平成 16 年度広島大学公開講座「数学の基礎と展望 – 数学の万華鏡 –」

# 数のひとつの拡張

## — 合同方程式の極限として方程式 $x^2+1=0$ を解く —

広島大学大学院理学研究科　都築 暢夫

小学校での算数から高等学校での数学の中で、数の範囲は、整数、有理数、実数、複素数と拡張されていきました。整数・有理数から始まる数の拡張は、実数・複素数への拡張だけでなく、それとは異なる拡張「$p$ 進数」もあります。$p$ 進数は、「整数の合同」という考え方をもとにして、その極限として定義されます。この講義では、方程式

$$x^2+1=0$$

を合同方程式とみなして解いていき、その極限として定まる数について解説したいと思います。

### 1. 整数の合同

$n$ を整数とします。整数 $a,b$ に対して

$$a \equiv b \pmod{n} \overset{\text{定義}}{\iff} a-b \text{ は } n \text{ の倍数} \overset{\text{定義}}{\iff} \begin{array}{c}\text{ある整数 } k \text{ が存在して}\\ a-b=kn\end{array}$$

と定めて、

$$\text{「}a \text{ と } b \text{ とは } n \text{ を法として合同」}$$

と言います。定義から

$$a \equiv b \pmod{n} \overset{\text{同値}}{\iff} a \equiv b \pmod{-n}$$

が成り立ちます。

まず、$n$ を法として合同と $n$ で割った余りの関係を見てみましょう。

**命題 1.** $n$ を 0 以上の整数、$a,b$ を整数とする。

(1) $n \neq 0$ とすると、次が成り立つ。

$$a \equiv b \pmod{n} \overset{\text{同値}}{\iff} a \text{ と } b \text{ をそれぞれ } n \text{ で割った余りが同じ}$$

(2) $n=0$ とすると、次が成り立つ。

$$a \equiv b \pmod{0} \overset{\text{同値}}{\iff} a=b$$

証明：(1) $a$ と $b$ をそれぞれ $n$ で割った商を $c$ と $d$、余りを $r$ と $s$ $(0 \leqq r,s<n)$ とする。すると

$$\begin{aligned} a &= cn+r \\ b &= dn+s \end{aligned}$$

となるので、

$$\begin{gathered} a-b=(c-d)n+r-s \\ -n<r-s<n \end{gathered}$$

である。$a \equiv b \pmod{n}$ とすると、$a-b$ は $n$ の倍数なので $r-s$ も $n$ の倍数である。$-n$ より大きく $n$ より小さい $n$ の倍数は 0 だけなので、

$$r = s$$

となる。よって、$a$ と $b$ をそれぞれ $n$ で割った余りは同じである。逆に、$r = s$ とすると $a-b$ は $n$ の倍数になるので、$a \equiv b \pmod{n}$ である。

(2) は明らか。 □

**例.** $a, b$ を整数とする。

(1) $a \equiv b \pmod{1}$

(2) $a \equiv b \pmod{2} \overset{\text{同値}}{\Longleftrightarrow} a$ と $b$ はともに偶数または奇数 □

整数の合同 $\equiv$ は次の定理の性質 (1) – (3) を満たします。数学用語では、「整数の合同関係は同値関係である」と言います。

**定理 1.** 整数 $a, b, c$ に対して、次の (1) - (3) が成り立つ。

(1) $a \equiv a \pmod{n}$

(2) $a \equiv b \pmod{n}$ ならば $b \equiv a \pmod{n}$

(3) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば $a \equiv c \pmod{n}$

証明 : (1) $a - a = 0 = 0 \times n$ なので、$a \equiv a \pmod{n}$ である。

(2) $a \equiv b \pmod{n}$ とすると、ある整数 $k$ が存在して $a - b = kn$ となる。よって、$b - a = -kn = (-k)n$ となるので、$b - a$ は $n$ の倍数となり、$b \equiv a \pmod{n}$ である。

(3) $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ とする。ある整数 $k, l$ が存在して $a - b = kn, b - c = ln$ となる。すると

$$a - c = a - b + b - c = kn + ln = (k + l)n$$

なので、$a - c$ は $n$ の倍数である。したがって、$a \equiv c \pmod{n}$ である。 □

法となる整数 $n$ を動かしてみましょう。

**命題 2.** $m, n, a, b$ を整数とする。このとき次が成り立つ。

$$a \equiv b \pmod{mn} \implies a \equiv b \pmod{n}$$

証明 : $a \equiv b \pmod{mn}$ とすると、ある整数 $k$ に対して $a - b = k(mn) = (km)n$ となる。したがって、$a \equiv b \pmod{n}$ である。 □

