给小狗的近世代数课

shenzhu

2025.3.3

我们是孩子，但是我们精力充沛，勇往直前……

1 序言

狭义上，近世代数（modern algebra）或抽象代数（abstract algebra）指研究群、环、域的基本性质的一门课程，其中群论部分最重要的定理可能是同态基本定理，域论部分最重要的定理可能是 Galois 理论基本定理。广义上，代数学是研究集合上运算的一门数学。科大泛函分析 H 的老师黄文有一句很著名的话：“代数是研究等号的，而分析是研究不等号的。”这里面有一些很精妙的数学哲学，但是所谓数学哲学与民科的区别，就是其必须建立在掌握真的数学知识上。

根据 Bourbaki 学派的看法，“数学即研究带结构的对象与对象间保持结构的态”，有三大基本结构：拓扑结构，代数结构和序结构。拓扑结构如开集族、闭集族与邻域族等，描述了一个集合中点的临近关系；序结构描述集合之间的序，如包含与代数序；而代数结构描述集合的运算。因此，我们一般见到的代数结构，如群（具体的定义我们后面再谈）：

定义 1.1（群）

群是 $(G, \cdot)$ 一个集合 G 配上一个映射 $\cdot : G \times G \to G$，其中乘法 $\cdot$ 满足群的几条性质（有时被称为群公理）。

可以看到，群是带一个内部操作的集合；作为对比，我们看线性空间的定义：

定义 1.2（线性空间）

域 $\mathbb{F}$ 上的线性空间 $(V, +, \cdot)$ 是一个集合 V 配上两个映射：加法 $+ : V \times V \to V$ 和数乘 $\cdot : \mathbb{F} \times V \to V$，其满足线性空间的几条性质（线性空间公理）。

即线性空间包含一个内部操作和一个外部操作。形如上面的映射即被称为一个集合上的代数结构，与之相对，一个集合 S 上的拓扑结构是其幂集 $\mathcal{P}(S)$ 的一个子集，而序结构是 $S \times S$ 的一个子集。如果你愿意，可以将某代数运算映射 $S \times S \to S$ 视为集合 $S \times S \times S$ 的一个子集，基于此可以看出 Bourbaki 对基本数学结构分类的观点。

由于我和邪恶小狗同学都是学物理的，我们自然要问：为什么我们要学代数？当然，这个问题没有标准的答案，任何涉及运算的地方都有代数结构，但我想提两件重要的事：其一是线性化，其二是对称性。

什么是线性化？我们在上面已经看到了，域上的线性空间是一个代数对象，事实上这也是物理学中可能是最重要的代数对象。我们都知道，量子力学的态空间是一个复 Hilbert 空间，其首先是一个复数域上的线性空间，其上的可观测量也构成复线性空间。事实上，经典物理是流形与其上的几何，当我们考虑局部观测时，我们考虑流形的局部性质，而欧氏空间是所有有限维实线性空间的模板。更进一步地，当我们考虑广义相对论时，物理量是张量场，而张量就是多重线性映射。这一切的基础在于：微分算子 d 是一个线性化的算子，而且是一个性质相当好的算子。从更物理的角度讲，线性化是现代物理的核心思想，因为线性化的结果是可计算的，任何微扰论本质上都是一种线性化。

什么是对称性？现代物理中老生常谈的一句话是物理研究的是世界的对称性，而对称性用群表示。为什么？一种最简单并容易理解的看法是这样的：假设系统状态用集合 S 表示（当然作为物理系统，其应当附带表征其物理性质的结构，如 Hamiltonian 以表征其演化），我们考察系统的变换 $T : S \to S$ 构成的集合 $\mathcal{T}$，即我们说集合 $\mathcal{T}$ 作用在 S 上，记作 $\mathcal{T} \curvearrowright S$。变换应是可以叠加的，这对应集合上的一个乘法；当我们考虑对称变化时，变换应是可逆的。基于此，我们说可逆变换是一个群作用 $G \curvearrowright S$。

在此，我们插入一个内容，这是曾经困扰我很长时间的一件事。我们常常听见一个说法（可能是杨振宁说的最多），叫对称性决定物理规律，物理规律应当是在对称性群作用下不变的。对于经典物理，这是比较容易理解的，此时物理量是流形上的函数，对称性变换可以被理解为微分同胚变换群。但是，在量子物理、特别是量子场论中应当如何理解对称性呢？我们常说，能量是时间平移的生成元、动量是空间平移的生成元、角动量是转动的生成元，应当如何理解呢？当然，我们可以形式化地写出变换的 Lie 群并计算其李代数，此时这些量可以被理解为李代数的生成元。我想引用 Talagrand 的讲法，通过 Stone 定理将这件事看得更清楚：

