# I216
# Computational Complexity
# and
# Discrete Mathematics

by
Prof. Ryuhei Uehara

# I216
# 計算量の理論
# と
# 離散数学

上原隆平

# I216
# Computational Complexity
# and
# Discrete Mathematics

Aim:

Learn discrete mathematics

- Introduction to Group, Ring, Field, Number theory

Maybe, one report will be…

Final exam will be on November 28th.

# I216
# 計算量の理論
# と
# 離散数学

目的:

離散数学の学習

　群，環，体，数論への入門

今のところレポート1回の予定

期末試験は11月28日.

# Textbooks and references

## English

- *A Course in Computational Algebraic Number Theory*, H. Cohen, Springer, 1993.
- *A Computational Introduction to Number Theory and Algebra*, V. Shoup, Cambridge, 2008. http://www.shoup.net/ntb

## Japanese

- *IT Text 情報セキュリティ*, 宮地充子, 菊池浩明, オーム社, 2003.
- *群・環・体入門*, 新妻弘, 木村哲三, 共立出版, 1999.

# 8
# Group(1)
# Axiom of Group
# Subgroup

# 第8回
# 群(1) 群の公理，部分群

# Today's topic:

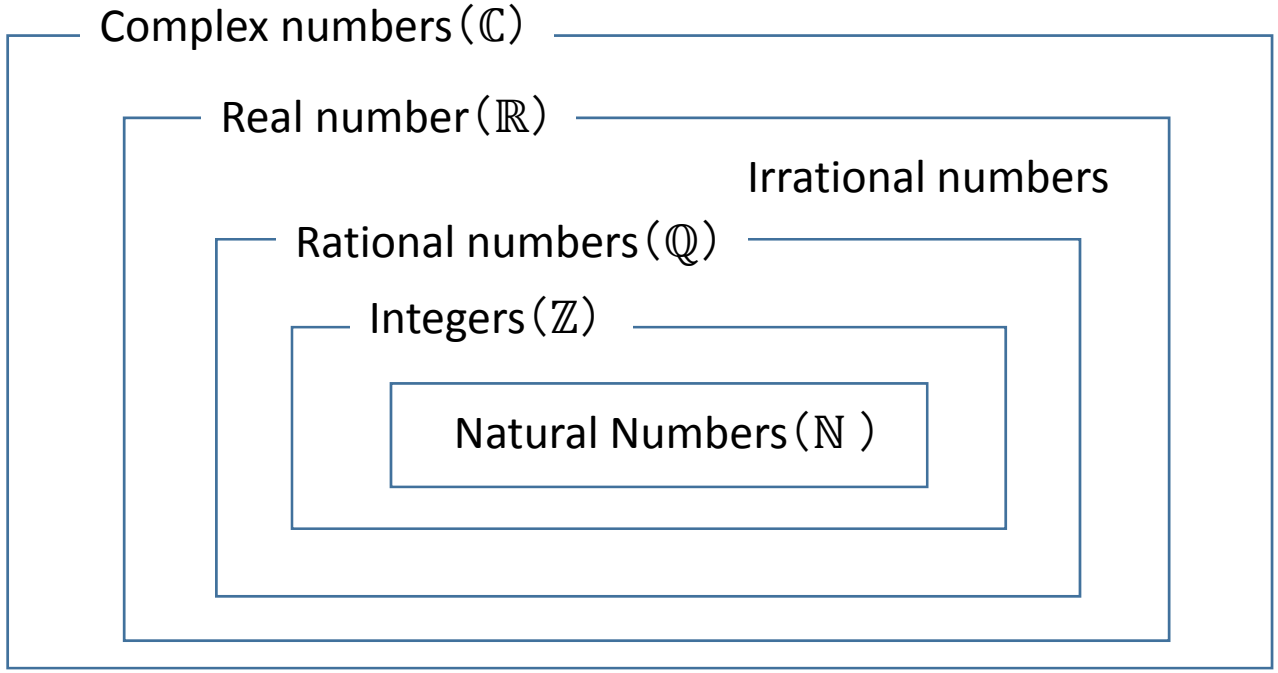
- Introduction
- Semi group
- Identity element , inverse
- Group
- Subgroup, Cyclic group
- Generating from element, order

