离散数学课程笔记

AUGPath

2023 年 3 月 8 日

第一章　集合论和简单数理逻辑

1.1　数理逻辑

1.1.1　命题

从高中开始, 我们似乎就开始处理各种各样的命题. 下面我们加一层抽象, 这样, 我们就可以把一些繁琐的内容交给计算机完成, 并且在探索的过程中对 “什么是有效的推理” 有一个更深的理解.

定义 1.1.1 (命题 (Proposition))**. 命题**是可以判定真假的陈述句 (不可既真又假).

1.1.2　命题逻辑

命题逻辑的语言

所以, 要完成这项任务, 第一步就是尽可能地形式化的描述一下这些一直在用的语言.

定义 1.1.2 (命题逻辑的语言)**.** 命题逻辑的语言有且仅有如下的内容构成:

- 任意多的命题符号
- 5 个逻辑连接词 (见下表1.1.2)
- 左括号, 右括号

定义 1.1.3 (公式)**.** 如果一个串是公式, 那么:

- 每个命题符号都是公式;
- 如果 α 和 β 都是公式, 则 $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$ 和 $(\alpha \leftrightarrow \beta)$ 也是公式;

符号	名称	英文读法	中文读法	LaTeX
$\neg$	negation(否定)	not	非	`\lnot`
$\wedge$	conjunction(合取)	and	与	`\land`
$\vee$	disjunction(析取)	or	或	`\lor`
$\to$	conditional	implies(if then)	蕴含 (如果, 那么)	`\to`
$\leftrightarrow$	biconditional	if and only if	当且仅当	`\leftrightarrow`

- 除此之外, 别无其它.

这里出现了很类似定义自然数的定义方法, 一个很自然的想法是我们能不能在这里运用数学归纳法. 答案是可以的. 我们称作 “归纳原理”.

定理 1.1.1 (归纳原理)**.** 令 $P(\alpha)$ 为一个关于公式的性质. 假设

- 对所有的命题符号 A_i, 性质 $P(A_i)$ 成立; 并且
- 对所有的公式 α 和 β, 如果 $P(\alpha)$ 和 $P(\beta)$ 成立, 则 $P((\neg\alpha))$, $P((\alpha * \beta))$ 也成立,

那么 $P(\alpha)$ 对所有的公式 α 都成立.

> $\mathbb{B}onus$ **思考题**
>
> 数学归纳法可以在正整数上使用, 但是不能再 $\mathbb{R}$ 上使用, 却可以在上面定义的结构中使用, 为什么? 什么样的结构可以运用数学归纳法?

规定了符号, 就一定要有对应的运算规律. 因此, 我们就给出如下定义, 和高中的内容类似.

定义 1.1.4 (命题符号的运算规则)**.** 一般地, 命题记号遵循如下的运算规则:

- 最外层的括号可以省略
- 优先级: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$
- 结合性: 右结合 ($\alpha \wedge \beta \wedge \gamma$, $\alpha \to \beta \to \gamma$)

有了命题, 我们很多时候希望 “假定” 这些命题的真假, 来考察最终结论的真假, 或者从中找到一点规律. 这样做其实有一个更专业的名字叫 “真值指派”.

定义 1.1.5 (真值指派 (v))**.** 令 S 为一个命题符号的集合. S 上的一个**真值指派** v 是一个从 S 到真假值的映射

$$v : S \to \{T, F\}.$$

如果对于只能指派一个的话太局限了, 我们不妨把所有可能的情况都枚举一遍映射过去. 也就是真值指派的 “扩张”.

定义 1.1.6 (真值指派的扩张 ($\overline{v}$))**.** 令 S 为一个命题符号的集合. 令 $\overline{S}$ 为只含有 S 中命题符号的公式集.

S 上的**真值指派** v **的扩张**是一个从 $\overline{S}$ 到真假值的映射

$$\overline{v} : \overline{S} \to \{T, F\}.$$

定义 1.1.7 (满足 (Satisfy))**.** 如果 $\overline{v}(\alpha) = T$, 则称真值指派 v **满足**公式 α.

很多时候一些逻辑表达式看上去就是废话. 比如 “如果我后天知道了考试的成绩, 那我明天就知道了”. 数学上面对这类问题有一个定义叫做 “重言蕴含”.

定义 1.1.8 (重言蕴含 (Tautologically Implies))**.** 设 Σ 为一个公式集.

Σ **重言蕴含**公式 α, 记为 $\Sigma \models \alpha$,

如果每个满足 Σ 中所有公式的真值指派都满足 α.

定义 1.1.9 (重言式/永真式 (Tautology))**.** 如果 $\emptyset \models \alpha$, 则称 α 为**重言式**, 记为 $\models \alpha$.

反之, 就是永远都不能成立的矛盾的形式.

定义 1.1.10 (矛盾式/永假式 (Contradiction))**.** 若公式 α 在所有真值指派下均为假, 则称 α 为**矛盾式**.

定义 1.1.11 (重言等价 (Tautologically Equivalent))**.** 如果 $\alpha \models \beta$ 且 $\beta \models \alpha$, 则称 α 与 β **重言等价**, 记为 $\alpha \equiv \beta$.

命题逻辑的运算律

上面我们发现了有很多的废话, 但是, 有时候 "废话" 并不是显然的. 这就需要一些推理规律来帮助我们联通看上去毫不相干的逻辑符号.

命题 1.1.1. (逻辑的运算律)

- 交换律:

$$(A \wedge B) \leftrightarrow (B \wedge A)$$

$$(A \vee B) \leftrightarrow (B \vee A)$$

- 结合律:

$$((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$$

$$((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$$

- 分配律:

$$(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$$

$$(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$$

- De Morgan 律:

$$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$$

$$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$$

- 双重否定律:

$$\neg\neg A \leftrightarrow A$$

- 排中律:

$$A \vee (\neg A)$$

- 矛盾律:

$$\neg(A \wedge \neg A)$$

- 逆否命题:

$$(A \to B) \leftrightarrow (\neg B \to \neg A)$$

那么, 这些内容化简到最后有没有一个目标呢? 其实是有的. 任何一个命题都可以写成 “合取范式 (CNF)” 或者 “析取范式” 的形式. 下面给出定义.

定义 1.1.12 (合取范式 (Conjunctive Normal Form))**.** 我们称公式 α 是**合取范式**, 如果它形如

$$\alpha = \beta_1 \wedge \beta_2 \wedge \cdots \wedge \beta_k,$$

其中, 每个 β_i 都形如

$$\beta_i = \beta_{i1} \vee \beta_{i2} \vee \cdots \vee \beta_{in},$$

并且 β_{ij} 或是一个命题符号, 或者命题符号的否定.

定义 1.1.13 (析取范式 (Disjunctive Normal Form))**.** 我们称公式 α 是**析取范式**, 如果它形如

$$\alpha = \beta_1 \vee \beta_2 \vee \cdots \vee \beta_k,$$

其中, 每个 β_i 都形如

$$\beta_i = \beta_{i1} \wedge \beta_{i2} \wedge \cdots \wedge \beta_{in},$$

并且 β_{ij} 或是一个命题符号, 或者命题符号的否定.

> $\mathbb{B}onus$ 思考题
>
> 根据上述的演算的规则, 有没有一种操作方法, 应该怎样把一个命题化作一个 CNF 或者 BNF?

命题逻辑的演算

命题逻辑的演算有时候也可以帮助我们理解命题之间的等价关系.

引入假设.

$$\frac{}{[x : P]} \quad \texttt{(assumption)}$$

所有引入的假设最终必须被 “**释放**” (discharged) 所谓释放, 其实就是在使用假设 α 作为假设的前提下推出了 β, 最后要写成 $\alpha \to \beta$ 的形式. 这就是假设的释放.

“$\wedge$” 推理规则.

$$\frac{P \qquad Q}{P \wedge Q} \quad \wedge\texttt{-intro}$$

$$\frac{P \wedge Q}{P} \quad \wedge\texttt{-elim-left}$$

$$\frac{P \wedge Q}{Q} \quad \wedge\texttt{-elim-right}$$

下面这条规则描述了双重否定的性质.

“$\neg\neg$” 推理规则.

$$\frac{\alpha}{\neg\neg\alpha}\neg\neg\texttt{-intro}$$

$$\frac{\neg\neg\alpha}{\alpha}\neg\neg\texttt{-elem}$$

“$\rightarrow$” 推理规则.

$$\frac{\alpha\rightarrow\beta \qquad \alpha}{\beta} \quad \rightarrow\texttt{-elim (modus ponens)}$$

$$\frac{\alpha\rightarrow\beta \qquad \neg\beta}{\neg\alpha}\texttt{modus tollens}$$

$$\begin{array}{c}[x:\alpha]\\ \vdots\\ \beta\end{array}$$

$$\frac{\beta}{\alpha\rightarrow\beta} \quad \rightarrow\texttt{-intro}/x$$

Assumption x is discharged

$\vee$ 推理规则.

$$\frac{\alpha}{\alpha\vee\beta} \quad \vee\texttt{-intro-left}$$

$$\frac{\alpha\vee\beta \qquad \alpha\rightarrow\gamma \qquad \beta\rightarrow\gamma}{\gamma} \quad \vee\texttt{-elim; (分情况分析)}$$

$\perp$ 推理规则.

$$\frac{\alpha \qquad \neg\alpha}{\perp} \quad \perp\texttt{-intro}$$

$$\frac{\perp}{\alpha} \quad \perp\texttt{-elim(Principle of Explosion)};$$

“$\neg$”. 推理规则

$$\frac{\alpha\rightarrow\perp}{\neg\alpha} \quad \neg\texttt{-intro}\frac{\neg\alpha}{\alpha\rightarrow\perp} \quad \neg\texttt{-elim}$$

定理 1.1.2 (命题逻辑的可靠性 (Soundness))**.** 如果 $\Sigma\vdash\alpha$, 则 $\Sigma\models\alpha$.

定理 1.1.3 (命题逻辑的完备性 (Completeness))**.** 如果 $\Sigma\models\alpha$, 则 $\Sigma\vdash\alpha$.

1.1.3 谓词逻辑

我们发现命题逻辑无法表达部分与整体的关系.

谓词逻辑的语法

定义 1.1.14 (谓词逻辑的构成)**.**

逻辑联词: $\neg, \wedge, \vee, \to, \leftrightarrow$

量词符号: $\forall$ (forall; 全称量词), $\exists$ (exists; 存在量词)

变元符号: $x, y, z, \ldots$

左右括号: $(,)$

常数符号: 零个或多个常数符号 $a, b, c, \ldots$, 表达特殊的个体

函数符号: n-元函数符号 $f, g, h, \ldots$ $(n \in \mathbb{N}^+)$, 表达个体上的运算

谓词符号: n-元谓词符号 $P, Q, R, \ldots$ $(n \in \mathbb{N})$, 表达个体的性质与关系

定义 1.1.15 (项 (Term))**.** 1. 每个变元 $x, y, z, \ldots$ 都是一个项;

2. 每个常数符号都是一个项;

3. 如果 $t_1, t_2, \ldots, t_n$ 是项, 且 f 为一个 n-元函数符号,
   则 $f(t_1, t_2, \ldots, t_n)$ 也是项;

4. 除此之外, 别无其它.

定义 1.1.16 (公式 (Formula))**.**

- 如果 $t_1, \ldots, t_n$ 是项, 且 P 是一个 n 元谓词符号,
  则 $P(t_1, \ldots, t_n)$ 为公式, 称为**原子公式**;
- 如果 α 与 β 都是公式, 则 $(\neg\alpha)$ 与 $(\alpha * \beta)$ 都是公式;
- 如果 α 是公式, 则 $\forall x.\ \alpha$ 与 $\exists x.\ \alpha$ 也是公式;
- 除此之外, 别无其它.

举个例子:

- 0 不是任何自然数的后继

$$\forall x.\ \neg(Sx = 0)$$

- 两个自然数相等当且仅当它们的后继相等

$$\forall x.\ \forall y.\ (x = y \leftrightarrow Sx = Sy)$$

- x 是素数 ($x > 1$ 且 x 没有除自身和 1 之外的因子)

$$\mathrm{Prime}(x) : S0 < x \wedge \forall y.\ \forall z.\ (y < x \wedge z < x) \to \neg(y \times z = x)$$

- 哥德巴赫猜想 (任一大于 2 的偶数, 都可表示成两个素数之和)

$$\forall x.\ (SS0 < 2 \wedge (\exists y.\ 2 \times y = x)) \to$$
$$(\exists x_1.\ \exists x_2.\ \mathrm{Prime}(x_1) \wedge \mathrm{Prime}(x_2) \wedge x_1 + x_2 = x)$$

定义 1.1.17 (作用域 (Scope)、约束变元 (Bind)、自由变元 (Free))**.** [(1)]

1. $\forall x.\ (P(x) \to Q(x))$
2. $(\forall x.\ P(x)) \to Q(x)$
3. $\forall x.\ \Big(P(x) \to \big(\exists y.\ R(x,y)\big)\Big)$
4. $\Big(\forall x.\ \forall y.\ \big(P(x,y) \land Q(y,z)\big)\Big) \land \exists x.\ P(x,y)$

定义 1.1.18 (改名 (Rename))**.** 为尽量避免重名, 可将约束变元或自由变元改名为新鲜 (fresh)变元

定义 1.1.19 (t is free for x in α)**.**

$$y-1 \text{ is free for } x \text{ in } \exists z.\ (z < x)$$

$$y-1 \text{ is } \textit{not} \text{ free for } x \text{ in } \exists y.\ (y < x)$$

在公式 α 中, 项 t 可以替换变量 x 写作 ($\alpha[t/x]$)

谓词逻辑的语义

在这里, 情况变复杂了. 我们需要考虑对象所处的数学空间来下结论. 也就是一个表达式的语义取决于:

- 对量词论域 (universe) 的解释, 限定个体范围
- 对常数符号、函数符号、谓词符号的解释
- 对自由变元的解释 (赋值函数 s)

也就是这种 "**解释**" 将公式映射到一个**数学结构** $\mathcal{U}$上, 决定了该公式的语义.

