片》的概念线索。视频从雪花、时钟和魔方的对称出发，经过 Galois 群、四元数、椭圆曲线和纠错码，最后把 Lie 群、标准模型、 $E_8$  与 Monster 群并置。下面把这些画面中的公式补成可计算的数学对象，并标出它们与正文主线的连接。

## 目录

|                                                      |    |
|------------------------------------------------------|----|
| 1. 背景、工程问题与总体逻辑 .....                                | 2  |
| 2. 集合、映射和运算 .....                                    | 7  |
| 3. 群论 (group theory): 对称性的代数 .....                   | 8  |
| 4. 环论 (ring theory): 加法和乘法同时存在 .....                 | 14 |
| 5. 模论: 线性代数的推广 .....                                 | 18 |
| 6. 域论和多项式 .....                                      | 20 |
| 7. Galois 理论: 方程根和对称性 .....                          | 22 |
| 8. 表示论: 用线性变换研究群和代数 .....                            | 24 |
| 9. 交换代数: 几何背后的环论 .....                               | 26 |
| 10. 同调代数: 用正合性测量结构 .....                             | 28 |
| 11. 与其他数学分支的关系 .....                                 | 29 |
| 12. 同态加密 (homomorphic encryption, HE): 加密后怎样计算 ..... | 31 |
| 13. 推荐学习顺序 .....                                     | 37 |
| 练习参考答案 .....                                         | 39 |
| 中英术语对照表 .....                                        | 43 |

# 1. 背景、工程问题与总体逻辑

## 1.1. 我们到底想解决什么问题

代数最初给人的印象是“把未知数 (unknown) 写成  $x$ ，再把它解出来”。例如已知长方形面积和一条边长，求另一条边；已知几笔交易的总量，求各类物品的单价。符号让具体数字背后的计算步骤可以重复使用。

但只会移项还不够。随着问题变复杂，我们会遇到几类更根本的疑问：

- **有没有解？**  $x^2 + 1 = 0$  在实数 (real number) 中无解，在复数 (complex number) 中有解。允许使用什么对象，是问题的一部分。
- **能不能用指定的方法求解？** 有二次方程 (quadratic equation) 求根公式 (quadratic formula)，并不意味着任意次数 (degree) 都有根式公式 (radical formula)。证明某种方法做不到，也是一种答案。
- **怎样组合和撤销操作？** 先旋转 (rotation) 再平移 (translation)，与先平移再旋转通常不同。需要保留操作次序，而不只是记录操作次数。
- **不同外观是否其实是同一个问题？** 换一组坐标 (coordinate) 后矩阵 (matrix) 变了，线性变换 (linear transformation) 的本质可能没变。需要区分表示方式与内在结构。
- **如何把大问题拆成可处理的小问题？** 多项式 (polynomial) 因式分解 (factorization)、线性空间 (linear space) 分解和魔方的局部循环 (cycle)，都在利用结构降低复杂度。

抽象代数 (abstract algebra) 逐渐把这些疑问统一为：**对象上允许什么运算？运算之间有什么关系？这些关系能推出哪些结论？** 群 (group)、环 (ring) 和域 (field) 的定义，是把解题中反复出现的规则提炼出来后的结果。

## 1.2. 为什么从解方程走向研究结构

一个重要转折来自多项式方程 (polynomial equation)。与其只盯着某个根 (root) 的表达式，不如研究：交换哪些根以后，根之间的代数关系仍然成立？这些允许的置换 (permutation) 可以复合 (composition)、可以撤销，于是形成群。Galois 理论 (Galois theory) 再把这个群的结构与根式可解性 (solvability by radicals) 联系起来。

另一条主线来自整数 (integer) 的整除 (divisibility) 与多项式的因式分解。整数可以带余除法 (division with remainder)，多项式也可以；两边都有最大公因子 (greatest common divisor, GCD)，也都能讨论不可约因子 (irreducible factor)。把共同规律抽出来，就得到环与理想 (ideal) 的语言。

因此，抽象不是为了让问题更难读，而是为了复用推理。例如一旦理解“同态 (homomorphism) 的核 (kernel) 记录被丢弃的信息”，就能同时理解取余、线性映射 (linear map) 压缩维数 (dimension)，以及只观察魔方角块而忽略棱块这三件事。

## 1.3. 工程上到底用在哪里

下面把实际问题、代数模型和所得能力放在一起。暂时不必掌握右栏的所有术语；后面的定义会逐一回应这些需求。

| 工程问题    | 代数模型                                                     | 能得到什么                   |
|---------|----------------------------------------------------------|-------------------------|
| 数据丢失与恢复 | 有限域 (finite field) 上的向量 (vector) 和线性方程 (linear equation) | 设计冗余，使部分分片丢失后仍能唯一恢复原数据。 |

| 工程问题       | 代数模型                                             | 能得到什么                                                                          |
|------------|--------------------------------------------------|--------------------------------------------------------------------------------|
| 机器人与图形变换   | 旋转、刚体变换 (rigid transformation) 组成的群              | 正确组合坐标变换 (coordinate transformation), 求逆变换 (inverse transformation), 判断顺序能否交换。 |
| 密码算法中的字节运算 | 有限域、多项式商环 (polynomial quotient ring)             | 在有限个精确状态上实现可逆变换与信息混合。                                                          |
| 并行汇总与增量计算  | 满足结合律 (associativity) 的运算、单位元 (identity element) | 决定数据能否分块计算、树形归并, 以及是否允许重新排序。                                                   |

### 1.3.1. 数据恢复：为什么多存一点就能补回丢失的数据

先看一个能手算的例子。把所有数都按模 5 计算，也就是只保留 0 到 4，超过 4 就取余。设两个数据符号为  $a, b$ ，另外存储：

$$p = a + b, \quad q = a + 2b \quad (\text{所有等式均按模 } 5) \quad (1)$$

若原数据是  $a = 2, b = 4$ ，则  $p = 1, q = 0$ 。现在假设  $a, b$  都丢失，但知道丢失的位置，并保留了  $p, q$ 。两式相减得  $b = q - p = -1 \equiv 4 \pmod{5}$ ，再得  $a = p - b = -3 \equiv 2 \pmod{5}$ ，原数据就被恢复。

这里存下的不是两个完整副本，而是两条互相独立的约束。进一步检查可知， $a, b, p, q$  中任意两个都足以恢复原来的两个符号：例如只剩  $a, q$  时，需要解  $2b = q - a$ ；模 5 中 2 的逆元 (inverse element) 是 3，所以仍能唯一求解。换成模 6 就未必成立，因为  $2b = 2$  同时允许  $b = 1$  和  $b = 4$ 。这就是工程中会专门使用域而不随便选择一个剩余类环 (residue class ring) 的原因。

这个小例子展示了擦除恢复 (erasure recovery) 的原理。实际分片可按符号逐项编码；Reed-Solomon 码 (Reed-Solomon code) 也利用有限域上的可逆线性关系，使接收端从足够多的未损坏符号恢复数据。这里假设知道哪些符号缺失；未知位置的错误还需要额外的检测与纠错设计。参见 [RFC 5510 的编码与解码原理](#)。

### 1.3.2. 坐标变换：为什么操作顺序必须成为模型的一部分

在平面上，设  $r$  为逆时针旋转 90 度， $t$  为向右平移 1。原点先旋转再平移，得到  $(1, 0)$ ；先平移再旋转，得到  $(0, 1)$ 。因此  $t \circ r \neq r \circ t$ 。这不是实现细节，而是操作本身的性质。

在机器人中，若  $T_{AB}$  把 B 坐标系 (coordinate system) 中的坐标换算到 A 坐标系，则：

$$T_{AC} = T_{AB}T_{BC}, \quad T_{BA} = T_{AB}^{-1} \quad (2)$$

三维刚体变换可以用齐次矩阵 (homogeneous matrix) 表示，组成  $SE(3)$  群。群的语言保证组合与求逆仍属于同类变换；实际标定中的噪声、优化与数值稳定性则还需其他数学工具。参见 [Modern Robotics：齐次变换矩阵 \(homogeneous transformation matrix\)](#)。

### 1.3.3. 密码与程序：代数规则直接进入实现

AES 的部分运算把一个字节看成  $\mathbb{F}_{2^8}$  的元素：加法对应逐位 XOR，乘法则是二进制系数 (coefficient) 多项式相乘，再模掉指定的不可约多项式 (irreducible polynomial)。这与普

通整数“乘完后模 256”是不同的规则。环、域和商结构 (quotient structure) 在这里直接决定程序应该怎样计算, 不能只把它们当成术语。参见 [FIPS 197 的 Mathematical Preliminaries](#)。这些结构解释了算法的运算部件, 但密码安全性还依赖整体设计与分析。

再看并程序: 如果汇总运算  $*$  有结合律, 就可以把  $(a * b) * c$  改成  $a * (b * c)$ , 将数据分块后按树形合并; 只有进一步满足交换律 (commutativity), 才可任意调整输入次序。字符串拼接能重新加括号, 却不能随意交换片段。数学实数加法满足结合律, 机器浮点加法因舍入通常不严格满足, 所以并行求和可能产生不同的末位结果。

工程中学习代数的收益, 往往是知道**什么变换合法、什么结果可恢复、什么优化保持语义、什么任务根本不可达**。并不是每个项目都会用到 Galois 理论或同调代数 (homological algebra); 先理解与手头问题相连的结构, 再向后扩展更有效。

### 练习 1 • 工程

答案 →

仍使用模 5 编码  $p = a + b, q = a + 2b$ 。若只收到  $a = 3, q = 1$ , 求  $b$  和  $p$ 。为什么这一步可以“除以 2”?

## 1.4. 带着问题看学习路线

可以把这条路线理解为: **从具体问题出发, 每遇到一种反复出现的困难, 就定义一个概念, 把解决它的方法保存下来**。下面依次说明这些概念为什么值得引入。

这是一张概念地图, 顺序不完全等同于定义的依赖顺序。正式学习时, 通常先讲群、环, 再具体定义它们的同态和商结构; 域一般也会在模 (module) 之前介绍。本文把模放在域扩张 (field extension) 之前, 是为了先串起群、环、模共有的结构语言; 阅读模论 (module theory) 时, 可以先用熟悉的有理数 (rational number)、实数、复数作为域的例子。

### 1.4.1. 集合 (set) 和映射 (map): 研究什么, 对象怎样变化

研究整数, 要先明确哪些数在讨论范围内; 研究魔方, 要先明确哪些状态算作可能的状态。这是集合的作用: 确定问题中的对象。

接着需要描述变化: 一个整数怎样变成它的余数, 一次转动怎样改变魔方状态。这就是映射。后面的各种操作、同态和表示 (representation), 首先都得是映射。

### 1.4.2. 运算和结构: 对象之间可以怎样组合

光列出整数还不够, 我们还要规定可以相加、相乘; 光列出魔方转法还不够, 还要规定两套转法怎样连续执行。

然后检查组合的规则: 能否交换次序? 能否撤销? 有没有“什么都不做”的操作? **集合加上运算及其规则, 就形成了结构**。同一个集合配上不同运算, 性质可能完全不同, 例如整数的加法与乘法。

### 1.4.3. 同态: 换一种表示, 怎样保留计算关系

假设只关心整数的奇偶性 (parity)。先把两个整数相加, 再判断奇偶, 与先记录它们的奇偶, 再按模 2 相加, 结果一致。

这种“转换前后, 运算仍然对得上”的映射就是同态。它让我们可以把复杂对象送到较简单的对象里研究, 并明确哪些信息保留下来了、哪些被丢掉了。并非每个同态都会丢失信息; 是否丢失, 要看它能否区分原来的元素。

#### 1.4.4. 商结构：有规则地忽略不关心的差别

只关心奇偶时，0、2、4 可以视为同一类，1、3、5 视为另一类。无穷多个整数被压缩为两个对象。

但合并必须与运算相容：从同一类中换一个代表，计算结果仍应落在同一类。商结构研究的就是这种**合并以后仍然能够计算**的办法。正规子群（normal subgroup）、理想等条件，正是为了保证这一点。同态与商结构密切相关：把具有相同像（image）的元素合并，常常就能得到与像同构（isomorphism）的结构。

#### 1.4.5. 群：统一研究可组合、可撤销的操作

魔方转动、空间旋转、元素置换，都可以连续执行，也都有逆操作。群提炼了这些共同规则。

有了群，我们就能统一讨论：某个目标能否到达？怎样撤销一串操作？哪些操作可以交换？重复多少次会回到原状？魔方里的“求逆”和“三循环（3-cycle）做三次归位”，都是这些问题的具体实例。

#### 1.4.6. 环：研究加法与乘法共同构成的计算系统

整数、多项式、矩阵都可以相加、相乘，而且乘法对加法满足分配律（distributivity）。环把这些共同规律组织起来，同时允许乘法逆元（multiplicative inverse）不存在，甚至允许乘法不交换。

这让整除、因式分解、余数和方程可以放在同一个框架里讨论。例如整数的带余除法与域上多项式的带余除法，就能使用相似的思路。进一步比较不同环，也能看出哪些结论依赖额外条件。

#### 1.4.7. 模：系数受到限制时，线性代数（linear algebra）还能保留多少

在线性代数里，我们熟悉用实数系数组合向量。但有些问题只允许整数系数，例如格点（lattice point）问题；有些问题让多项式充当系数，例如用多项式表达一个线性算子（linear operator）的反复作用。

模把“向量相加、标量（scalar）乘向量”推广到这些场景。由于系数未必能做除法，模可能没有基（basis），也可能出现非零元素被非零标量乘成零的现象。因此，需要比向量空间（vector space）更一般的理论来描述它们。

#### 1.4.8. 域：什么时候非零系数都能除掉

解  $ax = b$  时，我们希望只要  $a \neq 0$ ，就能唯一得到  $x = a^{-1}b$ 。域保证了这种能力，也为高斯消元（Gaussian elimination）等方法提供基础。

有理数、实数、复数都是域，有限域也一样。前面的数据恢复例子使用有限域，就是为了在有限个精确状态中，仍然拥有可靠的加减乘除。进一步研究域扩张，则是在问：为了容纳一个方程的根，需要把原来的数系扩大多少？

#### 1.4.9. Galois 理论：方程的根能怎样表达

已知二次方程有求根公式，自然会追问：更高次方程呢？哪些根可以通过有限次四则运算和开方得到？

Galois 理论把根加入更大的域，再研究哪些交换根的方式保持原有代数关系。这些变换形成群，于是可以通过群的结构判断方程是否根式可解（solvable by radicals）。它把前面“域”和“群”两条主线连接起来，也能解释为什么某些求根方法行不通。

#### 1.4.10. 后续方向：面对复杂问题，还需要什么工具

- **表示论 (representation theory)**：抽象群难以直接计算，能否让群元素作用为矩阵？这样就能用不变子空间 (invariant subspace)、特征值 (eigenvalue) 和迹 (trace) 等线性代数工具研究它。
- **交换代数 (commutative algebra)**：面对多元多项式方程组 (system of multivariate polynomial equations)，怎样组织方程之间的关系，并研究整个解集 (solution set)？理想、商环 (quotient ring) 和局部化 (localization) 提供了这套语言。
- **同调代数**：复杂对象拆解、转换后，信息究竟在哪里未能完整传递？它通过核、像与同调 (homology) 记录正合性 (exactness) 失败的部分，并研究这些差异之间的关系。

贯穿群、环、模和表示论的一条主线是：**结构 → 同态 → 核 → 商 → 同构定理 (isomorphism theorem)**。域之间的保单位元同态一定单射 (injection)，域论 (field theory) 中因此更常研究嵌入 (embedding) 与扩张，而不是非平凡的商域 (quotient of a field)。

读每个定义时，都可以先问一句：“如果没有这个概念，我眼前哪类问题就很难说清楚？”带着这个问题学习，定义就会逐渐变成解题工具。

#### 1.5. 用一个例子贯穿主线

考虑“只记录整数除以 3 的余数”的映射：

$$\pi: \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}, \quad n \mapsto \bar{n} \quad (3)$$

它保持加法，也保持乘法。所有 3 的倍数都映到零，所以核为  $3\mathbb{Z}$ 。整数虽然有无穷多个，但如果把相差 3 的倍数的整数看成同一个对象，就只剩三个剩余类 (residue class)。

这里的商不是普通除法，而是“按某种等价关系 (equivalence relation) 合并对象”。同构定理则说明：把映射无法区分的部分合并以后，得到的结构恰好就是像。

#### 1.6. 怎样读一个代数定义

从这里开始约定：本文的环均带单位元，环同态 (ring homomorphism) 保持单位元，模满足单位元作用公理 (axiom)。整环 (integral domain) 和域均要求  $1 \neq 0$ ；谈素理想 (prime ideal)、极大理想 (maximal ideal) 和交换代数时，默认环交换。

每遇到一个新结构，可以按以下顺序检查：

1. 元素是什么，运算是什麼，运算后是否仍在集合里？
2. 单位元、逆元是否存在，哪些公理可能失败？
3. 允许哪些保持结构的映射？
4. 能否给出一个满足定义的例子，以及一个只差一条公理的反例？

