目录

第 1 章 Group theory

1.1 Introduction

定义 1.1 (Group)

1. The binary operation * is associative.
2. There exists an identity element in G.
3. Each element in G has an inverse.

♣

例题 1.1 (Z, +): the set of all integers forms a group under addition.

例题 1.2 (Q*,×): the set of all nonzero rational numbers forms a group under multiplication.

第 2 章 Basic concepts

2.1 Set and Mapping

2.1.1 Set

定义 2.1 (Set)

1. A set is a **Well-defined** collection of objects;while are called the elements of the set.
2. The objects that belong to a set are called its elements or members. If an element x belongs to a set A then we denote this fact by writing $x \in A$; otherwise we write $x \notin A$.
3. The number of elements in a set A is denoted by |A|, which is called the cardinality of A.

♣

笔记

1. Classical set are based on Boolean logic
2. Every classical set has a sharp boundary
3. classical set can be extended to fuzzy sets

性质 [Representations]

1. A finite set with a small cardinality can be specified by directly listing all of its elements enclosed within curly brackets

$$S = \{x_1, x_2, \cdots, x_n\} \tag{2.1}$$

2. Alternatively, a set (possibly infinite) can be specified by stating the property used to determine its elements.

$$S = \{x|x \quad satisfies \quad properties\} \tag{2.2}$$

2.1.2 Subsets

定义 2.2 (Subsets)

1. A set B is said to be a subset of a set A, denoted by B⊆ A (or A⊇B) if every element of B is also an element of A.
2. If A is a subset of B but is not equal to B, then we say that A is a proper subset of Band write A⊂B (or B⊃A).

$$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B \tag{2.3}$$

♣

笔记 The empty set is a subset of every set
Every set is a subset of itself

2.1.3 Set operations

定义 2.3 (operations)

1. Union=$A \cap B = \{x|x \in A \vee x \in B\}$
2. Intersection=$A \cap B = \{x|x \in A \wedge x \in B\}$
3. Difference=$A \backslash B = A \cap B' = \{x = x \in A \wedge x \notin B\}$
4. Complement=$A' = \{x|x \in U \wedge x \notin A\} = \{x|x \in U : \neg(x \in A)\}$

♣

定义 2.4 (Mappings)

1. Let A and B be sets. A mapping f: A→B from A to B assigns to each element x in A exactly one element f(x) in B. The set A is called the domain of the mapping f, and the set B is called the co-domain of the mapping f
2. Let f: AtoB be a mapping and C be a subset of A. The image of C under f is the set f(C)=f(x): x∈C. In particular, the set f(A) is also known as the range of the mapping f. The inverse image of a subset D of B is the set $f^1(D)$=a∈A : f(a)∈D

♣

定义 2.5 (Basic properties of mappings)

1. A mapping f: A→B is surjective (or onto) if f(A)=B. We say that f is injective (or one-to-one) if a≠b implies f(a) ≠ f(b). A mapping is called bijective if it is both injective and surjective.
2. Note that f: X→Y is bijective if and only if, given any element b in Y, there exists exactly one element a in X with f(a)=b. The identity map on A is a mapping idA : A→A such that id_A(x)=x for all x in A.

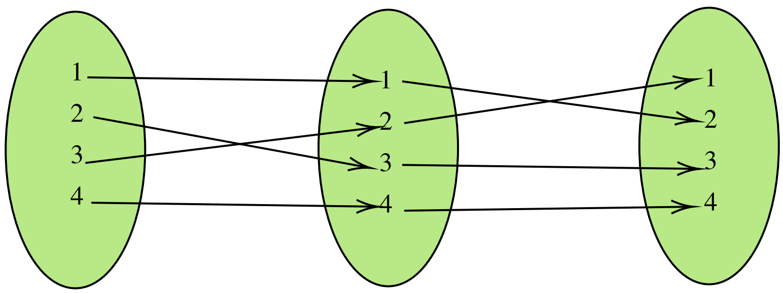
♣

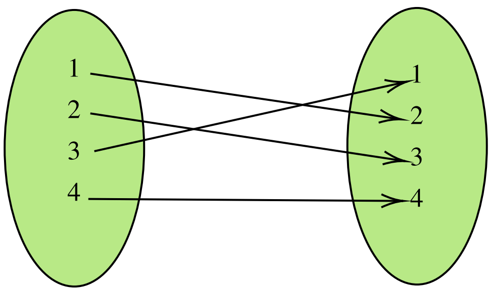
定义 2.6 (Composition of mappings)

1. Let f: A→B and g: B→C be mappings. The composition of f and g is a mapping g f: A→C defined by (g∘f)(x)=g(f(x)) for all x in A.
2. A mapping g: B→A is called an inverse mapping of the mapping f: A→B if g∘f = id_A and f∘fg=id_B . A mapping is said to be invertible if it has an inverse. The inverse of f is denoted by f_{-1}.

♣

例题 2.1





注 The functions f and g are composed to yield a new composite function $g \circ f$

定理 2.1

Let f:A→B,g:$B \to C$,and h:$C \to D$.Then

1. The composition of mappings is associative;that is,$(h \circ g) \circ f = h \circ (g \circ)$
2. If f and g are both one-to-one,them the mapping $g \circ f$is one-to-one;
3. If f and g are both onto,then mapping $g \circ f$ is onto;
4. If f and g are bijective,then so is $g \circ f$.

♡

定理 2.2

A mapping is invertible if and obly if it is both one-to-one and onto.

2.2 Cartesian products

定义 2.7

Given sets X and Y,the CAresian product of the sets X and Y,denoted by $x \times Y$,is the set of all ordered pairs(a,b) with a in X and b in Y.

