代数入門演習　NO. 7　　2014. 11.11

# 7　資料 1: 剰余類のなす集合

**このプリントは, 2011 年度「代数入門演習」担当 藤田玄さんの作成資料です. とても読みやすいので配布します.**

## 7.1　剰余類とその「和」「積」

整数を 4 で割ることを考えます. そのあまりが 0 から 3 までの整数となることに注目すると, 整数は次の 4 つのタイプに分類されます.

(0) 4 で割ってあまり 0 の数

(1) 4 で割ってあまり 1 の数

(2) 4 で割ってあまり 2 の数

(3) 4 で割ってあまり 3 の数

(0) から (3) までのタイプの数がなす集合は通常

$$4\mathbb{Z}, \quad 1+4\mathbb{Z}, \quad 2+4\mathbb{Z}, \quad 3+4\mathbb{Z}$$

と書かれます. つまり,

$$4\mathbb{Z} = \{4x \mid x \in \mathbb{Z}\},\ 1+4\mathbb{Z} = \{1+4x \mid x \in \mathbb{Z}\},\ \text{etc.}$$

です. これらを**法 4 に関する剰余類 (または合同類)** といいます. 記号が重いのでここからは剰余類を

$$4\mathbb{Z} = \bar{0},\ 1+4\mathbb{Z} = \bar{1},\ \text{etc.}$$

と書くことにしましょう. 法 4 に関する剰余類を集めた集合を $\mathbb{Z}/4\mathbb{Z}$ と書き, **法 4 に関する剰余類の集合**とよびます[1]. つまり,

$$\mathbb{Z}/4\mathbb{Z} = \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3}\}$$

です. $\bar{0}$ や $\bar{1}$ は数ではなく, ある性質をもつ数の集合であることに注意して下さい. 唐突ですが次の計算規則で $\mathbb{Z}/4\mathbb{Z}$ の中で「和 $+$」と「積 $\times$」を “定義 ” します.

**規則 : 普通の数と同じように和や積を計算して 4 を超えたら超えた分を差っぴく.**

例えば $\bar{3}+\bar{1}=\bar{0}$ ($3+1$ は 4 だから 4 を差っぴいて 0), $\bar{2}\times\bar{3}=\bar{2}$ ($2\times3$ は 6 だから 4 を差っぴいて 2) です. また, この演算は明らかに可換な演算です. この計算規則によって次の演算表を作ることができます.

| $+$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| $\times$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

[1] 文脈によっては剰余群や剰余環ともいいます. どうして $\mathbb{Z}/4\mathbb{Z}$ と書くかは深い理由があるのですが, それについてはまた後日 ···

普通の数の和や積と同様に, $\bar{0}$ は和に関する単位元, $\bar{1}$ は積に関する単位元になっていますね. この計算規則は結合律 $(a+b)+c=a+(b+c)$, $(ab)c=a(bc)$ をみたすことも確かめられます[2]. 例えば,

$$(\bar{1}+\bar{2})+\bar{3}=\bar{3}+\bar{3}=\bar{2},\quad \bar{1}+(\bar{2}+\bar{3})=\bar{1}+\bar{1}=\bar{2}$$

とか

$$(\bar{2}\times\bar{3})\times\bar{3}=\bar{2}\times\bar{3}=\bar{2},\quad \bar{2}\times(\bar{3}\times\bar{3})=\bar{2}\times\bar{1}=\bar{2}$$

です. さらに, 分配法則も成り立ちます. 例えば,

$$\bar{3}\times(\bar{1}+\bar{2})=\bar{3}\times\bar{3}=\bar{1},\quad \bar{3}\times\bar{1}+\bar{3}\times 2=\bar{3}+\bar{2}=\bar{1}$$

です.

