第7章　剰余類と剰余環

7.1　剰余類

定義 7.1 整数 m および a に対して，$x \equiv a \pmod{m}$ をみたす整数 x 全体の集合を $a + m\boldsymbol{Z}$ で表し，**法 m に関する（a の属する）剰余類**という;

$$a + m\boldsymbol{Z} = \left\{ x \in \boldsymbol{Z} \,\middle|\, x \equiv a \pmod{m} \right\}.$$

$0 + m\boldsymbol{Z}$ は $m\boldsymbol{Z}$ のことである． 後の説明にもあるように，m が特定されている場合には $\overline{a}$ と略記することがある; $\overline{a} = a + m\boldsymbol{Z}$.

次の命題は剰余類の定義から簡単に示すことができる．

命題 7.2 m および a, b, c を整数とする．

(1) $a + m\boldsymbol{Z} = b + m\boldsymbol{Z}$, $(a + m\boldsymbol{Z}) \cap (b + m\boldsymbol{Z}) = \phi$ のどちらか一方が必ず成り立つ．

(2) $b, c \in a + m\boldsymbol{Z}$ ならば $b \equiv c \pmod{m}$.

(3) 次の 4 つは互いに同値である;

$$a \equiv b \pmod{m}, \quad a \in b + m\boldsymbol{Z}, \quad b \in a + m\boldsymbol{Z}, \quad a + m\boldsymbol{Z} = b + m\boldsymbol{Z}$$

法 m で合同な整数をひとまとめにした $\boldsymbol{Z}$ の部分集合が，m を法とする剰余類である．合同式においては m を法として合同な数を “等しい” とみなして計算する． 言い換えれば，剰余類をあたかも数のように扱うのが合同式の計算であると言える．

定義 7.3 整数 m に対して，法 m に関するすべての剰余類を元とする集合を，**法 m に関する剰余環**といい，$\boldsymbol{Z}/m\boldsymbol{Z}$ で表す;

$$\boldsymbol{Z}/m\boldsymbol{Z} = \{ a + m\boldsymbol{Z} \mid a \in \boldsymbol{Z} \}.$$

さて，しばらくの間，自然数 m を固定し，剰余類 $a + m\boldsymbol{Z}$ を $\overline{a}$ と略す． すべての整数は m を法として $0, 1, 2, \cdots, m-1$ のどれかと合同で，これらは互いに合同ではないから

$$\boldsymbol{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{m-1}, \qquad \overline{a} \cap \overline{b} = \phi \quad (0 \le a < b < m).$$

したがって，剰余類は全部で m 個あり，

$$\boldsymbol{Z}/m\boldsymbol{Z} = \left\{ \overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1} \right\}$$

と書くことができる． たとえば，$\boldsymbol{Z}/7\boldsymbol{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ であるが，意地悪く，これを

$$\boldsymbol{Z}/7\boldsymbol{Z} = \left\{\overline{49},\ \overline{-13},\ \overline{9^7},\ \overline{5^5},\ \overline{123456},\ \overline{3\cdot 74},\ \overline{66^{33}}\right\}$$

と書いてもかまわない（ホントかな，確かめてね）．

7.2　剰余類の和と積

はじめに，合同式に関して

$$a_1 \equiv a_2,\ b_1 \equiv b_2 \pmod{m} \implies a_1 + b_1 \equiv a_2 + b_2,\ a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

が成り立つことに注意しよう（命題 5.2）． このことは，2 つの剰余類からそれぞれの元を選ぶとき，それらの和や積の属する剰余類が選んだ元によらずに定まることを示している． そこで，剰余環における剰余類の “和” や “積” を以下のように定義することができる．

定義 7.4 剰余類 $a + m\boldsymbol{Z},\ b + m\boldsymbol{Z} \in \boldsymbol{Z}/m\boldsymbol{Z}$ に対して，それらの和，積を

$$(a + m\boldsymbol{Z}) + (b + m\boldsymbol{Z}) = (a + b) + m\boldsymbol{Z}, \qquad (a + m\boldsymbol{Z})(b + m\boldsymbol{Z}) = (ab) + m\boldsymbol{Z}$$

