abstract algebra portal

19 pages

Table of Contents

data/lecture/math/abstract-algebra/抽象代数ポータル-講義.n.md md d645a9b

abstract algebra portal

抽象代数

abstract algebra studies the form of operations carried by numbers, transformations, and symmetries, rather than studying numbers only as individual objects. The first important point is not to memorize groups, rings, and fields as isolated names. They are languages for organizing which operations are allowed, what those operations preserve, and what information they forget.

The purpose of abstraction is not to throw away concrete examples. It is to extract the structure shared by concrete examples so that the same argument can be transported to other objects.

1 Viewpoints needed first

abstract algebra rests on discrete mathematics. In particular, the following topics are prerequisites.

→ 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

2 Reading order
順序

First, look at operations and structures.

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

Next, learn how to treat different elements as the same. This is the prerequisite for quotient groups and quotient rings.
商群
商環

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

After that, study groups.
群

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

Finally, move to rings and fields, which are structures with two operations.

環 体

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

→ Related page lecture math abstract-algebra

study.bem130.com

3 What changes and what is preserved

Viewpoint	What changes	What should be preserved
equivalence relation 同値関係	Individual representatives	The classification of belonging to the same class
quotient structure 商構造	Elements are grouped into classes	Operations do not depend on representatives
homomorphism 準同型	The representation of an object	The operational structure
isomorphism 同型	The names of elements	All algebraic relations
group action 群作用	A group is viewed as transformations	The structure of symmetry

This table is a guide for reading all of abstract algebra. Whenever you meet a definition, always ask: what does this definition change, and what is it designed not to change?
抽象代数 定義 定義

4 Exercise links

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

→ Related page exercise math abstract-algebra

study.bem130.com

5 Summary

abstract algebra is a language for comparing objects that carry operations. A group has one operation, a ring has addition and multiplication, and a field is a ring in which division by nonzero elements is also possible. Through homomorphisms and quotient structures, concrete calculation and abstract structure are connected.

抽象代数 群 環 体 準同型 商構造

data/lecture/math/abstract-algebra/代数的構造とは何か-講義.n.md md e34dbcb

What is an algebraic structure?

代数的構造

The first viewpoint to fix in abstract algebra is to regard an object as a pair consisting of a set and operations.
抽象代数　集合　演算
Algebra does not begin from a set of numbers alone. Only after specifying which operations are performed inside that set and which laws those operations satisfy do we obtain an algebraic structure.
代数的構造

For example, the set of all integers $\mathbb{Z}$ becomes a group when viewed with addition. But when viewed with
群
multiplication, it is not a group because not every nonzero element has an inverse in the integers. Even with the same underlying set, changing the operation changes the structure.

The terms group and inverse element will be defined formally later. At this point, we use only the idea that a
群　逆元
structure is not determined by a set alone; the operation must also be specified.

1 The form of a definition

定義

An algebraic structure is typically written in a form such as
代数的構造

$$(S, *)$$

or

$$(S, +, \cdot)$$

Here S is a set, and $*$, $+$, and $\cdot$ are operations.
集合

This notation separates "what the elements are" from "how the elements are operated on." A set alone is only a list or collection of elements, and an operation alone does not say where the calculation takes place. Only when both are specified is the world of calculation determined.

2 Why define by axioms?

Axioms are conditions that let us forget the details of concrete examples and keep only the properties needed for an argument.

公理

Addition of integers, rotations of the plane, and symmetries of a square look completely different. However, they share common features: operations can be composed, there is an operation that does nothing, and there are operations that return an element to where it was. Extracting just these common features gives the axioms of a group.

群

→ Related page lecture math abstract-algebra

study.bem130.com

3 What changes and what is preserved

In abstraction, the concrete presentation changes. Integers, matrices, permutations, and residue classes look different. On the other hand, we preserve and study the laws satisfied by the operations.

For example, two isomorphic groups may have elements with different names, but the structure of their operation tables is the same. In other words, the information about which element is obtained by combining which elements is preserved. Isomorphism will be defined later together with homomorphisms, so here it should be read only as the preview that operation structure can remain the same even when names change.

→ Related page lecture math abstract-algebra

study.bem130.com

4 Concrete example: the same set can have different structures

Consider the set $\mathbb{Z}$.

$$(\mathbb{Z}, +)$$

is a group. The identity element is 0, and the inverse of an integer a is $-a$.

群 単位元

However,

$$(\mathbb{Z}, \cdot)$$

is not a group. For example, the multiplicative inverse of 2 does not exist among the integers. If there were an integer b with $2b = 1$, the left-hand side would be even, so it could not equal 1.

The important point is that we cannot decide whether something is a group by looking only at the set. We must always judge it together with its operation.

5 Connections with other areas

abstract algebra also appears in linear algebra. For example, the set of all invertible matrices forms a group under matrix multiplication.

抽象代数 群

→ Related page lecture math linear-algebra

study.bem130.com

This section is only a preview of connections; matrix knowledge is not used as a prerequisite for later definitions or proofs here.

In number theory, addition and multiplication of residue classes become basic examples in abstract algebra.

抽象代数

→ Related page lecture math number-theory

study.bem130.com

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

An algebraic structure is a set equipped with operations, with required properties specified by axioms. Even if the underlying set is the same, changing the operation changes the structure. In abstract algebra, we focus not on appearance but on the structure preserved by operations.

代数的構造

抽象代数

data/lecture/math/abstract-algebra/二項演算と閉包性-講義.n.md md f0b87eb

binary operation and closure

二項演算　　閉包性

The first operation to check in abstract algebra is an operation that takes two elements and produces one element. This is called a binary operation.

抽象代数　　二項演算

A binary operation on a set S is a map

二項演算

$$* : S \times S \to S$$

That is, for any $a, b \in S$, the result $a * b$ is again an element of S.

Here a map means a rule that assigns one output to each input. The set $S \times S$ means the set of ordered pairs of elements of S.

The condition that "the result returns to the same set" is closure.

閉包性

1　Why closure is necessary

閉包性

Without closure, an operation cannot be repeated inside the same set.

閉包性

For example, consider subtraction on the natural numbers $\mathbb{N}$:

$$2 - 5 = -3$$

The result is not a natural number. Therefore subtraction is not a binary operation on $\mathbb{N}$.

二項演算

On the other hand, if subtraction is considered on the integers $\mathbb{Z}$, then for any integers a, b, the result $a - b$ is an integer. Thus subtraction is a binary operation on $\mathbb{Z}$.

二項演算

2　Associative law and commutativity

The associative law says that when three or more elements are operated on, the position of parentheses does not affect the result.

結合法則

$$(a * b) * c = a * (b * c)$$

When the associative law holds, writing $a * b * c$ is not ambiguous.

結合法則

Commutativity says that changing the order does not change the result.

可換性　順序

$$a * b = b * a$$

Commutativity is not always assumed. Matrix multiplication and composition of permutations are generally not commutative.

→ Related page lecture math linear-algebra

study.bem130.com

Matrices and permutations are mentioned only as examples of noncommutative operations; they are not used in the tests on this page.

3 Identity element and inverse element

逆元

An identity element is an element that leaves the other element unchanged when operated with it.

単位元

$$e * a = a * e = a$$

An inverse element is an element that brings an element back to the identity element through the operation.

逆元　単位元

$$a * a^{-1} = a^{-1} * a = e$$

Identity elements and inverses are important for solving equations. If we want to solve $a * x = b$, we want to apply a^{-1} from the left and get $x = a^{-1} * b$. This operation requires the existence of an inverse.

4 Concrete example: reading an operation table

Put addition modulo 3 on the set $S = \{0, 1, 2\}$.

$$a * b \equiv a + b \pmod 3$$

The operation table is as follows.

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Every result lies in S, so closure holds. The element 0 is the identity element, the inverse of 1 is 2, and the inverse of 2 is 1.

閉包性 単位元

5 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

6 Summary

A binary operation is a map that takes two elements of a set and produces an element of the same set. Closure, the associative law, commutativity, an identity element, and inverse elements are the basic vocabulary used to define groups, rings, and fields.

二項演算 閉包性 結合法則 可換性 単位元 逆元 群 環 体

7 Test supplement: check properties of an operation separately

演算

Given a set S and a rule $*$, first check $a, b \in S \Rightarrow a * b \in S$ to see whether $* : S \times S \to S$ is a binary operation. This checks only closure it does not yet guarantee associativity, commutativity, an identity element, or inverse elements.

二項演算 閉包性 単位元

For example, subtraction $a * b = a - b$ on $\mathbb{Z}$ has closure, but

$$(5 - 3) - 1 = 1, \qquad 5 - (3 - 1) = 3$$

so it does not satisfy associativity. Thus having closure and having group-like properties are separate questions.

data/lecture/math/abstract-algebra/同値関係と剰余類の基本-講義.n.md md 4eb6de5

equivalence relation and residue class

同値関係　　剰余類

Before building quotient structures in abstract algebra, we must decide which elements will be treated as the same. The tool for doing this is an equivalence relation.

