

# I. Logic

**proposition** 命题, either true or false

| Connective | symbol        |
|------------|---------------|
| and        | $\wedge$      |
| or         | $\vee$        |
| not        | $\neg$        |
| implies    | $\Rightarrow$ |

| set operations    | symbol      |
|-------------------|-------------|
| intersection      | $\cap$      |
| union             | $\cup$      |
| complement        | $A^c$       |
| 注: 2.2.1          |             |
| <u>difference</u> | $\setminus$ |

一定要注意, 推出不能想当然。

对  $P \Rightarrow q$ , 若  $P$  为假, 则命题真。

**propositional variables** letters used to represent propositions.

## Well-formed formulas (WFFs)

def 1.2.2 (1) A propositional variable is a WFF.

(2.0) If  $\phi, \psi$  are WFFs, then

(2.1)  $(\phi \wedge \psi)$  is a WFF

(2.2)  $(\phi \vee \psi)$  is a WFF

(2.3)  $(\phi \Rightarrow \psi)$  is a WFF

(2.4)  $\neg \phi$  is a WFF

否则, 语句不是 WFF.

Truth assignment function that (set of propositional variables)  $\rightarrow \{T, F\}$

如  $v: V \rightarrow \{T, F\}$ , 这个  $V$  就是  $p \vee$  的意思

$$v(p) = T, v(q) = F$$

以此可以得到 WFFs 的 Truth values.

$$\boxed{\text{Let } v(p) = F, v(q) = T, v(r) = T}$$

$$v((p \Rightarrow q)) = T$$

$$v(((p \vee q) \Rightarrow \neg r)) = T$$

Logically equivalent.

Two WFFs have the same truth table.

(1.9) Two first order formulas have  
same truth value in every interpretation

De Morgan's Laws

$$\neg(\phi \vee \psi) \equiv (\neg \phi \wedge \neg \psi)$$

取反全取反

$$\neg(\phi \wedge \psi) \equiv (\neg \phi \vee \neg \psi)$$

Distributivity

$$(\phi \wedge (\psi \vee \theta)) \equiv ((\phi \wedge \psi) \vee (\phi \wedge \theta))$$

注：和，或也可以  
结合、交换，左式  
去括号的形式也  
能分配

$$(\phi \vee (\psi \wedge \theta)) \equiv ((\phi \vee \psi) \wedge (\phi \vee \theta))$$

contrapositive (反证)

$$(\phi \Rightarrow \psi) \equiv (\neg \phi \Rightarrow \neg \psi)$$

## Adequacy

即 set of connectives  $C$  中的符号可以表示任意组合逻辑。

Eg.  $\{\wedge, \vee, \neg\}$  is adequate.

$\{\wedge, \neg\}$ ,  $\{\vee, \neg\}$  are also adequate

$\{\wedge, \vee\}$  is not.

## First Order Logic

### Quantifiers

$\forall :=$  for all

$\exists :=$  there exists

$$\neg(\forall x \in X : P(x)) \equiv \exists x \in X : \neg P(x) \quad \text{不是所有} = \text{存在不}$$

$$\neg(\exists x \in X : P(x)) \equiv \forall x \in X : \neg P(x) \quad \text{不存在} = \text{所有都不}$$

注: Quantifiers 的顺序不同含义不同, 要具体分析。

## II. Sets, functions, permutations.

$a \in X \leftarrow$  set  $\emptyset = \{\} \text{ empty set}$

↑  
element

$X \subseteq Y$

↑  
subset

$X \neq Y$

↑  
proper subset

$A \cup B$

Union

$A \cap B$

intersection

$A \setminus B$

set difference

$A^c$

complement

$|X|$  size, cardinality

$f: X \rightarrow Y \leftarrow$  codomain  
 ↑      ↑  
 domain  
 function,  
 map

$\{f(x); x \in X\}$  image  
 值域

Injective / one-to-one iff  $\forall a, b \in X \quad f(a) = f(b) \Rightarrow a = b$

Surjective / onto iff  $\forall b \in Y \exists a \in X \text{ s.t. } f(a) = b$

Bijection both

Function composition  $(g \circ f)(x) = g(f(x))$  具有结合律

Identity function  $\text{id}_X: X \rightarrow X$  where  $\text{id}_X(x) = x$

Left inverse  $gf = \text{id}_X \quad g \in \mathbb{Z}, g: Y \rightarrow X$

Right inverse  $fg = \text{id}_Y \quad g \in \mathbb{Z}, g: Y \rightarrow X$

inverse  $gf = \text{id}_X \quad fg = \text{id}_Y \quad \text{删除}$

Left invertible (injective) 有 LI

Right invertible (surjective) 有 RI

Invertible (bijective)