定义 1.1.20 ($(\mathcal{U}, s) \models \alpha$)**.** $\mathcal{U}$ 与 s 满足公式 α:

$$(\mathcal{U}, s) \models \alpha$$

- 将 α 中的常数符号、函数符号、谓词符号按照结构 $\mathcal{U}$ 进行解释,
- 将量词的论域限制在集合 $|\mathcal{U}|$ 上,
- 将自由变元 x 解释为 $s(x)$,
- 这样就将公式 α 翻译成了某个数学领域中的命题,
- 然后, 使用数学领域知识我们知道该命题成立

例如,

$$\alpha : \forall x.\ (x \times x \neq 1 + 1)$$

在 α 在数学结构 $\mathcal{U} = \mathbb{Q}$ 中为真, 在数学结构 $\mathcal{U} = \mathbb{R}$ 中为假.

定义 1.1.21 (语义蕴含 (Logically Imply)). 令 Σ 为一个公式集, α 为一个公式.

Σ **语义蕴含** α, 记为 $\Sigma \models \alpha$, 如果每个满足 Σ 中所有公式的结构 $\mathcal{U}$ 与赋值 s都满足 α. 记作

$$\{\forall x.\ P(x)\} \models P(y)$$

举例: 假设有

$$\alpha : \forall x \forall y \forall z((P(x, y) \wedge P(y, z)) \to P(x, z))$$

$$\beta : \forall x \forall y((P(x, y) \wedge P(y, x)) \to x = y)$$

$$\gamma : \forall x \exists y P(x, y) \to \exists y \forall x P(x, y)$$

那么我们还不可以推断出 $\{\alpha, \beta\} \models \gamma$, 除非我们知道 $\mathcal{U} = \mathbb{N}$, $P(x, y) : x \leq y$.

定义 1.1.22 (语义等价 (Logically Equivalent)). 如果 $\alpha \models \beta$ 且 $\beta \models \alpha$, 则称 α 与 β **语义等价**, 记为 $\alpha \equiv \beta$.

例如: $\neg(\forall x.\ \alpha) \equiv \exists x.\ \neg\alpha$. 这就相当于命题逻辑中的 “重言式”, 可用于公式推导.

定义 1.1.23 (普遍有效的 (Valid)). 如果 $\emptyset \models \alpha$, 则称 α 是**普遍有效的**, 记为 $\models \alpha$.

普遍有效的公式在所有可能的结构 $\mathcal{U}$ 与所有可能的赋值 s下均为真.
下面来看几组普遍有效的公式:

定理 1.1.4. (普遍有效的公式)

$$\boxed{\neg\forall x\alpha \leftrightarrow \exists x\neg\alpha}$$

$$\boxed{\neg\exists x\alpha \leftrightarrow \forall x\neg\alpha}$$

$$\neg(\forall x \in A.\ \alpha) \leftrightarrow \exists x \in A.\ \neg\alpha$$

$$\forall x\forall y\alpha \leftrightarrow \forall y\forall x\alpha$$

$$\exists x\exists y\alpha \leftrightarrow \exists y\exists x\alpha$$

$$\forall x\alpha \wedge \forall x\beta \leftrightarrow \forall x(\alpha \wedge \beta)$$

$$\exists x\alpha \vee \exists x\beta \leftrightarrow \exists x(\alpha \vee \beta)$$

$$\forall x\alpha \to \exists x\alpha$$

$$\exists x \forall y \alpha \to \forall y \exists x \alpha$$

$$\forall x \alpha \vee \forall x \beta \to \forall x (\alpha \vee \beta)$$

$$\exists x (\alpha \wedge \beta) \to \exists x \alpha \wedge \exists x \beta$$

对于 β 不含 x:

$$\forall x.\ (\alpha \vee \beta) \leftrightarrow (\forall x.\ \alpha) \vee \beta$$

$$\forall x.\ (\alpha \wedge \beta) \leftrightarrow (\forall x.\ \alpha) \wedge \beta$$

$$\exists x.\ (\alpha \vee \beta) \leftrightarrow (\exists x.\ \alpha) \vee \beta$$

$$\exists x.\ (\alpha \wedge \beta) \leftrightarrow (\exists x.\ \alpha) \wedge \beta$$

注意这条公式不成立: $\forall y \exists x \alpha \not\to \exists x \forall y \alpha$. 我们有反例: $U = \{a, b\}$, 关系 $P(a,b), P(b,a)$, $\forall y \exists x P(y,x) \equiv T$ $\exists x \forall y P(y,x) \equiv F$.

谓词逻辑的推演

定理 1.1.5. ($\forall$-elim)

$$\frac{\forall x.\ \alpha}{\alpha[t/x]} \quad (\forall x\text{-elim})$$

where t is free for x in α

例子:

$$\forall x.\ P(x) \vdash P(c) \quad (c \text{ 是任意常元符号})$$

$$\forall x.\ \exists y.\ (x < y) \vdash \exists y.\ (z < y) \quad (z \neq y \text{ 是任意变元符号})$$

$$\forall x.\ \exists y.\ (x < y) \nvdash \exists y.\ (y < y) \quad (y \text{ is } \textit{not} \text{ free for } x \text{ in } \alpha)$$

定理 1.1.6.

$$\frac{\begin{array}{c}[t] \\ \vdots \\ \alpha[t/x]\end{array}}{\forall x.\ \alpha} \quad (\forall x\text{-intro})$$

where, t is a fresh variable

这个定理的意思是任取 t, 如果能证明 α 对 t 成立, 则 α 对所有 x 成立. 例如:

$$\Big\{P(t), \forall x(P(x) \to \neg Q(x))\Big\} \vdash \neg Q(t)$$

我们可以有如下的推理:

$$P(t) \quad (\text{前提}) \tag{1.1}$$
$$\forall x.\ (P(x) \to \neg Q(x)) \quad (\text{前提}) \tag{1.2}$$
$$P(t) \to \neg Q(t) \quad (\forall\text{-elim}, (1.2)) \tag{1.3}$$
$$\neg Q(t) \quad (\to\text{-elim}, (1.1), (1.3)) \tag{1.4}$$

另一个例子:

$$\left\{\forall x.\ (P(x) \to Q(x)), \forall x.\ P(x)\right\} \vdash \forall x.\ Q(x)$$

$$\forall x.\ (P(x) \to Q(x)) \quad (\text{前提}) \tag{1.1}$$
$$\forall x.\ P(x) \quad (\text{前提}) \tag{1.2}$$
$$[x_0] \quad (\text{引入变量}) \tag{1.3}$$
$$P(x_0) \to Q(x_0) \quad (\forall\text{-elim}, (1.1), (1.3)) \tag{1.4}$$
$$P(x_0) \quad (\forall\text{-elim}, (1.2), (1.3)) \tag{1.5}$$
$$Q(x_0) \quad (\to\text{-elim}, (1.4), (\mathbf{??})) \tag{1.6}$$
$$\forall x.\ Q(x) \quad (\forall\text{-intro}, (1.3) - (1.6)) \tag{1.7}$$

定理 1.1.7 ($\exists$-intro)**.**

$$\frac{\alpha[t/x]}{\exists x.\ \alpha} \quad (\exists x\text{-intro})$$

where t is free for x in α

也就是说如果 α 对某个项 t 成立, 则 $\exists x.\ \alpha$ 成立. 也就是说我们有

$$P(c) \vdash \exists x.\ P(x) \quad c \text{ 是任意常元符号}$$

如果变量不是自由的, 那么就不能做这样的替换, 如下所示

$$\forall y.\ (y = y) \nvdash \exists x.\ \forall y.\ (x = y) \quad (y \text{ is } \textit{not} \text{ free for } x \text{ in } \alpha)$$

定理 1.1.8 ($\exists$-elim)**.**

$$\frac{\exists x.\ \alpha \qquad [x_0] \qquad \begin{matrix}[\alpha[x_0/x]] \\ \vdots \\ \beta\end{matrix}}{\beta} \quad (\exists\text{-elim})$$

where x_0 is free for x in α

这句话的意思是假设 x_0 使得 α 成立, 如果从 $\alpha[x_0/x]$ 可以推导出 β, 则从 $\exists x.\ \alpha$ 可以推导出 β. 看如下的例子:

$$\forall x.\ P(x) \vdash \exists x.\ P(x)$$

有如下的证明:

$$\forall x.\ P(x) \quad \text{(前提)} \tag{1.1}$$
$$[x_0] \quad \text{(引入变量)} \tag{1.2}$$
$$P(x_0) \quad (\forall\text{-elim}, (1.1), (1.2)) \tag{1.3}$$
$$\exists x.\ P(x) \quad (\exists\text{-intro}, (1.3)) \tag{1.4}$$

1.1.4 数学归纳法

定理 1.1.9 (第一数学归纳法 (The First Mathematical Induction))**.** 设 $P(n)$ 是关于自然数的一个性质. 如果

1. $P(0)$ 成立;
2. 对任意自然数 n, 如果 $P(n)$ 成立, 则 $P(n+1)$ 成立.

那么, $P(n)$ 对所有自然数 n 都成立.

翻译成形式化的方法, 也就是

$$\frac{P(0) \qquad \forall n \in \mathbb{N}.\ \Big(P(n) \to P(n+1)\Big)}{\forall n \in \mathbb{N}.\ P(n)} \quad \text{(第一数学归纳法)}$$

$$\Big(P(0) \wedge \forall n \in \mathbb{N}.\ \Big(P(n) \to P(n+1)\Big)\Big) \to \forall n \in \mathbb{N}.\ P(n).$$

定理 1.1.10 (第二数学归纳法 (The Second Mathematical Induction))**.** 设 $Q(n)$ 是关于自然数的一个性质. 如果

1. $Q(0)$ 成立;
2. 对任意自然数 n, 如果 $Q(0), Q(1), \ldots, Q(n)$ 都成立,
   则 $Q(n+1)$ 成立.

那么, $Q(n)$ 对所有自然数 n 都成立.

同样的, 翻译成形式化的表示形式, 也就是

$$\frac{Q(0) \ \ \forall n \in \mathbb{N}.\ \Big(\big(Q(0) \wedge \cdots \wedge Q(n)\big) \to Q(n+1)\Big)}{\forall n \in \mathbb{N}.\ Q(n)} \quad \text{(第二数学归纳法)}$$

$$\Big(Q(0) \wedge \forall n \in \mathbb{N}.\ \Big(\big(Q(0) \wedge \cdots \wedge Q(n)\big) \to Q(n+1)\Big)\Big) \to \forall n \in \mathbb{N}.\ Q(n).$$

定理 1.1.11 (数学归纳法)**.** 第一数学归纳法与第二数学归纳法等价.

第二数学归纳法也被称为**“强” (Strong)** 数学归纳法, 它强在可以使用的条件更多了. 我们可以来证明这件事情.

引理 1.1.1. 第一数学归纳法蕴含第二数学归纳法.

证明. 要证第二类数学归纳法,也即任给一个命题 F ,若满足 $F(1)$ 及 $(F(1)\wedge F(2)\wedge\cdots\wedge F(n))\Rightarrow F(n+1)$ ，则有 $\forall k\in\mathbb{N}.F(k)$. 那么，我们可以构造命题 $G(n):=F(1)\wedge F(2)\wedge\cdots\wedge F(n)$. 显然，$G(n)\Rightarrow F(n+1)$ ，又有 $G(n)\Rightarrow G(n)$ ，则 $G(n)\Rightarrow(F(n+1)\wedge G(n))$ ，而后者即为 $G(n+1)$. 故，命题 G 满足第一类数学归纳法的条件，所以 $\forall k\in\mathbb{N}$. $G(k)$ 成立. 而 $G(k)\Rightarrow F(k)$ ，故 $\forall k\in\mathbb{N}$. $F(k)$ ，也即第二类数学归纳法成立. □

引理 1.1.2. 第二数学归纳法蕴含第一数学归纳法.

证明. 要证第一类数学归纳法，也即任给一个命题 F ，若满足 $F(1)$ 及 $F(n)\to F(n+1)$ ，则有 $\forall k\in\mathbb{N}$. $F(k)$. 显然，F 是满足第二类数学归纳法的条件的 (因为 1 的条件比 2 强)，故根据第二类数学归纳法，$F(k)$ 对所有正整数 k 成立，也即第一类数学归纳法成立. □

数学归纳法的更深层次的结果是自然数的 Peano 公理. Peano 公理体系刻画了**自然数的递归结构**.

