Theory of Groups, Rings, and Fields

作者：李志煊

目录

第 4 章 Example of groups

4.1 Permutatations

定义 4.1

Let X be a set. A **permutation** of X is a bijection from X to itself. (in other words, a 'rearrangement' of the elements of X)

♣

笔记 The fact that the function π is a bijection means that in this two-row notation no integer occurs more than once in the second row (since π is injective) and each integer in the set $\{1, 2, \ldots, n\}$ occurs at least once in the second row (since π is surjective). Thus the second row is indeed a rearrangement, or permutation, of the first row.

定义 4.2

Let n be a positive integer. Denote by $S(n)$ the set of all permutations of the set $\{1, 2, \ldots, n\}$, equipped with the operation of composition (of functions). $S(n)$ is called the **symmetric group** on n symbols(or elements).

♣

定理 4.1

Let n be a positive integer. Then $S(n)$ satisfies the following conditions:
(Closure) if π, σ [a]are members of $S(n)$, then so is the composition $\pi\sigma$. Then is the composition of any two bijections is a bijection. (Identity) the identity function id = $id_{1,\ldots,n}$ is in $S(n)$. (Inverse) if π is in $S(n)$ then the inverse function π^{-1} is also in $S(n)$. Also $S(n)$ has $n!$ elements (Hint: permutations and combinations).

[a] π, σ are permutations

♡

笔记 In the two-row notation, the first function, σ , takes 1 to k (since $'k'$ occurs below $'1'$ in the notation for σ), and then the second function, π , takes k to m - therefore the composition takes 1 to m, and so $'m'$ is placed below $'1'$ in the notation for $\pi\sigma$. Hence the operation of composition is **non-commutative** in the sense that $\pi\sigma$ need not equal $\sigma\pi$. Therefore, it is important to remember that we are using the convention that $\pi\sigma$ is the function obtained by applying σ and then applying π.

Calculate the inverse of a permutation

The inverse is calculated by exchanging the upper and lower rows, and then reordering the columns so that the entries on the upper row occur in the natural order.

定义 4.3

A permutation $\pi \in S(n)$ is **cyclic** or a **cycle** if the elements $1, \ldots, n$ may be rearranged, as say $k_1, \ldots, k_r, k_{r+1}, \ldots, k_n$ (we allow the possibilities that $r+1 = 1$ or $r = n$), in such a way that π fixes each of $k_{r+1}, \ldots, k_n$ and 'cycles' the remainder, sending k_1 to k_2 sending k_2 to k_3, ..., sending k_{r-1} to k_r and finally sending k_r back to k_1. The integer r (that is, the number of elements in, or the length of, the cycling part) is called the **length** of π. (The algebraic significance of this integer will be explained later.) We say that the length of the identity permutation is 1. A cycle of length 2 is called a **transposition**. A cycle of length r is termed an r**-cycle**.

♣

笔记 The point of the cycle at which to start mat be chosen arbitrarily. Note that in the definition of cyclic permutation the case $r+1 = 1$ corresponds to the permutation which does not move anything - in other words to the identity permutation id (which is therefore a cycle: its cycle notation would be empty, so we continue to write it as id).

定义 4.4

Let π and σ be elements of $S(n)$. Then π and σ are **disjoint** if every integer in $\{1, \ldots, n\}$ which is moved by π is fixed by σ and every integer moved by σ is fixed by π (we say that π **moves** $k \in \{1, \ldots, n\}$ if $\pi(k) \neq k$, otherwise π **fixes** k).

♣

定理 4.2

If π and σ are disjoint permutations in $S(n)$, then π and σ commute, that is, $\pi\sigma = \sigma\pi$.

♡

证明 For any permutation ρ in $S(n)$, let $\mathrm{Mov}(\rho)$ be the set of integers in $\{1, 2, \ldots, n\}$ which are moved by ρ. More formally

$$\mathrm{Mov}(\rho) = \{m : 1 \leq m \leq n \quad \text{and} \quad \rho(m) \neq m\}.$$

To say that π and σ are disjoint is just to say that the intersection of $\mathrm{Mov}(\pi)$ with $\mathrm{Mov}(\sigma)$ is empty. We have the following possibilities for $m \in \{1, \ldots, n\}$:

- $m \in \mathrm{Mov}(\pi)$;
- $m \in \mathrm{Mov}(\sigma)$;
- m is in neither $\mathrm{Mov}(\pi)$ nor $\mathrm{Mov}(\sigma)$.

In the first case m is sent to $\pi(m)$ by both $\pi\sigma$ and $\sigma\pi$. For we have $\pi\sigma(m) = \pi(\sigma(m)) = \pi(m)$ (since m is moved by π it is fixed by σ): on the other hand we have $\sigma\pi(m) = \sigma(\pi(m)) = \pi(m)$. The last equality follows since $\pi(m)$ is moved by π (so is fixed by σ): for otherwise we would have $\pi(\pi(m)) = \pi(m)$ and so, since π is 1-1, $\pi(m) = m$, a contradiction. The other two cases are dealt with by similar arguments . Thus $\pi\sigma = \sigma\pi$, since they have the same effect on the elements of $\{1, \ldots, n\}$.

Any permutation may be written as a product of disjoint cycles.

定理 4.3

Let π be an element of $S(n)$. Then π can be expressed as a product of disjoint cycles. This **cycle decomposition** of π is unique up to rearrangement of the cycles involved. ♡

Multiply together two permutations

In order to multiply together two permutations which are written using cycle notation, one can write down their two-row notations, multiply, and then write down the cycle notation for the result. But this is a cumbersome process, and the multiplication is best done directly. The basic manipulation involved is what we will call a switch. Suppose we are given a product, π, of cycles and we want to compute its cycle decomposition. We visualise the effect of π on an integer i moving from right to left, encountering the various cycles, possibly being switched to a new value at each encounter. To switch i, seek the first occurrence of i to the left of its present position. This lies in a cycle of π, and i is now switched to the number, k say, to which this cycle takes i. Now think of k continuing to move to the left, and repeat this switching process until the left-hand end is reached. The number, m say, which finally emerges at the left-hand end is $\pi(i)$.

Multiplication table for $S(3)$

	id	(123)	(132)	(12)	(13)	(23)
id	id	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	id	(13)	(23)	(12)
(132)	(132)	id	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	id	(132)	(123)
(13)	(13)	(12)	(23)	(123)	id	(132)
(23)	(23)	(13)	(12)	(132)	(123)	id

The entry at the intersection of the row labelled σ and the column labelled τ is $\pi\tau$

Write an inverse of a cycle

One sumple reverses the order of the terms which appear (and then, if one wishes to, rewrites the resulting cycle with the smallest integer first). For example, $(1\,2\,3\,4)^{-1} = (4\,3\,2\,1) = (1\,4\,3\,2)$. If a permutation is written as a product of disjoint (hence commuting) cycles then the inverse is found by applying this process to each of its component cycles. If a permutation is written as a product of **not necessarily disjoint cycles** then the order of the components must also be reversed, because $(\pi\sigma)^{-1} = \sigma^{-1}\pi^{-1}$

若置换π 分解为不相交轮换： $\pi^{-1} = \prod \gamma_i^{-1}$ (顺序任意).

若分解为相交轮换： $\pi^{-1} = \prod \sigma_i^{-1}$ (严格反序).

4.2 The order and sign of a permutation

定义 4.5

Let π be a permutation. The positive **powers**, π^n, of π are defined inductively by setting $\pi^1 = \pi$ and $\pi^{k+1} = \pi \cdot \pi^k$ (k a positive integer). We also define the negative powers: $\pi^{-k} = (\pi^{-1})^k$ where k is a positive integer, and finally set $\pi^0 = \mathrm{id}$.

♣

定理 4.4

Let π be a permutation and let r, s be positive integers. Then

$$\pi^r \pi^s = \pi^{r+s}$$

$$(\pi^r)^s = \pi^{rs}$$

$$\pi^{-r} = (\pi^r)^{-1}$$

if π, σ are permutations such that $\pi\sigma = \sigma\pi$ then $(\pi\sigma)^r = \pi^r\sigma^r$

♡

证明 The fourth part also is proved by induction. We actually need a slightly stronger statement: that $(\pi\sigma)^k = \pi^k\sigma^k$ and $\sigma\pi^k = \pi^k\sigma$ (we use the second equation within the proof). By assumption the result is true for $k = 1$. So suppose inductively that $(\pi\sigma)^k = \pi^k\sigma^k$ and $\sigma\pi^k = \pi^k\sigma$. Then

$$\begin{aligned}(\pi\sigma)^{k+1} &= \pi\sigma(\pi\sigma)^k \quad \text{(by definition)}\\ &= \pi\sigma\pi^k\sigma^k \quad \text{(by induction)}\\ &= \pi\pi^k\sigma\sigma^k \quad \text{(also by induction)}\\ &= \pi^{k+1}\sigma^{k+1} \quad \text{(by definition)}\end{aligned}$$

Also

$$\begin{aligned}\sigma\pi^{k+1} &= \sigma\pi\pi^k = \pi\sigma\pi^k \quad \text{(by assumption)}\\ &= \pi\pi^k\sigma \quad \text{(by induction)}\\ &= \pi^{k+1}\sigma \quad \text{(by definition).}\end{aligned}$$

So we have proved both parts of the induction hypothesis for $k+1$ and the result therefore follows by induction.

