Algebra Supplementaries

ζ

November 22, 2022

Contents

Chapter 1

Introduction

1.1 Basic Concepts

1.1.1 Basic Concepts in Set Theory

Maps

A map f between two nonempty sets A and B is a correspondence between elements of A and B. For each $a \in A$, there is a unique corresponding element b in B. We write it as $f : A \to B$ and b is called the image of a under map f, a is in the preimage of b under f, and we write it as $b = f(a)$. And

$$f(A) := \{\, b \in B \,|\, \exists\, a \in A, s.t\ f(a) = b \,\}.$$

$$f^{-1}(S) = \{\, a \in A \,|\, f(a) \in S \,\}\ ,\ \text{for}\, S \subseteq B.$$

Definition 1.1.1. We call f is **injective** if $f(a_1) \neq f(a_2)$ for $a_1, a_2 \in A$, $a \neq b$. We call f is **surjective** if $f^{-1}(b) \neq \emptyset\ \forall\, b \in B$. We call f is **bijective** if f is both injective and surjective.

Cartesian product

Definition 1.1.2. (Cartesian product) Let A, B be given nonempty sets, we define

$$A \times B := \{\, (a, b) \,|\, a \in A \textit{ and } b \in B \,\}$$

Example. *We can view xOy plane as a set of coordinate* (x, y), $x, y \in \mathbb{R}$. *Or we can write it as* $\mathbb{R} \times \mathbb{R}$ *or* $\mathbb{R}^2$. *It can also be viewed as the complex plane* $\mathbb{C}$.

Example.

$$\{a, b\} \times \{c, d\} = \{(a, c), (a, d), (b, c), (b, d)\}.$$

Operation

An **operation** is essentially a map from the Cartesian product $S \times S$ to original set S.

Example. *Some operations:*

1. *Addition.* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (*also* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). *for example, we have* $1 + 1 = 2$.
2. *Subtraction.* $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$).
3. *Multiplication.* $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$)
4. *Division.* $\mathbb{Q} \times \mathbb{Q}^* \to \mathbb{Q}$ ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$), *it is not an operation strictly.*

Relations

A relation, for example $x < y$ is an inequality with the notation "$<$", and we call this relation "less than". For general pairs (x, y), we can also define some relation $\sim$, and x, y having this relation if $x \sim y$.

Definition 1.1.3. A **relation** of pairs $(x, y) \in S \times S$ is a subset R of $S \times S$, and call x, y having this relation when $(x, y) \in R$, denoted as $x \sim_R y$, we usually ignore R when there is no ambiguity.

Example. *There are some common relations.*

- *Total ordering relation.*
- *Partial ordering relation.*
- *Equivalence relation.*

Problem. *Let* $S = \{a, b, c, d\}$, *and* $\mathcal{P}(S)$ *be the power set of* S, *find the relation set* R *of* $\mathcal{P}(S) \times \mathcal{P}(S)$ *for the inclusion relation "*$\subseteq$*".*

1.1.2 Equivalence relation

Definition 1.1.4 (**Equivalence relation**)**.** A binary relation $\sim$ on a set X is said to be an equivalence relation, if and only if it is reflexive, symmetric and transitive. That is, for all a, b, and c in X:

- $a \sim a$ (reflexivity).
- $a \sim b$ if and only if $b \sim a$ (symmetry).
- If $a \sim b$ and $b \sim c$ then $a \sim c$. (transitivity).

1.2 Number Systems

1.2.1 Natural Numbers

This all comes from **Peano Axioms**, The first axiom states that the constant 0 is a natural number:

(i) 0 is a natural number.

(ii) If n is a natural number, $n++$ is a natural number.

(iii) For every natural number n, $n = 0$ is false. That is, there is no natural number whose successor is 0.

(iv) For all natural numbers m and n, $m = n$ if and only if $m++ = n++$. That is, $++$ is an injection.

(v) If P is a unary predicate such that: $P(0)$ is true, and for every natural number n, $P(n)$ being true implies that $P(n++)$ is true, then P(n) is true for every natural number n.

1.2.2 Integers

We already have the definition of natural numbers $\mathbb{N}$, now we define integers $\mathbb{Z}$. Define $(a, b) \in \mathbb{N} \times \mathbb{N}$ to be integers with the equivalence relation $(a, b) \sim (c, d)$ if $a + d = b + c$.

1.2.3 Rational Numbers

Define (p, q) from $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}^* \to Q$. The equivalence relation $(p, q) \sim (r, s)$ if $ps = qr$.

1.2.4 Real Numbers

We Define Real Number from Cauchy sequences (We need metrics). Which is naturally closed under limitation.

1.2.5 Complex Numbers

We add i into $\mathbb{R}$, which is actually from Cartesian product (a, b).Define some operating rules and get complex number. $(a, b) \sim a + bi$.

We have the chain: $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$.

Chapter 2

Set theory REPEEK

2.1 Cardinality and Orders

The study of infinity is a natural requirement in the progress and completion of mathematical theory. The research work on set theory began at the end of the nineteenth century, and was first carried out by Cantor. This brand-new theory gradually formed and developed through hardships. So far, it has become one of the most important cornerstones of the mathematics edifice.

If there is a 1-1 map between set A, B, we say that A and B have the same **cardinality**.

Definition 2.1.1 (**Cardinality**)**.** All sets (equivalence class) that have the same cardinality with A is called the cardinality of A, denoted as $\bar{\bar{A}}$.

The cardinality of natural numbers is denoted as d of $\aleph_0$, and the cardinality of $(0, 1]$ is called **continuum**, denoted as c. The cardinality of a set is generally represented by lower case letters. If A have the same cardinality a with a subset B' of B in b, we have $a \leq b$.

Theorem 2.1.1 (Bernstein)**.** *If $a \leq b$, $b \leq a$, then $a = b$.*

If $a \leq b$ and $a \neq b$, the notation is $a < b$.

Theorem 2.1.2 (Cantor)**.** *The cardinality of power set of A is always larger than of A, specifically $\overline{\overline{A}} < \overline{\overline{P(A)}}$.*

Definition 2.1.2 (Operation of cardinality)**.** Define the addition, multiplication and power by $\overline{\overline{A}} + \overline{\overline{B}} \coloneqq \overline{\overline{A \sqcup B}}$. $\overline{\overline{A}} \cdot \overline{\overline{B}} \coloneqq \overline{\overline{A \times B}}$. $\overline{\overline{A}}^{\overline{\overline{B}}} \coloneqq \overline{\overline{A^B}}$.

Then there are commutativity, associativity and distribution law of addition and multiplication. The law of exponential has the same form as that of real numbers.

In addition, we give the cardinality of some common sets:

Example. *Examples of continuum:*
***Any interval**:* $\overline{\overline{(a,b)}} = c$, $(b > a)$.
***Real (complex) numbers**:* $\overline{\overline{\mathbb{R}}} = \overline{\overline{\mathbb{C}}} = c$.
***Rational numbers**:* $\overline{\overline{\mathbb{Q}}} = d$.
***Operations**:* $\overline{\overline{\mathbb{N} \times \mathbb{N}}} = d$. $\overline{\overline{2^{\mathbb{N}}}} = c$.

2.1.1 Ordered set and ordinal

Definition 2.1.3 (Partially ordered set)**.** Orders are special binary relations. Suppose that P is a set and that $\leq$ is a relation on P. Such that it is

1. Reflexive: $\forall x \in S$, $x \leq x$.
2. Transitive: $x \leq y$, $y \leq z$, 则 $x \leq z$.
3. Antisymmetric: $x \leq y$, $y \leq x$, 则 $x = y$.

Then P is a **partially ordered set**.

Suppose P and P' are patially ordered sets, if there is a bijection f from P to P', such that

$$x \leq y \quad \text{if and only if} \quad f(x) \leq f(y)$$

then P is **similar** to P', denoted as $S \sim S'$, f is called an order preserving mapping. Similarity relation is an equivalence relation. If any two elements have a partial order relation $\leq$, then the partial order become a totally ordered set.

Definition 2.1.4 (Order type)**.** Each (totally) ordered set corresponds to a uniquely determined notation, and make the two ordered set similar if and only if their order type are the same. Essentially, it is the equivalence class for similar relations. The order type of the (totally) ordered set M is denoted as $\overline{M}$. Generally, Greek letters are used to represent the order type, such as $\overline{\mathbb{N}} = \omega$.

Definition 2.1.5 (Addition of order type)**.** $\overline{A} = \sigma$, $\overline{B} = \tau$, define the order on $A \sqcup B$ by:

1. If $x, y \in A$, then $x \leq y$ is in A,
2. If $x, y \in B$, then $x \leq y$ is in B,
3. If $x \in A$, $y \in B$, then $x \leq y$.

Definition 2.1.6 (Multiplication of order type)**.** $\overline{A} = \sigma$, $\overline{B} = \tau$, (x_1, y_1), $(x_2, y_2) \in A \times B$, define the order on $A \times B$ by:

1. If $x_1 < x_2$, then $(x_1, y_1) < (x_2, y_2)$,

2. If $x_1 = x_2$, $y_1 < y_2$, then $(x_1, y_1) < (x_2, y_2)$,
3. If $x_1 = x_2$, $y_1 = y_2$, then $(x_1, y_1) = (x_2, y_2)$.

The addition and multiplication of order types satisfy the associative law respectively, and the addition and multiplication satisfy only the first distribution law: $\sigma(\tau + \rho) = \sigma\tau + \sigma\rho$.

Cardinality of order types: If the order type $\sigma = \overline{M}$, then the cardinality of M, $\overline{\overline{M}}$ is the cardinality of σ.

Ordered set of cardinality: Let a be a cardinality, all ordered sets with cardinality a are called the ordered set of a. Denoted as $T(a)$.

Definition 2.1.7 (Well-ordered set)**.** If any nonempty subset of an ordered set, as a sub-ordered set, always has a minimal element, then the ordered set is called a well ordered set.

Theorem 2.1.3 (**The Fundamental Theorem of Well-Ordered Sets**)**.** *For any two dissimilar well ordered sets, one must have a proper initial segment similar to the other.*

Definition 2.1.8 (**Order number**)**.** Order types of well ordered sets are called order numbers.

Theorem 2.1.4. *Set of arbitrary order numbers is naturally a well-ordered set. All ordered numbers smaller that a given order number σ forms a well-ordered set, whose order number is exactly σ.*

Limit number and non-limit number: when σ has no predecessor, that is no τ such that $\sigma = \tau + 1$, we call σ a limit number, or non-limit number.

2.2 Paradoxes and Set games

Banach-Mazur game, Guess real number, Russell's paradox.

2.2.1 Banach-Mazur game

Dreamwastaken and Georgenotfound are playing a game about closed intervals on $\mathbb{R}$ to decide who to pay the bill: Dream choose a closed interval D_1 and George choose its sub close interval G_1, the only restriction is that the length of G_1 is less than half of D_1. The round n: Dream choose closed $D_n \subseteq G_{n-1}$, and George choose $G_n \subseteq D_n$, the only restriction is that the length of G_n is less than half of D_n. And they get a chain of closed intervals:

$$D_1 \supset G_1 \supset D_2 \supset G_2 \supset \cdots \supset D_n \supset G_n \supset \cdots$$

Dream and George found that $\bigcap_{n\geq 1} D_n = \bigcap_{n\geq 1} G_n = \{x\}$ is a real number. If x is rational then Dream win, or George win. The question is, who will pay the bill?

2.2.2 Guess real number

This subsection is in Chinese, see

2.3 Axiom of Choice, Zorn's Lemma and Well-Ordering Theorem

We have not introduced the three most basic axioms in set theory before, namely, the axiom of choice, the well-ordering theorem, and the Zorn's lemma. Generally, we define the axiom of choice as an axiom, and derive other axioms from it. In essence, the three are equivalent to each other, and can all be assumed to be axioms. We give the proposition of the three, and the proofs can be found in the last chapter. See 12.1

Axiom 2.3.1 (Axiom of choice)**.** For any set family, there is a selection function. That is, for any set family X, we have

$$\forall X \ [\emptyset \notin X \implies \exists f : X \to \cup X \quad \forall A \in X, \ f(A) \in A] .$$

Axiom 2.3.2 (Well-ordeing theorem)**.** For each set, there is a ordering on it which makes it into a well-ordered set.

Axiom 2.3.3 (Zorn's lemma)**.** In any nonempty poset, if any chain (totally ordered subset) has an upper bound, then there is a maximal element in the poset.

Chapter 3

Basic structures

3.1 Vector spaces

3.1.1 Definition and examples

Definition 3.1.1 (**Vector space**)**.** A vector space over a field F is a set V together with two binary operations that satisfy the eight axioms listed below.

