

MATH 40001

IUM LOGIC

& SET

proof of $\vee$ when proving $P \vee Q$ is true, we need to show that:
if P is false, then Q is true

<u>truth table</u>	P	Q	$P \Rightarrow Q$	$\neg P \vee Q$	在证明时将 $P \Leftrightarrow Q$ 转化为 $(\neg P \vee Q) \wedge (\neg Q \vee P)$ 或 $(P \wedge Q) \vee (\neg P \wedge \neg Q)$
	true	false	false	false	
	false	true	true	true	
	false	false	true	true	

注意: 我们要如何理解 $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$

① if P is true, then Q needs to be true for
 $P \Rightarrow Q$ to be true

② if P is false, $P \Rightarrow Q$ is true automatically

transitivity $(P \Rightarrow Q, Q \Rightarrow R) \Leftrightarrow (P \Rightarrow R)$

proof: assume P is true;

$\because P \Rightarrow Q, \therefore Q$ is true

$\because Q \Rightarrow R, \therefore R$ is true $\therefore P \Rightarrow R$

所有证明均可用
logic table 证明

contrapositive: $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

proof: assume $\neg Q$ is true:

if $\neg Q \Rightarrow P$: $P \Rightarrow P \Rightarrow Q, \therefore \neg Q \Rightarrow Q$, contradiction

so $\neg Q \Rightarrow \neg P$. [另一言]

* $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ 证明同理

★ 证明时可考虑 contradiction / contrapositive
尤其是证明无妄条件时

proposition formulas 在写 proposition formulas 时写括号避免
误解

set

$$X \setminus Y = \{x \in X \mid x \notin Y\}$$

if Ω is a set and $X \subseteq \Omega$; $\bar{X} = \{t \in \Omega \mid t \notin X\}$

let P be a proposition and X be an empty set.

$(\exists x \in X, P)$ must be false

$(\forall x \in X, P)$ must be true

注意: 在画有关于 set 的 truth table 时,

题头应为 $x \in X, x \in Y, \dots$

单纯地写 $X, Y, \dots$ 毫无意义

function if X, Y are sets, $f: X \rightarrow Y$ or $x \mapsto f(x)$ is a function.
if and only if $\forall x \in X, \exists! y \in Y, f(x) = y$.

- ① X is domain, Y is codomain. (different to range/image)
a function depends on both domain and codomain.
- ② f is well-defined if it is a function.
- ③ if $f(x) = x$, then f is an identity function.

一些易错点:

- $(f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^2)$ 不同于 $(f: \mathbb{R} \rightarrow \mathbb{R}_{>0}, f(x) = x^2)$
codomain 很重要, $\text{range} \subseteq \text{codomain}$.
- if X is a set, $(f: \emptyset \rightarrow X)$ is always a function.
- $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = \frac{1}{x}$ is not a function since $f(0)$ is not defined.
- $f: \mathbb{N} \rightarrow \mathbb{N}, f(x) = \frac{x}{2}$ is not a function since $f(1)$ is out of codomain.
- $f: \mathbb{C} \rightarrow \mathbb{C}, f(x) = \sqrt{x}$ is not a function since $f(i)$ has two output

injective $f: X \rightarrow Y$ is injective if distinct elements of X get mapped to distinct elements of Y . $\forall a, b \in X, f(a) = f(b) \Rightarrow a = b$

proving a function is injective

for $f: X \rightarrow Y$, show $\forall a, b \in X, f(a) = f(b) \Rightarrow a = b$

- ① pick arbitrary $a, b \in X$
- ② assume $f(a) = f(b)$
- ③ show $a = b$

surjective $f: X \rightarrow Y$ is surjective if every element of Y gets 'hit' 3

by f . $\forall y \in Y, \exists x \in X, f(x) = y$

• proving a function is surjective

for $f: X \rightarrow Y$, show $\forall b \in Y, \exists a \in X, f(a) = b$

① pick arbitrary $b \in Y$

② find $a \in X$ such that $f(a) = b$

a function $f: X \rightarrow Y$ is bijective if it is both injective and bijective surjective.

let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ be functions, and say $g \circ f: X \rightarrow Z$ composition be the composition of f and g .

① if f and g are both injective, so is $g \circ f$

② if f and g are both surjective, so is $g \circ f$

③ if f and g are both bijective, so is $g \circ f$

$f: X \rightarrow Y$ is a function, we say a function $g: Y \rightarrow X$ is a inverse two-sided inverse of f if both of the following are true:

① for all $x \in X, g(f(x)) = x$

② for all $y \in Y, f(g(y)) = y$

a function $f: X \rightarrow Y$ has a two-sided inverse if and only if it is a bijection

proof:

① inverse $\Rightarrow$ bijection

assume $f: X \rightarrow Y$ has an inverse, say $g: Y \rightarrow X$

• for injective:

let $x_1, x_2 \in X$, assume $f(x_1) = f(x_2)$

$$g(f(x_1)) = g(f(x_2))$$

$$x_1 = x_2$$

• for surjective:

assume $y \in Y$, pick $g(y) \in X$, then $f(g(y)) = y$

② inverse $\Leftarrow$ bijective

assume f is bijective

$\forall y \in Y, \exists x \in X, f(x) = y$ (f is surjective)

define $g(y) = x, g: Y \rightarrow X$

• g is well-defined: show that there is exactly one $x \in X$ such that $g(y) = x$

assume $g(y_1) = x_1, g(y_2) = x_2$

$\because f(x_1) = y_1, f(x_2) = y_2, f$ is injection

$\therefore$ if $x_1 \neq x_2$, then $y_1 \neq y_2$. if $y_1 = y_2$, then $x_1 = x_2$

• g is two-sided inverse:

let $y \in Y$:

$$f(g(y)) = f(x) = y$$

let $x \in X$

$$g(f(x)) = g(y) = x$$



注意: 证明时要定义所有变量/function

考虑到 $f: X \rightarrow Y$ 时, 不是所有 y 都有对应 x

a binary relation R on a set X is a subset of X^2 . binary relations
this set is usually denoted $R(x, y)$.