# 本講義の内容

- はじめに
- 半群
- 単位元，逆元
- 群
- 部分群，巡回群
- 生成元，位数

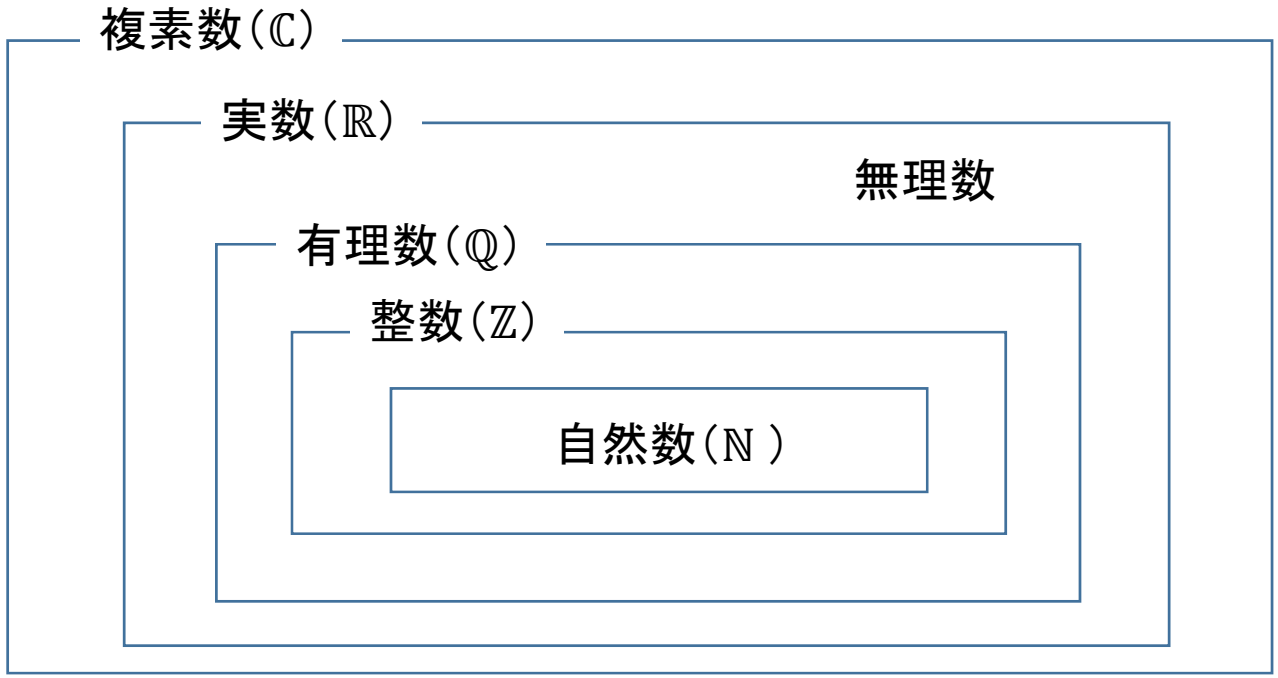
# Background: Extension of numbers

- … to solve equation
- It is important to be close under operations
  - For example, it is known that equations with coefficients of complex numbers have their solutions in complex numbers.



# 背景：数の世界を広げる

- 方程式を解くために数の世界を広げてきた
- 演算に関して閉じていることが重要
  - 複素数を係数とする代数方程式は複素数の範囲で解を持つことが知られている



# Binary relationship

## Definition 8.1

- For a given set $G$, suppose that a mapping from $G \times G$ to $G$ is given. This mapping is called a binary relation of $G$. The image of an element $(a, b)$ in $G \times G$ by this mapping is called *product* of $a$ and $b$, denoted by $a \cdot b$ or $ab$. Then, we say that a binary operation (or just operation for short) is given to the set $G$, and denote by $(G, \cdot)$.

## Examples of binary operations

- Arithmetic operations (+,-, ×,/), set union (∪)

Binary relation has an important property; it is closed under binary operation

- "＋"
  - Natural number＋natural number＝natural number
  - We say that natural numbers are "*closed* with respect to operation +."
- "－"
  - Integer－integer＝integer
  - The set of Integers is "closed with respect to (or under) operation －."

# 二項演算

定義8.1

- 集合$G$の直積集合$G \times G$から$G$への写像が1つ与えられているとする．この写像を$G$の二項演算という．$G \times G$の元$(a, b)$のこの写像による像を$a$と$b$の積といい，$a \cdot b$または$ab$で表す．また，このとき集合$G$に1つの二項演算（あるいは単に演算）が与えられているといい，$(G, \cdot)$と表す．

二項演算子

- 四則演算や和集合など

二項演算は，演算に関して閉じているという重要な性質を持つ

- 「＋」
  - 自然数＋自然数＝自然数
  - 自然数は「＋という演算に関して閉じている」という
- 「－」
  - 整数－整数＝整数
  - 整数は「－という演算に関して閉じている」という

# Overview of Group・Ring・Field

- Field
  - Like set of real numbers, arithmetic operations (＋, －, ×, /) can be defined over the set.
- Finite field
  - Sets consists of discrete and finite elements, and we can define arithmetic operations.
  - In cryptography/coding theories, we need this notion since we cannot deal with real numbers directly.
- Ring
  - Sets without “identity element”, “inverse”, “commutative” for products in the properties of fields
- Group
  - Sets with one operation that satisfies “closed”, “identity element”, “inverse”, and “associativity”.
- Intuitively, group has ＋ and －, ring has ＋, －, and ×, and field has ＋, －, ×, and ／, respectively.