- (Associativity) $\mathbf{u}+(\mathbf{v}+\mathbf{w})=(\mathbf{u}+\mathbf{v})+\mathbf{w}$.
- (Commutativity) $\mathbf{u}+\mathbf{v}=\mathbf{v}+\mathbf{u}$.
- (Identity element) There exists and element $\mathbf{0}\in V$ such that $\mathbf{v}+\mathbf{0}=\mathbf{v}$ for all $\mathbf{v}\in V$.
- (Inverse element) For every $\mathbf{v}\in V$, there exists and element $-\mathbf{v}\in V$, such that $\mathbf{v}+(-\mathbf{v})=\mathbf{0}$.
- (Compatibility) $a(b\mathbf{v})=(ab)\mathbf{v}$.
- (Identity of scalar mutiplication) $1\mathbf{v}=\mathbf{v}$.
- (Distributivity of vector addition) $a(\mathbf{u}+\mathbf{v})=a\mathbf{u}+a\mathbf{v}$.
- (Distributivity of field addition) $(a+b)\mathbf{v}=a\mathbf{v}+b\mathbf{v}$.

This is the first algebraic system throughout learning, and there are some conclusions that can't be taken for granted. We list and prove some of those propositions that we thought obvious below.

Proposition 3.1.1. In a vector space, the following conclusion holds:

(i) Zero element $\mathbf{0}$ is unique,

(ii) Every vector $\boldsymbol{\alpha}$ has a unique inverse,

(iii) For each vector $\boldsymbol{\alpha}$, we have $0\boldsymbol{\alpha}=\mathbf{0}$,

(iv) For each vector $\boldsymbol{\alpha}$, we have $(-1)\boldsymbol{\alpha}=-\boldsymbol{\alpha}$.

证明. We just sketch the proof:

(i) Suppose there is another $\mathbf{0}'$, then $\mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}'$.

(ii) Suppose there is one vector $\boldsymbol{\alpha}$ with inverses $\boldsymbol{\beta}, \boldsymbol{\beta}'$, then $\boldsymbol{\beta} = \boldsymbol{\beta}+(\boldsymbol{\alpha}+\boldsymbol{\beta}') = (\boldsymbol{\beta}+\boldsymbol{\alpha})+\boldsymbol{\beta}' = \boldsymbol{\beta}'$

(iii) $0\boldsymbol{\alpha} = (0+0)\boldsymbol{\alpha} = 0\boldsymbol{\alpha} + 0\boldsymbol{\alpha}$, then $0\boldsymbol{\alpha} = \mathbf{0}$.

(iv) $\mathbf{0} = (1+(-1))\boldsymbol{\alpha} = \boldsymbol{\alpha} + (-1)\boldsymbol{\alpha}$, therefore $(-1)\boldsymbol{\alpha} = -\boldsymbol{\alpha}$.

□

We list some examples of vector spaces, and the examination is left as exercise.

Example (n-dimensional Euclidean space.)**.** *n-dimensional Euclidean space $\mathbb{R}^n$ over field $\mathbb{R}$ is a vector space. n -dimensional space $\mathbb{R}^n$ can be viewed as a table with n entries.*

Example (Matrices of the same shape)**.** *$m \times n$ matrices over Ω is a vector space, addition and scalar multiplication are as usual.*

Example. *All continuous real functions over $[0, 1]$, denoted as $C[0, 1]$, is a vector space. Addition of functions is pointwise, scalar mutiplication on $\mathbb{R}$ is as usual mutiplication.*

Linear dependence and basis

We introduce the concepts of linear dependence and basis through the example of Euclidean spaces.

In an Euclidean space $\mathbb{R}^n$, we have vectors of the following form:

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \boldsymbol{e}_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots \quad , \boldsymbol{e}_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

which is often called the basis of the n-dimensional Euclidean space, for the form $k_1\boldsymbol{e}_1 + k_2\boldsymbol{e}_2 + \cdots + k_n\boldsymbol{e}_n$ can't be combined into $\mathbf{0}$, otherwise $k_1 = k_2 = \cdots = k_n = 0$. The vectors are then called **linear independent**.

For example, $\boldsymbol{x}_1 = (1, 2, 3)^T$, $\boldsymbol{x}_2 = (1, 1, 1)^T$, $\boldsymbol{x}_3 = (0, 2, 4)^T$. we have $\boldsymbol{x}_1 = \boldsymbol{x}_2 + \frac{1}{2}\boldsymbol{x}_3$. The vectors are then called **linear dependent**.

Definition 3.1.2 (Linear dependence)**.** For m vectors $\boldsymbol{x}_i$ in a vector space V, if there exist coefficients k_i that are not all zero, such that $k_1\boldsymbol{x}_1 + k_2\boldsymbol{x}_2 + \cdots + k_m\boldsymbol{x}_m = \mathbf{0}$, the m vectors are **linear dependent**, or **linear independent** if not.

All vectors of the "linear combination" form are called **spanned by $\boldsymbol{x}_i$**, all vectors spanned by $\boldsymbol{x}_i$ make a vector space, called the vector space spanned by $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_m$, denoted as $\text{span}[\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_m]$.

If a vector space can be spanned by a finite number of vectors, it is said that the vector space is **finite dimensional**, otherwise it is **infinite dimensional**. For a finite dimensional vector space, the minimum number of vectors that span it (prove that the number is well defined) is called the **dimension of the vector space**, denoted as $n = \dim V$. And those n vectors are called the basis of the vector space V.

The basis of a linear space are linear independent vectors, and the linear space spanned by linearly independent vectors of number $\dim V$ is exactly V.

3.1.2 Linear mapping

Definition 3.1.3. A linear mapping from vector spaces V to W over field Ω is a map f satisfying

(i) $f(\boldsymbol{\alpha} + \boldsymbol{\beta}) = f(\boldsymbol{\alpha}) + f(\boldsymbol{\beta})$,

(ii) $f(k\boldsymbol{\alpha}) = kf(\boldsymbol{\alpha})$.

where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in V$, $k \in \Omega$.

We skip the definition of subspaces, the reader who don't know yet can look up for thenselves.

Definition 3.1.4. Given a linear mapping f from V to W over field Ω, we define

$$\ker f = \{\boldsymbol{v} \in V \mid f(\boldsymbol{v}) = \mathbf{0} \in W\}.$$
$$\mathrm{Im} f = \{f(\boldsymbol{v}) \in W \mid \boldsymbol{v} \in V\}.$$

Please show that they are both subspaces of V, W respectively.

Proposition 3.1.2. Given a linear mapping f from V to W over field Ω, and given basis $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in V$ 和 $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m$. Then f gives a matrix representation

$$f(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)\, \boldsymbol{A}_{m\times n}.$$

which means $f(\boldsymbol{v}_i) = a_{1i}\boldsymbol{w}_1 + a_{2i}\boldsymbol{w}_2 + \cdots + a_{mi}\boldsymbol{w}_m$, $1 \le i \le n$.

We find that although we can give a characterization of a linear mapping corresponding to the basis, it seems that a linear mapping is an inner relationship between two vector spaces. If we change the basis, how would the matrix change?

Suppose another basis in V, $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$, satisfying

$$(\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n) = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)\, \boldsymbol{P}_{n\times n}.$$

where the invertible matrix $\boldsymbol{P}$ is called **transition matrix**, then

$$f(\boldsymbol{v}_1', \boldsymbol{v}_2', \ldots, \boldsymbol{v}_n') = f\left((\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)\boldsymbol{P}_{n\times n}\right) = f\left((\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n)\right)\boldsymbol{P}_{n\times n}$$
$$= (\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_m)\,\boldsymbol{A}_{m\times n}\boldsymbol{P}_{n\times n}.$$

Thinking: Why the matrix can be taken out of f? If the linear mapping is from V to V, and take the same basis for both side, how would the matrix behind change?

To help understanding linear mappings, we give more examples, where vector spaces are not necessarily finite dimensional.

Example. *$C^1[0,1]$ are the set of all continuous differentiable functions (the derivatives are continuous) over interval $[0,1]$, the **differential operator** d is a linear mapping from $C^1[0,1]$ to $C[0,1]$.*

$$d : g \in C^1[0,1] \to g' \in C[0,1].$$

with $\ker d = \{g \in C^1[0,1] \mid g \equiv \text{const}\}$.

To achieve the isomorphism theorems, we define the quotient space. Suppose W is a subspace of V, we define a equivalence relation on V by $u \sim v$ iff $u - v \in W$.

Definition 3.1.5. The space whose elements are the equivalence classes $[u]$ of V, with operations defined by (prove well-defined)

$$[u] + [v] = [u + v], \quad k[u] = [ku].$$

is called the quotient space of V by W, it is also a vector space.

3.2 Groups

Definition 3.2.1 (**Group**)**.** A group is a set G together with a binary operation on G, here denoted $\cdot$, such that the following three group axioms, are satisfied

- (**Associativity**) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (**Identity**) There exists an element $e \in G$, such that $e \cdot a = a \cdot e = a,\ \forall a \in G$. (Prove uniqueness).
- (**Inverse**) For each $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$. b is called the inverse of a, commonly denoted a^{-1}.

3.3 Rings

Definition 3.3.1 (**Ring**)**.** A ring is a set R equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following three sets of axioms, called the ring axioms

- R is an abelian group under addition.
- R is a monoid under muliplication.
- Multiplication is distributive with respect to addition, meaning that:
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$.
  $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$.

Domain: A ring with no zero divisors. That is, $a \cdot b = 0$ in R implies $a = 0$ or $b = 0$.

Integral domain: Commutative domain.

3.4 Fields

Definition 3.4.1 (**Field**)**.** A field is a set F which is a Integral domain, and every nonzero element in it has a multiplicative inverse.

Problem. *Prove that* $\mathbb{F}_p = \left\{\bar{k} \mid \bar{k} \text{ is the equivalence class mod } p, p \text{ prime}\right\}$ *is a field.*

3.5 Modules

Definition 3.5.1 (**Module**)**.**

Thinking. What is the definition of **number field** in our textbook? Are there really a concept called "number field"?

3.6 Polynomials I

3.6.1 $P(x)$: from definition

Definition of Polynomials : Undetermined variable. Monadic polynomial ring.

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Equivalence:

$$Q(x) = b_m x^m + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0.$$

Polynomials $P(x) = Q(x)$ means $m = n$ and $a_i = b_i$ for each i.

Operations: Addition, Subtraction, Multiplication.

Functions on them: deg, LT.

3.6.2 Division algorithm

$f(x)$, $g(x)$ $\in \Omega[x]$, and $g(x) \neq 0$, Ω is a field. We have

$$f(x) = q(x)g(x) + r(x).$$

with $deg(r(x)) < deg(g(x))$.

Chapter 4

Linear algebra done right

4.1 Matrices revisit

We will list some basic techniques in matrix theory.

4.2 Rank inequalities

We will list some rank inequalities of vector spaces and matrices. The notes are 11.7

$$\begin{pmatrix} \boldsymbol{I}_m & \boldsymbol{0} \\ -\boldsymbol{C}\boldsymbol{A}^{-1} & \boldsymbol{I}_n \end{pmatrix} \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{D}-\boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

$$\begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_m & -\boldsymbol{A}^{-1}\boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{C} & \boldsymbol{D}-\boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

$$\begin{pmatrix} \boldsymbol{I}_m & \boldsymbol{0} \\ -\boldsymbol{C}\boldsymbol{A}^{-1} & \boldsymbol{I}_n \end{pmatrix} \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_m & -\boldsymbol{A}^{-1}\boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{D}-\boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

Problem. *(1)* 若 $k \neq 0$, $\operatorname{rank}(k\boldsymbol{A}) = \operatorname{rank}(\boldsymbol{A})$;

(2) $\operatorname{rank}(\boldsymbol{A}\boldsymbol{B}) \leq \min\{\operatorname{rank}(\boldsymbol{A}), \operatorname{rank}(\boldsymbol{B})\}$;

(3) $\operatorname{rank}\begin{pmatrix} \boldsymbol{A} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{B} \end{pmatrix} = \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$.

