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

$$r_1 \equiv r_2,\ s_1 \equiv s_2 \pmod m \implies r_1+s_1 \equiv r_2+s_2,\ r_1s_1 \equiv r_2s_2 \pmod m$$

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 $\mathcal{R}, \mathcal{S} \in \boldsymbol{Z}/m\boldsymbol{Z}$ 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 $\mathcal{T} \in \boldsymbol{Z}/m\boldsymbol{Z}$ を $\mathcal{R}, \mathcal{S}$ の和といい，積 rs の属する剰余類 $\mathcal{U} \in \boldsymbol{Z}/m\boldsymbol{Z}$ を $\mathcal{R}, \mathcal{S}$ の積という．それぞれ，通常のとおり，

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

と書く．

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

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

によって定めようということである．あるいは，略記法で

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

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？ つまり，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…．いずれにしろ，剰余類の間の等式 $\overline{a}+\overline{b}=\overline{c}$, $\overline{a}\overline{b}=\overline{d}$ 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，$\boldsymbol{Z}/m\boldsymbol{Z}$ の元に関する等式 $\overline{a}x=\overline{b}$ と同等であり，こうすることでより簡明になる．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 $\boldsymbol{Z}/m\boldsymbol{Z}$ の元を想定するのである．

8.2　剰余集合の分解

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 $A \times B$ の二つの元 (a,b), (a',b') に対して

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

によって和，積が自然に定義できる．とくに，直積 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ には自然に和や積が定まる．

さて，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

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

が定まり全単射になることを示したが，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，

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

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

証明　$r \in \mathcal{R},\ s \in \mathcal{S}$ とするとき，

$$\mathcal{R}=r+mn\boldsymbol{Z}, \quad \mathcal{S}=s+mn\boldsymbol{Z}, \quad \mathcal{R}+\mathcal{S}=(r+s)+mn\boldsymbol{Z}$$

に注意して，

$$\begin{aligned}
F(\mathcal{R}+\mathcal{S}) &= F((r+s)+mn\boldsymbol{Z}) \\
&= ((r+s)+m\boldsymbol{Z},\ (r+s)+n\boldsymbol{Z}) && \text{【}F\text{ の定義】} \\
&= ((r+m\boldsymbol{Z})+(s+m\boldsymbol{Z}),\ (r+n\boldsymbol{Z})+(s+n\boldsymbol{Z})) && \text{【剰余類の和の定義】} \\
&= (r+m\boldsymbol{Z},\, r+n\boldsymbol{Z})+(s+m\boldsymbol{Z},\, s+n\boldsymbol{Z}) && \text{【直積の和の定義】} \\
&= F(r+mn\boldsymbol{Z})+F(s+mn\boldsymbol{Z}) && \text{【}F\text{ の定義】} \\
&= F(\mathcal{R})+F(\mathcal{S}).
\end{aligned}$$

積についても同様である．　□

この定理をみたすような写像を，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 $\boldsymbol{Z}/mn\boldsymbol{Z}$ は 2 つの剰余集合の直積 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ 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，

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

と書いたりするんだけど，詳しくは「代数 I」で学ぶ．

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．

まず，剰余類 $\mathcal{R} \in \boldsymbol{Z}/m\boldsymbol{Z}$ のある元 r が法 m に関して可逆で，s をその逆元とする． このとき，$\mathcal{R}$ の任意の元は法 m に関して可逆であり，さらに $\overline{s} = \mathcal{S}$ の任意の元を逆元として持つ． すなわち $a \in \mathcal{R}, b \in \mathcal{S}$ ならば $ab \equiv 1 \pmod{m}$，あるいは $\mathcal{RS} = \overline{1}$ と書くこともできる（ああ，ややこしい）． このようなとき，$\mathcal{R}$ は**可逆**であるという． また，$\mathcal{S}$ を $\mathcal{R}$ の**逆元**といい $\mathcal{R}^{-1}$ で表す． 法 m に関する剰余類の逆元は，もし存在するならば一意的である． たとえば，$\boldsymbol{Z}/10\boldsymbol{Z}$ においては，$\overline{3}\cdot\overline{7} = \overline{1}$ なので，$\overline{3}$ は可逆で，$\overline{3}^{-1} = \overline{7}$ である．

一方，剰余類 $\mathcal{R} \in \boldsymbol{Z}/m\boldsymbol{Z}$ が法 m に関する零因子をひとつでも持つならば，$\mathcal{R}$ 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 $\mathcal{R} \in \boldsymbol{Z}/m\boldsymbol{Z}$ が零因子であるための必要十分条件は，$\mathcal{RS} = \overline{0}$ をみたす剰余類 $\mathcal{S} \neq \overline{0}$ が存在することである．

次の命題は定理 5.9 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 $\overline{a}$ 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 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ で表す．

例 8.5 $\boldsymbol{Z}/10\boldsymbol{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{9}\}$ のうち，逆元をもつ剰余類は $\overline{1}, \overline{3}, \overline{7}, \overline{9}$ であり，零因子は $\overline{0}, \overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}$ である． すなわち既約剰余類群は $(\boldsymbol{Z}/10\boldsymbol{Z})^{\times} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ である． また，$\overline{1}^{-1} = \overline{1},\ \overline{3}^{-1} = \overline{7},\ \overline{7}^{-1} = \overline{3},\ \overline{9}^{-1} = \overline{9}$ となっている．

一般に法 m に関する既約剰余類群 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ 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 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ が乗法に関して “群” であることを示しているのだが，これも詳しいことは「代数 I」で． なお，$(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ の元の個数が $\varphi(m)$ であることは，定義 6.9 と命題 8.3 からすぐにわかる．

8.4 既約剰余類群の分解

この節では，宿題であった第 6 章最後の

補題 6.11 [**再記**] 互いに素な自然数 m, n に対して $\varphi(mn) = \varphi(m)\varphi(n)$.

の証明を与えよう．前章，定理 7.1 の第 3 証明で導入し，この章でも扱っている写像

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

が全単射であることが重要な根拠となる．

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 とも n とも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 $(\boldsymbol{Z}/mn\boldsymbol{Z})^\times$ に制限することにより，写像

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

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．そこで，全射性を示すために，$\xi \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times \times (\boldsymbol{Z}/n\boldsymbol{Z})^\times$ を任意にとると，

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

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

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

をみたす $x \in \boldsymbol{Z}$ が存在する．このとき，$\gcd(a,m) = \gcd(b,n) = 1$ から，$\gcd(x, mn) = 1$ がすぐに確かめられる（ホントに確かめよ！）．よって $x + mn\boldsymbol{Z} \in (\boldsymbol{Z}/mn\boldsymbol{Z})^\times$ かつ $G(x+mn\boldsymbol{Z}) = \xi$ 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”

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

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”

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

が成り立つことがわかる．ただし，後者の “同型” は，“積の構造” 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性を導いている．これらに違いに注目して二つの証明のストーリーを味わえるようになれば，キミも立派な数学科学生というわけだ．