一些写法: $R(a, b)$, aRb , $a \xrightarrow{R} b$, $a \sim_R b$, $a \sim b$.

注意: order 很重要, "a is related to b" $\neq$
"b is related to a"

- reflexive: $\forall x \in X, R(x, x)$
- transitive: $\forall a, b, c \in X, R(a, b) \wedge R(b, c) \Rightarrow R(a, c)$
- symmetric: $\forall a, b \in X, R(a, b) \Rightarrow R(b, a)$
- antisymmetric: $\forall a, b \in X, R(a, b) \wedge R(b, a) \Rightarrow a = b$
- partial order: reflexive, transitive, antisymmetric
- total: $R(a, b) \vee R(b, a)$ is true
- total order: partial order and total.
- equivalence relation: reflexive, transitive, symmetric
- R is total order if R is partial order and (total)

let X be a set and $\sim$ be an equivalence relation on X .
 $s \in X$, and its equivalence class is defined as:

$$cl(s) = \{x \in X \mid s \sim x\}$$

let $t \in X$: if $s \sim t$, $cl(s) = cl(t)$

- $s \sim t, cl(s) = cl(t)$
- $\neg (s \sim t), cl(s) \cap cl(t) = \emptyset$

proof: con-

by contrapositive, if $cl(s) \cap cl(t) \neq \emptyset$, WTP $s \sim t$

$\therefore \exists x, x \in cl(s) \cap cl(t), x \in cl(s), x \in cl(t)$

$\therefore s \sim x, t \sim x \therefore s \sim t$

a partition of a set X is a set V of non-empty subsets of X with the property that each element of X is in exactly one of the subsets

- $V = \{cl(s) \mid s \in X\}$ for $\sim$ is a partition of X .

注意:

- (1) relation性质的判断严格按照定义!
"if False, then..."均为True, 因此 antisymmetric 与 symmetric 可同时成立!
- (2) 对于 relation on ϕ , reflexive is satisfied.
- (3) binary relation 仅限两个元!
- (4) relation 必须全部拥有定义! (True or False)

MATH 40001

IUM APPLIED

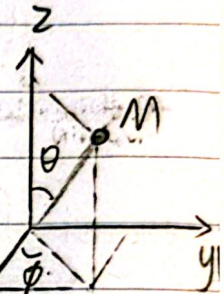
• coordinate for sets A, B : $A \times B = \{(a, b) \mid a \in A, b \in B\}$

• polar: $(r, \phi) = (\sqrt{x^2 + y^2}, \underline{\text{atan2}(y, x)})$

cylindrical: $(\rho, \phi, z) = (\sqrt{x^2 + y^2}, \underline{\text{atan2}(y, x)}, z)$

spherical: $(r, \phi, \theta) = (\sqrt{x^2 + y^2 + z^2}, \underline{\text{atan2}(y, x)}, \underline{\arctan \frac{z}{r}})$

$$(x, y, z) = (r \sin \theta \cos \phi, r \sin \theta \sin \phi, r \cos \theta)$$



★ 必须写 $(r, \phi, \theta) = \dots$ etc.

★ 画图时接受 $r < 0$, 答题时 $r \geq 0$

★ 判断 spherical ϕ 时仅关注 'x-y' plane 即可

polar coordinate (r, ϕ) and $(-r, \phi \pm \pi)$ represents the same point when sketching

line (2D) parametric $\begin{cases} x = x_0 + \lambda a \\ y = y_0 + \lambda a \end{cases}$ where x_0, y_0, a constants $(a, b) \neq (0, 0)$

cartesian: $ax + by + c = 0$ where a, b, c constants, $(a, b) \neq (0, 0)$

line (3D) parametric $\begin{cases} x = x_0 + \lambda u_1 \\ y = y_0 + \lambda u_2 \\ z = z_0 + \lambda u_3 \end{cases}$ where x_0, y_0, z_0, u_i constants

cartesian (intersection of two planes)

$$\begin{cases} a_1 x + b_1 y + c_1 z + d_1 = 0 \\ a_2 x + b_2 y + c_2 z + d_2 = 0 \end{cases} \text{ where } a_i, b_i, c_i, d_i \text{ constants.} \\ (a_i, b_i, c_i) \neq (0, 0, 0)$$

plane parametric: $\begin{cases} x = x_0 + \lambda u_1 + \mu v_1 \\ y = y_0 + \lambda u_2 + \mu v_2 \\ z = z_0 + \lambda u_3 + \mu v_3 \end{cases}$ where $x_0, y_0, z_0, u_1, v_1, u_2, v_2, u_3, v_3$ constants

cartesian $ax + by + cz + d = 0$ where a, b, c, d constants $(a, b, c) \neq 0$

line & polar: 过原点的线可用角度表达, 主要关注不过原点的线

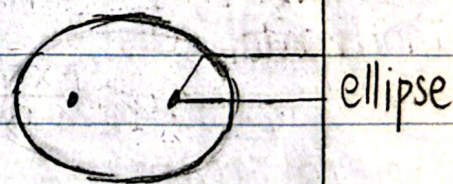
$$r = \frac{a \cos \theta + b \sin \theta}{\cos(\theta - \alpha)} \quad \text{where } \alpha = \frac{a}{c}, \beta = \frac{b}{c} \text{ if } ax + by = c$$

