9
Group (2)
Residue Class（Lagrange's Theorem）
Normal subgroup
Factor group

Ryuhei Uehara

第9回
群(2) 剰余類（Lagrangeの定理），正規部分群，剰余群

上原隆平

Contents

- Operations over sets
- Normal subgroup
- Residue class
- Lagrange's Theorem
- Factor group (quotient group)

本講義の内容

- 集合の演算
- 正規部分群
- 剰余類
- ラグランジュの定理
- 剰余群

Operations over sets

Let G be a group, H a subset of G, $\circ$ binary operation of G, and $a \in G$.

Then, the operation over an element and a set is defined by;

$$a \circ H = \{a \circ h | h \in H\}$$

- Sometimes operation is omitted and denoted as aH

Example

For a subset $H = \{-3,0,1,4\}$ of $\mathbb{Z}$, what $6 + H$ is?

Of course, we can define the following in the same manner:

- $H \circ a = \{h \circ a | h \in H\}$
- $H_1 \circ H_2 = \{h_1 \circ h_2 | h_1 \in H_1, h_2 \in H_2\}$
- $H^{-1} = \{h^{-1} | h \in H\}$

集合の演算

- Gを群，HをGの部分集合，$\circ$をGの二項演算子，$a \in G$とする
- このとき，集合と元との演算は以下で定義できる

$$a \circ H = \{a \circ h | h \in H\}$$

  - 二項演算子が省略されてaHと表記することが多い

例

- $\mathbb{Z}$の部分集合$H = \{-3,0,1,4\}$とするとき，$6 + H$は？

- もちろん，以下の演算も同様に定義できる．
  - $H \circ a = \{h \circ a | h \in H\}$
  - $H_1 \circ H_2 = \{h_1 \circ h_2 | h_1 \in H_1, h_2 \in H_2\}$
  - $H^{-1} = \{h^{-1} | h \in H\}$

Preliminaries: equivalence relation and equivalence class

Definition 9.1（Equivalence relation）

A relation $\sim$ is an equivalence relation if it has the following three properties

（1）Reflectivity：$S \ni \forall x,\ x \sim x$

（2）Symmetry：$S \ni x, y,\ x \sim y \Rightarrow y \sim x$

（3）Transitivity：$S \ni x, y, z,\ x \sim y, y \sim z \Rightarrow x \sim z$

Definition 9.2（Equivalence class）

Assume that an equivalence relation $\sim$ is defined on a set S. For $S \ni a$, the set of elements equivalent to a is the equivalence class with representative element a, and denoted by $\bar{a}$, that is,

$$\bar{a} = \{x \in S | a \sim x\}$$

準備：同値関係と同値類

- 定義9.1（同値関係）
  - 集合S上の関係~が同値関係であるとは，以下の3つの性質が成り立つことである
    （1）反射律：$S \ni \forall x$に対して，$x \sim x$
    （2）対称律：$S \ni x, y$に対して，$x \sim y \Rightarrow y \sim x$
    （3）推移律：$S \ni x, y, z$に対して，$x \sim y, y \sim z \Rightarrow x \sim z$
- 定義9.2（同値類）
  - 集合S上に同値関係~が定義されているとき，$S \ni a$に対してaに同値である元を全て集めた集合を，aを代表元とする同値類とよび，$\bar{a}$とかく

$$\bar{a} = \{x \in S | a \sim x\}$$

Classification by subgroup

Theorem 9.1

Let H be a subgroup of a group G. Then for $a, b \in G$, the conditions from (1) to (5), and from (1') to (5') are equivalent, respectively.

$(1) aH = bH,\ (2) a^{-1}b \in H,\ (3) b \in aH,\ (4) a \in bH,\ (5) aH \cap bH \neq \phi$

$(1') Ha = Hb,\ (2') ab^{-1} \in H,\ (3') b \in Ha,\ (4') a \in Hb,\ (5') Ha \cap Hb \neq \phi$