笔记 The cartesian product $X_1 \times X_2 \times \cdots \times X_n$ of the sets $X_1, X_2, \cdots, x_n$ consists of all n-tuples$(a_1, a_2, \cdots, a_n)$with$a_i in X_i$for i=1,2,...,n.If $X = X_1 = X_2 = \cdots = X_n$ their Cartesian product is simply written as X^n

Keywords

- binay relation
- homogeneous
- n-ary
- reflexive
- symmetric
- transitive
- preorder
- ineflexive
- asymmetric
- total
- antisymmetric
- complete
- poset
- relatively prime
- quasi prder
- partial order
- total order
- chain
- minimum
- maximum
- minimal
- partition
- equivalence relation
- equivalence class
- quotient
- tolerance relation
- singleton

2.3 Binary relation

定义 2.8 (binary)

1. A binary operation on a nonempty set A is a mapping.be written as $A \times A \longrightarrow A$
2. A binary operation * on A is associative if (ab)c=a(bc) for all abc∈ A
3. A binary operation * on A is comunative of ab=ba for all abc∈ A

♣

定义 2.9 (identity)

Let *:A×A →be a binary operation A

1. if l∈A,la=a l is left identity
2. if l∈A,al=a l is right identity
3. if l∈A,al=la=a l is identity

♣

定理 2.3

if l and r respectively left and right identity in A,then l = r is an identity

♡

定理 2.4

The identity is unique in A if it exist.

♡

证明 Assume A has more than a identity,$e_1, e_2, \cdots, e_n$
we know :

$$e_1 = e_1 \cdot e_2 = e_2$$
$$e_3 = e_2 \cdot e_3 = e_3$$
$$\vdots$$
$$e_{n-1} = e_{n-1} \cdot e_n = e_n$$

so $e_1 = e_2 = \cdots = e_n$,the identity is only one,if it exists.

定义 2.10

Let R be a binary relation between A and B. If (a,b) ∈ R, then we say that a is R-related to b (or a, b are R-related), which is denoted by a R b.

注 The domain of R is the set of all x ∈ A such that x R y for some y ∈ B. The range of R is the set of all y ∈ B such that x R y for some x ∈ A.

例题 2.2 Let A=Gardner, Valerian, Olivia, Frank, Daisy and B=London, Berlin, Paris, Boston. Suppose that:

1. Gardner and Valerian were born in London;
2. Olivia was born in Boston;
3. Frank and Daisy were born in Paris.

证明 The above information can be described in terms of a binary relation R given by:

$$R = (Gardner, London), (Valerian, London), (Olivia, Boston), (Frank, Paris), (Daisy, Paris)$$

性质 A binary relation R on A is said to be:

- reflexive ⇔ $\forall x$∈A, x R x.
- irreflexive (or strict) ⇔ ∀ x ∈A, ¬(x R x)
- symmetric⇔ ∀x, y ∈ A, x R y⇒ y R x.
- antisymmetric ⇔ ∀ x, y ∈ A, $(xRy) \wedge (yRx)$ ⇒ x=y
- asymmetric ⇔ ∀ x, y ∈ A, x R y ⇔ ¬(y R x).
- transitive⇔ ∀ x, y,Z ∈ A, (xRy)∧ (y R z) ⇒ x R z.
- complete ⇔x, y ∈ A, x ≠ y ⇒ (x R y) ∨ (y R x).
- total (or strong complete) ⇔ ∀x, y ∈ A, (x R y) ∨ (y R x).

例题 2.3

1. The relations =, ≤ and ≥ are reflexive.
2. The relations < and > are irreflexive.
3. The relations = and “relatively prime” are symmetric.
4. The relations ≤ and ≥ are antisymmetric.
5. The relations < and > are asymmetric.
6. The relations =, ≤ and ≥ are transitive
7. The relations < and > are complete but not total
8. The relations ≤ and ≥ are total.

定理 2.5

Let R be a binary relation on A. Then the following are equivalent:

1. R is antisymmetric.
2. ∀x,y∈A,(x R y)∧(x ≠ y)⇒¬(y R x)

证明

$$\begin{aligned}
Risantisymmetric &\Leftrightarrow \forall x, y \in A, (xRy) \wedge (yRx) \rightarrow x = y \\
&\Leftrightarrow \forall x, y \in A, (xRy) \rightarrow ((yRx) \rightarrow x = y)(CP.rule) \\
&\Leftrightarrow \forall x, y \in A, (xRy) \rightarrow (x \neq y \rightarrow \neg(yRx)) \\
&\Leftrightarrow \forall x, y \in A, (xRy) \wedge (x \neq y) \Rightarrow \neg(yRx)
\end{aligned}$$

定理 2.6

Let R be a binary relation on A. Then the following are equivalent:

1. R is asymmetric.
2. R is antisymmetric and irreflexive.

证明

1. Assume that R is asymmetric,Then we have (x R y)⇒¬(yRx).It follows that ∀x,y∈A,(x R y)∧(x ≠ y)⇒¬(y R x),Thus R is antisymmetric,Let x∈A.since R is asymmetric,we have xRy→ ¬(yRx)
2. Assume that R is not irreflexive.Then there exists $x_0 \in A$such that $x_0 Rx$.It follows that $\neg(x_0 R_0 x_0)$.This lead to a contradication.Therefore,R is irreflexive
3. Assume that R is antisymmetric and irreflexive,Let XRy for x,y∈A,Note first that $x \neq y$since R is irreflexive thus we have $\neg(yRx)$since R is antisiymmetric.Therefore R is antisymmetric

