关于本笔记 (About This Notebook)

1. 缘起与致谢 (Origin & Acknowledgments)

本笔记的内容核心整理自 **王崧 (Song Wang)** 老师讲授的《代数》课程。王崧老师的课程以其深刻的洞察力和严谨的结构著称，本笔记旨在记录并消化这些宝贵的教学内容。

2. 整理理念 (Philosophy)

这并非一份逐字逐句的课堂速记，而是一次对代数知识体系的**重构 (Reconstruction)**。在整理过程中，我们遵循以下核心原则：

- **重构逻辑顺序**：打破线性的记录方式，将相关联的知识点（如群、环、域的构造逻辑）进行串联与对比，突显代数结构的内在联系。
- **强化直观理解**：代数往往被认为是抽象的，因此本笔记特别引入了更多的几何直观、物理比喻以及具体算例，试图在形式化的定义背后建立起感性的认知图景。
- **突出思想方法**：不只关注定理的证明细节，更关注证明背后的策略（如商集构造法、归纳法、反证法等）及其普适性。

3. 免责声明 (Disclaimer)

本笔记的整理与润色工作由 AI 助手 **Gemini 3.0 Pro** 辅助完成。虽然我们尽力确保内容的准确性与逻辑的通顺，但 AI 生成内容可能在数学严谨性、术语规范或特殊符号处理上存在疏漏或偏差。**请读者在使用时保持批判性思维，一切定义与定理以标准教材或原始课程内容为准。**

Chapter 0: 引言与基础 (Introduction & Preliminaries)

阅读说明 (Reading Guide)

意图与目标

本章并非对中学数学的简单回顾，而是用**代数 (Algebra)** 的眼光重新审视我们熟悉的“数”。在代数学中，我们关注的不再是具体的计算（如 $1+2=3$），而是对象背后的**结构 (Structure)** 与**公理 (Axioms)**。

章节结构逻辑

本章遵循“数系扩张”的历史与逻辑脉络：

1. **起点 ($\mathbb{N}$)**：通过皮亚诺公理确立“计数”的结构。
2. **扩张 ($\mathbb{Z}, \mathbb{Q}$)**：为了解决减法与除法的封闭性，引入环与域的概念，通过构造商集来扩张数系。
3. **终点 ($\mathbb{R}$)**：为了解决度量的完备性（填补数轴空隙），引入实数公理体系。

使用建议

- 关注**“直观理解”**板块，尝试建立几何或物理图像。
- 注意 $\mathbb{N}_0$ 与 $\mathbb{N}_1$ 的区别，这对后续群论中单位元的讨论至关重要。
- 重点理解**商集构造法**，这是代数中构造新对象的通用手段。

Lecture 1: 数 系 的 构 建 与 层 级

1 数学的图谱与数系阶梯 (The Map & Hierarchy)

代数并非孤立存在。从宏观图谱来看，数学源于人类对**数 (Numbers)** 与**形 (Geometry)** 的原始直觉。随着抽象程度的加深，**算术 (Arithmetics)** 演化为研究结构的**代数 (Algebra)**，而对形与度量的研究在引入极限后演化为**分析 (Analysis)**。

我们在代数课程中主要处理以下数系对象。理解它们的包含关系与结构差异是后续学习的基础：

符号	名称	集合定义	代数特征简述
$\mathbb{N}_1$	正整数	$\{1, 2, 3, \dots\}$	封闭于加法、乘法，无单位元 (加法)
$\mathbb{N}_0$	自然数	$\{0, 1, 2, \dots\}$	引入单位元 0，形成幺半群
$\mathbb{Z}$	整数	$\{\dots, -1, 0, 1, \dots\}$	**环 (Ring)**：加法可逆
$\mathbb{Q}$	有理数	$\{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$	**域 (Field)**：乘法可逆 (非零)
$\mathbb{R}$	实数	对应连续数轴	**完备域**：填补了所有缝隙
$\mathbb{C}$	复数	$\{a + bi\}$	代数闭域

2 起点：自然数的结构 ($\mathbb{N}$)

自然数是整个数学大厦的地基。在现代数学中，我们不通过“数苹果”来定义它，而是使用**皮亚诺公理 (Peano Axioms)** 从结构上刻画它。

2.1 结构的公理化

一个集合要被称为自然数集 $\mathbb{N}_1$，必须拥有一个起始点 1 和一个**后继映射 (Successor Map)** $a \mapsto a^+$。这个结构必须满足三个核心公理：