例如非零整数在乘法下有单位元且满足结合律，但 2 没有整数乘法逆元，因此不是群。反例能帮助分辨“看起来像”与“确实满足定义”。

##### 练习 1

答案 →

对映射  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$ ，求  $\pi(8)$ 、 $\text{Ker}(\pi)$  和  $\text{Im}(\pi)$ ，并判断  $\pi$  是否单射、是否满射 (surjection)。

## 2. 集合、映射和运算

### 2.1. 集合和映射

代数对象首先是集合。映射是比较两个集合的基本方式：

$$f : A \rightarrow B \quad (4)$$

常见性质：

- 单射：  $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ 。
- 满射：  $\forall b \in B, \exists a \in A, f(a) = b$ 。
- 双射 (bijection)：既是单射又是满射。

复合映射 (composite map)：

$$(g \circ f)(a) = g(f(a)) \quad (5)$$

恒等映射 (identity map)：

$$\text{id}_{A(a)} = a \quad (6)$$

双射有逆映射 (inverse map)，但只有保持运算的双射才是代数结构 (algebraic structure) 之间的同构。两个集合元素一样多，并不意味着它们作为群或环也相同。

### 2.2. 等价关系与商集 (quotient set)

等价关系  $\sim$  满足自反性 (reflexivity)、对称性 (symmetry) 和传递性 (transitivity)。元素  $a$  的等价类 (equivalence class) 以及商集分别是：

$$[a] = \{b \in A : b \sim a\}, \quad A / \sim = \{[a] : a \in A\} \quad (7)$$

等价类把集合分成互不相交的块。例如在整数上定义  $a \sim b$  当且仅当  $4 \mid (a - b)$ ，就得到模 4 的四个剩余类。

在商集上定义运算时，必须检查**良定义 (well-definedness)**：换一个代表元 (representative)，结果仍在同一个等价类里。对于模 4 加法，若  $a - a'$  和  $b - b'$  都是 4 的倍数，则  $(a + b) - (a' + b')$  也是 4 的倍数，因而  $[a] + [b] = [a + b]$  与代表元的选择无关。

### 2.3. 二元运算 (binary operation)

集合  $S$  上的二元运算是一个映射：

$$* : S \times S \rightarrow S \quad (8)$$

常见运算律：

$$(a * b) * c = a * (b * c) \quad \text{结合律} \quad (9)$$

$$a * b = b * a \quad \text{交换律} \quad (10)$$

单位元：

$$e * a = a * e = a \quad (11)$$

逆元：

$$a * a^{-1} = a^{-1} * a = e \quad (12)$$

只有结合律时称为半群 (semigroup)；再加单位元得到幺半群 (monoid)；每个元素都有逆元时得到群。非负整数在加法下是幺半群，整数在加法下是群。

注意运算会改变结论： $\mathbb{Z}$  在加法下是群，在乘法下却不是群。结合律允许省去括号，交换律才允许任意交换次序；矩阵乘法通常只有前者。

## 2.4. 逻辑关系

- 集合提供对象的载体。
- 运算赋予集合结构。
- 映射比较对象，同态比较带结构的对象。
- 结合律、单位元、逆元、交换律的不同组合，会产生半群、幺半群、群、环等结构。

### 练习 2

答案 →

在模 4 的商集上计算  $[3] + [2]$ 。再用代表元 7 和 6 计算一次，并说明为什么两个结果相同。

## 3. 群论 (group theory)：对称性的代数

### 3.1. 群的定义

群是一个集合  $G$  配备二元运算，使得：

$$(ab)c = a(bc) \quad (13)$$

$$\exists e \in G, \quad ea = ae = a \quad (14)$$

$$\forall a \in G, \exists a^{-1} \in G, \quad aa^{-1} = a^{-1}a = e \quad (15)$$

如果还满足：

$$ab = ba \quad (16)$$

则称为 Abel 群 (abelian group)。

典型例子包括加法群 (additive group)  $(\mathbb{Z}, +)$ 、模  $n$  加法群  $\mathbb{Z}/n\mathbb{Z}$ 、非零有理数的乘法群 (multiplicative group)  $\mathbb{Q}^*$ ，以及  $n$  个元素的置换群 (permutation group)  $S_n$ 。在加法记号下，单位元写作 0，逆元写作  $-a$ 。

群的公理能推出消去律 (cancellation law)：若  $ab = ac$ ，在两侧左乘  $a^{-1}$  就得到  $b = c$ 。同样可以证明单位元和每个元素的逆元唯一，且  $(ab)^{-1} = b^{-1}a^{-1}$ ；后一个式子中的次序不能随意交换。

### 3.2. 子群 (subgroup) 和生成元 (generator)

子群  $H \leq G$  是在同一运算下仍为群的子集 (subset)。

子群判别法 (subgroup criterion)：

$$H \leq G \Leftrightarrow H \neq \emptyset \text{ 且 } \forall a, b \in H, ab^{-1} \in H \quad (17)$$

由集合  $S \subset G$  生成的子群记作：

$$\langle S \rangle \quad (18)$$

循环群 (cyclic group)：

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \quad (19)$$

元素阶 (order of an element):

$$\text{ord}(g) = \min\{n \geq 1 : g^n = e\} \quad (20)$$

如果这样的正整数不存在, 就称  $g$  的阶为无穷。在加法群中,  $g^n$  对应  $ng$ 。例如  $\mathbb{Z}/8\mathbb{Z}$  中  $\bar{2}$  的阶为 4, 因为它依次生成  $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ 。

### 3.3. 陪集 (coset) 和 Lagrange 定理 (Lagrange's theorem)

左陪集 (left coset):

$$gH = \{gh : h \in H\} \quad (21)$$

右陪集 (right coset):

$$Hg = \{hg : h \in H\} \quad (22)$$

有限群 (finite group) 的 Lagrange 定理:

$$|G| = [G : H] |H| \quad (23)$$

推论:

$$\text{ord}(g) \mid |G| \quad (24)$$

原因是左陪集两两相同或不相交, 且每个陪集都与  $H$  等势 (equinumerosity), 所以它们把有限群分成大小相同的块。但其逆命题 (converse) 一般不成立:  $d \mid |G|$  并不保证存在阶 (order) 为  $d$  的子群。

### 3.4. 正规子群和商群 (quotient group)

正规子群:

$$N \text{ normal in } G \Leftrightarrow gNg^{-1} = N \quad \forall g \in G \quad (25)$$

商群:

$$G/N = \{gN : g \in G\} \quad (26)$$

商群运算:

$$(gN)(hN) = (gh)N \quad (27)$$

这个运算良定义需要  $N$  normal in  $G$ 。

所有 Abel 群的子群都正规; 一般群则未必。例如  $S_3$  中由换位 (transposition)  $(12)$  生成的子群不是正规子群, 因为用  $(123)$  共轭 (conjugation) 会把  $(12)$  变成  $(23)$ 。

### 3.5. 群同态 (group homomorphism)

群同态:

$$\varphi : G \rightarrow H, \quad \varphi(ab) = \varphi(a)\varphi(b) \quad (28)$$

核:

$$\text{Ker}(\varphi) = \{g \in G : \varphi(g) = e_H\} \quad (29)$$

像:

$$\text{Im}(\varphi) = \{\varphi(g) : g \in G\} \quad (30)$$

同态基本定理 (fundamental homomorphism theorem):

$$G / \text{Ker}(\varphi) \cong \text{Im}(\varphi) \quad (31)$$

具体的同构是  $g \text{Ker}(\varphi) \mapsto \varphi(g)$ 。它的良定义依赖于: 两个元素属于同一个核的陪集, 当且仅当它们具有相同的像。特别地, 群同态单射当且仅当核只含单位元。

### 3.6. 群作用 (group action)

群作用是群对集合的对称操作:

$$G \times X \rightarrow X, \quad (g, x) \rightarrow gx \quad (32)$$

满足:

$$ex = x \quad (33)$$

$$(gh)x = g(hx) \quad (34)$$

轨道 (orbit):

$$Gx = \{gx : g \in G\} \quad (35)$$

稳定子 (stabilizer):

$$G_x = \{g \in G : gx = x\} \quad (36)$$

轨道-稳定子定理 (orbit-stabilizer theorem):

$$|Gx| = [G : G_x] \quad (37)$$

当  $G$  和  $X$  都有限时, Burnside 引理 (Burnside's lemma) 给出轨道数:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)| \quad (38)$$

例如用两种颜色给正三角形的顶点着色, 只把旋转视为同一种着色。恒等旋转固定全部  $2^3 = 8$  种着色, 两个非恒等旋转各固定 2 种单色着色, 因此共有  $(8 + 2 + 2)/3 = 4$  类。这里没有把翻转加入作用群, 选择怎样的对称操作是建模的一部分。

### 3.7. 实例: 用代数还原魔方

魔方的困难是: 一转动, 就同时改变很多块。只把某一块送回原位, 往往会破坏已经还原的部分。代数要帮助我们寻找的是**整体效果很局部的操作组合**, 并判断某个局面是否可能由合法转动产生。

以下讨论普通三阶魔方, 固定六个中心块所确定的空间方向, 只使用外层转动, 不追踪中心贴纸自身的旋转方向。

#### 3.7.1. 从手上的转动到群元素

记上、下、左、右、前、后六个面为 U D L R F B。单个字母表示**正对该面观察时**顺时针转 90 度;  $R'$  表示反向转 90 度,  $R_2$  表示转 180 度。执行过程中保持整个魔方的朝向不变。

**本节有两种记号, 顺序必须分清:** 等宽字体中的转法如 R U, 按从左到右执行, 即先右面后上面; 数学映射的复合沿用全文约定, 从右向左作用。因此, 若  $r, u$  分别是两次转动对应的映射, 转法 R U 对应的是  $u \circ r$ 。

给每张贴纸一个独立编号，转动就是对这些编号的置换。把效果相同的转法视为同一个元素，所有合法转法的效果组成群：

- 接着执行另一套转法，对应群运算。
- 什么都不做，对应单位元  $e$ 。
- 倒过来执行各步的逆操作，对应逆元，例如  $R U$  的逆是  $U' R'$ 。
- $r^4 = e$ ，因为同一个面转四次就回到原状；但一般  $ru \neq ur$ 。

六个基本面转动生成整个魔方群 (Rubik's Cube group)。若已知完整的打乱记录，倒序求逆就能还原；真正的解题任务是不知道打乱记录时，从当前状态找出一套能实现逆变换的基本转法。

### 3.7.2. 为什么只记录“哪个块在哪里”还不够

三阶魔方有 8 个角块、12 个棱块。一个角块即使回到正确位置，也可能扭转了 120 度；一个棱块也可能原地翻转。因此完整状态必须同时记录位置和朝向，不能只记录 20 个块的置换。可以给每个角块的扭转编号为 0, 1, 2，给每个棱块的翻转编号为 0, 1。参见 [Kociemba: 块的位置与朝向表示](#)。

采用一致的标准朝向约定，从还原态出发，合法转动保持以下三个条件：

1. 所有角块扭转编号之和模 3 为零。
2. 所有棱块翻转编号之和模 2 为零。
3. 角块置换与棱块置换的奇偶性相同。

第三条可以从一次面转动看出：90 度转动分别对四个角块、四个棱块做一个四循环 (4-cycle)，两边都是奇置换 (odd permutation)；连续组合后，两边的奇偶性始终一致。前两条需要跟踪朝向的改变，它们表达了扭转与翻转不能单独凭空出现。

所以“只扭一个角块”“只翻一条棱块”“只交换两条棱块、其余完全不动”都不能由合法面转动产生。对于普通三阶魔方的装配状态，这三个条件也是可还原性的完整判据。代数在这里先回答了有没有解，避免对不可能的局面盲目搜索。相关不变量 (invariant) 与构造见 [Jaap 的 Useful Mathematics](#)。

### 3.7.3. 一个可以拿实物复现的三棱块还原例子

用位置名称给块命名：UF 是本来应该位于上前方的棱块，UR 是上右方，UL 是上左方。记这三个位置为  $a, b, c$ 。从上方俯视，前面 F 在图的下方：

|         |         |         |
|---------|---------|---------|
| 角块      | UB: 上后  | 角块      |
| UL: $c$ | U 中心    | UR: $b$ |
| 角块      | UF: $a$ | 角块      |

前面 F

考虑下面这套转法，把整个序列命名为 P：

$$R U' R U R U R U' R' U' R^2$$

逐步跟踪贴纸，可以得到它的净效果：

$$p : a \mapsto b, \quad b \mapsto c, \quad c \mapsto a \quad (39)$$

也就是三循环  $p = (a\ b\ c)$ ，即  $UF \rightarrow UR \rightarrow UL \rightarrow UF$ 。**这三条棱块不翻转，其余 9 条棱块、8 个角块都保持位置和朝向不变。**中间几步会暂时打乱其他块，只有完整做完这一套后才得到上述效果。

现在给定一个具体待解局面：除了这三条棱块，其他块全部还原；三条棱块朝向正确，但放在下表的位置。块的名称按其“应该去哪里”确定，不按它当前所在的位置确定。

| 目标位置   | 当前放着的块   | 执行 P 后放着的块  |
|--------|----------|-------------|
| UF (a) | UR 块 (b) | UF 块 (a)，归位 |
| UR (b) | UL 块 (c) | UR 块 (b)，归位 |
| UL (c) | UF 块 (a) | UL 块 (c)，归位 |

这个状态把原来的块  $a$  送到了  $c$ 、 $c$  送到了  $b$ 、 $b$  送到了  $a$ ，所以它对应  $p^2 = (a\ c\ b)$ 。执行一次 P，总效果就是：

$$p \circ p^2 = p^3 = e \quad (40)$$

魔方因此完全还原。若想自己制造这个练习局面，从还原态连续执行两次 P，再按表观察；执行第三次便回到还原态。这里利用了**三循环的阶为 3**，不是依赖重新找回原来的打乱记录。

若当前局面恰好是相反方向的三循环  $p$ ，就执行  $p^{-1} = p^2$ 。可以把 P 做两次，也可以倒序取逆，得到较短的转法：

$$R^2\ U\ R\ U\ R'\ U'\ R'\ U'\ R'\ U\ R'$$

这个例子解决的是明确的三棱块局面；任意打乱的魔方还需要处理其他块的位置与朝向。它展示了一个完整的推理链：**识别当前置换 → 确定需要的逆置换 (inverse permutation) → 用已知转法实现它 → 验证其他部分未被破坏。**

#### 3.7.4. 这种局部转法如何构造：交换子 (commutator) 与共轭

上例先给出了转法再分析效果。若希望主动设计局部操作，两个常用工具是交换子和共轭。

对映射  $a, b$ ，采用交换子的约定：

$$[a, b] = aba^{-1}b^{-1} \quad (41)$$

如果  $a, b$  可以交换，上式等于  $e$ ；如果不能完全交换，撤销操作后就可能留下一个较小的净变化。比如在五个抽象位置上取  $a = (1\ 2\ 3)$ 、 $b = (3\ 4\ 5)$ ，按从右到左复合逐个跟踪，就得到：

$$[a, b] = (1\ 4\ 3) \quad (42)$$

原来两套操作合起来涉及五个位置，交换子只移动其中三个。这个五位置例子解释的是置换计算原理，并不是另一套可直接照转的魔方公式。实际魔方还必须验证块的朝向，以及预定的  $a, b$  能否用合法转动实现。

如果转法 A、B 对应映射  $a, b$ ，上述数学交换子应按  $B'\ A'\ B\ A$  执行，其中撇号表示整套转法的逆。魔方资料也常把从左到右执行的  $A\ B\ A'\ B'$  称为交换子；两种约定都可以用，但不能混用顺序。选择干扰范围大部分可以抵消的操作，是设计局部转法的关键；交换子并不自动保证“只动三块”。

共轭则解决**怎样复用一套已经验证的转法**。设  $s$  是一套准备操作，把需要处理的块送入工作位置； $p$  是工作位置上的局部算法。先准备、再处理、再撤销准备，数学上为：

$$s^{-1}ps \quad (43)$$

实际执行顺序是  $s p s'$ 。若  $p$  只移动位置集合  $W$ ，这个共轭只移动  $s^{-1}(W)$ ：对其他位置  $x$ ， $s(x)$  不在工作区域内，故  $s^{-1}ps(x) = x$ 。这就是“搬到工作区 → 做已知操作 → 搬回去”的严格解释。用于魔方时，工作区域必须把朝向也纳入描述。

### 3.7.5. 怎样从这个小例子走向整个求解器

人工解法会积累若干局部算法，再按局面选择并组合。计算机解法还会利用子群缩小搜索：例如 Kociemba 两阶段算法先把魔方送入子群：

$$H = \langle u, d, r^2, l^2, f^2, b^2 \rangle \quad (44)$$

然后仅用这些生成元继续还原。第一阶段的目标不必是完整还原，而是满足角块和棱块朝向已整理、四条中层棱块位于中层等条件。第二阶段允许的转动保持这些条件，于是后续搜索只需解决剩余排列问题。参见 [Kociemba：两阶段算法](#)。

