DRAFT [March 4, 2015]

分析基础

Fundamentals of Analysis

孙伟

25-10-2014

DRAFT [March 4, 2015]

前言

本书内容起源于2014年秋季学期华东师范大学针对数学专业本科一年级新生所开课程《数学分析（1）短课程》。该课程的原先计划是介绍些集合论的知识和一些大学数学的基础，演示如何独立理解问题并完成证明，以及介绍一些常用的基本不等式技巧等。在具体课程中，因为时间限制（每周一次课程），以及课程安排的限制（很多基础课程尚未修习），部分原先计划的内容被删减或者被改为选读内容。由于课程形式为大课，课堂上略去了一些细节的推导和短时间无法完成推导的内容。为了弥补这部分内容，在本书中给出了课堂上所涉及内容之完整版，同时也在最后的附件中简略的给出了一些所需的背景知识。

在集合论部分，我们介绍了朴素集合论，以及朴素集合论中需要注意的一些问题（比如罗素悖论等），但是我们并没有按照严格的公理系统来介绍ZF集合公理体系。 选择公理对于初学者是不太好理解的，但是基于选择公理在现代数学中的重要性，我们也比较详细的介绍了选择公理，以及由选择公理派生出来的结果（比如三歧律、佐恩引理、良序化公理等）。我们也介绍了集合论的基数，Cantor基数悖论以及连续统假设等。

在实数公理体系部分，我们从自然数的Peano公理出发，推导出自然数的各种结构（序结构、加法和乘法结构等）。基于此，通过对加法和乘法运算的Grothendieck化，依次得到整数和有理数，以及其上的各种结构（包括距离结构）。基于有理数和其上的距离结构，通过完备化，我们引入了实数的定义和其上的各种结构。在此基础上，我们推导了实数的一些基本而重要的性质，比如确界原理、闭区间套定理等。

在不等式技巧部分，我们简单介绍了一些常用的不等式证明思路并且给出了基于凸性的不等式证明方法。基于此，我们进一步介绍了如Cauchy-Schwartz不等式、Hölder不等式、Minkowski不等式等常用不等式。

Banach-Tarski悖论是二十世纪初所发现的一个在ZFC公理体系上成立但是和朴素直观相悖的数学现象。历史上，该现象也引出了群的顺从性之概念。同时，该现象也和不可测集有着一定的关系。虽然测度论和顺从性分别是数学专业本科高年级和相关方向研究生阶段的内容，但是我们认为在具备相关集合论知识和数学证明方法的基础上，数学系本科新生是可以大体上理解Banach-Tarski悖论后面的数学的。同时，通过介绍Banach-Tarski悖论，我们可以演示一个相对完整并且不是很平凡的数学问题及其解决方法，并且希望可以帮助加深对其中所涉及内容（顺从群、群在集合上之作用、测度论、可测集、选择公理等）之理解。

每部分内容后面有相应的习题。习题之间难度相差不小，有些题不是很容易，可能需要几天时间完成。这些题应该会是不错的练习和思考的机会。

课程中和集合论以及自然数Peano公理相关的内容，参考了华东师范大学周青教授以前《数学分析（1）荣誉课程》之讲义。在针对大一数学系新生的课程中介绍Banach-Tarski悖论的想法，起

源于2014年7月在菲尔兹研究所和龚贵华教授的一次谈话。在此特向周青教授和龚贵华教授表示感谢。

本书中的部分问题和内容，来自于课堂上学生的提问和课后答疑。这从不同的角度提供了很好的借鉴和补充，在此一并对以2014级数学系本科新生为主的学生们表示感谢。

孙伟

2015年2月16日

DRAFT [March 4, 2015]

目录

第1章

集合论

1.1 集合之定义、基本运算和性质

定义 1.1.1. 集合是由元素构成的全体。对于集合 X 和元素 a，如果 a 在 X 中，则记为 $a \in X$；如果 a 不在 X 中，则记为 $a \notin X$。

定义 1.1.2. 对于两个集合 X 和 Y，我们说 X 包含于 Y，或者等价的，Y 包含 X，如果对于任意 X 中元素均在 Y 中。若 X 包含于 Y，我们记为 $X \subset Y$。$X \subset Y$ 也可以读作“X 是 Y 的子集”。

定义 1.1.3. 对于两个集合 X 和 Y，我们说它们是相等/相同的，记为 $X = Y$，如果 X 和 Y 中的元素完全相同。换言之，对于任意元素 a，若 $a \in X$，则 $a \in Y$，并且若 $a \in Y$，则 $a \in X$。如果 X 和 Y 不相等，我们记为 $X \neq Y$。

根据上述定义，$X = Y$ 当且仅当 $X \subset Y$ 且 $Y \subset X$。

定义 1.1.4. 对于两个集合 X 和 Y，我们说 X 真包含于 Y，或者等价的，X 是 Y 的真子集，如果 $X \subset Y$ 且 $X \neq Y$。若 X 真包含于 Y，我们记为 $X \subsetneq Y$。

为了描述一个集合，如果该集合包含有限个元素（“有限”的严格定义会在后面给出），我们可以枚举其中的元素。

集合中的元素是互不相同的。例如，如果我们说 $X = \{a, b\}$，则 a 和 b 是不同的元素。

关于集合的一个要点是，集合中的元素也可能是一个集合。比如 $\{1, \{2, 3\}\}$ 是个集合，包含两个元素。第一个是 1，第二个是 $\{2, 3\}$。

给定集合 X，给定元素 a，那么只有如下两种可能：$a \in X$ 或者 $a \notin X$。

给定集合 X，给定元素 a，一定可以确定 $a \in X$ 和 $a \notin X$ 这两种可能中哪种是成立的。

在集合论中，$Y \subset X$ 和 $Y \in X$ 是可能同时满足的。例如，$X = \{1, 2, \{1, 2\}\}$，$Y = \{1, 2\}$。

定义 1.1.5 (空集). 如果某个集合不包含任何元素，则我们称该集合为空集，记为 $\emptyset$ 。

定理 1.1.1 (空集是任何集合的子集). 对于任意集合 A ， 均有 $\emptyset \subset A$ 。

证明： 对于任意集合 A ， 我们只需要证明 “如果元素 $x \in \emptyset$ ， 则 $x \in A$” 。

根据空集的定义， $x \in \emptyset$ 永远是不成立的。因此 “若 $x \in \emptyset$ ， 则 $x \in A$” 为永真命题。 ∎

定理 1.1.2 (空集的唯一性). 如果集合 X 和 Y 都是空集，则 $X = Y$ 。

证明： 因为 X 为空集，根据定理1.1.1， $X \subset Y$ 。 同理，我们有 $Y \subset X$ 。 故而我们有 $X = Y$ 。 ∎

根据上述的空集唯一性，我们可以用一个记号 $\emptyset$ 来表示空集。

定义 1.1.6. 对于集合 A 和 B ， 我们定义它们的交（交集）为 $\{x\colon x \in A \text{ 且 } x \in B\}$ ， 并记为 $A \cap B$ 。

定义 1.1.7. 对于集合 A 和 B ， 我们定义它们的并（并集）为 $\{x\colon x \in A \text{ 或 } x \in B\}$ ， 并记为 $A \cup B$ 。 如果 $A \cap B = \emptyset$ ， 则 $A \cup B$ 可记为 $A \sqcup B$ ， 读作 “A 和 B 的无交并”。

定义 1.1.8. 对于集合 A 和 B ， 我们定义它们的差为 $\{x\colon x \in A \text{ 且 } x \notin B\}$ ， 并记为 $A - B$ 。

在朴素集合论中，我们可以通过描述的方式来定义一个集合。例如，在1900年和2000年之间的所有闰年构成一个集合。当然，对于这个集合，我们也是可以用枚举法定义的。又如，华东师范大学2014级数学系的所有学生也构成一个集合。

通过描述的方式来定义集合，往往比通过枚举元素来定义集合更方便。有的情况下，通过描述来定义集合是唯一可行的方法。例如，在2014年大洋洲所有植物的种类所构成的集合。由于可能有尚未发现的植物，我们无法通过枚举法来刻画上述的集合，但是任然可以通过描述的方式来进行刻画。这是朴素集合论强大的地方。

1901年，英国数学家和哲学家罗素提出了著名的罗素悖论，该悖论表明，在朴素集合论中，通过任意描述来定义集合的行为会导致矛盾。罗素悖论可以如下叙述：

“ 设 $X = \{x\colon x \notin x\}$ 。 其中的 x 为这样的集合：x 不在集合 x 中。考虑如下问题：$X \in X$ 是否成立？

如果 $X \notin X$ ， 则 X 符合集合 X 中元素的描述，故 $X \in X$ 。 矛盾。

如果 $X \in X$ ， 则 X 必然满足 X 中元素的描述，因此 $X \notin X$ 。 矛盾。 ”

为了解决罗素悖论，需要对“通过任意描述必然可以得到一个集合”进行限制。用 “$P(x)$ 成立” 来表示 “元素 x 满足性质 P”。在 ZF 公理体系中，对于任意的元素 x 和任意的性质 P ， $P(x)$ 是否成立并不一定是可以判断的。在 ZF 公理体系中，给定集合 X ，对于任意的 X 中元素 x 和 任意性质 P ， $P(X)$ 是否成立是一定可以判断的。基于此，就可以避开上述的罗素悖论。

定义 1.1.9. 给定集合 X 和 Y ， 定义它们的积（记为 $X \times Y$）为 $\{(x,y)\colon x \in X, y \in Y\}$ 。对于 $X \times X$ ， 我们也简记为 X^2 。

习题：

习题 1.1.1. 对于任意集合 A 、B 和 C ， 证明： $(A\cap B)\cap C=A\cap(B\cap C)$ 。

习题 1.1.2. 对于任意集合 A 、B 和 C ， 证明： $(A\cup B)\cup C=A\cup(B\cup C)$ 。

习题 1.1.3. 对于任意集合 A 、B 和 C ， 证明： $(A\cup B)\cap C=(A\cap C)\cup(B\cap C)$ 。

习题 1.1.4. 对于任意集合 A 、B 和 C ， 证明： $(A\cap B)\cup C=(A\cup C)\cap(B\cup C)$ 。

习题 1.1.5. 对于任意集合 A 和 B ， 证明： $A\cup B=(A-B)\sqcup(A\cap B)\sqcup(B-A)$ 。

习题 1.1.6. 如果集合 A 是任意集合的子集，证明：$A=\emptyset$ 。

习题 1.1.7. 给定集合 X ， 我们是否可以定义 X 的子集 Y 为 $\{y\in X\colon y\notin y\}$ ？这样的定义是否一定会触发类似罗素悖论的现象？为什么？

1.2 映射

定义 1.2.1. 给定集合 X 和 Y ， 我们说 $f\colon X\to Y$ 是一个从 X 到 Y 的映射，如果对于任意的 $x\in X$ ， 存在唯一的 $f(x)\in Y$ 。 对于这样的映射 f ， 我们称 X 为其定义域（domain），Y 为其codomain。$f(x)$ 也被称为 x 在 f 下的像。所有这些像全体构成的集合称为 f 的值域（range），记为 $f(X)$ 。换言之，$f(X)=\{f(x)\colon x\in X\}$ 。

注 1.2.1. 因为历史原因和翻译的原因，部分中文数学书中，将上述的 codomain 也称为值域。

定义 1.2.2. 我们说映射 $f\colon X\to Y$ 是单的（单射，injective map, one-to-one map），如果 $\forall(x\in X)\ \forall(x'\in X)\ ((f(x)=f(x'))\Rightarrow(x=x'))$ 。 我们说它是满的（满射，surjective map），如果 $\forall(y\in Y)\ \exists(x\in X)\ (f(x)=y)$ 。 如果 f 是既单且满的，我们就说 f 是个一一对应（双射，bijective map, one to one correspondence）。

注 1.2.2. 因为历史原因和翻译的原因，部分中文数学书中，不太区分 one-to-one map 和 one to one correspondence 的中文翻译，都统称为一一映射或者一一对应。

例 1.2.1. 对于映射 $f\colon\mathbb{R}\to\mathbb{R}^2$ ， 其定义域为 $(-\infty,\infty)$ ， codomain 为 $(-\infty,\infty)$ ， 值域为 $[0,\infty)$ 。 该映射 f 不是单射，也不是满射。

例 1.2.2. 对于映射 $g\colon\mathbb{R}\to[0,\infty)$ ， 其定义域为 $(-\infty,\infty)$ ， codomain 为 $[0,\infty)$ ， 值域为 $[0,\infty)$ 。 该映射 g 不是单射，是满射。

映射的复合、逆映射

定义 1.2.3. 给定映射 $f\colon A\to B$ 和 $g\colon B\to C$，定义其复合（记为 $g\circ f$）为

$$g\circ f : A\to C,\ a\mapsto g(f(a))\ 。$$

定义 1.2.4. 给定集合A，定义其上的恒等映射（记为id_A）为

$$\mathrm{id}_A\colon A\to A,\ a\mapsto a\ 。$$

对于任何集合 X，其上的恒等映射 id_X 总是存在的。

定义 1.2.5. 给定双射 $f\colon A\to B$，定义其逆映射（记为 f^{-1}）为

$$f^{-1}\colon B\to A,\ b\mapsto \text{“满足 } f(x)=b \text{ 的唯一 } x\text{”}\ 。$$

根据逆映射的定义，对于上述定义中双射 f，总有 $f^{-1}\circ f=\mathrm{id}_A$ 和 $f\circ f^{-1}=\mathrm{id}_B$。

习题：

习题 1.2.1. 若映射 $f,g\colon X\to X$ 满足 $f\circ g=g\circ f$，则 f 和 g 是否一定互为逆映射？

习题 1.2.2. 给定映射 $f\colon X\to X$，如果 $f\circ f$ 存在唯一的不动点，证明 f 存在唯一的不动点。【定义：对于映射$g\colon X\to X$，我们说 x 是 g 的一个不动点，如果 $g(x)=x$。】

习题 1.2.3. 对于映射 $f\colon X\to X$，如果 f 存在唯一的不动点，是否可以断言 $f\circ f$ 也一定存在唯一的不动点？若是，给出证明；若否，给出反例。

习题 1.2.4. 构造映射 $f\colon[0,1]\to[0,1]$，使得 f 不存在不动点。

习题 1.2.5. 如果 $f:X\to Y$ 为单射，对于 X 中的子集 A 和 B，证明 $f(A)\cap f(B)\subset f(A\cap B)$。

习题 1.2.6. 用 $\mathbb{Z}$ 代表整数全体构成的集合。试构造 $\mathbb{Z}$ 和 $\mathbb{Z}\times\mathbb{Z}$ 之间的双射。

习题 1.2.7. 证明：对于任意集合 X 和 Y，存在 $X\times Y$ 和 $Y\times X$ 之间的双射。

习题 1.2.8. 证明：对于任意集合 X，Y 和 Z，存在 $(X\times Y)\times Z$ 和 $X\times(Y\times Z)$ 之间的双射。

习题 1.2.9. 如果 $f\colon A\to B$ 和 $g\colon B\to C$ 都是单射，证明 $g\circ f$ 也是单射。

习题 1.2.10. 如果 $f\colon A\to B$ 和 $g\colon B\to C$ 都是满射，证明 $g\circ f$ 也是满射。

习题 1.2.11. 对于双射 $f\colon A \to B$ ， 证明其逆映射 f^{-1} 也是双射。

习题 1.2.12. 对于双射 $f\colon A \to B$ 和其逆映射 $g\colon B \to A$ ， 证明 $g \circ f = \mathrm{id}_A$ 且 $f \circ g = \mathrm{id}_B$ 。

习题 1.2.13. 对于映射 $f\colon A \to B$ 和 $g\colon B \to A$ ， 如果 $g \circ f = \mathrm{id}_A$ ， 证明 f 为单射。如果 $f \circ g = \mathrm{id}_B$ ， 证明 f 为满射 。

1.3 有限集、无限集

定义 1.3.1. 我们称集合 A 是无限的，如果存在 A 的真子集 B，使得 A 可以一一对应到 B 。

例 1.3.1. 希尔伯特旅馆 (Hilbert’s Hotel)

某旅游胜地的一家旅馆所有房间已经客满。该旅馆的房间编号为 $1, 2, 3, \ldots$ 。 这时又来了一名新的客人需要入住。虽然已经客满，但是可以把 1 号房间的客人搬到 2 号房间，2 号房间的客人搬到 3 号房间，3 号房间的客人搬到 4 号房间，$\cdots$ 。 这样就腾空出了 1 号房间供新来的客人入住。

定义 1.3.2. 我们称集合 A 是有限的，如果 A 不是无限的。

注 1.3.1. 上述Hilbert旅馆的例子刻画了有限和无限的本质区别。类似的例子还有“明日歌”中的诗句“明日复明日，明日何其多。我生待明日，万事成蹉跎。” 因为人生的日子是个有限集，因此用类似Hilbert旅馆的策略来将事情推迟到下一天的做法是行不通的。

问题：上面是先定义了无限，然后将有限定义为其反面形式。如果让你来定义有限，你会如何定义？ 注意不能循环定义。

定理 1.3.1. 空集 $\emptyset$ 是有限集。

证明： 假设空集 $\emptyset$ 是无限的，那么存在其一个真子集 A ， 使得 $\emptyset$ 和 A 有一一对应。由于 A 是 $\emptyset$ 的真子集，它必然也是 $\emptyset$ 的子集。故而如果存在元素 $x \in A$ ， 则 $x \in \emptyset$ 。 而这与 $\emptyset$ 为空集矛盾。从而 A 必定不包含任何元素。由前面关于空集的唯一性，我们知道 $A = \emptyset$ ， 与 A 为 $\emptyset$ 的真子集矛盾。 ∎

我们先定义了“无限“，然后将“有限”定义为其反面情况。你能够直接给出“有限”的定义么？当然，你的定义，需要与这里已有的定义“相容”。

下面的定理告诉我们，两个有限集合的交集仍然是有限集。

定理 1.3.2. 若 A 和 B 都是有限集，则 $A\cap B$ 也是有限集。

证明： 已知 A 和 B 都是有限集，需要证明 $A\cap B$ 也是有限。如若不然，则 $A\cap B$ 为无限。根据定义，存在 $A\cap B$ 的真子集 C ， 使得 $A\cap B$ 和 C 之间有一一对应。 不妨用 f 来记这个从 $A\cap B$ 到 C 的一一映射。我们试图构造一个从 A 到 A 之真子集 D 的一一映射

$$g\colon A\to D\,。$$

如果上述 g 存在，则 A 为无限集，与题设矛盾。

构造映射

$$g:(A\cap B)\sqcup(A-B)\longrightarrow C\sqcup(A-B)$$

如下：

如果 $x\in A\cap B$ ， 则 $g(x)=f(x)$ 。 反之，如果 $x\in A-B$ 中，则 $g(x)=x$ 。

由于 f 为满射，故 g 也为满射（为什么？）。

下面我们来证明 g 是单射。

如果 $g(x)=g(y)$ ， 则 x 和 y 要么同在 $A-B$ 中，要么同在 $A\cap B$ 中。否则 $g(x)$ 和 $g(y)$ 会一个在 C 中，一个在 $A-B$ 中，从而不可能相等。

如果 x 和 y 同在 $A-B$ 中，则由 g 的定义和 $g(x)=g(y)$ ， 我们直接得到 $x=y$ 。

如果 x 和 y 同在 $A\cap B$ 中，由 g 的定义，我们知道 $g(x)=f(x)$ ， $g(y)=f(y)$ 。 我们假定了 $g(x)=g(y)$ ， 从而可以得到 $f(x)=f(y)$ 。 由于 f 为一一的，我们有 $x=y$ 。

因此，我们得到了 g 也是单射。

目前为止，我们证明了 g 也是一一的。注意到

$$(A\cap B)\sqcup(A-B)=A$$

且

$$C\sqcup(A-B)\subsetneq(A\cap B)\sqcup(A-B)=A\,,$$

我们通过 g 得到了 A 和其真子集 $C\sqcup(A-B)$ 之间的一一对应，从而 A 是无限集，与题设矛盾。 ∎

问题：如果将“ A 和 B 都是有限集”改为“ A 和 B 中有一个是有限集”，上述的证明是否仍然成立？

定理 1.3.3. 如果 A 和 B 都是有限集，则 $A\cup B$ 也是有限集。

这个定理的证明，比起前面“两个有限集的交为有限集”的证明要更难和更复杂一点（当然，从反证法入手的大体思路是一样的）。我们给出一个该定理的“简化版”，并附上证明。

定理 1.3.4. 如果 A 是有限集，则 $A\cup\{x\}$ 也是有限集。

证明： 不妨假定 $x\notin A$ ， 否则 $A\cup\{x\}=A$ ， 显然是有限集。

若 $A\sqcup\{x\}$ 不是有限，则其为无限。故而存在 $A\sqcup\{x\}$ 中的真子集 B ， 使得 $A\sqcup\{x\}$ 和 B 之间有一一对应。记这个从 $A\sqcup\{x\}$ 到 B 的一一映射为 f 。

情形一： $x \notin B$ 。 此情形下，$B \subset A$ 。

我们断言 $f(x) \notin f(A)$ 。不然，存在 $a \in A$ ， 使得 $f(x) = f(a)$ 。 由于 f 为一一的，我们有 $x = a \in A$ ， 故 $x \in A$ ， 与 $x \notin A$ 矛盾。

我们同时断言 $f(x) \neq x$ 。否则，我们有 $x = f(x) \in f(A \sqcup \{x\}) = B$ ， 故 $x \in B$ ， 与本情形假设 $x \notin B$ 矛盾。

由于 $f(x) \neq x$ ， 我们有 $f(x) \in A$ 。

考虑 f 在 A 上的限制，由于 $f(A) \subset f(A \sqcup \{x\}) = B \subset A$ ， 我们有 $f(A) \subset A$ 。

令 $g = f|_A : A \to A$ 。 由于 f 为单射， 故 g 也为单射。事实上，g 给出了 A 到 $g(A)$（注意 $g(A) = f(A) \subset A$）上的一个一一映射。

断言：$g(A) \subsetneq A$ 。该断言成立，因为从上面的论述，我们有 $f(x) \in A$ 且 $f(x) \notin f(A) = g(A)$ 。

至此，我们得到了 A 到 A 的一个真子集 $g(A)$ 上的一一对应，从而 A 是无限集，与题设矛盾。

情形二： $x \in B$。

对于一一映射 $f: A \sqcup \{x\} \to B$，因为 B 是 $A \sqcup \{x\}$ 的真子集且 $x \in B$，我们可得 $B \cap A$ 是A的真子集。不妨假定 $a \in A$ 且 $a \notin B \cap A$。令 $y = f^{-1}(x)$ 。 （ y 可能在 A 中，y 也可能就是 x ， 这个不重要）

定义 $g = f|_A$ ， 则 g 给出了 A 到 A 的子集 $g(A)$ 的一一对应。

定义映射 $g: A \sqcup \{x\} \to A \sqcup \{x\}$ 如下：如果 $c \neq y$ ， 则 $g(c) = f(c)$ 。 如果 $c = y$ ， 则 $g(c) = a$ 。 则 g 是个单射并且 $x \notin g(A \sqcup \{x\})$ 。 注意到 g 给出了 $A \sqcup \{x\}$ 到 $g(A \sqcup \{x\})$ 上的一一对应，并且 $x \notin g(A \sqcup \{x\})$ （从而 $g(A \sqcup \{x\})$ 为 $A \sqcup \{x\}$ 中的真子集），根据对于情形一的讨论，我们得到矛盾。

综上，证毕。 ∎

习题：

习题 1.3.1. 假定 X 和 Y 都是有限集，并且存在 X 到 Y 的单射 f 和 Y 到 X 的单射 g 。证明：f 和 g 必定都是满射。（据此可以得到有限集上的Cantor-Berstein定理）

习题 1.3.2. 证明 $\mathbb{N}$ 是无限集。证明 $\mathbb{Z}$ 是无限集。

习题 1.3.3. 证明如果 A 是无限集且 A 和 B 存在一一对应，则 B 也是无限集。

习题 1.3.4. 证明集合 $\{x\}$ 是有限集。

习题 1.3.5. 证明：如果 A 和 B 中有一个是有限集，则 $A\cap B$ 也是有限集。

习题 1.3.6. 证明：有限集合的子集仍然是有限集。

习题 1.3.7. 如果集合 A 是无限集且 A 是集合 B 的子集，证明 B 也一定是无限集。

1.4 基数

定义 1.4.1. 对于集合 X 和 Y，我们说 $|X|\leq|Y|$，如果存在 X 到 Y 的单射。

根据此定义，由于两个单射的复合仍然是单射，如果 $|X|\leq|Y|$ 且 $|Y|\leq|Z|$，则 $|X|\leq|Z|$。

注 1.4.1. 一个很自然的问题就是，可否将 $|X|\leq|Y|$ 定义为存在从 Y 到 X 的满射？这个想法很好，在大多数情况下也确实没有问题。但是对于非空集合 X，这样的定义无法得出 $|\emptyset|\leq|X|$。这是因为根据映射的定义，从非空集合到空集的映射是不存在的，而从空集到任何集合的映射总是存在的。

定义 1.4.2. 对于集合 X 和 Y，我们说 $|X|<|Y|$，如果 $|X|\leq|Y|$ 且 $|X|\neq|Y|$。

我们有如下的命题。该命题证明作为练习。

命题 1.4.1. 对于集合 X，Y 和 Z，如果 $|X|<|Y|$ 且 $|Y|\leq|Z|$，则 $|X|<|Z|$。

Cantor-Bernstein定理

下面的定理也被称为 Cantor-Schröder-Bernstein 定理。该定理之证明是构造性质的。

定理 1.4.1 (Cantor-Bernstein定理). 对于任意集合 X 和 Y，如果 $|X|\leq|Y|$ 且 $|Y|\leq|X|$，则 $|X|=|Y|$。

证明： 由题设假定，存在单射 $f\colon A\to B$ 和 单射 $g\colon B\to A$ 。需构造 A 到 B 的双射。定义

$$C=\bigcup_{n=0}^{\infty}(g\circ f)^n(A-g(B))\ 。$$

定义 $h\colon A\to B$ 为：

$$h(a)=\begin{cases} f(a), & a\in C \\ g^{-1}(a). & a\notin C \end{cases}\ 。$$

因为 g 为单射并且 $A-C\in g(B)$ ， 故 h 是良性定义的（具体的说，对于任意 $a\notin C$ ，$g^{-1}(a)$ 是存在并且唯一的）。

下面我们来证明 h 为 A 到 B 的双射。

先证明 h 为单射。

考虑 h 限定在 C 上的映射，不妨记为 $h|_C$ ， 因为 f 为单射，故 $h|_C$ 是单射。 因为 g 为映射，故 $h|_{A-C}$ 也为单射。

由于 $h(C)\cap h(A-C)=\emptyset$（为什么？） ， 我们可以得到 h 是单射。

下面来证明 h 是满射。

为此，我们先证明如下断言。

断言1：对于任意 $b\in B$ ， $b\in f(C)$ 当且仅当 $g(b)\in C$ 。

断言1之证明： 假定 $b\in f(C)$ ， 根据 C 的定义，存在 $n\in\mathbb{N}$ ， 使得 $b=f((g\circ f)^n(x))$ ，其中 $x\in A-g(B)$ 。 由于

$$g(b)=g(f((g\circ f)^n(x)))=(g\circ f)^{n+1}(x)\quad 其中\ x\in A-g(B)\ ，$$

根据 C 之定义，我们有 $g(b)\in C$ 。

反之，若 $g(b)\in C$ ， 则存在 $n\in\mathbb{N}$ 和 $x\in A-g(B)$ ， 使得

$$g(b)=(g\circ f)^n(x)\ 。$$

若 $n=0$ ， 则 $g(b)=x\in A-g(B)$ ， 矛盾。

由于 $n\geq 1$ ， 我们有

$$g(b)=(g\circ f)^n(x)=g\circ f\circ(g\circ f)^{n-1}(x)=g(f\circ(g\circ f)^{n-1}(x))\ 。$$

因为 g 为单射且 $x\in A-g(b)$，故

$$b=f(\circ(g\circ f)^{n-1}(x))\in f(C)\ 。$$

断言2：对于任意 $b\in B$ ， $b\in g^{-1}(A-C)$ 当且仅当 $g(b)\in A-C$ 。

断言2之证明： 如果 $b\in g^{-1}(A-C)$ ， 则 $g(b)\in g(g^{-1}(A-C))=A-C$ 。

反之，如果 $g(b) \in A - C$ ， 由于 g^{-1} 在 $A - C$ 上是良性定义的，我们有 $g^{-1}(g(b)) \in g^{-1}(A - C)$ 。 换言之，$b \in g^{-1}(A - C)$ 。

根据上述两个断言，$f(C) \sqcup g^{-1}(A - C) = B$ ， 故而 h 是满射。 ∎

Cantor基数定理

一个常见的关于基数的问题是：“最大”基数是否存在。下面的定理给出了否定的回答。

定理 1.4.2 (Cantor基数定理). 对于任意集合 X ， $|X| < |\mathcal{P}(X)|$ 。

证明： 为了证明 $|X| < |\mathcal{P}(X)|$ ， 我们需证明 $|X| \leq |\mathcal{P}(X)|$ 且 $|X| \neq |\mathcal{P}(X)|$ 。

为了证明$|X| \leq |\mathcal{P}(X)|$ ， 只需要验证如下映射

$$f\colon X \to \mathcal{P}(X), x \mapsto \{x\}$$

是单射即可。

下面我们来说明 $|X| \neq |\mathcal{P}(X)|$ 。 假设 $|X| = |\mathcal{P}(X)|$ ， 我们试图得出矛盾。

因为 $|X| = |\mathcal{P}(X)|$ ， 故存在双射 $f\colon X \to \mathcal{P}(X)$ 。 我们定义 $Y \in \mathcal{P}(X)$（换言之，$Y \subset X$）如下： 对于任意的 $x \in X$ ， 如果 $x \in f(x)$ ， 则 $x \notin Y$ 。 如果 $x \notin f(x)$ ， 则 $x \in Y$。

这样定义的 Y ， 一定满足 $Y \neq f(x)\ \forall x \in X$ 。 由于 Y 是 X 的子集，故 $Y \in \mathcal{P}(X)$ 。由于 f 是满射，故存在 $z \in X$ ， 使得 $Y = f(z)$ ， 这与 $Y \neq f(x)\ \forall x \in X$ 矛盾。

∎

基于**定理1.4.2**（Cantor 基数定理），我们可以断言 “由所有集合所构成的集合” 是不存在的。论证如下：

假定 X 是由所有集合构成的集合，考虑 $\mathcal{P}(X)$ 。 根据 Cantor 基数定理，$|X| < |\mathcal{P}(X)|$ 。由于 $\mathcal{P}(X)$ 是幂集，故其中的每个元素都是集合。因为 X 是由所有集合构成的集合，从而 $\mathcal{P}(X) \subset X$ ， 因此 $|\mathcal{P}(X)| \leq |X|$ 。 又注意到 $|X| < |\mathcal{P}(X)|$ ， 根据 Cantor-Bernstein 定理，$|\mathcal{P}(X)| = |X|$ ， 这与 $|X| < |\mathcal{P}(X)|$ 矛盾。

类似的，我们也可以证明：不存在集合 X ， 使得对于任意集合 Y ， 均有 $|Y| \leq |X|$ 。 换言之，“最大的集合” 是不存在的。当然，“最小的集合” 是存在的，它就是空集。

另外一个自然的关于基数之问题是：任意两个基数，是否总是可以比较大小？换言之，给定任意两个集合 X 和 Y ， 是否一定有 $|X| \leq |Y|$ 或者 $|Y| \leq |X|$ 中的至少一种成立？事实上，这个问题等价于基数的三歧律（trichotomy）。为了给出三歧律，我们需要承认选择公理（或者其定价形式）。关于选择公理，可以参看本章后面部分的内容。

定义 1.4.3 (三岐律). 我们说集合基数满足三岐律，如果对于任意集合 A 和 B ， 以下三种情况必有且仅有一种成立：i) $|A|<|B|$ ； ii) $|A|=|B|$ ； iii) $|B|<|A|$ 。

习题：

习题 1.4.1. 证明：对于集合 X ， Y 和 Z ， 如果 $|X|\leq|Y|$ 且 $|Y|<|Z|$ ， 则 $|X|<|Z|$ 。

习题 1.4.2. 证明：$|\mathbb{N}|=|\mathbb{N}\times\mathbb{N}|$ 。 这里 $\mathbb{N}$ 就是高中所定义的自然数集。