抽象代数　　同値関係

An equivalence relation is a rule for classifying objects. Each box in the classification is an equivalence class, and the set of all equivalence classes is the quotient set.

同値関係　　同値類　　商集合

→ Related page lecture math discrete-math

study.bem130.com

1 The three conditions for an equivalence relation

同値関係

A relation $\sim$ on a set X is an equivalence relation if it satisfies the following conditions.

同値関係

$$x \sim x$$

$$x \sim y \Rightarrow y \sim x$$

$$x \sim y \text{ and } y \sim z \Rightarrow x \sim z$$

These are called reflexivity, symmetry, and transitivity, respectively.

2 Equivalence classes

The equivalence class of an element $a \in X$ is defined by

同値類

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

An equivalence class is not the representative a itself, but the set of all elements regarded as the same as a.

同値類

The representative is a name; the equivalence class is the actual object. Therefore, if $a \sim b$, then

同値類

$$[a] = [b]$$

The set of all equivalence classes is called the quotient set. Thus, in a quotient set, the new elements are not the original elements themselves, but their equivalence classes.
商集合

3 Residue classes

For integers, fix n. For integers a, b, define

$$a \sim b \quad \Longleftrightarrow \quad n \mid (a-b)$$

This is an equivalence relation. The equivalence class of a,
同値関係 同値類

$$[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$$

is called a residue class.
剰余類

For example, when $n = 5$,

$$[2]_5 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$

All of these integers have remainder 2 when divided by 5.

4 The issue of well-definedness

When defining an operation on a quotient set, the result must not depend on the choice of representative. This property is called well-definedness.
商集合

For example, if we want to define addition of residue classes by

$$[a] + [b] = [a + b]$$

then we must check that changing a to another representative a' of the same class and changing b to another representative b' of the same class does not change the resulting class.

If this check is omitted, the operation on the quotient set may not actually be determined.

5 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

6 Summary

An equivalence relation is a rule for classifying elements. A residue class is an equivalence class that classifies integers by remainder, and it is the basis for congruences and quotient rings. To operate on a quotient set, one must always check that the result is independent of the representative.

7 Proof supplement: why congruence is an equivalence relation

For integers a, b, define

$$a \sim b \iff n \mid (a-b)$$

where n is a positive integer. We check that this relation is an equivalence relation.

Reflexivity follows because $a - a = 0$ is divisible by n. Symmetry follows because if $n \mid (a-b)$, then $b - a = -(a-b)$ is also divisible by n. Transitivity follows because if $n \mid (a-b)$ and $n \mid (b-c)$, then

$$a - c = (a-b) + (b-c)$$

is also divisible by n.

Thus congruence is a valid equivalence relation that classifies integers into residue classes.

8 Warning: an example of a definition that is not well-defined

定義

In $\mathbb{Z}/2\mathbb{Z}$, suppose we try to define a map that sends a residue class $[a]$ to the integer representative a itself. This fails because $[0] = [2]$, but choosing representative 0 gives value 0, while choosing representative 2 gives value 2.

An element of a quotient set is a class, not a representative. Whenever something is defined on classes, one must check that changing representatives gives the same value.

congruence and mod operation

合同式 演算

If congruences (合同式) are viewed only as the calculation rule "the remainders are the same," it is hard to see why addition and multiplication are justified. In abstract algebra (抽象代数), a congruence (合同式) is viewed as equality of residue classes (剰余類).

$$a \equiv b \pmod{n}$$

means

$$n \mid (a-b)$$

and at the same time means that a and b belong to the same residue class.

→ Related page lecture math abstract-algebra

study.bem130.com

1 The set of residue classes

Let $n \geq 2$. Classifying all integers by their remainders modulo n gives the quotient set (商集合)

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

The elements of this set are not integers themselves, but equivalence classes of integers.

Here the quotient set is the set obtained by grouping integers with the same remainder into one class and then treating those classes as the elements.

2 Addition and multiplication

Define addition and multiplication of residue classes by

$$[a] + [b] = [a+b]$$

$$[a][b] = [ab]$$

The important point is that the right-hand side does not depend on the choice of representatives. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$(a+b) - (a'+b') = (a-a') + (b-b')$$

is a multiple of n. Also,

$$ab - a'b' = a(b-b') + b'(a-a')$$

is a multiple of n. Therefore the sum and product are well-defined.

3 The condition for an inverse

A residue class $[a]$ has a multiplicative inverse if there exists a class $[x]$ such that

$$[a][x] = [1]$$

This is the same as

$$ax \equiv 1 \pmod{n}$$

The condition for this congruence to have a solution is

合同式

$$\gcd(a, n) = 1$$

This is the same condition for the linear Diophantine equation

$$ax + ny = 1$$

to have an integer solution.

→ Related page lecture math algebra

study.bem130.com

Here we are not dividing by a symbol; we are proving the existence of an inverse from the fact that the greatest common divisor is 1. Therefore, whenever a division-like operation is used, one must first check the condition that an inverse exists.

4 Connection to Fermat's little theorem

If p is prime, every nonzero residue class has an inverse. Therefore

$$(\mathbb{Z}/p\mathbb{Z})^{\times}$$

forms a group under multiplication. From the structure of this group, when $p \nmid a$,

群

$$a^{p-1} \equiv 1 \pmod{p}$$

is obtained. This is Fermat's little theorem.

This section is a preview of later material on groups and Lagrange's theorem. The main thread of this page uses only the well-definedness of residue-class operations and the condition for inverses to exist.

5 Proof supplement: why congruence is preserved by addition and multiplication

合同式

Let n be a positive integer. If the congruences

合同式

$$a \equiv b \pmod{n}, \qquad c \equiv d \pmod{n}$$

hold, then

$$a + c \equiv b + d \pmod{n}, \qquad ac \equiv bd \pmod{n}$$

also hold.

First prove the statement for addition. The congruence $a \equiv b \pmod{n}$ means $n \mid (a-b)$, and $c \equiv d \pmod{n}$ means $n \mid (c-d)$. Therefore

合同式

$$(a+c) - (b+d) = (a-b) + (c-d)$$

is also divisible by n. Hence $a + c \equiv b + d \pmod{n}$.

For multiplication, rewrite

$$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d)$$

Since $n \mid (a-b)$ and $n \mid (c-d)$, both terms on the right are divisible by n. Hence $n \mid (ac-bd)$, so $ac \equiv bd \pmod{n}$.

This proof does not divide by n it uses the fact that n divides a difference. Therefore no issue of division by zero in symbolic division arises. However, in the notation $\pmod{n}$, the modulus n is fixed as a positive integer.

証明

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

A congruence is equality of residue classes. Mod operations are justified because addition and multiplication on residue classes are determined independently of representatives. Multiplicative inverses do not always exist; the condition $\gcd(a, n) = 1$ is necessary.

合同式

data/lecture/math/abstract-algebra/半群・モノイド・群への入口-講義.n.md md b57221b

Entrance to semigroups, monoids, and groups

半群　モノイド　群

If the definition of a group is memorized all at once as four conditions, it is hard to see why those conditions are needed. Instead, add conditions one by one to a binary operation.

定義　群　二項演算

$$\text{binary operation} \longrightarrow \text{semigroup} \longrightarrow \text{monoid} \longrightarrow \text{group}$$

Viewed in this order, a group is a structure in which operations can be repeated, there is an operation that does nothing, and operations can be undone.

順序　群

1 Semigroups

A semigroup is a pair consisting of a set S and a binary operation $*$ satisfying the associative law.

半群　二項演算　結合法則

$$(a * b) * c = a * (b * c)$$

A semigroup does not require an identity element or inverse elements. Because associativity holds, parentheses can be omitted in a long product such as

単位元

$$a_1 * a_2 * \cdots * a_n$$

2 Monoids

A monoid is a semigroup with an identity element. That is, there exists an element e such that for every a,

モノイド　単位元

$$e * a = a * e = a$$

For example, the natural numbers $\mathbb{N}$ form a monoid under addition with identity element 0. However, within the natural numbers, not every element has an additive inverse, so this is not a group.

単位元

3 Groups

A group is a monoid in which every element has an inverse. For every a, there exists an element a^{-1} such that

群

$$a * a^{-1} = a^{-1} * a = e$$

In a group, an operation that moves forward can be undone by an inverse. This property of being able to return is what makes groups the mathematics of symmetries and transformations.

4 Concrete examples: natural numbers, integers, and rational numbers

With addition,

$$(\mathbb{N}, +)$$

is a monoid. The identity element is 0, but there is no natural number that brings 3 back to 0 by addition.