$f, g$  invertible  $\Rightarrow f \circ g$  invertible

Permutation of set  $X$  is a bijection  $X \rightarrow X$

$S_n$  (交换群, alg 2 详讲) is the set of all permutations of  $\{1, \dots, n\}$

交换和函数一样, 仅具结合律

$$|S_n| = n!$$

Cycles

$$f = (a_1, a_2, \dots, a_m) \text{ s.t.}$$

$$f(a_i) = a_{i+1}, \quad f(a_m) = a_1,$$

$m$ -cycle

$$(1, 2, 3) \in S_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$(1, 2, 3) \in S_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

$$(a_1, a_2, \dots, a_{m-1}, a_m)^{-1} = (a_m, a_{m-1}, \dots, a_2, a_1)$$

Let  $a, b$  be disjoint cycles. Then  $ab = ba$

Every  $s \in S_n$  equals a product of disjoint cycles

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow 7 & \downarrow 6 & 3 & \downarrow 1 & \downarrow 2 & \downarrow 5 & \downarrow 4 \end{pmatrix} = (1, 7, 4)(2, 6, 5)(3)$$
$$= (1, 7, 4)(2, 6, 5)$$

$$(1, 2, 3)^0 = \text{id} \quad (1, 2, 3)^{-2} = (1, 3, 2)(1, 3, 2) = (1, 2, 3)$$

$$s^a s^b = s^{a+b} \quad (s^a)^b = s^{ab} \quad (st)^k \neq s^k t^k$$

**Order** ~~s~~ the smallest positive number  $n$  s.t.  $s^n = \text{id}$   
the order of an  $m$ -cycle is  $m$ .

the order of a product of disjoint cycles is  
the lowest common multiple of the lengths of cycles.

**Transposition** 2-cycle

$$(a_1, \dots, a_m)(a_m, a_{m+1}) = (a_1, \dots, a_{m+1})$$

$$(1, 2, 3, 4) = (1, 2)(2, 3)(3, 4)$$

**odd** odd number of transposition **1-cycles**

**even** even number of transposition

$$\text{sign}(s) = \begin{cases} 1, & \text{even} \\ -1, & \text{odd} \end{cases}$$

$$\text{sign}((a_1, \dots, a_m)) = (-1)^{m-1}$$

$$\text{sign}(s) = \text{sign}(s^{-1})$$

$$\text{sign}(st) = \text{sign}(s) \text{ sign}(t)$$

### III - matrices

关于矩阵记住“先行后列”。

$$3 \times 2 \text{ matrix} \quad \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \quad \begin{array}{l} \text{三行二列} \\ \text{a}_{22}, 2, 2 \text{ entry} \\ \text{a}_{32}, 3, 2 \text{ entry} \end{array}$$

square matrix :  $n \times n$

column vector :  $n \times 1 \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

row vector :  $1 \times n \quad (1 \ 2)$

先行

$$\left( \begin{array}{cc} a_{11} & a_{12} \\ a_{21} & a_{22} \end{array} \right) \left( \begin{array}{c} b_{11} \\ b_{21} \end{array} \right) = \left( \begin{array}{c} a_{11}b_{11} + a_{12}b_{21} \\ \dots \\ \dots \end{array} \right)$$

有结合律

Linear combination  $a_1 c_1 + \dots + a_n c_n$

Every column of  $AB$  is a LC of columns of  $A$

你要不要猜一下这里的  $a_1, \dots, a_n$  是  $B$  的哪列

Standard basis vectors

$$(\text{in } \mathbb{R}^n) \quad e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Transpose  $A^T \quad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

~~(AB)<sup>T</sup> = B<sup>T</sup>A<sup>T</sup>~~

数字要

$0_{m \times n}$  matrix with all entries 0.

In  $n \times n$  identity matrix with  $i, j$  entry 0 if  $i \neq j$  else 1.

MATH0005 没有 determinants, 所以考试别用它证可逆性

$(\exists \underline{v} \neq 0 \text{ s.t. } A\underline{v} = \underline{0}) \Rightarrow A \text{ is not invertible}$

$$(A_1 A_2 \cdots A_k)^{-1} = A_k^{-1} A_{k-1}^{-1} \cdots A_1^{-1}$$

$$(A^T)^{-1} = (A^{-1})^T$$

有整行、整列为0的矩阵不可逆

- Row Operations
1. 把某<sup>行</sup>的元素加给<sup>行</sup>另行。
  2. 乘某行。
  3. 交换两行。

elementary matrix 对  $I_n$  做单次 RO.

可以写成  $r(I)$ ,  $r(A) = r(I)A$

虽然 RO 可逆，一系列 RO 也可逆

Augmented matrix  $(A|b)$ , 关于  $Ax = b$  的方程组

$$\text{如 } \begin{pmatrix} 1 & -1 & 5 \\ 2 & 3 & 4 \end{pmatrix} \quad \begin{array}{l} x - y = 5 \\ 2x + 3y = 4 \end{array}$$

对 AM 做 RO, 方程组的解不变

Leading entry (LE) 每行中首个非零元素。

Row Reduced Echelon Form (RREF)

1. 所有 LE 为 1。
2. 全零行在底部。
3. 有 LE 的列其它行均为零。
4. 上面的 LE 靠左。

$$\begin{pmatrix} 1 & \alpha & \beta & 3 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ is in RREF if } \beta = 0$$

对任意矩阵，有且仅有一个对应 RREF 矩阵。

Solutions?

