代数学 I 第 3 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

2.1 合同算術 (続き)

n を 2 以上の整数とする．前回，n 元からなる有限集合 $\mathbb{Z}/n\mathbb{Z}$($\mathbb{Z}$ の n を法とする剰余類環と呼ばれる) に二項演算

$$\pm\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a]_n \pm [b]_n := [a \pm b]_n$$
$$\times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a]_n[b]_n := [ab]_n.$$

を定義した．では四則演算の最後の 1 つ “割り算” は $\mathbb{Z}/n\mathbb{Z}$($\mathbb{Z}$ の中で考えられるだろうか？ まず，“$\div\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a/b]_n$” は明らかにダメである．($a/b$ は一般に有理数なので，$[a/b]_n$ という元は $\mathbb{Z}/n\mathbb{Z}$ において定義されない．)

普通の数において，“a で割る” ということは “逆数 a^{-1} を掛ける” ということであった．これにならって，まず $\mathbb{Z}/n\mathbb{Z}$ における “逆数” を考えてみる．まず $a \neq 0$ に対し，逆数 a^{-1} は

$$aa^{-1} = 1$$

を満たす元であった．そこで，次のように考えてみよう．

定義 2.1

- $\mathbb{Z}/n\mathbb{Z}$ における “1” を $[1]_n$ とする．
- $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して，$[a]_n^{-1}$ を
$$[a]_n[a]_n^{-1} = [1]_n \tag{2.1}$$
を満たす $\mathbb{Z}/n\mathbb{Z}$ の元とする．この元を $[a]_n$ の $\times$ に関する**逆元**という．

例 1 ((2.1) を満たす元の例)**.** $\mathbb{Z}/7\mathbb{Z}$ において，

$$[4]_7[2]_7 = [8]_7 = [1]_7$$

となるので，$[4]_7^{-1} = [2]_7$ である．$\mathbb{Z}/12\mathbb{Z}$ において，

$$[5]_{12}[5]_{12} = [25]_{12} = [1]_{12}$$

となるので，$[5]_{12}^{-1} = [5]_{12}$ である．

“1” を $[1]_n$ とするのはいかにも自然だが，もう少しちゃんとした理由を，次回群の定義を説明する際に説明する．実際にこれは “1” の満たして欲しい以下の性質を満たしている．

$$[1]_n[a]_n = [a]_n = [a]_n[1]_n$$

また，条件 (2.1) によって $[a]_n^{-1}$ が確かにただ 1 つに定まることが，以下の補題からわかる．

補題 2.2

$[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して，条件 (2.1) を満たす元は高々 1 つである．

* *e-mail*：hoya@shibaura-it.ac.jp

証明. $[b]_n$ と $[b']_n$ が共に $[a]_n^{-1}$ の条件 (2.1) を満たすとする．つまり，

$$[a]_n[b]_n = [1]_n = [a]_n[b']_n$$

とする．このとき，

$$[b]_n = [1]_n[b]_n = ([a]_n[b']_n)[b]_n = [abb']_n = ([a]_n[b]_n)[b']_n = [1]_n[b']_n = [b']_n.$$

□

さて，$\mathbb{C}$ において 0^{-1} が存在しなかったように，$\mathbb{Z}/n\mathbb{Z}$ においても $\times$ に関する逆元がいつも存在するとは限らない．そこで，以下のように定義する：

定義 2.3

$$(\mathbb{Z}/n\mathbb{Z})^\times \coloneqq \{[a]_n \mid [a]_n^{-1}\text{が存在}\} = \{[a]_n \mid \text{ある } b \in \mathbb{Z} \text{ が存在して，} [a]_n[b]_n = [1]_n\}.$$ [*1]

命題 2.4

(1) $(\mathbb{Z}/n\mathbb{Z})^\times$ は演算 $\times$ で閉じている．

(2) $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である．

証明. (1) $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n[b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であること，つまり $[a]_n[b]_n$ に $\times$ に関する逆元が存在することを示せばよい．いま，$[a]_n^{-1}, [b]_n^{-1} \in \mathbb{Z}/n\mathbb{Z}$ は存在するので，

$$([a]_n[b]_n)([b]_n^{-1}[a]_n^{-1}) = [a]_n([b]_n[b]_n^{-1})[a]_n^{-1} = [a]_n[1]_n[a]_n^{-1} = [a]_n[a]_n^{-1} = [1]_n.$$

