1 基本定义与性质

【定义1.1】（集合、元素）集合是事物的无序的组合 (A set is an unordered collection of objects)。集合中的事物称为集合的元素 (element, member)，称集合**包含 (contain)** 这些元素。

注：几何中的元素是无序的，且是互异的；集合中的元素可以是集合。

【定义1.2】（属于）如果集合 S 包含了元素 a，亦可称 a 属于集合 S，记作 $a \in S$。

【定义1.3】（不属于）如果集合 S 不包含元素 a，亦可称 a 不属于集合 S，记作 $a \notin S$。

【定义1.4】（相等，外延原则，不相等）两个集合相等当且仅当他们含有相同的元素。即若 A, B 是两个集合，那么 A 和 B 相等当且仅当 $\forall a \in A, a \in B$ 且 $\forall b \in B, b \in A$。记 A 和 B 相等为 $A = B$。其余情况 A 和 B 不相等，记作 $A \neq B$。

【定义1.5】（集合的构造）将集合中的元素需要满足的性质以如下方式列写，即可构造一个由所有的满足所有性质的元素构成的集合。

$$S = \{x | Prop_1(x), Prop_2(x), \dots, Prop_n(x)\}$$

其中，$Prop_i(x)$ 表示 x 满足第 i 条性质，x 为代表元，可替换为其他不含歧义的字母。

【定义1.6】（特殊集合）定义如下符号表示特殊集合：

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ 表示自然数集合；
- $\mathbb{N}^* = \mathbb{N}^+ = \{1, 2, 3, \dots\}$ 表示除0以外的自然数集合；
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ 表示整数集合；
- $\mathbb{Z}^* = \{\dots, -3, -2, -1, 1, 2, 3, \dots\}$ 表示除0以外的整数集合；
- $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ 表示正整数集合。
- $\mathbb{Q} = \{\frac{p}{q} | p \in Z, q \in Z, (p, q) = 1, q \neq 0\}$ 表示有理数集合；
- $\mathbb{R}$ 表示实数集合。
- U 全集，表示当前考虑范围下的所有可能元素 (all possible elements under consideration)。
- $\varnothing = \{\}$ 空集 (empty set, null set)，不含任何元素的集合。

【定义1.7】如果一个集合 S 只包含一个元素，称其为单项集（singleton set）。

【定义1.8】（子集）集合 A 称为集合 B 的子集当且仅当 A 中的任意元素都是 B 的元素，即 $\forall a \in A, a \in B$。记作 $A \subseteq B$。那么上述定义可以用逻辑形式表示为：

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

【定理1.1】对于任意集合 S，有基本关系：$S \subseteq S, \varnothing \subseteq S$。

【定义1.9】（真子集）如果集合 A 是集合 B 的子集，且 $A \neq B$，称 A 是 B 的真子集 (proper set)。记作 $A \subset B$，即

$$A \subset B \iff (A \subseteq B) \land \neg(A = B) \Leftrightarrow (A \subseteq B) \land (A \neq B)$$

【定义1.10】（有限集的势）如果 S 是一个集合，且 S 中恰好有 $n (n \geq 0)$ 个元素，我们称 S 是一个**有限集 (finite set)**，且 n 是集合 S 的**势 (cardinality)**，记 $|S| = n$。

【定义1.11】（幂集）给定集合 S，S 的**幂集 (power set)**是 S 的所有子集的集合，记作 $P(S)$ 或 $\mathrm{p}S$
。

【定理1.2】对于任意集合 A，$\varnothing \in P(S), A \in P(A)$；且如果 $|A| = n$，则 $|P(A)| = 2^n$。

证明：第一部分根据【定理1.1】和【定义1.11】显然；第二部分显然对于 A 的每一个元素可以选择取或者不取，于是共有 $2^{|A|}$ 种取出不同子集的方法，即 $|P(A)| = 2^{|A|}$。

【定义1.12】（维恩图 (Venn Diagram)）一种集合的几何直观表示。

【定义1.13】（集合并）设 A, B 是集合，集合的**并 (union)** 为一个包含 A, B 中所有元素的集合，记作 $A \cup B$。

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

【定义1.14】（集合交）设 A, B 是集合，集合的**交 (intersection)** 为一个包含了所有同时属于 A, B 的元素的集合，记作 $A \cap B$，即

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

【定义1.15】（集合的差）设 A, B 是集合，集合的**差 (difference)** 为一个包含了所有不属于 B 但是属于 A 的元素的集合，记作 $A - B$，也称为 B 在 A 中的补集，即

$$A - B = \{x | x \in A \wedge x \notin B\} = A \cap \bar{B}$$

【定义1.16】（集合的补）设 U 为全集，那么 A 的**（绝对）补 (complement)** 为 A 在 U 中的补集，即 $U - A$，记作 $-A$ 或 $\bar{A}$，即

$$\bar{A} = U - A = \{x | x \notin A\}$$

【定义1.17】（集合的对称差）设 A, B 是集合，集合的**对称差 (symmetric difference)** 定义为所有在 A 中或在 B 中、但是不在 $A \cap B$ 中的元素所组成的集合，记作 $A \oplus B$，即

$$A \oplus B = \{x | (x \in A \wedge x \in B) \wedge x \notin A \cap B\} = (A - B) \cup (B - A)$$