命题 2.1

if $P_1 \Rightarrow P_2$ then $P_2 \rightarrow Q \Rightarrow P_1 \rightarrow Q$

证明 if $P_1 \Rightarrow P_2$:

$$\begin{aligned}(P_2 \rightarrow Q) \rightarrow (P_1 \rightarrow Q) &\Leftrightarrow \neg(P_1 \rightarrow Q) \rightarrow \neg(P_2 \rightarrow Q)\\ &\Leftrightarrow (P_1 \wedge \neg Q) \rightarrow (P_2 \wedge \neg Q)\end{aligned}$$

Since $v(P_1)$≤ v(P$_2$), $v(p_1 \wedge \neg Q)$≤v(p$_2$ $\wedge \neg Q$),Hence $P_1 \Rightarrow P_2$ then $P_2 \rightarrow Q \Rightarrow P_1 \rightarrow Q$

定理 2.7

Let R be a binary relation on A. Then the following are equivalent:

1. R is complete.
2. $\forall x, y \in A, (x = y) \vee (xRy) \vee (yRx)$.

定理 2.8

Let R be a binary relation on A. Then the following are equivalent:

1. R is total.
2. R is reflexive and complete.

笔记 total = feflexive + complete

证明

$$\begin{aligned}\underbrace{(xRy) \vee (yRx)}_{totoal} &\Leftrightarrow ((x = y) \wedge (x \neq y)) \wedge (xRy) \wedge (yRx)\\ &\Leftrightarrow ((x = y) \rightarrow (xRy) \wedge (yRx)) \wedge (x \neq y) \rightarrow (xRy) \wedge (yRx)\\ &\Leftrightarrow \underbrace{((x = y) \rightarrow xRy)}_{reflexive} \wedge \underbrace{(x \neq y \vee (xRy) \vee (yRx)}_{complete}\end{aligned}$$

2.4 Order relation

命题 2.2

Let $\leq$ be a binary relation on A.Then we say that:

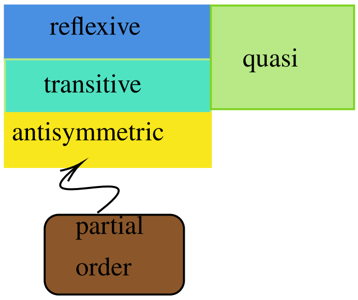
1. $\leq$ is a preorder (or quasi order)$\Leftrightarrow\leq$ is re flexive and transitive.
2. $\leq$ is a weak order $\Leftrightarrow$ $\leq$ is total and transitive
3. $\leq$ partial order $\Leftrightarrow$ $\leq$is reflexive,antisymmetric and transitive
4. $\leq$ is a total order$\Leftrightarrow\leq$ is total,antisymmetric and transive
5. $\leq$ is a strict partial order $\Leftrightarrow\leq$ is irreflexive and transitive
6. $\leq$ is a strict total order $\Leftrightarrow$ $\leq$ is irreflexive,compete and transitive

注 Strict total orders are not total oeders

定理 2.9

Let $\leq$ be a binary relation on A. Then the following are equivalent:

1. $\leq$ is a partial order
2. $\leq$ is an antisymmetric preorder.



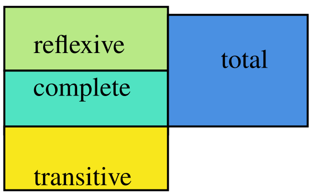
定理 2.10

Let $\leq$ be a binary relation on A.then:

1. $\leq$ is a weak order
2. $\leq$ is a complete preorder

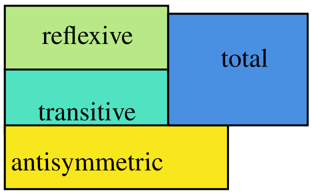
证明

$$\Leftrightarrow \text{R is a complete,reflexive and transitive}$$
$$\Leftrightarrow \text{R is total and transitive}$$
$$\Leftrightarrow \text{R is weak order}$$

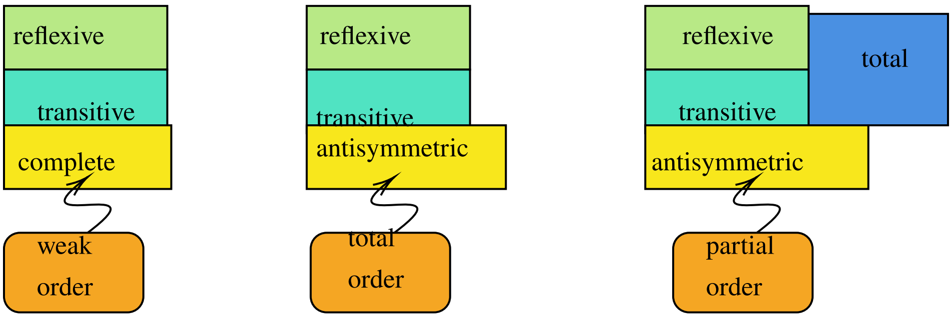


定理 2.11
Let $\leq$ be a binary relation on A,Then:

1. $\leq$ is a total order
2. $\leq$ is a complete partial order
3. $\leq$ is an antisymmetric weak order



笔记



2.5 Equivalence relation

定理 2.12
A binary relation R on A is called an equivalence relation if it is reflexive, symmetric and transitive. For a $\in$ A, the set $[a]_R$=$\{b \in A|aRb\}$ is called the equivalence class of a under R.

例题 2.4 [1]The equivalence class of (a,b) under cross-multiplication, where a,b$\in$ Z and b $\neq$ 0,is:

$$[(a, b)] = \{(c, d) : ad = bc\}$$

If we denote [(a,b)] by a/b, then this equivalence class is precisely the fraction usually denoted by a=b. After all, it is plain that (1,2)$\neq$(2,4), but [(1,2)]=[(2,4)]; that is, $\frac{1}{2} = \frac{2}{4}$

例题 2.5 An equivalence class[(P,Q)] of arrows, as in Example 2.17(iv), is called a vector; we denote it by [(P,Q)]=$\overrightarrow{PQ}$

引理 2.1
If $\equiv$ is an equivalence relation on a set X, then x $\equiv$ y if and only if [x]=[y].