(4) $\operatorname{rank}\begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{O} & \boldsymbol{B} \end{pmatrix} \geq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}\begin{pmatrix} \boldsymbol{A} & \boldsymbol{O} \\ \boldsymbol{D} & \boldsymbol{B} \end{pmatrix} \geq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$;

(5) $\operatorname{rank}\begin{pmatrix} \boldsymbol{A} \\ \boldsymbol{B} \end{pmatrix} \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}(\boldsymbol{A}\,\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$

(6) $\operatorname{rank}(\boldsymbol{A}+\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A})+\operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}(\boldsymbol{A}-\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A})+\operatorname{rank}(\boldsymbol{B})$

(7) $\operatorname{rank}(\boldsymbol{A}-\boldsymbol{B}) \geq |\operatorname{rank}(\boldsymbol{A})-\operatorname{rank}(\boldsymbol{B})|$

Problem (**Sylvester Inequality**)**.** *Let* $\boldsymbol{A}$ *be* $m \times n$*,* $\boldsymbol{B}$ *be* $n \times k$ *matrices, prove that*

$$\operatorname{rank}(\boldsymbol{AB}) \geq \operatorname{rank}(\boldsymbol{A})+\operatorname{rank}(\boldsymbol{B})-n.$$

Problem (**Frobenius Inequality**)**.** *Assume all mulitiplications holds, then*

$$\operatorname{rank}(\boldsymbol{ABC})+\operatorname{rank}(\boldsymbol{B}) \geq \operatorname{rank}(\boldsymbol{AB})+\operatorname{rank}(\boldsymbol{BC}).$$

Problem. *Prove that* $\operatorname{rank}(\boldsymbol{A})=\operatorname{rank}\left(\boldsymbol{A}^{T} \boldsymbol{A}\right)$

Problem. *Let* $\boldsymbol{A}$ *be an* $n \times m$ *matrix,* $\boldsymbol{B}$ *be an* $m \times n$ *matrix, for each nonzero* λ_0 *we have*

$$m-\operatorname{rank}(\lambda_0 \boldsymbol{I}_m-\boldsymbol{BA})=n-\operatorname{rank}(\lambda_0-\boldsymbol{AB}).$$

4.3 Dual spaces

This section is in connection with functional analysis, category theory, representation theory.

4.4 Eigen-theory

Just normal eigenvalues and eigenvectors.

4.5 Canonical forms of matrices

For classification.

4.6 λ-matrices

Another way for classification.

4.7 Quadratic form

We will add symplectic spaces and unitary spaces here.*

Chapter 5

Mutilinear algebra

5.1 Mutilinear algebra

To discuss multilinear functions, another view of matrices.

5.1.1 Basic concepts

5.1.2 Tensor product

5.1.3 Wedge product

Chapter 6

Topology Theory

6.1 Basics in topology

6.1.1 Topological spaces

Definition 6.1.1. A **topology** on a set X is a collection $\mathcal{T}$ of subsets of X having the following properties:
(1) $\emptyset$ and X are in $\mathcal{T}$.
(2) The union of the elements of any subcollection of $\mathcal{T}$ is in $\mathcal{T}$.
(3) The intersection of the elements of any finite subcollection of 7 is in $\mathcal{T}$.
A set X for which a topology $\mathcal{T}$ has been specified is called a topological space.

Properly speaking, a topological space is an ordered pair $(X, \mathcal{T})$ consisting of a set X and a topology $\mathcal{T}$ on X, but we often omit specific mention of $\mathcal{T}$ if no confusion would arise.

Example. *Let X be a three-element set, $X = \{a, b, c\}$. Find some topologies on X.*

Example. *If X is any set, the collection of all subsets of X is a topology on X, it is called the **discrete topology**. The collection consisting of X and $\emptyset$ only is also a topology on X; we shall call it the **indiscrete topology**, or the **trivial topology**.*

Definition 6.1.2. Suppose that $\mathcal{T}$ and $\mathcal{T}'$ are two topologies on a given set X. If $\mathcal{T}' \supset \mathcal{T}$, we say that $\mathcal{T}'$ is finer than $\mathcal{T}$; if $\mathcal{T}'$ properly contains $\mathcal{T}$, we say that $\mathcal{T}'$ is strictly finer than $\mathcal{T}$. We also say that $\mathcal{T}$ is coarser ihan $\mathcal{T}'$, or strictly coarser, in these two respective situations. We say $\mathcal{T}$ is comparable with $\mathcal{T}'$ if either $\mathcal{T}' \supset \mathcal{T}$ or $\mathcal{T} \supset \mathcal{T}'$.

Definition 6.1.3 (Basis)**.** If X is a set, a basis for a topology on X is a collection of subsets of X (called basis elements) such that

(1) For each $x \in X$, there is at least one basis element B containing x.
(2) If x belongs to the intersection of two basis elements B_1 and B_2, then there is a basis element B_3 containing x such that $B_3 \subset B_1 \cap B_2$.

If $\mathcal{B}$ satisfies these two conditions, then we define the topology $\mathcal{T}$ generated by $\mathcal{B}$ as follows: A subset U of X is said to be open in X (that is, to be an element of $\mathcal{T}$) if for each $x \in U$, there is a basis element $B \in \mathcal{B}$ such that $x \in B$ and $B \subset U$. Note that each basis element is itself an element of $\mathcal{T}$.

6.1.2 Closed Sets and Limit Points

Closed sets

Definition 6.1.4. A subset A of a topological space X is said to be closed if the set $X—A$ is open.

Hence we have the same properties dual to those listed the definition of topology (open sets).

Definition 6.1.5. Given a subset A of a topological space X, the **interior** of A is defined as the union of all open sets contained in A, and the **closure** of A is defined as the intersection of all closed sets containing A, denoted by $\text{Int}A$, $\bar{A}$ respectively.

Obviously $\text{Int}A$ is open while $\bar{A}$ is closed, furthermore,

$$\text{Int}A \subset A \subset \bar{A}.$$

Theorem 6.1.1. *Let A be a subset of the topological space X, then $x \in \bar{A}$ if and only if every open set U containing x intersects A.*

Mathematicians often use some special terminology here. They shorten the statement "U is an open set containing x" to the phrase

"U is a **neighborhood** of x."

Limit Points

Definition 6.1.6. If A is a subset of the topological space X and if x is a point of X, we say that x is a **limit point** (or "cluster point," or "point of accumulation") of A if every neighborhood of x intersects A in some point other than x itself.

Example. *Consider the real line $\mathbb{R}$ with usual metric topology (skip definition), $A = \left\{\frac{1}{n} \mid n \in N^*\right\}$. Then 0 is a limit point of A.*

Theorem 6.1.2. *Let A be a subset of the topological space X, let A' be the set of all limit points of A. Then*

$$\bar{A} = A \cup A'.$$

6.1.3 Continuous Maps

Definition 6.1.7. Let X and Y be topological spaces. A function $f : X \to Y$ is said to be continuous if for each open subset V of Y, the set $f^{-1}(V)$ is an open subset of X.

Theorem 6.1.3. *Let X and Y be topological spaces; let $f : X \to Y$. Then the following are equivalent:*

1. *f is continuous.*
2. *For every subset A of X, one has $f(\bar{A}) \subset f(\bar{A})$.*
3. *For every closed set B of Y, the set $f^{-1}(B)$ is closed in X.*
4. *For each $x \in X$ and each neighborhood V of $f(x)$, there is a neighborhood U of x such that $f(U) \subset V$.*

6.1.4 Special topologies

The Order Topology

Induced Topology (Subspace Topology)

Product Topology and Box Topology

Quotient Topology

6.1.5 Metric Spaces

6.2 Compactness

Semicompact, paracompact*, sequential compact, with metric spaces.

6.3 Connectedness

6.4 Countability and Separation Axioms

Chapter 7

Basics in Homological Algebra

7.1 Basics in homological algebra

7.1.1 Exact sequences

7.1.2 Chain complexes

Short to Long.

7.1.3 Diagram chasing

Snake's Lemma, Five lemma,

7.2 Special Modules

7.2.1 Projective Modules

7.2.2 Injective Modules

7.2.3 Flat Modules

Chapter 8

Category theory

8.1 Category theory

8.1.1 Categories, functors

Give some examples.

8.1.2 Natural transformations

Representable functors, equivalences of categories, Yoneda lemma.

8.2 Yoneda Lemma

8.2.1 Representable Functor

8.2.2 Universal property

8.3 Limits

Just give concrete examples here.

8.3.1 Limits in Sets

8.3.2 Special Cases

Kernel and cokernel

Product and coproduct

Pullback and pushout

Chapter 9

Galois Theory

9.1 Galois theory

9.1.1 Field extension

Chapter 10

Other Problems

10.1 Basic tricks

10.1.1 Wonderful Σ

$$\sum_i \sum_j a_{ij} = \sum_j \sum_i a_{ij}.$$

$$\sum_{j=1}^{n} \sum_{i=1}^{i} a_{ij} = \sum_{i=1}^{n} \sum_{j=i}^{n} a_{ij} = \sum_{1 \le i \le j \le n} a_{ij}.$$

$$\Big(\sum_{i=1}^{n} a_i\Big)^2 = \sum_{i=1}^{n} a_i^2 + 2 \sum_{i \le j} a_i a_j.$$

$$\sum_{i \le j} (a_i - a_j)^2 = (n-1) \sum_{i=1}^{n} a_i^2 - 2 \sum_{i \le j} a_i a_j.$$

$$\sum_{cyc} f(x,y,z) =$$

$$\sum_{sym} f(x,y,z) =$$

$$\sum_{i=1}^{n} a_i b_i = A_n b_n + \sum_{i=1}^{n-1} A_n (a_i - a_{i+1}). \quad \textbf{(Abel)}$$

$$x^3 + y^3 + z^3 = 3xyz, \text{ if } x + y + z = 0.$$

10.1.2 Newton identities (Polynomials)

10.2 Other Problems

10.2.1 Problems from other notes

Problem.

$$\begin{cases} x_1 + x_2 + \cdots + x_n = 0 \\ x_1^2 + x_2^2 + \cdots + x_n^2 = 0 \\ \cdots \\ x_1^n + x_2^n + \cdots + x_n^n = 0 \end{cases}$$

Prove that:

$$x_1 = x_2 = \cdots = x_n = 0.$$

Problem (Ziwen MENG, 22-fall note 4)**.** *Let* $\boldsymbol{A} = (a_{ij})$ *be a* $n \times n$ *matrix, where* $a_{ij} = \gcd(i, j)$*, prove that*

$$\det \boldsymbol{A} = \varphi(1)\varphi(2)\cdots\varphi(n).$$

where φ *is Euler function.*

Hints: $\boldsymbol{B} = (b_{ij})$, $\boldsymbol{C} = (c_{ij})$, *where*

$$b_{ij} = \begin{cases} 1 & , j \mid i \\ 0 & , j \nmid i \end{cases}, \quad c_{ij} = \varphi(i) b_{ij}.$$

10.2.2 Mason-Stothers theorem and Fermat's last theorem

10.2.3 Marden's theorem

Chapter 11

Previous Lecture Notes

11.1 Linear algebra - 3

1. **(基础题)** 证明下述结论（整除、最大公因式、最小公倍式）.

   a) 设 $f, g, h \in \Omega[x]$. 若 $f|h, g|h$, 且 f, g 互质, 则 $fg \mid h$.

   b) 设 f, g 都是首一多项式, 则 $[f, g] = \frac{fg}{(f,g)}$.（考虑两种证法，思考 $[f, g, h] = \frac{fgh}{(f,g,h)}$ 是否成立?）

   c) $(f^n, g^n) = (f, g)^n$. (思考为什么在某个域上的不可约因式分解可以决定最大公因式?)

2. **(基础题)** 证明 Ω 上非常数多项式, 在 Ω 上有有限个根, 且个数至多为多项式的次数.

3. **（选讲，考虑用两种方法）**证明

$$[[f, g], h] = [f, [g, h]], \quad [f, (g, h)] = ([f, g], [f, h]), \quad (f, [g, h]) = [(f, g), (f, h)].$$

4. 证明函数 $f(x) = \sin(x)$ 不能表示为实多项式.

5. 求 $x^5 + 7x^4 + 18x^3 + 22x^2 + 13x + 3$ 的所有不可约因式

6. 设 $f(x)$ 是一个整系数多项式, a, b, c 是三个互异的整数. 证明不可能有

$$f(a) = b, f(b) = c, f(c) = a.$$

7. 证明: $x^2 + x + 1 \mid (x^{3m} + x^{3n+1} + x^{3k+2})$，其中 $m, n, k \in \mathbb{N}$.

8. **(提高题)** 设 f 是 Ω 上的 n 次既约多项式, u 是 f 在 $\mathbb{C}$ 中的一个根, $\Omega[u] = \{h(u) \mid h(x) \in \Omega[x]\}$.

   证明：

   (a) $\Omega[u] = \{h(u) \mid h(x) \in \Omega[x], \deg h(x) \leq n - 1\}$;

   (b) $\Omega[u]$ 是数域.