【定义1.18】（广义并）设 $A = \{A_1, A_2, \ldots, A_n\}$ 是集合的集合，则定义**广义并 (arbitrary unions)** 为

$$\cup A = A_1 \cup A_2 \cup \ldots \cup A_n$$

代表了 A 中含有的所有元素的集合，即至少属于 A 中的一个元素的元素所组成的集合，即为

$$\cup A = \{x | (\exists z)(z \in A \wedge x \in z)\}$$

【定义1.19】（广义交）设 $A = \{A_1, A_2, \ldots, A_n\}$ 是集合的集合，则定义**广义交 (arbitrary intersections)** 为

$$\cap A = A_1 \cap A_2 \cap \ldots \cap A_n$$

代表了 $A_1, A_2, \ldots, A_n$ 中都含有的元素的集合，即属于 A 的全部元素的元素所组成的集合，即为

$$\cap A = \{x | (\forall z)(z \in A \to x \in z\}$$

注：$\cup \varnothing = \varnothing$，而 $\cap \varnothing$ 未定义 (undefined)。

【定义1.20】（优先级）定义符号之间的优先级关系为

$$(()) \geq (\bar{A}, P(A), \cup A, \cap A) \geq (-, \cap, \cup, \oplus, \times) \geq (=, \subseteq, \subset, \in) \geq (\neg) \geq \ldots$$

后面接逻辑方面的符号优先级。同一优先级的符号从左到右依次计算。

【定理1.3】（集合的性质）

- 同一律 (identity laws)：$A \cup \varnothing = A, A \cap U = A$；
- 稀释律 (domination laws)：$A \cup U = U, A \cap \varnothing = \varnothing$；
- 幂等律 (idempotent laws)：$A \cup A = A, A \cap A = A$；

- 补集律 (complementation law)：$\overline{(\bar{A})} = A$;
- 交换律 (commutative laws)：$A \cup B = B \cup A, A \cap B = B \cap A$;
- 结合律 (associative laws)：$A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C$;
- 分配律 (distributive laws)：
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
- 摩根律 (De Morgan's laws)：$\overline{A \cup B} = \bar{A} \cap \bar{B}, \overline{A \cap B} = \bar{A} \cup \bar{B}$;
- 吸收律 (absorption laws)：$A \cup (A \cap B) = A, A \cap (A \cup B) = A$;
- 补余律 (complement laws)：$A \cup \bar{A} = U, A \cap \bar{A} = \varnothing$。

证明：所有以上性质都可以通过逻辑中的推导来证明，例如证明 De Morgan's law 的第二形式 $\overline{A \cap B} = \bar{A} \cup \bar{B}$:

$$A \cap B = \{x|x \notin A \cap B\} = \{x|\neg(x \in A \wedge x \in B)\} = \{x|x \notin A \vee x \notin B\} = \{x|x \in \bar{A} \cup \bar{B}\} = \bar{A} \cup \bar{B}$$

【定理1.4】（补集运算的性质）

- $A - B = A \cap -B$;
- $A - B = A - (A \cap B)$;
- $A \cup (B - A) = A \cup B$;
- $A \cap (B - C) = (A \cap B) - C$。

证明：

- $A - B = \{x|x \in A \wedge x \notin B\} = \{x|x \in A \wedge x \in -B\} = \{x|x \in A \cap -B\} = A \cap -B$;
- $$A - (A \cap B) = \{x|x \in A \wedge x \notin A \cap B\} = \{x|x \in A \wedge x \in \overline{A \cap B}\} = \{x|x \in A \wedge (x \in \bar{A} \vee x \in \bar{B})\}$$
  从而，$A - (A \cap B) = \{x|x \in A \wedge x \in \bar{B}\} = A - B$;
- $A \cup (B - A) = \{x|x \in A \vee (x \in B \wedge x \notin A)\} = \{x|x \in A \wedge x \in B\} = A \cup B$;
- $A \cap (B - C) = \{x|x \in A \wedge x \in B \wedge x \notin C\} = \{x|x \in (A \cap B) \wedge x \notin C\} = (A \cap B) - C$。

【定理1.5】（对称差运算的性质）

- $A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$;
- $A \oplus \varnothing = A, A \oplus A = \varnothing$;
- 交换律：$A \oplus B = B \oplus A$;
- 分配律：$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$;
- 结合律：$(A \oplus B) \oplus C = A \oplus (B \oplus C)$
- $A \oplus (A \oplus B) = B$

证明：(1) 用定义及逻辑的推导证明；(2) 利用 (1) 即可证明；(3) 利用 (1) 即可证明；(4) 利用 (1) 及分配律即可证明；(6) 是 (2) 和 (5) 的直接推论，下面证明 (5)：

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

同理可知，

$$(A \oplus B) \oplus C = (A \cup B \cup C) \cap (A \cup \bar{B} \cup \bar{C}) \cap (\bar{A} \cup \bar{B} \cup C) \cap (\bar{A} \cup B \cup \bar{C})$$

从而 $(A \oplus B) \oplus C = A \oplus (B \oplus C)$。

【定理1.6】（集合属于关系的性质）对于任何集合 A, B, C, D，

- $A \subseteq B \Longleftrightarrow (A \cup C) \subseteq (B \cup C) \Longleftrightarrow (A \cap C) \subseteq (B \cap C)$;
- $(A \subseteq B) \wedge (C \subseteq D) \Longrightarrow (A \cap C) \subseteq (B \cap D)$;

- $(A \subseteq B) \wedge (C \subseteq D) \Longrightarrow (A \cup C) \subseteq (B \cup D)$;
- $(A \subseteq B) \wedge (C \subseteq D) \Longrightarrow (A - D) \subseteq (B - C)$;
- $C \subseteq D \Longrightarrow (A - D) \subseteq (A - C)$。

证明：(1) (2) (3) 利用定义可证；(4) 可以利用 $\bar{D} \subseteq \bar{C}$ 代入 (3) 可知；(5) 是 (4) 的直接推论（令 $B = A$ ）。