定理 1.3（*Stone* 定理）

给定一个 Hilbert 空间 $\mathcal{H}$，则其上的强连续单参幺正变换 $\hat{U}(t)$ 和其上的自伴算子 $\hat{A}$ 是一一对应的。

因此，我们考虑一个系统的连续对称性群，这是一个 Lie 群；其的单参数子群可以被幺正表示到系统的 Hilbert 空间上，从而对应一个自伴算子，即一个系统的可观测量。从而，我们可以将系统的经典对称性与量子可观测量对应起来。正是因此，我们说量子场就是对称性群的（不可约）幺正表示。这是 Lie 理论在物理学中的一个重要应用，自然也是基于代数和代数表示论的。

2 集合论基础

此节内容可以略去或作参考。公理化集合论的详细内容见另一篇文章。

定义 2.1（集合）

集合（set）S 是一个良定的数学对象。对于任意元素，我们可以谈论其属于或不属于一个集合，分别记作 $x \in S$ 和 $x \notin S$。

定义 2.2 *集合间可以谈论包含。考虑集合 A 和 B，若 $\forall x \in A, x \in B$，则称 A 包含于 B，A 为 B 的一个子集，记作 $A \subset B$。*

命题 2.3 $A \subset B, B \subset A \iff A = B$

定义 2.4 全集（或有些书，特别是测度相关的书，喜欢称之为空间）是一个集合，记为 C。全集的任意子集也是集合。对于给定的全集，存在空集（*void set*）使得任意元素不属于其，记作 $\varnothing$。

以下谈论的集合间操作均是对于同一个全集的子集而言的。

定义 2.5 同一个全集中的集合中的两个集合是可以取并集（*union*）的，其并集仍然是一个全集的子集，定义为：

$$A \cup B := \{x | x \in A \wedge x \in B, \forall x \in \mathrm{C}\}$$

定义 2.6 同一个全集中的两个集合是可以取交集（*intersection*）的，其交集仍然是一个全集的子集，定义为：

$$A \cap B := \{x | x \in A \vee x \in B, \forall x \in \mathrm{C}\}$$

定义 2.7 某一个全集中的集合是可以取补集（*complement*）的，其补集仍然是一个全集的子集，定义为：

$$\mathrm{C} \backslash A := \{x | x \notin A, \forall x \in \mathrm{C}\}$$

定义 2.8 同一个全集中的两个集合是可以取差集（*difference*）的，其差集仍然是一个全集的子集，定义为：

$$A - B := A - C \backslash B$$

定义 2.9 同一个全集中的两个集合是可以取对称差集（*symmetric difference*）的，其对称差集仍然是一个全集的子集，定义为：

$$A \triangle B := (A - B) \cup (B - A)$$

定义 2.10 任意两个集合（无论包不包含于同一个全集）可以定义其卡氏积集（*Cartesian product*）：设 A 的全集为 C_A，B 的全集为 C_B，则其卡氏积集的全集记为 $\mathrm{C}_A \times \mathrm{C}_B$，其中元素记为：

$$A \times B := \{(a, b) | \forall a \in A, b \in B\}$$

以上对集合的操作除了补集，都可以被看作某种集合的集合到集合的集合的一种直观上的“二元映射”，但其事实上是非良定的（因为集合的集合是非良定的）。但是我们可以谈论集合间的映射，利用卡氏积集也是一个集合，我们可以谈论二元以至于多元的映射。将集合视为对象，则其间映射可以直观地表示为一个集合：

定义 2.11（映射）

任意两个集合（无论其是否属于同一个全集）间的所有映射（*map*）构成一个集合：

$$\mathcal{C}(A, B) := \{f | f : A \to B, a \mapsto f(a), \forall a \in A\}$$

记 $\mathrm{Dom}(f) := A$。

集合间的映射满足一些性质：

命题 2.12 可叠加性：任意集合 A、B、C，存在这样的一个映射：

$$\mathcal{C}(A,B)\times\mathcal{C}(B,C)\to\mathcal{C}(A,C),\,(f,g)\mapsto h=g\circ f$$

其满足：

a. 结合律（*associative law*）

$$\forall f\in\mathcal{C}(A,B),g\in\mathcal{C}(B,C),h\in\mathcal{C}(C,D)$$

$$h\circ(g\circ f)=(h\circ g)\circ f$$

b. 存在恒元（*identity*）

$$\forall A,\exists\,\mathrm{Id}_A\in\mathcal{C}(A,A)\,s.t.\forall B,f\in\mathcal{C}(A,B),g\in\mathcal{C}(B,A),f=f\circ\mathrm{Id}_A,g=\mathrm{Id}_A\circ g$$