定理 4.5

Let π be an element of $S(n)$. Then there is an integer m, greater than or equal to 1, such that $\pi^m = \mathrm{id}$.

♡

证明 Consider the successive powers of π: π; π^2; π^3; ... Each of these powers is a bijection from $\{1, \ldots, n\}$ to itself. Since there are only finitely many such functions there must be repetitions within the list: say $\pi^r = \pi^s$ with $r < s$. Since π^{-1} exists, we may multiply each side by π^{-r} to obtain $\mathrm{id} = \pi^{s-r}$. So m may be taken to be $s - r$.

定义 4.6

The **order** of a permutation π, $o(\pi)$, is the least positive integer n such that $\pi^n = \mathrm{id}$. Note that the order of id is 1 and id is the only permutation of order 1.

例题 4.1 The order of any transposition is 2

定理 4.6

Let π be a permutation of order n. Then $\pi^r = \pi^s$ if and only if $r \equiv s \mod n$.

证明 From the proof of 4.2.2 it follows that if $\pi^r = \pi^s$ then $\pi^{s-r} = \mathrm{id}$. If, conversely, $\pi^{s-r} = \mathrm{id}$ then, multiplying each side by π^r and using 4.2.1, we obtain $\pi^s = \pi^r$. We will therefore have proved the result if we show that $\pi^k = \mathrm{id} = (\pi^0)$ precisely if k is congruent to $0 modulo n$, that is, precisely if k is divisible by n. To see this, observe first that if k is a multiple of n, say $k = nt$, then, using 4.2.1(ii),

$$\pi^k = \pi^{nt} = (\pi^n)^t = (\mathrm{id})^t = \mathrm{id}.$$

Suppose conversely that $\pi^k = \mathrm{id}$. Apply the division algorithm (1.1.1) to write k in the form $nq + r$ with $0 \leq r < n$. Then, again using 4.2.1, we have

$$\mathrm{id} = \pi^k = \pi^{nq+r} = \pi^{nq}\pi^r = (\pi^n)^q\pi^r = (\mathrm{id})^q\pi^r = \mathrm{id} \cdot \pi^r = \pi^r.$$

The definition of n (as giving the least positive power of π equal to id) now forces r to be zero: that is, n divides k.

定理 4.7

Let π be a cycle in $S(n)$. Then $o(\pi)$ is equal to the length of the cycle π.

引理 4.1

If π, σ are disjoint permutations in $S(n)$ then the order of $\pi\sigma$ is the least common multiple, $lcm(o(\pi), o(\sigma))$, of the orders of π and σ.

例题 4.2 The permutation $\pi = (1\,6)(3\,7\,4\,2)$ is already expressed as the product of disjoint cycles, one of length 4 and the other of length 2. The order of π is therefore the lcm of 4 and 2: $o(\pi) = 4$.

定理 4.8

Let π be an element of $S(n)$, and suppose that $\pi = \tau_1\tau_2...\tau_k$ is a decomposition of π as a product of disjoint cycles. Then the order of π is the least common multiple of the lengths of the cycles $\tau_1, ..., \tau_k$

笔记 We say that permutations π and σ are **conjugate** if there exists some permutation τ such that $\sigma = \tau^{-1}\pi\tau$. Then it may be shown that two permutations have the same shape if and only if they are conjugate.

定义 4.7

Let $n \geq 2$ be an integer. Define the polynomial $\Delta = \Delta(x_1, \ldots, x_n)$ in the indeterminates $x_1, \ldots, x_n$ to be

$$\Delta(x_1, \ldots, x_n) = \prod\{(x_i - x_j) : i, j \in \{1, \ldots, n\}, i < j\}$$

the product of all terms of the form $(x_i - x_j)$ where $i < j$. For instance:

$$\Delta(x_1, x_2) = (x_1 - x_2);$$

$$\Delta(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3);$$

$$\Delta(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

笔记 Now let $n \geq 2$ and let $\pi \in S(n)$. We define a new polynomial, denoted $\pi\Delta$, from $\Delta = \Delta(x_1, \ldots, x_n)$ and π by the following rule: wherever Δ has a factor $x_i - x_j$, $\pi\Delta$ has the factor $x_{\pi(i)} - x_{\pi(j)}$. It is important to observe that $\pi\Delta$ is as Δ but with x_i replaced throughout by $x_{\pi(i)}$ for each i. More formally, we define $\pi\Delta$ by

$$\pi\Delta(x_1, \ldots, x_n) = \prod\{(x_{\pi(i)} - x_{\pi(j)}) : i, j \in \{1, \ldots, n\}, i < j\}$$

例题 4.3 Suppose that $n = 3$ and that π is the transposition $(2\,3)$. Then $\pi\Delta$ is obtained from Δ by replacing x_2 by x_3 and x_3 by x_2:

$$\pi\Delta(x_1, x_2, x_3) = (x_1 - x_3)(x_1 - x_2)(x_3 - x_2)$$

Now we note that this is just $-\Delta(x_1, x_2, x_3)$. To see this, just interchange the first two factors of $\pi\Delta$ and alse write $(x_3 - x_2)$ as $-(x_2 - x_3)$

引理 4.2

Let $\pi \in S(n)$ and let $\Delta(x_1, \ldots, x_n)$ be the polynomial as defined above. Then either $\pi\Delta = \Delta$ or $\pi\Delta = -\Delta$

证明 Consider a single factor $x_i - x_j$ of Δ. Since π is a bijection, there are unique values k and l in $\{1, \ldots, n\}$ such that $\pi(k) = i$ and $\pi(l) = j$; also $k \neq l$ since $i \neq j$. There are two possibilities:

- If $k < l$, then the factor $x_k - x_l$ occurs in Δ, and it is transformed in $\pi\Delta$ into $x_i - x_j$.
- If $k > l$, then the factor $x_l - x_k$ occurs in Δ, and it is transformed in $\pi\Delta$ into $x_j - x_i = -(x_i - x_j)$.

Thus, for every factor $x_i - x_j$ of Δ, either it or its negative occurs as a factor of $\pi\Delta$. Clearly (by the construction of $\pi\Delta$), Δ and $\pi\Delta$ have the same number of factors. It follows therefore (on collecting all the minus signs together) that $\pi\Delta$ is either Δ or $-\Delta$

这里通过定义 $sgn()$ 函数来定义偶置换和奇置换。

定义 4.8

Let $\pi \in S(n)$. Define the **sign** of π, sgn(π), to be 1 or -1 according as $\pi\Delta = \Delta$ or $-\Delta$. Thus $\pi\Delta = sgn(\pi) \cdot \Delta$. If sgn($\pi$) is 1 then π is said to be an **even** permutation: if sgn(π) $= -1$ then π is an **odd** permutation.

定理 4.9

Let $\pi, \sigma \in S(n)$. Then sgn($\sigma\pi$)= sgn(σ) $\cdot$ sgn(π)

证明 We compute, in two slightly different ways, the effect of applying the composite permutation $\sigma\pi$ to $\Delta = \Delta(x_1, \ldots, x_n)$. First we apply π to Δ, to get $\pi\Delta$: the effect is to replace, for each i, x_i by $x_{\pi(i)}$ through-

out. Without rearranging, we immediately apply the permutation σ: this results in each $x_{\pi(i)}$ being replaced throughout by $x_{\sigma(\pi(i))} = x_{\sigma\pi(i)}$. The net result is that for each i, x_i has been replaced throughout by $x_{\sigma\pi(i)}$. So the resulting polynomial is, by definition, $(\sigma\pi)\Delta$ and, by definition, $(\sigma\pi)\Delta = \mathrm{sgn}(\sigma\pi)\cdot\Delta$. Now we also have, by definition, that $\pi\Delta = \mathrm{sgn}(\pi)\cdot\Delta$. So, when we apply σ to $\pi\Delta$, we are just applying σ to $\mathrm{sgn}(\pi)\cdot\Delta$ (which is either Δ or $-\Delta$). The result of that is therefore equal to $\mathrm{sgn}(\pi)\cdot\sigma\Delta$, which equals $\mathrm{sgn}(\pi)\cdot\mathrm{sgn}(\sigma)\cdot\Delta$. So the net result of applying $\sigma\pi$ to Δ may be expressed in two ways, as $\mathrm{sgn}(\sigma\pi)\cdot\Delta$ and as $\mathrm{sgn}(\pi)\mathrm{sgn}(\sigma)\cdot\Delta$. Equating these expressions, we obtain that the polynomials $\mathrm{sgn}(\sigma\pi)\cdot\Delta$ and $\mathrm{sgn}(\pi)\cdot\mathrm{sgn}(\sigma)\cdot\Delta$ are identical. Hence it must be that $\mathrm{sgn}(\sigma\pi) = \mathrm{sgn}(\pi)\cdot\mathrm{sgn}(\sigma)$, as required.

实质：If $\pi,\sigma\in S(n)$, then $(\sigma\pi)p = \sigma(\pi p)$ for any polynomial p in n variables.