习题 1.4.3. 证明：对于任意 $m\in\mathbb{N}_{\geq 1}$ ， 证明 $|\mathbb{N}|=|\mathbb{N}^m|$ 。 这里 $\mathbb{N}$ 就是高中所定义的自然数集。

习题 1.4.4. 证明：$|\mathbb{Q}|=|\mathbb{N}|$ 。 这里 $\mathbb{N}$ 和 $\mathbb{Q}$ 分别是高中所定义的自然数和有理数。

习题 1.4.5. 证明**命题1.4.1**。

1.5 可数集，不可数集

定义 1.5.1 (可数集). 我们说集合 X 是可数集，如果 $|X|=|\mathbb{N}|$ 。

可数集也被称为可列集。直观的说，可数集总是可以写成一列的形式。这是由于如下的定理。

定理 1.5.1. 集合 X 是可数集，当且仅当 $X=\{x_1,x_2,\cdots,\}$ 。

证明： 对于可数集 A ， 我们需要找到一种方式，使得每个元素可以一一的写成 a 下标某个正整数的形式。

由于 A 是可数集，故存在 A 和 $\mathbb{N}$ 的一一对应。由于 $\mathbb{N}$ 和 $\mathbb{N}_{\geq 1}$ 之间有自然的一一对应。不妨设 $f\colon A\longrightarrow\mathbb{N}_{\geq 1}$ 为一一映射。

对于任意 $x\in A$ ， 我们将其记为 $a_{f(x)}$ 。

我们需要证明上面的记法是良性定义的（well defined）。换言之，我们需要确保 “如果 $x\neq y$ ， 则 $f(x)\neq f(y)$ ”。 由于 f 为单，上述要求是满足的。

同时，为了说明这样写下的集合 A 的下标没有空隙（比如 $\{a_1, a_5, a_6, \cdots\}$），我们需要 f 是满的。由于 f 为一一，故而 f 为满。证毕。 ∎

定义 1.5.2. 我们说无限集 X 是不可数集，如果 $|X| \neq |\mathbb{N}|$ 。 换言之，不可数集是基数不等于 $\mathbb{N}$ 之基数的无限集。

关于无限集，一个重要的事实是：可数集是基数最小的无限集。

定理 1.5.2 (自然数集/可数集是“最小”的无限集). 若集合 A 是无限集，则 $\aleph_0 \leq |A|$ 。

证明： 因为 A 是无限集，根据无限集的定义，存在 A 到其真子集 A_1 的一一映射，不妨记为

$$f\colon A \longrightarrow A_1 \text{ 。}$$

由于 $A_1 \subsetneq A$ ， 存在 $x \in A - A_1$ 。

断言1： $f(A_1) \subsetneq A_1$ 且 $f(x) \in A_1 - f(A_1)$ 。

断言1之证明： 事实上，由于 f 将 A 映到 A_1 ， 我们显然有 $f(A_1) \subset f(A) = A_1$ 。 对于上述的 $x \in A - A_1$ ， 因为 $x \in A$ ， 我们有 $f(x) \in f(A) = A_1$ 。 因为 $x \notin A_1$ 且 f 为单射，我们有 $f(x) \notin f(A_1)$ （若 $f(x) \in f(A_1)$ ， 则存在 $y \in A_1$ ， 使得 $f(x) = f(y)$ 。 由于 $x \notin A_1$ ， 我们有 $x \neq y$ 。 但是 $f(x) = f(y)$ 与 f 为单射矛盾）。故 $f(x) \in A_1 - f(A_1)$ ， 从而 $f(A_1) \subsetneq A_1$ 。

若我们将 $f(A_1)$ 记为 A_2 ， $f(A_2)$ 记为 A_3 ， $\cdots$ ， 类似的（为什么？），我们可以得到

$$A_{k+1} \subsetneq A_k \text{ 且 } f^k(x) \in A_k - A_{k+1} \text{ 。}$$

断言2： 如果 $k \neq j$ ， 则 $f^k(x) \neq f^j(x)$ 。

断言2之证明： 该断言比较容易证明，可以作为练习。

断言3： 存在从 $\mathbb{N}$ 到 A 的单射。

断言3之证明： 练习。

根据断言3，存在 $\mathbb{N}$ 到 A 的单射，故 $\aleph_0 \leq |A|$ 。 证毕。 ∎

注 1.5.1. 上述**定理1.5.2**的证明中，并没有用到选择公理。换言之，“自然数是基数最小的无限集”这个事实是不依赖于选择公理的。

习题：

习题 1.5.1. 大家所熟知的抽屉原理也称为鸽笼原理（Pidgeon Hole Principle），其最简单的情形就是如果有 $n+1$ 只鸽子和 n 个鸽笼，无论怎样将这些鸽子放入鸽笼中，一定有个鸽笼中至少有 2 只鸽子。关于这种鸽笼原理的证明，也是反证法的典型例子。

基于目前所学集合论的知识，证明如下的广义鸽笼原理：

集合 X 为不可数集，下标集 A 为可数集。假定

$$X = \bigsqcup_{i \in A} X_i \ 。$$

则一定存在某个 $k \in A$ ， 使得 X_k 为不可数集。换言之，若将不可数集分为可数多份，则其中至少有一份仍然是不可数集。

习题 1.5.2. 证明**定理 1.5.2**中的断言2。

习题 1.5.3. 证明**定理 1.5.2**中的断言3。

1.6 选择公理

选择公理（Axiom of Choice）是现代数学中很重要的一条公理。选择公理的内容初看起来平淡无奇，但是它是很多重要数学理论的基础之一，而且可以蕴含很多看似与直观相悖的结果。虽然刚开始理解起来比较困难，但是（虽然很多时候看起来不是很明显）在现代数学中的很多地方选择公理确实是不可缺少的（这点我们会给出简单的说明）。我们在此会给出选择公理的介绍。

公理 (选择公理，Axiom of Choice). 设 C 为一个集合，其中每个元素都是一个非空集合，则我们可以从 C 中的每个元素（一个非空集合）中选择一个元素。用数学的语言来讲，存在

$$f \colon C \to \bigcup_{x \in C} x$$

满足 $f(c) \in c \ \forall c \in C$ 。

选择公理引入之初，是一条很有争议的公理。它看起来如此明显，并且很多“自然”的结果也需要选择公理来支持。同时，基于选择公理，又可以得出很多看起来难以想象，与直观完全相悖的结论（比如著名的Banach-Tarski悖论等等）。1963年，Cohen证明了选择公理是独立于ZF集合公理体系的。换言之，无论将选择公理还是将其否作为公理加入ZF公理体系中，都是不会有矛盾的。这样一个自然的问题就是，是否要将选择公理作为数学的基石？随着对选择公理（以及其等价形式，比如佐恩引理等）认识的深入，以及越来越多“基础”的结果（比如泛函分析中的Hahn-Banach定

理等）的确需要选择公理，目前主流的数学是默认承认选择公理的。换言之，目前的主流数学，是构建于ZFC（ZF + AC）公理体系上的。

如果我们承认选择公理，那么我们可以得到：

1. 佐恩引理（Zorn's Lemma）：如果一个偏序集（poset） $(X,\leq)$ 中的任意非空有序链皆有上界，则一定存在着极大元 x （我们说 x 是极大的，是指对于任意的 X 中元素 $y\neq x$ ， 均不可能有 $x\leq y$）。

2. 三歧律（Trichotomy Law）： 对于任意两个集合 A 和 B ， 以下三种情况必有一种（且仅有一种）成立： i）$|A|<|B|$ ； ii）$|A|=|B|$ ； iii）$|A|>|B|$ 。

3. Banach-Tarski悖论： 一个半径为 1 的球可以通过拆分为有限部分并重组（刚体变换）的方式得到两个半径为 1 的球。

注 1.6.1. 选择公理中的“选择”，可以是从无限种可能中选择，也可能是从有限种可能中选择（比如两种可能中）。

注 1.6.2. 如果前面选择公理定义中的集合 C 是包含有限个元素（其中每个元素是非空集），那么这样的选择总是存在的（不需要额外假定选择公理）。直观的说，这是因为我们可以在“有限步“完成这样的选择。从数学上讲，有限集合对应着从 1 到某个 n 的自然数。而根据数学归纳法，只要我们可以进行“多一次选择”，我们就一定可以进行“有限次”选择。

注 1.6.3. 和连续统假设（CH）不同，如果你的结论用到了选择公理（AC），你不需要单独指出使用了AC这个事实，因为目前主流数学的基石是ZFC，也就是ZF + AC。

注 1.6.4. 在很多场合，佐恩引理（Zorn's Lemma，选择公理的等价形式之一）使用起来更为直接和方便。

问题：定义集合 $X_1=\{1\}$ ， $X_2=\{1,2\}$ ， $X_3=\{1,2,3\}$ ， $\cdots$ 。 在下面的叙述中，是否分别用到了选择公理？为什么？

1）取 $x_1\in X_1$ 。

2）对于给定的自然数 n（$n\geq 1$）取 $x_1\in X_1$ ， $x_2\in X_2$ ， $\cdots$ ， $x_n\in X_n$ 。

3）取 $x_1\in X_1$ ， $x_2\in X_2$ ， $\cdots$。

4）在每个集合 X_k 中，取其中的最大元素 x_k ， 这样我们就得到 $x_1\in X_1$ ， $x_2\in X_2$ ， $\cdots$。

初学者一个很自然的误解就是：选择公理是人为制造出来的一个非自然的东西。下面我们通过一个例子来说明选择公理某种意义上是不可或缺，并且很可能使用了选择公理而不自知。

例 1.6.1 (无穷多个集合的乘积). 集合的乘积是非常自然的概念。对于集合 $X_1,X_2,\cdots$ ， 我们定义它们的积为

$$X_1\times X_2\times\cdots=\{(x_1,x_2,\cdots):x_i\in X_i\ \forall i\in\mathbb{N}_{\geq 1}\}\ 。$$

比如，对于 $[0,1]\times[0,1]$ （可以记为 $[0,1]^2$），它是个二位的方块。$[0,1]^3$ 是个立方体。可数多个 $[0,1]$ 的乘积被称为 Hilbert Cube ，记为 $[0,1]^\infty$ 。

我们知道 $[0,1]$ 不是空集， $[0,1]^2$ 不是空集，$[0,1]^3$ 不是空集，$\cdots$ 。 那么 $[0,1]^\infty$ 是不是空集呢？答案是否定的。因为我们知道 $(0,0,0,\cdots,)\in[0,1]^\infty$ 。

对于集合 $X_1 \times X_2 \times \cdots$ ， 如果 X_i 中有一个为空集，根据定义，$X_1 \times X_2 \times \cdots$ 一定是空集。如果每个 X_i 都不是空集，那么 $X_1 \times X_2 \times \cdots$ ， 一定也不是空集吗？ 正确答案是：这取决于你是否假定选择公理。如果假定选择公理，那么在每个 X_i 都不是空集的前提下， $X_1 \times X_2 \times \cdots$ 一定也不是空集。如果没有选择公理，对于一般的情况（这些一般的 X_i 之间未必什么关系，比如两两相等或者交集非空等等），如果不假定选择公理，是无法在 $X_1 \times X_2 \times \cdots$ 中找到任何元素的。

习题：

例 1.6.2. 定义集合 A 为

$$\{(a_1, a_2, \ldots,): a_i \in \{0, 1, 2, \cdots, 9\},\ \forall i\}$$

其中两个元素相等当且仅当它们的每个分量都相等。证明这样的集合 A 是不可数集合。额外要求：在证明中禁止使用选择公理

例 1.6.3. 为了证明 $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ ， 是否需要选择公理？

例 1.6.4. 任意给定满射 $f: A \to B$ ， 在不假定选择公理的前提下，是否一定存在映射 $g: B \to A$ ， 满足 $f \circ g = \mathrm{id}_B$ ？ 如果假定选择公理呢？

例 1.6.5. 对于 $X_1 = \{1\}$ ， $X_2 = \{1, 2\}$ ， $X_3 = \{1, 2, 3\}$ ， $\cdots$ ， 在不假设选择公理的前提下，可否得出 $X_1 \times X_2 \times X_3 \times \cdots$ 非空？仍然不假定选择公理，可否得出 $X_1 \times X_2 \times X_3 \times \cdots$ 至少包含可数无穷多个元素？不使用选择公理，可否得出 $X_1 \times X_2 \times X_3 \times \cdots$ 是不可数集？

1.7 序关系

我们先定义“关系”。

定义 1.7.1 (关系). 给定集合 X 和 Y ， X 和 Y 的一个关系，是指 $X \times Y$ 中的一个子集 R 。 如果 $(x, y) \in R$ ， 则记为 xRy 。

上面的定义是相当抽象的，关于关系本身（作为$X \times Y$中的一个子集），没有任何限制。

下面我们将定义集合上的序（偏序）关系、全序关系和良序关系。

简单的说，序（偏序）关系是一种特殊的关系，全序关系是一种特殊的偏序关系，良序关系是一种特殊的全序关系。

定义 1.7.2 (偏序关系). 给定集合 X ， 其上的一个偏序（partial order）关系是 $X \times X$ 中的一个子集 R ， 满足

1) $xRx, \forall x \in X$ （**自反性**）

2) 若 xRy 且 yRz ， 则 xRz （**传递性**）

3) 若 xRy 且 yRx ， 则 $x = y$ （**反对称性**）

偏序关系 R 也可以记为 $\leq_R$ 。 换言之，如果 xRy（或者等价的，$(x,y) \in R$），则记为 $x \leq_R y$ 。 在没有歧义的情况下，可以进一步简记为 $x \leq y$ 。 上述偏序集合（具有偏序关系的集合）可记为 (X,R) 或者 $(X,\leq)$ 。

根据上面序（偏序）关系的定义，并不是所有 $X \times X$ 中的子集 R 都可以定义一个序关系的（虽然的确可以定义一个关系）。只有满足自反性、传递性和反对称性的关系，才是序（偏序）关系。

例 1.7.1. 在 $\mathbb{R}$ 中，考虑通常意义下的 $<$ 关系。则该关系不是序（偏序）关系。这是因为 $<$ 关系不满足自反性。

定义 1.7.3 (偏序集). 如果集合 X 上有偏序关系 $\leq$ ， 则我们称 $(X,\leq)$ 为偏序集（partially ordered set, or in brief, poset）。

基于偏序，我们可以定义极大元（maximal element）和极小元（minimal element）。

定义 1.7.4 (极大元、极小元). 给定偏序集 (X,R) ， 对于 $D \subset X$ ， 我们说 $x \in X$ 是该偏序集子集 D 上的极大元（maximal element），如果对于任何 $y \in X$ ， 要么 $(x,y) \notin R$ 且 $(y,x) \notin R$ ， 要么 $(y,x) \in R$ 。 简单的说，我们说 x 是偏序集 $(X,\leq_R)$ 上的极大元，如果 x 不小于 X 中任何元素。我们说 $x \in X$ 是该偏序集子集 D 上的极小元（minimal element），如果对于任何 $y \in X$ ， 要么 $(x,y) \notin R$ 且 $(y,x) \notin R$ ， 要么 $(x,y) \in R$ 。 简单的说，我们说 x 是偏序集 $(X,\leq_R)$ 上的极小元，如果 x 不大于 X 中任何元素。

同时，基于偏序，我们也可以定义最大元（greatest element）和最小元（smallest element）。

定义 1.7.5 (最大元、最小元). 给定偏序集 (X,R) ， 对于 $D \subset X$ ， 我们说 $x \in D$ 是该偏序集子集 D 上的最大元（greatest element），如果对于任何 $y \in D$ ， 我们有 $y \leq x$ 。 我们说$x \in D$ 是该偏序集子集 D 上的最小元（least element），如果对于任何 $y \in D$ ， 我们有 $x \leq y$ 。

注 1.7.1. 极大元、极小元未必存在。比如，在 $(\mathbb{R},\leq)$ 中（其中 $\leq$ 为实数通常意义下的小于等于），令 $D=X$ ， 则 D 中不存在极大元或者极小元。类似的，最大元、最小元也未必存在。但是，如果最大元存在，必定是唯一的。如果最小元存在，必定也是唯一的。极大/极小元即使存在，也未必是唯一的，这方面的例子不难构造。

如果在序关系（偏序关系）的基础上，额外要求任意两个元素都是可以“比较大小”的，则这个关系就是全序关系。

定义 1.7.6 (全序 (关系)). 对于集合 X 上的序关系 R ， 如果对于任意 $x,y\in X$ ， 总有 xRy 或者 yRx ， 则称该序关系为全序（关系）。

例 1.7.2. 在集合$\mathbb{N}_{\geq 1}$上，定义关系如下：$m\leq n$ 当且仅当 $m|n$ 。则这个关系是序关系，但不是全序关系。比如考虑 3 和 5 之间的整除关系，我们有 $3\nmid 5$ 且 $5\nmid 3$ 。

例 : 对于非空集合 X ， 考虑 $R=\{(x,x)\colon x\in X\}\subset X\times X$ 。 容易验证该关系是序关系，但不是全序关系。

定义 1.7.7 (全序集). 如果集合 X 上的序关系 R 是个全序关系，则称 X 是关于 R 的全序集。

例 1.7.3. 设 X 为非空集。对于 $x,y\in\mathcal{P}(x)$ ， 定义 $x\leq y$ 为 $x\subset y$ 。 可以直接验证该关系的确是序（偏序）关系，但是不是全序关系。

定义 1.7.8 (良序 (关系)). 对于集合 X 上的序关系 R ， 如果对于任意 X 中的非空子集 D ， 总是存在 $x\in D$ ， 满足 xRy ， $\forall y\in D$ ， 则称该序关系为良序关系，或者简称该序是良序。

类似的，我们可以定义良序集。

定义 1.7.9 (良序集). 对于集合 X 上的序关系 R 是个良序关系，则称 X 是关于 R 的良序集。

注 1.7.2. 根据定义，可以直接验证全序关系一定是序（偏序）关系。可能没有这么明显的事实是：良序关系一定是全序关系。该事实的证明留作练习。

例 1.7.4. 考虑实数集 $\mathbb{R}$ ， 其上的序关系 xRy 定义为 $x\leq y$（或者等价的： $y-x\geq 0$ ）。容易验证这个序关系是全序，但是不是良序。考虑非负实数 $\mathbb{R}_{\geq 0}$ 上的序关系（定义如前），该序关系是全序的，但也不是良序的。比如，考虑其中的子集 $\{\frac{1}{n}\colon n\in\mathbb{N}_{\geq 1}\}$ 。 在这个子集中，是不存在最小的元素的。

例 1.7.5. 考虑自然数集 $\{0,1,2,\cdots,n\}$ ， 其上的序关系 xRy 定义为 $x\leq y$（或者等价的： $y-x\geq 0$ ）。可以验证这个序关系是全序，也是良序。

例 1.7.6. 考虑整数集 $\mathbb{Z}$ ， 其上的序关系 xRy 定义为 $x\leq y$（或者等价的： $y-x\geq 0$ ）。可以验证这个序关系是全序，但不是良序。

定义 1.7.10 (良序集). 如果集合 X 上的序关系 R 是个良序关系，则称 X 是关于 R 的良序集。

例 1.7.7. 对于自然数 $\mathbb{N}$ ， 考虑在高中学过的 $\mathbb{N}$ 上的大小比较关系（序关系），$\mathbb{N}$ 在该序关系下是个良序集。类似的，$\mathbb{Z}$ 在大小比较关系下也是一个良序集。实数集 $\mathbb{R}$ （在通常的序关系下）并不是个良序集合。如果考虑 $\mathbb{R}$ 的子集 $\mathbb{R}_{>0}$ ， 我们是无法找到其中的最小元素的。

在上面的例子中，在通常的序关系下，实数集 $\mathbb{R}$ 并不是良序集。但是我们可以在 $\mathbb{R}$ 上赋上（定义）新的序关系，使得 $\mathbb{R}$ 在新的序关系下是良序集。这是因为我们有如下的良序化公理/定理（在承认选择公理的前提下）。

公理 (良序化公理). 任何集合都是可以良序化的。

事实上，良序化公理和前面的选择公理（或者佐恩引理）是等价的。我们会在介绍完佐恩引理后给出这些等价关系的证明，有兴趣的读者可以参考。

习题：

习题 1.7.1. 给定偏序集合 $(X, \leq_X)$ 和 $(Y, \leq_Y)$ 。 在 $X \times Y$ 上定义 $\leq$ 如下：

$$(x_1, y_1) \leq (x_2, y_2) \text{ 当且仅当 } x_1 \leq_X x_2 \text{ 且 } y_1 \leq_Y y_2 \text{ 。}$$

证明上述定义的 $\leq$ 给出了 $X \times Y$ 上的一个序（偏序）关系。

习题 1.7.2. 证明任何良序集一定是全序集。

习题 1.7.3. 证明：对于偏序集 $(X, \leq)$ ， 若其非空子集 D 上的最大元存在，则最大元必唯一。若 D 上的最小元存在，则最小元必唯一。

习题 1.7.4. 给出一个偏序集，使得其上不存在极大元。或者，要求更高点，给出一个全序集，使得其上不存在极大元。

1.8 序数

1.9 超限归纳法

超限归纳法（Transfinite Induction）可以看成数学归纳法的某种扩展。数学归纳法是基于自然数 $\mathbb{N}$ 的Peano公理体系的，其适用范围为下标集为 $\mathbb{N}$ 的情形。普通的数学归纳法（基于自然数

$\mathbb{N}$ 的） 之正确性，本质上是个集合论的问题。

例如，所谓的“第一类数学归纳法”，等价于：假定 $\mathbb{N}$ 的子集 D 满足 $0\in D$ ， 并且如果 $x\in D$ ， 则 $x^+\in D$ 。 那么 $D=\mathbb{N}$ 。 而所谓的“第二数学归纳法”，等价于：假定 $\mathbb{N}$ 的子集 D 满足 $0\in D$ ， 并且对于任意 $x^+\in\mathbb{N}$ ， 如果 $\mathbb{N}_{\leq x}\subset D$ ， 则 $x\in D$ 。 那么 $D=\mathbb{N}$ 。

超限归纳法的适用范围为良序集。具体的说，超限归纳法是指如下的事实：设 A 是良序集，设 a_0 为 A 中的最小元素。假定 1） 性质 $P(a_0)$ 成立；2）对于任意 $a\in A$ ， 若性质 $P(x)$ 对于任意 $x\in A_{<a}$ 均成立，则性质 $P(a)$ 也成立。那么可以断言对于任意 $a\in A$ ， 性质 $P(a)$ 均是成立的。

下面，我们来证明超限归纳法的正确性。正如前面所言，本质上是一个集合论的问题。

定理 1.9.1 (超限归纳法). 对于（非空）良序集 A ， 用 a_0 代表 A 之唯一最小值。如果 A 之子集 D 满足

1） $a_0\in D$

2）对于任意 $a\in A$ ， 如果 $\{x\in A\colon x<a\}\subset D$ ， 则 $a\in D$ ，

则 $D=A$ 。

注 1.9.1. 在上述定理叙述中，不难验证条件 2）是包含条件 1）的（因为 $\emptyset\subset D$ ）。我们这里故意冗余的写出了条件 1），是为了强调归纳起点是得到满足的。

证明： 假定 $D\subsetneq A$ ， 则 $A-D\subset A$ 且 $A-D\neq\emptyset$ 。 由于 A 是良序集，故存在 $A-D$ 中的最小元，不妨记为 b 。 对于任何 $x<b$ ， 若 $x\notin D$ ， 则 $x\in A-D$ 。 而这与 b 是 $A-D$ 中的最小元矛盾。

由于 $\{x\in A\colon x<b\}\in D$ ， 根据条件 2），$b\in D$ 。 而这与 $b\in A-D$ 矛盾。 ∎

在上述的证明中，关键用到了良序集的非空子集一定有最小元这个事实。如果上面的集合 A 不是良序集，则类似的 A 上之归纳法未必成立。

在关于 $\mathbb{N}$ 的通常数学归纳法中，分别有第一归纳法和第二归纳法。

（自然数集上）第一归纳法： 若性质 P 在 $n=0$ 时成立（记为 $P(0)$ 成立），且对于任意 $n\in\mathbb{N}$ ， 如果 $P(n)$ 成立则 $P(n+1)$ 成立，则性质 $P(k)$ 对于所有的自然数 k 都成立。

（自然数集上）第二归纳法： 若性质 P 在 $n=0$ 时成立（记为 $P(0)$ 成立），且对于任意 $n\in\mathbb{N}$ ， 如果 $P(s)$ 对于所有 $s<n$ 成立则 $P(n)$ 成立，则性质 $P(k)$ 对于所有的自然数 k 都成立。

注 1.9.2. 形式上看起来，超限归纳法相当于“良序集”上的第二归纳法。有没有良序集上的“第一归纳法”呢？

假定 A 是良序集。对于给定的 $a\in A$ ， 什么是 a 的后继（不妨记为 a^+ 或者 $a+1$）？首先，后继是未必存在的。比如考虑良序集 $1,2$ （其中序关系就是通常的大小关系）。其中 2 就是没有后继的。虽然如此，我们还是可以用如下的方式定义良序集中的后继。

定义（良序集上的后继元）： 在良序集 A 中，对于 $a\in A$ ， 如果 $(a,>):=\{x\in A\colon x>a\}$

非空，则定义 a 的后继（记为 $a+1$ ）为

$$a+1=\min(a,>) \text{ 。}$$

由于 A 是良序集合，因此任意非空集合存在最小值，从而上述定义是良性的。

事实上，根据上述定义：不难得到在任何良序集 A 中，不存在后继的元素最多只有一个，如果该元存在，则一定是最大元（即大于等于任何其他元）。换言之，在良序集中，除了最多一个例外，上述定义的后继元总是存在的。

基于上述定义，我们是否有类似的良序集上的第一归纳法？换言之，下述关于良序集的猜想是否成立？

猜想： 设 A 为（非空）良序集，并用 a_0 代表 A 上的唯一最小值。如果 A 中子集 D 满足：

1) $a_0 \in D$

2) 对于任意 $a \in A$ ， 如果 $a \in D$ ， 则如上定义的后继元 $a+1 \in D$ ，

则 $D=A$ 。

该猜想是错的！最简单的反例可能如下：

令 $A=\mathbb{N}\cup\{\omega\}$ 。 除了 $\mathbb{N}$ 上的自然序关系，额外定义 $m \leq \omega \quad \forall m \in \mathbb{N}$ 。

正如常见的数学归纳法一样，超限归纳法本身意义不大，就是普通的关于集合论的练习。其真正意义在于应用。

我们前面给出了良序化公理的证明。如果我们承认选择公理（这个问题不大，因为目前主流数学是构建在ZFC公理体系上的），那么任意集合均是可以良序化的。而基于良序集，我们可以做超限归纳法。

在实际应用中，超限归纳法往往是结合了良序化公理的（如果原来没有良序结构的话）。

下面我们通过一个例子来演示超限归纳法的应用。这个例子是用到了良序化公理的（因而用到了选择公理）。

定理 1.9.2 ($\mathbb{R}^3-\{0\}$ 可以剖分成直线的无交并). 令 $X=\mathbb{R}^3-\{0\}$ ， 则可以将 X 剖分成 $\mathbb{R}^3$ 中的直线之无交并。

注 1.9.3. 若将 X 换为 $\mathbb{R}^2-\{0\}$ ， 则 X 不可能剖分成 $\mathbb{R}^2$ 中的直线之无交并。为什么？

证明： [定理 1.10.2]

根据良序化公理，我们可以在 $X=\mathbb{R}^3-\{0\}$ 上引入良序关系 $\leq$ 。 基于此良序集 $(X,\leq)$ ，我们用超限归纳法来完成证明。

我们首先证明如下断言。

断言： 若 $\bigsqcup_{i\in A} L_i \subsetneq \mathbb{R}^3-\{0\}$ ， 则一定存在 $\mathbb{R}^3$ 中直线 L ， 使得

$$\left(\bigsqcup_{i\in A} L_i\right)\bigsqcup L \subsetneq \mathbb{R}^3-\{0\} \text{ 。}$$

这里每个 L_i 都是 $\mathbb{R}^3$ 中的直线，A 是下标集。

QQQ

∎

1.10 佐恩引理

简单的说来，佐恩引理（Zorn's Lemma）指的是：如果一个有序（偏序）集中任何有序链（全序子集）都有上界，则该偏序集中存在极大元。佐恩引理和选择公理是等价的，但是在很多场合，佐恩引理使用起来更为方便。目前佐恩引理（Zorn's Lemma）已经广泛应用于近代数学中。比如近代泛函分析基石之一的Hahn-Banach定理就是基于佐恩引理的。

叙述佐恩引理前，先回顾下偏序集中的一些概念。

令 $(X, \leq)$ 为有序集（偏序集），我们说子集 D 有上界，如果存在 $x \in X$ ， 使得 $d \leq x$ $\forall d \in D$ 。 我们说子集 $D \subset X$ 是个全序子集，如果 $(D, \leq)$ 是个全序集。

我们说有序集（偏序集） $(X, \leq)$ 有极大元（极大元素），如果存在 $x \in X$ ， 使得若 X 中元素 y 满足 $x \leq y$ ， 则一定有 $x = y$ 。

下面我们来给出佐恩引理的**定义**。

定义 1.10.1 (佐恩引理). 在（偏序）有序集 $(X, \leq)$ 上，如果任意链（换言之，全序子集）均有上界，则 X 中一定存在极大元素。

佐恩引理可以由选择公理（Axiom of Choice）推出。

定理 1.10.1 (选择公理 $\Rightarrow$ 佐恩引理). 如果我们承认选择公理，则佐恩引理成立。

QQQ

前面我们提到过，选择公理，佐恩引理还有三歧律都是相互等价的。这里我们来从佐恩引理推出三歧律。

定理 1.10.2 (佐恩引理 $\Rightarrow$ 三歧律). 如果我们承认佐恩引理，则有如下关于集合基数的三歧律 任意两个集合 X 和 Y ， $|X| < |Y|$ $|X| = |Y|$ 和 $|X| > |Y|$ 这三种情况必有一种成立，且仅有一种成立。

证明： 根据基数小于关系的定义和Cantor-Bernstein定理，我们可以证明上述三种关系最多只有一种成立。

下面我们来证明三种关系中至少有一种成立。具体的，对于集合 X 和 Y ， 我们不妨假设 $|X|<|Y|$ 和 $|X|=|Y|$ 都不成立。下面我们来证明 $|X|>|Y|$ ， 换言之，存在从 Y 到 X 的单射。

如果 Y 为空集，根据映射的定义，一定存在 Y 到 X 的单射。

如果 Y 不为空集，则我们在如下集合 $\mathcal{A}$ 上定义偏序关系

$$\{f \mid f\colon D \to Y,\ \text{其中 } D \subset X \text{ 且 } f \text{ 为单射}\}$$

为: 若 f 之定义域 $D(f)$ 为 g 之定义域 $D(g)$ 的子集且 $g\big|_{D(f)} = f$ ， 则称 $f \le g$ 。

可自行验证该关系的确是序关系（满足自反性、反对称性和传递性）。

在该序关系下，考虑 $\mathcal{A}$ 中的任意全序子集 $\mathcal{B}$ 。 定义映射 h 如下：

h 的定义域为 $\bigcup_{f\in\mathcal{B}} D(f)$ 。 对于任意 $x \in D(h) = \bigcup_{f\in\mathcal{B}} D(f)$ ， 定义 $h(x) = g(x)$ ， 其中 $g \in \mathcal{B}$ 且 $x \in D(g)$ 。 注意，这样的 g 未必是唯一的。但是根据 $\mathcal{A}$ 中序关系的定义，以及注意到 $\mathcal{B}$ 是个全序子集，我们关于 h 的定义仍然是良性的。

由于 $\mathcal{B}$ 中每个 f 都是单射，故 h 也是单射。事实上，若存在 $x, y \in D(h)$ ，使得 $h(x) = h(y)$ ， 根据 $D(h)$ 的定义，存在 $f \in \mathcal{B}$ ， 使得 $x, y \in D(f)$ 。 根据 $\mathbb{A}$ 中序关系的定义，且注意到 $\mathbb{B}$ 是全序集，我们有 $h\big|_{D(f)} = f$ 。 故而 $f(x) = f(x)$ ， 这与 f 是单射矛盾。

根据 h 的定义，我们有 $f \le h$ ， $\forall f \in \mathcal{B}$ 。

至此，我们证明了，$\mathcal{A}$ 中的任意全序子集 $\mathcal{B}$ 一定是有上界的。根据佐恩引理，$\mathcal{A}$ 中一定有极大元。不妨设 H 为极大元。则我们可以断言 $D(H) = Y$ 。

