数理逻辑

预备知识

姚宁远

yaony@fudan.edu.cn

复旦大学

哲学学院

目录

如何发现真？

- 经验-自然科学
- 数学知识为什么可靠？
- 证明本质上是什么？

例1：

- 一个正整数p是素数当且仅当$p \neq 1$且p只能被1和p整除；
- 31, 331, 3331, 33331, ... 均是素数；
- 333333331不是素数！

例2：费马定理

费马定理

对任意$n \geq 3$, 方程$x^n + y^n = z^n$有整数解。

- 方程$x^3 + y^3 + z^3 = w^3$有整数解是否有整数解？
- $(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42^3$;
- 方程$x^4 + y^4 + z^4 = w^4$有整数解是否有整数解？

例3：$\sqrt{2}$是无理数

证明：

- 设存在互素的整数a, b使得$\sqrt{2} = a/b$;
- $2b^2 = a^2$;
- a是偶数，故b是偶数。矛盾。

例3：无穷多个素数

证明：

- 设存在有限多个素数$p_1, ..., p_n$;
- $q = p_1 ... p_n + 1$;
- 则q不能被任何一个p_i整除。矛盾。

数学证明的

- 公理集;
- 推理规则;
- 定理。

目录

集合的表示

- $A = \{a_0, ..., a_n\}$;
- $\mathbb{N} = \{0, 1, 2, ...\}$;
- $A = \{x;\ P(x)\}$，　P是一个性质。
- $A = \{x;\ x$是红色的$\}$。
- $x \in A$表示x是A的一个元素。
- $x \notin A$表示x不是A的元素。

集合的外延原理

外延原理

一个集合完全由其元素确定，即集合A与B相同当且仅当A的元素都是B的元素，并且B的元素都是A的元素。

- $A = \{0, 1, 2, 3, 4, 5, 6\}$;
- $B = \{x |\ x$是自然数且$x^2 < 40\}$;
- $A = B$;
- $C = \{x;\ x$是实数并且$x^2 = 1\}$;
- $D = \{1, -1\}$;
- $C = D$。

集合的运算

- 交： $A \cap B = \{x : \ x \in A且x \in B\}$
- 并： $A \cup B = \{x : \ x \in A或者x \in B\}$
- 差： $A - B = \{x : \ x \in A且x \notin B\}$

子集、幂集和空集

- 子集： $A \subset B$ 表示A的元素都是B的元素，称A为B的子集;
- 幂集： A的所有子集构成的集合称为A的幂集，记作

$$\mathcal{P}(A) = \{x : x \subset A\};$$

- 空集： 不包含任何元素的集合称为空集，记作$\emptyset$。

集合族 I

集合族

如果集合$\mathcal{F}$的元素都是集合，则称$\mathcal{F}$是一个集合族。

一般交和一般并

设$\mathcal{F}$是一个集合族。

- 一般交：$\bigcap \mathcal{F} = \{x : \text{存在一个} F \in \mathcal{F} \text{使得} x \in F\}$
- 一般并：$\bigcup \mathcal{F} = \{x : \text{对每个一个} F \in \mathcal{F} \text{都有} x \in F\}$
- $\bigcap\{A, B\} = A \cap B$，$\bigcup\{A, B\} = A \cup B$

集合族 II

其他的表示

- 若$\mathcal{F}=\{F_0,...,F_n\}$，则

$$\bigcap\mathcal{F}=\bigcap_{i=0}^{i=n}F_i,\ \bigcup\mathcal{F}=\bigcup_{i=0}^{i=n}F_i.$$

- 若$\mathcal{F}=\{F_i:\ i\in\mathbb{N}\}$，则

$$\bigcap\mathcal{F}=\bigcap_{i\in\mathbb{N}}F_i,\ \bigcup\mathcal{F}=\bigcup_{i\in\mathbb{N}}F_i.$$

