1.2 整数の剰余類

整数をある数で割った余りで分類したものは，整数の合同類と呼ばれる。$n \in \mathbb{Z}$ とし

$$n\mathbb{Z} = \{\, nk \mid k \in \mathbb{Z} \,\}$$

とする。すなわち，$n\mathbb{Z}$ は n の整数倍全体の集合であり，イデアルであった。

例えば，$2\mathbb{Z}$ は 2 の倍数全体の集合であり，従って偶数全体の集合である。イデアル $n\mathbb{Z}$ に関する関係を次のように定義すると同値関係になる。

$$a \sim b \quad \Longleftrightarrow \quad a - b \in n\mathbb{Z}$$

すなわち，$a - b$ が n の倍数となった時に同値と定義するわけである。

この同値関係を，特に次の記号で表す。

$$a \equiv b \mod n$$

この時，整数 a と b は，n **を法として 合同** であるという。

演習問題 1.4　関係 $\sim$ が次の 3 つを満たすとき同値関係と言う。

(1) $a \sim a$

(2) $a \sim b \implies b \sim a$

(3) $a \sim b \wedge b \sim c \implies a \sim c$

上で定義した $\equiv$ が同値関係であることを示せ。

$n\mathbb{Z} = (-n)\mathbb{Z}$ なので，n としては $n \geqq 0$ のものだけ考えれば良い。$n = 0$ ならば $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ なので，$a - b \in 0\mathbb{Z}$ ということは $a = b$ である。そこで以下では，$n > 0$ とする。

さて，a を任意の整数とするとき，

$$a + n\mathbb{Z} = \{\, a + nk \mid k \in \mathbb{Z} \,\}$$

とする。例えば $n = 3$ の場合，

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \end{aligned}$$

となる。すべての整数はこの 3 つの集合のどれかに属する。これを $3\mathbb{Z}$ による**合同類**または**剰余類**という。一般に整数 n に対し $a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$ という集合を $n\mathbb{Z}$ による**合同類**または**剰余類**という。

$a+n\mathbb{Z}$ に含まれる２つの整数 m_1, m_2 は，ある整数 k_1, k_2 があって $m_1 = a+nk_1, m_2 = a+nk_2$ と書けているので，

$$m_1 - m_2 = (a + nk_1) - (a + nk_2) = n(k_1 - k_2)$$

となり，n を法として合同である。

命題 1.11 $n\mathbb{Z}$ による剰余類としては

$$n\mathbb{Z}\ ,\ 1+n\mathbb{Z}\ ,\ 2+n\mathbb{Z}\ ,\ \cdots\ ,\ (n-1)+n\mathbb{Z}$$

の n 個しかない。また，これらは全て異なる剰余類である。

証明　a を任意の整数とする。$a = qn+r$ であって $0 \leqq r < n$ とすると，$a-r = qn \in n\mathbb{Z}$ より，$a \equiv r \mod n$ である。従って，$a \in r+n\mathbb{Z}$ である。すなわち，任意の整数は，上のどれかの剰余類に含まれる。従って，上の n 個の剰余類以外の剰余類は存在しない。

次にこれらが互いに相異なる剰余類であることを示す。$0 \leqq r_1 < r_2 < n$ となる $r_1 < r_2$ で $r_1+n\mathbb{Z} = r_2+n\mathbb{Z}$ ならば $r_1 \equiv r_2 \mod n$ となっていなければならないが，それは $r_2 - r_1$ が n の倍数となっているということである。しかし，$0 < r_2 - r_1 < n$ であるので，それはあり得ない。従って，$\{0, 1, 2, \cdots, n-1\}$ に含まれる相異なる r_1, r_2 に対しては，$r_1+n\mathbb{Z}, r_2+n\mathbb{Z}$ は異なる剰余類である。 ∎

$n\mathbb{Z}$ による剰余類 $k+n\mathbb{Z}$ を $[k]$ と書く。$[k] = k+n\mathbb{Z} = \{\ldots, k-2n, k-n, k, k+n, k+2n, \ldots,\}$ なので，

$$a \in [k] \iff \exists q \in \mathbb{Z}\ a = qn + k$$

が成立する。即ち $n\mathbb{Z}$ による剰余類 $[k]$ に含まれる整数 a は n **で割った時の余り** が k になるような整数である。これが剰余類という名前の理由である。

$5\mathbb{Z}$ による剰余類を考える。$[1] = 1+5\mathbb{Z} = \{\ldots, -4, 1, 6, 11, \ldots\}$ であり $[6] = 6+5\mathbb{Z} = \{\ldots, 1, 6, 11, 16, \ldots\}$ なので $[1] = [6]$ である。