事实上，如果 $D(H) \subsetneq Y$ ， 则存在 $b \in Y - D(H)$ 。 由于 D 为单射并且 $|X| \neq |Y|$ ，我们有 $H(Y) \subsetneq X$ （否则就有 $|X| = |Y|$ ， 矛盾）。取 $a \in X - H(Y)$ 。 定义

$$H'\colon D(H) \sqcup \{b\} \longrightarrow X,\ b \mapsto a \text{ 且 } y \mapsto H(y),\ \forall y \in H(Y) \text{ 。}$$

则 H' 也是单射，故而 $H' \in \mathcal{A}$ 。 注意到 $H \le H'$ 且 $H \neq H'$ ， 故 H 不是 $\mathcal{A}$ 中的极大元，矛盾。

证毕。 ∎

类似的，如果承认佐恩引理，则我们可以得到选择公理。

定理 1.10.3 (佐恩引理 $\Rightarrow$ 选择公理). 如果我们承认佐恩引理，则可以得到选择公理（Axiom of Choice）。

证明： 基本的思路，和上面佐恩引理推出三岐律之证明中部分内容之思路大体一致。

假定佐恩引理成立，我们来证明选择公理。换言之，给定非空集合 Y_i ， 其中 $i \in X$ ， 而 X 是某个下标集，我们一定可以找到映射 $H\colon X \to \cup_{i\in A} Y_i$ ， 使得 $H(x) \in Y_x$ ， $\forall x \in X$ 。

定义 $\mathcal{A}$ 为所有这样的映射 g 全体构成的集合，其中 g 的定义域 $D(g)$ 是 X 的子集，并且对任意 $x \in D(g)$ ，我们有 $g(x) \in Y_x$ 。 在 $\mathcal{A}$ 上定义 $\le$ 关系为：如果 $D(f) \subset D(g)$ ， 并且 $g\big|_{D(f)} = f$ ， 则称 $f \le g$ 。

类似于上面的证明，可以验证上述定义的 $\leq$ 关系的确是序关系。

对于 $\mathcal{A}$ 中的任意全序子集 $\mathcal{B}$ ， 一定存在 $\mathcal{B}$ 的上界，定义为

$$h\colon \bigcup_{f\in\mathcal{B}} D(f)\to\bigcup_{i\in X} Y_i,\ \ h(x)=f(x)\ \text{其中}\ x\in D(f)\ \text{且}\ f\in\mathcal{B}\ 。$$

在上面的定义中，满足 $x\in D(f)$ 且 $f\in\mathcal{B}$ 的 f 当然未必是唯一的，但是根据 $\mathcal{A}$ 上 $\leq$ 关系的定义，我们知道上面的 h 仍然是良性定义的。另外，我们在定义 h 的时候是没有借助选择公理的（当然，也不能用选择公理，因为这是我们要证明的结论）。

根据佐恩引理，$\mathcal{A}$ 中一定存在极大元，不妨设 H 为极大元。我们可以断言 H 的定义域为整个下标集 X （否则，取定 $a\in X-D(H)$ ， 我们一定可以找到映射 $H'\colon D(H)\sqcup\{a\}\to\bigcup_{i\in X}Y_i$ ，满足 $H'(x)\in Y_x$ ， $\forall x\in D(H')$ 且 $H'\big|_{D(H)}=H$ ，而这与 H 是 $\mathcal{A}$ 中极大元矛盾）。

至此，证毕。 ∎

下面，我们来证明佐恩引理（或者选择公理）与前面的良序化公理是相互等价的。为了简单起见，我们采用的证明路径是：佐恩引理推出良序化公理，良序化公理推出选择公理，然后利用上面已经证明的佐恩引理和选择公理的等价性。

定理 1.10.4. 佐恩引理蕴含良序化公理。

证明： 给定集合 X ， 我们试图在其上赋予一个良序结构。

大体思路如下：我们首先在 X 的子集上试图给出良序结构。例如，在 X 的子集 $\{x,y\}$ 上，良序结构总是存在的。考虑所有这些子集上的良序结构（不同子集上的序结构可能不一样），对于“相容”的良序结构，根据佐恩引理证明“最大的良序结构”存在。而“最大的良序结构”一定是定义在整个 X 上的。

下面是具体证明：

QQQ ∎

定理 1.10.5. 良序化公理蕴含选择公理。

证明： 设 C 为一个集合，其中每个元素都是一个非空集合。考虑

$$A=\bigcup_{c\in C} c\ 。$$

在集合 A 上，根据良序化公理，可以引入一个良序 $\leq$ 。 由于 $(A,\leq)$ 是良序的，因此对于任意 $c\subset A$ ， $(c,\leq)$ 也是良序的。

构造如下的选择函数即可完成证明：

$$f\colon C\longrightarrow\bigcup_{c\in C} c=A,$$

其中对于任意 $c\in C$ ， $f(c)$ 为良序集 $(c,\leq)$ 上的最小元。 ∎

DRAFT [March 4, 2015]

第2章

自然数、有理数和实数

2.1 Peano公理体系、数学归纳法

意大利数学家Peano通过如下的五条公理来刻画自然数（给出自然数的定义）：

1) $0 \in \mathbb{N}$ （这里 0 只是一个记号，写成阿拉伯数字 0 的样子是为了和常用的习惯记法一致）

2) 存在一个后继映射（Next） $^+ : \mathbb{N} \longrightarrow \mathbb{N}$

3) 不存在 $n \in \mathbb{N}$ ， 使得 $n^+ = 0$

4) $^+$ 是单射

5) 如果有 $\mathbb{N}$ 的子集 D ，满足 $0 \in D$ 且对于任意的 $n \in D$ 都有 $n^+ \in D$ ， 则 $D = \mathbb{N}$

其中第5条公理又被称为归纳公理，这是关于自然数的数学归纳法成立的基础。

在讨论基于Peano公理的性质之前，我们先考虑如下问题：Peano公理是不是良性定义的？换言之，满足Peano公理的数学对象是否存在？如果存在，这样的数学对象是否唯一？只有这两点都同时成立的时候，我们才可以说“Peano公理完全的刻画/定义了自然数集 $\mathbb{N}$ ”。

关于满足Peano公理的数学对象的存在性，一种作弊的方法是：既然Peano公理是大家广泛承认的，因此一定存在符合Peano公理的数学对象。这种“’聪明’的做法并不能在数学上说明问题。

基于Peano公理，我们可以得到自然数的如下性质。

定理 2.1.1. 对任意 $n \in \mathbb{N}$ ， 我们有 $n \neq n^+$ 。

证明： 设 $M = \{n \in \mathbb{N} : n \neq n^+\}$ 。 根据Peano公理（**第几条？**），$0 \in M$ 。 如果 $n \in M$ ，我们来证明 $n^+ \in M$ 。

事实上，如果 $n \in M$ ， 则 $n \neq n^+$ 。 如果 $n^+ \notin M$ ， 则 $n^+ = (n^+)^+$ 。 根据Peano公理（**第几条？**），我们有 $n = n^+$ ， 矛盾。故如果 $n \in M$ ， 则 $n^+ \in M$ 。 根据Peano公理中的归纳公理，$M = \mathbb{N}$ 。 证毕。 ∎

定理 2.1.2. 对于任意自然数 $n \in \mathbb{N}$， 如果 $n \neq 0$， 则存在唯一的 $m \in \mathbb{N}$，满足 $n = m^+$。

证明： 根据Peano公理中的4)，我们可以得到 m 的唯一性。下面来证明 m 的存在性。

设 $M = \{0\} \cup \{n \in \mathbb{N}: \exists k \in \mathbb{N}$，满足$n = k^+\}$。 则 $0 \in M$。 如果 $n \in M$，则 $n^+ \in M$（为什么？）。根据Peano公理中的归纳公理，我们有 $M = \mathbb{N}$。 证毕。 ∎

一种定义自然数 $\mathbb{N}$ 的方式是使用基于集合论的构造。具体的说，考虑如下一列集合

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \cdots$$

其中第一个位置的集合是空集，下一个是由空集作为元素构成的集合，再下一个是由前面这些集合作为元素构成的集合，如此下去。

我们将 $\emptyset$ 看成Peano公理中的 0， 并如此定义后继映射：对于集合 X， X^+ 定义为由 X 中所有元素和 X 本身作为一个元素构成的集合。 至此，我们验证了Peano公理的前两条。

关于Peano公理的第三条，如果 $\emptyset = X^+$，由于 $X \in X^+$， 从而 X^+ 不是空集，矛盾。

关于第四条公理，如果 $X^+ = Y^+$，则 $X \in Y^+$。

为了验证第五条公理，只需要考虑上面一列集合的构造方式：先写下 $\emptyset$， 然后是 $\emptyset^+$， 然后是 $(\emptyset^+)^+$， 等等。因此如果集合 D 是上述一列集合的子集，包含 $\emptyset$， 则QQQ

如果考虑大学以前学过的实数轴上的点列 $0, 1, \cdots$，将后继映射定义为+1映射，则容易验证它们也是满足五条Peano公理体系的。

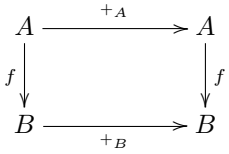
通过上面的讨论，我们知道满足Peano公理的例子不是唯一的，但是为什么我们可以用唯一的记号 $\mathbb{N}$ 来表示自然数呢？这是由于如下的定理：

定理 2.1.3. 如果集合 A 和集合 B 都满足Peano公理，其中 A 上的“起始元”和“后继映射”记为 0_A 和 $^{+_A}$，B上的“起始元”和“后继映射”记为 0_B 和 $^{+_B}$。 则存在映射 $f: A \to B$， 满足

1) $f(0_A) = 0_B$

2) f 是双射

3) $\forall a \in A$, $f(a^{+_A}) = (f(a))^{+_B}$。 换言之，我们有如下**关于映射的交换图**



注：这个定理的证明并不难。事实上， f 要满足的上述条件1) 和 3)已经完全确定了 f，确定了 f 后我们只需要验证该 f 满足 2)。该证明可以作为简单的练习。

注：一般的，数学对象就是**集合**加上**其上的结构（比如序关系，运算等等）**。例如，从Peano公理的角度来看，自然数就是一个集合（不难证明该集合是无限的）加上其上的“后继”结构（其他

结构，比如加法、乘法、带余除法、序结构等都可以由“后继”结构派生出来）。如果存在两个数学对象间的双射，并且该双射与两个数学对象上的结构是相容的（具体的，参看前面定理中关于映射的交换图），我们就可以把这两个数学对象认为是等价的，从而看作一个对象。

下面我们通过一个例子，来说明我们可以将所有的整系数多项式和 $\mathbb{R}$ 中的一个关于乘法和加法封闭的子集认为是同一个数学对象。

例 2.1.1. 令 $P(x)$ 为所有以 x 为系数的整系数多项式。我们不加证明的承认 π 是超越数这个事实。换言之，π 不是任何整系数多项式的根。令 $E \subset \mathbb{R}$ 定义为

$$E = \{f(\pi) \colon f \in P(x)\} \text{ 。}$$

我们试图说明存在从 $P(x)$ 到 E 的一一对应 ρ ， 并且 ρ 保持着加法和乘法的结构。换言之，对于任意的 $f, g \in P(x)$ ，我们有

$$\rho(f+g) = \rho(f) + \rho(g),\ \rho(f \cdot g) = \rho(f) \cdot \rho(g) \text{ 。}$$

定义 ρ 为 Ev_π ，其中 Ev_π 为在 π 处的估值(evaluation)函数，定义如下：

$$\mathrm{Ev}_\pi \colon P(x) \longrightarrow E, \quad f \mapsto \mathrm{Ev}_\pi(f) = f(\pi) \text{ 。}$$

根据 E 的定义，ρ 是满射。

由于 π 是超越数，我们可以断言 ρ 为单射。否则存在两个不同的整系数多项式 f 和 g ， 使得 $\rho(f) = \rho(g)$ 。 换言之，$f(\pi) = g(\pi)$ 。 故而我们有

$$(f-g)(\pi) = 0 \text{ 。}$$

由于 $f \neq g$ ， $f-g$ 为非零的整系数多项式。故 $(f-g)(\pi) = 0$ 与 π 为超越数矛盾。

至此，我们证明了ρ为双射。下面我们需要验证 ρ 保持乘法和加法结构。也即是

$$(f+g)(\pi) = f(\pi) + g(\pi) \text{ 和 } (f \cdot g)(\pi) = f(\pi) \cdot g(\pi) \text{ 。}$$

这个验证比较简单，这里留作练习。

习题：

习题 2.1.1. 本题是关于运用数学归纳法的一个常见错误。

我们这里不加证明的引用下面事实：若 A 和 B 都是有限集，则 $A \cup B$ 也是有限集。

下面的论述错在哪里？

“首先，空集是有限集。如果所有包含 n 个元素的集合是有限集，则包含 $n+1$ 个元素的集合可以写为一个包含 n 个元素的集合 和另一个只包含一个元素的集合之并。根据不加证明引用的事实，我们知道任意 $n+1$个元素的集合是有限集。从而根据数学归纳法（换言之，根据Peano公理中的归纳公理），自然数集 $\mathbb{N}$ 是有限集。”

习题 2.1.2. 证明**定理2.1.3**。

习题 2.1.3. 完成**例2.1.1**中最后关于 ρ 保持乘法和加法结构之验证。

2.2 自然数中的的加法和序关系

定义 2.2.1 (自然数上加法). 定义：定义自然数的加法为一个 $\mathbb{N}\times\mathbb{N}$ 到 $\mathbb{N}$ 的映射 f ， 满足 $f(m,0)=m$ 且 $f(m,n^+)=f(m,n)^+$ 。 对于 $f(m,n)$ ， 一般记为 $m+n$ 。

我们需要说明上述定义是良性的（well-defined）。换言之，我们需要说明 $f(m,0)=m$ 和 $f(m,n^+)=f(m,n)^+$这两条性质完全决定了映射 $f\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ 。

给定$m\in\mathbb{N}$ ，考虑集合

$$D=\{n\in\mathbb{N}\colon f(m,n)\text{按照上面定义可以给出}\}$$

由于 $f(m,0)$ 定义为 m ， 我们有 $0\in D$ 。 假设 $n\in D$ ， 也就是 $f(m,n)$ 是有定义的，则按照定义 $f(m,n^+)=f(m,n)^+$ ， 从而也是有定义的。根据归纳公理，我们有 $D=\mathbb{N}$ 。 从而上面的定义 $f\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ 是良性定义的（well-defined）。

我们先来证明自然数上加法的结合律。

定理 2.2.1 (加法结合律). 对于任意自然数 m 、n 和 k ， 我们有

$$(m+n)+k=m+(n+k)\,。$$

证明： 我们对 k 做归纳。令

$$D=\{k\in\mathbb{N}\colon (m+n)+k=m+(n+k)\,，\ \forall m,n\in\mathbb{N}\}\,。$$

注意到

$$\begin{aligned}(m+n)+0&=m+n && [x+0=x\,，\ \forall x\in\mathbb{N}]\\ &=m+(n+0) && [x+0=x\,，\ \forall x\in\mathbb{N}]\end{aligned}$$

我们有 $0\in D$ 。

假定 $k \in D$ 。换言之，$(m+n)+k = m+(n+k)$， $\forall m,n \in \mathbb{N}$ 。 则

$$\begin{aligned}(m+n)+k^+ &= ((m+n)+k)^+ && \text{[加法之定义]}\\ &= (m+(n+k))^+ && \text{[归纳假设 } k \in D\text{]}\\ &= m+(n+k)^+ && \text{[加法之定义]}\\ &= m+(n+k^+) && \text{[加法之定义]}\end{aligned}$$

从而 $k^+ \in D$ 。故$D = \mathbb{N}$ ，加法结合律证毕。 ∎

为了证明加法的交换律，我们证明如下两个引理。

引理 2.2.1. 对于任意自然数 m 和 n ， 我们有 $m^+ + n = m + n^+$ 。

证明： 我们对 n 做归纳。

$n = 0$ 时，对于任意 $m \in \mathbb{N}$ ， $m^+ + 0 = m^+$ ，而$m + 0^+ = (m+0)^+ = m^+$ ，故$n = 0$时，引理中等式对任意 $m \in \mathbb{N}$ 都成立。

假定 $m^+ + k = m + k^+$ $\forall m \in \mathbb{N}$ ， 则

$$\begin{aligned}m^+ + k^+ &= (m^+ + k)^+ && \text{[加法之定义]}\\ &= (m + k^+)^+ && \text{[归纳假设]}\\ &= m + (k^+)^+ && \text{[加法之定义]}\end{aligned}$$

因此对于任意 $m,n \in \mathbb{N}$ ，我们都有 $m^+ + n = m + n^+$ ， 证毕。 ∎

注：如果我们用 1 来表示 0^+ ， 用 2 来表示 $(0^+)^+$ ， 则根据加法的定义和上面的引理，我们可以证明 $1+1=2$ 。 具体证明细节如下：

$$\begin{aligned}1+1 &= 0^+ + 0^+ && \text{[1 代表 } 0^+\text{]}\\ &= (0^+)^+ + 0 && \text{[}m^+ + n = m + n^+,\ \forall m,n \in \mathbb{N}\text{]}\\ &= 2+0 && \text{[2 代表 } (0^+)^+\text{]}\\ &= 2 && \text{[加法之定义]}\end{aligned}$$

注： 为了证明 $1+1=2$ ， 也可以不依赖上面的引理。细节如下：

$$\begin{aligned}1+1 &= 0^+ + 0^+ && \text{[1 代表 } 0^+\text{]}\\ &= (0^+ + 0)^+ && \text{[加法之定义]}\\ &= (0^+)^+ && \text{[加法之定义]}\\ &= 2 && \text{[2 代表 } (0^+)^+\text{]}\end{aligned}$$

下面的引理，这是我们证明加法交换律时归纳的起点。

引理 2.2.2. 对于任意自然数 n ，我们有 $0+n=n+0=n$ 。

证明： 根据加法的定义，我们始终有 $n+0=n$ ， $\forall n\in\mathbb{N}$ 。因此只需要证明 $0+n=n+0$ 即可。

我们对 n 做归纳。令

$$D=\{n\colon 0+n=n+0\}$$

由于 $0+0=0+0$ ，$0\in D$ 。

假定 $k\in D$ ，换言之， $0+k=k+0$ ，则

$$\begin{aligned} 0+k^+ &= (0+k)^+ && [\text{加法之定义}]\\ &= (k+0)^+ && [k\in D]\\ &= k^+ && [n+0=n,\ \forall n\in\mathbb{N}]\\ &= k^+ + 0 && [n+0=n,\ \forall n\in\mathbb{N}] \end{aligned}$$

从而若 $k\in D$ ， 则 $k^+\in D$ 。 因此 $D=\mathbb{N}$ ， 证毕。 ∎

下面我们来证明加法之交换律。

定理 2.2.2 (自然数上加法交换律). 对于任意自然数 m 和 n ， 我们有 $m+n=n+m$ 。

证明： 令

$$D=\{m\in\mathbb{N}\colon m+n=n+m,\ \forall n\in\mathbb{N}\}$$

根据上面的引理，$0\in D$ 。

假定$k\in D$ 。也就是$k+n=n+k$ ， $\forall n\in\mathbb{N}$ 。则 $\forall n\in\mathbb{N}$ ， 我们有

$$\begin{aligned} k^+ + n &= k+n^+ && [m^+ + n = m + n^+,\ \forall m,n\in\mathbb{N}]\\ &= (k+n)^+ && [\text{加法之定义}]\\ &= (n+k)^+ && [\text{归纳假设 } k\in D]\\ &= n+k^+ && [\text{加法之定义}] \end{aligned}$$

从而得到$k^+\in D$ 。故而$D=\mathbb{N}$ ，从而加法交换律成立。证毕。 ∎

自然数上的加法是满足消去律（the law of cancellation）的。

定理 2.2.3 (自然数上加法消去率). 对于自然数 m 、 n 和 k ，如果 $m+k=n+k$ ， 则 $m=n$ 。

注：该定理证明也是通过归纳。比如我们对 k 进行归纳。当 $k=0$ 时先证明消去律成立。然后假定 $k=p$ 时消去律成立。注意到

$$m+p^+=(m+p)^+ \quad 且 \quad n+p^+=(n+p)^+ 。$$

利用$^+$是单射和归纳假设（$k=p$ 时消去律成立），我们不难完成本证明。具体细节留作练习。

注：上面的自然数加法之消去律，实际上是“右消去律”。根据自然数加法的交换律，我们可以立即从“右消去律”得到“左消去律”。

根据自然数的加法，我们可以定义自然数上的序关系。

定义 2.2.2 (小于等于关系). 给定两个自然数 m 和 n， 我们说 $m \leq n$（或者等价的，$n \geq m$），如果存在 $k \in \mathbb{N}$，使得 $n = m + k$。

对于任意的自然数 n， 由于 $n = 0 + n$， 因此 $n \geq 0$。 换言之，0 是最小的自然数。

定义 2.2.3 (小于关系). 给定两个自然数 m 和 n， 我们说 $m < n$（或者等价的，$n > m$），如果 $m \leq n$ 且 $m \neq n$。

上面定义的自然数的序关系，一个重要的性质是：自然数上的序关系是良序，从而是全序集合。

为了证明自然数在如上定义的序关系下是良序集，我们证明如下性质：自然数的任何非空子集中有最小元素。

定理 2.2.4 (自然数的良序性). 对于任意自然数集 $\mathbb{N}$ 的子集 D， 一定存在 D 中的唯一元素 m， 使得对于任意 $n \in D$， 我们有 $m \leq n$。

证明：

考虑集合

$$E = \{k \in \mathbb{N} \colon k \leq n，\ \forall n \in D\}.$$

由于 $n = 0 + n \quad \forall n \in D$， 故 $0 \leq n$。 从而 $0 \in E$。

断言： $E \cap D \neq \emptyset$.

断言之证明：如若不然，则 $E \cap D = \emptyset$。 换言之，对于 E 中任何元素 k， 均有 $k < n$，$\forall n \in D$。 基于此，我们来证明 $E = \mathbb{N}$， 从而得到矛盾。

我们已经知道 $0 \in E$。 假定 $k \in E$， 我们来证明 $k^+ \in E$。 事实上，对于任意的$n \in D$，由于 k 在 E 中且 $E \cap D = \emptyset$， 我们有 $k < n$。 换言之，$k \leq n$ 且 $k \neq n$。 等价的，我们有 $n = k + s$ 且 $s \neq 0$。 由于 $s \neq 0$，存在 $j \in \mathbb{N}$， 使得 $s = j^+$。 故

$$n = k + s = k + j^+ = k^+ + j.$$

从而 $k^+ \leq n$。 由于 n 的任意性，我们有 $k^+ \in E$。 根据归纳公理，我们得到 $E = \mathbb{N}$。

由于$D \neq \emptyset$，我们可以取 D 中元素 n。 注意到 $E = \mathbb{N}$， 我们有 $k \leq n,\ \forall k \in \mathbb{N}$。 故而 $n^+ \leq n$。 换言之，

$$n = n^+ + k = n + k^+.$$

根据加法之消去律，我们得到 $0 = k^+$ ， 这与Peano公理中的“0不是任何元素的后继”矛盾。从而断言得证。

根据断言，我们知道存在 m ， 使得 $m \in D$ 并且 $m \leq n,\ \forall n \in D$ 。 下面我们来证明这样的 m 的唯一性。

假定存在 $m_1, m_2 \in D$ ， 使得 $m_i \leq n,\ \forall n \in D$ ， $i = 1, 2$ 。 则

$$m_1 \leq m_2 \quad 且 \quad m_2 \leq m_1 \ 。$$

下面我们来证明 $m_1 = m_2$ 。

由于$m_1 \leq m_2$ ，故$m_2 = m_1 + s_1$ 。 同理，$m_1 = m_2 + s_2$ 。 两边相加，得到

$$m_2 + m_1 = m_1 + s_1 + m_2 + s_2 \ 。$$

根据加法的交换律和消去律，有

$$0 = s_1 + s_2 \ 。$$

由此我们可以断言 $s_1 = s_2 = 0$ 。 不然，不妨假定 $s_1 \neq 0$ ， 则存在 $p \in \mathbb{N}$ ， 使得 $s_1 = p^+$ ， 故

$$0 = s_1 + s_2 = p^+ + s_2 = p + s_2^+ = (p + s_2)^+ \ ，$$

和Peano公理中的“0不是任何元素的后继”矛盾。

由于 $s_1 = s_2 = 0$ ， 我们有 $m_1 = m_2$ 。

至此，证毕。 ∎

习题：

习题 2.2.1. 证明：若自然数 m 、 n 和 k 满足 $m \leq n$ 且 $n < k$ ，则 $m < k$ 。

习题 2.2.2. 自然数序关系的三歧性：对于任何两个自然数 m 和 n ， 证明以下三种情况必有一种成立，且仅有一种成立

a) $m < n$

b) $m = n$

c) $m > n$ （或等价的， $n < m$ ）

注：该三歧性也可以确保自然数上的关系 $\leq$ 是个全序关系。

2.3 自然数中的乘法

本节中我们给出自然数上乘法的定义，并证明了乘法的一些基本性质。基于自然数上的乘法，我们给出了整除、因子和素数等定义，并且证明了自然数的素分解定理。

定义 2.3.1 (自然数 $\mathbb{N}$ 上的乘法). 定义自然数的乘法为一个 $\mathbb{N}\times\mathbb{N}$ 到 $\mathbb{N}$ 的映射 g ， 满足 $g(m,0)=0$ 且 $g(m,n^+)=g(m,n)+m$ ， $\forall m,n\in\mathbb{N}$ 。 对于 $g(m,n)$ ， 一般记为 $m\cdot n$ 。

类似于加法的情况，我们需要检查这个乘法的定义（一个从 $\mathbb{N}\times\mathbb{N}$ 到 $\mathbb{N}$的映射）是良性定义的（well-defined）。这个过程和加法的比较类似，在此作为练习。

我们先来证明乘法和加法之间的分配律。

定理 2.3.1 (分配律). 对于任意自然数 m 、n 和 k ， 我们有

$$m\cdot(n+k)=m\cdot n+m\cdot k。$$

证明： 令

$$D=\{k\colon m\cdot(n+k)=m\cdot n+m\cdot k\quad\forall m,n\in\mathbb{N}\}。$$

注意到

$$\begin{aligned} m\cdot(n+0)&=m\cdot n && \text{[加法之定义]}\\ &=m\cdot n+0 && \text{[加法之定义]}\\ &=m\cdot n+m\cdot 0 && \text{[加法之定义]} \end{aligned}$$

我们有 $0\in D$ 。

假定 $p\in D$ ， 注意到

$$\begin{aligned} m\cdot(n+p^+)&=m\cdot(n+p)^+ && \text{[加法之定义]}\\ &=m\cdot(n+p)+m && \text{[乘法之定义]}\\ &=(m\cdot n+m\cdot p)+m && \text{[归纳假设 } p\in D\text{]}\\ &=m\cdot n+(m\cdot p+m) && \text{[加法结合律]}\\ &=m\cdot n+m\cdot p^+ && \text{[乘法之定义]} \end{aligned}$$

我们有 $p^+\in D$ 。 根据归纳公理， $D=\mathbb{N}$ ，从而分配律证毕。 □

下面我们来证明自然数乘法本身的交换律。为了使得证明连贯，我们使用了另外一种风格。具体的说，我们没有专门把其中用到的重要中间结论作为引理给出，而是作为证明中的断言给出。

定理 2.3.2 (乘法交换律). 对于任意自然数 m 和 n ， 我们有 $m\cdot n=n\cdot m$ 。

证明： 令

$$D = \{n \in \mathbb{N}: mn = nm \forall m \in \mathbb{N}\} \text{ 。}$$

断言1：$0 \in D$ 。

断言1之证明：令

$$E = \{m \in \mathbb{N}: m \cdot 0 = 0 \cdot m\} \text{ 。}$$

则 $0 \in E$ （因为 $0 \cdot 0 = 0 \cdot 0 = 0$）。

假定 $m \in E$ 。 换言之，$m \cdot 0 = 0 \cdot m$ 。 我们需要证明 $m^+ \cdot 0 = 0 \cdot m^+$ 。

事实上，根据乘法之定义，有 $m^+ \cdot 0 = 0$ 。 注意到

$$\begin{aligned} 0 \cdot m^+ &= 0 \cdot m + 0 && \text{[乘法之定义]} \\ &= m \cdot 0 + 0 && \text{[归纳假设}m \in E\text{]} \\ &= 0 + 0 && \text{[乘法之定义]} \\ &= 0 && \text{[加法之定义]} \end{aligned}$$

我们得到“如果 $m \in E$ ， 则 $m^+ \in E$ ”。根据归纳原理，$E = \mathbb{N}$ 。 从而断言1得证。

基于断言1，我们知道 $0 \in D$ 。 下面我们来证明

“ 如果 $n \in D$ ， 则 $n^+ \in D$ 。 ”

换言之，如果 $mn = nm \quad \forall m \in \mathbb{N}$ ，则

$$mn^+ = n^+ m \ \forall m \in \mathbb{N}。$$

断言2：$\forall m, n \in \mathbb{N}$ ， $n^+ m = nm + m$ 。

断言2之证明：我们对 m 使用归纳。

当 $m = 0$ 的时候，根据乘法的定义，有$n^+ \cdot 0 = 0$ 。 同时注意到

$$\begin{aligned} n \cdot 0 + 0 &= 0 + 0 && \text{[乘法之定义]} \\ &= 0 && \text{[加法之定义]} \end{aligned}$$

故 $n^+ \cdot 0 = n \cdot 0 + 0 \quad \forall n \in \mathbb{N}$ 。

假定存在固定的 $m \in \mathbb{N}$ ， 使得

$$n^+ m = nm + m \ \forall m \in \mathbb{N} \text{ 。}$$

我们来证明

$$n^+ m^+ = nm^+ + m^+ \ \forall m \in \mathbb{N} \text{ 。}$$

事实上，我们有

$$\begin{aligned} n^+m^+ &= n^+m + n^+ && [\text{乘法之定义}] \\ &= (nm+m)+n^+ && [\text{归纳假设}] \\ &= nm + (m+n^+) && [\text{加法结合律}] \end{aligned}$$

注意到

$$\begin{aligned} nm^+ + m^+ &= (nm+n)+m^+ && [\text{乘法之定义}] \\ &= nm + (n+m^+) && [\text{加法结合律}] \\ &= nm + (m^+ + n) && [\text{加法交换律}] \\ &= nm + (m+n^+) && [m^+ + n = m + n^+] \end{aligned}$$

我们有

$$n^+m^+ = nm^+ + m^+ \ \forall m \in \mathbb{N} \ 。$$

从而断言2得证。

基于上述断言，我们来完成自然数乘法交换律的证明。

前面已经有 $0 \in D$ 。 只需要证明

“ 如果 $n \in D$ ， 则 $n^+ \in D$ 。 ”

换言之，如果 $mn = nm \quad \forall m \in \mathbb{N}$ ，则需证明

$$mn^+ = n^+m \ \forall m \in \mathbb{N}。$$

事实上，

$$\begin{aligned} n^+m &= nm + m && [\text{断言2}] \\ &= mn + m && [\text{归纳假设}] \\ &= mn^+ && [\text{乘法之定义}] \end{aligned}$$

故自然数乘法之交换律得证。 ∎

定理 2.3.3 (自然数乘法结合律). 对于任意自然数 m 、 n 和 k ， 我们有 $(m\cdot n)\cdot k = m\cdot(n\cdot k)$。

这里的证明也是采用归纳的办法。证明比较简单，留作练习。

另外一个关于自然数乘法的基本性质是自然数乘法的消去律。

定理 2.3.4 (自然数乘法消去律). 对于任意自然数 m 、 n 和 k ， 如果 $m \cdot k = n \cdot k$ 且 $k \neq 0$ ， 则 $m = n$ 。

该定理证明比较简单，这里留作练习。

基于自然数的乘法，我们可以定义整除和因子。

定义 2.3.2. 对于两个自然数 m 和 n ， 如果存在 $k \in \mathbb{N}$ ， 使得 $m = n \cdot k$ ，则称 n 整除 m （或者等价的， m 被 n 整除），记为 $n|m$ 。 这里 n 和 k 被称为是 m 的因子（factor）。