Proof

- $(1) \Rightarrow (2)$:
  Since $b \in bH = aH$, there is an h in H that satisfies $b = ah$. Therefore, $a^{-1}b = h \in H$
- $(2) \Rightarrow (3)$:
  仮By assumption, there is an h in H that satisfies $a^{-1}b = h$. Therefore, $b = ah \in aH$
- $(3) \Rightarrow (4)$:
  By assumption, there is an h in H with $b = ah$. Therefore, $a = bh^{-1} \in bH$
- $(4) \Rightarrow (5)$: By assumption and $a \in aH$, we have $a \in aH \cap bH$. Therefore, $aH \cap bH \neq \phi$
- $(5) \Rightarrow (1)$: Omitted

部分群による類別

- 定理9.1
  - 群Gの部分群をHとするとき，$a, b \in G$について，次の(1)から(5)の条件，及び(1')から(5')は同値である
    - $(1) aH = bH$，$(2) a^{-1}b \in H$，$(3) b \in aH$，$(4) a \in bH$，$(5) aH \cap bH \neq \phi$
    - $(1') Ha = Hb$，$(2') ab^{-1} \in H$，$(3') b \in Ha$，$(4') a \in Hb$，$(5') Ha \cap Hb \neq \phi$
- 証明
  - $(1) \Rightarrow (2)$:
    $b \in bH = aH$より$b = ah$を満たすHの元hがある．ゆえに，$a^{-1}b = h \in H$
  - $(2) \Rightarrow (3)$:
    仮定より$a^{-1}b = h$を満たすHの元hがある．ゆえに，$b = ah \in aH$
  - $(3) \Rightarrow (4)$:
    仮定より$b = ah$を満たすHの元hがある．ゆえに，$a = bh^{-1} \in bH$
  - $(4) \Rightarrow (5)$: 仮定と$a \in aH$より$a \in aH \cap bH$．ゆえに，$aH \cap bH \neq \phi$
  - $(5) \Rightarrow (1)$: 省略

Normal subgroup（1/2）

Definition 9.3

- A subgroup N of a group G satisfies the following, N is said to be a normal subgroup of G, and denoted by $G \rhd N$

$$aN = Na \ (\forall a \in G)$$

Note

- The equation is equivalent to $a^{-1}Na = N \ (\forall a \in G)$
- When G is commutative group, any subgroup is normal subgroup

正規部分群(1/2)

- 定義9.3
  - 群Gの部分群Nが次式を満たすとき，NはGの正規部分群であるといい，$G \rhd N$とかく

$$aN = Na \ (\forall a \in G)$$

- 注意
  - 上式は $a^{-1}Na = N \ (\forall a \in G)$ と同値
  - Gが可換群のとき，任意の部分群は正規部分群である

Normal subgroup（2/2）

Theorem 9.2

If a subgroup N of Gsatisfies the following, we have $G \rhd N$

$$a^{-1}Na \subseteq N \ (\forall a \in G)$$

Proof

Since $N = aa^{-1}Naa^{-1} \subseteq aNa^{-1} \subseteq N$, we have $N = aNa^{-1}$.

Therefore, we have $Na = aN$, and hence,

N is a normal subgroup of G $(G \rhd N)$.

Example of a group (rotation of triangle)

- Subgroups of G are following six;
  $\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e\}$
- Among them, normal subgroups are; $\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e\}$

正規部分群(2/2)

- 定理9.2
  - 群Gの部分群Nが次式を満たすならば，$G \rhd N$である
$$a^{-1}Na \subseteq N \quad (\forall a \in G)$$
- 証明
  - $N = aa^{-1}Naa^{-1} \subseteq aNa^{-1} \subseteq N$より，$N = aNa^{-1}$．ゆえに，$Na = aN$が成り立つため，$N$は$G$の正規部分群($G \rhd N$)である
- 群(三角形の回転)の例
  - Gの部分群は，$\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e, a\}, \{e, b\}, \{e, c\}, \{e\}$の6つ
  - この中で正規部分群は，$\{e, r, \ell, a, b, c\}, \{e, r, \ell\}, \{e\}$

Confirm that $N_1 = \{e, r, \ell\}$ is a normal subgroup

- $G = \{e, r, \ell, a, b, c\}$
- $r \circ \{e, r, \ell\} = \{e, r, \ell\} \circ r \ (= \{r, \ell, e\})$
- $\ell \circ \{e, r, \ell\} = \{e, r, \ell\} \circ \ell \ (= \{\ell, e, r\})$
- $a \circ \{e, r, \ell\} = \{e, r, \ell\} \circ a \ (= \{a, b, c\})$
- $b \circ \{e, r, \ell\} = \{e, r, \ell\} \circ b \ (= \{b, c, a\})$
- $c \circ \{e, r, \ell\} = \{e, r, \ell\} \circ c \ (= \{c, a, b\})$

