數理基础

工程师学院数学理论基础

Fondements des Théories Mathématiques de l'Ecole d'Ingénieur de Chimie Pékin

第一部分:基础知识

Partie I: Notions Élémentaires

Augustin

最后更新于:2023 年 10 月 16 日

目录

第一章　逻辑与证明

Logique et Démonstration

这一章内容是数学最基本的、最底层的概念.对于绝大多数阅读这份讲义的人而言,前几节的东西都已经学习过了,或者显而易见的. 但这并不意味着这一章的内容就很好写,或者很好讲明白.也因此,为了保持知识的丰富度和连贯性,有许多还没在本讲义里被严格定义,但是其实已经学过的知识会出现在本章(后面也是). 对于绝大多数这类情况,并不存在阅读障碍.但是,如果你发现有什么地方不太对劲,或者有什么地方不太懂,欢迎联系我,我会尽快修改.

这一章(以及后面的章节里)有相当多的符号,关于这些符号的采用和相关的历史,欢迎参阅`https://jeff560.tripod.com/set.html`.

1.1　基本逻辑 Basic Logique

1.1.1　命题逻辑 Logique propositionnelle

命题(Proposition)是一个陈述句所表达的判断,不是真的就是假的.例如“我不懂数学”就是一个命题.当然,在本讲义中,带有Proposition节标题的内容都被认为是真的.

逻辑析取:或 la disjonction: ou

定义符号 $\vee$ 表示两个命题的逻辑析取.对于命题p, q,若p是真的或者q是真的,则$p \vee q$是真的.

逻辑合取:与 la conjonction: et

定义符号 $\wedge$ 表示两个命题的逻辑合取.对于命题p, q,若p和q都真的,则$p \wedge q$是真的.

逻辑否定:非 la négation: non

定义符号 $\neg$ 表示命题的逻辑否定.若命题p是真的,则$\neg(p)$是假的.

逻辑蕴含 l'implication

定义符号 $\Rightarrow$ 表示两个命题的逻辑蕴含.对于命题p, q,将$p \vee (\neg q)$记为$q \Rightarrow p$. 表示若q是真的则p也是真的.注意,如果p, q都不是真的,$q \Rightarrow p$也是真的.

逻辑等价 l'équivalence

定义符号 $\Rightarrow$ 表示两个命题的逻辑等价.对于命题p, q,将$(p \Rightarrow q) \wedge (q \Rightarrow p)$记为$p \Leftrightarrow q$. 称作p等价于q.

1.1.2 逻辑公理 Axiomes de la logique

公理被认为是清晰地为真的命题.以下给出逻辑的四条公理.

AL_1

$(p \vee p) \Rightarrow p$是真的.这说明,如果$(p \vee p)$为真,则p为真.

AL_2

$p \Rightarrow (p \vee q)$是真的.这说明,如果p为真,则$(p \vee q)$为真.

AL_3

$(p \vee q) \Rightarrow (q \vee p)$是真的.这说明,如果$(p \vee q)$为真,则$(q \vee p)$为真.

AL_4

$(p \Rightarrow q) \Rightarrow [(p \vee r) \Rightarrow (q \vee r)]$是真的.

1.1.3 De Morgan定律 Lois de De Morgan

数学家Augustus De Morgan发现了命题逻辑中存在着如下关系:

- $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$
- $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$

称为De Morgan定律,又叫对偶律.

1.1.4 量词 Quantificateur

全称量词 Quantification Universelle

全称量词$\forall$表示“对所有的(pour tout)”.由Gerhard Gentzen首先于1933年使用,将德语“一切(alle)”的首字母倒过来.

存在量词 Quantification Existentielle

存在量词$\exists$表示“存在(il existe)”.由Giuseppe Peano首先于1897年使用,后被Bertrand Arthur William Russell正式用于表示“存在”. 此外,存在量词$\exists!$表示“有且仅有唯一的(il existe et seul)”.

1.2 证明 Démonstration

给定命题p,现在并不清楚命题是真是假.如果我们想要命题为真,就需要从逻辑上证明.同理,如果想要为假,也要从逻辑上证伪.这些都属于证明.

1.2.1 逻辑变换 Transformations logiques

蕴含命题$p \Rightarrow q$,全称命题$\forall x, p(x)$和存在命题$\exists x, q(x)$有如下的逻辑变换:

逆命题 Implication Réciproque

蕴含命题$p \Rightarrow q$的逆命题为$q \Rightarrow p$,逆命题不受量词影响,即$\forall x, p(x) \Rightarrow q(x)$的逆命题为$\forall x, q(x) \Rightarrow p(x)$.

否命题

蕴含命题$p \Rightarrow q$的否命题为$\neg p \Rightarrow \neg q$. 全称命题$\forall x, p(x)$的否命题为$\exists x, \neg p(x)$,存在命题$\exists x, q(x)$的否命题为$\forall x, \neg q(x)$.

逆否命题 Proposition Contraposée

蕴含命题$p \Rightarrow q$的逆否命题为$\neg q \Rightarrow \neg p$.逆否命题与原命题等价.

1.2.2 三段论 Syllogisme

三段论是涉及三个命题的论证,形式如$[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$. 一般而言,一个三段论分为大前提(Prémisse majeure),小前提(Prémisse mineure)和结论(Conclusion)三段. 大前提是某种普遍性质的规律,小前提是一个特殊陈述,结论就是我们要证明的内容. 例如要证明114是偶数,我们需要:

- 大前提:能整除2的数是偶数.
- 小前提:114能整除2.

- 结论:114是整数.

三段论的每段共有四种含义,分别为:

- A:$\forall s, p(s)$.例如:所有自然数都是实数.
- E:$\forall s, \neg p(s)$.例如:所有自然数都不是负数.
- I:$\exists s, p(s)$.例如:存在实数是自然数.
- O:$\exists s, \neg p(s)$.例如:存在实数不是自然数.

因此一个三段论可以被简写称诸如AAA或者AEO这样的形式,共计256种!然而只有24种是有效的.在这里我就不一一列出了,有兴趣的读者自行查阅相关内容. 下面我们直接介绍具体的证明方法.当然,如果你能将证明方法与对应的三段论结构联系起来,那是非常棒的!

1.2.3 举例证明 Preuve par exemple

假设要证明命题“存在不可导连续函数”,我们只需要举出一个例子就行,比如绝对值函数$f(x) = |x|$. 同理,证伪命题“所有连续函数都可导”也是这样.

1.2.4 逆否证明 Preuve par contraposée

逆否命题与原命题等价,因此只需证明或者证伪逆否命题,就能间接证明或证伪原命题.

1.2.5 反证法 Preuve par l'absurde

假设我们要证明命题A为真,我们可以假设¬A为真,然后推出一个矛盾的结果⊥,因此¬A为假,从而证明A为真.

例如,我们要证明素数有无限个.采用反证法:¬(素数有无限个) ⇒ 素数有有限个.设全体素数组成的集合$\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$, 设$n = 1 + \prod_{i=1}^{n} p_1$,显然$n \notin \mathbb{P}$.若$n$是素数,则我们得到了一个不属于全体素数集合的素数,这显然矛盾.若n不是素数,对其质因数分解,选择任意一个质因子m. 若$m \in \mathbb{P}$,则m既是$1 + \prod_{i=1}^{n} p_1$的因子,又是$\prod_{i=1}^{n} p_1$的因子,因此必须是两者之差1的因子,也就是1.因此$n = m \cdot 1$,n显然是素数, 所以我们又得到了矛盾的结果.所以,只能是我们的前提“素数有有限个”是错的,故素数有无限个.

1.2.6 归纳法 Preuve par récurrence

1.2.7 分类讨论 Preuve par cas

更多关于证明的例子和技巧,可以参阅roofs from THE BOOK这本书(中文名叫《数学天书中的证明》),其涵盖了数论、几何、分析、组合数学和图论的许多精美的证明.

1.3 严格逻辑公式 Formules strictes

通过以上的逻辑符号和公理,加上两个用于判断的符号 $\bot$ 表示”假”和 $\top$ 表示”真”,我们可以构造出一些严格逻辑公式.

1.3.1 Définition: Formule stricte

严格逻辑公式的定义实际上是一种归纳法.

1. $\bot$ 和 $\top$ 是严格逻辑公式.
2. 任意的变量都是严格逻辑公式.
3. 对任意严格逻辑公式A, $\neg A$也是严格逻辑公式.

4. 对任意两个严格逻辑公式A和B, $(A \wedge B)$,$(A \vee B)$,$(A \Rightarrow B)$,$(A \Leftrightarrow B)$也是严格逻辑公式.

在一些推理中,利用$\circ$代表$\wedge, \vee, \Rightarrow, \Leftrightarrow$中的任意一个,并将 formule stricte 简称为逻辑公式 formule. 此外,对于除了$\bot$和$\top$以外的逻辑公式,我们称其为可分解的(décomposable).

Exemple

$(a \vee (\neg b \wedge c))$是逻辑公式,但是$a \vee (\neg b \wedge c)$和$(a \vee (\neg(b) \wedge c))$不是.

1.3.2 Définition: 子公式 Sous-formule stricte

称(严格)公式 A 的任何因子为A的子公式.例如$(\neg b \wedge c)$是$(a \vee (\neg b \wedge c))$的子公式.

1.3.3 Définition: 公式的长度 Longueur d'une formule

公式 A 的长度是用于编写 A 的符号数量,用 $l(A)$ 表示. 如果我们将公式视为用词汇表中的元素构成的词,其中的元素包括常量、变量、括号和连接符. 则在这个词汇表上的一个词是该词汇表中元素的一个序列,而该词的长度是该序列的长度. 例如$A = (a \wedge b)$,$B = (A \vee \neg A)$,则$l(A) = 5$, $l(B) = 4 + 5 + 5 = 14$.

1.3.4 Définition: 公式的前缀 Préfixe d'une formule

对任意公式A,其前缀(préfixe)是从该公式的开头一直延伸到某个位置的部分. 这个位置可以是一个特定的字符,一个操作符或一个括号,用来截断公式的前缀. 例如(和(a都是$A = (a \wedge b)$的前缀.但是)或者b)不是. 此外,对于长度严格小于A的前缀,我们称其为严格前缀(préfixe strict).