11.2 Linear algebra - 4

1. (基础回顾) 叙述以下的概念或性质
   (a) 叙述数域 Ω 上既约多项式的定义，并给出其几个性质
   (b) 叙述代数学基本定理
   (c) 复数域、实数域、有理数域上的既约多项式可能有哪些形式?
   (d) 叙述本原多项式的概念，本原多项式的高斯引理
   (e) 整系数多项式在整数域与有理数域上既约性的关系，为什么?
   (f) 叙述整系数多项式的 Eisenstein 判别法

2. 判断以下多项式是否为给定域上的既约多项式，并给出理由
   (a) $f(x) = x^2 + i$, 在 $\mathbb{C}$ 上
   (b) $f(x) = x^2 + 1$, 在 $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ 上
   (c) $f(x) = x^3 + x - 4$, 在 $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ 上
   (d) $f(x) = x^4 + 4x^2 - 14x - 2$, 在 $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ 上
   (e) $f(x) = x^4 + 1$, 在 $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ 上

3. 设 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ 的 n 个根为 $x_1, \ldots, x_n$. 求:
   (a) $\sum_{i=1}^n x_i^{-1}$
   (b) $\sum_{i=1}^n x_i^2$
   (c) $\sum_{i=1}^n x_i^{-2}$

4. 证明对于一元复多项式 $f(x)$, 存在一对二元实多项式 $u(x,y), v(x,y)$ 使得

$$f(x + yi) = u(x,y) + iv(x,y).$$

   举例说明存在二元实多项式 $u(x,y), v(x,y)$ 使得 $u(x,y) + iv(x,y)$ 不是 $x + yi$ 的多项式.

5. 设 p 是素数. 证明 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ 是 $\mathbb{Q}$ 上的既约多项式

6. 设 $f \in \mathbb{R}[x]$ 且在 $\mathbb{R}$ 上恒有 $f(x) \geq 0$. 证明有 $g, h \in \mathbb{R}[x]$ 使得 $f = g^2 + h^2$.

7. 设 $a_1, a_2, \ldots, a_n$ 是互异的整数. 证明 $(x - a_1)(x - a_2)\ldots(x - a_n) - 1$ 是 $\mathbb{Q}$ 上的既约多项式.

11.3 Linear algebra - 5

基础回顾

1. 将下列对称多项式化为初等对称多项式的多项式：
   (i) $f(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$,
   (ii) $f(x_1, x_2, x_3, x_4) = x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_4^2 + x_2^2x_3^2 + x_2^2x_4^2 + x_3^2x_4^2$,
2. 设方程 $px^3 + qx^2 + rx + s = 0$ $(p \neq 0)$ 的三个根为 a, b, c, 试计算: $(a^2 + ab + b^2)(b^2 + bc + c^2)(c^2 + ca + a^2)$.
3. 设多项式 $x^3 + px^2 + qx + r$ 的三个根都是实数, 求证：$p^2 \geqslant 3q$.
4. 若 n 是奇数, 求证：$(x + y)(y + z)(x + z)$ 可整除 $(x + y + z)^n - x^n - y^n - z^n$.

强化训练

1. 设 $\mathbb{Q}(\sqrt[n]{2}) = \left\{a_0 + a_1\sqrt[n]{2} + a_2\sqrt[n]{4} + \cdots + a_{n-1}\sqrt[n]{2^{n-1}} \mid a_i \in \mathbb{Q},\ 0 \leq i \leq n-1\right\}$, 求证 $\mathbb{Q}(\sqrt[n]{2})$ 是一个数域. (Hints: 第 3 次讲义第 8 题)
2. 设 $f(x)$ 是有理数域上的多项式, 若 $a + b\sqrt{c}$ 是 $f(x)$ 的根, 其中 a, b, c 是有理数, $\sqrt{c}$ 是无理数. 求证: $a - b\sqrt{c}$ 也是 $f(x)$ 的根.

拓展话题 (选讲)

根与不可约多项式

1. 设 $p(x)$ 是数域 $\mathbb{F}$ 上的不可约多项式,$f(x)$ 是 $\mathbb{F}$ 上的多项式. 证明: 若 $p(x)$ 的某个根 α 也是 $f(x)$ 的根, 则 $p(x) \mid f(x)$. 特别地, $p(x)$ 的任一复根都是 $f(x)$ 的根.

   (由此理解为什么域的扩张不影响最大公因式, 以及为什么在某个特定域上的不可约分解能决定两多项式的最大公因式)

2. 设 u 是复数域中某个数, 若 u 适合某个非零有理系数多项式 $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, 则称 u 是一个**代数数**. 证明:

   (i) 对任一代数数 u, 存在唯一一个 u 适合的首一有理系数多项式 $g(x)$, 使得 $g(x)$ 是 u 适合的所有非零有理系数多项式中次数最小者. 这样的 $g(x)$ 称为 u 的极小多项式. (注: u 适合 $g(x)$ 指的是 u 为 $g(x)$ 的根).

   (ii) 设 $g(x)$ 是一个 u 适合的首一有理系数多项式, 则 $g(x)$ 是 u 的极小多项式的充要条件是 $g(x)$ 是有理数域上的不可约多项式.

插值与中国剩余定理

1. **(插值公式)** 设 $x_1, x_2, \ldots, x_n$ 是域 $\mathbb{F}$ 上互异的数, 设另有 $y_1, y_2, \ldots, y_n \in \mathbb{F}$. 求证：存在一个次数不超过 $n-1$ 的多项式 $f(x)$ 使得 $f(x_i) = y_i$, $i = 1, 2, \ldots, n$.

2. 设 $f(x)$ 是一个 n 次多项式, 若 $k = 0, 1, \cdots, n$ 时有 $f(k) = \frac{k}{k+1}$, 求 $f(n+1)$.

3. **(中国剩余定理)** 设 $\{f_i(x) \mid i = 1, \cdots, n\}$ 是两两互素的多项式, $a_1(x), \cdots, a_n(x)$ 是 n 个多项式. 求证: 存在多项式 $g(x)$, 适合 $g(x) = f_i(x)q_i(x) + a_i(x)$, $(i = 1, \cdots, n)$.

空间解析几何

在一个仿射坐标系中, 三张平面的方程为

$$\pi_1 : ax + y + z + 1 = 0,$$
$$\pi_2 : x + ay + z + 2 = 0,$$
$$\pi_3 : x + y - 2z + 3 = 0,$$

讨论 a 变化时, 三张平面的位置关系.

11.4 Linear algebra - 6

Problem. 请思考以下问题

(i) 请给出你知道的行列式值的定义.

(ii) 请给出行列式值的一些计算性质.

Problem. 计算行列式的值

(i) 计算行列式

$$|\boldsymbol{A}| = \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & C_2^1 & \dots & C_n^1 \\ 1 & C_3^2 & \dots & C_{n+1}^2 \\ \vdots & \vdots & & \vdots \\ 1 & C_n^{n-1} & \dots & C_{2n-2}^{n-1} \end{vmatrix}$$

(ii) 计算 n 阶行列式 $(a_i \neq 0)$:

$$|\boldsymbol{A}| = \begin{vmatrix} x_1 - a_1 & x_2 & x_3 & \dots & x_n \\ x_1 & x_2 - a_2 & x_3 & \dots & x_n \\ x_1 & x_2 & x_3 - a_3 & \dots & x_n \\ \vdots & \vdots & \vdots & & \vdots \\ x_1 & x_2 & x_3 & \dots & x_n - a_n \end{vmatrix}$$

Problem. 证明题

(i) 设 $|\boldsymbol{A}| = |a_{ij}|$ 是一个 n 阶行列式, A_{ij} 是它的第 (i, j) 元素的代数余子式, 求证:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} & x_1 \\ a_{21} & a_{22} & \dots & a_{2n} & x_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} & x_n \\ y_1 & y_2 & \dots & y_n & 1 \end{vmatrix} = |\boldsymbol{A}| - \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} x_i y_j$$

(ii) 设

$$f(x) = \begin{vmatrix} x - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & x - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \dots & x - a_{nn} \end{vmatrix}$$

其中 x 是未知数, a_{ij} 是常数. 证明: $f(x)$ 是一个最高次项系数为 1 的 n 次多项式, 且其 $n-1$ 次项的系数等于 $-(a_{11} + a_{22} + \cdots + a_{nn})$.

Problem. 三线型的计算

(i) 求下列 $n+1$ 阶行列式的值, 其中 $a_i \neq 0, 1 \leq i \leq n$:

$$|\boldsymbol{A}| = \begin{vmatrix} a_0 & b_1 & b_2 & \dots & b_n \\ c_1 & a_1 & 0 & \dots & 0 \\ c_2 & 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ c_n & 0 & 0 & \dots & a_n \end{vmatrix}$$

(ii) 计算 n 阶行列式 $(bc \neq 0)$:

$$D_n = \begin{vmatrix} a & b & & & & \\ c & a & b & & & \\ & c & a & b & & \\ & & \ddots & \ddots & \ddots & \\ & & & c & a & b \\ & & & & c & a \end{vmatrix}$$

Problem. * 上下分块型矩阵, 计算行列式的值

$$\begin{vmatrix} a_1 & x & \dots & x \\ y & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & x \\ y & \dots & y & a_n \end{vmatrix}$$

Problem. 其他类型题目:

1. 计算:

$$|\boldsymbol{A}| = \begin{vmatrix} x & y & z & w \\ y & x & w & z \\ z & w & x & y \\ w & z & y & x \end{vmatrix}$$

2. 计算下列行列式:

$$|\boldsymbol{A}| = \begin{vmatrix} 1+x_1 & 1+x_1^2 & \dots & 1+x_1^n \\ 1+x_2 & 1+x_2^2 & \dots & 1+x_2^n \\ \vdots & \vdots & & \vdots \\ 1+x_n & 1+x_n^2 & \dots & 1+x_n^n \end{vmatrix}$$

11.5 Linear algebra - 7

Problem. 请思考以下问题

(i) 写出矩阵乘法法则, 并证明矩阵的乘法结合律.

(ii) 利用矩阵乘法法则, 写出矩阵乘积 ABC 的各分量值, 其中 A 为 $m \times n$, B 为 $n \times k$, C 为 $k \times l$ 型矩阵, $m, n, k, l \in \mathbb{N}^*$.

(iii) 叙述矩阵迹 *(trace)* 的定义, 并给出它的一些性质.

(iv) 叙述矩阵的转置, 共轭, 共轭转置的定义; 对角矩阵, 纯量矩阵的定义.

(v) 叙述上 *(*下*)* 三角矩阵; *(*反/斜*)* 对称矩阵, *(*反/斜*)Hermite* 矩阵的定义.

(vi) 叙述正交矩阵, 酉矩阵; 正规矩阵; 幂零矩阵, 幂等矩阵, 对合矩阵的定义.

*(*按照分号以类记忆*)*

Problem. 计算矩阵的乘积幂

(i) 设

$$\boldsymbol{A}_n = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

求证:

$$\boldsymbol{A}^k = \begin{pmatrix} \boldsymbol{O} & \boldsymbol{I}_{n-k} \\ \boldsymbol{I}_k & \boldsymbol{O} \end{pmatrix} \quad (k = 1, 2, \dots, n)$$

(ii) 设

$$\boldsymbol{A}_n = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

试求它的 k 次幂.

Problem. 求证:

(i) 任一 n 阶矩阵均可表示为一个对称矩阵与一个反对称矩阵之和.

(ii) $\boldsymbol{A}$ 为 n 阶矩阵, 则 $\boldsymbol{A}^T\boldsymbol{A}$ 为对称矩阵.

(iii) $\boldsymbol{A}$ 为 n 阶复矩阵, 则 $\boldsymbol{A}^H\boldsymbol{A}$ 为 *Hermite* 矩阵.

(iv) $\boldsymbol{A}$ 为 n 阶复矩阵, $\boldsymbol{U}$ 为酉矩阵. 证明: $\boldsymbol{A}$ 是正规矩阵当且仅当 $\boldsymbol{U}^H\boldsymbol{A}\boldsymbol{U}$ 是正规矩阵.

Problem. 关于对角矩阵的交换性.

(I) 求证: 和所有 n 阶矩阵乘法可交换的矩阵必是纯量矩阵 $k\boldsymbol{I}_n$.

(II) 设

$$\boldsymbol{A}=\begin{pmatrix} a_1\boldsymbol{E}_1 & & & \boldsymbol{0} \\ & a_2\boldsymbol{E}_2 & & \\ & & \ddots & \\ \boldsymbol{0} & & & a_r\boldsymbol{E}_r \end{pmatrix}$$

为分块对角矩阵, 且当 $i\neq j$ 时, $a_i\neq a_j$, $\boldsymbol{E}_i$ 是 n_i 阶单位矩阵, 证明: 与 $\boldsymbol{A}$ 可交换的矩阵只能是如下形式的矩阵

$$\begin{pmatrix} \boldsymbol{A}_1 & & & \boldsymbol{0} \\ & \boldsymbol{A}_2 & & \\ & & \ddots & \\ \boldsymbol{0} & & & \boldsymbol{A}_r \end{pmatrix}$$

其中 A_i 为任意 n_i 阶矩阵.

Problem. 设 $\boldsymbol{A}$ 为 n 阶矩阵, $\boldsymbol{\alpha}$ 是 n 维列向量. 证明: $\boldsymbol{A}\boldsymbol{\alpha}=\boldsymbol{0}$ 当且仅当 $\boldsymbol{A}^H\boldsymbol{A}\boldsymbol{\alpha}=\boldsymbol{0}$.