# 群・環・体

- 体
  - 実数の集合のように，その上で加減乗除の四則演算が定義できる集合
- 有限体
  - 離散的な有限個の要素からなり，四則演算が定義できる集合
  - 暗号や符号等では実数を直接取り扱うことができないためこれが必要
- 環
  - 体の条件のうち，乗法に関する「単位元の存在」「逆元の存在」「可換則」の条件を除いたものを満たす集合
- 群
  - 1つの演算が定義されていて，その1つの演算に関して「演算が閉じている」「単位元の存在」「逆元の存在」「結合則」の条件を満たす集合
- 直感的には，群は加減算，環は加減乗算，体は加減乗除算が定義されている集合と考えることができる

# Semi group

## Definition 8.2

- For a set $A$ and operation $\cdot$, if $(A, \cdot)$ satisfies the following conditions, it is said a semi group:
  - For any $A \ni a, b$, $a \cdot b \in A$ (That is, $A$ is closed under $\cdot$)
  - For any $A \ni a, b, c$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ （associative law）

## Exercise

- $(\mathbb{Z}, +)$ is a semi group
  - For any $\mathbb{Z} \ni a, b$, we have $a + b \in \mathbb{Z}$
  - For any $\mathbb{Z} \ni a, b, c$, we have $(a + b) + c = a + (b + c)$
- Is $(\mathbb{Z}, \times)$ a semi group?

- A semi group is a group if it has an identity element, and every element has its inverse.

# 半群

**定義8.2**

- 集合$A$が演算$\cdot$に対して以下を満たすとき，$(A, \cdot)$を半群という
  - $A \ni a, b$に対して，$a \cdot b \in A$ （演算に関して閉じている）
  - $A \ni a, b, c$に対して，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ （結合律）

**例題**

- $(\mathbb{Z}, +)$は半群
  - $\mathbb{Z} \ni a, b$に対して，$a + b \in \mathbb{Z}$
  - $\mathbb{Z} \ni a, b, c$に対して，$(a + b) + c = a + (b + c)$
- $(\mathbb{Z}, \times)$は半群？

- 半群は，単位元を持ち，全ての元が逆元をもつと群になる

# Identity element

## Definition 8.3

- An element $e$ in a semi group $(A,\ \cdot)$ is called an identity element if it satisfy the following for $A \ni \forall x$

$$e \cdot x = x \cdot e = x$$

## Exercise

- For a semi group $(\mathbb{Z},\ +)$, does it have an identity element?
  - It should satisfy $\mathbb{Z} \ni \forall a,\ [\quad] + a = a + [\quad] = a$
- For a semi group $(\mathbb{Z},\ \times)$, does it have an identity element?
  - It should satisfy $\mathbb{Z} \ni \forall a\ ,\ [\quad] \times a = a \times [\quad] = a$

# 単位元

## 定義8.3

- 半群$(A, \cdot)$の元$e$が，$A \ni \forall x$に対して以下を満たすとき，$e$を単位元とよぶ

$$e \cdot x = x \cdot e = x$$

## 例題

- $(\mathbb{Z}, +)$は半群で，単位元は？
  - $\mathbb{Z} \ni \forall a$に対して，$[\quad] + a = a + [\quad] = a$
- $(\mathbb{Z}, \times)$は半群で，単位元は？
  - $\mathbb{Z} \ni \forall a$に対して，$[\quad] \times a = a \times [\quad] = a$

# Uniqueness of an identity element

## Theorem 8.1

For a semi group $(A, \cdot)$, if $A$ has an identity element $e$, it is unique.

## Proof

Suppose that $e, f$ are elements such that both satisfy $ae = a, fa = a$ for any $a \in A$. Then, for $e$, we have $fe = f$. On the other hand, for $f$, we have $fe = e$. Therefore, we have $f = e$.

## Definition 8.4

- If a semi group $(A, \cdot)$ has the identity element, $A$ is called monoid.

## Exercise

- Are $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \times)$ monoids?

# 単位元の一意性

## 定理8.1

- 半群$(A, \cdot)$に対して，$A$に単位元$e$が存在すれば一意的である

## 証明

- $e, f$が，それぞれ $ae = a, fa = a$ を満たす元とする．このとき，$e$に関して，$fe = f$．一方，$f$に関して，$fe = e$が成り立つ．よって，$f = e$となる．

## 定義8.4

- 半群$(A, \cdot)$に単位元が存在するとき，$A$をモノイド（monoid）という

## 例題

- $(\mathbb{Z}, +)$ および $(\mathbb{Z}, \times)$ はモノイド？

# Inverse element

## Definition 8.5

- For an element $u$ of a monoid $(A, \cdot)$, if an element $u'$ in $A$ satisfies

$$u \cdot u' = u' \cdot u = e$$

$u$ is a regular element in $A$, and $u'$ is the inverse element of $u$.

## Theorem 8.2

- For a regular element $u$ in a monoid $(A, \cdot)$, its inverse element is unique.

## Proof

- Suppose that we have two inverse elements $u'$, $u''$ of an element $u$. Then, by associative law, we have the following;

$$u' = u' \cdot e = u' \cdot (u \cdot u'') = (u' \cdot u) \cdot u'' = e \cdot u'' = u''$$

- For a regular element $u$ of a monoid $(A, \cdot)$, its inverse element is denoted by $u^{-1}$.