【定理1.7】对于任意集合 A, B, C，证明： $A \cap B = A \cap C, A \cup B = A \cup C \Longrightarrow B = C$。

证明：反证，不失一般性，设 $\exists b \in B, b \notin C$。若 $b \in A$，则 $b \in A \cap B, b \notin A \cap C$，与 $A \cap B = A \cap C$ 矛盾；若 $b \notin A$，则 $b \in A \cup B, b \notin A \cup C$，与 $A \cup B = A \cup C$ 矛盾。因此，$B = C$。

【定理1.8】对于任意集合 A, B，$A - B = \varnothing \Longleftrightarrow A \subseteq B$。

证明：充分性根据定义显然，对于必要性，若 $A - B = \{x | x \in A \wedge x \notin B\} = \varnothing$，则 $(\forall x)\neg(x \in A \wedge x \notin B)$，即 $(\forall x)(\neg(x \in A) \vee x \in B) = (\forall x)(x \in A \to x \in B)$，从而 $A \subseteq B$。

【引理1.1】对于任意集合 A, B，$A \subseteq B \wedge B \subseteq A \Longleftrightarrow A = B$。

证明：根据定义显然。

【定理1.9】对于任意集合 A, B，$A \oplus B = \varnothing \Longleftrightarrow A = B$。

证明：一方面，若 $A \oplus B = (A - B) \cup (B - A) = \varnothing$，则 $A - B = \varnothing, B - A = \varnothing$，从而根据【定理1.8】有 $A \subseteq B, B \subseteq A$，从而根据【引理1.1】有 $A = B$；另一方面若 $A = B$，则 $A \cap B = A$，从而根据对称差定义，$A \oplus B = \varnothing$。

【定理1.10】（幂集的性质）对于任意集合 A, B;

- $A \subseteq B \Longleftrightarrow P(A) \subseteq P(B)$;
- $A = B \Longleftrightarrow P(A) = P(B)$;
- $P(A) \in P(B) \Longrightarrow A \in B$;
- $P(A) \cap P(B) = P(A \cap B)$;
- $P(A) \cup P(B) \subseteq P(A \cup B)$。

证明：

- 一方面，若 $A \subseteq B$，则 $\forall z \in P(A)$ 有 $z \subseteq A$，由于 $A \subseteq B$，从而 $z \subseteq B$，从而 $z \in P(B)$，所以 $P(A) \subseteq P(B)$；另一方面，若 $P(A) \subseteq P(B)$，则$\forall a \in A$，存在单项集合 $\{a\} \in P(A)$，于是 $\{a\} \in P(B)$，于是 $a \in B$，即 $A \in B$。
- 为 (1) 的直接推论。
- $P(A) \in P(B)$，则说明 $P(A) \subseteq B$，从而对于 $A \in P(A)$，$A \in B$。
- $\forall C$，$C \in P(A) \cap P(B) \Longleftrightarrow C \subseteq A \wedge C \subseteq B \Longleftrightarrow C \subseteq A \cap B \Longleftrightarrow C \in P(A \cap B)$。
- $\forall C$，$C \in P(A) \cup P(B) \Longleftrightarrow C \subseteq A \vee C \subseteq B \Longrightarrow C \subseteq A \cup B \Longleftrightarrow C \in P(A \cup B)$。

注：证明含有幂集的定理时，常用转换：$A \in P(B) \Longleftrightarrow A \subseteq B$。

【定理1.11】（广义交、广义并的性质）

- $\varnothing \neq A \subseteq B \Longrightarrow \cap B \subseteq \cap A$;
- $A \subseteq B \Longrightarrow \cup A \subseteq \cup B$;
- $A \cup \cap B = \cap\{A \cup X | X \in B\} \quad (B \neq \varnothing)$;
- $A \cap \cup B = \cup\{A \cap X | x \in B\}$。

证明：

- $\forall x \in \cap B, \forall B_i \in B, x \in B_i$，由于 $A \subseteq B$，故 $\forall A_i \in A, A_i \in B$，则 $x \in A_i$，故 $x \in \cap A$。故 $\cap B \subseteq \cap A$
- $\forall x \in \cup A, \exists A_i \in A, x \in A_i$，由于 $A \subseteq B$，故 $A_i \in B$，从而 $x \in \cup B$，从而 $\cup A \subseteq \cup B$。

- (3), (4) 根据定义可知。

2 关系与函数

【定义2.1】（有序数对）定义**有序数对 (Ordered pairs)** $\langle x, y\rangle \stackrel{def}{=} \{\{x\},\{x, y\}\}$。

【定理2.1】（有序数对的唯一性）$\langle u, v\rangle=\langle x, y\rangle \Longleftrightarrow u=x \wedge v=y$

证明：充分性显然，必要性则有 $\{\{x\},\{x, y\}\}=\{\{u\},\{u, v\}\}$，从而只能 $\{x\}=\{u\},\{x, y\}=\{u, v\}$，从而 $x=u, y=v$。

【定义2.2】（笛卡尔积）定义 $A \times B=\{\langle x, y\rangle \mid x \in A \wedge y \in B\}$ 为集合 A 和 B 的**笛卡尔积 (Cartesian Product)** 。

【定义2.3】（有序 n 元组）若 $n \in \mathbb{N}$ 且 $n>1$，对于 n 个元素 $x_1, x_2, \ldots, x_n$，称 $\langle x_1, x_2, \ldots, x_n\rangle$ 为**有序 n 元组 (Ordered n-tuples)**，递归定义为：