1. 若最右列有 LE, 无解。
2. 若存在 free variables (所在列无 LE), 有无数解。
3. 有唯一解。

## Fundamental solution.

对( $A|0$ )，若有几个 free variables，将它们依次设为1，求其它值，就是它的 fundamental solutions.

如  $\begin{pmatrix} 1 & 0 & \boxed{1} & 1 & 0 \\ 0 & 1 & \boxed{-1} & 2 & 0 \end{pmatrix}$  先设  $x_3 = 1$ ,  $\underline{x} = (-1 \ 1 \ 1 \ 0)^T$

设  $x_4 = 1$ ,  $\underline{x} = (-1 \ -2 \ 0 \ 1)^T$

它有2个 f.s.

下面三种情况等价：(虽然A是方块矩阵)

1. A 可逆。

2.  $A\underline{x} = 0 \Leftrightarrow$  有唯一解  $\underline{x} = 0$ 。

3. A 可用 RO 变为  $I_n$ 。

找逆方法，对方块矩阵  $A$ ：求  $(A|I_n)$  的 RREF，

如果它是  $(I_n|B)$ ，则  $B$  是  $A$  的逆，  
反之， $A$  不可逆。

对方块矩阵，有左逆、有右逆、有逆 等值。

## IV Linear Algebra

Fields, 可以加、减、乘、除的代数结构。

在0003有一定介绍，不是0005的主要考点。

$\mathbb{R}, \mathbb{C}, \mathbb{Q}$  是域,  $\mathbb{Z}, \mathbb{N}$  不是

Finite fields 通常以  $\mathbb{F}_p$  (其中  $p$  为质数) 为例, 对超过  $p$  的运算值取模。  
更进一步的内容是0006的范围。

### vector space

A vector space over a field  $F$  is a set  $V$  satisfying:

①  $\forall x, y \in V \quad \exists \underline{x+y} \in V \text{ s.t. }$

②  $\underline{x+(y+z)} = (\underline{x+y})+z$

③  $\exists \underline{0} \in V \text{ s.t. } \underline{x+0} = \underline{x}$

④  $\forall \underline{x} \in V \quad \exists \underline{-x} \in V \text{ s.t. } \underline{x+(-x)} = \underline{0}$

$\forall a \in F \text{ and } \forall \underline{x} \in V \quad \exists \underline{ax} \in V \text{ s.t. }$

$\forall a, b \in F \text{ and } \forall \underline{x}, \underline{y} \in V:$

⑤  $a(b\underline{x}) = (ab)\underline{x}$

⑥  $1\underline{x} = \underline{x}$

⑦  $a(\underline{x+y}) = a\underline{x} + a\underline{y}$

⑧  $(a+b)\underline{x} = a\underline{x} + b\underline{x}$

可以推知  $0V = \underline{0}$

Vector space 写法

$\mathbb{R}^n$ ,  $\mathbb{C}^n$ ,  $\mathbb{F}^n$

$M_{m \times n}(\mathbb{R})$  是 over  $\mathbb{R}$  的一个空间

$\mathbb{C}[x]$  是以  $f(x) = 0$  为零向量的空间，包含一系列多项式（其实就是所有）

(注：一般不定义向量乘，只定义数乘)

$\mathbb{C}_{\leq n}[x]$  其中最大次数为  $n$

$F$  是  $\mathbb{R} \rightarrow \mathbb{R}$  的函数的空间

~~从头到尾~~  $\mathbb{F}$ -vector space 和 vector space over  $\mathbb{F}$  同意。

## Subspace

① 包含  $0$

② 仍可加，封闭

③ 仍可数乘，封闭

Let  $A$  be  $m \times n$  matrix with entries in  $\mathbb{F}$

$N(A) = \{K \in \mathbb{F}^n : AK = \underline{0}_m\}$ . Then  $N(A) \subseteq \mathbb{F}^n$

$N(A)$  is the nullspace of  $A$  能把  $A$  变成  $0$  的向量的集合。

## Linear independence

if  $\exists \lambda_1, \dots, \lambda_k$  not all zero s.t.  $\sum_{i=0}^k \lambda_i v_i = 0$

then  $v_1, \dots, v_k$  is called linear dependent (LD) 一列向量可以被消

若  $\neg(LD)$ , linear independent (LI) 不能被消为零 为零

$$\lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \underline{0}_2 \Rightarrow \lambda_1 = \lambda_2 = 0, \text{ 它们 LI}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \underline{0}_2, \text{ 它们 LD}$$

将  $\underline{v}_1, \dots, \underline{v}_k$  合成矩阵 A

$$a_1 \underline{v}_1 + \dots + a_k \underline{v}_k = \begin{pmatrix} 1 & \dots & 1 \\ \underline{v}_1 & \dots & \underline{v}_k \\ 1 & \dots & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$$

若  $A \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = 0$  也就是原式为 0，也就是若它有非(全)零解。  
它就 linearly dependent.