## 7.2 合同式との関係

さて, このようにして $\mathbb{Z}/4\mathbb{Z}$ にちょっと変わった「和」と「積」を定義したわけですが,「$\bar{1}+\bar{3}=\bar{0}$ とかまた意味わからんこと言ってんな」と文句の一つでもつけたくなるかもしれません. しかし, $\bar{1}$=「4 で割って 1 余る数の全体」であったことを思い出すと, $\bar{1}+\bar{3}=\bar{0}$ とは

**「4 で割って 1 余る数」と「4 で割って 3 余る数」の和は「4 で割って 0 余る数」**

という事実を数式で表したものと考えることもできます. 他の計算もそのように解釈できます. 例えば $\bar{2}\times\bar{3}=\bar{2}$ は

**「4 で割って 2 余る数」と「4 で割って 3 余る数」の積は「4 で割って 2 余る数」**

ということです. また, ここで定義した「和」と「積」は 4 を法とした合同式の計算と非常に似ています. 例えば合同式では

$$1+3=4\equiv 0 \bmod 4,\quad 2\cdot 3=6\equiv 2 \bmod 4$$

という計算があります. 実際, ここで定義した $\mathbb{Z}/4\mathbb{Z}$ での計算は**同値関係**と**剰余群 (環)** という概念を通して合同式の計算そのものであるということがわかります. 詳しいことは代数まで待つことにして, とりあえずしばらくは

**剰余類の計算とは合同式の計算である**

と理解しておいて下さい.

## 7.3 一般の剰余類の集合 $\mathbb{Z}/m\mathbb{Z}$

これまで 4 で割ることを考えてきましたが, 一般に自然数 $m$ による割り算を考えることで法 $m$ に関する剰余類の集合 $\mathbb{Z}/m\mathbb{Z}=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$ が定義されます. ここでは $m$ による割り算を考えているので

$$\bar{a}=a+m\mathbb{Z}=\{a+mx\mid x\in\mathbb{Z}\}$$

です[3]. この $\mathbb{Z}/m\mathbb{Z}$ においても $\mathbb{Z}/4\mathbb{Z}$ のときと同様の計算規則 **“$m$ を超えたら差っぴく ”** で $+$ と $\times$ を定義することができます.

[2] とサラッと書きましたが, $a,b,c$ の全ての組み合わせで成り立つことを直接確かめようとすると, その組み合わせはたくさん出てきて大変です. そういうのを涼しい顔で証明するための一般論は来年の代数で教えてもらえるでしょう.

[3] この $\bar{a}$ という記号は便利なのですが, $m$ がなんなのかはっきりしないので使うときは注意が必要です. $\bar{a}=[a]_m$ **と書く人もいます.**

### 7.4　剰余類の「差」「商」

剰余類の集合 $\mathbb{Z}/m\mathbb{Z}$ で剰余類の和と積ができることがわかったので, 次に「差」と「商」も考えてみましょう. 「差」とは「和に関する逆元」を足す操作です. 「和に関する逆元」とは「足して $\bar{0}$ になる相方」のことです. 再び話を $\mathbb{Z}/4\mathbb{Z}$ に戻して, 演算表をもとに相方探しをすると次のようになります.

(0) $\bar{0}$ の和に関する逆元は $\bar{0}$ (つまり $-\bar{0} = \bar{0}$).

(1) $\bar{1}$ の和に関する逆元は $\bar{3}$ (つまり $-\bar{1} = \bar{3}$).

(2) $\bar{2}$ の和に関する逆元は $\bar{2}$ (つまり $-\bar{2} = \bar{2}$).

(3) $\bar{3}$ の和に関する逆元は $\bar{1}$ (つまり $-\bar{3} = \bar{1}$).

これで「差」も好きなようにできます. では「商」はどうでしょうか? 「商」とは「積に関する逆元」をかける操作です. 「積に関する逆元」とは「かけて $\bar{1}$ になる相方」のことです. 演算表をもとに相方探しをすると次のようになります.

(0) $\bar{0}$ の積に関する逆元は存在しない.

(1) $\bar{1}$ の積に関する逆元は $\bar{1}$ (つまり $\bar{1}^{-1} = \bar{1}$).