## 2. 合同と加法・乗法

**定理 2.** 整数 $n, a, b, c, d$ を $a \equiv b \pmod{n}$ かつ $c \equiv d \pmod{n}$ とすると、次の (1) と (2) が成り立つ。

(1) $a \pm c \equiv b \pm d \pmod{n}$

(2) $ac \equiv bd \pmod{n}$

証明 : (2) のみ証明する。ある整数 $k, l$ に対して、$a - b = kn, c - d = ln$ とおける。すると

$$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d = a(ln) + (kn)d = (al + kd)n$$

なので、$ac \equiv bd \pmod{n}$ である。 □

**例.** 整数の合同における加法・乗法の表を書いてみましょう。

(1) $n = 2$ とする。

$a + b \pmod 2$

| $a\backslash b$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$cd \pmod 2$

| $c\backslash d$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

(2) $n = 5$ とする。

$a + b \pmod 5$

| $a\backslash b$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

$cd \pmod 5$

| $c\backslash d$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

□

法となる整数 $n$ を動かしてみましょう。命題 2 から次の命題が成り立ちます。

**命題 3.** $m, n, a, b, c, d$ を整数とし、次の合同式 $\begin{cases} c \equiv a + b \pmod{mn} \\ d \equiv ab \pmod{mn} \end{cases}$ が成り立つとする。このとき、次の (1) と (2) が成り立つ。

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

(2) $d \equiv ab \pmod{n}$

命題 3 が意味することは、25 を法として計算した加法や乗法

$$12 + 20 \equiv 32 \equiv 7 \pmod{25}$$
$$12 \times 20 \equiv 120 \equiv 20 \pmod{25}$$

は、5 を法としても成り立つということです。すなわち、

$$12 + 20 \equiv 32 \equiv 2 \equiv 7 \pmod{5}$$
$$12 \times 20 \equiv 120 \equiv 0 \equiv 20 \pmod{5}$$

となります。

## 3. 合同類

$n$ を正の整数とします。整数 $a$ に対して、整数全体の集合 $\mathbb{Z}$ の部分集合 $[a]_n$ を

$$[a]_n = \{x \,|\, x \equiv a \,(\mathrm{mod}\, n)\}$$

と定めます。定理 1 (1) から $a \in [a]_n$ です。例えば、$n = 1$ のときはすべての整数 $a$ に対して

$$[a]_1 = \mathbb{Z}$$

となります。また、$n = 2$ のとき次のようになります。

$$[a]_2 = \begin{cases} \{\text{ 奇数全体 }\} & \text{if } a \equiv 1 \,(\mathrm{mod}\, 2) \\ \{\text{ 偶数全体 }\} & \text{if } a \equiv 0 \,(\mathrm{mod}\, 2) \end{cases}$$

**定理 3.** $a, b$ を整数とする。このとき、次の (1) と (2) が成り立つ。

(1) $a \equiv b \,(\mathrm{mod}\, n) \overset{\text{同値}}{\Longleftrightarrow} [a]_n = [b]_n$.

(2) $a \not\equiv b \,(\mathrm{mod}\, n) \overset{\text{同値}}{\Longleftrightarrow} [a]_n \cap [b]_n = \emptyset$.

ただし、$a \not\equiv b \,(\mathrm{mod}\, n)$ は「$a$ と $b$ は $n$ を法として合同でない」ことを意味し、$\emptyset$ は空集合を表す。

証明：証明には定理 1 を用いる。詳しくは省略する。 □

$[a]_n$ のことを $n$ を法とする $a$ の合同類といいます。$a$ のことを合同類 $[a]_n$ の代表元といいます。$a \equiv b \,(\mathrm{mod}\, n)$ ならば $[a]_n = [b]_n$ なので、合同類 $[a]_n$ の代表元として $b$ をとることもできます。定理 3 から

$$\mathbb{Z} = [0]_n \cup [1]_n \cup \cdots \cup [n-1]_n$$

です。特に、右辺のそれぞれは互いに共通部分を持ちません。

さて、集合 $A_n$ を $n$ を法とする合同類全体の集合

$$A_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$$

とします。$A_n$ 上に加法と乗法を

$$\begin{aligned} [a]_n \pm [b]_n &= [a \pm b]_n \\ [a]_n \times [b]_n &= [ab]_n \end{aligned}$$