$\Rightarrow gN_1 = N_1 g \ (\forall g \in G)$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

$N_1 = \{e, r, \ell\}$が正規部分群であることを確かめる

- $G = \{e, r, \ell, a, b, c\}$
- $r \circ \{e, r, \ell\} = \{e, r, \ell\} \circ r \ (= \{r, \ell, e\})$
- $\ell \circ \{e, r, \ell\} = \{e, r, \ell\} \circ \ell \ (= \{\ell, e, r\})$
- $a \circ \{e, r, \ell\} = \{e, r, \ell\} \circ a \ (= \{a, b, c\})$
- $b \circ \{e, r, \ell\} = \{e, r, \ell\} \circ b \ (= \{b, c, a\})$
- $c \circ \{e, r, \ell\} = \{e, r, \ell\} \circ c \ (= \{c, a, b\})$

$\Rightarrow gN_1 = N_1 g \ (\forall g \in G)$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

Confirm that $N_2 = \{e, a\}$ is *not* a normal subgroup

- $G = \{e, r, \ell, a, b, c\}$
- For $a \in G$
  - $a \circ \{e, a\} = \{a, e\}$
  - $\{e, a\} \circ a = \{a, e\}$
  - $a \circ \{e, a\} = \{e, a\} \circ a$
- For $r \in G$
  - $r \circ \{e, a\} = \{r, c\}$
  - $\{e, a\} \circ r = \{r, b\}$
  - $r \circ \{e, a\} \neq \{e, a\} \circ r$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

$N_2 = \{e, a\}$が正規部分群でないことを確かめる

- $G = \{e, r, \ell, a, b, c\}$
- $a \in G$の場合
  - $a \circ \{e, a\} = \{a, e\}$
  - $\{e, a\} \circ a = \{a, e\}$
  - $a \circ \{e, a\} = \{e, a\} \circ a$
- $r \in G$の場合
  - $r \circ \{e, a\} = \{r, c\}$
  - $\{e, a\} \circ r = \{r, b\}$
  - $r \circ \{e, a\} \neq \{e, a\} \circ r$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

For Residue Class (or coset)

- You can define equivalence relation on elements in a group G
  - Once we have equivalence relation, the group G can be partitioned by equivalence class
- Using a subset H of a group G, we consider an equivalence relation $\sim$
  - When $aH = bH, a, b \in G$ are left equivalent for H.
  - This quotient set given by the left equivalent relation is called left residue class (or left coset).
  - Let $\bar{b}$ be the set of left equivalent elements to $b \in G$, then
$$\bar{b} = \{a | b^{-1}a \in H\}$$
  - Since $b^{-1}a \in H \Leftrightarrow a \in bH$, we have $\bar{b} = bH$.
- That is, the set of left equivalent elements of $b \in G$ is bH.

剰余類について

- 群Gの元に同値関係を定義できる
  - 同値関係があるということは，群Gを同値類に分けることができる
- 群Gの部分集合Hを使って同値関係~を考える
  - $aH = bH$のとき，$a, b \in G$はHに関して左合同であるという
  - この左合同という同値関係によって作られた商集合を左剰余類という
  - ここで，$b \in G$と左合同な元を全て集めた集合を$\bar{b}$とおくと
    $$\bar{b} = \{a | b^{-1}a \in H\}$$
  - $b^{-1}a \in H \Leftrightarrow a \in bH$より，$\bar{b} = bH$となる
- つまり，$b \in G$と左合同な元全体からなる集合はbHである

Definitions for Residue Class (or coset)

Definition 9.4

Let G be a group, H a subgroup of G, and $a, b \in G$. When $aH = bH$, a and b are left congruence modulo H. Similarly, when $Ha = Hb$, a and b are right congruence modulo H.

Definition 9.5

Let G be a group, H a subgroup of G, and $a \in G$. The set of left congruence elements to a modulo H is left residue class (or left coset) of a modulo H (left residue class of H). The set of right congruence elements to a modulo H is right residue class of modulo H (right residue class of H). Especially, since $H = 1H = H1$, H itself is left residue class and right residue class.