1.3.5 括号的平衡Équilibre des parenthèses

任何公式都具有相等数量的开括号"("和闭括号")".可直接由定义和归纳法得到.

1.3.6 括号的关联 Relation entre les parenthèses

任何公式的前缀都具有至少与闭括号相等数量的开括号.

Démonstration

首先假设对于任意长度小于n的公式,该定理都成立。接着假设$l(A) = n$.

1. 若A是一个变量或者常量,则A没有括号,因此该定理成立.
2. 若$A = \neg B$,则A的前缀要么是空的或者$\neg$,要么是$\neg$跟随B的前缀,而$l(B) < n$,因此该定理成立.
3. 若$A = (B \circ C)$,则A的前缀要么是空的或者开括号,要么是开括号跟随B的前缀,要么是开括号跟随$B\circ$和C的前缀.根据以上结论,都满足该定理.

因此,如果引理对于所有长度小于n的公式都成立,那么它也对于长度为n的任何公式成立。通过归纳法,我们可以得出它对于任何长度的公式都成立。这个证明证明了数学逻辑中公式的括号平衡性质。

1.3.7 Définition: 公式的大小 Taille d'une formule

对公式A定义$|A|$为:

- 若A是$\perp$或$\perp$,则$|A| = 0$.
- 若A是变量,则$|A| = 0$.(?)
- $|\neg A| = 1 + |A|$.
- $|A \circ B| = 1 + |A| + |B|$.

1.3.8 严格前缀引理 Lemme des préfixes stricts

任何公式的严格前缀不是一个公式.

Tout préfixe strict d'une formule n'est pas une formule.

Démonstration

仍然采用归纳法.对于基本情况$|A| = 0$,A要么是变量要么是常量,其严格前缀只能是空的,故不是公式. 假设对于任意长度小于n的公式,该定理都成立。接着假设$|A| = n$.

若$A = \neg B$,则A的严格前缀要么是空的或者$\neg$,要么是$\neg$跟随B的严格前缀,而$|B| < n$,因此该定理成立.

若$A = (B \circ C)$,假设A有一个为公式的严格前缀$A_0 = (B \circ C_0)$,其中C_0是C的前缀. 为了保持公式的开括号与闭括号数量一致,我们必须有$C_0 = C$.因此$A_0 = A$,与严格前缀矛盾.因此该定理成立.

1.3.9 Proposition

对于任何公式A,其有且仅有可能为以下形式之一:

- A是一个变量
- A是一个常量
- $A = \neg B$,其中B是一个公式,且A是唯一的
- $A = (B \circ C)$,其中B, C是公式,且A是唯一的

Démonstration

事实上我们只需证明最后一种形式.同样可以假设$A = (B \circ C) = (B_0 \circ C_0)$然后证明$B_0 = B$, $C_0 = C$.与之前没什么差别.

1.3.10 优先级 Priorité

在定义公式时,我们写了很多不必要的括号,例如每个公式周围的括号。现在,我们通过定义优先级为语法引入了更多的灵活性。同样利用归纳法定义具有优先级的公式(或称为优先级公式 formule à priorité):

- $\bot$ 和 $\top$ 是优先级公式.
- 任意的变量都是优先级公式.
- 对任意优先级公式A, $\neg A$也是优先级公式.
- 对任意两个优先级公式A和B, $A \circ B$也是优先级公式.
- 对任意优先级公式A, (A)也是优先级公式.

例如$a \vee \neg b \wedge c$是一个优先级公式,但它并不是公式.为了确保公式的唯一性,我们需要定义连接词的优先级顺序.

优先级顺序 Ordre de priorité des connecteurs

定义连接词的优先级顺序(由高到低)如下:

1. $\neg$ 否定 la négation
2. $\wedge$ 合取 la conjonction
3. $\vee$ 析取 la disjonction
4. $\Rightarrow$ 蕴含 l'implication
5. $\Leftrightarrow$ 等价 l'équivalence

Remarque

在相同优先级的情况下,左侧的连接词具有更高的优先级,但对于蕴含操作符,它是右结合的。我们将一个具有优先级的公式视为使用优先级可重新构建的公式的缩写。除非另有说明,我们将一个公式与其缩写视为相同。换句话说,我们关注的是一个公式的结构,而不是它的表面写法,这一结构通过"stricte"语法得以明确。因此,具有优先级的公式的大小将等于它所代表的严格公式的大小。

1.4 公式的意义 Sens des formules

在这一部分,我们将探讨如何确定一个公式的真假,而不依赖于为其变量分配的值。我们首先会定义逻辑连接词的含义,然后解释如何计算一个公式的真值,并展示紧凑性定理。最后,我们将介绍逻辑学中的基本概念定义,这些构成了逻辑学家们的通用语言。

1.4.1 连接词的真假 Valeur de vérité des connecteurs

通常用0表示值为假,用1表示值为真.这样,可以分别依据变量x和y的真假给出连接词的真假.

x	y	$\neg x$	$x \vee y$	$x \wedge y$	$x \Rightarrow y$	$x \Leftrightarrow y$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

表 1.1: 连接词真值表 Table de vérité des connecteurs

1.4.2 公式的值 Valeur d'une formule

我们为公式中的每个变量分配一个来自集合 $B = \{0, 1\}$ 的值。公式的值通过将变量替换为它们的值并根据表1.1的操作来计算得到。然而,为了对公式进行推理,我们需要正式定义公式的值。

Définition: 赋值 Assignation

赋值是将公式中的所有变量映射到集合B中.

Une assignation est une application de l'ensemble de toutes les variables d'une formule dans l'ensemble B.

Définition: 公式的值 Valeur d'une formule

对于一个公式A和一个赋值v,我们定义A在v下的值$[A]_v$如下,其中A, B是公式,x是变量,v是赋值.

- $[x]_v = v(x)$
- $[\bot]_v = 1$, $[\bot]_v = 0$
- $[\neg A]_v = 1 - [A]_v$
- $[A \wedge b]_v = \max\{[A]_v, [B]_v\}$
- $[A \vee b]_v = \min\{[A]_v, [B]_v\}$
- $[A \Rightarrow b]_v = \begin{cases} 1 & [A]_v = 0 \\ [B]_v & [A]_v \neq 0 \end{cases}$
- $[A \Leftrightarrow b]_v = \begin{cases} 1 & [A]_v = [B]_v \\ 0 & [A]_v \neq [B]_v \end{cases}$

根据第1.3.9 节的结论,根据第14页的定理1.1.13,每个严格的公式都可以唯一分解为上述情况之一。这意味着将变量的赋值扩展到所有公式是一个从公式到B的映射。例如，对于四个公式 A、A_0、B 和 B_0 以及两个操作符 $\circ$ 和 $\circ_0$, 如果 $(A \circ B) = (A_0 \circ_0 B_0)$，则根据分解的唯一性，我们可以得出 $A = A_0$,$B = B_0$,$\circ = \circ_0$。因此，公式 $(A \circ B)$ 的值仅由值定义中的一行唯一确定。这表明公式的值仅与其包含的变量和结构有关，因此公式的计算以真值表的形式展示,如表1.2所示.

x	y	$\neg x$	$x \vee y$	$x \wedge y$	$x \Rightarrow y$	$x \Leftrightarrow y$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

表 1.2: 公式真值表 Table de vérité des formules suivantes

1.5 替换和取代 Substitution et remplacement

1.6 标准形式 Formes normales

将一个公式转化为标准形式是将其转化为一个具有结构性质的等价公式的过程。我们引入了两种标准形式的概念:析取范式(Disjunctive Normal Form,DNF),用于突出模型, 以及合取范式(Conjunctive Normal Form,CNF),用于展示反例。标准形式的定义需要引入文字(literal)、单项式(monomial)和子句(clause)的概念。

1.7 Boole代数 Algèbre de Boole

1.8 Boole函数 Fonctions booléennes

1.9 二进制决策图计算器 Binary Decision Diagram based Calculator

1.10 一阶逻辑 Logique du premier ordre

待修改

第二章　集合

Ensembles

我们先从数学最基础的内容开始.前面这一部分内容在大一就已经讲过了,然而为了保持本讲义的连贯与严谨,不突兀地出现公理化集合论之类的东西,我们还是从头开始讲起.

2.1　集合

为了便于你的理解,我们先给出集合的定义,并且顺着这些定义讨论,随后会在第2.4 节这里把这些概念全部公理化,以求得到更深刻的理解. 事实上,本讲义的许多内容,都是先讲个基础的概念,随后在某个内容里将这个概念公理化.

2.1.1　Définition

我们朴素地认为,一个集合就是将对象归类而分成为一个或数个形态各异的大小整体. 一般来讲,集合是具有某种特性的事物的整体,或是一些确认对象的汇集.构成集合的事物或对象称为元素.集合的元素可以是任何东西.

2.1.2　集合的特性

集合具有以下几个特性:

- 无序性:一个集合中,每个元素的地位都是相同的,元素之间是无序的.[1]
- 互异性:一个集合中,每个元素只能出现一次,没有相同的元素出现.
- 确定性:给定一个集合,任给一个元素,该元素或者属于或者不属于该集合.

2.1.3 索引族 Famille Indexée

若集合I中的每个元素,比如i,都对应着一个集合A_i,那么称$\mathscr{A} = \{A_i | i \in I\}$为集合$A$的索引族,集合$I$是其索引集.

Exemple

$A_n = \{1, 14, n^2\}$,且有$\mathscr{A} = \{A_n | n \in [\![5, 14]\!]\}$,则$\mathscr{A}$就是$A_n$的索引族,并且$\mathscr{A} = \{\{1, 14, 25\}\{1, 14, 36\} \dots \{1, 14, 196\}\}$.

2.1.4 子集 Sous-ensemble

若集合B中的每个元素都属于集合A,则集合B是集合A的子集,则集合A是集合B的超集,记为$B \subseteq A$或者$A \supseteq B$. 此外,若$B \subseteq A$且$A \subseteq B$,说明二者的元素相同,是同一个集合,记为$A = B$.

Proposition

对于任意集合A,有$\varnothing \subseteq A$.