定义 1.1.24 (Peano Axioms)**.** 自然数的 Peano 公理有如下几条:

1. 0 是自然数;
2. 如果 n 是自然数, 则它的后继 $\mathbf{S}n$ 也是自然数;
3. 0 不是任何自然数的后继;
4. 两个自然数相等当且仅当它们的后继相等;
5. **数学归纳原理:** 如果
   (a) $P(0)$ 成立;
   (b) 对任意自然数 n, 如果 $P(n)$ 成立, 则 $P(n+1)$ 成立.

   那么, $P(n)$ 对所有自然数 n 都成立.

   自然数集具有良序原理.

定义 1.1.25 (良序原理 (The Well-Ordering Principle))**.** 自然数集的任意非空子集都有一个最小元.

定理 1.1.12. 良序原理与 (第一) 数学归纳法等价.

引理 1.1.3. (第一) 数学归纳法蕴含良序原理.

证明. By mathematical induction on the size n of non-empty subsets of $\mathbb{N}$.

$$P(n):\text{All subsets of size } n \text{ contain a minimum.}$$

Inductive Hypothesis:

- Basis Step: $P(1)$

- Inductive Hypothesis: $P(n)$
- Inductive Step: $P(n) \to P(n+1)$
  - $A' \leftarrow A \setminus a$
  - $x \leftarrow \min A'$
  - Compare x with a

□

> *Example* **例子:**
>
> Of the 1000 islanders, it turns out that **100 of them have blue eyes** and **900 of them have brown eyes**, although the islanders are not initially aware of these statistics (each of them can of course only see 999 of the 1000 tribespeople).
>
> One day, a **blue-eyed foreigner** visits to the island and wins the complete trust of the tribe.
>
> One evening, he addresses the entire tribe to thank them for their hospitality.
>
> However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking "**how unusual it is to see another blue-eyed person like myself in this region of the world**".
>
> **What effect, if anything, does this** *faux pas (失礼)* **have on the tribe?**

定理 1.1.13. Suppose that the tribe had $n > 0$ blue-eyed people.

Then n days after the traveller's address, all n blue-eyed people commit suicide.

证明.

基础步骤: $n = 1$.
这个**唯一的蓝眼人**的内心独白: **"你直接念我身份证吧"**

归纳假设: 有 n 个蓝眼人时, 前 $n-1$ 天无人自杀, 第 n 天集体自杀.

归纳步骤: 考虑恰有 $n+1$ 个蓝眼人的情况.
每个**蓝眼人**都如此推理: 我看到了 n 个蓝眼人, 他们应该在第 n 天集体自杀.
但是, 每个蓝眼人都在等其它 n 个蓝眼人自杀, 因此, 第 n 天无人自杀.
每个**蓝眼人**继续推理: 一定不止 n 个蓝眼人, 但是我看到的其余人都不是蓝眼.
所以, **"小丑竟是我自己"**. □

这就像是考虑 $n = 1, n = 2$ 的简单情况, 出现了类似 "我知道你知道我知道 ..." 的思维递归情形.

1.2 朴素集合论

1.2.1 公理体系

在中学的时候, 我们定义的集合是如下的一个数学对象: 集合就是任何一个有明确定义的对象的整体.

定义 1.2.1 (集合)**.** 我们将集合理解为任何将我们思想中那些确定而彼此独立的对象放在一起而形成的聚合.

这也引出了概括原则:

定理 1.2.1 (概括原则)**.** 对于任意性质/谓词 $P(x)$, 都存在一个集合 X:

$$X = \{x \mid P(x)\}$$

很多时候我们需要判别两个集合是不是相等, 那么我们有外延性原理:

定义 1.2.2 (外延性原理 (Extensionality))**.** 两个集合相等 $(A = B)$ 当且仅当它们包含相同的元素.

$$\forall A.\, \forall B.\, \Big(\big(\forall x.\, (x \in A \leftrightarrow x \in B)\big) \leftrightarrow A = B\Big)$$

这条公理意味着集合这个对象完全由它的元素决定.

有时候我们需要从一个集合里面抽出一部分, 也就是寻找一个集合的子集. 因此我们有如下的定义.

定义 1.2.3 (子集)**.** 设 A、B 是任意两个集合.

$A \subseteq B$ 表示 A 是 B 的子集 (subset):

$$A \subseteq B \iff \forall x \in A.\, (x \in A \to x \in B)$$

$A \subseteq B$ 表示 A 是 B 的真子集 (proper subset):

$$A \subseteq B \iff A \subseteq B \wedge A \neq B$$

我们还可以证明两个集合相等, 当二者互为对方的子集时候.

定理 1.2.2. 两个集合相等当且仅当它们互为子集.

$$A = B \iff A \subseteq B \wedge B \subseteq A$$

1.2.2 简单操作

现在我们不妨把高中定义的文字性的内容重新定义一下:

定义 1.2.4 (集合的并 (Union))**.**

$$A \cup B \triangleq \{x \mid x \in A \vee x \in B\}$$

定义 1.2.5 (集合的交 (Intersection))**.**

$$A \cap B \triangleq \{x \mid x \in A \wedge x \in B\}$$

定理 1.2.3 (分配律 (Distributive Law))**.**

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

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

对于这样的命题, 我们同样给出证明.

证明. 对任意 x,

$$\begin{aligned}
& x \in A \cup (B \cap C) && (1.5)\\
\iff & (x \in A) \vee (x \in B \wedge x \in C) && (1.6)\\
\iff & (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) && (1.7)\\
\iff & (x \in A \cup B) \wedge (x \in A \cup C) && (1.8)\\
\iff & x \in (A \cup B) \cap (A \cup C) && (1.9)
\end{aligned}$$

□

同样, 像命题符号一样, 集合的运算也遵循吸收率:

定理 1.2.4 (吸收律 (Absorption Law))**.**

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

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

证明. 对任意 x,

$$\begin{aligned}
& x \in A \cup (A \cap B) && (1.10)\\
\iff & x \in A \vee (x \in A \wedge x \in B) && (1.11)\\
\iff & x \in A && (1.12)
\end{aligned}$$

□

有了这个我们就可以使用这个证明一个比较重要的习题.

定理 1.2.5.

$$A \subseteq B \iff A \cup B = B \iff A \cap B = A$$

证明. 对任意 x

$$\begin{aligned}
& x \in B && (1.1)\\
\implies & x \in A \vee x \in B && (1.2)\\
\implies & x \in A \cup B && (1.3)
\end{aligned}$$

□

定义 1.2.6 (集合的差 (Set Difference); 相对补 (Relative Complement))**.**

$$A \setminus B = \{x \mid x \in A \land x \notin B\}$$

定义 1.2.7 (绝对补 (Absolute Complement); $\overline{A}, A', A^c$)**.** 设全集为 U.

$$\overline{A} = U \setminus A = \{x \in U \mid x \notin A\}$$

期中, 全集 U (Universe) 是当前正在考虑的所有元素构成的集合. 一般均默认存在. 注意: 不存在 "包罗万象" 的全集.

相对补和绝对补之间存在一些联系.

定理 1.2.6 ("相对补" 与 "绝对补" 之间的关系)**.** 设全集为 U.

$$\boxed{A \setminus B = A \cap \overline{B}}$$

证明. 对任意 x,

$$\begin{aligned}
& x \in A \setminus B && (1.1)\\
\iff & x \in A \land x \notin B && (1.2)\\
\iff & x \in A \land (x \in U \land x \notin B) && (1.3)\\
\iff & x \in A \land x \in \overline{B} && (1.4)\\
\iff & x \in A \cap \overline{B} && (1.5)
\end{aligned}$$

□

定理 1.2.7 (德摩根律 (绝对补))**.** 设全集为 U.

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

证明. 对任意 x,

$$\begin{aligned}
& x \in \overline{A \cup B} && (1.1)\\
\iff & x \in U \land \neg(x \in A \lor x \in B) && (1.2)\\
\iff & x \in U \land x \notin A \land x \notin B && (1.3)\\
\iff & (x \in U \land x \notin A) \land (x \in U \land x \notin B) && (1.4)\\
\iff & x \in \overline{A} \land x \in \overline{B} && (1.5)\\
\iff & x \in \overline{A} \cap \overline{B} && (1.6)
\end{aligned}$$

□

定理 1.2.8 (德摩根律 (相对补))**.**

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$$
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$$

证明.

$$
\begin{aligned}
& C \setminus (A \cup B) && (1.1)\\
\iff & C \cap \overline{A \cup B} && (1.2)\\
\iff & C \cap (\overline{A} \cap \overline{B}) && (1.3)\\
\iff & (C \cap \overline{A}) \cap (C \cap \overline{B}) && (1.4)\\
\iff & (C \setminus A) \cap (C \setminus B) && (1.5)
\end{aligned}
$$

□

由此, 我们可以在集合的操作的层面上证明如下四个定理而不需要取集合中的一个元素进行证明.

定理 1.2.9.

$$A \cap (B \setminus C) = (A \cap B) \setminus C = (A \cap B) \setminus (A \cap C)$$

$$A \setminus (B \setminus C) = (A \cap C) \cup (A \setminus B)$$

$$A \subseteq B \implies \overline{B} \subseteq \overline{A}$$

$$A \subseteq B \implies (B \setminus A) \cup A = B$$

这里面有一个类似一个异或操作的运算符: 对称差.

定义 1.2.8 (对称差 (Symmetric Difference))**.**

$$A \oplus B = (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A})$$

1.2.3 高级集合操作

既然集合的对象是一组元素, 那么集合也是对象, 集合中的元素自然也可以被传进去看作运算. 由此, 我们需要定义关于集合的集合的运算.

定义 1.2.9 (广义并 (Arbitrary Union))**.** 设 $\mathbb{M}$ 是一组集合 (a *collection* of sets)

$$\bigcup \mathbb{M} = \left\{ x \mid \exists A \in \mathbb{M}.\ x \in A \right\}$$

举一些例子, 比如 $\mathbb{M} = \Big\{\{1,2\}, \{\{1,2\},3\}, \{4,5\}\Big\}$, 那么 $\bigcup \mathbb{M} = \Big\{1,2,3,4,5,\{1,2\}\Big\}$. 注意元素只被解开了一次而不是一次解包到我们认为的 “基本元素”. 因为有时候 “基本元素” 也是用集合定义的. 我们后来会发现我们可以把整个数学基础建立到集合论的基础上.

和求和记号一样, 为了方便书写, 我们也有类似的记号:

$$\bigcup_{j=1}^{n} A_j \triangleq A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcup_{j=1}^{\infty} A_j \triangleq A_1 \cup A_2 \cup \cdots$$

$$\bigcup_{\alpha \in I} A_\alpha \triangleq \left\{ x \mid \exists \alpha \in I.\ x \in A_\alpha \right\}$$

和广义并一样, 我们还有广义交. 定义如下:

定义 1.2.10 (广义交 (Arbitrary Intersection))**.** 设 $\mathbb{M}$ 是一组集合 (a *collection* of sets)

$$\bigcap \mathbb{M} = \left\{ x \mid \forall A \in \mathbb{M}.\ x \in A \right\}$$

同样的, 如果 $\mathbb{M} = \left\{ \{1,2\}, \{\{1,2\},3\}, \{4,5\} \right\}$ 是全集, $\bigcap \mathbb{M} = \emptyset$. 同样只是展开一次就行了. 注意一个有趣的情况: $\bigcap \emptyset = U$. "包含所有元素的集合" 在后面会发现会导出一个矛盾, 有时候我们也会认为这样说的结果是未定义的.

那么类似的, 我们也希望广义集合里面有没有像普通集合的一些操作. 答案是肯定的. 下面我们来探讨一些有趣的内容.

定理 1.2.10 (德摩根律)**.**

$$X \setminus \bigcup_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I} (X \setminus A_\alpha)$$

$$X \setminus \bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} (X \setminus A_\alpha)$$

证明. 对任意 x,

$$x \in X \setminus \bigcup_{\alpha \in I} A_\alpha \tag{1.1}$$

$$\iff x \in X \wedge \neg(\exists \alpha \in I.\ x \in A_\alpha) \tag{1.2}$$

$$\iff x \in X \wedge (\forall \alpha \in I.\ x \notin A_\alpha) \tag{1.3}$$

$$\iff \forall \alpha \in I.\ (x \in X \wedge x \notin A_\alpha) \tag{1.4}$$

$$\iff x \in \bigcap_{\alpha \in I} (X \setminus A_\alpha) \tag{1.5}$$

□

我们同样可以用这条规律来化简集合, 而不用真正在一个集合的集合里面取出来一个元素.

Example **举例:**

如果

$$X_n = \{-n, -n+1, \cdots, 0, \cdots, n-1, n\}$$

请化简:

$$A = \mathbb{R} \setminus \bigcap_{n \in \mathbb{Z}^+} (\mathbb{R} \setminus X_n)$$

证明.

$$\begin{aligned} A &= \mathbb{R} \setminus \bigcap_{n \in \mathbb{Z}^+} (\mathbb{R} \setminus X_n) \\ &= \mathbb{R} \setminus \left(\mathbb{R} \setminus \bigcup_{n \in \mathbb{Z}^+} X_n \right) \\ &= \mathbb{R} \setminus \left(\mathbb{R} \setminus \mathbb{Z} \right) \\ &= \mathbb{Z} \end{aligned}$$

□

1.2.4 集合的操作: 排列的力量

在高中, 我们学习了排列组合. 如果对于集合中的元素进行 “选择性缺席”, 这样就可以让我们构造出更加复杂而全面的集合了.

