Discrete mathematics portal

23 pages

Table of Contents

1 Discrete mathematics portal 19
離散数学

1.1 Logic and proof 19

1.2 Sets 20

1.3 Relations 20

1.4 Orders and lattices 21

1.5 Maps 21

1.6 What changes and what does not change 22

1.7 Exercise links 23

1.8 Summary 24

2 Propositions, predicates, and quantification 25
命題 述語 量化

2.1 What is a proposition? 25
命題

2.2 Reading a predicate as a truth set 25
真理集合

2.3 Logical connectives 26
論理結合子

2.4 Universal quantification and existential quantification 26
全称量化 存在量化

2.5 Move negation outside quantifiers 27

2.6 Example: read an inclusion relation logically 27
包含関係

2.7 Exercise link and summary 27

3 Proof methods and counterexamples 28
証明法 反例

3.1 Direct proof 28
直接証明

3.2 Proof by contraposition 28
対偶証明

3.3 Proof by contradiction 29
背理法

3.4 Proof by cases 29
場合分け

3.5 Counterexample 30
反例

3.6 Exercise link and summary 30

4 Mathematical induction and recursive definitions 31
数学的帰納法 再帰的定義

4.1 Induction form 31

4.2 Why it works 31

4.3 Worked theorem: size of a power set 32

4.4 Recursive definitions 33

4.5 Warning 33

4.6 Related links 33

4.7 Summary 34

5 Basics of sets 35
集合

5.1 Introduction 35

5.2 Terms and definitions 35

5.3 Method 36

5.4 Intuitive explanation 36

5.5 Rigorous explanation 36

5.6 Worked example: checking a subset relation from the definition 37

5.6.1 Problem 37

5.6.2 Explanation 37

5.7 What changes and what is preserved 37

5.8 How to distinguish the ideas 38

5.9 Exercise link 38

5.10 Related links 38

6 Set operations and inclusion relations 39
集合演算 包含関係

6.1 Introduction 39

6.2 Terms and definitions 39

6.3 Method 39

6.4 Intuitive explanation 40

6.5 Rigorous explanation 40

6.6 Worked example: proving De Morgan’s law by elements 41

6.6.1 Problem 41

6.6.2 Explanation 41

6.7 What changes and what is preserved 41

6.8 How to distinguish the ideas 42

6.9 Proof supplement: why set operations preserve inclusion 42

6.10 Exercise link 43

6.11 Related links 43

7 Families of sets and index sets 44
集合族 添字集合

7.1 Introduction 44

7.2 Terms and definitions 44

7.3 Method 44

7.4 Intuitive explanation 45

7.5 Precise point: the empty index set 45
添字集合

7.6 Worked example: indexed intersection 45
添字付き共通部分

7.6.1 Problem 45

7.6.2 Explanation 45

7.7 How to identify it and related links 46

8 Basics of the Cartesian product 47
直積集合

8.1 Introduction 47

8.2 Terms and definitions 47

8.3 Strategy 47

8.4 Intuitive explanation: tables and counting 48

8.5 Precise explanation 48

8.6 Worked example: Cartesian products and order 49

8.6.1 Problem 49

8.6.2 Explanation 49

8.7 What changes and what is preserved 49

8.8 Recognition criteria 50

8.9 Proof supplement: when products preserve inclusion 50

8.10 Exercise links 51

8.11 Related links 51

9 Basics of the power set 52
べき集合

9.1 Introduction 52

9.2 Terms and definition 52

9.3 Method: count the cardinality 52
個数

9.4 Intuitive example 53

9.5 Precise use 53

9.6 Boundary case: the empty set 53
空集合

9.7 Worked example: decide membership in a power set 54
[元であること] べき集合

9.7.1 Problem 54

9.7.2 Explanation 54

9.8 The power set as an inclusion order 54
べき集合 包含順序

9.9 Proof supplement: equivalence between power sets and inclusion 55

9.10 How to identify it and related links 55

10 Cardinality and countability of sets 57
濃度 可算性 集合

10.1 Introduction 57

10.2 Terms and definitions 57

10.3 Method 58

10.4 Intuitive explanation 58

10.5 Precise idea: entrance to the diagonal argument 58
対角線論法

10.6 Worked example: the positive even numbers are countable 59
可算

10.6.1 Problem 59

10.6.2 Explanation 59

10.7 How to identify it and related links 59

11 Basics of relations 60
関係

11.1 Introduction 60

11.2 Terms and definitions 60

11.3 Strategy 60

11.4 Intuitive explanation 61

11.5 Important properties 性質 61

11.6 Worked example: check the divisibility relation 整除関係 62

11.6.1 Problem 62

11.6.2 Explanation 62

11.7 How to identify it and related links 62

12 Composition 合成 and closure 閉包 of relations 関係 64

12.1 Introduction 64

12.2 Terms and definition: composition 合成 64

12.3 Terms and definitions: identity relation 恒等関係 and inverse relation 逆関係 64

12.4 What is closure? 閉包 65

12.5 Strategy 65

12.6 Intuitive explanation 65

12.7 Worked example: construct a transitive closure 推移閉包 66

12.7.1 Problem 66

12.7.2 Explanation 66

12.8 Proof supplement: minimality of the transitive closure 推移閉包 66

12.9 How to identify it and related links 67

13 Equivalence relations and partitions 68
同値関係 分割

13.1 Introduction 68

13.2 Terms and definitions 68

13.3 Strategy 69

13.4 Intuitive explanation 69

13.5 Precise explanation: from equivalence relations to partitions 69

13.6 Conversely, from partitions to equivalence relations 70

13.7 Example: equivalence by congruence 70

13.7.1 Problem 70

13.7.2 Explanation 70

13.8 Recognition criteria 71

13.9 Proof supplement: equivalence relations and partitions are the same data 71

13.10 Exercise links 72

13.11 Related links 72

14 Quotient sets and the canonical projection 73
商集合 自然な射影

14.1 Introduction 73

14.2 Terms and definitions 73

14.3 Strategy 73

14.4 Intuitive explanation 74

14.5 What is well-definedness? 74
well-defined 性

14.6 Worked example: the canonical projection 75
自然な射影

14.6.1 Problem 75

14.6.2 Explanation 75

14.7 How to identify it and related links 75

15 Partial orders and total orders 77
半順序関係 全順序関係

15.1 Introduction 77

15.2 Terms and definitions 77

15.3 Method 78

15.4 Intuitive explanation 78

15.5 Representative examples 78

15.5.1 1. Inclusion order on a power set 78

15.5.2 2. Divisibility order on positive integers 79

15.5.3 3. Usual numerical order 79

15.6 Worked example: partial but not total 79

15.6.1 Problem 79

15.6.2 Explanation 79

15.7 Recognition criteria 80

15.8 Proof supplement: restricting an order to a subset preserves the order 80

15.9 Exercise links 80

15.10 Related links 81

16 Hasse diagrams, maximal elements, and minimal elements 82
Hasse 図 極大元 極小元

16.1 Introduction 82

16.2 Terms and definitions 82

16.3 Maximal, greatest, minimal, and least 82

16.4 Method 83

16.5 Intuitive explanation 83

16.6 Worked example: maximal elements and greatest elements 83
極大元 最大元

16.6.1 Problem 83

16.6.2 Explanation 84

16.7 How to tell them apart 84

16.8 Exercise and related links 84

17 Order isomorphisms and well-orders 86
順序同型 整列順序

17.1 Order-preserving maps 86

17.2 Order isomorphism 86

17.3 Chains and antichains 87

17.4 Well-orders 87

17.5 What we are viewing without changing 88

17.6 Exercise links 88

17.7 Summary 89

17.8 Related links 89

18 Basics of lattices 90
束

18.1 Introduction 90

18.2 Terms and definitions 90

18.3 Strategy 91

18.4 Intuitive explanation 91

18.5 Examples 92

18.5.1 1. Powersets ordered by inclusion 92

18.5.2 2. Positive integers ordered by divisibility 92

18.6 Worked example: finding join and meet in inclusion order 92

18.6.1 Problem 92

18.6.2 Explanation 93

18.7 What changes and what is preserved 93

18.8 Recognition criteria 94

18.9 Proof supplement: monotonicity of meet and join 94

18.10 Exercise links 95

18.11 Related links 95

19 Basics of Boolean algebra 96
ブール代数

19.1 Correspondence between propositions and sets 96

19.2 A power set is a Boolean algebra 97
冪集合 ブール代数

19.3 De Morgan’s laws 97
ド・モルガンの法則

19.4 What is being abstracted 97

19.5 Proof supplement: uniqueness of complements 98
補元

19.6 Proof supplement: De Morgan’s laws 98
ド・モルガンの法則

19.7 Exercise link and summary 99

20 Basics of maps 100
写像

20.1 Introduction 100

20.2 Terms and definition 100

20.3 Images and preimages 100
像 逆像

20.4 Strategy 101

20.5 Intuitive explanation 101

20.6 Precise explanation 101

20.7 Worked example: distinguish codomain and range 102
終域 値域

20.7.1 Problem 102

20.7.2 Explanation 102

20.8 What changes and what is preserved 102

20.9 How to check and related links …… 103

21 Images and preimages of a map …… 104
像 逆像 写像

21.1 Image …… 104
像

21.2 Preimage …… 104
逆像

21.3 Preimages work well with set operations …… 105
逆像 集合演算

21.4 Be careful with intersections of images …… 105
共通部分 像

21.5 Counterexample: images do not preserve intersections …… 105
像 共通部分

21.6 What changes and what is preserved …… 106

21.7 Proof supplement: why preimages preserve set operations …… 106
逆像 集合演算

21.8 Exercise link and summary …… 106

22 Injections, surjections, and bijections …… 107
単射 全射 全単射

22.1 Introduction …… 107

22.2 Terms and definitions …… 107

22.3 Strategy …… 107

22.4 Intuitive explanation …… 108

22.5 Counting viewpoint for finite sets …… 108

22.6 Warning for infinite sets 109

22.7 Worked example: decide injection and surjection 109
単射 全射

22.7.1 Problem 109

22.7.2 Explanation 109

22.8 How to identify them and related links 109

23 Composite maps and inverse maps 111
合成写像 逆写像

23.1 Introduction 111

23.2 Terms and definitions 111

23.3 Method 112

23.4 Intuitive explanation 112

23.5 Rigorous explanation: inverse maps and bijections 112

23.6 Worked example: composite maps and inverse maps 113

23.6.1 Problem 113

23.6.2 Explanation 113

23.7 How to distinguish the ideas 113

23.8 Proof supplement: why composition preserves injectivity and surjectivity 114

23.9 Exercise link 114

23.10 Related links 114

data/lecture/math/discrete-math/離散数学ポータル-講義.n.md md a27bca6

Discrete mathematics portal

離散数学

Discrete mathematics 離散数学 is mathematics that studies separated objects and their relationships, not quantities that change continuously. The central topics to learn first are sets 集合, relations 関係, and maps 写像. However, these are not isolated terms. They stand on propositions 命題, predicates 述語, quantification 量化, and proof 証明.

Therefore, read this field in the following order.

1. Use logic 論理 and proof 証明 to prepare to read definitions precisely.
2. Use sets 集合 and set operations 集合演算 to handle collections of objects.
3. Use relations 関係 to handle connections between objects.
4. Use orders 順序 and lattices 束 to handle comparison and upper-lower structure.
5. Use maps 写像 to handle rules that send objects to other objects.

This order expresses dependencies. Later chapters reuse sets 集合, relations 関係, and maps 写像 defined earlier, so do not memorize terms as isolated labels. Follow how the ideas are connected.

1 Logic and proof

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

2 Sets

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

3 Relations

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

4 Orders and lattices

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

5 Maps

→ **Related page** lecture math discrete-math

study.bem130.com

→ Related page lecture math discrete-math

study.bem130.com

→ Related page lecture math discrete-math

study.bem130.com

→ Related page lecture math discrete-math

study.bem130.com

6 What changes and what does not change

In discrete mathematics 離散数学, each operation asks, "What changes, and what is preserved?"

Object	What changes	What we want to see preserved
Set operation 集合演算	membership conditions for elements	logical structure of membership conditions
Equivalence relation 同値関係	the viewpoint on individual elements	the structure by which elements are classified as the same kind
Order isomorphism 順序同型	names and representations of elements	comparison relations, maximum elements, minimum elements, upper bounds, and lower bounds
Map 写像	sending inputs to outputs	the rule, image, inverse image, and type of composition

Having this viewpoint first lets you follow why each definition is needed instead of memorizing definitions by rote.

For each operation, explicitly check which of the input type, membership condition, comparison relation, and reachability is preserved. This check prevents mistaken analogies when similar symbols appear.

7 Exercise links

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

8 Summary

At the entrance to discrete mathematics 離散数学, do not memorize sets 集合, relations 関係, and maps 写像 as separate items. Understand them as connected topics built on predicates 述語, quantification 量化, and proof 証明.

Propositions, predicates, and quantification
命題 述語 量化

In discrete mathematics 離散数学, the first thing to fix is what a statement is about. Sets 集合, relations 関係, and maps 写像 are all built from conditions on objects. Therefore organizing propositions 命題 and predicates 述語 first makes later definitions easier to read.

→ Related page lecture math discrete-math
study.bem130.com

1 What is a proposition? 命題

A proposition 命題 is a statement whose truth value is determined.

$$2 + 3 = 5$$

is true. In contrast,

$$x + 3 = 5$$

does not have a truth value until x is specified. Therefore it is a predicate 述語 about x.