这里并不要求  $H$  是正规子群；利用子群和陪集组织搜索，不等于声称存在商群  $G/H$ 。求出一种还原方法，也不等于已经求出了最短方法；步数还取决于如何计算一次转动的代价。

因此，“用代数解魔方”包含三个层面：用不变量判断可达性，用置换、逆元、交换子与共轭设计操作，用子群安排搜索阶段。它既能解释公式为什么有效，也能指导构造新的解法。

#### 练习 3 · 魔方

答案 →

已知  $P$  的净效果为  $p = (a \ b \ c)$ ，并且其余块的位置与朝向均不变。如果当前局面是从还原态执行  $P$  后得到的，还需要执行几次  $P$  才能还原？一套准备操作  $s$  把目标区域移到工作区域后，怎样复用  $P$  并撤销准备？

### 3.8. 有限群的进一步结构

Cauchy 定理 (Cauchy's theorem) 指出：素数 (prime number)  $p$  若整除有限群的阶，就存在阶为  $p$  的元素。Sylow 定理 (Sylow theorems) 进一步控制最大的  $p$  幂阶子群：若  $|G| = p^a m$  且  $p$  不整除  $m$ ，则存在阶为  $p^a$  的子群，所有这样的子群互相共轭，其个数  $n_p$  满足：

$$n_p \mid m, \quad n_p \equiv 1 \pmod{p} \quad (45)$$

若  $n_p = 1$ ，这个唯一的 Sylow 子群 (Sylow subgroup) 就正规。这些限制常用来判断小阶群的结构。

### 3.9. 从魔方状态数看群的规模

三阶魔方的合法状态数为：

$$\frac{8! \cdot 3^7 \cdot 12! \cdot 2^{10}}{2} = 43252003274489856000 \quad (46)$$

分母 2 来自角块与棱块置换奇偶性必须相同；指数 7 和 10 则来自角块扭转和棱块翻转的总和约束。这个数是群的阶，而不是“需要尝试的所有贴纸图案”的数量。上文的三个不变量说明了哪些状态属于同一个魔方群的轨道。

视频中出现的“上帝之数 20”是另一类问题：在半转计数（half-turn metric）下，任意状态都能在不超过 20 次面转动内还原。它是关于 Cayley 图直径的算法结论，不是群的定义，也不意味着每个状态都恰好需要 20 步。

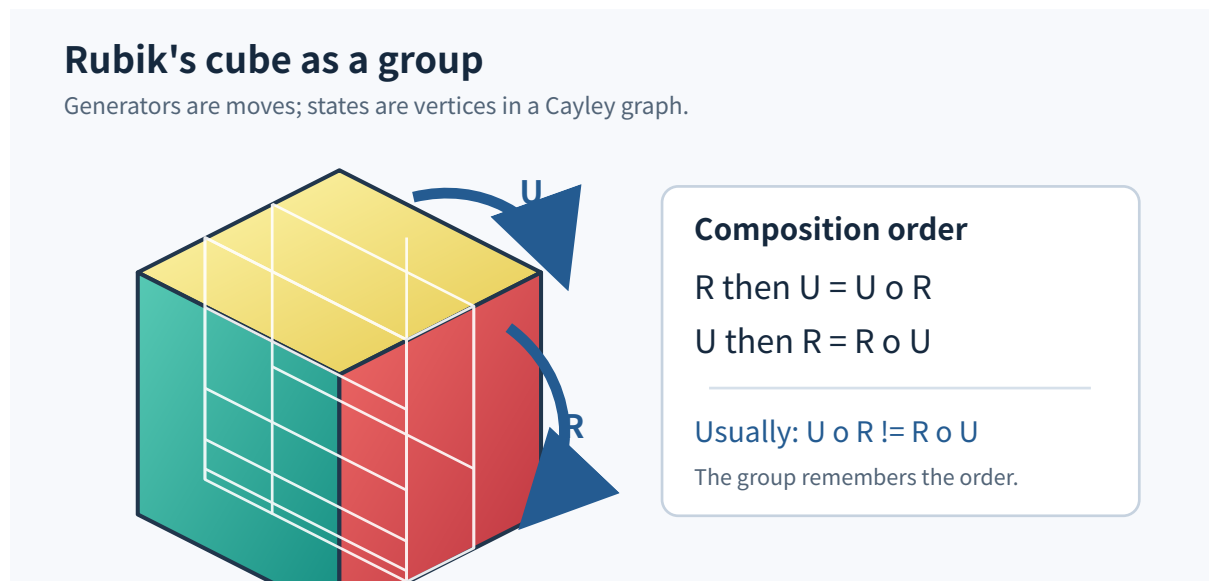


图 1 魔方群的生成元与运算顺序（示意图）。U、R 是生成元；同一组转动按不同顺序通常得到不同状态。

### 3.10. 逻辑关系

- 子群描述局部结构。
- 陪集把群按子群分块。
- 正规子群让商群成为合法结构。
- 同态把一个群映到另一个群，核记录“被压扁”的部分。
- 群作用把抽象群变成具体对称操作，是连接几何、组合和表示论的桥。

#### 练习 3

答案 →

在加法群  $G = \mathbb{Z}/8\mathbb{Z}$  中，令  $H = \langle 2 \rangle$ 。列出  $H$  和所有不同的陪集，求商群  $G/H$  的阶，并指出它同构于哪个循环群。

## 4. 环论（ring theory）：加法和乘法同时存在

### 4.1. 环的定义

环  $R$  是一个集合，带有加法和乘法，满足：

- $(R, +)$  是 Abel 群。
- 乘法结合： $(ab)c = a(bc)$ 。
- 分配律成立：

$$a(b + c) = ab + ac \quad (47)$$

$$(a + b)c = ac + bc \quad (48)$$

本文还要求乘法有单位元，记为  $1_R$ 。如果乘法交换，则称为交换环（commutative ring）。

## 4.2. 基本例子

- 整数环 (ring of integers)  $\mathbb{Z}$ 。
- 多项式环 (polynomial ring)  $F[x]$ 。
- 矩阵环 (matrix ring)  $M_{n(F)}$ 。
- 剩余类环  $\mathbb{Z}/n\mathbb{Z}$ 。
- 函数环 (ring of functions)。

这些例子说明：环不只是“数”，也可以是多项式、矩阵、函数和算子。

### 4.2.1. 四元数：非交换的除环与三维旋转

四元数环  $\mathbb{H}$  由基  $1, i, j, k$  生成，关系为：

$$i^2 = j^2 = k^2 = ijk = -1, \quad ij = k, \quad ji = -k \quad (49)$$

因此乘法一般不交换，例如  $ij \neq ji$ 。每个非零四元数都有逆元，所以  $\mathbb{H}$  是除环 (division ring)，却不是域。写成  $q = a + bi + cj + dk$  时，共轭与范数为：

$$\bar{q} = a - bi - cj - dk, \quad N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2 \quad (50)$$

三维向量可看成纯虚四元数。单位四元数  $q$  通过

$$v \mapsto qvq^{-1} \quad (51)$$

给出一个三维旋转； $q$  与  $-q$  表示同一个旋转。这解释了为什么旋转的组合适合用群描述，也说明四元数是矩阵表示之外的另一种表示工具。实际数值计算仍要处理归一化误差，四元数本身并不会替代坐标标定或数值优化。

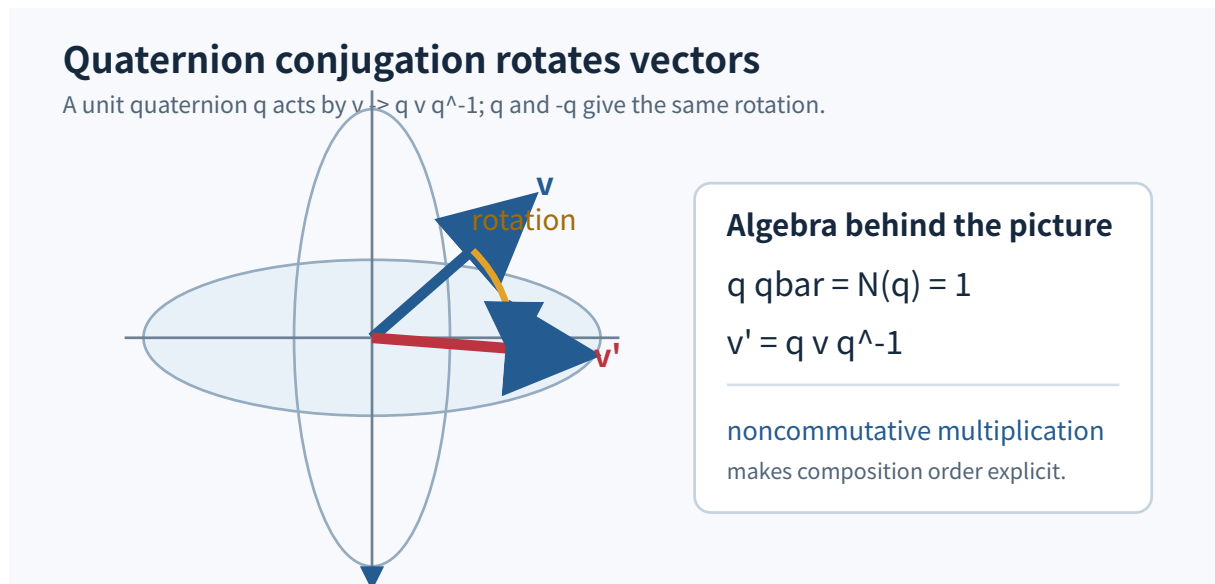


图2 单位四元数通过共轭把向量旋转到新方向（示意图）。球面投影帮助区分几何旋转与四元数乘法。

单位 (unit) 是具有乘法逆元的元素，所有单位组成乘法群  $R^\times$ 。零因子 (zero divisor) 是非零元素  $a$ ，它与某个非零元素  $b$  的乘积为零。例如在  $\mathbb{Z}/6\mathbb{Z}$  中， $2\bar{3} = \bar{0}$ ，因此不能像在域中那样随意约去非零因子。

在  $\mathbb{Z}/n\mathbb{Z}$  中， $\bar{a}$  是单位当且仅当  $\gcd(a, n) = 1$ 。这是 Bézout 等式 (Bézout's identity)  $ua + vn = 1$  的直接应用：模  $n$  后， $\bar{u}$  就是  $\bar{a}$  的逆元。

### 4.3. 理想和商环

理想是可以做商环的子结构。左理想 (left ideal) 首先非空, 并满足:

$$a, b \in I \Rightarrow a - b \in I \quad (52)$$

$$r \in R, a \in I \Rightarrow ra \in I \quad (53)$$

非交换环 (noncommutative ring) 中还要区分右理想 (right ideal) 与双边理想 (two-sided ideal); 构造商环需要双边理想。交换环中三者一致。子环 (subring) 只要求内部运算封闭, 理想还要求吸收来自整个环的乘法, 后者正是商环乘法良定义的关键。

交换环中, 理想  $I$  的商环:

$$R/I = \{a + I : a \in R\} \quad (54)$$

商环运算:

$$(a + I) + (b + I) = (a + b) + I \quad (55)$$

$$(a + I)(b + I) = ab + I \quad (56)$$

主理想 (principal ideal):

$$(a) = \{ra : r \in R\} \quad (57)$$

### 4.4. 环同态

环同态:

$$\varphi : R \rightarrow S \quad (58)$$

满足:

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad (59)$$

$$\varphi(ab) = \varphi(a)\varphi(b) \quad (60)$$

通常还要求:

$$\varphi(1_R) = 1_S \quad (61)$$

核:

$$\text{Ker}(\varphi) = \{r \in R : \varphi(r) = 0\} \quad (62)$$

环同态基本定理 (fundamental theorem of ring homomorphisms):

$$R / \text{Ker}(\varphi) \cong \text{Im}(\varphi) \quad (63)$$

### 4.5. 整环、域和素理想

整环: 满足  $1 \neq 0$  的交换环  $R$  中没有零因子:

$$ab = 0 \Rightarrow a = 0 \text{ 或 } b = 0 \quad (64)$$

域: 满足  $1 \neq 0$  的交换环中, 每个非零元素都有乘法逆元:

$$\forall a \neq 0, \exists a^{-1}, \quad aa^{-1} = 1 \quad (65)$$

真理想 (proper ideal)  $p \neq R$  是素理想, 当且仅当:

$$ab \in p \Rightarrow a \in p \text{ 或 } b \in p \quad (66)$$

理想  $m$  是极大理想:

$$m \neq R \text{ 且不存在理想 } I \text{ 满足 } m \subsetneq I \subsetneq R \quad (67)$$

重要判别:

$$R/p \text{ 是整环} \Leftrightarrow p \text{ 是素理想} \quad (68)$$

$$R/m \text{ 是域} \Leftrightarrow m \text{ 是极大理想} \quad (69)$$

因此极大理想一定是素理想, 反过来不一定成立。例如  $\mathbb{Z}$  的零理想 (zero ideal) 是素理想, 但不是极大理想;  $\mathbb{Z}$  自身是整环却不是域。对于素数  $p$ ,  $(p)$  是  $\mathbb{Z}$  的极大理想, 因为  $\mathbb{Z}/p\mathbb{Z}$  是域。

## 4.6. Euclidean 整环 (Euclidean domain)、PID 和 UFD

Euclidean 整环  $\rightarrow$  主理想整环 (principal ideal domain, PID)  $\rightarrow$  唯一分解整环 (unique factorization domain, UFD):

$$\text{Euclidean domain} \Rightarrow \text{PID} \Rightarrow \text{UFD} \quad (70)$$

整数和一元多项式环 (univariate polynomial ring) 的整除理论有相同结构:

$$a = up_1^{e_1} \dots p_k^{e_k} \quad (71)$$

其中  $u$  是单位,  $p_i$  是不可约元 (irreducible element)。

唯一性允许交换因子的顺序, 也允许把因子乘以单位。Euclidean 整环通过带余除法求最大公因子; PID 要求每个理想由单个元素生成; UFD 则只保证非零非单位元素的唯一分解。这三种要求不能混为一谈。

## 4.7. 多项式商环与中国剩余定理 (Chinese remainder theorem)

域  $F$  上的多项式环  $F[x]$  可以按次数做带余除法。模掉一个  $d$  次多项式  $f$  后, 每个剩余类都有唯一的次数小于  $d$  的代表元; 乘法就是相乘后除以  $f$  取余。

若  $f$  不可约, 则  $(f)$  极大,  $F[x]/(f)$  是域。例如  $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ , 因为在商环中  $\bar{x}^2 = -1$ ,  $\bar{x}$  扮演虚数单位 (imaginary unit) 的角色。

中国剩余定理说明: 若交换环中的理想  $I + J = R$ , 则自然映射 (natural map) 给出:

$$R/(I \cap J) \cong R/I \times R/J \quad (72)$$

这里  $I \cap J = IJ$ 。例如  $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ , 同构把  $\bar{a}$  送到它模 2 和模 3 的两个余数。右侧虽是两个域的直积 (direct product), 却不是域, 因为  $(1, 0)(0, 1) = (0, 0)$ 。

## 4.8. 逻辑关系

- 理想在环论中扮演正规子群的角色。
- 商环让“模掉某些关系”成为合法操作。
- 素理想和极大理想控制商环是否是整环或域。
- 整除、因式分解、多项式根都可以放到环论框架中统一处理。

在  $R = \mathbb{Z}/12\mathbb{Z}$  中列出所有单位。令  $I = (\overline{4})$ ，列出  $I$  的元素，并判断  $R/I$  是否是域。

## 5. 模论：线性代数的推广

### 5.1. 模的定义

设  $R$  是环。左  $R$ -模  $M$  是一个 Abel 群，并且有标量乘法 (scalar multiplication)：

$$R \times M \rightarrow M \quad (73)$$

满足：

$$r(x + y) = rx + ry \quad (74)$$

$$(r + s)x = rx + sx \quad (75)$$

$$(rs)x = r(sx) \quad (76)$$

$$1_R x = x \quad (77)$$

如果  $R$  是域，则  $R$ -模就是向量空间。

任何 Abel 群都有自然的  $\mathbb{Z}$ -模结构：正整数乘法是重复相加，负整数乘法再取加法逆元 (additive inverse)。因此  $\mathbb{Z}/6\mathbb{Z}$  也是一个模，即使它不是任何域上的向量空间。

另一个关键例子来自线性算子。给定  $F$ -向量空间  $V$  上的线性算子  $T$ ，规定  $p(x) \cdot v = p(T)v$ ，就把  $V$  变成  $F[x]$ -模。此时研究模结构，相当于研究线性算子的相似分类。