定义 1.2.11 (幂集 (Powerset))**.**

$$\mathcal{P}(A) = \Big\{ X \mid X \subseteq A \Big\}$$

这个之所以强大, 是因为给定一个 A, 就有如下的内容可以被生成.

$$A = \{1, 2, 3\}$$

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

因为对于 $|A| = n$ 的句子, $|\mathcal{P}(A)| = 2^n$, 因此有时候也写做 2^A 或者 $\{0, 1\}^A$.

接下来看一个 (看似) 没啥用的定理:

定理 1.2.11.

$$S \in \mathcal{P}(X) \iff S \subseteq X$$

这个定理的作用是在 $\in$ 和 $\subseteq$ 之间转换, 同时脱去一层 $\mathcal{P}()$ 记号.

> Example **举例:**
> 请证明:
> $$\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S)))$$

证明. 根据上面的定理, 我们有

$$\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(S))) \iff \{\emptyset, \{\emptyset\}\} \subseteq \mathcal{P}(\mathcal{P}(S)).$$

分别证明之:

$$\begin{aligned} &\emptyset \in \mathcal{P}(\mathcal{P}(S)) \\ &\iff \emptyset \subseteq \mathcal{P}(S) \end{aligned}$$

$$\begin{aligned} &\{\emptyset\} \in \mathcal{P}(\mathcal{P}(S)) \\ &\iff \{\emptyset\} \subseteq \mathcal{P}(S) \\ &\iff \emptyset \in \mathcal{P}(S) \\ &\iff \emptyset \subseteq S \end{aligned}$$

□

其实幂集生成之间也有一些关系. 不妨看一看.

定理 1.2.12. 证明:

$$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$$

证明. 对于任意 x,

$$\begin{aligned} & x \in \mathcal{P}(A) \cap \mathcal{P}(B) \\ \iff & x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B) \\ \iff & x \subseteq A \wedge x \subseteq B \\ \iff & x \subseteq A \cap B \\ \iff & x \in \mathcal{P}(A \cap B) \end{aligned}$$

□

定理 1.2.13. 证明:

$$\bigcap_{\alpha \in I} \mathcal{P}(A_\alpha) = \mathcal{P}(\bigcap_{\alpha \in I} A_\alpha)$$

证明. 对于任意 x,

$$\begin{aligned} & x \in \bigcap_{\alpha \in I} \mathcal{P}(A_\alpha) \\ \iff & \forall \alpha \in I.\, x \in \mathcal{P}(A_\alpha) \\ \iff & \forall \alpha \in I.\, x \subseteq A_\alpha \\ \iff & x \subseteq \bigcap_{\alpha \in I} A_\alpha \\ \iff & x \in \mathcal{P}(\bigcap_{\alpha \in I} A_\alpha) \end{aligned}$$

□

1.2.5 悖论的出现

前面我们提到 “不存在含有任何东西的集合”. 这就是我们以前知道的通俗讲述的 “理发师悖论”. 形式化的, 根据概括原则, 如果性质 P 是 $P(x) \triangleq$ “$x \notin x$”, 集合 $R = \{x \mid x \notin x\}$, 那么 $R \in R$ 吗?

> “悖论出现于数学的边界上, 而且是靠近哲学的边界上”
> — 哥德尔

之后, 数学家们提出了 ZF(ZFC) 公理化集合论, 避免了这样的内容. 通过粗暴的避免了这种情况, 我们得到了一个还可以使用, 但是丧失了一部分确定性的集合.

定理 1.2.14 (Russell's Paradox)**.**

$$\{x \mid x \notin x\} \text{ is } \textit{not} \text{ a set.}$$

第二章　关系, 函数关系, 序关系

其实本节的内容也是《数学分析》建立基础的地方. 也可以找到很多相似的地方.

2.1　关系

我们在初中和高中的学习中学习了很多的 “关系”. 比如, 比较两个数的大小, 我们引入了 “大于”, “小于” 和 “等于” 的关系. 这样的内容我们可以进一步的抽象, 提炼出 “关系” 的一些共性.

比如, 我们可以在 $\mathbb{R}$ 上定义 “Near” 关系.

> Example **举例:**
>
> 如果 $|a-b|<1(a,b\in\mathbb{R})$, 则称 a,b 具有 Near 关系.

回顾我们学过的表达 “关系” 的运算符, 相当一部分满足下面的性质:

自反性.

$$\forall a\in X.\ (a,a)\in R$$

对称性.

$$\forall a,b\in X.\ ((a,b)\in R\to(b,a)\in R)$$

传递性.

$$\forall a,b,c\in X.\ ((a,b)\in R\wedge(b,c)\in R\to(a,c)\in R)$$

很多时候, 自反性 + 对称性 = 相容关系. 相容关系的含义其实是表明这两个关系之间有交叉.[1]

[1]不是很确定直观上表

这样, 我们就可以把关系表示成一个集合. 不严格的说, 在上面的定义中, 我们可以有这样的集合: $R=\{(a,b)\mid|a-b|<1\}$.

下面来看几个更多的例子. 比如整除关系.

> Example **举例:**
>
> 假设 $X=\{1,2,3,4,5,6,10,12,15,20,30,60\}$, “关系” 是 X 上的整除关系.

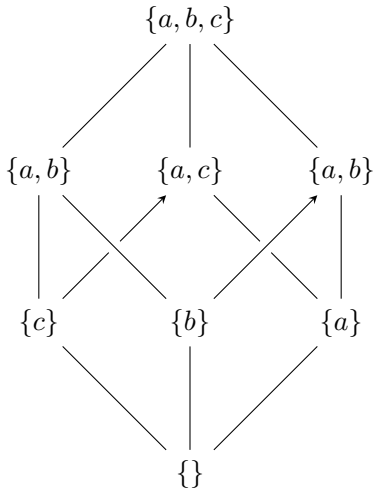
按照上面的展开, 我们就有所有整除的全体 (有序对 (a,b) 表示的关系是 $a|b$):

$$R=\{(1,2),\dots,(4,12),\dots,(12,60),\dots,(4,60),\dots,(60,60)\}$$

可以看到在上述的关系中, 上面的自反性, 对称性, 传递性仍然满足. 这种结构十分的常见. 比如地图上面的地方的 “可达” 关系, 还有给定集合的幂集按 “包含” 关系排序, 自然数按照大小关系排序, 等等. 满足上述的三条性质的关系叫做 “偏序关系”. 特殊的, 我们或许还会发现自然数可以唯一地按照大小被排成一排, 这是一种比较特殊的偏序关系, 后来我们会定义它为全序关系.

特别的, 我们可以把上述偏序关系画成一张图, 也就是在多个维度上都有不同的序, 因此没办法唯一的列成一列, 包含所有元素.

比如上述的幂集的例子, 化作一张图如下图所示:



观察正整数集, 发现这是一条链式结构, 它和上述的偏序集最大的区别是什么呢? 其实, 最大的区别是在整数中的大于关系存在 “连接性”.

连接性.

$$\forall a, b \in X.\ ((a, b) \in R \vee (b, a) \in R)$$

也就是自反性 + 反对称性 + 传递性 + 连接性 = 全序关系.

2.1.1 有序对

我们可能会很自然的想 $(a, b) = (c, d) \iff a = c \wedge b = d$, 对于这样自然产生的概念, 我们同样要将它严格化, 给出一个定义.

历史上, 很多人会用集合的观念来刻画有序对. Norbert Wiener 在 1914 年给出了这样的定义.

定义 2.1.1 (Ordered Pairs (Norbert Wiener; 1914))**.**

$$(a, b) \triangleq \Big\{\{\{a\}, \emptyset\}, \{\{b\}\}\Big\}$$

这样一来, 有序对之间的相等关系看上去就自然了很多.

定理 2.1.1.

$$(a, b) = (c, d) \iff a = c \wedge b = d$$

证明. 也就是证明

$$\Big(\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}\Big) \iff (a = c \land b = d)$$

我们有:

$$\begin{aligned}
&\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\} \\
\iff &(\{a\} = \{c\} \lor \{a\} = \{c,d\}) \land (\{a,b\} = \{c\} \lor \{a,b\} = \{c,d\}) \\
\iff &(\{a\} = \{c\} \land \{a,b\} = \{c\}) \lor \\
&(\{a\} = \{c\} \land \{a,b\} = \{c,d\}) \lor \\
&(\{a\} = \{c,d\} \land \{a,b\} = \{c\}) \lor \\
&(\{a\} = \{c,d\} \land \{a,b\} = \{c,d\})
\end{aligned}$$

□

有了有序对, 我们还可以把它拓广到 n 个元素的情况. 于是我们有定义:

定义 2.1.2 (n-元组 (n-ary tuples))**.**

$$(x,y,z) \triangleq ((x,y),z)$$

$$(x_1,x_2,\ldots,x_{n-1},x_n) \triangleq ((x_1,x_2,\ldots,x_{n-1}),x_n)$$

在这个结构上同样是可以应用数学归纳法的. 不过一般我处理而二元组就行了. 多数情况下, 我们仅处理 “二元关系”, 因此也仅使用 “有序对”

2.1.2 笛卡尔积: 一种组合方式

如果我们有两个集合, 从两个集合中各取得一个元素, 把它们组合成一个有序对, 塞到一个新的集合里面, 这样, 我们就可以对于集合做一点组合, 生成更加复杂的集合了. 这样的操作叫做笛卡尔积.

定义 2.1.3 (笛卡尔积 (Cartesian Products))**.** The *Cartesian product* $A \times B$ of A and B is defined as

$$A \times B \triangleq \{(a,b) \mid a \in A \land b \in B\}$$

那么 “笛卡尔积” 这个操作满足哪些运算律呢? 我们首先来考察一些例子.

> Example **举例:**

$$X \times \emptyset = \emptyset \times X$$
$$X \times Y \neq Y \times X$$
$$(X \times Y) \times Z \neq X \times (Y \times Z)$$
$$A = \{1\} \qquad (A \times A) \times A \neq A \times (A \times A)$$

我们发现这个符号既没有普遍的交换律, 也没有普遍的结合律. 但是是有分配律的.

定理 2.1.2 (分配律 (Distributivity))**.**

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C)$$

下面我们来以证明 $A \times (B \cap C) = (A \times B) \cap (A \times C)$ 为例, 看一下这个是如何进行起作用的.

证明. 对任意有序对 (a, b),

$$(a, b) \in A \times (B \cap C) \tag{2.1}$$
$$\iff a \in A \wedge b \in (B \cap C) \tag{2.2}$$
$$\iff a \in A \wedge b \in B \wedge b \in C \tag{2.3}$$
$$\iff (a \in A \wedge b \in B) \wedge (a \in A \wedge b \in C) \tag{2.4}$$
$$\iff (a, b) \in A \times B \wedge (a, b) \in A \times C \tag{2.5}$$
$$\iff (a, b) \in (A \times B) \cap (A \times C) \tag{2.6}$$

□

同样的, 我们可以有多个元素的笛卡尔积.

定义 2.1.4 (n-元笛卡尔积 (n-ary Cartesian Product))**.**

$$X_1 \times X_2 \times X_3 \triangleq (X_1 \times X_2) \times X_3$$

$$X_1 \times X_2 \times \cdots \times X_n \triangleq (X_1 \times X_2 \times \cdots \times X_{n-1}) \times X_n$$

回想我们从数轴到平面直角坐标系再到空间直角坐标系, 我们可以发现这样的过程也就是对于一个维度反复做笛卡尔积的结果.

但在本节的情况下, 我们仅处理 “二元关系”, 因此也仅使用 “二元笛卡尔积”.

2.1.3 用有序对定义二元关系

我们以前做了有关关系的定义, 但是我们可能还要给 “什么是关系” 在集合方面下一个稍微集合化的定义. 于是我们有定义:

定义 2.1.5 (关系 (Relations))**.** A *relation* R from A to B is a subset of $A \times B$:

$$R \subseteq A \times B$$

Sepcially, if $A = B$, R is called a relation on A.

为了简化符号, 我们有时候也通过这样的方式来书写:

定义 2.1.6 (Notations)**.**

$$(a, b) \in R \qquad aRb$$

$$(a, b) \notin R \qquad a\overline{R}b$$

举一些例子: $A \times B$ 和 $\emptyset$ 都是从 A 到 B 的关系, 前者的意义是任意两个 A 和 B 中的元素都有关系, 后者是都没有关系. 回顾我们在小学中学更一般的关系, 我们就会发现有更加有趣的二元关系:

- 小于关系: $< = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a \text{ is less than } b\}$
- 整除关系: $D = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid \exists q \in \mathbb{N}.\ a \cdot q = b\}$

在生活中更有这样的关系. 比如 P 是所有人的集合, 如果我们定义 $M = \{(a, b) \in P \times P \mid a \text{ is the mother of } b\}$, $B = \{(a, b) \in P \times P \mid a \text{ is the brother of } b\}$, 那么上述定义的 M 和 B 都满足 “关系” 的定义.