1. **起始性**：1 不是任何数的后继（链条有起点）。
2. **单射性**：$a^+ = b^+ \implies a = b$（链条不汇合）。
3. **归纳性**：这是自然数的灵魂。若一个性质对 1 成立，且由 n 成立可推得 n^+ 成立，则该性质对所有自然数成立。这保证了链条没有断裂，也没有“飞地”。

2.2 运算的递归定义与性质

在公理基础上，加法与乘法不再是理所当然的，而是通过**递归 (Recursion)** 定义的：

- **加法**：定义 $a + 1 = a^+$，并规定 $a + (b^+) = (a + b)^+$。
- **乘法**：定义 $a \cdot 1 = a$，并规定 $a \cdot (b^+) = a \cdot b + a$。

基于这些定义，我们可以证明加法与乘法满足**交换律**、**结合律**以及**分配律**。同时，我们定义了严格序关系 $a < b \iff \exists k, b = a + k$。

直观理解：最小数原理

$\mathbb{N}$ 的序结构有一个极强的性质：**最小数原理 (Well-Ordering Principle)**——自然数的任意非空子集必有最小元。这等价于数学归纳法。想象一下，如果在自然数里往回走（$5, 4, 3 \ldots$），你必然会在有限步内停下来，不可能无限倒退。

3 扩张：从 $\mathbb{Z}$ 到 $\mathbb{Q}$ (Construction of Rings & Fields)

自然数虽然美好，但它在运算上是“残缺”的。代数的发展史，就是一部为了让运算**封闭**而不断扩张数系的历史。

3.1 整数环 $\mathbb{Z}$：修补减法

在 $\mathbb{N}$ 中，方程 $x + 5 = 3$ 无解。为了修补这个缺陷（引入加法逆元），我们构造了整数。

- **构造方法：**在 $\mathbb{N}_0 \times \mathbb{N}_0$ 上定义等价关系 $(a, b) \sim (c, d) \iff a + d = b + c$。每一类 $[(a, b)]$ 代表一个整数 $a - b$。
- **代数结构：**$\mathbb{Z}$ 构成了一个**整环 (Integral Domain)**。
  - 它有加法单位元 0 和逆元 $-a$。
  - 它满足**消去律**：$ab = ac, a \neq 0 \implies b = c$（即无零因子）。
  - **核心性质：**虽然 $\mathbb{Z}$ 没有除法，但它有**带余除法**和**算术基本定理**（唯一分解定理），这是初等数论的基石。

3.2 有理数域 $\mathbb{Q}$：修补除法

在 $\mathbb{Z}$ 中，方程 $2x = 3$ 无解。为了修补这个缺陷（引入乘法逆元），我们构造了有理数。

- **构造方法：**在 $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ 上定义等价关系，本质上是分数的相等定义。
- **代数结构：**$\mathbb{Q}$ 构成了一个**域 (Field)**。
  - 域是代数运算极其完美的结构，非零元素均可逆。
  - $\mathbb{Q}$ 也是**有序域**，保持了大小关系的相容性。

NOTE: 通用构造法 (Quotient Construction)

这种“缺什么补什么”并在集合对上定义等价关系的方法，是代数中构造**商群**、**商环**、**分式域**的原型。

4 终章：实数与完备性 ($\mathbb{R}$)

尽管 $\mathbb{Q}$ 在代数运算上已经很完美，但它在几何度量上有一个致命的漏洞：**不连续**。第一次数学危机（$\sqrt{2}$ 的发现）揭示了数轴上布满了有理数无法覆盖的“孔隙”。为了填补这些孔隙，我们需要引入实数。

4.1 卓里奇四条 (Zorich's 4 Conditions)