$(a, b) \neq (0, 0)$

proof: 因为不过原点, 因此形为 $ax + by = c$,
即 $r(a \cos \theta + b \sin \theta) = c$

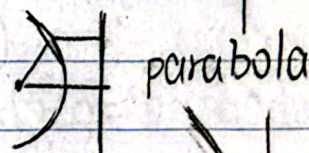
- conic section: given a point (called focus) and a line not containing this point (called directrix), the set of points for which the ratio of the distance to the focus and the directrix is $e \in \mathbb{R}^+$ (called eccentricity) is called

ellipse when $e < 1, \Delta < 0$



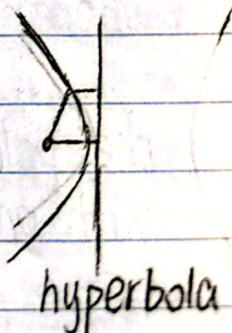
ellipse

parabola when $e = 1, \Delta = 0$



parabola

hyperbola when $e > 1, \Delta > 0$



hyperbola

where the cartesian equation of conic section is in form

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$$

$$\Delta := B^2 - 4AC$$

特殊点: the sum of distances from one point to each of two focus is the same ellipse

我们一般称长的axis长度为 $2a$, 短的长度为 $2b$

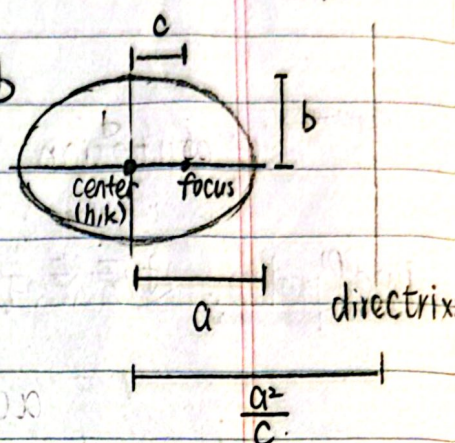
distance from center to focus: $c = \sqrt{a^2 - b^2}$

horizontal major axis:

$$\left(\frac{x-h}{a}\right)^2 + \left(\frac{y-k}{b}\right)^2 = 1$$

vertical major axis:

$$\left(\frac{x-h}{b}\right)^2 + \left(\frac{y-k}{a}\right)^2 = 1$$

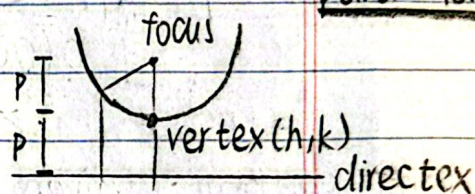


horizontal directrix: $y = k - p$

$$(x-h)^2 = 4p(y-k)$$

vertical directrix: $x = h - p$

$$(y-k)^2 = 4p(x-h)$$



parabola

特殊点: the absolute value of difference between distance from one point to each of the focus is the same hyperbola

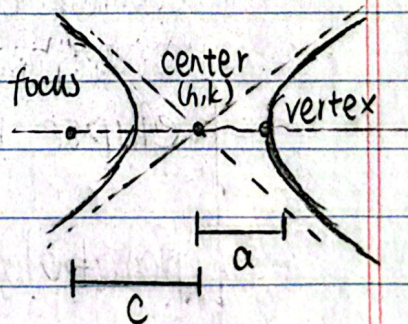
horizontal axis:

$$\left(\frac{x-h}{a}\right)^2 - \left(\frac{y-k}{b}\right)^2 = 1$$

vertical axis:

$$\left(\frac{y-k}{a}\right)^2 - \left(\frac{x-h}{b}\right)^2 = 1$$

where $c^2 = a^2 + b^2$, $e = \frac{c}{a}$



the polar equation of a conic section with one focus at the pole:

conic section & polar

$$r = \frac{l}{1 + e \cos(\phi + \phi_0)}$$

where e is eccentricity, l is the length of a straight line between one focus and the conic section along direction parallel to directrix

复数(2D): $z = |z|e^{i\phi} \therefore \ln z = \ln|z| + i\phi$

四元数(4D): $z = a_1 + a_2i + a_3j + a_4k$

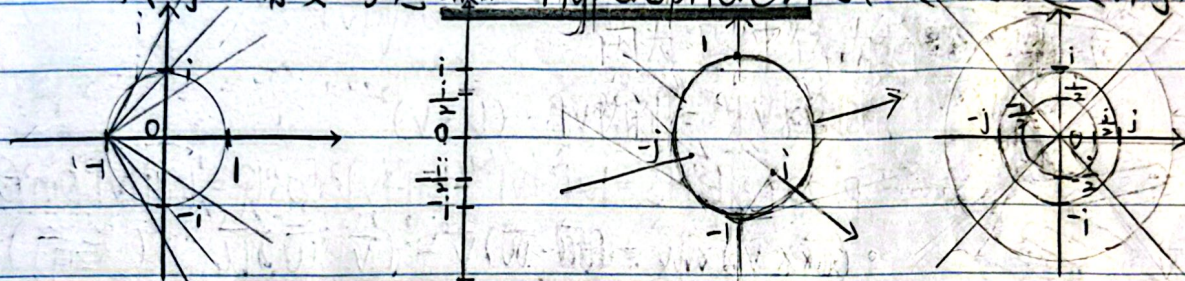
实部 imag 虚部

考虑一个四维空间, 其中实数轴, i 轴, j 轴, k 轴均垂直
但是我们做不到这一点, 因此我们考虑将其投影至三维空间

$$z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot \frac{z_1}{|z_1|} \frac{z_2}{|z_2|}$$

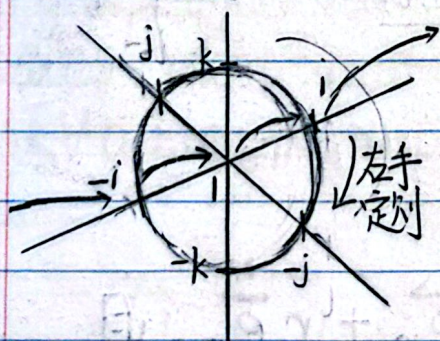
沿轴旋转要改变的点

我们只需要考虑 unit hypersphere 即可 (仅考虑旋转即可)