- For a normal subgroup, its left residue class is equal to the right residue class.

剰余類に関係する定義

- 定義9.4
  - Gを群，HをGの部分群とし，$a, b \in G$とする．$aH = bH$のとき，aとbはHを法として左合同であるという．同様に，$Ha = Hb$のとき，aとbはHを法として右合同であるという．
- 定義9.5
  - Gを群，HをGの部分群とし，$a \in G$とする．このとき，Hを法としてaと左合同であるGの元全体の集合をaのHを法とする左剰余類（Hの左剰余類）という．また，Hを法としてaと右合同であるGの元全体の集合をaのHを法とする右剰余類（Hの右剰余類）という．特に，$H = 1H = H1$であるから，H自身は左剰余類かつ右剰余類である．
- 正規部分群の右剰余類と左剰余類は一致する

Residue Class (1/2)

Theorem 9.3

- Let G be a group, H a subgroup of G, and $a \in G$. Then the relation of the left congruence modulo H $(a \sim b \overset{\text{def}}{\Leftrightarrow} aH = bH)$ is equivalence relation, and the equivalence class $\{x = a | G \ni x\}$ containing a of G is aH. Similar claim holds for the right congruence.

Proof (for left congruence)

1. First we show that $\sim$ is an equivalence relation:
   (1) Reflective : For $G \ni a$, since $aH = aH$ we have $a \sim a$
   (2) Symmetry : For $G \ni a, b$, $a \sim b \Leftrightarrow aH = bH \Leftrightarrow bH = aH \Leftrightarrow b \sim a$
   (3) Transitive : For $G \ni a, b, c$, $a \sim b, b \sim c \Leftrightarrow aH = bH, bH = cH \Leftrightarrow aH = cH \Leftrightarrow a \sim c$
2. Next, on the relation of the left congruence modulo H, we show that $X = \{x = a | G \ni x\}$ implies $X = aH$. That is, we show $X \supseteq aH$ and $X \subseteq aH$.

剰余類(1/2)

- 定理9.3
  - Gを群，HをGの部分群とし，$a \in G$とする．このとき，Hを法として左合同という関係($a \sim b \overset{\text{def}}{\Leftrightarrow} aH = bH$)は同値関係で，$G$の$a$を含む同値類$\{x = a | G \ni x\}$は$aH$である．右合同についても同様に成り立つ．
- 証明(左合同について)
  - ~が同値関係であることを示す
    - (1)反射律：$G \ni a$に対して，$aH = aH$より，$a \sim a$
    - (2)対称律：$G \ni a, b$に対して，$a \sim b \Leftrightarrow aH = bH \Leftrightarrow bH = aH \Leftrightarrow b \sim a$
    - (3)推移律：$G \ni a, b, c$に対して，$a \sim b, b \sim c \Leftrightarrow aH = bH, bH = cH \Leftrightarrow aH = cH \Leftrightarrow a \sim c$
  - 次に，Hを法として左合同という関係において，$X = \{x = a | G \ni x\}$とするとき$X = aH$となることを示す，すなわち，$X \supseteq aH$かつ$X \subseteq aH$を示す

Residue Class（2/2）

（Proof continued）

- We show $aH \subseteq X$ $(X = \{x = a | G \ni x\})$
  - It is sufficient to show that $aH \ni \forall ah$ is equivalence relation to a.
  - $a^{-1}(ah) = (a^{-1}a)h = h \in H$
  - By Theorem 9.1, $ah \sim a$
  - Therefore, since $\forall ah \subseteq X$, we have $aH \subseteq X$
- We show $X \subseteq aH$
  - For any $X \ni \forall x$, we have $x \sim a$, that is, $xH = aH$
  - Since $H \ni 1$, $xH \ni x$
  - Thus $aH \ni x$
  - Hence $aH \supseteq X$
- Therefore, the equivalence class including a is aH.
- For right congruence is similar.