A predicate is a statement that becomes a proposition after an object is inserted. For example, if $P(x)$: x is even, then $P(2)$ is true and $P(3)$ is false.

A proposition is a statement whose truth value is fixed. A statement with a remaining free variable is treated as a predicate 述語. A predicate becomes a proposition after a value is substituted or after it is quantified 量化.

2 Reading a predicate as a truth set 真理集合

It is important to connect a predicate 述語 with a set 集合. Fix a universal set 全体集合 U and consider a predicate $P(x)$. Then

$$\{x \in U \mid P(x)\}$$

is the set of all elements 元 that make $P(x)$ true. This set is called the truth set 真理集合.

Intuitively, a predicate is a filter, and the truth set is the collection of objects that pass through the filter.

A truth set 真理集合 depends on the domain 領域 of objects being allowed. Even with the same formula, changing the domain can change the truth set and the truth value of universal quantification 全称量化 or existential quantification 存在量化.

3 Logical connectives 論理結合子

Operations that build new propositions 命題 from propositions are called logical connectives 論理結合子.

Symbol	Reading	Meaning
$P \wedge Q$	and	both P and Q are true
$P \vee Q$	or	at least one of P, Q is true
$\neg P$	not	reverses the truth value of P
$P \Rightarrow Q$	implies	if P is true, then Q is true
$P \Leftrightarrow Q$	equivalent	P and Q have the same truth value

The implication 含意 $P \Rightarrow Q$ asserts that whenever P is true, Q is also true.

4 Universal quantification 全称量化 and existential quantification 存在量化

Quantification 量化 creates a proposition by specifying the range of a variable.

$$\forall x \in A,\ P(x)$$

means that $P(x)$ holds for every x in A. This is universal quantification 全称量化.

$$\exists x \in A,\ P(x)$$

means that there is at least one x in A satisfying $P(x)$. This is existential quantification 存在量化.

5 Move negation outside quantifiers

When negating a proposition with quantifiers, the quantifier switches.

$$\neg(\forall x \in A,\, P(x)) \Leftrightarrow \exists x \in A \text{ such that } \neg P(x)$$
$$\neg(\exists x \in A,\, P(x)) \Leftrightarrow \forall x \in A,\, \neg P(x).$$

The negation of “everything holds” is “there is at least one counterexample (反例).” The negation of “there exists” is “every candidate fails.”

→ **Related page** lecture math discrete-math

study.bem130.com

6 Example: read an inclusion relation (包含関係) logically

The statement $A \subseteq B$ means

$$\forall x,\, x \in A \Rightarrow x \in B.$$

Therefore the negation of $A \subseteq B$ is

$$\exists x \text{ such that } x \in A \text{ and } x \notin B.$$

Thus a single element (元) that belongs to A but not to B breaks the inclusion.

7 Exercise link and summary

→ **Related page** exercise math discrete-math

study.bem130.com

A proposition (命題) has a truth value, and a predicate (述語) becomes a proposition after an object is inserted. Quantification (量化) fixes the range of a variable and supports the definitions of sets (集合), relations (関係), and maps (写像).

Proof methods and counterexamples

証明法 反例

In discrete mathematics 離散数学, it is important to keep the path from definition to conclusion short. More than algebraic manipulation, the central skill is choosing which definition to expand. This page organizes basic types of proof 証明.

→ **Related page** lecture math discrete-math

study.bem130.com

1 Direct proof

直接証明

A direct proof 直接証明 starts from the assumptions, uses definitions in order, and derives the conclusion.

For example, to prove $A \subseteq C$ from $A \subseteq B$ and $B \subseteq C$, expand the definition of the inclusion relation 包含関係. Take arbitrary x and assume $x \in A$. Then $x \in B$ by $A \subseteq B$, and $x \in C$ by $B \subseteq C$. Therefore $A \subseteq C$.

2 Proof by contraposition

対偶証明

A proof by contraposition 対偶証明 proves

$$\neg Q \Rightarrow \neg P$$

instead of

$$P \Rightarrow Q.$$

The two statements are equivalent.

The injection 単射 example below previews the later chapter on maps 写像. At this point, only the condition "if $f(x) = f(y)$, then $x = y$" is being used in order to see the form of a contrapositive.

This method is often natural for proving injectivity 単射性. Saying that $f : A \to B$ is an injection 単射 means $f(x) = f(y) \Rightarrow x = y$ its contrapositive is $x \neq y \Rightarrow f(x) \neq f(y)$.

→ **Related page** lecture math discrete-math

study.bem130.com

3 Proof by contradiction 背理法

A proof by contradiction 背理法 assumes the negation of the desired conclusion and derives a contradiction.

The next example previews partial orders 半順序関係. It does not use the full later theory; it only uses the assumptions needed for this proof. A greatest element 最大元 is an element a such that $x \leq a$ for every $x \in P$, and antisymmetry 反対称性 means that $a \leq b$ and $b \leq a$ imply $a = b$.

For example, prove that if a greatest element exists, it is unique. Suppose a partially ordered set 半順序集合 P has greatest elements a and b. By the definition of greatest element, $a \leq b$ and $b \leq a$. By antisymmetry 反対称性, $a = b$. Hence two distinct greatest elements cannot exist.

In a proof by contradiction, assume the negation of the conclusion and derive a contradiction with known definitions or assumptions. If one assumes the conclusion itself, that is not a proof.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Proof by cases 場合分け

A proof by cases 場合分け is used when the object splits into finitely many exhaustive types. In set operations 集合演算, cases often come from which sets an element 元 belongs to.

For example, to prove

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

track, for arbitrary x, the truth values of $x \in A$, $x \in B$, and $x \in C$. Membership in the left side is $x \in A$ and ($x \in B$ or $x \in C$), which is equivalent to ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$).

5 Counterexample（反例）

A counterexample（反例） is one example that disproves a universal proposition.

The claim "every relation（関係） is symmetric（対称）" is false. Consider the relation on $A = \{1, 2\}$

$$R = \{(1, 2)\}.$$

Then $(1, 2) \in R$ but $(2, 1) \notin R$. Therefore R does not have symmetry（対称性）.

For a counterexample, explicitly check both that the object satisfies the assumptions and that the conclusion fails.

A counterexample（反例） must satisfy all assumptions while breaking the conclusion. An example that does not satisfy the assumptions does not show that the claim fails.

6 Exercise link and summary

→ **Related page** exercise math discrete-math

study.bem130.com

In a proof（証明）, expand definitions, make the necessary quantifiers（量化） explicit, and choose the right proof pattern. A counterexample（反例） is a powerful way to show that something fails, but the counterexample must still be checked against the assumptions.

In exercises, explicitly name whether you are using a direct proof, a contrapositive（対偶）, proof by contradiction（背理法）, proof by cases（場合分け）, or a counterexample（反例）. This makes the relation between assumptions and conclusion easier to follow.

Mathematical induction（数学的帰納法） and recursive definitions（再帰的定義）

In discrete mathematics（離散数学）, arguments often add objects one by one. Mathematical induction（数学的帰納法） turns the structure "it holds at the start, and if it can advance to the next case, then it holds everywhere" into a proof method.

Mathematical induction（数学的帰納法） is a proof method that extends a proposition along the natural numbers（自然数）. A recursive definition（再帰的定義） defines objects by giving an initial value and a rule that determines the next value from earlier values.

1 Induction form

Suppose we want to prove a proposition（命題） $P(n)$ about a natural number（自然数） n for all $n \geq n_0$. Then we prove the following two statements.

$$P(n_0)$$

$$P(k) \Rightarrow P(k+1) \quad (k \geq n_0)$$

The first statement is the base case（基底段階）, and the second statement is the induction step（帰納段階）. The temporary assumption $P(k)$ used inside the induction step is the induction hypothesis（帰納法の仮定）.

Both the base case（基底段階） and the induction step（帰納段階） are necessary. Checking several examples does not prove all n the proof needs a logical step that derives $P(n+1)$ from the assumption $P(n)$.

2 Why it works

Mathematical induction（数学的帰納法） can be understood through the domino metaphor. The base case（基底段階） says that the first domino falls. The induction step（帰納段階） says that whenever an arbitrary domino falls, the next one also falls. Therefore every domino falls.

More rigorously, induction can be understood as a principle equivalent to the well-ordering property（整列性） of the natural numbers. If some n failed to satisfy $P(n)$, there would be a smallest failing n. That smallest value cannot be the base case, and the previous case should already hold, so the induction step gives a contradiction.

The base case（基底段階） gives the first reachable point, and the induction step（帰納段階） gives the rule for moving one step forward. Repeating this rule finitely many times reaches any chosen natural number（自然数）.

3 Worked theorem: size of a power set

This example appears before the formal lecture on power sets[べき集合]. Here, $|A|$ means the number of elements（元） of A, $\mathcal{P}(A)$ means the set（集合） of all subsets（部分集合） of A, and a finite set（有限集合） is treated as a set with n elements.

We prove that if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

As the base case（基底段階）, when $n = 0$ we have $A = \emptyset$ and

$$\mathcal{P}(\emptyset) = \{\emptyset\},$$

so $|\mathcal{P}(A)| = 1 = 2^0$. It is important to state the case $n = 0$ explicitly. The empty set is not an exception; it is the starting point of the formula.

For the induction step（帰納段階）, assume that $|A| = k$ implies $|\mathcal{P}(A)| = 2^k$. Add a new element（元） $a \notin A$ and consider $A' = A \cup \{a\}$. Each subset（部分集合） of A' either does not contain a or does contain a. The subsets not containing a are exactly the subsets of A, and the subsets containing a correspond one-to-one to sets of the form $B \cup \{a\}$ with $B \subseteq A$. Therefore

$$|\mathcal{P}(A')| = 2^k + 2^k = 2^{k+1}.$$

→ **Related page** lecture math discrete-math

study.bem130.com

4 Recursive definitions

A recursive definition gives initial data and a rule for producing the next object, such as

$$a_0 = 1, \qquad a_{n+1} = 2a_n + 1$$

Specifying a_0 is necessary; the rule for producing the next term alone does not determine the values.

For a recursive definition 再帰的定義, always check the following points.

- Initial values are specified.
- The rule for producing the next object is clear.
- The range of n for which the rule is used is clear.

For a recursive definition 再帰的定義, check that neither the initial value nor the recursion rule is missing. The fact that the same initial value and rule determine a unique object can often be proved by mathematical induction 数学的帰納法.

5 Warning

The induction hypothesis is not the statement to be proved for all n at once. It is a temporary assumption for one arbitrary k, used only to prove the next case.

6 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

7 Summary

Mathematical induction（数学的帰納法） is a basic proof method for statements over the natural numbers（自然数）. Recursive definitions（再帰的定義） are used frequently when defining finite sequences, trees, graphs, and computational procedures.

Basics of sets（集合）

1 Introduction

The first question to fix when studying sets（集合） is this: what are we treating as one collection, and what are we treating as a different collection? A set is not merely a bag. It is a language for collecting objects（対象） that satisfy a condition（条件） and then reasoning by whether each object is included.

This lecture organizes elements（元）, membership（所属）, the empty set（空集合）, subsets（部分集合）, and extensionality（外延性）. If this point is vague, later topics such as relations（関係）, maps（写像）, and power sets（冪集合） become confusing because one loses track of whether something is an element or a subset.

2 Terms and definitions

A set（集合） is a collection of objects（対象）. We write

$$x \in A$$

when an object x is contained in a set A, and we call x an element（元） of A. The notation $x \notin A$ means that x is not an element of A.

The empty set（空集合） $\emptyset$ is the set with no elements. It is not a nonexistent set; it is a set whose elements do not exist.

A subset（部分集合） expresses inclusion（包含）. The statement $A \subseteq B$ means that, for every x,

$$x \in A \Longrightarrow x \in B$$

holds. Here $A \subseteq B$ allows $A = B$. The notation $A \subsetneq B$ means $A \subseteq B$ and $A \neq B$.

3 Method

When working with sets 集合, do not decide only from a picture or intuition. First take an arbitrary element 元 x and transform the condition $x \in A$ into another membership condition.

This method is simple but powerful. To prove a set equality $A = B$, it is enough to prove

$$A \subseteq B \quad \text{and} \quad B \subseteq A.$$

This checks that the two sets have exactly the same elements from both directions.

4 Intuitive explanation

It is useful to imagine a set 集合 as a collection of objects carrying a label. The statement $x \in A$ says that x has the label A. The statement $A \subseteq B$ says that every object with label A also has label B.

From this point of view, the empty set 空集合 is an empty box. Therefore it is a subset 部分集合 of every set A. There is no x with $x \in \emptyset$, so the conditional statement "if $x \in \emptyset$, then $x \in A$" has no counterexample.

5 Rigorous explanation

The identity of a set 集合 is determined by extensionality 外延性. Extensionality is the principle that if

$$x \in A \Longleftrightarrow x \in B$$

holds for every x, then $A = B$. In other words, a set is determined by its elements, not by the way it was written.

For example,

$$A = \{1, 2, 3\}, \qquad B = \{3, 2, 1, 1\}$$

still gives $A = B$. In a set, order and repetition are not recorded. If order must be recorded, use an ordered pair 順序対 or a sequence 列. If repetition must be recorded, use a multiset 多重集合.

6 Worked example: checking a subset relation from the definition

6.1 Problem

Let $A = \{2, 4, 6\}$ and $B = \{n \in \mathbb{Z} \mid n \text{ is even and } 1 \leq n \leq 6\}$. Prove $A = B$.