证明 Assume that x$\equiv$ y. If z $\in$[x], then z$\equiv$x, and so transitivity gives z $\equiv$y; hence [x] [y]. By symmetry, y$\equiv$ x, and this gives the reverse inclusion[y]$\subseteq$ [x]. Thus, [x]=[y] Conversely, if [x]= [y], then x $\in$ [x], by reflexivity, and so x $\in$ [x] = [y]. Therefore, x $\equiv$ y

[1] A first course in Abstract algebra.98

定理 2.13

Let R be an equivalence relation on A. Then

$$A/R = \{[a]_R | a \in A\}$$

is called the quotient set of A by R.

定理 2.14

Let R be an equivalence relation on A. Then the following are equivalent:

1. a R b
2. $b \in [a]_R$
3. $[a]_R = [b]_R$

定义 2.11

Let R be an equivalence relation on A. Then either $[a]_R = [b]_R$ or $[a]_R \cap [b]_R = \emptyset$ for all a,b ∈ A.

笔记 [2] A partition of a set X is a family of nonempty pairwise disjoint subsets, called blocks, whose union is all of X. Notice that if X is a finite set and $A_1, A2, \ldots, A_n$ is a partition of X, then

$$|X| = |A_1| + |A_2| + \cdots + |A_n|$$

We are now going to prove that equivalence relations and partitions are merely different views of the same thing

命题 2.3

If ≡ is an equivalence relation on a set X, then the equivalence classes form a partition P of X. Conversely, given a partition of X, there is an equivalence relation on X whose equivalence classes are the blocks in P.

证明 [3]Assume that an equivalence relation ≡ on X is given. Each x ∈ X lies in the equivalence class [x] because ≡is reflexive; it follows that the equivalence classes are nonempty subsets whose union is X. To prove pairwise disjointness, assume that a ∈ [x] ∩ [y], so that a ≡x and a ≡y. By symmetry, x ≡a, and so transitivity gives x ≡y. Therefore,[x] = [y], by the lemma, and so the equivalence classes form a partition of X.

Conversely, let P be a partition of X. If x,y∈X, define x ≡y if there is A ∈ P with x ∈ A and y ∈ A. It is plain that ≡is reflexive and symmetric. To see that ≡is transitive, assume that x ≡y and y ≡z; that is, there are A,B∈ P with x, y ∈ A and y, z ∈ B. Since y ∈ A B, pairwise disjointness gives A D B and so x, z ∈ A; that is, x ≡z. We have shown that ≡is an equivalence relation.

It remains to show that the equivalence classes are the subsets in P . If x ∈ X, then x ∈ A for some A ∈ P. By definition of , if y ∈ A, then y ≡x and y ∈ [x]; hence, A ⊆[x]. For the reverse inclusion, let z ∈ [x], so that z ≡x. There is some B with x ∈ B and z ∈ B; thus, x ∈ A ∩ B. By pairwise disjointness, A = B, so that z ∈ A, and [x] ⊆ A. Hence, [x]=A. •

定义 2.12

Let R be an equivalence relation on A. Then $\cap\{[a]_R | a\in A\}$ = A

[2]A first course in Abstract algebra.99

[3]A first course in Abstract algebra.99

2.6 Partitions

定理 2.15

Let R be an equivalence relation on A. Then

$$A/R = \{[a]_R | a \in A\}$$

forms a partion of A

定理 2.16

Let P = $\{A_i | i \in I\}$ be a partition of A. Then the binary relation R on A given by

$$aRb \Leftrightarrow \exists i \in I, \{a, b\} \subseteq A_i$$

is an equivalence relation on A.

2.7 Division

定义 2.14

If a and b are integers, then a is a divisor(or **factor**) of b if there is an integer d with b = ad (synonyms are a divides b and also b is a **multiple** of a). We denote this by:

$$a|b$$

证明 Note that 3|6, because 6 = 3×2, but that 3|5 (that is, 3 does not divide 5):even though 5 = 3 × 5=$\frac{5}{3}$ ×3,the fraction$\frac{5}{3}$is not an integer.

定义 2.15

A common divisor of integers a and b is an integer c with c|a and $c|b$. **The greatest common divisor** of a and b, denoted by gcd(a, b) [or, more briefly, by (a, b)], is defined by:

$$gdc(a, b) = \begin{cases} 0 \quad if a = 0 = b \\ \text{the largest common divisor of a and b otherwise.} \end{cases}$$

笔记 The notation (a, b) for the gcd is, obviously, the same notation used for the ordered pair. The reader should have no difficulty understanding the intended meaning from the context in which the symbol occurs.

笔记

- If a and m are positive integers with $a|m$, say, m = ab, we claim that $a \leq m$. Since $0 < b$, we have 1 ≤ b, because b is an integer, and so a ≤ ab = m. It follows that gcd' s always exist.
- If c is a common divisor of a and b,then so is −c. Since one of $\sqrt{m}$ c is non negative, the gcd is always nonnegative. It is easy to check that if at least one of a and b is nonzero, then (a,b)>0.

命题 2.4

if p is a prime and b is any integer, then:

$$(p.b) = \begin{cases} \text{p if } p|b \\ \text{1 otherwise.} \end{cases}$$

证明 A common divisor c of p and a is, of course, a divisor of p. But the only positive divisors of p are p and 1, and so (p,a) = p or 1; it is p if $p|a$, and it is 1 otherwise.