2.1.5 幂集 Ensemble Puissance

对于任意集合A,其幂集为由该集合全部子集为元素构成的集合,记为$\mathcal{P}, \mathcal{P}(A) = \{B | B \subseteq A\}$. 有时也称之为ensemble des parties.

[1] 当然,如果我们在集合上定义了序,那么元素之间就可以按照序关系排序.但就集合本身的特性而言,元素之间没有必然的序.序关系将在后续阐明.

2.2 二元关系 Relation Binaire

2.2.1 有序对 Couple

有序对是包含了两个元素的特殊的集合(a,b).不同于一般的集合,有序对上的两个元素是有顺序的, 分别被称为左投影和右投影,法语也叫première composante和deuxième composante.有序对的相等要求:

$$(a_1,b_1)=(a_2,b_2)\Leftrightarrow(a_1=a_2)\wedge(b_1=b_2)$$

有序对可以有其他有序对作为投影,所以有序对使得能够递归定义有序. 例如,有序三元组 (a,b,c)可以定义为(a, (b,c)),一个对嵌入了另一个对.

2.2.2 Définition

二元关系将一个集合的元素与另一个集合的元素相关联.例如集合X和Y上的二元关系$\mathcal{R}$是一组新的有序对(x,y)组成的集合$\mathcal{G}$,其中$x\in X,y\in Y$. 如果$(x,y)\in\mathcal{G}$,则称x,y有关系$\mathcal{R}$,记作$x\mathcal{R}y$或者$\mathcal{R}(x,y)$.

Exemple

$\mathbb{N}$上的大于关系>可以表示为$\{(a,b)|\exists r\in\mathbb{N},(a=b+r)\}$.记作$a>b$.

2.2.3 关系的性质

二元关系R可能拥有以下的某些性质:

自反性 Relation Réflexive

$\forall x\in X,(x,x)\in R$

非自反性 Relation Irréflexive

$\forall x\in X,(x,x)\notin R$

对称性 Relation Symétrique

$$\forall x \in X, y \in Y, (x, y) \in R \Leftrightarrow (y, x) \in R$$

反对称性 Relation Antisymétrique

$$\forall x \in X, y \in Y, (x, y) \in R \wedge (y, x) \in R \Leftrightarrow x = y$$

非对称性 Relation Asymétrique

$$\forall x \in X, y \in Y, (x, y) \in R \Rightarrow (y, x) \notin R$$

传递性 Relation Transitive

$$\forall (x, y) \in R, \forall (y, z) \in R \Rightarrow (x, z) \in R$$

2.2.4 等价关系 Relation d'Équivalence

若二元关系~满足自反性、传递性和对称性,则称其为等价关系,记作$a \sim b$.

Exemple

- 集合的相等是等价关系.
- 三角形的相似关系和全等关系是等价关系.
- 温度相同是等价关系.

等价类 Classe d'Équivalence

集合E上定义等价关系~,对$a \in E$,a的等价类为集合中所有与其等价的元素组成的集合$\{x | x \sim a \wedge x \in E\}$.

2.2.5 序关系 Relation d'Ordre

前文说过,集合上的元素本身是无序的,这意味着元素之间是平等的,无法比较的. 例如给定集合{2000CNY,3000USD,1919JPY,400EUR},我们并不知道四个元素分别意味着什么,也不知道他们的关系.现在给出 *Champion* 断言: 2000CNY≥3000USD. 为什么可以这么说?显然,这说明存在某种“顺序”,这种“顺序”可以通过符号≥来表示两个元素的关系.事实上,这就是一种序关系.下面我们分别介绍各种序关系.

全序关系 Relation d'Ordre Total

若集合X上的关系≤满足自反性、传递性和反对称性,并且是“完全的(Totalité)”,也就是$\forall a \in X, \forall b \in X, (a \leq b) \vee (b \leq a)$. 则称此关系为全序关系,或者非严格全序关系.

相对应的,若集合X上的关系<定义为$a < b \Leftrightarrow \neg(b \leq a)$,则称为严格全序关系(Ordre strict total).其满足反自反性、传递性和非对称性.

良序关系 Relation Bien Ordonné

若集合X上的全序关系≤使得对任意子集$S, \exists i \in S, \forall s \in S, i \leq s$,则称此关系为良序关系. 换句话说,任意子集有最小值的全序关系称为良序关系.

偏序关系 Relation d'Ordre Partiel

若集合X上的关系≤满足自反性、传递性和反对称性,即不“完全”的全序关系被称为偏序关系. 同理也有相对应的严格偏序关系$a < b$,使得$a < b \vee a = b \Rightarrow a \leq b$.

预序关系 Relation Préordre

若集合X上的关系$\preceq$满足自反性和传递性,则称之为一个预序关系.它既不一定是反对称的,也不一定是非对称的. 预序关系有时也用$\lesssim$表示.将预序集的等价元素等同起来,可得到由该预序集所导出的偏序集.对称的预序就是等价关系.

2.3 集合的运算 Opérateur

集合之间有以下几种常见的运算:

2.3.1 交集 Intersection

集合A和B的交集是两者共同包含的元素组成的集合,用符号$\cap$表示,即:

$$A \cap B = \{x | (x \in A) \wedge (x \in B)\}$$

2.3.2 并集 Union/Réunion

与交集相对应,集合A和B的并集是两者包含的所有元素组成的集合,用符号$\cup$表示,即:

$$A \cup B = \{x | (x \in A) \vee (x \in B)\}$$

2.3.3 Remarque: 交集与并集的性质 Propriété de l'lntersection et de l'union

- 对于任意集合A,$A \cap A = A = A \cup A$.
- 交换律: $A \cap B = B \cap A, A \cup B = B \cup A$.
- 结合律: $(A \cap B) \cap C = A \cap (B \cap C), (A \cup B) \cup C = A \cup (B \cup C)$.
- $(A \cap B) \subseteq A \subseteq (A \cup B)$.

- $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.

2.3.4 集合的分配律 Distributivité

有限个集合的交集与并集符合分配律,这是很重要的性质.对$n \in \mathbb{N}$:

$$A \cup (\bigcap_{i=1}^{n} B_i) = \bigcap_{i=1}^{n} (A \cup B_i)$$

$$A \cap (\bigcup_{i=1}^{n} B_i) = \bigcup_{i=1}^{n} (A \cap B_i)$$

2.3.5 补集 Complémentaire

集合A对于集合B的补集是属于B却不属于A的元素组成的集合, 记为$\complement_B^A$或者A^C:

$$\complement_B^A = \{x \in B | x \notin A\}$$

2.3.6 差集 Différence

集合A对于集合B的差集是A中不属于B的元素组成的集合,可以被看作是补集的一种形式记为$A \backslash B$或者$A - B$:

$$A \backslash B = \{x \in B | x \notin A\}$$

对称差 Différence symétrique

集合A和集合B的对称差是属于B或者属于A,却不同时属于两者的元素组成的集合, 记为$A \Delta B$:

$$A \Delta B = (A \cup B) \backslash (A \cap B) = (A \backslash B) \cup (B \backslash A)$$

2.3.7 笛卡尔积 Produit Cartésien

定义两个集合的笛卡尔(Descartes)积为其元素组成的有序对的集合,即:

$$X \times Y = \{(x, y) | x \in X, y \in Y\}$$

对于同一个集合对自身做笛卡尔积,我们采用幂的符号.如$A \times A = A^2$.

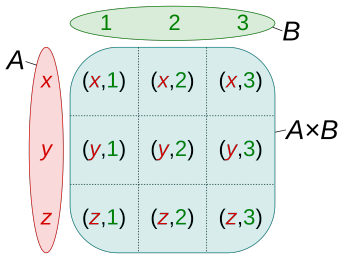

图 2.1: Produit Cartésien(图源wiki)

Exemple

我们最熟悉的平面直角坐标系就是$\mathbb{R}^2$.

2.3.8 De Morgan定律的集合形式

在集合论中,De Morgan定律表现为如下形式:

- $(A \cap B)^C = A^C \cup B^C$
- $(A \cup B)^C = A^C \cap B^C$

在经典命题逻辑的外延中,此二元性依然有效.即对于任意的逻辑运算符,我们都能找他它的对偶. 这导致了基于传统逻辑的逻辑学的一个重要性质,即否定范式的存在性:如果其中否定仅出现在作用于公式中非逻辑的原子,任何公式都有它的等价公式.

2.4 公理化的集合论

主观意义上说,无论是ZF还是ZFC,在本讲义(或学院的课程)的“使用体验”上与原来朴素的直观的集合论没有什么区别,并且,有很多概念我们没有清晰. 因此其实不必看懂这一章讲了什么,它不会影响你对后续章节内容的理解.

2.4.1 Russell悖论

现在,回头看看第2.1.2 节,尝试回答以下问题:
设集合A是所有不属于自身的集合的集合,即$A = \{x|x \notin x\}$.那么请问A是否属于它自己?

- $A \in A$,说明A满足不满足其定义的不属于自身的性质,则$A \notin A$.
- $A \notin A$,说明A满足不属于自身的性质,则$A \in A$.

该悖论由数学家Bertrand Arthur William Russell提出,故称为Russell悖论.从经典逻辑的爆炸原理来看,任何命题都可以从矛盾中得到证明. 因此,存在像Russell悖论这样的矛盾是灾难性的,因为如果任何公式可以被证明为真,它就破坏了真和假的含义. 此外,由于集合论被视为所有其他数学分支公理化发展的基础,Russell悖论威胁到了整个数学的基础 [2],这激发了发展无矛盾的集合论的大量研究.

2.4.2 Zermelo-Fraenkel集合论:ZF公理体系

Zermelo-Fraenkel公理是众多集合论公理中的一员,也是对于不需要深入学习数学(特别是集合论)的我们最常见的公理体系. 这套公理是二十世纪早期为了建构一个不会导致类似Russell悖论的矛盾的集合理论所提出的一个公理系统,简称为ZF公理. 该公理体系包含以下公理:

[2]其实除了Russell悖论,还有Burali-Forti悖论和Cantor悖论,但是相关的前置内容没有涉及,所以不放在这里讨论.

外延性公理 Axiome d'extensionnalité

如果两个集合具有相同的元素则它们相等.