# 逆元

定義8.5

- モノイド$(A, \cdot)$の元$u$に対して，$A$の元$u'$が以下を満たすとき，$u$を$A$の正則元であるといい，$u'$を$u$の逆元とよぶ

$$u \cdot u' = u' \cdot u = e$$

定理8.2

- モノイド$(A, \cdot)$の正則元$u$に対して，その逆元は一意的に存在する

証明

- $u', u''$がともに$u$の逆元であるとする．このとき，結合律を用いて以下が成り立つ

$$u' = u' \cdot e = u' \cdot (u \cdot u'') = (u' \cdot u) \cdot u'' = e \cdot u'' = u''$$

- モノイド$(A, \cdot)$の正則元$u$の逆元を$u^{-1}$で表す

# Group

## Definition 8.6

- For a monoid $(A,\ \cdot)$, if $A \ni \forall a$ has its inverse element $a^{-1}$, $A$ is called a group.

## Definition 8.7 (Axioms of Group)

If a set $G$ and operation $\cdot$ satisfy the following, $G$ is called a group:

①(Closed under the operation) For any $G \ni a, b$, we have $a \cdot b \in G$

②(Associative) For any $G \ni a, b, c$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

③(Identity element) There is an element $e \in G$ such that

$$e \cdot a = a \cdot e = a \text{ for any } G \ni \forall a$$

④(Inverse) For each $G \ni \forall a$, there is an element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

Moreover, $G$ is called commutative group or abelian group if it satisfies

⑤(commutative) $a \cdot b = b \cdot a$

- A group is called finite group if it consists of finite elements.

# 群

- 定義8.6
  - モノイド$(A, \cdot)$が$A \ni \forall a$に対して逆元$a^{-1}$を持つとき，$A$を群（group）とよぶ
- 定義8.7（群の公理）
  - 集合$G$が演算$\cdot$に対して以下を満たすとき，$G$を群という
  - ①（演算に関して閉じている）$G \ni a, b$に対して，$a \cdot b \in G$
  - ②（結合律）$G \ni a, b, c$に対して，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - ③（単位元の存在）$G \ni \forall a$に対して，$e \cdot a = a \cdot e = a$となる$e \in G$が存在
  - ④（逆元の存在）$G \ni \forall a$について，$a \cdot a^{-1} = a^{-1} \cdot a = e$となる$a^{-1} \in G$が存在
- さらに以下を満たすとき$G$を可換群，またはアーベル群とよぶ
  - ⑤（可換律）$a \cdot b = b \cdot a$
- 元の個数が有限個の群を有限群とよぶ

# Examples of groups

## Exercise 8.1

- $(\mathbb{Z},\ +)$ is a monoid with the identity element 0
- What is the inverse element of $\mathbb{Z} \ni \forall a$?
  - $[\ \ ] + a = a + [\ \ ] = 0$
- Any element in $\mathbb{Z}$ is a regular element with respect to addition.
- Is $(\mathbb{Z},\ +)$ a group?

## Exercise 8.2

- $(\mathbb{Z},\ \times)$ is a monoid with the identity element 1
- What is the inverse element of $\mathbb{Z} \ni 3$?
  - $[\ \ ] \times 3 = 3 \times [\ \ ] = 1$
- $\mathbb{Z}$ has an element which is not regular with respect to multiplication.
- Is $(\mathbb{Z},\ \times)$ a group?

# 群の例

## 例題8.1

- $(\mathbb{Z},\ +)$はモノイド，単位元は0
- $\mathbb{Z} \ni \forall a$の逆元は？
  - $[\quad] + a = a + [\quad] = 0$
- $\mathbb{Z}$の任意の元は加法に関して正則元となる
- $(\mathbb{Z},\ +)$は群？

## 例題8.2

- $(\mathbb{Z},\ \times)$はモノイド，単位元は1
- $\mathbb{Z} \ni 3$の逆元は？
  - $[\quad] \times 3 = 3 \times [\quad] = 1$
- $\mathbb{Z}$には乗法に関して正則元とならない元がある
- $(\mathbb{Z},\ \times)$は群？

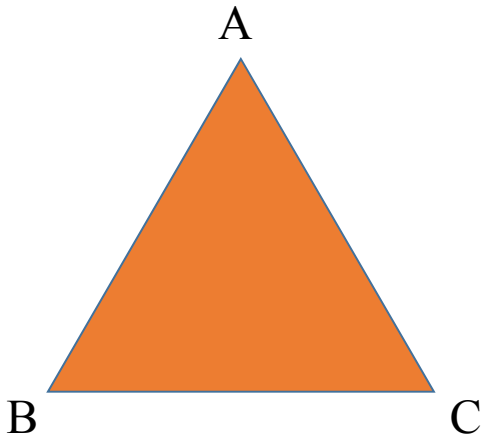
# Non-numerical group (rotation of a triangle)