让我们考虑一下我们在对二、三维空间投影时发生了什么, 于是我们从四维空间的 $(-1, 0, 0, 0)$ 对 unit hypersphere 投影

我们发现: ① 在 unit hypersphere 中, 实数值为 0 的 unit complex 投影后为三维空间中的 unit sphere. 实数值为 $[-1, 0)$ 的 unit complex 投影后在该 unit sphere 外, 实数值为 $(0, 1]$ 的 unit complex 投影后在该 unit sphere 之内



② $(-1, 0, 0, 0)$ 跟往常一样投影至任意无穷远的点

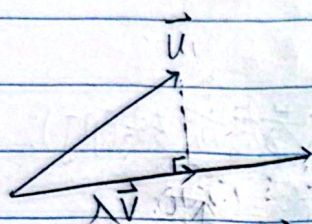
③ 过 $\pm i, \pm i$ (或 $\pm i, \pm j$; 或 $\pm i, \pm k$) 的在 unit hypersphere 上的 circle 投影为 line

④ 过 $\pm i, \pm j$ (或 $\pm i, \pm k$; 或 $\pm j, \pm k$) 的在 unit hypersphere 上的 circle 投影为 circle.

由此, 在计算四元数时, 若以左例乘数代表旋转方向, 则遵守右手定则:

$$\begin{cases} i \cdot i = 1 \\ j \cdot j = -1 \\ i \cdot j = k \\ i \cdot k = -j \end{cases} \quad \begin{cases} j \cdot i = -k \\ j \cdot j = -1 \\ j \cdot k = i \end{cases} \quad \begin{cases} k \cdot i = j \\ k \cdot j = -i \\ k \cdot k = -1 \end{cases}$$

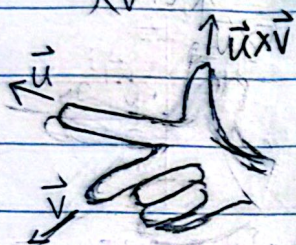
这个知识点在很久之前被人用来表示三维空间的变位。
(令四元数的实部为0即可)



若 $\lambda \vec{v}$ 为 $\vec{u}$ 在 $\vec{v}$ 方向上的分量, 则 $(\vec{u} - \lambda \vec{v}) \perp \vec{v}$

点乘叉乘

所以 $\text{proj}_{\vec{v}} \vec{u} = \lambda \vec{v} = \frac{\vec{u} \cdot \vec{v}}{|\vec{v}|^2} \vec{v}$



• $|\vec{u} \times \vec{v}|^2 = |\vec{u}|^2 |\vec{v}|^2 - (\vec{u} \cdot \vec{v})^2$

proof: $\text{RHS} = |\vec{u}|^2 |\vec{v}|^2 - |\vec{u}|^2 |\vec{v}|^2 \cos^2 \theta = |\vec{u}|^2 |\vec{v}|^2 \sin^2 \theta = \text{LHS}$

• $(\vec{u} \times \vec{v}) \times \vec{w} = (\vec{u} \cdot \vec{w}) \vec{v} - (\vec{v} \cdot \vec{w}) \vec{u}$ (后前)

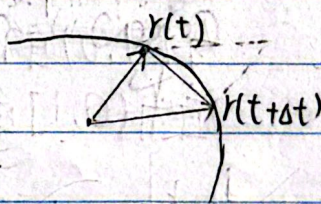
• $\vec{u} \times (\vec{v} \times \vec{w}) = (\vec{u} \cdot \vec{w}) \vec{v} - (\vec{u} \cdot \vec{v}) \vec{w}$ (前后)

the areal velocity is the rate of change of the area swept out vector function by the position vector as it moves around a curve

$$\frac{dA}{dt} = \frac{\vec{r}(t) \times \dot{\vec{r}}(t)}{2}$$

proof:

$$\begin{aligned} \frac{dA}{dt} &= \lim_{\Delta t \rightarrow 0} \frac{\Delta A}{\Delta t} = \lim_{\Delta t \rightarrow 0} \frac{\vec{r}(t) \times \vec{r}(t + \Delta t)}{2 \Delta t} \\ &= \lim_{\Delta t \rightarrow 0} \frac{\vec{r}(t)}{2} \times \frac{\vec{r}(t + \Delta t) - \vec{r}(t)}{\Delta t} \\ &= \lim_{\Delta t \rightarrow 0} \frac{\vec{r}(t) \times \dot{\vec{r}}(t)}{2} \end{aligned}$$



注意: $\vec{r} = r \vec{e}_r$ 时, $\dot{\vec{r}} = \dot{r} \vec{e}_r + r \dot{\vec{e}}_r$, 且 $\dot{\vec{e}}_r \cdot \vec{e}_r = 0$ (consider $\vec{e}_r$ 长度)

• if $\vec{r} \times \vec{a} = \vec{b}$, $\vec{a} \cdot \vec{b} = 0$. then $r(\omega) = \frac{\vec{a} \times \vec{b}}{|\vec{a}|^2} + \lambda \vec{a}$

• path of $\vec{r}(t)$ within $[a, b]$: $\int_a^b |\dot{\vec{r}}(t)| dt$

• a group G is a set of elements together with a binary operation, denoted by $\circ$, that satisfy the following four properties: group •

(1) closure: $\forall a, b \in G, a \circ b \in G$

(2) associativity: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$

(3) identity element: $\exists$ an identity element $I \in G, \forall a \in G, I \circ a = a \circ I = a$

(4) inverse: $\forall a \in G, \exists$ the inverse of a $b \in G, a \circ b = b \circ a = I$