$[k_1], [k_2] \in \mathbb{Z}_n$ に対し

$$[k_1] = [k_2] \iff k_1 \equiv k_2 \mod n$$

が成立する。

定義 1.12 $n\mathbb{Z}$ による剰余類全体がつくる集合を $\mathbb{Z}_n$ または $\mathbb{Z}/n\mathbb{Z}$ と書き，$\mathbb{Z}$ の $n\mathbb{Z}$ による**剰余群**という。整数論では $\mathbb{Z}/n\mathbb{Z}$ を使うが，この講義では $\mathbb{Z}_n$ の方を使う。命題 1.11 より

$$\mathbb{Z}_n = \{\,[0], [1], [2], \ldots, [n-1]\,\}$$

である。$\mathbb{Z}_n$ における「たし算」(和) を次の様に定義する。$[k_1], [k_2] \in \mathbb{Z}_n$ に対し $a_1 \in [k_1]$，$a_2 \in [k_2]$ となる整数を任意に決める。$a_1 + a_2$ を含む剰余類 $[k_3]$ が存在するので，

$$[k_1] + [k_2] = [k_3]$$

と定義する。k_3 が a_1, a_2 の選び方によらないかということが問題だが，このことについては後で議論する。剰余群における「和」は整数の和と同じ性質をもつ，即ち次が成立する。

(1) $\forall [k_1], [k_2], [k_3] \in \mathbb{Z}_n\ \ ([k_1] + [k_2]) + [k_3] = [k_1] + ([k_2] + [k_3])$ (**結合法則**)

(2) $\exists[k_0] \in \mathbb{Z}_n \ \forall[k_1] \in \mathbb{Z}_n \ \ [k_0]+[k_1]=[k_1]$ (**零元の存在**)

(3) $\forall[k_1] \in \mathbb{Z}_n \ \exists[k_2] \ \ [k_1]+[k_2]=[k_0]$(零元) (**逆元の存在**)

(4) $\forall[k_1],[k_2] \ \ [k_1]+[k_2]=[k_2]+[k_1]$ (**交換法則**)

上で述べたことを示す前に例を見よう。Z_5 を考える。$\mathbb{Z}_5=\{\,[0],[1],[2],[3],[4]\,\}$ であり，

$$[0]=\{\ldots,-5,0,5,10,\ldots\}$$
$$[1]=\{\ldots,-4,1,6,11,\ldots\}$$
$$[2]=\{\ldots,-3,2,7,12,\ldots\}$$
$$[3]=\{\ldots,-2,3,8,13,\ldots\}$$
$$[4]=\{\ldots,-1,4,9,14,\ldots\}$$

である。$[3]+[4]$ を考える。$[3]$ の元として 8，$[4]$ の元として 9 を選ぶ。$8+9=17$ なので 17 を含む剰余類を探すと $[2]=\{\ldots,-3,2,7,12,17\ldots\}$ なので $[3]+[4]=[2]$ となる。$8,9$ の代わりに $3,4$ を選ぶと (普通はこのように選ぶ)，$3+4=7$ で 7 を含む剰余類はやはり $[2]$ である。このように剰余類の和 $[k_1]+[k_2]$ は，k_1+k_2 を考え，これを (今の場合)5 で割った余りを k_3 とするとき $[k_1]+[k_2]=[k_3]$ となっている。

定義 1.12 で述べたことを証明する。$n\mathbb{Z}$ による剰余類を考える。最初は $a_1 \in [k_1], a_2 \in [k_2]$ の選び方によらずに $[k_1]+[k_2]$ が決まることを示す。そのためには $a_1, b_1 \in [k_1]$，$a_2, b_2 \in [k_2]$ となる任意の a_1, b_1, a_2, b_2 に対し $[a_1+a_2]=[b_1+b_2]$ を示せばよい。$a_1, b_1 \in [k_1]$ よりある整数 p_1, q_1 が存在して $a_1=p_1n+k_1$，$b_1=q_1n+k_1$ と書けている。$a_2, b_2 \in [k_2]$ よりある整数 p_2, q_2 が存在して $a_2=p_2n+k_2$，$b_2=q_2n+k_2$ と書けている。

$$a_1+a_2=p_1n+k_1+p_2n+k_2=(p_1+p_2)n+k_1+k_2$$
$$b_1+b_2=q_1n+k_1+q_2n+k_2=(q_1+q_2)n+k_1+k_2$$