若 $n=2$，即为 $\langle x_1, x_2\rangle$；

若 $n>2$，则为 $\langle\langle x_1, x_2, \ldots, x_{n-1}\rangle, x_n\rangle$。

【定义2.4】（ n 个集合的笛卡尔积）定义 $A_1 \times A_2 \times \ldots \times A_n=\{\langle x_1, x_2, \ldots, x_n\rangle \mid x_i \in A_i(i=1,2, \ldots, n)\}$ 为 n 个集合的笛卡尔积。

【定理2.2】对于任意集合 A, B 和集合 $C \neq \varnothing$，

- $A \times \varnothing=\varnothing \times B=\varnothing$；
- $A \neq \varnothing, B \neq \varnothing, A \neq B \Longrightarrow A \times B \neq B \times A$；
- $A \times(B \times C) \neq(A \times B) \times C$。

证明：(1) (2) 显然用定义即可说明；(3) 由于左右两边集合的元素利用 Ordered-pair 定义的时候形式不同。

【定理2.3】对于任意集合 A, B, C，

- $x \in A, y \in A \Longrightarrow\langle x, y\rangle \in P(P(A))$；
- $A \times(B \cup C)=(A \times B) \cup(A \times C)$；
- $A \times(B \cap C)=(A \times B) \cap(A \times C)$；
- $(A \cup B) \times C=(A \times C) \cup(B \times C)$；
- $(A \cap B) \times C=(A \times B) \cap(A \times C)$。

证明：(1) 需要利用【定义2.1】中对于 ordered-pair 的定义；(2) ~ (5) 利用定义即可证明。

【定理2.4】对于任意集合 A, B, C，如果 $C \neq \varnothing$，

$$A \subseteq B \Longleftrightarrow A \times C \subseteq B \times C \Longleftrightarrow C \times A \subseteq C \times B$$

证明：利用笛卡尔积的定义即可证明。

【定理2.5】对于任意非空集合 A, B, C, D，

$$A \times B \subseteq C \times D \Longleftrightarrow A \subseteq C \wedge B \subseteq D$$

证明：充分性显然，下面证明必要性。

$\forall a \in A, \exists b \in B,\langle a, b\rangle \in A \times B \subseteq C \times D$，所以 $a \in C$，于是 $A \subseteq C$；$B \subseteq D$ 同理可得。

【定义2.5】（关系）有序数对的集合是**关系 (relation)**。若 R 是关系且 $\langle x, y\rangle \in R$ ，可简记为 $x R y$。

【定义2.6】（定义域、值域、域）如果 R 是关系，则定义 R **的定义域 (the domain of R,** $\operatorname{dom} R$**)**，R **的值域 (the range of R,** $\operatorname{ran} R$**)**，R **的域 (the field of R,** $\operatorname{fld} R$**)** 为：

- $x \in \mathrm{dom}R \iff (\exists y)xRy$
- $y \in \mathrm{ran}R \iff (\exists x)xRy$
- $\mathrm{fld}R = \mathrm{dom}R \cup \mathrm{ran}R$

【引理2.1】如果 $\langle x, y\rangle \in A$，那么 $x \in \cup\cup A, y \in \cup\cup A$。

证明：$\{\{x\}, \{x, y\}\} \in A$，从而 $\{x, y\} \in \cup A$，从而 $x \in \cup\cup A, y \in \cup\cup A$。

【定义2.7】（定义域、值域、域的等价描述）由【引理2.1】，【定义2.6】可重新表述为：

- $\mathrm{dom}R = \{x \in \cup\cup R | (\exists y)xRy\}$
- $\mathrm{ran}R = \{y \in \cup\cup R | (\exists x)xRy\}$
- $\mathrm{fld}R = \cup\cup R$

【定义2.8】（n 元关系）n **元关系 (n-ary relations)**是有序 n 元组的集合，是 n 个集合笛卡尔积的子集。

【定义2.9】（逆）若 R 是关系，定义 R 的**逆 (inverse)** 为

$$R^{-1} = \{\langle u, v\rangle | vRu\}$$

【定义2.10】（复合）若 F, G 是关系，定义 F 和 G 的**复合 (composition)**为

$$F \circ G = \{\langle u, v\rangle | (\exists t)(uGt \wedge tFv)\}$$

【定义2.11】（限制）若 F 是关系，A 是集合，则 F **对** A **的限制 (the restriction of F to A)** 定义为

$$F \uparrow A = \{\langle u, v\rangle | uFv \wedge u \in A\}$$

【定义2.12】（像）若 F 是关系，A 是集合，则 A **在** F **下的像 (the image of A under F)** 定义为

$$F[A] = \mathrm{ran}(F \uparrow A) = \{v | (\exists u)(u \in A \wedge uFv)\}$$

注：inverse, composition 和 restriction 都是 ordered-pairs 的集合，而 image 是 elements 的集合。

【定理2.6】若 R 是从 X 到 Y 的关系，S 是从 Y 到 Z 的关系，则

- $\mathrm{dom}(R^{-1}) = \mathrm{ran}(R), \mathrm{ran}(R^{-1}) = \mathrm{dom}(R)$；
- $(R^{-1})^{-1} = R$；
- $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$。

证明：按照定义证明即可。

【定理2.7】（复合的结合律）如果 Q, S, R 分别是 $X \to Y, Y \to Z, Z \to W$ 的关系，则

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

证明：按照定义即可。

注：复合一般来说不满足交换律，即一般地，$A \circ B \neq B \circ A$。

【定理2.8.1】（复合对于交、并的分配律1）如果 R_1 是 $Y \to Z$ 的关系，R_2, R_3 是 $X \to Y$ 的关系，那么

- $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$；
- $R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$；

证明：

- $\forall \langle x, z\rangle$，
  $x(R_1 \circ (R_2 \cup R_3))z \iff (\exists y)(x(R_2 \cup R_3)y \wedge yR_1 z) \iff (\exists y)((xR_2 y \vee xR_3 y) \wedge yR_1 z)$