定义 2.16

Let $a_1, \cdots, a_n$ be positive integers. The smallest positive integer m which is $divisiblebyalla_i$ $(i = 1, \cdots, n)$, is called the least common multiple of $a_1, \cdots, a_n$, and is denoted by $m = lcm(a_1, \cdots, a_n)$.

定义 2.17

A positive integer p greater than 1 is said to be prime if 1 and p are the only positive factors of p. An interger p>1 is called a composite number if it is not prime.

定理 2.17

Every integer n ≥ 2 is either a prime or a product of primes.

证明 Were this not so, there would be "criminals:" there are integers n ≥ 2 which are neither primes nor products of primes; a least criminal m is the smallest such integer. Since m is not a prime, it is composite; there is thus a factorization m D ab with 2 ≤ a < m and 2 ≤b <m (since a is an integer, 1 < a implies 2 ≤ a). Since m is the least criminal, both a and b are "honest," i.e.,

$$a = pp'p'' \dots \quad b = qq'q'' \dots$$

where the factors$a = pp'p'' \dots \quad b = qq'q'' \dots$are primes.Therefore,

$$m = ab == pp'p'' \dots qq'q'' \dots$$

is a product of (at least two) primes, which is a contradiction.

命题 2.5

If m ≥ 2 is a positive integer which is not divisible by any prime p with p ≤ $\sqrt{m}$, then m is a prime.

证明 If m is not prime, then m = ab, where a < m and b < m are positive integers. If a > $\sqrt{m}$ and b > $\sqrt{m}$, then m = ab >$\sqrt{m}\sqrt{m}$ = m, a contradiction. Therefore, we may assume that a≤ $\sqrt{m}$. By Theorem 2.17, a is either a prime or a product of primes, and any (prime) divisor p of a is also a divisor of m. Thus, if m is not prime, then it has a "small" prime divisor p; i.e., p≤ $\sqrt{m}$. The contrapositive says that if m has no small prime divisor, then m is prime.

笔记 can be used to show that 991 is a prime. It suffices to check whether 991 is divisible by some prime p with p ≤ 991 ≈ 31.48; if 991 isnot divisible by 2, 3, 5, ... , or 31, then it is prime.

定义 2.18

Two integers are relatively primeif their greatest common divisor is 1. The integers $a_1, , a_n$ are pairwise relatively prime if gcd(a_i, a_j)=1 whenever $1 \le i < j \le n$.

例题 2.6 Determine whether 10, 17 and 21 are pairwise relatively prime.
sol:Since gcd(10,17)=gcd(10,21)=gcd(21,17)=1,we deduce that they are pairwise relatively prime.

定理 2.18

Let a,b,c be integers.Then

1. $a|b \wedge a|c \Rightarrow \forall x, y \in Z, a|(xb + yc)$;
2. $a|b \Rightarrow a|bc$;
3. $a|b \wedge b|c \Rightarrow a|c$;

证明 Assume that b+c=a($d_1 + d_2$).Thus there exist $d_1, d_2 \in Z$such that $b = ad_1$and c = bd_2=$(ad_1)d_2$,Hense $a|c$
We will give a direct proof of (1). Suppose that $a|b$ and $a|c$. Then, from the definition of divisibility, it follows that there

are integers s and t with b = as and c = at. Hence,

$$b + c = as + at = a(s + t).$$

Integers Divisible by the Positive Integer d.

定理 2.19 (Division Algorithm)

Let a and d be integers with d >0. Then there are unique integers q, r such that

$$a = dq + r$$

with $0 \leq r < d$.We refers to a,d,q,r as dividend divisor,quotient and remainder,respectively.

2.8 Well ordering principle

定义 2.19

The pair (A,(≤) is called a partially ordered set,or simply a poset,if ≤is a partial order on A

定义 2.20

The pair (A, ≤) is called a totally ordered set, or simply a chain, if ≤is a total order on A.

定义 2.21

Let (A, ≤) be a poset and B⊆A. Then

1. l ∈ B is called the minimum in B if l ≤ b for all b ∈ B.
2. g ∈ B is called the maximum in B if b ≤ g for all b ∈ B.

定义 2.22

Let (A, ≤) be a poset and B⊆A. Then

1. n ∈ B is minimal in B ⇔ ¬(∃ b ∈ B, b < n).
2. m ∈ B is maximal in B ⇔ $\neg(\exists b \in B, b >> m)$.

定理 2.20

Let (A, ≤) be a poset and B⊆A. Then n ∈ B is minimal in B ⇔ ∃b ∈ B, b ≤ n → b=n.

定理 2.21

Let (A, ≤) be a poset and B⊆A. Then n ∈ B is maximal in B ⇔ ∀b ∈ B, m ≤ b → b=m.

定义 2.23

A totally ordered set (A, ≤) is called a well ordered set if every nonempty subset of A has a least element.

定理 2.22 (Well ordering principle)

Every nonempty subset of N has a least element.

笔记 The set of natural numbers is well ordered.

定理 2.23 (principle of Mathematical Induction)

Let S be a subset of natural numbers such that

1. 0∈S;
2. n∈S⇒n+1∈S

then S = N;

注 Why Mathematical Induction is Valid? [4]Why is mathematical induction a valid proof technique? The reason comes from **the well- ordering property**, listed in Appendix 1, as an axiom for the set of positive integers, which states that every nonempty subset of the set of positive integers has a least element. So, suppose we know that P (1) is true and that the proposition P (k) →P (k + 1) is true for all positive integers k. To show that P(n) must be true for all positive integers n, assume that there is at least one positive integer for which P (n) is false. Then the set S of positive integers for which P (n) is false is nonempty. Thus, by the well-ordering property, S has a least element, which will be denoted by m. We know that m cannot be 1, because P (1) is true. Because m is positive and greater than 1, m - 1 is a positive integer. Furthermore, because m – 1 is less than m, it is not in S, so P (m - 1) must be true. Because the conditional statement P (m - 1) → P (m) is also true, it must be the case that P (m) is true. This contradicts the choice of m. Hence, P (n) must be true for every positive integer n.

