サイエンスセミナー (数理科学の世界３)

＜２００４年４月３０日＞

担当：数理科学科 原田 昌晃

1　$\mathbb{Z}$ から $\mathbb{Z}_k$ へ

集合と整数全体 $\mathbb{Z}$

ある条件を満たす (数学的な) ものの集まりを集合とよぶ. 集合を作っているものを元とよぶ. A を集合とするとき x が A の元であるとき $x \in A$, x が A の元でないとき $x \notin A$ と表す. 集合を表すとき, 元を列挙して $\{\quad\}$ で囲むことによって表す.

例 整数全体の集合をここでは $\mathbb{Z}$ と表すことにすると

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \dots\}$$

となる.

$a, b \in \mathbb{Z}$ とすると

$$a + b \in \mathbb{Z},\ a \cdot b \in \mathbb{Z},\ a - b \in \mathbb{Z}$$

を満たす. このとき集合 $\mathbb{Z}$ はそれぞれの演算 $+, \cdot, -$ で閉じているとよぶ.

$\mathbb{Z}_k$ と k を法とする計算

k を 2 以上の自然数として

$$\mathbb{Z}_k = \{0, 1, 2, 3, \dots, k-1\}$$

とする.

$x, y \in \mathbb{Z}_k$ に対して, 新しい演算を

$$x \oplus y : x + y \text{ を } k \text{ で割った余り}$$
$$x \otimes y : x \cdot y \text{ を } k \text{ で割った余り}$$

で定義する. また $\ominus x$ を $k - x$ と定義. これを k **を法とする計算**とよぶ. 余りは 0 から $k-1$ の間の値になるので, $\mathbb{Z}_k$ はこれらの演算で閉じていることが分かる.

例 $k = 7$ とする. $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ となる. 次を計算せよ：

$1 \oplus 3 =$	$4 \oplus 5 =$	$5 \oplus 6 =$
$2 \otimes 3 =$	$3 \otimes 3 =$	$4 \otimes 5 =$
$\ominus 3 =$	$2 \ominus 5 =$	

2　ベクトルの内積

n 個の $\mathbb{Z}_k$ の元 $x_1, x_2, \ldots, x_n$ を順序付けて並べた組 $(x_1, x_2, \ldots, x_n)$ をベクトルとよび, このベクトル全体の集合を $\mathbb{Z}_k^n$ と表すことにする.

注意　既に $\mathbb{Z}_k$ において新しい演算 $\oplus, \otimes, \ominus$ を定義したが, 混乱のない限り, 通常の和, 積, 差の記号を用いることにする.

$\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_k^n$ に対して

$$\mathbf{x} \cdot \mathbf{y} = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_n \cdot y_n$$

を $\mathbf{x}$ と $\mathbf{y}$ の**内積**とよぶ. ここで, 内積の値は $\mathbb{Z}_k$ の元だと考える.

例 $\mathbf{x} = (1, 0, 3, 4, 5), \mathbf{y} = (2, 3, 1, 2, 4) \in \mathbb{Z}_6^5$ とすると

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \\ &= \end{aligned}$$

$\mathbf{x} \cdot \mathbf{y} = 0$ のとき $\mathbf{x}$ と $\mathbf{y}$ は**直交**しているとよぶ.

3　国際標準図書番号 (ISBN)

ほとんどの本には、裏表紙あたりに国際標準図書番号 (International Standard Book Number, ISBN) が書かれている. ISBN は世界中で一つの本に一つだけ割り振られている１０桁の番号である. では, この ISBN がどのような性質を持っているかを調べよう.

まず１０桁の ISBN をベクトルだと思って $\mathbf{x} = (x_1, x_2, x_3, \ldots, x_{10})$ とおく. ただし, 最後の一桁が X という記号の場合は $x_{10} = 10$ だと考えることにする. $\mathbf{y} = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ として, ここでは, どちらのベクトルも $\mathbb{Z}_{11}^{10}$ の元だと考える.

性質 1. $\mathbf{x}$ と $\mathbf{y}$ は直交する.

例 線形代数入門, 内田他著 (裳華房) の ISBN は

$$4\text{-}7853\text{-}1053\text{-}7$$

となっている. $\mathbf{x} = (4, 7, 8, 5, 3, 1, 0, 5, 3, 7)$ なので

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= 4 \cdot 1 + 7 \cdot 2 + 8 \cdot 3 + 5 \cdot 4 + 3 \cdot 5 + 1 \cdot 6 \\ &\qquad + 0 \cdot 7 + 5 \cdot 8 + 3 \cdot 9 + 7 \cdot 10 \\ &= 220 = 0 \end{aligned}$$

少し ISBN 自体の説明もしておこう. 最初の 4 は日本を表し, 次の 7853 は出版社である裳華房を意味する. 次の 1053 はこの本に与えられた番号になる. 最後の一桁はチェックのために設けられている.