王崧老师引用俄罗斯教材体系（V.A. Zorich），给出了实数 $\mathbb{R}$ 的公理化定义。一个集合若满足以下四组公理，即为实数集：

1. **域公理 (Field Axioms)**：保证四则运算的封闭性（继承自 $\mathbb{Q}$）。
2. **序公理 (Order Axioms)**：保证全序关系（继承自 $\mathbb{Q}$）。
3. **阿基米德公理 (Archimedean Property)**：

   $$\forall x > 0, y \in \mathbb{R}, \exists n \in \mathbb{N}, nx > y$$

   这排除了“无穷小量”的存在，连接了有限与无限。
4. **完备性公理 (Completeness)**：这是 $\mathbb{R}$ 区别于 $\mathbb{Q}$ 的核心。它有多种等价表述，如**柯西收敛准则**（柯西列必收敛）或**确界原理**（有上界必有上确界）。

4.2 为什么需要完备性？

完备性是分析学（微积分）赖以生存的基础。

- 在 $\mathbb{Q}$ 中，你可以构造一个数列 $1, 1.4, 1.41, 1.414\ldots$，它的项都在 $\mathbb{Q}$ 中，且越来越“挤”（柯西列），但它最终指向的目标 $\sqrt{2}$ 却掉进了“虚空”。
- **完备性**保证了所有这样的数列最终都能在 $\mathbb{R}$ 中找到落脚点。

术语百科 (Terminology)

卓四条 (Zhuō Sì Tiáo)

Source: V.A. Zorich, "Mathematical Analysis"

这是课程中对实数公理化体系的课堂简称。这一称呼强调了从**公理化** (Axiomatic) 角度而非**构造性** (Constructive，如戴德金分割) 角度来理解实数。它由域、序、阿基米德性、完备性四个维度组成，是现代分析学的标准起点。

Lecture 2: 复数、群论初步与环域分类

5 最终的扩张：复数域 ($\mathbb{C}$)

数系的最后一次飞跃，是为了解决代数方程的求根问题。虽然实数 $\mathbb{R}$ 填满了数轴，但像 $x^2+1=0$ 这样的简单方程在 $\mathbb{R}$ 中依然无解。

5.1 定义与运算 (Definition & Operations)

我们将复数定义为实数的扩充，引入虚数单位 i（满足 $i^2=-1$）。

- **集合定义：** $\mathbb{C}=\{a+bi \mid a,b\in\mathbb{R}\}$
- **域扩张符号：** $\mathbb{C}=\mathbb{R}[i]$ （意为在 $\mathbb{R}$ 中添加元素 i 生成的扩域）。

在 $\mathbb{C}$ 中，运算规则如下：

1. **加法：** $(a+bi)+(c+di)=(a+c)+(b+d)i$
2. **乘法：** $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$
3. **嵌入：** $a\mapsto a+0i$ （实数是复数的子集，$\mathbb{R}\hookrightarrow\mathbb{C}$）。

直观理解：关键技巧：除法与共轭

为了证明 $\mathbb{C}$ 是一个域，我们需要找到非零元素的逆元。利用恒等式 $(a+bi)(a-bi)=a^2+b^2$（实数），我们可以将分母实数化：

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

这保证了除法的封闭性。

5.2 代数基本定理 (Fundamental Theorem of Algebra)

这是数系扩张的终点，也是代数学的里程碑。

NOTE: 定理内容

任何复系数多项式方程必有根。
推论：任何 n 次多项式方程在复数域中恰有 n 个根（计入重数）。

直观意义 (Intuition)：这被称为**代数闭域 (Algebraically Closed Field)**。这意味着我们不需要再为了解方程而去发明“超复数”了。数系的扩张到此为止，$\mathbb{C}$ 已经足够包容所有的代数运算。

习题 (Exercise) 整理代数基本定理的证明思路（通常利用复分析中的刘维尔定理或拓扑学方法证明）。

6 代数结构的抽象：从数系到群 (Abstraction: From Numbers to Groups)

核心线索：回顾我们将 $\mathbb{N}$ 扩充到 $\mathbb{Z}$ 的过程，本质上是为了让“减法”（即加法的逆运算）可行。当我们把这种“可逆的运算结构”提取出来，不关心它具体是整数还是矩阵，我们就得到了**群 (Group)**。

6.1 群的定义 (Definition of Groups)

根据板书 P9，群不仅仅是一个集合，它是一个**结构 (Structure)**，记作 $(G, *, e)$。它包含三个要素：

1. **集合** G：一堆对象。
2. **二元运算** $*$：$G \times G \to G$：一种将两个对象变成一个对象的方法。
3. **特殊元** e：一个“基准点”或“单位”。

