

第8章 剰余類の演算

8.1 剰余類の和と積

はじめに，合同式に関して

$$r_1 \equiv r_2, s_1 \equiv s_2 \pmod{m} \implies r_1 + s_1 \equiv r_2 + s_2, r_1 s_1 \equiv r_2 s_2 \pmod{m}$$

が成り立つことに注意しよう（命題 5.2）．このことは，二つの剰余類からそれぞれの元を選ぶとき，それらの和や積から定ま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，“剰余類”の“和”や“積”を以下のように定義できることがわかる．

定義 8.1 剰余類 $\mathcal{R}, \mathcal{S} \in \mathbb{Z}/m\mathbb{Z}$ に対して， $r \in \mathcal{R}, s \in \mathcal{S}$ をとるとき，和 $r + s$ の属する剰余類 $\mathcal{T} \in \mathbb{Z}/m\mathbb{Z}$ を \mathcal{R}, \mathcal{S} の和といい，積 rs の属する剰余類 $\mathcal{U} \in \mathbb{Z}/m\mathbb{Z}$ を \mathcal{R}, \mathcal{S} の積という．それぞれ，通常のとおり，

$$\mathcal{R} + \mathcal{S} = \mathcal{T}, \quad \mathcal{R}\mathcal{S} = \mathcal{U}$$

のように書く．

定義を書き換えれば， $a, b \in \mathbb{Z}$ で定まる剰余類 $a + m\mathbb{Z}, b + m\mathbb{Z}$ の和や積を

$$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}, \quad (a + m\mathbb{Z})(b + m\mathbb{Z}) = (ab) + m\mathbb{Z}$$

によって定めようということである．あるいは，略記法で

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a}\bar{b} = \overline{ab}$$

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？つまり，たとえば，7 を法として $\bar{2} + \bar{3} = \bar{5}$ とか $\bar{2} \cdot \bar{3} = \bar{6}$ など...．一方， $\bar{3} + \bar{5} = \bar{1}$ や $\bar{4} \cdot \bar{6} = \bar{3}$ となると少しはアタリマエじゃなくなる...．いずれにしろ，剰余類の間の等式 $\bar{a} + \bar{b} = \bar{c}$, $\bar{a}\bar{b} = \bar{d}$ は，合同式 $a + b \equiv c$, $ab \equiv d \pmod{m}$ における和や積を，剰余類の和，積とみなして表したものと考えればよい．つまり，整数における合同式は剰余類における等式であり，その意味で，剰余類の演算は合同式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， $\mathbb{Z}/m\mathbb{Z}$ の元に関する等式 $\bar{a}x = \bar{b}$ と同等であり，こうすることでより簡明になる．ただし，前者の x は整数を想定するのに対し，後者の x は剰余類つまり $\mathbb{Z}/m\mathbb{Z}$ の元を想定するのである．

8.2 剰余集合の分解

前章，定理 7.1 の第 3 証明において，整数 m, n が互いに素ならば，写像

$$F : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$$

が定まり全単射になることを示した．一般に，集合 A, B にそれぞれ和や積が定義されているとき，直積集合の 2 元 $(a, b), (a', b') \in A \times B$ に対して

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b)(a', b') = (aa', bb')$$

によって和，積が自然に定義できる．次の定理は，前節で定義した剰余類の和や積が F によって保存されることを示している．

定理 8.2 互いに素な整数 m, n について，写像 F を上のように定めるとき，

$$F(\mathcal{R} + \mathcal{S}) = F(\mathcal{R}) + F(\mathcal{S}), \quad F(\mathcal{R}\mathcal{S}) = F(\mathcal{R})F(\mathcal{S})$$

が任意の $\mathcal{R}, \mathcal{S} \in \mathbb{Z}/mn\mathbb{Z}$ に対して成り立つ．

証明 $r \in \mathcal{R}, s \in \mathcal{S}$ とするとき， $\mathcal{R} = r + mn\mathbb{Z}, \mathcal{S} = s + mn\mathbb{Z}, \mathcal{R} + \mathcal{S} = (r + s) + mn\mathbb{Z}$ に注意して，

$$\begin{aligned} F(\mathcal{R} + \mathcal{S}) &= F((r + s) + mn\mathbb{Z}) \\ &= ((r + m\mathbb{Z}) + (s + m\mathbb{Z}), (r + n\mathbb{Z}) + (s + n\mathbb{Z})) \\ &= (r + m\mathbb{Z}, r + n\mathbb{Z}) + (s + m\mathbb{Z}, s + n\mathbb{Z}) \\ &= F(r + mn\mathbb{Z}) + F(s + mn\mathbb{Z}) \\ &= F(\mathcal{R}) + F(\mathcal{S}). \end{aligned}$$

積についても同様である．

この定理をみたとような写像を，一般に“可換環の間の準同型写像”という．“可換環”とは和と積がふつうにできる集合のことであるが，今の場合， F は全単射であったから，剰余集合 $\mathbb{Z}/mn\mathbb{Z}$ は 2 つの剰余集合の直積 $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ と演算（和と積）も込めて同じ“構造”であることがわかる．つまり，“可換環として同型”であり，

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

と書いたりするんだけど，詳しくは「代数 I」でね．

8.3 既約剰余類群

法 m に関する逆元や零因子の概念も、剰余類のもつ性質ととらえることで簡明になる。剰余類 $\mathcal{R} \in \mathbb{Z}/m\mathbb{Z}$ のある元 r が法 m に関する逆元 $s \in \mathbb{Z}$ をもつとする。このとき、剰余類 $\mathcal{S} = \bar{s}$ の任意の元は法 m に関する r の逆元であり、さらに \mathcal{R} の任意の元は \mathcal{S} の任意の元を法 m に関する逆元として持つ。すなわち $a \in \mathcal{R}, b \in \mathcal{S}$ ならば $ab \equiv 1 \pmod{m}$ 、あるいは $\mathcal{R}\mathcal{S} = \bar{1}$ と書くこともできる（ああ、ややこしい）。このようなとき、 \mathcal{S} は \mathcal{R} の逆元であると定義し \mathcal{R}^{-1} で表す。この定義のもとで次が成り立つ。