有了这样的抽象, 我们就可以很开心的研究另外一些更重要的问题了. 具体地, 我们要研究这些重要的关系:

- 等价关系
- 序关系
- 函数

2.2 等价关系和序关系

总体而言, 在这一小节中我们会给出三个定义, 5 个操作, 以及 7 个对应的性质.

其实, 这一节的内容很大程度上和中学定义的函数类似. 但是有一个重大的区别. 从现在开始, 我们稍微忘记我们高中关于 “函数” 的定义, 但是留下 “函数” 带给我们的思考方式. 下面我们来用有序对重新解释这一切.

2.2.1 三个定义

定义 2.2.1 (定义域 (Domain))**.**

$$\mathrm{dom}(R) = \{a \mid \exists b.\ (a,b) \in R\}$$

我们在函数中说 "定义域" 是函数中有定义的地方的横坐标构成的集合, 在这里面的 $\exists b$ 就保证了在这个点一定被定义了, 那么我们就取出来它的 a(横坐标). "扫描" 所有这样的有序对 (a,b) 并将满足条件的 a 取出来, 我们就完成了这样类似概念的迁移.

定义 2.2.2 (值域 (Range))**.**

$$\mathrm{ran}(R) = \{b \mid \exists a.\ (a,b) \in R\}$$

我们在函数中说 "值域" 是函数中所有有定义的横坐标所对应的纵坐标, 在这里面的 $\exists a$ 就说明了有这样的点被取到, 那么我们就取出来它的 b(横坐标). "扫描" 所有这样的有序对 (a,b) 并将满足条件的 b 取出来, 同样有类似的概念.

定义 2.2.3 (域 (Field))**.**

$$\mathrm{fld}(R) = \mathrm{dom}(R) \cup \mathrm{ran}(R)$$

定义域和值域并起来就是域. 这样可以让我们直观的明确了解 "二元关系" 之间的空间映射关系.

举个例子: 对于 $R = \{(x,y) \mid x^2+y^2 = 1\} \subseteq \mathbb{R}\times\mathbb{R}$, 它的 $\mathrm{dom}(R) = [1,1]$, $\mathrm{ran}(R) = [-1,1]$, $\mathrm{fld}(R) = [-1,1]$.

我们来看一个更抽象的. 不过别忘了本质上就是用集合的操作解决这一切问题.

定理 2.2.1.

$$\mathrm{dom}(R) \subseteq \bigcup\bigcup R \qquad \mathrm{ran}(R) \subseteq \bigcup\bigcup R$$

证明. 对任意 a,

$$\begin{aligned}
& a \in \mathrm{dom}(R) && (2.7)\\
\Longrightarrow\ & \exists b.\ (a,b) \in R && (2.8)\\
\Longrightarrow\ & \exists b.\ \{\{a\},\{a,b\}\} \in R && (2.9)\\
\Longrightarrow\ & \exists b.\ \{a,b\} \in \bigcup R && (2.10)\\
\Longrightarrow\ & \exists b.\ a \in \bigcup\bigcup R && (2.11)\\
\Longrightarrow\ & a \in \bigcup\bigcup R && (2.12)
\end{aligned}$$

□

这个例子的直观解释就是任何的定义域, 值域都会在二元组的某一个元素中 "出现".

2.2.2 五种操作

1. 逆变换. 像 “反函数” 的概念一样, 关系有时候也有逆变换.

定义 2.2.4 (逆 (Inverse))**.** The *inverse* of R is the relation

$$R^{-1} = \{(a, b) \mid (b, a) \in R\}$$

我们可以来看几组例子:

- 如果 $R = \{(x, y) \mid x = y\} \subseteq \mathbb{R} \times \mathbb{R}$, $R^{-1} = R$
- $R = \{(x, y) \mid y = \sqrt{x}\} \subseteq \mathbb{R} \times \mathbb{R}$, $R^{-1} = \{(x, y) \mid y = x^2 \wedge x > 0\}$
- $\leq = \{(x, y) \mid x \leq y\} \subseteq \mathbb{R} \times \mathbb{R}$, $\leq^{-1} = \geq \triangleq \{(x, y) \mid x \geq y\}$

直观地, 我们自然会想到反关系的反仍然是原来的关系. 所以我们有如下定理:

定理 2.2.2.

$$(R^{-1})^{-1} = R$$

证明. 对任意 (a, b),

$$(a, b) \in (R^{-1})^{-1} \tag{2.1}$$
$$\iff (b, a) \in R^{-1} \tag{2.2}$$
$$\iff (a, b) \in R \tag{2.3}$$

□

既然关系也是集合定义的, 那我们自然可以证明它的交, 并, 补. 在我们做的有益的探索中, 我们会发现这个定理还是比较重要的.

定理 2.2.3 (关系的逆)**.** 如果 R, S 均为关系, 那么有

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$$

$$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$$

$$(R \setminus S)^{-1} = R^{-1} \setminus S^{-1}$$

2. 限制. 由于问题的定义和性质, 有时候我们可能需要对于构造的 “全面” 集合的状态空间进行 “裁切”, 来打造更精细的集合. 这样就可以自然地引入集合的限制操作. 我们希望引入这样的记号, 使得它可以对于这个关系二元组 (a, b) 中的 a, b 分别加以筛选. 于是我们有定义:

定义 2.2.5 (左限制 (Left-Restriction))**.** Suppose $R \subseteq X \times Y$ and $S \subseteq X$. The *left-restriction* relation of R to S over X and Y is

$$R|_S = \{(x, y) \in R \mid x \in S\}$$

定义 2.2.6 (右限制 (Right-Restriction))**.** Suppose $R \subseteq X \times Y$ and $S \subseteq Y$. The *right-restriction* relation of R to S over X and Y is

$$R|^S = \{(x, y) \in R \mid y \in S\}$$

定义 2.2.7 (限制 (Restriction))**.** Suppose $R \subseteq X \times X$ and $S \subseteq X$. The *restriction* relation of R to S over X is

$$R|_S = \{(x, y) \in R \mid x \in S \land y \in S\}$$

哎呀! "限制" 和 "左限制" 的记号重复了! 但是仔细看一下他们的前提是不一样的. "左限制" 的前提是有 $R \subseteq X \times X$, 而 "限制" 的前提是 $R \subseteq X \times X$, 也就是自己集合中元素到自己集合元素的关系.

下面我们来看刚刚举的例子: 如果 $R = \{(x, y) \mid x^2 + y^2 = 1\} \subseteq \mathbb{R} \times \mathbb{R}$, $R|_{\mathbb{R}^+}$ 的含义就是表示关系的二元组 (a, b) , a 只取 $\mathbb{R}^+$ 的时候满足的才被认为 "满足" 关系.

> $\mathbb{B}onus$ **思考题**
>
> 对于这样的情况, 我们能不能使用 xOy 平面表达这种关系呢? 限制在平面上的意义是什么?

3. 像 (Image). 想一想这种 "有所对应" 的感觉, 好像在高中学习函数那一节里面见过类似的, 也就是有点像函数里面 $f()$ 做的事情. 同样的, 这里面也有类似描述这样一种 "有所对应" 的定义.

定义 2.2.8 (像 (Image))**.** The *image* of X under R is the set

$$R[X] = \{b \in \operatorname{ran}(R) \mid \exists a \in X.\ (a, b) \in R\}$$

为了简化符号, 一般而言 $R[a] \triangleq R[\{a\}] = \{b \mid (a, b) \in R\}$.

4. 逆像. 同样的, 我们有时候可能需要顺藤摸瓜, 这就自然地导出了像也有 "逆" 的概念.

定义 2.2.9 (逆像 (Inverse Image))**.** The *inverse image* of Y under R is the set

$$R^{-1}[Y] = \{a \in \operatorname{dom}(R) \mid \exists b \in Y.\ (a, b) \in R\}$$

同样为了简化记号, 我们有 $R^{-1}[b] \triangleq R^{-1}[\{b\}] = \{a \mid (a, b) \in R\}$.

有了这两个操作之后, 事情就变得复杂了. 比如 $R^{-1}[R[X]]$ 和 X 的关系如何, $R[R^{-1}[Y]]$ 和 Y 的关系又如何? 经过证明, 我们给出如下的定理:

定理 2.2.4.

$$R[X_1 \cup X_2] = R[X_1] \cup R[X_2]$$

$$R[X_1 \cap X_2] \subseteq R[X_1] \cap R[X_2]$$

$$R[X_1 \setminus X_2] \supseteq R[X_1] \setminus R[X_2]$$

证明. 对任意 (a,b),

$$
\begin{aligned}
& (a,b) \in (R \circ S)^{-1} && (2.1)\\
\iff & (b,a) \in R \circ S && (2.2)\\
\iff & \exists c.\ (b,c) \in S \wedge (c,a) \in R && (2.3)\\
\iff & \exists c.\ (c,b) \in S^{-1} \wedge (a,c) \in R^{-1} && (2.4)\\
\iff & (a,b) \in S^{-1} \circ R^{-1} && (2.5)
\end{aligned}
$$

□

定理 2.2.5.

$$(R \circ S) \circ T = R \circ (S \circ T)$$

5. 复合像复合函数一样, 这是一种构建复杂系统的很好的一种方法. 因此我们自然给出定义:

定义 2.2.10 (复合 (Composition; $R \circ S$, $R; S$))**.** The *composition* of relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ is the relation

$$R \circ S = \{(a,c) \mid \exists b.\ (a,b) \in S \wedge (b,c) \in R\}$$

举个例子, $R = \{(1,2),(3,1)\}$ $S = \{(1,3),(2,2),(2,3)\}$, 那么 $R \circ S = \{(1,1),(2,1)\}$, $S \circ R = \{(1,2),(1,3),(3,3)\}$. 因为这个和 "乘法" 比较相似, 有时候我们也用空心圆圈表示. $R^{(2)} \triangleq R \circ R = \{(3,2)\}$, $(R \circ R) \circ R = \emptyset$.

> $\mathbb{B}onus$ **思考题**
>
> 有的人习惯记号 $A \circ B \circ C = A \circ (B \circ C)$, 还有的人习惯 $A \circ B \circ C = (A \circ B) \circ C$. 这样做有区别吗?

定理 2.2.6.

$$(R \circ S) \circ T = R \circ (S \circ T)$$

证明. 对任意 (a,b),

$$
\begin{aligned}
& (a,b) \in (R \circ S) \circ T && (2.1)\\
\iff & \exists c.\ \Big((a,c) \in T \wedge (c,b) \in R \circ S\Big) && (2.2)\\
\iff & \exists c.\ \Big((a,c) \in T \wedge (\exists d.\ (c,d) \in S \wedge (d,b) \in R)\Big) && (2.3)\\
\iff & \exists d.\ \exists c.\ \Big((a,c) \in T \wedge (c,d) \in S \wedge (d,b) \in R\Big) && (2.4)\\
\iff & \exists d.\ \Big((\exists c.\ (a,c) \in T \wedge (c,d) \in S) \wedge (d,b) \in R\Big) && (2.5)\\
\iff & \exists d.\ \Big((a,d) \in S \circ T \wedge (d,b) \in R\Big) && (2.6)\\
\iff & (a,b) \in R \circ (S \circ T) && (2.7)
\end{aligned}
$$

□

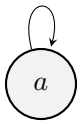
这就表明关系的复合满足结合律, 但是不满足交换律 (和矩阵乘法很相似).

2.2.3 七个性质

1. 自反的.

定义 2.2.11 (自反的 (Reflexive)). $R \subseteq X \times X$ is *reflexive* if

$$\forall a \in X.\ (a, a) \in R$$



举几个例子:

- $\leq \subseteq \mathbb{R} \times \mathbb{R}$ is reflexive
- 三角形上的全等关系是自反的

其实所有自反的关系都是这个关系的一个子集, 可以有如下的表达.

定理 2.2.7.

$$R \text{ is reflexive} \iff I \subseteq R$$

其中

$$I = \{(a, a) \in A \times A \mid a \in A\}.$$

定理 2.2.8.

$$R\text{is reflexive} \iff R^{-1} = R$$

2. 反自反.

定义 2.2.12 (反自反 (Irreflexive)). $R \subseteq X \times X$ is *irreflexive* if

$$\forall a \in X.\ (a, a) \notin R$$

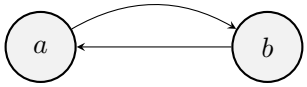
同样的, 我们给一些例子:

- $< \subseteq \mathbb{R} \times \mathbb{R}$ is irreflexive
- $> \subseteq \mathbb{R} \times \mathbb{R}$ is irreflexive

3. 对称.

定义 2.2.13 (对称 (Symmetric)). $R \subseteq X \times X$ is *symmetric* if

$$\forall a, b \in X.\ aRb \to bRa$$



$$\forall a, b \in X.\ aRb \leftrightarrow bRa$$

对称就意味着 R 的逆是的形式是很好的. 具体的, 有如下定义.

定理 2.2.9.

$$R \text{ is symmetric} \iff R^{-1} = R$$

4. 反对称.