となるので $(a_1+a_2)-(b_1+b_2)=(p_1+p_2-q_1-q_2)n$ となるので $a_1+a_2 \equiv b_1+b_2 \mod n$ となる。即ち $[a_1+a_2]=[b_1+b_2]$ となる。

a_1, a_2 として k_1, k_2 を選ぶことにより

$$[k_1]+[k_2]=[k_1+k_2]$$

が成立することが分かる。

最初に結合法則を示す。整数の和に関して結合法則 $(k_1+k_2)+k_3=k_1+(k_2+k_3)$ は成立している。

$$\begin{aligned}([k_1]+[k_2])+[k_3]&=[k_1+k_2]+[k_3]=[(k_1+k_2)+k_3]\\&=[k_1+(k_2+k_3)]=[k_1]+[k_2+k_3]=[k_1]+([k_2]+[k_3])\end{aligned}$$

となる。

$[0]$ が零元になることを示す。任意の $[k] \in \mathbb{Z}_n$ に対し

$$[0]+[k]=[0+k]=[k]$$

となり [0] が零元であることが分かる。

$$[k] + [-k] = [k + (-k)] = [0]$$

となるので $[k]$ の逆元は $[-k]$ である。

整数に対しては交換法則 $k_1 + k_2 = k_2 + k_1$ が成立しているので，

$$\begin{aligned}[k_1] + [k_2] &= [k_1 + k_2] = [k_2 + k_1] \\ &= [k_2] + [k_1]\end{aligned}$$

となり，交換法則も成立する。

整数の引き算は逆元を加えることと定義された。$\mathbb{Z}_n$ でも同様に定義ができる。即ち

$$[k_1] - [k_2] = [k_1] + [-k_2]$$

と定義する。

1.3 群論からの準備

以下の議論のために必要な群論の知識を簡単に紹介する。

定義 1.13 G を 2 項演算 $\circ$ が定義されている集合とする。演算 $\circ$ が次を満たすとき G を**群**という。

(1) $\forall g_1, g_2, g_3 \in G \;\; (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$ (**結合法則**)

(2) $\exists e \in G \; \forall g \in G \;\; e \circ g = g \circ e = g$ (**単位元の存在**)

(3) $\forall g \in G \; \exists g' \in G \;\; g \circ g' = g' \circ g = e$ (**逆元の存在**)

前の 3 つに加え次も成立するとき G を**可換群**という。

(4) $\forall g_1, g_2 \in G \;\; g_1 \circ g_2 = g_2 \circ g_1$ (**交換法則**)

(3) の元 g' を g の**逆元**といい，g^{-1} と書く。

整数 Z は和に関して可換群をなす。演算は $a \circ b = a + b$ と考える。単位元は 0，a の逆元は $-a$ である。0 を除く有理数 $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ は積に関し郡をなす。$a \circ b = a \cdot b$ であり，単位元は 1，a の逆元は $\dfrac{1}{a}$ である。$\mathbb{Z}_n$ は和に関して可換群をなす。

定義 1.14 群 G の部分集合 H が次を満たすとき G の**部分群**という。

(1) $H \neq \emptyset$

(2) $\forall h_1, h_2 \in H \;\; h_1 \circ h_2 \in H$

(3) $\forall h \in H \;\; h^{-1} \in H$

群 G に対し 部分群 H も同じ 演算に関し 群をなす。

$\mathbb{Z}$ を加法に関する群と考えたとき，任意の整数 n に対し $n\mathbb{Z}$ は $\mathbb{Z}$ の部分群である。

以下この節では群 G は**有限集合**とする。このとき G を有限群という。集合 G の要素の個数を $|G|$ と書き，G の**位数**という。g を群 G の元とする。$g^2 = g \circ g$ とし，g^n を $g^{k+1} = g^k \circ g$ と帰納的に定義する。また $g^0 = e, g^{-n} = \left(g^{-1}\right)^n$ と定義する。

命題 1.15 $\langle g \rangle = \{ g^n \mid n \in \mathbb{N} \}$ と定義すると，これは G の部分群である。$\langle g \rangle$ を g で**生成される**部分群と呼ぶ。

証明　部分群の定義の (1) は $g \in \langle g \rangle$ であるから成立する。(2) は $g^n, g^m \in \langle g \rangle$ に対し $g^n \circ g^m = g^{n+m}$ となるので成立する。