Problem. 设 $\boldsymbol{\alpha}$ 是非零的 n 维列向量, $\boldsymbol{A}=\boldsymbol{I}-\frac{2}{\boldsymbol{\alpha}^T\boldsymbol{\alpha}}\boldsymbol{\alpha}\boldsymbol{\alpha}^T$, 证明 A 是正交矩阵.

(关于这个公式的形式从何而来, 我们不妨先考虑平面上向量. 设 $\boldsymbol{\alpha}$ 是平面上某一非零向量, 则其确定其所在直线; 此时对于任一其它非零向量 $\boldsymbol{\beta}$, 它关于 $\boldsymbol{\alpha}$ 所在直线的对称向量 $\boldsymbol{\beta}'$ 是什么样子?)

Problem. * 下列形状的矩阵称为循环矩阵:

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

求证: 同阶循环矩阵之积仍是循环矩阵.

(***Hints***: 考察问题 2. **注记**: 在学习矩阵运算与行列式的关系后, 我们可以求得一般循环矩阵的行列式的值, 感兴趣可以自行查阅.)

Supplementary - 7

矩阵分解法

Problem. 计算下列循环矩阵 $\boldsymbol{A}$ 的行列式的值:

$$\boldsymbol{A}=\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

Problem. 计算下列矩阵 $\boldsymbol{A}$ 的行列式的值:

$$\boldsymbol{A}=\begin{pmatrix} \cos\theta & \cos 2\theta & \cos 3\theta & \dots & \cos n\theta \\ \cos n\theta & \cos\theta & \cos 2\theta & \dots & \cos(n-1)\theta \\ \cos(n-1)\theta & \cos n\theta & \cos\theta & \dots & \cos(n-2)\theta \\ \vdots & \vdots & \vdots & & \vdots \\ \cos 2\theta & \cos 3\theta & \cos 4\theta & \dots & \cos\theta \end{pmatrix}$$

Problem. 设多项式

$$f_k(x)=c_{k,n-1}x^{n-1}+\cdots+c_{k,1}x+c_{k,0},\quad k=1,2,\dots,n.$$

考虑矩阵

$$\begin{pmatrix} f_1(a_1) & f_2(a_1) & \dots & f_n(a_1) \\ f_1(a_2) & f_2(a_2) & \dots & f_n(a_2) \\ \vdots & \vdots & & \vdots \\ f_1(a_n) & f_2(a_n) & \dots & f_n(a_n) \end{pmatrix}$$

试求其矩阵乘积分解, 以此我们可以获得特殊情况行列式一个求法.

Binet-Cauchy 公式

Problem. 设 $\boldsymbol{A},\boldsymbol{B}$ 都是 $m\times n$ 的实矩阵, 求证:

$$|\boldsymbol{A}\boldsymbol{A}^{\boldsymbol{T}}||\boldsymbol{B}\boldsymbol{B}^{\boldsymbol{T}}|\geq|\boldsymbol{A}\boldsymbol{B}^{\boldsymbol{T}}|^2$$

降阶公式

降阶公式来自于矩阵初等变换下的行列式求值, 可以得到不同行列式的一个恒等式, 首先考虑以下问题:

Problem. 若 $\boldsymbol{A}$ 是 m 阶可逆矩阵, $\boldsymbol{D}$ 是 n 阶矩阵, $\boldsymbol{B}$ 为 $m\times n$ 矩阵, $\boldsymbol{C}$ 为 $n\times m$ 矩阵, 则

$$\begin{vmatrix}\boldsymbol{A} & \boldsymbol{B}\\ \boldsymbol{C} & \boldsymbol{D}\end{vmatrix}=|\boldsymbol{A}||\boldsymbol{D}-\boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B}|$$

若仅有 $\boldsymbol{D}$ 可逆, 则有

$$\begin{vmatrix}\boldsymbol{A} & \boldsymbol{B}\\ \boldsymbol{C} & \boldsymbol{D}\end{vmatrix}=|\boldsymbol{D}||\boldsymbol{A}-\boldsymbol{B}\boldsymbol{D}^{-1}\boldsymbol{C}|$$

则当 $\boldsymbol{A},\boldsymbol{D}$ 都可逆时, 我们有等式:

$$|\boldsymbol{A}||\boldsymbol{D}-\boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B}|=|\boldsymbol{D}||\boldsymbol{A}-\boldsymbol{B}\boldsymbol{D}^{-1}\boldsymbol{C}|$$

接下来见几道例题

Problem. 求下列矩阵 $\boldsymbol{A}$ 的行列式的值:

$$\boldsymbol{A}=\begin{pmatrix}0 & 2 & 3 & \dots & n\\ 1 & 0 & 3 & \dots & n\\ 1 & 2 & 0 & \dots & n\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & 2 & 3 & \dots & 0\end{pmatrix}$$

Problem. 计算下列矩阵的行列式的值, 其中 $a_i\neq 0\,(1\leq i\leq n)$

$$\boldsymbol{A}=\begin{pmatrix}0 & a_1+a_2 & \dots & a_1+a_n\\ a_2+a_1 & 0 & \dots & a_2+a_n\\ \vdots & \vdots & & \vdots\\ a_n+a_1 & a_n+a_2 & \dots & 0\end{pmatrix}$$

迹及其应用

首先列举迹的基本性质, 设 $\boldsymbol{A},\boldsymbol{B}$ 是 n 阶矩阵, 则有

(1) $\mathrm{tr}(\boldsymbol{A}+\boldsymbol{B})=\mathrm{tr}\boldsymbol{A}+\mathrm{tr}\boldsymbol{B}$

(2) $\mathrm{tr}(k\boldsymbol{A})=k(\mathrm{tr}\boldsymbol{A})$

(3) $\mathrm{tr}(\boldsymbol{A}^T)=(\mathrm{tr}\boldsymbol{A})$

(4) $\mathrm{tr}(\boldsymbol{A}\boldsymbol{B})=(\mathrm{tr}\boldsymbol{B}\boldsymbol{A})$

迹与特殊矩阵

Problem. 证明下列结论:

(1) 若 $\boldsymbol{A}$ 是 n 阶实矩阵, 则 $\mathrm{tr}(\boldsymbol{AA^T}) \geq 0$, 等号成立的充要条件是 $\boldsymbol{A} = \boldsymbol{O}$;
(2) 若 $\boldsymbol{A}$ 是 n 阶复矩阵, 则 $\mathrm{tr}(\boldsymbol{AA^H}) \geq 0$, 等号成立的充要条件是 $\boldsymbol{A} = \boldsymbol{O}$.

Problem. 设 $\boldsymbol{A}$ 为 n 阶实矩阵, 满足 $\boldsymbol{AA^T} = \boldsymbol{A}^2$, 求证: $\boldsymbol{A}$ 是对称矩阵. *(*提示: 利用上题结论*)*

Problem. 证明: 不可能存在 n 阶矩阵 $\boldsymbol{A}, \boldsymbol{B}$, 使得 $\boldsymbol{AB} - \boldsymbol{BA} = k\boldsymbol{I}_n$, 其中 $k \in \mathbb{F}$ 非零.

Problem. 设 $\boldsymbol{A}$ 为 $m \times n$ 矩阵, $\boldsymbol{B}$ 为 $n \times m$ 矩阵, 试考虑 $\mathrm{tr}(\boldsymbol{AB})$ 与 $\mathrm{tr}\boldsymbol{BA}$ 的关系.

Problem. 若 n 阶实矩阵满足 $\boldsymbol{AA^T} = \boldsymbol{I}_n$, 则称为正交矩阵. 证明: 不存在 n 阶正交矩阵 $\boldsymbol{A}, \boldsymbol{B}$, 满足 $\boldsymbol{A}^2 = c\boldsymbol{AB} + \boldsymbol{B}^2$, 其中 c 是非零常数.

迹的刻画

Problem. 设 f 是数域 $\mathbb{F}$ 上 n 阶矩阵集合到 $\mathbb{F}$ 的一个映射, 它满足下列条件:
(1) 对任意 n 阶矩阵 $\boldsymbol{A}, \boldsymbol{B}$, $f(\boldsymbol{A} + \boldsymbol{B}) = f(\boldsymbol{A}) + f(\boldsymbol{B})$;
(2) 对任意 n 阶矩阵 $\boldsymbol{A}$ 和 $k \in \mathbb{F}$, $f(k\boldsymbol{A}) = kf(\boldsymbol{A}))$;
(3) 对任意 n 阶矩阵 $\boldsymbol{A}, \boldsymbol{B}$, $f(\boldsymbol{AB}) = f(\boldsymbol{BA})$;
(4) $f(\boldsymbol{I}_n) = n$.
求证: f 就是迹, 即 $f(\boldsymbol{A}) = \mathrm{tr}(\boldsymbol{A})$ 对一切 $\mathbb{F}$ 上的 n 阶矩阵 $\boldsymbol{A}$ 成立.

矩阵的逆

Problem. 设 $\boldsymbol{A}$ 是 n 阶可逆矩阵, $\boldsymbol{\alpha}, \boldsymbol{\beta}$ 是 n 维列向量, 且 $1 + \boldsymbol{\beta^T A^{-1} \alpha} =\neq 0$. 求证:

$$(\boldsymbol{A} + \boldsymbol{\alpha\beta^T})^{-1} = \boldsymbol{A}^{-1} - \frac{1}{1 + \boldsymbol{\beta^T A^{-1} \alpha}} \boldsymbol{A}^{-1} \boldsymbol{\alpha\beta}^T \boldsymbol{A}^{-1}.$$

注记: 上述公式称为 *Sherman-Morrison* 公式.

Problem. 设 $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ 均为 n 阶矩阵.
(1) 若 $\boldsymbol{A}^2 = \boldsymbol{A}$, $\boldsymbol{B}^2 = \boldsymbol{B}$, $\boldsymbol{A} + \boldsymbol{B}^2 = \boldsymbol{A} + \boldsymbol{B}$, 证明: $\boldsymbol{AB} = \boldsymbol{BA} = \boldsymbol{O}$.
(2) 若存在正整数 k, 使得 $(\boldsymbol{AB})^k = \boldsymbol{O}$, 证明: $\boldsymbol{I}_n - \boldsymbol{BA}$ 是可逆阵.
(3) 若 $\boldsymbol{A}, \boldsymbol{D}, \boldsymbol{D} - \boldsymbol{CA^{-1}B}$ 均为可逆阵, 证明: $\boldsymbol{A} - \boldsymbol{BD^{-1}C}$ 也是可逆阵, 并求其逆矩阵.

摄动法

Problem. 设 $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ 是 n 阶矩阵且 $\boldsymbol{AC} = \boldsymbol{CA}$, 求证:

$$\begin{vmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{vmatrix} = |\boldsymbol{AD} - \boldsymbol{CB}|.$$

Problem. 设 $\boldsymbol{A}, \boldsymbol{B}$ 为 n 阶矩阵, 证明有

$$|\boldsymbol{I}_n + \boldsymbol{AB}| = |\boldsymbol{I}_n + \boldsymbol{BA}|.$$

11.6 Linear algebra - 8

Problem. 设 $\boldsymbol{A},\boldsymbol{B}$ 为 n 阶实矩阵, 证明前两个式子:

$$\begin{vmatrix}\boldsymbol{A} & \boldsymbol{B}\\ \boldsymbol{B} & \boldsymbol{A}\end{vmatrix}=|\boldsymbol{A}+\boldsymbol{B}||\boldsymbol{B}+\boldsymbol{A}|;\quad \begin{vmatrix}\boldsymbol{A} & -\boldsymbol{B}\\ \boldsymbol{B} & \boldsymbol{A}\end{vmatrix}=|\det(\boldsymbol{A}+i\boldsymbol{B})|^2;\quad \begin{vmatrix}\boldsymbol{A} & \boldsymbol{B}\\ \boldsymbol{C} & \boldsymbol{D}\end{vmatrix}$$

注记: 可以按书中的思路, 也可以联想分块矩阵乘法, 矩阵的行列式与乘积的关系. 思考: 若 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ 均为 n 阶矩阵, 其中 A 为可逆矩阵, 化简如上第三个行列式:

Problem. 分析矩阵的可逆性质:

(1) 设 n 阶矩阵 $\boldsymbol{A}$ 满足等式 $\boldsymbol{A}^2-3\boldsymbol{A}+2\boldsymbol{I}_n=\boldsymbol{O}$, 求证: $\boldsymbol{A}$ 和 $\boldsymbol{A}+\boldsymbol{I}_n$ 都是可逆矩阵, 而若 $\boldsymbol{A}\neq\boldsymbol{I}_n$ 则 $\boldsymbol{A}-2\boldsymbol{I}_n$ 必不是可逆矩阵

(2) 若 $\boldsymbol{A}^2=\boldsymbol{B}^2=\boldsymbol{I}$ 且 $|\boldsymbol{A}|+|\boldsymbol{B}|=0$, 求证: $\boldsymbol{A}+\boldsymbol{B}$ 必是奇异矩阵 (即不可逆矩阵).