単位元

$$(\mathbb{Z}, +)$$

is a group. The inverse of an integer a is $-a$.

群

With multiplication,

$$(\mathbb{Q} \setminus \{0\}, \cdot)$$

is a group. The reason for excluding 0 is that 0 has no multiplicative inverse.

群

5 What changes and what is preserved

Moving from semigroups to monoids makes the "do nothing" operation available. Moving from monoids to groups makes the "undo" operation available. In all cases, closure of the operation inside the same set and the associative law are preserved.

閉包性

結合法則

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

A semigroup is an operation with associativity, a monoid is a semigroup with an identity element, and a group is a monoid in which every element has an inverse. Understanding this staircase makes the group axioms appear as minimal necessary conditions.

8 Counterexample supplement: the hierarchy of semigroups, monoids, and groups is strict

Semigroups, monoids, and groups form a hierarchy obtained by adding conditions one at a time. However, the stronger notions do not collapse to the weaker ones.

$(\mathbb{Z}_{>0}, +)$ is a semigroup because addition is associative. It is not a monoid, because the identity element 0 is not in $\mathbb{Z}_{>0}$.

$(\mathbb{Z}_{\geq 0}, +)$ is a monoid because it has 0 as its identity element. It is not a group, because the additive inverse -1 of 1 is not in $\mathbb{Z}_{\geq 0}$.

$(\mathbb{Z}, +)$ is a group because it has 0 and all additive inverses. Thus each newly required condition has real content.

data/lecture/math/abstract-algebra/群の基本-講義.n.md md 1af7739

Basics of groups

群

A group is a structure in which operations can be composed and, when necessary, undone. Addition of integers, addition of residue classes, rotations of figures, and products of invertible matrices look different. However, they all satisfy the same four conditions.

1 Definition of a group

A pair $(G, *)$ consisting of a set G and a binary operation $*$ is a group if it satisfies the following conditions.

$$a, b \in G \Rightarrow a * b \in G$$

$$(a * b) * c = a * (b * c)$$

$$\exists e \in G \text{ such that } e * a = a * e = a$$

$$\forall a \in G, \exists a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e$$

These are closure, the associative law, an identity element, and inverse elements, respectively.

2 Why these four conditions?

Closure guarantees that the result of an operation stays in the same world. Associativity guarantees that when operations are repeated, the position of parentheses does not matter. The identity element is the operation that does nothing, and an inverse is an operation that cancels another operation.

With these four conditions, the equation

$$a * x = b$$

can be solved as

$$x = a^{-1} * b$$

This uses the existence of a^{-1}, so the existence of inverses is essential.

3 Abelian groups

A group in which

群

$$a * b = b * a$$

holds for all $a, b \in G$ is called an abelian group. Addition of integers is commutative. In contrast, composition

可換群

of permutations and matrix multiplication are generally not commutative.

→ Related page lecture math linear-algebra

study.bem130.com

Here a permutation is used only as an operation that rearranges elements of a set, and matrix multiplication is used only as an example of a noncommutative operation.

4 Basic examples

group 群	Operation	Identity element	Inverse
$(\mathbb{Z}, +)$	Addition	0	$-a$
$(\mathbb{Z}/n\mathbb{Z}, +)$	Addition of residue classes	$[0]$	$[-a]$
$(\mathbb{R}^\times, \cdot)$	Multiplication	1	$1/a$
S_n	Composition of permutations	Identity permutation	Inverse permutation
$GL_n(\mathbb{R})$	Matrix multiplication	Identity matrix	Inverse matrix

Here $\mathbb{R}^\times$ is the set of all nonzero real numbers. The element 0 is excluded because it has no multiplicative inverse.

The group S_n is the set of all bijections from $\{1, \ldots, n\}$ to itself, that is, all permutations. The group $GL_n(\mathbb{R})$ is the set of all $n \times n$ real matrices that have inverses under multiplication. Detailed matrix calculations are not used as a prerequisite for the proofs on this page.

5 What changes and what is preserved

When objects are viewed as groups, the concrete appearance of the elements becomes less important. Integers, permutations, and matrices are different kinds of objects. However, the ability to repeat the operation, the existence of an identity element, and the ability to return by an inverse are shared. Group theory studies arguments while preserving this common structure.

単位元

6 Proof supplement: identity elements, inverses, and cancellation

In a group, the identity element is unique. Suppose e and e' are both identity elements. Since e is an identity element, $ee' = e'$. Since e' is an identity element, $ee' = e$. Therefore $e = e'$.

群 単位元 単位元 単位元

Inverses are also unique. Suppose b and c are both inverses of a. That means $ab = e$ and $ca = e$. Then

$$b = eb = (ca)b = c(ab) = ce = c$$

Here the associative law is used.

結合法則

Furthermore, the cancellation law holds in a group:

消去法則

$$ab = ac \quad \Longrightarrow \quad b = c$$

Indeed, multiplying by a^{-1} from the left gives

$$a^{-1}(ab) = a^{-1}(ac)$$

By associativity, $(a^{-1}a)b = (a^{-1}a)c$, so $eb = ec$. Therefore $b = c$.

This proof shows that in a group, the ability to undo operations is what gives us the power to solve equations.

証明

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A group is an algebraic structure with closure, associativity, an identity element, and inverse elements. The
群 代数的構造 閉包性 単位元
reason to study groups is to handle numbers, permutations, matrices, and symmetries in the same language.

data/lecture/math/abstract-algebra/部分群と生成-講義.n.md md ef2b946

subgroups and generation

部分群　　生成

Inside a group, we often want to find a smaller part that still preserves the structure of a group. Such a subset is a subgroup.
群　　部分群

A subgroup is not merely a subset. When elements are operated on, the result must remain inside, and inverse elements must also remain inside.
部分群

1 Definition of a subgroup

部分群

A subset $H \subseteq G$ of a group G is a subgroup if H becomes a group using the operation inherited from G.
部分群

In practice, it can be tested by the following criterion.

$$H \neq \emptyset$$

and for all $a, b \in H$,

$$ab^{-1} \in H$$

If these hold, then H is a subgroup.
部分群

This criterion may look like division, but it uses the fact that the inverse b^{-1} exists inside the group. Therefore it is assumed that b is an element of the group and that its inverse lies in the group.

2 Concrete examples

Inside $(\mathbb{Z}, +)$, the set of all even integers

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$$

is a subgroup. It contains 0, and the difference of two even integers is even.
部分群

On the other hand, the set of natural numbers $\mathbb{N}$ is not a subgroup of $(\mathbb{Z}, +)$. For example, it contains 3 but does not contain the inverse -3.

部分群

3 Generators

Given a subset A of a group G, the set of all elements obtained by applying the operation finitely many times to elements of A and their inverses is the subgroup generated by A.

部分群 生成

It is written

$$\langle A \rangle$$

A group generated by one element a,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

is called a cyclic group.

巡回群

4 Example: cyclic groups of residue classes

In $(\mathbb{Z}/6\mathbb{Z}, +)$, the element $[1]$ generates the whole group.

$$[0], [1], [2], [3], [4], [5]$$

are obtained by repeatedly adding $[1]$. On the other hand, the subgroup generated by $[2]$ is

部分群

$$\{[0], [2], [4]\}$$

5 What is preserved

In a subgroup, the operation, identity element, and inverses of the group are preserved as they are. What changes is the range of elements available. In generation, starting from a small number of specified elements, closure and inverses are used to build the smallest necessary subgroup.

部分群 単位元 閉包性 部分群

6 Proof supplement: subgroup criterion and minimality of generated subgroups

Let G be a group and let $H \subseteq G$ be a nonempty subset. If

$$x, y \in H \implies xy^{-1} \in H$$

holds, then H is a subgroup.

Proof. Since H is nonempty, there exists $h \in H$. Then $hh^{-1} = e \in H$. Next let $x \in H$. Since $e \in H$, applying the condition to e, x gives $ex^{-1} = x^{-1} \in H$. Finally, if $x, y \in H$, we already know $y^{-1} \in H$, so applying the condition to x, y^{-1} gives $x(y^{-1})^{-1} = xy \in H$. Thus H contains the identity, inverses, and products.

The generated subgroup $\langle S \rangle$ can be defined as the intersection of all subgroups that contain S:

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

This intersection is a subgroup, because the identity lies in every such H and products and inverses are closed in each H. Also, since every such H contains S, the intersection contains S. Moreover, any subgroup K containing S is one of the subgroups being intersected, so $\langle S \rangle \subseteq K$. Therefore $\langle S \rangle$ is the smallest subgroup containing S.

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A subgroup is obtained by restricting the elements while preserving the group structure. Generation is the operation of building the smallest closed subgroup from specified elements, and a cyclic group is a group generated by one element.