也就是说，证明 LD 的办法，就是找到这样的解

证明 LI 的办法，是证  $\sum \lambda_i \underline{v} = 0 \Rightarrow \lambda_1 = \dots = \lambda_k = 0$   
(省流：RREF)

对 LI 的向量来说，若它们表示的结果相同，则所有系数相同。

Span  $\text{span}(\underline{c}_1, \dots, \underline{c}_n) = \left\{ \sum_{i=1}^n \lambda_i \underline{c}_i : \lambda_1, \dots, \lambda_n \in F \right\}$

即它们的全部线性结合。

$$\text{span}(\dots) \leq V$$

↑ 整根线  
↑ span(V)

spanning sequence for V is  $\underline{v}_1, \dots, \underline{v}_k$  s.t.  $\text{span}(\dots) = V$

如  $e_1, e_2$ ;  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  等都是  $\mathbb{R}^2$  的 SS.

另外根据定义，空数列是 { } 的 SS.

## Bases (基数 basis)

LI 的 spanning sequence.

要说明一系列元素构成 basis, ① 把 V 用 basis 表示

例)  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aE_{11} + bE_{12} + cE_{21} + dE_{22}$

② 证 LI.

例)  $aE_{11} + \dots + dE_{22} = 0_{2 \times 2} \Rightarrow a = \dots = d = 0$

## Steinitz exchange

### Steinitz Exchange Lemma

若有  $\underline{s}_1, \dots, \underline{s}_m$  是  $V$  的 spanning sequence ;  $\underline{l}_1, \dots, \underline{l}_n$  是 linearly independent elements of  $V$ . 则  $n \leq m$ .

### Corollary

$V$  的 bases 都有相同的 size.

dimension of a vector space  $V$ ,  $\dim V$ , 是它的 basis 的 size.

$$\dim F^n = n \text{ bks } \underline{e}_1, \dots, \underline{e}_n$$

### the Extension Lemma

若  $\underline{v}_1, \dots, \underline{v}_n$  LI,  $\underline{u} \notin \text{span}(\underline{v}_1, \dots, \underline{v}_n) \Rightarrow \underline{v}_1, \dots, \underline{v}_n, \underline{u}$  LI.

有  $U \leq V$

$$\textcircled{1} \dim U \leq \dim V$$

$$\textcircled{2} \text{ 若 } \dim U = \dim V \text{ 则 } U = V$$

一串 LI 的 “元素必然被某个 basis 包含”

$$U \leq X, V \leq X \Rightarrow U + V \leq X \quad (\text{虽然只是简单相加, 但实际效果是方向都加在一起了, 所以是维度的并集}, \text{ 不是 } UV \text{ 的并集})$$
$$U \cap V \leq X \quad (\text{我也不知道为什么要考虑交集})$$

$$\dim(X+Y) = \dim X + \dim Y - \dim X \cap Y$$

例如两个平面相加, 结果是三维空间,  $3 = 2 + 2 - 1$  (平面的交线)

除了之前提到的使  $A\mathbf{v} = \mathbf{0}$  的 nullspace, 对于  $A \in M_{m \times n}(\mathbb{F})$

Column space  $C(A)$  span of columns of  $A \leq \mathbb{F}^m$

Row space  $\text{Row}(A)$  span of rows of  $A \leq M_{1 \times n}(\mathbb{F})$

对  $A$ , 有可逆矩阵  $E$ ,  $\text{Row}(EA) = \text{Row}(A)$

↑  
可逆矩阵是方矩, 规模显然不变.

① RREF matrix 的非零行是其 row space 的 basis

② 若要求 column space, 可以求  $A^T$  的 RREF.

③  $A\underline{x} = \underline{0}_m$  的 fundamental solutions 是  $N(A)$  的 basis.

总结一下: 令  $L = \underline{l}_1, \dots, \underline{l}_n$  为  $LI$ ,  $S = \underline{s}_1, \dots, \underline{s}_n$  是  $SS$ .

$|L| \leq \dim V \leq |S|$ ,  $\text{span}(L) \leq V = \text{span}(S)$

对于空间, 合并后维数要减去先共有的方向。

求用矩阵生成的  $C(A)$ ,  $\text{Row}(A)$ ,  $N(A)$  都与 RREF 有关。

Linear map 令  $V, W$  为  $\mathbb{F}$ -vector spaces, 若

①  $\forall \lambda \in \mathbb{F}, \underline{x} \in V$  s.t.  $f(\lambda \underline{x}) = \lambda f(\underline{x})$

②  $\forall \underline{x}, \underline{y} \in V$  have  $f(\underline{x} + \underline{y}) = f(\underline{x}) + f(\underline{y})$

则  $f: V \rightarrow W$  是线性映射。

例如  $D: \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ , 其中  $D(f) = \frac{df}{dx}$

$V, W$  的形式可以不一样

对  $T: V \rightarrow W$

kernel  $\ker T := \{v \in V : T(v) = \underline{0}_W\}$  所有能变成  $0$  的向量

Image  $\text{im } T := \{T(v) : v \in V\}$   $T$  的值域

If  $T$  is linear then  $T(\underline{0}_V) = \underline{0}_W$

$$\ker T \leq V, \text{im } T \leq W$$

Rank-Nullity Theorem  $\dim \text{im } f + \dim \ker f = \dim V$

↑                      ↑

rank of  $f$       nullity of  $f$ , null  $f$ .