### 5.2. 子模 (submodule)、商模 (quotient module) 和同态

子模  $N \subset M$  在加法和标量乘法下封闭。

商模：

$$M/N = \{x + N : x \in M\} \quad (78)$$

模同态 (module homomorphism)：

$$f : M \rightarrow N, \quad f(rx + y) = rf(x) + f(y) \quad (79)$$

同态基本定理：

$$M/\text{Ker}(f) \cong \text{Im}(f) \quad (80)$$

### 5.3. 自由模 (free module) 和有限生成模 (finitely generated module)

有限秩 (finite rank) 自由模具有一组有限的基，等价于：

$$M \cong R^n \quad (81)$$

一般自由模也可以有无限的基，此时每个元素仍只能是有限多个基向量 (basis vector) 的线性组合 (linear combination)。

有限生成模：

$$M = Rx_1 + \dots + Rx_n \quad (82)$$

在域上，有限生成（finitely generated）向量空间都有基。但在一般环上，模不一定有基，这是模论比线性代数复杂的地方。

以整环  $R$  为标量环时，若存在非零  $r \in R$  使  $rm = 0$ ，则称  $m$  为扭元（torsion element）。例如  $\mathbb{Z}/6\mathbb{Z}$  中  $6\bar{1} = \bar{0}$ ，但  $\bar{1} \neq \bar{0}$ 。非零自由  $\mathbb{Z}$ -模没有非零扭元，所以这个有限生成模不可能自由。

## 5.4. PID 上的有限生成模结构定理（structure theorem for finitely generated modules）

若  $R$  是 PID，有限生成  $R$ -模  $M$  可以分解为：

$$M \cong R^r \oplus R/(d_1) \oplus \dots \oplus R/(d_k) \quad (83)$$

其中：

$$d_1 \mid d_2 \mid \dots \mid d_k \quad (84)$$

其中  $r \geq 0$ ，各  $d_i$  为非零非单位元素；自由部分与这些不变因子（invariant factor）在相伴（association）意义下唯一确定。对  $\mathbb{Z}$ -模而言，例如  $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ ，这是按互素（coprime）素数幂分解的形式。

这个定理统一了两个重要结论：

- 有限生成 Abel 群分类。
- 矩阵的有理标准形（rational canonical form）和 Jordan 标准形（Jordan canonical form）的代数基础。

对线性算子的  $F[x]$ -模应用结构定理，总能得到有理标准形；只有当相关多项式在  $F$  上分裂时，才能进一步写出  $F$  上的 Jordan 标准形。

## 5.5. 正合列（exact sequence）

正合列：

$$\dots \rightarrow M_{i-1} \rightarrow M_i \rightarrow M_{i+1} \rightarrow \dots \quad (85)$$

在  $M_i$  处正合表示：

$$\text{Im}(f_{i-1}) = \text{Ker}(f_i) \quad (86)$$

短正合列（short exact sequence）：

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0 \quad (87)$$

表示  $A$  嵌入  $B$ ，而  $C$  是对应的商。

例如  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$  中，两个整数模之间的映射为  $n \mapsto 2n$ ，后一个映射为取模 2。它正合，但中间项不是  $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ：后者有非零扭元，前者没有。

如果满射  $q: B \rightarrow C$  有模同态截面（section） $s: C \rightarrow B$ ，满足  $q \circ s = \text{id}_C$ ，则短正合列称为分裂（split），此时  $B \cong A \oplus C$ 。向量空间的短正合列都分裂，一般模则不然。

## 5.6. 张量积（tensor product）的基本想法

对交换环  $R$  上的模， $M \otimes_R N$  由符号  $m \otimes n$  生成，并满足加法分配和标量平衡关系：

$$(rm) \otimes n = m \otimes (rn) \quad (88)$$

它把双线性映射 (bilinear map) 转成线性映射：每个双线性映射  $M \times N \rightarrow P$  都唯一地经过一个线性映射  $M \otimes_R N \rightarrow P$ 。常用计算是：

$$(R/I) \otimes_R M \cong M/IM \quad (89)$$

例如  $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z}) = 0$ ，因为在  $\mathbb{Z}/3\mathbb{Z}$  上乘以 2 已经是满射。这也为后面理解张量积为何不保持单射作准备。

## 5.7. 逻辑关系

- 向量空间是域上的模。
- Abel 群是  $\mathbb{Z}$ -模。
- 模论把线性代数、Abel 群、表示论放进同一语言。
- 正合列是现代代数中追踪结构损失和结构保留的基本工具。

### 练习 5

答案 →

把  $M = \mathbb{Z}/6\mathbb{Z}$  看成  $\mathbb{Z}$ -模。给出一个生成元，证明它不是自由模，并求其中满足  $2m = 0$  的所有元素。

## 6. 域论和多项式

### 6.1. 域扩张

如果  $F \subset K$  且  $K$  是包含  $F$  的域，则称  $K/F$  是域扩张。

扩张次数 (degree of an extension)：

$$[K : F] = \dim_F K \quad (90)$$

塔公式 (tower law)：

$$[L : F] = [L : K][K : F] \quad (91)$$

这里以  $F \subset K \subset L$  且各扩张次数有限的情形为主。次数是向量空间维数，不是域中元素个数之比。例如  $\mathbb{Q}(\sqrt{2})$  的元素可唯一写成  $a + b\sqrt{2}$ ，其中  $a, b \in \mathbb{Q}$ ，所以扩张次数为 2。

### 6.2. 特征 (characteristic) 与素域 (prime field)

域的特征是满足  $n \cdot 1 = 0$  的最小正整数  $n$ ；若不存在则为 0。正特征一定是素数  $p$ ，否则  $n = ab$  会让两个非零元素  $(a \cdot 1)$  和  $(b \cdot 1)$  的乘积为零。

每个域都包含一个最小子域 (subfield)，称为素域：特征 0 时是  $\mathbb{Q}$  的一个同构副本，特征  $p$  时是  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  的一个同构副本。有限域作为  $\mathbb{F}_p$  上的有限维向量空间，元素个数自然是  $p^n$ 。

### 6.3. 代数元 (algebraic element) 和超越元 (transcendental element)

元素  $\alpha \in K$  在  $F$  上代数，如果存在非零多项式 (nonzero polynomial)  $f(x) \in F[x]$ ，使得：

$$f(\alpha) = 0 \quad (92)$$

否则称为超越元。

最小多项式 (minimal polynomial)：

$$m_{\alpha, F}(x) \quad (93)$$

满足：

$$m_{\alpha, F}(\alpha) = 0 \quad (94)$$

并且它是所有使  $\alpha$  为根的非零多项式中次数最低的首一多项式 (monic polynomial)。

若  $\alpha$  在  $F$  上代数，则：

$$[F(\alpha) : F] = \deg m_{\alpha, F}(x) \quad (95)$$

最小多项式一定不可约：如果分解为两个低次非零因子的乘积，把  $\alpha$  代入后至少有一个因子为零，就与次数最小矛盾。求值映射 (evaluation map) 的核由最小多项式生成，因此：

$$F(\alpha) = F[\alpha] \cong F[x]/(m_{\alpha, F}) \quad (96)$$

若最小多项式次数为  $d$ ，则  $1, \alpha, \dots, \alpha^{d-1}$  构成一组基，任何更高次幂都能用最小多项式降次。例如在  $\mathbb{Q}(\sqrt{2})$  中， $(1 + \sqrt{2})^{-1} = \sqrt{2} - 1$ 。

#### 6.4. 怎样判断多项式不可约

在域上，二次或三次多项式不可约当且仅当它没有该域中的根；四次及以上则不够，例如  $(x^2 + 1)^2$  在  $\mathbb{R}$  中没有根却可约。

有理系数多项式可以先清除分母，转为本原整系数多项式 (primitive polynomial over the integers)。Eisenstein 判别法 (Eisenstein's criterion) 指出：若存在素数  $p$  整除所有非首项系数、不整除首项系数，且  $p^2$  不整除常数项，则该多项式在  $\mathbb{Q}$  上不可约。例如  $x^3 - 2$  可取  $p = 2$ 。

#### 6.5. 分裂域 (splitting field) 和代数闭包 (algebraic closure)

多项式  $f(x) \in F[x]$  的分裂域是包含  $F$  并使  $f$  分解成一次因子的最小域。

$$f(x) = c \prod_{i=1}^n (x - \alpha_i) \quad (97)$$

代数闭包  $\bar{F}$  是  $F$  的代数扩张 (algebraic extension)，且其中每个非常数多项式都有根。两条要求都需要：例如  $\mathbb{C}$  代数闭，但由于它含有相对于  $\mathbb{Q}$  的超越元，它不是  $\mathbb{Q}$  的代数闭包。

分裂域往往需要加入不止一个根。例如  $\mathbb{Q}(\sqrt[3]{2})$  只包含  $x^3 - 2$  的实根 (real root)；还要加入一个非平凡三次单位根 (cube root of unity)，才能得到它在  $\mathbb{Q}$  上的分裂域。

#### 6.6. 有限域

有限域的大小一定是素数幂：

$$|F| = p^n \quad (98)$$

有限域的乘法群是循环群：

$$F_q^* \cong C_{q-1} \quad (99)$$

有限域元素满足：

$$a^q = a \quad \forall a \in F_q \quad (100)$$

因此：

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a) \quad (101)$$

每个素数幂  $q$  都存在一个  $q$  元域，且在同构意义下唯一。但  $\mathbb{F}_{p^n}$  在  $n > 1$  时不是  $\mathbb{Z}/p^n\mathbb{Z}$ ：前者特征为  $p$  且没有零因子，后者特征为  $p^n$  且有零因子。实际构造有限域，可以取  $\mathbb{F}_{p[x]}$  模掉一个  $n$  次不可约多项式。

## 6.7. 逻辑关系

- 域是可以做除法的交换环。
- 多项式的根常常不在原域中，所以需要域扩张。
- 最小多项式控制单个代数元生成的扩张。
- 分裂域把一个多项式的所有根放进同一个最小环境。

### 练习 6

答案 →

令  $K = \mathbb{F}_2[x]/(x^2 + x + 1)$ ，并记  $\alpha = \bar{x}$ 。证明  $K$  是域，列出它的全部元素，求  $\alpha^2$  和  $\alpha^{-1}$ 。

## 7. Galois 理论：方程根和对称性

### 7.1. Galois 群 (Galois group)

设  $K/F$  是域扩张。Galois 群定义为：

$$\text{Gal}(K/F) = \{\sigma \in \text{Aut}(K) : \sigma(a) = a \quad \forall a \in F\} \quad (102)$$

它描述扩张域 (extension field) 中保持基域 (base field) 不动的自同构 (automorphism)。

如果  $K$  是  $f(x) \in F[x]$  的分裂域，则  $\text{Gal}(K/F)$  会作用在  $f$  的根上。

这是因为  $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$ 。但不是根的任意置换都对应域自同构 (field automorphism)：置换还必须保持根之间的全部代数关系。

### 7.2. 正规扩张 (normal extension)、可分扩张 (separable extension) 和 Galois 扩张 (Galois extension)

有限扩张 (finite extension)  $K/F$  是 Galois 扩张，通常要求：

- 正规：  $F[x]$  中的不可约多项式只要在  $K$  中有一个根，就在  $K$  中完全分裂。
- 可分：  $K$  中每个元素在  $F$  上的最小多项式都没有重根 (repeated root)。

有限 Galois 扩张满足：

$$|\text{Gal}(K/F)| = [K : F] \quad (103)$$

特征 0 的域上的代数扩张都可分。判断一个多项式是否有重根，可以计算它与形式导数 (formal derivative) 的最大公因子：  $\gcd(f, f') = 1$  当且仅当没有重根。

例如  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  是 Galois 扩张，两个自同构分别把  $\sqrt{2}$  送到  $\sqrt{2}$  和  $-\sqrt{2}$ 。相反，  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  不是正规扩张，因为缺少另外两个非实根；其自同构群 (automorphism group) 只有恒等映射，大小小于扩张次数 3。

### 7.3. Galois 基本定理 (fundamental theorem of Galois theory)

设  $K/F$  是有限 Galois 扩张。中间域 (intermediate field) 和子群之间存在反向对应：

$$E \text{ 中间域} \leftrightarrow H \leq \text{Gal}(K/F) \quad (104)$$

对应关系：

$$E \rightarrow \text{Gal}(K/E) \quad (105)$$

$$H \rightarrow K^H = \{x \in K : \sigma(x) = x \quad \forall \sigma \in H\} \quad (106)$$

并且：

$$[E : F] = [\text{Gal}(K/F) : \text{Gal}(K/E)] \quad (107)$$

$$[K : E] = |\text{Gal}(K/E)| \quad (108)$$

正规性对应：

$$E/F \text{ 是 Galois 扩张} \Leftrightarrow \text{Gal}(K/E) \text{ normal in } \text{Gal}(K/F) \quad (109)$$

此时：

$$\text{Gal}(E/F) \cong \text{Gal}(K/F) / \text{Gal}(K/E) \quad (110)$$

“反向”意味着固定的元素越多，允许的自同构就越少。整个群对应最小的基域  $F$ ，平凡子群 (trivial subgroup) 对应最大的域  $K$ 。使用此定理前必须先确认扩张有限且 Galois。

## 7.4. 根式可解

以下在特征 0 的基域上讨论。“根式可解”是指多项式的所有根都能置于一个由有限次添入根式得到的扩张中。

可解群 (solvable group) 有正规列 (subnormal series)：

$$\{e\} = G_0 \text{ normal in } G_1 \text{ normal in } \dots \text{ normal in } G_n = G \quad (111)$$

并且每个商群 Abel：

$$G_{i+1}/G_i \text{ 是 Abel 群} \quad (112)$$

核心结论：

$$f(x) \text{ 根式可解} \Leftrightarrow \text{Gal}(f) \text{ 是可解群} \quad (113)$$

这里  $\text{Gal}(f)$  指  $f$  的分裂域相对于基域的 Galois 群。

一般五次方程 (quintic equation) 不可根式求解，本质原因是一般五次多项式的 Galois 群为  $S_5$ ，而  $S_5$  不可解。

视频用  $x^5 - x - 1$  的五个根作了一个具体画面。这个多项式的 Galois 群是  $S_5$ ；其交错子群  $A_5$  的阶为 60，并且是非 Abel 单群。因为  $S_5$  含有  $A_5$ ，它不可能有由 Abel 商群组成的正规列，所以不是可解群。这里“答案是一个群”的含义是：方程是否有根式公式，取决于根之间允许的对称性，而不是取决于把五个根写成更复杂的符号。

并非每个五次方程都落在  $S_5$  这一最坏情形；有些五次方程的 Galois 群是可解群，仍可用根式表达。判断具体多项式时，通常结合分裂域、模素数分解型和判别式，而不能只看次数。

这并不是说每个五次方程都无法用根式求解，例如  $x^5 - 2 = 0$  的全部根可以用  $\sqrt[5]{2}$  和五次单位根 (fifth root of unity) 表达；结论也不妨碍对根进行数值近似。

## 7.5. 逻辑关系

- 多项式根之间的置换形成群。
- 域扩张记录“为了加入根而扩大的数系”。
- Galois 群记录扩张中保留原域结构的对称性。
- 中间域和子群的对应把“域的问题”转化为“群的问题”。

### 练习 7

答案 →

设  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ，已知  $[K : \mathbb{Q}] = 4$ 。列出  $\text{Gal}(K/\mathbb{Q})$  中所有自同构对两个平方根的作用，并求同时改变两个平方根符号的自同构所生成子群的固定域 (fixed field)。

## 8. 表示论：用线性变换研究群和代数

### 8.1. 群表示 (group representation)

群  $G$  在向量空间  $V$  上的表示是同态：

$$\rho : G \rightarrow \text{GL}(V) \quad (114)$$

满足：

$$\rho(gh) = \rho(g)\rho(h) \quad (115)$$

表示把抽象群元素变成矩阵，使群论可以使用线性代数工具。

子空间 (subspace)  $W \subseteq V$  若在每个  $\rho(g)$  下都保持不变，就给出一个子表示 (subrepresentation)。非零表示若只有零子空间与自身两个不变子空间，就称为不可约表示 (irreducible representation)。若表示能分解为不可约子表示 (irreducible subrepresentation) 的直和 (direct sum)，就称为完全可约 (completely reducible)。

两个表示等价，是指存在可逆线性映射  $T$  满足  $T\rho(g) = \rho'(g)T$ ，也就是统一地换一组基。研究表示通常要回答：有哪些不可约表示，以及给定表示含有它们各多少份？

### 8.2. 完全可约的条件

Maschke 定理 (Maschke's theorem)：若  $G$  有限，且域  $F$  的特征不整除  $|G|$ ，则每个有限维  $F$ -表示完全可约。证明的关键是把一个投影 (projection) 对群作用取平均，得到与群作用相容的投影。

条件不能省略。例如在特征 2 的域上，阶为 2 的群可以让生成元作用为：

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A^2 = I \quad (116)$$

该矩阵有非零非对角项，却只有一个一维特征子空间 (eigenspace)，因此这个二维表示不能分解成两个一维表示的直和。

### 8.3. 特征标 (character)

有限维表示的特征标：

$$\chi_{\rho(g)} = \text{tr}(\rho(g)) \quad (117)$$

对有限群的复表示 (complex representation)，特征标内积 (inner product) 为：

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} \quad (118)$$

不可约表示的特征标满足正交关系 (orthogonality relations)：相同不可约特征标的内积为 1，不同的为 0。由于复表示完全可约， $\langle \chi_V, \chi_W \rangle$  就是不可约表示  $W$  在  $V$  中出现的次数。