6.2 Explanation

A set equality is proved by proving inclusion (包含) in both directions.

First take $x \in A$. Then x is one of $2, 4, 6$. Each of these is an integer (整数), is an even number (偶数), and satisfies $1 \leq x \leq 6$. Hence $x \in B$, so $A \subseteq B$.

Conversely, take $x \in B$. Then x is an even integer satisfying $1 \leq x \leq 6$. Therefore x is one of $2, 4, 6$, so $x \in A$. Hence $B \subseteq A$.

Both inclusions hold, so $A = B$. This example checks the central point of this page: sets are compared by equality of elements, not by the surface form of their descriptions.

7 What changes and what is preserved

Operation or viewpoint	What changes	What is preserved
Rewriting in set-builder notation (内包的記法)	The form of the description	The whole collection of elements (元)
Rewriting in roster notation (外延的記法)	The way the elements are listed	The set (集合) itself
Reordering the list	The written order	The set (集合) itself
Listing an element repeatedly	The visual appearance	Whether each element (元) is present

8 How to distinguish the ideas

- If the question is whether $x \in A$, it is a question about membership.
  所属

- If the question is whether $A \subseteq B$, start from an arbitrary $x \in A$ and derive $x \in B$.

- If the question is whether $A = B$, check $A \subseteq B$ and $B \subseteq A$ separately.

- If order or repetition matters, a plain set does not contain enough information.
  集合

9 Exercise link

→ **Related page** exercise math discrete-math

study.bem130.com

10 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Set operations (集合演算) and inclusion relations (包含関係)

1 Introduction

The important point in set operations (集合演算) is not coloring regions in a diagram, but transforming the condition (条件) that an element (元) satisfies. Union (和集合) corresponds to "or", intersection (共通部分) corresponds to "and", and complement (補集合) corresponds to "not".

Once this correspondence is fixed, De Morgan's laws (ド・モルガンの法則) and the distributive law (分配法則) are not memorized rules. They are derived by transforming logical conditions.

2 Terms and definitions

For sets (集合) A, B, define union (和集合), intersection (共通部分), and set difference (差集合) by

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}, A \cap B = \{x \mid x \in A \text{ and } x \in B\}, A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}.$$

After fixing a universal set (全体集合) U, the complement (補集合) of A is

$$A^c = U \setminus A = \{x \in U \mid x \notin A\}.$$

The complement depends on which universal set is being used. If this premise is omitted, the same A can have different complements.

3 Method

To prove an identity of set operations (集合演算), take arbitrary x and translate the statement into a membership condition. For example, $x \in A \cap (B \cup C)$ means

$$x \in A \quad \text{and} \quad (x \in B \text{ or } x \in C).$$

Using the distributive law 分配法則 of logic, this becomes

$$(x \in A \text{ and } x \in B) \quad \text{or} \quad (x \in A \text{ and } x \in C),$$

which is equivalent to $x \in (A \cap B) \cup (A \cap C)$.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

A set operation 集合演算 is a way to view a combination of conditions 条件 as a set. The set $A \cup B$ consists of objects that have the label A or the label B. The set $A \cap B$ consists of objects that have both labels. The set $A \setminus B$ consists of objects that have label A but not label B.

In this view, De Morgan's laws ド・モルガンの法則

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c$$

are natural. The negation of "in A or in B" is "not in A and not in B". The negation of "in A and in B" is "not in A or not in B".

5 Rigorous explanation

The statement $A \subseteq B$ means that, for every x, $x \in A \Rightarrow x \in B$ holds. Therefore a proof of an inclusion relation 包含関係 must make the starting point and the target clear.

For example, $A \cap B \subseteq A$ is proved in one sentence: take arbitrary $x \in A \cap B$. Then $x \in A$ and $x \in B$, so in particular $x \in A$.

On the other hand, $A \subseteq A \cup B$ is proved as follows. Take arbitrary $x \in A$. Then $x \in A$ or $x \in B$ is true, so $x \in A \cup B$. Here no information about $x \in B$ is needed because an "or" statement is true when one side is true.

6 Worked example: proving De Morgan's law by elements

6.1 Problem

For subsets A, B of a universal set 全体集合 U, prove $(A \cup B)^c = A^c \cap B^c$.

6.2 Explanation

Take arbitrary $x \in U$. Then

$$x \in (A \cup B)^c \iff x \notin A \cup B.$$

By the definition of union 和集合, $x \notin A \cup B$ means that it is not true that $x \in A$ or $x \in B$. Hence

$$x \notin A \cup B \iff (x \notin A \text{ and } x \notin B).$$

This is equivalent to

$$x \in A^c \quad \text{and} \quad x \in B^c,$$

that is, $x \in A^c \cap B^c$. Since the equivalence holds for every x, extensionality 外延性 gives $(A \cup B)^c = A^c \cap B^c$.

7 What changes and what is preserved

Operation	What changes	What is preserved
$A \cup B$	The condition is weakened by "or"	All elements 元 of A and B are included
$A \cap B$	The condition is tightened by "and"	Only elements belonging to both sets remain
$A \setminus B$	Elements belonging to B are removed	No element outside A is added
A^c	The viewpoint moves outside A	The universal set 全体集合 U is fixed

8 How to distinguish the ideas

- If the condition contains "or", think of a union.
  和集合
- If the condition contains "and", think of an intersection.
  共通部分
- If the condition contains "not", think of a complement or a set difference.
  補集合 差集合
- When using a complement, first check what the universal set is.
  全体集合

9 Proof supplement: why set operations preserve inclusion

Here we prove concretely what preservation means. Assume
保存

$$A \subseteq B.$$

Then, for every set C,

$$A \cup C \subseteq B \cup C, \qquad A \cap C \subseteq B \cap C$$

hold.

To prove the first inclusion, take $x \in A \cup C$. Then $x \in A$ or $x \in C$. If $x \in A$, then $x \in B$ by $A \subseteq B$, hence $x \in B \cup C$. If $x \in C$, then again $x \in B \cup C$. Therefore $A \cup C \subseteq B \cup C$.

Next take $x \in A \cap C$. Then $x \in A$ and $x \in C$. Since $A \subseteq B$, we have $x \in B$, so $x \in B \cap C$. Therefore $A \cap C \subseteq B \cap C$.

For complements, the direction reverses. If the universal set U is fixed, then

$$A \subseteq B \implies U \setminus B \subseteq U \setminus A.$$

Indeed, if $x \in U \setminus B$, then $x \notin B$. If $x \in A$ were true, then $A \subseteq B$ would imply $x \in B$, a contradiction. Hence $x \notin A$, so $x \in U \setminus A$.

This proof is also practice in reading set operations not as symbol manipulation, but as conditions on whether an element belongs to a set.

10 Exercise link

→ **Related page** exercise math discrete-math

study.bem130.com

11 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Families of sets 集合族 and index sets 添字集合

1 Introduction

A family of sets 集合族 is introduced to handle many sets 集合 at once, not only two or three. For example, when considering the open intervals $(-1/n, 1/n)$ for $n = 1, 2, 3, \ldots$, it is clearer to write $A_n = (-1/n, 1/n)$ and treat all the A_n together.

The important point is that an index 添字 is not usually an element of the set itself; it is a label pointing to a set.

2 Terms and definitions

Given an index set 添字集合 I, if each $i \in I$ is assigned a set 集合 A_i, then $(A_i)_{i \in I}$ is called a family of sets 集合族.

The union 和集合 of the family is defined by

$$\bigcup_{i \in I} A_i = \{x \mid \text{there exists } i \in I \text{ such that } x \in A_i\}.$$

The intersection 共通部分 of the family is defined by

$$\bigcap_{i \in I} A_i = \{x \mid \text{for every } i \in I,\ x \in A_i\}.$$

3 Method

For an indexed union 添字付き和集合, look for “there exists an index.” For an indexed intersection 添字付き共通部分, check “for every index.” This difference between existence and universality determines the proof strategy.

For example, if $x \in \bigcup_{i \in I} A_i$, then there exists $i_0 \in I$ such that $x \in A_{i_0}$. In contrast, if $x \in \bigcap_{i \in I} A_i$, then $x \in A_i$ for every $i \in I$.

4 Intuitive explanation

A family of sets（集合族） can be imagined as numbered drawers, each containing a set（集合）. The union（和集合） accepts an element if it appears in at least one drawer. The intersection（共通部分） accepts an element only if it appears in every drawer.

In this view, union weakens the condition, while intersection strengthens it.

5 Precise point: the empty index set（添字集合）

The case $I = \emptyset$ is a boundary case. The union（和集合） $\bigcup_{i \in \emptyset} A_i$ is the empty set（空集合）, because there is no index $i \in \emptyset$ that can witness membership.

For the intersection（共通部分） $\bigcap_{i \in \emptyset} A_i$, if a universal set（全体集合） U is fixed, it is often taken to be U. The condition “for every $i \in \emptyset$, $x \in A_i$” has no counterexample.

6 Worked example: indexed intersection（添字付き共通部分）

6.1 Problem

Let $A_n = \{m \in \mathbb{Z} \mid n \text{ divides } m\}$. Describe $\bigcap_{n=1}^{3} A_n$ in words.

6.2 Explanation

The statement $m \in \bigcap_{n=1}^{3} A_n$ means that all of $m \in A_1$, $m \in A_2$, and $m \in A_3$ hold. In other words, m is an integer（整数） divisible by all of $1, 2, 3$.

Therefore $\bigcap_{n=1}^{3} A_n$ is the set of all multiples of 6. This example shows that intersection（共通部分） extracts elements（元） satisfying several conditions at the same time.

7 How to identify it and related links

- If many sets with the same form appear, organize them as a family of sets.
  集合 集合族
- Use $\bigcup$ for “belongs to at least one.”
- Use $\bigcap$ for “belongs to all.”
- When the index set is empty, union and intersection behave differently.
  添字集合 和集合 共通部分

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Basics of the Cartesian product

直積集合

1 Introduction

The first thing to understand about the Cartesian product 直積集合 is that it turns several choices into one ordered object. Choosing one element from A and one from B is not recorded as the unordered list a, b, but as the ordered pair 順序対 (a, b).

The order is important. In general, (a, b) and (b, a) are different objects. Therefore the Cartesian product is a common foundation for relations 関係, maps 写像, coordinates 座標, and state spaces.

2 Terms and definitions

For sets A and B, the Cartesian product 直積集合 $A \times B$ is defined by

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

Here (a, b) is an ordered pair 順序対 its first component is a and its second component is b.

More generally, for $A_1, A_2, \ldots, A_n$,

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ for every } i\}.$$

This is the set of ordered tuples [順序付き組].

3 Strategy

When working with a Cartesian product 直積集合, remember that an element is not a single unstructured value. It is an ordered pair or tuple. Thus, if $x \in A \times B$, write $x = (a, b)$ and extract the facts $a \in A$ and $b \in B$.

This strategy is used directly when studying relations 関係. A relation is a subset of $A \times B$. In other words, a relation is a choice of which ordered pairs to accept.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation: tables and counting

It is often useful to view $A \times B$ as the operation of forming rows and columns of a table. Use the elements of A as row labels and the elements of B as column labels. Each cell corresponds to one ordered pair (a, b).

For example, if $A = \{1, 2\}$ and $B = \{x, y, z\}$, then

$$A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}.$$

In this example, $\mid A \mid = 2$ and $\mid B \mid = 3$, so $\mid A \times B \mid = 6$. For finite sets, in general,

$$\mid A \times B \mid = \mid A \mid \mid B \mid .$$

There are two stages of choice: $\mid A \mid$ choices for the first component and $\mid B \mid$ choices for the second component.

5 Precise explanation

The essential equality rule for ordered pairs 順序対 is

$$(a, b) = (a', b') \iff (a = a' \text{ and } b = b').$$

This property lets us compare the first and second components separately. When proving equality or inclusion involving Cartesian products, decompose elements as ordered pairs.

The boundary case involving the empty set is also important. If $A = \emptyset$ or $B = \emptyset$, then

$$A \times B = \emptyset.$$

To make an ordered pair (a, b), both $a \in A$ and $b \in B$ are required. If one side has no elements, no ordered pair can be made.

6 Worked example: Cartesian products and order

6.1 Problem

Let $A = \{0, 1\}$ and $B = \{1, 2\}$. List $A \times B$ and $B \times A$, and confirm that they are not generally equal.

6.2 Explanation

By definition,

$$A \times B = \{(0, 1), (0, 2), (1, 1), (1, 2)\}.$$

On the other hand,

$$B \times A = \{(1, 0), (1, 1), (2, 0), (2, 1)\}.$$

For example, $(0, 1) \in A \times B$, but $(0, 1) \notin B \times A$. Therefore $A \times B \neq B \times A$.

This confirms that the Cartesian product is not just an unordered combination. It records order.

直積集合

7 What changes and what is preserved

Operation	What changes	What is preserved
switching from $A \times B$ to $B \times A$	positions of the components	the sets used as materials for selection
taking a subset of $A \times B$	which ordered pairs are accepted 順序対	each component still comes from A and B

extending to $A_1 \times \cdots \times A_n$	the number of components	each component comes from its specified set

8 Recognition criteria

- Use a Cartesian product 直積集合 when several choices are recorded simultaneously.
- If order matters, treat the result as an ordered pair 順序対.
- To define a relation 関係, first identify the ambient set $A \times B$.
- To define a map 写像, consider a subset of $A \times B$ in which, for each $a \in A$, the second component is unique.