可见，映射是集合元素间的一种对应关系。

定义 2.13 映射 $f\in\mathcal{C}(A,B)$ 的像是 B 的一个子集：

$$f(A')=:\{b\in B|\,\exists\,a\in A'\subset A,\,b=f(a)\}$$

映射的原像是 A 的一个子集：

$$f^{-1}(B')=\{a\in A|\,f(a)\in B'\subset B\}$$

注意该定义不一定要求映射可逆，即可能存在 B' 中的元素不存在 A 中元素与之对应。

有一些映射是特殊的。

定义 2.14 考虑 A 和 B 是集合，则一一映射（*one-one map*）或单射是这样的一些映射：

$$f\in\mathcal{C}(A,B),\forall a,b\in A,a\neq b\Rightarrow f(a)\neq f(b)$$

到上映射（*onto map*）或满射是这样的一些映射：

$$f\in\mathcal{C}(A,B),\forall b\in B,\exists!a\in A\;s.t.\;f(a)=b$$

如果一个映射既是一一映射又是到上映射，我们称其为一个一一到上映射或双射（*bijection*）。

现在，我们已经获得了一个定义较为良好的工具即集合和其上映射。这套语言是非常有用的，我们以后的所有定义都是基于此的。作为一个应用，我们定义等价关系，来体会集合语言的美。

定义 2.15（关系）

考虑 A 和 B 是集合，则关系（*relation*）是一个子集：

$$R \subset A \times B$$

$a \in A$，$b \in B$ 被称为 R-相关的，如果 $(a, b) \in R$，记作 aRb

定义 2.16 (等价关系)
等价关系（*equivalent relation*）是一个特殊的关系 $R \subset A \times B$，满足：
a. 自反性（*reflexivity*）$\forall a \in A, (a, a) \in R$
b. 对称性（*symmetry*）$\forall a, b \in A, (a, b) \in R \Rightarrow (b, a) \in R$
c. 传递性（*transitivity*）$\forall a, b, c \in A, (a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$
若 $(a, b) \in R$，则记 $a \sim b$。

给定某一种等价关系，我们就可以借其定义一个等价类，它们是一些原集的子集：

定义 2.17 考虑 $a \in A$，则其诱导的等价类定义为：

$$[a] := \{x | x \sim a, \forall x \in A\}$$

称 a 为 $[a]$ 的代表元。

对于一个集合，给定一个其上的等价关系，我们可以考虑它的所有等价类。由于传递性，任意两个等价类要么是交集为空的，要么是相等的。因此，从直观上，等价类构成了集合的一个“划分”。这种概念在数学上和物理上都是非常有用的：面对一个完整的对象集合，当我们要研究其中的某些性质时，可以借助等价类的概念将我们关心的性质提取出来；而将其余性质隐去，可以由商集的概念完成（这不是数学上最初的动机）。

定义 2.18 给定一个集合 A 及其中的一个等价关系 $\sim$，则该等价关系诱导的商集（*quotient set*）定义为：

$$A/\sim := \{[a] | \forall a \in A\}$$

有时全集的性质并不良好，而商集可以帮我们获得一个性质良好的集合，比如我们会在微分几何中的余切向量场的定义中这样做。

这里补充一个被我们忽略的细节：我们已经谈论了元素相等的概念，直观上说，两个元素相等当且仅当它们是同一个元素。但是我们也可以换个角度看：我们考虑一种平凡的等价关系，这个 R 中只包含形如 (a, a) 这样的元素，则我们可以说元素的相等也是一种等价关系。将这个定义反过来使用，我们可以说，元素相等当且仅当其当集合元素作为商集的标记时，其属于同一个等价类。这使得我们谈论相等时更安心。事实上，我们后面还将看到，相等概念有时意味着一种地位的相同，比如我们有时候会不经意间不区分实体的全同和同构意义下的相等。

以上的定义方法完全来自集合论的语言。在绝大多数情况下，这就足够了，而无需借助范畴论的语言。我们只需知道，使用范畴论的定义是确实可行且严谨的，而不用将过多的精力放在其上。我们后面在介绍近世代数时，也将使用集合论的语言而不必思考有关范畴层面上的问题。

定义 2.19 两个集合被称为等势的，若存在其间的双射。

按照上面的观点，我们立刻得出结论：等势是一种等价关系 $\sim$，其给出的等价类即等势的集合。那么若我们考虑“所有集合的集合”，记为 $\mathcal{A}$，则我们给出了一个自然数的定义：