定理 2.24 (Strong Induction)

To prove that P (n) is true for all positive integers n, where P (n) is a propositional function, we complete two steps:

1. We verify that the proposition P (1) is true.
2. We show that the conditional statement $[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$is true for all positive integers k.

笔记 Strong induction is sometimes called **the second principle of mathematical induction** or **complete induction**.

2.9 Modular arithmetic

定义 2.24

Let a, n ∈ Z with n > 0. We denote by a mod n the remainder when a is divided by n.

定义 2.25

Let a, b, n∈ Z with n > 0. We say that a is congruent to b modulo n, which is denote by a≡b (mod n), if $n|(a-b)$.

定理 2.25

Let n be a positive integer. Then the congruent modulo n relation is an equivalence relation on Z.

证明

- reflexive:
- transitive:
- symmetric:

[4]Discrete mathematics and its applications

定义 2.26

Let n be a positive integer. Then the quotient set

$$Z_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} = Z/R_n$$

is called the set of residue classes of integers modulo n, where R_n is the congruent modulo n relation.

定理 2.26

Let a, b, c, d, n ∈ Z with n < 0. Then

1. $a \equiv b(modn) \wedge c \equiv d(modn) \Rightarrow a + c \equiv b + d(modn)$.
2. $a \equiv b(modn) \wedge c \equiv d(modn) \Rightarrow a \cdot c \equiv b \cdot d(modn)$.

2.10 Groups

2.10.1 Binary operations

定义 2.27

A binary operation on a nonempty set A is a mapping ⊙: A×A →A.

A binary operation ⊙ on A is associative if a(bc) =(ab) c for all a,b,c∈ A. A binary operation ⊙ on A is commutative if ab=ba for all a,b∈ A.

定义 2.28

Let ⊙ : A× A → A be a binary operation on A. Then

1. An element l∈ A is called a left identity if la=a for all a∈ A.
2. An element r∈ A is called a right identity if ar=a for all a∈ A.
3. An element e∈ A is called an identity if ae=ea=a for all a∈ A.
4. An element a∈ A is called an idempoten if $a^2 = a, \exists a$ ∈A.

定理 2.27

Let ⊙ : A× A → A be a binary operation on A. If l and r are respectively left and right identities in A, then l=r is an identity

定理 2.28

Let ⊙ : A× A → A be a binary operation on A. Then the identity in A is unique if it exists.

2.10.2 Semigroups

定义 2.29 (Groupoid(群胚))

A groupoid (G,⊙) is a nonempty settogether with a binary operation ⊙ on G.

定义 2.30 (Semigroups(半群))

A groupoid (G,⊙) is called a semigroup if the operation ⊙ is associative.

定义 2.31 (monoid(幺半群))

A semigroup (G,⊙) is called a monoid if it contains an identity.

注 Group has only one idempotent.But probality has not one idempotent.

例题 2.7 A = [0,1],$a \vee b = \max\{a, b\}$,$S^{'} = (A, \vee)$,we can know

$$\forall a \in A \quad a \vee a = a \Rightarrow aRa = a$$

The idempotent has more than one in semigroup.

定义 2.32 (Abelian(阿贝尔群))
A semigroup (G,⊙) is said to be Abelian if the operation ⊙ is commutative.

2.10.3 Groups

定义 2.33
A monoid (G,⊙) with identity e is a called a group if for every a in G, there exists b in Gsuch that ab=ba=e. The element b, denoted by b=a^{-1}, is called the inverse of a.

定义 2.34
The order of a group (G,⊙) is the cardinality of the set G.

例题 2.8

1. groups($\mathbb{Z}$,+),The identity is 0.Inverse is -a.
2. groups($\mathbb{Q}^{*}$,·),The identity is 1.Inverse is 1/a.
3. GL(n,R)=$R^{n\times n}$=A|is an n×n real matrix is a groups under the multipliaction

命题 2.6

1. The identity e is unique.
2. The inverse a^{-1} is unique for each a in G.
3. The inverse of a^{-1} is the element a.
4. The inverse of ab is the element $b^{-1}a^{-1}$.
5. The identity e is the unique idempotent element in G
6. For all a,b,c∈G, ab=ac ⇒ b=c
7. For all a,b,c∈G, ba=ca ⇒ b=c
8. For a,b∈G, the equations ax=b and ya=b have unique solutions x=a^{-1}b and y=ba^{-1}, respectively.

证明

1. Assume that e_1 and e_2 are both identities.so
$$e_1 = e_1 * e_2 = e_2$$
the identity is unique.
2. Assume that a_1^{-1}, a_2^{-1} are both inverses.we know
$$a_1^{-1} * (e) = a_1^{-1} * (a * a_2^{-1}) = e * a_2^{-1} = a_2^{-1}$$
3. According definition, We can know a^{-1} is inverse of a
4. Note first $ab * (b^{-1}a^{-1}) = e$,so The inverse of ab is the element $b^{-1}a^{-1}$
5. Note first that e is idempotent.If$a^2 = a$,the we can deduce that e=$a^{-1}a = a^{-1}a^2 = ea = a$
6. If ab=ac,then we have
$$b = eb = (a^{-1}a)b = a^{-1}ac = c$$
7. etc

8. if ax=b and ya=b we have

$$x = ex = (a^{-1}a)x = a^{-1}ax = a^{-1}b$$

定理 2.29

A semigroup (G,⊙) is a group if and only if it satisfies the following:

1. G has a left identity l;
2. for all a ∈ G, ∃ a^*∈ G such that a^* a=l

♡

证明 ⇒ Obviously that is true

⇐ Assume that G is (G,Q) is a semigroup such that ax=b and ya=b.Given $b_0 \in G$,the equation $yb_0 = b_0$ is a solution y=l.For every a∈G.the equation $b_0x = a$ as a solutionx=C_0It fllows that la=l$(b_0c_0) = b_0c_0 = a$,Which shows that l is note also that the equation ya=l has a solution y=a^* the left inverse of a.Therefor G is a group.