剰余類(2/2)

- (証明のつづき)
  - $aH \subseteq X$ を示す($X = \{x = a | G \ni x\}$)
    - $aH \ni \forall ah$がaと同値関係であることを示せばよい
    - $a^{-1}(ah) = (a^{-1}a)h = h \in H$
    - 定理9.1より, $ah \sim a$
    - ゆえに, $\forall ah \subseteq X$より$aH \subseteq X$
  - $X \subseteq aH$を示す
    - $X \ni \forall x$をとると$x \sim a$, すなわち$xH = aH$
    - $H \ni 1$より, $xH \ni x$
    - よって, $aH \ni x$
    - ゆえに, $aH \supseteq X$
  - したがって, aを含む同値類はaHとなる
  - 右合同についても同様

Complete system of representatives

Partition of G according to the equivalence relation of "the left congruence modulo H" into disjoint sets $\{aH\}$:

$$G = \bigcup_{i \in I} a_i H = \sum_{i \in I} a_i H$$

- This is called left coset partition of G by H
- I is the set of indices of the left residue class

- The whole set of the left residue classes is denoted by $G/H = \{a_i H\}_{i \in I}$
- The set $\{a_i\}_{i \in I}$ of representative elements a_i for each left residue class is called complete system of representatives of G/H.
- The set of the right residue classes of H is denoted by $H \setminus G$.

完全代表系

- Gを「Hを法として左合同」という同値関係でdisjointな集合$\{aH\}$に分割する

$$G = \bigcup_{i \in I} a_i H = \sum_{i \in I} a_i H$$

  - これをGのHによる左分解とよぶ
  - Iは左剰余類の添字集合である
- 左剰余類の全体を$G/H = \{a_i H\}_{i \in I}$で表す
- 各左剰余類の代表元a_iの集合$\{a_i\}_{i \in I}$をG/Hの完全代表系という
- Hの右剰余類の全体を$H \setminus G$と表す

Left residue class of $N_2 = \{e, a\}$

- $G = \{e, r, \ell, a, b, c\}$
- For each element, find the set of elements of left congruence:
  - $eN_2 = \{e, a\}, rN_2 = \{r, c\}, \ell N_2 = \{\ell, b\}$
  - $aN_2 = \{a, e\}, bN_2 = \{b, \ell\}, cN_2 = \{c, r\}$
- Therefore, the left residue class is:
  - $\{\{e, a\}, \{r, c\}, \{\ell, b\}\}$
- The left coset partition of G by N_2
  - $G = N_2 + rN_2 + \ell N_2$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

$N_2 = \{e, a\}$の左剰余類

- $G = \{e, r, \ell, a, b, c\}$
- 各元に対して左合同な元の集合を求める
  - $eN_2 = \{e, a\}, rN_2 = \{r, c\}, \ell N_2 = \{\ell, b\}$
  - $aN_2 = \{a, e\}, bN_2 = \{b, \ell\}, cN_2 = \{c, r\}$
- よって，左剰余類は以下
  - $\{\{e, a\}, \{r, c\}, \{\ell, b\}\}$
- GのN_2による左分解
  - $G = N_2 + rN_2 + \ell N_2$

$\circ$	e	r	ℓ	a	b	c
e	e	r	ℓ	a	b	c
r	r	ℓ	e	b	c	a
ℓ	ℓ	e	r	c	a	b
a	a	c	b	e	ℓ	r
b	b	a	c	r	e	ℓ
c	c	b	a	ℓ	r	e

Right residue class of $N_2 = \{e, a\}$

- $G = \{e, r, \ell, a, b, c\}$
- For each element, find the set of elements of right congruence:
  - $N_2 e = \{e, a\}, N_2 r = \{r, b\}, N_2 \ell = \{\ell, c\}$
  - $N_2 a = \{a, e\}, N_2 b = \{b, r\}, N_2 c = \{c, \ell\}$
- Therefore, the right residue class is:
  - $\{\{e, a\}, \{r, b\}, \{\ell, c\}\}$
- The right coset partition of G by N_2
  - $G = N_2 + N_2 r + N_2 \ell$
- The left and right coset partition of $N_2 = \{e, a\}$ are not equal to.

  which means that $N_2 = \{e, a\}$ is not normal subgroup.