其实很好理解，不会变成  $0$  的，可以体现原有维度结构，

变成  $0$  的维度就没有，要作为 rank 加进去。

Coordinate map

例如  $E = \underline{B} e_1, \dots, \underline{B} e_n$   $\underline{V} = [V]_E$ , 即使用 basis 表示

对  $\mathbb{F}$ -vector space  $V$ , 有 basis  $B = \underline{b}_1, \dots, \underline{b}_n$

在电子化表达中，基的字母是手写体(script)，手写时无差别。

对  $v \in V$  存在唯一的表达  $v_1 \underline{b}_1 + \dots + v_n \underline{b}_n$

把它们写成 column vector  $(v_1, \dots, v_n)^T \in \mathbb{F}^n$

就是  $[v]_B$

$v \mapsto [v]_B$  就是 coordinate map with respect to  $B$ .

对  $f: V \rightarrow W$ , ①  $f$  is surjective iff  $\dim \text{im } f = \dim W$   
(线性映射)

②  $f$  is injective iff  $\ker f = \{\underline{0}_V\}$

可以证明，coordinate map 满足以上两条， $\Leftrightarrow$  bijection.

isomorphism bijection

isomorphic  $\Leftrightarrow$  two vector spaces have isomorphism between them

每个非无穷维的空间都与某个  $\mathbb{F}$  isomorphic.

The matrix of  $T$  with respect to initial basis  $B$  and final basis  $C$ , written  $[T]_C^B$

对  $T: V \rightarrow W$

可以将  $T(b_j)$  表示为  $\sum_{i=1}^m a_{ij} c_i$

这个矩阵就是  $(a_{ij})$

也就是用  $C$  逐个表示  $B$ , 对  $b_j$ , 有  $[T(b_j)]_C$ , 被填在  $j$  列。

$$[T \circ S]_D^B = [T]_D^C [S]_C^B$$

对  $V$  的 bases  $B, B'$ ,  $W$  的 bases  $C, C'$ , 有

$$[T]_{C'}^{B'} = [id_W]_C^C [T]_C^B [id_V]_B^{B'}$$

为了确保我和小伙伴们考试顺利及  $alg3$  顺利, 我有一句重要的  
话要讲:

古人这样排版

即这些 Bases 的表示顺序与古书排版顺序相同。

题目一般考的是  $[T]_B^B$ , 按以下方法求:

$$[T]_B^B = [id]_B^\Sigma [T]_\Sigma^\Sigma [id]_\Sigma^B$$

$$([id]_\Sigma^B)^{-1}$$

一般很简单, 例如

$T$  的结果就是第一列

把  $B$  中 bases 逐列写出

## Algebra 2

## I 数论

① 整除 a divides b if  $b = az$  for some  $z \in \mathbb{Z}$

$$a | b$$

~~2 | 6~~ ;  $5 | 11$

prime composite : has a non-trivial factorization

质数

合数

↑  
被分解为含±的两数。

↑  
units  
units

对  $a \div b = q \dots r$ , 答案是唯一的, 即  $a = bq + r$  有唯一整解,

使得  $0 \leq r < b$

最大公因数

highest common factor  $\text{hcf}(a, b)$

greatest common divisor  $\text{gcd}(a, b)$

$$\text{hcf}(6, 25) = 1$$

$$\text{hcf}(-8, -12) = 4$$

辗转相除

求  $\text{hcf}(1169, 560)$

$$1169 = 560 \times 2 + 49$$

$$1169 \div 560 = 2 \dots 49 \quad \text{gcd}(560, 49)$$

$$560 = 49 \times 11 + 21$$

$$560 \div 49 = 11 \dots 21 \quad \text{gcd}(49, 21)$$

$$49 = 21 \times 2 + 7$$

$$49 \div 21 = 2 \dots 7 \quad \text{gcd}(21, 7)$$

$$21 = 7 \times 3$$

Hence  $\text{hcf}(1169, 560) = 7$

## 线性结合

上一节中的过程也用于求一个整数对 两个整数的线性结合。  
以其为公因数

$$\text{hcf}(5, 7) = \boxed{1}$$

$$7 = 5 \times 1 + 2$$

$$\begin{aligned} 5 &= 2 \times 2 + 1 & \Rightarrow 1 &= 5 - 2 \times 2 = 5 - (7 - 5) \times 2 = 5 \times 3 - 7 \times 2 \\ 2 &= 1 \times 2 \end{aligned}$$

## 分解其它数字系统

质因数分解

常见的数字系统，如  $\mathbb{Z}$ ，是有分解唯一性的。也有不唯一的。

课纲不要求背任何其它系统，但知道下面的内容为宜。

$\mathbb{Z}[i]$  是包含了  $a+bi : a, b \in \mathbb{Z}$  的集，它的分解是唯一的，其中的 units 是可以与另一元素形成  $uv=1$  的元素。只有 4 个， $\pm 1, \pm i$ 。

$R = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$  就无分解唯一性。

## Relations

reflexive  $\forall a \in X, aRa$

symmetric  $\forall a, b \in X, aRb \Rightarrow bRa$

transitive  $\forall a, b, c \in X, aRb \text{ and } bRc \Rightarrow aRc$

比如，对  $a < b$ ，就无自身性，不可反，可类推。

如果某种关系同时满足这三项，被称为 equivalence relation.