9 Calculation supplement: the subgroup generated by $[k]$ in $\mathbb{Z}/n\mathbb{Z}$

部分群

In the additive group $(\mathbb{Z}/n\mathbb{Z}, +)$, the elements of the subgroup generated by $[k]$ are

部分群

$$[0], [k], [2k], [3k], \dots$$

The first positive integer m for which this sequence returns to $[0]$ is the smallest m satisfying $n \mid mk$.

Therefore, if $d = \gcd(n, k)$, then

$$| \langle [k] \rangle | = \frac{n}{d}$$

For example, in $\mathbb{Z}/12\mathbb{Z}$, consider $[8]$. Since $\gcd(12, 8) = 4$, the generated subgroup has order $12/4 = 3$. Indeed,

部分群 位数

$$\langle [8] \rangle = \{[0], [8], [4]\}$$

data/lecture/math/abstract-algebra/剰余類とラグランジュの定理-講義.n.md md a113a4d

cosets and Lagrange's theorem

剰余類

Residue classes of integers classify integers by remainders. In a group, elements can also be classified using a subgroup as the standard. This classification is the group-theoretic notion of a coset.

群 部分群 剰余類

1 Left cosets

剰余類

For a subgroup H of a group G and an element $g \in G$,

部分群

$$gH = \{gh \mid h \in H\}$$

is called the left coset of H by g.

左剰余類

The set obtained by multiplying from the right,

$$Hg = \{hg \mid h \in H\}$$

is called the right coset.

右剰余類

If the group is commutative, left cosets and right cosets coincide. In a general group, however, they need not coincide.

剰余類 剰余類

2 Cosets partition a group

Any two left cosets are either equal or disjoint. Also, the collection of all left cosets covers all of G.

剰余類 剰余類

This means that cosets divide G into boxes of the same size.

剰余類

3 Lagrange's theorem

For a finite group G and a subgroup H,

部分群

$$| G | = [G : H] | H |$$

holds. Here $[G : H]$ is the number of left cosets of H.
剰余類

Therefore,

$$| H | \mid | G |$$

This is Lagrange's theorem.
ラグランジュの定理

4 Concrete example

Let $G = \mathbb{Z}/6\mathbb{Z}$ and $H = \{[0], [3]\}$. The order of H is 2. The cosets are
位数 剰余類

$$[0] + H = \{[0], [3]\}$$

$$[1] + H = \{[1], [4]\}$$

$$[2] + H = \{[2], [5]\}$$

There are three such cosets, so $| G | = 6 = 3 \cdot 2$.
剰余類

5 What is preserved

When a group is divided into cosets, we no longer look at individual elements, but at boxes consisting of
剰余類
elements shifted by a subgroup. The size of the subgroup is preserved in every box. This shows that, in a
部分群 部分群
finite group, the order of a subgroup divides the order of the group.
位数 部分群 位数

6 Warning about quotient groups
商群

The set of cosets can always be formed. However, it is not always possible to make that set into a group by
剰余類
multiplying cosets. To build a quotient group, the subgroup must be a normal subgroup.
剰余類 商群 部分群 正規部分群

→ Related page lecture math abstract-algebra

study.bem130.com

7 Proof supplement: coset partitions and Lagrange's theorem

剰余類

Let $H \leq G$. Two left cosets aH and bH are either disjoint or exactly equal.

剰余類

Proof. Suppose $aH \cap bH \neq \emptyset$, and take $x \in aH \cap bH$. Then there exist $h_1, h_2 \in H$ such that $x = ah_1 = bh_2$.

From this,

$$b^{-1}a = h_2 h_1^{-1} \in H$$

For any $ah \in aH$,

$$ah = b(b^{-1}a)h$$

and since $(b^{-1}a)h \in H$, we have $ah \in bH$. Thus $aH \subseteq bH$. The same argument gives $bH \subseteq aH$, so $aH = bH$.

Also, the map

$$H \to aH, \qquad h \mapsto ah$$

is a bijection. Surjectivity follows from the definition of aH. Injectivity follows because if $ah_1 = ah_2$, then

定義

multiplying by a^{-1} from the left gives $h_1 = h_2$. This uses the existence of a^{-1}, that is, it uses that G is a group.

Therefore, in a finite group G, the group is partitioned into left cosets of equal size. If the number of left

剰余類

cosets is $[G : H]$, then

剰余類

$$| G | = [G : H] | H |$$

This is Lagrange's theorem.

ラグランジュの定理

8 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

9 Summary

A group coset is a way of dividing a group into equally sized boxes using a subgroup as the standard. In a finite group, the order of a subgroup divides the order of the group. To construct a quotient group, normality is additionally required.

10 Corollary: the order of an element divides the order of the group

Let g be an element of a finite group G, and consider the subgroup $\langle g \rangle$ generated by g. By Lagrange's theorem,

$$| \langle g \rangle | \, | \, | G |$$

The number $| \langle g \rangle |$ is the order of g, so in a finite group, the order of every element divides the order of the group.

In particular, if $| G | = p$ is prime and g is not the identity, then the order of g is not 1 and must divide p, so it is p. Hence $G = \langle g \rangle$, and every group of prime order is cyclic.

data/lecture/math/abstract-algebra/正規部分群と商群-講義.n.md md 62a31e5

normal subgroups and quotient groups

正規部分群 商群

To merely form the set of cosets, any subgroup is enough. But if we want to multiply cosets and obtain cosets again, the result must not depend on the choice of representatives. A subgroup satisfying this condition is a normal subgroup.

剰余類 部分群 剰余類 剰余類 部分群 正規部分群

1 Definition of a normal subgroup

正規部分群

A subgroup $N \leq G$ is a normal subgroup if for every $g \in G$,

部分群 正規部分群

$$gN = Ng$$

holds. In this case we write

$$N \trianglelefteq G$$

An equivalent condition is that for every $g \in G$ and $n \in N$,

$$gng^{-1} \in N$$

holds.

2 Why normality is necessary

We want to define the product of cosets by

剰余類

$$(gN)(hN) = (gh)N$$

For this definition to be independent of representatives, replacing g or h by another element in the same coset must produce the same resulting coset.

定義 剰余類 剰余類

Normality is the condition that guarantees this well-definedness.

3 Quotient groups

When $N \trianglelefteq G$, the set of all cosets
剰余類

$$G/N = \{gN \mid g \in G\}$$

becomes a group under the product
群

$$(gN)(hN) = (gh)N$$

This group is called a quotient group.
商群

In a quotient group, differences lying inside N are collapsed as if they were 0. In other words, we ignore
商群
movement inside N and study the remaining structure.

4 Concrete example: quotient groups of integers
商群

In $(\mathbb{Z}, +)$, the subgroup $n\mathbb{Z}$ is normal because $\mathbb{Z}$ is an abelian group, and every subgroup of an abelian group
部分群
部分群
is normal.

The quotient group
商群

$$\mathbb{Z}/n\mathbb{Z}$$

is the group obtained by classifying integers by their remainders modulo n.

5 What changes and what is preserved

In a quotient group, differences inside N are no longer distinguished. What changes is the granularity of
商群
elements: the elements are cosets rather than individual elements. What is preserved is the group operation
剰余類
structure in a well-defined form.

6 Proof supplement: the condition for quotient-group operations to be well-defined

Let $N \leq G$. We want to define multiplication of cosets by
剰余類

$$(aN)(bN) = (ab)N$$

For this definition to be independent of the chosen representatives, N must be a normal subgroup.
定義 正規部分群

First suppose N is normal. Let $aN = a'N$ and $bN = b'N$. Then there exist $n_1, n_2 \in N$ such that $a' = an_1$ and $b' = bn_2$. Hence

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2$$

Since N is normal, $b^{-1}n_1b \in N$, and therefore $(b^{-1}n_1b)n_2 \in N$. Thus $a'b'N = abN$. The product is independent of representatives.

Conversely, suppose this product is always well-defined. Take any $g \in G$ and $n \in N$. As left cosets, $(gn)N = gN$, so changing the representative of the first factor from g to gn must give the same product with $g^{-1}N$. Therefore
剰余類

$$(gN)(g^{-1}N) = N, \qquad ((gn)N)(g^{-1}N) = gng^{-1}N$$

must be the same coset. Hence $gng^{-1}N = N$, so $gng^{-1} \in N$. Since this holds for every g, n, the subgroup N is normal.
剰余類

Thus normality is precisely the condition that makes it consistent to multiply cosets as elements.
剰余類

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A normal subgroup is the condition needed to put a group structure on the set of cosets. A quotient group is the structure that remains after collapsing the differences inside a normal subgroup.