根据乘法中定义，对于任何 $n \in \mathbb{N}$ ， 我们有

$$n \cdot 0^+ = n \cdot 0 + n = 0 + n = n + 0 = n。$$

从而 0^+ 是任何自然数的因子。

一个重要的事实是：自然数没有零因子。换言之，如果 $mn = 0$ ， 则 m 和 n 中至少一个为零。

定理 2.3.5 (自然数没有零因子). 若自然数 m 和 n 满足 $mn = 0$ ， 则 $m = 0$ 或 $n = 0$ 。

证明： 若自然数 m 和 n 满足 $mn = 0$ ，且 m 和 n 均不为零，我们来找到矛盾。

由于 $n \neq 0$ ，根据定理**2.1.2**，存在 $k \in \mathbb{N}$ ， 使得 $n = k^+$ 。 同理，由于 $m \neq 0$ ， $\exists\ p \in \mathbb{N}$ ， 使得 $m = p^+$ 。

故

$$0 = mn = mk^+ = mk + m = mk + p^+ = (mk + p)^+ \ ，$$

而这与Peano公理中的“ 0 不是任何元素的后继”矛盾。 ∎

基于因子的概念，我们来定义素数（prime number）。为了简单起见，我们用 1 来代表 0^+ 。

定义 2.3.3 (素数和合数). 我们说自然数 n 是素数（prime number），如果 $n > 1$ 且 n 的所有因子只能是 n 和 1 。 否则，我们说 n 是合数（composite number）。

关于自然数的因子分解，很重要的一个性质就是任意自然数存在素因子分解。

定理 2.3.6 (自然数的素因子分解定理). 对于任意

基于上述的素因子分解定理，我们可以证明素数的数目是无限的。

定理 2.3.7 (素数数目无限). 全体素数构成的集合是个无限集。

证明：[欧几里得之证法] 这里的证明方法是欧几里得给出的。证明的后面部分我们基于Peano公理给出了相关基本事实的严格论证。

用 P 代表全体素数构成的集合。假定 P 是个有限集，则不妨设存在 $N \in \mathbb{N}$ ， 使得

$$P = \{p_1, \cdots, p_N\}。$$

令 $q = p_1 p_2 \cdots p_n + 1$ 。 由于 P 是全体素数构成的集合，根据定理 2.3.6，存在 $p \in \{p_1, p_2, \cdots, p_N\}$ ， 使得 $p|q$ 。 根据整除之定义，$p|p_1 p_2 \cdots p_N$ 。 故存在 $k, s \in \mathbb{N}$ ， 使得

$$q = kp \text{ 且 } p_1 p_2 \cdots p_N = sp 。$$

由于 $q > p_1 p_2 \cdots p_N$ ， 故 $k > s$ （为什么？）。故存在 $h \in \mathbb{N} - \{0\}$ ， 使得 $k = s + h$ ， 从而

$$kp = (s + h)p = sp + hp 。$$

换言之

$$q = p_1 p_2 \cdots p_N + hp 。$$

将 $q = p_1 p_2 \cdots p_n + 1$ 带入上式左边，有

$$p_1 p_2 \cdots p_n + 1 = p_1 p_2 \cdots p_n + hp 。$$

由加法消去律

$$hp = 1 。$$

由于 $h \in \mathbb{N} - \{0\}$ ， 根据定理 2.1.2，存在 $l \in \mathbb{N}$ ， 使得 $h = l^+$ 。 因此

$$hp = ph = p \cdot l^+ = pl + p \geq p > 1 ，$$

这与 $hp = 1$ 矛盾。证毕。 ∎

习题：

习题 2.3.1. 证明定理**2.3.4** （乘法之消去律）。（提示：可以使用反证法。假定 $m \neq n$ ，根据**习题 2.2.2**中的结论，有 $m < n$ 或者 $m > n$ ，根据小于或者大于的定义，$\cdots$ 。 或者不用反证法，直接利用自然数没有零因子这个事实，也就是**定理 2.3.5**）。

2.4 自然数中的Euclidean性、带余除法

自然数上的另外一个重要结构就是带余除法。高中学到的，有理数的小数表示方法，就是通过带余除法（可能要做无穷多次）来实现的。同时，通过带余除法，我们可以定义整除和因子分解，进而可以进一步定义素数（或者称为质数）。

具体的说，基于自然数的序结构和乘法结构，我们可以定义自然数上的带余除法。我们先得到自然数的阿基米德性，然后由此得到自然数的欧几里得性，从而可以给出自然数带余除法之定义。

定理 2.4.1 (自然数的阿基米德性). 对于任意 $m \in \mathbb{N}$ 和 $n \in \mathbb{N} - \{0\}$ ，一定存在 $k \in \mathbb{N}$ ，使得 $m \leq n \cdot k$ 。

证明： 由于$n \in \mathbb{N} - \{0\}$ ，存在 $p \in \mathbb{N}$ ，使得 $n = p^+$ 。 对于任意的 $m \in \mathbb{N}$ ， 取 $k = m$ ，则

$$\begin{aligned} n \cdot k &= n \cdot m \\ &= m \cdot n \\ &= m \cdot p^+ \\ &= m \cdot p + m \end{aligned}$$

根据 $\leq$ 之定义，我们有 $m \leq n \cdot k$ 。 ∎

基于上述的定理，我们有如下定理（自然数的欧几里得性）。

定理 2.4.2 (自然数的欧几里得性). 对于任意 $m \in \mathbb{N}$ 和 $n \in \mathbb{N} - \{0\}$ ，存在唯一的 $k \in \mathbb{N}$ ，使得

$$n \cdot k \leq m < n \cdot (k+1) \text{ ，其中1定义为} 0^+ \text{。}$$

证明： 我们先证 k 的唯一性，然后证 k 的存在性。

“唯一性”

假定我们有

$$n \cdot k_i \leq m < n \cdot (k_i + 1) \ , \ i = 1, 2$$

并且 $k_1 \neq k_2$ 。 我们来推出矛盾。

由于 $k_1 \neq k_2$ ， 根据自然数上序关系的三歧律（trichotomy），必有 $k_1 < k_2$ 或者 $k_1 > k_2$ 。

我们不妨设 $k_1 < k_2$ （为什么可以不妨这样假设？）。则 $k_1^+ \leq k_2$ （QQQ. Detailed needed）。注意到 $k_1^+ = k_1 + 1$ （为什么？），我们有 $k_1 + 1 \leq k_2$ 。

断言1：如果自然数 m 和 n 满足 $m \leq n$ ，则对于任意自然数 p ， 有 $m \cdot p \leq m \cdot n$ 。

断言1之证明：根据定义，不难证明。这里留作练习。

根据上面的断言，注意到 $k_1 + 1 \leq k_2$ ， 我们有 $n \cdot (k_1 + 1) \leq n \cdot k_2$ 。 由于 $m < n \cdot (k_1 + 1)$ ，我们有

$$m < n \cdot (k_1 + 1) \leq n \cdot k_2 \text{。}$$

断言2：对于自然数 m 、n 和 p ， 如果 $m<n$ 且 $n\leq p$ ，则 $m<p$ 。

断言2之证明： 练习。

根据断言2，注意到 $m<n\cdot(k_1+1)\leq n\cdot k_2$ ， 我们有

$$m<n\cdot k_2 \text{ 。}$$

根据题设，我们有

$$m\geq n\cdot k_2 \text{ 。}$$

$m<n\cdot k_2$ 和 $m\geq n\cdot k_2$ 同时成立是违背了自然数序关系的三岐律的，矛盾。

至此，我们证明了定理中 k 的唯一性。

“存在性”

对于题设中 m ， 根据 定理［自然数阿基米德性］，

存在 $p\in\mathbb{N}$ ，使得

$$m+1\leq n\cdot p \text{ 。}$$

令

$$D=\{p\in\mathbb{N}\colon m+1\leq n\cdot p\} \text{ 。}$$

则 $D\neq\emptyset$ 。 根据自然数的良序性，存在 D 中的最小元素。换言之，存在 $q\in D$ ，满足 $q\leq p$ ，$\forall p\in D$ 。

我们可以断言上述的 q 不为零。否则有 $m+1\leq 0$ 。 注意到 $0\leq m+1$ ，我们有 $m+1=0$ 。换言之，$m^+=0$ 。 这与Peano公理矛盾。

由于 $q\neq 0$ ，存在 $k\in\mathbb{N}$ ， 使得 $q=k^+=k+1$ 。

故而我们有

$$m+1\leq n\cdot(k+1) \text{ 。}$$

注意到 $m<m+1\leq n\cdot(k+1)$ ， 根据断言2，我们有

$$m<n\cdot(k+1) \text{ 。}$$

下面我们来证明 $n\cdot k\leq m$ 。 该证明需要用到 q 是 D 中最小元素这个事实。

我们先证明 $n\cdot k<m+1$ 。 如这个不成立，根据自然数序关系的三岐律，必然有

$$m+1\leq n\cdot k \text{ 。}$$

考虑 D 的定义，我们有 $k\in D$ 。 由于 q 是 D 中最小元素，故而 $q\leq k$ 。 注意到 $q=k^+$ ， 我们有 $k^+\leq k$ 。 根据定义，$k^+=(k+0)^+=k+0^+$ ，故而 $k\leq k^+$ 。 又由于 $0^+\neq 0$ ，我们有 $k\neq k^+$ 。 故而得到 $k<k^+$ 。

现在我们同时有 $k^+\leq k$ 和 $k<k^+$ ，和自然数序关系之三岐律矛盾。故而 $n\cdot k<m+1$ 。

现在我们有 $n\cdot k<m+1$ ，我们来证明 $n\cdot k\leq m$ 。 事实上，由于 $n\cdot k<m+1$ ，有 $n\cdot k\leq m+1$ 且 $n\cdot k\neq m+1$ 。 QQQ (detailed needed)，我们有 $n\cdot k+1\leq m+1$ 。 换言之，存在 $s\in\mathbb{N}$ ，使得

$$m+1=n\cdot k+1+s \text{ 。}$$

根据加法之交换律和消去律，可得 $m=n\cdot k+s$ ， 故而

$$m\geq n\cdot k \text{ 。}$$

至此，我们证明了 $n\cdot k\leq m$ 且 $m<n\cdot(k+1)$ ，故

$$n\cdot k\leq m<n\cdot(k+1) \text{ 。}$$

证毕。 ∎

基于上述自然数的欧几里得性，我们可以定义 $\mathbb{N}$ 上的带余除法如下：

定义 2.4.1 (自然数上带余除法). 对于任意自然数 $m\in\mathbb{N}$ 和 $n\in\mathbb{N}-\{0\}$ ， 一定存在唯一的自然数对 (q,r) ， 使得 $m=n\cdot q+r$ ， 其中 $0\leq r<n$ 。 这里的 q 称为 m 除以（带余除法） n 的商（quotient），r 称为 m 除以（带余除法） n 的余数（remainder）。

注 2.4.1. 上面的定理“自然数的欧几里得性” 确保了上述带余除法的定义是 well-defined 。换言之，对于任意自然数 $m\in\mathbb{N}$ 和 $n\in\mathbb{N}-\{0\}$ ，上述 q 和 r 是存在并且唯一的。

习题：

习题 2.4.1. 证明定理2.4.2中的断言1：如果自然数 m 和 n 满足 $m\leq n$ ， 则对于任意自然数 p ， 有 $mp\leq mn$ 。

习题 2.4.2. 证明定理2.4.2中的断言2：对于自然数 m 、n 和 p ， 如果 $m<n$ 且 $n\leq p$ ，则 $m<p$ 。

2.5 基于自然数的有限集、无限集之定义

我们以前定义 X 为无限集，如果存在 X 到 X 之真子集的一一对应。定义 X 为有限集，如果 X 不是无限集。

现在我们有了自然数的概念，可以借助自然数的概念定义有限、无限集如下：

定义 2.5.1. 我们说集合 X 是有限集，如果 X 为空集或者 X 与 $\{1,\cdots,n\}$ 有一一对应。我们称集合 X 为无限集，如果 X 不是有限集。

下面我们来说明这样定义的有限集、无限集和以前定义的有限集、无限集是完全一样的。事实上，我们只需证明如下定理即可。

定理 2.5.1. 集合 X 可以一一对应到自身的某个真子集，当且仅当 X 不是空集并且对于任意 $n\in\mathbb{N}_{\geq 0}$ ， X 不能一一对应到 $\{1,\cdots,n\}$

2.6 整数：$(\mathbb{N},+)$之Grothendieck化

在 $\mathbb{N}$ 中，我们已经定义了加法，一个自然的问题就是如何定义减法。关于减法，一种看法是将 $m-n$ 定义为 $m+(-n)$ 。 当然这样就必须首先定义 $-n$ 。 一种关于 $-n$ 的定义是将其定义为 $x+n=0$ 的解。但是，限定在自然数上，如果 $n\in\mathbb{N}-\{0\}$ ， 可以验证 $x+n=0$ 是没有解的（具体验证留作练习）。

另外一种定义减法的方式是：如果自然数 m 、 n 和 k 满足 $n+k=m$ ， 则定义 $m-n$ 为 k 。 但是这样的定义本身就假定了 $n\leq m$ 。

简单的说，限定在 $\mathbb{N}$ 上，是无法完整的定义减法的。为了定义减法，必须在更大的范围类考虑。这就是如何将自然数扩展到整数的问题。这里用到了半群Grothendieck化的思想。稍微具体的说，就是在更广的，更抽象的范畴下定义所谓的“减法”。并且最终所定义的减法和 $a\geq b$ 时可以基于 $\mathbb{N}$ 直接定义的 $a-b$ 是相容的。

为了得到整数，我们考虑如下的自然数对 $[m,n]$ 。 这里记为 $[m,n]$ ， 而不是 (m,n) ， 因为 (m,n) 代表 $\mathbb{N}\times\mathbb{N}$ 中的元素，而我们这里的 $[m,n]$ 并不是在 $\mathbb{N}\times\mathbb{N}$ 中的。事实上，这里的 $[m,n]$ 代表一个等价类。具体的说，我们有

$$[m,n]=[m',n'] \text{ 当且仅当 } m+n'=m'+n \text{ 。}$$

注意，定义上面的等价，我们用到是自然数 $\mathbb{N}$ 上的加法。

可以直接验证，上述的“等价”关系满足自反性和传递性。换言之，

$$[m,n]=[m,n]$$

并且若 $[m_1,n_1]=[m_2,n_2]$ 且 $[m_2,n_2]=[m_3,n_3]$ ， 则

$$[m_1,n_1]=[m_3,n_3] \qquad \text{（具体验证留作练习）}$$

我们将上面的等价类定义为整数 $\mathbb{Z}$ 。

定义 2.6.1 (整数之定义). 上述定义的 $[m,n]$ 全体，记为整数集合 $\mathbb{Z}$ 。 换言之，

$$\mathbb{Z}=\{[m,n]\colon m,n\in\mathbb{N}\} \text{ 。}$$

当然，这里的整数 $\mathbb{Z}$ 只是在集合意义下给出的定义。在我们进一步定义其上的结构（加法、乘法、序关系等）之前，这里的 $\mathbb{Z}$ 给出的信息仅仅是一个可数集（$\mathbb{Z}$ 是可数集这个事实，留作练习）。

定义 2.6.2 (整数上的加法). 上述定义的 $\mathbb{Z}$ 中，定义其上加法为

$$[m,n]+[m',n']=[m+m',n+n'] \text{ 。}$$

注 2.6.1. 由于 $\mathbb{Z}$ 是通过等价类定义的，因此 $[m,n]$ 这个等价类的表示方法是不唯一的。换言之，对于任意的 $k\in\mathbb{N}$ ， 我们都有 $[m,n]=[m+k,n+k]$ 。 对于这样的等价类做定义的时候，一定要注意定义是well-defined。也就是要确保定义本身和等价类的具体表示方法（比如究竟用 $[m,n]$ 还是 $[m+k,n+k]$ ）是无关的。关于 $\mathbb{Z}$ 上加法定义是well-defined，留作练习。

自然数上加法的一些性质，比如交换律和结合律，在整数的加法中也得到了保持。

定理 2.6.1 (整数加法的交换律和结合律). 整数的加法满足交换律和结合律。

证明： 证明不难。主要是基于定义和自然数上加法的交换律以及结合律。具体证明留作练习。 ∎

我们也可以定义 $\mathbb{Z}$ 上序关系。

定义 2.6.3 (整数上的序关系). 上述定义的 $\mathbb{Z}$ 中，定义其上序关系 $\leq$ 为

$$[m,n]\leq[m',n'] \text{ 当且仅当 } m+n'\leq m'+n \text{ 。}$$

注 2.6.2. 由于$[m,n]$代表的是一个等价类，我们需要验证该定义是 well-defined 。换言之，我们需要验证

“若 $[m,n]=[m',n']$ ， $[p,q]=[p',q']$ 且 $[m,n]\leq[p,q]$ ， 则 $[m',n']\leq[p',q']$ 。 ”

同时，为了验证该关系确实是序关系，我们需要验证该关系满足自反性和传递性。

至此，我们定义了 $\mathbb{Z}$ 和其上的加法结构和序结构。

注 2.6.3. 下面我们来说明这样定义的 $\mathbb{Z}$ 中是“包含”了自然数 $\mathbb{N}$，并且 $\mathbb{Z}$ 上的结构（加法、序结构等）和 $\mathbb{N}$ 上的结构是“相容”的。

考虑如下映射

$$\rho\colon \mathbb{N} \longrightarrow \mathbb{Z},\ n \mapsto [n,0]$$

则 ρ 是单射，但不是满射（为什么？）。ρ 不仅仅在集合意义下将 $\mathbb{N}$ “嵌入” 了 $\mathbb{Z}$，ρ 还保持了相关的结构（加法、序关系等）。下面我们来分别说明这些性质。

命题 2.6.1. 上述定义的 ρ 保持加法结构和序结构。换言之，对于任意的 $m,n \in \mathbb{N}$，$\rho(m+n)=\rho(m)+\rho(n)$。对于 $m,n\in\mathbb{N}$ 且 $m\le n$，我们有 $\rho(m)\le\rho(n)$。

证明： 练习。 ∎

注 2.6.4. 至此，我们已经完整的演示了Grothendieck化的核心思想：在更抽象的范畴里面定义半群的Grothendieck化，并且Grothendieck化后得到的结构与之前的结构“相容”。更具体的说，对我们的情况，为了定义类似减法，先抽象出减法的“基本性质”，然后在抽象的对象$\{[m,n]\colon m,n\in\mathbb{N}\}$ 中试图保持这种“基本性质”。

我们已经通过得到了 $\mathbb{Z}$ 上的加法结构，下面我们用类似的办法来得到 $\mathbb{Z}$ 上的乘法结构。

定义 2.6.4 (整数上的乘法). 对于任意的 $\mathbb{Z}$ 中元素 $[m,n]$ 和 $[p,q]$，定义其乘法为

$$[m,n]\cdot[p,q]=[mp+nq,mq+np]\ 。$$

一个自然的问题是，为什么整数乘法按照上面的方法定义，而不是直接将 $[m,n]\cdot[p,q]$ 定义为 $[mp,nq]$？为了回答为什么不能将 $[m,n]\cdot[p,q]$ 定义为 $[mp,nq]$，只需要注意到如下事实（如果定义 $[m,n]\cdot[p,q]$ 为 $[mp,nq]$ 的话）：

1) $[m+k,n+k]=[m,n]$
2) $[m+k,n+k]\cdot[p,q]=[mp+kp,nq+kq]$
3) $[m,n]\cdot[p,q]=[mp,nq]$
4) 如果 $p\neq q$，则 $[mp+kp,nq+kq]\neq[mp,nq]$。

至于为什么整数的乘法是按照定义2.6.4中的方式定义，可以做如下的简单计算/验证：

$$(m-n)(p-q)=mp-mq-np+nq=(mp+nq)-(mq+np)\ 。$$

至此，我们定义了整数上的乘法。考虑注2.6.3中定义的 ρ，该映射和乘法结构也是相容的。换言之，我们有如下命题：

命题 2.6.2. 对于上述 ρ 和任意 $m,n\in\mathbb{N}$，我们有 $\rho(mn)=\rho(m)\cdot\rho(n)$。

证明： 练习。 ∎

关于整数上的加法和乘法，它们之间也是有分配律的。

定理 2.6.2 (整数加法乘法之分配率). 对于任意整数 x,y 和 z， 我们有 $x\cdot(y+z)=x\cdot y+x\cdot z$ 。

证明： 练习。 ∎

习题：

习题 2.6.1. 证明：如果 $b\in\mathbb{N}-\{0\}$， 任何自然数 x 都不满足 $x+b=0$ 。

习题 2.6.2. 证明：如果 $[m_1,n_1]=[m_2,n_2]$ 且 $[m_2,n_2]=[m_3,n_3]$， 则 $[m_1,n_1]=[m_3,n_3]$ 。

习题 2.6.3. 根据定义2.6.1，证明 $\mathbb{Z}$ 是可数集。

习题 2.6.4. 证明定义2.6.2是良性定义的（well-defined）。具体的说，对于这个加法之定义，要证明了其与等价类的具体表示方式无关。

习题 2.6.5. 证明定理2.6.1。

习题 2.6.6. 证明定义2.6.3中给出的序关系是个良性定义的序关系（首先该定义是良性的，其次该定义的确给出了一个偏序关系），并进一步证明该序关系是个全序关系。

习题 2.6.7. 证明命题2.6.1。

习题 2.6.8. 证明命题2.6.2。

习题 2.6.9. 证明整数之乘法（见定义2.6.4）是良性定义的（well-defined）。

习题 2.6.10. 证明定理2.6.2。

2.7 最大公因子和辗转相除法

给定整数 m 和 整数 $n>0$， 我们仍然可以定义其上的带余除法。具体的说，我们有如下性质：

命题 2.7.1 (带余除法). 对于任意给定整数 m 和 整数 $n>0$， 存在唯一的整数 p 和 r，使得

$$m=pn+r\ ,$$

其中 $0\leq r<n$ 。

该命题证明不难，可以作为练习。

对于两个正整数，我们可以定义他们的最大公因子（greatest common divisor）。

定义 2.7.1. 对于正整数 m 和 n， 它们的最大公因子是同时整除 m 和 n 的正整数中最大的那个，记为 $\gcd(m,n)$ 。 最大公因子也被称为最大公约数。

命题 2.7.2. 对于任意给定正整数 m 和 n， 假定在带余除法下有 $m=pn+r$， 则 $\gcd(m,n)=\gcd(r,n)$ 。

证明. 如果整数 x 满足 $x|m$ 且 $x|n$， 注意到 $r=m-pn$， 可得 $x|r$ 。 因此，如果整数 x 同时整除 m 和 n， 则 x 必定同时整除 r 和 n 。

反之，如果整数 x 同时整除 r 和 n， 注意到 $m=pn+r$， 可得 $x|m$ 。 因此，如果整数 x 同时整除 r 和 n， 则 x 必定同时整除 m 和 n 。

至此，我们证明了 m 和 n 的公约数集合等于 r 和 n 的公约数集合。因此 $\gcd(m,n)=\gcd(r,n)$ 。 □

基于上述命题，为了得到正整数 m 和 n 的最大公因子，我们只需要考虑 r 和 n 的最大公因子即可。由于 r 是余数，因此 r 是“相对较小”的，从而 r 和 n 的最大公因子是相对“容易”计算的。基于这个直观的观察， 我们可以通过所谓的辗转相除法来得到两个正整数的最大公因子。

比如，为了计算 13 和 7 的最大公因子，由于 $13=7\cdot 1+6$， 故而 $\gcd(13,7)=\gcd(6,7)$ 。由于 $7=6\cdot 1+1$， 故而 $\gcd(6,7)=\gcd(6,1)$ 。 由于 $1|6$， 故 $\gcd(6,1)=1$ 。 因此 $\gcd(13,7)=1$ 。

用数学的形式语言来讲，我们有如下命题：

命题 2.7.3 (辗转相除法). 给定任意正整数 m 和 n， 我们可以令 $r_1=m$, $r_2=n$ 。 r_1 对 r_2 做带余除法得到的余数记为 r_3， r_2 对 r_3 做带余除法得到的余数记为 r_4， $\cdots$， r_k 对 r_{k+1} 做带余除法得到的余数记为 r_{k+2} 。 如此下去，直到某个 $r_s=0$ 首次出现（这是一定会出现的，因为 $r_1,r_2,\cdots$ 是严格单调递减的正整数列）。那么 r_{s-1} 就一定等于 $\gcd(m,n)$ 。 这就是通过辗转相除法来得到两个正整数的最大公因子。

命题 2.7.4. 对于任意正整数 m 和 n， 一定存在 $a,b\in\mathbb{Z}$， 使得 $am+bn=\gcd(m,n)$ 。

证明：[大略证明] 考虑辗转相除法倒过来走一遍即可。 ■

习题：

习题 2.7.1. 证明命题 2.7.2 。

习题 2.7.2. 若 p 为素数且 $p|mn$ ， 其中 m 和 n 都是正整数，证明 p 一定整除 m 和 n 中的至少一个。

习题 2.7.3. 对于两个非零自然数 m 和 n ， 我们已经定义他们的最大公因子为他们所有公因子全体中的最大的那个，并且记为 $\gcd(m,n)$ 。 类似的，对于三个非零自然数 m,n 和 k，我们这里定义它们的公约数集合为（cd for common divisors）

$$\mathrm{cd}(m,n,k)=\{r\in\mathbb{N}-\{0\}\colon r|m,\quad r|n \text{ 且 } r|k\}\ ,$$

并且定义 $\gcd(m,n,k)$ 为 $\mathrm{cd}(m,n,k)$ 中的最大值。由于 $1\in\mathrm{cd}(m,n,k)$，并且 $\mathrm{cd}(m,n,k)$ 中任意元素大小不会超过 m ， 因此 $\gcd(m,n,k)$ 也是良性定义的。

基于上述定义（关于三个非零自然数的最大公因子）和课上学过的内容（比如辗转相除法等），完成如下：

i）证明：对于任意三个非零自然数 m,n 和 k，

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

ii）证明：对于任意非零自然数 m 和 n， 存在 $p,q\in\mathbb{Z}$ ， 使得

$$mp+nq=\gcd(m,n)$$

iii）证明：对于任意三个非零自然数 m,n 和 k， 存在 $p,q,r\in\mathbb{Z}$ ， 使得

$$mp+nq+kr=\gcd(m,n,k)$$

iv）在 ii）中，对于给定非零自然数 m 和 n ， 满足 $mp+nq=\gcd(m,n)$ 的二元整数组 $(p,q)\in\mathbb{Z}^2$ 是唯一的吗？若是，给出证明；若否，给出反例。

2.8 有理数：$(\mathbb{Z}-\{0\},\times)$ 之 Grothendieck 化

现在我们定义了整数。在整数上，我们可以做乘法，但是未必一直可以做“除法”。这里说的“除法”，是基于如下自然的想法（naive idea）： “我们说 x 除以 y 等于 z ， 如果 y 乘以 z 等于 x 。 ”

前面我们证明了整数上乘法的消去律。和加法消去律不一样，整数乘法的消去律是对非零元素成立的。

对于 $\mathbb{Z}-\{0\}$ ， 我们使用Grothendieck化的思想来定义 $\mathbb{Q}-\{0\}$ 。 这个过程和 $(\mathbb{N},+)$ 的Grothendieck化是非常类似的，我们这里不再详细的给出证明之细节，只是给出基本的定义和事实。

定义 2.8.1. 对于 $m,n\in\mathbb{Z}$ 且 $n\neq 0$ ， 定义等价类 $[m,n]$ 如下：

$$[m,n]=[m',n'] \text{ 当且仅当 } mn'=nm' \text{ 。}$$

定义 2.8.2 ($\mathbb{Q}$). 上述等价类的全体定义为 $\mathbb{Q}$ 。 对于全体 $m,n\in\mathbb{Z}-\{0\}$ ， 其对应的 $[m,n]$ 等价类全体定义为 $\mathbb{Q}^*$ 。

定义 2.8.3 ($\mathbb{Q}$ 上乘法). 对于$[m,n],[m',n']\in\mathbb{Q}$，定义其乘法为 $[m,n]\cdot[m',n']=[mm',nn']$ 。

目前为止，所有的定义都是非常直观的。

定义 2.8.4 ($\mathbb{Q}$ 上加法). 对于$[m,n],[p,q]\in\mathbb{Q}$，定义其加法为 $[m,n]+[p,q]=[mq+np,nq]$ 。

注 2.8.1. 关于 $\mathbb{Q}$ 上加法，我们没有将 $[m,n]+[p,q]$ 定义为 $[m+p,n+q]$ 。 因为这样定义不是良性的。为什么？

注 2.8.2. 为什么 $\mathbb{Q}$ 上的加法如此定义？该定义是否为良性的？

定理 2.8.1. $\mathbb{Q}$ 上加法满足结合律和交换律 。

定理 2.8.2. $\mathbb{Q}$ 上乘法和加法满足分配率 。

定理 2.8.3. $\mathbb{Q}^*$ 上乘法满足消去率 。

$\mathbb{Q}$ 中零元指的是 $[0,n]$ ， 其中 $n\in\mathbb{Z}-\{0\}$。

定理 2.8.4. 对于任意 $s,t\in\mathbb{Q}$ ， $\mathbb{Q}$ 中的方程 $x+s=t$ 存在唯一的解。 如果更进一步有 $s\neq 0$ ， 则 $\mathbb{Q}$ 中的方程 $x\cdot s=t$ 存在唯一的解。

类似于 $\mathbb{Z}$ 是 $\mathbb{N}$ 的扩展，我们也可以说明 $\mathbb{Q}$ 是 $\mathbb{Z}$ 的扩展。事实上，我们可以定义

$$\rho\colon\mathbb{Z}\longrightarrow\mathbb{Q},\quad m\mapsto[m,1] \text{ 。}$$

定理 2.8.5. 上述定义的 ρ 是一一对应（双射），且 ρ 保持乘法和加法结构。换言之，$\forall m,n\in\mathbb{Z}$ ， 我们有 $\rho(m+n)=\rho(m)+\rho(n)$ 并且 $\rho(m\cdot n)=\rho(m)\cdot\rho(n)$

该定理的证明并不难，只要根据 ρ 的定义，还有自然数以及有理数上加法和乘法的定义，就能够完成证明。这样的看似无聊无难度的验证，在数学中还是需要的。这样的验证（或者类似的推导），有时被非正式的称为 “abstract nonsense” 。比如，“We can prove the theorem above (that ρ is ...) due to some abstract nonsense.”