定理 2. ISBN は一つ間違えた場合は間違えたことが認識される.

(証明) 本質的には同じなので, 上の例で考えてみることにする. 4-7853-1053-7 の２桁目の「7」が a であった場合, 内積の値は次のように変わる：

a	0	1	2	3	4	5	6	8	9	10
$\mathbf{x}\cdot\mathbf{y}$	8	10	1	3	5	7	9	2	4	6

したがって 7 以外の数であれば内積の値が 0 にならないので, 性質 1 を満たさないことから間違っていることが分かる. □

4　バーコード (JAN 規格)

次の応用例としてバーコードがどのようになっているか説明する. バーコードには幾つかの種類があるが, ここでは JAN (Japanese Article Number) 規格のバーコードについて解説する.

JAN 規格のバーコードは, いろいろな商品のパッケージに印刷されているので, 日常の生活の中で目にする機会も多いはずです. このバーコードは１３桁の数からなるのでこの１３桁の数をベクトルだと思って $\mathbf{x} = (x_1, x_2, x_3, \dots, x_{13})$ とおき, 今回は $\mathbb{Z}_{10}^{13}$ の元だと考える. また $\mathbf{y} = (1,3,1,3,1,3,1,3,1,3,1,3,1)$ とする.

性質 3. $\mathbf{x}$ と $\mathbf{y}$ は直交する.

例 Mr.Children の新譜「シフクノオト」のバーコードは

4 9 8 8 0 6 1 8 6 1 6 1 6

となっている.

$$\begin{aligned}\mathbf{x}\cdot\mathbf{y} &= 4\cdot1+9\cdot3+8\cdot1+8\cdot3+0\cdot1+6\cdot3\\ &\qquad +1\cdot1+8\cdot3+6\cdot1+1\cdot3+6\cdot1+1\cdot3+6\cdot1\\ &= 130 = 0\end{aligned}$$

ISBN のときと同様に JAN 規格のバーコードについて簡単に説明する. まず, 最初の２桁は必ず 45 か 49 で日本を意味する. 次の５桁がメーカーを表し次の５桁が商品を示し, 最後の１桁がチェック用の数になる. 上の例では 88061 が CD の発売元であるトイズファクトリーを表し, 86161 がこの CD を表している (確かにこの CD には TFCC-86161 という番号が書かれてある).

定理 2 と同様に次が成り立つ.

定理 4. バーコードは読み取りの際に, 一つ間違えた場合は間違えたことが認識される.

5　補足 (合同式と曜日の計算)

$m, n \in \mathbb{Z}$ に対して $m - n$ がある整数 k の倍数であるとき, m, n は k **を法として合同**であるといい

$$m \equiv n \pmod{k}$$

と表す. 言い換えれば m を k で割った余りと n を k で割った余りが一致する場合に m, n が k を法として合同になる.

この関係 $\equiv$ は k を法とする合同式とよばれる. 既に定義した k を法とする計算と合同式の次の関係は明らかである：

(1) $x \oplus y \equiv x + y \pmod{k}$

(2) $x \otimes y \equiv x \cdot y \pmod{k}$

(3) $x \ominus y \equiv x - y \pmod{k}$

合同式については次が成り立つ.

定理 5. $a \equiv b \pmod{k}$ かつ $c \equiv d \pmod{k}$ であれば

(1) $a + c \equiv b + d \pmod{k}$

(2) $a - c \equiv b - d \pmod{k}$

(3) $a \cdot c \equiv b \cdot d \pmod{k}$

が成り立つ.

上の定理を用いることで

$$365a + b \equiv a + b \pmod{7}$$

が成り立つことが分かる. なぜならば $365 - 1 = 364 = 7 \cdot 52$ より $365 \equiv 1 \pmod{7}$ となるので両辺に a を掛けて b を加えればよい.

例 上の式は曜日の計算に便利である. 例えば 2004 年 1 月 1 日は木曜日であったが 2024 年 1 月 1 日の曜日を求めてみる. 2004, 2008, 2012, 2016, 2020 年がうるう年であることを考慮して

$$365 \cdot 20 + 5 \equiv 20 + 5 \equiv 4 \pmod{7}$$

であることより 2024 年 1 月 1 日の曜日は 2004 年 1 月 1 日の 4 日後の曜日と同じになるので, 月曜日となる.

サイエンスセミナー 小テスト

学科名：　　学籍番号：

氏名：

1 身の回りにある書籍名 (雑誌を除く) とその ISBN または商品名とバーコードを書き, 書籍の ISBN が性質 1 を満たすこと, または商品のバーコードが性質 3 を満たすことを確認せよ.

2 バーコードにおいて２桁目の読み取りに失敗した場合に間違いが発見されることを確認せよ.

時間があればこの授業についての感想を裏面に書いて下さい.