Similarly we can conclude that:

定理 2.30

A semigroup (G,⊙) is a group if and only if it satisfies the following:

1. G has a right identity r
2. for all a ∈ G, ∃ a^* ∈ G such that aa*=r.

♡

定理 2.31

A semigroup (G,⊙) is a group if and only if for all a,b ∈ G, the equations ax=b and ya=b have solutions in G

♡

证明 ⇒ Straightforward

⇐ Assume that G is semigroup such that ax=b and ya=b have solutions.Given $b_0 \in G$,the equation $yb_0 = b_0$ has a solution y = l.For every a∈G,the equation $b_0x = a$ has a solution $x = c_0$ It follows that la=l$(b_0c_0) = b_0c_0 = a$ which shows that l is a left identity.Note that the equation ya=l has a solution y=a^*.Hence,$a^*$is the left inverse of a. According Theorem2.29 we know that it is a group.

Keywords

- subgroup 子群
- trivial subgroup 平凡子群
- subgroup generated by X 由 X 生成的子群
- cyclic 循环的
- generator 生成元
- finitely generated 有限生成的

2.10.4 Subgroup

定义 2.35

A nonempty set H of a group (G,⊙) is called a subgroup of G, denoted by H ≤ G, if H forms a group under the binary operation ⊙ of G(restricted to its subset H) .

定理 2.32

A nonempty set H of a group (G,⊙) is called a subgroup of G, denoted by H G, if it satisfies the following conditions:

1. H contains the identity of G;
2. For all x,y∈ H, xy∈ H; $(i.e., H^2 \subseteq H)$
3. For all x,y∈ H, xy^{-1}∈H. $(i.e., H^{-1} \subseteq H)$

定义 2.36

A nonempty set H of a group(G,∘) is called a subgroup of G,if it satisfied

1. $\forall x, y \in H$,xy∈h
2. H contains the identity of G
3. ∀ y∈ $H, y^{-1} \in H$

笔记

1. 1,2 can proves the G is submoinod.
2. 1,2,3 can proves the G is subgroup

定理 2.33

H is a sub group of G

1. H≤G
2. $\forall x, y \in H$,$xy \in H$ and $y^{-1} \in H$
3. ∀ x,y∈ H,$xy^{-1} \in H$

证明 3⇒1 Assum that $xy^{-1} \in H$ whenever x,y∈H,since $H \neq \emptyset$,there exits some a ∈ H.Thus e = $aa^{-1} \in H$,Hence

$$b^{-1} = eb^{-1} \in H$$

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

Therefore,H≤G

定理 2.34

If G is a group and $\bigcap_{i\in I} H_i$,then $\cap_{i\in I}H_i$is a subgroup of G.

证明 Let H = $\bigcap_{i\in I} H_i$,if x,y∈H,then x,y∈ H_i,for all $i \in I$.
Thus $xy^{-1} \in H_i \leq G$for all i∈I.Hence $xy^{-1} \in H$.Therefore H≤G

笔记 The intersection of some subgroups of a group G is also a subgroup of G.

定义 2.37

Let G be a group and x⊆G.Then

$$< x >= \cap\{H|X \subseteq H \leq G\}$$

is called **the subgroup of G generated by X**

笔记 The subgroup generated by the set X is the smallest subgroup of G containing X.

笔记 <∅>=e

笔记 G 中的真子群分布是不均匀的，不是一直都是一层包含一层的关系，很大可能是离散的每个群包含的元素有的相同，有的不同，比如 Z_6 中的剩余类群就是不一样的（2，4）和（0，3）。

定义 2.38

Let G be a group and H = <X>≤ G,Then

1. The elements of X are called the generated of H.
2. H is said to be finitely generated if it has a finite set of generators.
3. H is said to be cyclic if it can be generated by a single generator.

定理 2.35

Let G be a group and $\emptyset \neq X \subseteq G$. If H is the set of all finite product of elements in X $\cup X^{-1}$,then H is the subgroup of generated by X.

笔记 The subgroup generated by X contains exactly all the finite product elements in X orX^{-1}

定理 2.36

Let G be a group and $\emptyset \neq X \subseteq G$.Then

$$< X >= \{a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}\}$$

1. $a^0 = e, a^2 = aa, a^{-2} = (a^2)^{-1}$
2. <X> contains excutly all the finite product of elements in X or X^{-1}

Keywords

- homomorphism 同态
- homomorphic image 同态像
- monomorphism 单同态
- epimorphism 满同态
- endomorphism 自同态
- automorphism 自同构
- isomorphism 同构
- isomorphic to 同构于
- kernel 核

2.10.5 Homomorphisms

定义 2.39

Let(F,⊙) and (K,+) be semigroups. A mapping f:G→K is called a homomorphism if

$$f(a \odot b) = f(a) + f(b)$$

for all a,b∈ G.