有理数上的序关系

问题：在 $\mathbb{N}$ 上，我们定义了序关系 $\leq$ 。 如何将这个序关系扩展定义到 $\mathbb{Z}$ 上（参考本课件前面部分之内容）？如果更进一步扩展定义到 $\mathbb{Q}$ 上 ？

练习：给出 $\mathbb{Q}$ 上的序关系（$\leq$），使得这个序关系和高中所知道的有理数的大小比较关系相一致。换言之，根据 $\mathbb{Q}$ 的严格定义，给出高中所学的有理数上$\leq$关系之严格定义。

为了定义 $r \leq s$ ， 只需要定义 $r - s \leq 0$ 。 当然，先要定义什么是 $r - s$ 。 一种方法是将 $r - s$ 定义为 $r + (-s)$ ， 而 $-s$ 为满足方程 $x + s = 0$ 的唯一 x 。

根据自己的直观，给出上述概念的定义，是很好的数学训练的机会。

习题：

习题 2.8.1. 回答**注2.8.1** 和 **注2.8.2** 中的问题。

习题 2.8.2. 证明**定理2.8.1**。

习题 2.8.3. 证明**定理2.8.2**。

习题 2.8.4. 证明**定理2.8.3**。

习题 2.8.5. 证明**定理2.8.4**。

2.9 自然数、整数、有理数上的距离

目前为止，我们通过Peano公理定义了自然数 $\mathbb{N}$ ， 并且基于Peano公理中的后继映射依次定义了自然数中加法、乘法、序关系和带余除法等运算和结构。基于加法半群 $(\mathbb{N}, +)$ ， 根据 Grothendieck 话的思想，我们得到了加法群 $(\mathbb{Z}, +)$ 。 基于 $(\mathbb{Z}, +)$ 的群结构，我们可以定义 $\mathbb{Z}$ 上的减法为 $m - n = m + (-n)$ ，其中 $m, n \in \mathbb{Z}$ 。 同时，我们可以自然地将 $\mathbb{N}$ 上的乘法结果扩展到 $\mathbb{Z}$ 上。$\mathbb{Z}$ 关于加法是个群，但是关于乘法不是个群，这是因为 0 在乘法下是不可逆的。根据附件中环的定义，$\mathbb{Z}$ 是一个环。因为 $\mathbb{Z}$ 关于乘法交换，$\mathbb{Z}$ 还是个交换环。

上述的工作，是纯代数（purely algebraic）的。这一节里面，我们引入距离的概念，并且对于任意两个有理数，给出了它们之间的距离。

首先我们需要明白，什么是距离（distance）？距离，顾名思义，就是用来描述两个对象的远近。距离这个概念，是分析中许多基本概念的基础。比如，关于函数 f 连续性的 $\epsilon-\delta$ 定义，这里的 ϵ 和 δ ， 分别描述的就是 f 的值域和定义域上的距离。

其次，如何得到有理数的距离？根据有理数的引入方式，我们可以先得到自然数上的距离结构，然后得到整数上的距离结构，最后得到有理数上的距离结构。

基于序关系，我们可以定义两个元素 a 和 b 之间的距离为 $|a-b|$ ， 其中若 $a\leq b$ ， 则定义 $|a-b|$ 为 $b-a$ ， 否则定义 $|a-b|=a-b$ 。 简单的说，距离结构是由序结构和减法决定的。

QQQ

在 $\mathbb{Q}$ 上，基于上面练习给出的序关系 $\leq$ ， 我们可以定义两个有理数 r,s 的距离为 $|r-s|$ 。证明该距离满足三角不等式。换言之，对于任意 $r,s,t\in\mathbb{Q}$ ， 我们有 $|r-t|\leq|r-s|+|s-t|$ 。

习题：

习题 2.9.1. 证明有理数上的距离结构满足三角不等式。

2.10 实数：有理数的完备化

目前为止，我们已经给出了有理数集 $\mathbb{Q}$ 的严格定义，并且定义了有理数上的序结构、加法和乘法结构、以及距离结构等。本节中我们给出有理数的完备化，并将其定义为实数集 $\mathbb{R}$ 。 当然，我们也会将序结构、加法乘法结构和距离结构等推广到实数上。

注 2.10.1. 从历史上讲，有理数集上的戴特金分割（Dedekind Cut）是更早给出的实数严格定义。该方法基于 $\mathbb{Q}$ 给出了 $\mathbb{R}$ 的严格定义。但是该方法过于依赖于序结构，适用范围不如完备化。例如，如果要基于 $\mathbb{Q}^2$ 来得到 $\mathbb{R}^2$ ， 那么戴特金分割不能直接不加改动的适用，但是完备化方法是完全可以直接不加修改的使用的。

2.11 实数的基本性质

我们已经给出了实数的严格定义（有理数的完备化）。基于此，我们来给出实数的一些基本性质，比如确界原理，闭区间套原理等等。

2.12 应用：有限/无限集的另一种定义

第 3 章

常用不等式技巧

3.1 基本思路和方法

不等式证明（上下界估算）没有统一的固定方法。只能依靠多积累、多分析。本节中我们通过一些练习，大略的说明下如何处理不等式。

例题：对于任意 $p \in \mathbb{N}_{\geq 1}$和 $a, b \in \mathbb{R}_{\geq 0}$ ， 证明 $(a+b)^p \geq a^p + b^p$ 。

这个证明比较简单，通过多项式展开即可完成。

例题：对于任意 $p \in \mathbb{R}_{\geq 1}$ 和 $a, b \in \mathbb{R}_{\geq 0}$ ， 证明 $(a+b)^p \geq a^p + b^p$ 。

这个例题中，因为 p 为实数，我们无法直接用多项式展开的方式来完成证明。但是我们可以尽量将我们不熟悉（或者是不太容易处理的）划归为我们比较熟悉的（或者相对容易处理的）。

一种思路是：上面不等式两边如果有一边为常数，可能会好处理些。我们在不等式两边同时除上 $(a+b)^p$ （需要确保 $(a+b)^p$ 不是0 。 根据题意，只要不是 $a = b = 0$ 的情况，我们都是有 $(a+b)^p \neq 0$ 的），就得到 $1 \geq \frac{a^p}{(a+b)^p} + \frac{a^p}{(a+b)^p}$ 。 注意到$1 = \left(\frac{a}{a+b}\right)^1 + \left(\frac{b}{a+b}\right)^1$ ， 剩下的就容易多了。

另一种思路是：对于实数 p ， 我们可以写成 p 的正整数部分和小数部分 $p = [p] + p'$ ， 其中 $[p] \in \mathbb{N}$ 且 $[p] \leq p < p+1$ ， $p' = p - [p]$ 。 对于整数次幂的情况我们是有上面的不等式的，因此我们有

$$\begin{aligned}(a+b)^p &= (a+b)^{[p]}\cdot(a+b)^{p'}\\ &\geq (a^{[p]}+b^{[p]})\cdot(a+b)^{p'}\\ &= a^{[p]}(a+b)^{p'}+b^{[p]}(a+b)^{p'}\\ &\geq a^{[p]}a^{p'}+b^{[p]}b^{p'}\\ &= a^p+b^p.\end{aligned}$$

习题：

习题 3.1.1. 对于任意 $n\in\mathbb{N}_{\geq 1}$和 $x\in\mathbb{R}_{\geq 0}$ ， 证明 $(1+x)^n\geq 1+nx$ 。

提示：该证明比较简单，直接多项式展开比较即可。

习题 3.1.2. 对于任意 $n\in\mathbb{N}_{\geq 1}$和 $x\in\mathbb{R}_{\geq 0}$ ， 证明 $(1-x)^n\geq 1-nx$ 。

提示：这个不等式证明起来不是那么直接。一种思路是用数学归纳法。

习题 3.1.3. 对于任意 $a,b\in\mathbb{R}$ ， 证明

$$\frac{|a+b|}{1+|a+b|}\leq\frac{|a|}{1+|a|}+\frac{|b|}{1+|b|}。$$

提示：上面的不等式证明，基本方法还是缩放（以及多次尝试）。

习题 3.1.4. 对于任意 $p>0$ ，证明

$$|a+b|^p\leq 2^p\max\left(|a|^p,|b|^p\right)$$

3.2 基于凸性的不等式证明

函数的凸性是类似于凸集的概念。具体的说，其定义如下：

定义 3.2.1. 我们说实函数 $f\colon \mathbb{R} \to \mathbb{R}$ 在 $[a,b]$ 上是凸的（concave up），如果对于任意 $x,y \in [a,b]$ 和 $\lambda \in (0,1)$，均有 $f(\lambda x + (1-\lambda)y) \le \lambda f(x) + (1-\lambda)f(y)$。我们说 f 是严格凸的，如果对于任意 $x,y \in [a,b]$ 和 $\lambda \in (0,1)$，均有 $f(\lambda x + (1-\lambda)y) < \lambda f(x) + (1-\lambda)f(y)$。

我们说实函数 $f\colon \mathbb{R} \to \mathbb{R}$ 在 $[a,b]$ 上是凹的（concave down），如果 $-f$ 是凸的。

根据上面的定义，$f\colon \mathbb{R} \to \mathbb{R}$ 是凸的，当且仅当 f 图像上方的部分（作为线性空间 $\mathbb{R} \times \mathbb{R}$ 中的子集）是凸集。

很多常见函数都是凸的或者严格凸的。

例 3.2.1. $f(x) = x^2$ 在 $(-\infty, \infty)$ 上是凸的。事实上，该函数是严格凸的。

例 3.2.2. 线性函数 $f(x) = kx + b$ 在 $(-\infty, \infty)$ 上是凸的，但不是严格凸的。

例 3.2.3. $f(x) = x^2$ 在 $[0, \infty)$ 上是凸的。事实上，该函数在 $[0, \infty)$ 上是严格凸的。

例 3.2.4. $f(x) = \tan x$ 在 $[0, \pi/2)$ 上是严格凸的。

对于连续函数，凸性的定义可以改为如下：

定义 3.2.2. 我们说连续函数 $f\colon \mathbb{R} \to \mathbb{R}$ 在 $[a,b]$ 上是凸的，如果对于任意 $x,y \in [a,b]$，均有

$$f\left(\frac{x+y}{2}\right) \le \frac{f(x)+f(y)}{2}.$$

对于连续函数，我们只需要在凸性定义中取 $\lambda = \frac{1}{2}$，因为有如下定理。

定理 3.2.1. 对于连续函数 $f\colon [a,b] \to \mathbb{R}$，如果

$$f\left(\frac{x+y}{2}\right) \le \frac{f(x)+f(y)}{2} \quad \forall x,y \in [a,b],$$

则对于任意 $\lambda \in (0,1)$，均有

$$f(\lambda x + (1-\lambda)y) \le \lambda f(x) + (1-\lambda)f(y) \quad \forall x,y \in [a,b].$$

该定理证明不难。可以先证明对于任意 $\lambda \in \{\frac{k}{2^n} : k,n \in \mathbb{N}, k \le 2^n\}$，不等式成立。注意到 $\{\frac{k}{2^n} : k,n \in \mathbb{N}, k \le 2^n\}$ 在 $[0,1]$ 中是稠密的，根据 f 的连续性，即可得到不等式对于任意 0 和 1 之间的 λ 均成立。

如果我们已知一个函数为凸函数，根据凸性的定义，我们可以直接得到相关的不等式。如何判断一个函数在某个区间上是否为凸函数呢？

函数凸性之判断

为了判断一个函数 f 在区间 $[a,b]$ 上是否为凸，最基本的方法当然还是根据定义。

例 3.2.5. 证明 $f(x)=x^2$ 在 $\mathbb{R}$ 上是凸函数。

证明： 显然，$f(x)=x^2$ 是连续函数。根据定理3. 2. 1，为了说明 $f(x)$ 为凸函数，我们只需要证明对于任意 $x,y\in\mathbb{R}$ ， 均有

$$f\left(\frac{x+y}{2}\right)\leq\frac{f(x)+f(y)}{2}\ 。$$

由于

$$f\left(\frac{x+y}{2}\right)=\left(\frac{x+y}{2}\right)^2=\frac{x^2+2xy+y^2}{4}\leq\frac{x^2+(x^2+y^2)+y^2}{4}=\frac{x^2+y^2}{2}=\frac{f(x)+f(y)}{2}\ ,$$

证毕。 ∎

对于二次可导的函数，判断凸性可以通过比较二阶导数和零的大小来得到。事实上，我们有如下定理。

定理 3.2.2. 假定函数 $f\colon(a,b)\to\mathbb{R}$ ， 二次可导并且二阶导函数连续。换言之，$f\in C^2(a,b)$ 。如果 $f''(x)\geq 0$ ，$\forall x\in(a,b)$ ，则 f 在 (a,b) 上为凸函数。

证明： 对于任意 $x,y\in(a,b)$ 和 $\lambda\in(0,1)$ ， 我们需要证明

$$f(\lambda x+(1-\lambda)y)\leq\lambda f(x)+(1-\lambda)f(y)\ 。$$

对于任意如上给定的 x,y 和 λ ， 不妨假定 $x<y$ 。 令 $z=\lambda x+(1-\lambda)y$ 。 容易验证

$$z-x=(1-\lambda)(y-x)\quad 且\quad y-z=\lambda(y-x)\ 。$$

根据中值定理，存在 $c_1\in[x,z],c_2\in[z,y]$ ， 使得

$$f(z)-f(x)=(z-x)f'(c_1)=(1-\lambda)(y-x)f'(c_1)$$

且

$$f(y)-f(z)=(y-z)f'(c_2)=\lambda(y-x)f'(c_2)\ 。$$

据此，我们有

$$\begin{aligned}f(z)-[\lambda f(x)+(1-\lambda)f(y)]&=[\lambda f(z)+(1-\lambda)f(z)]-[\lambda f(x)+(1-\lambda)f(y)]\\&=\lambda[f(z)-f(x)]+(1-\lambda)[f(z)-f(y)]\\&=\lambda(1-\lambda)(y-x)f'(c_1)-(1-\lambda)\lambda(y-x)f'(c_2)\\&=\lambda(1-\lambda)(y-x)[f'(c_1)-f'(c_2)]\end{aligned}$$

由于 f' 是 (a,b) 上的可微函数，根据中值定理，存在 $d\in[c_1,c_2]$ ， 使得 $f'(c_1)-f'(c_2)=(c_1-c_2)f''(d)$ 。 因此

$$\begin{aligned}f(z)-[\lambda f(x)+(1-\lambda)f(y)]&=\lambda(1-\lambda)(y-x)[f'(c_1)-f'(c_2)]\\&=\lambda(1-\lambda)(y-x)(c_1-c_2)f''(d)\ 。\end{aligned}$$

根据题设，$f''(d) \geq 0$ 。 由于 $c_1 \in [x,z]$ 且 $c_2 \in [z,y]$ ， $c_1 - c_2 \leq 0$ 。 至此，我们有

$$f(z) - [\lambda f(x) + (1-\lambda) f(y)] \leq 0 \ ,$$

证毕。 ∎

注 3.2.1. 在假定 $f \in C^2(a,b)$ 的前提下，上述定理的逆也是成立的。否则，存在 $c \in (a,b)$ ，使得 $f''(c) < 0$ 。 根据连续函数介值定理，f'' 一定在 c 的某个邻域里面为严格负。在该小邻域里面用上述定理证明中的方法，可以得到 f 在这个小邻域里面是凹的，而这与 f 在 (a,b) 上的凸性矛盾。

上述**定理3.2.2**（以及其逆）使得对于 $C^2(a,b)$ 上函数凸性的判断变成了简单的验证二阶导函数的符号，从而大大简化了判断。

例 3.2.6. 通过判断二阶导函数符号的方式，很容易得到如下结论：

1) e^x 是凸函数；

2) 对于任意正的偶数 n ， x^n 是凸函数；

3) $\ln x$ 是凹函数；

4) 在 $[-1,1]$ 上，$\sqrt{1-x^2}$ 是凹函数。

习题：

习题 3.2.1. 若函数 f 在 $[a,b]$ 上为凸函数，f 是否一定为连续函数？若是，给出证明；若否，给出反例。

习题 3.2.2. 证明定理 3.2.1 。

习题 3.2.3. 证明 $\ln(x+1)$ 是凹函数。

习题 3.2.4. 若函数 f 和 g 在 (a,b) 上为凸函数，证明 $f+g$ 在 (a,b) 上也一定是凸函数。

习题 3.2.5. 若函数 f 和 g 在 (a,b) 上为凸函数， $f \cdot g$ 在 (a,b) 上是否一定是凸函数？若是，给出证明；若否，给出反例。

习题 3.2.6. 若函数 $f,g\colon \mathbb{R} \to \mathbb{R}$ 都是凸函数， $f \circ g$ 在 $\mathbb{R}$ 上是否一定是凸函数？若是，给出证明；若否，给出反例。

习题 3.2.7. 完成**注3.2.1**中所提到的逆命题之证明。

3.3 Cauchy-Schwartz不等式、Hölder不等式和Minkowski不等式等

本节中所介绍的不等式，均可以看做基于函数凸性不等式技巧之应用。

定理 3.3.1 (Jensen不等式). 设 f 为 $[a,b]$ 上的凸函数。对于任意 $x_1,\cdots,x_n\in[a,b]$ 和正数 $\lambda_1,\cdots,\lambda_n$ ， 均有

$$f\left(\frac{\sum_{i=1}^n\lambda_i x_i}{\sum_{i=1}^n\lambda_i}\right)\leq\frac{\sum_{i=1}^n\lambda_i f(x_i)}{\sum_{i=1}^n\lambda_i}\ 。$$

注 3.3.1. $n=2$ 时，Jensen不等式和凸函数的定义是一样的。对于一般的 n ， 可以用数学归纳法来证明Jensen不等式。

定理 3.3.2 (Cauchy-Schwartz不等式). 对于实数 $a_1,\cdots a_n$ 和 $b_1,\cdots,b_n$ ， 我们有

$$\left|\sum_{i=1}^n a_ib_i\right|\leq\left(\sum a_i^2\right)^{\frac{1}{2}}\left(\sum b_i^2\right)^{\frac{1}{2}}$$

在内积空间中，有与上述类似的不等式（可以认为是上述Cauchy-Schwartz不等式的推广），被称为Cauchy-Bunyakovsky-Schwartz不等式。

Hölder不等式可以认为是Cauchy-Schwartz不等式的推广。

定理 3.3.3 (Hölder不等式). 对于满足 $\frac{1}{p}+\frac{1}{q}=1$ 的正实数 p 、q 和实数 $a_1,\cdots a_n$ 以及 $b_1,\cdots,b_n$ ， 我们有

$$\sum_{i=1}^n|a_ib_i|\leq\left(\sum_{i=1}^n|a_i|^p\right)^{\frac{1}{p}}\left(\sum_{i=1}^n|b_i|^q\right)^{\frac{1}{q}}\ 。$$

因为Cauchy-Schwartz不等式是Hölder不等式中 $p=q=2$ 之特列，我们只需要证明Hölder不等式即可。为此，我们先证明如下引理。

引理 3.3.1. 对于任意正数 a,b 和满足 $\frac{1}{p}+\frac{1}{q}=1$ 的正数 p,q ， 均有

$$a^{\frac{1}{p}}b^{\frac{1}{q}}\leq\frac{a}{p}+\frac{b}{q}\ 。$$

证明： 注意到 e^x 为凸函数（因为其二阶可导并且二阶导数处处大于等于零），我们有

$$\begin{aligned}a^{\frac{1}{p}}b^{\frac{1}{q}}&=e^{\ln(a^{\frac{1}{p}}b^{\frac{1}{q}})}\\&=e^{\frac{1}{p}\ln a+\frac{1}{q}\ln b}\\&\leq\frac{1}{p}e^{\ln a}+\frac{1}{q}e^{\ln b}\\&=\frac{a}{p}+\frac{b}{q}\ 。\end{aligned}$$

■

下面这个齐次性质是比较明显的，其证明作为练习。

命题 3.3.1. 对于任意的 $1 \leq p < \infty$ 、$\lambda \geq 0$ 和正数 $a_1, \cdots, a_n$ ， 均有

$$\lambda \left(\sum_{i=1}^{n} a_i^p \right)^{\frac{1}{p}} = \left(\sum_{i=1}^{n} (\lambda a_i)^p \right)^{\frac{1}{p}}$$

现在我们来证明 Hölder不等式。

证明：[Hölder不等式之证明]

对于Hölder不等式中出现的实数 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_n$ ， 我们不妨假定它们都是非负的。

根据命题3.3.1中的其次性质，我们不妨假定

$$\left(\sum_{i=1}^{n} a_i^p \right)^{\frac{1}{p}} = \left(\sum_{i=1}^{n} b_i^q \right)^{\frac{1}{q}} = 1 \ 。$$

换言之，我们假定

$$\sum_{i=1}^{n} a_i^p = \sum_{i=1}^{n} b_i^q = 1 \ 。$$

对于任意 $1 \leq i \leq n$ ， 根据引理3.3.1 ，我们有

$$a_i b_i \leq \frac{a_i^p}{p} + \frac{b_i^q}{q} \ 。$$

故

$$\sum_{i=1}^{n} a_i b_i \leq \frac{1}{p} \sum_{i=1}^{n} a_i^p + \frac{1}{q} \sum_{i=1}^{n} b_i^q = \frac{1}{p} + \frac{1}{q} = 1 = \left(\sum_{i=1}^{n} a_i^p \right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} b_i^q \right)^{\frac{1}{q}} \ 。$$

■

定理 3.3.4 (Minkowski不等式). 对于任意 $p \in [1, \infty)$ 和实数 $a_1, \cdots, a_n$ 以及 $b_1, \cdots, b_n$ ，我们均有

$$\left(\sum_{i=1}^{n} |a_i + b_i|^p \right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} |a_i|^p \right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} |b_i|^p \right)^{\frac{1}{p}}$$

证明： 不妨假定所有的 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_n$ 都是非负的。

不妨更进一步假定 $\sum_{i=1}^{n} |a_i + b_i|^p \neq 0$ 。 通过对所有的 $a_1, \cdots, a_n$ 和 $b_1, \cdots, b_n$ 同时乘上某个正数 λ ， 我们可以有

$$\sum_{i=1}^{n} |\lambda a_i + \lambda b_i|^p = 1$$

注意到Minkowski不等式两边是其次的，我们可以不妨假设

$$\sum_{i=1}^{n}|a_i+b_i|^p=1 \ 。$$

注意到

$$\begin{aligned}\left(\sum_{i=1}^{n}|a_i+b_i|^p\right)^{\frac{1}{p}} &= \sum_{i=1}^{n}|a_i+b_i|^p \\ &= \sum_{i=1}^{n}(|a_i+b_i|)\cdot|a_i+b_i|^{p-1} \\ &\le \sum_{i=1}^{n}(|a_i|+|b_i|)\cdot|a_i+b_i|^{p-1} \\ &= \sum_{i=1}^{n}\left(|a_i|\cdot|a_i+b_i|^{p-1}+|b_i|\cdot|a_i+b_i|^{p-1}\right) \\ &= \sum_{i=1}^{n}|a_i|\cdot|a_i+b_i|^{p-1}+\sum_{i=1}^{n}|b_i|\cdot|a_i+b_i|^{p-1} \ 。\end{aligned}$$

由于 $\frac{1}{p}+\frac{1}{q}=1$ ， 根据**定理3.3.3** （Hölder不等式），我们有

$$\sum_{i=1}^{n}|a_i|\cdot|a_i+b_i|^{p-1}\le\left(\sum_{i=1}^{n}|a_i|^p\right)^{\frac{1}{p}}\cdot\left(\sum_{i=1}^{n}|a_i+b_i|^{(p-1)q}\right)^{\frac{1}{q}} \ 。$$

由于 $\frac{1}{p}+\frac{1}{q}=1$ ， $(p-1)q=p$ 。 根据我们的假设，$\sum_{i=1}^{n}|a_i+b_i|^p=1$ 。 因此我们有

$$\sum_{i=1}^{n}|a_i|\cdot|a_i+b_i|^{p-1}\le\left(\sum_{i=1}^{n}|a_i|^p\right)^{\frac{1}{p}} \ 。$$

同理，

$$\sum_{i=1}^{n}|b_i|\cdot|a_i+b_i|^{p-1}\le\left(\sum_{i=1}^{n}|b_i|^p\right)^{\frac{1}{p}} \ 。$$

基于此，Minkowski不等式得证。 ∎

习题：

习题 3.3.1. 证明**命题3.3.1**。

习题 3.3.2. 证明Jensen不等式。

习题 3.3.3. 对于任意正实数 $a_1,\cdots,a_n$ ， 证明

$$\frac{\sum_{i=1}^n a_i^2}{n} \geq \left(\frac{\sum_{i=1}^n a_i}{n}\right)^2 \quad 。$$

习题 3.3.4. 对于任意正实数 $a_1,\cdots,a_n$ ， 根据Jensen不等式证明

$$\sqrt[n]{a_1\cdots a_n} \leq \frac{\sum_{i=1}^n a_i}{n} \quad 。$$

习题 3.3.5. 证明如下之广义Hölder不等式。

假定正实数 p,q,r 满足 $\frac{1}{p}+\frac{1}{q}=\frac{1}{r}$ 。 则对于任意实数 $a_1,\cdots,a_n$ 和 $b_1,\cdots,b_n$ ， 均有

$$\left(\sum_{i=1}^n |a_ib_i|^r\right)^{\frac{1}{r}} \leq \left(\sum_{i=1}^n |a_i|^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^n |b_i|^q\right)^{\frac{1}{q}} \quad 。$$

习题 3.3.6. 在Minkowski不等式中，若 $p\in(0,1)$ ， 不等式仍然成立吗？若是，给出证明；若否，给出反例。

DRAFT [March 4, 2015]

第4章

离散群以及离散群作用相关性质

Banach-Tarski悖论（定理）是数学中非常著名和重要的一个结果。事实上，正是受到Banach-Tarski悖论的启发，德国数学家John von Neumann提出了群的“顺从性”概念。虽然一般被称为Banach-Tarski悖论，在数学上，如果承认选择公理（目前主流数学是承认的），它是完全正确的。之所以称为Banach-Tarski悖论，只是说与日常的朴素直观相悖，并不是说数学上是错误的。该悖论的典型构造涉及到数学中的选择公理、测度论、群的顺从性（amenability）和群在集合上的作用等概念。

本章介绍群以及群在集合上的作用，并且引出相悖性和顺从性的概念。这些知识，除了是理解Banach-Tarski悖论（定理）的必要准备外，本身也是很重要的。

4.1 群和群在集合上的作用

我们首先给出群的定义如下：

定义 4.1.1 (群). 群是一个集合 G 和 其上的群结构 （代数运算）· ， 其中该运算满足：

1) ［封闭性］对任意 $a,b \in G$ ， $a \cdot b$ 仍在 G 中

2) ［结合律］$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ， $\forall a,b,c \in G$

3) [恒等元] $\exists e \in G$ ，满足 $e \cdot a = a \cdot e = a$ ， $\forall a \in G$

4) [逆元] $\forall a \in G$ ， $\exists b \in G$ ， 满足 $a \cdot b = b \cdot a = e$

上述的群，可以记为 $(G, \cdot)$ ， 或者简记为 G 。 $a \cdot b$ 也可以简记为 ab 。

如果群的运算是交换的，则我们称这个群为交换群（或者Abel群）。

定义 4.1.2 (交换群). 我们说群 $(G, \cdot)$ 是交换的（或者换言之，G 是交换群），如果对于任意 $a, b \in G$ ， 都有 $ab = ba$ 。

下面我们给出一些和群相关的例子：

例 4.1.1. $(\mathbb{Z}, +)$ 是群。

例 4.1.2. $(\mathbb{Z}, \times)$ 不是群。

例 4.1.3. $(\mathbb{Q}, +)$ 是群。

例 4.1.4. $(\mathbb{Q}, \times)$ 不是群。

例 4.1.5. $(\mathbb{Q} - \{0\}, \times)$ 是群。

例 4.1.6. $(\mathbb{Q}_{>0}, \times)$ 是群。

例 4.1.7. $(M_n(\mathbb{C}), +)$ 是群，其中加法为矩阵加法。

例 4.1.8. $(M_n(\mathbb{C}), \times)$ 不是群，其中乘法为矩阵乘法。

例 4.1.9. $(GL_n(\mathbb{C}), \times)$ 是群，其中乘法为矩阵乘法，$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \colon \det(A) \neq 0\}$ 。$GL_n(\mathbb{C})$ 也被称为复数域上的一般线性群（general linear group）。

例 4.1.10. 令 $G = \{f \in C[0,1] \colon f(0) = f(1)\}$ 并定义其上加法为函数的加法，乘法为函数的乘法。则 $(G, +)$ 是个群，但是 $(G, \times)$ 不是个群。

例 4.1.11. 令 $G = \{f \in C[0,1] \colon f(0) = f(1)$ 且 $f(x) > 0 \ \forall x \in [0,1]\}$ 并定义其上乘法为函数的乘法。则 $(G, \times)$ 是个群。

例 4.1.12. 令 $G = \{f \in C[0,1] \colon f(0) = f(1)^2$ 且 $f(x) > 0 \ \forall x \in [0,1]\}$ 并定义其上乘法为函数的乘法。则 $(G, \times)$ 是个群。

例 4.1.13. 令 X 为非空集合。用 $\mathrm{BIJ}(X)$ 表示 X 上的双射全体构成的集合。由于 $\mathrm{id}_X \in \mathrm{BIJ}(X)$ ， 故 $\mathrm{BIJ}(X)$ 非空。对于任意 $f, g \in \mathrm{BIJ}(X)$ ， 定义其乘法 $f \cdot g$ 为函数的复合 $f \circ g$ 。则 $(\mathrm{BIJ}(X), \cdot)$ 是个群。

命题 4.1.1. 群 G 中恒等元 e 是唯一的。

证明： 如果 e_1 和 e_2 都是恒等元，根据恒等元的性质，我们有

$$e_1 = e_1 \cdot e_2 = e_2 \ 。$$

证毕。 ∎

命题 4.1.2. 群 G 中任意元素 a 的逆元是唯一的。

证明： 假设 b_1 和 b_2 都是 a 的逆元，则

$$a \cdot b_1 = e \text{ 且 } b_2 \cdot a = e \text{ 。}$$

故

$$b_2 = b_2 \cdot e = b_2 \cdot (a \cdot b_1) = (b_2 \cdot a) \cdot b_1 = e \cdot b_1 = b_1 \text{ 。}$$

证毕。 ∎

定义 4.1.3 (子群). 我们说 H 是群 $(G, \cdot)$ 的子群，如果 $H \subset G$ 并且该子集 H 在运算 $\cdot$ 下满足群定义中的四条性质。

例 4.1.14. $(\mathbb{Z}, +)$ 是个群。其中所有的偶整数构成一个子群，但是所有的奇整数不构成一个子群。

例 4.1.15. $(\mathbb{Z}, +)$ 是个交换群。

例 4.1.16. $(M_2(\mathbb{R}), \cdot)$ 不是个群。这里的乘法为矩阵乘法。

例 4.1.17. 在矩阵乘法下，$GL_2(\mathbb{R})$ 是个群，但不是交换群。这里 $GL_2(\mathbb{R})$ 定义为 $(M_2(\mathbb{R}), \cdot)$ 中行列式不为零（换言之，可逆）的矩阵全体。

例 4.1.18. 对于 $n \in \mathbb{N}_{\geq 1}$ ， 记 $\mathbb{R}^n$ 上的刚体变换全体为 $\mathbb{E}_n$ ， 则 $\mathbb{E}_n$ 是个非交换群。

注 4.1.1. 若群 G 的子群 H 为非交换群，则 G 为非交换群。

注 4.1.2. 由群的定义可知，对于任意 $a \in G$ ， 都可以通过“左乘 a ”定义一个 G 到 G 的双射

$$L_a \colon G \longrightarrow G, \quad g \mapsto a \cdot g \text{ 。}$$

类似的，右乘 a （不妨记为 R_a ）也是个双射。

定义 4.1.4 (群在集合上的作用). 我们说群 G 作用在集合 X 上（G acts on X），如果有映射

$$G \times X \longrightarrow X, \quad (g, x) \mapsto g(x) \text{ ，}$$

满足

1) $e_G(x) = x$ ， $\forall x \in X$ ， 其中 e_G 为 G 中单位元

2) $(g \cdot h)(x) = g(h(x))$ ， $\forall g, h \in G, x \in X$

注 4.1.3. 如果 $X = G$ ， 我们总是可以定义 G 在 G 上的作用为 $G \times G \longrightarrow G$ ， $(g, h) \mapsto g \cdot h$ 。 换言之，G 通过左乘作用在自身上。

定义 4.1.5. 群 G 作用在集合 X 上。对于 $E \subset X$ ， 我们说 E 是 $G-$“相悖” 的，如果 E 可以无交的划分成子集 $A_1, \cdots, A_m, B_1, \cdots, B_n$ ， 并且存在 G 中元素 $g_1, \cdots, g_m, h_1, \cdots, h_n$ ， 使得

$$X = \bigcup_{i=1}^{m} g_i(A_i) = \bigcup_{j=1}^{n} h_j(B_j) \ 。$$

据此，我们可以定义 “X 是 G-相悖”的 ，这也被称为 “该作用是相悖的”。

注 4.1.4. 在上述定义中，E 是划分为有限个子集。

定义 4.1.6. 我们说群 G 是相悖的，如果 G 在 $X = G$ 上的左乘作用是相悖的。

定义 4.1.7. 群 G 在集合 X 上的作用是自由 (free) 的，如果对于任何 $g \in G - \{e_G\}$ ， g 在 X 上的作用没有不动点。换言之，如果 $g(x) = x$ ， 则 g 一定为 e_G 。

例 4.1.19. 群 G 在 G 上的左乘作用是自由的。证明不难，不妨作为练习。

4.2 刚体变换群

在这里，我们给出空间上刚体变换群的定义，并且介绍刚体变换群作用之相悖性。这些相悖性质是 Banach-Tarski 悖论的基础之一。

首先，我们给出 $\mathbb{R}^n$ 上刚体变换的严格定义。

定义 4.2.1 ($\mathbb{R}^n$ 上刚体变换). 在空间 $\mathbb{R}^n$ 中，定义任意两点 $x = (x_1, \cdots, x_n)$ 和 $y = (x_1, \cdots, x_n)$ 之间的距离为

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \ 。$$

我们说 $\mathbb{R}^n$ 到自身的**双射** f 是个 $\mathbb{R}^n$ 上的**刚体变换**，如果对于任意的 $x, y \in \mathbb{R}^n$ ， 我们有

$$d(f(x), f(y)) = d(x, y) \ 。$$

注 4.2.1. 简单的说，刚体变化就是等距变换（或者叫保距变换）。

注 4.2.2. 为了简单起见，我们将刚体变换定义为“双射+保距”。事实上，上面**刚体变化的定义中，可以将双射换成映射**。事实上，根据保距性，可以得到刚体变换一定为单射（为什么？）