(3) 若 $\boldsymbol{A},\boldsymbol{B}$ 是 n 阶矩阵, $\boldsymbol{I}_n+\boldsymbol{AB}$ 可逆, 求证: $\boldsymbol{I}_n+\boldsymbol{BA}$ 可逆.

Problem. 设 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{A}-\boldsymbol{B}$ 都是 n 阶矩阵, 证明:

$$\boldsymbol{B}^{-1}-\boldsymbol{A}^{-1}=\left(\boldsymbol{B}+\boldsymbol{B}\left(\boldsymbol{A}-\boldsymbol{B}\right)^{-1}\boldsymbol{B}\right)^{-1}.$$

Problem. 设 $\boldsymbol{A},\boldsymbol{B}$ 为 n 阶矩阵, 求证: $(\boldsymbol{AB})^*=\boldsymbol{B}^*\boldsymbol{A}^*$.

Problem. 证明伴随矩阵的相关结论, 此处我们用 A^* 表示 A 的伴随矩阵.

(1) $(\boldsymbol{A}^T)^*=(\boldsymbol{A}^*)^T$.

(2) $(c\boldsymbol{A})^*=c^{n-1}\boldsymbol{A}^*$, $\boldsymbol{A}$ 为 n 阶矩阵, c 为常数.

(3) 若 $\boldsymbol{A}$ 可逆, 则 $\boldsymbol{A}^*$ 也可逆, 并且 $(\boldsymbol{A}^*)^{-1}=(\boldsymbol{A}^{-1})^*$.

(4) $|\boldsymbol{A}^*|=|\boldsymbol{A}|^{n-1}$, $\boldsymbol{A}$ 为 n 阶矩阵.

(5) $(\boldsymbol{A}^*)^*=|\boldsymbol{A}|^{n-2}\boldsymbol{A}$, 其中 $\boldsymbol{A}$ 为 $n\,(n>2)$ 阶矩阵.

注记: *(4), (5)* 可先考虑可逆矩阵的情形, 不可逆情形留作思考.

Problem. 使用 *Binet-Cauchy* 公式证明 *Lagrange* 恒等式:

$$\left(\sum_{i=1}^{n}a_i^2\right)\left(\sum_{i=1}^{n}b_i^2\right)-\left(\sum_{i=1}^{n}a_ib_i\right)^2=\sum_{1\le i<j\le n}\left(a_ib_j-a_jb_i\right)^2.$$

Problem. 设 $\boldsymbol{A}=(A_{ij})_{n\times n}$, 其中

$$a_{ij}=s_{i+j-2},\quad s_k=x_1^k+x_2^k+\cdots+x_n^k,$$

求 $|\boldsymbol{A}|$ 的值, 并思考第 7 次讨论班循环矩阵的行列式求值问题.

Problem. 计算下列 $n+1$ 阶矩阵的行列式的值:

$$\begin{pmatrix} (a_0+b_0)^n & (a_0+b_1)^n & \dots & (a_0+b_n)^n \\ (a_1+b_0)^n & (a_1+b_1)^n & \dots & (a_1+b_n)^n \\ \vdots & \vdots & & \vdots \\ (a_n+b_0)^n & (a_n+b_1)^n & \dots & (a_n+b_n)^n \end{pmatrix}$$

Supplementary - 8

等价关系构造映射

等价关系构造映射的思想来源于很多领域, 其本质是将等价关系的等价类" 浓缩" 为一点, 由此便可以生成新的结构. 为了诱导新的映射, 我们要求所考虑的映射在等价类上取相同的值. 粗浅地讲, 我们进行了如下过程.

Proposition 11.6.1. 设 f 为集合 S 到集合 T 的映射, $\sim$ 为 S 上的一个等价关系. 若 $x \sim y \in S$ 时有 $f(x) = f(y)$, 则存在一个诱导的映射 $\tilde{f} : \tilde{S} = S/\sim \to T$. 其中 $S/\sim$ 指的是 S 商去等价关系, 即将等价类看作一个元素. 我们还有商映射 $\pi : S \to \tilde{S}$, $\pi : x \to [x]$, 将每个元素映射至其等价类.

在某些特殊结构上, 我们可以得到很多丰富的结果, 我们列举如下几则, 感兴趣可自行查阅.

(1) $f : V \to W$ 为线性空间之间的线性映射, 等价关系取 $x \sim y$ 当且仅当 $x - y \in \ker f$. 由 $\ker f$ 子空间诱导.

(2) $\phi : G \to H$ 为群之间的同态, 等价关系取 $x \sim y$ 当且仅当 $x^{-1}y \in \ker\phi$. 由 $\ker\phi$ 正规子群诱导.

(3) $\phi : R \to S$ 为环之间的同态, 等价关系取 $x \sim y$ 当且仅当 $x - y \in \ker\phi$. 由 $\ker\phi$ 环的理想诱导.

(4) $f : X \to Y$ 为拓扑空间之间的连续映射, 等价关系取 $x \sim y$ 可自行构造, 则可诱导商空间与商拓扑.

(5) 任意两个 R 模 M, N, 其张量积 $M \otimes N$ 是在其笛卡尔积生成的模上取等价关系 $(rm, n) \sim (m, rn)$, 其中 $m \in M$, $n \in N$, $r \in R$.

Kronecker 积 (Tensor Product)

设 $\boldsymbol{A}=(a_{ij})$ 和 $\boldsymbol{B}=(b_{ij})$ 分别是 $m\times n$ 阶和 $k\times l$ 阶矩阵, 定义他们的 Kronecker 积为一个 $mk\times nl$ 阶矩阵:

$$\boldsymbol{A}\otimes\boldsymbol{B}=\begin{pmatrix} a_{11}\boldsymbol{B} & a_{12}\boldsymbol{B} & \dots & a_{1n}\boldsymbol{B} \\ a_{21}\boldsymbol{B} & a_{22}\boldsymbol{B} & \dots & a_{2n}\boldsymbol{B} \\ \vdots & \vdots & & \vdots \\ a_{m1}\boldsymbol{B} & a_{m1}\boldsymbol{B} & \dots & a_{mn}\boldsymbol{B} \end{pmatrix}$$

Problem. 证明矩阵的 *Kronecker* 积满足下列性质 *(*假设以下的矩阵加法和乘法都有意义*):*

(1) $(\boldsymbol{A}+\boldsymbol{B})\otimes\boldsymbol{C}=\boldsymbol{A}\otimes\boldsymbol{C}+\boldsymbol{B}\otimes\boldsymbol{C}$*;*

(2) $\boldsymbol{A}\otimes(\boldsymbol{B}+\boldsymbol{C})=\boldsymbol{A}\otimes\boldsymbol{B}+\boldsymbol{A}\otimes\boldsymbol{C}$*;*

(3) $(k\boldsymbol{A})\otimes\boldsymbol{B}=k(\boldsymbol{A}\otimes\boldsymbol{B})=\boldsymbol{A}\otimes(k\boldsymbol{B})$*;*

(4) $\boldsymbol{I}_m\otimes\boldsymbol{I}_n=\boldsymbol{I}_{mn}$*;*

(5) $(\boldsymbol{AB})\otimes(\boldsymbol{CD})=(\boldsymbol{A}\otimes\boldsymbol{C})(\boldsymbol{B}\otimes\boldsymbol{D})$*;*

(6) $(\boldsymbol{A}\otimes\boldsymbol{B})\otimes\boldsymbol{C}=\boldsymbol{A}\otimes(\boldsymbol{B}\otimes\boldsymbol{C})$*;*

(7) 若 $\boldsymbol{A},\boldsymbol{B}$ 都是可逆矩阵, 则 $\boldsymbol{A}\otimes\boldsymbol{B}$ 也是可逆矩阵, 并且

$$(\boldsymbol{A}\otimes\boldsymbol{B})^{-1}=\boldsymbol{A}^{-1}\otimes\boldsymbol{B}^{-1};$$

(8) 若 $\boldsymbol{A}$ 是 m 阶矩阵, $\boldsymbol{B}$ 是 n 阶矩阵, 则 $|\boldsymbol{A}\otimes\boldsymbol{B}|=|\boldsymbol{A}|^n|\boldsymbol{B}|^m$.

矩阵可逆性刻画

Problem. n 阶方阵 $\boldsymbol{A}$ 的行列式为零的**充分必要**条件是, 其某行 *(*列*)* 可以表示为其它行 *(*列*)* 的线性组合. *(*我们在行列式运算中曾了解充分性, 其实此命题是充分必要的*)*

Problem. 我们称一个矩阵是**行对角占优**的, 指对于方阵 $\boldsymbol{A}$ 的元素 a_{ij}, 有

$$|a_{ii}|\geq\sum_{j=1,j\neq i}^{n}|a_{ij}|\quad(i=1,\dots,n)$$

如果上述定义的不等式都严格成立, 则称为**行严格对角占优矩阵**.

证明*:* 如果 $\boldsymbol{A}$ 具有严格对角占优, 则 $\boldsymbol{A}$ 为非奇异矩阵*;* 如果此外 A 的主对角线元素均为正数, 则 $\boldsymbol{A}$ 的行列式大于零.

11.7 Linear algebra - 9

Problem. 请思考以下的知识点

(1) 矩阵的初等变换有哪些, 具有哪些性质.

(2) 给矩阵作行 *(*列*)* 初等变换如何用矩阵表示.

(3) 给出矩阵等价的定义, 及其充分必要条件.

(4) 给出矩阵秩数的定义, 并给出其它相同数值的刻画.

(5) 请给出矩阵打洞法 *Schur* 公式的证明.

Problem. 设 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ 均为 n 阶矩阵且 $\boldsymbol{A}$ 和 $\boldsymbol{C}$ 可换. 证明

$$\begin{vmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{vmatrix} = |\boldsymbol{AD}-\boldsymbol{CB}|.$$

Problem. 判断矩阵的奇异性 *(*即可逆性*)*.

(1) 求证: n 阶方阵 A 是奇异矩阵的充分必要条件是, 存在非零的同阶方阵 $\boldsymbol{B}$, 使得 $\boldsymbol{AB}=\boldsymbol{O}$.

(2) 求证: n 阶方阵 $\boldsymbol{A}$ 是奇异矩阵的充分必要条件是, 存在 n 维非零列向量 $\boldsymbol{x}$, 使得 $\boldsymbol{Ax}=\boldsymbol{0}$.

Problem. 使用矩阵初等变换的方法求矩阵 $\boldsymbol{A}$ 的逆矩阵:

$$\boldsymbol{A}=\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ n & 1 & 2 & \dots & n-2 & n-1 \\ n-1 & n & 1 & \dots & n-3 & n-2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$$

Problem. 求证: 任一 n 阶矩阵均可表示为形如 $\boldsymbol{I}_n+a_{ij}\boldsymbol{E}_{ij}$ 这样的矩阵之积, 其中 $\boldsymbol{E}_{ij}$ 是 n 阶基础矩阵, a_{ij} 为一实数.

Problem. 设 $\boldsymbol{A}$ 为 n 阶实反对称矩阵, 证明:

(1) 对任意 n 维列向量 $\boldsymbol{x}$, 有 $\boldsymbol{x}^T\boldsymbol{Ax}=0$. *(*这个条件也是充分的*)*.

(2) $\boldsymbol{I}_n-\boldsymbol{A}$ 是非奇异矩阵.

Problem. 证明以下矩阵秩的不等式 **(*各组可按情况拓展理解矩阵秩不等式*)*

(1) 证明: $\mathrm{rank}\boldsymbol{A}-\mathrm{rank}\boldsymbol{B}\le\mathrm{rank}(\boldsymbol{A}-\boldsymbol{B})\le\mathrm{rank}\boldsymbol{A}+\mathrm{rank}\boldsymbol{B}$.

(2) $\mathrm{rank}(\boldsymbol{A}\ \boldsymbol{B})\le\mathrm{rank}\boldsymbol{A}+\mathrm{rank}\boldsymbol{B}$.

Problem. 证明: n 阶矩阵 $\boldsymbol{A}$ 与其伴随矩阵 $\boldsymbol{A}^*$ 的秩数有如下关系:

$$\mathrm{rank}\boldsymbol{A}^*=\begin{cases} n, & \mathrm{rank}\boldsymbol{A}=n, \\ 1, & \mathrm{rank}\boldsymbol{A}=n-1, \\ 0, & \mathrm{rank}\boldsymbol{A}\le n-2. \end{cases}$$

在拥有矩阵初等变换, 等价标准型的知识后, 我们可以给出如下两个比较重要的命题.