(3) の成立を示すために「ある自然数 n_0 が存在して $g^{n_0} = e$ となる」ことを示す。G は有限集合であるので，

$$g = g^1, g^2, g^3, \ldots, g^n, \ldots,$$

がすべて異なる元になることはない。即ち異なる自然数 m, n が存在して $g^m = g^n$ となる。今 $m > n$ と仮定しても一般性を失わない。このとき $n_0 = m - n$ とおくと n_0 は自然数であり $g^{n_0} = g^{m-n} = g^m \circ g^{-n} = g^m \circ (g^n)^{-1} = g^m \circ (g^m)^{-1} = g^m \circ g^{-m} = g^{m-m} = g^0 = e$ となる。$\langle g \rangle$ の任意の元を g^m とする。m を n_0 で割ったとき商を q 余りを r とすると，$m = qn_0 + r$ $(0 \leq r < n_0)$ より

$$g^m = g^{qn_0+r} = g^{qn_0} \circ g^r = (g^{n_0})^q \circ g^r = e^q \circ g^r = e \circ g^r = g^r$$

となる。よって $m < n_0$ としてよい。このとき $m' = n_0 - m$ とおくと $g^{m'} \in \langle g \rangle$ であり，$g^m g^{m'} = g^{m+m'} = g^{n_0} = e$ となるので，$g^{m'}$ は g^m の逆元であり，(3) が示される。 ∎

命題 1.15 の証明中に示した「ある自然数 n_0 が存在して $g^{n_0} = e$ となる」から次が定義できる。

定義 1.16 有限群 G の元 g に対し $g^n = e$ となる最小の自然数を元 g の**位数**といい，$|g|$ で表す。

$\mathbb{Z}_6$ の元の位数を考える。$\mathbb{Z}_6$ の演算は和であるので，上で $g \circ h$ は $g + h$，g^n は ng 等に変わることに注意する。

$$\mathbb{Z}_6 = \{ [0], [1], [2], [3], [4], [5] \}$$

である。[0] はすでに単位元 (零元) である。即ち $1[0] = [0]$ なので $|[0]| = 1$ である。

[1] は $2[1] = [1] + [1] = [2] \neq [0]$，$3[1] = 2[1] + [1] = [2] + [1] = [3] \neq [0]$，$4[1] = 3[1] + [1] = [3] + [1] = [4] \neq [0]$，$5[1] = 4[1] + [1] = [4] + [1] = [5] \neq [0]$，$6[1] = 5[1] + [1] = [5] + [1] = [6] = [0]$ なので $|[1]| = 6$ である。

[2] は $2[2] = [2] + [2] = [4] \neq [0]$，$3[2] = 2[2] + [2] = [4] + [2] = [6] = [0]$ なので $|[2]| = 3$ である。[3] は $2[3] = [3] + [3] = [6] = [0]$ なので $|[3]| = 2$ である。[4] は $2[4] = [4] + [4] = [8] = [2]$，$3[4] = 2[4] + [4] = [2] + [4] = [6] = [0]$ なので $|[4]| = 3$ である。

[5] は $2[5] = [5] + [5] = [10] = [4]$，$3[5] = 2[5] + [5] = [4] + [5] = [9] = [3]$，$4[5] = 3[5] + [5] = [3] + [5] = [8] = [2]$，$5[5] = 4[5] + [5] = [2] + [5] = [7] = [1]$，$6[5] = 5[5] + [5] = [1] + 5 = [6] = [0]$ より $|[5]| = 6$ である。元の位数はすべて群の位数 $|\mathbb{Z}_6| = 6$ の約数になっている。

演習問題 1.5　$\mathbb{Z}_{10}$ および $\mathbb{Z}_9$ の各元の位数を求めよ。

例から見ると，元の位数は群の位数の約数になっているようである。このことを示すために群の剰余類を考える。

G を群 H をその部分群とする。以下では，群における演算 $a \circ b$ は，$\circ$ を省略して単に ab と書くことにする。

命題 1.17 G を群とし，H をその部分群とする。G の 2 つの元 a, b に対して，

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

となるとき $a \sim_H b$ と決めると，これは G 上の同値関係となる。$a \sim_H b$ である時，a と b は H に関して**同値である** (*equivalent*) という。

証明　同値関係の定義を満たすことを言えば良い。

反射律：　任意の $a \in G$ に対して $aa^{-1} = e \in H$ であるから，反射律を満たす。

対称律：　$a \sim_H b$ ならば $ab^{-1} \in H$ である。H は部分群なので，H の元の逆元も H に属する。すなわち $(ab^{-1})^{-1} = ba^{-1} \in H$ である。従って $b \sim_H a$ であり，対称律を満たす。

推移律：　$a \sim_H b, b \sim_H c$ ならば $ab^{-1} \in H, bc^{-1} \in H$ である。H は部分群なので，H の元の積は H に属する。すなわち，$ab^{-1}bc^{-1} = ac^{-1} \in H$ である。従って，$a \sim_H c$ であり，推移律を満たす。 ∎