9 Proof supplement: when products preserve inclusion

The Cartesian product 直積集合 preserves inclusion in each component. That is,

$$A \subseteq A', \quad B \subseteq B' \implies A \times B \subseteq A' \times B'.$$

Proof. Take $(a, b) \in A \times B$. This means $a \in A$ and $b \in B$. Since $A \subseteq A'$ and $B \subseteq B'$, we have $a \in A'$ and $b \in B'$. Therefore $(a, b) \in A' \times B'$.

The converse direction needs a nonempty-set condition. If $A \times B \subseteq A' \times B'$ and both A and B are nonempty, then $A \subseteq A'$ and $B \subseteq B'$. For example, take $a \in A$. Since B is nonempty, choose $b \in B$. Then $(a, b) \in A \times B \subseteq A' \times B'$, so $a \in A'$. The same argument shows $B \subseteq B'$.

If the nonempty assumption is omitted, this conclusion can fail. Since $A \times \emptyset = \emptyset$, the left-hand side may contain no information about A.

10 Exercise links

→ **Related page** exercise math discrete-math

study.bem130.com

11 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Basics of the power set

べき集合

1 Introduction

The key shift in a power set is that subsets themselves become new elements, rather than focusing only on the elements of the original set. The power set collects every possible choice of which elements of A to include.

べき集合 部分集合 元
集合

This viewpoint connects to counting, logic, state spaces, and Boolean lattices. A power set is an operation that turns a set into an object one level higher.

論理 状態空間 ブール束

2 Terms and definition

For a set A, the power set $\mathcal{P}(A)$ is defined by

集合 べき集合

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Thus the elements of $\mathcal{P}(A)$ are the subsets of A.

元 部分集合

The statements $x \in A$ and $B \in \mathcal{P}(A)$ are different kinds of statements. The first says that x is an element of A, while the second says that B is a subset of A.

3 Method: count the cardinality

個数

To understand a power set, think of two choices for each element: include it or do not include it. If A is finite and $\mid A \mid = n$, then each element gives two choices, so

べき集合 元

$$\mid \mathcal{P}(A)| = 2^n.$$

This formula is also the reason for the name “power set.”

→ **Related page** lecture math probability

study.bem130.com

4 Intuitive example

Let $A = \{a, b, c\}$. The power set（べき集合） is the collection of all results obtained by deciding whether to include each of a, b, c.

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Both $\emptyset$ and A itself are subsets（部分集合） of A, so both are elements（元） of $\mathcal{P}(A)$.

5 Precise use

By definition, $B \in \mathcal{P}(A)$ is equivalent to $B \subseteq A$. Therefore proofs about a power set（べき集合） usually begin by expanding

$$B \in \mathcal{P}(A) \iff B \subseteq A.$$

For example, if $A \subseteq C$, then $\mathcal{P}(A) \subseteq \mathcal{P}(C)$. Take arbitrary $B \in \mathcal{P}(A)$. Then $B \subseteq A$, and since $A \subseteq C$, transitivity（推移性） of inclusion（包含） gives $B \subseteq C$. Hence $B \in \mathcal{P}(C)$.

6 Boundary case: the empty set（空集合）

For $A = \emptyset$, the only subset（部分集合） of $\emptyset$ is $\emptyset$ itself. Therefore

$$\mathcal{P}(\emptyset) = \{\emptyset\}.$$

Thus $|\mathcal{P}(\emptyset)| = 1 = 2^0$, which agrees with the counting formula.

7 Worked example: decide membership（[元であること]） in a power set（べき集合）

7.1 Problem

Let $A = \{1, 2\}$. Decide the truth values of the following statements.

$$1 \in \mathcal{P}(A), \qquad \{1\} \in \mathcal{P}(A), \qquad \emptyset \in \mathcal{P}(A)$$

7.2 Explanation

The elements（元） of $\mathcal{P}(A)$ are the subsets（部分集合） of A. The object 1 is an element of A, but it is not a subset of A, so $1 \in \mathcal{P}(A)$ is false.

On the other hand, $\{1\} \subseteq A$, so $\{1\} \in \mathcal{P}(A)$ is true. Also, the empty set（空集合） is a subset of every set（集合）, so $\emptyset \in \mathcal{P}(A)$ is true.

8 The power set（べき集合） as an inclusion order（包含順序）

The formal definitions of orders（順序） and lattices（束） come later. This section is a preview, and it uses only the minimum vocabulary for the inclusion order. A least element（最小元） lies below every element, and a greatest element（最大元） lies above every element. The least upper bound（上限） of two elements is the smallest element above both, and the greatest lower bound（下限） is the largest element below both.

The set $\mathcal{P}(A)$ can be ordered by inclusion（包含） $\subseteq$. For $B, C \in \mathcal{P}(A)$, if $B \subseteq C$, we regard B as being below C.

In this order（順序）, the least element（最小元） is $\emptyset$ and the greatest element（最大元） is A. The least upper bound（上限） of B and C is $B \cup C$, and the greatest lower bound（下限） is $B \cap C$. This structure is a Boolean lattice（ブール束）.

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

9 Proof supplement: equivalence between power sets and inclusion

An important theorem is

$$A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B).$$

First assume $A \subseteq B$. If $X \in \mathcal{P}(A)$, then $X \subseteq A$. Since $A \subseteq B$, we get $X \subseteq B$, so $X \in \mathcal{P}(B)$.

Conversely, assume $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Take arbitrary $a \in A$. Then $\{a\} \subseteq A$, so $\{a\} \in \mathcal{P}(A)$. By the assumption, $\{a\} \in \mathcal{P}(B)$, hence $\{a\} \subseteq B$ and $a \in B$. Therefore $A \subseteq B$.

10 How to identify it and related links

- If a problem says to collect all subsets, think of the power set.
  部分集合 べき集合
- Translate $B \in \mathcal{P}(A)$ into $B \subseteq A$.
- Distinguish $x \in A$ from $\{x\} \in \mathcal{P}(A)$.
- For a finite set with $|A| = n$, use $|\mathcal{P}(A)| = 2^n$.
  有限集合

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

data/lecture/math/discrete-math/集合の濃度と可算性-講義.n.md md 69f8c88

Cardinality and countability of sets

濃度 可算性 集合

1 Introduction

For a finite set, we compare size by counting elements. For an infinite set, counting to the end is impossible.
集合 大きさ 元 無限集合
The key idea is: if a one-to-one correspondence can be built, the sets have the same size.

In this viewpoint, cardinality is compared using a bijection. A bijection is a correspondence with no leftovers
濃度 全単射 対応
and no overlaps, so it abstracts the act of matching elements one by one.

When comparing cardinality, use bijections rather than visual size. For infinite sets, the boundary is whether
濃度
the set can be listed and whether a diagonal argument can defeat any proposed listing.
対角線論法

Order note: the formal lectures on maps, injections, surjections, and bijections appear later. On this page,
写像 単射 全射 全単射
use the minimum needed meanings: a map assigns one output to each input, an injection has no overlaps, a surjection has no leftovers, and a bijection has neither overlaps nor leftovers.

2 Terms and definitions

Two sets A, B have the same cardinality when there exists a bijection $A \to B$.
集合 濃度 全単射

A set A is a finite set if, for some natural number n, there is a bijection between A and $\{1, 2, ..., n\}$. The case
有限集合 自然数
$n = 0$ corresponds to $A = \emptyset$.

A set A is a countable set if it is finite or has the same cardinality as the set of natural numbers $\mathbb{N}$.
可算集合 濃度 自然数

3 Method

To compare cardinalities (濃度), construct a map (写像) rather than trying to count directly. To show $|A| \leq |B|$, look for an injection (単射) from A to B. To show $|A| \geq |B|$, look for a surjection (全射) from A to B. To show $|A| = |B|$, construct a bijection (全単射).

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

The set of even natural numbers $2\mathbb{N}$ is a part of $\mathbb{N}$. However, $n \mapsto 2n$ is a bijection (全単射) from $\mathbb{N}$ to $2\mathbb{N}$. Therefore, in the sense of cardinality (濃度), $\mathbb{N}$ and $2\mathbb{N}$ have the same size.

This is where intuition for infinite sets (無限集合) differs from intuition for finite sets. For finite sets, a proper subset (真部分集合) has fewer elements. For infinite sets, a proper subset can correspond bijectively to the whole set.

5 Precise idea: entrance to the diagonal argument (対角線論法)

A countable set (可算集合) is a set (集合) that can be listed. In contrast, the interval $(0, 1)$ of real numbers (実数) is not countable.

The basic idea is Cantor's diagonal argument (対角線論法). Suppose the real numbers in $(0, 1)$ could be listed as $r_1, r_2, r_3, \ldots$. Write their decimal expansions in a table, and choose a new real number s whose i-th digit differs from the i-th digit of r_i. Then s differs from every r_i at the i-th digit, so it is not in the list.

In a diagonal argument (対角線論法), assume an arbitrary listing and construct a new object that differs from the n-th listed object at the n-th position. This construction shows that the listing is not a surjection (全射).

6 Worked example: the positive even numbers are countable 可算

6.1 Problem

Show that the set of positive even numbers $E = \{2, 4, 6, \dots\}$ has the same cardinality 濃度 as $\mathbb{N} = \{1, 2, 3, \dots\}$.

6.2 Explanation

Define $f : \mathbb{N} \to E$ by $f(n) = 2n$. If $f(n_1) = f(n_2)$, then $2n_1 = 2n_2$. Dividing by the nonzero constant 2 gives $n_1 = n_2$, so f is an injection 単射.

Take arbitrary $e \in E$. By the definition of E, there exists $n \in \mathbb{N}$ such that $e = 2n$. Therefore $f(n) = e$, so f is a surjection 全射. Hence f is a bijection 全単射, and E and $\mathbb{N}$ have the same cardinality 濃度.

7 How to identify it and related links

- To compare sizes, look for a bijection 全単射.
- To prove countability, construct a listing from the natural numbers 自然数.
- To prove uncountability, construct an element 元 missing from an arbitrary list.
- Intuition valid for finite sets may fail for infinite sets 無限集合.

→ Related page exercise math discrete-math

study.bem130.com

→ Related page lecture math discrete-math

study.bem130.com

Basics of relations

関係

1 Introduction

The central question for a relation（関係） is whether connections between objects（対象） can be recorded by choosing which ordered pairs（順序対） to include. A relation is not a vague word; it is a subset（部分集合） of a Cartesian product（直積集合）.

This definition lets statements that look different, such as “a equals b,” “a is below b,” “a divides b,” and “a has the same remainder as b,” be treated in the same form（形式）.

2 Terms and definitions

For sets（集合） A, B, a relation（関係） from A to B is a subset（部分集合） of $A \times B$.

$$R \subseteq A \times B.$$

When $(a, b) \in R$, we say that a is related to b by R, and often write

$$aRb.$$

When $A = B$, a relation $R \subseteq A \times A$ is called a binary relation（二項関係） on A. Equivalence relations（同値関係） and order relations（順序関係） are special kinds of binary relations.

3 Strategy

When studying a relation（関係）, first identify the ambient Cartesian product（直積集合）. Then identify which ordered pairs（順序対） are included.

To prove a property（性質）, check that the condition holds for all relevant elements（元）. One example cannot prove reflexivity（反射性） or transitivity（推移性）. To show failure, one counterexample（反例） is enough.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

A relation 関係 can be viewed as marking cells in a table. Each ordered pair 順序対 (a, b) in $A \times B$ corresponds to the cell at row a and column 列 b. The relation R is the set of cells judged to hold.

Changing a relation means changing which ordered pairs are included. As long as the ambient product $A \times B$ is fixed, the type is preserved: first components come from A and second components come from B.

5 Important properties 性質

For a binary relation 二項関係 R on A, consider the following properties 性質.

Property	Definition	Intuition
Reflexivity 反射性	aRa for every $a \in A$	each element is related to itself
Symmetry 対称性	aRb implies bRa	the relation holds in the reverse direction
Antisymmetry 反対称性	aRb and bRa imply $a = b$	two different elements cannot be mutually related
Transitivity 推移性	aRb and bRc imply aRc	relations can be chained

Symmetry 対称性 and antisymmetry 反対称性 have similar names, but their meanings are not opposites.

6 Worked example: check the divisibility relation 整除関係

6.1 Problem

On $A = \{1, 2, 3, 6\}$, define a relation 関係 R by letting aRb mean "a divides b." Check that R satisfies reflexivity 反射性, antisymmetry 反対称性, and transitivity 推移性.

6.2 Explanation

For reflexivity 反射性, every $a \in A$ satisfies $a = a \cdot 1$, so a divides itself. Hence aRa.

For antisymmetry 反対称性, suppose aRb and bRa. Then there are positive integers 整数 k, ℓ such that $b = ak$ and $a = b\ell$. Hence $a = ak\ell$. Since $a \in A$, $a \neq 0$, so dividing by a gives $1 = k\ell$. Because k, ℓ are positive integers, $k = \ell = 1$, and therefore $a = b$.

For transitivity 推移性, suppose aRb and bRc. Then $b = ak$ and $c = b\ell$. Thus $c = a(k\ell)$, so aRc.

7 How to identify it and related links

- If the question is whether a and b are connected, think of a relation 関係.
- If objects in the same set 集合 are compared, think of a binary relation 二項関係.
- If objects are grouped into classes, suspect an equivalence relation 同値関係.
- If objects are compared by size or order, suspect an order relation 順序関係.

