

## 第8章 既約剰余類群，オイラー関数

### 8.1 剰余群の分解

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

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

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．とくに，第6章の最後に述べたように， $(\mathbb{Z}/m\mathbb{Z}), (\mathbb{Z}/n\mathbb{Z})$  にはそれぞれ和，積が定義されるから，直積  $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$  にも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

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

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 8.1** 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，任意の  $\mathcal{R}, \mathcal{S} \in \mathbb{Z}/mn\mathbb{Z}$  に対して

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

が成り立つ．

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

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

となっている．これらを用いて，注意深く式変形すれば

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

積についても同様である.

この定理をみたとすような写像を, 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, 剰余群  $Z/mnZ$  は2つの剰余群の直積  $(Z/mZ) \times (Z/nZ)$  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,

$$Z/mnZ \cong (Z/mZ) \times (Z/nZ)$$

と書いたりするんだけど, 詳しくは「代数I」で学ぶ.

## 8.2 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  $\mathcal{R} \in Z/mZ$  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  $\bar{s} = S$  の任意の元を逆元として持つ. すなわち  $a \in \mathcal{R}, b \in S$  ならば  $ab \equiv 1 \pmod{m}$ , あるいは  $\mathcal{R}S = \bar{1}$  と書くこともできる(ああ, ややこしい). このようなとき,  $\mathcal{R}$  は可逆であるという. また,  $S$  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である. たとえば,  $Z/10Z$  においては,  $\bar{3} \cdot \bar{7} = \bar{1}$  なので,  $\bar{3}$  は可逆で,  $\bar{3}^{-1} = \bar{7}$  である.

一方, 剰余類  $\mathcal{R} \in Z/mZ$  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  $\mathcal{R} \in Z/mZ$  が零因子であるための必要十分条件は,  $\mathcal{R}S = \bar{0}$  をみたく剰余類  $S \neq \bar{0}$  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 8.2  $m$  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 8.3  $m$  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  $(Z/mZ)^\times$  で表す.

すなわち, 既約剰余類とは,  $\gcd(a, m) = 1$  である  $a \in Z$  によって表される剰余類  $a+mZ$  のことである.

例 8.4  $Z/10Z = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{9}\}$  のうち, 零因子は  $\bar{0}, \bar{2}, \bar{4}, \bar{5}, \bar{6}, \bar{8}$  であり, 逆元をもつ剰余類は  $\bar{1}, \bar{3}, \bar{7}, \bar{9}$  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  $(Z/10Z)^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$  となる. ここで,  $\bar{1}, \bar{3}, \bar{7}, \bar{9}$  のそれぞれの逆元が何かは, すぐに答えられるよね?

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。

これらの性質は  $(\mathbb{Z}/m\mathbb{Z})^\times$  が乗法に関して“群”であることを示しているのだが、これも詳しいことは「代数 I」で。

## 8.3 オイラー関数

**定義 8.5** 自然数  $m$  に対して、 $0 \leq a < m$  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  $\varphi$  をオイラー関数という。

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、先生のいじわるさ）。

|              |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |
|--------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|
| $m$          | 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 |

$m > 1$  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。たとえば、 $m = 10$  のとき、1, 3, 7, 9 の 4 個が 10 と互いに素となることから  $\varphi(10) = 4$  がわかる。次の定理から、 $m$  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 8.6** 自然数  $m$  の素因数分解を  $m = \prod_{j=1}^r p_j^{e_j}$  ( $p_j$  は相異なり  $e_j > 0$ ) とすると、

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

たとえば、 $\varphi(2160) = \varphi(2^4 \cdot 3^3 \cdot 5) = (16 - 8)(27 - 9)(5 - 1) = 576$  と計算される。この定理は次の 2 つの補題から導くことができる（はずだ、キミならば）。はじめの補題の証明は次の節でね…。

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

**補題 8.8** 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च्छうことは、そいつが  $p$  で割り切れないच्छうことと同じや。そやから、 $\varphi$  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च्छ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च्छうわけや。

## 8.4 既約剰余類群の分解

この節では, 補題 8.7 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

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

が全単射であることが重要な根拠となる.

補題 8.7 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  $(\mathbb{Z}/mn\mathbb{Z})^\times$  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. そこで, 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,

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

のような  $a, b \in \mathbb{Z}$  がとれる. さらに,  $F$  は全射であったから,  $F(x + mn\mathbb{Z}) = \xi$  すなわち

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

をみたく  $x \in \mathbb{Z}$  が存在する(ここんこ「中国の剰余定理」っす, よろしくっ). 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(ってホントかよ. 本当に確かめるよ, マジで). 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, 剰余群について“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, 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“乗法群に関する同型”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, 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.