注意:

an Abelian group is a group with extra property of

commutativity: $\forall a, b \in G, a \circ b = b \circ a$

a field is a set $\mathbb{F}$ with two commutative operations (let us call them "addition" and "multiplication" here). it is an Abelian group under addition, with 0 as the additive identity. all elements apart from 0 are an Abelian group under multiplication with 1 as the multiplication identity. multiplication distributes over addition: $\forall a, b, c \in \mathbb{F}, a(b+c) = ab+ac$ and $(a+b)c = ac+bc$. field •

let $\mathbb{F}$ be a field, the elements of which we will denote as scalars. a set of elements V , forming an Abelian

vector space

9.

group under a vector addition $V \times V \rightarrow V$, denoted by $+$, together with a scalar multiplication $\mathbb{F} \times V \rightarrow V$ is called a vector space over field $\mathbb{F}$ if the following properties are fulfilled for $\forall \lambda, \mu \in \mathbb{F}, \vec{u}, \vec{v} \in V$

(i) distributivity: $(\lambda + \mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$

$$\lambda(\vec{u} + \vec{v}) = \lambda\vec{u} + \lambda\vec{v}$$

(ii) associativity: $(\lambda\mu)\vec{v} = \lambda(\mu\vec{v})$

(iii) multiplication identity in $\mathbb{F}$: $1\vec{v} = \vec{v}$

elements of the vector space V are called vectors. the identity element of the vector addition is called zero vector.

- a non-empty subset $W \subseteq V$ of a vector space is sub vector space of V if

(i) $\forall \vec{w}_1, \vec{w}_2 \in W, \forall \lambda \in \mathbb{F}, \vec{w}_1 + \vec{w}_2 \in W, \lambda\vec{w}_1 \in W$

(ii) $\vec{0} \in W, \forall \lambda \in \mathbb{F}, \lambda\vec{w} \in W$

- the set of all linear combinations of a given set of vectors $\{\vec{u}_j\}$ with arbitrary coefficients, is called the span of the vectors $\{\vec{u}_j\}$

- the largest possible number N of linearly independent vectors in a vector space V is called the dimension of V

linear map a map $T: V \rightarrow V$ is linear if $\forall \lambda, \mu \in \mathbb{F}, \vec{u}, \vec{v} \in V$

$$T(\lambda\vec{u} + \mu\vec{v}) = \lambda T(\vec{u}) + \mu T(\vec{v})$$

a linear map $T: V \rightarrow V$ is invertible if there exist a linear map T^{-1} such that $\forall \vec{v} \in V, T(T^{-1}(\vec{v})) = T^{-1}(T(\vec{v}))$. the map T^{-1} is the inverse of T .

- Complex vector space an inner product space is a complex vector space V together with a map $V \times V \rightarrow \mathbb{C}$, written as $(\vec{u}, \vec{v})$.
 - (1) if $\vec{u} = \sum_{i=1}^n u_i \hat{b}_i, \vec{v} = \sum_{i=1}^n v_i \hat{b}_i, u_i, v_i \in \mathbb{C}$, then $(\vec{u}, \vec{v}) = \sum_{i=1}^n u_i^* v_i$.
 $\forall \vec{u}, \vec{v}, \vec{w} \in V$ and $\lambda, \mu \in \mathbb{C}$:
 - (2) (anti)-symmetric: $(\vec{u}, \vec{v}) = (\vec{v}, \vec{u})^*$ where the asterisk denotes complex conjugate
 - (3) non-negativity: $(\vec{u}, \vec{v}) \geq 0$ and $(\vec{u}, \vec{u}) = 0 \Leftrightarrow \vec{u} = \vec{0}$
 - (4) linearity in one of the element:
 $(\vec{u}, \lambda \vec{v} + \mu \vec{w}) = \lambda (\vec{u}, \vec{v}) + \mu (\vec{u}, \vec{w})$

triangular inequality $|\vec{u} + \vec{v}| \leq |\vec{u}| + |\vec{v}|$

MATH 40001.

IUM. NUMBER

11

• $\mathbb{N}$

Peano axioms:

the natural numbers $\mathbb{N}$ are defined as:

- 0 is a natural number
- if n is a natural number, then its successor $S(n)$ is a natural number
- that's it (meaning no other natural numbers exist)

* original axioms:

$$\forall x \in \mathbb{N}, S(x) \neq 0$$

$$\forall x, y \in \mathbb{N}, (S(x) = S(y)) \Rightarrow (x = y)$$

① the addition is defined as, for $a \in \mathbb{N}$:

- $a+0$ is defined as a
- $a+S(n)$ is defined as $S(a+n)$, where $n \in \mathbb{N}$

the addition is commutativity:

proof:

Lemma 1. $0+x=x$, where $x \in \mathbb{N}$

by induction; $P_n = 0+n=n$

① P_0 : $0+0=0$, P_n is true

② assume P_n is true $0+n=n$, for P_{n+1} :

$$0+S(n) = S(0+n) = S(n), P_n \Rightarrow P_{n+1}$$

③ P_n : $0+n=n$ is true for all $n \in \mathbb{N}$

Lemma 2. $S(a)+x = S(a+x)$, where $a, x \in \mathbb{N}$

by induction; $P_n = S(a)+n = S(a+n)$

① P_0 : LHS = $S(a)+0 = S(a)$

$$\text{RHS} = S(a+0) = S(a), P_0 \text{ is true}$$

② assume P_n is true $S(a)+n = S(a+n)$, for P_{n+1} :

$$\text{LHS} = S(a)+S(n) = S(S(a)+n) = S(S(a+n))$$

$$\text{RHS} = S(a+S(n)) = S(S(a+n)), P_n \Rightarrow P_{n+1}$$

③ P_n : $S(a)+x = S(a+x)$ is true for all $n \in \mathbb{N}$

theorem 1. $a+b=b+a$, where $a, b \in \mathbb{N}$

by induction; $P_n: a+n=n+a$.