最后，我们考虑集合的操作。我们上面给出了集合的映射，集合的操作本质上是一种特殊的映射。

定义 2.20 考虑 A 是一个集合，一个内部（*internal*）操作是一个映射：

$$i : A \times A \to A$$

定义 2.21 考虑 A 是一个集合，O 是另一个集合，一个外部操作（*external*）是一个映射：

$$e : O \times A \to A$$

其中 $o \in O$ 被称为一个算子（*operator*）。

可以发现，外部操作即集合在集合上的作用。

3　范畴与交换图

我们说：所有集合构成一个范畴 $\mathcal{SET}$，其被称为集合范畴。有人说，范畴论是数学的数学，这种话听听就好了。对于我们，最好的状态可能就是我们熟悉这种语言，但不会被其打扰。

具体地说，一个范畴 $\mathcal{C}$ 包括一些对象（objects）Ob($\mathcal{C}$) 和对象间的态射（morphisms）Mor($\mathcal{C}$)，配上两个指定。任意范畴 $\mathcal{C}$ 中的对象 A 与 B，其间态射记为 $\mathrm{Hom}_{\mathcal{C}}(A, B)$，其中 A 被称为定义域，B 被称为陪域。请注意，这里的 Obj($\mathcal{C}$) 与 $\mathrm{Hom}_{\mathcal{C}}(A, B)$ 一般都不应被理解为集合。例如，由于著名的 Russell 悖论，集合范畴的 Obj($\mathcal{SET}$) 不是集合。比起理发师悖论，我更喜欢的版本是“当代女权现状”：

例 3.1（*Russell* 悖论）

当一个女权主义者说出“我是不被定义的”时，其就被定义为了“不被定义的”，这触发了 *Russell* 悖论。翻译成数学的语言就是，若 Obj($\mathcal{SET}$) 是一个集合（例如考虑 *ZFC* 集合体系），则其中的元素可以构成新的集合，即我们考虑那些“所有不属于自身的集合构成的集合”，即发现这个集合既不能属于自身，又不能不属于自身，这就是 *Russell* 悖论。

Russell 悖论的存在意味着 Obj($\mathcal{SET}$) 不是一个集合，我们一般称之为一个“类”（class）。当然，我们也无需特别考虑这种东西，虽然这很好玩。当一个范畴 $\mathcal{C}$ 的 Obj($\mathcal{C}$) 是一个集合，且任意态射 $\mathrm{Hom}_{\mathcal{C}}(A, B)$ 也是集合时，其被称为是小的；当任意 $\mathrm{Hom}_{\mathcal{C}}(A, B)$ 是集合时，其被称为局部小的。集合范畴即是一个局部小但非小的范畴。

为了叙述方便，我们仅考虑局部小的范畴。这样做的主要原因是我们今后考虑的主要的范畴，如集合范畴 $\mathcal{SET}$、群范畴 $\mathcal{GROUP}$、线性空间范畴 $\mathcal{VEC}$ 等，都是集合范畴的子范畴（对象都是集合），因此其都是局部小的（态射都过构成集合）。

一个范畴应当满足一些条件。对于任意 $\mathrm{Obj}(\mathcal{C})$ 中对象 A，有恒等态射 $\mathrm{Id}_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$。态射可以复合：对于任意对象 A，B，C，D，任意态射 $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$，$g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ 唯一确定一个态射 $g \circ f \in \mathrm{Hom}_{\mathcal{C}}(A,C)$。复合满足以下两个条件：任意态射与恒等态射复合为自身：

$$f \circ \mathrm{Id}_A = \mathrm{Id}_B \circ f = f$$

复合满足结合律：任意 $h \in \mathrm{Hom}_{\mathcal{C}}(C,D)$，有：

$$h \circ (g \circ f) = (h \circ g) \circ f$$

我们使用交换图的语言来表达上面的式子。交换图是一种可视化的语言。图中的“点”是一个范畴中的对象，连接点的“线”是对象间的态射，用方向表示态射的方向。一张图被称为交换的，若两个点之间的任意连线表示同样的态射。因此，只有一个态射的图总是交换的：

$$\begin{tikzcd} A \arrow[r, "f"] & B \end{tikzcd}$$

恒等态射表示为：

$$\begin{tikzcd} A \arrow[loop above, "\mathrm{Id}_A"] \end{tikzcd}$$

态射复合可以表示为：

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

态射复合的条件可以被表示为交换图：

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"] \arrow[rr, bend left, "h\circ g"] & C \arrow[r, "h"] & D \end{tikzcd}$$

$$\begin{tikzcd} A \arrow[loop left, "\mathrm{Id}_A"] \arrow[r, "f"] & B \arrow[loop right, "\mathrm{Id}_B"] \end{tikzcd}$$

交换图是一种非常方便的手段，可以使用其写出简单的定义。我们将在后面使用这种语言。比如，集合范畴的卡氏积可以表达为：考虑集合 A 与 B，其卡氏积集 $A \times B$ 与投影映射 $\pi_A : A \times B \to A$ 与 $\pi_B : A \times B \to B$ 可以写为这样一张图：

$$\begin{tikzcd} & A \\ A \times B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & \\ & B \end{tikzcd}$$