定理 4.10

Let π and σ be in $S(n)$. Then

1. $\mathrm{sgn}(\mathrm{id}) = 1$,
2. $\mathrm{sgn}(\pi) = \mathrm{sgn}(\pi^{-1})$,
3. $\mathrm{sgn}(\pi^{-1}\sigma\pi) = \mathrm{sgn}(\sigma)$,
4. if τ is a transposition then $\mathrm{sgn}(\tau) = -1$.

♡

证明 (i) This is immediate from the definition of sign.

(ii)

$$\mathrm{sgn}(\pi^{-1})\mathrm{sgn}(\pi) = \mathrm{sgn}(\pi^{-1}\pi) = \mathrm{sgn}(\mathrm{id}) = 1$$

So either both π^{-1} and π are even or both are odd, as required. (iii)

$$\begin{aligned}\mathrm{sgn}(\pi^{-1}\sigma\pi) &= \mathrm{sgn}(\pi^{-1})\mathrm{sgn}(\sigma\pi) = \mathrm{sgn}(\pi^{-1})\mathrm{sgn}(\sigma)\mathrm{sgn}(\pi)\\ &= \mathrm{sgn}(\pi^{-1})\mathrm{sgn}(\pi)\mathrm{sgn}(\sigma) = \mathrm{sgn}(\pi^{-1}\pi)\mathrm{sgn}(\sigma)\\ &= \mathrm{sgn}(\sigma)\end{aligned}$$

(iv) The proof proceeds by showing this for increasingly more general transpositions. First notice that the result is obviously true for $\tau = (1\ 2)$ since the only factor of Δ whose sign is changed by interchanging 1 and 2 is $x_1 - x_2$. Secondly, note that any transposition involving '1' is a conjugate of $(1\ 2)$:

$$(1\ k) = (2\ k)(1\ 2)(2\ k) = (2\ k)^{-1}(1\ 2)(2\ k).$$

So by (iii) $\mathrm{sgn}(1\ k) = \mathrm{sgn}(1\ 2) = -1$. Finally we notice that every transposition is conjugate to one involving '1':

$$(m\ k) = (1\ k)(1\ m)(1\ k) = (1\ k)^{-1}(1\ m)(1\ k).$$

So, by another application of (iii), we obtain $\mathrm{sgn}(m\ k) = -1$, as required.

注记：$\mathrm{sgn}(1\ 2) = -1$. $(1\ k)$ 的对换，构造 $(1\ k) = (2\ k)(1\ 2)(2\ k) = (2\ k)^{-1}(1\ 2)(2\ k)$，得 $\mathrm{sgn}(1\ k) = -1$.

对换的逆置换等于其本身.

例题 4.4 For any positive integer n, let $A(n)$ denote the set of all even permutations (permutatations with sign $+1$) in $S(n)$. Since $(1\ 2)$ is odd, multiplying an even permutation by $(1\ 2)$ gives an odd permutation, and

multiplying an odd permutation by $(1\ 2)$ gives an even permutation. The map f from the set of even permutations to the set of odd permutations defined by $f(\pi) = (1\ 2)\pi$ is a bijection, so it follows that half the elements of $S(n)$ are even and the other half are odd. Hence $A(n)$ has $\frac{n!}{2}$ elements. You can think of the map f more concretely by imagining the elements of $A(n)$ written out in a row; then, beneath each such element π, write its image $(1\ 2)\pi$. It is easy to show that the second row contains no repetitions and contains all odd permutations, so it is clear that $A(n)$ contains exactly half of the $n!$ elements of $S(n)$.

定理 4.11

Every cycle is a product of transpositions. If π is a cycle then $\text{sgn}(\pi) = (-1)^{\text{length}(\pi)-1}$.

♡

证明 To see that a cycle $(x_1\ x_2\ \dots\ x_k)$ can be written as a product of transpositions, we just check:

$$(x_1\ x_2\ \dots\ x_k) = (x_1\ x_k)\dots(x_1\ x_3)(x_1\ x_2). \quad \text{循环分解为对换的乘积 定理如下}$$

笔记 数学归纳法证明

$$(x_1\ x_2\ \dots\ x_{k+1}) = (x_1\ x_{k+1})(x_1\ x_2\ \dots\ x_k) = (x_1\ x_{k+1})(x_1\ x_k)\cdots(x_1\ x_3)(x_1\ x_2)$$

There are $k-1 = \text{length}(\pi) - 1$ terms on the right - hand side each with sign -1, by Theorem 4.2.9(iv). By Theorem 4.2.8 it follows that

$$\text{sgn}(\pi) = \text{sgn}((x_1\ x_k)\cdots(x_1\ x_3)(x_1\ x_2)) = (-1)^{\text{length}(\pi)-1}$$

定理 4.12

Suppose $n \geq 2$. Every permutation in $S(n)$ is a product of transpositions. Although there are many ways of writing a given permutation π as a product of transpositions, the number of terms occurring will always be either even or odd according as π is even or odd.

♡

证明 It is immediate from Theorems 4.1.3 and 4.2.10 that every permutation may be written as a product of transpositions. Suppose that we write π as a product of transpositions. Then, by the multiplicative property of sign (Theorem 4.2.8) and Theorem 4.2.9(iv), we have that $\text{sgn}(\pi)$ is -1 raised to the number of terms in the decomposition. Thus the statement follows.

4.3 Definition and examples of groups

定义 4.9

A **group** is a set G, together with an operation$*$, which satisfies the following properties:

Closure: $\forall g, h \in G, g * h \in G$. **Associativity**: $\forall g, h, k \in G$ then $(g * h) * k = g * (h * k)$.

Identity: There exists an identity element $e \in G$ such that $\forall g \in G, e * g = g * e = g$. **Inverse**: Every element $g \in G$ has an inverse $g^{-1} \in G$ s.t. $g * g^{-1} = g^{-1} * g = e$. ♣

笔记 请注意规定的operation.

4.3.1 Groups of numbers

例题 4.5 $(\mathbb{Z}, +)$ is an Abelian group: identity element is 0 since

$$0 + g = g + 0 = g, \forall g \in \mathbb{Z}$$

The inverse of $g \in \mathbb{Z} : g + (-g) = (-g) + g = 0$. The group is Abelian as $g + h = h + g, \forall g, h \in \mathbb{Z}$. Similarly, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are Abelian groups. Abelian group 是一种特殊的群，其运算满足交换律[1]. 有理数集、实数集和复数集在加法下也构成 Abelian group.

The set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ together with the operation $+$ is not a group since $-1 \notin \mathbb{N}$. (So 1 does not have an inverse in $\mathbb{N}$.)

The set of $\mathbb{Z}$ together with the operation $\times$ is not a group since 2 does not have an inverse in Z.

例题 4.6 The set $(\mathbb{Z}_n, +)$ is an Abelian group:

$$[a]_n + [b]_n = [a + b]_n \in \mathbb{Z}_n$$

$$([a]_n + [b]_n) + [c]_n = [a + b + c]_n = [a_n] + ([b]_n + [c]_n)$$

the identity element is $[0]_n$ since

$$[0]_n + [a]_n = [a]_n + [0]_n = [a]_n$$

the inverse of $[a]_n$ is $[-a]_n$ since

$$[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$$

the groups is Abelian because

$$[a]_n + [b]_n = [b]_n + [a]_n (= [a + b]_n)$$

However, $(\mathbb{Z}_n, \times)$ is not a group because $[0]_n$ does not have an inverse in $\mathbb{Z}_n$.

证明 If the inverse of $[0]_n$ exists, then there exists $[x]_n \in \mathbb{Z}_n$ such that $[0]_n * [x]_n = [1]_n$. That is $0 \cdot x \equiv 1 \mod n \Rightarrow 0 \equiv 1 \mod n$.

例题 4.7 $(G_n, \times)$ (or $(G_n, \cdot)$)is an Abelian groups: the identity element is $[1]_n$. By definition of G_n, every element of G_n has an inverse, we know $|G_n| = \phi(n)$. G_n 代表模 n 下的乘法群，$\phi(n)$ 是欧拉函数，表示小于 n 且与 n 互质的正整数的个数.

[1] Abelian group 的交换律是其定义的群运算满足交换性

笔记 Both Fermat Theorem & Euler Theorem are special cases of Lagrange Theorem: for any finite group $(G, \times)$ and any $g \in G$, we have $g^{|G|} = e$. $\leftarrow g * \ldots * g$ $|G|$ terms.

例题 4.8 $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$, $(\mathbb{C}, \times)$ are not groups because 0 does not have a multiplicative inverse. However, $(\mathbb{Q} \setminus \{0\}, \times)$, $\mathbb{R} \setminus \{0\}, \times)$ and $(\mathbb{C} \setminus \{0\}, \times)$ are Abelian groups: The identity element is 1. The inverse of $a \neq 0$ is $\frac{1}{a}$.

例题 4.9 We can define a group using a table: let $G = \{e, a, b, c\}$ with operation given by :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

e represents the identity element. The group is Abelian since $g * h = h * g, \forall g, h \in G$. One can check that this is an Abelian group with 4 elements. Also,it is called Klein four-group(克莱因四元群).