$\iff (\exists y)((xR_2y \wedge yR_1z) \vee (xR_3y \wedge yR_1z)) \iff (\exists y)(xR_2y \wedge yR_1z) \vee (\exists y)(xR_3y \wedge yR_1z)$
$\iff x((R_1 \circ R_2) \cup (R_1 \circ R_3))z$

- $\forall \langle x, z \rangle$,
  $x(R_1 \circ (R_2 \cap R_3))z \iff (\exists y)(x(R_2 \cap R_3)y \wedge yR_1z) \iff (\exists y)((xR_2y \wedge xR_3y) \wedge yR_1z)$
  $\iff (\exists y)((xR_2y \wedge yR_1z) \wedge (xR_3y \wedge yR_1z)) \implies (\exists y)(xR_2y \wedge yR_1z) \wedge (\exists y)(xR_3y \wedge yR_1z)$
  $\iff x((R_1 \circ R_2) \cap (R_1 \circ R_3))z$

【定理2.8.2】（复合对于交、并的分配律2）如果 R_1, R_2 是 $Y \to Z$ 的关系，R_3 是 $X \to Y$ 的关系，则

- $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$；
- $(R_1 \cap R_2) \circ R_3 \subseteq (R_1 \circ R_3) \cap (R_2 \circ R_3)$。

证明：和【定理2.8.1】完全类似。

【定理2.9】设 $A, B \subseteq X$，R 是一个 $X \to Y$ 的关系，则

- $R[A \cup B] = R[A] \cup R[B]$;
- $R[\cup \mathcal{A}] = \cup\{R[B] | B \in \mathcal{A}\}$;
- $R[A \cap B] \subseteq R[A] \cap R[B]$;
- $R[\cap \mathcal{A}] \subseteq \cap\{R[B] | B \in \mathcal{A}\}$;
- $R[A] - R[B] \subseteq R[A - B]$。

证明：

- $\forall y$,
  $y \in R[A \cup B] \iff (\exists x)(x \in A \cup B \wedge xRy) \iff (\exists x)((x \in A \wedge xRy) \vee (x \in B \wedge xRy))$
  $\iff (\exists x)(x \in A \wedge xRy) \vee (\exists x)(x \in B \wedge xRy) \iff y \in (R[A] \cup R[B])$;
- 是 (1) 的推论；
- $\forall y$,
  $y \in R[A \cap B] \iff (\exists x)(x \in A \cap B \wedge xRy) \iff (\exists x)((x \in A \wedge xRy) \wedge (x \in B \wedge xRy))$
  $\implies (\exists x)(x \in A \wedge xRy) \wedge (\exists x)(x \in B \wedge xRy) \iff y \in (R[A] \cap R[B])$;
- 是 (3) 的推论；
- $\forall y \in R[A] - R[B]$，有 $(\exists x)(x \in A \wedge xRy)$ 且 $(\forall x')(x' \in B \to \neg x'Ry)$，从而 $x \notin B$，从而 $x \in A - B$，从而 $y \in R[A - B]$。

【定义2.13】（函数）一个**函数 (function)** 是一个关系 F 满足 $\forall x \in \mathrm{dom}F$，仅有一个 y 满足 xFy，那么 y 叫做 F 在 x 处的函数值，记作 $F(x) = y$。

【定义2.14】（映射，满射，单射，双射）我们说 F 是一个从 A 到 B 的映射（或 F 将 A 映射到 B）当且仅当 F 是一个满足 $\mathrm{dom}F = A, \mathrm{ran}F \subseteq B$ 的函数；特别地，如果 $\mathrm{ran}F = B$，我们称 F 是一个**满射 (surjective function)**；如果对于任意 $x, y \in \mathrm{dom}F$，若 $x \neq y$ 则 $F(x) \neq F(y)$，称 F 是一个**单射 (injective function)**；如果 F 既是满射又是单射，称 F 是一个**双射 (bijective function)。**

【定义2.15】（单根）关系 R 是**单根 (single-rooted)**的当且仅当对于任意 $y \in \mathrm{ran}R$，只存在唯一的 $x \in \mathrm{dom}R$ 满足 xRy。

【定理2.10】函数 F 是单根的等价于函数 F 是单射。

【定义2.16】（单位函数）对于任意非空集合 A，**单位函数 (identity function)** $I_A : A \to A$ 定义为：

$$I_A(x) = x \quad (\forall x \in A)$$

显然单位函数是一个双射。

【定理2.11】对于函数 f, g，若 $g : A \to B, f : B \to C$，那么 $f(g(x)) = (f \circ g)(x)$。

【定理2.12】对于关系 F，有 $\mathrm{dom}(F^{-1}) = \mathrm{ran}F, \mathrm{ran}(F^{-1}) = \mathrm{dom}F$，且 $(F^{-1})^{-1} = F$。

【定理2.13】对于关系 F，F^{-1} 是一个函数当且仅当 F 是单根的；F 是一个函数当且仅当 F^{-1} 是单根的。

以上三个定理均可以用定义说明。

【定理2.14】如果函数 F 是双射，那么如果 $x \in \mathrm{dom}F$，那么 $F^{-1}(F(x)) = x$；如果 $y \in \mathrm{ran}F$，那么 $F(F^{-1}(y)) = y$。

证明：设 $x \in \mathrm{dom}F$，那么 $\langle x, F(x)\rangle \in F, \langle F(x), x\rangle \in F^{-1}$，所以 $F(x) \in \mathrm{dom}(F^{-1})$。由于 F 是双射，那么由【定理2.13】知 F^{-1} 是一个函数，所以 $F^{-1}(F(x)) = x$。另一部分同理可得。

