第8章　既約剰余類群とオイラー関数

8.1　既約剰余類群

m を 2 以上の整数とし，α を法 m に関する剰余類，すなわち $\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ とする． いま，$a \in \alpha$ とすると $\alpha = a + m\boldsymbol{Z}$ である． a が法 m に関して可逆ならば，α に属するすべての整数は法 m に関して可逆となる． さらに，整数 b が m を法とする a の逆元ならば，剰余類 $b + m\boldsymbol{Z}$ に属するすべての整数は法 m に関する a の逆元である． 一方，a が法 m に関する零因子ならば，α に属するすべての整数は法 m に関する零因子である（これらのことを確かめてみよ）． したがって，法 m に関する “可逆”，“逆元”，“零因子” という概念は，どれも法 m に関する剰余類がもっている性質ととらえることができる． 次の定義は，このような考え方によって与えられたものである．

定義 8.1 m を 2 以上の整数とし，$\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ を剰余類とする．

(1) $a \in \alpha$ が法 m に関して可逆であるとき，α は**可逆**であるという．

(2) 整数 b が法 m に関する $a \in \alpha$ の逆元であるとき，b の属する剰余類を α の**逆元**とよぶ．

(3) $a \in \alpha$ が法 m に関する零因子であるとき，α は**零因子**であるという．

剰余類の逆元は，もし存在するならば一意的である． 実際，β, γ がともに α の逆元であるとすると，$\alpha\beta = \alpha\gamma = \overline{1}$ だから，

$$\gamma = \overline{1}\gamma = (\alpha\beta)\gamma = (\beta\alpha)\gamma = \beta(\alpha\gamma) = \beta\overline{1} = \beta.$$

そこで，剰余類 α の逆元を α^{-1} で表す（場合によっては $1/\alpha$ と書くこともある）． たとえば，$7 \cdot 13 = 91 \equiv 1 \pmod{15}$ なので，$\boldsymbol{Z}/15\boldsymbol{Z}$ において $\overline{7}, \overline{13}$ はともに可逆であり互いに逆元，したがって $\overline{7}^{-1} = \overline{13},\ \overline{13}^{-1} = \overline{7}$ と書くことできる．

定義 8.2 m を 2 以上の整数とする． $\boldsymbol{Z}/m\boldsymbol{Z}$ に属する可逆な剰余類全体からなる集合を，**法 m に関する既約剰余類群**といい $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ で表す;

$$(\boldsymbol{Z}/m\boldsymbol{Z})^\times = \{\, \alpha \in \boldsymbol{Z}/m\boldsymbol{Z} \mid \alpha \text{ は可逆} \,\}.$$

この元を，**法 m に関する既約剰余類**ということがある．

定理 5.9 によって，次のように表わすこともできる．

$$\begin{aligned}(\boldsymbol{Z}/m\boldsymbol{Z})^{\times} &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ \gcd(a,m)=1\,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として可逆}\,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として零因子でない}\,\}.\end{aligned}$$

ここで，それぞれの $a\in\boldsymbol{Z}$ は $1\le a<m$ の範囲に限定してもよい．

例 8.3 $\boldsymbol{Z}/10\boldsymbol{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{9}\}$ のうち，可逆な剰余類は $\overline{1},\overline{3},\overline{7},\overline{9}$ であり，零因子は $\overline{0},\overline{2},\overline{4},\overline{5},\overline{6},\overline{8}$ である（どうしてなのか，ちゃんと考えること）． とくに，既約剰余類群は $(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ となる． ここで，$\overline{1},\overline{3},\overline{7},\overline{9}$ のそれぞれの逆元が何かは，すぐに答えられるよね？

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．

これらの性質は $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ が乗法に関して “群” であることを示しているのだが，詳しくは「代数 I」をお楽しみに．

8.2　オイラー関数

定義 8.4 自然数 m に対して，$0\le a<m$ である整数 a のうち m と互いに素なものの個数を $\varphi(m)$ で表す． また，このようにして定まる自然数上の関数 φ を**オイラー関数**という．

すなわち，

$$\varphi(m)=|\{\, a\in\boldsymbol{Z} \mid 0\le a<m,\ \gcd(a,m)=1\,\}|$$

であり，$m\ge 2$ ならば，法 m に関する既約剰余類の個数が $\varphi(m)$ に他ならない;

$$\varphi(m)=\left|(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}\right|.$$

たとえば，$m=10$ のとき，$(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ だから $\varphi(10)=4$． 小さい m に対するオイラー関数の値は次の表のようになる（実は 1 個間違いがある，どれでしょう？ もぉ，先生のいじわるぅ）．