证明

Closure: 运算结果均为 G 中的元素.

Associativity: $(a \cdot b) \cdot c = c \cdot c = e = a \cdot (b \cdot c)$

Inverse: $a \cdot a = e \;\; b \cdot b = e \;\; c \cdot c = e$

Identity: $e \cdot a = a \cdot e = a \;\; e \cdot b = b \cdot e = b \;\; e \cdot c = c \cdot e = c$

Commutativity: $a \cdot b = c = b \cdot a \;\; a \cdot c = b = c \cdot a \;\; b \cdot c = a = c \cdot b$

例题 4.10 The set $T = \{e^{ir} : r \in \mathbb{R}\}$ under multiplication forms an Abelian group. The identity element is $e^{i0} = 1$ and the inverse of e^{ir} is e^{-ir}. The group is Abelian since $e^{ir}e^{is} = e^{i(r+s)} = e^{is}e^{ir}$.

4.3.2 Groups of permutations

例题 4.11 We proved that the set $S(n)$ together with the composition operation is a group. The indentity element is id. Every permutation $\pi \in S(n)$ has an inverse π^{-1} (i.e. $\pi\pi^{-1} = \pi^{-1}\pi = id$). It has the associativity property: $(\pi\sigma)\tau = \pi(\sigma\tau), \forall \pi, \sigma, \tau \in S(n)$. This groups has $n!$ elements. For $n \geq 3$, $S(n)$ is non-Abelian: $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$.

例题 4.12 For $n \geq 2$, let $A(n) = \{\pi \in S(n) : \text{sgn}(\pi) = 1\}$. This is a group with $\frac{n!}{2}$ elements.

Closure: $\forall \pi, \sigma \in A(n)$, we have $\text{sgn}(\pi\sigma) = \text{sgn}(\pi)\text{sgn}(\sigma) = 1$. So $\pi\sigma \in A(n)$.

Associativity: $S(n)$ satisfies this property, and $A(n) \subset S(n)$. Indentity: id is the identity element of $A(n)$.

Inverse: $\forall \pi \in A(n)$, we have $sgn(\pi^{-1}) = sgn(\pi) = 1$, so $\pi^{-1} \in A(n)$

The map $(1\ 2) : S(n) \to S(n)$, $\pi \to (1\ 2)\pi$ induces a bijection between $A(n)$ and $S(n) \setminus A(n)$. That is $|A(n)| = |S(n) \setminus A(n)|$. Hence $|A(n)| = \frac{1}{2}|S(n)| = \frac{n!}{2}$.

证明 pre: we know map $(1\ 2)$ is a bijection. If $\pi \in A(n)$, then π is even and $(1\ 2)\pi$ is odd. So $(1\ 2)\pi \in S(n) \setminus A(n)$. If $\pi \in S(n) \setminus A(n)$, then π is odd and $(1\ 2)\pi$ is even , because $sgn[(1\ 2)\pi] = sgn(1\ 2) \cdot sgn(\pi) = (-1) \cdot (-1) = 1$. So $(1\ 2)\pi \in A(n)$.

4.3.3 Groups of matrices

例题 4.13 $(Mat(n,\mathbb{R}),+)$ is an Abelian group. The identity matrix is the zero matrix. The inverse of $A \in Mat(n,\mathbb{R})$ is $-A$.

例题 4.14 $GL(n,\mathbb{R}) := \{A \in Mat(n,\mathbb{R}) : \text{A is invertible}\}$. The set $GL(n,\mathbb{R})$ under matrix multiplication is a (non-Abelian) group. The identity element is $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ The inverse of $A \in GL(n,\mathbb{R})$ is the inverse matrix A^{-1}.

例题 4.15 Let $G = \left\{ A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{R},\ a \neq 0,\ c \neq 0 \right\}$. Together with the operation of matrix multiplication, G forms a group. $G \subset GL(2,\mathbb{R})$. Closure:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \in G$$

Inverse:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} \in G$$

笔记 Suppose $(G,*)$ is a group, and G' is a subset of G. If $g*h \in G'$ for $\forall g,h \in G'$, and $g^{-1} \in G'$ for $\forall g \in G'$, then $(G',*)$ is a group. the inverse of g is in G'

例题 4.16 $G = \{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a,b \in \mathbb{R} \setminus \{0\} \}$. G is a group under matrix multiplication.

The identity element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The inverse of $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in G$ is $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \in G$.

例题 4.17 $(\mathbb{R}^n,+)$ is an Abelian group.

笔记 HW 4.3 1

(i): $\mathbb{Q}$ under multiplication is not a group because 0 does not have an inverse: $0x = 0 \neq 1\ \forall x \in \mathbb{Q}$. 1 is the multiplicative identity: $x1 = 1x = x\ \forall x \in \mathbb{Q}$

(vii): set of integers under substraction. This is not a group since $(3-2)-1 = 0 \neq 2 = 3-(2-1)$

HW 4.3.2: G is a group. Show that $(ab)^{-1} = b^{-1}a^{-1}\ \forall a,b \in G$.

证明 We have

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

So the inverse of (ab) is $b^{-1}a^{-1}$.

4.4 Algebraic structures

Rings: $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),\ldots$[2]

定义 4.10

A ring is a set $\mathbb{R}$ together with two operations $+$, $*$[a] is called a ring if it satisfies the following axioms:

1. $(\mathbb{R},+)$ is an Abelian group. $\Downarrow$
   - $x+y\in\mathbb{R}\ \forall x,y\in\mathbb{R}$
   - $(x+y)+z=x+(y+z)$
   - $x+0=0+x=x$
   - $x+(-x)=(-x)+x=0$
   - $x+y=y+x$ ← Abelian group 满足的
2. $\forall x,y\in\mathbb{R}$, we have $x*y\in\mathbb{R}$.
3. $\forall x,y,z\in\mathbb{R}$, we have $(x*y)*z=x*(y*z)$. ← *associativity*
4. $\forall x,y,z\in\mathbb{R}$, $(x+y)z=xz+yz$. ← *distributivity*
5. $\forall x,y,z\in\mathbb{R}$, $x(y+z)=xy+xz$. ← *distributivity*

[a] 对于加法构成 Abelian Group，对于乘法构成 semigroup

♣

笔记 We say that a ring $\mathbb{R}$ is commutative[3] if $x*y=y*x,\ \forall x,y\in\mathbb{R}$.

笔记 Convention: We usually write xy instead of $x*y$ if the multiplication operation $*$ is clear from the context.

例题 4.18 $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ are commutative rings.

The set $2\mathbb{Z}$ is also a commutative ring.

例题 4.19 The set $Mat(2,\mathbb{R})$ of 2×2 real matrices is a ring under addition of multiplication of matrices.

axioms(1): ✓

axioms(2): ✓

axioms(3): $(AB)C=A(BC)$ ✓

证明

$$\underbrace{\begin{pmatrix}a&b\\c&d\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}}_{B}=\begin{pmatrix}aa'+bc'&ab'+bd'\\ca'+dc'&cb'+dd'\end{pmatrix}\quad C=\begin{pmatrix}e&f\\g&h\end{pmatrix}$$

$$(AB)C=\begin{pmatrix}aa'+bc'&ab'+bd'\\ca'+dc'&cb'+dd'\end{pmatrix}\begin{pmatrix}e&f\\g&h\end{pmatrix}=\begin{pmatrix}(aa'+bc')e+(ab'+bd')g&(aa'+bc')f+(ab'+bd')h\\(ca'+dc')e+(cb'+dd')g&(ca'+dc')f+(cb'+dd')h\end{pmatrix}$$

$$BC=\begin{pmatrix}a'&b'\\c'&d'\end{pmatrix}\begin{pmatrix}e&f\\g&h\end{pmatrix}=\begin{pmatrix}a'e+b'g&a'f+b'h\\c'e+d'g&c'f+d'h\end{pmatrix}$$

[2] 环的公理体系仅围绕加法和乘法构建，不包含其他未经明确定义的运算

[3] 在环的定义中，若称环是 commutative，指的是乘法运算满足交换律. 加法在环的定义中已被明确要求是 commutative，因为 $(\mathbb{R},+)$ 是 Abelian group.

$$A(BC) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a'e + b'g & a'f + b'h \\ c'e + d'g & c'f + d'h \end{pmatrix} = \begin{pmatrix} aa'e + bc'e + ab'f + bd'g & aa'f + bc'f + ab'h + bd'h \\ ca'e + dc'e + cb'f + dd'g & ca'f + dc'f + cb'h + dd'h \end{pmatrix}$$

$$\Rightarrow (AB)C = A(BC)$$

笔记 $Mat(2, \mathbb{R})$ is **NOT** commutative. E.q.

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$$

More generally, $Mat(n, \mathbb{R})$ is a ring for every $n \geq 1$. Actually, for any commutative ring $\mathbb{R}$, $Mat(n, \mathbb{R})$ is a ring.

例题 4.20 $\mathbb{Z}$ is a ring.

例题 4.21 Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[\sqrt{2}]$ is a ring. $\mathbb{Z}[\sqrt{2}]$ is an Abelian group:

- $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
- $(a + b\sqrt{2}) + 0 = 0 + (a + b\sqrt{2})$.
- $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$
- $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})$
- $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

$\rightarrow \mathbb{Z}[\sqrt{2}]$ is a commutative ring. (Note that $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ satisfies all other axioms.)