【定理2.15】如果 F, G 是函数，那么 $F \circ G$ 是函数，且 $\mathrm{dom}(F \circ G) = \{x | x \in \mathrm{dom}G \wedge G(x) \in \mathrm{dom}F\}$，且 $\forall x \in \mathrm{dom}(F \circ G), (F \circ G)(x) = F(G(x))$。

证明：首先说明 $F \circ G$ 是函数，设 $x(F \circ G)y$ 且 $x(F \circ G)y'$，则 $(\exists c)(c = G(x) \wedge F(c) = y)$ 且 $(\exists c')(c' = G(x) \wedge F(c') = y')$。由于 G 是函数，则 $c' = G(x) = c$，所以 $y' = F(c') = F(c) = y$，从而 $F \circ G$ 是函数。剩下的结论显然。

【定理2.16】如果 F, G 是关系，那么 $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$。

证明：首先，$(F \circ G)^{-1}$ 和 $G^{-1} \circ F^{-1}$ 都是关系，故

$$\begin{gathered}\langle x, y\rangle \in (F \circ G)^{-1} \iff \langle y, x\rangle \in (F \circ G) \iff (\exists t)(yGt \wedge tFx) \iff (\exists t)(xF^{-1}t \wedge tG^{-1}y) \\ \iff \langle x, y\rangle \in G^{-1} \circ F^{-1}\end{gathered}$$

【定理2.17】设 $F: A \to B$ 是函数，且 A 非空，则：

- 存在函数 $G: B \to A$（左逆），使得 $G \circ F = I_A$ 当且仅当 F 是单射。
- 存在函数 $H: B \to A$（右逆），使得 $F \circ H = I_B$ 当且仅当 F 是满射。

证明：

- 必要性，若 $x \neq y$ 且 $F(x) = F(y)$，从而 $x = G(F(x)) = G(F(y)) = y$，矛盾，从而 F 是单射；充分性，若 F 是单射，则取定 $a \in A$，存在函数 G 定义如下
$$\begin{gathered}G(x) = F^{-1}(x) \quad (x \in \mathrm{ran}F) \\ G(x) = a \quad (x \in B - \mathrm{ran}F)\end{gathered}$$
使得 $G \circ F = I_A$。
- 必要性，$\forall b \in B$，$(F \circ H)(b) = F(H(b)) = b$，从而 F 是满射；充分性，若 F 是满射，当构造 H 时，若存在 $x_1, x_2, \ldots, x_n$，使得 $F(x_i) = b$，则 $H(b)$ 的值应该选择哪一个呢？这就需要【公理1】（第一形式选择公理）。

【公理1】（第一形式选择公理 **Axiom of Choice 1st, AC (first form)**）对于任意关系 R，可以找到函数 H，满足 $H \subseteq R$，且 $\mathrm{dom}H = \mathrm{dom}R$。

有了选择公理，对于关系 $R = F^{-1}$，即可构造出 H，证明【定理2.17】的正确性。

【定理2.18】下面定理对于任意关系 F 成立（F 不必为函数）

- $F[A \cup B] = F[A] \cup F[B], F[\cup A] = \cup\{F[a] | a \in A\}$
- $F[A \cap B] \subseteq F[A] \cap F[B], F[\cap A] \subseteq \cap\{F[a] | a \in A\}$，且 F 单射时取等（对于广义交需要满足 $A \neq \varnothing$）
- $F[A] - F[B] \subseteq F[A - B]$，且 F 单射时取等

证明：

- $\forall y$,
$y \in F[A \cup B] \iff (\exists x)(x \in A \cup B \wedge xFy) \iff (\exists x)(x \in A \wedge xFy) \vee (\exists x)(x \in B \wedge xFy)$
$\iff y \in F[A] \cup F[B]$，广义并类似。

- $\forall y$,
  $y \in F[a \cap B] \iff (\exists x)(x \in A \cap B \wedge xFy) \implies (\exists x)(x \in A \wedge xFy) \wedge (\exists x)(x \in B \wedge xFy)$
  $\iff y \in F[A] \cap F[B]$，若 F 单射，则存在唯一的 x 使得 xFy，从而上式的 $\implies$ 可以替换为 $\iff$；广义交类似。
- $\forall y \in F[A] - F[B]$，$y \in F[A] \wedge y \notin F[B] \iff (\exists x)(x \in A \wedge xFy) \wedge (\forall x')(x'Fy \to x' \notin B)$ $\implies (\exists x)(x \in A \wedge x \notin B \wedge xFy) \iff y \in F[A - B]$，若 F 单射，则存在唯一的 x 使得 xFy，从而上式的 $\implies$ 可以替换为 $\iff$。

【定义2.17】对于集合 A, B，我们将所有 $A \to B$ 的函数 F 组成一个集合，记作 ${}^AB$，即

$$
{}^AB = \{F | (F : A \to B) \wedge (F\ is\ a\ function)\}
$$

【定义2.18】（无限笛卡尔积）定义 **无限笛卡尔积 (Infinite Cartesian Products)** 为

$$
\times_{i \in I} H(i) = \{f | (\mathrm{dom} f = I) \wedge (f\ is\ a\ function) \wedge (\forall i \in I)(f(i) \in H(i))\}
$$