9 Counterexample: not every subgroup is normal

In the symmetric group S_3, consider $H = \{e, (12)\}$. This is a subgroup. However, if $g = (13)$, then

$$gH = \{(13), (13)(12)\}$$

while

$$Hg = \{(13), (12)(13)\}$$

Here $(13)(12)$ and $(12)(13)$ are different permutations. Therefore $gH \neq Hg$, so H is not a normal subgroup.

In this example, the set of cosets can be formed, but multiplication of cosets cannot be defined independently of representatives. Thus in noncommutative groups, checking normality is essential.

data/lecture/math/abstract-algebra/群準同型と同型-講義.n.md md 2b20198

group homomorphisms and isomorphisms

群準同型　　同型

When comparing groups, the names of the elements do not need to match. What matters is that the operation structure is preserved. A map that preserves operations in this way is a group homomorphism.

群　　群準同型

1 Group homomorphisms

準同型

For groups G, H, a map $\varphi : G \to H$ is a group homomorphism if for all $a, b \in G$,

群準同型

$$\varphi(ab) = \varphi(a)\varphi(b)$$

holds.

Here the product on the left is the operation in G, and the product on the right is the operation in H. Even if the same symbol is used, it is necessary to distinguish which group's operation is being used.

2 What a homomorphism automatically preserves

準同型

A group homomorphism $\varphi : G \to H$ sends the identity element to the identity element:

群準同型　　単位元　　単位元

$$\varphi(e_G) = e_H$$

It also sends inverses to inverses:

$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

These facts are not written directly in the definition, but they follow from preservation of the operation.

定義

3 Kernel and image

像

The kernel of a group homomorphism $\varphi : G \to H$ is defined by

核　　群準同型

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$$

The kernel is the part collapsed to the identity element by the map.
核 単位元

The image is
像

$$\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$$

It is the set of all elements actually reached by the map.

4 Isomorphisms

A group homomorphism $\varphi : G \to H$ is a group isomorphism when it is bijective. In that case, G and H have
群準同型 同型

the same structure as groups.

$$G \cong H$$

In an isomorphism, the names of elements may change. However, the operation table, identity element,
同型 単位元

inverses, subgroup structure, order, and other group-theoretic properties are preserved.
部分群 位数

5 Concrete example

Define $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$\varphi(k) = [k]$$

This is a group homomorphism because
群準同型

$$\varphi(a+b) = [a+b] = [a] + [b]$$

The kernel of this map is
核

$$\ker\varphi = n\mathbb{Z}$$

6 Proof supplement: what homomorphisms preserve
準同型

Let $\varphi : G \to H$ be a group homomorphism. Then
群準同型

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

First, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Multiplying by $\varphi(e_G)^{-1}$ from the left gives $e_H = \varphi(e_G)$. Next,

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

so $\varphi(g^{-1})$ is the inverse of $\varphi(g)$. Hence $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Moreover, the kernel $\ker\varphi$ is a normal subgroup of G. If $a, b \in \ker\varphi$, then

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H^{-1} = e_H$$

so $ab^{-1} \in \ker\varphi$, and the subgroup criterion gives that it is a subgroup. Also, for $g \in G$ and $a \in \ker\varphi$,

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

so $gag^{-1} \in \ker\varphi$. Thus the kernel is normal.

Finally, φ is injective if and only if $\ker\varphi = \{e_G\}$. If φ is injective, then $\varphi(g) = e_H = \varphi(e_G)$ implies $g = e_G$. Conversely, suppose $\ker\varphi = \{e_G\}$ and $\varphi(g_1) = \varphi(g_2)$. Then

$$\varphi(g_1 g_2^{-1}) = e_H$$

so $g_1 g_2^{-1} \in \ker\varphi$, hence $g_1 g_2^{-1} = e_G$. Therefore $g_1 = g_2$, and φ is injective.

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A group homomorphism is a map that preserves operations. The kernel is the part that is collapsed, and the image is the part that is reached. An isomorphism is a homomorphism that preserves structure completely, expressing the idea of being essentially the same in abstract algebra.

data/lecture/math/abstract-algebra/群作用と対称性-講義.n.md md 054692a

group actions and symmetry

群作用　　対称性

A group can be viewed not only as an operation table, but also as a collection of transformations that move a set. This viewpoint is a group action.

Using group actions, we can directly describe how elements of a group move objects. Rotations of figures, permutations, and linear transformations by matrices are all examples of group actions.

→ Related page　lecture　math　linear-algebra

study.bem130.com

Linear transformations are included only as an application preview. The definitions and proofs on this page use only transformations that move elements of a set to other elements.

1　Definition of a group action

A group G acts on a set X if, for each $g \in G$ and $x \in X$, an element $g \cdot x \in X$ is defined and the following conditions hold.

$$e \cdot x = x$$

$$(gh) \cdot x = g \cdot (h \cdot x)$$

The first equation says that the identity element does nothing. The second says that multiplication in the group corresponds to composition of transformations.

2　Orbits

The orbit of an element $x \in X$ is defined by

$$Gx = \{ g \cdot x \mid g \in G \}$$

The orbit is the set of all elements reachable from x by the action of the group.
作用

3 Stabilizers

The set of group elements that do not move $x \in X$,

$$G_x = \{g \in G \mid g \cdot x = x\}$$

is called the stabilizer. It is a subgroup of G.
固定部分群 部分群

The orbit describes where an element can move, and the stabilizer describes what remains unchanged.

4 Concrete example: symmetries of an equilateral triangle

Let $X = \{1, 2, 3\}$ be the vertex set of an equilateral triangle. The rotational and reflection symmetries of the triangle permute the vertices. Therefore the symmetry group acts on X.

The orbit of vertex 1 is $\{1, 2, 3\}$, because a symmetry can move vertex 1 to any vertex. On the other hand, the symmetries that fix vertex 1 are the identity transformation and the reflection across the axis passing through vertex 1.

5 What changes and what is preserved

In a group action, elements of the group are viewed as transformations. What changes is the position of elements of the set. What is preserved is the structure that multiplication in the group corresponds to composition of transformations.
群作用

The idea of group actions appears widely in geometry, linear algebra, physics, and combinatorics.
幾何 線型代数 物理 組合せ論

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

A group action is a way to view a group as transformations of a set. An orbit is the range of possible movement, and a stabilizer is the symmetry that does not move an element. Group actions let us understand abstract groups as concrete transformations.

群作用 軌道 固定部分群

8 Theorem: orbit-stabilizer theorem

Let a finite group G act on a set X, and let $x \in X$. Then

有限群

$$| Gx | = [G : G_x]$$

Therefore, when G is finite,

$$| G | = | Gx | | G_x|$$

This is the orbit-stabilizer theorem.

軌道固定部分群定理

The idea of the proof is to match cosets with points in the orbit. Consider the map

証明 剰余類

$$G/G_x \to Gx, \qquad gG_x \mapsto g \cdot x$$

If $gG_x = hG_x$, then $h^{-1}g \in G_x$, so $(h^{-1}g) \cdot x = x$ and hence $g \cdot x = h \cdot x$. Thus the map is well-defined. Conversely, if $g \cdot x = h \cdot x$, then $h^{-1}g \in G_x$, so $gG_x = hG_x$. Therefore the map is a bijection.

Here a bijection means a map that sends different inputs to different outputs and reaches every element of the target. For finite sets, the existence of a bijection implies that the two sets have the same number of elements.

For the symmetry group of an equilateral triangle, the orbit of vertex 1 has 3 elements, and the stabilizer has 2 elements. Hence the order of the group is $3 \cdot 2 = 6$.
位数

9 Proof supplement: why the orbit-stabilizer theorem holds

Suppose a group G acts on a set X, and fix $x \in X$. Write the stabilizer of x as $G_x = \{g \in G \mid g \cdot x = x\}$.
群 固定部分群

Consider the map

$$G/G_x \to G \cdot x, \qquad gG_x \mapsto g \cdot x.$$

We check that this map is well-defined. If $gG_x = hG_x$, then $h^{-1}g \in G_x$. Therefore

$$(h^{-1}g) \cdot x = x.$$

Acting by h on the left gives $g \cdot x = h \cdot x$. Hence changing the representative does not change the output.

Conversely, if $g \cdot x = h \cdot x$, then $h^{-1}g \cdot x = x$, so $h^{-1}g \in G_x$ and therefore $gG_x = hG_x$. Thus the map is both injective and surjective. For a finite group,

$$| G \cdot x | = [G : G_x] = \frac{| G |}{| G_x |}$$

follows.

data/lecture/math/abstract-algebra/環の基本-講義.n.md md 4fe62c2

Basics of rings

環

A group was a structure with one operation. A ring is a structure with two operations at the same time: addition and multiplication.