笔记 Suppose $\mathbb{R}$ is a ring. Let $\mathbb{S}$ be a subset of $\mathbb{R}$ s.t.

- $x + y \in \mathbb{S}\ \forall x, y \in \mathbb{S}$
- $-x \in \mathbb{S}\ \forall x \in \mathbb{S}$
- $xy \in \mathbb{S}\ \forall x, y \in \mathbb{S}$

then $\mathbb{S}$ is a ring. If $\mathbb{R}$ is commutative, then so does $\mathbb{S}$.

Field 域

定义 4.11

A commutative ring $\mathbb{R}$ is called a **field** if $\mathbb{R}$ contains the unit element 1 such that $1x = x1 = x\ \forall x \in \mathbb{R}$, and every $x \in \mathbb{R} \setminus \{0^a\}$ has an inverse $x^{-1} \in \mathbb{R}$ s.t. $xx^{-1} = x^{-1}x = 1$.

[a] 加法的单位元. $0 + a = a$

♣

笔记 If $\mathbb{R}$ is a field, then $\mathbb{R} \setminus \{0\}$ is an Abelian group under multiplication.

例题 4.22 $\mathbb{Q}$ is a field. So are $\mathbb{R}, \mathbb{C}$.

例题 4.23 $\mathbb{Z}$ is a commutative ring, but it is **NOT** a field because 2 doesn't have a multiplicative inverse ($\frac{1}{2} \notin \mathbb{Z}$). $\mathbb{Z}[\sqrt{2}]$ is not a field since $\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} \notin \mathbb{Z}[\sqrt{2}]$.

However, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field ! ($\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}[\sqrt{2}]$)

定理 4.13

Let $\mathbb{R}$ be any ring. Then $\forall x \in \mathbb{R}$

$$x0 = 0x = 0$$

♡

证明 $x0 + 0x = x(0 + 0) = x0$

Adding $(-x)0$ to both sides, we get

$$x0 = 0$$

4.5 Supplementary to Fields Theory

笔记 $\mathbb{F}$ 是域，首先要满足环的定义，$\mathbb{F}$ 对乘法有单位元，对任意非零元[4]都有逆元且 $\mathbb{F}$ 可交换.

笔记 性质：域 $\mathbb{F}$ 中不含有零因子[5]

证明 Let $a \in \mathbb{R}$, $a \neq 0$. If $ab = 0 \to a^{-1}(ab) = 0 \to (a^{-1}a)b = 0 \to eb = b = 0$

特征：若环 $\mathbb{R}$ 中元素（对加法）有最大阶 n.

笔记 性质：

1. 域 $\mathbb{F}$ 的特征[6]一定是素数.

   证明 只需证明特征不是合数即可. $\mathbb{F}$ 中所有非零元对加法的阶均相同. 设 $Char\mathbb{F} = n$, 若 $n = n_1 n_2, 1 \leq n_i \leq n, i = 1, 2$ 在 $\mathbb{F}$ 中任取 $a \neq 0, n_1 a \neq 0, n_2 a \neq 0$ But

   $$(n_1 a)(n_2)a = n_1 n_2 a^2 = (na)a = 0$$

   矛盾。

2. $\mathbb{F}$ 中所有非零元对加法的阶均相同.

   证明 因为域不含有零因子。若 $\mathbb{F}$ 中某个元素 $a \neq 0$ 的阶为 n, 则任取 $b \in \mathbb{F}$, $b \neq 0$

   $$a(nb) = (na)b = 0b = 0$$

   矛盾。 $n \in \mathbb{F}$, $\underbrace{1 + \cdots + 1}_{n个1}$

[4]零元指在加法下的单位元

[5]零因子是指两个非零元素相乘结果为零的情况. 在域中，非零元素相乘不可能为零. 严格定义：$\forall a \neq 0$, $a \in \mathbb{R}$, 若存在 $b \in \mathbb{R}, b \neq 0$, s.t. $ab = 0$, 则称 a 为 $\mathbb{R}$ 中零因子

[6]$\forall a \in \mathbb{R}$, $\underbrace{a + \cdots + a}_{n_1个a} = 0$, $\mathrm{Char}\,\mathbb{R} = \max\{n_1, \cdots, n_k\}$

定义 4.12

(Vector space)[a] Let $\mathbb{F}$ be a field. A vector space over $\mathbb{F}$ is an Abelian group $(\mathbb{V}, +)$ together with scalar multiplication

$$\mathbb{F} \times \mathbb{V} \to \mathbb{V}$$

$$(\lambda, v) \mapsto \lambda v$$

satisfying the following:

1. $(\alpha + \beta)v = \alpha v + \beta v \ \ \forall \alpha, \beta \in \mathbb{F}, \forall v \in \mathbb{V}$
2. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2 \ \ \forall \alpha \in \mathbb{F}, \forall v_1, v_2 \in \mathbb{V}$
3. $1v = v \ \ \forall v \in \mathbb{V}$
4. $(\alpha\beta)v = \alpha(\beta v) \ \ \forall \alpha, \beta \in \mathbb{F}, v \in \mathbb{V}$

Elements of $\mathbb{V}$ are called vectors. Elements of $\mathbb{F}$ are called scalars.

[a]向量加法构成阿贝尔群，标量乘法满足线性运算公理（分配律、结合律）

笔记 Vector space 是定义在一个域 $\mathbb{F}$（如实数域 $\mathbb{R}$、复数域 $\mathbb{C}$）上的代数结构[7]，包含一个阿贝尔群和一个标量乘法运算。

需满足四条公理：

1. 标量加法分配到向量.
2. 标量分配到向量加法.
3. 标量乘法的单位元.
4. 标量乘法结合律.

例题 4.24

$$\mathbb{R}^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{R}\}$$

Scalar multiplication: $\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n) \ \forall \lambda \in \mathbb{R}$.

Addition: $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$.

Then the set $\mathbb{R}^n$ equipped with the above addition and scalar multiplication is a vector space over $\mathbb{R}$.

1. $(\alpha + \beta)(x_1, \ldots, x_n) = ((\alpha + \beta)x_1, \ldots, (\alpha + \beta)x_n) = \alpha(x_1, \ldots, x_n) + \beta(x_1, \ldots, x_n)$
2. $$\begin{aligned} \alpha((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) &= \alpha(x_1 + y_1, \ldots, x_n + y_n) \\ &= (\alpha(x_1 + y_1), \ldots, \alpha(x_n + y_n)) \\ &= (\alpha x_1 + \alpha y_1, \ldots, \alpha x_n + \alpha y_n) \\ &= \alpha(x_1, \ldots, x_n) + \alpha(y_1, \ldots, y_n) \end{aligned}$$
3. $1(x_1, \ldots, x_n) = (1x_1, \ldots, 1x_n) = (x_1, \ldots, x_n)$
4. $(\alpha\beta)(x_1, \ldots, x_n) = (\alpha\beta x_1, \ldots, \alpha\beta x_n) = \alpha(\beta x_1, \ldots, \beta x_n) = \alpha(\beta(x_1, \ldots, x_n))$

例题 4.25 The set $\mathbb{R}[x]$ of polynomials with real coefficients is a vector space over $\mathbb{R}$. The set $\mathbb{R}_{\leq n}[x]$ of real

[7]代数结构是指在集合上定义的运算满足某些公理的结构. 其核心目标是通过公理化的规则，抽象出不同数学对象的共同特性，从而统一研究它们的性质.
代数结构的三大要素：集合、运算、公理.
常见的代数结构：群、环、域、向量空间、模

polynomials of degree at most n is a vector space over $\mathbb{R}$.

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_nx^n) = (a_0 + b_0) + \cdots + (a_n + b_n)x^n$$

$$\lambda(a_0 + a_1x + \cdots + a_nx^n) = (\lambda a_0) + (\lambda a_1)x + \cdots + (\lambda a_n)x^n$$

So as vector spaces, $\mathbb{R}_{\leq n}[x]$ and $\mathbb{R}^{n+1}$ are "the same".

例题 4.26 The set of all functions $f : \mathbb{R} \to \mathbb{R}$ forms a vector space over $\mathbb{R}$.

Addition of two functions: $(f + g)(x) := f(x) + g(x)\ \forall x$

Scalar multiplication: $(\lambda f)(x) = \lambda f(x)\ \forall x$

例题 4.27 $Mat(n, \mathbb{R})$ is a vector space over $\mathbb{R}$.

Scalar multiplication: $\lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$ Actually, we can view a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as a vector (a, b, c, d) in $\mathbb{R}^4$

第 5 章 Group theory and error-correcting codes

5.1 Preliminaries

笔记 Recall that for any group G[1]:

1. the identity element is unique
2. inverse of an element is unique
3. $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$

定理 5.1

Let G be a group and let $a, b \in G$. Then

1. The equation $a = bx$ has a unique solution $x = b^{-1}a$.
2. The equation $a = xb$ has a unique solution $x = ab^{-1}$.

