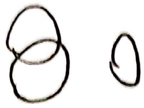
Part 1

1、set

① Venn Diagram   Euler Diagram

② Cartesian Product

set A, B

$A\times B=\{(a,b)\mid a\in A, b\in B\}$ (ordered pairs 针对2个元素)

$(a,b):=\{\{a\},\{a,b\}\}$

(a,b,c) 3个元素或以上，叫 ordered tuples

2、statement 必须为 true 或 false，有确定的结果

$p\wedge q$ conjunct $p\vee q$ disjunct

CNF: 全是 and   DNF: 全是 or

$p\to q$

converse: $q\to p$

inverse: $\neg p\to\neg q$

contrapositive: $\neg q\to\neg p$

negation: $\neg(p\to q)$

Tautology: 恒成立的东西(contradiction的反面)

predicate: 可以无确定结果 e.g.: $x^3>10$

vacuous truth: $\forall x\in\emptyset,\ x>x$ (x取值范围为空集)

$\forall x\exists y$ 与 $\exists x\forall y$

3、Induction

base case

inductive case

N：从0开始 +1

Structural Induction

true for n or <n elements, then true for n+1 elements

4、Relation and Function

Relation：可多个x对应多个y

Function：1个x只能对应1个y

$(x,y)\in R$　$(x,y)\in F$ 或 xRy, xFy

domain, range

∃! 存在且唯一

injective, one-to-one 单射

surjective, onto 满射

reflexive : $aRa \Rightarrow T$

irreflexive : $aRa \Rightarrow \perp$

total : $aRb \vee bRa \Rightarrow T$

transitive : $aRb \wedge bRc \Rightarrow aRc$

symmetric : $aRb \Leftrightarrow bRa$

anti-symmetric : $aRb \wedge bRa \Rightarrow a=b$

asymmetric : $aRb \wedge bRa \Rightarrow \perp$

Partial order : reflexive, anti-symmetric, transitive, $\leq$

Equivalence relation : reflexive, symmetric, transitive, $\equiv$, $=$

Equivalence class of x : a set containing all the elements that xRt is true

$$[x]_R := \{t\in A \mid xRt\}$$

Partition：一个集合的一种分割，没有重复，没有遗漏（这些集合再组成一个集合，才是partition）

如：$\{1,2,3,4,5\}$，Partition 可为 $\{\{1,3\},\{2,4\},\{5\}\}$

Quotient set: 集合 A 上有 equivalence relation R

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

有时也会用 A/运算符号表示, Quotient set 是一种 partion

5. Numbers and Equinumerosity

自然数: 从0开始, +1

整数: (N, N), 作差

有理数: (Z, Z^+), 作商

实数: 通过柯西序列定义出无穷小, 再通过无穷小定义

Equinumerosity: A is equinumerous to B ($A \approx B$), A与B存在双射

$R \not\approx N$

$x_1 = 0.\underline{7}87909$

$x_2 = 0.2\underline{3}4567$

$x_3 = 0.98\underline{9}654$

$x_4 = 0.237\underline{8}92$

考虑 $x_0 = 0.8490\ldots$ (与前面的位都不同)

$A \not\approx P(A)$ $f: A \to P(A)$

f is not surjective

$B = \{x \in A \mid x \notin f(x)\} \in P(A)$

$\exists z \in A$ 使 $f(z) = B$

若 $z \in B$, 则 $z \notin f(z)$, 但 $f(z) = B$

若 $z \notin B$, 则 $z \in f(z)$, 但 $f(z) = B$

6. Cardinality

有限集就是元素个数

无限集: $\aleph$ 或其它 (如 N 为 $\aleph_0$ R 为 $2^{\aleph_0}$)