この同値関係に関する同値類はどのような集合だろうか？

定義 1.18 $A \subseteq G$ を G の部分集合とし，$b \in G$ とするとき，

$$Ab = \{\ ab \mid a \in A\ \}$$

と書く。

命題 1.19 $a \sim_H b$ であるための必要十分条件は $a \in Hb$ である。($a \sim_H b$ は同値関係なので，$a \sim_H b$ ならば $b \sim_H a$ である。すなわち，$b \in Ha$ が成り立つ。)

証明　$a \sim_H b$ であるということは，定義から，$ab^{-1} \in H$ ということである。すなわち，ある H の元 $h \in H$ が存在して，$ab^{-1} = h$ となっている，ということである。この両辺に b をかけることにより，これは，ある H の元 $h \in H$ が存在して $a = hb$，ということと同値である。$hb \in Hb$ なので，これは，$a \in Hb$ と同値である。 ∎

H を部分群とし，この同値関係による G の 同値類分割を考える。

命題 1.19 より,「H に関して同値」という関係による同値類は全て，ある $b \in G$ があって Hb という形をしていることが分かった。これを b を含む H による**剰余類** (*residue class*)[(1)]という。単位元 e を含む剰余類は H 自身である。G は互いに共通部分を持たない剰余類の和として書ける。

$$G = Ha_1 \cup Ha_2 \cup \cdots Ha_k$$

[(1)] 一般には左剰余類と右剰余類がある。同値関係を $a^{-1}b \in H$ で定義して得られる剰余類を左剰余類といい，ここで定義した剰余類を右剰余類と呼ぶ。この講義では可換群を扱うので右剰余類を剰余類と呼ぶことにする。

これを G の H による**剰余類分解** (*residue class decomposition*) あるいは**剰余類分割** (*residue class partition*) という。剰余類の個数 k を $|G:H|$ と書きこれを**指数**という。

例を見る。演算は加法で $G=\mathbb{Z}_9$ とする。$H=\langle\,[3]\,\rangle$ とする。$2[3]=[6], 3[3]=[9]=[0]$ なので $H=\{\,[0],[3],[6]\,\}$ である。$H+[1]=\{\,[1],[4],[7]\,\}$ である。上では演算を乗法で書いているので剰余類は Ha の形になっているが，ここで演算は加法なので $H+a$ の形になる。$H+[2]=\{\,[2],[5],[8]\,\}$ である。よって

$$G=H\cup(H+[1])\cup(H+[2])$$

と剰余類分割される。[1] の代わりに [4] をとっても

$$H+[4]=\{\,[4],[7],[10]\,\}=\{\,[4],[7],[1]\,\}=\{\,[1],[4],[7]\,\}=H+[1]$$

となっている。

演習問題 1.6　$G=\mathbb{Z}_{12}$ とする。$H=\langle\,9\,\rangle$ とするとき剰余類分割を求めよ。また $N=\langle\,2\,\rangle$ とするとき，剰余類分割を求めよ。

定理 1.20 G を有限群とし H をその部分群とする。このとき，

$$|G|=|G:H|\cdot|H|$$

が成り立つ。

証明　剰余類分解は共通部分をもたない分割なので $|G|=\sum_{i=1}^{k}|Ha_i|$ が成立している。すべての i (i=1,...,k) に対し $|H|=|Ha_i|$ が成立することを示す。H から Ha_i への写像 f を $f(h)=ha_i$ で定義する。$f(h_1)=f(h_2)$ のとき $h_1a_i=h_2a_i$ である。右から a_i^{-1} をかけることにより $h_1=h_2$ が得られる。よって f は単射である。Ha_i の任意の元 w に対し $h\in H$ が存在して $w=ha_i$ と書ける。このとき $f(h)=ha_i=w$ なので f は全射である。以上により f は全単射になるので H と Ha_i の元の個数は等しい，即ち $|H|=|Ha_i|$ である。よって

$$|G|=\sum_{i=1}^{k}|Ha_i|=\sum_{i=1}^{k}|H|=k|H|=|G:H|\cdot|H|$$

が成立する。∎

これにより，次の定理が成り立つ。

定理 1.21 [Lagrange's theorem] G を有限群とし H をその部分群とする。$|H|$ 及び $|G:H|$ は G の約数である。

この定理と次の演習問題から元の位数は群の位数の約数であることが分かる。

演習問題 1.7　$|\langle\,g\,\rangle|=|g|$ を示せ。