♡

证明 (i)We have $bx = a \Leftrightarrow b^{-1}(bx) = b^{-1}a \Leftrightarrow (b^{-1}b)x = b^{-1}a \Leftrightarrow x = b^{-1}a$. (ii)$xb = a \Leftrightarrow (xb)b^{-1} = ab^{-1} \Leftrightarrow x(bb^{-1}) = ab^{-1} \Leftrightarrow x = ab^{-1}$.

定义 5.1

Let G be a group and let $a \in G$. The positive powers of a is defined recursively by $a^1 = a$ and $a^{k+1} = a \cdot a^k$ for $k \geq 1$.

Define $a^0 = e$. The negative powers of a are given by $a^{-k} = (a^{-1})^k$ for $k \geq 1$.

♣

笔记 If $a = xy$, then $a^2 = (xy)(xy)$. In general, this is different from x^2y^2.

定理 5.2

Let G be a group and let $g, h \in G$. For $\forall r, s \in \mathbb{Z}$, we have

1. $g^r g^s = g^{r+s}$
2. $(g^r)^s = g^{rs}$
3. $g^{-r} = (g^r)^{-1} = (g^{-1})^r$
4. If $gh = hg$, then $(gh)^r = g^r h^r$.

♡

证明 (iv) For $r \geq 0$, the proof is identical to that of Theorem 4.2.1(iv). Suppose $r < 0$. Then $r = -k$ for some positive integer k. We have

$$g^{-k}h^{-k} = (g^{-1})^k(h^{-1})^k = (g^{-1}h^{-1})^k \text{[2]} = ((hg)^{-1})^k \overset{hg=gh}{=} ((gh)^{-1})^k \overset{def}{=} (gh)^{-k}$$

(iii) Note that

$$gg^{-1} = g^{-1}g = e$$

Applying (iv) with $h = g^{-1}$ yields

$$g^r(g^{-1})^r = (gg^{-1})^r = e^r = e$$

[1] see Corollary 5.1.2

[2] Since $g^{-1}h^{-1} = h^{-1}g^{-1}$ and $k > 0$.The inverse of gh and hg are $h^{-1}g^{-1}$ and $g^{-1}h^{-1}$respectively.

$\Rightarrow (g^r)^{-1} = (g^{-1})^r \overset{def}{=} g^{-r}$

(i)

$$g^{r+s} = g^r g^s \ \forall r, s \in \mathbb{Z}$$

We admit this fact. (ii)

$$(g^r)^s = g^{rs}$$

Consider two cases:

case 1: $s \geq 0$. We prove by induction on s. The base case $s = 0$ holds since $(g^r)^0 = e = g^0 = g^{r0}$. Let $s > 0$, and suppose the statement holds for $s - 1$. Then

$$(g^r)^s \overset{def}{=} g^r (g^r)^{s-1} \overset{ih}{=} g^r g^{r(s-1)} \overset{(i)}{=} g^{r+r(s-1)} = g^{sr}$$

ih represents induction hypothesis.

case 2: $s \leq 0$. Then $s = -k$ for some $k \geq 0$. We prove by induction on k that $(g^r)^{-k} = g^{-rk}$.

$$(g^r)^{-k} = (g^r)^{-1}(g^r)^{-(k-1)} = g^{-r} g^{-r(k-1)} \overset{(i)}{=} g^{-rk}$$

定义 5.2

Let G be a (not necessarily finite) group. An element $a \in G$ is said to have infinite order if there is no positive integer n such that $a^n = e$. Otherwise, the order of $a \in G$ is the smallest positive integer n for which $a^n = e$. ♣

定理 5.3

Let G be a group. Suppose $a \in G$ has finite order n. Then $a^r = a^s$ if and only if $n|(r - s)$. ♡

证明 Copy the proof of Theorem 4.2.3 (for symmetric group).

$$a^r = a^s \Leftrightarrow a^{r-s} = e$$

Suppose $r - s \geq 0$. We write $r - s = nq + t,\ 0 \leq t < n. \Rightarrow e = a^{r-s} = a^{nq+t} = (a^n)^q a^t = a^t \Rightarrow t = 0.$

例题 5.1 The order of a permutation $\pi \in S(n)$ can be computed from the cycle decomposition of π.

For a general group G, it is usually hard to determine the order of an element.

例题 5.2 If $|G| < \infty$, then every element of G has finite order (See Theorem 4.2.2)[3].

Consider the group $GL(2, \mathbb{R})$[4] of invertible 2×2 real matrices. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then A has infinite order. $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \ldots, A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for every positive integer n.

定义 5.3

Let $(G, *)$ be a group. A non-empty subset $H \subseteq G$ is a subgroup of G if $(H, *)$ forms a group. ♣

To check whether H is a subgroup of G or not, we don't have to verify the four group axioms:

[3] 如果群 G 的阶有限，则 G 中每个元素的阶都是有限的. $|G|$: 群中元素的个数

[4] 可逆 2×2 实矩阵的群. General Linear Group

定理 5.4

Let G be a group and let $H \subseteq G$ be non-empty. The following are equivalent:

1. H is a subgroup of G.
2. H satisfies:
   (a). if $a \in H$ then $a^{-1} \in H$.
   (b). if $a, b \in H$, then $a * b \in H$.
3. If $a, b \in H$, then $a * b^{-1} \in H$.

♡

证明 (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i)

(i) $\Rightarrow$ (ii): follows from the definition of a group.

(ii) $\Rightarrow$ (iii): $b \in H \overset{(a)}{\Rightarrow} b^{-1} \in H$. $a, b^{-1} \in H \overset{(b)}{\Rightarrow} a * b^{-1} \in H$

(iii) $\Rightarrow$ (i): we need to verify the four group axioms.

- Associativity law: If $a, b, c \in H$, then $a, b, c \in G$. By the associativity law for G

$$(ab)c = a(bc)\ \forall a, b, c \in H$$

- Take $\forall a \in H$, since a, $a \in H$, we have

$$e = aa^{-1} \overset{(iii)}{\in} H, i.e.$$

  H contains the identity element e.
- Consider $a \in H$. Since $e, a \in H$, we obtain $ea^{-1} \in H$, so that $a^{-1} \in H$.
- Consider $a, b \in H$, we have shown that $b^{-1} \in H$.

$$a, b^{-1} \in H \overset{(iii)}{\Rightarrow} a(b^{-1})^{-1} \in H \Rightarrow ab \in H$$

例题 5.3 Let $G = (\mathbb{Z}, +)$. We know that G is a group. Let $H = \{2n, n \in \mathbb{Z}\} \subseteq G$. Consider $2m, 2n \in H$. We have $2m + (-2n) = 2(m - n) \in H$. By the theorem, H is a subgroup of G.

定理 5.5

Let G be a group and let H, K be subgroups of G. Then $H \cap K$ is a subgroup of G.

♡

证明 By Thm 5.1.5 it suffices to show $H \cap K \neq \emptyset$ and

$$xy^{-1} \in H \cap K\ \forall x, y \in H \cap K$$

Since $e \in H \cap K, H \cap K \neq \emptyset$. For $\forall x, y \in H \cap K$, we have xy^{-1} and $xy^{-1} \in K$ (since H, K are groups), so that $xy^{-1} \in H \cap K$.

定理 5.6

Let G be a group and let $g \in G$. Then the set

$$\text{<g>} := \{g^n : n \in \mathbb{Z}\}$$

is a subgroup of G. It has n elements if $ord(g) = n$ and it is infinite if $ord(g) = \infty$.

♡

证明 <g> $\neq \emptyset$ since $g \in$ <g>. Consider $\forall x, y \in$ <g>. Then $x = g^m, y = g^n$ for some $m, n \in \mathbb{Z}$. By Thm 5.1.3

$$xy^{-1} = g^m(g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \text{<g>}$$

Therefore, <g> is a subgroup. If $ord(g) = n$, then <g> has exactly n distinct elements

$$e = g^0, g^1, \ldots, g^{n-1} \quad \text{by Thm 5.1.4}[5]$$

If g has infinite order, then g^1, g^2, ... are all distinct. Otherwise, $g^i = g^j$ for some $i > j$, which implies $g^{i-j} = e$, a contradiction. Hence <g> has infinitely many elements.

笔记

1. <g> is called the cyclic subgroup of G generated by g.
2. By Thm 5.1.3, <g> is Abelian:

$$g^m g^n = g^{m+n} = g^n g^m$$

例题 5.4 Consider S(3). The cyclic subgroups of S(3) are: <id> = $\{id\}$, <(1,2)> = $\{id, (1,2)\}$, <(1,3)> = $\{id, (1,3)\}$, <(2,3)> = $\{id, (2,3)\}$, <(1,2,3)> = $\{id, (1,2,3), (1,3,2)\}$ and <(1,3,2)> = $\{id, (1,3,2), (1,2,3)\}$.

[5] $g^i = g^j \Leftrightarrow ord(g) \mid i - j$

5.2 Cosets and Lagrange's theorem

定义 5.4

Let G be a group, and let H be a subgroup of G. For $a \in G$, the set

$$aH := \{ah : h \in H\}$$

is called the (left) coset of H.