Problem. n 阶方阵 $\boldsymbol{A}$ 的行列式为零的**充分必要**条件是, 其某行 *(*列*)* 可以表示为其它行 *(*列*)* 的线性组合. *(*我们在行列式运算中曾了解充分性, 其实此命题是充分必要的*)*

Problem. 我们称一个矩阵是**行对角占优**的, 指对于方阵 $\boldsymbol{A}$ 的元素 a_{ij}, 有

$$|a_{ii}| \geq \sum_{j=1, j\neq i}^{n} |a_{ij}| \quad (i = 1, \ldots, n)$$

如果上述定义的不等式都严格成立, 则称为**行严格对角占优矩阵**.

证明*:* 如果 $\boldsymbol{A}$ 具有严格对角占优, 则 $\boldsymbol{A}$ 为非奇异矩阵.

Supplementary - 9

秩不等式

回想我们如何描述一个空间代数本质上的大小, 我们曾使用维数, 秩数等词汇. 我们在线性空间中可以定义维数, 在矩阵中可以定义秩数, 那么这些概念互相有如何的联系?

Proposition 11.7.1. 矩阵 $\boldsymbol{A}$ 的秩 = 矩阵 $\boldsymbol{A}$ 列空间的秩 = 矩阵 $\boldsymbol{A}$ 行空间的秩.

在矩阵打洞和求秩时, Schur 定理也有举足轻重的左右, 因此我们将其列举至此.

Theorem 11.7.1 (Schur)**.** 关于分块矩阵的初等变换有

$$\begin{pmatrix} \boldsymbol{I}_m & \boldsymbol{0} \\ -\boldsymbol{C}\boldsymbol{A}^{-1} & \boldsymbol{I}_n \end{pmatrix} \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{D} - \boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

$$\begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_m & -\boldsymbol{A}^{-1}\boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{C} & \boldsymbol{D} - \boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

$$\begin{pmatrix} \boldsymbol{I}_m & \boldsymbol{0} \\ -\boldsymbol{C}\boldsymbol{A}^{-1} & \boldsymbol{I}_n \end{pmatrix} \begin{pmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_m & -\boldsymbol{A}^{-1}\boldsymbol{B} \\ \boldsymbol{0} & \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{D} - \boldsymbol{C}\boldsymbol{A}^{-1}\boldsymbol{B} \end{pmatrix}$$

Problem. 我们列举秩的一些等式与不等式, 为求简便, 我们以 $\mathrm{rank}\boldsymbol{A}$ 记矩阵的秩.

(1) 若 $k \neq 0$, $\mathrm{rank}\,(k\boldsymbol{A}) = \mathrm{rank}\,(\boldsymbol{A})$*;*

(2) $\mathrm{rank}\,(\boldsymbol{A}\boldsymbol{B}) \leq \min\{\mathrm{rank}\,(\boldsymbol{A}), \mathrm{rank}\,(\boldsymbol{B})\}$*;*

(3) $\mathrm{rank} \begin{pmatrix} \boldsymbol{A} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{B} \end{pmatrix} = \mathrm{rank}\,(\boldsymbol{A}) + \mathrm{rank}\,(\boldsymbol{B})$.

(4) $\operatorname{rank}\begin{pmatrix}\boldsymbol{A} & \boldsymbol{C}\\ \boldsymbol{O} & \boldsymbol{B}\end{pmatrix} \geq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}\begin{pmatrix}\boldsymbol{A} & \boldsymbol{O}\\ \boldsymbol{D} & \boldsymbol{B}\end{pmatrix} \geq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$;

(5) $\operatorname{rank}\begin{pmatrix}\boldsymbol{A}\\ \boldsymbol{B}\end{pmatrix} \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}(\boldsymbol{A}\,\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$

(6) $\operatorname{rank}(\boldsymbol{A}+\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$, $\operatorname{rank}(\boldsymbol{A}-\boldsymbol{B}) \leq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B})$

(7) $\operatorname{rank}(\boldsymbol{A}-\boldsymbol{B}) \geq |\operatorname{rank}(\boldsymbol{A}) - \operatorname{rank}(\boldsymbol{B})|$

Problem (对合矩阵)**.** 设 $\boldsymbol{A}$ 是 n 阶对合矩阵当且仅当 $\operatorname{rank}(\boldsymbol{I}+\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{I}-\boldsymbol{A}) = n$.

Problem (幂等矩阵)**.** 设 $\boldsymbol{A}$ 是 n 阶幂等矩阵当且仅当 $\operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{I}-\boldsymbol{A}) = n$.

Problem (**Sylvester 不等式**)**.** 设 $\boldsymbol{A}$ 为 $m \times n$, $\boldsymbol{B}$ 为 $n \times k$ 阶矩阵, 证明

$$\operatorname{rank}(\boldsymbol{AB}) \geq \operatorname{rank}(\boldsymbol{A}) + \operatorname{rank}(\boldsymbol{B}) - n.$$

Problem (**Frobenius 不等式**)**.** 假设矩阵形状可以满足下式一切乘法, 证明

$$\operatorname{rank}(\boldsymbol{ABC}) + \operatorname{rank}(\boldsymbol{B}) \geq \operatorname{rank}(\boldsymbol{AB}) + \operatorname{rank}(\boldsymbol{BC}).$$

Problem. 证明: $\operatorname{rank}(\boldsymbol{A}) = \operatorname{rank}\left(\boldsymbol{A}^T\boldsymbol{A}\right)$

Problem. 设 $\boldsymbol{A}$ 为 $n \times m$ 矩阵, $\boldsymbol{B}$ 为 $m \times n$ 矩阵, 则对任意的非零常数 λ_0 均有

$$m - \operatorname{rank}(\lambda_0\boldsymbol{I}_m - \boldsymbol{BA}) = n - \operatorname{rank}(\lambda_0 - \boldsymbol{AB}).$$

我们以 n 维欧氏空间内的向量举例, 介绍**截断**与**补长**的概念. 对于一个 n 维列向量, 其 k 截断 $(k < n)$ 定义为其前 k 项分量形成的 k 维列向量; 其 m 补长 $(m > n)$ 指的是某一个 m 维列向量, 使得此向量的 n 截断为原向量. 注意补长的选取不是唯一的.

Proposition 11.7.2. 我们概述线性关系与截断和补长的关系.

(1) 线性相关向量组的截断仍然线性相关.
(2) 线性相关向量组的补长可能线性无关.
(3) 线性无关向量组的截断可能线性相关.
(4) 线性无关向量组的补长仍然线性无关.

通过此种方法和秩的行 (列) 向量空间维数的定义方式, 我们可以更好地理解某些矩阵秩不等式的关系.

矩阵相抵等价

利用矩阵的相抵标准型, 我们可以清晰明了地构造出一些零化关系, 秩的刻画等非显然的内容.

Theorem 11.7.2 (相抵标准型)**.** 一个 $m \times n$ 矩阵 $\boldsymbol{A}$ 可以写成如下的形式, 其中 r 为矩阵的秩数, $\boldsymbol{P}, \boldsymbol{Q}$ 为可逆矩阵.

$$\boldsymbol{A} = \boldsymbol{P}_m \begin{pmatrix} \boldsymbol{I}_r & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{O} \end{pmatrix} \boldsymbol{Q}_n$$

Theorem 11.7.3. 数域 Ω 上 $m \times n$ 矩阵 $\boldsymbol{A}, \boldsymbol{B}$ 相抵当且仅当他们的秩相等.

Problem. 设 $\boldsymbol{A}$ 是数域 Ω 上的 $s \times n$ 矩阵, 证明: $\boldsymbol{A}$ 的秩为 r 当且仅当存在数域 Ω 上的 $s \times r$ 列满秩矩阵 $\boldsymbol{B}$ 与 $r \times n$ 行满秩矩阵 $\boldsymbol{C}$, 使得 $\boldsymbol{A} = \boldsymbol{BC}$.

Problem. 设 $\boldsymbol{A}$ 是数域 Ω 上的 $m \times n$ 矩阵, 其秩为 r. 试寻找秩为 $n - r$ 的 n 阶矩阵 $\boldsymbol{B}$ 使得 $\boldsymbol{AB} = \boldsymbol{O}$. 思考: $n - r$ 的秩能更大吗?

此处摘有趣画作一则, 以弥补讲义前文贫瘠的内容.

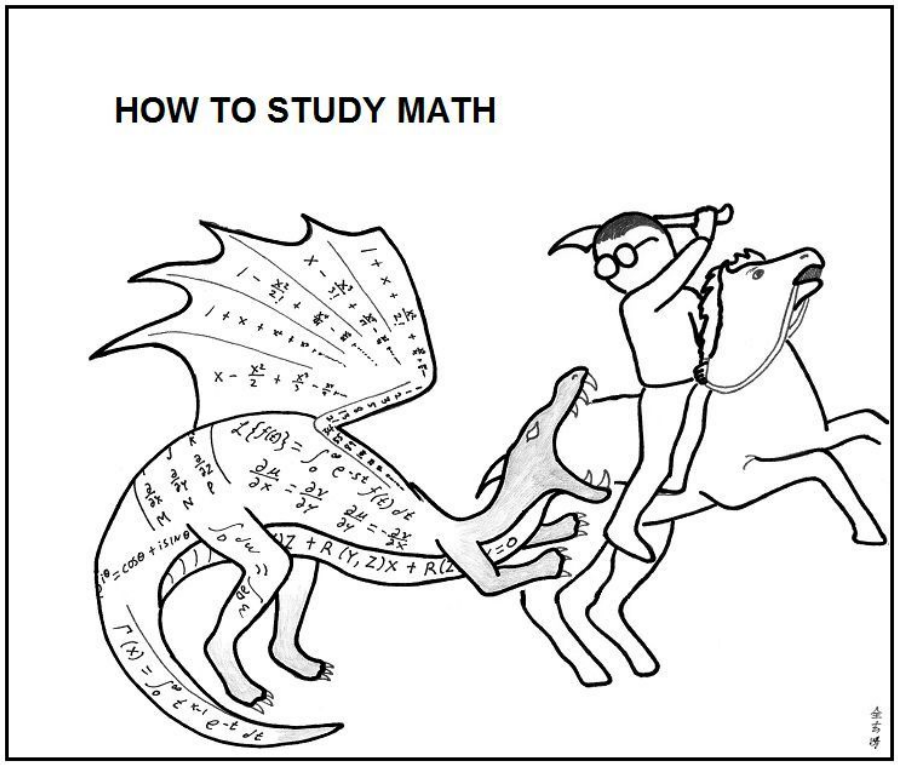

图 11.1: 不要光读, 动笔练习!

11.8 Linear algebra - 10

Problem. 回答等价关系的相关问题

(1) 叙述等价关系的定义,

(2) 证明: $\bmod a, a \in \mathbb{Z}^+$ 的同余是等价关系,

(3) 两个 n 阶矩阵称为**相似** *(***合同***)*, 如果有可逆矩阵 $\boldsymbol{P}$ 使得 $\boldsymbol{B} = \boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P}$ *(*$\boldsymbol{B} = \boldsymbol{P}^{T}\boldsymbol{A}\boldsymbol{P}$*)*. 证明: 相似和合同都是 n 阶矩阵集合上的等价关系,

(4) 给定数对 $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^+$, 给定关系 $(a,b) \sim (c,d)$ 当且仅当 $ad = bc$, 证明这是一个等价关系.

Problem. 求可逆矩阵 $\boldsymbol{P}, \boldsymbol{Q}$ 使得下列矩阵 $\boldsymbol{A}$ 满足 $\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q}$ 是 $\boldsymbol{A}$ 的等价标准型.

$$\begin{pmatrix} 1 & -1 & -1 & 0 \\ 2 & -2 & -1 & 2 \\ 3 & -3 & -1 & 4 \\ 1 & -1 & 1 & 1 \end{pmatrix}$$

Definition 11.8.1. 在进入秩数的问题前, 我们先规定所使用的术语.

A. 设 $\boldsymbol{G}$ 是 $m \times r\,(r < m)$ 矩阵, 则若矩阵 $\boldsymbol{G}$ 的矩阵秩等于 r, 称其为**列满秩矩阵**;

B. 一个 $m \times n$ 矩阵 $\boldsymbol{A}$ 称为**左 (右) 可逆矩阵**, 若存在 $n \times m$ 矩阵 $\boldsymbol{B}$ 使得 $\boldsymbol{B}\boldsymbol{A} = \boldsymbol{I}_n$ $(\boldsymbol{A}\boldsymbol{B} = \boldsymbol{I}_m)$; 此时 $\boldsymbol{B}$ 为 $\boldsymbol{A}$ 的一个**左 (右) 逆**;

C. 对于一个 $m \times n$ 矩阵 $\boldsymbol{A}$, 若存在 $k \times m$ 非零矩阵 $\boldsymbol{B}$ 使得 $\boldsymbol{B}\boldsymbol{A} = \boldsymbol{0}_{k\times n}$, 则称 $\boldsymbol{B}$ 为 $\boldsymbol{A}$ 的一个**左零化子**, 同理可以定义**右零化子**.