满足对于任意集合 Z，任意映射 $f_A : Z \to A$，$f_B : Z \to B$，存在唯一态射 $\sigma : Z \to A \times B$ 使得下图交换：

$$\begin{tikzcd} & & A \\ Z \arrow[urr, bend left, "f_A"] \arrow[r, "\sigma"] \arrow[drr, bend right, "f_B"'] & A \times B \arrow[ur, "\pi_A"'] \arrow[dr, "\pi_B"] & \\ & & B \end{tikzcd}$$

类似这样的定义被称为“泛性质”。类似地，我们可以考虑集合无交并的泛性质：

$$\begin{tikzcd} A \arrow[dr, "\iota_A"'] \arrow[drr, bend left, "g_A"] & & \\ & A \sqcup B \arrow[r, "\gamma"] & Z \\ B \arrow[ur, "\iota_B"] \arrow[urr, bend right, "g_B"'] & & \end{tikzcd}$$

对于某一个构造的对象，使用泛性质作为其定义可以凸显其性质，我们将在自由群中看到这种定义的好处。

最后，我们考虑态射的逆。对于态射 $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$，其被称为可逆的若存在 $f^{-1} \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ 使得下图交换：

$$\begin{tikzcd} A \arrow[loop left, "\mathrm{Id}_A"] \arrow[r, shift left, "f"] & B \arrow[l, shift left, "f^{-1}"] \arrow[loop right, "\mathrm{Id}_B"] \end{tikzcd}$$

可以发现，一个态射可逆，则其逆唯一。一个可逆的态射被称为一个同构（isomorphism），且同构是一个等价关系（验证）。

4 半群与群

群是一种特殊的代数结构，其由一个集合和其上的操作构成。我们首先来看半群的定义。

定义 4.1（半群）

半群（*semi-group*）是一个集合 X 配上一个结合的外部操作。

$$X \times X \to X, (x, y) \mapsto xy \ or \ x \cdot y$$

其中结合性是指：

$$(xy)z = x(yz), \forall x, y, z \in X$$

这种操作被称为（半）群乘法。

注意谈论某一个集合是一个半群是没有意义的，比如实数在加法操作和乘法操作下都构成半群。因此，一般的语言是“集合 X 在乘法 · 下构成一个半群”。但是，如果我们知道讨论的对象是群，有时也使用 G 是一个半群这样的语言，只要记得其暗示存在着一种群乘法。

进一步地，我们有：

定义 4.2 含幺半群（*monoid*）*X* 是一个半群, 若其中存在一个这样的元素：

$$e \in X, \forall x \in X, ex = xe = e$$

e 被称为幺元（*unit*），有时也被记为 1 或 1_G。

根据幺元的定义，我们有若幺元存在，则其唯一。

证明.

$$e_1 = e_1 e_2 = e_2$$

∎

定义 4.3 群（*group*）*G* 是一个含幺半群，若其中的任意元素都可逆：

$$\forall g \in G, \exists g^{-1} \in G \ s.t. \ gg^{-1} = g^{-1}g = e$$

g^{-1} 被称为 g 的逆。

任意元素的逆也是唯一的，且左逆等于右逆。

我们在此不特别给出例子，我们会在后面常常遇到这些定义，到时再讨论具体例子对定义的符合。我们在后面可以看到，所有群构成群范畴，这是一个集合范畴的子范畴。

定义 4.4 *Abel* 群（或交换群）是群乘法满足交换律（*commutative*）的群：

$$\forall g_1, g_2 \in G, g_1 g_2 = g_2 g_1$$

Abel 性是非常好的性质。对于 Abel 群，我们记群乘法为 $+$，称为加法。Abel 群也构成范畴，但是这是一个和群范畴性质差异巨大的范畴，此事在量子力学中亦有记载。

我们在最前面提到了从物理的角度看，为什么要研究群。现在有了范畴的语言，我们从数学上、即从形式语言的角度来看看为什么要研究群。

我们在前面看到，一个群定义中最重要的部分就是其元素可逆。事实上，这确实是本定义的核心，并且是群比半群更常见的原因。回忆范畴中同构的定义，一个范畴若其中的任何态射都是同构，则其被称为一个广群（groupoid）。我们可以借此给出群的第二个定义：

定义 4.5（群）

任何群和一个只有一个对象的广群范畴一一对应。

我们可以记这个元素为 $\{*\}$，则群作为集合是 $\mathrm{Hom}_{\mathcal{GROUPOID}}(*,*)$。由于其是广群，复合、逆都是良定的。事实上这反映了群的重要性质：任何群都是某个独点广群范畴的自同构。