よって，$[b]_n^{-1}[a]_n^{-1}$ が $[a]_n[b]_n$ の $\times$ に関する逆元となる． □

(2) $\mathbb{Z}/n\mathbb{Z}$ においては $[a]_n[b]_n = [b]_n[a]_n$ が成立するので，$[a]_n[a]_n^{-1} = [1]_n$ のとき，$[a]_n^{-1}[a]_n = [1]_n$．よって，$[a]_n^{-1}$ の $\times$ に関する逆元は $[a]_n$ であり，特に $[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である． □

集合 $(\mathbb{Z}/n\mathbb{Z})^\times$ に二項演算 $\times\colon (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ を考えたもの $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ を $\mathbb{Z}/n\mathbb{Z}$ の**乗法群**という．$(\mathbb{Z}/n\mathbb{Z})^\times$ には，"割り算"

$$\div\colon (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times, ([a]_n, [b]_n) \mapsto [a]_n[b]_n^{-1}$$

も定義できる．なお，$[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n[b]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ となることは，命題 2.4 (2) より $[a]_n, [b]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ であることから，命題 2.4 (1) よりわかる．

$(\mathbb{Z}/n\mathbb{Z})^\times$ の元の具体的表示：

さて，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ においては，0 以外のすべての元が $\times$ に関する逆元を持っていたが，$\mathbb{Z}/n\mathbb{Z}$ はどうだろうか．$(\mathbb{Z}/n\mathbb{Z})^\times$ に含まれる具体的な元について考えてみよう．これは次の同値関係をたどっていくとわかる．

$$\begin{aligned}[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \text{ある } x \in \mathbb{Z} \text{ が存在して，} [ax]_n (= [a]_n[x]_n) = [1]_n \\ &\Leftrightarrow \text{ある } x, y \in \mathbb{Z} \text{ が存在して，} ax + ny = 1 \\ &\Leftrightarrow a \text{ と } n \text{ は互いに素. (第 1, 2 回講義資料, 系 1.5)}\end{aligned}$$

これより，以下がわかる：

命題 2.5

$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}.$[*2]

上の同値関係で結んだ部分の考え方に基づけば，$(\mathbb{Z}/n\mathbb{Z})^\times$ における各元の $\times$ に関する逆元は次のように求められることがわかる：

[*1] $\mathbb{X} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ に対し，$\mathbb{X}^\times \coloneqq \mathbb{X} \setminus \{0\}$ も $\mathbb{X}$ の中で $\times$ に関する逆元を持つものの集まりとなっていたことに注意しよう，

[*2] 負の数に対応する gcd については，補足プリント "拡張ユークリッド互除法について" を参照のこと．

$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，

$$ax + ny = 1$$

を満たす整数の組 (x, y) を見つければ，$[x]_n$ が $[a]_n$ の $\times$ に関する逆元である．このような (x, y) は拡張ユークリッド互除法で見つけることができる．(第 1, 2 回講義資料参照)

例 2. 以下の問題を考えてみよう．

$(\mathbb{Z}/60\mathbb{Z})^\times$ において，$[17]_{60}$ の $\times$ に関する逆元を求めよ．

なお，$\gcd(17, 60) = 1$ なので，$[17]_{60}$ は確かに $(\mathbb{Z}/n\mathbb{Z})^\times$ の元である．(命題 2.4)

解答. $17x + 60y = 1$ を満たす整数の組 (x, y) を拡張ユークリッド互除法で求める：

$$60 = 3 \times 17 + 9 \qquad 17 = 1 \times 9 + 8$$
$$9 = 1 \times 8 + 1 \qquad 8 = 8 \times 1 + 0$$

であるので，

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 + (-1) \times (17 - 1 \times 9) \\ &= (-1) \times 17 + 2 \times 9 \\ &= (-1) \times 17 + 2 \times (60 - 3 \times 17) \\ &= (-7) \times 17 + 2 \times 60 \end{aligned}$$

より，$(x, y) = (-7, 2)$ が $17x + 60y = 1$ を満たす整数の組の例である．よって，求める逆元は $[-7]_{60} = [53]_{60}$．
□