Problem. 证明课本的**定理** ***3.9.2***. 即设 $\boldsymbol{G}$ 是 $m \times r\,(r < m)$ 矩阵, 则下列陈述等价:

(1) $\boldsymbol{G}$ 为列满秩矩阵;

(2) $\boldsymbol{G}$ 有一个 r 阶非奇异子块;

(3) $\boldsymbol{G}$ 行等价于 $\begin{pmatrix} \boldsymbol{I}_r \\ \boldsymbol{0} \end{pmatrix}$

(4) 有矩阵 $\boldsymbol{H}$ 使得 $(\boldsymbol{G}\ \boldsymbol{H})$ 是可逆矩阵;

(5) 有矩阵 $\boldsymbol{K}$ 使得 $\boldsymbol{K}\boldsymbol{G} = \boldsymbol{I}_r$, 即 $\boldsymbol{G}$ 有左逆;

Problem. 设 $\boldsymbol{G}$ 是 $m \times n\,(n < m)$ 矩阵, 若矩阵的秩数 $r < n$, 证明 $\boldsymbol{G}$ 有右零化子; 若 $r = n$, 证明 $\boldsymbol{G}$ 没有右零化子.

Problem. 证明 $\boldsymbol{C}$ 为列满秩矩阵当且仅当 $\det \boldsymbol{C}^H\boldsymbol{C}$.

扩展话题

我们发现, 关于课本内列满秩矩阵的相关证明, 是纯矩阵观点下的. 似乎些结论并不方便瞥见列满秩矩阵的本质, 因此亦不便进行记忆. 为便学习理解, 我们在此提前引出相关内容.

尽管此种方法是更加直观的, 原始的矩阵方法也应熟稔于心. 在此节中, 我们不加以严格定义地引用课本接下来章节的概念, 有兴趣的同学可以自行查阅.

在我们定义列满秩矩阵时, $m \times n$ 矩阵 $\boldsymbol{A}$ 总是满足 $n \leq m$, 而列满秩恰为 $\mathrm{rank}\boldsymbol{A} = n$ 的情况. 实际上, 列满秩的本质定义为 "列空间满秩", 而此时列空间满秩恰好对于 $\mathrm{rank}\boldsymbol{A} = n$.

观察到, 一个 $m \times n$ 的矩阵可以看作 n 个 $m \times 1$ 的列向量, 亦可以看作 m 个 $1 \times n$ 的行向量. 正如我们在解析几何中所见, 一个向量可以生成线, 两个不共线向量生成平面, 三个不共面的向量生成三维空间. 我们一般所称的**列 (行) 空间**便指的是所对应**列 (行) 向量组**张成的空间.

在解析几何中我们会把向量做**线性组合**, 以得到所张成空间的所有向量. 矩阵的左乘和右乘分别对应行空间和列空间的向量组的组合. 注意到 $m \times n$ 的矩阵 $\boldsymbol{A}$ 右乘一个 $n \times 1$ 列向量恰好得到 $\boldsymbol{A}$ 的列向量组的某一个线性组合.

在三维欧氏空间里面取四个非零向量, 总有一个向量可以被其它三个向量线性组合表示出来, 这样的性质便称为**线性相关**. 若某向量组没有这样的性质, 则称为**线性无关**. 一个向量组最多选出 r 个线性无关的向量组, 则称向量组的**秩数**为 r, 称其张成空间的**维数**为 r. 秩数刻画了一个向量组本质上有多少个 "有用的" 向量.

Definition 11.8.2. 一个矩阵的列向量组的秩数, 或列向量组生成的列空间的维数, 称为矩阵的**列秩**. 同理地可以定义**行秩**.

我们有如下结论, 感兴趣的同学可尝试证明:

Theorem 11.8.1. *在任何情况下, 矩阵的秩 = 矩阵的行秩 = 矩阵的列秩.*

一般地, 一个 $m \times n$ 的矩阵的三个秩数必然会小于 $\min\{m, n\}$, 这也是我们在课本的列满秩定义中要求 $n \leq m$ 的原因. 在此我们给出列满秩的另一个定义. 上述定理确保了课本定义与下述定义的一致性.

Definition 11.8.3. 若 $m \times n (n \leq m)$ 矩阵 $\boldsymbol{A}$ 的列秩恰好为 n, 则称 $\boldsymbol{A}$ 为**列满秩矩阵**.

在此止步, 回望前述的定理结论等, 是否豁然开朗?

11.9 Analytic Geometry

Problem. 证明: 四点 A, B, C, D 共面的充分必要条件为: 存在不全为 0 的数 $\lambda, \mu, \nu, \omega$, 使得 $\lambda + \mu + \nu + \omega = 0$, 并且

$$\lambda\overrightarrow{OA} + \mu\overrightarrow{OB} + \nu\overrightarrow{OC} + \omega\overrightarrow{OD} = 0.$$

其中 O 是任意点.

Problem. 证明:

$$(\alpha \times \beta) \cdot (\gamma \times \delta) + (\alpha \times \delta) \cdot (\beta \times \gamma) + (\alpha \times \gamma) \cdot (\delta \times \beta) = 0$$

Problem. 在一个仿射坐标系中, 三张平面的方程为

$$\begin{aligned}
\pi_1 &: ax + y + z + 1 = 0, \\
\pi_2 &: x + ay + z + 2 = 0, \\
\pi_3 &: x + y - 2z + 3 = 0,
\end{aligned}$$

讨论 a 变化时, 三张平面的位置关系.

Problem. 在空间仿射坐标系中, 直线 l_1, l_2 分别有一般方程如下:

$$l_1 : \begin{cases} x + y - z + 1 = 0, \\ x - y + 2z = 0, \end{cases} \quad l_2 : \begin{cases} 3x - z + 1 = 0, \\ y + 2z - 2 = 0. \end{cases}$$

(i) 写出经过 l_1, 并且平行于 l_2 的平面的方程;
(ii) 求与 l_1, l_2 都共面, 并且平行于向量 $\boldsymbol{u}(1, 2, 1)$ 的直线的方程.

Problem. 在空间直角坐标系中, 求下列直线绕 z 轴旋转所得旋转曲面的方程.

$$\begin{cases} z = ax + b \\ z = cy + d \end{cases}$$

其中 a, c 都不为零.

Chapter 12

DONT KNOW, Proofs?

12.1 Proofs in the set theory

12.1.1 Axioms in the set theory

选择公理证明 Zorn 引理

设偏序集为 X, 假设 Zorn 引理不成立, 则存在一个选择函数 g, 对于任意一个全序子集 A, $g(A)$ 为其严格上界 $g(A) \in X \backslash A$. Zorn 引理不成立体现在" 严格" 上. 定义

$$A_{<a} = \{x \in A : x < a\}.$$

同时称一个子集 $A \subset X$ 为" 好集", 是指其满足以下条件:

- A 是全序集.
- A 中不含有严格下降的列.
- $\forall a \in A$, $g(A_{<a}) = a$.

观察到这样的" 好集" 是存在的, 如取 $\{g(\emptyset)\}$, 且如果 A 是" 好集", 则有 $A \cup g(A)$ 是" 好集".

下面我们证明, 若 A, B 是两个不同的" 好集", 则必有 $A = B_{<b}$ 或 $A_{<a} = B$. 首先定义

$$C = \{c \in A \cap B : A_{<c} = B_{<c}\}$$

易知 C 不是空集. 下面证明, 若 $C \neq A$, 则存在 a, 使得 $C = A_{<a}$. 由于 $C \subset A$, 取 $A \backslash C$ 中的最小元 a, 则 $A_{<a} \subset C$. 若有 $c \in C \backslash A_{<a}$, 则 $a < c$, $a \in A_{<c} \subset C$. 矛盾! 则必有 $C = A_{<a}$.

若此时 $C = A_{<a}$, $C = B_{<b}$, 则有

$$a = g(A_{<a}) = g(B_{<b}) = b.$$

则 $a = b \in C$, 矛盾, 命题成立.

设 E 是所有" 好集" 的并, 则若 $a \in E$, A 是含有 a 的" 好集", 有 $A_{<a} = E_{<a}$. 下面说明 E 是一个" 好集".

- E 是全序集: 由其构成集合的关系易知.
- E 中不含无穷减列: 任意取出来减列中元素 a_1, 则取包含 a_1 的" 好集" 讨论即可.
- $g(E_{<a}) = a$: $a = g(A_{<a}) = g(E_{<a})$.

这说明了 E 是最大的" 好集", 但 $E \cup \{g(E)\}$ 也是" 好集", 与最大性矛盾!

选择公理证明良序定理

选择集合 X 的幂集的子集族, 并选取一般的选择函数. 任意选择最小元, 并使用

$$g(\alpha) = f(X \backslash \cup_{\beta<\alpha} \{g(\beta)\}).$$

进行归纳, 配合最大良序集的反证法即可.

良序定理证明选择公理

设 X 为一集族, 将 $\cup X$ 良序化. 则对于任意集族中的元素 A, 定义选择函数 f 为

$$f(A) = \min \{x | x \in A\}$$

即可.

Zorn 引理证明良序定理

设集合为 X, 若其子集 W 上能够定义一个良序 $\leq$, 则将 $(W, \leq)$ 看作一个对. 定义偏序关系 $(W, \leq) \preceq (W', \leq')$, 指 $W \subset W'$ 且 $\leq'$ 在 W 上的限制为 $\leq$. 则易知其满足 Zorn 引理的条件, X 上必有一个极大的良序对 $(W_M, \leq_M)$.

若 $W_M \neq X$, 则取 $x_0 \in X \backslash W_M$, 定义新的良序子集:

$$W'_M = W_M \cup \{x_0\}, \quad x \leq'_M x_0, \forall x \in W_M.$$

则与 W_M 的极大性矛盾, 因此必有 $W_M = X$, 即良序定理成立!

Zorn 引理证明选择公理

思路同上, 在幂集 X 的子集上若有选择函数存在, 可以定义偏序关系:

$$(X_1, f_1) \preceq (X_2, f_2).$$

即 X_1 是 X_2 的子集族, 且选择函数 $f_2|_{X_1} = f_1$. 则类似地使用 Zorn 引理与反证法, 可以说明极大子集族恰为集族 X.

12.1.2 Guess real number game

假设有 100 个绝顶聪明的人要参加一个游戏, 这个游戏参与**过程中**所有人不能以任何形式交流.[1]

道具: 假设有 100 个完全一样的房间, 房间中按顺序有相同的可列无穷张正面朝下的纸条, 纸条下写了一个实数.

规则:100 个人同时进入这些房间 (一人一个房间), 进入房间后, 可以查看除了一张以外的所有纸条 (不要求在一开始就决定不看哪张, 可以先看一部分之后再做决定最后留下哪张不

同, 每个人选择留下的纸条可能不同). 这时候, 他需要猜测这张未翻开纸条上的数, 如果猜错了, 死亡.

问题: 这 100 个人是否可以提前商量一个策略, 使得至少有 99 个人可以存活?

这个问题初看是荒唐的, 但是借助选择公理我们可以得到问题的解答.

解答

假设按顺序所有的纸条构成了一个可列无穷长的向量

$$x = (x_1, x_2, \dots,) \in R^\omega.$$

在 R^ω 上构造等价关系 $\sim$: $x \sim y$ 当且仅当存在 x 与 y 仅有有限项不同. 此时在游戏前, 100 名玩家统一一套等价类表, 从每个等价类中选取特殊的 x (选择公理).

下面给出第 i 个人的策略. 考虑 $y^k = (x_k, x_{k+100}, \dots,)$ 为所有下标模 100 余 k 的元素构成的子列. 那么 i 保留 y^i 而查看剩下所有的位置.

考虑 y^t 对应的代表元为 x^t, 设 $N_t = \max_{j\in N}\left\{x_j^t \neq y_j^t\right\}$. 于是 N_t 是良定义的且 i 能观察到所有的 N_t, $t \neq i$.

设 $M_i = 1 + \max_{j\neq k}\{N_j\}$, 则 i 保留 y^i 的第 M_i 位, 查看其余所有数, 此时 i 已知道 y^i 的等价类 x^i, 并猜测 $y^i_{M_i} = x^i_{M_i}$.

可知 i 猜错仅当 $N_i \geq M_i = 1 + \max_{j\neq i} N_j$. 这个条件至多在一处满足. 因此这个策略可以保证至少 99 个人存活.

12.1.3 to be filled

12.2 a

参考文献

[1] 知乎网, 用户 Bellaris, 选择公理有哪些反直觉的应用? [EB/OL]. LINK

[2] Joseph J.Rotman. Advanced Modern Algebra[M]. Third Edition, Part 1, Volume 165. American Mathematical Society 2015: 341-343, 494-495.

[3] James R.Munkres. Topology [M], Second Edition, Prentice Hall 2000: 207-210, 230-235.

[4] Emily Riehl, Category Theory in Context [M], Dover Publications, 2016: 74-75.