群 演算 環 構造 加法 乗法

The reason to study rings is to handle integers, polynomials, matrices, and residue classes in the same language. They look different, but their addition and multiplication are connected by distributive laws.

整数 多項式 行列 剰余類 分配法則

1 Definition of a ring

A triple $(R, +, \cdot)$ consisting of a set R and two operations $+$ and $\cdot$ is a ring if it satisfies the following conditions.

集合 演算 環

First, $(R, +)$ is an abelian group. That is, addition has 0, and each element a has an additive inverse $-a$.

可換群 元 加法逆元

Next, multiplication is closed and satisfies the associative law.

結合法則

$$(ab)c = a(bc)$$

Furthermore, addition and multiplication are connected by the distributive laws.

分配法則

$$a(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

Many conventions require a multiplicative identity 1. In this material, unless stated otherwise, rings are treated as having a multiplicative identity.

乗法単位元

2 Why multiplicative inverses are not required

In the integer ring $\mathbb{Z}$, the multiplicative inverse of 2 does not exist among the integers. If the definition of a ring required every nonzero element to have a multiplicative inverse, the integers could not be treated as a ring.

定義

A ring does not require division. Instead, it preserves the structure in which addition and multiplication work together.

A commutative ring in which every nonzero element has a multiplicative inverse is a field.
体

→ Related page lecture math abstract-algebra

study.bem130.com

3 Basic examples

ring 環	Addition	Multiplication	Feature
$\mathbb{Z}$	Addition of integers	Multiplication of integers	Division is generally not closed
$\mathbb{Z}/n\mathbb{Z}$	Addition of residue classes	Multiplication of residue classes	Zero divisors appear when the modulus is composite
$F[x]$	Addition of polynomials	Multiplication of polynomials	Polynomial ring over a coefficient field F 体
$M_n(F)$	Addition of matrices	Matrix multiplication	Generally noncommutative

Because matrix multiplication is noncommutative, commutativity of multiplication is not always required in rings.

→ Related page lecture math linear-algebra

study.bem130.com

The example $M_n(F)$ is included as a standard noncommutative ring. The detailed theory of matrices is not needed for the definition of rings in this chapter.

4 What is preserved

In a ring (環), the additive group structure, the associativity of multiplication, and the distributive laws are preserved. Looking only at addition gives a group; looking only at multiplication gives a structure close to a monoid. Because the distributive law holds, calculations such as expansion and factorization are possible.

5 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

6 Summary

A ring (環) is an algebraic structure (代数的構造) that connects addition (加法) and multiplication (乗法) by distributive laws. It allows integers, polynomials, residue classes, and matrices to be treated in a common language. Because multiplicative inverses (乗法逆元) are not required for all elements, integers and polynomials are naturally included.

7 Supplement: units and the difference from fields

An element u of a ring (環) R is a unit (単元) if there exists $v \in R$ such that

$$uv = vu = 1$$

In a field (体), every nonzero element is a unit. In a general ring, however, only some elements are units.

For example, the only units in $\mathbb{Z}$ are 1 and -1. The element 2 is an element of $\mathbb{Z}$, but there is no integer v such that $2v = 1$. Thus in rings, being able to multiply and being able to divide must be distinguished.

8 Warning: noncommutative rings

In the matrix ring $M_n(F)$, generally $AB \neq BA$. Therefore, in ring calculations, the order of multiplication (順序) cannot be changed freely. When an argument uses commutativity, the assumption that the ring is commutative must be stated explicitly.

ideals and quotient rings

イデアル　　商環

To construct a quotient group from a group, a normal subgroup was needed. To construct a quotient ring from a ring, we need a subset that plays the corresponding role. That subset is an ideal.

商群　正規部分群　商環　環　イデアル

1 Definition of an ideal

イデアル

A subset I of a ring R is an ideal if $0 \in I$ and it satisfies the following conditions.

イデアル

$$a, b \in I \Rightarrow a - b \in I$$

$$r \in R,\ a \in I \Rightarrow ra \in I \text{ and } ar \in I$$

The condition $0 \in I$ makes I nonempty. The first condition says that I is a subgroup with respect to addition. The second says that multiplying by any element of the ring still leaves the result inside I.

部分群

In a commutative ring, ra and ar are the same, so it is enough to check one side.

2 Why ideals are necessary

イデアル

In a quotient ring, elements of I are treated as 0. In other words, a and b are treated as the same element when their difference belongs to I.

商環

$$a \sim b \iff a - b \in I$$

Using the equivalence classes built from this equivalence relation, we want to define

同値関係

$$[a] + [b] = [a + b]$$

$$[a][b] = [ab]$$

The ideal condition is necessary so that this multiplication is determined independently of representatives.

イデアル

Here the equivalence class of a can be written as $a + I = \{a + i \mid i \in I\}$. In a quotient ring, these classes are treated as the elements.

3 Example from the integers

$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is an ideal (イデアル) of $\mathbb{Z}$.

The quotient ring (商環)

$$\mathbb{Z}/n\mathbb{Z}$$

groups integers while ignoring differences that are multiples of n. This is exactly the world of congruences (合同式).

→ Related page lecture math abstract-algebra

study.bem130.com

4 Correspondence with quotient groups (商群)

Group theory	Ring theory
normal subgroup (正規部分群)	ideal (イデアル)
quotient group (商群)	quotient ring (商環)
Kernel of a group homomorphism (群準同型)	Kernel of a ring homomorphism (環準同型)
First isomorphism theorem (同型)	First isomorphism theorem (同型)

In both settings, the part collapsed as a kernel (核) is treated as 0 and a quotient is formed.

Ring homomorphisms and the first isomorphism theorem are treated later. This table is a roadmap showing that ideals will later appear as kernels.

5 What changes and what is preserved

In a quotient ring, differences inside the ideal are collapsed to 0. What changes is the granularity of elements. On the other hand, addition, multiplication, and distributive laws are preserved on the quotient in a well-defined way.

6 Proof supplement: why quotient-ring operations do not depend on representatives

Let I be an ideal of a ring R. Define the sum and product of residue classes by

$$(a+I)+(b+I)=(a+b)+I, \qquad (a+I)(b+I)=ab+I$$

We prove that this definition does not depend on representatives.

Suppose $a+I=a'+I$ and $b+I=b'+I$. This means $a'-a\in I$ and $b'-b\in I$. For addition,

$$(a'+b')-(a+b)=(a'-a)+(b'-b)\in I$$

so $(a'+b')+I=(a+b)+I$.

For multiplication,

$$a'b'-ab=a'b'-a'b+a'b-ab=a'(b'-b)+(a'-a)b$$

Since $b'-b\in I$ and I remains inside itself when multiplied by elements of the ring, $a'(b'-b)\in I$. Similarly, $(a'-a)b\in I$. Therefore $a'b'-ab\in I$, so $a'b'+I=ab+I$.

This proof shows that the ideal condition is exactly the condition needed so that multiplying classes of remainders does not break the quotient.

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

An ideal (イデアル) is the kind of subset needed to construct a quotient ring (商環). In a quotient ring (商環), elements of the ideal (イデアル) are treated as 0, and addition and multiplication are placed on the remaining residue classes. The ring $\mathbb{Z}/n\mathbb{Z}$ is the most basic example of a quotient ring (商環).

data/lecture/math/abstract-algebra/整域・零因子・多項式環-講義.n.md md 1726d54

integral domains, zero divisors, and polynomial rings

整域 零因子 多項式環

In a ring, the product of two nonzero elements may become 0. This phenomenon means that information is lost through multiplication. An element that causes this phenomenon is called a zero divisor.

環 零因子

1 Zero divisors

A nonzero element a of a ring R is a zero divisor if there exists a nonzero element b such that

零因子

$$ab = 0$$

or

$$ba = 0$$

For example, in $\mathbb{Z}/6\mathbb{Z}$,

$$[2][3] = [6] = [0]$$

Both $[2]$ and $[3]$ are nonzero, so they are zero divisors.

零因子

2 Integral domains

An integral domain is a commutative ring in which the product of nonzero elements is never 0. That is,

整域

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

holds.

The integer ring $\mathbb{Z}$ is an integral domain. The real field $\mathbb{R}$ is also an integral domain. On the other hand, $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

整域 体 整域 整域

3 Why integral domains are important

整域

In an integral domain, multiplying by a nonzero element does not destroy information. For example, if $a \neq 0$, then

整域

$$ab = ac \Rightarrow b = c$$

Indeed, moving all terms to one side gives

$$a(b - c) = 0$$

and since the ring is an integral domain, $b - c = 0$.

整域

No division is used here. We are not dividing by a nonzero element; we are using the absence of zero divisors

零因子

to cancel.

4 Polynomial rings

The set of all polynomials over a ring R,

$$R[x]$$

forms a ring. When the coefficients belong to a field F, the ring $F[x]$ is especially important.