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Composition 合成 and closure 閉包 of relations 関係

1 Introduction

Sometimes we do not want to check a relation 関係 only once; we want to know where repeated use of the relation can reach. For example, if direct train connections are given, we may want to know what stations are reachable with transfers. This idea is composition 合成 of relations.

A closure 閉包 is an operation that adds the minimum missing ordered pairs 順序対 needed to satisfy a property 性質.

2 Terms and definition: composition 合成

Let $R \subseteq A \times B$ and $S \subseteq B \times C$ be relations 関係. Define the composite relation 合成関係 $S \circ R \subseteq A \times C$ by

$$a(S \circ R)c \iff \text{there exists } b \in B \text{ such that } aRb \text{ and } bSc.$$

This says that we can move from a to b by R and then from b to c by S.

3 Terms and definitions: identity relation 恒等関係 and inverse relation 逆関係

For a relation 関係 R on A, the identity relation 恒等関係 is written

$$\Delta_A = \{(a, a) \mid a \in A\}.$$

The inverse relation 逆関係 R^{-1} is

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

4 What is closure 閉包?

The reflexive closure 反射閉包 adds the self-pairs (a, a) needed for reflexivity 反射性.

$$R_{\text{ref}} = R \cup \Delta_A$$

The symmetric closure 対称閉包 adds reverse ordered pairs 順序対.

$$R_{\text{sym}} = R \cup R^{-1}$$

The transitive closure 推移閉包 is the smallest transitive 推移的 relation 関係 obtained by repeatedly adding pairs aRc forced by aRb and bRc.

5 Strategy

When constructing a closure 閉包, track what must be added until the desired property 性質 holds. The original relation 関係 must not be destroyed. A closure is an adding operation, not a deleting operation.

Here a path 経路 means a finite chain that follows relation arrows, such as aRb and then bRc. The term directed graph 有向グラフ means only the viewpoint of drawing elements 元 as points and ordered pairs 順序対 as arrows.

The reflexive closure 反射閉包 adds diagonal pairs, the symmetric closure 対称閉包 adds reverse arrows, and the transitive closure 推移閉包 adds direct relation pairs for destinations reachable by paths.

Being a minimal addition 最小の追加 is also part of closure. That is, every relation 関係 that contains the original relation and satisfies the desired property must contain the ordered pairs 順序対 added by the closure.

6 Intuitive explanation

If a relation 関係 is viewed as a directed graph, composition 合成 means following two arrows in sequence. The transitive closure 推移閉包 can be thought of as adding a direct arrow whenever a destination is reachable by following some number of arrows.

In this view, the transitive closure is the relation 関係 that records reachability. The original relation means "reachable in one step," while the transitive closure means "reachable in some positive number of steps."

In terms of path length, the reflexive closure 反射閉包 allows movement of length 0, while the transitive closure 推移閉包 adds destinations reachable by paths of positive length as direct relation pairs.

7 Worked example: construct a transitive closure 推移閉包

7.1 Problem

Find the transitive closure 推移閉包 of the relation 関係 $R = \{(1, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$.

7.2 Explanation

Because $1R2$ and $2R3$, transitivity 推移性 requires $1R3$. Therefore add $(1, 3)$.

The resulting relation 関係 is

$$R^+ = \{(1, 2), (2, 3), (1, 3)\}.$$

No further ordered pair 順序対 is forced, so this is the transitive closure 推移閉包.

8 Proof supplement: minimality of the transitive closure 推移閉包

Think of the transitive closure 推移閉包 of a relation 関係 R as

$$R^+ = R \cup R^2 \cup R^3 \cup \cdots,$$

where R^n is the relation obtained by composing R with itself n times.

The relation R^+ contains R. Also, if $(a, b) \in R^+$ and $(b, c) \in R^+$, then for some $m, n \geq 1$, $(a, b) \in R^m$ and $(b, c) \in R^n$. Concatenating the paths gives $(a, c) \in R^{m+n}$, so $(a, c) \in R^+$.

Finally, if S is any transitive relation with $R \subseteq S$, induction gives $R^n \subseteq S$ for every n. Hence $R^+ \subseteq S$, so R^+ is the smallest transitive relation containing R.

9 How to identify it and related links

- If a relation is used repeatedly, think of composition.
  合成
- If missing self-loops are added, it is the reflexive closure.
  反射閉包
- If reverse arrows are added, it is the symmetric closure.
  対称閉包
- If reachability is recorded as a direct relation, it is the transitive closure.
  関係 推移閉包

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Equivalence relations and partitions
同値関係 分割

1 Introduction

The purpose of an equivalence relation 同値関係 is to classify objects 対象 by a rule that says when they should be treated as the same. The point is not that the objects are literally equal, but that they are the same for the purpose currently being considered.

For example, if integers are classified by their remainder when divided by 3, then $1, 4, 7$ belong to the same class. This does not mean $1 = 4$. It means they are the same as long as only the remainder modulo 3 is being observed.

2 Terms and definitions

A binary relation 二項関係 $\sim$ on a set 集合 A is an equivalence relation 同値関係 if it satisfies the following three conditions.

Condition	Formula	Meaning
reflexivity 反射性	$a \sim a$	every element is equivalent to itself
symmetry 対称性	$a \sim b \Rightarrow b \sim a$	being equivalent has no direction
transitivity 推移性	$a \sim b, b \sim c \Rightarrow a \sim c$	a chain of equivalences remains an equivalence

For $a \in A$, the equivalence class 同値類 of a is defined by

$$[a] = \{x \in A \mid x \sim a\}.$$

An equivalence class is the set of elements regarded as the same kind as a.

A partition 分割 of A is a collection of nonempty subsets of A that are pairwise disjoint and whose union is all of A. The subsets in the partition are often called blocks.

3 Strategy

To verify an equivalence relation 同値関係, prove the three conditions separately. In particular, transitivity 推移性 is easy to miss: from $a \sim b$ and $b \sim c$, one must be able to derive $a \sim c$.

The reason to introduce an equivalence relation is to divide a set into equivalence classes. Therefore, before asking what changes, ask what feature is being ignored so that objects are identified.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

An equivalence relation 同値関係 can be imagined as coloring the elements of a set. Elements with the same color are treated as equivalent. Reflexivity 反射性 means every element has some color, symmetry 対称性 means sameness of color has no direction, and transitivity 推移性 means the color does not change in the middle of a chain.

When this coloring is valid, the set is divided into non-overlapping subsets. That division is a partition 分割.

5 Precise explanation: from equivalence relations to partitions

Suppose an equivalence relation 同値関係 $\sim$ is given on A. The collection of equivalence classes forms a partition 分割 of A. This means two things.

1. Every $a \in A$ belongs to at least one equivalence class.

2. Any two equivalence classes are either equal or disjoint.

The first point follows from reflexivity 反射性. Since $a \sim a$, we have $a \in [a]$.

For the second point, suppose $[a] \cap [b] \neq \emptyset$. Then there exists x such that $x \in [a]$ and $x \in [b]$. By definition, $x \sim a$ and $x \sim b$. By symmetry 対称性, $a \sim x$, and by transitivity 推移性, $a \sim b$.

Now take any $y \in [a]$. Then $y \sim a$. Since $a \sim b$, transitivity gives $y \sim b$, so $y \in [b]$. Hence $[a] \subseteq [b]$. The same argument gives $[b] \subseteq [a]$, so $[a] = [b]$.

6 Conversely, from partitions to equivalence relations

Let a partition 分割 of A be given. Define $a \sim b$ to mean that a and b belong to the same block of the partition. Then $\sim$ is an equivalence relation 同値関係.

Reflexivity 反射性 holds because every element belongs to some block. Symmetry 対称性 holds because the statement "belong to the same block" is symmetric in a and b. Transitivity 推移性 holds because distinct blocks of a partition do not overlap: if a, b are in the same block and b, c are in the same block, then those two blocks share b and therefore must be the same block, so a, c are in the same block.

7 Example: equivalence by congruence

7.1 Problem

On the set of all integers $\mathbb{Z}$, define $a \sim b$ to mean that $a - b$ is a multiple of 3. Verify that this is an equivalence relation 同値関係 and describe the equivalence classes 同値類.

7.2 Explanation

For reflexivity 反射性, $a - a = 0$ is a multiple of 3, so $a \sim a$.

For symmetry 対称性, suppose $a \sim b$. Then $a - b = 3k$ for some integer k. Hence $b - a = -3k = 3(-k)$, so $b \sim a$.

For transitivity 推移性, suppose $a \sim b$ and $b \sim c$. Then $a - b = 3k$ and $b - c = 3\ell$ for integers k, ℓ. Adding the two equations gives $a - c = 3(k + \ell)$, so $a \sim c$.

The equivalence classes are the classes according to remainders modulo 3:

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$
$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$
$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

This example shows how an equivalence relation 同値関係 decomposes a set into non-overlapping classes.

→ **Related page** lecture math abstract-algebra

study.bem130.com

8 Recognition criteria

- Use an equivalence relation 同値関係 when objects should be divided into classes of the same kind.
- To prove that a relation is an equivalence relation, check reflexivity 反射性, symmetry 対称性, and transitivity 推移性 separately.
- An equivalence class 同値類 is not a chosen representative. It is the set of all elements equivalent to the representative.
- When a partition 分割 appears, one can define an equivalence relation by saying that two elements are in the same block.

9 Proof supplement: equivalence relations and partitions are the same data

From an equivalence relation 同値関係, form the collection of equivalence classes

$$X/\sim = \{[x] \mid x \in X\}.$$

This is a partition 分割 of X. First, by reflexivity, $x \sim x$, so $x \in [x]$. Therefore every element lies in at least one class.

Next, suppose two equivalence classes $[x]$ and $[y]$ intersect. Take $z \in [x] \cap [y]$. Then $z \sim x$ and $z \sim y$. By symmetry, $x \sim z$ by transitivity, $x \sim y$. If $u \in [x]$, then $u \sim x \sim y$, so $u \in [y]$. The same argument gives $[y] \subseteq [x]$. Hence $[x] = [y]$.

Conversely, let $\mathcal{C}$ be a partition of X. Define $x \sim y$ to mean that x and y belong to the same block. Each element belongs to a block, so reflexivity holds. The condition is symmetric, so symmetry holds. If x, y are in the same block and y, z are in the same block, then the two blocks intersect at y, and because blocks of a partition do not overlap, they are the same block. Therefore x, z are in the same block, so transitivity holds.

10 Exercise links

→ **Related page** exercise math discrete-math

study.bem130.com

11 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math abstract-algebra

study.bem130.com

Quotient sets（商集合） and the canonical projection（自然な射影）

1 Introduction

After classifying objects（対象） by an equivalence relation（同値関係）, the next question is whether the resulting boxes themselves can be treated as elements（元）. This idea is the quotient set（商集合）.

In a quotient set, individual elements are replaced by equivalence classes（同値類） as the new objects. In other words, it forgets fine distinctions and collapses equivalent objects to the same point（点）.

2 Terms and definitions

For an equivalence relation（同値関係） $\sim$ on a set（集合） A, define the quotient set（商集合） $A/\sim$ by

$$A/\sim = \{[a] \mid a \in A\}.$$

Here $[a]$ is the equivalence class（同値類） of a.

Order note: the formal lecture on maps（写像） appears later. On this page, $\pi : A \to A/\sim$ is used only in the minimal sense of a rule assigning $[a]$ to each $a \in A$.

The canonical projection（自然な射影） $\pi : A \to A/\sim$ is defined by

$$\pi(a) = [a].$$

It is the map（写像） sending each element（元） to the equivalence class containing it.

3 Strategy

When working with a quotient set（商集合）, distinguish a representative（代表元） from an equivalence class（同値類）. The object a is an element（元） of A, while $[a]$ is an element of $A/\sim$.

When defining a map (写像) on a quotient set, check well-definedness (well-defined 性). Even if the same equivalence class is written using a different representative, the defined value (値) must not change.

As a procedure, first check that the relation is an equivalence relation (同値関係), and then form the equivalence classes (同値類). The canonical projection (自然な射影) sends each element (元) to the equivalence class containing it.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

A quotient set (商集合) is the set of the boxes produced by classification. The canonical projection (自然な射影) sends each element (元) to “the box it belongs to.”

For example, if integers are classified by remainders modulo 3, the quotient set is

$$\mathbb{Z}/\sim = \{[0], [1], [2]\}.$$

Here $[1] = [4] = [-2]$. The representatives (代表元) differ, but the equivalence class (同値類) they denote is the same.

It is useful to think of an equivalence class (同値類) as a box. One may compute using a chosen representative (代表元), but one must check that the result does not depend on which representative was chosen; this is the check of well-definedness (well-defined 性).

5 What is well-definedness (well-defined 性)?

In a quotient set (商集合), one element (元) can be written using several representatives (代表元). Therefore, when defining something like $F([a])$, one must check that if $a \sim b$, then $F([a]) = F([b])$.

This check is the check of well-definedness (well-defined 性). If well-definedness fails, the same element of the quotient set can receive different values (値) depending on the chosen representative.

To prove well-definedness（well-defined 性）, take two equivalent representatives and prove that the values or equivalence classes obtained from them are the same. Computing with only one representative is not enough.