Si deux ensembles ont les mêmes éléments, alors ils sont égaux.

$$\forall A \forall B, \forall x, (x \in A \Leftrightarrow x \in B) \Rightarrow A = B$$

正规公理 Axiome de fondation/régularité

每个非空集合X都包含一个元素y,使得X和y不相交.

Tout ensemble X non vide contient un élément y tel que X et y sont des ensembles disjoints (qui n'ont aucun élément en commun).

$$\forall X \neq \varnothing, \exists y \in X, y \cap X = \varnothing$$

分类公理 Schéma d'axiomes de compréhension/séparation

设$\mathbb{A}$为一个集合,且P为任一个描述$\mathbb{A}$内元素x的特征的性质,则存在$\mathbb{A}$的子集A包含$\mathbb{A}$内满足这个性质的x.

Pour tout ensemble A et toute propriété P exprimée dans le langage, il existe un ensemble dont les éléments sont les éléments de A vérifiant P.

$$\forall \{x|P(x)\} \subseteq \mathbb{A}, \exists A \subseteq \mathbb{A}, A = \{x|P(x)\}$$

这样我们就可以定义空集了,例如对于集合$\mathbb{A}, \varnothing = \{x|x \in \mathbb{Z}, x \neq x\}$. 有时这也被称为空集公理(Axiome de l'ensemble vide).

配对公理 Axiome de la paire

若X和Y是集合,则存在一个集合包含X和Y.

Si X et Y sont deux ensembles, alors il existe un ensemble contenant X et Y et eux seuls comme éléments.

$$\forall X \forall Y, \exists Z, X \in Z, y \in Z$$

并集公理 Axiome de la réunion

对任一个集合$\mathcal{F}$,存在一个集合A,包含每个为$\mathcal{F}$的某个元素的元素的集合.

Pour tout ensemble $\mathcal{F}$, il existe un ensemble A dont les éléments sont précisément les éléments des éléments de $\mathcal{F}$ et eux seuls.

$$\forall \mathcal{F} \exists A, \forall F \subseteq \mathcal{F}, \forall x \in F \Rightarrow x \in A$$

替换公理 Schéma d'axiomes de remplacement

任何可定义函数下的集合的像也将落在集合内.

Pour tout ensemble A et toute relation fonctionnelle P,formellement définie comme une proposition$P(x, y)$ et tel que $P(x, y)$ et $P(x, z)$ impliquent que $y = z$, il existe un ensemble contenant précisément les images par P des éléments de l'ensemble d'origine A.

无穷公理 Axiome de l'infini

存在包含无限多个元素的集合.

Il existe un ensemble W dont $\varnothing$ est élément et tel que pour tout X appartenant à W,$X \cup \{X\}$appartient aussi à W.

$$\forall X,\ \exists \mathbb{W}, X \subseteq \mathbb{W} \Rightarrow X \cup \{X\} \subseteq \mathbb{W}$$

幂集公理 Axiome de l'ensemble des parties

对任一个集合X,存在一个集合Y为X的幂集的超集.

Pour tout ensemble X, il existe un ensemble dont les éléments sont précisément tous les sous-ensembles de X.

$$\forall \mathbb{X}, \exists \mathbb{Y}, \forall X, X \subseteq \mathbb{X} \Rightarrow X \in \mathbb{Y}$$

良序定理 Théorème de Zermelo/du bon ordre

所有集合都可以被良序排序.[3]

Tout ensemble peut être muni d'une structure de bon ordre.

2.4.3 选择公理 l'Axiome du choix: ZFC公理体系

对于所有的非空的索引族$(S_i)_{i\in I}$,存在一个索引集$(X_i)_{i\in I}$使得$\forall i \in I, X_i \in S_i$.它可以被理解为:给定任何非空集合的族,可以通过从每个集合中任意选择一个元素来构造一个新集合,即使其包含集合是无限的.

对于Zermelo-Fraenkel集合论,若讨论的是其不包含学选择公理的形式,则称为ZF公理体系;若是其包含学选择公理的形式,则称为ZFC公理体系.

[3]若给定前八个公理,就可以找到许多个和良序定理等价的叙述,例如选择公理.

第三章　映射

Applications

内容调整中.

Me: Mom, can we get $f(x)$?
Mom: No, we have $f(x)$ at home.
$f(x)$ at home:

$$y$$

第四章　运算与代数结构

Opérations et Structure Algébrique

4.1　运算

在我的数学学习经历中,我最先认识了数字,也就是1、2、3、4这些,随后就开始学习了加法,然后是减法、乘法、除法之类的东西. 这些东西都被称为运算.有些运算是一元的,例如$\cos x$和$|x|$,我们输入一个变量,得到一个返回结果;有些运算是二元(多元)的,例如a^b或者$A \times B$.本章里我们主要讨论二元运算. 有些运算与数没有关系,例如逻辑运算里,$1 \vee 0 = 1$,这里1和0只是表示逻辑上的真和假,与具体的数字无关. 此外,还有一种题目叫做“定义新运算”,一般会给出一个自定义的算符,比如$\star$,然后解释这个算符怎么计算,比如说$a \star b = 114a + \frac{514}{b} - 19^{\frac{a}{b}}$,让你求解一些具体的返回值. 这些统统都是运算.为了应付日益复杂的数学,我们需要把运算统一起来研究,以便于尝试找到普适性的规律.

4.1.1　Définition

给定集合X,所有$f : X \times X \to X$的映射称为集合X上的运算.直观上看,运算将X上的有序点对映射为X的元素. 我们姑且将运算符号记为$\star$. 这样我们可以将

一个运算表示为$(x,y) \in X*2, f(x,y) \to x \star y$.

Exemple

在$\mathbb{R}$上两个区间的并$(-114,81] \cup (-91,514) = (-114,514)$是一个运算.

4.1.2 结合律 Associative

设X上的运算$f(x,y) \to x \star y$,若:

$$\forall (x,y,z) \in X^3, x \star (y \star z) = (x \star y) \star z$$

称此运算满足结合律.

4.1.3 交换律 Commutative

设X上的运算$f(x,y) \to x \star y$,若:

$$\forall (x,y) \in X^2, x \star y = y \star x$$

称此运算满足交换律.

4.1.4 中性元/单位元 l'élément neutre/identité

单位元又叫中性元.设X上的运算$f(x,y) \to x \star y$,若:

$$\forall x \in X, \exists e \in X, e \star x = x$$

称e是左单位元,若:

$$\forall x \in X, \exists e \in X, x \star e = x$$

称e是右单位元,若e同时为左单位元及右单位元,则称e为单位元. 单位元也被记作Id,即identité的前两个字母.或者在很多地方都有自己的记号.

Exemple

$\mathbb{R}$上的加法单位元为0,乘法单位元为1.幂运算$a \star b = a^b$的右单位元为1,没有左单位元.

Exemple

集合X上交集运算的单位元为X,并集运算的单位元为$\varnothing$.

Exemple

设集合$A = \{e, f\}$上的运算为:

$$e \star e = f \star e = e$$
$$f \star f = e \star f = f$$

则e, f都是左单位元.

Proposition:单位元唯一

一个运算如果有单位元,则单位元是唯一的.

Démonstration

$\neg$(单位元是唯一的) $\Rightarrow$ $\exists(e_1, e_2)$都是单位元 $\Rightarrow$ $e_1 \star e_2 = e_1, e_1 \star e_2 = e_2 \Rightarrow e_1 = e_2$

Remarque

一个运算有若干个左单位元是可能的. 事实上,每一个元素都可以是左单位元.同样地,右单位元也一样. 但若同时存在有右单位元和左单位元,则它们会相同且只存在一个单位元.

4.1.5 可逆元/可对称元 Symétrique

设X上的运算$f(x,y) \to x \star y$有单位元e,若:

$$\forall x \in X, \exists x' \in X, x' \star x = e$$

称x'是左可对称的,若:

$$\forall x \in X, \exists x' \in X, x \star x' = e$$

称e是右可对称的.所有满足$x \star x' = x' \star x = e$的$x'$称为$x$的可对称元.使用乘法符号时一般把可对称称为可逆,$x'$记作$x^{-1}$.

4.2 符合结合律的有单位元运算

符合结合律且有单位元的运算具有一些有趣的性质.本节讨论均假设X上满足结合律的运算$f(x,y) \to x \star y$有单位元e.

4.2.1 可对称元唯一性

当且仅当左对称元x'和右对称元x''是唯一且相同时,x是可对称的.

Démonstration

$$x'' = e \star x'' = (x' \star x) \star x'' = x' \star (x \star x'') = x' \star e = x'$$

4.2.2 可对称的运算不变性

若x和y是可对称的,则$x \star y$也可对称,且$(x \star y)' = y' \star x'$.

Démonstration

$$(y' \star x') \star (x \star y) = y' \star (x' \star x) \star y = y' \star e \star y = y' \star y = e$$

反过来同理.

4.2.3 解的唯一性

设a可对称,对于b,仅有唯一一个x使得$a \star x = b$,即$x = a' \star b$.

Démonstration

$$a \star x = b \Rightarrow a' \star b = a' \star (x \star x) = (a' \star x) \star x = e \star x = x$$

反过来同理. 这意味着,例如,在乘法中,形如$ax = b$的方程有且仅有唯一解$x = a^{-1}b$.

4.3 代数结构 Structure Algébrique

在数学中,代数结构由非空集合A和A上的运算集合(通常是二元运算)和一组有限的恒等式(公理)组成,这些运算必须满足这些公理. 研究代数结构的好处在于,当一个新问题涉及与这种代数结构相同的定律时,仅使用结构定律证明的所有结果都可以直接应用于新问题.

Exemple

$\mathbb{R}$上的加法$(\mathbb{R}, +)$就是一个代数结构,其具有以下公理:

- 交换律:$a + b = b + a$.
- 结合律:$(a + b) + c = a + (b + c)$.

- 单位元0: $a+0=0+a=a$.
- 可逆性:$a+(-a)=(-a)+a=0$.

Exemple

回看前言里第?? 节所展现的分析学知识,可见大部分内容都与代数结构相关.