と定めます。これは合同類の代表元の取り方によらずに定まります。実際、$a \equiv c \,(\mathrm{mod}\, n)$ かつ $b \equiv d \,(\mathrm{mod}\, n)$ とすると、定理 2 と定理 3 から

$$\begin{aligned} [a \pm b]_n &= [c \pm d]_n \\ [ab]_n &= [cd]_n \end{aligned}$$

となります。分配法則

$$([a]_n + [b]_n) \times [c]_n = [a]_n \times [c]_n + [b]_n \times [c]_n$$

が成り立つので、数学用語では「$A_n$ は環になる」といいます。

命題 2 と命題 3 から、整数 $m, n$ に対して、写像

$$\begin{aligned} A_{mn} &\to A_n \\ [a]_{mn} &\mapsto [a]_n \end{aligned}$$

が代表元の取り方によらずに定まり、加法と乗法を保ちます。

## 4. 合同方程式

$n$ を正の整数とします。2 つの整数係数多項式 $f(x), g(x)$ に対して

$$f(x) \equiv g(x) \pmod{n}$$

を、$n$ を法とする合同方程式といいます。

$$f(a) \equiv g(a) \pmod{n}$$

を満たす整数 $a$ のことを、合同方程式の解といいます。定理 2 から、次の命題が成り立ちます。

**命題 4.** $n$ を整数、$f(x)$ を整数係数多項式とする。整数 $a, b$ に対し次が成り立つ。

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$$

特に、合同方程式の解は合同類だけできまる。

命題 4 は、$n$ を法とする合同方程式が $A_n$ 上の方程式ということを意味しています。特に、合同方程式の解は合同類を用いて表せます。この講義では、合同方程式の解を

$$x = [a]_n$$

というふうに表すことにします。解の個数が有限個の方が精神衛生上よいですから。

**例.** 合同方程式の例をあげてみましょう。

(1) 5 を法とする 1 次合同方程式

$$3x \equiv 2 \pmod{5}$$

を考える。2 節の 5 を法とする乗法の表を見ると、5 を法として

$$3 \times 0 \equiv 0,\ 3 \times 1 \equiv 3,\ 3 \times 2 = 6 \equiv 1,\ 3 \times 3 = 9 \equiv 4,\ 3 \times 4 = 12 \equiv 2$$

となるので、

$$x = [4]_5$$

が解になる。

(2) 2 を法とする 2 次合同方程式

$$x^2 + x + 1 \equiv 0 \pmod{2}$$

を考える。2 節の 2 を法とする加法・乗法の表から、2 を法として

$$0^2 + 0 + 1 \equiv 1,\ 1^2 + 1 + 1 = 3 \equiv 1$$

となるので、方程式に整数解は存在しない。言い換えると、$A_2$ 上の方程式 $x^2 + x + 1 = 0$ には $A_2$ の中に解が存在しない。 □

さて、法となる整数 $n$ を動かしてみましょう。命題 3 から次の定理が成り立ちます。

**命題 5.** $m, n$ を整数、$f(x), g(x)$ を整数係数多項式とする。このとき、整数 $a$ に対して次が成り立つ。

$$f(a) \equiv g(a) \pmod{mn} \quad \Rightarrow \quad f(a) \equiv g(a) \pmod{n}$$

$A_{mn}$ 上の方程式に対して $n$ を法とすると $A_n$ 上の方程式が定まります。$A_{mn}$ 上に解 $x = [a]_{mn}$ があれば $x = [a]_n$ は $A_n$ 上の解になります。

**例.** 10 を法とする 1 次合同方程式

$$3x \equiv 7 \pmod{10}$$

は、10 を法として

$$3 \times 0 \equiv 0,\ 3 \times 1 \equiv 3,\ 3 \times 2 \equiv 6,\ 3 \times 3 \equiv 9,\ 3 \times 4 \equiv 2,$$
$$3 \times 5 \equiv 5,\ 3 \times 6 \equiv 8,\ 3 \times 7 \equiv 1,\ 3 \times 8 \equiv 4,\ 3 \times 9 \equiv 7$$