目录

关系

- 关系=集合+“结构”;
- 楼房=砖头+“结构”;
- 自然数上的序结构 $\mathcal{N}_1 = (\mathbb{N}, <)$:

$$0 < 1 < 2 < ...$$

- 自然数上的其他序结构 $\mathcal{N}_2 = (\mathbb{N}, \prec)$:

$$... \prec 6 \prec 4 \prec 2 \prec 0 \prec 1 \prec 3 \prec 5 \prec 7...$$

有序对

- 关系可以看作是一种对应或映射；
- 有序对来刻画： a与b有“关系”，表示为(a, b)；
- 当$a \neq b$时，总有$\{a, b\} = \{b, a\}$， 但是$(a, b) \neq (b, a)$；
- 有序性： $(a, b) = (a', b')$当且仅当$a = a'$且$b = b'$。

卡氏积

卡氏积

集合X与Y的卡氏积定义为

$$X \times Y = \{(x, y) : \ x \in X且y \in Y\}.$$

当$X = Y$时， 将$X \times X$记作X^2。

二元关系

- 称$R \subset X \times Y$为X到Y的一个二元关系；
- 如果$(x, y) \in R$，则称x和y有关系R。
- $(x, y) \in R$记作$R(x, y)$或者xRy。
- 如果$R \subset X^2$，则称R是X上的关系。

例：

- 整数上的整除关系：

$$R = \{(x, y) \in \mathbb{Z}^2 : \ x|y\}.$$

$(x, y) \in R \iff$ 存在$z \in \mathbb{Z}$使得$y = xz$；

- 整数上的“小于”关系；
- $R = \{(x, y) \in \mathbb{Z}^2 : \ $存在$z \in \mathbb{Z}$使得$x^2 + y^2 = z^2\}$。

二元关系 I

设R是一个二元关系

- R的定义域为：$\operatorname{dom} R = \{x : \text{存在} y \text{使得} R(x, y)\}$;
- R的值域为：$\operatorname{ran} R = \{y : \text{存在} x \text{使得} R(x, y)\}$;
- 集合X在R下的像定义为：

$$R[X] = \{y \in \operatorname{ran} R : \text{存在} x \in X \text{使得} R(x, y)\};$$

- 集合Y在R下的逆像定义为：

$$R^{-1}[Y] = \{x \in \operatorname{dom} R : \text{存在} y \in Y \text{使得} R(x, y)\};$$

二元关系 II

- R的逆定义为：

$$R^{-1} = \{(x, y) \in R : \ R(y, x)\};$$

- 二元关系R和S的复合定义为：

$$S \circ R = \{(x, z) : \text{ 存在}y\text{使得}R(x, y)\text{且}S(y, z)\}.$$

例： I

- $R = \{(x, y) : x, y \in \mathbb{R}且x = y\}$。 $R^{-1} = R且R \circ R = R$;
- 考虑$\mathbb{R}$上的关系$\geq, \leq$，则

$$\geq \circ \geq = \geq,\ \leq \circ \leq = \leq,\ \geq \circ \leq = \mathbb{R} \times \mathbb{R},\ \leq \circ \geq = \mathbb{R} \times \mathbb{R};$$

- 整数上的模n同余关系定义R为：

$$R(a, b) \iff n|(b - a)$$

$R(a, b)$习惯上记作$a \equiv b(\mod n)$。 验证： 对任意$x \in \mathbb{Z}$总有$R(x, x)$， 且

$$R^{-1} = R,\ R \circ R \subset R.$$

一般卡氏积 I

- 三元有序组定义为：

$$(x_1, x_2, x_3) =_{\text{def}} ((x_1, x_2), x_3)$$

- 四元有序组定义为：

$$(x_1, x_2, x_3, x_4) =_{\text{def}} ((x_1, x_2, x_3), x_4)$$

- 一般地，n 元有序组定义为：

$$(x_1, ..., x_n) =_{\text{def}} ((x_1, ..., x_{n-1}), x_n)$$

- n 个集合的卡氏积定义为：

$$X_1 \times ... \times X_n = \{(x_1, ..., x_n) : \ x_1 \in X_1, \ ..., \ x_n \in X_n\}$$