4.3.1 封闭性

当我们想使用一个代数结构,也就是对一个集合上的元素进行运算时,为了得到一些良好的性质或者进行后续的运算, 我们通常希望运算的结果能拥有一些性质.最简单的就是这个结果可以再次被拿来运算.这意味着这个运算结果也属于代数结构的集合. 也即

$$\forall (x,y)\in A\times A, x\star y=z\Rightarrow z\in A$$

这样的性质称为封闭性.

想象一个没有封闭性的代数结构上的运算,比如$\mathbb{R}$上,某个运算结果为:$1\star 4=$西红柿炒鸡蛋. 显然,1和4都在$\mathbb{R}$上,但是西红柿炒鸡蛋不属于$\mathbb{R}$,我们也并不清楚西红柿炒鸡蛋有什么性质,它与$\mathbb{R}$上的元素有什么关系,也不能拿来继续运算.这样的性质就很糟糕.

现在,我希望你假装忘记掉曾经学习的这些运算,也就是第4.1 节开头我提到的那些以前的东西(特别是加法和乘法),以便我们从另一个角度重新出发学习它们.

4.4 群 Groupe

4.4.1 Définition

群是一种代数结构,依托于集合上的运算"$\times$",称为"乘法",记为$(G,\times)$或者$(G,\cdot)$(有时运算符号可省略). 为了避免与笛卡尔积混淆,我们统一采用$(G,\cdot)$记号. 其满足以下公理:

- 封闭性:$\forall(a,b)\in G^2, a\cdot b=c\in G$.
- 结合律:$\forall(a,b,c)\in G^3, (a\cdot b)\cdot c=a\cdot(b\cdot c)$.
- 单位元e: $\forall a\in G, \exists e\in G, a\cdot e=e\cdot a=a$.
- 可逆性: $\forall a\in G, \exists a^{-1}\in G, a\cdot a^{-1}=a^{-1}\cdot a=e$.
- **Bonus:**交换律:$\forall(a,b)\in G^2, a\cdot b=b\cdot a$.

满足前四项公理的代数结构称为群.额外满足第五项交换律的群称为"阿贝尔群(Groupe Abélien)".

Exemple

- 整数的通常意义加法$(\mathbb{Z},+)$构成群,但是通常意义乘法$(\mathbb{Z},\cdot)$不构成群,因为不满足有可逆元.
- (n阶非奇异矩阵[1],矩阵乘法)是一个群.

4.4.2 阶 Ordre

在有限群范围内,群$(G,\cdot)$的阶等于集合G里元素的个数,也就是$|G|=\text{card } G$. 元素的阶等于让该元素通过幂运算得到单位元的最小幂,也就是$n_{min}, a^n=e$.

[1]万一你还没学过这个定义,它意味着矩阵的行列式值不等于0.

4.4.3 乘法表 Table de multiplication

乘法表常被用来表示简单的群上的元素和运算,它列举了群内任意两个元素的乘积.下面我们通过一个简单的例子来理解乘法表.

C_3群

想象一个等边三角形ΔABC,我们将它绕着垂直于几何中心的州进行旋转操作：

- 操作a:顺时针旋转120°
- 操作b:逆时针旋转120°
- 操作e:不旋转

我们发现,经过操作a后,原来的A点变成了B点,B点变成了C点,C点变成了A点,得到了三角形ΔBCA. 而与此同时,经过两次操作b后也能让原来的A点变成了B点,B点变成了C点,C点变成了A点.也就是说,两次操作b与一次操作a等价.同理,两次操作a与一次操作b等价. 进一步地,我们发现,三次操作a、三次操作b、操作b后操作a、操作a后操作b与操作e相互都是等价的.如果我们把操作看作一个集合,操作的复合看作运算·,就得到了一个群.其中的运算关系如下:

- $a = b \cdot b = a \cdot e$
- $b = a \cdot a = b \cdot e$
- $e = e \cdot e = a \cdot a \cdot a = b \cdot b \cdot b = a \cdot b = b \cdot a$

这个群被称为C_3群.其阶数为3,元素a和b的阶数也是3. 将这些运算关系组合成一个表,第一行表示在运算符号前的元素,第一列表示运算符号后的元素,就可以填入所有的运算结果.也即:

$(C_3,\cdot)$	**a**	**b**	**e**
a	b	e	a
b	e	a	b
e	a	b	e

表 4.1: C_3群的乘法表

4.4.4 重排定理 Théorème de réarrangement

考虑代数结构$(A,\star)$,对$a\in A$,定义$a\star A=\{a\star a_\alpha|a_\alpha\in A\}$.对群$G$,有:

$$\forall a\in G, a\cdot G=G\cdot a=G$$

也即群内的每个元素和某个元素相乘得到的仍然是原来的群,这被称为群的重排定理.

Démonstration

由运算的封闭性知$a\cdot G\subseteq G$, 由可逆性知$\forall(a,g)\in G\times G,\exists(a'\cdot g)\in G$使得$g=a\cdot(a'\cdot g)=g\Rightarrow g\in a\cdot G\Rightarrow G\subseteq a\cdot G$.

4.4.5 生成元 Générateur

生成元是描述一个群的重要方式.下面我们由循环群开始逐渐介绍生成元和其应用方法.

循环群 Groupe cyclique

由一个元素R及其幂次构成的有限群称为由R生成的循环群,记为C_n,其中n为循环群的阶,R称为循环群的生成元. 这就是为什么第4.4.3 节介绍的群叫C_3群.在C_3群中,a和b都是其生成元.对于n阶循环群, 其阶数等于其生成元的阶数.

有限群的生成元与秩 Générateur et rang d'un groupe fini

对任一有限群, 是否同样有生成元呢?答案是肯定的,由此还能引出有限群的秩的概念.对有限群G,任取一元素R_1,得到其幂次构成的集合$\mathbf{R_1}$. 若${\mathbf{R_1}}^C \neq \varnothing$,即无法填满整个群,则在${\mathbf{R_1}}^C$内任取一元素$R_2$并得到$\mathbf{R_2}$,以此类推. 将选取的元素组成集合$\{R_i\}$,该集合即为群$G$的生成元,且$\mathrm{card}\{R_i\}$称为群的秩.

Proposition

有限群的生成元的选择不唯一,但秩不变.

4.5 从原群到群 De magma à groupe

一个代数结构想成为群需要符合四个条件,那不能全部符合四个条件的代数结构又是什么呢?

4.5.1 原群 Magma

对代数结构$(E, \star)$,若其运算满足封闭性,则该代数结构为一个原群.

4.5.2 半群 Demi-groupe

对原群$(E, \star)$,若其运算满足结合律,则该原群为一个半群.

4.5.3 幺半群 Monoïde

对半群$(E, \star)$,若其含有中性元,则该半群为一个幺半群.

4.5.4 拟群 Quasigroupe

对原群$(E,\star)$,若有:

$$\forall(a,b)\in E\times E,\exists(x,y)\in E\times E\text{使得}a\star x=y\star a=b$$

则该原群为一个拟群.

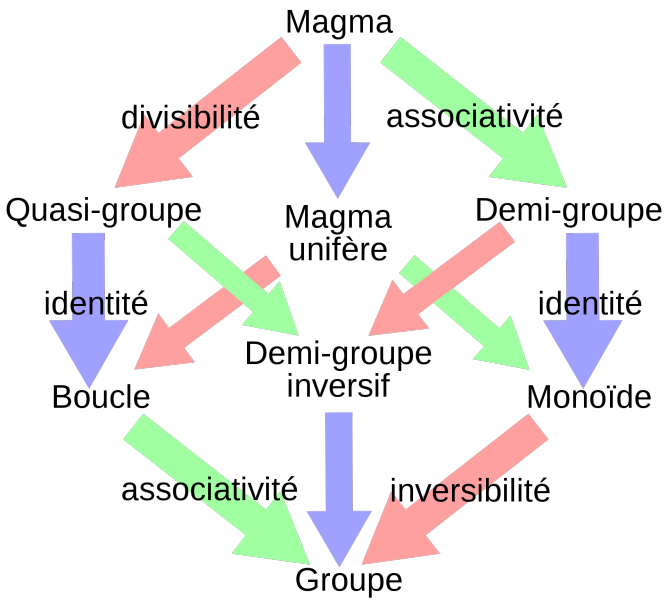

图 4.1: 从原群到群(图源wiki)

4.6 群论基础 La Théorie Rudimentaire des Groupes

在数学中,特别是在一般代数中,群论是研究群的代数结构的学科.群论的发展起源于数论、代数方程理论和几何学,在理论物理、化学、材料科学和非对称密码学中有多种应用. 本章只对群论内容做一个基础的、入门的介绍.事实上,关于群、环和域相关的知识在本讲义中并不怎么重要,很多结论也不会有后续应用(所

以有相当多平凡的推论我没有写出证明,摸了).但是有些概念和定义还是会用上的,因此我还是简单地列出来.

4.6.1 共轭关系 Conjugaison

定义二元关系 为:对$(a,b) \in G \times G, \exists g \in G$使得$b = g^{-1} \cdot a \cdot g$.称该关系为共轭关系,a b为a与b共轭.

Proposition

共轭关系是等价关系.

Démonstration

- $a = a^{-1} \cdot a \cdot a \Rightarrow a \sim a$
- $a \sim b \Rightarrow b = g^{-1} \cdot a \cdot g \Rightarrow g \cdot b \cdot g^{-1} = a \Rightarrow a = (g^{-1})^{-1} \cdot b \cdot g^{-1} \Rightarrow b \sim a$
- $b = g^{-1} \cdot a \cdot g, c = f^{-1} \cdot a \cdot f \Rightarrow b = f \cdot c \cdot f^{-1} = g^{-1} \cdot a \cdot g \Rightarrow c = (f^{-1} \cdot g^{-1}) \cdot a \cdot (g \cdot f) \Rightarrow c \sim a$

共轭类 Action par conjugaison

a的共轭类是群内所有与其共轭的元素组成的集合,记为$Cl(a)$或C_a,即$Cl(a) = \{g \cdot a \cdot g^{-1} | g \in G\}$.

接下来给出一些共轭类的简单推论:

Proposition

$a \sim b \Leftrightarrow Cl(a) \cap Cl(b) \neq \varnothing$

Proposition

共轭类内元素的阶相同.