$A \preceq B$ 表示 card $A \leq$ card B

countable set: $\preceq N$ 的集合, 这与有限集概念不同

N、Z、Q 为 countable

7. Finite sets and Pigeonhole Principle

若序列长度 $n \geq sr + 1$, 则最大递增/递减子序列的长度至少大于等于 r 或 s

8、Partial Order

total order：是 partial order 且任意两项均可比较

poset 偏序集，其中元素满足 partial order 关系

图像可用 Hasse Diagram 表示

Poset $(P, \leq)$

edge：一条线

质数、同余、RSA

Fermat primes : $F_n = 2^{2^n}$

$F_0 \sim F_4$ 为质数，F_5 为合数

费马小定理：① $p \in P, \gcd(a,p)=1$，$a^{p-1} \equiv 1 \pmod p$

② $p \in P$，$a^p \equiv a \pmod p$

欧拉定理：若 $\gcd(a,m)=1$，则 $a^{\varphi(m)} \equiv 1 \pmod m$

Fermat Primality Test

$2^n \not\equiv 2 \pmod n$，n 为合数

$2^n \equiv 2 \pmod n$，n 可能为质数

然后再测 $3^n \equiv 3 \pmod n$、$5^n \equiv 5 \pmod n$ 是否成立

Fermat witness 和 Fermat Liar

Carmichael number : $a^n \equiv a \pmod n$ for all a

中国剩余定理

① 整理成 mod 的数全部互质

② 对每个式子整理成 mod 自己余 1，是其它的倍数（利用欧拉定理）

③ 每个式子余数乘 ② 中计算出的数，全部相加

RSA

① 生成

两个质数 p, q

$n = pq$

$A = \varphi(n) = (p-1)(q-1)$

挑选 E

公开 (n, E)

② 加密

$y = e(x) = x^E \pmod n$

③ 解密

$D = E^{-1} \pmod A$（即 $DE \equiv 1 \pmod A$）

$x = d(y) = y^D \pmod n$

Group

$(G, \cdot)$ $\because G\times G \to G$

① 结合律：$(ab)c=a(bc)$

② 有相当于1的元素，$1\cdot a=a\cdot 1=a$

③ $\forall a\in G$，$a^{-1}\in G$

④ Closure：$\forall a,b\in G$，$a\cdot b\in G$

不一定符合交换律

Abelian group：符合交换律的group

$(ab)^{-1}=b^{-1}a^{-1}$

$ba=ca \Rightarrow b=c$ $\quad ab=ac\Rightarrow b=c$

subgroup：$1\in H$，若$a,b\in H$，则$ab\in H$ 若$a\in H$，$a^{-1}\in H$

Fundamental Theorem of Arithmetic

正整数可写成若干个质数的积

Cyclic group：由1个元素生成的，可有限可无限 $\langle x\rangle$

元素的order：最小的m使$x^m=1$，记为$|x|$

group的order：元素个数，记为$|G|$

Symmetric Group：S_n，为n个元素所有排列(permutation)的集合 $(|S_n|=n!)$

$S_1=\{e\}$

$S_2=\{e,\tau\}$ $e=\begin{pmatrix}1&2\\1&2\end{pmatrix}=(1)$ $\tau=\begin{pmatrix}1&2\\2&1\end{pmatrix}$ $\quad$ e,τ之类的称为排列

$S_3=\{e,\tau,\tau',\tau'',\sigma,\sigma'\}$

$e=()=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\sigma=(123)=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $\sigma'=(132)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

$\tau=(12)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $\tau'=(23)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\tau''=(13)=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

计算：必须从右向左计算，$(ab)(bc)=(abc)$

Transposition：两个元素互换的排列 (a,b)

Even permutation：由偶数个 transposition 组成

Odd transposition：由奇数个 transposition 组成

$$\mathrm{sgn}(\sigma)=\begin{cases}+1, & \sigma \text{ even}\\ -1, & \sigma \text{ odd}\end{cases}$$

Homomorphism

$f: G\to G'$，$f(xy)=f(x)f(y)$ （G, G'为Group）

$f(1_G)=1_{G'}$

$f(a^{-1})=f(a)^{-1}$

image：值域

kernel：$\{a\in G \mid f(a)=1_{G'}\}$

$a,b\in G$，$K=\ker f$

$f(a)=f(b)\Leftrightarrow a^{-1}b\in K\Leftrightarrow b\in aK\Leftrightarrow aK=bK$

homomorphism injective $\Leftrightarrow \ker f=\{1_G\}$

Isomorphism：bijective homomorphism $\Leftrightarrow \ker f=\{1_G\}$ 且 $\operatorname{im} f=G'$

Coset

Group G 的 subgroup H，$aH=\{g \mid g=ah, h\in H\}$

aH 为 left coset，Ha 为 right coset

coset 元素数量与 subgroup H 元素数量相同

H 的不同 coset 的数量为 index $[G:H]$

对于不同的 a，总共有 $|G|$ 个 coset

共有 $\frac{|G|}{|H|}$ 个不同的，其中每个都有 $|H|$ 个 a 对应

总数正确，所有不同的组合起来为整个 group G

$b\in aH$（即 $a^{-1}b\in H$）这个关系为 equivalence class

左截线集（Left transversal）：从每个不同的 coset 中提取一个元素组成

正规子群(Normal subgroup)

的左陪集等于右陪集，

记作 $H \trianglelefteq G$

可通过以下证明：

① $\forall h \in H, \forall g \in G, ghg^{-1} \in H$