となるので、

$$x = [9]_{10}$$

が解になる。$10 = 2 \times 5$ なので、2 と 5 を法として方程式を見ることができる。

(i) 2 を法とする。$3 \equiv 1 \pmod{2}, 7 \equiv 1 \pmod{2}$ となるので、方程式は 2 を法とすると

$$x \equiv 1 \pmod{2}$$

となる。その解は、

$$x = [1]_2$$

です。

$$9 \equiv 1 \pmod{2}$$

なので、10 を法とする解を法 2 すると、2 を法とする解になる。

(ii) 5 を法とする。$3 \equiv 3 \pmod{5}, 7 \equiv 2 \pmod{5}$ となるので、方程式は 5 を法とすると

$$3x \equiv 2 \pmod{5}$$

となる。前の例 (1) から

$$x = [4]_5$$

が解である。

$$9 \equiv 4 \pmod{5}$$

なので、10 を法とする解を法 5 すると、5 を法とする解になる。

## 5. 合同方程式 $x^2+1 \equiv 0 \pmod{5^r}$ を解く

この節では、整数係数方程式

$$x^2+1=0$$

を、$5, 5^2, 5^3, \cdots$ を法として次々と解いていくことを考えます。

$r=1,2,3\cdots$ とし、合同方程式

$(*)_r$ $$x^2+1 \equiv 0 \pmod{5^r}$$

を考えます。最初の注意として、$x=[a]_{5^r}$ が $(*)_r$ の解ならば

$$x=[-a]_{5^r}=[5^r-a]_{5^r}$$

も解になります。実際、

$$(-a)^2+1=a^2+1 \equiv 0 \pmod{5^r}$$

です。

まず、$r=1,2,3$ のときに合同方程式 $(*)_r$ を解いてみましょう。

◯ $r=1$ のとき：2 節の 5 を法とする乗法の表から、合同方程式 $(*)_1$ の解は

$$x=[2]_5, [3]_5$$

となります。

◯ $r=2$ のとき：下の表から合同方程式 $(*)_2$ の解は

$$x=[7]_{5^2}, [18]_{5^2}$$

となります。$18=5^2-7$ に注意してください。

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^2 \pmod{25}$ | 0 | 1 | 4 | 9 | 16 | 0 | 11 | 24 | 14 | 6 | 0 | 21 | 19 |

◯ $r=3$ のとき：$r=2$ のときと同様に表を書いてみると、合同方程式 $(*)_3$ の解は

$$x=[57]_{5^3}, [68]_{5^3}$$

となります。

ここで気づくことは、

$$\begin{aligned} 57 &= 2+1\times 5+2\times 5^2 \\ 68 &= 3+3\times 5+2\times 5^2 \end{aligned}$$

から、自然な写像の列において

$$\begin{array}{ccccc} A_{5^3} & \to & A_{5^2} & \to & A_5 \\ [57]_{5^3} & \mapsto & [7]_{5^2} & \mapsto & [2]_5 \\ [68]_{5^3} & \mapsto & [18]_{5^2} & \mapsto & [3]_5 \end{array}$$

というように、2 つの系列をなしていることです。この系列は、自然な写像の無限列

$$\cdots \to A_{5^{r+1}} \to A_{5^r} \to \cdots \to A_{5^5} \to A_{5^4} \to A_{5^3} \to A_{5^2} \to A_5$$

へと一意的に延びるのでしょうか。答えはイエスです。それが次の定理です。

**定理 4.** $x=[a]_{5^r}$ を合同方程式 $(*)_r$ の解とする。このとき、合同方程式 $(*)_{r+1}$ の解 $x=[b]_{5^{r+1}}$ で

$$b \equiv a \,(\mathrm{mod}\, 5^r)$$

となるものがただ一つ存在する。特に、合同方程式 $(*)_r$ には異なる 2 つの解が存在する。

証明：求める整数 $b$ が存在すると、$b \equiv a \,(\mathrm{mod}\, 5^r)$ なので、ある整数 $y$ が存在して $b=a+y\times 5^r$ と表せる。よって、$y$ の方程式

$$(a+y\times 5^r)^2+1 \equiv 0 \,(\mathrm{mod}\, 5^{r+1})$$

の解を求めればよい。この合同式を展開すると

$$a^2+2\times 5^r ay+y^2\times 5^{2r}+1 \equiv 0 \,(\mathrm{mod}\, 5^{r+1})$$

となる。$r$ は正の整数なので、$2r \geqq r+1$ となり、$y^2\times 5^{2r} \equiv 0 \,(\mathrm{mod}\, 5^{r+1})$ である。よって、