6 Worked example: the canonical projection（自然な射影）

6.1 Problem

On $\mathbb{Z}$, define $a \sim b$ to mean that $a - b$ is a multiple of 3. Find $\pi(5)$ and $\pi(-1)$ for the canonical projection（自然な射影） $\pi : \mathbb{Z} \to \mathbb{Z}/\sim$.

6.2 Explanation

The canonical projection（自然な射影） is $\pi(a) = [a]$. Therefore

$$\pi(5) = [5].$$

Since $5 \sim 2$ and $5 \sim -1$, this is the same equivalence class（同値類） as $[2]$ and $[-1]$.

Also

$$\pi(-1) = [-1],$$

and $[-1] = [2] = [5]$. Therefore $\pi(5) = \pi(-1)$. This example shows that the canonical projection collapses equivalent elements（元） to the same equivalence class.

7 How to identify it and related links

- If boxes formed by an equivalence relation（同値関係） are treated as elements（元）, think of a quotient set（商集合）.
- Distinguish a from $[a]$. The former is an element of the original set（集合）, while the latter is an element of the quotient set.
- If a map（写像） on a quotient set is defined using representatives, check well-definedness（well-defined 性）.

- The canonical projection sends each element to its equivalence class.
  自然な射影 同値類

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math abstract-algebra

study.bem130.com

Partial orders (半順序関係) and total orders (全順序関係)

1 Introduction

For an order relation (順序関係), the first point is to separate what it means for two objects to be comparable. In ordinary numerical order, any two numbers can usually be compared. In inclusion (包含) of sets or divisibility (整除) of integers, two objects need not be comparable.

This distinction leads to partial orders (半順序関係) and total orders (全順序関係). A partial order compares the pairs that the structure allows us to compare. A total order requires every pair of elements to be comparable.

2 Terms and definitions

A binary relation (二項関係) $\leq$ on a set (集合) P is a partial order (半順序関係) if it satisfies the following three conditions.

Condition	**Formula**	**Meaning**
Reflexivity (反射性)	$a \leq a$	each element is below itself
Antisymmetry (反対称性)	$a \leq b, b \leq a \Rightarrow a = b$	mutual comparison forces equality
Transitivity (推移性)	$a \leq b, b \leq c \Rightarrow a \leq c$	the order can be relayed through an intermediate element

If $a \leq b$ or $b \leq a$ holds, then a and b are comparable (比較可能). If every two elements of a partially ordered set (半順序集合) are comparable, the order is a total order (全順序関係).

3 Method

To prove that a relation is a partial order 半順序関係, check reflexivity, antisymmetry, and transitivity separately. These three checks are the partial-order part.

After that, check whether every pair of elements is comparable. If yes, the order is total. If not, it remains a partial order but is not total.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

A total order 全順序関係 is an order that can be placed in one line. The usual order $\leq$ on real numbers is total because, for any a, b, either $a \leq b$ or $b \leq a$.

A partial order 半順序関係 allows branching. The sets $\{1, 2\}$ and $\{1, 3\}$ are not comparable by inclusion, because neither contains the other. However, $\{1\} \subseteq \{1, 2\}$ is comparable. Thus inclusion is a partial order, but not usually a total order.

5 Representative examples

5.1 1. Inclusion order on a power set

On $\mathcal{P}(A)$, define $B \leq C$ by $B \subseteq C$. This is a partial order 半順序関係. Reflexivity is $B \subseteq B$ antisymmetry is the fact that $B \subseteq C$ and $C \subseteq B$ imply $B = C$ transitivity is the fact that $B \subseteq C$ and $C \subseteq D$ imply $B \subseteq D$.

It is not usually total. If $A = \{1, 2, 3\}$, the sets $\{1, 2\}$ and $\{1, 3\}$ are not comparable.

→ Related page lecture math discrete-math

study.bem130.com

5.2 2. Divisibility order on positive integers

On the positive integers, define $a \le b$ to mean that a divides b. This is a partial order 半順序関係. But 2 and 3 do not divide each other, so they are not comparable. Therefore divisibility is not a total order.

5.3 3. Usual numerical order

The usual order $\le$ on $\mathbb{R}$ is a total order 全順序関係 because for all $a, b \in \mathbb{R}$, either $a \le b$ or $b \le a$.

6 Worked example: partial but not total

6.1 Problem

Let $A = \{1, 2, 3\}$, and define an order on $\mathcal{P}(A)$ by

$$B \le C \iff B \subseteq C.$$

Show that this is a partial order 半順序関係 but not a total order 全順序関係.

6.2 Explanation

Reflexivity holds because $B \subseteq B$ for every $B \in \mathcal{P}(A)$.

Antisymmetry holds because $B \subseteq C$ and $C \subseteq B$ imply $B = C$ by extensionality 外延性 of sets.

Transitivity holds because $B \subseteq C$ and $C \subseteq D$ imply $B \subseteq D$. Thus inclusion on $\mathcal{P}(A)$ is a partial order.

However, $\{1, 2\}$ and $\{1, 3\}$ are not comparable because neither contains the other. Hence the order is not total.

7 Recognition criteria

- If the comparison relation satisfies reflexivity（反射性）, antisymmetry（反対称性）, and transitivity（推移性）, suspect a partial order（半順序関係）.
- If every two elements（元） are comparable, the order is a total order（全順序関係）.
- A single incomparable pair is enough to show that an order is not a total order（全順序関係）.
- Do not confuse an equivalence relation（同値関係） with an order relation. Equivalence relations use symmetry（対称性）, while order relations use antisymmetry（反対称性）.

8 Proof supplement: restricting an order to a subset preserves the order

Let $(X, \le)$ be a partially ordered set（半順序集合）, and let $Y \subseteq X$. Define a relation on Y by

$$y_1 \underset{Y}{\le} y_2 \iff y_1 \le y_2.$$

Then $(Y, \underset{Y}{\le})$ is also a partially ordered set（半順序集合）.

Reflexivity（反射性） follows because every $y \in Y$ is also an element of X, so $y \le y$ holds in X. Antisymmetry（反対称性） follows because $y_1 \underset{Y}{\le} y_2$ and $y_2 \underset{Y}{\le} y_1$ mean $y_1 \le y_2$ and $y_2 \le y_1$ in X, hence $y_1 = y_2$. Transitivity（推移性） is inherited in the same way from X.

Furthermore, if $(X, \le)$ is a totally ordered set（全順序集合）, then $(Y, \underset{Y}{\le})$ is also totally ordered, because any two elements of Y are also elements of X and are therefore comparable.

This proof shows that restricting an order to a smaller set（集合） does not break the order axioms.

9 Exercise links

→ Related page exercise math discrete-math

study.bem130.com

10 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Hasse diagrams, maximal elements, and minimal elements

Hasse 図 極大元 極小元

1 Introduction

In a partially ordered set 半順序集合, not every two elements 元 have to be comparable. Therefore the structure is often easier to see by drawing vertical order information instead of forcing all elements into one line. This drawing is a Hasse diagram Hasse 図.

The terms maximal element 極大元 and greatest element 最大元, and likewise minimal element 極小元 and least element 最小元, are easy to confuse. A Hasse diagram makes the difference visible.

2 Terms and definitions

For a partially ordered set 半順序集合 $(P, \leq)$, the notation $a < b$ means $a \leq b$ and $a \neq b$.

If $a < b$ and there is no $c \in P$ such that $a < c < b$, then b covers 被覆 a. In a Hasse diagram Hasse 図, only this cover relation 被覆関係 is drawn, smaller elements 元 are placed lower, and larger elements are placed higher.

3 Maximal, greatest, minimal, and least

A maximal element 極大元 is an element 元 with no strictly larger element above it. A greatest element 最大元 is an element m such that $x \leq m$ for every $x \in P$.

A minimal element 極小元 is an element with no strictly smaller element below it. A least element 最小元 is an element m such that $m \leq x$ for every $x \in P$.

4 Method

When drawing a Hasse diagram (Hasse 図), do not draw every comparison relation (比較関係). Omit the lines forced by transitivity (推移性) and keep only the cover relations (被覆関係).

This omission reduces the visible number of edges, but it preserves the reachable up-down structure of the partial order (半順序関係).

→ **Related page** lecture math discrete-math

study.bem130.com

5 Intuitive explanation

A greatest element (最大元) is one element (元) above every element. A maximal element (極大元) is an element from which you cannot move upward. Thus there may be several maximal elements, but if a greatest element exists, it is unique.

The lower side is analogous. A least element (最小元) is one element below every element, while a minimal element (極小元) is an element from which you cannot move downward.

6 Worked example: maximal elements (極大元) and greatest elements (最大元)

6.1 Problem

Order $P = \{\{1\}, \{2\}, \{1,2\}, \{1,3\}\}$ by inclusion (包含) $\subseteq$. Find the maximal elements (極大元) and the greatest element (最大元).

6.2 Explanation

The set $\{1, 2\}$ contains $\{1\}$, and $\{1, 3\}$ also contains $\{1\}$. However, $\{1, 2\}$ and $\{1, 3\}$ do not contain each other, so they are incomparable.

There is no element 元 of P strictly larger than $\{1, 2\}$, and likewise none strictly larger than $\{1, 3\}$. Therefore the maximal elements 極大元 are $\{1, 2\}$ and $\{1, 3\}$.

A greatest element 最大元 would have to contain every element of P. Since $\{1, 2\}$ does not contain $\{1, 3\}$ and $\{1, 3\}$ does not contain $\{1, 2\}$, no greatest element exists.

7 How to tell them apart

- A greatest element 最大元 must be above every element 元.
- A maximal element 極大元 only has to have no strictly larger element above it.
- A least element 最小元 must be below every element.
- A minimal element 極小元 only has to have no strictly smaller element below it.
- A Hasse diagram Hasse 図 omits edges implied by transitivity 推移性.

8 Exercise and related links

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

data/lecture/math/discrete-math/順序同型と整列順序-講義.n.md md 0e62ee4

Order isomorphisms and well-orders

順序同型 整列順序

The purpose of studying partial orders 半順序関係 is to treat size and comparison not only as numerical values, but also as structure. The important ideas here are maps 写像 that preserve order and order isomorphisms 順序同型, which express that two order structures are essentially the same.

For an order isomorphism 順序同型, look not at the names or representations of elements, but at whether the comparison relation itself is the same. For a well-order 整列順序, every nonempty subset 部分集合, not just the whole set, is required to have a least element 最小元.

→ **Related page** lecture math discrete-math

study.bem130.com

1 Order-preserving maps

Order note: the formal lectures on maps 写像 and bijections 全単射 appear later. On this page, use a map as a rule assigning one destination to each element, and use a bijection as a correspondence with neither overlaps nor leftovers.

For partially ordered sets 半順序集合 P, Q, a map 写像 $f : P \to Q$ is an order-preserving map 順序保存写像 if

$$x \underset{P}{\leq} y \Rightarrow f(x) \underset{Q}{\leq} f(y).$$

This means that the map does not destroy comparable relationships. It does not have to preserve the names of elements or numerical distances. What it preserves is the order 順序.

2 Order isomorphism

A map 写像 $f : P \to Q$ is an order isomorphism 順序同型 if it is a bijection 全単射 and

$$x \underset{P}{\leq} y \Leftrightarrow f(x) \underset{Q}{\leq} f(y).$$

When an order isomorphism（順序同型） exists, P and Q are the same as order structures. Even if the element names are different, the information about which element is below which other element corresponds perfectly.

→ **Related page** lecture math discrete-math

study.bem130.com

3 Chains and antichains

A chain（鎖） is a subset（部分集合） in which every two elements are comparable. An antichain（反鎖） is a subset in which any two distinct elements are incomparable.

If the power set（冪集合） $\mathcal{P}(\{1,2\})$ is ordered by inclusion, then

$$\emptyset \subseteq \{1\} \subseteq \{1,2\}$$

is a chain（鎖）. On the other hand,

$$\{1\},\ \{2\}$$

is an antichain（反鎖）, because neither set contains the other.

In a chain（鎖）, every two elements are comparable. In an antichain（反鎖）, any two distinct elements are incomparable. Only comparisons inside the chosen subset matter.

4 Well-orders

A totally ordered set（全順序集合） P is a well-order（整列順序） if every nonempty subset（部分集合） has a least element（最小元）.

The natural numbers（自然数） $\mathbb{N}$ with the usual order are well-ordered. On the other hand, the integers（整数） $\mathbb{Z}$ with the usual order form a totally ordered set（全順序集合）, but not a well-order（整列順序）, because $\mathbb{Z}$ itself has no least element.

A well-order（整列順序） is a stronger condition than a total order（全順序）. It is not enough for the whole set to have a least element; every nonempty subset must have a least element.

5 What we are viewing without changing

An order-preserving map (順序保存写像) preserves the direction of order. An order isomorphism (順序同型) preserves order-theoretic properties such as comparability, greatest elements, least elements, upper bounds, lower bounds, joins, and meets.

The joins (結び) and meets (交わり) listed here are defined formally in the next lecture on lattices (束). At this point, they are only being named in advance as examples of properties determined by the order alone.

Conversely, element names, concrete representations, and numerical distances are not what is being preserved.

In particular, if $f : P \to Q$ is an order isomorphism (順序同型), then greatest elements, least elements, maximal elements, minimal elements, upper bounds, lower bounds, chains, antichains, joins, and meets are preserved. For example, if g is greatest in P, then for every $q \in Q$ there is $p \in P$ with $f(p) = q$, and $p \underset{P}{\leq} g$ gives $q = f(p) \underset{Q}{\leq} f(g)$. Thus $f(g)$ is greatest in Q.