比如  $xRy := 3 | y-x$  就是这样一种关系。

对这样的关系  $R$ ，定义 equivalence class of  $a$  :

$[a] = \{x \in X : aRx\}$  比如  $[0]$  在上面就是所有 3 的倍数

$[a] = [b] \Leftrightarrow aRb$   $[a] \cap [b] = \emptyset$  or  $[a] = [b]$

## II 群

群 (group) 的定义基于一个集合和一个二元运算，除了封闭性外，对  $\star$  on  $G$  满足：

- ①  $\star$  is associative.
- ②  $G$  has an identity element under  $\star$ .
- ③ each element of  $G$  has an inverse under  $\star$ .

如果它还满足：

$$\forall g, h \in G, g \star h = h \star g$$

则 the group is called Abelian or commutative.

题外话：如果你看到 denoted by juxtaposition，那这种运算本身没有符号，比如  $xx = x^2$  这样，没写乘号。

另外，只要运算满足结合律，不论是左零、左逆、右零、右逆，都能推出上面给出的②、③

$$fg = fh \quad \text{for } \forall g \in G, \{gx : x \in G\} = G$$

$\uparrow$   
 $g, (g^{-1}g) = g$ , 所以任何元素若理解为函数，都是 surjective 的。

## 对称群, Symmetric group

对  $X = \{1, 2, \dots, n\}$ ,  $S(X) = S_n = \{f: X \rightarrow X \text{ s.t. } f \text{ is bijective}\}$

如果你往前翻 15 页, 你就能找到一个伏笔。

它还有一个别名叫自同构群 automorphism, 我觉得不会考, 总得来讲就是  $\text{Aut}(X)$  中的函数可以继承  $X$  的数学结构, 如  $f(u) + f(v) = f(u+v)$

如果你往前翻 10 页, 你就能找到另一个伏笔。

这种群被记作  $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ 。

对加法运算,  $n$  可以取任意值。

对乘法, 群不含 0, 且  $n$  为质数。记作  $\mathbb{Z}_n^* = \{\overline{1}, \overline{2}, \dots, \overline{n-1}\}$ .

这两个群都是 abelian group

可以用求 1 的线性结合的方法求  $\overline{P}^{-1}$  在  $\mathbb{Z}_{p_2}^*$  中的值

这样吧, 你看它: 

|   |   |
|---|---|
| 1 | 3 |
| 2 |   |

, 这个数字华容道能还原吗?

不能, 因为它的移动来自一个 ~~抽象~~ 空间对称群的两个 ~~元素~~ 元素。

isometry: 双射  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  s.t.  $|f(x) - f(y)| = |x - y|$

令  $T$  是包含平面上点的集,  $\text{Sym}(T)$  是所有能在其中进行的 isometry.

你不用管这些傻逼大学生才看的东西, 把上面 1, 2, 3 在的位置

视作  $T = \{1, 2, 3\}$ , 那  $|\text{Sym}(T)| = 6$ , 因为有不变、交换 12, 23, 31, 顺逆时针转动 6 种操作。它不可能超过 6 用 ~~抽象~~ 排列很好证明。

将以上记作  $e, x_1, x_2, x_3, y_1, y_2$

|       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|
| $e$   | $x_1$ | $x_2$ | $x_3$ | $y_1$ | $y_2$ |
| $e$   | $x_1$ | $x_2$ | $x_3$ | $y_1$ | $y_2$ |
| $x_1$ | $x_1$ | $e$   | $y_2$ | $y_1$ | $x_3$ |
| $x_2$ | $x_2$ | $y_1$ | $e$   | $y_2$ | $x_1$ |
| $x_3$ | $x_3$ | $y_2$ | $y_1$ | $e$   | $x_2$ |
| $y_1$ | $y_1$ | $x_2$ | $x_3$ | $x_1$ | $e$   |
| $y_2$ | $y_2$ | $x_3$ | $x_1$ | $x_2$ | $e$   |

而用  $y_1, y_2$  不存在组合出  $x_3^{-1}$  的可能,  
故不能还原。

记  $x = x_1, y = y_1$

$$\text{Sym}(T) = \{e, y, y^2, x, yx, y^2x\}$$

我们上一页讲到  $\text{Sym}(T) = \{e, y, y^2, xy, yx, y^2x\}$

它也可以表示为  $\langle x, y : y^3 = e, x^2 = e, xy = y^2x \rangle$

这个过程叫 finding a presentation.

它可以很复杂也可以很简单，但有鉴于多数对称群本来就很复杂，所以找的过程从来都不简单，要打表硬找。

(把所有关系都写一遍也行，但很累)

Order ① of a group  $|G|$ , number of elements in G.