## Definition of elements

- $r$ : rotation equilateral triangle ($\triangle$) 120° clockwise
- $\ell$ : rotation $\triangle$ 120° counterclockwise
- $a$ : flip along the vertical line
- $b$ : flip along the line of 60° passing down-left corner
- $c$ : flip along the line of -60° passing down-right corner
- $e$ : do nothing

## Definition of an operation

- $a \circ r$ : operate $a$ after operation $r$




| $\circ$ | $e$ | $r$ | $\ell$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $\ell$ | $a$ | $b$ | $c$ |
| $r$ | $r$ | $\ell$ | $e$ | $b$ | $c$ | $a$ |
| $\ell$ | $\ell$ | $e$ | $r$ | $c$ | $a$ | $b$ |
| $a$ | $a$ | $c$ | $b$ | $e$ | $\ell$ | $r$ |
| $b$ | $b$ | $a$ | $c$ | $r$ | $e$ | $\ell$ |
| $c$ | $c$ | $b$ | $a$ | $\ell$ | $r$ | $e$ |

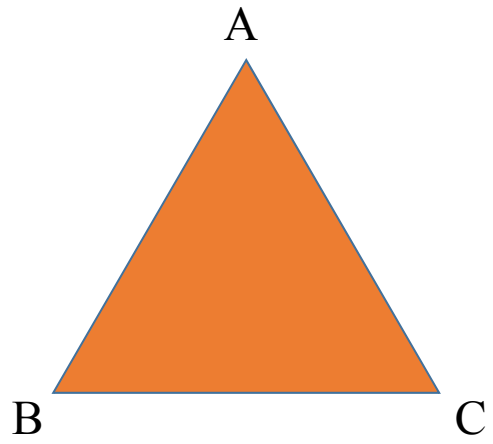
# 数以外の群（三角形の回転）を考える

## 次の元を定義

- $r$：正三角形を右に120度回転させる操作
- $\ell$：正三角形を左に120度回転させる操作
- $a$：上を頂点として左右対称に回転する操作
- $b$：左下を頂点として左右対称に回転する操作
- $c$：右下を頂点として左右対称に回転する操作
- $e$：何もしない

## 演算を定義

- $a \circ r$：操作$r$をしてから操作$a$をする




| $\circ$ | $e$ | $r$ | $\ell$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $\ell$ | $a$ | $b$ | $c$ |
| $r$ | $r$ | $\ell$ | $e$ | $b$ | $c$ | $a$ |
| $\ell$ | $\ell$ | $e$ | $r$ | $c$ | $a$ | $b$ |
| $a$ | $a$ | $c$ | $b$ | $e$ | $\ell$ | $r$ |
| $b$ | $b$ | $a$ | $c$ | $r$ | $e$ | $\ell$ |
| $c$ | $c$ | $b$ | $a$ | $\ell$ | $r$ | $e$ |

# Check the rotation system is a group

Confirm that $G = \{e, r, \ell, a, b, c\}$ is a group:

- (Closed under the operation)
  - It is clear the table in the previous page.
  - However, it is not commutable→it is not an abelian group
- (Associative)
  - $(r \circ a) \circ b = r \circ (a \circ b) = \ell$
- (An identity element)
  - $e$ is an identity element
- (Inverse element)
  - The inverse of $r$ is $\ell$, the inverse of $a$ is $a$, etc.

# 三角形の回転が群であることを確かめる

$G = \{e, r, \ell, a, b, c\}$が群であることを確認する

- （演算に関して閉じている）
  - 前ページの群表より明らか
  - ただし，可換律は成り立たない→アーベル群ではない
- （結合律）
  - $(r \circ a) \circ b = r \circ (a \circ b) = \ell$ など
- （単位元の存在）
  - $e$が単位元
- （逆元の存在）
  - $r$の逆元は$\ell$，$a$の逆元は$a$ など

# Example of proof of group

## Exercise 8.3

- Show the set $\mathbb{Q}[\sqrt{2}]^*$ which is obtained by removing 0 from $\mathbb{Q}[\sqrt{2}]$ is a group with respect to multiplication. (Here, we assume that arithmetic operations over $\mathbb{Q}$ are defined in a usual way.)

## Proof (outline)

Follow the axioms of group;

① For any $x, y \in \mathbb{Q}[\sqrt{2}]^*$, show it is closed under multiplication.

② For any $x, y, z \in \mathbb{Q}[\sqrt{2}]^*$, show they satisfy associative law.

③ Show there is an identification element.

④ Show there is an inverse for any $x \in \mathbb{Q}[\sqrt{2}]^*$.

# 群であることの証明例

## 例題8.3

- $\mathbb{Q}[\sqrt{2}]$から0を除いた集合$\mathbb{Q}[\sqrt{2}]^*$は乗法に関して群になることを示せ
  （ただし，$\mathbb{Q}$上の四則演算は定義されているとする）

## 証明（方針）

群の公理にしたがって証明

① $x, y \in \mathbb{Q}[\sqrt{2}]^*$に対して，乗法に関して閉じていることを示す

② $x, y, z \in \mathbb{Q}[\sqrt{2}]^*$に対して，結合律を満足することを示す

③ 単位元の存在を示す

④ 任意の元に対する逆元の存在を示す

# Example of proof of closeness of operation

## Exercise 8.4

- Let $S = \mathbb{R} \setminus \{-1\}$ and consider an operation defined by $a \circ b = a + b + ab$. Then prove that "$\circ$" is an operation on $S$. Here, we suppose that arithmetic operations over $\mathbb{R}$ are defined.