迹在共轭变换下不变，所以特征标在每个共轭类 (conjugacy class) 上取常值。在单位元处， $\chi_{V(e)} = \dim V$ 。有限群的不可约复表示共有多少个，恰好等于其共轭类的个数；它们的维数还满足：

$$\sum_i (\dim V_i)^2 = |G| \quad (119)$$

#### 8.4. 群代数 (group algebra)

群代数：

$$F[G] = \left\{ \sum_{g \in G} a_g g : a_g \in F \right\} \quad (120)$$

如果  $G$  无限，上式要求只有有限多个  $a_g$  非零。

乘法由群运算线性延拓 (linear extension)：

$$\left( \sum_g a_g g \right) \left( \sum_h b_h h \right) = \sum_{g,h} a_g b_h (gh) \quad (121)$$

表示论也可以看作研究  $F[G]$ -模。

#### 8.5. 连续对称：Lie 群、 $E_8$ 与物理中的群

有限群描述离散对称；旋转角度可以连续变化时，需要 Lie 群 (Lie group)：它既是群，又是光滑流形，乘法和取逆都是光滑映射。单位元处的切空间带有 Lie 括号，形成 Lie 代数 (Lie algebra)；指数映射把无穷小生成元送回群的局部邻域。

特殊酉群  $SU(n)$  由满足  $U^*U = I$  且  $\det(U) = 1$  的复矩阵组成，实维数为  $n^2 - 1$ 。因此  $SU(2)$  有 3 个独立生成元， $SU(3)$  有 8 个。表示论研究这些生成元如何作用在粒子态或其他向量空间上；视频中的“八重态”正是  $SU(3)$  表示分解的可视化线索。

粒子物理标准模型常用的规范对称群写作：

$$SU(3) \times SU(2) \times U(1) \quad (122)$$

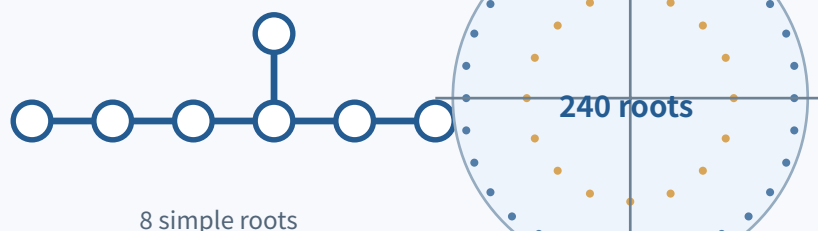
三因子分别对应色相互作用、弱相互作用和超荷的规范结构。这里的群只是理论的对称输入；粒子内容、表示、耦合常数和动力学还需要量子场论，不能由群的记号单独推出。

$E_8$  是最大的例外型紧致单 Lie 群之一，其 Lie 代数维数为 248，根系有 240 个根。它与标准模型的关系属于研究方向或模型构造，不等于标准模型已经由  $E_8$  唯一解释。

## E8: a finite root system behind a large symmetry

The left panel is the Dynkin diagram; the right panel is a symmetric 2D projection of its roots.

### Dynkin diagram



The projection preserves symmetry cues, not the full 8-dimensional geometry.

2D projection (schematic)

图3  $E_8$  的 Dynkin 图和根系二维投影（示意图）。右图只表达对称性和数量级，不代表 8 维根系的等距投影。

Monster 群是最大的散在单群，阶为：

$$808017424794512875886459904961710757005754368000000000 \quad (123)$$

约为  $8 \times 10^{53}$ 。它的最小非平凡复表示维数是 196883，所以视频中出现的  $196884 = 196883 + 1$  是模函数与 Monster 表示中著名的数值线索，而不是群的阶。巨大数字的意义在于展示“对称性”可以有极高的内部复杂度，仍能由有限的生成关系精确组织。

## 8.6. 逻辑关系

- 群表示把群作用线性化。
- 特征标把矩阵表示压缩成函数，但仍保留很多结构信息。
- 群代数把群论转化为环和模的问题。

### 练习 8

答案 →

设  $C_2 = \{e, s\}$  在  $\mathbb{C}^2$  上作用为  $\rho(s)(u, v) = (v, u)$ 。找出两个一维不变子空间，写出表示的直和分解，并计算  $\chi(e)$  与  $\chi(s)$ 。

## 9. 交换代数：几何背后的环论

### 9.1. 素谱 (prime spectrum)

交换环  $R$  的素谱：

$$\text{Spec}(R) = \{p \subset R : p \text{ 是素理想}\} \quad (124)$$

这是代数几何 (algebraic geometry) 中的基本对象。直观上，素理想可以看作广义的点。

例如  $\text{Spec}(\mathbb{Z})$  包括零理想以及每个素数  $p$  对应的理想  $(p)$ 。在代数闭域 (algebraically closed field)  $k$  上，多项式环  $k[x]$  的极大理想都形如  $(x - a)$ ，于是可以把它看成直线上的点  $a$ ；零理想则不是这种普通的点。

给定理想  $I$ ，令  $V(I)$  为所有包含  $I$  的素理想组成的集合。这些集合构成 Zariski 拓扑 (Zariski topology) 的闭集 (closed set)。包含关系是反向的：加入更多方程、增大理想，通常会缩小满足方程的点集。

## 9.2. 局部化

给定乘法闭集 (multiplicative set)  $S \subset R$ ，局部化：

$$S^{-1}R = \{a/s : a \in R, s \in S\} \quad (125)$$

它把  $S$  中的元素都变成可逆元 (invertible element)。

这里要求  $1 \in S$  且  $S$  对乘法封闭；通常还取  $0 \notin S$ 。在有零因子的环中，分数相等应理解为：存在  $u \in S$  使  $u(at - bs) = 0$ ，才有  $a/s = b/t$ 。不能未经检查就使用整环里的交叉相乘规则。

在素理想  $p$  处的局部环 (local ring)：

$$R_p = (R - p)^{-1}R \quad (126)$$

局部环是只有一个极大理想的环； $R_p$  的唯一极大理想是  $pR_p$ 。例如：

$$\mathbb{Z}_{(3)} = \{a/b \in \mathbb{Q} : a, b \in \mathbb{Z}, 3 \nmid b\} \quad (127)$$

其中 2 可逆，3 不可逆；写成分母不被 3 整除的形式后，分子也不被 3 整除的分数恰好是单位。它与  $\mathbb{Z}/3\mathbb{Z}$  不同：局部化仍保留 3，而取商把 3 变成零。

## 9.3. Noether 环 (Noetherian ring)

Noether 环的定义：

$$I_1 \subseteq I_2 \subseteq \dots \Rightarrow \exists n, \forall k \geq n, I_k = I_n \quad (128)$$

即理想升链 (ascending chain of ideals) 稳定。

这等价于每个理想都有限生成，并不是说环的元素个数有限，或一切模都有限生成。例如  $\mathbb{Z}$  和  $k[x_1, \dots, x_n]$  都是 Noether 环；无限多个变量的多项式环则有严格升链  $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$ 。

Hilbert 基定理 (Hilbert's basis theorem)：

$$R \text{ Noether} \Rightarrow R[x] \text{ Noether} \quad (129)$$

Noether 环的商环与局部化仍是 Noether 环。因此有限多个变量、有限组关系构造出的很多环，都处在这个可控的框架内。

## 9.4. 逻辑关系

- 交换环的理想结构可以编码几何对象。
- 局部化表示只关注某个点或某个区域附近的信息。
- Noether 条件 (Noetherian condition) 保证每个理想有限生成，让理想层面的运算具有有限描述。

### 练习 9

答案 →

在  $\mathbb{Z}_{(3)}$  中，判断  $2/5$  和  $3/5$  是否为单位，并在可逆时写出逆元。再说明  $1/3$  为什么不属于这个环。

## 10. 同调代数：用正合性测量结构

### 10.1. 为什么需要同调

很多自然函子 (functor) 不能保持正合。例如固定一个交换环  $R$  上的模  $M$ ，函子  $M \otimes_R -$  总是右正合 (right exact)，但不一定左正合 (left exact)； $\text{Hom}_{R(M, -)}$  总是左正合，但不一定右正合。

同调代数的思想是：用派生函子 (derived functor) 测量正合性失败的程度。

具体地，对短正合列  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ ，右正合保证张量后  $M \otimes_R A \rightarrow M \otimes_R B \rightarrow M \otimes_R C \rightarrow 0$  正合，但最左边的箭头未必单射。

对  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$  (第一个非零箭头为乘以 2) 张量  $\mathbb{Z}/2\mathbb{Z}$  后，这个乘以 2 的箭头变成  $\mathbb{Z}/2\mathbb{Z}$  上的零映射 (zero map)，从而丢失单射性。

### 10.2. Tor 和 Ext

Tor 测量张量积保持正合的失败：

$$\text{Tor}_1^{R(M, N)} \quad (130)$$

Ext 测量 Hom 保持正合的失败：

$$\text{Ext}_R^1(M, N) \quad (131)$$

粗略理解：

- Tor 和张量积、模的扭元信息有关。
- Ext 和扩张、分类短正合列有关。

短正合列：

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0 \quad (132)$$

可以看成  $B$  是用  $A$  和  $C$  拼出来的对象，而  $\text{Ext}^1(C, A)$  控制这种拼法的分类。

更精确地， $\text{Ext}_R^1(C, A)$  分类固定两端  $A, C$  的短正合列的等价类，其中零元对应分裂扩张 (split extension)。相同的两端不决定中间项，例如  $0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow B \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$  可以取分裂的  $B = (\mathbb{Z}/2\mathbb{Z})^2$ ，也可以取不分裂的  $B = \mathbb{Z}/4\mathbb{Z}$ 。

### 10.3. 链复形 (chain complex) 和同调群 (homology group)

链复形：

$$\dots \rightarrow C_{n+1} \rightarrow C_n \rightarrow C_{n-1} \rightarrow \dots \quad (133)$$

满足：

$$d_n \circ d_{n+1} = 0 \quad (134)$$

同调群：

$$H_{n(C)} = \text{Ker}(d_n) / \text{Im}(d_{n+1}) \quad (135)$$

含义：闭的对象模掉边界 (boundary) 对象。

更具体地， $\text{Ker}(d_n)$  中的元素叫循环 (cycle)， $\text{Im}(d_{n+1})$  中的元素叫边界。条件  $d_n \circ d_{n+1} = 0$  保证边界一定是循环，因此这个商有定义。 $H_{n(C)} = 0$  恰好意味着复形 (complex) 在  $C_n$  处正合。

## 10.4. 用自由分解 (free resolution) 做一次计算

取整数模  $\mathbb{Z}/n\mathbb{Z}$  的自由分解, 其中  $n \geq 2$ :

$$0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0 \quad (136)$$

它把一个不自由的模换成自由模组成的复形。与模  $N$  张量后, 计算非增广部分  $N \xrightarrow{n} N$  的同调, 得到:

$$\mathrm{Tor}_1^{\mathbb{Z}(\mathbb{Z}/n\mathbb{Z}, N)} \cong \{v \in N : nv = 0\} \quad (137)$$

对同一分解应用  $\mathrm{Hom}_{\mathbb{Z}(-, N)}$  并计算上同调 (cohomology), 则得到:

$$\mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/n\mathbb{Z}, N) \cong N/nN \quad (138)$$

因此  $\mathrm{Tor}_1^{\mathbb{Z}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})} \cong \mathbb{Z}/2\mathbb{Z}$ , 它恰好记录前面张量后消失的单射性。计算派生函子的基本步骤就是: 选分解、应用函子、求同调。

## 10.5. 逻辑关系

- 正合列描述结构是否完整传递。
- 同调群测量“差一点正合”的部分。
- 同调代数代数拓扑 (algebraic topology)、代数几何、表示论和数论 (number theory) 提供统一语言。

### 练习 10

答案 →

考虑链复形  $0 \rightarrow C_1 = \mathbb{Z} \xrightarrow{2} C_0 = \mathbb{Z} \rightarrow 0$ , 其中  $d_1$  为乘以 2。计算  $H_1$  和  $H_0$ 。若先把这个复形与  $\mathbb{Z}/2\mathbb{Z}$  张量, 这两个同调群分别变成什么?

## 11. 与其他数学分支的关系

### 11.1. 和线性代数

线性代数是域上的模论:

$$\text{vector spaces over } F = F\text{-modules} \quad (139)$$

矩阵相似 (matrix similarity)、Jordan 标准形、有理标准形, 都可以通过  $F[x]$ -模理解。

这里  $x$  的作用就是线性算子  $T$ 。与  $T$  交换的线性映射正是这种  $F[x]$ -模的自同态 (endomorphism); 因此“矩阵与哪个算子可交换”也能转成模论问题。

### 11.2. 和数论

整数环、代数整数环 (ring of algebraic integers)、理想分解 (ideal factorization) 构成代数数论 (algebraic number theory) 基础。

在数域 (number field) 的代数整数环中, 每个非零真理想都能唯一分解为非零素理想的乘积。特别地, 非零非单位元素生成的主理想有分解:

$$(\alpha) = p_1^{e_1} \dots p_k^{e_k} \quad (140)$$

唯一分解失败时, 理想分解往往仍然可控。

这一结论有环的条件，不能推广到任意整环。例如  $\mathbb{Z}[\sqrt{-5}]$  中， $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$  给出元素层面的两种本质不同分解；研究理想可以恢复更稳定的分解语言。

### 11.3. 和几何

代数几何的基本反向关系：

$$\text{几何对象} \leftrightarrow \text{函数环} \quad (141)$$

例如仿射代数簇（affine algebraic variety）和坐标环（coordinate ring）之间存在深刻对应。

把平面曲线的方程写成  $y - x^2 = 0$ ，其坐标环就是  $k[x, y]/(y - x^2)$ 。取商后  $y = x^2$ ，所以这个环同构于  $k[x]$ 。这表达了抛物线（parabola）可以用一个参数描述： $t \mapsto (t, t^2)$ 。

若几何映射是  $f: X \rightarrow Y$ ，那么  $Y$  上的函数  $h$  会拉回（pullback）成  $X$  上的函数  $h \circ f$ ，所以函数环上的映射方向与几何映射相反。这是代数几何反向对应的来源。

### 11.4. 和计算机科学

第一章已经从数据恢复、坐标变换、AES 和并行归并说明工程动机，第三章则把魔方求解拆成可验证的操作。这里再补一个与“恢复已知丢失”不同的问题：怎样检测未知位置的错误？

一个最简单的编码例子是在  $\mathbb{F}_2$  上给数据位  $a, b$  添加校验位（parity bit） $a + b$ 。合法码字（codeword）为  $(a, b, a + b)$ ，它们构成  $\mathbb{F}_2^3$  的子空间，任意一位翻转都会破坏三个坐标之和为零的关系。这个码可以检测单比特错误，但不能单靠该关系确定错误位置。

这说明“数据属于某个代数结构”可以产生可检验的约束，但检错、定位错误和恢复数据是不同能力，需要分别证明。类似地，程序验证会把运算律写成明确的前提，再证明优化和重构保持哪些性质。

#### 11.4.1. 从有限域到二维码

视频中二维码旁边的“纠错等级 H，恢复约 30% 的码字”对应 Reed-Solomon 纠错，而不是普通的复制备份。编码器把数据视为有限域上的符号，并添加校验符号，使合法码字落在一组满足多项式约束的序列中。读取时，即使部分符号被擦除或被错误污染，也可以利用这些约束恢复原值。

二维码的四个等级通常标为 L、M、Q、H，目标纠错能力约为 7%、15%、25%、30% 的码字。这里的百分比是标准规定下的码字恢复能力；实际能否读出还受损坏位置、污渍形状、定位图案和扫描质量影响。有限域提供了可逆的代数运算，交织和定位图案则是编码工程的其他部分。

#### 11.4.2. 椭圆曲线：把几何曲线变成群

在特征不为 2、3 的域上，非奇异椭圆曲线可写成：

$$E: y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0 \quad (142)$$

补上无穷远点  $O$  后，曲线上的点构成 Abel 群。几何加法是“过  $P, Q$  作直线，取第三个交点，再关于  $x$  轴反射”；当  $P = Q$  时使用切线。这正是视频中沿直线寻找第三个交点的画面。代数上，这个几何规则在有限域中仍成立，因此  $E(\mathbb{F}_p)$  是有限 Abel 群。

密码学使用标量乘法  $kP = P + P + \dots + P$ ，而不是把点坐标做普通乘法。以比特币使用的 secp256k1 为例：

$$y^2 = x^3 + 7 \quad \text{over } \mathbb{F}_p, \quad p = 2^{256} - 2^{32} - 977 \quad (143)$$

公钥通常写成  $Q = kG$ ，其中  $G$  是公开基点， $k$  是私钥。已知  $k$  求  $Q$  很快，反向求解椭圆曲线离散对数在参数正确时被认为困难；这是假设，不是由群公理单独保证的安全性。换曲线、实现随机数或参数出错，都可能破坏安全性。