定义 2.2.14 (反对称 (AntiSymmetric))**.** $R \subseteq X \times X$ is *antisymmetric* if

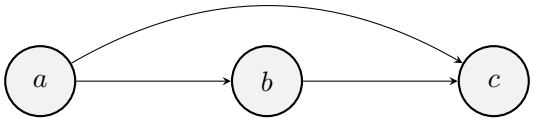
$$\forall a, b \in X.\ (aRb \wedge bRa) \to a = b$$

例如 $>, |$ 都具有反对称性.

5. 传递性

定义 2.2.15 (传递的 (Transitive))**.** $R \subseteq X \times X$ is *transitive* if

$$\forall a, b, c \in X.\ (aRb \wedge bRc \to aRc)$$



有了传递性, 有时候就意味着关系的封闭性.

定理 2.2.10.

$$R \text{ is transitive} \iff R \circ R \subseteq R$$

证明. 对任意 (a, b),

$$(a, b) \in R \circ R \tag{2.1}$$
$$\implies \exists c.\ (a, c) \in R \wedge (b, c) \in R \tag{2.2}$$
$$\implies (a, b) \in R \tag{2.3}$$

对任意 a, b, c

$$(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R \circ R \implies (a, c) \in R$$

□

传递性和上面的内容一起构成了 “序关系”. 上回我们定义了 “偏序关系”. 接下来看到 “偏序关系” 到全序关系的重要关系, 就是下面的一个内容.

6. 连接性.

定义 2.2.16 (连接的 (Connex))**.** $R \subseteq X \times X$ is *connex* if

$$\forall a, b \in X.\ (aRb \vee bRa)$$

我们发现, 在以前我们涉及 “关系” 的比较重, $a > b$, $b < a$, $b = a$ 三种关系中, 有且只有一种关系成立. 这样我们可以抽象出 “三分的” 性质.

7. 三分的.

定义 2.2.17 (三分的 (Trichotomous))**.** $R \subseteq X \times X$ is *trichotomous* if

$$\forall a, b \in X.\ (\text{exactly one of } aRb, bRa, \text{ or } a = b \text{ holds})$$

其实这些关系是可以刻画 “求逆” 的可行性和唯一性. 具体的, 有如下的定理.

定理 2.2.11.

$$R \text{ is symmetric and transitive} \iff R = R^{-1} \circ R$$

证明. 对任意 (a, b),

$$(a, b) \in R \circ R \tag{2.1}$$

$$\implies \exists c.\ (a, c) \in R \wedge (b, c) \in R \tag{2.2}$$

$$\implies (a, b) \in R \tag{2.3}$$

□

2.2.4 等价关系

很多时候, 我们在研究数学关系会发现很多相同点. 比如在模意义下, 很多数是相等的. 比如 $3 \equiv 6 \bmod 3$. 他们的余数都是 0. 这就有一个很有趣的相似关系了.

用同余的例子, 我们会发现这种 “等价性” 满足这样几条性质:

定义 2.2.18 (Equivalence Relation)**.** $R \subseteq X \times X$ is an *equivalence relation* on X iff R is

- reflexive: $\forall a \in X.\ aRa$
- symmetric: $\forall a, b \in X.\ (aRb \leftrightarrow bRa)$
- transitive: $\forall a, b, c \in X.\ (aRb \wedge bRc \to aRc)$

更一般的, 我们发现各个等价关系其实把整个区间 “划分” 成了不同的区域, 其中每一个区域里面都有和其他地方在某些意义下完全相同的特性.

就像我们把所有属于中国的领土通过 “划分” 的方式形成了省, 其中每个省都有自己的地方行政机关, 他们彼此等价. 因此, 我们可以说这个是在中国领土上划分的情况下, 行政机关的等价关系.

更具体的, 划分有如下定义:

定义 2.2.19 (划分 (Partition))**.** A family of sets $\Pi = \{A_\alpha \mid \alpha \in I\}$ is a *partition* of X if

1. (不空) $\forall \alpha \in I.\ A_\alpha \neq \emptyset, (\forall \alpha \in I.\ \exists x \in X.\ x \in A_\alpha)$
2. (不漏) $\bigcup_{\alpha \in I} A_\alpha = X, (\forall x \in X.\ \exists \alpha \in I.\ x \in A_\alpha)$

3. (不重) $\forall \alpha, \beta \in I.\ A_\alpha \cap A_\beta = \emptyset \vee A_\alpha = A_\beta (\forall \alpha, \beta \in I.\ A_\alpha, \cap A_\beta \neq \emptyset \implies A_\alpha = A_\beta)$

那么, 将划分的结果, 把每一类处于 “等同地位的元素” 拿出来看, 就可以被称作等价类了.[2] 等价类其实可以看作拉拢所有的等价关系. 正式的, 我们有如下的定义:

[2] 语言表述不清楚, 要

定义 2.2.20 (等价类 (Equivalence Class))**.** The *equivalence class* of a *modulo* R is a set:

$$[a]_R = \{b \in X.\ aRb\}$$

为什么等价类如此重要? 一个原因是它提供了一个抽象, 让我们方便的研究很多问题.

像整数的模运算一样, 我们在 “集合” 的也想有类似的运算. 因此我们有 “商集” 的概念. 这样我们就可以把所有相互等价的元素取用出来, 进行研究.

定义 2.2.21 (商集 (Quotient Set))**.** The *quotient set* of X by R (X modulo R) is a set:

$$X/R = \{[a]_R \mid a \in X\}$$

同样的, 这样取, 只不过是用另外一种维度划分整个集合罢了. 这在直觉上看起来是对的, 下面我们来做一下证明.

定理 2.2.12.

$$X/R = \{[a]_R \mid a \in X\} \text{ is a partition of } X.$$

证明. $\forall a \in X.\ [a]_R \neq \emptyset$,

$\forall a \in X.\ \exists b \in X.\ a \in [b]_R$. □

在等价关系中, 下面这个定理可以很方便的从三个不同的侧面刻画 “划分”, 同时帮助我们更容易的证明某些由 “划分” 产生的等价性问题.

定理 2.2.13.

$$\forall a \in X, b \in X.\ [a]_R \cap [b]_R = \emptyset \vee [a]_R = [b]_R$$

证明. $\forall a \in X, b \in X.\ [a]_R \cap [b]_R \neq \emptyset \to [a]_R = [b]_R$

一方面, 不妨设 $x \in [a]_R \wedge [b]_R$

$$\begin{aligned} & x \in [a]_R \wedge [b]_R && (2.1)\\ \implies & aRx \wedge xRb && (2.2)\\ \implies & aRb && (2.3) \end{aligned}$$

另一方面, 对于任意 x,

$$\begin{aligned} & x \in [a]_R && (2.1)\\ \iff & xRa && (2.2)\\ \iff & xRb && (2.3)\\ \iff & x \in [b]_R && (2.4) \end{aligned}$$

□

定理 2.2.14.

$$\forall a, b \in X.\ ([a]_R = [b]_R \leftrightarrow aRb)$$

这就意味着我们的划分在某种意义上也是一个等价关系!

定义 2.2.22. If partition Π of $X \implies$ Equivalence Relation $R \subseteq X \times X$, $(a,b) \in R \iff \exists S \in \Pi.\ a \in S \wedge b \in S$, $R = \{(a,b) \in X \times X \mid \exists S \in \Pi.\ a \in S \wedge b \in S\}$

定理 2.2.15. R is an equivalence relation on X.

2.2.5 构造实数

定义 2.2.23.

$$\sim \subseteq \mathbb{N} \times \mathbb{N}$$

$$(a,b) \sim (c,d) \iff a +_{\mathbb{N}} d = b +_N c$$

那么, $\mathbb{N} \times \mathbb{N}/\sim$ 是 $\mathbb{Z}$.

定义 2.2.24 ($\mathbb{Z}$)**.**

$$\mathbb{Z} \triangleq \mathbb{N} \times \mathbb{N}/\sim$$

定义 2.2.25 ($+_{\mathbb{Z}}$)**.**

$$[(m_1,n_1)] +_{\mathbb{Z}} [(m_2,n_2)] = [m_1 +_{\mathbb{N}} m_2, n_1 +_{\mathbb{N}} n_2]$$

定义 2.2.26 ($\cdot_{\mathbb{Z}}$)**.**

$$[(m_1,n_1)] \cdot_{\mathbb{Z}} [(m_2,n_2)]$$
$$= [m_1 \cdot_{\mathbb{N}} m_2 +_{\mathbb{N}} n_1 \cdot_{\mathbb{N}} n_2, m_1 \cdot_{\mathbb{N}} n_2 +_{\mathbb{N}} n_1 \cdot_{\mathbb{N}} m_2]$$

定义 2.2.27.

$$\sim \subseteq \mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})$$

$$(a,b) \sim (c,d) \iff a \cdot_{\mathbb{Z}} d = b \cdot_{\mathbb{Z}} c$$

定义 2.2.28 ($\mathbb{Q}$)**.**

$$\mathbb{Q} \triangleq \mathbb{Z} \times (\mathbb{Z} \setminus \{0_{\mathbb{Z}}\})/\sim$$

如何用有理数定义实数? 请参见《数学分析》Dedekind 分割.

2.3 函数

2.3.1 函数: 作为关系的一个子集

函数不允许一对多, 这就是它和 "关系" 最大的去区别.

回想我们以前学习过的东西, 好像 "关系" 和方程的图像有点相似. 也就是我们在高中的时候在平面直角坐标系中做的椭圆的图线: $x^2/a^2 + y^2/b^2 = 1 (a, b > 0)$. 接下来, 我们不妨来看一种特殊的 "关系": 函数.

𝔹onus 思考题

为什么函数不允许 “一对多”? 在定义上有什么合理性?

让我们重新定义一下以前学过的函数.

定义 2.3.1 (Function)**.** $f \subseteq A \times B$ is a *function* from A to B if

$$\forall a \in A.\ \exists!\ b \in B.\ (a, b) \in f.$$

在函数中, 除了定义域和值域之外, 还有陪域. 通常被称作 “cod”. 比如对于一个映射 (函数)$f : A \to B$, $\mathrm{dom}(f) = A, \mathrm{cod}(f) = B$, 对于一个函数的值域 $\mathrm{ran}(f) = f(A) \subseteq B$.

为什么这样定义? 值域为什么不是 B? 原因是很多时候函数的值域难以求解, 这样就使得我们的表达造成很多不便. 而且很多时候如果强行把 B 当作值域很多时候可能会出现运算不封闭的问题, 在研究某些问题的时候非常不方便. 因此, 我们不妨把这个值域扩大一些, 这样才可以更方便一些. 因此, B 就叫做 “陪域”. 值域只不过是陪域的一个子集.

对于证明而言, 我们同样有一套形式化的证明语言: $\forall a \in A., \forall a \in A.\ \exists b \in B. (a, b) \in f, \exists! b \in B., \forall b, b' \in B.\ (a, b) \in f \wedge (a, b') \in f \implies b = b'$.

当然我们可以看一些有趣的函数.

1. 恒等函数. “恒等” 在数学的各个领域里面都是重要的. “恒等函数” 的地位有时候和加法意义下的 ‘0’, 乘法意义下的 ‘1’ 很相似, 其特点是经过一次复合之后还是一样的. 我们一般用 I_X 表示, I 的意思是 identity 的缩写. 其中,

$$\forall x \in X.\ I_X(x) = x.$$

𝔽un *fact* 趣事

Weierstrass 构造了一个处处连续, 处处不可导的函数.

$$f(x) = \sum_{n=0}^{\infty} a^n \cos(b^n \pi x),$$

其中, $0 < a < 1$, b is a positive odd integer, $ab > 1 + \frac{3}{2}\pi$.

当然, 我们也可以把相似的函数放在一个集合里面.

定义 2.3.2 (Y^X)**.** The *set* of all functions from X to Y:

$$Y^X = \{f \mid f : X \to Y\}$$

举一些例子, $|X| = x, |Y| = y, |Y^X| = x^y$.

𝔼xample 举例:

- $\forall Y.\ Y^{\emptyset} = \{\emptyset\}$
- $\emptyset^{\emptyset} = \{\emptyset\}$
- $\forall X \neq \emptyset.\ \emptyset^X = \emptyset$

- $2^X = \{0,1\}^X \cong \mathcal{P}(X)$

类似的, 我们可以问: 是否存在由所有函数组成的集合? 像 Russell 一样, 我们的答案是否定的.

定理 2.3.1. There is no set consisting of all functions.

证明. Suppose by contradiction that A is the set of all functions. For every set X, there exists a function $I_{\{X\}} : \{X\} \to \{X\}$.

$$\bigcup_{I_X \in A} \mathrm{dom}(I_X) \text{ would be the universe that does not exist!}$$

□

既然函数和集合的结论如此相似, 我们自然地想到函数有没有和集合一样的性质?

2.3.2 作为集合的函数

定理 2.3.2 (函数的外延性原理 (The Principle of Functional Extensionality))**.** f, g are functions:

$$f = g \iff \mathrm{dom}(f) = \mathrm{dom}(g) \wedge \big(\forall x \in \mathrm{dom}(f).\ f(x) = g(x)\big)$$

注意定义并没有要求陪域相同, 只要 $f = g \iff \forall (a,b).\ ((a,b) \in f \leftrightarrow (a,b) \in g)$ 满足, 我们就认为这是相等的.