要成为一个群，必须满足三条**公理 (Axioms)**：

- **结合律 (Associative Law)**：

$$(a * b) * c = a * (b * c)$$

(直观理解：运算的次序不重要，括号可以随意拆。)

- **单位元律 (Identity Law)**：

$$e * a = a * e = a$$

(直观理解：e 是“什么都不做”的操作，比如加法里的 0。)

- **逆元律 (Inverse Law)**：

$$\forall a \in G, \exists a^{-1}, \text{ 使得} a^{-1} * a = a * a^{-1} = e$$

(直观理解：任何操作都可以被“撤销”或“复原”。)

6.2 例子与反例 (Examples & Counter-examples)

板书 P10 通过我们刚刚构建的数系，清晰地划分了群与非群的界限。

是群 (Groups) 以下数系在**加法**运算下都构成群（且是交换群）：

- $(\mathbb{Z}, 0, +)$：整数加法群。
- $(\mathbb{Q}, 0, +)$：有理数加法群。
- $(\mathbb{R}, 0, +)$：实数加法群。
- $(\mathbb{C}, 0, +)$：复数加法群。

不是群 (Not Groups)

- $(\mathbb{N}_1, +)$：**不是群**。因为没有 0（缺单位元），也没有负数（缺逆元）。
- $(\mathbb{N}_0, 0, +)$：**不是群**。虽然有了单位元 0，但依然没有负数，无法满足逆元律。

6.3 结构的阶梯：半群与幺半群 (Semigroups & Monoids)

如果一个结构不满足群的所有条件，它叫什么？板书 P10 给出了精确的分类：

1. **半群 (Semigroup)**：$(\mathbb{N}_1, +)$

- 只满足：**封闭性 + 结合律**。
- 缺陷：没有单位元，无法“不动”；没有逆元，无法“回头”。

2. **幺半群 (Monoid)**：$(\mathbb{N}_0, 0, +)$
   - 满足：**封闭性 + 结合律 + 单位元**。
   - 缺陷：依然没有逆元。
3. **群 (Group)**：$(\mathbb{Z}, 0, +)$
   - 满足：**封闭性 + 结合律 + 单位元 + 逆元**。
   - 完美状态：运算完全可逆。

直观理解：术语：阿贝尔群 (Abelian Group)

板书最后指出，上述 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 不仅是群，还是**交换群**（Commutative Group），又称**阿贝尔群**。这意味着运算满足交换律：$a * b = b * a$。注意：交换律并非群定义的必要条件（如矩阵乘法不交换），但它是数系运算的普遍特征。

7 环与域：以 $\mathbb{Z}_n$ 为例 (Rings, Fields & Integers Modulo n)

核心线索：群 $(G, *)$ 只有一种运算。但我们熟悉的整数 $\mathbb{Z}$ 既能加也能乘。当我们把“加法群”和“乘法半群”通过分配律粘合在一起，就诞生了**环 (Ring)**。

7.1 环的定义与分类 (Ring Structure)

根据板书 P11，一个集合 R 如果配备了两种运算 $(+, \cdot)$ 以及两个特殊元 $0, 1$，满足以下条件，则称为**交换幺元环 (Commutative Unital Ring)**：

1. **加法结构：**$(R, 0, +)$ 是交换群（阿贝尔群）。
2. **乘法结构：**满足结合律、交换律、单位元 $1 \cdot a = a$。
3. **粘合剂：**分配律 $a(b + c) = ab + ac$。

推论：

- 0 是强吸附剂：$0 \cdot a = 0$。
- 符号规则：$(-1) \cdot a = -a$。

7.2 关键分野：整环 vs 域 (Integral Domain vs Field)

板书 P12 展示了两个看似相似但有本质区别的概念。这是代数学中关于“除法”的灵魂拷问：

概念	定义核心	直观理解
整环 (Integral Domain)	**无零因子：** $ab = 0 \implies a = 0 \vee b = 0$	不能随便除，但可以**消去**。若 $c \neq 0, ac = bc \implies a = b$。 例：$\mathbb{Z}$
域 (Field)	**可逆：** $\forall a \neq 0, \exists a^{-1}$	可以**除**。每个非零元素都有倒数。 例：$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