Proposition

单位元e只与自己共轭.

Proposition

Abel群里每个元素只与自己共轭.

Proposition

$a \sim b \Rightarrow \forall k \in \mathbb{N}, a^k \sim b^k$.

4.6.2 子群 Sous-groupe

直观上说,子群就是群的一个同样是群的子集.

Définition

对群$(G, \cdot)$,若$H \subseteq G$使得$(H, \cdot)$也是一个群,则称H是G的子群.

Proposition

G和$\{e\}$显然都是子群.它们被称为平凡子群(sous-groupe trivial)或者 sous-groupe impropre. 不是平凡子群的子群称为特征子群(sous-groupe propre).

Remarque

质数阶(或者1阶)循环群没有特征子群.

Proposition

对于pq阶循环群(p, q为正整数),其只有一个p阶子群.该子群是由g^q生成的循环群.

4.6.3 陪集 Classe suivant un sous-groupe

法语里并没有专门的陪集的专有名词,而是直接叫classe suivant un sous-groupe,这是个很形象的说法.英语称陪集为coset,其实也和suivant有异曲同工之妙吧.

Définition

群$(G, \cdot)$有子群H.对任意$g \in G$,H有如下两个陪集:

- 左陪集(classe à gauche de g suivant H): $gH = \{g \cdot h | h \in H\}$
- 右陪集(classe à gauche de g suivant H): $Hg = \{h \cdot g | h \in H\}$

陪集分解 Décomposition en classes suivant un sous-groupe

群G可以被分解成若干个左陪集的并,或者若干个右陪集的并.对应的分解称为左/右陪集分解.即:

$$G = \bigcup_{\alpha \in G} \alpha H = \bigcup_{\alpha \in G} H\alpha$$

Proposition

$f \in gH \Leftrightarrow fH = gH, f \in Hg \Leftrightarrow Hf = Hg.$

Proposition

$gH = H \Leftrightarrow g \in H \Leftrightarrow Hg = H.$

Proposition

$|gH| = |H|$

Proposition

“属于同一左陪集”是一个等价关系.

Proposition

任意两个左陪集要么不相交要么相等.

4.6.4 群论的Lagrange定理 Théorème de Lagrange

Lagrange定理的直接叙述为:子群的阶整除群的阶,即:若群$(G, \cdot)$有子群H,则$|G| = k|H|, k \in \mathbb{N}$. 将其倍数$k$记为$[G : H]$,表示$H$在$G$中左陪集的个数.

Démonstration

考虑子群H关于G内所有元素的左陪集组成的集族$\mathbb{H} = \{g_i H | g_i \in G\}$, 每个左陪集的阶都相同,$|g_k H|$并且$\sum_i^{\text{card } \mathbb{H}} |g_i H| = |G|$ 此时card $\mathbb{H}$就是$[G : H]$.

Proposition

素数阶的群只有平凡子群,没有特征子群.

Proposition

元素的阶整除群的阶.(元素的阶可以组成子群)

Fermat小定理 Théorème de Fermat

对整数a和素数p,若a不是p的倍数,则$a^p - 1$是p的倍数,即:

$$a^{p-1} \equiv 1(\mod p)$$

Démonstration

为了证明这个推论,我们考虑$G = \{1, 2, \ldots, p-1\}$和模运算组成的群.假设$a \equiv b(\mod p)$,显然$b \in G$. 设$b$的阶数为$k$,即$b^k \equiv 1(\mod p)$,则可得到子群$H = \{a, b, \ldots, b^{k-1}\}$则$k$可以整除$G$的阶数,也就是$p-1$. 此时再设$p-1 = km$,此时有:

$$a^{p-1} \equiv b^{km} \equiv (b^k)^m \equiv 1^m \equiv 1(\mod p)$$

得证.

4.6.5 正规子群 Sous-groupe normal

正规子(Sous-groupe normal) 又叫不变子群(Sous-groupe invariant),法语里还有称Sous-groupe distingué.其代表共轭变换下不变的子群.

Définition

对群$(G, \cdot)$,若子群N满足:

$$\forall n \in N, \forall g \in G, g \cdot n \cdot g^{-1} \in N$$

则称N是G的正规子群,记作$N \lhd G$或者$N \trianglelefteq G$.

等价条件

下列条件等价于子群N在G中是正规子群:

- $\forall g \in G, gNg^{-1} \subseteq N$
- $\forall g \in G, gN = Ng$
- $\forall (g, h) \in G \times G, gh \in N \Leftrightarrow hg \in N$

4.6.6 商群 Groupe quotient

子群的乘法

设群$(G,\cdot)$有子群H和F,定义其乘法为:

$$H \cdot F = \{h \cdot f | (h,f) \in G \times F\}$$

Définition

利用正规子群的左陪集和右陪集相同的这个特点将群按照陪集的方法进行分割. 分割后的所有陪集形成的集合能够形成一个新的群,称之为商群,记为G/H.也即:

$$G/H = \{gH \ | H \lhd G, g \in G\}$$

Démonstration

- 单位元: $aH = H = Ha$
- 逆元: $aH \cdot a^{-1}H = aa^{-1}HH = H$
- 结合律: $aH \cdot bH \cdot cH = (ab)cH = a(bc)H = aH \cdot (bH \cdot cH)$
- 封闭性: $aH \cdot bH = (ab)H \in G/H$

Proposition

$|G/H| = [G:H]$,商群的阶是群的阶除以子群的阶的商.

Proposition

若$(G,\cdot)$是Abel群/循环群/有限生成群,则G/H也是.

4.6.7 同态 Homomorphisme

Définition

同态是两个群之间的一种特殊的映射,其概念非常直观.“同”表示映射的两端有什么东西是一样的,或者不变的.“态”就是群的某种“状态”. 群只有集合和运算两个要素,集合映射过去后不可能保持不变,那能保持的也就只有运算了.因此,同态就是两个群之间保持乘法运算的映射,即对于$(G,\cdot)$和$(H,\star)$上的映射$f:G\to H$,若

$$\forall(x,y)\in G\times G, f(x\cdot y)=f(x)\star f(y)$$

称f是$(G,\cdot)$和$(H,\star)$上的同态映射.存在同态映射的两个群是同态的.若同态是单射,则称单同态(Monomorphisme),若为满射则称满同态(Épimorphisme).

Exemple

正实数上通常加法群到通常乘法群上的映射$f(x)=e^x$就是一个同态.$e^{a+b}=e^a\cdot e^b$.

Proposition

同态的一个重要性质是保证了单位元映射到单位元,$f(e_G)=e_H$.

自同态 Endomorphisme

群$(G,\cdot)$到自身上的同态映射称为自同态.

态射 Morphisme

同态的推广被称为态射.在讨论群的内容时,法语有时直接用态射指代同态,记住两者在此时是同一概念.

4.6.8 同构 Isomorphisme

若同态映射f为双射,则称为同构映射,两个群是同构的,记作$G \cong H$.

Proposition

同构是等价关系.

自同构 Automorphisme

同理,群$(G, \cdot)$到自身上的同构映射称为自同构.

Remarque: 同构与相等

一般来说,如果忽略掉同构的对象的属性或操作的具体定义,单从结构上讲,同构的对象是完全等价的. 但这并不意味着同构就是相等.例如,我们很容易知道C_3群可以和某个群{西红柿炒鸡蛋,醋溜土豆丝,糖醋排骨}同构(例如 $f(a) =$ 西红柿炒鸡蛋, $f(b) =$ 醋溜土豆丝, $f(e) =$ 糖醋排骨), 但这并不代表两个群,或者两个集合就是相等的.起码西红柿炒鸡蛋不在C_3群里面.

4.6.9 核 Noyau

Définition

对于同态$f : G \to H$, G中映射到H单位元的元素称为同态的核,记作:

$$\ker f = \{f(g) = e_H \mid g \in G\}$$

Proposition

$\ker f \lhd G$,核是正规子群.

Proposition

$G/\ker f \cong H$,核的商群与H同构.

其实到这里我想接着讲同构基本定理的, 但是这一章内容太多了,而且毕竟不是写代数讲义,因此我们点到为止,快速过完这一章的内容.

4.7 环 Anneau

4.7.1 Définition

与群类似,环也是一种代数结构,依托于集合上的运算“+”和“×”,分别被称为“加法”和“乘法”.同样将乘法符号记为$\cdot$, 则一个环写作$(R,+,\cdot)$.其满足以下公理:

1.$(R,+)$是Abel群,即:

- 封闭性:$\forall (a,b)\in R^2, a+b=c\in R$.
- 结合律:$\forall (a,b,c)\in R^3, (a+b)+c=a+(b+c)$.
- 单位元0: $\forall a\in R, \exists 0\in R, a+0=0+a=a$.
- 可逆性: $\forall a\in R, \exists -a\in R, a+(-a)=(-a)+a=0$.有时将此类运算用减法符号代替,即$a+(-b)=a-b$,这样就熟悉多了.
- 交换律:$\forall (a,b)\in R^2, a+b=b+a$.

2.$(R,\cdot)$是幺半群,即:

- 封闭性:$\forall (a,b)\in R^2, a\cdot b=c\in R$.
- 结合律:$\forall (a,b,c)\in R^3, (a\cdot b)\cdot c=a\cdot (b\cdot c)$.

- 单位元1: $\forall a \in R, \exists 1 \in R, a \cdot 1 = 1 \cdot a = a$.

3.乘法对于加法满足分配律,即:

- 左分配:$\forall (a,b,c) \in R^3, a \cdot (b+c) = (a \cdot b) + (a \cdot c)$.
- 右分配:$\forall (a,b,c) \in R^3, (b+c) \cdot a = (b \cdot a) + (c \cdot a)$.

值得注意的是,在1960年代以前,多数抽象代数的书籍并不将乘法单位元列入环的必要条件中; 而1960年代后的书籍则更倾向将乘法单位元列入环的必要条件中. 那些不要求乘法单位元为环的必要条件的作者可能会把包含乘法单位元的环给称为“单位环(Anneau Unitaire/Unifère)”, 与之相对地,那些要求乘法单位元为环的必要条件的作者,可能会把不包含乘法单位元的环给称为“伪环(Pseudo-anneau,Rng)”.