## Proof (Outline)

It is sufficient to show that $a, b \in S \Rightarrow a \circ b \in S$.

It is equivalent to $a \neq -1$ and $b \neq -1 \Rightarrow a \circ b \neq -1$ since $a \in S \Leftrightarrow a \neq -1$

We can show that by contraposition.

# 演算に関して閉じていることの証明例

- 例題8.4
  - $S = \mathbb{R} \setminus \{-1\}$として演算$a \circ b = a + b + ab$を考える．「$\circ$」が$S$上の演算であることを示せ（ただし，$\mathbb{R}$上の四則演算が成り立つとする）

- 証明（方針）
  - $a, b \in S \Rightarrow a \circ b \in S$であることを示せばよい
    - $a \in S \Leftrightarrow a \neq -1$であることに注意すると，$a \neq -1$ and $b \neq -1 \Rightarrow a \circ b \neq -1$と同値
  - 対偶で示す

# Subgroup（1/2）

Definition 8.8

For a group $G$, if its subset $H$ itself is a group with the same operation over $G$, $H$ is called a subgroup of $G$. Precisely,

① For any $H \ni a, b,$ we have $a \cdot b \in H$,

② For any $H \ni a, b, c$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

③ $e \in H$ exists, and

④ For any $\forall a \in H,$ its inverse $a^{-1} \in H$ exists.

To show a subset being a subgroup, the following theorem is useful;

# 部分群(1/2)

- 定義8.8
  - 群$G$の部分集合$H$において，$G$の乗法を$H$の上に制限して考えて，$H$自身が群になるとき，$H$を$G$の部分群(subgroup)という，つまり，
  - ① $H \ni a, b$に対して，$a \cdot b \in H$
  - ② $H \ni a, b, c$に対して，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - ③ $e \in H$が存在
  - ④ $\forall a \in H$に対して，$a^{-1} \in H$が存在
- 部分群であることを示すには次の定理が有効

# Subgroup (2/2)

## Theorem 8.3 (Decision theorem for subgroup)

Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$ if and only if $H$ satisfies the following two conditions (1) and (2):

(1) $\forall a, b \in H \Rightarrow a \cdot b \in H$

(2) $\forall a \in H \Rightarrow a^{-1} \in H$

Moreover, two conditions (1) and (2) are equivalent to the following single condition:

(3) For $\forall a, b \in H$, we have $a \cdot b^{-1} \in H$

## Proof of equivalence

($\Rightarrow$) If $H$ is a subgroup of $G$, it is clear that for $\forall a, b \in H$, we have $a \cdot b^{-1} \in H$.

($\Leftarrow$) It is sufficient to show that $H$ satisfies the axioms of group when (3) holds.

(Identity element) For any $H \ni a, a$ since $a \cdot a^{-1} = e \in H$, the identity element of $G$ is in $H$.

(Inverse) $H \ni e, \forall a,$ we have $e \cdot a^{-1} = a^{-1} \in H$. Thus, every element has its inverse in $H$ $\Rightarrow$ We have (2)

(Closed under operation) For any $H \ni a, b$ , since its inverse exists in $H$, we have $H \ni a, b^{-1}$ and hence $a \cdot (b^{-1})^{-1} = a \cdot b \in H$ $\Rightarrow$ We have (1)

(Associative) Trivial.

# 部分群(2/2)

## 定理8.3(部分群の判定定理)

群$G$の空でない部分集合を$H$とする．$H$が部分群であるための必要十分条件は，$H$が次の条件(1)(2)を満足していることである．

(1) $\forall a, b \in H \Rightarrow a \cdot b \in H$

(2) $\forall a \in H \Rightarrow a^{-1} \in H$

さらに(1)(2)は，次の条件(3)と同値である

(3) $\forall a, b \in H$に対して$a \cdot b^{-1} \in H$

## 同値の証明

(⇒) $H$が$G$の部分群であれば，$\forall a, b \in H$に対して$a \cdot b^{-1} \in H$は明らか

(⇐) (3)を満たすとき，$H$が群の公理を満たすことを示せばよい

(単位元の存在) $H \ni a, a$ について，$a \cdot a^{-1} = e \in H$より単位元が存在

(逆元の存在) $H \ni e, \forall a$ について，$e \cdot a^{-1} = a^{-1} \in H$より任意の元に逆元が存在　⇒(2)を満たす

(演算に関して閉じている) $H \ni a, b$ に対して，逆元が存在するため$H \ni a, b^{-1}$であり，$a \cdot (b^{-1})^{-1} = a \cdot b \in H$　⇒(1)を満たす