体

In $F[x]$, one can use degree, division, irreducible polynomials, and related ideas to make arguments similar to those in number theory.

→ Related page lecture math algebra

study.bem130.com

5 Relation with fields

体

The formal definition of a field is given in the next lecture. In this section, as a preview, we use the following minimum meaning: a field is a commutative ring in which every nonzero element has a multiplicative inverse.

体

Every field is an integral domain. If $a \neq 0$ and $ab = 0$, multiplying by a^{-1} gives

$$b = 0$$

This step uses a^{-1}, so it is necessary to check that $a \neq 0$.

6 Proof supplement: why cancellation holds in an integral domain

In an integral domain, if $a \neq 0$ and $ab = ac$, then $b = c$.

Proof. From $ab = ac$,

$$ab - ac = 0$$

By the distributive law,

$$a(b - c) = 0$$

Since $a \neq 0$ and there are no zero divisors in an integral domain, $b - c = 0$ must hold. Hence $b = c$.

Here we do not divide symbolic expressions. Instead of dividing by a, we use the fact that if $a \neq 0$ and $a(b - c) = 0$, then $b - c = 0$ because zero divisors do not exist. Cancellation in a field can also be explained by multiplying by an inverse, but in an integral domain this proof is the essential one.

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A zero divisor is an element that makes the product of nonzero elements become 0. In an integral domain, such collapse does not occur. A polynomial ring is a basic example connecting ring theory with algebra and number theory.

9 Theorem: a polynomial ring over an integral domain is an integral domain

多項式環 整域 整域

If R is an integral domain, then $R[x]$ is also an integral domain.

整域 整域

Proof. Take nonzero polynomials $f(x), g(x) \in R[x]$. Let a be the leading coefficient of f, and let b be the leading coefficient of g. Since f and g are nonzero, $a \neq 0$ and $b \neq 0$. Because R is an integral domain, $ab \neq 0$.

整域

The leading coefficient of the product fg is ab, so fg is not the zero polynomial. Therefore the product of two nonzero polynomials is nonzero, and $R[x]$ is an integral domain.

整域

This theorem explains why arguments using degree work stably in the polynomial ring $F[x]$ over a field F.

多項式環 体

Basics of fields

体

A field is a commutative ring in which division by nonzero elements is possible. Fields are studied because they make computations in equations, linear algebra, and polynomials stable.

In the integers, the equation $2x = 1$ cannot be solved within the integers. In the rational numbers or real numbers, however, it has the solution $x = 1/2$. A field is the structure that expresses this difference.

1 Definition of a field

Definition of a field

A commutative ring F is a field if every nonzero element $a \in F$ has a multiplicative inverse.

$$\forall a \in F,\ a \neq 0 \Rightarrow \exists a^{-1} \in F \text{ such that } aa^{-1} = 1$$

It is important to exclude 0. The element 0 has no multiplicative inverse. If there were an element b such that $0b = 1$, the left-hand side would be 0, which is impossible.

2 Basic examples

Basic examples

$$\mathbb{Q},\quad \mathbb{R},\quad \mathbb{C}$$

are fields.

On the other hand, $\mathbb{Z}$ is not a field, because the multiplicative inverse $1/2$ of 2 is not an integer.

Also, when p is prime,

$$\mathbb{Z}/p\mathbb{Z}$$

is a field. For every nonzero residue class $[a]$, we have $\gcd(a, p) = 1$, so an inverse exists.

3 Why linear algebra works over fields

体

In linear algebra, operations that divide by coefficients appear frequently. For example, in Gaussian elimination, one divides by a nonzero number to make a pivot equal to 1.

掃き出し法　　主成分

→ Related page lecture math linear-algebra

study.bem130.com

This operation is justified because coefficients are elements of a field, and every nonzero element has an inverse.

体

This section is a preview of applications; results from linear algebra are not used as prerequisites for the later definitions or proofs about fields.

4 Fields and integral domains

整域

Every field is an integral domain. If $ab = 0$ and $a \neq 0$, then multiplying by a^{-1} gives

体　　整域

$$b = 0$$

This argument uses the condition $a \neq 0$. We are not dividing by 0; we are using the inverse of a nonzero element.

Conversely, not every integral domain is a field. The ring $\mathbb{Z}$ is an integral domain but not a field.

整域　　体　　整域　　体

5 What changes and what is preserved

Moving from rings to fields makes division by nonzero elements possible. What is preserved is addition, multiplication, distributive laws, and commutativity. What is added is a multiplicative inverse for every nonzero element.

体　　分配法則　　可換性　　乗法逆元

6 Proof supplement: every field is an integral domain

体 整域

A field has no zero divisors. That is, if $ab = 0$, then $a = 0$ or $b = 0$.

体 零因子

Proof. Suppose $ab = 0$, and assume $a \neq 0$. In a field, the nonzero element a has an inverse a^{-1}. Multiplying

体

by a^{-1} from the left gives

$$a^{-1}(ab) = a^{-1}0$$

By associativity, $(a^{-1}a)b = 0$, so $b = 0$. Therefore, if $ab = 0$, then $a = 0$ or $b = 0$.

Here a^{-1} is used only after checking $a \neq 0$. If $a = 0$, the conclusion already holds and no inverse is needed.

7 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

8 Summary

A field is a commutative ring in which every nonzero element has a multiplicative inverse. Because division

体 可換環 乗法逆元

is possible, basic operations in equations and linear algebra are naturally justified.

data/lecture/math/abstract-algebra/有限体の入口-講義.n.md md ff5949d

Entrance to finite fields

有限体

A finite field is a field with only finitely many elements. The important point is that division is possible even though the set is finite. Such fields appear in coding theory and cryptography.

The first example is

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

for a prime number p.

1 Why prime numbers are necessary

For $\mathbb{Z}/n\mathbb{Z}$ to be a field, every nonzero residue class must have an inverse.

The condition for $[a]$ to have an inverse is

$$\gcd(a, n) = 1$$

If $n = p$ is prime, then $[a] \neq [0]$ means $p \nmid a$. Therefore $\gcd(a, p) = 1$, so an inverse exists.

On the other hand, if n is composite and $n = ab$ with $1 < a, b < n$, then

$$[a][b] = [0]$$

while neither $[a]$ nor $[b]$ is 0. Since zero divisors exist, the structure is not a field.

2 Concrete example: F_5

$\mathbb{F}_5 = \{[0], [1], [2], [3], [4]\}$.

The inverse of $[2]$ is $[3]$ because

$$[2][3] = [6] = [1]$$

In this way, in a finite field, addition and multiplication can be completely described by finite tables.
有限体

3 Finite fields of prime-power order
体 位数

The number of elements in a finite field is always of the form
有限体

$$p^m$$

where p is prime and $m \geq 1$.

Proving this fact requires more preparation about finite fields. On this page, we use it only as a preview of the possible shapes of the number of elements.

The case $m = 1$ is $\mathbb{F}_p$. A finite field with $m > 1$ is not simply $\mathbb{Z}/p^m\mathbb{Z}$. Indeed, $\mathbb{Z}/4\mathbb{Z}$ has the zero-divisor relation $[2]^2 = [0]$, so it is not a field.
有限体 体

Higher-order finite fields are constructed as quotient rings by irreducible polynomials:
位数 有限体

$$\mathbb{F}_p[x]/(f(x))$$

where $f(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$.

An irreducible polynomial is a polynomial that cannot be factored into a product of two nonconstant polynomials over its coefficient field. This construction is a preview; the basic calculations on this page focus on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

4 What changes and what is preserved

In a finite field, the number of elements becomes finite. However, addition, multiplication, and division by nonzero elements are preserved as field operations. Finiteness makes these fields easy to handle computationally and useful in cryptography and error correction.
有限体 体 体

5 Proof supplement: every finite integral domain is a field

整域 体

A finite integral domain R is a field.

整域 体

Proof. Take $a \in R$ with $a \neq 0$. To show that R is a field, it is enough to show that a has a multiplicative inverse.

体

Consider the map

$$\mu_a : R \to R, \qquad x \mapsto ax$$

If $\mu_a(x) = \mu_a(y)$, then $ax = ay$. Since $a \neq 0$ and R is an integral domain, cancellation gives $x = y$. Therefore μ_a is injective.

整域 単射

Because R is a finite set, every injective map from R to R is surjective. Hence for $1 \in R$, there exists $x \in R$ such that $ax = 1$. This means that x is the inverse of a.

単射 全射

Finiteness is used exactly at the step where injective implies surjective. For a finite set, injectivity means the image has as many elements as the domain, and the target has the same size as the domain, so every target element is reached. For infinite sets, that inference is not valid in general.