♣

笔记

1. H is a (left) coset of H since $H = eH$.
2. If $b \in aH$, then $aH = bH$. In particular, any two cosets are either the same or disjoint.

   $$b \in aH \Rightarrow b = ah \text{ for some } h \in H$$

   we have

   $$bH = \{bk : k \in H\} = \{(ah)k : k \in H\} = \{a\underbrace{(hk)}_{\in H} : k \in H\} \subseteq aH$$

   and hence $aH \subseteq bH$

例题 5.5

If $H = G$, then it has only one coset. If $H = e$, then $aH = \{a\}\ \forall a \in G$, and so each element of G forms a coset of H.

例题 5.6 Take $G = (\mathbb{Z}, +)$ and $H = \{nk : k \in \mathbb{Z}\}$, where $n \geq 2$ is an integer. $H =$ congruence class of 0 modulo n. $1 + H = \{1 + nk : k \in \mathbb{Z}\} =$ congruence class of 1 modulo n, etc. So cosets of $H(in\ G)$ are congruence classed modulo n.

定理 5.7

Let H be a subgroup of G. Then $\forall a, b \in G$, either

$$aH = bH \text{ or } aH \cap bH = \emptyset$$

♡

定理 5.8

Let $H \leq G$ (i.e. H is a subgroup of G). $\forall a \in G$,

$$|aH| = |H|$$

♡

证明 Define $\varphi : H \to aH, h \mapsto ah$. Obviously, φ is a surjective.

φ is injective: if $\varphi(h) = \varphi(k)$, then $ah = ak$. Multiplying on the left by a^{-1}, we get $h = a^{-1}(ah) = a^{-1}(ak) = k$.

Hence φ is a bijection, giving $|aH| = |H|$

Lagrange's theorem

定理 5.9

Let G be a finite group, and let H be a subgroup of G. Then $|H|$ divides $|G|$.

♡

证明 By Thm 5.2.1, G is a disjoint union of some cosets of H(in G), say

$$G = a_1H \cup ... \cup a_mH$$

We have

$$|G| = |a_1H| + ... + |a_mH| = {}^{6}|H| + \cdots + |H| = m|H|$$

笔记 $|G|$ is called the order of G. Sometimes denoted by $o(G)$

笔记 Let G be a finite group. Then for any $g \in G$, $ord(g)$ divides $|G|$

证明 We know that <g> is a subgroup of G with $ord(g)$ elements. By Thm5.2.3

$$ord(g) \mid |G|.$$

笔记 If G is a group of prime order p. Then G is cyclic.

证明 Let $g \in G \setminus \{e\}$. Then <g> has at least 2 elements e and g. By Thm 5.2.3

$$|\text{<g>}| \text{ divides } |G|$$

Since p is a prime, we must have

$$|\text{<g>}| = p$$

This implies $G =$ <g>

笔记 **Fermat's Theorem**

Let p be a prime and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then $a^{p-1} \equiv 1 \mod p$.

证明 The group G_p has exactly $p-1$ elements. As $p \nmid a$, $[a]_p \in G_p$ By Lagrange's theorem, $ord([a]_p)$ divides $|G_p| = p-1$. We have

$$[a]_p^{p-1} = ([a]_p^{ord(a)})^{\frac{p-1}{ord(a)}} = ([1]_p)^{\frac{p-1}{ord(a)}} = [1]_p$$

笔记 **Euler's Theorem**

Let $a, n \in \mathbb{Z}$ with $n \geq 2$ and $\gcd(a, n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \mod n$$

where $\phi(n)$ is the Euler totient function.

证明 Note that $\phi(n)$ is the number of elements of G_n. We proceed as in the proof of Corollary 5.2.6.

笔记 **Lagrange's Theorem**

If $H \leq G$, then $|H| \mid |G|$

[6] (Thm 5.2.2)

5.3 Groups of small order

定义 5.5

Let G and H be groups. A function $\varphi : G \to H$ is a (group) isomorphism if it is a bijection, and it preserves the group structures, i.e.,

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in G$$

♣

笔记

1. $id_G : G \to G$ is a (group) isomorphism.
2. If $\varphi : G \to H$ is a (group) isomorphism, then $\varphi^{-1} : H \to G$ is also a (group) isomorphism.
3. $$G \xrightarrow[\varphi]{\cong} H \xrightarrow[\psi]{\cong} K, \quad \psi\circ\varphi$$

   If $\varphi : G \to H$ and $\psi : H \to K$ are isomorphism, then $\psi \circ \varphi : G \to K$ is an isomorphism
4. By 1. - 3., the relation of being isomorphic is an equivalence relation.

定理 5.10

Let G, H be groups, and let $\varphi : G \to H$ be an isomorphism. Then $\varphi(e_G{}^a) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1}$

[a] identity element of G

♡

证明 For $\forall g \in G$

$$e_H \cdot \varphi(g) = \varphi(g) = \varphi(e_G \cdot g) = \varphi(e_G) \cdot \varphi(g)$$

$\Rightarrow e_H = \varphi(e_G)$.

For $\forall g \in G$

$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_H$$

$\Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$

定义 5.6

Given groups G, H, the direct product $G \times H$ is the set of ordered pairs (g, h) with $g \in G, h \in H$, equipped with the following multiplication

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$$

♣

定理 5.11

$G \times H$ is a group.

♡

证明

Closure: $\forall g_1, g_2 \in G$ and $h_1, h_2 \in H$

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2) \in G \times H$$

Since G and H are groups.

Associativity: $\forall g_1, g_2, g_3 \in G, h_1, h_2, h_3 \in H$

$$((g_1, h_1)(g_2, h_2))(g_3, h_3) = (g_1g_2, h_1h_2)(g_3, h_3) = ((g_1g_2)g_3, (h_1h_2)h_3)$$

$$(g_1, h_1)((g_2, h_2)(g_3, h_3)) = (g_1, h_1)(g_2g_3, h_2h_3) = (g_1(g_2g_3), h_1(h_2h_3))$$

Identity element: $(e_G, e_H) \in G \times H$

$\forall (g, h) \in G \times H$

$$(e_G, e_H)(g, h) = (e_Gg, e_Hh) = (g, h)$$

$$(g, h)(e_G, e_H) = (ge_G, he_H) = (g, h)$$

Inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1}) :

$$(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H)$$

$$(g^{-1}, h^{-1})(g, h) = (e_G, e_H)$$

笔记

1. $G \times H \cong H \times G$ The map $(g, h) \mapsto (h, g)$ is an isomorphism from $G \times H$ to $H \times G$
2. For groups G, H, K, we have

$$(G \times H) \times K \cong G \times (H \times K)$$

Since the map $((g, h), k) \mapsto (g, h, k)$ is an isomorphism. So we may write $G \times H \times K$, and so on

定义 5.7

Let C_n denote the cyclic group on n elements. Note that $C_n \cong (\mathbb{Z}_n, +)$

笔记

1.

$$\mathbb{Z}_n = <[1]_n> = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

2. Any two cyclic groups on n elements are isomorphic. If $G = <g>, H = <h>$, where $ord(g) = ord(h) = n$, then the map $\varphi : G \to H, g^k \mapsto h^k$ is an isomorphism.

定理 5.12

If m, n are positive integers s.t. $(m, n) = 1$, then

$$C_m \times C_n \cong C_{mn}$$

[a]

[a] $C_m \times C_n$ is a cyclic group

证明 Let $C_m = <a>$ and $C_n = <b>$. We show that $C_m \times C_n = <(a, b)>$ and (a, b) has order mn. We have $ord(a) = m, ord(b) = n$. For $\forall k \in \mathbb{Z}$

$$(a, b)^k = (a^k, b^k)$$

We have $(a, b)^k = e \Leftrightarrow a^k = e \wedge b^k = e \Leftrightarrow ord(a) \mid k \wedge ord(b) \mid k \Leftrightarrow m \mid k \wedge n \mid k \Leftrightarrow mn \mid k, since(m, n) =$

1 So (a, b) has order mn. Moreover, $C_m \times C_n$ has mn elements $\Rightarrow C_m \times C_n = <(a, b)>$

笔记

If $|G|$ is a prime, then G must be cyclic.

Classification of groups of order at most 8.

1 2 3 4 5 6 7 8

Group of order 1: there is only one such group, namely $G = e$.

Group of order $\{2, 3, 5, 7\}$: C_p is the unique group of order p. To classify groups of order 4, we use the follow theorem

定理 5.13

Let G be a group. If $x^2 = e\ \forall x \in G$, then G is Abelian. ♡

证明 $(xy)^2 = e \Rightarrow (xy) = (xy)^{-1} = y^{-1}x^{-1} = yx\ \forall x, y \in G$

笔记 Continue the note 30.

Groups of order 4:

- If G has an element of order 4, then G is the cyclic group of order 4.
- Suppose G doesn't have any element of order 4.

Recall that for $\forall x \in G$, we have

$$ord(x) \mid |G| = 4$$

$\Rightarrow ord(x) = 2$ if $x \in G \setminus \{e\}$. In particular, $x^2 = e\ \forall x \in G$. By Thm 5.3.4, G is Abelian. Write $G = \{e, g, h, k\}$. Then $gh \neq g, h, e = g^2$, so that $gh = k$. Similarly, $gk = h$ and $hk = g$.