既然是集合, 我们就要考察一些集合的运算. 如果 f 和 g 是函数, $f \cap g, f \cup g$ 是函数吗? 因此我们有如下的定理:

定理 2.3.3 (Intersection of Functions)**.**

$$A = \{x \mid x \in A \cap C \wedge f(x) = g(x)\}$$

$$f \cap g = \{(x,y) \mid x \in A, y = f(x) = g(x)\}$$

定理 2.3.4 (Union of Functions)**.**

$$f \cup g : (A \cup C) \to (B \cup D) \iff \forall x \in \mathrm{dom}(f) \cap \mathrm{dom}(g).\ f(x) = g(x)$$

举几个例子. 如果我们有 $f : \mathcal{P}(\mathbb{R}) \to \mathbb{Z}$, $f(A) = \begin{cases} \min(A \cap \mathbb{N}) & \text{if } A \cap \mathbb{N} \neq \emptyset \\ -1 & \text{if } A \cap \mathbb{N} = \emptyset \end{cases}$. 注意 $\mathbb{N}$ 的良序原理, $\mathrm{dom}(f) \cap \mathrm{dom}(g) = \emptyset$. Dichlet 函数也可以看作函数的并. 它是 $f : \mathbb{R} \to \mathbb{R}$ 的一个映射. 表达式写做: $D(x) = \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$ 注意到这个函数是 “处处不连续” 的.

2.3.3 特殊函数关系

有时候函数之间的映射关系也是重要的. 比如, $f : A \to B$, A 在 B 中的对应元素是不是都是不同的? B 中的元素有没有全部对应上 A 中的元素 (可能不止被对应了一次)? A 有没有和 B 中元素一一对应? 这样我们就有了单射, 满射的概念.

定义 2.3.3 (Injective (one-to-one; 1-1) 单射函数)**.**

$$f : A \to B \qquad f : A \rightarrowtail B$$

$$\forall a_1, a_2 \in A.\ a_1 \neq a_2 \to f(a_1) \neq f(a_2)$$

对于证明而言, 我们可以这样写: $\forall a_1, a_2 \in A.\ f(a_1) = f(a_2) \to a_1 = a_2$. 证明一个函数不是单射函数, 就可以这样写: $\exists a_1, a_2 \in A.\ a_1 \neq a_2 \wedge f(a_1) = f(a_2)$.

定义 2.3.4 (Surjective (onto) 满射函数)**.**

$$f : A \to B \qquad f : A \twoheadrightarrow B$$

$$\mathrm{ran}(f) = B$$

同样的, 对于证明给定的函数是满射而言, 我们可以这样写: $\forall b \in B.\ \big(\exists a \in A.\ f(a) = b\big)$, 反之, 我们可以这样写: $\exists b \in B.\ \big(\forall a \in A.\ f(a) \neq b\big)$.

既是双射又是满射的函数一定很特殊, 因为它有一个一一对应的关系. 因此我们给出如下定义:

定义 2.3.5 (Bijective (one-to-one correspondence) 双射; 一一对应)**.**

$$f : A \to B \qquad f : A \overset{1-1}{\underset{onto}{\longleftrightarrow}} B$$

1-1 & onto

那么, 一个集合和它的幂集之间可不可以找到一个满射呢? 其实是不行的. Cantor 给出了一个证明.

定理 2.3.5 (Cantor Theorem)**.** If $f : A \to 2^A$, then f is not onto.

证明. Let A be the set and let $f : A \to 2^A$. To show that f is not onto, we must find $B \in 2^A (i.e. B \subseteq A)$ for which there is no $a \in A$ with no $f(a) = B$. In other words, B is a set that f "misses". To this end, let

$$B = x \in A | x \notin f(x)$$

We claim there is no $a \in A$ with $f(a) = B$. Suppose, for the sake of contradiction, there is an $a \in A$ such that $f(a) = B$, we pounder: Is $a \in B$?

- if $a \in B$, then, since $B = f(a)$, we have $a \in f(a)$. So by the definition of B , $a \notin f(a)$. that is $a \notin B$. Contradiction!

- If $a \notin B = f(a)$, then by the definition of B, $a \in B$. Contradiction!

To sum up, it can't be onto. □

除了反证之外, 还有一个构造性的证明, 我们一并给出.

对角线论证 *(Cantor's diagonal argument)*(以下仅适用于可数集合 A). []

a	$f(a)$					
	1	2	3	4	5	$\cdots$
1	1	1	0	0	1	$\cdots$
2	0	0	0	0	0	$\cdots$
3	1	0	0	1	0	$\cdots$
4	1	1	1	0	1	$\cdots$
5	0	1	0	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$

□

2.3.4 作为关系的函数

函数的限制

和关系一样, 函数也有限制等操作. 我们来看看.

定义 2.3.6 (Restriction)**.** The *restriction* of a function $f : A \to B$ to X is the function:

$$f|_X = \{(x, y) \in f \mid x \in X\}$$

注意 $X \subseteq A$ 并不是必要的 (虽然平时经常这样用).

像和逆像

定义 2.3.7 (像 (Image))**.** The *image* of X under a function $f : A \to B$ is the set

$$f(X) = \{y \mid \exists x \in X.\ (x, y) \in f\}$$

同样, $X \subseteq \mathrm{dom}(f) = A$ 也不是必要条件, 尽管通常是这样的. 记号层面, $f(\{a\}) = \{b\}$ 简记为 $f(a) = b$.

也就是 $y \in f(X) \iff \exists x \in X.\ y = f(x)$.

定义 2.3.8 (逆像 (Inverse Image))**.** The *inverse image* of Y under a function $f : A \to B$ is the set

$$f^{-1}(Y) = \{x \mid \exists y \in Y.\ (x, y) \in f\}$$

注意不一定要 $Y \subseteq \mathrm{ran}(f)$, 但是很多情况都是满足这样的. 但是注意

$$f^{-1}(\{b\}) = \{a\} \quad \text{可简记为} \quad f^{-1}(b) = \{a\} \quad \text{不能简记为} \quad f^{-1}(b) = a$$

想一想, 为什么会这样?

定义 2.3.9 (逆像 (Inverse Image))**.** The *inverse image* of Y under a function $f : A \to B$ is the set

$$f^{-1}(Y) = \{x \mid \exists y \in Y.\ (x, y) \in f\}$$

这样一来, 我们就有这样的关系:$y \in f(X) \iff \exists x \in X.\ y = f(x), x \in f^{-1}(Y) \iff f(x) \in Y$.

需要注意的是, 如果有 $f : a \to b,\ a \in A_0 \not\Longrightarrow f(a) \in f(A_0)$, 这个式子才可以成立: $a \in A_0 \cap A \implies f(a) \in f(A_0)$.

关于求逆也有很多的性质. 很多时候我们可能会想当然的误用. 所以使用之前一定要小心, 小心, 再小心.

幸运的是, 它还保留有很多性质. 我们一一罗列, 并给出一些证明.

定理 2.3.6 (Properties of f and f^{-1})**.**

$$f : A \to B \qquad A_1, A_2 \subseteq A,\ B_1, B_2 \subseteq B$$

1. f preserves only $\subseteq$ and $\cup$:
   (a) $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$
   (b) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
   (c) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
   (d) $f(A_1 \setminus A_2) \supseteq f(A_1) \setminus f(A_2)$
2. f^{-1} preserves $\subseteq$, $\cup$, $\cap$, and $\setminus$:
   (a) $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$
   (b) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
   (c) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
   (d) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$

对于 $A_1 \subseteq A_2 \implies f(A_1) \subseteq f(A_2)$, 证明如下:

证明.

$$\begin{aligned} & b \in f(A_1) && (2.1)\\ \iff & \exists a \in A_1.\ b = f(a) && (2.2)\\ \implies & \exists a \in A_2.\ b = f(a) && (2.3)\\ \iff & b \in f(A_2) && (2.4) \end{aligned}$$

□

对于 $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$, 证明如下. 注意是哪一步变换, 使得它的箭头方向变为单向了, 为什么?

证明. 对任意 b,

$$
\begin{aligned}
& b \in f(A_1 \cap A_2) && (2.1)\\
\iff & \exists a \in A_1 \cap A_2.\ b = f(a) && (2.2)\\
\implies & \big(\exists a \in A_1.\ b = f(a)\big) \wedge \big(\exists a \in A_2.\ b = f(a)\big) && (2.3)\\
\iff & b \in f(A_1) \wedge b = f(A_2) && (2.4)\\
\iff & b \in f(A_1) \cap f(A_2) && (2.5)
\end{aligned}
$$

□

对于 $f(A_1 \setminus A_2) \supseteq f(A_1) \setminus f(A_2)$:

证明. 对任意 b,

$$
\begin{aligned}
& b \in f(A_1) \setminus f(A_2) && (2.1)\\
\iff & b \in f(A_1) \wedge b \notin f(A_2) && (2.2)\\
\iff & (\exists a_1 \in A_1.\ b = f(a_1)) \wedge (\forall a_2 \in A_2.\ b \neq f(a_2)) && (2.3)\\
\implies & \exists a \in A_1 \setminus A_2.\ b = f(a) && (2.4)\\
\iff & b \in f(A_1 \setminus A_2) && (2.5)
\end{aligned}
$$

□

对于 $B_1 \subseteq B_2 \implies f^{-1}(B_1) \subseteq f^{-1}(B_2)$, 证明如下:

证明. 对任意 a,

$$
\begin{aligned}
& a \in f^{-1}(B_1) && (2.1)\\
\iff & f(a) \in B_1 && (2.2)\\
\implies & f(a) \in B_2 && (2.3)\\
\iff & a \in f^{-1}(B_2) && (2.4)
\end{aligned}
$$

□

对于 $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$, 证明如下:

证明. 对任意 a,

$$
\begin{aligned}
& a \in f^{-1}(B_1 \cap B_2) && (2.1)\\
\iff & f(a) \in B_1 \cap B_2 && (2.2)\\
\iff & f(a) \in B_1 \wedge f(a) \in B_2 && (2.3)\\
\iff & a \in f^{-1}(B_1) \wedge a \in f^{-1}(B_2) && (2.4)\\
\iff & a \in f^{-1}(B_1) \cap f^{-1}(B_2) && (2.5)
\end{aligned}
$$

□

对于 $A_0 \subseteq A \implies A_0 \subseteq f^{-1}(f(A_0))$, 有

证明. 对任意 b,

$$
\begin{aligned}
& a \in A_0 && (2.1)\\
\implies & a \in A_0 \cap A && (2.2)\\
\implies & f(a) \in f(A_0) && (2.3)\\
\iff & a \in f^{-1}(f(A_0)) && (2.4)
\end{aligned}
$$

□

对于 $B_0 \supseteq f(f^{-1}(B_0))$, 思考什么时候这个条件是充要的 ($\iff$)?

证明. 对任意 b,

$$
\begin{aligned}
& b \in f(f^{-1}(B_0)) && (2.1)\\
\iff & \exists a \in f^{-1}(B_0).\ b = f(a) && (2.2)\\
\iff & \exists a \in A.\ f(a) \in B_0 \wedge b = f(a) && (2.3)\\
\implies & b \in B_0 && (2.4)
\end{aligned}
$$

"iff" when f is surjective and

$$B_0 \subseteq \operatorname{ran}(f)$$

. □

函数的复合

作为化简单为复杂的利器, 和关系一样, 函数也有复合.

定义 2.3.10 (Composition)**.**

$$f : A \to B \qquad g : C \to D$$

$$\operatorname{ran}(f) \subseteq C$$

The *composite function* $g \circ f : A \to D$ is defined as

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

> $\mathbb{B}onus$ **思考题**
>
> 回顾关系复合的定义: The *composition* of relations R and S is the relation
>
> $$R \circ S = \{(a, c) \mid \exists b : (a, b) \in S \wedge (b, c) \in R\}$$
>
> 和函数的有什么不同? 为什么是存在?

定理 2.3.7 (Associative Property for Composition)**.**

$$f : A \to B \quad g : B \to C \quad h : C \to D$$

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

证明. 我们只需证明:

1.
$$\mathrm{dom}(h \circ (g \circ f)) = \mathrm{dom}((h \circ g) \circ f)$$

2.
$$\forall x \in A.\ (h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$$

对于 $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$:

$$\begin{aligned} & (h \circ (g \circ f))(x) && (2.1)\\ &= h((g \circ f)(x)) && (2.2)\\ &= h(g(f(x))) && (2.3) \end{aligned}$$

$$\begin{aligned} & ((h \circ g) \circ f)(x) && (2.1)\\ &= ((h \circ g)(f(x))) && (2.2)\\ &= h(g(f(x))) && (2.3) \end{aligned}$$

□

定理 2.3.8. $f : A \to B \qquad g : B \to C,$

- If f, g are injective, then $g \circ f$ is injective.
- If f, g are surjective, then $g \circ f$ is surjective.
- If f, g are bijective, then $g \circ f$ is bijective.

对于第一条, 我们写出 “injective” 的定义, 然后完成逻辑推演.