(結合律)自明

# Check subgroups of the group defined by rotation of $\triangle$

$G = \{e, r, \ell, a, b, c\}$ has 6 subgroups defined by the following 6 subsets;

$$\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e\}$$

For example, show that the subset$\{e, r, \ell\}$ is a subgroup of $G$;

$$e \circ r^{-1} = e \circ \ell = \ell$$
$$e \circ \ell^{-1} = e \circ r = r$$
$$r \circ \ell^{-1} = r \circ r = \ell$$
$$r \circ e^{-1} = r \circ e = r$$
$$\ell \circ e^{-1} = \ell \circ e = \ell$$
$$\ell \circ r^{-1} = \ell \circ \ell = r$$

That implies we have $a \cdot b^{-1} \in H$ for $\forall a, b \in H$

# 群（三角形の回転）の部分群を調べる

$G = \{e, r, \ell, a, b, c\}$の以下の6つの部分集合は部分群である

$$\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e\}$$

例えば，集合$\{e, r, \ell\}$が$G$の部分群であることを示す

$$e \circ r^{-1} = e \circ \ell = \ell$$
$$e \circ \ell^{-1} = e \circ r = r$$
$$r \circ \ell^{-1} = r \circ r = \ell$$
$$r \circ e^{-1} = r \circ e = r$$
$$\ell \circ e^{-1} = \ell \circ e = \ell$$
$$\ell \circ r^{-1} = \ell \circ \ell = r$$

以上より，$\forall a, b \in H$に対して$a \cdot b^{-1} \in H$が成り立つ

# Example of a proof of being subgroup

## Definition 8.9

Let $e$ be the identification of a group $G$. Then we define as follows for any element $a$ and integer $n$.

$a^n = \overbrace{a \cdots a}^{n}\ (n > 0),\ a^n = e\ (n = 0),\ a^n = (a^{-1})^{|n|}\ (n < 0)$

## Exercise 8.5

Let $a$ be a rational number not equal to 0. Then show that the set $H = \{a^n | n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Q}^*$, which is the multiplicative group formed by non-zero rational numbers. (Here we assume that arithmetic operations over $\mathbb{Z}$ are defined.)

## Proof（Outline）

We use subgroup decision theorem.

First confirm $H \neq \phi$.

（1）Show $x, y \in H \Rightarrow x \cdot y \in H$

（2）Show $x \in H \Rightarrow x^{-1} \in H$

By（1）and（2）, $H$ is a subgroup of the multiplicative group $\mathbb{Q}^*$

# 部分群であることの証明例

## 定義8.9

群$G$の単位元を$e$とするとき，$G$の任意の元$a$と整数$n$について，次のように定義する

$$a^n = \overbrace{a \cdots a}^{n}\ (n > 0), \qquad a^n = e\ (n = 0), \qquad a^n = (a^{-1})^{|n|}\ (n < 0)$$

## 例題8.5

$a$を0でない有理数とする．このとき，集合$H = \{a^n | n \in \mathbb{Z}\}$は0でない有理数のつくる乗法群$\mathbb{Q}^*$の部分群であることを示せ（ただし，$\mathbb{Z}$上の四則演算が成り立つとする）

## 証明（方針）

部分群の判定定理を使う

$H \neq \phi$ を確認する

(1) $x, y \in H \Rightarrow x \cdot y \in H$ を示す

(2) $x \in H \Rightarrow x^{-1} \in H$ を示す

上記(1)(2)より，$H$は乗法群$\mathbb{Q}^*$の部分群である

# Generation of group

- For the rotations of a $\triangle$, consider a set $H = \{r\}$, which is not a subgroup
- We generate a subgroup from this set.
- It is sufficient to add elements to satisfy the subgroup decision theorem
  - Since $H$ does not contain an inverse element $\ell$ of $r$;
    thus add $\ell \rightarrow \{r, \ell\}$
  - To be closed under the operation, from $r \circ \ell = e$, add $e \rightarrow \{e, r, \ell\}$
- Now we obtain a subgroup $\{e, r, \ell\}$ of $G$.

# 群の生成について

- 三角形の回転において，部分群でない集合$H = \{r\}$を考える
- この集合から部分群を生成してみる
- 部分群の判定定理を満たすように元を追加すればよい
  - $H$には$r$の逆元$\ell$が含まれていないので，$\ell$を加える →$\{r, \ell\}$
  - 演算に関して閉じているためには，$r \circ \ell = e$ により$e$を加える →$\{e, r, \ell\}$
- 以上により，$G$の部分群$\{e, r, \ell\}$が出来上がる

# Definition of order and cyclic group

**Definition 8.10（order of group）**

The order of a group $G$ is defined by the number of elements in $G$, and denoted by $|G|$. If $G$ contains infinitely many elements, we define as $|G| = \infty$.

**Definition 8.11（order of an element）**

Let $G$ be a group with an identity element $e$. For an element $a$ in $G$, the minimum positive integer n with $a^n = e$ (if it exists) is called the order of $a$. If such an integer does not exist, the order of $a$ is infinite.