What an order isomorphism (順序同型) preserves is order-theoretic structure such as comparison, maximal elements (極大元), greatest elements (最大元), upper bounds (上界), and lower bounds (下界). Numerical differences and element names are not the preserved data.

6 Exercise links

→ **Related page** exercise math discrete-math

study.bem130.com

7 Summary

Order isomorphism 順序同型 expresses that two order structures are essentially the same. A well-order 整列順序 is an order structure that supports induction 帰納法 and minimal-counterexample arguments.

An order isomorphism 順序同型 says that the order structure stays the same after renaming elements. A well-order 整列順序 is the strong order condition that every nonempty subset has a least element.

8 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** exercise math discrete-math

study.bem130.com

data/lecture/math/discrete-math/束の基本-講義.n.md md abdd845

Basics of lattices

束

1 Introduction

The central idea of a lattice (束) is that, in a partially ordered set (半順序集合), any two elements (元) have a best common upper element and a best common lower element. These are called the join (結び) and the meet (交わり).

In a total order (全順序関係), the larger and smaller of two objects are determined immediately. In a partial order (半順序関係), two objects may be incomparable. Even then, if there is a best candidate above both and a best candidate below both, a lattice (束) structure is present.

For a lattice (束), every pair of elements must have both a join (結び) and a meet (交わり). A partially ordered set is not automatically a lattice; one must check whether the best upper and lower bounds exist.

The words "larger" and "smaller" do not always mean ordinary numerical size. In an inclusion order (包含順序) they mean being a larger or smaller set, and in a divisibility order (整除順序) they mean divisibility. Therefore the join and meet must always be read from the order being used.

2 Terms and definitions

Let $(P, \leq)$ be a partially ordered set (半順序集合). An upper bound (上界) of $a, b \in P$ is an element $u \in P$ such that

$$a \leq u, \qquad b \leq u.$$

A least upper bound (最小上界) of a and b is the smallest element among their upper bounds. It is called the join (結び) and is written

$$a \vee b.$$

A lower bound (下界) of $a, b \in P$ is an element $l \in P$ such that

$$l \leq a, \qquad l \leq b.$$

A greatest lower bound（最大下界） of a and b is the largest element among their lower bounds. It is called the meet（交わり） and is written

$$a \wedge b.$$

A partially ordered set is a lattice（束） if every pair of elements has both a join and a meet.

Distinguish an upper bound（上界） from a least upper bound（最小上界）, and a lower bound（下界） from a greatest lower bound（最大下界）. When there are several candidates, the join or meet is the best one with respect to the order.

3 Strategy

To check whether a partially ordered set is a lattice（束）, do not look only for ordinary maximum and minimum. For every pair a, b, check the set of common upper bounds and the set of common lower bounds. If the upper bounds have a least element and the lower bounds have a greatest element for every pair, the poset is a lattice.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

The join（結び） $a \vee b$ is the smallest element that is still above both a and b. The meet（交わり） $a \wedge b$ is the largest element that is still below both a and b.

For sets（集合） ordered by inclusion, "above" means "contains." Therefore the smallest set containing both sets is their union（和集合）, and the largest set contained in both is their intersection（共通部分）. For positive integers（整数） ordered by divisibility, "above" means "is a multiple of," so join becomes least common multiple and meet becomes greatest common divisor.

5 Examples

5.1 1. Powersets ordered by inclusion

For a set A, the power set [べき集合] $\mathcal{P}(A)$ is ordered by inclusion $\subseteq$. For $B, C \subseteq A$,

$$B \vee C = B \cup C, \qquad B \wedge C = B \cap C.$$

Thus $(\mathcal{P}(A), \subseteq)$ is a lattice 束. Moreover, $\emptyset$ is the least element 最小元 and A is the greatest element 最大元. This is a basic example of a Boolean lattice [ブール束].

→ **Related page** lecture math discrete-math

study.bem130.com

5.2 2. Positive integers ordered by divisibility

For positive integers, define $a \leq b$ to mean that a divides b. In this order, $a \vee b$ is the least common multiple 最小公倍数, and $a \wedge b$ is the greatest common divisor 最大公約数.

For example, for 6 and 10, the upper bounds are common multiples of 6 and 10, and the least one is 30. Hence $6 \vee 10 = 30$. The lower bounds are common divisors of 6 and 10, and the greatest one is 2. Hence $6 \wedge 10 = 2$.

6 Worked example: finding join and meet in inclusion order

6.1 Problem

Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$, and $C = \{2, 3\}$. Find $B \vee C$ and $B \wedge C$ in $(\mathcal{P}(A), \subseteq)$.

6.2 Explanation

In the inclusion order 包含順序, the join 結び is union. Therefore

$$B \vee C = B \cup C = \{1, 2, 3\}.$$

This is the smallest set containing both B and C.

The meet 交わり is intersection. Therefore

$$B \wedge C = B \cap C = \{2\}.$$

This is the largest set contained in both B and C.

This example confirms that the abstract definition of a lattice 束 corresponds to the set operations $\cup$ and $\cap$ in the powerset ordered by inclusion.

7 What changes and what is preserved

Viewpoint	What changes	What is preserved
Looking at a partially ordered set 半順序集合	incomparable pairs are allowed	reflexivity 反射性, antisymmetry 反対称性, transitivity 推移性
Looking at a lattice 束	every pair is required to have a join and a meet	the partial order 半順序関係
Looking at a Boolean lattice ［ブール束］	complements 補集合 are also considered	the lattice structure given by union and intersection

An order isomorphism 順序同型 preserves comparison, so if a join 結び or meet 交わり exists, its corresponding element has the same role on the other side. What is preserved is not a numerical value, but the optimality determined by the order.

8 Recognition criteria

- If every pair has a least upper bound 最小上界 and a greatest lower bound 最大下界, the poset is a lattice 束.
- In the inclusion order 包含順序, join is ∪ and meet is ∩.
- In the divisibility order 整除順序, join is least common multiple and meet is greatest common divisor.
- In a total order 全順序関係, the larger of two elements is their join and the smaller is their meet.

To decide whether a poset is a lattice 束, check arbitrary pairs, not only representative examples. If even one pair lacks a join 結び or a meet 交わり, that partially ordered set is not a lattice.

9 Proof supplement: monotonicity of meet and join

In a lattice 束, if $a \le b$, then

$$a \wedge c \le b \wedge c, \qquad a \vee c \le b \vee c.$$

This means that meet and join preserve order.

First prove the statement for meet. The element $a \wedge c$ is a lower bound of a and c, so $a \wedge c \le a$ and $a \wedge c \le c$. Since $a \le b$, we also have $a \wedge c \le b$. Hence $a \wedge c$ is a lower bound of b and c. Because $b \wedge c$ is the greatest lower bound of b and c, it follows that $a \wedge c \le b \wedge c$.

The join statement is proved dually 双対的. The element $b \vee c$ is an upper bound of b and c. Since $a \le b \le b \vee c$ and $c \le b \vee c$, it is also an upper bound of a and c. Because $a \vee c$ is the least upper bound of a and c, we get $a \vee c \le b \vee c$.

10 Exercise links

→ **Related page** exercise math discrete-math

study.bem130.com

11 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

data/lecture/math/discrete-math/ブール代数の基本-講義.n.md md 98cb7db

Basics of Boolean algebra

ブール代数

Boolean algebra (ブール代数) is a structure for treating logic (論理) and set operations (集合演算) in the same formal shape. The propositional operations “and,” “or,” and “not” correspond to intersection (共通部分), union (和集合), and complement (補集合) of sets (集合).

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

1 Correspondence between propositions and sets

Fix a universal set (全体集合) U, and let the truth set (真理集合) of a predicate $P(x)$ be

$$S_P = \{x \in U \mid P(x)\}.$$

Then logical operations and set operations correspond as follows.

Logic	Set
$P \land Q$	$S_P \cap S_Q$
$P \lor Q$	$S_P \cup S_Q$
$\neg P$	$U \setminus S_P$
$P \Rightarrow Q$	$S_P \subseteq S_Q$
$P \Leftrightarrow Q$	$S_P = S_Q$

This correspondence lets us read transformations of logical formulas as set operations (集合演算).

2 A power set（冪集合） is a Boolean algebra（ブール代数）

For any set U, the power set（冪集合） $\mathcal{P}(U)$ becomes a Boolean algebra using the inclusion order, union, intersection, and complement.

$$X \vee Y = X \cup Y$$
$$X \wedge Y = X \cap Y$$
$$\neg X = U \setminus X$$

Here $\vee$ corresponds to join（結び）, and $\wedge$ corresponds to meet（交わり）.

→ **Related page** lecture math discrete-math

study.bem130.com

3 De Morgan's laws（ド・モルガンの法則）

De Morgan's laws（ド・モルガンの法則） say that negation interchanges "and" and "or."

In logic,

$$\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$$

and for sets,

$$U \setminus (A \cap B) = (U \setminus A) \cup (U \setminus B)$$
$$U \setminus (A \cup B) = (U \setminus A) \cap (U \setminus B).$$

4 What is being abstracted

Boolean algebra（ブール代数） temporarily ignores whether the objects are propositions or sets, and focuses only on the laws satisfied by the operations. The preserved structure concerns joins（結び）, meets（交わり）, complements（補元）, greatest elements, and least elements.

This abstraction lets logical circuits, families of sets, conditional branches, and search conditions be handled by the same formal rules.

The point is that even after replacing concrete propositions（命題）or sets（集合）, calculations use the same laws for joins（結び）, meets（交わり）, and complements（補元）. We are looking at the structure preserved by the operations, not at the objects themselves.

5 Proof supplement: uniqueness of complements（補元）

In a Boolean algebra（ブール代数）, the complement（補元）of x is unique. Suppose y and z are both complements of x, meaning

$$x \wedge y = 0, \quad x \vee y = 1, \qquad x \wedge z = 0, \quad x \vee z = 1.$$

Then

$$y = y \wedge 1 = y \wedge (x \vee z) = (y \wedge x) \vee (y \wedge z) = 0 \vee (y \wedge z) = y \wedge z \leq z.$$

The same argument gives $z \leq y$, so antisymmetry（反対称性）implies $y = z$.

6 Proof supplement: De Morgan's laws（ド・モルガンの法則）

Using uniqueness of complements（補元）, De Morgan's laws（ド・モルガンの法則）can be proved cleanly. For example, it is enough to show that $x' \vee y'$ is a complement of $x \wedge y$.

$$(x \wedge y) \wedge (x' \vee y') = ((x \wedge y) \wedge x') \vee ((x \wedge y) \wedge y') = 0,$$
$$(x \wedge y) \vee (x' \vee y') = (x \vee x' \vee y') \wedge (y \vee x' \vee y') = 1.$$

Therefore uniqueness of complements gives

$$(x \wedge y)' = x' \vee y'.$$

The same method gives $(x \vee y)' = x' \wedge y'$.

7 Exercise link and summary

→ **Related page** exercise math discrete-math

study.bem130.com

Boolean algebra is a structure connecting logic and set operations. The power set is the most basic Boolean
ブール代数 論理 集合演算 冪集合
algebra, and De Morgan’s laws are central calculation laws in it.
ド・モルガンの法則

Basics of maps (写像)

1 Introduction

The first question for a map (写像) is whether each input (入力) determines a unique output (出力). A map is a special kind of relation (関係), but it has stronger conditions than an arbitrary relation.

This condition is what makes the notation $f(a)$ meaningful. If one a had several outputs, $f(a)$ would not be a single value (値). If it had no output, $f(a)$ would be undefined.

2 Terms and definition

For sets (集合) A, B, a map (写像) $f : A \to B$ is a rule assigning to each $a \in A$ a unique element $b \in B$.

The set A is the domain (定義域), and B is the codomain (終域). The assigned value (値) is written $f(a)$. The range (値域), or image (像), is the set of outputs (出力) that actually appear:

$$f(A) = \{f(a) \mid a \in A\}.$$

Always $f(A) \subseteq B$.

3 Images (像) and preimages (逆像)

For a subset (部分集合) $S \subseteq A$, the image (像) of S is

$$f(S) = \{f(a) \mid a \in S\}.$$

For a subset $T \subseteq B$, the preimage (逆像) is

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}.$$

The notation $f^{-1}(T)$ does not assume that an inverse map (逆写像) exists. A preimage is defined for every map (写像).

4 Strategy

To check whether a relation is a map (写像), separate two requirements.

1. For every $a \in A$, at least one output (出力) exists.
2. For every $a \in A$, at most one output exists.

If both hold, each input has exactly one output, and the relation is a map. From the relation (関係) viewpoint, f is a subset (部分集合) of $A \times B$ such that for every $a \in A$ there is exactly one b with $(a, b) \in f$.

→ **Related page** lecture math discrete-math

study.bem130.com

5 Intuitive explanation

A map (写像) can be pictured as drawing one arrow from each element (元) on the input side to the output side. The defining condition is that exactly one arrow leaves every input (入力).

An element on the output side may have no incoming arrows, or it may have several incoming arrows. That is not a problem for being a map. Additional restrictions on these incoming arrows lead to injections (単射) and surjections (全射).