検算してみると，確かに $[17]_{60}[-7]_{60} = [-119]_{60} = [1]_{60}$ となっている．

定義 2.6

正の整数 n に対し，n と互いに素な 1 以上 n 以下の自然数の個数を $\varphi(n)$ と書く．つまり，

$$\varphi(n) \coloneqq \#\{m \in \mathbb{N} \mid 1 \leq m \leq n, \gcd(m, n) = 1\}^{*3}$$

とする．n に対して $\varphi(n)$ を与える関数 $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}, n \mapsto \varphi(n)$ を**オイラー (Euler) の φ 関数**という．

例 3.

$$\varphi(1) = 1 \qquad \varphi(2) = 1 \qquad \varphi(3) = 2 \qquad \varphi(4) = 2 \qquad \varphi(5) = 4 \qquad \varphi(6) = 2$$

特に，p が素数のとき，$1, \ldots, p-1$ は全て p と互いに素なので，$\varphi(p) = p - 1$ である．逆に $\varphi(n) = n - 1$ となるとき，n は素数である．

命題 2.5 より，以下のことは直ちにわかる．

命題 2.7

$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$.

命題 2.7 と例 3 での考察から，

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = n - 1 \Leftrightarrow n \text{ は素数}$$

*3 $\#(\ldots)$ は "集合 $(\ldots)$ の元の個数" を表す記号である．

であることがわかる．ここで (2.1) を思い出すと，$[0]_n$ は明らかに $\times$ に関する逆元を持たないので，$\#(\mathbb{Z}/n\mathbb{Z})^\times = n-1$ は，

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\}$$

と同値である．つまり，

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]_n\} \Leftrightarrow n \text{ が素数}. \tag{2.2}$$

となる．“$[0]_n$ 以外のすべての元が $\times$ に関する逆元を持つ” というのは，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等と似た性質である．実際にこういった代数系の抽象化は**体**と呼ばれるもので，本講義では体論は扱わないが，以下のように言うこともできる．

$$\mathbb{Z}/n\mathbb{Z} \text{ が体である} \Leftrightarrow n \text{ が素数}.$$

$\mathbb{Z}/p\mathbb{Z}$ (p は素数) という形の体は，有限個の元からなる体ということで，**有限体**と呼ばれるものの例となる．

<u>応用例：フェルマーの小定理 (続)</u> 前回扱ったフェルマーの小定理にもう一つ主張を付け足したものをここで述べておこう．実際にはこの追加された主張をフェルマーの小定理と呼ぶことが多い．

定理 2.8 (フェルマーの小定理, Fermat’s little theorem)

p を素数する．このとき，任意の $a \in \mathbb{Z}$ に対し，

$$[a^p]_p = [a]_p.$$

となる．さらに，a が p の倍数でないとき，

$$[a^{p-1}]_p = [1]_p. \tag{2.3}$$

証明. $[a^p]_p = [a]_p$ は第 1, 2 回講義資料の定理 1.2 の言い換えである．[*4]よって，式 (2.3) を示す．a が p の倍数でないとき，$[a]_p \neq [0]_p$ である．いま p は素数なので，このとき (2.2) より $[a]_p^{-1}$ が存在する．$[a]_p^{-1}$ を $[a^p]_p = [a]_p$ の両辺に掛けると，

$$[a^{p-1}]_p = [1]_p$$

を得る． □

実は，(2.3) は以下のような形で p が素数でない場合についても一般化される：

定理 2.9 (オイラーの定理, Euler’s theorem)

n が正の整数，$a \in \mathbb{Z}$, $\gcd(a, n) = 1$ のとき，

$$[a^{\varphi(n)}]_n = [1]_n.$$

この定理の証明は，もう少し群論の勉強を進めてから行う．群論の一般論によって実はこの定理は容易に示される (お楽しみに！)．なお，オイラーの定理で，n を素数とすると，a が n の倍数でさえなければ $\gcd(a, n) = 1$ となり，しかも $\varphi(n) = n-1$ となるので，確かにこの定理はフェルマーの小定理を含んでいる．

[*4] 正確には前回は a が負の場合は証明をしていないが，この主張は成立する．確かめてみよ．