那么，$\times_{i \in I} H(i)$ 的元素被称为 **I-组 (I-tuples)**。

【公理2】（第二形式选择公理 **Axiom of Choice 2nd, AC (second form)**）$\forall I$，$\forall H$，H 是函数且 $\mathrm{dom} H = I$，如果 $\forall i \in I, H(i) \neq \varnothing$，那么

$$
\times_{i \in I} H(i) \neq \varnothing
$$

【定理2.19】第一形式选择公理和第二形式选择公理等价，即【公理1】等价于【公理2】。

【定义2.19】（自反，对称，反对称，传递，逆自反）设二元关系 R 定义在集合 A 上。

- 若 $(\forall a)(a \in A \wedge aRa)$，则称 R 有**自反性 (reflexive)**；
- 若 $(\forall a)(\forall b)(a \in A \wedge b \in A \wedge (aRb \to bRa))$，则称 R 有**对称性 (symmetric)**；
- 若 $(\forall a)(\forall b)(a \in A \wedge b \in A \wedge ((aRb \wedge a \neq b) \to \neg(bRa)))$，则称 R 有 **反对称性 (anti-symmetric)**；
- 若 $(\forall a)(\forall b)(\forall c)(a \in A \wedge b \in A \wedge c \in A \wedge ((aRb \wedge bRc) \to aRc))$，则称 R 有**传递性 (transitive)**；
- 若 $(\forall a)(a \in A \wedge \neg(aRa))$，则称 R 有**逆自反性 (anti-reflexive)**。

【定义2.20】（等价关系 **(equivalence relation)**）定义 R 是等价关系，当且仅当二元关系 R 定义在集合 A 上，且在 A 上具有自反性、对称性、传递性。

【定理2.20】如果 R 是一个具有对称性、传递性的关系，则 R 是一个 $\mathrm{fld}R$ 上的等价关系。

证明：

- 首先，$\forall x \in \mathrm{dom}R, \exists y \in \mathrm{ran}R$，满足 xRy；$\forall x \in \mathrm{ran}R, \exists y \in \mathrm{dom}R$，满足 yRx，由对称性即 xRy；因此 $\forall x \in \mathrm{fld}R, \exists y$，满足 xRy 或 yRx；
- $\forall x \in \mathrm{fld}R, \exists y$ 满足 xRy，从而运用对称性有 yRx，再运用传递性有 xRx，从而在 $\mathrm{fld}R$ 上具有自反性；
- R 自身具有对称性、传递性，因此 R 是 $\mathrm{fld}R$ 上的等价关系。

注：对称性和传递性可以继承！

【定义2.21】定义 $[x]_R$ 为

$$
[x]_R = \{t | xRt\}
$$

【定理2.21】如果 R 是 A 上的等价关系，那么若 $x, y \in A$，那么

$$
[x]_R = [y]_R \iff xRy
$$

证明：必要性，由 R 是 A 上等价关系知 $[x]_R \neq \varnothing, [y]_R \neq \varnothing$，由 $[x]_R = [y]_R$，$\exists t \in [x]_R = [y]_R, xRt \wedge yRt$，从而由对称性有 $xRt \wedge tRy$，从而由传递性有 xRy；若 xRy，则 $\forall t \in [x]_R, xRt$，由于 xRy 及对称性有 yRx，由传递性 yRt，从而 $t \in [y]_R$，故 $[x]_R \subseteq [y]_R$，同理有 $[y]_R \subseteq [x]_R$，故 $[x]_R = [y]_R$。

【定义2.22】（分划）一个集合 A 的**分划 (partition)** π 是一个 A 的不相交但详尽的（即并集为全集）子集的集合，即

- 没有两个 π 中的集合含有相同的元素；
- 每个 A 中的元素都存在于 π 中的集合中。

【定理2.22】如果 R 是 A 上的等价关系，那么 $\{[x]_R|x \in A\}$ 组成了 A 上的分划 π。

证明：如果有 $t \in [x]_R$ 且 $t \in [y]_R$ 且 $\neg(xRy)$，则 xRt, yRt，根据对称、传递性有 xRy，矛盾。因此若 $\neg(xRy)$，$[x]_R \cap [y]_R = \varnothing$。若 xRy，由【定理2.21】知 $[x]_R = [y]_R$；所以若 $[x]_R \neq [y]_R$，则必有 $[x]_R \cap [y]_R = \varnothing$；而且 $\{[x]_R|x \in A\}$ 包含了所有的 A 中元素（由于 R 有自反性），所以其组成了 A 上分划。

【定义2.23】（商集）如果 R 是 A 上的等价关系，那么**商集 (quotient set)** A/R 定义为

$$A/R = \{[x]_R|x \in A\}$$

注：A/R 可念作 A modulo R。

【定义2.24】（自然映射）定义**自然映射 (natural map)** 或**规范映射 (canonical map)** $\alpha : A \to A/R$ 为

$$\alpha(x) = [x]_R$$

【定义2.25】（线性序）设 A 为集合，A 上的**线性序 (linear order)** 或 **全序 (total order)** 是一个 A 上的二元关系 R 满足如下两个条件：

- R 具有传递性；
- R 具有 A 上的**三岐性 (trichotomy)**，即 $\forall x, y \in A$，以下三个式子仅成立一项：

$$xRy, x = y, yRx$$

【定理2.23】如果 R 是 A 上的线性序，必然有

- 不存在 x 使得 xRx；
- $\forall x, y \in A$，若 $x \neq y$，则必有 xRy 或 yRx 成立。

证明显然。

注：这说明了一个线性序 R 不会成环！

【定义2.26】（偏序）设 A 为非空集合，R 是 A 上的二元关系，若 R 满足自反性、反对称性、传递性，则称 R 是 A 上的**偏序 (partial order)**。

【定义2.27】（传递闭包）设 A 为非空集合，R 是 A 上的二元关系，R 在 A 上的**传递闭包 (transitive closure)** R^+ 为最小的包含 R 的具传递性的关系。特别地，若 R 满足传递性，则 $R^+ = R$。