5 同态与子群

同态（homomorphism）是代数对象间的态射（morphism），如群同态、环同态等。当然，任意群都是一个集合，作为集合，我们可以考虑群间的映射；但是在大部分时候，这意义不大。我们要始终记得，一个群不仅仅是一个集合，而是一个集合配上一个群乘法。因此，很自然地，我们希望群同态也不仅仅是一个集合间的映射，还希望其“保持集合上的结构”，即将一个群的乘法“推前”到另一个群上。

定义 5.1（群同态）

考虑 $(G,\cdot)$ 与 $(G',\circ)$ 是群，则其间的群同态 $f:G\to G'$ 是一个映射，使得：

$$\forall a,b\in G, f(a\cdot b)=f(a)\circ f(b)$$

若我们总是记得对不同的群使用正确的群乘法，则可简记为：

$$f(ab)=f(a)f(b)$$

用范畴的语言，我们可以用交换图重写群同态的定义。首先，群乘法写为：

$$G\times G\xrightarrow{\quad\cdot\quad}G$$

$$G'\times G'\xrightarrow{\quad\circ\quad}G'$$

同态是一个映射：

$$G\xrightarrow{\quad f\quad}G'$$

根据卡氏积的定义（事实上卡氏积是一种诱导映射），同态诱导一个卡氏积空间上的映射：

$$f\times f:G\times G\to G'\times G',(a,b)\mapsto(f(a),f(b))$$

$$G\times G\xrightarrow{\quad f\times f\quad}G'\times G'$$

则 f 被称为一个同态映射，当且仅当下图可交换（或下图是一个交换图）：

$$
\begin{tikzcd}
G \times G \arrow[r, "f\times f"] \arrow[d, "\cdot"'] & G' \times G' \arrow[d, "\circ"] \\
G \arrow[r, "f"'] & G'
\end{tikzcd}
$$

因此，所有群构成一个范畴 $\mathcal{GROUP}$ 或 $\mathcal{GRP}$，被称为群范畴；其中的对象是群，态射是群同态。

回忆前面对单射与满射的定义，单同态作为映射是单的，而满同态作为映射是满的。

定义 5.2 (像与核)
同态 f 作为映射，其像与幺元的原像被称为像（*image*）与核（*kernel*）:

$$ker(f) := f^{-1}(e_2), im(f) := f(G_1)$$

群范畴的同构即群同构:

定义 5.3 (同构)
一个群同态被称为一个群同构（*isomorphism*），若其作为映射是一个双射，记为 $G \cong G'$，并称两个群是彼此同构的（*isomorphic*）。

定义 5.4 (自同态和自同构)
群 G 到自身的同态被称为自同态（*endomorphism*）。群全体自同态构成一个集合，记为 End(G) 群 G 到自身的同构被称为自同构（*automorphism*）。群全体自同构也构成一个集合，记为 Aut(G)。

命题 5.5 注意到群的自同构是可以复合的，复合的结果仍然是一个自同构。取幺元为恒等映射，其也是一个自同构。考虑到双射一定存在逆映射，其也是可逆的。因此，群的自同构在复合的群乘法下构成一个群。

这与群的广群定义相似。

我们可以发现，若两个群是同构的，则其作为集合首先存在一个彼此间的双射映射，即元素间存在对应的关系。进一步地，其作为一个群的群乘法也是类似的。所以我们可以说，两个同构的群是几乎一模一样的，有的时候我们就说它们是一样的。很多场合下，很多人习惯不区分相等与同构意义下相等，这是有一定道理的，只是我们要清晰地意识到映射 f 的存在。类似地，任何范畴中的同构都可以被理解为相等。

相比而言，同态就没那么好了，因为其有可能将不同的元素映为同一个元素。举个极端的例子，考虑只有一个元素的平凡群，将任意群的所有元素都映为它，则这个映射也是一种同态。虽然同态刻画的两个群并不一定是完全相等的，但是这显然是更普遍的情形；而且，被映为同一个元素的那些原群中的元素之间也应该存在一些关系。为了描述这些性质，我们先考虑子群。

定义 5.6 考虑 G_1 与 G_2 是群，则 G_1 被称为 G_2 的子群（*subgroup*），若存在一个单射的同态 $\tau : G_1 \to G_2$。

注意到此时我们已经体现了不区分彼此同构的代数对象：

命题 5.7 与 τ 映射方式相同的同态 $\tau' : G_1 \to \tau(G_1)$ 是一个同构。因此，有时也称 $\tau(G_1)$ 为 G_2 的子群，记为 $\tau(G_1) \leq G_2$。