一般卡氏积 II

- $X^n =_{\text{def}} \underbrace{X \times \ldots \times X}_{n次}$;
- 若$R \subset X_1 \times \ldots \times X_n$， 则称$R$是一个$n$ 元关系;
- 若$R \subset X^n$， 则称X是X上的一个n 元关系;
- 若$R \subset X^n$， $Y \subset X$, 则$R' = R \cap Y^n$是Y上的n元关系，称R'是R在Y上的限制， R是R'的扩张。

目录

函数的定义 I

函数

设f是一个二元关系。如果对任意的$x \in \operatorname{dom} f$，存在唯一的$y \in \operatorname{ran} f$使得$(x, y) \in f$，则称$f$是一个函数。

- $(x, y) \in f$经常记作$f(x) = y$，或者$f : x \mapsto y$，并且称y为f在x处的值。
- 如果$X = \operatorname{dom} f$且$\operatorname{ran} f \subset Y$，则称$f$是$X$到$Y$的函数（关系），记作$f : X \longrightarrow Y$。
- 对任意的集合X，定义$\mathrm{id}_X : X \longrightarrow X$为$\mathrm{id}_X(x) = x$，则称$\mathrm{id}_X$是$X$上的等同函数。

函数的性质 I

定理1

函数f和g相等当且仅当$\operatorname{dom} f = \operatorname{dom} g$并且对每个$x \in \operatorname{dom} f$都有$f(x) = g(x)$

Proof.

- 函数是集合；
- 集合由其元素确定。

□

函数的性质 II

定理2

设f和g是函数，则它们的复合$g \circ f$也是函数。复合函数的定义域为$\mathrm{dom}(g \circ f) = f^{-1}[\mathrm{dom}\, g]$。对任意的$x \in \mathrm{dom}(g \circ f)$，有$(g \circ f)(x) = f(g(x))$。

函数的性质 III

Proof.

- $g \circ f$是一个二元关系；
- $(x,z),(x,z') \in g \circ f$当且仅当存在$y,y'$使得$(x,y) \in f$，$(y,z) \in g$，$(x,y') \in f$，$(y',z') \in g$；
- 由于f是函数，$y = y'$，由于g是函数，$z = z'$。故$g \circ f$是函数；
- $x \in \operatorname{dom}(g \circ f) \iff$ 存在z使得$(x,y) \in f$，$(y,z) \in g$。故

$$\operatorname{dom}(g \circ f) = \bigcup_{y \in \operatorname{dom} g} f^{-1}[\{y\}] = f^{-1}[\operatorname{dom} g].$$

□

其他记号

设$f : X \longrightarrow Y$是一个函数：

- 单射函数/一一映射： 对任意的$x, y \in X$，如果$f(x) = f(y)$，则$x = y$;
- 满射函数：$\operatorname{ran} f = Y$。满射不是函数f的性质，而是与Y的选取有关。
- 双射函数/一一对应：f既是单射又是满射。
- 如果$A \subset X$，则称$f \cap A \times Y$为f在A上的限制，记作$f \restriction A$，它也是一个函数。

目录

模n同余关系 I

回忆模n同余关系 [23] 具有一下性质:

- 对每个$x \in \mathbb{Z}$，有$x \equiv x \pmod{n}$;
- 设$x, y \in \mathbb{Z}$，如果$x \equiv y \pmod{n}$，则$y \equiv x \pmod{n}$;
- 设$x, y, z \in \mathbb{Z}$，如果$x \equiv y \pmod{n}$且$y \equiv z \pmod{n}$，则$x \equiv z \pmod{n}$;

模n同余关系 II

观察：

- $x \equiv x \pmod 2$当且仅当x与y有相同的奇偶性；
- $x \equiv x \pmod 2$将整数划分为两大类：奇数和偶数；
- 一般地，$x \equiv x \pmod n$当且仅当x与y除n有相同的余数；
- x除n有相同的可能的余数有$\{0, 1, ..., n-1\}$；
- $x \equiv x \pmod n$将整数划分为n大类。