によって定める．

この定義による和と積は，略記法で

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a}\,\overline{b} = \overline{ab}$$

と書いても同じである． こう表すとアタリマエのように見えるでしょ？ たとえば，7 を法として $\overline{2} + \overline{3} = \overline{5}$ とか $\overline{2}\cdot\overline{3} = \overline{6}$ など…． 一方，$\overline{3} + \overline{5} = \overline{1}$ や $\overline{4}\cdot\overline{6} = \overline{3}$ となると少しはアタリマエじゃなくなる…． 剰余類の等式

$$\overline{a} + \overline{b} = \overline{c}, \quad \overline{a}\,\overline{b} = \overline{d}$$

における和や積は，合同式

$$a + b \equiv c, \quad ab \equiv d \pmod{m}$$

における整数の和，積を，剰余類の和，積とみなして表したもの，と考えればよい． **「合同式」**は**「剰余環における等式」**であり，その意味で，剰余類の演算は合同式に現れる演算を，より直感的に表現していると考えられる． たとえば，未知数 x をもつ合同式

$$ax \equiv b \pmod{m}$$

は，剰余類に関する方程式

$$\overline{a}x = \overline{b}$$

と同等であり，より簡明になる． ただし，未知数 x として，前者の場合は整数を想定するのに対し，後者は剰余類つまり $\boldsymbol{Z}/m\boldsymbol{Z}$ の元を想定するという違いがある． しかし，慣れてくると，これらをあまり区別せずに議論できるようになる．

なお，“$\equiv \pmod{\ }$” を $\boldsymbol{Z}$ 上の**同値関係**とみなし，それによって $\boldsymbol{Z}$ を**同値類別**して得られる**商集合**として $\boldsymbol{Z}/m\boldsymbol{Z}$ をとらえることもできる． この考え方はめっちゃ一般化され，数学のいろんな分野に現れるけど，詳しくは演習の時間にまかせちゃったりして，ずるい？

7.3 剰余環の分解

自然数 m の倍数 M をとる． いま，整数 a, b が $a \equiv b \pmod{M}$ をみたすならば，$M|(a-b)$ だから $m|(a-b)$，よって $a \equiv b \pmod{m}$ もみたすので，写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow \boldsymbol{Z}/m\boldsymbol{Z}, \qquad a + M\boldsymbol{Z} \mapsto a + m\boldsymbol{Z}$$

を定めることができる． さらに，M がふたつの自然数 m, n の公倍数ならば，上と同様にして

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}, \qquad a + M\boldsymbol{Z} \mapsto a + n\boldsymbol{Z}$$

も定まり，これらをあわせて剰余環の直積への写像

$$F : \boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z}), \qquad a + M\boldsymbol{Z} \mapsto (a + m\boldsymbol{Z}, a + n\boldsymbol{Z})$$

が定義できる． 別の書き方をすれば，$F(\overline{a}) = (\overline{a}, \overline{a})$ となる． ただし，それぞれの $\overline{a}$ は，法 M および法 m，法 n に関する剰余類を考えるわけである． このような写像を**自然な写像**とよぶ．

ここで，とくに M が m, n の最小公倍数のときは，F は単射である． これを確かめるために，$a, b \in \boldsymbol{Z}$ が $F(a + M\boldsymbol{Z}) = F(b + M\boldsymbol{Z})$ をみたすとすると，

$$a + m\boldsymbol{Z} = b + m\boldsymbol{Z} \quad \text{かつ} \quad a + n\boldsymbol{Z} = b + n\boldsymbol{Z},$$