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	10	8	16

次の定理から，どんなに大きな m についても，その素因数分解さえわかればオイラー関数の値 $\varphi(m)$ が簡単に計算できる．

定理 8.5 自然数 m の素因数分解を $m = \prod_{j=1}^{r} p_j^{e_j}$ (p_j は相異り $e_j > 0$) とすると，

$$\varphi(m) = \prod_{j=1}^{r} \left(p_j^{e_j} - p_j^{e_j - 1} \right) = m \prod_{j=1}^{r} \left(1 - \frac{1}{p_j} \right).$$

たとえば，2016 の素因数分解は $2^5 \cdot 3^2 \cdot 7$ だから

$$\varphi(2016) = \varphi(2^5 \cdot 3^2 \cdot 7) = (32 - 16)(9 - 3)(7 - 1) = 576$$

と計算される． この定理は，以下の 2 つの補題から導くことができる（はずだ）．

補題 8.6 素数のべき p^e ($e > 0$) に対して $\varphi(p^e) = p^e - p^{e-1}$.

証明 ある整数が p^e と互いに素っちゅうことは，そいつが p で割り切れないっちゅうことと同じや． そやから，φ の定義を見れば，$0 \leq a < p^e$ をみたす整数 a 全部の個数 p^e から，p の倍数の個数を引けばええんとちゃう？ ほんでもって，p の倍数は $a = jp$, $0 \leq j < p^{e-1}$ で表される p^{e-1} 個で全部やから，$\varphi(p^e) = p^e - p^{e-1}$ が答えっちゅうわけや． □

補題 8.7 互いに素な自然数 m, n に対して $\varphi(mn) = \varphi(m)\varphi(n)$.

証明 まず，m, n は互いに素な整数なので，前章，定理 7.6 より，写像

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

は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 $\varphi(mn) = \varphi(m)\varphi(n)$ となって証明が完了する．
そこで，全射性を示すために，$\xi \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times \times (\boldsymbol{Z}/n\boldsymbol{Z})^\times$ を任意にとって，

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

のように $a, b \in \boldsymbol{Z}$ で表しておく． 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（ここんとこ,「中国の剰余定理」を使ってもよい）． このとき，$\gcd(x, mn) = 1$ が成り立つ． なぜなら，もし $\gcd(x, mn) > 1$ ならば，$\gcd(x, m) > 1$, $\gcd(x, n) > 1$ の少なくとも一方が成り立つ． ところが，$x \equiv a \pmod{m}$ より，前者の場合 $\gcd(a, m) > 1$（ユークリッドの互除法を思い出せ）となって a の取り方に矛盾，後者の場合

も同様に矛盾するから，$\gcd(x, mn) = 1$ が確かめられた．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． □

さて，上の証明もそのアイデアの出所であった定理 7.6 の証明も，一見，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あるときに，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 7.6 の証明では，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．

8.3　剰余環の分解再論

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，通常の演算規則が成り立っている．

いま，整数 m, n に対して，剰余環 $\boldsymbol{Z}/m\boldsymbol{Z}$, $\boldsymbol{Z}/n\boldsymbol{Z}$ にはそれぞれ和，積が定義されている（定義 7.4）から，直積 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ にも和や積が自然に定まる．命題 7.5 から，m, n の公倍数 M をとると，写像

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

が定まる．このとき，任意の $\alpha, \beta \in \boldsymbol{Z}/mn\boldsymbol{Z}$ に対して

$$F(\alpha + \beta) = F(\alpha) + F(\beta), \qquad F(\alpha\beta) = F(\alpha)F(\beta)$$

が成り立つ（それぞれの右辺にある和や積が直積集合の上で定められていることに注意して，実際に確かめてみよ）．このような写像を，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．

とくに，m, n が互いに素である場合，$M = mn$ であって，定理 7.6 より F は全単射となる．このことは，「剰余環 $\boldsymbol{Z}/mn\boldsymbol{Z}$ は 2 つの剰余環の直積 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ と演算（和と積）も込めて同じ “構造” である」ことを意味している．定理 7.6 の重要性（また，その言い換えであった**中国の剰余定理**の重要性）もここにある．このことを，

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

と書いて “可換環として同型” であると言ったりするんだけど，詳しくは「代数 I」で勉強しましょ．一方，前節，補題 8.7 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，“和” を考えず “積” だけに着目していることに注意せよ（前者は “可換環としての同型”，後者は “乗法群としての同型” である）．