模n同余的数是等价的

等价关系

等价关系

设$R \subset X^2$是一个二元关系，如果：

- 对每个$x \in X$，有$R(x,x)$，则称R是自反的；
- 对每个$x, y \in X$，如果$R(x,y)$则$R(y,x)$，则称R是对称的；
- 对每个$x, y, z \in X$，如果$R(x,y)$且$R(y,z)$，则有$R(x,z)$，则称R是传递的；
- 如果R是自反的，对称的，传递的，则称R是一个等价关系。

例：I

设P是所有人的集合：

- $D = \{(x, y) \in P^2 : x$是y的后代$\}$，
  则D不是自反的，不是对称的，是传递的；
- $B = \{(x, y) \in P^2 :$ 至少有一个x的祖先也是y的祖先$\}$，
  则B是自反的，是对称的，不是传递的；
- $S = \{(x, y) \in P^2 : x$的父母也是y的父母$\}$，
  则S是自反的，对称的，传递的。

例： II

其他等价关系：

- 任意集合上的相等“=”是等价关系；
- 平面上的直线之间的平行关系是等价关系；
- 在去掉原点的坐标平面上定义关系R为： $R(p,q)$当且仅当经过p和q的直线通过原点，则R是等价关系；
- 整数上的模n同余关系 是等价关系。

等价类

等价类

设$\sim$是X上的一个等价关系，$x \in X$。则x关于$\sim$的等价类是集合

$$[x]_{\sim} = \{t \in X | \ t \sim x\}.$$

当等价关系$\sim$清楚的时候，我们将$[x]_{\sim}$简记作$[x]$。

例：

- 集合X上的相等关系“=”的每个等价类中含有一个元素：$[x] = \{x\}$；
- 平面上的直线之间的平行关系的一个等价类是一族斜率相同的直线：$\{y = k_0 x + b : b \in \mathbb{R}\}$；
- 在去掉原点的坐标平面上定义等价关系R为：$R(p, q)$当且仅当经过p和q的直线通过原点。则每个等价类恰好构成一条过原点的（不含原点的）射线。
- 整数上的模n同余关系的等价类一共有n个，其中$[0] = \{nx : x \in \mathbb{Z}\}$。

性质

引理

设$\sim$是X上的一个等价关系，则对任意的$x, y \in X$，
有$[x]_\sim = [y]_\sim$或$[x]_\sim \cap [y]_\sim = \emptyset$。

Proof.

- 若$x \sim y$，则对任意的$t \in [x]_\sim$，有$t \sim x$。根据传递性，有$t \sim y$，从而$t \in [y]_\sim$，故$[x]_\sim \subset [y]_\sim$;
- 类似地，利用对称性，由$x \sim y$可以推出$[y]_\sim \subset [x]_\sim$。
- 若$x \nsim y$，则$[x]_\sim \cap [y]_\sim = \emptyset = \emptyset$。
- 否则设$u \in [x]_\sim \cap [y]_\sim$，则$u \sim x$且$u \sim y$。由对称性和传递性，由$x \sim y$。这是一个矛盾。

划分

划分

设X是一个集合，$S \subset \mathcal{P}(X)$。如果S满足：

- 对任意的$A, B \in S$，如果$A \neq B$，则$A \cap B = \emptyset$;
- $\bigcup S = X$;

则称S是X的一个划分。

商集

设X是一个集合，设$\sim$是 X上的一个等价关系，则

$$X/\sim =_{\text{def}} \{[x]_\sim : x \in X\}$$

称为X（关于$\sim$）的商集。

划分与商集I

定理1

设$\sim$是 X上的一个等价关系，则$X/\sim$是X的一个划分。

Proof.

$x \in [x]_\sim$ □

划分与商集II

定理2

设S是X是的一个划分，定义X上的关系：

$$\sim_S =_{\text{def}} \{(x,y) \in X^2 : \text{存在 } A \in S \text{ 使得 } x,y \in A\}$$

则$\sim_S$是等价关系。

Proof.

习题。 □

划分与商集III

定理3

- 设S是X的一个划分，则$X/\sim_S = S$;
- 设$\sim$是X上的等价关系，且$S = X/\sim$，则$\sim = \sim_S$。

Proof.