$N_2 = \{e, a\}$の右剰余類

- $G = \{e, r, \ell, a, b, c\}$
- 各元に対して右合同な元の集合を求める
  - $N_2e = \{e, a\}, N_2r = \{r, b\}, N_2\ell = \{\ell, c\}$
  - $N_2a = \{a, e\}, N_2b = \{b, r\}, N_2c = \{c, \ell\}$
- よって，右剰余類は以下
  - $\{\{e, a\}, \{r, b\}, \{\ell, c\}\}$
- GのN_2による右分解
  - $G = N_2 + N_2r + N_2\ell$
- $N_2 = \{e, a\}$の左剰余類と右剰余類は一致しない
  - これは，$N_2 = \{e, a\}$が正規部分群でないことを意味している

Residue class of $N_1 = \{e, r, \ell\}$

- $G = \{e, r, \ell, a, b, c\}$
- For each element, find the set of left congruent
  - $eN_1 = \{e, r, \ell\}, rN_1 = \{r, \ell, e\}, \ell N_1 = \{\ell, e, r\}$
  - $aN_1 = \{a, b, c\}, bN_1 = \{b, c, a\}, cN_1 = \{c, a, b\}$
- For each element, find the set of right congruent
  - $N_1 e = \{e, r, \ell\}, N_1 r = \{r, \ell, e\}, N_1 \ell = \{\ell, e, r\}$
  - $N_1 a = \{a, c, b\}, N_1 b = \{b, a, c\}, N_1 c = \{c, b, a\}$
- Then, the left and right congruent are equal to each other as
  - $\{\{e, r, \ell\}, \{a, b, c\}\}$
  - Thus $N_1 = \{e, r, \ell\}$ is a normal subgroup
- The partition of G by N_1
  - $G = N_1 + aN_1 = N_1 + N_1 a$

$N_1 = \{e, r, \ell\}$の剰余類

- $G = \{e, r, \ell, a, b, c\}$
- 各元に対して左合同な元の集合を求める
  - $eN_1 = \{e, r, \ell\}, rN_1 = \{r, \ell, e\}, \ell N_1 = \{\ell, e, r\}$
  - $aN_1 = \{a, b, c\}, bN_1 = \{b, c, a\}, cN_1 = \{c, a, b\}$
- 各元に対して右合同な元の集合を求める
  - $N_1 e = \{e, r, \ell\}, N_1 r = \{r, \ell, e\}, N_1 \ell = \{\ell, e, r\}$
  - $N_1 a = \{a, c, b\}, N_1 b = \{b, a, c\}, N_1 c = \{c, b, a\}$
- よって，左剰余類と右剰余類は以下で一致
  - $\{\{e, r, \ell\}, \{a, b, c\}\}$
  - $N_1 = \{e, r, \ell\}$は正規部分群である
- GのN_1による分解
  - $G = N_1 + aN_1 = N_1 + N_1 a$

Order of G, N_1, N_2

- Left coset partition of G by $N_1 (= \{e, r, \ell\})$
  - $G = N_1 + aN_1 = (e + a)N_1$
- Left coset partition of G by $N_2 (= \{e, a\})$
  - $G = N_2 + rN_2 + \ell N_2 = (e + r + \ell)N_2$
- The number of elements of each left residue class is the same
- Therefore, the order of N_1, N_2 divides the order of G

G と N_1, N_2 の位数について

- G の $N_1(=\{e, r, \ell\})$ による左分解
  - $G = N_1 + aN_1 = (e + a)N_1$
- G の $N_2(=\{e, a\})$ による左分解
  - $G = N_2 + rN_2 + \ell N_2 = (e + r + \ell)N_2$
- 各剰余類の元の個数は同じである
- よって，N_1, N_2の位数は，Gの位数の約数になっている

index

- When G/H is a finite set, so $H \setminus G$ is, and the number of the left and right congruent are equal to each other.
- This number is denoted by $|G:H|$, and called index of H on G.
- When $|G:H| = n$, we have $G = a_1H + \cdots + a_nH$
- Especially, note that $|G:\{e\}| = |G|, |G:G| = 1$.

指数

- G/Hが有限集合であるとき$H \setminus G$も有限集合であり，左剰余類の個数と右剰余類の個数が一致する
- これを$|G:H|$で表し，HのGにおける指数と呼ぶ
- $|G:H| = n$のとき，$G = a_1H + \cdots + a_nH$となる
- 特に，$|G:\{e\}| = |G|, |G:G| = 1$となることに注意

Lagrange's Theorem

Theorem 9.4（Lagrange's Theorem）

Let G be a finite group, and H a subgroup of G. Then

（1）$|G| = |G:H||H|$, that is, $|G:H| = |G|/|H|$

（2）Both of order and index of H divide the order of G

Proof

For the right coset partition $G = \sum_{i=1}^{n} Ha_i$ by H, we have $|G| = \sum_{i=1}^{n} |Ha_i|$

Here since $n = |G:H|, |H| = |Ha_i|$, we have（1）.