我们以有限群（因为有限群是可以想象的）为例，考虑子群的存在性。对于有限群，我们有定义：

定义 5.8（阶）
群的势被称为阶：$|G| \in N$。

给定一个群，其有多少可能的子群？首先，幺元由群乘法唯一确定，所以幺元必定在子群中。两个极端的情况分别是：

$$\{e\} \leq G, G \leq G$$

我们称第一种情况为平凡子群，任何群都有平凡子群和其本身作为子群。我们下面考虑非平凡的子群有应当什么性质。

对于群 G 的一个子群 H，由于群的封闭性，我们有：

$$\forall h \in H,\, H = hH := \{hg|g \in H\},\, H = Hh := \{gh|g \in H\}$$

当我们使用类似的记号时，即一个群元乘上一个群，其代表一个如上这样作用出的集合。另外，当我们谈论群的子集之间的乘法时，我们默认定义为：

定义 5.9 考虑 G 是群，$A, B \in G$，其乘法定义为：

$$AB := \{ab|\forall a \in A, b \in B\}$$

以上命题是显然的，因为子群也是群，其自然封闭。但是对于那些不在子群中的元素，如上构造出的集合就不是群了。一般地，我们有：

定义 5.10 对于群 G 的一个子群 H，A 被称为其的一个左陪集（*left coset*）若：

$$\exists g \in G,\, A = gH$$

注意到若 A 不等于 H 本身，则其一定不是一个群（因为其中没有幺元）。我们有如下命题成立（其证明并不困难）：

命题 5.11 对于群 G 的一个子群 H，其可以给出一个原群的左陪集分解：

$$G = \bigcup_{r \in R} rH,\, where\, if\, r_1 \neq r_2 \in R,\, r_1 H \cap r_2 H = \varnothing$$

其中 R 被称为指标集，其阶被称为子群 H 的指数（*exponent*），记为 $|R| = [G : H]$。

即对于群的任意子群，其可以通过和指标集作用遍历生成整个群。那么在直观上，我们有一个显然的定理：

定理 5.12（*Lagrange* 定理）

对于有限阶群 G 的任意子群 H

$$|G| = |H|[G:H]$$

这是群论中第一个重要的定理。Lagrange 定理指出，对于有限阶群，其子群阶数一定是其阶数的因数，这使得我们可以更为直观地看待一个群的子群。例如，我们考虑元素的阶。

定义 5.13 考虑 $g \in G$ 是群中的任意元素，则其阶数 n 定义为使得下式成立的最小正整数：

$$g^n = e$$

这个定义与后面域论中的指标类似，因此，有时若 g 的任意次都不为单位元，称其阶为 0（这个定义并不常用）。注意到有限群的元素阶一定有限：

命题 5.14 有限群的元素阶是群阶数的因数。

证明. 设 $g \in G$ 的阶为 m。则 $\{e, g, g^2, ..., g^{m-1}\}$ 构成 G 的一个子群。由 Lagrange 定理，命题得证。 ∎

我们称 $\{e, g, g^2, ..., g^{m-1}\}$ 为由 g 生成的子群，g 被称为生成元。更一般的，生成元可以是一个集合，使得其中元素通过群乘法类似地生成一个群。

Lagrange 引理的形式使得我们想起等价关系和商集，我们希望获得类似的结构，即商群。此时，我们自然想问：群的商集是一个群吗？答案是不一定的。

例 5.1 考虑 $H \leq G$，其给出划分：

$$G = \bigcup_{r \in R} rH, \, where \, if \, r_1 \neq r_2 \in R, \, r_1H \cap r_2H = \varnothing$$

则商集为 $A := \{rH | r \in R\}$。

注意到对于 $a, b \in R$，$(ab)H = aHbH$ 不一定能够成立，即商集并不能自然的给出群结构。但是一旦 $aH = Ha$ 对指标集中的任意元素成立，那么自然可以给出上面的群乘法。

这代表着子群的交换性。如果子群和群中任意元素都是交换的，那么这自然成立。注意这并不要求子群中的任意元素都是和群中的任意元素交换的，因为我们可以让子群乘上一个元素后每个元素都改变、而又重新形成原来的子群。更清晰的定义是：

定义 5.15 考虑 $H \leq G$，其正规化子（*normalizer*）和中心化子（*centralizer*）定义为：

$$N_G(H) := \{g \in G | gH = Hg\}$$

$$C_G(H) := \{g \in G | gh = hg, \forall h \in H\}$$

其描述了群中与子群交换的部分。显然，中心化子的定义比正规化子更严格；我们有以下命题：

命题 5.16 正规化子和中心化子都是子群。

$$C_G(H) \leq N_G(H) \leq G$$

对于 Abel 群，其中的任意元素显然都是可以任意交换的，则我们有一个群是 Abel 的当且仅当 $C_G(G) = G$。我们需要的定义就呼之欲出了，不是任意子群都可以给出商集的群结构，只有那些交换性很好的子群，即：