习题。 □

目录

线序 I

线序

设$R \subset X^2$是一个二元关系，如果R满足

- R是反对称的，即对每个$x, y \in X$，当$R(x, y)$且$R(y, x)$时，有$x = y$；
- R是传递的，即对每个$x, y, z \in X$，如果$R(x, y)$且$R(y, x)$，则有$R(x, z)$；
- 对每个$x, y \in X$，有$R(x, y)$或$R(y, x)$。

则称R是X上的线序/全序。

线序 II

例：

- $\mathbb{N}$， $\mathbb{Z}$， $\mathbb{Q}$， $\mathbb{R}$上的自然大小关系都是线序；
- $a < b < c < ...$是字母表上的线序；
- 字典中英文单词的排序是线序，称为字典序；
- 一般地，设X上有线序$<_X$，则$X \times ... \times X$依字典序也是一个线序。

偏序 I

偏序

设$\leq \subset X^2$是一个二元关系，如果$\leq$满足

- $\leq$是自反的，即对每个$x \in X$，有$x \leq x$；
- $\leq$是反对称的，即对每个$x, y \in X$，当$x \leq y$且$y \leq x$时，有$x = y$；
- $\leq$是传递的，即对每个$x, y, z \in X$，如果$x \leq y$且$y \leq z$，则有$x \leq z$；

则称$\leq$是X上的偏序/序。 一般用$(X, \leq)$表示$\leq$上X上的偏序，此时称X为偏序集。

偏序 II

例：

- 线序都是偏序；
- 对任意的集合X，$(\mathcal{P}(X), \subset)$是一个偏序集；
- 当X中至少有两个元素时，$(\mathcal{P}(X), \subset)$不是线序；
- 定义$n|m$为n整除m，则$|$是集合$\mathbb{Z} - \{0\}$上的偏序，但不是线序。

目录

结构的例子 I

域

结构的例子 II

一个域是一个集合F，其上有两个运算，记作加法 $+$ 和乘法 $\cdot$，满足以下性质：

- 对任意的$a, b, c \in F$， $a + (b + c) = (a + b) + c$;
- 对任意的$a, b \in F$， $a + b = b + a$;
- 存在一个元素，记作0，满足：对任意的$a \in F$, $a + 0 = a$;
- 对任意的$a \in F$， 存在$b \in F$使得 $a + b = 0$;
- 对任意的$a, b, c \in F$， $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- 对任意的$a, b \in F$， $a \cdot b = b \cdot a$;
- 存在一个元素，记作1，满足：对任意的$a \in F$, $a \cdot 1 = a$;
- 对任意的$a \in F$， 如果$a \neq 0$，则存在$b \in F$使得 $a \cdot b = 1$;
- 对任意的$a, b, c \in F$， $a \cdot (b + c) = a \cdot b + a \cdot b$。

结构的例子 III

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$都是域；
- 有限域$\mathbb{F}_p$；
- $\mathbb{F}_5[x] = \{a + bx : \ a, b \in \mathbb{F}_5\}$， 定义：

$$(a+bx)\cdot(c+dx) = (ac-bd)(\mod 5)+(ad+bc-bd)(\mod 5)x,$$

$$(a + bx) + (c + dx) = (a + c) + (b + d)x$$

则$\mathbb{F}_5[x]$是一个域，记作$\mathbb{F}_{5^2}$。

结构的例子 IV

皮亚诺算术

考虑结构$(\mathbb{N}, S, 0)$，其中$S : \mathbb{N} \longrightarrow \mathbb{N}$是后继函数。皮亚诺公理如下：

- 0是自然数；
- 如果n是自然数，则$S(n)$也是自然数；
- 0不是任何自然数的后继；
- 如果$S(n) = S(m)$，则$m = n$；
- （归纳原理）设Q是关于自然数的一个性质。如果
  - 0具有性质Q；
  - 如果n具有性质Q，则$S(n)$也具有性质Q，

  那么所有自然数都具有性质Q。