（2）is clear from（1）.

Corollary 9.1

For any finite group G of order ℓ, the order of $\forall a \in G$ divides ℓ. Especially, we have

$$a^{\ell} = 1$$

ラグランジュの定理

- 定理9.4（ラグランジュの定理）
  - Gを有限群，HをGの部分群とする
  - （1）$|G| = |G:H||H|$，すなわち$|G:H| = |G|/|H|$
  - （2）Hの位数も指数も共にGの位数の約数である
- 証明
  - $G = \sum_{i=1}^{n} Ha_i$をHによる右分解とすれば，$|G| = \sum_{i=1}^{n} |Ha_i|$となる．
  - ここで，$n = |G:H|, |H| = |Ha_i|$であるから（1）が成り立つ
  - （2）は（1）より明らか
- 系9.1
  - 位数ℓの有限群Gにおいて，$\forall a \in G$の位数はℓの約数である．特に，

$$a^{\ell} = 1$$

Example of Lagrange's Theorem

Example

- $G = \{1, i, i^2, i^3\}$ is a subgroup of $\mathbb{C}^*$, multiplicative group of complex numbers without 0.
- $|G| = 4$
- What the order of a subgroup$H = \langle i^2 \rangle$ of G?
  - $i^2 = -1, (i^2)^2 = 1, (i^2)^3 = -1, \cdots$

ラグランジュの定理の例

例

- $G = \{1, i, i^2, i^3\}$は，0でない複素数のつくる乗法群$\mathbb{C}^*$の部分群
- $|G| = 4$
- Gの部分群$H = \langle i^2 \rangle$の位数は？

$$i^2 = -1, (i^2)^2 = 1, (i^2)^3 = -1, \cdots$$

For a normal subgroup $N_1 = \{e, r, \ell\}$

- $G = \{e, r, \ell, a, b, c\}$
- N_1 is residue class and normal subgroup of G.
- Consider a set $\{N_1, aN_1\}$ on $G = N_1 + aN_1$
  - ${N_1}^2 = N_1$
  - $N_1 \circ aN_1 = aN_1$
  - $aN_1 \circ N_1 = aN_1$
  - $aN_1 \circ aN_1 = N_1$

	N_1	aN_1
N_1	N_1	aN_1
aN_1	aN_1	N_1

- As in the right table, the group constructed by residue class is called residue class group.
- If there is a normal subgroup, we have hierarchy of level 2.

R.C.G R.C.G
(order 2) (order 3)
$G \supset N_1 \supset e$
(order 6) (order 3) (order 1)

正規部分群$N_1 = \{e, r, \ell\}$について

- $G = \{e, r, \ell, a, b, c\}$
- N_1はGの剰余類かつ正規部分群である
- $G = N_1 + aN_1$で$\{N_1, aN_1\}$という集合を考える
  - ${N_1}^2 = N_1$
  - $N_1 \circ aN_1 = aN_1$
  - $aN_1 \circ N_1 = aN_1$
  - $aN_1 \circ aN_1 = N_1$
- 右表のように，剰余類で構成される群を剰余群とよぶ
- 正規部分群があると2階建て構造を持つ

	N_1	aN_1
N_1	N_1	aN_1
aN_1	aN_1	N_1

剰余群　剰余群
（位数2）（位数3）
$G \supset N_1 \supset e$
（位数6）（位数3）（位数1）

Residue class group

- Let G be a group, and N normal subgroup of G.
- Then, its residue class $\{g \circ N | g \in G\}$ is a group.
- This group is called residue class group for N, and denoted by G/N
- For any element (aN, bN) in $G/N \times G/N$, make a correspondence to $aN \circ bN = a \circ bN$ in G/N.
  - If $\bar{g} \coloneqq g \circ N, \overline{g} \in G/N$
  - Then define as $\overline{g_1} \circ \overline{g_2} = \overline{g_1 \circ g_2}$
- This correspondence gives us a binary relation on G/N
- Then G/N is a group for this operation.
  - The identity element of the group G/N is N
  - The inverse on the group G/N is $(aN)^{-1} = a^{-1}N$