**Definition 8.12（cyclic group）**

If every element in a group $G$ is a power of an element $a$ in $G$, $G$ is said to be a cyclic group generated by $a$, and the element $a$ is called generator. That is,

$G$ : cyclic group $\Leftrightarrow \exists a \in G, G = \langle a \rangle$

- A cyclic group is a commutative group.
- Finite cyclic group
  - The element $a$ will return to the identity element after applying operation in a finite number.

# 位数と巡回群の定義

- 定義8.10（群の位数）
  - 群$G$に属する元の個数を$G$の位数といい，$|G|$で表す．$G$が無限大のときは$|G| = \infty$とする
- 定義8.11（元の位数）
  - 単位元を$e$とする群$G$の元$a$に対して，$a^n = e$となるような最小の正整数$n$を（それがあるときは）$a$の位数といい，そのような整数がないとき，$a$の位数は無限という．
- 定義8.12（巡回群）
  - 群$G$のすべての元が$G$のある元$a$の累乗になっているとき，$G$は$a$で生成された巡回群であるといい，$a$をその生成元という．すなわち，

$$G:\text{巡回群} \Leftrightarrow \exists a \in G, G = \langle a \rangle$$

- 巡回群は可換群である
- 有限巡回群
  - $a$を何回か演算したら必ず単位元に戻る

# Example

## Order

- For an element $i$, let $G = \{1, i, i^2, i^3\}$ be a multiplicative group. Then, what the orders of $G \ni i, i^2$?
- What the order of $\langle 1 \rangle$?
- Can $i^2$ be a generator of $G$?

## Cyclic group

- The group $\langle 1 \rangle$ of natural numbers with respect to $+$ is a cyclic group
- The group $\langle i \rangle$ of complex numbers with respect to $\times$ is a cyclic group

# 例

- 位数
  - $i$に対して$G = \{1, i, i^2, i^3\}$を乗法群と考える. $G \ni i, i^2$の位数は？
  - $\langle 1 \rangle$の位数は？
  - $i^2$は$G$の生成元となれるか？

- 巡回群
  - 整数の$+$に関する群$\langle 1 \rangle$は巡回群
  - 複素数$i$の$\times$に関する群$\langle i \rangle$は巡回群

# Theorem for cyclic group

**Theorem 8.4**

Let $a$ be an element in $G$. Then the subset $\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$ of $G$ that contains all powers of $a$ is a subgroup of the group $G$. (This $\langle a\rangle$ is called a cyclic subgroup of $G$.)

**（Proof）**

By the decision theorem for subgroup, we show that $\langle a\rangle$ is a subgroup of $G$.

① Show $x, y \in \langle a\rangle \Longrightarrow xy \in \langle a\rangle$

$$x = a^m, y = a^n \ (\exists m, n \in \mathbb{Z})$$
$$xy = a^m a^n = a^{m+n} \in \langle a\rangle$$

② Show $x \in \langle a\rangle \Longrightarrow x^{-1} \in \langle a\rangle$

$$x = a^n \ (\exists n \in \mathbb{Z})$$
$$x^{-1} = (a^n)^{-1} = a^{-n} \in \langle a\rangle$$

By ①②, $\langle a\rangle$ is a subgroup of $G$.

# 巡回群に関連する定理

**定理8.4**

群$G$の元$a$の累乗の全体からなる$G$の部分集合$\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$は$G$の部分群になる（この$\langle a\rangle$を$G$の巡回部分群という）.

**（証明）**

部分群の判定定理を用いて，$\langle a\rangle$が$G$の部分群であることを示す

① $x, y \in \langle a\rangle \Longrightarrow xy \in \langle a\rangle$であることを示す

- $x = a^m, y = a^n$ $(\exists m, n \in \mathbb{Z})$
- $xy = a^m a^n = a^{m+n} \in \langle a\rangle$

② $x \in \langle a\rangle \Longrightarrow x^{-1} \in \langle a\rangle$であることを示す

- $x = a^n$ $(\exists n \in \mathbb{Z})$
- $x^{-1} = (a^n)^{-1} = a^{-n} \in \langle a\rangle$

①②より，$\langle a\rangle$は$G$の部分群である

# Exercise（8）

（1）例題8.4において，$(S, \circ)$が群であることを示せ（Prove that $(S, \circ)$ is a group in Example 8.4.）

- 演算に関して閉じていることは証明しなくてよい（Not need to prove “Closure”）

（2）$G$を可換群，$k$を正の整数とするとき，$G^{(k)} = \{x^k \in G | x \in G\}$が$G$の部分群であることを示せ（Let $G$ be an Abelian group and $k$ be a positive integer. Prove that $G^{(k)} = \{x^k \in G | x \in G\}$ is a subgroup of $G$.）

- ただし，$G$が可換群のとき，$G$の任意の元$a, b$について$(a \cdot b)^n = a^n \cdot b^n$が成立することを利用してよい（You can use $(a \cdot b)^n = a^n \cdot b^n$ for $a, b \in G$ when $G$ is an Abelian group.）