② of an element, the least positive integer  $n$  s.t.  $g^n = e$ .  
denoted  $o(g)$

e.g.  $\mathbb{Z}_5^*$  under multiplication

$$\bar{2}^4 = \bar{16} = 1 \quad \text{so} \quad o(\bar{2}) = 4$$

循环群 cyclic group

$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \subseteq G$ , if  $G = \langle g \rangle$ , then G is said to be generated by g,  $\Rightarrow G$  is cyclic.

可以无穷，比如对加法  $\langle 1 \rangle = \mathbb{Z}$ , 叫 infinite cyclic group,  $C_\infty$   
对有限群，记作  $C_n$

子群 Subgroups

①  $e \in H$

②  $hk \in H$

这基本上就是废话，意思是  $H \subseteq G$  也是个群。

③  $h^{-1} \in H$

例如  $S_n$  的所有偶置换组成的 alternating group  $A_n$ .

$$|S_n| = n!, \quad |A_n| = \frac{n!}{2}$$

## 拉格朗日定理 Lagrange's theorem

$$H \subseteq G \Rightarrow |H| \mid |G|$$

对  $g \in G$   $\bullet := g^{-1}k \in H$

$[g] = gH$  指  $g$  有这个 equivalence relation 的元素的集，又与  $g$  与  $H$  中全体元素左乘的结果相同。

而  $|G| = |[g_1]| + \dots + |[g_r]|$  注意  $R$  的定义没有规定  $gk$  是什么，所以全部都能展开

$$= |g_1 H| + \dots + |g_r H| \quad gh = gh' \Rightarrow g^{-1}gh = g'g'h' \Rightarrow h = h'$$

$$\text{故 } |gH| = |H|$$

$$= r|H| \quad \square$$

⑩

$g \in G$ ,  $G$  is finite  $\Rightarrow o(g) \mid |G|$

对  $|G| = p$  where  $p$  is a prime,  $G = C_p$

Let  $p$  be a prime,  $a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

$$\text{e.g. } 2^{66} \pmod{17} = 2^{16 \times 4 + 2} \pmod{17} = 4 \pmod{17}$$

## 群同态 Group homomorphisms

它是一种映射，和线性映射类似，保留群的结构。

$\phi: G \rightarrow H$  is a group homomorphism if

$$\forall g, k \in G, \phi(gk) = \phi(g)\phi(k)$$

$$\text{e.g. } \phi: \mathbb{Z} \rightarrow \mathbb{Z}, \text{ by } \phi(z) = \bar{z}$$

$$\phi: C_6 \rightarrow C_4 \text{ 只能 } \phi(e) = \phi(a^3) = \phi(a^4) = e \dots \dots \text{ 否则不符合定义。}$$

回顾一下，kernel 是可得 0 的输入，image 是值域

Let  $\phi: G \rightarrow H$

$$\text{Ker}(\phi) = \{g \in G : \phi(g) = e\}$$

$$\text{Im}(\phi) = \{\phi(g) : g \in G\}$$

$$\text{比如对 } \phi: \mathbb{Z} \rightarrow \mathbb{R} \quad \text{Ker}(\phi) = 2\mathbb{Z} \quad \text{Im}(\phi) = \{-1, 1\}$$

## 群同构 Group isomorphisms

如果 group homomorphism is bijective then it's called a group isomorphism.

所以两个群 homo，说明它们是同，如果 iso，说明完全相同？

总之，记作  $G \cong H$ .

$$(\mathbb{Z}_5^*, \times) \cong (\mathbb{Z}_4, +)$$

## III determinants

好日子来了！

$$\det A = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

我们回忆一下  $3 \times 3$  的行列式求法：

$$\begin{pmatrix} a & b & c \\ \vdots & |a_1, a_2| \\ \vdots & |a_3, a_4| \end{pmatrix} = a a_1 a_4 - a a_2 a_3 - b \underline{\dots}$$

↑                      ↑  
对应  $\sigma = (1)$    对应  $\sigma = (2, 3)$       这样一共有 6 项，对应  $|S_3| = 6$ 。  
 $\text{sign} \neq +1$        $\text{sign} \neq -1$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$A^{-1} = \frac{1}{\det A} C^T \quad \textcircled{1} \quad M = \begin{pmatrix} |e| & | & \dots & \dots \\ |h| & i & | & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

$$\textcircled{2} \quad C = \begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

$$\textcircled{3} \quad C^T = \begin{pmatrix} \nearrow & \nearrow \\ \nwarrow & \nearrow \end{pmatrix}$$

$$\det(A^T) = \det(A)$$

对 lower triangular matrix  $\det(A) = a_{11} a_{22} \cdots a_{nn}$

$$\begin{pmatrix} a_{11} & 0 & 0 & \cdots \\ \cdots & a_{22} & 0 & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

row ops 对 det 的影响：

① 交换两行  $\det$  变号

② 乘某行  $\det$  乘此倍数

③ 把某行的数倍加到另一行 不变

A matrix is invertible iff  $\det \neq 0$

下面写的 E 是 17 页前的 elementary matrix, 表示 RO.