→ **Related page** lecture math discrete-math

study.bem130.com

6 Precise explanation

For a map (写像) $f : A \to B$, images (像) and preimages (逆像) go in opposite directions. An image sends a subset (部分集合) of the A side to the B side:

$$S \subseteq A \implies f(S) \subseteq B.$$

A preimage sends a subset of the B side back to the A side:

$$T \subseteq B \implies f^{-1}(T) \subseteq A.$$

A preimage is defined even when the map is neither an injection 単射 nor a surjection 全射.

7 Worked example: distinguish codomain 終域 and range 値域

7.1 Problem

Define $f : \{1, 2, 3\} \to \{a, b, c, d\}$ by $f(1) = a$, $f(2) = b$, and $f(3) = b$. Find the codomain 終域 and the range 値域.

7.2 Explanation

The codomain 終域 is the set 集合 specified in advance as part of the type of the map 写像. Therefore the codomain is $\{a, b, c, d\}$.

The range 値域 is the set of outputs 出力 that actually occur as values. In this example only a and b occur, so

$$f(A) = \{a, b\}.$$

The elements c, d are in the codomain, but not in the range.

8 What changes and what is preserved

Change	What changes	What is preserved
Enlarging the codomain 終域	whether surjectivity 全射性 holds	the value 値 of each input 入力
Restricting the domain 定義域	the range 値域 and the judgment of injectivity 単射性	the values of the remaining inputs

Extracting a map 写像 from a relation 関係	which ordered pairs 順序対 may be used	the ambient product $A \times B$

9 How to check and related links

- If every input 入力 has exactly one output 出力, it is a map 写像.
- If one input has multiple outputs, it is not a map.
- The codomain 終域 is the declared set of possible outputs.
- The range 値域 is the set of outputs actually reached.
- A preimage 逆像 is defined even when no inverse map 逆写像 exists.

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Images（像） and preimages（逆像） of a map（写像）

A map（写像） sends elements（元） by a rule. In set theory, however, we often study how whole subsets（部分集合） move, not only individual elements. The tools for this are the image（像） and the preimage（逆像）.

→ **Related page** lecture math discrete-math

study.bem130.com

1 Image（像）

Let $f : A \to B$ and $S \subseteq A$. The image（像） of S is defined by

$$f(S) = \{f(x) \in B \mid x \in S\}.$$

This is the set（集合） obtained by applying f to the elements（元） of S.

In particular, $f(A)$ is the range（値域）. Distinguish the codomain（終域） B from the range $f(A)$.

2 Preimage（逆像）

Let $T \subseteq B$. The preimage（逆像） of T is defined by

$$f^{-1}(T) = \{x \in A \mid f(x) \in T\}.$$

Although the notation $f^{-1}(T)$ is used, no inverse map（逆写像） has to exist. A preimage means “all inputs（入力） whose outputs（出力） lie in T,” so it is a different concept from an inverse map.

→ **Related page** lecture math discrete-math

study.bem130.com

3 Preimages work well with set operations

逆像 集合演算

Preimages preserve unions, intersections, and complements.
逆像 和集合 共通部分 補集合

$$f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$$

$$f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$$

$$f^{-1}(B \setminus T) = A \setminus f^{-1}(T)$$

The reason is that each statement is decided only by whether $f(x)$ belongs to the relevant output-side set.

4 Be careful with intersections of images

共通部分 像

Images behave well with unions:
像 和集合

$$f(S_1 \cup S_2) = f(S_1) \cup f(S_2).$$

However, for intersections, generally only
共通部分

$$f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$$

can be guaranteed. Equality does not always hold.

5 Counterexample: images do not preserve intersections

像 共通部分

For a concrete example, let $A = \{1, 2\}$, $B = \{0\}$, with $f(1) = 0$ and $f(2) = 0$. Let $S_1 = \{1\}$ and $S_2 = \{2\}$. Then

$$S_1 \cap S_2 = \emptyset,$$

so $f(S_1 \cap S_2) = \emptyset$. But

$$f(S_1) \cap f(S_2) = \{0\} \cap \{0\} = \{0\}.$$

This happens because f is not an injection: different inputs collapse to the same output.
単射 入力 出力

6 What changes and what is preserved

An image（像） carries an input-side subset（部分集合） to the output side. If a map（写像） is not an injection（単射）, different elements（元） may collapse to the same element, so the size of a set and the structure of intersections may change.

A preimage（逆像） pulls an output-side condition back to an input-side condition. Because the truth of the condition is checked directly through $f(x)$, preimages interact well with set operations（集合演算）.

7 Proof supplement: why preimages（逆像） preserve set operations（集合演算）

For $f : X \to Y$ and $B_1, B_2 \subseteq Y$, prove

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$$

by rewriting the membership condition:

$$x \in f^{-1}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \text{ or } f(x) \in B_2 \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2).$$

The intersection and complement（補集合） identities are proved in the same form.

8 Exercise link and summary

→ **Related page** exercise math discrete-math

study.bem130.com

An image（像） pushes a set forward, while a preimage（逆像） pulls a condition backward. Always distinguish a preimage from an inverse map（逆写像） a preimage is defined even when no inverse map exists.

Injections 単射, surjections 全射, and bijections 全単射

1 Introduction

For a map 写像 $f : A \to B$, the next questions are whether the map collapses information 情報 and whether it reaches the whole codomain 終域.

An injection 単射 sends distinct inputs 入力 to distinct outputs 出力. A surjection 全射 reaches every element 元 of the codomain. A bijection 全単射 has both properties and has an inverse map 逆写像 as a one-to-one correspondence.

2 Terms and definitions

A map 写像 $f : A \to B$ is an injection 単射 if for all $a_1, a_2 \in A$,

$$f(a_1) = f(a_2) \Longrightarrow a_1 = a_2.$$

Equivalently, $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$.

A map $f : A \to B$ is a surjection 全射 if for every $b \in B$ there exists $a \in A$ such that $f(a) = b$. This is equivalent to $f(A) = B$.

A map $f : A \to B$ is a bijection 全単射 if it is both an injection and a surjection.

3 Strategy

To prove injectivity 単射性, assume $f(a_1) = f(a_2)$ and derive $a_1 = a_2$. This proves the direction “same output implies same input.”

To prove surjectivity（全射性）, take arbitrary $b \in B$ and construct $a \in A$ satisfying $f(a) = b$. The important point is to start with an arbitrary element（元） of the codomain（終域） B.

To prove bijectivity（全単射性）, either check injection and surjection separately, or construct an explicit inverse map（逆写像）.

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

An injection（単射） preserves distinctions on the input side. Different inputs（入力） do not collapse to the same output（出力）, so the output can distinguish the input.

A surjection（全射） covers the codomain（終域）. Every element（元） declared in the codomain must actually be reached from some input.

A bijection（全単射） is a correspondence（対応） with no collisions and no unused codomain elements. For finite sets, the existence of a bijection corresponds to the two sets having the same number of elements.

5 Counting viewpoint for finite sets

When A, B are finite sets（有限集合）, the existence of an injection（単射） $A \to B$ implies $|A| \le |B|$, because distinct inputs（入力） require distinct outputs（出力）.

The existence of a surjection（全射） $A \to B$ implies $|A| \ge |B|$, because covering the whole codomain（終域） requires at least as many reached values as elements of B.

For finite sets with $|A| = |B|$, injection implies surjection, and surjection implies injection. This conclusion uses finiteness.

6 Warning for infinite sets

For infinite sets (無限集合), finite counting intuition does not directly apply. For example, if $\mathbb{N} = \{0, 1, 2, \ldots\}$, then $n \mapsto n + 1$ is an injection (単射) $\mathbb{N} \to \mathbb{N}$, but it is not a surjection (全射) because 0 is not reached.

7 Worked example: decide injection (単射) and surjection (全射)

7.1 Problem

Let $f : \{1, 2, 3\} \to \{a, b, c\}$ be defined by $f(1) = a$, $f(2) = b$, and $f(3) = b$. Decide whether f is an injection (単射), a surjection (全射), or a bijection (全単射).

7.2 Explanation

We have $f(2) = b$ and $f(3) = b$ with $2 \neq 3$. Different inputs (入力) are sent to the same output (出力), so f is not an injection (単射).

Also, for the codomain (終域) element c, there is no $x \in \{1, 2, 3\}$ such that $f(x) = c$. Therefore f is not a surjection (全射).

Since a bijection (全単射) must be both injective and surjective, f is not a bijection.

8 How to identify them and related links

- For an injection (単射), check whether any output collision occurs.
- For a surjection (全射), check whether any codomain (終域) element is missed.
- For a bijection (全単射), check for both no collisions and no missed codomain elements.
- Changing the codomain can change whether surjectivity (全射性) holds.

→ **Related page** exercise math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

Composite maps and inverse maps

合成写像 逆写像

1 Introduction

The key to a composite map 合成写像 is to read a map 写像 as an operation. A map $f : A \to B$ sends an element 元 of A to an element of B, and a map $g : B \to C$ sends that result further into C. Performing these two operations in sequence is composition.

An inverse map 逆写像 is an operation that restores the original input. To restore inputs, no two inputs may have collapsed to the same output, and no element of the output side may be left unused. This condition is exactly bijection 全単射.

2 Terms and definitions

Given maps $f : A \to B$ and $g : B \to C$, define the composite map 合成写像 $g \circ f : A \to C$ by

$$(g \circ f)(a) = g(f(a)).$$

The notation $g \circ f$ means that f is applied first and g is applied second.

The identity map 恒等写像 $\mathrm{id}_A : A \to A$ on a set A is the map defined by

$$\mathrm{id}_A(a) = a.$$

For a map $f : A \to B$, if a map $h : B \to A$ satisfies

$$h \circ f = \mathrm{id}_A, \qquad f \circ h = \mathrm{id}_B,$$

then h is called the inverse map 逆写像 of f and is written f^{-1}.

3 Method

For a composite map 合成写像, check the types first. To form $g \circ f$, the codomain 終域 of f must match the domain 定義域 of g. At minimum, $f(A) \subseteq \mathrm{dom}(g)$ must hold.

For an inverse map 逆写像, check that f is a bijection 全単射 before writing f^{-1} as a map. A preimage 逆像 $f^{-1}(T)$ is defined for any map, but an inverse map $f^{-1} : B \to A$ exists only when f is bijective.

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com

4 Intuitive explanation

A composite map 合成写像 is like connecting machines in series. Put an input 入力 a into the first machine f, and the output is $f(a)$. Put that output into the second machine g, and the output is $g(f(a))$. The whole machine is therefore $g \circ f$.

An inverse map 逆写像 is a machine that reconstructs the input from the result. If two inputs collapse to the same output, the output alone cannot tell which input was used. If some element of the codomain 終域 is never reached, there is no input to send back from that element.

5 Rigorous explanation: inverse maps and bijections

Suppose $f : A \to B$ has an inverse map 逆写像 $h : B \to A$. If $f(a_1) = f(a_2)$, then applying h to both sides gives

$$h(f(a_1)) = h(f(a_2)).$$

Since $h \circ f = \mathrm{id}_A$, we get $a_1 = a_2$. Hence f is an injection 単射.

Also, for any $b \in B$, put $a = h(b)$. Then $f(a) = f(h(b)) = b$ by $f \circ h = \mathrm{id}_B$. Hence f is a surjection 全射.

Conversely, if f is a bijection 全単射, then for every $b \in B$ there exists $a \in A$ with $f(a) = b$, and injectivity 単射性 makes this a unique. Therefore one can define $f^{-1}(b) = a$. Without this uniqueness, the value of the inverse map would not be determined.

6 Worked example: composite maps and inverse maps

6.1 Problem

Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. Define $f : A \to B$ by

$$f(1) = b, \qquad f(2) = c, \qquad f(3) = a.$$

Check that f is a bijection 全単射 and find its inverse map 逆写像.

6.2 Explanation

The values $f(1), f(2), f(3)$ are b, c, a, and they are distinct. Thus distinct inputs 入力 are sent to distinct outputs 出力, so f is an injection 単射.

Every element 元 of the codomain 終域 $B = \{a, b, c\}$ appears as a value of f. Therefore f is a surjection 全射. Hence f is a bijection 全単射.

The inverse map 逆写像 is obtained by reading the arrows backward:

$$f^{-1}(a) = 3, \qquad f^{-1}(b) = 1, \qquad f^{-1}(c) = 2.$$

7 How to distinguish the ideas

- In $g \circ f$, f is applied first and g is applied second.

- Before forming a composite map 合成写像, check that the output type and the next input type match.
- An inverse map 逆写像 exists only for a bijection 全単射.
- Do not confuse a preimage 逆像 with an inverse map 逆写像.

8 Proof supplement: why composition preserves injectivity and surjectivity

Let $f : X \to Y$ and $g : Y \to Z$. If both f and g are injective, then $g \circ f$ is injective 単射.

To prove this, assume $(g \circ f)(x_1) = (g \circ f)(x_2)$. This means $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Since f is injective, $x_1 = x_2$. Therefore $g \circ f$ is injective.

If both f and g are surjective 全射, then $g \circ f$ is surjective. Take arbitrary $z \in Z$. Since g is surjective, there exists $y \in Y$ with $g(y) = z$. Since f is surjective, there exists $x \in X$ with $f(x) = y$. Hence $(g \circ f)(x) = z$.

Combining these two statements, the composite of bijections 全単射 is again a bijection. The existence of an inverse map is another way to say that injectivity and surjectivity hold at the same time.

9 Exercise link

→ **Related page** exercise math discrete-math

study.bem130.com

10 Related links

→ **Related page** lecture math discrete-math

study.bem130.com

→ **Related page** lecture math discrete-math

study.bem130.com