注 A homomorphism between two semigroups is a mapping which is compatible to the binary operation defined on the semigroups

定义 2.40

Let f:G→H be a homomorphism.Then f is called

1. a monomorphism if it is injective
2. an epimorphism if it is surjective
3. an isomorphism if it is bijective
4. an endomorphism if G=H
5. an automorphism if G=H and f is bijective

定义 2.41

Let G and H be semigroups.Then G is said to be isomorphic to H if there exists an isomorphism from G to H.This is denoted by G ≅ H

笔记 The realtion ≅ is an equivalence relation

定义 2.42

Let f: G→K be a homomorphism of groups Then Im(f)=f(G) is called the homomorphic image of G,and ker(f) $=f^{-1}(< e_K >)$ is called the kernel of f

1. Ker(f) = $f^{-1}(\{e_K\})$=$\{a \in G | f(a) = e_K\}$
2. Ker(f) 是 E_k 原象集
3. $e_G \in Ker(f)$

证明 1⟹3,First assume that f is monomorphism,since $f(e_G) = e_K$,we have $e_G \in Ker(f) = f^{-1}(\{e_K\})$,Let $a \in Ker(f)$,Then f(a)=$e_K = f(e_G)$.since f is injective it follows that a = e_G ,Therefore Ker(f)=$\{e_G\}$
3⟹1 Let a,b belongs to G,f(a)=f(b).Then

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

Thus $ab^{-1} \in Ker(f) = \{e_G\}$,That is $ab^{-1} = e_G$,Hence $a = (b^{-1})^{-1} = b$,Therefore f is a monomorphism

注 Let G be an Abelian group consider the mapping f:G→ G given by

$$f(x) = X^{-1}$$

Show that f is an automorphism of groups

定义 2.43

Let f:G→K be a homoorphism of groups.Then Im(f)=f(G) is called the homomorphic image of G,and Ker(f)=$f^{-1}(\{e_k\}$ is called the kernel of f

例题 2.9 Let $3Z = \{3n|n \in Z\}$. It can be seenthat 3Z is a subgroup of the additive group ofintegers. Consider the mapping f: Z→ 3Z given by f(n) =3n. One can verify that f is anisomorphism of groups.

命题 2.7

Let A,B,C be subgroups.Let f:AtoB and g:B→C be mappings.Then we have:

1. If f and g are homomorphisms, then g∘ f is a homomorphism.
2. If f and g are monomorphisms, then g∘ f is a monomorphism.
3. If f and g are epimorphisms, then g∘ f is an epimorphism.
4. If f and g are isomorphisms, then g∘ f is an isomorphism.

命题 2.8

Let f:G→K be a homomorphism of groups.Then we have:

1. $f(e_G)$=e_k.
2. $f(x^{-1})$=$(f(x))^{-1}$.

证明

1. Since f is a group homomorphism,$f(e_G)f(e_G) = f(e_Ge_G) = f(e_G)$, The shows that $f(e_G)$ is idempotent.Note also that e_K is the unique idenpotent in K,Thus $f(e_G) = e_K$
2. let $x \in G$,since

$$f(x) \cdot f(x^{-1}) = f(e_G) = e_k \Rightarrow f(x) = (f(x^{-1}))^{-1}$$

–

笔记 The identity and inverses are preserved under the homomorphism of groups

命题 2.9

Let f:G→K be a homomorphism of groups.Then we have:

1. $K_1 \leq K \Rightarrow f^{-1}(K_1) \leq G$.
2. $G_1 \leq G \Rightarrow f(G_1) \leq K$.

证明

1. Note first that $f^{-1}(K_1) \neq \emptyset$,since $f(e_G) = e_K \in K_1 \leq K$.Let$x, y \in f^{-1}(K_1)$ Then f(x),f(y)∈ K_1,since$K_1 \leq K$,it follows that $f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^1) \in K_1$,Thus $xy^{-1} \in f^{-1}(K_1)$,Which shows that $f^{-1} \leq G$
2. Note first that $f(G_1 \neq \emptyset$ since $e_K = f(e_G) \in f(G_1)$,If $x, y \in G_1 \leq G$and $f(x_1y_1^{-1}) = f(x_1)f(y_1^{-1}) = f(x_1)f(y_1)^{-1} = xy^{-1} \in f(G_1$.Hence $f(G_1) \leq K$

2.10.6 Cyclic groups

定义 2.44

Let G be a group and $X \subseteq G$.Then

$$< X >= \cap\{H|X \subseteq\leq G\}$$

is called the **subgroup of G generated by X**

♣

定义 2.45

Let G be a group and $H \leq G$.Then H is said to be cyclic if $H =< a >$ for some a in H

♣

定义 2.46

Let G be a group and ainG.The orderof the element a,denoted by $|a|$,is the order of the cyclic groups generated by a

♣

定义 2.47 (cyclic groups)

Let n be a positive integer.Then the quotient set

$$Z_n = \overline{0}, \overline{1}, \cdots, \overline{n-1}$$

♣

例题 2.10 we can know the equation that $\overline{r} = \{k \in Z|r \equiv k(modn)\} = \{k \in Z \mid mod\ n = r\}$
The set Z forms a groups under the binary operation:

$$\overline{r} + \overline{s} = \overline{r+s}$$

例题 2.11

1. The additive groups of integers is an infinite cyclic group generated by the genrator 1.
2. The groups Z_n consisting of all the residue classes of integer modulo n is a finite cyclic group generated by the generator $\overline{1}$

例题 2.12 Consider the residue class groups Z_6.As shown in the foregoing,$\{\overline{0}, \overline{3}\}$ and $\{\overline{0}, \overline{2}, \overline{4}\}$are subgroups of Z_6.In addition,it is easy to verify the following facts:

$$|\overline{3}| = | < \overline{3} > | = |\{|\overline{3}, \overline{0}\}| = 2$$

$$\overline{0} + \overline{2} + \overline{4}| = 3$$