$\rightarrow$ multiplication table of G:

	e	g	h	k
e	e	g	h	k
g	g	e	k	h
h	h	k	e	g
k	k	h	g	e

笔记

Exercise: $G \cong C_2 \times C_2$.

In summary, there are two groups of order 4: $C_4, C_2 \times C_2$

Groups of order 6 :

- If G has an element of order 6, then

$$G \cong C_6$$

- Suppose G doesn't have an element of order 6. Hence, for $\forall x \in G \setminus \{e\}$,

$$order(x) \in \{2, 3\}$$

(Since $ord(x) \neq 1, 6$ and $ord(x) \mid 6$)

笔记 **Consider two cases**:

case 1 All elements $x \in G \setminus \{e\}$ have order 2. Since $x^2 = e\ \forall x \in G$, by Thm 5.3.4, G is Abelian. Let

$a, b \in G \setminus \{e\}$. Then $ab \neq a, b, e = a^2$. $\Rightarrow H := \{e, a, b, ab\}$ has 4 elements. It is a subgroup of G. (Since $xy^{-1} \in H, \forall x, y \in H$). By **Lagrange's Theorem**, $4 = |H|$ divides $6 = |G|$, which is impossible. So this case cannot happen.

case 2 G has an element a of order 3. $\Rightarrow e, a, a^2$ are distinct elements of G. Let $b \in G \setminus \{e, a, a^2\}$.

$\Rightarrow a^2 = e, a, a^2, b, ba, ba^2$ are distinct elements (by checking that any two of them are distinct). $\Rightarrow G = \{e, a, a^2, b, ba, ba^2\}$.

We can check that $b^2 \neq a, a^2, b, ba, ba^2$. (E.q. If $b^2 = a$, then $e, b, b^2, \cdots, b^5$ are distinct, which implies $G \cong C_6$). Hence $b^2 = e$. Similarly, $ab = ba^2$. $\rightarrow$ multiplication table of G **Cayley table** 凱萊表:

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

$\Rightarrow G \cong S(3)$

Isomorphism f: $G \rightarrow S(3)$ $f(e) = id, f(a) = (1\,2\,3), f(a^2) = (1\,3\,2), f(b) = (1\,2), f(ba) = (2\,3), f(ba^2) = (1\,3)$

5.4 Error-detecting & error-correcting codes

Let $B = \{0, 1\}$

定义 5.8

A word of length n is a string of n binary bits (For example, 0110 is a word of length 4.) The set of words of length n is denoted by $B^n = \underbrace{B \times \cdots \times B}_{n \text{ copies}}$. Given $x = x_1 \cdots x_n \in B^n$, the weight of x is defined as

$$wt(x) = \#\{i : x_i = 1\}$$

(For example, $wt(0110) = 2$)

The (Hamming) distance between two words $x = x_1 \cdots x_n,\ y = y_1 \cdots y_n \in B^n$ is defined as

$$d(x, y) = \#\{i : x_i \neq y_i\}$$

(For example, $d(1011, 0011) = 1$)

♣

定义 5.9

A coding function is a map $f : B^m \to B^n$. For $x \in B^m$, $f(x)$ is called a code word.

♣

例题 5.7 $f : B^2 \to B^6$, $f(x) = xxx\ \forall x \in B^2$. For instance, $f(00) = 000000$, $f(01) = 010101$.

定理 5.14

Let $f : B^m \to B^n$. The f allows the detection of k or fewer if and only if $d(u, v) \geq k + 1\ \forall$ codeswords $u \neq v$.

♡

证明 ($\Leftarrow$)Suppose u' is obtained from a codeword, say a, by changing at most k bits. Then u' cannot be a codeword, since otherwise $d(u, u') \geq k + 1$. ($\Rightarrow$) Suppose f allows the detection of k or fever errors. If we have two codewords u, v with $d(u, v) \leq k$, then k errors can convert u to v and we can not detect the change.

定理 5.15

$f : B^m \to B^n$. f allows the correction of k or fewer errors. $\Leftrightarrow\ d(u, v) \geq 2k + 1\ \forall$ codewords $u \neq v$.

♡

证明 ($\Leftarrow$) Let u be the original codeword[7]. u' is obtained from u by changing at most k bits. u is the unique codeword that is at distance $\leq k$ from u'. Suppose otherwise that $\exists$ a codeword $v \neq u$ s.t. $d(v, u') \leq k$. **Fact** (triangle inequality): $\forall x, y, z \in B^n$, $d(x, y) + d(y, z) \geq d(x, z)$. By the above fact, we get

$$2k + 1 \leq d(u, v) \leq d(u, u') + d(u', v) \leq k + k = 2k$$

a contradiction. ($\Rightarrow$) Suppose otherwise that $\exists$ codewords $u \neq v$ with $d(u, v) \leq 2k$. Then one can find $w \in B^n$ such that $d(u, w)$ and $d(v, w)$ are both $\leq k$. Both u and v can be converted to w by changing $\leq k$ bits.

$$u = \underbrace{0 \cdots 0}_{2k}$$
$$v = \underbrace{1 \cdots 1}_{2k}$$
$$w = \underbrace{0 \cdots 0}_{k}\underbrace{1 \cdots 1}_{k}$$

[7] unknown

笔记 Properties of (Hamming) distance:

1. (Symmetry) $\forall x, y \in B^n$, $d(x,y) = d(y,x)$.
2. (triangle inequality) $\forall x, y, z \in B^n,\ d(x,y) + d(y,z) \geq d(x,z)$

It is computationally hard to determine the minimum distance between codewords, and to "correct" the corrupted codewords. $\rightsquigarrow$ consider a more restrive class of coding functions. Equip $B = \{0,1\}$ with addition and multiplication operations:

$$0+0=0 \quad 0\cdot 0=0$$

$$0+1=1+0=1 \quad 0\cdot 1=1\cdot 0=0$$

$$1+1=0 \quad 1\cdot 1=1$$

(Actually $B \cong \mathbb{Z}_2$ is a field. Thus, B^n is a vector space over $\mathbb{Z}_2$)

定义 5.10

A (coding) function $f : B^m \to B^n$ is called a linear code if

$$f(u+v) = f(u) + f(v) \ \ \forall\, u, v \in B^m$$

i.e. f is a linear map

♣

定理 5.16

Let $f : B^m \to B^n$ be a linear code. Then $min\ d(u,v)^a$ = $min\ wt(w)^b$

[a] codewords $u \neq v$

[b] non-zero codeword w

♡

证明 We have $d(u,v) = wt(u-v)$. $(= wt(u+v))$

$u = 01101, v = 11001, u-v = 10100, d(u,v) = 2, wt(u-v) = 2$

定义 5.11

Let $m < n$. A generator matrix G is a $m \times n$ binary matrix of the form

$$G = (I_m \ \ A)$$

I_m is a $m \times m$ identity matrix. A is a $m \times (n-m)$ binary matrix

♣

例题 5.8

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(I_2: columns 1–2; A: columns 3–5)

$m = 2, n = 5$

Let $n < m$, and let G be a $m \times n$ generator matrix. Define $f_G : B^m \to B^n,\ x \mapsto xG$. A m-D row vector times matrix G

例题 5.9

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$f_G : B^2 \to B^5$

$$f_G(x) = (x_1\ x_2)\begin{pmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 0\end{pmatrix} = (x_1\ x_2\ x_1\ (x_1+x_2)\ 0)$$

笔记 f_G is an injective function.

定义 5.12

Let $G = (I_M\ \ A)$ be a $m \times n$ generator matrix. The corresponding parity-check (奇偶校验) matrix is the $n \times (n-m)$ matrix

$$H = \begin{pmatrix}A\\ I_{n-m}\end{pmatrix}$$

♣

例题 5.10

$$\text{If } G = \begin{pmatrix}1 & 0 & 1 & 1 & 0\\ \underbrace{0 & 1}_{I_2} & \underbrace{0 & 1 & 0}_{A}\end{pmatrix}, \text{ then } H = \begin{pmatrix}1 & 1 & 0\\ \underbrace{0 & 1 & 0}_{A}\\ 1 & 0 & 0\\ 0 & 1 & 0\\ \underbrace{0 & 0 & 1}_{I_3}\end{pmatrix}$$

笔记 generator matrix $G \to$ linear code f_G

$\searrow$ parity-check matrix H

定理 5.17

Let $G = (I_m\ \ A)$ be a $m \times n$ generator matrix. Consider the linear code $f_G : B^m \to B^n$ ($f_G(x) = xG$). Then, w is a codeword if and only if

$$wH = 0$$

where $H = \begin{pmatrix}A\\ I_{n-m}\end{pmatrix}$ is the parity-check matrix corresponding to G.

♡

证明 $w \in B^n$ is a codeword $\Leftrightarrow w = f_G(x)$ for some $x \in B^m \Leftrightarrow w = x(I_m\ \ A) = (x\ \ xA)$[8]

$$0 = xA - (xA)I_{n-m} = xA + (xA)I_{n-m} = (x\ \ xA)\begin{pmatrix}A\\ I_{n-m}\end{pmatrix} = wH$$

[8] $x \in B^m, xA \in B^{n-m}$