単射 全射

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

A finite field is a field with finitely many elements. The ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field when p is prime, but composite moduli produce zero divisors and do not give fields. General finite fields have a prime-power number of elements.

有限体 体 有限体 零因子 体 有限体

8 Example: a finite field with 4 elements

有限体

The ring $\mathbb{Z}/4\mathbb{Z}$ is not a field, but a finite field with 4 elements does exist. In $\mathbb{F}_2[x]$, consider

体 有限体

$$f(x) = x^2 + x + 1$$

This polynomial has no root over $\mathbb{F}_2$, so it is irreducible. Define

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$$

Write $\alpha = [x]$. From the relation

$$\alpha^2 + \alpha + 1 = 0$$

and characteristic 2, we get

$$\alpha^2 = \alpha + 1$$

Thus the elements are

$$0,\ 1,\ \alpha,\ \alpha + 1$$

This example shows that finite fields of prime-power order are not simply $\mathbb{Z}/p^m\mathbb{Z}$ they appear as quotient rings by irreducible polynomials.

有限体 位数

For polynomials of degree 2 or 3, having no root implies irreducibility. Characteristic 2 means that $1 + 1 = 0$ holds.

data/lecture/math/abstract-algebra/準同型の基本-講義.n.md md 1e7b436

Basics of homomorphisms

準同型

A homomorphism is a map that preserves operations. In abstract algebra, not only the objects themselves but also the maps that move between objects without breaking structure are important.

Just as a linear map in linear algebra preserves addition and scalar multiplication, a homomorphism in abstract algebra preserves the operations of groups or rings.

→ Related page lecture math linear-algebra

study.bem130.com

This analogy is only a preview. The definitions and proofs on this page use only groups, rings, and maps introduced earlier.

1 Group homomorphisms

準同型

A map $\varphi : G \to H$ between groups G, H is a group homomorphism if it satisfies

群準同型

$$\varphi(ab) = \varphi(a)\varphi(b)$$

From this condition, identity elements and inverses are also preserved.

2 Ring homomorphisms

準同型

A map $\varphi : R \to S$ between rings R, S is a ring homomorphism if it satisfies

環準同型

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

For rings with identity, many conventions additionally require

$$\varphi(1_R) = 1_S$$

In this material, a ring homomorphism is taken by default to preserve the identity element.
環準同型 単位元

3 Kernel and image
像

The kernel of a homomorphism is the part collapsed to the identity element or to 0.
核 準同型 単位元

For a group homomorphism,
群準同型

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}$$

For a ring homomorphism,
環準同型

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0_S\}$$

The image is the set of all elements actually reached:
像

$$\mathrm{Im}\, \varphi = \{\varphi(x) \mid x \in \text{domain}\}$$

4 What changes and what is preserved

In a homomorphism, the names or representations of elements may change. However, operating first and then mapping gives the same result as mapping first and then operating. In this sense, a homomorphism is a structure-preserving map.
準同型 準同型

An isomorphism is an invertible homomorphism. When an isomorphism exists, the structure is completely preserved.
同型 準同型 同型

5 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

6 Summary

A homomorphism is a map that preserves operations. A group homomorphism preserves the group product, and a ring homomorphism preserves addition and multiplication. The kernel is the part collapsed, the image is the part reached, and these concepts lead to quotient structures and homomorphism theorems.

7 Example: evaluation maps are ring homomorphisms

For a field F and $c \in F$, the map from the polynomial ring $F[x]$ to F defined by

$$\mathrm{ev}_c : F[x] \to F, \qquad f(x) \mapsto f(c)$$

is called the evaluation map. It is a ring homomorphism because

$$\mathrm{ev}_c(f+g) = f(c) + g(c)$$

and

$$\mathrm{ev}_c(fg) = f(c)g(c)$$

hold.

The kernel of this map is the set of all polynomials that have c as a root:

$$\ker(\mathrm{ev}_c) = \{ f(x) \in F[x] \mid f(c) = 0 \}$$

The fact that this kernel is an ideal is a basic example connecting homomorphisms with quotient rings.

8 Proof supplement: the kernel of a ring homomorphism is an ideal

Let $\varphi : R \to S$ be a ring homomorphism. Define its kernel by

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0 \}.$$

First, $\varphi(0_R) = 0_S$, so $0_R \in \ker \varphi$ hence the kernel is nonempty. If $a, b \in \ker \varphi$, then

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0,$$

so $a - b \in \ker \varphi$. Also, if $r \in R$ and $a \in \ker \varphi$, then

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0, \qquad \varphi(ar) = \varphi(a)\varphi(r) = 0\varphi(r) = 0,$$

so $ra, ar \in \ker \varphi$. Therefore the kernel of a ring homomorphism is an ideal.
核 環準同型 イデアル

The image $\operatorname{Im} \varphi$ is closed under sums, differences, and products. In the convention where ring homomorphisms preserve identity elements, $\varphi(1_R) = 1_S$ as well, so the image can be treated as a subring of S with the inherited operations.
像

data/lecture/math/abstract-algebra/準同型定理の見取り図-講義.n.md md 2e84104

Overview of the homomorphism theorem

準同型定理

The central idea of the homomorphism theorem is simple. If elements that collapse to the same value under a homomorphism are first identified, the remaining structure is the same as the image.

準同型定理　準同型　像

This viewpoint is common to groups, rings, and linear algebra.

群　環

→ Related page lecture math linear-algebra

study.bem130.com

Linear algebra is included only as an analogy. The proofs on this page use only kernels, images, and quotients already introduced for groups and rings.

1 Form of the first homomorphism theorem

準同型

For a group homomorphism $\varphi : G \to H$,

群準同型

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

holds.

For a ring homomorphism $\varphi : R \to S$, the same form holds:

環準同型

$$R/\ker\varphi \cong \operatorname{Im}\varphi$$

The formula has the same shape. The difference is that in group theory the kernel is a normal subgroup, while in ring theory the kernel is an ideal.

核　正規部分群　核　イデアル

2 Why this happens

The map φ sends elements in the kernel to the identity element or to 0. Therefore elements that differ only by the kernel have the same image.

核　単位元　核　像

In the group case, consider the map that sends the coset
剰余類

$$g \ker \varphi$$

to

$$\varphi(g)$$

This map is independent of the choice of representative. If $g \ker \varphi = g' \ker \varphi$, then $g^{-1}g' \in \ker \varphi$, so $\varphi(g) = \varphi(g')$.

This argument uses inverses, so the group structure is needed.

3 Correspondence with linear algebra

For a linear map $T : V \to W$, the kernel is
核

$$\ker T = \{v \in V \mid T(v) = 0\}$$

and the image is
像

$$\operatorname{Im} T = \{T(v) \mid v \in V\}$$

Collapsing the kernel directions leaves the degrees of freedom that become the image. This intuition connects
核
像
to rank, degeneracy, and quotient spaces.

→ Related page lecture math linear-algebra

study.bem130.com

This correspondence is only a preview; the first homomorphism theorem is not being proved by using theorems about linear maps.

4 What changes and what is preserved

In the homomorphism theorem, differences inside the kernel are collapsed. What changes is the fineness with which elements are distinguished. What is preserved is the structure actually observable through the homomorphism, namely the image.

5 Proof supplement: proof of the first isomorphism theorem

Let $\varphi : G \to H$ be a group homomorphism. The first isomorphism theorem states that

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

Here we prove the group case. The ring case follows the same strategy, with ideals used in place of normal subgroups.

Define the map

$$\Phi : G/\ker\varphi \to \operatorname{Im}\varphi, \qquad g\ker\varphi \mapsto \varphi(g)$$

First show that it is well-defined. If $g\ker\varphi = g'\ker\varphi$, then $g'^{-1}g \in \ker\varphi$. Hence

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

and $\varphi(g')^{-1}\varphi(g) = e$, so $\varphi(g) = \varphi(g')$.

Next, Φ is a homomorphism:

$$\Phi((g\ker\varphi)(h\ker\varphi)) = \Phi(gh\ker\varphi) = \varphi(gh) = \varphi(g)\varphi(h)$$

Surjectivity follows from the definition of the image. Injectivity follows because if $\Phi(g\ker\varphi) = e$, then $\varphi(g) = e$, so $g \in \ker\varphi$ and therefore $g\ker\varphi = \ker\varphi$.

Thus Φ is an isomorphism, and $G/\ker\varphi \cong \operatorname{Im}\varphi$. The content of the proof is the intuition that after collapsing the kernel and then mapping, exactly the image remains.

6 Exercise link

→ Related page exercise math abstract-algebra

study.bem130.com

7 Summary

The first homomorphism theorem says that "quotienting by the kernel gives the image." The same form appears for groups, rings, and linear maps, making it an important overview that connects abstract algebra with linear algebra.

準同型 核 像 抽象代数