【定理2.24】（传递闭包的构造）我们定义 $R^0 = R$，定义 R^i 为

$$R^i = R^{i-1} \cup \{\langle s_1, s_3\rangle \,|(\exists s_2)(\langle s_1, s_2\rangle \in R^{i-1} \wedge \langle s_2, s_3\rangle \in R^{i-1})\}$$

那么显然有 $R^+ = \cup_{i \in \mathbb{N}} R^i$。

【定义2.28】（自反闭包）设 A 为非空集合，R 是 A 上的二元关系，R 在 A 上的**自反闭包 (reflexive closure)** R_R 为最小的包含 R 的在 A 上具自反性的关系。特别地，若 R 满足 A 上的自反性，则 $R_R = R$。

【定理2.25】（自反闭包的构造）$R_R = R \cup \{\langle x, x\rangle \,| x \in A\} = R \cup I_A$。

【定义2.29】（对称闭包）设 A 为非空集合，R 是 A 上的二元关系，R 在 A 上的**对称闭包 (symmetric closure)** S_R 为最小的包含 R 的具对称性的关系。特别地，若 R 满足对称性，则 $S_R = R$。

【定理2.26】（对称闭包的构造）$S_R = R \cup \{\langle x, y\rangle \mid \langle y, x\rangle \in R\} = R \cup R^{-1}$。

3 悖论和基数

【定理3.1】（罗素悖论）不存在一个集合，任意集合都属于他。

证明：令 A 为任意一个集合，我们将构造一个集合 B，$B \notin A$。

令 $B = \{x \in A | x \notin x\}$

我们说明 $B \notin A$：由集合的构造知，$B \in B$ 当且仅当 $B \in A \wedge B \notin B$。

若 $B \in A$，则说明了 $B \in B$ 当且仅当 $B \notin B$。

矛盾，故必然有 $B \notin A$。

【定义3.1】（自然数集合定义）**冯·诺依曼自然数集合定义 (von Neumann's natural number definition)** 每个自然数是比他小的所有元素的集合。即，$0 = \varnothing, 1 = \{0\} = \{\varnothing\}, 2 = \{1, 0\} = \{\{\varnothing\}, \varnothing\}, \ldots$，以此类推。将自然数集合另外记作 ω。

【定理3.2】（自然数集合定义的性质）

- $0 \in 1, 1 \in 2, 2 \in 3, \ldots, i \in j (i < j);$
- $0 \subseteq 1 \subseteq 2 \subseteq 3 \ldots, i \subseteq j (i < j)$。

根据定义显然。

【定义3.2】（等势）集合 A 和集合 B **等势 (equinumerous)**当且仅当有一个双射函数 $f : A \to B$，记作 $A \approx B$。其中，这个双射函数被称为一个 A 与 B 间的**一一对应 (one-to-one correspondence)**。

【例3.1】下面两个集合等势：

- $\omega \times \omega \approx \omega$
- $\omega \approx \mathbb{Q}$
- $(0, 1) \approx \mathbb{R}$
- $(0, 1) \approx (n, m)$
- $[0, 1] \approx (0, 1), [0, 1] \approx [0, 1), [0, 1] \approx (0, 1]$

【定理3.3】（等势的自反性、对称性、传递性）对于任意集合 A, B, C，

- $A \approx A$
- $A \approx B \Longrightarrow B \approx A$
- $A \approx B, B \approx C \Longrightarrow A \approx C$

【定理3.4】ω 和 $\mathbb{R}$ 不等势；不存在集合 A 和其幂集 $P(A)$ 等势。

证明：

- 说明对于任意 $f : \omega \to \mathbb{R}$，存在 $z \in \mathbb{R}, z \notin \operatorname{ran} f$。构造 z 如下：整数部分为0，小数部分第 i 位构造为 $f(i)$ 的小数后第 i 位，则 $\forall t \in \omega, z \neq f(t)$。则 $z \in \mathbb{R}, z \notin \operatorname{ran} f$，所以 ω 和 $\mathbb{R}$ 不等势。

- 同理，说明对于任意 $f: A \to P(A)$，存在 $B \in P(A)$ （即 $B \subseteq A$）且 $B \notin \mathrm{ran} f$。令 $B = \{x \in A | x \notin f(x)\}$，则 $B \subseteq A$ 即 $B \in P(A)$。但是对于任意 $x \in A$，$x \in B \Longleftrightarrow x \notin f(x)$，从而，故不存在 $x \in A$，$f(x) = B$，因为如果成立则 $x \in B \Longleftrightarrow x \notin B$，矛盾。从而 A 和 $P(A)$ 不等势。

【定义3.3】（优势）集合 B **优势 (dominate)** 于集合 A 当且仅当存在一个单射 $f: A \to B$。记作 $A \preceq B$。

【定理3.5】设 A, B 为集合。

- 任意集合优势于其自身；
- 如果 $A \subseteq B$，那么 $A \preceq B$。
- $A \preceq B$ 当且仅当 A 和 B 的一个子集 B' 等势。

【定理3.6】（Schroder-Bernstein 定理）若 $A \preceq B, B \preceq A$，那么 $A \approx B$。

注：这个定理的作用是，证明等势时，只需要构造两个单射即可！

【推论3.1】如果 $A \subseteq B \subseteq C$，$A \approx C$，则 A, B, C 等势。

【定义3.4】（最小无限基）令 n_0 为**最小无限基 (least infinite cardinal)**，即对于任意无限集 A，$\omega \preceq A$，则 n_0 是 ω 的势。

【定理3.6】（**连续统假设 (continuum hypothesis general type)**）对于任意无限集的势 n，不存在集合 A，使得 A 的势 $k \in [\mathrm{n}, 2^{\mathrm{n}}]$。