⋆ **思考题** ⋆ **：**证明 $\mathbb{R}^n$ 到自身的保距变换一定是双射。

提示：证明是单射比较容易，关键要证明是满射。不妨先想想如何证明 $\mathbb{R}^1$ 中的保距映射一定是满射。注意到 $\mathbb{R}^n$ 中的距离结构是“严格凸”的。换言之，如果 x 和 y 是 $\mathbb{R}^n$ 中两个不同的点， 则对于任意的 $0 \leq s \leq \mathrm{dist}(x,y)$ ， 存在唯一的 $z \in \mathbb{R}^n$ ， 使得 $\mathrm{dist}(x,z) = s$ 且 $\mathrm{dist}(y,z) = \mathrm{dist}(x,y) - s$ ， 并且 z 一定在连接 x 和 y 的线段上。

关于该思考题，证明方法有很多。一种方法是先考虑一维情形，证明 $\mathbb{R}$ 到自身的保距变换一定是双射。然后让维数足够增加，对维数做归纳。还有一种方法是直接证明所有的刚体变换都是仿射变换（affine maps）。

在《数学分析》课程中，你们应该已经学过了函数的连续性。基于其概念，我们也可以定义从 $\mathbb{R}^n$ 到自身的映射之连续性。

定义 4.2.2 ($\mathbb{R}^n$ 到 $\mathbb{R}^n$ 映射之连续性). 对于 $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ ， 我们说 f 在 $x \in \mathbb{R}^n$ 处连续，如果 $\forall \epsilon > 0, \exists \delta > 0$ ， 使得对于任意满足 $d(y,x) < \delta$ 的 $y \in \mathbb{R}^n$ ，均有 $d(f(y), f(x)) < \epsilon$ 。我们说 f 是连续的，如果 f 在 $\mathbb{R}^n$ 中的每点上都连续。

注 4.2.3. 根据刚性变换的定义，我们立即可以得到如下事实：**所有的刚体变换都是连续的**。事实上，因为刚体变换是保距的，只需要将 δ 取为 ϵ 即可。

注 4.2.4. 我们前面已经证明了这样的定理：如果一个相悖的群 G 自由的作用在 X 上，则这个作用是相悖的（换言之，X 是 G-相悖的）。刚体变换群可否自由的作用在 $\mathbb{R}^n$ 中的单位球上呢（其中 $n \in \mathbb{N}_{\geq 1}$）？答案是否定的！我们这里不假证明的介绍Brouwer不动点定理的一种简单形式。

定理 4.2.1 (Brouwer不动点定理). 在 $\mathbb{R}^n$ 中，用 B^n 代表 $\{x \in \mathbb{R}^n \colon d(x,0) \leq 1\}$ （换言之，B^n 是闭单位球）。则任意从 B^n 到自身的连续映射一定存在不动点。

4.3 顺从群、Tarski定理

群的相悖性和群的顺从性是等价的。

定理 4.3.1 (Tarski定理). 群 G 是相悖的，当且仅当 G 是顺从的。

习题：

习题 4.3.1. 对于群 G 在 X 上的作用 $G\times X\to X$， $(g,x)\mapsto g(x)$， 固定 $g\in G$，我们得到 $X\to X, x\mapsto g(x)$。 证明：对于任意固定的 $g\in G$， 其诱导的映射 $X\to X, x\mapsto g(x)$ 一定是双射。

习题 4.3.2. 令 H 为 G 的子群。证明 H 在集合 $X=G$ 上的左乘 $H\times X\longrightarrow X$， $(h,x)\mapsto h\cdot x$ 也是一个作用。

习题 4.3.3. 我们首先定义 $\mathbb{R}^n$ 上的线性变换。$f\colon \mathbb{R}^n\longrightarrow \mathbb{R}^n$ 被称为是线性映射，如果任意 $x,y\in\mathbb{R}^n$ 和 $\lambda\in\mathbb{R}$， 均有 $f(x+y)=f(x)+f(y)$ 和 $f(\lambda x)=\lambda f(x)$。 其中 $x=(x_1,\cdots,x_n)$， $y=(y_1,\cdots,y_n)$， 加法定义为 $(x_1,\cdots,x_n)+(y_1,\cdots,y_n)=(x_1+y_1,\cdots,x_n+y_n)$， 乘法定义为 $\lambda(x_1,\cdots,x_n)=(\lambda x_1,\cdots,\lambda x_n)$。

然后我们定义 $\mathbb{R}^n$ 上的仿射变换。$f\colon \mathbb{R}^n\longrightarrow \mathbb{R}^n$ 被称为是仿射变换，如果任意 $x,y\in\mathbb{R}^n$ 和 $\lambda\in\mathbb{R}$， 均有 证明：刚体变换一定是线性变换。并给出线性变换不是刚体变换的例子。

习题 4.3.4. 验证如下关于刚体变换的事实：

1) **[封闭性]** 假设 f 和 g 都是 $\mathbb{R}^n$ 到自身的保距映射，则 $f\circ g$ 也是保距映射。

2) **[结合律]** 假定 f,g 和 h 都是 $\mathbb{R}^n$ 到自身的保距映射，则 $(f\circ g)\circ h$ 和 $f\circ(g\circ h)$ 都是$\mathbb{R}^n$ 到自身的保距映射，并且 $(f\circ g)\circ h=f\circ(g\circ h)$。

3) **[恒等元]** 假定 f 是 $\mathbb{R}^n$ 到自身的保距映射，则 $f\circ \mathrm{Id}_{\mathbb{R}^n}$ 和 $\mathrm{Id}_{\mathbb{R}^n}\circ f$ 都是$\mathbb{R}^n$ 到自身的保距映射，并且 $f\circ \mathrm{Id}_{\mathbb{R}^n}=\mathrm{Id}_{\mathbb{R}^n}\circ f$， 其中 $\mathrm{Id}_{\mathbb{R}^n}$ 为 $\mathbb{R}^n$ 上的恒等映射。

4) **[逆元]** 假定 f 是 $\mathbb{R}^n$ 到自身的保距映射，则 f^{-1} 也是保距的。

根据上面的验证，我们知道 $\mathbb{R}^n$ 中 **所有的刚体变换构成一个群**，记为 $\mathbb{E}_n$。

习题 4.3.5. 对于所有 $n\in\mathbb{N}_{\geq 1}$， $\mathbb{E}_n$ 不是交换群。

4.4 群以及群作用、作用的相悖性

我们首先给出群的定义，然后给出群在集合上作用之定义，并讨论相关的性质。

定义 4.4.1. 群是一个集合 G 和 其上的群结构 （代数运算）$\cdot$， 其中该运算满足：

1) [封闭性] 对任意 $a,b\in G$， $a\cdot b$ 仍在 G 中

2) [结合律] $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ ， $\forall a,b,c\in G$

3) [恒等元] $\exists e\in G$ ，满足 $e\cdot a=a\cdot e=a$ ， $\forall a\in G$

4) [逆元] $\forall a\in G$ ， $\exists b\in G$ ， 满足 $a\cdot b=b\cdot a=e$

上述的群，可以记为 $(G,\cdot)$ ， 或者简记为 G 。 $a\cdot b$ 也可以简记为 ab 。

命题 4.4.1. 群 G 中恒等元 e 是唯一的。

证明： 如果 e_1 和 e_2 都是恒等元，根据恒等元的性质，我们有

$$e_1=e_1\cdot e_2=e_2 \text{ 。}$$

∎

命题 4.4.2. 群 G 中任意元素 a 的逆元是唯一的。

证明： 假设 b_1 和 b_2 都是 a 的逆元，则

$$a\cdot b_1=e \text{ 且 } b_2\cdot a=e \text{ 。}$$

故

$$b_2=b_2\cdot e=b_2\cdot(a\cdot b_1)=(b_2\cdot a)\cdot b_1=e\cdot b_1=b_1 \text{ 。}$$

∎

用类似上面的方法，我们可以证明 a. 群中任意元素的左逆唯一； b. 群中任意元素的右逆唯一；c. 群中任意元素的左逆等于右逆。

定义 4.4.2. 我们说 H 是 群 $(G,\cdot)$ 的子群，如果 $H\subset G$ 并且该子集 H 在 运算 $\cdot$ 下满足群定义中的四条性质。

例 4.4.1. $(\mathbb{Z},+)$ 是个群。其中所有的偶整数构成一个子群，但是所有的奇整数不构成一个子群。

定义 4.4.3 (交换群/Abel群). 我们说群 $(G,\cdot)$ 是交换的（或者换言之，G 是交换群），如果对于任意 $a,b\in G$ ， 都有 $ab=ba$ 。

例 4.4.2. $(\mathbb{Z},+)$ 是个交换群。

例 4.4.3. $(M_2(\mathbb{R}),\cdot)$ 不是个群。这里的乘法为矩阵乘法。

例 4.4.4. 在矩阵乘法下，$GL_2(\mathbb{R})$ 是个群，但不是交换群。这里 $GL_2(\mathbb{R})$ 定义为 $(M_2(\mathbb{R}),\cdot)$ 中行列式不为零（换言之，可逆）的矩阵全体。

例 4.4.5. 对于 $n\in\mathbb{N}_{\geq 1}$ ， 记 $\mathbb{R}^n$ 上的刚体变换全体为 $\mathbb{E}_n$ ， 则 $\mathbb{E}_n$ 是个非交换群。

根据定义，若群 G 的子群 H 为非交换群，则 G 为非交换群。

注 4.4.1. 由群的定义可知，对于任意 $a \in G$ ， 都可以通过“左乘 a”定义一个 G 到 G 的双射

$$L_a \colon G \longrightarrow G, \quad g \mapsto a \cdot g \ 。$$

类似的，右乘 a （不妨记为 R_a ）也是个双射。

定义 4.4.4 (群在集合上的作用). 我们说群 G 作用在集合 X 上（G acts on X），如果有映射

$$G \times X \longrightarrow X, \quad (g, x) \mapsto g(x) \ ,$$

满足

1) $e_G(x) = x$ ， $\forall x \in X$ ， 其中 e_G 为 G 中单位元

2) $(g \cdot h)(x) = g(h(x))$ ， $\forall g, h \in G, x \in X$

注 4.4.2. 如果 $X = G$ ， 我们总是可以定义 G 在 G 上的作用为 $G \times G \longrightarrow G$ ， $(g, h) \mapsto g \cdot h$ 。 换言之，G 通过左乘作用在自身上。

习题 4.4.1. 对于群 G 在 X 上的作用 $G \times X \to X$ ， $(g, x) \mapsto g(x)$ ， 固定 $g \in G$ ， 我们得到 $X \to X, x \mapsto g(x)$ 。 证明：对于任意固定的 $g \in G$ ， 其诱导的映射 $X \to X, x \mapsto g(x)$ 一定是双射。

习题 4.4.2. 群 G 在自身上的右乘是否给出了一个作用？换言之，对于 $X = G$ ， $G \times X \longrightarrow X$, $(h, x) \mapsto x \cdot h$ 是否一定是个作用？若 G 是交换群呢？

习题 4.4.3. H 为 G 的子群。证明 H 在 $X = G$ 上的左乘 $H \times X \longrightarrow X$ ， $(h, x) \mapsto h \cdot x$ 也是一个作用。

定义 4.4.5 (群作用之相悖性). 群 G 作用在集合 X 上。对于 $E \subset X$ ， 我们说 E 是 G–“相悖” 的，如果 E 可以存在无交的子集 A_1，$\cdots$，A_m，B_1，$\cdots$，B_n ， 并且存在 G 中元素 g_1，$\cdots$，g_m，h_1，$\cdots$，h_n ， 使得

$$E = \bigcup_{i=1}^{m} g_i(A_i) = \bigcup_{j=1}^{n} h_j(B_j) \ 。$$

据此，我们可以定义 “X 是 G–相悖”的 ，这也被称为 “该作用是相悖的”。

注 4.4.3. 在上述定义中，E 是划分为有限个子集。

注 4.4.4. 在上述关于作用相悖性的定义中，不难得出，如果作用是相悖的，则定义中的 m 和 n 一定都是大于等于 2 的自然数。换言之，如果集合 X 在群 G 的作用下存在（Banach-Tarski）相悖性，则集合 X 至少要分成 4 块然后进行重组。试证明之。

问题：在上面关于群作用相悖性的定义中，我们没有要求 $A_1, \cdots, A_m$ 和 $B_1, \cdots, B_n$ 都是非空的。事实上，如果我们额外要求这些子集是非空的，得到的仍然是同一个定义。为什么？

注 4.4.5. 在上面的 “E 是 G-相悖”之定义中，我们没有要求 $g_i(A_i)$ 之间是互不相交的，也没有要求 $h_j(B_j)$ 之间是互不相交的。事实上，如果把上述定义中的

$$E=\bigcup_{i=1}^{m} g_i(A_i)=\bigcup_{j=1}^{n} h_j(B_j)$$

换为

$$E=\bigsqcup_{i=1}^{m} g_i(A_i)=\bigsqcup_{j=1}^{n} h_j(B_j)\ ,$$

得到的还是同一个定义。为什么？

提示：如有相交，考虑更细的剖分。

注 4.4.6. 在上面的“E 是 G-相悖”之定义中，我们也没有要求无交的子集 $A_1,\cdots,A_m$ ，$B_1,\cdots,B_m$ 并起来就是 E （可能它们的并只是 E 的真子集）。事实上，如果在上述定义中，额外要求

$$E=\left(\bigsqcup_{i=1}^{m} A_i\right)\bigsqcup\left(\bigsqcup_{j=1}^{n} B_j\right)\ ,$$

得到的还是同一个定义。为了说明这一点（也为了以后构造Banach-Tarski悖论时方便），我们需要后面提到的Banach-Schröder-Bernstein定理（可以看做某种Cantor-Bernstein定理）。【集合论中Cantor-Berstein定理也被称为Cantor-Schröder-Berstein定理，或Schröder-Berstein定理】。

如果我们将群在集合上作用之相悖性的定义改为如下，是否得到的还是同一个定义？为什么？

“

改动后定义：群 G 作用在集合 X 上。对于 $E\subset X$ ，我们说 E 是 $G-$“相悖” 的，如果 E 可以存在无交的子集 A_1，$\cdots$，A_m ，满足 $\bigsqcup_{i=1}^{m} A_i\subsetneq E$ ，并且存在 G 中元素 g_1，$\cdots$，g_m ，使得

$$E=\bigcup_{i=1}^{m} g_i(A_i)\ 。$$

”

注 4.4.7. 如果只要求 $A_1,\cdots,A_m$ 通过群的作用后并起来可以得到 E ，而不再要求 $B_1,\cdots,B_n$ 那部分，得到的不再是原来的相悖性之定义。

事实上，如果去掉 $B_1,\cdots,B_n$ 这部分，我们可以直接令 $A_1=X$ ，则我们始终有 $X=e_G(A_1)$ 。但是我们并不能说任何作用都是相悖的。如果这样还不足够令人信服，可以额外要求 $\bigsqcup_{i=1}^{m} A_i$ 是 X 的真子集 ，我们来说明即使如此，得到的仍然不是原来相悖性之定义。

为了说明这一点，我们考虑 $\mathbb{Z}$ 在自身上的作用：

$$\mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z},\ (m,n)\mapsto m+n\ 。$$

令 $A_1=\mathbb{Z}_{>0}$ ， $A_2=\mathbb{Z}_{<0}$ 。 令 $g=1\in\mathbb{Z}$ 。 则 $g(A_2)=g(\mathbb{Z}_{<0})=\mathbb{Z}_{<0}+1=\mathbb{Z}_{\leq 0}$ 。 故而

$$\mathbb{Z}=\mathbb{Z}_{\leq 0}\bigsqcup\mathbb{Z}_{>0}=g(A_2)\bigsqcup A_1\ ,$$

并且这里 $A_1\bigsqcup A_2\subsetneq\mathbb{Z}$ 。

关于 $(\mathbb{Z},+)$ ， 一个事实（该事实的详细证明，会在选读部分给出）就是，它是非相悖的。因此，如果我们在相悖性的定义中不要求 $B_1,\cdots,B_n$ 那部分通过群的作用可以得到 X ，这样得到的不再是原来的定义。

命题 4.4.3. 群 $(\mathbb{Z},+)$ 是非相悖的。

习题：

习题 4.4.4. 证明**注4.4.4**中提到的事实。

习题 4.4.5. 完成如下练习：

i) 在群 G 中，若将 a 的逆元记为 a^{-1} ， 将 b 的逆元记为 b^{-1} 。 证明：$a\cdot b$ 的逆元是 $b^{-1}\cdot a^{-1}$ 。

ii) 证明：群 G 的左乘，的确是个群 G 在集合 G 上的作用。其中左乘定义如下（作为集合， $X=G$）：

$$G\times X\longrightarrow X,\quad (g,x)\mapsto g\cdot x\quad \forall g\in G,x\in G\ 。$$

iii) 群 G 的右乘，是不是个群 G 在集合 G 上的作用？若是，给出证明；若否，给出证明。这里右乘定义为（作为集合， $X=G$）：

$$G\times X\longrightarrow X,\quad (g,x)\mapsto x\cdot g\quad \forall g\in G,x\in G\ 。$$

iv) 假定

$$G\times X\longrightarrow X,(g,x)\mapsto g(x)\quad \forall g\in G,x\in X$$

给出了群 G 在集合 X 上的作用。对于 G 的任意子群 H ， 证明

$$H\times X\longrightarrow X,(h,x)\mapsto h(x)\quad \forall h\in H,x\in X$$

给出了群 H 在集合 X 上的作用。

4.5 群的相悖性以及顺从性

这里我们介绍群的相悖性以及顺从性。事实上，群的相悖性等价于群的非顺从性质。

定义 4.5.1. 我们说群 G 是相悖的，如果 G 在 $X=G$ 上的左乘作用是相悖的。

定义 4.5.2. 群 G 在集合 X 上的作用是自由(free)的，如果对于任何 $g\in G-\{e_G\}$ ， g 在 X 上的作用没有不动点。换言之，如果 $g(x)=x$ ， 则 g 一定为 e_G 。

例 4.5.1. 群 G 在 G 上的左乘作用是自由的。证明不难，不妨作为练习。

习题 4.5.1. 若 G 是有限群 （换言之，存在 $n\in\mathbb{N}$ ， 使得 $|G|=n$ ），证明 G 一定不是相悖的。

后面会介绍到，任意交换群都一定不是相悖的。

下面的定理给出了类似Banach-Tarski悖论之现象存在的一个充分条件。

定理 4.5.1. 如果 G 在 X 上的作用是自由的并且 G 是相悖的，则 X 是 G-相悖的。

注 4.5.1. 该定理使得我们可以从群 G 的相悖性得到 G 在 X 上作用之相悖性。当然，此定理需要该作用本身是自由的。该定理的证明是需要选择公理（AC）的。

注 4.5.2. 我们后面会给出群的顺从性（amenability）之定义，并且会介绍Tarski定理，该定理主要内容就是“一个群 G 是相悖的，当且仅当 G 是非顺从的”。

下面我们来证明该定理。

证明： 首先，我们按照群 G 在 X 上的作用在 X 上定义等价类（或称为轨道）。对于 $x,y\in X$ ， 我们说 $x\sim y$ ， 如果存在 $g\in G$ ， 使得 $y=g(x)$ 。

断言：上面我们定义的 $\sim$ 关系是等价关系。换言之，该关系满足自反性、对称性和传递性。

断言之证明： 对于任意 $x\in X$ ， 由于 $e_G(x)=x$ ，故 $x\sim x$ 。 自反性得证。

关于对称性，如果 $x\sim y$ ， 则存在 $g\in G$ ，使得 $y=g(x)$ 。 因此

$$x=e_G(x)=g^{-1}(g(x))=g^{-1}(y)\ ,$$

故 $y\sim x$ 。

下面我们证明传递性。对于任意 $x,y,z\in X$ ， 假定 $x\sim y$ 且 $y\sim z$ ， 我们来证明 $x\sim z$ 。 事实上，根据 $\sim$ 之定义，存在 $f,g\in G$ ，满足 $y=f(x)$ 和 $z=g(y)$ 。 故 $z=g(y)=g(f(x))=(g\cdot f)(x)$ 。 换言之，$x\sim z$ 。传递性得证。至此，上述断言证明完毕。

基于上面的断言，我们可以将 X 按照等价关系 $\sim$ 进行划分。令

$$\langle x\rangle=\{y\in X\colon y\sim x\}\ 。$$

根据 $\sim$ 的定义，

$$\langle x\rangle=\{g(x)\colon g\in G\}\ 。$$

所有也可以将 $\langle x\rangle$ 记为 $G\cdot x$ ， 这里 $G\cdot x$ 代表

$\{g(x)\colon g\in G\}$ （轨道） 。每个 $\langle x\rangle$ 代表了所有和 x 等价的元素构成的等价类。对于任意 $f\in G$ ， 显然有 $\langle x\rangle=\langle f(x)\rangle$ 。

根据选择公理，在每个等价类中，选取一个元素 x_i 。 这里 $i\in\mathcal{I}$ ，而 $\mathcal{I}$ 的基数等于 X 中由所有等价类（这里也是轨道）构成的集合之基数。换言之，我们有

$$X=\bigsqcup_{i\in\mathcal{I}}\langle x_i\rangle=\bigsqcup_{i\in\mathcal{I}}G\cdot x_i \ 。$$

令 $D=\{x_i\colon i\in\mathcal{I}\}$ 。 基于群作用的自由性，我们有：

断言：在 $\langle x_i\rangle=G\cdot x_i$ 中的任意元素 y ，存在唯一 $g\in G$ ，使得 $y=g(x_i)$ 。 这里 $i\in\mathcal{I}$ 。

断言之证明：假定存在 $y\in X$ 和 $f,g\in G,f\neq g$ ， 使得 $f(x_i)=g(x_i)=y$ 。 则

$$x_i=e_G(x_i)=f^{-1}(f(x_i))=f^{-1}(g(x_i))=(f^{-1}\cdot g)(x_i) \ 。$$

由于群 G 的作用是自由的，基于 $(f^{-1}\cdot g)(x_i)=x_i$ ， 我们有 $f^{-1}\cdot g=e_G$ 。 故

$$f=f\cdot e_G=f\cdot(f^{-1}\cdot g)=(f\cdot f^{-1})\cdot g=e_G\cdot g=g \ 。$$

这与假设中的 $f\neq g$ 矛盾。故断言得证。

基于该断言和 G 的相悖性，我们可以构造性的证明 G 在 X 上作用的相悖性。

由于群 G 是相悖的，存在 G 的互不相交之子集 $A_1,\cdots,A_m$ ， $B_1,\cdots,B_n$ ， 以及 G 中元素 $g_1,\cdots,g_m$ 和 $h_1,\cdots,h_n$ ， 使得

$$G=\bigcup_{i=1}^{m}f_i(A_i)=\bigcup_{j=1}^{n}h_j(B_j) \ 。$$

断言：对于 X 中互不相交的子集 $A_1\cdot D,\cdots,A_m\cdot D$ ， $B_1\cdot D,\cdots,B_n\cdot D$ ， 以及上面的 G 中元素 $g_1,\cdots,g_m$ 和 $h_1,\cdots,h_n$ ， 我们有

$$X=\bigcup_{i=1}^{m}f_i(A_i\cdot D)=\bigcup_{j=1}^{n}h_j(B_j\cdot D) \ ,$$

这里 $A_i\cdot D$ 定义为 $\{g(x)\cdot\colon g\in A_i,x\in D\}$ ， $B_j\cdot D$ 定义为 $\{g(x)\cdot\colon g\in B_j,x\in D\}$ 。

断言之证明：证明不难，留作练习。

基于上述断言，我们完成了本定理之证明。 ∎

注 4.5.3. 为了从 G 的相悖性得到 G 在 X 上作用之相悖性，我们必须对作用加适当的条件（比如上述定理中的“作用是自由的”）。如果对作用不加任何条件，G 的相悖性是不足以确保 G 在 X 上的作用之相悖性的。比如，G 是个相悖的群，G 在 X 上的作用为恒等作用：$G\times X\to X,(g,x)\mapsto x\ \forall g\in G,x\in X$ 。 则该作用一定不可能是相悖的（虽然 G 是相悖的）。

注 4.5.4. 一个自然的问题就是，为了使得 G 在 X 上的作用是相悖的，是否需要 G 本身是相悖的？答案是肯定的。 换言之，为了得到群 G 在集合 X 上的相悖作用，一个必要条件就是“G 是相悖的”。下面我们给出这个事实的证明。该证明是不需要选择公理的。

定理 4.5.2. 如果群 G 在集合 X 上的作用是相悖的，则群 G 一定是相悖的。

证明： 首先，我们描述下证明的大体思路。基于群 G 在 X 上的作用，我们可以将 X 看成所有轨道的无交并。注意到 G 的作用不会产生轨道间的迁移（这个根据轨道 Gx 的定义可得），G 在 X 上作用的相悖性，一定表现为在每个轨道上作用的相悖性。取定 $x \in X$ ， 在轨道 Gx 上，我们试图根据该轨道上作用的相悖性来得到群 G 本身的相悖性。由于群在集合上的作用不要求是自由的，对于 $y \in Gx$ ， 可能有不止一个的 $g \in G$ ， 满足 $y = g(x)$ 。 但是这个并不重要。

下面是正式的证明。这里给出主要步骤，其他的一些验证性工作留作练习。

假设群 G 作用在集合 X 上并且该作用是相悖的。取定 $x \in X$ ， 令 $Gx = \{g(x) \colon g \in G, x \in X\}$ 。

断言：根据 G 在 X 上的作用，可以诱导 G 在 Gx 上的作用。其定义为

$$G \times Gx \longrightarrow Gx, \ (g, h(x)) \mapsto g(h(x)) \ 。$$

断言之证明：练习。要注意检查断言中的定义是良性的。比如对于 Gx 中某个元素 $h(x)$ ，可能该元素也可以写成 $s(x)$ 其中 $h, s \in G$ 。

断言：如果 G 作用在 X 上是相悖的，则前面断言中定义的 G 在 Gx 上的作用也是相悖的。

断言之证明：练习。根据作用相悖性的定义不难证明。关键要先证明如下事实（证明并不难）：对于任意 $f \in G$ 和 $A \subset X$ ， 有 $f(A) \cap Gx = f(A \cap Gx)$ 。

根据上述断言，我们得到了 G 在 Gx 上作用的相悖性。下面我们由此得到 G 在 G 上作用的相悖性。

对于任意 $y \in Gx$ ， 定义

$$H_y = \{g \in G \colon g(x) = y\} \ 。$$

断言： $\bigsqcup_{y \in Gx} H_y = G$ 。

断言之证明：根据定义不难得到，留作练习。

由于 G 在 Gx 上的作用是相悖的，存在 Gx 中互不相交的子集 $A_1, \cdots, A_m$ 和 $B_1, \cdots, B_n$ ， 以及 G 中元素 $g_1, \cdots, g_m$ 和 $h_1, \cdots, h_n$ ， 使得

$$Gx = \bigcup_{i=1}^{m} g_i(A_i) = \bigcup_{j=1}^{n} h_j(B_j) \ 。$$

断言：对于上述的 $A_1, \cdots, A_m$ 和 $B_1, \cdots, B_n$ ， 以及 $g_1, \cdots, g_m$ 和 $h_1, \cdots, h_n$ ， 令 $\mathcal{A}_i = \bigcup_{y \in A_i} H_y$ 和 $\mathcal{B}_j = \bigcup_{y \in B_j} H_y$ ， 其中 $1 \leq i \leq m$ ， $1 \leq j \leq n$ 。 则有

$$G = \bigcup_{i=1}^{m} g_i(\mathcal{A}_i) = \bigcup_{j=1}^{n} h_j(\mathcal{B}_j) \ 。$$

断言之证明：基本是按照定义验证，留作练习。

根据上面的断言，我们证明了群 G 本身是相悖的。 ∎

注 4.5.5. 为了得到群 G 在集合 X 上的相悖作用，上述定理告诉我们， G 必须是相悖的。前面我们也说明过，为了得到 G 在 X 上的相悖作用，光有 G 的相悖性是不够的，需要该作用满足一定的条件（反例就是相悖群 G 通过恒等作用作用在 X 上，则该作用一定不是相悖的）。那么，一个自然的问题就是：我们是否一定需要该作用（G 在 X 上的作用）是自由的？答案是否定的！这一点，在后面Banach-Tarski悖论的具体构造中可以看到。

根据上面的定理，注意到前面提过的事实，“$n=1,2$ 时，$\mathbb{E}_n$ 是顺从的（非悖论的）。$n\geq 3$ 时，$\mathbb{E}_n$ 是非顺从的（悖论的）”。对于 $k=1,2$ ， 考虑 $\mathbb{E}_k$ 在 $\mathbb{R}^k$ 上的作用，我们可以立即得到如下推论：

推论 4.5.1. 用 $\mathbb{E}_k$ 来表示 $\mathbb{R}^k$ 中刚体变换全体构成的群（称为刚体变换群）。在 $k=1$ 或者 $k=2$ 的情形下，任意 $\mathbb{E}_k$ 在 $\mathbb{R}^k$ 上的作用，都不可能是“相悖”的。

习题：

习题 4.5.2. 证明任意有限群一定是非相悖的。提示：数（3声）数（4声）。

4.6 自由群

关于群的相悖性，前面提到过，有限群一定不可能是相悖的。关于相悖的群，可能最简单的例子就是自由群 $\mathbb{F}_2$ 了。这里我们给出自由群的定义和其基本性质。

定义 4.6.1. 对于 $n\in\mathbb{N}_{\geq 1}$ ， n 阶自由群（记为 $\mathbb{F}_n$ ）为所有由 $x_1,\cdots,x_n$ 及其逆 $x_1^{-1},\cdots,x_n^{-1}$ 构成的词（word）之全体。这里的词长度有限，并可写为 $s_1\cdots s_k$ 的形式，其中 $s_j\in\{e,x_1^{\pm 1},\cdots,x_n^{\pm 1}\}$ ， $\forall 1\leq j\leq k$ 。 词的乘法通过连接（concatenation）来定义。比如，“Hello”和“world” 的连接为“Helloworld”。

注 4.6.1. 在自由群定义中，唯一可能的消去（化简）情形为 $x_i x_i^{-1} = e$ ， $x_i^{-1} x_i = e$ ， $ex_i = x_i$ ， $x_i e = x_i$ ， $ex_i^{-1} = x_i^{-1}$ ， $x_i^{-1} e = x_i^{-1}$ 。 其中 e 为恒等元。

注 4.6.2. 自由群定义中的字，一般都是完全化简后的形式。比如，$baa^{-1}ea$ 一般记为 ba 。

注 4.6.3. $(\mathbb{Z}, +)$ 可以看做 $\mathbb{F}_1$ ，为什么？更精确的描述是，存在双射 $\rho\colon (\mathbb{Z}, +) \longrightarrow \mathbb{F}_1$ ，使得 $\rho(m+n) = \rho(m) \cdot \rho(n)$ ， $\forall m, n \in \mathbb{Z}$ 。 这里的 ρ ， 也被称为 $(\mathbb{Z}, +)$ 到 $\mathbb{F}_1$ 的（群）同构。

另外一个关于自由群的性质是，对于任意 $n \in \mathbb{N}_{\geq 2}$ ， $\mathbb{F}_n$ 都是相悖的。为了证明这个事实，我们首先证明 $\mathbb{F}_2$ 是相悖的，然后证明如果群 G 包含一个相悖群作为子群，则 G 一定也是相悖的。最后，注意到如果 $m \geq n$ ， 则 $\mathbb{F}_n$ 总是 $\mathbb{F}_m$ 的子群。至此， 便可以得到只要 $n \geq 2$ ， 则 $\mathbb{F}_n$ 都是相悖的。

命题 4.6.1. 自由群 $\mathbb{F}_2$ 是相悖的。

证明： 不妨假定 $\mathbb{F}_2$ 是由 a, b, a^{-1}, b^{-1} 生成的。 用 $W(a)$ 代表所有化简后以 a 开始的字，用 $W(b)$ 代表所有化简后以 b 开始的字。类似的，定义 $W(a^{-1})$ 和 $W(b^{-1})$ 。

注意到

$$\begin{aligned}\mathbb{F}_2 &= \{e\} \bigsqcup W(a) \bigsqcup W(b) \bigsqcup W(a^{-1}) \bigsqcup W(b^{-1}) \\ &= W(a) \bigsqcup aW(a^{-1}) \qquad \text{为什么?} \\ &= W(b) \bigsqcup bW(b^{-1}) \qquad \text{为什么?}\end{aligned}$$