Exemple

实数上的通常加法和乘法可以构成很多环,如$(\mathbb{R}, +, \times), (\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times)$都是环,并且乘法也是可交换的.与群一样,如果乘法满足交换律则称为*Abel*环.

Exemple: 多项式环

所有形如$P(X) = \sum_{i=0}^{n} a_i X_i$的多项式可以构成一个环.这要求$a_i$必须是某个环$R$上的元素,而$X$视作一个变量的形式符号.

Exemple: 矩阵环

所有$n \times n$阶的矩阵可以和矩阵加法/矩阵乘法构成一个环.例如$\mathcal{M}_n(\mathbb{R})$.

4.7.2 环的性质

4.7.3 特殊的环

整环 Anneau Intègre

设$(R,+,\cdot)$是一个交换环且加法和乘法的单位元不相同$(1 \neq 0)$.若满足:

$$\forall (a,b) \in A^2, a \cdot b = o \Rightarrow a = 0 \text{或} b = 0$$

则称该环是一个整环.

唯一分解环 Anneau Factoriel,UFD

对一个整环$(R,+,\cdot)$,如果其中的每个元素都可以表示为一个可逆元和若干个不可约元素的乘积,即:

$$\forall x \in R, \exists (u, p_1, \ldots, p_n) \in R^{n+1}, n \in \mathbb{N}, x = u \cdot p_1 \cdot \ldots \cdot p_n$$

并且

$$x = u \cdot p_1 \cdot \ldots \cdot p_n = v \cdot q_1 \cdot \ldots \cdot q_m \Rightarrow n = m$$

则称该环是一个唯一分解环.

主理想 Idéal Principal

若某环$(R,+,\cdot)$的子集I为在原环加法的定义下的子群$(I,+)$,且其中的元素在原环乘法下与任意原环中的元素结果都在该子群中,则称其为原环的理想(Idéal).即满足:

- 左理想: $\forall (i,r) \in I \times R, i \cdot r \in I$
- 右理想: $\forall (i,r) \in I \times R, r \cdot i \in I$

每个理想均可由单个元素生成的环称为主理想环.

4.8 域 Corps

4.8.1 Définition

域是一种特殊的环,和一般的环的区别在于域要求它的非零元素可以进行除法运算,这等于说每个非零的元素都要有乘法逆元.域中的运算关于乘法是可交换的. 在域上我们有了熟悉的四则运算的表示(是的,我们终于学到了小学数学的内容,多么伟大!):

- $a + (-b) = a - b$
- $a \cdot b^{-1} = a/b$

Exemple

域可以说是我们最熟悉的代数结构了.实数域$(\mathbb{R}, +, \cdot)$,复数域$(\mathbb{C}, +, \cdot)$,有理数域$(\mathbb{Q}, +, \cdot)$是最常见的域.

Exemple

一个域的元素如果是有限个,则被称为有限域.例如最小的有限域Boole值域只含有元素$0, 1$. 其满足加法$0 + 0 = 0, 1 + 0 = 1, 1 + 1 = 0$和乘法$0 \cdot 0 = 0, 0 \cdot 1 = 0, 1 \cdot 1 = 1$.

4.8.2 域的性质

非零元素的集合

域$\mathbb{K}$上所有非零元素构成的集合$\mathbb{K}^x$是一个关于乘法的Abel群,其每个有限子群都是循环群.

特征 Caractéristique

若存在$n \in \mathbb{N}$使得$n \cdot 1 = 0$,则称最小的n为域的特征.$n = 0$表示特征不存在.

有序域 Corps Ordonné

若可以在域$\mathbb{K}$上定义序关系,则称该域是一个有序域.例如有理数域和实数域上具有通常的序关系.

交换环的理想

一个交换环是域当且仅当它的理想只有自身和零理想.

关于群、环和域的更多内容将在代数课程中详细展开.

第五章　从自然数到有理数
Des nombres naturels aux nombres rationnels

5.1　自然数集的公理化 Axiomatique de l'ensemble des nombres naturels

5.1.1　Peano公理 Axiome de Peano

关于自然数,每个人都知道,就是$\mathbb{N} = \{1, 2, 3, \dots\}$.但这显然不是一个好的定义,因为这样的定义并不清楚自然数的性质. 比如说,3后面是什么数?114在哪里?它和前后的数有什么关系?于是,我们需要对自然数进行公理化. 这部分工作主要是在十九世纪后半叶由意大利数学家Giuseppe Peano在德国数学家Richard Dedekind的工作上完善得到的,因此被称为Peano公理:

设集合X和集合上的映射$\mathcal{S}$,若满足:

1. $x \in X$
2. $x \notin \mathcal{S}(X)$
3. $\mathcal{S}$是一个单射

4. [1]对于$A \subseteq X$,若$x \in A$且$\forall a \in A$, $\mathcal{S}(a) \in A$,则$A = X$

则称X是自然数集$\mathbb{N}$,其元素称为自然数.x称为初始元素,$\mathcal{S}$称为后继映射,$\mathcal{S}(x)$称为x的后继元素. 此时可以认为:

$$\mathbb{N} = \{x, \mathcal{S}(x), \mathcal{S}^2(x), \dots, \mathcal{S}^n(x), \dots\}$$

在通常意义下,认为$x = 0$,即:

$$\mathbb{N} = \{0, 1, 2, \dots, n, \dots\}$$

对于不含0的自然数集,则称为正整数集$\mathbb{N}^*$.

5.1.2 自然数集中的加法运算 Addition dans l'ensemble des nombres naturels

根据自然数集的特点, 可以分两步“归纳地” 定义自然数的加法. 首先定义任一自然数和初始元的加法规则,然后假定已经知道了任一自然数与n的加法规则, 在此假定下规定任一自然数与n的后继元的加法规则. 由数学归纳原理可知,这样就定义了任意两个自然数的加法规则. 也就是:

$$\begin{aligned} \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (n, m) &\longmapsto n + m \end{aligned}$$

该映射满足:

$$\begin{cases} n + 1 = \mathcal{S}(n) \\ n + \mathcal{S}(m) = \mathcal{S}(n + m) \end{cases}$$

则称该映射为加法.显然有$\mathcal{S}^n(a) = a + n$.

[1]即数学归纳公理

关于加法的一些结论

以下是一些简单的关于加法的结论.其证明过程都非常简单,基本上就是利用归纳法先证明某个数为0的情况,然后一步步加上去即可.故为了节省篇幅,我直接给出结论.

1. 交换律:$\forall (a,b) \in \mathbb{N}^2, a+b=b+a$
2. 结合律:$\forall (a,b,c) \in \mathbb{N}^3, (a+b)+c=a+(b+c)$
3. 消除律:$\forall (a,b,c) \in \mathbb{N}^3, a+b=a+c \Leftrightarrow b=c$
4. $\forall b \in \mathbb{N}^*, \exists a \in \mathbb{N}, \mathcal{S}(a)=b$
5. $\forall a \in \mathbb{N}^*, \forall b \in \mathbb{N}, a+b \in \mathbb{N}^*$
6. $a,b \in \mathbb{N}$且$a+b=0 \Leftrightarrow a=b=0$

5.2 自然数集上的序关系 Relations d'ordre sur l'ensemble des nombres naturels

5.3 整数集的构造 Construction de l'ensemble des nombres entiers

5.4 整数集中的运算 Opérations dans l'ensemble des nombres entiers

5.5 整数集上的序关系 Relations d'ordre sur l'ensemble des nombres entiers

5.6 有理数集的构造 Construction de l'ensemble des nombres rationnels

5.7 数域 Corps

5.8 有理数域上的序关系 Relations d'ordre sur l'ensemble des nombres rationnels

第六章　实数
Nombres Reéls

6.1　实数域的构造 Construction de l'ensemble des nombres réels

6.2　Dedekind分割 Coupure de Dedekind

6.3　实数集上的序关系 Relations d'ordre sur l'ensemble des nombres réels

6.4　实数域的完备性 Complétude de l'ensemble des nombres réels

第七章　可数性

Dénoembrabilité

本章将研究两种不同类型的无限集：可数集和不可数集,并阐明什么是可数,什么不可数.

7.1　基数 La cardinalité

7.1.1　Définition

定义关系$\sim$.基数指集合中元素的个数,又叫势 [1]. 对于集合A和B,若当且仅当存在双射$f : A \to B$时,称$A \sim B$,即A和B拥有相同的基数.

7.1.2　有限集 Finite

设集合A,若$A = \varnothing$或者$\exists n \in \mathbb{N}^*$, $A \sim \{1, 2, \ldots, n\}$,则称$A$是有限集.

Proposition

对有限集A和B,$\mathrm{card}A = \mathrm{card}B \Leftrightarrow A \sim B$.

[1]在某些语境下,势的概念只用于比较两个无穷集的元素多寡,而不能直接指称某集合的元素个数.在一般语境下,尤其是当一切都定义好了以后,也经常使用势作为基数的同义词

Démonstration

⇒:
设$A=\{a_1,a_2,\ldots,a_n\},B=\{b_1,b_2,\ldots,b_n\}$有双射$f:a_i\to b_i\Rightarrow A\sim B$

⇐:
1.$\forall x\in A,\exists y\in B$,使得$f(x)=y\Rightarrow \mathrm{card}A\leq \mathrm{card}B$
2.$\forall y\in B,\exists x\in A$,使得$f^{-1}(y)=x\Rightarrow \mathrm{card}B\leq \mathrm{card}A$
$\Rightarrow \mathrm{card}A=\mathrm{card}B$

7.1.3 Proposition

势是等价关系.

Démonstration

1.$A\sim A:\forall x\in A,f:x\to x$即为所求双射.
2.$A\sim B\Rightarrow B\sim A:f^{-1}$即为所求双射.
3,$A\sim B,B\sim C\Rightarrow A\sim C:f:x\to y,g:y\to z,f\circ g$即为所求双射.

7.2 可数性 Dénoembrabilité

可数性的定义非常贴近生活.想一想,平时你怎么计数?比如数一数本讲义共有几章呢?1,2,3,4,... 计数的记号显然属于自然数集合$\mathbb{N}$.于是很自然地,我们认为一个集合如果能用自然数这样一个一个数出来,就说明它是可数的.