剰余群

- Gを群，NをGの正規部分群とする
- このとき，その剰余類$\{g \circ N | g \in G\}$は群となる
- この群のことをNに関する剰余群といい，G/Nで表す
- $G/N \times G/N$の任意の元(aN, bN)にG/Nの元$aN \circ bN = a \circ bN$を対応させる
  - $\bar{g} \coloneqq g \circ N$とすると，$\bar{g} \in G/N$
  - このとき，$\overline{g_1} \circ \overline{g_2} = \overline{g_1 \circ g_2}$と定義する
- この対応はG/Nに1つの二項演算を与える
- G/Nはこの演算に関して群をなす
  - 群G/Nの単位元はN
  - 群G/Nの逆元は$(aN)^{-1} = a^{-1}N$

Example of residue class group

- Let $\mathbb{Z} \ni m > 0$. Then $m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ is a subgroup of the group $\mathbb{Z}$ with operation of addition.
  - For example, $3\mathbb{Z} = \{0, \pm 3, \pm 6, \cdots\}$ is a subgroup of $\mathbb{Z}$.
  - Then the residue class of the subgroup $3\mathbb{Z}$ is $\{n + 3\mathbb{Z} | n \in \mathbb{Z}\}$.
- $3\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$
  - Since for $\forall n \in \mathbb{Z}$ we have $n + 3\mathbb{Z} = 3\mathbb{Z} + n$.
- Therefore, $\mathbb{Z}/3\mathbb{Z}$ is residue class group.
- $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}\}$
  - Since $4 + 3\mathbb{Z} = 1 + 3 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$, we have these three residue classes
  - Note that $\bar{n} \in \mathbb{Z}/3\mathbb{Z}$

剰余群の例

- $\mathbb{Z} \ni m > 0$とする．このとき，$m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ は$\mathbb{Z}$の加法に対する群の部分群である
  - 例えば，$3\mathbb{Z} = \{0, \pm 3, \pm 6, \cdots\}$は$\mathbb{Z}$の部分群である
  - このとき，部分群$3\mathbb{Z}$の剰余類は $\{n + 3\mathbb{Z} | n \in \mathbb{Z}\}$ となる
- $3\mathbb{Z}$は$\mathbb{Z}$の正規部分群である
  - $\forall n \in \mathbb{Z}$に対して，$n + 3\mathbb{Z} = 3\mathbb{Z} + n$であるため
- よって，$\mathbb{Z}/3\mathbb{Z}$は剰余群である
- $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}\}$
  - $4 + 3\mathbb{Z} = 1 + 3 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$となるので，結局この剰余類は3つ
  - $\bar{n} \in \mathbb{Z}/3\mathbb{Z}$であることに注意する

Exercise 9

- (1)位数が素数である群は，真部分群を持たない巡回群であることを証明せよ(Prove that the group whose order is a prime number is a cyclic group without a proper subgroup.)
  - 巡回群であることと真部分群を持たないことの両方を示す(Prove it is a cyclic group and it does not have a proper subgroup.)

- (2)群Gの部分群をHとする．Hが指数2の部分群であるとき，Hが正規部分群であることを示せ．(Let H be the subgroup of a group G. Prove that H is a normal subgroup, when H has the index 2.)
  - $a \in H$と$a \notin H$に場合分けして考えると分かりやすい(It is better to divide into $a \in H$ and $a \notin H$.)

Schedule(残りの予定)

11/21(Mon): Today

11/24(Thu)

09:00-10:40 Ring, Field

12:30 (pls submit till 10:40…) deadline of Report (3) (レポート(3)締切出題);

13:30-15:10 Ans & Cmts by Duc, and Number Theory

- Last class (最後の講義); I'll make questionnaire in the last 10 minutes

11/28(Mon): final exam (期末試験) (by TA Duc)

40 points

Choices are;

1. Pens and pencils
2. +hand written notes
3. +copy of slides
4. +textbooks
5. +anything without electricity

Range of exam: Lesson 8~（講義8~）