① $P_0: LHS = a+0 = a$

$RHS = 0+a = a$, P_0 is true

② assume P_n is true: $a+n=n+a$, for P_{n+1} :

$LHS = a+S(n) = S(a+n) = S(n+a)$

$RHS = S(n)+a = S(n+a)$, $P_n \Rightarrow P_{n+1}$

③ $P_n: a+n=n+a$ is true for all $n \in \mathbb{N}$

the addition is also associativity:

proof: $P_n: (a+b)+n = a+(b+n)$

① $P_0: a+(b+0) = a+b = (a+b)+0$, P_0 is true

② assume P_n is true, $(a+b)+n = a+(b+n)$, for P_{n+1}

$LHS = (a+b)+S(n) = S((a+b)+n) = S(a+b+n)$

$RHS = a+(b+S(n)) = a+S(b+n) = S(a+(b+n))$

$LHS = RHS$, $P_n \Rightarrow P_{n+1}$

③ $P_n: (a+b)+n = a+(b+n)$ is true for all $n \in \mathbb{N}$

⑤ the multiplication is defined as, for $a \in \mathbb{N}$:

• $a \times 0 = 0$

• $a \times S(n) = a \times n + a$, where $n \in \mathbb{N}$

the multiplication is commutativity, associativity, distributivity

⑥ if $x+n=y+n$, then $x=y$.

if $x+n=n$, then $x=0$

proof: by induction

proof: $x+n=0+n$

let x and y be natural numbers, we say that $x \leq y$ if order there exists a natural number n such that $y = x + n$.

say $x, y, z \in \mathbb{N}$

- ① reflexivity: $x \leq x$
- ② transitivity: if $x \leq y$ and $y \leq z$, then $x \leq z$
- ③ antisymmetry: if $x \leq y$ and $y \leq x$, then $x = y$
- ④ totality: either $x \leq y$ or $y \leq x$

自然数比大小
只定义了 $\leq$!

we have a set X . you can make a function F which recursion sends a natural number n to an element of the set X by doing the following:

- define the element $F(0) \in X$
- define a function p_n from X to X and define $F(S(n)) = p_n(F(n))$

一个体现所有 hypothesis 和 WTP 的内容的表格

goal state diagram

$x: \mathbb{N}$	} 题目中的定义
$y: \mathbb{N}$	
$z: \mathbb{N}$	
$hxy: x \leq y$	} h 表示是 hypothesis, 名字自己起 (后续差不多不用列可以删去, 如果翻译要改写)
$hyz: y \leq z$	
$a: \mathbb{N}$	
$ha: y = x + a$	} 证明过程如实写出
$b: \mathbb{N}$	
$hb: z = y + b$	
$x \leq z$	} WTP 的内容

在 induction 中, 我们的 goal state diagram - 一般为

- case BaseCase

$a: \mathbb{N}$

$$\vdash \text{succ } a \times 0 = a \times 0 + 0$$

- case InductiveStep

$a: \mathbb{N}$

$d: \mathbb{N}$

$$\text{IH: succ } a \times d = a \times d + d$$

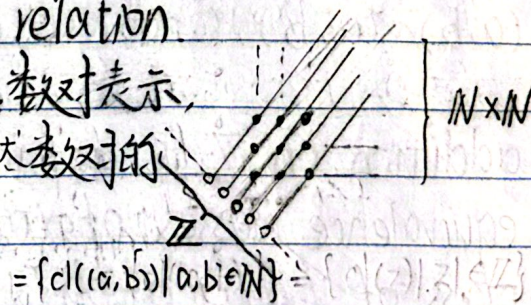
$$\vdash \text{succ } a \times \text{succ } d = a \times \text{succ } d + \text{succ } d$$

- $\mathbb{Z}$ the following binary relation on $\mathbb{N}^2$

$(a, b) \sim (c, d)$ if and only if $a + d = b + c$
is an equivalence relation.

the set of integers $\mathbb{Z}$ is the set of all equivalence classes for $\mathbb{N}^2$ under this equivalence relation.

*本质上就是把一个整数用一类自然数对表示, 两者等价 (equivalent)。通过定义自然数对的运算, 计算整数间的运算。



let X be a set, $\sim$ be an equivalence relation, V be the set of equivalence classes, and $cl: X \rightarrow V$ be the function which takes an element of X and sends it to its equivalence class. say Y is an arbitrary set and $h: X \rightarrow Y$ is an arbitrary function. assume that for all $x_1, x_2 \in X$, if $x_1 \sim x_2$ then $h(x_1) = h(x_2)$, then there exist a unique function $g: V \rightarrow Y$ such that $h = g \circ cl$

13

* 事实上, there exist a $g: V \rightarrow X$ such that $h = g \circ \iota \iff$ for all

x_1, x_2 , if $x_1 \sim x_2$ then $h(x_1) = h(x_2)$

** 总之, 我们通过证明一类 equivalence class 的结果证明, 证明我们的想法是可行的

pre-negation function from $\mathbb{N}^2$ to $\mathbb{N}^2$ is defined by defining $-(a, b)$ to be (b, a) ①

• $(a, b) \sim (c, d) \iff -(a, b) \sim -(c, d)$

the negation plays well with equivalence:

negation on $\mathbb{Z}$ is defined as the function sending the equivalence class of (a, b) to the equivalence class of (b, a)

pre-addition function from $\mathbb{N}^2$ to $\mathbb{N}^2$ is defined by defining ②