7.2.1 Définition

- 对集合A,若$A\sim\mathbb{N}$称它是可数的(dénoembrable).

- 若集合A有限或可数,称A是至多可数的(au plus dénoembrable).
- 若集合A无限且不可数,称A是不可数的(indénombrable).

可数集的基数

可数集的基数定义为$\aleph_0$.

7.2.2 Exemple

$\mathbb{Z}$是可数的.我们可以找到双射$f:\mathbb{N}\to\mathbb{Z}$:

$$f(n)=\begin{cases}\frac{n}{2} & n=2k\\ \frac{1-n}{2} & n=2k+1\end{cases}$$

7.2.3 Proposition

若$A\sim B$则A,B同属于"有限""无限可数""不可数"三种类型之一.

Démonstration

1.有限:见 第7.1.2 节

2.无限可数:$A\sim\mathbb{N}$,由等价关系(第7.1.3 节)可知$\mathbb{N}\sim A\Rightarrow\mathbb{N}\sim B$则$B$无限可数.

3.无限不可数:$\neg(B$可数$)\Rightarrow\mathbb{N}\sim B\Rightarrow\mathbb{N}\sim A\Rightarrow\perp$故$B$不可数.

需注意:逆命题对3不成立.两个不可数集不一定能一一对应.

7.3 无限集的可数性 Dénoembrabilité des ensembles infinis

7.3.1 Définition

无限集是指至少与他的一个真子集的势相同的集合.对集合A,若：

$$\exists B \subset A, B \sim A$$

称A是一个无限集.

7.3.2 Exemple

设S是区间$(0,1)$上所有元素的集合,则S是不可数集.

那么,如何证明S是不可数集？如果S是不可数集,那么当我们选取S的一个可数子集E时,S中应该还有一些不包含在 E 中的元素,对吧？也就是

$$\forall E \subset S, E \sim \mathbb{N} \Rightarrow \exists x \in S, x \notin E$$

因此,如果我们可以证明S的每个可数子集都是一个真子集,那么S就是不可数集.这是因为如果S的每个可数子集都是一个真子集并且S是可数集,那么S本身就是它自己的一个真子集,这是不可能的！这基本上意味着无论我们如何计数S中的元素,总会有一些元素被漏掉.

Démonstration

这里我们用到了著名的Cantor对角线法.我们把每个S中的元素都用一个无限小数表示出来 [2],形如$0.d_1d_2d_3d_4\ldots$. 现在尝试选出可数集E,排列成:

$$\begin{aligned}
e_1 &= 0.d_{1,1}d_{1,2}d_{1,3}d_{1,4}\ldots \\
e_2 &= 0.d_{2,1}d_{2,2}d_{2,3}d_{2,4}\ldots \\
e_3 &= 0.d_{3,1}d_{3,2}d_{3,3}d_{3,4}\ldots \\
e_4 &= 0.d_{4,1}d_{4,2}d_{4,3}d_{4,4}\ldots \\
e_5 &= 0.d_{5,1}d_{5,2}d_{5,3}d_{5,4}\ldots \\
&\vdots
\end{aligned}$$

那么这个任意的E包含了S中的所有元素吗？错！我们可以找到这样一个数

$$s = s_1s_2s_3s_4\ldots \text{使得} s_i \neq d_{i,i}$$

这意味着s与第1个数的第1位小数不一样,与第2个数的第2位小数不一样,与第3个数的第3位小数不一样... 也就是与E中每个数都不一样,显然不属于E. 这里构造s的方法沿着上面那个有点像矩阵一样的东西的对角线一直走下去,所以叫对角线. 该方法由集合论的创始人康托尔(Cantor)提出,故称为Cantor对角线法.

7.3.3 可数集的笛卡尔积 Countable Union of Countable Sets

设n个可数集$C_1, C_2, \ldots, C_n$,则其笛卡尔积$C_1 \times C_2 \times \cdots \times C_n$是可数的.

7.3.4 可数子集

任意无限集S都有可数子集.

Démonstration

先取一个a_1,取完后剩下的集合不是空集,故可以以此类推一直取下去.

[2]我们不加证明地认为每个实数都可以写成一个无限小数

7.3.5 最小基数 Cardinalité minimale

无限集的最小基数是$\aleph_0$.

Démonstration

利用反证法,设无限集A有$\mathrm{card}A < \aleph_0$,则存在一个可数子集$A_1 \sim \mathbb{N}$.即:

$$\aleph_0 = \mathrm{card}A_1 \leq \mathrm{card}A < \aleph_0$$

故矛盾.

7.3.6 子集可数关系

设$E \subseteq A$,则有:
A至多可数 $\Rightarrow$ E至多可数
E不可数 $\Rightarrow$ A不可数

7.3.7 Proposition:可数集可数并可数

考虑可数个集合E_i:

$$E_i \sim \mathbb{N}, S = \bigcup_{i=1}^{\infty} E_i \Rightarrow S \sim \mathbb{N}$$

Démonstration

有点复杂,哪天想起来再慢慢画.

Remarque

对于可数集的不可数并,这个结果是错误的.

Proposition

可数集任意可数并可数.

Proposition

$\mathbb{R}$不可数.

7.3.8 Proposition:可数集元组可数

设A是可数集,A^n是由A中元素构成的全体n元组的集合,那么A^n是可数的.

Démonstration

数学归纳法,先证明A^1可数,再假设A^{i+1}可数,得出A^n是可数集的可数并,于是A^n至多可数. 详细证明留给读者.

7.3.9 Proposition:有理数集可数

一个简化的证明过程:我们知道任何有理数都可以写成$\frac{p}{q}, (p,q) \in \mathbb{Z}^2$的形式,并且第7.2.2 节告诉我们$\mathbb{Z}$是可数的,第7.3.8 节告诉我们$\mathbb{Z}^2$是可数的. 显然$\mathbb{Z}^2$的一个子集可以与$\mathbb{Q}$构造双射,所以$\mathbb{Q}$是可数的.

7.3.10 Proposition:无理数集不可数

一个简单的证明过程:我们知道$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$,且$\mathbb{Q}$是可数的. 若$\mathbb{I}$是至多可数的,则根据第7.3.7 节可知$\mathbb{R}$是至多可数的,这显然矛盾. 故$\mathbb{I}$是不可数的.

7.3.11 Cantor-Bernstein定理 Théorème de Cantor-Bernstein

设A, B是两个集合,$A_1 \subset A$, $B_1 \subset B$, 若存在双射$f : A \to B_1, g : B \to A_1$,则$A \sim B$.

7.4 代数数和超越数 Nombres algébriques et nombres transcendants

7.4.1 Définition

对实数x,若其满足多项式方程:

$$\sum_{i=0}^{n} a_i x^{n-i} = 0$$

其中$a_0 \in \mathbb{Z}^*$, $a_1, \ldots, a_n \in \mathbb{Z}$,则称$x$是一个代数数(nombre algébrique).否则,称x是一个超越数(nombre transcendant).

7.4.2 Proposition

由代数数全体组成的集合是可数的.

Démonstration

本节内容待补充.

7.5 连续统 Continuum

7.5.1 Définition

对集合A,若$A \sim \mathbb{R}$,则称A是连续统. 连续统的基数称为连续基数或连续统势(cardinal du continuum),记作$\aleph_1$或$\mathfrak{c}$.

7.5.2 Exemple

- $\mathbb{R}$上的任一区间是连续统.
- 全体超越数组成的集合是连续统.

- 平面上的点集是连续统.

7.5.3 Cantor定理 Théorème de Cantor

设非空集合A,则A的幂集$\mathcal{P}(A)$的基数大于A的基数,也即:

$$\mathrm{card}A < \mathrm{card}\mathcal{P}(A)$$

Démonstration

A是有限集时显然成立.设$A = \{a_I\}$是无限集,假设$\mathrm{card}A = \mathrm{card}\mathcal{P}(A)$,则存在双射$f : A \to \mathcal{P}(A)$. 设$B = \{a_I \in A \,|\, a_I \notin f(a_I)\}$.显然$B \in \mathcal{P}(A)$,但不存在$f(a_\lambda) = B$,故$f$不是满射,矛盾.

Proposition

Cantor定理表明,不存在最大的基数.因为对于任意集合A,总有基数更大的集合$\mathcal{P}(A)$.

7.5.4 可数集幂集的势

可数集幂集的势等于连续基数.

$$\mathrm{card}\mathcal{P}(\mathbb{N}) = 2^{\aleph_0} = \aleph_1$$

Démonstration

设集合$A = \{0, 1\}$, $J = A^\infty$.考虑映射:

$$\begin{aligned} f : \mathcal{P}(\mathbb{N}) &\to J \\ E &\to (a_1, a_2, \dots) \end{aligned}$$

其中

$$a_i = \begin{cases} 1 & i \in E \\ 0 & i \notin E \end{cases}$$

f是单射.由映射的关系知道$\forall \alpha = (a_1, a_2, \dots), \exists! E \in \mathcal{P}(\mathbb{N}), f(E) = \alpha$. 故$f$是双射.有

$$\mathrm{card}\mathcal{P}(\mathbb{N}) = \mathrm{card}J = 2^{\aleph_0} = \aleph_1$$

7.5.5 连续统假设 Hypothèse du continu

1874年Cantor提出了连续统假设,即不存在基数介于$\aleph_0$和$\mathfrak{c}$之间的集合. 1940年Kurt Friedrich Gödel证明了连续统假设和集合的ZFC公理系统不矛盾,即ZFC 理系统无法证伪连续统假设. 1963年Cohen进一步证明连续统假设无法被ZFC公理系统证明.

第八章　复数与Euclide空间

Nombre Complexe et Espace Euclidien

第九章　初等数论
Théorie Élémentaire des Nombres

9.1　素数和最大公因子 Nombres premiers et Plus Grand Commun Diviseur

9.2　同余 Congruence

9.3　乘性函数 Fonction Multiplicative

9.4　原根 Racine Primitive

9.5　二次剩余 Quadratic Residue

9.6　Gauss整数 Gauss Entier