证明.

$$\forall a_1, a_2 \in A.\ \Big((g \circ f)(a_1) = (g \circ f)(a_2) \to a_1 = a_2\Big)$$

$$
\begin{aligned}
& (g \circ f)(a_1) = (g \circ f)(a_2) && (2.4)\\
\iff & g(f(a_1)) = g(f(a_2)) && (2.5)\\
\implies & f(a_1) = f(a_2) && (2.6)\\
\implies & a_1 = a_2 && (2.7)
\end{aligned}
$$

□

对于第二条, 我们写出 “surjective” 的定义.

证明.

$$\forall c \in C.\ \Big(\exists a \in A.\ (g \circ f)(a) = c\Big)$$

□

对于第三条, 如出一辙.

证明. 对任意 a_1, a_2,

$$
\begin{aligned}
& f(a_1) = f(a_2) && (2.1)\\
\implies & g(f(a_1)) = g(f(a_2)) && (2.2)\\
\implies & (g \circ f)(a_1) = (g \circ f)(a_2) && (2.3)\\
\implies & a_1 = a_2 && (2.4)
\end{aligned}
$$

□

定理 2.3.9.

$$f : A \to B \qquad g : B \to C$$

1. If $g \circ f$ is injective, then f is injective.
2. If $g \circ f$ is surjective, then g is surjective.

因为 (1) 和 (2) 很像, 因此只证明 (2). 注意充要条件是在哪一步消失的.

证明. 对任意 a_1, a_2,

$$
\begin{aligned}
& g \circ f \text{ is surjective} && (2.1)\\
\iff & \forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c && (2.2)\\
\iff & \forall c \in C.\ \exists a \in A.\ g(f(a)) = c && (2.3)\\
\implies & \forall c \in C.\ \exists b \in B.\ g(b) = c && (2.4)\\
\iff & g \text{ is surjective} && (2.5)
\end{aligned}
$$

□

反函数

什么时候有反函数? 反函数具有哪些性质? 在高中的时候老师可能不会和我们讲, 现在我们来探索一下反函数的性质.

定义 2.3.11 (反函数 (Inverse Function))**.** Let $f : A \to B$ be a function.

The *inverse* of f is a function from B to A, denoted $f^{-1} : B \to A$ if f is bijective.

We call f^{-1} the *inverse function* of f.

定义 2.3.12 (Invertible)**.** $f : X \to Y$ is *invertible* if there exists $g : Y \to X$ such that

$$f(x) = y \iff g(y) = x.$$

下面这个定理展示了什么时候具有反函数.

定理 2.3.10. f is invertible $\iff$ f is bijective.

定理 2.3.11. Suppose that $f : A \to B$ is bijective. Then, its inverse function $f^{-1} : B \to A$ is unique.

证明. By contradiction. Omitted. □

定理 2.3.12.

$$\boxed{f : A \to B \text{ is bijective}}$$

1. $f \circ f^{-1} = I_B$
2. $f^{-1} \circ f = I_A$
3. f^{-1} is bijective
4. $g : B \to A \wedge f \circ g = I_B \implies g = f^{-1}$
5. $g : B \to A \wedge g \circ f = I_A \implies g = f^{-1}$

这些定理是帮助我们找到反函数/说明反函数不存在的一些好的结论.

对于 (1).

证明. 对任意 $b \in B$,

$$(f \circ f^{-1})(b) = f(f^{-1}(b))$$

Suppose that $a = f^{-1}(b)$

$$\boxed{a = f^{-1}(b) \iff f(a) = b}$$

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$$

□

对于 (2).

证明. $g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ I_B = f^{-1}$ □

我们当然可以看一看反函数的复合是怎样的一个情况. [3]

[3] 理由不充分, 需要补

定理 2.3.13 (Inverse of Composition)**.**

$$\text{Both } f : A \to B \text{ and } g : B \to C \text{ are bijective}$$

1. $g \circ f$ is bijective
2. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
3. $f \circ g = I_B \wedge g \circ f = I_A \implies g = f^{-1}$

那么, 我们就从集合论的角度构建了我们高中学习过的内容.

第三章　无穷

3.1　简介

我们在高中的学习中, 对于极限的了解仅仅停留在表面和直观感受上. 那么, 我们有没有办法把这件事情严格化呢? 这是我们这次主要需要的事情.

> From his paradise that Cantor with us unfolded, we hold our breath in awe; knowing, we shall not be expelled.
>
> — David Hilbert

3.2　在 Cantor 以前

在《几何原本》中, Euclid 明确提出: “整体大于部分” 的公理. 但我们对无穷多个元素的集合而言, 部分是可以 “等于” 整体的.

考虑下面的两个集合:

$$S_1 = \{1, 2, 3, \cdots, n, \cdots\}$$

$$S_2 = \{1, 4, 9, \cdots, n^2, \cdots\}$$

我们可以给 S_1 的每一个 S_1 中的元素 a 做映射 a^2, 使得 $a^2 \in A_2$, 因此可以认为这是相等的. 但是明显的, $S_2 \subseteq S_1$. 这就是所说的 “部分等于全体”. 用我们有限的心智来讨论无限 $\cdots$

> “说到底，‘等于’、‘大于’ 和 ‘小于’ 诸性质不能用于无限，而只能用于有限的数量。”
> — Galileo Galilei

当时也有人反对使用 “无穷” 的论点, 认为这是一派胡言.

> “无穷数是不可能的。” — Gottfried Wilhelm Leibniz

但是 Cantor 坚定地认为, 以前我们的 “大于”, “小于” 那一套东西已经过时了, 要讨论 “无穷”, 当然要建立一套新的体系, 来帮助我们理解这一套内容.

> “这些证明一开始就期望那些数要具有有穷数的一切性质，或者甚至于把有穷数的性质强加于无穷。
>
> 相反，这些无穷数，如果它们能够以任何形式被理解的话，倒是由于它们与有穷数的对应，它们必须具有完全新的数量特征。

这些性质完全依赖于事物的本性，··· 而并非来自我们的主观任意性或我们的偏见。
”

— Georg Cantor (1885)

于是他们尝试使用映射的观念来定义无穷:

定义 3.2.1 (Dedekind-infinite & Dedekind-finite (Dedekind, 1888))**.** A set A is *Dedekind-infinite* if there is a bijective function from A to some proper subset B of A.

A set is *Dedekind-finite* if it is not Dedekind-infinite.

但是我们还没有定义 “finite” 和 “infinite”. 所以下面我们要用函数的观念来比较集合.

3.3 集合的比较

3.3.1 集合的个数相等

从开始的问题中, 我们可以看到, 只要出现了一个双射函数, 我们就可以说两个集合的元素个数相等. 于是给出如下定义:

定义 3.3.1 ($|A| = |B|$ ($A \approx B$) (1878))**.** A and B are *equipotent (等势)* if there exists a *bijection* from A to B.

一个集合其实是不关心这个集合元素的次序, 在 “势” 的考量下, 也不关心集合中的元素是什么, 就是两层抽象. 有时候也写作 $\overline{\overline{A}}$.

那么, 等势关系是一个等价关系吗? 不要关注太多, 要想证明远没有想象的那么简单.

定理 3.3.1. The “Equivalence Concept” of Equipotent For any sets A, B, C:

1. $A \approx B$
2. $A \approx B \implies B \approx A$
3. $A \approx B \wedge B \approx C \implies A \approx C$

有了 “势” 的概念, 我们就可以对 “有限” 进行定义了.

定义 3.3.2 (Finite)**.** X is finite if

$$\exists n \in \mathbb{N} : |X| = |n| = |\{0, 1, \ldots, n-1\}|.$$

我们很多时候写作 $|X| = n$. 这就意味着集合 X 是有穷的当且仅当它与某个自然数等势.

相反的, 我们可以定义无穷.

定义 3.3.3 (Infinite)**.** X is infinite if it is not finite:

$$\forall n \in \mathbb{N} : |X| \neq n.$$

我们既然定义了, 当然要说明它是存在的. 于是我们有这样的一个定理:

定理 3.3.2 (Existence of Infinite Sets!)**.** $\mathbb{N}$ is infinite.(So are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.)

我们可以使用反证法证明.

证明. 假设 $\exists n \in \mathbb{N}$, 使得 $|\mathbb{N}| = n$, 那么我们就存在 $f : \mathbb{N} \xleftrightarrow[onto]{1-1} \{0, 1, \cdots, n-1\}$.

下面, 我们构造限制映射 $g \triangleq f|_{\{0,1,\ldots,n\}} : \{0, 1, \cdots, n\} \to \{0, 1, \cdots, n-1\}$. 由于抽屉原理, g 不是一一映射, 那么 f 也不是一一映射.

□

我们注意到无穷也有几种. 比如有的无穷是可以一个一个计数清楚的, 有的无穷是不行的.

定义 3.3.4 (Infinite)**.** For any set X,

- Countably Infinite:
$$|X| = |\mathbb{N}| \triangleq \aleph_0$$
- Countable.
$$(\text{finite} \vee \text{countably infinite})$$
- Uncountable.
$$(\neg \text{ countable})$$
$$(\text{infinite}) \wedge \Big(\neg \ (\text{countably infinite})\Big)$$

自然的, 我们会发现 $\mathbb{Z}$ 是可数的. 如果我们把 $\mathbb{N}$ 的每一个元素扩大到原来了 2 倍, 中间就会稀疏一些, 可以容纳下负数.

Cantor 发现 $\mathbb{Q}$ 也是可数的. 因为 Cantor 是发现了一种数出有理数的方法. 其一句就是任何一个有理数 (quotient) 都可以成为形如 $a/b, \gcd(a, b) = 1$ 成比例的数. 如此:

$$\begin{array}{cccc} 1/1 & & & \\ 1/2 & 2/1 & & \\ 1/3 & 2/2 & 3/1 & \\ 1/4 & 2/3 & 3/2 & 4/1 \end{array}$$

因此, 有理数是可数的. 更进一步的, $\mathbb{N} \times \mathbb{N}$ 也是可数的. 因为我们只要做一个映射就行了. 具体的, 可以把 $\mathbb{N} \times \mathbb{N}$ 压缩到 $\mathbb{N}$ 上. 也就是 $\pi(k_1, k_2) = \frac{1}{2}(k_1 + k_2)(k_1 + k_2 + 1) + k_2$.

按照归纳的方法, 也就是 $\pi^{(n)}(k_1, \ldots, k_{n-1}, k_n) = \pi(\pi^{(n-1)}(k_1, \ldots, k_{n-1}), k_n) \quad (n \geq 3)$, 有如下的定理:

定理 3.3.3 ($\mathbb{N}^n$ is Countable.)**.**
$$|\mathbb{N}^n| = |\mathbb{N}|$$

进一步的推广, 我们有:

定理 3.3.4. The Cartesian product of finitely many countable sets is countable.

另外, 任意有限集的并集都是可数的, 我们还可以用刚刚的想法, 使用对角线计数.

再后来的研究中, 我们惊奇的发现, 有些无穷的大小之间是有着深刻的差别的. 例如, $\mathbb{R}$ 是不能够被数出来的. 同样也是用对角线证明法得到的结论.

定理 3.3.5 ($\mathbb{R}$ is Uncountable. (Cantor 1873-12; Published in 1874))**.**

$$|\mathbb{R}| \neq |\mathbb{N}|$$

这个定理就告诉我们了实数不能被表示成有理数的有序对. 这就说明了 $\mathbb{R}$ 是一个连续统. 另外一个惊人的事情是, $(0,1)$ 之间的实数和 $\mathbb{R}$, $\mathbb{R}\times\mathbb{R}$ 的势是一致的.

定理 3.3.6 ($|\mathbb{R}|$ (Cantor 1877))**.**

$$|(0,1)| = |\mathbb{R}| = |\mathbb{R}\times\mathbb{R}| = |\mathbb{R}^{n\in\mathbb{N}}|$$

一个可能的证明方式是考虑

$$(x = 0.a_1a_2a_3\cdots, y = 0.b_1b_2b_3\cdots) \mapsto 0.a_1b_1a_2b_2a_3b_3\cdots$$

但是很不幸, 这个证明是错误的. 严格的证明需要系统地学习数学分析才可以知道.

在成功证明这件事情之后, Cantor 写给 Dedekind 的一封信里面说到: "Je le vois, mais je ne le crois pas !" 翻译成英语就是 "I see it, but I don't believe it !". 可见这样对于 "无穷" 的探讨是十分激动人心同时也是令人感到违背常识的.

更惨的还在后面: 我们在《线性代数》课程和之前的理解上, 维数好像总是有限的. 但是 Cantor 的论述让我们对于 "维数" 的理解出现了很多问题. 其中一个问题是, 我们能不能通过一个双射把 m 维的东西映射到 n 维去?

定理 3.3.7 (Brouwer (Topological Invariance of Dimension))**.** There is no continuous bijections between $\mathbb{R}^m$ and $\mathbb{R}^n$ for $m \neq n$.

什么是 continuous 的双射? 这个就需要更多数学专业的知识了. 在这里不做阐述了.

3.4 连续统假设

连续统假设说明的是

$$\nexists A : \aleph_0 < |A| < \mathfrak{c}$$

事实上, 这是一个没有办法证明的命题.