$(a, b) + (c, d)$ to be $(a+c, b+d)$

• $(a, b) \sim (a', b'), (c, d) \sim (c', d') \implies (a+c, b+d) \sim (a'+c', b'+d')$

addition on $\mathbb{Z}$ is defined as the function sending the equivalence classes of (a, b) (c, d) to the equivalence class of $(a+c, b+d)$, with associativity and commutativity

pre-multiplication function from $\mathbb{N}^2$ to $\mathbb{N}^2$ is defined ③

by defining $(a, b) \times (c, d)$ to be $(ac+bd, ad+bc)$

• $(a, b) \sim (a', b') \implies (a, b) \times (c, d) \sim (a', b') \times (c, d)$

• $(c, d) \sim (c', d') \implies (a, b) \times (c, d) \sim (a, b) \times (c', d')$

multiple on $\mathbb{Z}$ is defined as the function sending

the equivalence classes of (a,b) (c,d) to the equivalence class of $(ac+bd, ad+bc)$ with associativity, commutativity and distributivity.

say we have a set X , you can make a function F which Strong Induction sends a natural number n to an element of the set X by providing the following things:

- for every n , a function p_n from $X^{\{t \in \mathbb{N} \mid t < n\}}$ to X
- the resulting function F will have the property that $F(s(n))$ is equal to $p_n(F|_{\{t \in \mathbb{N} \mid t < n\}})$

*也就是说, 如果想要证明 $P_n, n \in \mathbb{N}$, 正确, 则只需证明 if P_t is true for all $t < n$, then P_n is true.

let $b \in \mathbb{N}$ with b nonzero, define the quotient function division.

$q_b: \mathbb{N} \rightarrow \mathbb{N}$ as follows: for a natural number a ,

- if $a \geq b$: then there exists k such that $a = b + k$, and we set $q_b(a) = q_b(k) + 1$
- otherwise: we set $q_b(a) = 0$

let $b \in \mathbb{N}$ with b nonzero, define the remainder function

$r_b: \mathbb{N} \rightarrow \mathbb{N}$ as follows: for a natural number a ,

- if $a \geq b$: then there exists k such that $a = b + k$, and we set $r_b(a) = r_b(k)$
- otherwise: we set $r_b(a) = a$

define a sequence of function $\gcd_a: \mathbb{N} \rightarrow \mathbb{N}$ as follows: ②

- for $a=0$: $\forall b \in \mathbb{N}, \gcd_a(b) = b$

- for nonzero a : $\gcd_a$ is defined on the input b in terms of the remainder on division by a

$$\gcd_a(b) = \gcd_{r_a(b)}(a)$$

注意: 一些写法有 $\gcd(a, b)$, $\gcd_a(b)$

- $\gcd_a(b)$ is always positive, unless $a, b = 0$
- $\gcd_a(b)$ divides both a and b .

proof:

assume for all t, s such that $t < a$, it is true that $\gcd_t(s)$ divides t and s .

① if $a = 0$: then $\gcd_a(b) = b$ divides both a and b

② if $a > 0$: then $\gcd_a(b) = \gcd_{r_a(b)}(a)$

by assumption, $\gcd_{r_a(b)}(a)$ divides $r_a(b)$ and a .
 $\gcd_a(b)$ divides $q_a(b) \cdot a + r_a(b)$ and a .

- if x is any number divides a and b , then it divides $\gcd_a(b)$.

proof:

assume for all t, s such that $t < a$, it is true that if x is any number divides t and s , then it divides $\gcd_t(s)$.

① if $a = 0$: $\gcd_a(b) = b$, so x being a factor of b shows that it is a factor of $\gcd_a(b)$

② if $a > 0$: then $b = q_a(b)a + r_a(b)$

since x divides a, b , then x divides $r_a(b)$

by assumption, x divides $\gcd_{r_a(b)}(a) = \gcd_a(b)$

- let a and b be natural numbers, there are integers λ and μ such that $\gcd_a(b) = \lambda a + \mu b$

proof:

assume for all t, s with $t < a$, there exist λ, μ such that $\gcd_t(s) = \lambda t + \mu s$

proof:

assume for all t, s with $t < a$, there exists λ, μ such that $\gcd_t(s) = \lambda t + \mu s$

① if $a=0$: then $\gcd_a(b) = b$

② if $a > 0$: then $\gcd_a(b) = \gcd_{r_a(b)}(a)$

by assumption, $\gcd_{r_a(b)}(a) = \lambda r_a(b) + \mu a$

since $b = q_a(b)a + r_a(b)$

$$\gcd_a(b) = \lambda(b - q_a(b)a) + \mu a$$

$$= \lambda b + (\mu - q_a(b)\lambda)a$$

• number theory every natural number greater than 1 can be factored as a finite product of prime number

proof:

assume every $1 < m < n$ has a prime factorisation

① if n is prime:

② if n is composite: $\exists a, b \in \mathbb{N}, 1 < a, b < n, n = ab$

by assumption, a and b has prime factorisation

then n has a prime factorisation

let p is prime and $a, b \in \mathbb{N}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$

proof:

since p is prime, $\gcd_a(p)$ is 1 or p .

① if $\gcd_a(p) = p$: $p \mid a$

② if $\gcd_a(p) = 1$: $\exists \lambda, \mu \in \mathbb{Z}, 1 = \lambda a + \mu p$

$$\text{so } b = \lambda ab + \mu bp$$

since $p \mid ab$, $p \mid \lambda ab + \mu bp$

so $p \mid b$.