定义 5.17 正规子群（*normal subgroup*）是那些正规化子是整个群的子群：

$$H \leq G, N_G(H) = G$$

记作 $H \lhd G$。

则商集作为群也是良定的：

定义 5.18 考虑 $H \lhd G$，则其诱导的商群定义为：

$$G/H := \{rH|r \in R\}$$

商群中乘法为：

$$aH \circ bH = (a \cdot b)H$$

这种乘法定义的合理性在于：对于子群，$HH = H$，若 $aH = a'H, bH = b'H$，则

$$a'b'H = a'b'HH = a'Hb'H = aHbH = abH$$

于是，我们终于可以给出群论中可能是最重要的定理：

定理 5.19（同态基本定理）

考虑 G_1 和 G_2 是群，f 是 G_1 到 G_2 的一个同态，则：

$$im(f) \leq G_2, ker(f) \lhd G_1$$

且存在一个同构：

$$\bar{f} : G/ker(f) \cong im(f)$$

我们略去其证明，经过前面的铺垫，这不是特别困难。直观上，我们应当如何理解这个定理？首先，同态作为一个群间映射，保持了群乘法的性质。其次，原群中属于某个正规子群中的元素差异被抹除，其陪集中的元素的差异也被抹除。最后，同态相当于这样的一个操作，其使得原群商掉了自己的一个正规子群。很多时候这是很有意义的：当我们要提取原群的某些性质时，可以将不关心的东西商掉。

这种“将不好的东西商掉”的想法是很重要的。我们在此举两个例子：数学上，当我们面对一个集合，其幺元不好定义、或是由于别的什么性质不好导致不构成一个我们想要的群，但又有类似的群乘法时，我们可以构建类似同态基本定理的映射获得一个群。我们后面会看到，

这正是我们在流形上构造余切矢量场的方式。物理上，当我们考虑某一个物理系统的对称性群时，特别是考虑其量子化，有时会出现没有物理意义的规范对称性，而规范固定其实就是取对称性群的商群的过程。

6 环、域、模与线性空间

在近世代数中，群是集合上的第一层结构，其上还有很多其他结构，如环和域的。

定义 6.1 环（*ring*）*R* 是一个集合配上两个内部操作，对于第一个操作 + 其构成一个 *Abel* 群，被称为环加法，对于第二个操作 · 其构成半群，被称为环乘法，二者构成分配律（*distributive law*）：

$$\forall x, y, z \in R,\, x \cdot (y + z) = x \cdot y + x \cdot z,\, (x + y) \cdot z = x \cdot z + y \cdot z$$

记加法幺元为 0。

所以，环首先是一个群；因此，环的含幺性和 Abel 性都是对于其第二个操作而言的，和群的定义完全相同，故不赘述。特别地，一个幺环的乘法幺元如果存在，则被记为 1 以示与加法的区分。

定义 6.2 域（*field*）*F* 是一个交换幺环，其满足除加法幺元 0 外所有元素在乘法下的逆都是存在的、且加法幺元不等于乘法幺元：

$$\forall x \neq 0 \in F, \exists x^{-1} \in F\ s.t.\ x^{-1}x = xx^{-1} = 1$$

其中加法幺元与乘法幺元不等杜绝了平凡情况被称为域的可能性（否则平凡群也是域）。

例 6.1 有理数、实数和复数在通常意义下的加法与乘法下都是域。记有理数域为 $\mathbb{Q}$，实数域为 $\mathbb{R}$，复数域为 $\mathbb{C}$。

所以你现在可以理解那个笑话：

一个数学家想学习类域论。由于英语水平不佳，最后他学习了经典场论。

下面我们来添加外部操作。注意我们开始谈论外部操作后，总是会加上如"X 上的⋯⋯"，X 上的就意味着我们有一个算子集来给我们构造外部操作。

定义 6.3 环 *R* 上的模（*module*）*X* 是一个 *Abel* 群配上一个外部操作：

$$R \times X \to X,\, (\alpha, x) \to \alpha x$$

$$s.t. \forall \alpha, \beta \in R,\, x, y \in X$$

$$\alpha(x + y) = \alpha x + \alpha y,\ (\alpha + \beta)x = \alpha x + \beta x,\ (\alpha\beta)x = \alpha(\beta x)$$

我们很少处理一个不是域的环上的模。

定义 6.4 线性空间（*linear space*）*X* 是一个域上的模。线性空间中的元素被称为向量。

特别地，我们称实数域上的线性空间为实线性空间，复数域上的线性空间为复线性空间。