$$\det(E_n \cdots E_1 A) = \det(E_n) \cdots \det(E_1) \det(A)$$

可见最终若得到一个 RREF 的矩阵, 显然只有其为  $I_n$  才可逆, 而这是唯一  $\det \neq 0$  的 RREF 矩阵。

$$\det(AB) = \det(A) \det(B)$$

minor  $(i, j)$ -minor  $M_{ij}$  去  $i$  行  $j$  列的  $\det$

cofactor  $(i, j)$ -cofactor  $C_{ij}$  乘  $(-1)^{i+j}$

例如  $M_{23} = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix}$

$$C_{23} = -M_{23}$$

$$\det(A) = \sum_{j=1}^n a_{ij} C_{ij} \text{ for any } i.$$

这就是为什么当  $n=3$ ,  $\det(A) = a_{11} C_{11} + a_{12} C_{12} + a_{13} C_{13}$

当然, 列也可以。那么若一个大矩阵有一行  $-M_{12}$   
几乎是 0, 可以从那行开始消。

## Adjugate

$\text{adj}(A)$ , 在  $(i, j)$  上填  $C_{ji}$

把  $C_{ji}$  找到并 transpose, 对应了 3 阶求取的那三步。

$$A^{-1} = \frac{\text{adj}(A)}{\det(A)}$$

## IV 对角化

$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$  记作  $\text{diag}(d_1, \dots, d_n)$

diagonalizable  $\exists P$  s.t.  $P^{-1}AP$  is diagonal.

eigenvalues 特征值

e eigenvectors 特征向量

每一个向量都大概率有特征向量，而这些又对应特征值。

$$A\mathbf{v} = \lambda \mathbf{v}$$

$\det(\lambda I - A) = 0 \Leftrightarrow \lambda$  is an eigenvalue of  $A$

如对  $\begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix}$   $\det\begin{pmatrix} \lambda-1 & -2 \\ -6 & \lambda-2 \end{pmatrix} = (\lambda-5)(\lambda+2) = 0 \Rightarrow \lambda = 5 \text{ or } -2$

虽然特征值可以共同翻倍，但就用这俩。

$$\lambda = 5 \Rightarrow \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 5 \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow 2x = 0y \Rightarrow \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$\lambda = -2 \Rightarrow \begin{pmatrix} 1 & 2 \\ 6 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = -2 \begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{pmatrix} -2 \\ 3 \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & -2 \\ 2 & 3 \end{pmatrix}$$

$$D = P^{-1}AP = \begin{pmatrix} 5 & 0 \\ 0 & -2 \end{pmatrix}$$

我们使用的这个多项式是有名字的

characteristic polynomial  $c_A(t) = \det(tI_n - A)$

有了  $C_A(t)$ , 就可以快速判断其对角化过程。

① 若  $C_A(t)$  在 field  $\mathbb{F}$  上不可因式分解, 则 A 不可对角化。

② 反之它可以被分解为:

$$C_A(t) = (t - \lambda_1)^{f_1} \cdots \cdots (t - \lambda_r)^{f_r}$$

这里的  $\lambda_i$  就是特征值

这里的  $f_i$  叫  $\lambda_i$  的 algebraic multiplicity.

代数重数

eigenspace

$$E_\lambda = \{ \underline{v} \in \mathbb{F}^n : A\underline{v} = \lambda \underline{v} \}$$

而  $\lambda_i$  的 geometric multiplicity 是  $e_i = \dim(E_{\lambda_i})$

几何重数

若  $e_i = f_i$ , 则 A 可对角化, 否则不能。

所有的这些向量可以组成一个等于  $\mathbb{F}^n$  的 basis, 将它们作为  
一个 matrix 的列, 就是 P, 其必然可逆。

$$\textcircled{3} \quad D = P^{-1}AP$$

Direct sums.

Let  $U, W \subseteq V$ , if  $U \cap W = \{0\}$ , then the sum  $U + W$  is direct and we write  $U + W = U \oplus W$ .

例 如  $U = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R} \right\}$ ,  $W = \left\{ \begin{pmatrix} x \\ x \end{pmatrix} : x \in \mathbb{R} \right\}$

$$U + W = \left\{ \begin{pmatrix} x+y \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}, \text{ 显然等于 } \mathbb{R}^2, \text{ 且其为直和。}$$

若存在  $P$  使  $B = P^{-1}AP$ , 则  $A$  和  $B$  are similar.

如果它们相似, 则  $C_A(t) = C_B(t)$

④  $\exists a_i \in F$ , for  $n \times n$  matrix  $A$ , s.t.

$$\sum_{i=0}^{n^2} a_i A^i = 0$$

所以考试里可能会出要你写  $f(A) \in F[t]$ , 使  $f(A) = 0$  的题

如果  $A$  可以对角化, 那  $f(D) = f(A)$ , 因为  $f(P^{-1}AP) = P^{-1}f(A)P$

应该会强调 monic polynomial, 不要担心, 过大的多项式次数是加倍的,

$$C_A(A) = 0 \quad \text{and} \quad m_A | C_A$$

所以可以写出  $\det(IA - A) = 0$ , 然后看一下能不能拆成一样的。

↑  
其中它作为系数, 不变, 另一个展开。