(2) $\bar{2}$ の積に関する逆元は存在しない.

(3) $\bar{3}$ の積に関する逆元は $\bar{3}$ (つまり $\bar{3}^{-1} = \bar{3}$).

$\bar{0}^{-1}$ はあきらめるとしても, $\bar{2}^{-1}$ が存在しないということから, **商は自由にできるわけではない**ということがわかりました. これらをまとめると,

**$\mathbb{Z}/4\mathbb{Z}$ において結合律と分配法則をみたす「和」「積」が定義され, 「差」も自由にできる.**

ということになります[4]. いま見たように「商」に関しては注意が必要となります.

### 7.5　いつ「商」ができるか?

では剰余類の集合においていつ「商」ができるか, つまり, どんな剰余類に対して積に関する逆元が存在するか考えてみましょう. 例えば,「$\mathbb{Z}/4\mathbb{Z}$ において $\bar{3}^{-1}$ はあるのに $\bar{2}^{-1}$ がないのは何故か」ですが, それは 2 と 4 の関係と 3 と 4 の関係にある違いがあるからです. まずは自分で考えてみてほしいのですが, 答えは**互いに素かどうか**ということです. 一般に次が成り立ちます.

**命題 7.1.** 剰余類の集合 $\mathbb{Z}/m\mathbb{Z}$ の剰余類 $\bar{a} = a + m\mathbb{Z}$ の積に関する逆元 $\bar{a}^{-1}$ が存在するための必要十分条件は $\gcd(a, m) = 1$ である.

剰余類 $\bar{b}$ が $\bar{a}$ の積に関する逆元であるとは

$$\bar{a} \times \bar{b} = \bar{b} \times \bar{a} = \bar{1}$$

となることでした. それをふまえると, 合同式の計算で命題 7.1 に対応するものはすでに習った次の命題となります.

**命題 7.2.** $a \in \mathbb{Z}$ に対して

$$ab \equiv ba \equiv 1 \bmod m$$

となる $b \in \mathbb{Z}$ が存在するための必要十分条件は $\gcd(a, m) = 1$ である.

[4] 一言でいうと $\mathbb{Z}/4\mathbb{Z}$ は**可換環**になる, ということです.

命題 7.1 と命題 7.2 を比べると, 「剰余類の逆元とは $m$ を法とした逆元で, $\bar{a}^{-1} = \bar{b}$ である」ということがわかります. 一般に, 逆元が存在する剰余類を**既約剰余類 (または可逆類)** といいます[5]. 既約剰余類全体のなす集合を $(\mathbb{Z}/m\mathbb{Z})^\times$ と表し, $\mathbb{Z}/m\mathbb{Z}$ の**単数群**といいます. 例えば $\mathbb{Z}/4\mathbb{Z}$ の既約剰余類は $\bar{1}$ と $\bar{3}$ なので $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ です. 剰余類 $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ に対して, $\bar{a}^n = \bar{1}$ をみたす自然数 $n$ が存在するとき, そのような自然数で最小のものを $\bar{a}$ の位数といいます. $\mathbb{Z}/4\mathbb{Z}$ において, $\bar{3} \neq \bar{1}$ かつ $\bar{3}^2 = \bar{1}$ より $\bar{3}$ の位数は 2 です.

## 7.6 問題編

**問題 7.1.** 次の問に答えよ.
(1) $\bar{3} \in \mathbb{Z}/13\mathbb{Z}$ の位数を求めよ.
(2) $\bar{2} \in \mathbb{Z}/13\mathbb{Z}$ について, $\bar{2}^n = \overline{11}$ となる最小の自然数 $n$ を求めよ.
(3) $\bar{2} \in \mathbb{Z}/13\mathbb{Z}$ の位数を求めよ.
(4) $\bar{3} \in \mathbb{Z}/13\mathbb{Z}$ について, $\bar{3}^n = \overline{11}$ となる自然数 $n$ は存在しないことを示せ.

[5] 分数 $\frac{a}{m}$ が既約分数になる, ということです.