故 $\mathbb{F}_2$ 是个相悖的群。 ∎

命题 4.6.2. 若群 G 的子群 H 是相悖的，则 G 也是相悖的。

证明： 我们这里只给出框架，具体细节不难，请自行填充。

前面已经给出了群 G 在自身上的左乘作用。这里我们定义子群 H 在群 G 上的左乘如下：

$$H \times G \longrightarrow G, \ (h, g) \mapsto h \cdot g \ 。$$

断言： 上述子群 H 在群 G 上的左乘的确是个作用。

断言之证明： 练习。

断言： 上述子群 H 在群 G 上的左乘作用是自由的。

断言之证明： 练习。根据群的定义不难得到。

基于上述的断言，我们知道 H 在群 G 上的作用（具体的说，左乘作用）是自由的。由于群 H 是相悖的，根据定理“如果相悖群自由的作用在集合上，则该作用是相悖的”，我们知道 G 是 H-相悖的，从而 G 是个相悖群（为什么？）。 ∎

命题 4.6.3. 若 $m, n \in \mathbb{N}_{\geq 1}$ 且 $m \leq n$ ，则存在群 $\mathbb{F}_m$ 到群 $\mathbb{F}_n$ 的单射 ρ ，满足 $\rho(ab) = \rho(a)\rho(b)$ ， $\forall a, b \in \mathbb{F}_m$ 。 换言之，$\mathbb{F}_m$ 可看成 $\mathbb{F}_n$ 的子群。

证明： 这个证明是平凡（trivial）的。 ∎

基于上述结论，可以直接得到如下定理。

定理 4.6.1 (自由群 $\mathbb{F}_n$ 的相悖性). 当 $n \in \mathbb{N}_{\geq 2}$ 时， 自由群 $\mathbb{F}_n$ 是相悖的。

习题：

习题 4.6.1. 对于任意 $n \in \mathbb{N}_{\geq 1}$ ， 证明 $\mathbb{F}_n$ 作为集合是可数集。

习题 4.6.2. 对于任意 $n \in \mathbb{N}_{\geq 2}$ ， 证明 $\mathbb{F}_n$ 是非交换的。

习题 4.6.3. 证明**命题4.6.2**的证明中之断言。

4.7 刚体变换群及其相关性质

根据前面的结果，如果一个群 G 是相悖的，则任意包含 G 作为子群的群 F 也一定是相悖的。这个事实，在用来判断群是否是相悖的时候，是非常有用的。比如，考虑三维空间 $\mathbb{R}^3$ 上的刚体变换构成的群，$\mathbb{E}_3$ 。 我们后面会说明，在 $\mathbb{E}_3$ 中存在子群同构于 $\mathbb{F}_2$ ， 这样就证明了群 $\mathbb{E}_3$ 是相悖的。为了找到 $\mathbb{E}_3$ 中同构于 $\mathbb{F}_2$ 的子群，关键是找到 $\mathbb{E}_3$ 中的两个“完全独立的”元素 a 和 b 。 这里的“完全独立”是指不可能出现类似 $a^2 = b^{-3}$ 或者 $a^3 = ba^7b^{-1}$ 等等之类的情形。

首先，我们给出 $\mathbb{R}^n$ 上刚体变换的严格定义。

定义 4.7.1. 在空间 $\mathbb{R}^n$ 中，定义任意两点 $x = (x_1, \cdots, x_n)$ 和 $y = (y_1, \cdots, y_n)$ 之间的距离为

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \ 。$$

我们说 $\mathbb{R}^n$ 到自身的双射 f 是个 $\mathbb{R}^n$ 上的刚体变换，如果对于任意的 $x, y \in \mathbb{R}^n$ ， 我们有

$$d(f(x), f(y)) = d(x, y) \ 。$$

注 4.7.1. 简单的说，刚体变化就是等距变换（或者叫保距变换）。

注 4.7.2. 为了简单起见，我们将刚体变换定义为“双射+保距”。事实上，上面刚体变化的定义中，可以将双射换成映射。事实上，根据保距性，可以得到刚体变换一定为单射（为什么？）

【⋆ 思考题 ⋆】证明：$\mathbb{R}^n$ 到自身的保距变换一定是双射。（提示：证明是单射比较容易，关键要证明是满射。不妨先想想如何证明 $\mathbb{R}^1$ 中的保距映射一定是满射。）

在《数学分析》课程中，你们应该已经学过了函数的连续性。基于其概念，我们也可以定义从 $\mathbb{R}^n$ 到自身的映射之连续性。

定义 4.7.2. 对于 $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ ， 我们说 f 在 $x \in \mathbb{R}^n$ 处连续，如果 $\forall \epsilon > 0, \exists \delta > 0$ ， 使得对于 $y \in \mathbb{R}^n$ ， 若 $\mathrm{d}(y,x) < \delta$ ， 则 $\mathrm{d}(f(y), f(x)) < \epsilon$ 。 我们说 f 是连续的，如果 f 在 $\mathbb{R}^n$ 中的每点上都连续。

注 4.7.3. 根据刚性变换的定义，我们立即可以得到如下事实：所有的刚体变换都是连续的。事实上，因为刚体变换是保距的，只需要将 δ 取为 ϵ 即可。

注 4.7.4. 我们前面已经证明了这样的定理：如果一个相悖的群 G 自由的作用在 X 上，则这个作用是相悖的（换言之，X 是 G-相悖的）。刚体变换群可否自由的作用在 $\mathbb{R}^n$ 中的单位球上呢（其中 $n \in \mathbb{N}_{\geq 1}$）？答案是否定的。我们这里不假证明的介绍Brouwer不动点定理的一种简单形式

定理 4.7.1 (Brouwer Fixed Point Theorem). 在 $\mathbb{R}^n$ 中，用 B^n 代表 $\{x \in \mathbb{R}^n \colon d(x,0) \leq 1\}$（换言之，$B^n$ 是闭单位球）。则任意从 B^n 到自身的连续映射一定存在不动点。

根据Brouwer不动点定理，n 维单位球 B^n 到自身的连续映射是一定存在不动点的。

注 4.7.5. 对于所有 $n \in \mathbb{N}_{\geq 1}$ ， n 维单位球面 S^n 到自身的不存在不动点的连续映射是始终存在的。比如，考虑对径映射（antipodal map）。其中 $S^n \subset \mathbb{R}^{n+1}$ 为 $\{(x_1, \cdots, x_{n+1}) \in \mathbb{R}^{n+1} \colon \sum_{i=1}^{n+1} x_i^2 = 1\}$ 。

习题：

习题 4.7.1. 验证如下关于刚体变换的事实：

1) [封闭性] 假设 f 和 g 都是 $\mathbb{R}^n$ 到自身的保距映射，则 $f \circ g$ 也是保距映射。

2) [结合律] 假定 f, g 和 h 都是 $\mathbb{R}^n$ 到自身的保距映射，则 $(f \circ g) \circ h$ 和 $f \circ (g \circ h)$ 都是$\mathbb{R}^n$ 到自身的保距映射，并且 $(f \circ g) \circ h = f \circ (g \circ h)$ 。

3) [恒等元] 假定 f 是 $\mathbb{R}^n$ 到自身的保距映射，则 $f \circ \mathrm{Id}_{\mathbb{R}^n}$ 和 $\mathrm{Id}_{\mathbb{R}^n} \circ f$ 都是$\mathbb{R}^n$ 到自身的保距映射，并且 $f \circ \mathrm{Id}_{\mathbb{R}^n} = \mathrm{Id}_{\mathbb{R}^n} \circ f$ ， 其中 $\mathrm{Id}_{\mathbb{R}^n}$ 为 $\mathbb{R}^n$ 上的恒等映射。

4) [逆元] 假定 f 是 $\mathbb{R}^n$ 到自身的保距映射，则 f^{-1} 也是保距的。

习题 4.7.2. 根据上面的验证，我们知道 $\mathbb{R}^n$ 中所有的刚体变换构成一个群，记为 $\mathbb{E}_n$ 。 对于所有 $n \in \mathbb{N}_{\geq 1}$ ， 证明 $\mathbb{E}_n$ 不是交换群。

习题 4.7.3. 证明一维情形下的Brouwer不动点定理。

4.8 群作用G-等价、G-小于等于，Banach-Schröder-Bernstein 定理

作为Banach-Tarski悖论构造所需的技术准备，对于群 G 在 X 上的作用，我们给出 G-等价 和 G-小于等于 之定义。

定义 4.8.1. 群 G 作用在 X 上。X 的两个子集 A 和 B 被称为是 G-等价 的，如果存在 A 的剖分 $A = \bigsqcup_{i=1}^m A_i$ 和 B 的剖分 $B = \bigsqcup_{i=1}^m B_i$ ，以及 G 中元素 $g_1, \cdots, g_m$ ， 满足 $g_i(A_i) = B_i$ ， $\forall 1 \leq i \leq m$ 。 我们说 A 是 G-小于等于 B 的，如果 A 可以 G-等价到 B 的一个子集。

一个自然的问题就是，G-小于等于是否满足反对称性（若满足，结合上面练习的结果，则 G-小于等于 就是个偏序关系）？换言之，如果 A “G-小于等于” B 并且 B “G-小于等于” A ， 是否有 A “G-等价于” B ？ 答案是肯定的。这就是下面的Banach-Schröder-Bernstein定理。该定理证明和 Cantor-Bernstein 定理之证明比较类似，区别在于需要考虑群作用这个额外的结构。

定理 4.8.1 (Banach-Schröder-Bernstein Theorem). 群 G 作用在集合 X 上。A 和 B 是 X 的子集。若 A G-小于等于 B 且 B G-小于等于 A ， 则 A G-等价于 B 。

证明： 为了简化书写，我们用 $\lesssim_G$ 来代表 G-小于等于，用 $\sim_G$ 来代表 G-等价于。

由于 $A \lesssim B$ ， 存在 $B' \subset B$ ， 使得 $A \sim_G B'$ 。 同理，存在 $A' \subset A$ ， 使得 $B \sim_G A'$ 。

由于 $A \sim_G B'$ ，存在关于 A 的剖分 $A = \bigsqcup_{i=1}^m A_i$ ， 以及 $f_1, \cdots, f_m \in G$ ， 使得 $B' = \bigsqcup_{i=1}^m g_i(A_i)$ 。

定义

$$f \colon A \longrightarrow B', \ a \mapsto g_i(a) \ a \in A_i \ 。$$

则 f 一定是双射（为什么？）。

类似于 f ， 我们可以得到 B 到 A' 的双射 g ， 这里 g （和 f 类似）也是通过有限个群元素的作用“拼起来”的。

定义 $C_0 = A - A' = A - g(B)$ ， 并且归纳定义 $C_n = g(f(C_{n-1}))$ ， $\forall n \in \mathbb{N}_{\geq 1}$ 。 令

$$C = \bigcup_{n=0}^{\infty} C_n \text{ 。}$$

断言： $A - C \subset A'$ 且 $g^{-1}(A - C) = B - f(C)$ 。

断言之证明：练习，标准的集合论之验证。

根据上述断言，以及 g 的选取（通过有限个群元素的作用“拼起来”），我们可以得到

$$A - C \sim_G B - f(C) \text{ 。}$$

根据 f 的定义（通过有限个群元素的作用“拼起来”），我们有

$$C \sim_G f(C) \text{ 。}$$

断言：群 G 作用在集合 X 上，对于 X 中的无交子集 X_1, X_2 ， 以及 Y 中的无交子集 Y_1, Y_2 ， 如果 $X_1 \sim_G Y_1$ 且 $X_2 \sim_G Y_2$ ， 则 $(X_1 \bigsqcup X_2) \sim_G (Y_1 \bigsqcup Y_2)$ 。

断言之证明：这是比较简单的验证，留作练习。

注意到 $A = (A - C) \bigsqcup C$ ， $B = (B - f(C)) \bigsqcup f(C)$ ， 以及上面的 $A - C \sim_G B - f(C)$ 和 $C \sim_G f(C)$ ， 根据上述断言，我们有

$$A \sim_G B \text{ 。}$$

证毕。 ∎

习题：

习题 4.8.1. 证明上面定义的 G-等价的确是等价关系。换言之，G-等价满足自反性，对称性和传递性。

习题 4.8.2. 证明上面定义的 G-小于等于 满足自反性和传递性。

4.9 群的顺从性

顺从性概念（amenability）的起源和Banach-Tarski悖论/定理有关。在Banach-Tarski悖论/定理中出现的剖分，其给出的每一小块都是不可以有类似“这一小块占了整个单位球的多大比例”的描述的，事实上，其反面形式（存在这样的描述）就是是早期关于顺从性的一种定义。

我们会介绍群的顺从性，以及相关的基本性质和典型例子（比如 $\mathbb{Z}$ ）。

群的顺从性有很多种等价定义方式，我们这里采用的是“存在有限可加不变概率测度”的定义。这个定义需要关于测度的概念。关于测度（以及拓扑空间）这部分知识，我们在附录中简单的给出，可供参考。我们这里（包括Banach-Tarski悖论的构造中）涉及到的主要是离散群，简单起见，我们给出离散群的顺从性之概念。

定义 4.9.1. 对于离散群（具有离散拓扑结构的群） G ， 我们说 G 是顺从（amenable）的，如果存在映射 $\mu\colon \mathcal{P}(G) \longrightarrow [0,1]$ ， 满足

i） $\mu(G) = 1$

ii） $\mu(gD) = \mu(D)$ ， $\forall g \in G, D \subset G$

iii）对于任意 G 的子集 D 和 E ， 若 $D \cap E = \emptyset$ ， 则 $\mu(D \sqcup E) = \mu(D) + \mu(E)$

注 4.9.1. i） 说明 μ 是概率测度，ii） 说明 μ 是左乘不变的，iii） 说明 （根据数学归纳法）μ 是有限可加的。

在上述关于群 G 之顺从性之定义中的 μ 和一般的测度是有很大区别的，比如：

1. 一般的测度是可数可加的，而群之顺从性定义中的 μ 是有限可加的。

2. 对于 X 上的满足某些平移不变性质的一般测度 ν ， $\nu(X)$ 未必是有限的。而群之顺从性定义中的 μ 是概率测度，即满足 $\mu(G) = 1$ 。

下面我们通过具体的例子 $G = \mathbb{Z}$ 来考虑上述的区别。

令 ν 为 $\mathbb{Z}$ 上的在 “$+n$” 变换下保持不变的,一般意义下的测度。如果 $\nu(\{0\}) = 0$ ， 则根据可数可加性不难得到：$\nu(D) = 0$ ， $\forall D \subset \mathbb{Z}$ 。 如果 $\nu(\{0\}) \neq 0$ ，通过乘上一个正的数，不妨假定 $\nu\{0\} = 1$ 。 根据可数可加性，不难得到（为什么？）$\nu(D) = \#(D)$ ， 其中 D 为任意的 $\mathbb{Z}$ 中子集，并且 $\#(D)$ 代表 D 中元素的数目。这个测度 ν 也被称为记数测度（counting measure）。

总结说来，在可数可加 以及 “$+n$” 不变的要求下，得到的 ν 为零测度，或者是记数测度。无论是哪种情形，都不可能有 $\nu(\mathbb{Z}) = 1$ 。

如果我们保持 “$+n$” 不变 这个要求，将 可数可加 减弱为 有限可加，已知的事实（ $\mathbb{Z}$ 是顺从群 ）告诉我们，这样的测度 μ 是的确存在的。事实上，我们有如下的性质。

命题 4.9.1. 对于上述的 μ ， 部分性质如下：

a) $\mu(\emptyset)=0$ ， $\mu(\mathbb{Z})=1$

b) $\mu(\text{偶整数全体})=1/2$ ， $\mu(\text{奇整数全体})=1/2$

c) 对于任意 $\mathbb{Z}$ 中有限子集 D ， $\mu(D)=0$

d) $\mu(\text{平方数全体})=0$

e) $\mu(\text{立方数全体})=0$

这些性质都可以从 μ 之定义中得到。作为练习，试证明性质 d) 。

注 4.9.2. 若离散群 G 上存在左乘不变的有限可加概率测度，则一定也存在右乘不变的有限可加概率测度。换言之，对于上面的定义，若ii)中的左乘（gD）换成右乘（Dg），得到的还是同一个定义。为什么？

例 4.9.1. 有限群都是顺从的。验证不难，留作练习。

例 4.9.2. 群 $(\mathbb{Z},+)$ 是顺从群。若直接根据定义验证，并不很容易。

例 4.9.3. 若 $n\geq 2$ ， $\mathbb{F}_n$ 都是非顺从（non-amenable）群。

例 4.9.4. 若 $n\geq 3$ ， $\mathbb{E}_n$ 都是非顺从（non-amenable）群。

为了说明群的相悖性和群的顺从性这两个概念之间的关系，我们这里暂时不假证明的介绍Tarski定理。

定理 4.9.1 (Tarski's Theorem). 假定群 G 作用在集合 X 上，则该作用是不相悖的，当且仅当存在 X 上的 G 作用不变且有限可加的概率测度。

注 4.9.3. 关于Tarski's定理，不难发现的是，有个方向的证明是平凡（trivial）的。

推论 4.9.1. 群 G 是相悖的，当且仅当 G 是非顺从的。

在非顺从群里面，鉴于 $\mathbb{F}_2$ 的相对简单结构以及早期找到的非顺从群之例子，J. von Neumann提出如下猜想：

猜想 [von Neumann Conjecture]：任何非顺从群一定包含 $\mathbb{F}_2$ 作为子群。

对于一般的群，von Neumann猜想是错误的。第一个反例（Tarski Monster Group）于1980年被给出。

前面例子中提到过，$n\geq 3$ 时，$\mathbb{E}_n$ 是非顺从的。这个事实，可以沿着如下思路证明。根据Tarski定理，我们只需要证明 $\mathbb{E}_n$ 是相悖的（$n\geq 3$）。事实上，由于 $\mathbb{F}_2$ 是相悖的，我们只需要证明 $\mathbb{E}_3$ 包含 $\mathbb{F}_2$ 作为子群即可（为什么？）。

我们试图在 $\mathbb{E}_3$ 中选择两个刚体变换 a 和 b ， 使得这两个刚体变换是“独立”的。换言之，若我们从集合 $\{e, a^{\pm 1}, b^{\pm 1}\}$ 中有放回的选取任意有限多个做乘法，所有可能的消去/化简情形如下（其中 e 为 $\mathbb{E}_3$ 中单位元）【 类似 $aa = a^2$ 的情形算简记，不是化简】：

$$e = a \cdot a^{-1}, \quad e = b \cdot b^{-1} \text{。}$$

这里我们给出一个相对初等的论述。构造 3×3 的实矩阵 A, B ， 并考虑它们对于的 $\mathbb{R}^3$ 到 $\mathbb{R}^3$ 的映射（规则就是矩阵的乘法）。比如：

$$A \colon \mathbb{R}^3 \longrightarrow \mathbb{R}^3, \quad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \longmapsto A \cdot x = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{。}$$

当然了，一般的说，这样定义的映射（实际上是线性映射）未必是刚体变换（保距变换）。

令 $\theta = \arccos 3/5$ ， 并令

$$A = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \text{。}$$

断言：上述 A 和 B 所对于的 $\mathbb{R}^3$ 到自身的映射的确都是刚体变换。

断言之证明：直接暴力验算即可。

用 a, b 分别代表 A 和 B 对应的刚体变换。为了说明它们生成 $\mathbb{F}_2$ ， 只需要说明 a 和 b 是“独立”的。事实上，我们有如下的命题。

命题 4.9.2. 对于上述的 A 和 B ， 对于任意化简后的 $S = T_1 \cdots T_k$ ， 其中 $T_j \in \{A, B, A^{-1}, B^{-1}\}$ $\forall 1 \leq j \leq k$ ， 我们有 $S \neq 1_{M_3(\mathbb{R})}$ 。

该命题的证明是比较初等的。QQQ 在练习？？中，已经给出了该性质的部分证明。其剩余部分，不难类似得到。

至此，我们得到了 $\mathbb{F}_2$ 的相悖性，从而得到了 $\mathbb{E}_3$ 的相悖性。根据 Tarski 定理，我们就得到了 $\mathbb{E}_3$ 的非顺从性。对于 $n > 3$ ， 由于 $\mathbb{E}_3$ 可以看做 $\mathbb{E}_n$ 的子群，我们可以从 $\mathbb{E}_3$ 的非顺从性得到任意 $\mathbb{E}_n$ 的非顺从性 （ $n \geq 3$ ）。换言之，我们有如下定理。

定理 4.9.2. 对于任意 $n \in \mathbb{N}_{\geq 3}$ ， $\mathbb{E}_n$ 都是非顺从的。

如果 $n = 1, 2$ ， $\mathbb{E}_n$ 的顺从性也是已知的。

定理 4.9.3. 对于任意 $n = 1, 2$ ， $\mathbb{E}_n$ 都是顺从的。

该定理证明如下。QQQ

习题：

习题 4.9.1. 证明**命题4.9.1**中的d）。提示：当 $n \to \infty$ 时，n^2 和 $(n+1)^2$ 中间的距离也是趋于无穷的。

DRAFT [March 4, 2015]

第 5 章

Banach-Tarski悖论

5.1 Banach-Tarski悖论简介

首先，我们回顾下Banach-Tarski悖论。需要说明的是，在承认选择公理的前提下，Banach-Tarski悖论在数学上是完全成立的，是个正确的定理。所谓的“悖论”，只是与大家通常的直观相悖。

定理 5.1.1 (Banach-Tarski悖论). 令 B 为 $\mathbb{R}^3$ 中的单位球，则可以将 B 分成有限个互不相交的子集 $A_1, \cdots, A_m, B_1, \cdots, B_n$ ，以及存在刚体变换 $f_1, \cdots, f_m, g_1, \cdots, g_n$，使得

$$B = \bigsqcup_{i=1}^{m} f_i(A_i) = \bigsqcup_{j=1}^{n} g_j(B_j) \ 。$$

注 5.1.1. 关于Banach-Tarski悖论，通俗点的描述是：三维空间中的球，可以通过拆分成**有限多块**、然后再**刚性重组**的方式，变成两个 尺寸和原来一样 的球。

注 5.1.2. Banach-Tarski悖论中，关键点之一就是拆分成 有限多块。如果没有有限拆分的条件，可以将球拆分到单个点，然后利用一个球的基数等于两个互不相交的球的基数，很容易得到相关的构造。但是这样的话，其 本质就完全是个集合基数比较的问题了。

注 5.1.3. Banach-Tarski悖论中，另外一个关键点就是维数（必须大于等于 3 ）。后面我们会简略的证明：如果是一维或者二维空间中的单位球，类似“悖论”是不存在的。

注 5.1.4. Banach-Tarski悖论与形状（球形）关系不大（ 在维数大于等于 3 的前提下）。如果换成椭球形、方块、矩形块、甜甜圈形等等，也有类似的现象。

注 5.1.5. Banach-Tarski悖论/定理，并不是个完全基于集合基数概念的现象。基数本身，是无法区分维数的。比如，Peano曲线是一个从 $[0,1]$ 到 $[0,1]\times[0,1]$ 的连续的满射（ 不可能是单射）。由Cantor-Bernstein定理，不难得到 $[0,1]$ 和 $[0,1]^2$ 的基数一样。

注 5.1.6. Banach-Tarski悖论中，不可能拆分出的每块都是“有体积”的。否则很容易得出类似“ $1=1+1$ ”的矛盾。这点前面课上已经详细讲过（找错题）。

注 5.1.7. 数学上讲，Banach-Tarski悖论的两大基石分别是选择公理和群的相关概念以及性质。其中涉及到群的部分包括群在空间上的作用、子群、轨道/陪集、群的“悖论性”（或者等价的，群的非顺从性）等等。我们这里给出下一章“Banach-Tarski悖论”中所需要的和群相关的一些基础知识。

注 5.1.8. $\mathbb{R}^3$ 中所有刚体变换构成一个群，不妨记为 $\mathbb{E}_3$ 。 该群中的元素，作用在球的子集上，就是对该子集做所谓的“刚体变换”。

注 5.1.9. 用 $\mathbb{E}_n$ 来表示 $\mathbb{R}^n$ 中所有刚体变换构成的群。后面会介绍如下事实：当 $n\geq 3$ 时，$\mathbb{E}_n$ 是非顺从的。当 $n=1,2$ 时，$\mathbb{E}_n$ 是顺从的。

5.2 经典的Banach-Tarski悖论

我们来构造/证明经典的Banach-Tarski悖论。基于该构造/证明，以及前面的相关概念和结果，我们可以得到：在更高维（$n\geq 3$)的情形下，对于 $\mathbb{R}^n$ 中更广义的子集 X（未必需要是单位球），Banach-Tarski悖论也是存在的。另一个重要的现象是，在低维情形下（比如一维或者二维空间中），类似的Banach-Tarski悖论是不存在的。

我们先介绍下相关历史： 1914年，Hausdorff首先证明了在 S^2-K 关于刚体变换是相悖的（Hausdorff悖论），其中 S^2 为 $\mathbb{R}^3$ 中的单位球面，K 是 S^2 上的一个可数子集。到了 1924年，Banach和Tarski证明了 S^2 关于刚体变换是相悖的，并且基于此证明了 R^3 中的单位球 D^3 关于刚体变换是相悖的。这就是经典的 Banach-Tarski 悖论。不仅如此，Banach还得到了更广义的 Banach-Tarski 悖论：$\mathbb{R}^3$ 中的任何两个有界并且包含实心球的子集 A 和 B ， 一定都是 $\mathbb{E}_3$-等价的，其中 $\mathbb{E}_3$ 为 $\mathbb{R}^3$ 中的刚体变换群。

定理 5.2.1 (Hausdorff’ s Paradox). 令 S^2 为 $\mathbb{R}^3$ 中单位球面，则存在 S^2 的一个可数子集 K ， 使得 S^2-K 是 $\mathbb{E}_3$ 相悖的，其中 $\mathbb{E}_3$ 为 $\mathbb{R}^3$ 上的刚体变换群。

证明： 令 $\theta=\arccos 3/5$，并取

$$A=\begin{pmatrix}\cos\theta & -\sin\theta & 0\\ \sin\theta & -\cos\theta & 0\\ 0 & 0 & 1\end{pmatrix},\quad B=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{pmatrix}\quad 。$$

则 $A,B\in\mathbb{E}_3$ ， 并且容易验证 A,B 都是 S^2 到 S^2 的变换（这是因为 A,B 都是刚体变换且都将原点映到原点）

根据前面的结论，A, B 所生成的群 $G(A,B)$ 就是（严格的讲，应该是同构于）自由群 $\mathbb{F}_2$ 。令

$$K = \{x \in S^2 : \text{ 存在 } g \in G(A,B) - e_{G(A,B)}, \text{ 使得 } g(x) = x\} \text{ 。}$$

则 $G(A,B)$ 在 $S^2 - K$ 上的作用一定是自由的。根据上一章中的内容，$G(A,B)$ 是相悖的（因为 $\mathbb{F}_2$ 是相悖的）。继续根据上一章中的定理，如果一个相悖群自由的作用在集合上，则该作用一定也是相悖的，我们就可以得到 $S^2 - K$ 是 $\mathbb{E}_3$-相悖的。

我们现在只需要证明 K 是可数的。根据上一章中的习题，$\mathbb{F}_2$ 是个可数集。故我们只需证明，对于任何 $g \in G(A,B) - e_{G(A,B)}$ ， g 最多有可数多不动点即可（为什么？）。

事实上，我们可以得到：

断言：对于任意 $H \in G(A,B) - e_{G(A,B)}$ ， g 在 S^2 的作用有正好两个不动点。

断言之证明：将 A 和 B 看成 3×3 实矩阵，容易验证 A 和 B 满足

$$AA^* = 1, \ BB^* = 1 \text{ ，}$$

这里 * 定义为 $(T^*)_{ij} = \overline{T_{ji}}$ 。 故 A 和 B 都是酉矩阵（我们说方阵 E 是个酉矩阵，如果 $EE^* = 1$）。对于任意给定的 $H \in G(A,B) - e_{G(A,B)}$ ， 我们可以将其也看成 3×3 矩阵。由于A 和 B 都是酉矩阵，故 H 也是酉矩阵。

如果 $x \in S^2$ 是 H 作用下的不动点，则 $H(x) = x$ 。 将 x 写成 $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ 。 用矩阵乘法的语言来表达 $H(x) = x$ ， 也就是

$$H \cdot x = x = 1_{\mathbb{C}} \cdot x \text{ 。}$$

这样就转化为一个求解矩阵 H 对应着特征值 1 的特征向量（特征子空间）的问题。对于上述矩阵 H ， 求解关于 λ 的特征方程

$$\det\left(H - \lambda \cdot 1_{M_3(\mathbb{R})}\right) = 0 \text{ ，}$$

就可以得到 H 的特征值。

假定 $\lambda_1, \lambda_2, \lambda_3$ 是这个三次方程的复根（重根计算重数）。我们不妨假定 $\lambda_1 \in \mathbb{R}$ 并且 $\lambda_2 = \overline{\lambda_3}$（为什么？）。

由于 H 是酉矩阵，其特征值 $\lambda_1, \lambda_2, \lambda_3$ [eigenvalues] 都是位于复平面中单位圆上的复数（换言之，一定可以写成 $e^{i\theta}$ 的形式，其中 $\theta \in \mathbb{R}$）。由于 $\lambda_1 \in \mathbb{R}$ ， 故 $\lambda_1 = 1$ 或者 $\lambda_1 = -1$ 。

注意到 H 由 $A^{\pm 1}$ 和 $B^{\pm 1}$ 通过有限步乘法运算得到，并且

$$\det(A) = \det(A^{-1}) = \det(B) = \det(B^{-1}) = 1 \text{ ，}$$

故而 $\det(H) = 1$ 。 注意到 $\det(H) = \lambda_1\lambda_2\lambda_3$ ，因此 $\lambda_1 = 1$ （为什么？）。

下面我们来说明 λ_2 和 λ_3 都不可能为 1 。 事实上，如果 λ_2 和 λ_3 中有一个为 1 ， 由于 λ_2 和 λ_3 互为复共轭，一定有

$$\lambda_2 = \lambda_3 = 1 \text{ 。}$$

这样 H 的三个特征值（计算重数）都是 1 。 由于 H 是酉矩阵，因此在相似变换下是可以被对角化成 $\begin{pmatrix}\lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3\end{pmatrix}$ 的。换言之，存在可逆矩阵 P ， 使得

$$H = P\begin{pmatrix}\lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3\end{pmatrix}P^{-1} \text{ 。}$$

由于 $\lambda_1 = \lambda_2 = \lambda_3 = 1$ ， 故

$$H = PP^{-1} = 1_{M_3(\mathbb{R})} \text{ ，}$$

这与 H 不是乘法恒等元矛盾。

由于 $\lambda_1 = 1$ 且 λ_2, λ_3 均不为 1 ， 故特征值 1 所对应的特征向量构成的空间一定是一维的。换言之，所有满足 $H \cdot x = 1 \cdot x$ 的 x 所构成的集合一定是某条通过原点的直线。注意到我们的作用是在 S^2 上，而任意通过原点的直线和 S^2 一定有正好两个交点，故而对于任意的 $H \in G(A,B) - e_{G(A,B)}$ ， $H \cdot x = x$ 在 S^2 上有两个解。换言之，H 作用在 S^2 上有两个不动点。

下面我们回到 Hausdorff 悖论的证明。

由于每个 $H \in G(A,B) - e_{G(A,B)}$ 有两个不动点并且 $G(A,B)$ 是可数的，我们可以得到 K 是可数的，至此我们完成了 Hausdorff 悖论之证明。 ∎

Banach和Tarski基于上述 Hausdorff 悖论做了改进，十年后得到如下结果（并基于该结果，得到了经典意义下的 Banach-Tarski 定理/悖论）：

定理 5.2.2. $\mathbb{R}^3$ 中的单位球面 S^2 是 $\mathbb{E}_3$ 相悖的。

这里的关键是证明 $S^2 \sim_{\mathbb{E}_3} (S^2 - K)$ ， 其中 K 是可数集 。这里采用的证明方法和作业二之 1. g) 所用之方法是类似的，当然，这里要考虑额外的结构：群 $\mathbb{E}_3$ 在 S^2 上的作用。具体证明如下。