- 法 m に関する剰余類の逆元は、もし存在するならば一意である。

実際、剰余類 $\mathcal{S}, \mathcal{T} \in \mathbb{Z}/m\mathbb{Z}$ がともに剰余類 $\mathcal{R} \in \mathbb{Z}/m\mathbb{Z}$ の逆元ならば、それぞれの元 $r \in \mathcal{R}, s \in \mathcal{S}, t \in \mathcal{T}$ をとるとき、 $rs \equiv rt \equiv 1 \pmod{m}$ だから、 $t \equiv t(rs) \equiv (rt)s \equiv s \pmod{m}$ 、ゆえに $\mathcal{T} = \bar{t} = \bar{s} = \mathcal{S}$ が成り立ち、一意性がいえた。

一方、剰余類 $\mathcal{R} \in \mathbb{Z}/m\mathbb{Z}$ のある元が法 m に関する零因子ならば、 \mathcal{R} に属するすべての元は法 m に関する零因子となる。そこで、このような剰余類を零因子とよぶことにする。つまり、剰余類 $\mathcal{R} \in \mathbb{Z}/m\mathbb{Z}$ が零因子であるための必要十分条件は、 $\mathcal{R}\mathcal{S} = \bar{0}$ をみたす剰余類 $\mathcal{S} \neq \bar{0}$ が存在することである。

次の命題は定理 5.6 からの直接の帰結である。

命題 8.3 m を 2 以上の自然数とする。法 m に関する剰余類が逆元もつためには、零因子でないことが必要十分である。また、このような剰余類は m と互いに素な整数 a によって \bar{a} と表される。

定義 8.4 m を 1 でない自然数とする。法 m に関する逆元をもつ剰余類（同じことだが、零因子でない剰余類）を、法 m に関する既約剰余類という。また、それら全体のなす集合を、法 m に関する既約剰余類群といい $(\mathbb{Z}/m\mathbb{Z})^\times$ で表す。

具体的な例をあげれば、 $\mathbb{Z}/10\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{9}\}$ のうち、逆元をもつ剰余類は $\bar{1}, \bar{3}, \bar{7}, \bar{9}$ であり、零因子は $\bar{0}, \bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$ である。すなわち既約剰余類群は $(\mathbb{Z}/10\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ である。また、 $\bar{1}^{-1} = \bar{1}, \bar{3}^{-1} = \bar{7}, \bar{7}^{-1} = \bar{3}, \bar{9}^{-1} = \bar{9}$ となっている。

一般に法 m に関する既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ について、次が成り立つ。

- 積について閉じている。
- 各元の逆元がその中に存在する。
- 元の個数は $\varphi(m)$ である。

はじめの 2 つの性質は $(\mathbb{Z}/m\mathbb{Z})^\times$ が乗法に関して群であることを示している（結合律が成り立たなきゃダメとか、必ずしも可換じゃなくてもいいよとか、いろいろ細かい話があるんだけど、詳しいことはオトナ（3年生）になってからね）。元の個数に関しては、定義 6.9 と命題 8.3 からすぐわかる。

さて、ここで、前章、定理 7.1 の第 3 証明で導入し前節でも扱った写像

$$F : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$$

を用いて、宿題であった第 6 章の補題 6.11 の証明を与えよう。

補題 6.11 の証明 まず、 m, n は互いに素な整数なので、 F が全単射であることに注意しておく。いま、整数 a が mn と互いに素ならば、 a は m と n とともに互いに素になることは明らかである。したがって、 F を既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ に制限することにより、写像

$$G : (\mathbb{Z}/mn\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

が定まる。 F が単射なので G も単射であるが、以下において G は全射でもあることを確かめよう。これにより、元の個数を比べて

$$\varphi(mn) = \varphi(m)\varphi(n)$$

より証明が完了する。全射性を示すために、 $\xi \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ を任意にとると、

$$\xi = (a + m\mathbb{Z}, b + n\mathbb{Z}), \quad \gcd(a, m) = \gcd(b, n) = 1$$

と書ける。ここで、 F は全射であったから、 $F(x + mn\mathbb{Z}) = \xi$ すなわち

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$$

をみたす $x \in \mathbb{Z}$ が存在する。このとき、簡単な考察により、 x と mn が互いに素であることはすぐにわかる（確かめよ！）。よって $x + mn\mathbb{Z} \in (\mathbb{Z}/mn\mathbb{Z})^\times$ かつ $G(x + mn\mathbb{Z}) = \xi$ であり、全射であることが示された。

前節で述べたように、 m, n が互いに素な整数のとき、剰余集合について“同型”

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

が成り立つことが定理 7.1 の第 3 証明の主旨であった。一方、上の証明から、既約剰余類群についても“同型”

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

が成り立つことがわかる。ただし、ここでいう“同型”は、積に関する“構造”だけに着目していることに注意せよ（前者は“可換環に関する同型”、後者は“群に関する同型”である）。このように考えると、上の証明も、そのアイデアの出所であった定理 7.1 第 3 証明も同じようなことをやっているように見える。しかし、上の証明では、2 つの集合の間に単射が存在するときに、その写像の全射性から集合の元の個数が等しいことを導いているのに対し、定理 7.1 第 3 証明では、逆に元の個数が等しいことから全射であることを導いている。これらに違いに注目して、証明の流れを味わうことができるようになれば、キミも立派な数学科学生というわけだ。