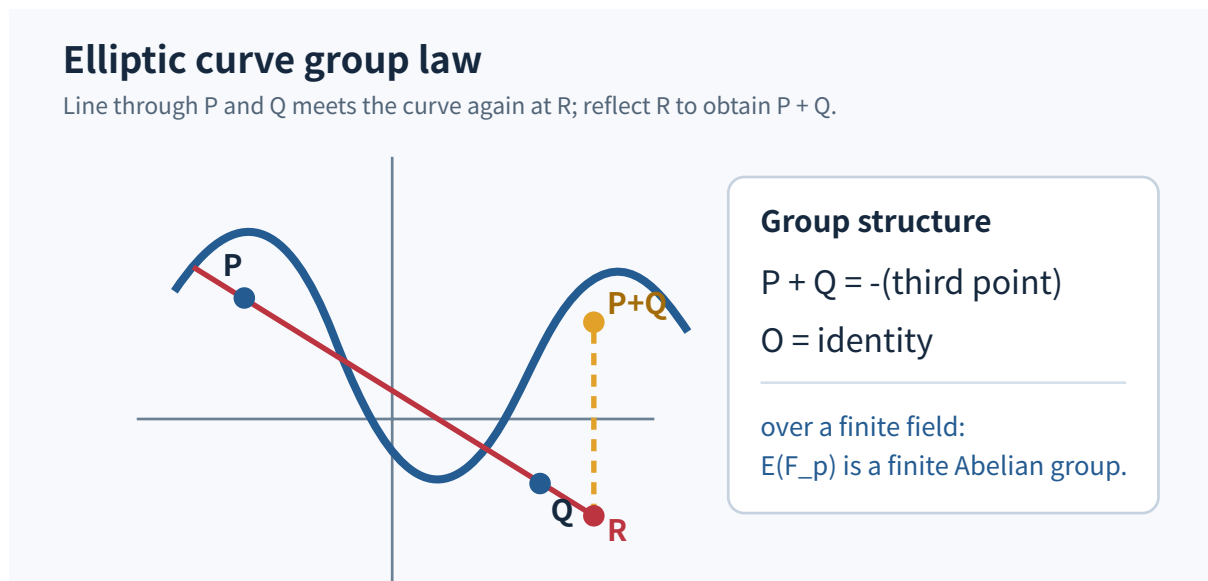


图 4 椭圆曲线上的群加法：直线第三交点再关于  $x$  轴反射（示意图）。无穷远点  $O$  扮演单位元。

### 练习 11

答案 →

设  $k$  为域，求同态  $\varphi : k[x, y] \rightarrow k[t]$ 、 $\varphi(f) = f(t, t^2)$  的像与核，并用同构定理说明抛物线的坐标环为什么同构于  $k[t]$ 。提示：把多项式看成关于  $y$  的多项式，除以  $y - x^2$ 。

## 12. 同态加密 (homomorphic encryption, HE)：加密后怎样计算

前面说同态是“换一种表示，仍然保留运算关系”。同态加密把这一点变成一个工程问题：能否把数据交给别人计算，同时让对方看不到数据的内容？本章先用群同态做一次可以手算的加密计算，再说明环、多项式和计算深度为什么会进入全同态加密 (fully homomorphic encryption, FHE)。

### 12.1. 从工资汇总理解目标

设你要让服务器计算若干工资的总和。原始工资称为明文 (plaintext)，加密后的数据称为密文 (ciphertext)。在本章的公钥加密 (public-key encryption) 场景中，公钥 (public key) 可以公开，私钥 (secret key) 由有权解密的人持有。

流程是：

1. 数据持有者用同一个公钥加密各项工资，把密文交给服务器。
2. 服务器执行指定的密文运算，得到结果密文，过程中不持有私钥。
3. 有权解密的人拿回结果，解密得到工资总额。

服务器能运行运算规则，却不能因此直接读出工资。这里默认密文属于兼容的密钥和参数；不同用户各自生成密钥后得到的密文，通常不能直接混在一起计算。

例如明文是 4 和 7，希望服务器最终交回一个解密后等于 11 的密文。至于密文长什么样、服务器应当相加还是相乘，要由具体方案决定。

## 12.2. 同态性质到底写成什么等式

代数中，对于运算分别为  $+$  与  $*$  的两个群，同态满足：

$$\varphi(a + b) = \varphi(a) * \varphi(b) \quad (144)$$

两边运算不必同名。加法同态加密 (additively homomorphic encryption) 要求密文运算对应明文加法；记该密文运算为  $\star$ ，则：

$$\text{Dec}_{\text{sk}}(\text{Enc}_{\text{pk}}(a) \star \text{Enc}_{\text{pk}}(b)) = a + b \quad (145)$$

右侧在方案规定的明文空间中计算，例如模  $n$  的加法。更一般地，同态求值 (homomorphic evaluation) 算法以公开的计算规则  $f$  和密文为输入：

$$c_i = \text{Enc}_{\text{pk}}(m_i ; r_i) \quad (146)$$

$$\text{Dec}_{\text{sk}}(\text{Eval}_{\text{evk}}(f, c_1, \dots, c_k)) = f(m_1, \dots, m_k) \quad (147)$$

这里  $r_i$  是加密时使用的随机量；evk 表示求值密钥 (evaluation key) 等公开辅助材料，简单方案可能不需要额外的求值密钥。等式表达正确性 (correctness)：在允许的计算范围与参数条件下，精确方案应当正确解密，可能允许可忽略的失败概率。近似方案则需要把等号换成带误差界的近似关系。

随机化加密 (randomized encryption) 允许同一明文产生多个密文，因此不能一般地要求：

$$\text{Eval}_{\text{evk}}(\text{add}, \text{Enc}_{\text{pk}}(a), \text{Enc}_{\text{pk}}(b)) = \text{Enc}_{\text{pk}}(a + b) \quad (148)$$

左右两边可能使用不同的随机量，字节表示不同。要检查的是解密后是否相等。也不能不加说明地把随机化的 Enc 当成一个只以明文为输入的普通群同态。

## 12.3. Paillier：密文乘法对应明文加法

### 12.3.1. 加密和解密规则

Paillier 加密 (Paillier encryption) 提供了一个直接连接群论的例子。以下采用  $g = n + 1$  的常见形式。取不同素数  $p, q$ ，令：

$$n = pq, \quad \lambda = \text{lcm}(p-1, q-1), \quad \gcd(n, \lambda) = 1 \quad (149)$$

$$g = n + 1, \quad \mu = \lambda^{-1} \bmod n \quad (150)$$

公钥是  $(n, g)$ ，私钥可以用  $(\lambda, \mu)$  表示。明文空间是  $\mathbb{Z}/n\mathbb{Z}$ ，密文位于乘法群  $(\mathbb{Z}/n^2\mathbb{Z})^\times$ 。选取与  $n$  互素的随机数  $r$ ，加密为：

$$\text{Enc}(m ; r) = g^m r^n \bmod n^2 \quad (151)$$

解密时定义  $L(u) = (u - 1)/n$ ，并计算：

$$\text{Dec}(c) = L(c^\lambda \bmod n^2) \mu \bmod n \quad (152)$$

对于合法密文，传给  $L$  的整数与 1 模  $n$  同余，所以这里的除以  $n$  是整数精确除法。上述密钥条件保证  $\mu$  存在。

乘两个密文会得到：

$$\text{Enc}(a ; r_1) \text{Enc}(b ; r_2) \equiv g^{a+b}(r_1 r_2)^n \bmod n^2 \quad (153)$$

这正是  $a + b \bmod n$  的一种加密。**密文侧做乘法，明文侧得到加法。**类似地，对公开的非负整数  $k$ ：

$$\text{Dec}(\text{Enc}(a ; r)^k) = ka \bmod n \quad (154)$$

因此可以计算公开权重下的加权和 (weighted sum)。这里的  $k$  已知；若  $a, b$  都只以密文给出，这些规则并没有提供计算  $ab$  的一般方法。算法及其安全假设见 [Paillier 原论文的 Scheme 1 与 Security 讨论](#)。

### 12.3.2. 用小整数完整算一次

为了能手算，取  $p = 3, q = 5$ ，于是：

$$n = 15, \quad n^2 = 225, \quad g = 16, \quad \lambda = 4, \quad \mu = 4 \quad (155)$$

这些小参数只用于展示算术：任何人都能立即分解 15，因而不能隐藏消息。取明文 4、7，分别选择  $r_1 = 2, r_2 = 4$ ：

$$c_1 = 16^4 \cdot 2^{15} \bmod 225 = 173 \quad (156)$$

$$c_2 = 16^7 \cdot 4^{15} \bmod 225 = 169 \quad (157)$$

服务器只做：

$$c = c_1 c_2 \bmod 225 = 212 \quad (158)$$

持有私钥的人解密：

$$212^4 \bmod 225 = 211 \quad (159)$$

$$\text{Dec}(212) = \frac{211 - 1}{15} \cdot 4 \bmod 15 = 11 \quad (160)$$

因此服务器确实算出了和的密文。若计算  $2 \cdot 4 + 7$ ，解密结果则是 0，因为明文运算按模 15 进行。需要普通整数结果时，必须事先控制数值范围，避免模回绕 (modular wraparound)；同态性质不会自动把模运算变成无限精度整数运算。

### 12.3.3. 核、陪集和商群在这里是什么

在上述参数条件下，解密给出一个满群同态：

$$\text{Dec} : (\mathbb{Z}/n^2\mathbb{Z})^\times \rightarrow (\mathbb{Z}/n\mathbb{Z}, +) \quad (161)$$

它的核是所有解密为零的密文，也就是随机化项组成的子群：

$$K = \text{Ker}(\text{Dec}) = \{r^n \bmod n^2 : r \in (\mathbb{Z}/n\mathbb{Z})^\times\} \quad (162)$$

明文  $m$  的所有密文形成陪集  $g^m K$ 。随机化就是在同一个陪集中选择不同代表；相乘时，陪集按照明文加法组合：

$$(g^a K)(g^b K) = g^{a+b} K \quad (163)$$

$$(\mathbb{Z}/n^2\mathbb{Z})^\times / K \cong (\mathbb{Z}/n\mathbb{Z}, +) \quad (164)$$

这让前面的“同态 → 核 → 商 → 同构定理”有了具体用途。解密忽略随机化造成的差别，保留明文。能够写出这些陪集，并不意味着没有私钥的人能高效判断密文属于哪个陪集；这种计算难度才与保密性（confidentiality）有关。

### 12.4. 从一种运算到全同态

把需要计算的函数拆成有限个运算节点，得到算术电路（arithmetic circuit）；用与、或、非等逻辑门表示时，得到布尔电路（Boolean circuit）。常见能力层次如下：

| 类型                                            | 能保证什么                          |
|-----------------------------------------------|--------------------------------|
| 部分同态加密（partially homomorphic encryption, PHE） | 支持一种运算的反复组合，例如 Paillier 的加法同态。 |
| 有限同态加密（somewhat homomorphic encryption, SHE）  | 能混合加法与乘法，但只支持受限的计算复杂度。         |
| 分层全同态加密（leveled fully homomorphic encryption） | 事先给定深度上界，再选择参数，支持该深度内的电路。      |
| 全同态加密                                         | 支持任意多项式规模的电路，并满足紧致性要求。         |

紧致性（compactness）要求每个输出密文的长度和解密工作量不随已经执行的电路规模任意增长。服务器应当交回可以直接解密的结果，而不能只是把原始密文和整个待执行程序打包退回来。全同态也不意味着零成本或无限资源；服务器仍要完成与计算规模相应的工作。正式定义见 [Gentry 学位论文的 Definitions Related to Homomorphic Encryption](#)。

#### 12.4.1. 为什么加法与乘法足以表达一般计算

对于取值为 0 或 1 的位，在  $\mathbb{F}_2$  上有：

$$a \text{ XOR } b = a + b, \quad a \text{ AND } b = ab, \quad \text{NOT } a = 1 + a \tag{165}$$

于是可以把有限的逻辑计算变成有限域上的算术电路。更一般的环上，加乘可以直接表示多项式，例如：

$$f(x, y) = (x + y)^2 + 3x \tag{166}$$

如果方案允许相应的密文加法、乘法以及公开常数运算，就能按相同的依赖关系计算该函数。乘法深度（multiplicative depth）指从输入到输出的一条路径上最多经过多少层乘法，它与乘法总次数不同。例如  $x^8$  若逐次乘以  $x$ ，要串行执行 7 次乘法；改用  $x^2, x^4, x^8$  的连续平方，只需要 3 层。这种代数改写会直接影响参数需求。

有密文条件的程序也需要改写。若  $b$  是加密的 0/1 选择位，可以通过  $bu + (1 - b)v$  选择结果；服务器不能先读出  $b$  再走普通分支。比较、查表和除法也需要对应的电路或近似方法，不能直接把任意现有程序交给一个加乘接口。

### 12.5. 为什么现代方案大量使用多项式商环

一类常见结构是：

$$R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^N + 1) \tag{167}$$

其中  $N$  常取 2 的幂,  $q$  是密文模数 (ciphertext modulus)。一个环元素用次数小于  $N$  的多项式表示: 系数按模  $q$  计算, 幂次按  $x^N = -1$  约化。它提供了有限、规则、适合批量运算的计算空间。

例如在  $R_{17} = (\mathbb{Z}/17\mathbb{Z})[x]/(x^4 + 1)$  中:

$$(1 + 2x)(3 + x^3) = 3 + 6x + x^3 + 2x^4 = 1 + 6x + x^3 \quad (168)$$

第二个等号使用了商环中的关系  $x^4 = -1$ 。这些规则与第四章多项式商环的运算完全一致。

以 BFV 一类精确方案为例, 明文可编码在:

$$R_t = (\mathbb{Z}/t\mathbb{Z})[x]/(x^N + 1) \quad (169)$$

这里  $t$  是明文模数 (plaintext modulus); 密文通常由  $R_q$  中的多个多项式组成, 而不是单个“加密后的数字”。 $t$  与  $q$  承担不同职责。它们之间的对应需要方案定义的编码、缩放和解密规则, 不能默认“把系数从模  $q$  改成模  $t$ ”就是加密或解密。

满足适当分解条件时, 中国剩余定理还能把明文环分解成多个分量, 从而实现批处理 (batching): 在一个密文里放入多个数据槽位, 让一次环运算同时完成多组运算。槽位的组织依赖编码和环的分解, 不能把多项式系数与独立数据槽位直接等同。

很多此类方案的安全基础涉及环上带误差学习问题 (Ring Learning With Errors, RLWE): 公开若干带有小误差的环上线性关系, 而隐藏其中的秘密。环结构提供计算规则; 困难问题假设解释为什么公开这些关系仍能隐藏秘密。构造背景见 [Fan-Vercauteren 的 Somewhat Practical Fully Homomorphic Encryption](#)。

## 12.6. 噪声为什么会限制计算

### 12.6.1. 解密需要分辨“消息”和“小误差”

为了理解带噪方案, 可以先看一个缩放后的整数示意。设解密中间量在选择适当代表后形如:

$$u = \Delta m + e \quad (170)$$

其中  $\Delta$  是缩放因子 (scaling factor),  $e$  是误差。若  $|e| < \Delta/2$ , 则对  $u/\Delta$  四舍五入可以恢复  $m$ 。例如  $\Delta = 100, m = 4, e = 7$  时,  $u = 407$ , 舍入 4.07 得到 4; 若误差增长到 60, 舍入 4.60 就会得到错误的 5。

这只是局部舍入过程的示意。真实方案还要处理模运算、边界、多个多项式以及秘密密钥; 不能把  $u = \Delta m + e$  单独拿来当成一个加密算法。

相加时误差变成  $e_1 + e_2$ 。直接展开两个中间量的乘积, 则会出现:

$$(\Delta m_1 + e_1)(\Delta m_2 + e_2) = \Delta^2 m_1 m_2 + \Delta(m_1 e_2 + m_2 e_1) + e_1 e_2 \quad (171)$$

所以乘法同时改变消息缩放和误差。实际同态乘法需要额外处理这些变化; 能够执行一次乘法, 并不保证随意重复后仍能正确解密。

### 12.6.2. 密文长度与噪声是两个问题

某些方案的解密关系涉及  $c_0 + c_1 s$ , 其中  $s$  是秘密。两份密文相乘后, 会出现包含  $s^2$  的项, 需要更多密文分量。重线性化 (relinearization) 借助求值密钥, 把这种表示转换回较少分量。

它主要处理密文表示的长度问题, 并不会自动把已经增长的噪声恢复到初始水平。噪声预算 (noise budget) 则表示距离不能可靠解密还有多少余量。具体变化依赖方案和参数; 串行乘法通常比加法更快消耗预算。相关实现解释见 [SEAL 的 example\\_bfv\\_basics\(\)](#) 示例。

## 12.7. 自举 (bootstrapping): 让密文重新获得计算余量

自举的关键思想是：把解密本身看成一个可以在密文上执行的电路。服务器拿到用于自举的辅助密钥，其中包含适当加密的秘密密钥信息，便能同态执行解密计算，输出仍然是密文。

可以把经典构造的语义写成：

$$c \rightarrow \text{Enc}_{\text{pk}_2}(\text{Dec}_{\text{sk}_1}(c)) \quad (172)$$