证明： 我们的证明基于如下断言：

断言1： 群 G 作用在 X 上，如果存在子集 A_1, A_2 和 B_1, B_2 ， 满足 $A_1 \bigcap A_2 = \emptyset$ ， $B_1 \bigcap B_2 = \emptyset$ ， 并且 $A_1 \sim_G B_1$ ， $A_2 \sim_G B_2$ ， 则 $A_1 \bigsqcup A_1 \sim_G B_1 \bigsqcup B_2$ 。

断言1之证明： 并不困难，留作练习。

由于 K 是可数集，一定存在通过原点的直线 L ， 使得 $L \bigcap K = \emptyset$ （为什么？）。我们用 R_θ 代表以 L 为轴（不妨设定 L 的一个正方向），按照右手系旋转 θ 角度的变换。容易验证 R_θ 一定是个刚体变换，并且将 S^2 映到 S^2 。 换言之，$\mathrm{R}_\theta \in \mathbb{E}_3$ 并且 $\mathrm{R}_\theta(S^2) = S^2$ 。

断言2： 任意给定 $\mathbb{R}$ 中的可数子集 $x_1, x_2, \cdots$ ， 一定存在 $\theta \in [0, 2\pi)$ ， 使得 $\theta \notin \{(x_i - x_j)/n \colon i, j, n \in \mathbb{N}_{\geq 1}\}$ 。

断言2之证明：由于 $[0,2\pi)$ 是不可数集，因此只需证明 $\{(x_i-x_j)/n\colon i,j,n\in\mathbb{N}_{\geq 1}\}$ 是可数集即可。具体细节是标准的集合论之训练，这里留作练习。

由于 K 是可数集，基于上述的断言，一定存在某个（事实上，存在不可数无穷多个） $\theta\in[0,2\pi)$ ， 使得对于任何 $y\in K$ 和 $n\in\mathbb{N}_{\geq 1}$ ， 都有 $\mathrm{R}_\theta^n(y)\notin K$ ， 这里 R_θ^n 代表 R_θ 作用 n 次。换言之，我们有

$$K\bigcap \mathrm{R}_\theta^n(K)=\emptyset,\ \forall n\in\mathbb{N}_{\geq 1}\ 。$$

基于此，对于任意的 $m,n\in\mathbb{N}_{\geq 0}$ 且 $m\neq n$ ， 我们一定有

$$\mathrm{R}_\theta^m(K)\bigcap \mathrm{R}_\theta^n(K)=\emptyset\ 。$$

否则，不妨假定 $0\leq m<n$ ， 且 $\mathrm{R}_\theta^m(K)\bigcap \mathrm{R}_\theta^n(K)\neq\emptyset$ 。 由于 R_θ 是刚体变换，因此是双射，故为单射。由此 R_θ^m 也是单射，从而 （根据集合论中的知识）

$$\mathrm{R}_\theta^m\left(K\bigcap \mathrm{R}_\theta^{n-m}\right)=\mathrm{R}_\theta^m(K)\bigcap \mathrm{R}_\theta^n(K)\neq\emptyset\ 。$$

故

$$K\bigcap \mathrm{R}_\theta^{n-m}\neq\emptyset\ ,$$

而这与 θ 之选取方式矛盾。

至此，我们证明了 $K,\mathrm{R}_\theta(K),\mathrm{R}_\theta^2(K),\cdots$ 都是两两不交的。下面我们利用第一个断言来证明 $S^2\sim_{\mathbb{E}_3} S^2-K$ 。

令

$$T=S-\bigsqcup_{j=0}^{\infty}\mathrm{R}_\theta^j(K)\ 。$$

则

$$S=T\bigsqcup\left(\bigsqcup_{j=0}^{\infty}\mathrm{R}_\theta^j(K)\right)\ \text{且}\ S-K=T\bigsqcup\left(\bigsqcup_{j=1}^{\infty}\mathrm{R}_\theta^j(K)\right)\ 。$$

由于 $\mathrm{R}_\theta\left(\bigsqcup_{j=0}^{\infty}\mathrm{R}_\theta^j(K)\right)=\bigsqcup_{j=1}^{\infty}\mathrm{R}_\theta^j(K)$ ， 我们有

$$\bigsqcup_{j=0}^{\infty}\mathrm{R}_\theta^j(K)\ \sim_{\mathbb{E}_3}\ \bigsqcup_{j=1}^{\infty}\mathrm{R}_\theta^j(K)\ 。$$

根据本证明中的第一个断言， 可以得到

$$S\ \sim_{\mathbb{E}_3}\ S-K\ ,$$

证毕。 ∎

基于上述定理，可以很容易得到如下关于 Hausdorff 悖论的推广（为什么？）。

定理 5.2.3. S^2 是 $\mathbb{E}_3$ 相悖的。

基于 S^2 上的相悖性，对于任意 $\lambda \in (0,1]$ ， 我们可以得到 λS^2 上的相悖性，从而得到 $D^3-\{0\}$ 上之相悖性，其中 D^3 为 $\mathbb{R}^3$ 中的单位球，$\{0\}$ 是原点。我们可以证明 $D^3 \sim D^3-\{0\}$ ，从而就得到了下面的经典 Banach-Tarski 定理。

定理 5.2.4 (Banach-Tarski 定理/悖论). $\mathbb{R}^3$ 中的单位球 D^3 是 $\mathbb{E}_3$ 相悖的。

证明： 证明的框架上面已经说的很清楚。关键是用到如下两个事实：

事实一： $D^3-\{0\} = \bigsqcup_{\lambda\in(0,1]} \lambda S^2$ 。

事实二： $D^3 \sim_{\mathbb{E}_3} D^3-\{0\}$ 。

事实一的证明是基本的验证，事实二的证明是前面定理中 “$S^2 \sim_{\mathbb{E}_3} S^2-K$” 之证明的类似（但更简单）。

为了证明事实二，我们试图找到一个刚体变换 $\rho \in \mathbb{E}_3$ ， 使得

$$\rho^m(0) \neq \rho^n(0) \ \forall m,n \in \mathbb{N}_{\geq 0},\ m \neq n \ 。$$

如果这个可以做到，那么由于

$$\rho\left(\bigsqcup_{k=0}^{\infty}\{\rho^k(0)\}\right) = \bigsqcup_{k=1}^{\infty}\{\rho^k(0)\}$$

且

$$D^3 = \left(D^3 - \bigsqcup_{k=0}^{\infty}\{\rho^k(0)\}\right) \bigsqcup \left(\bigsqcup_{k=0}^{\infty}\{\rho^k(0)\}\right) \ ,$$

$$D^3-\{0\} = \left(D^3 - \bigsqcup_{k=0}^{\infty}\{\rho^k(0)\}\right) \bigsqcup \left(\bigsqcup_{k=1}^{\infty}\{\rho^k(0)\}\right) \ ,$$

我们就可以得到 $D^3 \sim_{\mathbb{E}_3} D^3-\{0\}$ 。

现在的问题就是，如何找到刚体变换 $\rho \in \mathbb{E}_3$ ， 使得对于任意 $n \in \mathbb{N}$ ， $\rho^n(0) \in D^3$ ， 并且对于任意的互不相等的 $m,n \in \mathbb{N}$ ， $\rho^m(0) \neq \rho^n(0)$ ？我们这里不要求 ρ 将 D^3 映到 D^3 。事实上，这也是不可能的（为什么？这是不错的练习）。

关于 ρ 的构造，一个提示就是：圆圈上的无理旋转变换，就是让圆圈逆时针旋转角度 $\alpha\pi$ ，其中 α 是无理数。以前的课件中讲过，这样的变换（以及其关于自身的任意次复合构成的变换），一定是没有不动点的（为什么？）。

基于上述的提示，作为练习，请自行完成经典 Banach-Tarski 悖论/定理的证明。 ∎

注 5.2.1. 几乎完全平行于经典 Banach-Tarski 悖论/定理的证明，不难得到：对于任意 $n \geq 3$ ， $\mathbb{R}^n$ 中的单位球 D^n 是 $\mathbb{E}_n$ 相悖的。

注 5.2.2. 上一章开始部分提到过，Banach-Tarski 悖论中，“球形” 并不是个必须的条件。事实上，我们只需要 “有界” 并且 “包含实心球（即包含邻域）” 即可。

习题：

习题 5.2.1. 证明酉矩阵关于乘法运算和逆运算是封闭的。

5.3 更一般的Banach-Tarski悖论

我们前面说过，在 $\mathbb{R}^n$ （$n \geq 3$）上，Banach-Tarski 悖论/定理并不一定要求是对于实心球的。事实上，对于任意 $n \geq 3$ 中的子集 X ， 只要 X 包含某个实心球（大小大于 0 ）并且 X 是有界的，均有类似的 Banach-Tarski 悖论/定理。

定理 5.3.1 (Banach-Tarski Paradox/Theorem, the Strong Version). 假定 A 和 B 是 $\mathbb{R}^3$ 中的两个有界子集，A 中包含（实心）球 M 且 B 中包含（实心）球 N 。则 A 一定 $\mathbb{E}_3$-等价于 B ， 其中 $\mathbb{E}_3$ 为 $\mathbb{R}^3$ 上的刚体变换群。换言之，一定存在 A 的有限剖分

$$A = \bigsqcup_{i=1}^{k} A_i$$

和 $g_1, \cdots, g_k \in \mathbb{E}_3$ ， 使得

$$B = \bigsqcup_{i=1}^{k} g_i(A_i) \text{ 。}$$

证明： 本证明主要基于经典的 Banach-Tarski 定理、 Banach-Schröder-Bernstein 定理、以及如下事实：$\mathbb{R}^n$ 中的任意有界集一定可以被有限个实心球的并（这里不要求也不可能要求是无交并）覆盖。

为了简化书写，我们还是以 $\lesssim_{\mathbb{E}_3}$ 来代表 $\mathbb{E}_3$-小于等于，并以 $\sim_{\mathbb{E}_3}$ 来代表 $\mathbb{E}_3$-等价。

由于 A 是有界集，一定存在有限个实心球 $N_1, \cdots, N_p$ ， 使得每个的半径和 N 的半径一致且

$$A \subset \bigcup_{i=1}^{p} N_i \ 。$$

根据Banach-Tarski 定理以及QQQ 练习 QQQ 中的结论，可得

$$B \supset N \gtrsim_{\mathbb{E}_3} \bigcup_{i=1}^{p} N_i \supset A \ ,$$

因此

$$A \lesssim_{\mathbb{E}_3} B \ 。$$

类似的，我们有

$$B \lesssim_{\mathbb{E}_3} A \ 。$$

根据**定理4.8.1**（Banach-Schröder-Bernstein 定理），

$$A \sim_{\mathbb{E}_3} B \ ,$$

证毕。 ∎

5.4 维数为 1 和 2 时类似悖论的不存在性

正如前面提到的，在 $n = 1, 2$ 时，$\mathbb{R}^n$ 上是没有 Banach-Tarski 悖论这种现象的。这里我们比较详细的给出相关的论述。

为了说明低维情形下 Banach-Tarski 悖论不成立，我们先证明：如果顺从群 G 作用在集合 X 上，则该作用一定不是相悖的。

定理 5.4.1. 如果 G 是顺从的，并且 G 作用在 X 上，则该作用一定不是 G-相悖的。

证明： 为了说明该作用不是 G-相悖的，我们只需要说明存在 X 上的 G-不变的有限可加的概率测度 μ 即可。若这样的 μ 存在，则该作用不可能是 G-相悖的，否则就会出现类似 $1 = 1 + 1$ 的矛盾（为什么？）

因为 G 本身是顺从的，因此存在 G 上的 G-不变的有限可加的概率测度

$$\nu \colon \mathcal{P}(G) \longrightarrow [0, 1], \ H \mapsto \nu(H) \ 。$$

下面我们根据 ν 来定义 μ 。 取定 $x \in X$ 。 对于任意 $D \in \mathcal{P}(X)$ （换言之，$D \subset X$），定义

$$\mu(D) = \mu(\{g \in G \colon g(x) \in D\}) \text{ 。}$$

根据定义，并且根据 ν 的性质，不难验证如下断言：

断言1： $\mu(\emptyset) = 0$ ， $\mu(X) = 1$ 。

断言2： $\forall\ g \in G, D \subset X$ ， $\mu(g(D)) = \mu(D)$ 。

断言3： μ 是有限可加的。

根据这三个断言，可以直接得出定理结论。这三个断言之证明比较简单，作为练习。 ∎

根据上述定理的结论以及证明中所构造的 μ，注意到前面提到的事实（$\mathbb{E}_1$ 和 $\mathbb{E}_2$ 都是顺从群），我们可以立即得到如下定理。

定理 5.4.2. 对于 $n = 1, 2$ ， 刚体变换群 $\mathbb{E}_n$ （或者其任意子群）在 $\mathbb{R}^n$ 上的作用不可能是相悖的。

该定理证明作为练习。

目前为止，我们尚未说明在$\mathbb{R}^1$ 或者 $\mathbb{R}^2$中，不可能将半径为一的实心球通过有限拆分加上重组（刚体变换）的方式，来得到两个半径为一的实心球。这是因为刚体变换群（ $\mathbb{E}_1$ 或者 $\mathbb{E}_2$ ）作用在实心球上后，可能会不在原来实心球的范围内，比如考虑平移变换。

定理 5.4.3. 对于任意 $n \in \mathbb{N}$，假定 G 是由 $\mathbb{R}^n$ 中一些（未必是全部）刚体变换构成的群并且假设 G 是顺从的。则存在着在 $\mathcal{P}(\mathbb{R}^n)$ （ $\mathbb{R}^n$ 的所有子集 ）上定义的、G-不变的、有限可加的概率测度 μ ， 使得对于 $\mathbb{R}^n$ 上的Lebesgue测度 ν，对于任意 ν 可测集 $D \subset \mathbb{R}^n$ ， 我们有 $\mu(D) = \nu(D)$ 。

注 5.4.1. $\mathbb{R}^n$ 上的Lebesgue测度是 $\mathbb{R}^n$ 这样的一个可数可加正规（ normal ）测度 μ ：

$$\mu\left(\prod_{i=1}^{n}[a_i, b_i]\right) = \prod_{i=1}^{n}(b_i - a_i) \text{ 。}$$

换言之，$\mathbb{R}^n$ 中的Lebesgue测度对应着我们直观中的 体积。该测度是可数可加，并且是刚体变换下保持不变的。

注 5.4.2. 上面提到了Lebesgue测度的一些“好”的性质，对于我们现在的需求（证明低维情形下相悖性不存在），该测度有一个致命问题：$\mathbb{R}^n$ 的任意子集不一定是 Lebesgue 可测的。比如，考虑前面的Vitali不可测集，以及经典Banach-Tarski悖论中剖分得到的集合（一定有Lebesgue不可测集，否则就一定会出现类似 “$1 = 1 + 1$” 的矛盾）。为了解决这个问题，上面的定理对 Lebesgue 测度做了推广，得到的新测度在Lebesgue可测集上与原来的Lebesgue测度定义相同，

但是该新测度是在任意 $\mathbb{R}^n$ 的子集上都有定义的。作为交换（trade-off），该测度不具备“可数可加” 性质，只有相对较弱的 “有限可加” 性质。并且相比于 Lebesgue 测度的刚体变换不变性，该测度只是在 $\mathbb{E}_n$ 的顺从子群 G 下保持不变 （当然， 如果 $n = 1, 2$ ， 则 $\mathbb{E}_n$ 的任何子群都是顺从的）。

注 5.4.3. 上述定理证明的关键一步用到了Hahn-Banach定理。Hahn-Banach定理是泛函分析的重要基石之一，其证明是基于佐恩引理（选择公理的等价形式之一）的。换言之，为了说明低维（一维和二维）情形下Banach-Tarski悖论不成立，我们这里也用到了选择公理。

下面我们来证明上述定理。该证明用到了Hahn-Banach定理和测度论（测度，可测函数，Lebesgue积分）等概念和相关性质。

证明： QQQ ∎

基于上述定理，注意到 $n=1,2$ 时， $\mathbb{E}_n$ 是顺从的，并利用类似 “ $x=x+x$ ， $x\neq 0$ 且 $x\neq\infty$ ” 的归谬法，我们可以得到如下定理：

定理 5.4.4. 对于 $n=1,2$，假定 X 是 $\mathbb{R}^n$ 中的有界子集，并且 X 包含一个半径大于 0 的实心球，则 X 关于刚体变换是非相悖的。

问题：在上述定理中，为什么要求 X 是有界的？为什么要求 X 包含一个实心球？

基于上述**定理5.4.4**，我们可以得到：

推论 5.4.1. 对于 $n=1,2$ ， $\mathbb{R}^n$ 中的实心球（半径大于零）对于刚体变换是没有相悖性的。

注 5.4.4. 对于低维情形，如果 X 不满足 “有界 并且 包含一个实心球” 的条件，X 关于刚体变换是否可能存在相悖性呢？答案是肯定的。$\mathbb{R}^2$ 中就有相关的例子。

习题：

习题 5.4.1. 证明**定理5.4.1**中的三个断言。

习题 5.4.2. 证明**定理5.4.2**。

习题 5.4.3. 证明**定理5.4.4**。

第6章

附录

6.1 群、环、域、代数

在正文中已经简略给出了群的定义，这里给出相对完整的群（半群）、环、域和代数之定义

定义 6.1.1 (群). 群是一个集合 G 和 其上的群结构 （代数运算）$\cdot$， 其中该运算满足：

1) [封闭性] 对任意 $a,b\in G$， $a\cdot b$ 仍在 G 中

2) [结合律] $(a\cdot b)\cdot c=a\cdot(b\cdot c)$， $\forall a,b,c\in G$

3) [恒等元] $\exists e\in G$，满足 $e\cdot a=a\cdot e=a$， $\forall a\in G$

4) [逆元] $\forall a\in G$， $\exists b\in G$， 满足 $a\cdot b=b\cdot a=e$

上述的群，可以记为 $(G,\cdot)$， 或者简记为 G。 $a\cdot b$ 也可以简记为 ab。

如果群的运算是交换的，则我们称这个群为交换群（或者Abel群）。

定义 6.1.2 (交换群). 我们说群 $(G,\cdot)$ 是交换的（或者换言之，G 是交换群），如果对于任意 $a,b\in G$， 都有 $ab=ba$。

注 6.1.1. 对于一般的群，我们习惯上用乘法来表示其群运算。对于交换群，我们可以用加法来表示其群运算。习惯上来说，如果群运算用加法表示，那么该群一定是交换的。

定义 6.1.3 (半群). 半群（semigroup）是一个集合 X 以及其上的乘法 $\cdot$， 满足 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ $\forall a,b,c\in X$。 如果半群 $(X,\cdot)$ 中存在元素 $e\in X$， 满足 $e\cdot a=a\cdot e=a$ $\forall a\in X$，则我们称$(X,\cdot)$ 为含幺半群（unital semigroup, or monoid），称 e 为幺元（unit element）。

例 6.1.1. 我们已经学到了很多半群的例子。比如 $(\mathbb{N},+)$， $(\mathbb{N},\times)$， $(\mathbb{Z},\times)$ 等。事实上，我们引入 $\mathbb{Z}$ 和 $\mathbb{Q}$， 就是分别对半群 $(\mathbb{N},+)$ 和 $(\mathbb{Z}-\{0\},\times)$ 做了Grothendieck化，从而得到了相应的群。

半群定义中的要求是比较低的，只需要对群运算封闭并且满足结合律即可。

例 6.1.2. 关于加法，$\{5m+7n\colon m,n\in\mathbb{N}\}$ 构成一个半群。这个加法半群做Grothendieck化就会得到 $\mathbb{Z}$ 。

定义 6.1.4 (环). 简单的说，环 $(R,+,\cdot)$ 是一个交换群 $(R,+)$（用加法来表示其上的群运算）以及其上的乘法结构，使得 $(R,\cdot)$ 是个半群，并且满足如下分配率：

1) $(a+b)\cdot c=a\cdot c+b\cdot c$

2) $c\cdot(a+b)=c\cdot a+c\cdot b$ 。

如果 R 关于乘法是个含幺半群，则称 $(R,+,\cdot)$ 为含幺环（unital ring）。

我们说环 R 是交换/非交换的，如果 R 关于乘法是交换/非交换的。

一般说来，含幺环研究起来相对容易些。

例 6.1.3. $(\mathbb{Z},+,\cdot)$ 是交换环。$(M_2(\mathbb{R}),+,\cdot)$ 是非交换环。

例 6.1.4. $[0,1]$ 区间上的连续函数全体 $C[0,1]$ 是个交换环。其中的加法和乘法就是通常意义下函数的加法和乘法。

例 6.1.5. 考虑关于 x 的复系数多项式全体

$$P[x]=\left\{\sum_{k=0}^{n}a_kx^k\colon k\in\mathbb{N},a_k\in\mathbb{C}\ \forall\, 0\le k\le n\right\}\ 。$$

其上的加法和乘法定义为通常多项式的加法和乘法。则 $P[x]$ 是个交换环。

例 6.1.6. 考虑关于 x 的复系数形式级数全体

$$P(x)=\left\{\sum_{k=0}^{\infty}a_kx^k\colon k\in\mathbb{N},a_k\in\mathbb{C}\ \forall\, k\ge 0\right\}\ 。$$

其上的加法和乘法定义为通常关于 x 的形式级数之加法和乘法。则 $P(x)$ 是个交换环。

上述例子中的环都是含幺的，下面我们给出不含幺环之例子。

例 6.1.7.

定义 6.1.5 (域). 对于环 $(R,+,\cdot)$， 用 0 来表示其关于加法的单位元。如果 $(R-\{0\},\cdot)$ 还是个乘法群， 那么我们称 $(R,+,\cdot)$ 为一个域（field）。

由于域的要求比环要高，因此域的例子比环的要相对特殊。

例 6.1.8. $\mathbb{Q}$ ， $\mathbb{R}$ ， $\mathbb{C}$ 。 这是经典的交换域之例子。这三个域都是无限的（作为集合是无限集）。

例 6.1.9. 对于任意正素数 p ， $\mathbb{Z}/p\mathbb{Z}$ 是一个正好包含 p 个元素的有限域。这里，$\mathbb{Z}/p\mathbb{Z}$ 是通过等价类的方式来定义的。具体的说，

$$[m]=[n] \quad \Longleftrightarrow \quad m-n\in p\mathbb{Z}=\{px\colon x\in\mathbb{Z}\}\ ,$$

$$[m]+[n]:=[m+n] \quad 且 \quad [m]\cdot[n]:=[m\cdot n]\ 。$$

6.2 线性代数基础

6.3 点集拓扑

简单的说，拓扑空间就是集合加上其上的“开集结构”。具体的严格定义如下：

定义 6.3.1. 拓扑空间 $(X,\mathcal{A})$ 是指一个集合 X 和其幂集 $\mathcal{P}(X)$ 的一个子集 $\mathcal{A}$ ， 并且 $\mathcal{A}$ 满足

i) $\emptyset\in\mathcal{A}$ 且 $X\in\mathcal{A}$

ii) [有限交封闭] 对于任意有限多个 $D_1,\cdots,D_n\in\mathcal{A}$ ， 我们有 $\bigcap_{i=1}^n D_i\subset\mathcal{A}$

iii) [任意并封闭] 对于任意下标集 I ， 若 $D_i\in\mathcal{A}$ ， $\forall i\in I$ ， 则 $\bigcup_{i\in I}D_i\subset\mathcal{A}$

我们称上述 $\mathcal{A}$ 中的元素为开集。

定义 6.3.2. 拓扑空间 $(X,\mathcal{A})$ 中，我们称 E 是闭集，如果 $X-E$ 是开集（即 $X-E\in\mathcal{A}$）。

注 6.3.1. 给定集合 X ，其上的开集结构一定存在（比如，将 $\mathcal{A}$ 取为 $\mathcal{P}(X)$），并且一般不唯一。在 $\mathbb{R}^n$ 中，常见的一种开集定义方式（换言之，常见的拓扑）如下：

“ $\mathbb{R}^n$ 中的子集 D 是开集，如果对于任意 $x\in D$ ， 存在 $\delta>0$ ， 使得 $B(x;\delta)\subset D$ ，其中 $B(x;\delta)$ 定义为 $\{y\in\mathbb{R}^n\colon \mathrm{d}(y,x)<\delta\}$ 。 ”

容易验证，这样定义的开集全体，的确是满足上面定义中的几条性质的。

定义 6.3.3 (Discrete Topological Spaces). 对于拓扑空间 $(X,\mathcal{A})$ ， 我们说它是离散的（离散拓扑空间），如果对于任意 $x\in X$ ， $\{x\}$ 既是开集，也是闭集。

注 6.3.2. 我们直观上觉得 $\mathbb{Z}$ 是离散的，而 $\mathbb{R}$ 不是离散的。按照上述定义，可以给出严格的描述。根据 $\mathbb{Z}$ 上和 $\mathbb{R}$ 上的距离结构 $\mathrm{d}(x,y)=|x-y|$ ， 我们可以定义开集（类似于前面 $\mathbb{R}^n$ 中开集的定义方式），进而得到 $\mathbb{Z}$ 和 $\mathbb{R}$ 上的拓扑结构（开集结构）。对于任意 $m\in\mathbb{Z}$ ， $\{m\}$ 是 $\mathbb{Z}$ 中开集，但是 $\{m\}$ 不是 $\mathbb{R}$ 中开集。为什么？ 提示：对任意 $m\in\mathbb{Z}$ ， 可否找到某个 $\delta>0$ ，使得 $\{x\in\mathbb{Z}\colon \mathrm{d}(x,m)<\delta\}\subset\{m\}$? 如果要求 $\{x\in\mathbb{R}\colon \mathrm{d}(x,m)<\delta\}\subset\{m\}$ 呢?

前面提到过，给定集合 X ， 其上的拓扑结构总是存在的。比如，$(X,\mathcal{P}(X)$ 就一定是个拓扑空间。这样的拓扑空间（任意的 X 的子集都是开集）一定是离散拓扑空间（为什么？）。事实上，任意离散拓扑空间 $(Y,\mathcal{B})$ 一定满足 $\mathcal{B}=\mathcal{P}(Y)$ 。

命题 6.3.1. 拓扑空间 $(X,\mathcal{A})$ 是离散拓扑空间，当且仅当 $\mathcal{A}=\mathcal{P}(X)$ 。

证明： 我们分别证明两个方向。

“$\Rightarrow$” ：

若 $(X,\mathcal{A})$ 是离散拓扑空间，则对于任意 $x\in X$ ， $\{x\}$ 都是开集。根据开集结构（拓扑结构）的定义，任意多个开集的并还是开集。对于任意子集 $D\subset X$ ， 注意到

$$D=\bigcup_{x\in D}\{x\}\ ,$$

故而 D 也是开集。至此，我们证明了 $\mathcal{A}=\mathcal{P}(X)$ 。

“$\Leftarrow$” ：

假定 $\mathcal{A}=\mathcal{P}(X)$ ， 则对于任意 $D\subset X$ ， D 是开集（因为 $D\subset\mathcal{P}(X)$），同时 D 也是闭集（因为 $X-D\subset\mathcal{P}(X)$）。故而 对于任意 $x\in X$ ， $\{x\}$ 既是开集，也是闭集。因此 $(X,\mathcal{A})$ 是离散拓扑空间。

综上，证毕。 ∎

6.4 测度论

《实变函数》课程中会系统的介绍测度论以及基于此的Lebesgue积分等。从某种意义上说，R^n 上的测度对应着类似长度（$\mathbb{R}^1$）、面积（$\mathbb{R}^2$）、体积（$\mathbb{R}^3$）等概念。为了描述通常的Borel测度，我们需要先介绍拓扑空间（可参看本书附录之相关内容）。

这里我们对测度做简单介绍。测度的关键性质是“可数可加性”：若 X_i 两两不交并且都是关于测度 μ 可测的（其中 $i\in\mathbb{N}_{\geq 1}$），则 $\bigsqcup_{i\in\mathbb{N}_{\geq 1}} X_i$ 也是 $\mu-$可测的且

$$\mu\left(\bigsqcup_{i\in\mathbb{N}_{\geq 1}} X_i\right)=\sum_{i=1}^{\infty}\mu(X_i)\ 。$$

我们下面给出测度的正式定义。为了简单起见，我们这里定义的是有界正测度。

定义 6.4.1 (σ-代数). 给定集合 X，对于 $\Sigma\subset\mathcal{P}(X)$，我们说 Σ 是 X 上的一个 σ-代数，如果 Σ 中元素（即 X 的子集）关于最多可数多次集合交、并、差的运算是封闭的。

对于任意 $P(X)$ 的子集 D，包含 D 的最小 σ-代数被称为由 D 所生成的 σ-代数。

例 6.4.1. 对于给定的非空集合 X，$\{\emptyset,X\}$ 和 $\mathcal{P}(X)$ 都是关于集合 X 的 σ-代数。由 $\{\emptyset\}$ 所生成的 σ-代数为 $\{\emptyset,X\}$。

定义 6.4.2 (测度 (measure)). 集合 X 上的一个测度（不妨记为 μ）是从 X上的一个σ-代数 Σ 到 $\mathbb{R}_{\geq 0}$ 上的映射

$$\mu\colon\Sigma\longrightarrow\mathbb{R}_{\geq 0}\ ,$$

满足

1）$\mu(\emptyset)=0$

2）对于任意可数多个互补相交的 $E_1,E_2,\cdots\in\Sigma$，有

$$\mu\left(\bigsqcup_{i=1}^{\infty}E_i\right)=\sum_{i=1}^{\infty}\mu(E_i)\ 。$$

在上述的定义中，如果 X 是个拓扑空间，并且 Σ 包含了 X 上的所有开集，则称该测度 μ 为 Borel 测度。

注 6.4.1. 我们所说的和积分相关的测度，一般是指 Borel 测度。这是因为，在 Borel 测度意义下，任何连续函数都是可测的，从而可以做积分。

i）对于拓扑空间 X 和其上的 Borel 测度 μ，X 的任意子集 D 未必是 $\mu-$可测 的。事实上，根据我们平时习惯的长度概念，可以定义 $[0,1]$ 的长度（测度）μ。μ 对保持平移不变且 $\mu([0,1])=1$。根据佐恩引理，可以构造 $[0,1]$ 的子集 D，其中 D 是满足 “任意两个元素的差为无理数” 的所有集合中最大的。根据 D 之最大性，$\forall x,y\in\mathbb{Q}$，$D+x=D+y$ 当且仅当 $x-y\in\mathbb{Z}$，其中 $D+x$ 为 $\{s+x\ (\mathrm{mod}\ 1)\colon s\in D\}$，这里 $r\ (\mathrm{mod}\ 1)$ 定义为满足 $s\in[0,1)$ 且 $s-r\in\mathbb{Z}$ 的唯一实数 s。若 D 是可测的，则

$$1=\mu([0,1])=\mu(\bigsqcup_{p\in\mathbb{Q}\cap[0,1)}D+\ p\,(\mathrm{mod}1))=\sum_{p\in\mathbb{Q}\cap[0,1)}\mu(D)\ ,$$

矛盾（为什么？）。这个例子就是Vitali不可测集。

ii）一般我们所说的测度，指的是“可数可加”测度。若将“可数可加”换为“有限可加”，就是另外的概念。例如，考虑 $\mathbb{Z}$ 上（可数可加）测度 μ，满足 $\mu(\mathbb{Z})=1$，且若 D 为 $\mu-$可

测 ， 则 $\mu(D+n)=\mu(D)$ ， $\forall n\in\mathbb{Z}$ 。 不难得到这样的测度不存在。如果我们将可数可加减弱为有限可加，则这样的有限可加测度是存在的。类似的，在 $\mathbb{F}_2$ 上，考虑这样的测度 μ ， 满足 $\mu(\mathbb{F}_2)=1$ ， 且 $\mu(gD)=\mu(D)$ ， $\forall g\in\mathbb{F}_2, D\subset\mathbb{F}_2$ 。 则根据 $\mathbb{F}_2$ 的相悖性， 这样的 μ 一定不存在。 事实上，在群自身作用下不变的概率测度（对于群 G ， 满足 $\mu(G)=1$）之存在性，就是离散群顺从性之定义。

参考书目和文献

[1] 方启勤、林源渠，《数学分析习题集》，高等教育出版社

[2] 林源渠、方启勤，《数学分析解题指南》，北京大学出版社

[3] 华东师范大学数学系，《数学分析》，高等教育出版社

[4] 张筑生，《数学分析新讲》（第一册），北京大学出版社

[5] 裴礼文，《数学分析中的典型问题与方法》（第2版），高等教育出版社

[6] Halmos, P. R.《Naive Set Theory》

[7] Rudin, W. 《Principles of Mathematical Analysis》

[8] Wagon, S. 《The Banach-Tarski Paradox》，Cambridge University Press