NOTE: 包含关系

所有的**域**都是**整环**（可逆必然蕴含无零因子），但反之不成立（整数环 $\mathbb{Z}$ 是整环但不是域）。

7.3 具体的例子：$\mathbb{Z}_n$ (Integers Modulo n)

板书 P13 引入了同余类的概念，这是构造有限环的标准方法。

- **定义：** 在 $\mathbb{Z}$ 上定义同余关系 $a \equiv b \pmod{n} \iff n \mid (a - b)$。
- **集合：** $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$。
- **运算：**
  - $[a] + [b] = [a + b]$
  - $[a] \cdot [b] = [ab]$

性质： $\mathbb{Z}_n$ 是一个交换幺元环。其加法群 $(\mathbb{Z}_n, +)$ 是 n 阶循环群 (Cyclic Group)。

7.4 $\mathbb{Z}_n$ 何时是域？(When is $\mathbb{Z}_n$ a Field?)

板书 P14 给出了一个极其漂亮的数论结论，连接了代数结构与素数分布。

NOTE: 定理 (The Classification of $\mathbb{Z}_n$)

对于 $n > 1$，以下命题等价：

1. $\mathbb{Z}_n$ 是域。
2. $\mathbb{Z}_n$ 是整环。
3. n 是**素数 (Prime)**。

证明直观 (Intuition)：

- **情形 1: n 是合数 ($n = ab$)**
  - 在 $\mathbb{Z}_n$ 中，$[a] \neq [0], [b] \neq [0]$，但 $[a] \cdot [b] = [n] = [0]$。
  - **结论：**存在零因子，所以不是整环，更不是域。
  - 例子：在 $\mathbb{Z}_6$ 中，$2 \cdot 3 = 6 \equiv 0$。你不能消去 2，也不能除以 2。
- **情形 2: n 是素数 ($n = p$)**
  - **无零因子：**p 是素数，所以 $p \mid ab \implies p \mid a$ 或 $p \mid b$。这意味着在 $\mathbb{Z}_p$ 中没有零因子。
  - **可逆性：**对于任意 $[a] \neq [0]$（即 $p \nmid a$），由贝祖定理 (Bezout's Identity)，存在 $u, v \in \mathbb{Z}$ 使得 $ua + vp = 1$。

$$\implies ua \equiv 1 \pmod{p} \implies [u] = [a]^{-1}$$

  - **结论：**$\mathbb{Z}_p$ 是域，通常记作 $\mathbb{F}_p$。

7.5 模 n 的乘法群 ($\mathbb{Z}_n^\times$)

即使 $\mathbb{Z}_n$ 不是域，其中的**可逆元 (Units)** 也能组成一个群。

- **定义：**$\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$。
- **阶：**$|\mathbb{Z}_n^\times| = \phi(n)$ （欧拉 ϕ 函数）。
- 这个群在数论（如 RSA 加密）中至关重要。

Lecture 3: 进阶例子与四元数结合律

8 进阶例子与同态初探 (Further Examples & Introduction to Homomorphisms)

NOTE: Note

在进入正式的代数章节前，我们需要看几个稍复杂的例子。它们打破了之前数系的某些“完美规律”（如交换律），并向我们展示了如何用函数的语言去比较两个代数结构。

8.1 环中的群：可逆元群 (The Group of Units)

我们在第 7 节提到环 R 有加法和乘法。虽然 $(R,+)$ 永远是群，但 $(R,\cdot)$ 往往因为 0 的存在而不是群。然而，如果我们只看那些“好元素”，它们能构成一个乘法群。

- **定义：**设 R 为幺元环。若 $a \in R$ 存在乘法逆元（即 $ab = ba = 1$），则称 a 为 **可逆元 (Unit)**。
- **记号：**$R^\times$ 或 $U(R)$ 表示 R 中所有可逆元构成的集合。
- **结构：**$(R^\times, \cdot)$ 是一个群。

典型例子：

1. **整数环：**$\mathbb{Z}^\times = \{1, -1\}$ （只有这两个整数有整数倒数）。
2. **域：**$k^\times = k \setminus \{0\}$ （域中所有非零元都可逆）。
3. **模 n 环：**$\mathbb{Z}_n^\times = \{[a] \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$。*(注：这个群的阶数正是数论中的欧拉函数 $\phi(n)$。)*

8.2 非交换环：矩阵环 (Matrix Rings)