这里的箭头表示整个同态过程的效果；服务器没有拿到裸露的  $\text{sk}_1$ ，也没有在内存中先解出明文再加密。输出可以在另一把密钥下；若使用同一把密钥形成循环，还需要相应的密钥相关安全假设。

成功自举后，消息保持不变，噪声状态得到刷新，可以继续计算。它必须在输入仍满足自举正确性条件时进行，无法普遍挽救已经丢失信息的密文；刷新本身也有显著成本。经典构造见 [Gentry 学位论文的 Bootstrappable Encryption 与 Recrypt 算法](#)。

## 12.8. 精确结果与近似结果

不同方案的“正确”有不同含义：

| 方案       | 计算语义                                    | 需要关注                 |
|----------|-----------------------------------------|----------------------|
| Paillier | 模 $n$ 的精确加法与公开常数倍。                      | 结果范围；两个隐藏值的乘积需要其他能力。 |
| BFV、BGV  | 明文环上的精确加法、乘法。                           | 模回绕，以及运算后能否正确解密。     |
| CKKS     | 编码后的实数或复数近似运算 (approximate arithmetic)。 | 精度、缩放与误差传播。          |

这里“密文乘法”始终指某个密文算法；是否对应明文乘法，要看方案。Paillier 的密文相乘对应的是明文相加。

CKKS 把消息编码到多项式中，用缩放保留有效精度。乘法后，重缩放 (rescaling) 调整缩放大小，并带来舍入误差。例如某个数学结果是 0.3，解码结果可以是足够接近 0.3 的数，而不要求逐位精确。重缩放会消耗模数层级；它与用于继续深层计算的自举承担不同任务。参见 [CKKS 原论文 Homomorphic Encryption for Arithmetic of Approximate Numbers](#)。

整数计数与数值模型推理对误差的要求不同，因此应先确定结果语义，再选择方案。BFV、BGV、CKKS 的运算差异也可参见 [Microsoft SEAL 的 Introduction](#)。

## 12.9. 保留运算关系，为什么仍能隐藏数据

正确性与保密性是两个独立要求。恒等映射  $\text{Enc}(m) = m$  保留所有运算，却直接公开了消息；取余映射  $m \mapsto m \bmod n$  也是同态，却无法恢复任意整数  $m$ 。因此，同态性质本身既不能证明保密，也不能保证加密所需的可恢复性。

对于公钥加密，随机化还有一个直观作用：如果加密是确定的，服务器可以把每个候选工资自行加密，再与目标密文比较。随机化阻止这种直接比较；完整的安全性仍要依赖困难问题假设与安全证明。

同态加密允许服务器构造相关密文，例如把“工资的密文”变成“工资加 1 的密文”。这种可塑性 (malleability) 是计算能力的一部分，所以还需要单独回答两个问题：

- **服务器是否执行了约定计算？** 能正确执行算法，不等于能证明服务器实际照做了。验证计算结果需要额外机制。
- **允许解密哪些结果？** 若向服务器公开某人的精确工资总额，再公开排除该人的总额，相减就能得到个人工资。加密无法消除输出本身透露的信息。

同样，隐藏输入并不自动隐藏服务器的计算程序。后者属于电路隐私（circuit privacy），需要额外性质。工程上应分别定义输入保密、输出可见范围、程序隐私和结果验证要求。

### 12.10. 与前面代数知识的对应

| 代数概念    | 在本章中的具体作用               |
|---------|-------------------------|
| 群同态     | Paillier 解密把密文乘法映成明文加法。 |
| 核、陪集、商群 | 随机化项组成核；同一明文的密文属于同一陪集。  |
| 环与多项式商环 | 提供同时支持加法与乘法的有限计算空间。     |
| 中国剩余定理  | 在适当条件下把明文环分解成多个并行数据槽位。  |
| 多项式变形   | 改写计算电路，减少串行乘法深度。        |

学习本章不需要先掌握 Galois 理论或同调代数。群、商结构、环和多项式已经能解释许多关键规则；继续理解安全证明，则需要概率、计算复杂性（computational complexity）以及相应的数论或格理论（lattice theory）。

练习 12

答案 →

使用本章的 Paillier 小参数与  $c_1 = 173, c_2 = 169$ ，计算  $c_1^2 c_2 \bmod 225$  并解密。它对应哪个明文表达式？为什么结果不是普通整数 15？仅使用这些加法同态规则，能否从  $c_1, c_2$  得到两个隐藏值之积的密文？

练习 12 · 电路

答案 →

用加法、乘法和公开常数计算  $f(x) = (x^2 + 1)^2$ ，写出一种乘法深度为 2 的计算顺序。若采用模 17 的精确明文运算， $x = 3$  时解密结果是什么？换成 CKKS 后，应怎样描述正确性？

### 13. 推荐学习顺序

1. 集合、映射、等价关系、商集。
2. 群：子群、陪集、正规子群、商群、同态、群作用。
3. 环：理想、商环、整环、PID、UFD、多项式环。
4. 模：子模、商模、自由模、有限生成模、正合列。
5. 域：域扩张、代数元、最小多项式、分裂域、有限域。
6. Galois 理论：Galois 群、基本定理、根式可解。
7. 后续方向：表示论、交换代数、同调代数、代数数论、代数几何。
8. 应用专题：读过群、环与商结构后，可结合第 12 章学习同态加密；先手算 Paillier，再理解电路、噪声与自举。

学习时应该反复追问同一个问题：

- 这个结构的同态是什么？
- 核是什么？
- 商对象 (quotient object) 是什么？
- 同构定理是什么？

在群、环、模中反复回答这些问题，可以建立统一主线。进入域论后，要进一步追问：元素的最小多项式是什么？扩张次数是多少？自同构能把根送到哪里？

### 13.1. 分阶段检验掌握程度

- 第一阶段：能亲手列出小群的陪集、求同态的核，并解释商运算为什么良定义。
- 第二阶段：能在剩余类环中求逆元，判断多项式商环是否为域，分辨有限生成模与自由模。
- 第三阶段：能计算简单代数扩张的次数，并在二次或双二次扩张 (biquadratic extension) 中写出 Galois 对应 (Galois correspondence)。
- 第四阶段：能把一个具体问题翻译成表示、局部化或链复形，再完成一次小规模计算。

建议每学完一个定义就手算一个例子，每用一次定理就明确检查假设。若某一章练习无法独立完成，优先回到相关定义和例子，而不是只记住答案中的公式。

#### 练习 13

答案 →

用“不可约多项式 → 商环 → 域扩张 → 自同构”的顺序说明  $\mathbb{Q}[x]/(x^2 - 5)$ ：它为什么是域？在  $\mathbb{Q}$  上的维数是多少？它的  $\mathbb{Q}$ -自同构有哪些？

## 练习参考答案

这里按正文的章序给出答案和关键步骤。各题的“返回题目”链接可以回到原章末尾。

### 第 1 章：取余映射

$\pi(8) = \bar{2}$ ；核为所有 3 的倍数，即  $\text{Ker}(\pi) = 3\mathbb{Z}$ ；像是全部  $\mathbb{Z}/3\mathbb{Z}$ 。由于  $\pi(0) = \pi(3)$ ，它不是单射。三个剩余类分别由 0、1、2 映到，因此它是满射。

核记录哪些元素被映到零；任意两个整数的像相同，当且仅当它们的差在核中。

[← 返回第 1 章题目](#)

### 第 1 章补充：从冗余恢复数据

所有计算按模 5 进行。由  $q = a + 2b$ ，得  $2b = 1 - 3 = -2 \equiv 3 \pmod{5}$ 。因为  $2 \cdot 3 \equiv 1 \pmod{5}$ ，2 的逆元是 3，两边乘以 3 得  $b \equiv 9 \equiv 4 \pmod{5}$ 。

于是  $p = a + b \equiv 3 + 4 \equiv 2 \pmod{5}$ 。检验： $q = 3 + 2 \cdot 4 \equiv 1 \pmod{5}$ 。这里的“除以 2”是乘以模 5 意义下的逆元，不是对整数做截断除法。

[← 返回工程练习](#)

### 第 2 章：代表元与良定义

$[3] + [2] = [5] = [1]$ 。换用代表元后， $[7] + [6] = [13] = [1]$ 。因为  $7 - 3 = 4$ 、 $6 - 2 = 4$ ，两次和相差 8，是 4 的倍数，所以属于同一剩余类。

这一题不仅是在算余数，还验证了在商集上定义加法时，结果不依赖代表元。

[← 返回第 2 章题目](#)

### 第 3 章：循环群的商

$H = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ 。不同的陪集只有  $H$  和  $\bar{1} + H = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ 。因为  $G$  是 Abel 群， $H$  正规，所以商群有定义。

商群的阶为  $8/4 = 2$ ，因此  $G/H \cong \mathbb{Z}/2\mathbb{Z}$ 。也可以考虑从模 8 剩余类取奇偶性的满同态 (surjective homomorphism)，其核恰好为  $H$ ，再应用同构定理。

[← 返回第 3 章题目](#)

### 第 3 章补充：逆置换与准备操作

当前状态对应  $p$ 。再执行两次  $P$ ，总效果为  $p^2 \circ p = p^3 = e$ ，所以还需两次；再做一次只到  $p^2$ ，并未还原。

复用算法时执行  $S P S'$ ，即先准备、再执行局部转法、最后撤销准备。按映射从右到左复合的约定，总效果是  $s^{-1}ps$ 。如果需要的是逆向局部操作，则把中间一步换成  $P'$ ，执行  $S P' S'$ 。准备操作必须把目标块的位置和朝向都送到算法适用的状态。

[← 返回魔方练习](#)

### 第 4 章：单位与商环

与 12 互素的剩余类是  $\bar{1}, \bar{5}, \bar{7}, \bar{11}$ ，所以单位恰好是这四个。它们的平方都等于  $\bar{1}$ ，各自的逆元都是自身。

$I = (\bar{4}) = \{\bar{0}, \bar{4}, \bar{8}\}$ 。从模 12 取模 4 的满同态以  $I$  为核，因此  $R/I \cong \mathbb{Z}/4\mathbb{Z}$ 。后者有非零元素  $\bar{2}$  满足  $\bar{2}^2 = \bar{0}$ ，所以不是域，甚至不是整环。

[← 返回第 4 章题目](#)

## 第 5 章：有限生成不等于自由

$\bar{1}$  是一个生成元，因为任何剩余类都是它的整数倍。模中  $\bar{1} \neq 0$ ，但  $6\bar{1} = 0$ ，所以它有非零扭元。而自由  $\mathbb{Z}$ -模中，一个非零整数乘以非零向量不会得到零，因此  $M$  不自由。

$2\bar{a} = 0$  等价于  $6 \mid 2a$ ，也就是  $3 \mid a$ 。模 6 中的解为  $\bar{0}$  与  $\bar{3}$ 。

[← 返回第 5 章题目](#)

## 第 6 章：构造四元域

在  $\mathbb{F}_2$  中， $x^2 + x + 1$  代入 0、1 都得到 1，所以没有根。它是二次多项式，因此不可约，其生成的理想极大，商环是域。

每个剩余类有唯一的次数小于 2 的代表元，所以  $K = \{0, 1, \alpha, 1 + \alpha\}$ 。由  $\alpha^2 + \alpha + 1 = 0$ ，且特征为 2，得到：

$$\alpha^2 = \alpha + 1, \quad \alpha(\alpha + 1) = \alpha^2 + \alpha = 1 \quad (173)$$

因此  $\alpha^{-1} = \alpha + 1$ 。特别注意：这里  $1 + 1 = 0$ ，与  $\mathbb{Z}/4\mathbb{Z}$  中的运算不同。

[← 返回第 6 章题目](#)

## 第 7 章：双二次扩张的固定域

$K$  是  $(x^2 - 2)(x^2 - 3)$  在  $\mathbb{Q}$  上的分裂域，且特征为 0，所以是 Galois 扩张。两个平方根必须分别映到自身或其相反数，候选只有四种；由 Galois 群阶为扩张次数 4 可知，四种都确实出现：

$$(\sqrt{2}, \sqrt{3}) \mapsto (\sqrt{2}, \sqrt{3}), (-\sqrt{2}, \sqrt{3}), (\sqrt{2}, -\sqrt{3}), (-\sqrt{2}, -\sqrt{3}) \quad (174)$$

每个元素唯一写成  $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ ，其中系数均在  $\mathbb{Q}$  中。同时改变两个符号后，它变成  $a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$ 。固定条件恰好为  $b = c = 0$ ，所以固定域为  $\mathbb{Q}(\sqrt{6})$ 。

[← 返回第 7 章题目](#)

## 第 8 章：交换坐标的表示

令  $V_+ = \mathbb{C}(1, 1)$ 、 $V_- = \mathbb{C}(1, -1)$ ，则  $s$  分别在它们上作用为乘以 1 和乘以  $-1$ 。由于这两个向量线性无关（linearly independent）， $\mathbb{C}^2 = V_+ \oplus V_-$ ，即平凡表示（trivial representation）与符号表示（sign representation）的直和。

恒等元（identity element）的矩阵为二维单位阵（identity matrix），所以  $\chi(e) = 2$ 。交换坐标的矩阵对角元（diagonal entry）均为零，所以  $\chi(s) = 0$ ；也可由分解计算  $1 + (-1) = 0$ 。

[← 返回第 8 章题目](#)

## 第 9 章：局部化中的可逆性

$2/5$  是单位，逆元为  $5/2$ ，后者的分母不被 3 整除。 $3/5$  不是单位，因为它在  $\mathbb{Q}$  中唯一的逆元是  $5/3$ ，而这个有理数不能写成分母不被 3 整除的形式。

同理，若  $1/3 = a/b$  且 3 不整除  $b$ ，则  $b = 3a$ ，矛盾。因此  $1/3$  不在该局部环中。局部化只让指定乘法闭集里的元素变为可逆，并不是允许所有分母。

[← 返回第 9 章题目](#)

## 第 10 章：一次同调计算

原复形中,  $d_1: \mathbb{Z} \rightarrow \mathbb{Z}$  是乘以 2, 核为零;  $d_0$  的目标是零模 (zero module), 所以核是全部  $\mathbb{Z}$ 。于是:

$$H_1 = 0, \quad H_0 = \mathbb{Z}/2\mathbb{Z} \quad (175)$$

张量后两个非零项都变为  $\mathbb{Z}/2\mathbb{Z}$ , 中间的微分 (differential) 为零。因而新的同调为:

$$H_1 = \mathbb{Z}/2\mathbb{Z}, \quad H_0 = \mathbb{Z}/2\mathbb{Z} \quad (176)$$

新出现的  $H_1$  正是  $\text{Tor}_1^{\mathbb{Z}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})}$ 。这个例子说明, 不能假定“先求同调再张量”和“先张量再求同调”总得到相同结果。

[← 返回第 10 章题目](#)

## 第 11 章：抛物线的坐标环

因为  $\varphi(x) = t$ , 任意  $k[t]$  中的多项式都在像中, 故  $\text{Im}(\varphi) = k[t]$ 。显然  $\varphi(y - x^2) = 0$ , 所以  $(y - x^2) \subseteq \text{Ker}(\varphi)$ 。

反过来, 把  $f(x, y)$  按  $y$  除以首一多项式  $y - x^2$ , 得到  $f = q(x, y)(y - x^2) + r(x)$ 。若  $\varphi(f) = 0$ , 则  $r(t) = 0$  是零多项式 (zero polynomial), 故  $r = 0$ , 从而  $f \in (y - x^2)$ 。所以:

$$\text{Ker}(\varphi) = (y - x^2), \quad k[x, y]/(y - x^2) \cong k[t] \quad (177)$$

这里的  $t$  是不定元 (indeterminate),  $r(t) = 0$  表示多项式本身为零, 不是仅在若干点取值为零; 因此论证对有限域也成立。

[← 返回第 11 章题目](#)

## 第 12 章：密文加权和

服务器计算  $173^2 \cdot 169 \bmod 225 = 1$ , 解密得到  $L(1^4 \bmod 225) \cdot 4 \bmod 15 = 0$ 。

密文乘法对应明文加法, 密文的平方对应明文乘以公开常数 2, 因此它表示  $2 \cdot 4 + 7 = 15 \equiv 0 \bmod 15$ 。结果为 0 是明文空间的模运算规则, 并非解密失败。

仅用这些规则只能组合出公开系数的线性表达式, 不能一般地计算两个隐藏值的乘积。如果已经知道明文 4 与 7, 当然可以直接加密它们的乘积; 那没有实现未知明文之间的同态乘法。

[← 返回第 12 章题目](#)