15

every positive integer is uniquely the product of prime number, up to re-ordering.

proof:

assume that for all $m < n$, if $m = a_1 a_2 \dots a_s = b_1 b_2 \dots b_t$, where a_i and b_j are primes, then $s = t$ and $(a_1, a_2, \dots, a_s)$ can be reordered to $(b_1, b_2, \dots, b_t)$

now let us focus on n :

① if $s = 0$: then $n = 1$, so $t = 0$ and the factorisations are same

② if $s > 0$: consider prime factor a_s of $n = b_1 b_2 \dots b_t$ since $a_s | n$, then $a_s | b_1$ or $a_s | b_2$ or ... or $a_s | b_t$.

that is said, $a_s = b_1$ or $a_s = b_2$ or ... or $a_s = b_t$

WLOG, let $a_s = b_t$

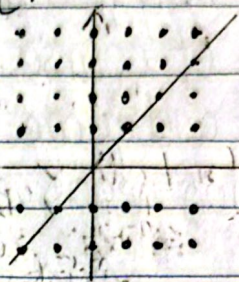
by cancellation, then $a_1 a_2 \dots a_{s-1} = b_1 b_2 \dots b_{t-1}$

by assumption, the factorisation is unique.

for $n > 0$, $[a]_n$ denotes the equivalence class of a under the modular arithmetic, and $\mathbb{Z}/n\mathbb{Z}$ denotes the set of all equivalence classes. modular

• Q the rational numbers are defined to be the quotient of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by $(a, b) \sim (c, d)$ if $ad = bc$.

*本质上就是用 (a, b) 表示 $\frac{a}{b}$. 在同一条过原点的线上的点表示相同大小的数, 并在一个 class 中.



① pre-addition on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is defined by $(a, b) + (c, d) = (ad + bc, bd)$

- $(a, b) \sim (a', b') \Rightarrow (a, b) + (c, d) \sim (a', b') + (c, d)$
- $(c, d) \sim (c', d') \Rightarrow (a, b) + (c, d) \sim (a, b) + (c', d')$

② pre-negation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is defined by $-(a, b) = (-a, b)$

- $(a, b) \sim (a', b') \Rightarrow -(a, b) \sim -(a', b')$

③ pre-multiplication on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is defined by $(a, b) \times (c, d) = (ac, bd)$

- $(a, b) \sim (a', b') \Rightarrow (a, b) \times (c, d) \sim (a', b') \times (c, d)$
- $(c, d) \sim (c', d') \Rightarrow (a, b) \times (c, d) \sim (a, b) \times (c', d')$

④ pre-reciprocal on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is defined by $(a, b)^{-1} = (b, a)$

- $(a, b) \sim (a', b')$ and $a, a' \neq 0 \Rightarrow (a, b)^{-1} = (a', b')^{-1}$
- if $x \neq 0$, then $x \times x^{-1} = x^{-1} \times x = 1$.

• ordering on $\mathbb{Q}$ (i) an integer is non-negative if it is in the image of the map $i: \mathbb{N} \rightarrow \mathbb{Z}$

(a) a rational number is non-negative if it has a representative (a, b) with a and b integers both of which are non-negative (and of course with $b \neq 0$)

(b) if x and y are rational numbers, then $x \leq y$ if $y - x$ is non-negative

• a field is a set X , equipped with two special elements $0 \in X$ and $1 \in X$ with $0 \neq 1$, two functions $+$: $X + X \rightarrow X$ and $\cdot$: $X \times X \rightarrow X$, and two other functions $-$: $X \rightarrow X$ and $(\cdot)^{-1}$: $(X - \{0\}) \rightarrow X$, satisfying the following axioms: for all $x, y, z \in X$, we have:

fields

(1) $0 + x = x + 0 = x$ * 0 is an additive identity

(2) $(-x) + x = x + (-x) = 0$ * negation is an additive inverse

(3) $(x + y) + z = (y + x) + z = 0$ * negation is an additive inverse

(4) $x + (y + z) = (x + y) + z$

(5) $1 \cdot x = x \cdot 1 = x$ * 1 is a multiplicative identity

(6) if $x \neq 0$ then $x \cdot x^{-1} = x^{-1} \cdot x = 1$

* reciprocal is a multiplication inverse

(7) $x \cdot y = y \cdot x$

(8) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(9) $x \cdot (y + z) = x \cdot y + x \cdot z$

(10) $1 \neq 0$

* fields have at least 2 elements

• an ordered field is a field $\mathbb{F}$ together with a total order $\leq$ such that additionally if $x, y, t \in \mathbb{F}$ with $x \leq y$ then

(i) $x + t \leq y + t$

• if $t \geq 0$, then $x \times t \leq y \times t$.

- let X be a totally ordered set; a subset $S \subseteq X$ is called bounded above if and only if there is $B \in X$ such that $\forall x \in S, x \leq B$
 - if B is an upper bound for S , then $\forall C \geq B, C$ is also an upper bound for S
 - $L \in X$ is a least upper bound for S if
 - L is an upper bound for S
 - if $x < L$ then x is not an upper bound for S
 - X is complete if every nonempty bounded-above subset of X has a least upper bound

• $\mathbb{R}$ the real numbers are defined to be the completion of the rationals.

- the reals are a complete ordered field
- for all $x \in \mathbb{R}$, there exists an $n \in \mathbb{N}$, such that $x < n$.

proof:

we should prove it by contradiction.

there exist a real number x , such that for all $n \in \mathbb{N}$, $n \leq x$, which means that x is an upper bound for $\mathbb{N}$ in $\mathbb{R}$.

so $\mathbb{N}$ is a nonempty bounded-above subset, so it has a least upper bound B .

consider $B-1$. since this isn't an upper bound for $\mathbb{N}$, so there exist $n \in \mathbb{N}$ such that $n > B-1$. then $n+1 > B$, impossible since B is upper bound. 17

- for all $x, y \in \mathbb{R}$, if $x > 0$ there exists an $n \in \mathbb{N}$ such that $nx > y$
- for all $x \in \mathbb{R}$, $x > 0$, there exists an $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < x$
- for all $x \in \mathbb{R}$, $x > 0$ there exists a rational number r such that $0 < r < x$
- for all $x, y \in \mathbb{R}$ such that $x < y$, there exists a number $r \in \mathbb{R}$ such that $x < r < y$

Field 相关问题是 inverse