暗号の数理要綱 #3

1.4 剰余類

以下では，群における演算 $a \cdot b$ は，$\cdot$ を省略して単に ab と書くことにする。また，

命題 1.21 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 1.22 $A \subseteq G$ 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 1.23 $a \sim_H b$ 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。

この命題より,「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。

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

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。

[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。

1.5 整数の合同類

剰余類分割の最も重要な例は，整数の合同類と呼ばれるものである。

$\mathbb{Z}$ 上に加法を演算として定義すると群になる。これは可換群である。$n \in \mathbb{Z}$ 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る。これは，部分群となる。なぜなら，$nk_1, nk_2 \in n\mathbb{Z}$ とすると，$nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}$ であり，nk の逆元は $-nk = n(-k) \in n\mathbb{Z}$ となって，命題 1.14 の条件を満たす。

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。

部分群 $n\mathbb{Z}$ に関する同値関係は次のようになる。

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

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。

- $n\mathbb{Z} = (-n)\mathbb{Z}$ 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 $a = b$ であり，全ての整数は異なる剰余類に属する。そこで以下では，$n > 0$ とする。

定理 1.24 [**整数の剰余定理**] n を自然数とする。任意の整数 a に対して，ある整数 q と，$0 \leqq r < n$ となる整数 r があって，

$$a = qn + r$$

となる。また，このような q と r は a から一意的に定まる。

証明

$$S_q = \{\ k \in \mathbb{Z} \mid qn \leqq k < (q+1)n\ \}$$

とすると，$\{S_q\}_{q \in \mathbb{Z}}$ は $\mathbb{Z}$ を分割している。

a を任意の整数とすると，a はある S_q に含まれる。また，そのような q は a に対してただ一つである。

$qn \leqq a < (q+1)n$ である。$r = a - qn$ とおくと，$a = qn + r$ であり，$r = a - qn \geqq 0$ である。また，$a < (q+1)n$ より，$r = a - qn < n.$ である。

$r = a - qn$ でなければならないから，r も a から一意的に決まる。∎

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，

$$3\mathbb{Z} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$
$$1 + 3\mathbb{Z} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}$$
$$2 + 3\mathbb{Z} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}$$

などとなる。

$a+n\mathbb{Z}$ 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。すなわち，$a + n\mathbb{Z}$ の元は全て同じ剰余類に含まれる。

命題 1.25 $n\mathbb{Z}$ 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。∎

この命題より，$n\mathbb{Z}$ による剰余類の代表元として，

$$\{\ 0, 1, 2, \cdots, n-1\ \}$$

がとれることがわかる。

$n\mathbb{Z}$ による剰余類 $r + n\mathbb{Z}$ に含まれる整数 a は $a = qn + r$ と書けるので，n **で割った時の余り**が r 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。

1.6　剰余群

G を可換群とし H を部分群とする。H によって G を剰余類に分割できるが，**その剰余類全体の集合** というものを考える。この場合，それぞれの剰余類がこの集合の各要素となる。この集合を G/H と書く。

$a \in G$ を含む剰余類は Ha という形をしており，これは G の部分集合だが，これを G/H の一つの要素と見なすことにする。

この表し方は混乱を引き起こす可能性もあるので，$a \in G$ を含む剰余類を $[a]$ という記号で表すこともある。この場合，H という部分群による剰余類である，ということが明示されていないので，注意が必要である。この記号を使うと，$a \in G$ であるとき $[a] \in G/H$ であるので，どの集合の元であるのかは明確になる。

当然 $a \sim_H b$ は $[a] = [b]$ と同値となる。
このセクションでは，可換群 G とその部分群 H を固定する。

G/H に群の構造を入れることができるかどうかを考えてみる。
さて，２つの剰余類 $[a]$ と $[b]$ の積というものをどのように定義したら良いだろうか？ 自然に考えられる積の定義としては，

$$[a] \cdot [b] = [ab]$$

というものである。しかし，この定義は代表元のとり方に依存している。これで剰余類同士の積を定義できる，という言うためには，別の代表元を使ったとしても，同じ剰余類が定義されていなければならない。すなわち，

$$a \sim a' \qquad b \sim b'$$

とする時，$ab \sim a'b'$ になっていれば，代表元の選び方によらずに，剰余類が指定できることになる。
$a \sim a'$ ということは $a(a')^{-1} \in H$ であるので，ある $h \in H$ があって $a(a')^{-1} = h$ となっている。同様に，$b \sim b'$ ということは，ある $k \in H$ があって $b(b')^{-1} = k$ となっている。
$a = ha', b = kb'$ であり，演算は可換と仮定しているので，$ab = ha'kb' = hk(a'b')$ であるから，

$$(ab)(a'b')^{-1} = hk \in H$$

となり，$ab \sim a'b'$ である。
以上から，剰余類全体の集合 G/H に

$$[a] \cdot [b] = [ab]$$

によって演算が定義できることがわかった。

命題 1.26 この演算によって，G の H による剰余類全体の集合は群になる。この群を，G の H による **剰余群** と言い G/H と書く。

例 1.27

$$\mathbb{Z}/n\mathbb{Z} = \{\ 0, 1, 2, \cdots, n-1\ \}$$

は，加法について群となる。これを n **を法とする合同類群** という。
$\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}_n$ と書く。

演習問題 1.12　命題 1.26 を証明せよ。