## 第 12 章补充：乘法深度与结果语义

依次计算  $u = x^2$ 、 $v = u + 1$ 、 $w = v^2$ 。两次平方依次依赖, 乘法深度为 2; 中间加 1 不增加乘法深度。

当  $x = 3$  时, 普通整数结果是  $(9 + 1)^2 = 100$ , 模 17 的结果为 15。在参数足够的精确方案中, 应当解密得到 15。

CKKS 的目标则是在所选编码、尺度和精度条件下得到接近 100 的结果, 并满足约定的误差容限; 不能把它的默认计算语义理解为模 17 的运算, 也不能要求精确相等。

[← 返回电路练习](#)

### 第 13 章：串起代数主线

$x^2 - 5$  由 Eisenstein 判别法（取素数 5）在  $\mathbb{Q}$  上不可约，因此  $(x^2 - 5)$  为极大理想，商环是域。

记  $\alpha = \bar{x}$ ，则  $\alpha^2 = 5$ ，每个元素唯一写成  $a + b\alpha$ ，所以  $1, \alpha$  是一组基，维数为 2。映射  $\alpha \mapsto \sqrt{5}$  给出商域与  $\mathbb{Q}(\sqrt{5})$  的同构。

保持  $\mathbb{Q}$  不动的自同构必须把  $\alpha$  送到  $x^2 - 5$  的根，因此只有恒等映射和  $a + b\alpha \mapsto a - b\alpha$  两个。它们组成阶为 2 的循环群，也验证了该 Galois 群的阶等于扩张次数。

[← 返回第 13 章题目](#)

## 中英术语对照表

汇总正文中的术语，按英文名称排序，便于查阅。

| 中文术语   | 英文                                |
|--------|-----------------------------------|
| 三循环    | 3-cycle                           |
| 四循环    | 4-cycle                           |
| Abel 群 | abelian group                     |
| 抽象代数   | abstract algebra                  |
| 加法群    | additive group                    |
| 加法逆元   | additive inverse                  |
| 加法同态加密 | additively homomorphic encryption |
| 仿射代数簇  | affine algebraic variety          |
| 代数     | algebra                           |
| 代数闭包   | algebraic closure                 |
| 代数元    | algebraic element                 |
| 代数扩张   | algebraic extension               |
| 代数几何   | algebraic geometry                |
| 代数数论   | algebraic number theory           |
| 代数结构   | algebraic structure               |
| 代数拓扑   | algebraic topology                |
| 代数闭域   | algebraically closed field        |
| 近似运算   | approximate arithmetic            |
| 算术电路   | arithmetic circuit                |
| 理想升链   | ascending chain of ideals         |
| 相伴     | association                       |
| 结合律    | associativity                     |
| 自同构    | automorphism                      |
| 自同构群   | automorphism group                |
| 公理     | axiom                             |
| 基域     | base field                        |
| 基      | basis                             |
| 基向量    | basis vector                      |
| 批处理    | batching                          |
| 双射     | bijection                         |
| 双线性映射  | bilinear map                      |
| 二元运算   | binary operation                  |
| 双二次扩张  | biquadratic extension             |

| 中文术语        | 英文                        |
|-------------|---------------------------|
| 布尔电路        | Boolean circuit           |
| 自举          | bootstrapping             |
| 边界          | boundary                  |
| Burnside 引理 | Burnside' s lemma         |
| Bézout 等式   | Bézout' s identity        |
| 消去律         | cancellation law          |
| Cauchy 定理   | Cauchy' s theorem         |
| 链复形         | chain complex             |
| 特征标         | character                 |
| 特征          | characteristic            |
| 中国剩余定理      | Chinese remainder theorem |
| 密文          | ciphertext                |
| 密文模数        | ciphertext modulus        |
| 电路隐私        | circuit privacy           |
| 闭集          | closed set                |
| 码字          | codeword                  |
| 系数          | coefficient               |
| 上同调         | cohomology                |
| 交换代数        | commutative algebra       |
| 交换环         | commutative ring          |
| 交换律         | commutativity             |
| 交换子         | commutator                |
| 紧致性         | compactness               |
| 完全可约        | completely reducible      |
| 复形          | complex                   |
| 复数          | complex number            |
| 复表示         | complex representation    |
| 复合映射        | composite map             |
| 复合          | composition               |
| 计算复杂性       | computational complexity  |
| 保密性         | confidentiality           |
| 共轭类         | conjugacy class           |
| 共轭          | conjugation               |
| 逆命题         | converse                  |
| 坐标          | coordinate                |

| 中文术语           | 英文                        |
|----------------|---------------------------|
| 坐标环            | coordinate ring           |
| 坐标系            | coordinate system         |
| 坐标变换           | coordinate transformation |
| 互素             | coprime                   |
| 正确性            | correctness               |
| 陪集             | coset                     |
| 三次单位根          | cube root of unity        |
| 循环             | cycle                     |
| 循环群            | cyclic group              |
| 次数             | degree                    |
| 扩张次数           | degree of an extension    |
| 派生函子           | derived functor           |
| 对角元            | diagonal entry            |
| 微分             | differential              |
| 维数             | dimension                 |
| 直积             | direct product            |
| 直和             | direct sum                |
| 分配律            | distributivity            |
| 整除             | divisibility              |
| 带余除法           | division with remainder   |
| 特征子空间          | eigenspace                |
| 特征值            | eigenvalue                |
| Eisenstein 判别法 | Eisenstein' s criterion   |
| 嵌入             | embedding                 |
| 自同态            | endomorphism              |
| 等势             | equinumerosity            |
| 等价类            | equivalence class         |
| 等价关系           | equivalence relation      |
| 擦除恢复           | erasure recovery          |
| Euclidean 整环   | Euclidean domain          |
| 求值密钥           | evaluation key            |
| 求值映射           | evaluation map            |
| 正合列            | exact sequence            |
| 正合性            | exactness                 |
| 扩张域            | extension field           |

| 中文术语        | 英文                                        |
|-------------|-------------------------------------------|
| 因式分解        | factorization                             |
| 域           | field                                     |
| 域自同构        | field automorphism                        |
| 域扩张         | field extension                           |
| 域论          | field theory                              |
| 五次单位根       | fifth root of unity                       |
| 有限扩张        | finite extension                          |
| 有限域         | finite field                              |
| 有限群         | finite group                              |
| 有限秩         | finite rank                               |
| 有限生成        | finitely generated                        |
| 有限生成模       | finitely generated module                 |
| 固定域         | fixed field                               |
| 形式导数        | formal derivative                         |
| 自由模         | free module                               |
| 自由分解        | free resolution                           |
| 全同态加密       | fully homomorphic encryption, FHE         |
| 函子          | functor                                   |
| 同态基本定理      | fundamental homomorphism theorem          |
| Galois 基本定理 | fundamental theorem of Galois theory      |
| 环同态基本定理     | fundamental theorem of ring homomorphisms |
| Galois 对应   | Galois correspondence                     |
| Galois 扩张   | Galois extension                          |
| Galois 群    | Galois group                              |
| Galois 理论   | Galois theory                             |
| 高斯消元        | Gaussian elimination                      |
| 生成元         | generator                                 |
| 最大公因子       | greatest common divisor, GCD              |
| 群           | group                                     |
| 群作用         | group action                              |
| 群代数         | group algebra                             |
| 群同态         | group homomorphism                        |
| 群表示         | group representation                      |
| 群论          | group theory                              |
| Hilbert 基定理 | Hilbert' s basis theorem                  |

| 中文术语    | 英文                                |
|---------|-----------------------------------|
| 齐次矩阵    | homogeneous matrix                |
| 齐次变换矩阵  | homogeneous transformation matrix |
| 同调代数    | homological algebra               |
| 同调      | homology                          |
| 同调群     | homology group                    |
| 同态加密    | homomorphic encryption, HE        |
| 同态求值    | homomorphic evaluation            |
| 同态      | homomorphism                      |
| 理想      | ideal                             |
| 理想分解    | ideal factorization               |
| 单位元、恒等元 | identity element                  |
| 恒等映射    | identity map                      |
| 单位阵     | identity matrix                   |
| 像       | image                             |
| 虚数单位    | imaginary unit                    |
| 不定元     | indeterminate                     |
| 单射      | injection                         |
| 内积      | inner product                     |
| 整数      | integer                           |
| 整环      | integral domain                   |
| 中间域     | intermediate field                |
| 不变量     | invariant                         |
| 不变因子    | invariant factor                  |
| 不变子空间   | invariant subspace                |
| 逆元      | inverse element                   |
| 逆映射     | inverse map                       |
| 逆置换     | inverse permutation               |
| 逆变换     | inverse transformation            |
| 可逆元     | invertible element                |
| 不可约元    | irreducible element               |
| 不可约因子   | irreducible factor                |
| 不可约多项式  | irreducible polynomial            |
| 不可约表示   | irreducible representation        |
| 不可约子表示  | irreducible subrepresentation     |
| 同构      | isomorphism                       |

| 中文术语        | 英文                                   |
|-------------|--------------------------------------|
| 同构定理        | isomorphism theorem                  |
| Jordan 标准形  | Jordan canonical form                |
| 核           | kernel                               |
| Lagrange 定理 | Lagrange' s theorem                  |
| 格点          | lattice point                        |
| 格理论         | lattice theory                       |
| 左陪集         | left coset                           |
| 左正合         | left exact                           |
| 左理想         | left ideal                           |
| 分层全同态加密     | leveled fully homomorphic encryption |
| 线性代数        | linear algebra                       |
| 线性组合        | linear combination                   |
| 线性方程        | linear equation                      |
| 线性延拓        | linear extension                     |
| 线性映射        | linear map                           |
| 线性算子        | linear operator                      |
| 线性空间        | linear space                         |
| 线性变换        | linear transformation                |
| 线性无关        | linearly independent                 |
| 局部环         | local ring                           |
| 局部化         | localization                         |
| 可塑性         | malleability                         |
| 映射          | map                                  |
| Maschke 定理  | Maschke' s theorem                   |
| 矩阵          | matrix                               |
| 矩阵环         | matrix ring                          |
| 矩阵相似        | matrix similarity                    |
| 极大理想        | maximal ideal                        |
| 最小多项式       | minimal polynomial                   |
| 模回绕         | modular wraparound                   |
| 模           | module                               |
| 模同态         | module homomorphism                  |
| 模论          | module theory                        |
| 首一多项式       | monic polynomial                     |
| 么半群         | monoid                               |

| 中文术语        | 英文                                    |
|-------------|---------------------------------------|
| 乘法深度        | multiplicative depth                  |
| 乘法群         | multiplicative group                  |
| 乘法逆元        | multiplicative inverse                |
| 乘法闭集        | multiplicative set                    |
| 自然映射        | natural map                           |
| Noether 条件  | Noetherian condition                  |
| Noether 环   | Noetherian ring                       |
| 噪声预算        | noise budget                          |
| 非交换环        | noncommutative ring                   |
| 非零多项式       | nonzero polynomial                    |
| 正规扩张        | normal extension                      |
| 正规子群        | normal subgroup                       |
| 数域          | number field                          |
| 数论          | number theory                         |
| 奇置换         | odd permutation                       |
| 轨道          | orbit                                 |
| 轨道-稳定子定理    | orbit-stabilizer theorem              |
| 阶           | order                                 |
| 元素阶         | order of an element                   |
| 正交关系        | orthogonality relations               |
| Paillier 加密 | Paillier encryption                   |
| 抛物线         | parabola                              |
| 奇偶性         | parity                                |
| 校验位         | parity bit                            |
| 部分同态加密      | partially homomorphic encryption, PHE |
| 置换          | permutation                           |
| 置换群         | permutation group                     |
| 明文          | plaintext                             |
| 明文模数        | plaintext modulus                     |
| 多项式         | polynomial                            |
| 多项式方程       | polynomial equation                   |
| 多项式商环       | polynomial quotient ring              |
| 多项式环        | polynomial ring                       |
| 素域          | prime field                           |
| 素理想         | prime ideal                           |

| 中文术语           | 英文                                     |
|----------------|----------------------------------------|
| 素数             | prime number                           |
| 素谱             | prime spectrum                         |
| 本原整系数多项式       | primitive polynomial over the integers |
| 主理想            | principal ideal                        |
| 主理想整环          | principal ideal domain, PID            |
| 投影             | projection                             |
| 真理想            | proper ideal                           |
| 公钥             | public key                             |
| 公钥加密           | public-key encryption                  |
| 拉回             | pullback                               |
| 二次方程           | quadratic equation                     |
| 求根公式           | quadratic formula                      |
| 五次方程           | quintic equation                       |
| 商群             | quotient group                         |
| 商模             | quotient module                        |
| 商对象            | quotient object                        |
| 商域             | quotient of a field                    |
| 商环             | quotient ring                          |
| 商集             | quotient set                           |
| 商结构            | quotient structure                     |
| 根式公式           | radical formula                        |
| 随机化加密          | randomized encryption                  |
| 有理标准形          | rational canonical form                |
| 有理数            | rational number                        |
| 实数             | real number                            |
| 实根             | real root                              |
| Reed–Solomon 码 | Reed–Solomon code                      |
| 自反性            | reflexivity                            |
| 重线性化           | relinearization                        |
| 重根             | repeated root                          |
| 表示             | representation                         |
| 表示论            | representation theory                  |
| 代表元            | representative                         |
| 重缩放            | rescaling                              |
| 剩余类            | residue class                          |

| 中文术语      | 英文                                               |
|-----------|--------------------------------------------------|
| 剩余类环      | residue class ring                               |
| 右陪集       | right coset                                      |
| 右正合       | right exact                                      |
| 右理想       | right ideal                                      |
| 刚体变换      | rigid transformation                             |
| 环         | ring                                             |
| 环同态       | ring homomorphism                                |
| 环上带误差学习问题 | Ring Learning With Errors, RLWE                  |
| 代数整数环     | ring of algebraic integers                       |
| 函数环       | ring of functions                                |
| 整数环       | ring of integers                                 |
| 环论        | ring theory                                      |
| 根         | root                                             |
| 旋转        | rotation                                         |
| 魔方群       | Rubik' s Cube group                              |
| 标量        | scalar                                           |
| 标量乘法      | scalar multiplication                            |
| 缩放因子      | scaling factor                                   |
| 私钥        | secret key                                       |
| 截面        | section                                          |
| 半群        | semigroup                                        |
| 可分扩张      | separable extension                              |
| 集合        | set                                              |
| 短正合列      | short exact sequence                             |
| 符号表示      | sign representation                              |
| 解集        | solution set                                     |
| 根式可解性     | solvability by radicals                          |
| 根式可解      | solvable by radicals                             |
| 可解群       | solvable group                                   |
| 有限同态加密    | somewhat homomorphic encryption, SHE             |
| 分裂        | split                                            |
| 分裂扩张      | split extension                                  |
| 分裂域       | splitting field                                  |
| 稳定子       | stabilizer                                       |
| 有限生成模结构定理 | structure theorem for finitely generated modules |

| 中文术语       | 英文                                          |
|------------|---------------------------------------------|
| 子域         | subfield                                    |
| 子群         | subgroup                                    |
| 子群判别法      | subgroup criterion                          |
| 子模         | submodule                                   |
| 正规列        | subnormal series                            |
| 子表示        | subrepresentation                           |
| 子环         | subring                                     |
| 子集         | subset                                      |
| 子空间        | subspace                                    |
| 满射         | surjection                                  |
| 满同态        | surjective homomorphism                     |
| Sylow 子群   | Sylow subgroup                              |
| Sylow 定理   | Sylow theorems                              |
| 对称性        | symmetry                                    |
| 多元多项式方程组   | system of multivariate polynomial equations |
| 张量积        | tensor product                              |
| 扭元         | torsion element                             |
| 塔公式        | tower law                                   |
| 迹          | trace                                       |
| 超越元        | transcendental element                      |
| 传递性        | transitivity                                |
| 平移         | translation                                 |
| 换位         | transposition                               |
| 平凡表示       | trivial representation                      |
| 平凡子群       | trivial subgroup                            |
| 双边理想       | two-sided ideal                             |
| 唯一分解整环     | unique factorization domain, UFD            |
| 单位         | unit                                        |
| 一元多项式环     | univariate polynomial ring                  |
| 未知数        | unknown                                     |
| 向量         | vector                                      |
| 向量空间       | vector space                                |
| 加权和        | weighted sum                                |
| 良定义        | well-definedness                            |
| Zariski 拓扑 | Zariski topology                            |

| 中文术语 | 英文              |
|------|-----------------|
| 零因子  | zero divisor    |
| 零理想  | zero ideal      |
| 零映射  | zero map        |
| 零模   | zero module     |
| 零多项式 | zero polynomial |

## 13.2. TODO

bilibili 上还有很多东西可以看看的: <https://www.bilibili.com/list/ml85366172> <https://www.bilibili.com/video/BV1sb411b7T6>

这个短片做的太好了 【已吓哭 opus5.5 真神降临 群论之美宣传片】 [https://www.bilibili.com/video/BV12Zhm6oE6m/?share\\_source=copy\\_web&vd\\_source=42e22c6b2f211ee75c7e2c895faf3c2a](https://www.bilibili.com/video/BV12Zhm6oE6m/?share_source=copy_web&vd_source=42e22c6b2f211ee75c7e2c895faf3c2a)

<https://news.ycombinator.com/item?id=41255456>