よって $a - b$ は，m の倍数でもあり n の倍数でもあるから，$M = \mathrm{lcm}(m, n)$ の倍数，すなわち $a + M\boldsymbol{Z} = b + M\boldsymbol{Z}$ を得る． これで F が単射であることが確かめられた． 以上は，2 つの自然数 m, n についての話だが，これを次のように一般化するのは難しくない．

命題 7.5 自然数 $m_1, \ldots, m_r$ に対して，M をそれらの公倍数とすると，自然な写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m_1\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/m_r\boldsymbol{Z})$$

が定義できる． とくに，M が $m_1, \ldots, m_r$ の最小公倍数ならば，この写像は単射である．

次に，自然数 M が 2 つの互いに素な約数の積として表される場合を考えよう． すなわち，$M = mn$ であって，かつ m, n は互いに素とする． このとき，m, n の最小公倍数は M と一致する． したがって，命題 7.5 より，自然な写像

$$F : \boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$$

は単射である． さらに今の場合，$\boldsymbol{Z}/M\boldsymbol{Z}$ の元の個数は $M = mn$ で，これは直積集合 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ の元の個数と等しいから，F は全射にもなっている． このことは，**元の個数が等しい** 2 つの有限集合 A, B に対して，A から B への写像は，**単射**ならば**全射**でもある，という事実に着目すれば納得できるはずである． さらに，どの 2 つも互いに素である自然数 $m_1, \ldots, m_r$ の最小公倍数が積 $m_1 \cdots m_r$ と一致することに注意すれば，上と同様にして次が得られる．

定理 7.6 どの 2 つも互いに素な自然数の組 $m_1, \ldots, m_r$ に対して，$M = m_1 \cdots m_r$ とおけば，自然な写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m_1\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/m_r\boldsymbol{Z})$$

が定義でき，さらにこれは全単射である．

とくに，自然数 n に対して，その素因数分解を

$$n = p_1^{e_1} \cdots p_r^{e_r} \qquad (p_i \text{ は相異なる素数},\ e_i > 0)$$

とすると，自然な写像

$$\boldsymbol{Z}/n\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/p_1^{e_1}\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/p_r^{e_r}\boldsymbol{Z})$$

は全単射であることがわかる． この場合，定理 7.6 は，直積分解を通して，剰余環 $\boldsymbol{Z}/n\boldsymbol{Z}$ の性質が，より単純と考えられる剰余環 $\boldsymbol{Z}/p_i^{e_i}\boldsymbol{Z}$ の性質に帰着されることを示唆している．

7.4 中国の剰余定理再論

定理 7.6 を用いて，**中国の剰余定理** (定理 6.5) の別証明を与えることができる．

定理 6.5 の第 3 証明 定理 7.6 の写像を F とする． いま，F が全射であることより，与えられた $a_1, \ldots, a_r \in \boldsymbol{Z}$ に対して $F(x + M\boldsymbol{Z}) = (a_1 + m_1\boldsymbol{Z}, \ldots, a_r + m_r\boldsymbol{Z})$ をみたす $x \in \boldsymbol{Z}$ が存在する． このとき，

$$x + m_1\boldsymbol{Z} = a_1 + m_1\boldsymbol{Z}, \quad \ldots, \quad x + m_r\boldsymbol{Z} = a_r + m_r\boldsymbol{Z}$$

が成り立つが，これらの等式は，x が連立合同式 $x \equiv a_i \pmod{m_i}$ $(i = 1, \ldots, r)$ の解であることを示している． また，x, x' がともに解であるとすると，$F(x + M\boldsymbol{Z}) = F(x' + M\boldsymbol{Z})$ であるが，F が単射であることから，$x + M\boldsymbol{Z} = x' + M\boldsymbol{Z}$，すなわち $x \equiv x' \pmod{M}$ が導かれ，法 M に関する一意性も示されたことになる． □

この証明の逆をたどれば，定理 6.5 から定理 7.6 を導くことができる． その意味で，定理 7.6 は**中国の剰余定理**の言い換えとみなせる．