之前我们遇到的 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ 都是 **交换环** $(ab = ba)$。矩阵环是打破这一直觉的重要反例。

- **定义**：设 k 是一个域，$M_n(k)$ 表示 k 上所有 $n \times n$ 矩阵的集合。
- **运算**：标准的矩阵加法与矩阵乘法。
- **单位元**：n 阶单位矩阵 I_n。
- **性质**：当 $n \geq 2$ 时，$M_n(k)$ 是 **非交换环 (Non-commutative Ring)**。

$$(M_n(k))^\times = GL_n(k) \quad \text{(一般线性群)}$$

8.3 结构间的桥梁：同态 (Homomorphisms)

如何判断两个代数结构是“相似”的？我们需要一种保持结构的映射，称为 **同态**。以环为例：

定义：设 R, S 是环，映射 $\phi : R \to S$ 称为 **环同态**，如果它“尊重”环的所有运算：

1. **保加法**：$\phi(a+b) = \phi(a) + \phi(b)$
2. **保乘法**：$\phi(ab) = \phi(a)\phi(b)$
3. **保单位元**：$\phi(1_R) = 1_S$

经典例子 vs 反例：

- **同态**：$\pi : \mathbb{Z} \to \mathbb{Z}_n$，定义为 $a \mapsto [a]$ （自然投影）。它完美地保持了加法和乘法结构。
- **不是同态**：$\psi : \mathbb{R} \to M_2(\mathbb{R})$，定义为 $a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$。虽然它保持了加法和乘法，但它将实数中的 1 映到了 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$，而不是矩阵环的单位元 $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$。因此它不是环同态。

直观理解：直观理解

同态就像是代数结构之间的“照相机”。它拍出来的照片（像）可能比原物小（信息有压缩，如 $\mathbb{Z} \to \mathbb{Z}_n$），但物体的结构特征（运算规则）被保留了下来。

9 四元数的矩阵表示与结合律 (Matrix Representation & Associativity)

验证四元数乘法的结合律 $(xy)z = x(yz)$ 如果直接代入 $x = a + bi + cj + dk$ 展开，计算量巨大。一种更优雅的方法是利用**矩阵同构**。

我们发现，四元数与 2×2 复矩阵之间存在一一对应关系。

9.1 矩阵的构造 (The Construction)

我们可以将四元数的基底 $1, i, j, k$ 映射到 2×2 复矩阵（这组矩阵与物理中的泡利矩阵密切相关）：

- $1 \mapsto I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $i \mapsto \mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$
- $j \mapsto \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
- $k \mapsto \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

9.2 一般形式 (General Form)

对于任意四元数 $q = a + bi + cj + dk$，其对应的矩阵表示为：

$$M(q) = aI + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

如果我们令复数 $z = a + bi, w = c + di$，则矩阵可以写得更紧凑：

$$M(q) = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$$

9.3 验证结合律 (Verification of Associativity)

为什么要大费周章写成矩阵？因为矩阵乘法的性质我们最熟悉。

- **前提 1**：矩阵乘法天然满足**结合律**。对于任意 n 阶方阵 A, B, C，线性代数告诉我们 $(AB)C = A(BC)$ 恒成立。
- **前提 2**：上述映射 $q \mapsto M(q)$ 是一个**环同态**（甚至是一个单射同态）。这意味着四元数的乘法完全对应于矩阵的乘法：$M(q_1 q_2) = M(q_1)M(q_2)$。*(这一点可以通过验证基底 i, j, k 的乘法表来保证，例如验证 $M(i)M(j) = M(k)$)*

证明逻辑：设 $x, y, z \in \mathbb{H}$ 是三个四元数，

$$\begin{aligned} M((xy)z) &= M(xy)M(z) \\ &= (M(x)M(y))M(z) \quad \text{(同态性质)} \\ &= M(x)(M(y)M(z)) \quad \text{(矩阵乘法结合律)} \\ &= M(x)M(yz) \\ &= M(x(yz)) \end{aligned}$$

由于该映射 M 是单射（即只有 0 映射到零矩阵），这意味着：

$$(xy)z = x(yz)$$

结论：通过将四元数“嵌入”到矩阵环 $M_2(\mathbb{C})$ 中，我们“免费”获得了结合律。这是代数学中**表示论 (Representation Theory)** 威力的第一个展示。