$$(2a)y\times 5^r \equiv -(a^2+1) \,(\mathrm{mod}\, 5^{r+1})$$

を得る。仮定から $a^2+1 \equiv 0 \,(\mathrm{mod}\, 5^r)$ なので、ある整数 $c$ が存在して

$$a^2+1=c\times 5^r$$

と表せる。これを代入すると、合同方程式は

$$(2ay+c)\times 5^r \equiv 0 \,(\mathrm{mod}\, 5^{r+1})$$

と変形できる。素因数分解の一意性より、この合同方程式は

$$2ay+c \equiv 0 \,(\mathrm{mod}\, 5) \tag{$**$}$$

と同値である。既に求めた $r=1$ に関する合同方程式 $(*)_1$ の解から、

$$a \equiv 2,3 \,(\mathrm{mod}\, 5)$$

となる。いずれにしても $2a \not\equiv 0 \,(\mathrm{mod}\, 5)$ なので、2 節の 5 を法とする乗法の表から、$(**)$ はただ一つの解を持つ。それを $y=[d]_5$ とおき、

$$b=a+d\times 5^r$$

とすると、$x=[b]_{5^{r+1}}$ は合同方程式 $(*)_{r+1}$ の解で、$b \equiv a \,(\mathrm{mod}\, 5^r)$ となる。$(**)$ の解は $y=[d]_5$ のみであるから、条件を満たす $(*)_{r+1}$ の解は $x=[b]_{5^{r+1}}$ だけである。

$r=1$ のとき、合同方程式 $(*)_1$ に異なる 2 つの解があるから、帰納的に合同方程式 $(*)_r$ には異なる 2 つの解が存在することがわかる。 □

合同方程式の解の系列を具体的に求めてみましょう。

$$\alpha = (\cdots \mapsto [\alpha_r]_{5^r} \mapsto \cdots \mapsto [\alpha_3]_{5^3} \mapsto [\alpha_2]_{5^2} \mapsto [\alpha_1]_5)$$

を定理 4 で存在が保証された合同方程式の系列 $(*)_r\,(r = 1, 2, 3, \cdots)$ の解の系列で

$$\alpha_1 = 2$$

となるものとします。$\alpha_1, \cdots, \alpha_r$ が求まっているとします。定理 4 の証明のキーポイントは、

$$2a \not\equiv 0 \,(\mathrm{mod}\, 5)$$

が $y$ の方程式 $(**)$ の解の存在を保証するということです。今の場合は、

$$2\alpha_r \equiv 2\alpha_1 \equiv 2 \times 2 \equiv 4 \not\equiv 0 \,(\mathrm{mod}\, 5)$$

です。$y$ を求める合同方程式は

$$4y \equiv -\frac{\alpha_r^2 + 1}{5^r} \,(\mathrm{mod}\, 5)$$

となります。ここで、右辺の分数は実際には整数です。$4 \equiv -1 \,(\mathrm{mod}\, 5)$ となることに気をつけると、

$$y = [\frac{\alpha_r^2 + 1}{5^r}]_5$$

ということになります。したがって、

$$\alpha_{r+1} \equiv \alpha_r + y \times 5^r \equiv \alpha_r + \frac{\alpha_r^2 + 1}{5^r} \times 5^r \equiv \alpha_r + \alpha_r^2 + 1 \,(\mathrm{mod}\, 5^{r+1})$$

となります。これを計算して、

$$\begin{aligned}\alpha = (\quad \cdots &\mapsto [123327057]_{5^{12}} \mapsto [25670807]_{5^{11}} \mapsto [6139557]_{5^{10}} \mapsto [280182]_{5^9} \mapsto [280182]_{5^8} \\ &\mapsto [45807]_{5^7} \mapsto [14557]_{5^6} \mapsto [2057]_{5^5} \mapsto [182]_{5^4} \mapsto [57]_{5^3} \mapsto [7]_{5^2} \mapsto [2]_5)\end{aligned}$$

となります。

同様に

$$\beta = (\cdots \mapsto [\beta_r]_{5^r} \mapsto \cdots \mapsto [\beta_3]_{5^3} \mapsto [\beta_2]_{5^2} \mapsto [\beta_1]_5)$$

を定理 4 で存在が保証された合同方程式の系列 $(*)_r\,(r = 1, 2, 3, \cdots)$ の解の系列で

$$\beta_1 = 3$$

となるものとします。$\beta_1, \cdots, \beta_r$ が求まっているとします。

$$2\beta_r \equiv 2\beta_1 \equiv 2 \times 3 \equiv 1 \not\equiv 0 \,(\mathrm{mod}\, 5)$$

なので、

$$y = [-\frac{\beta_r^2 + 1}{5^r}]_5$$

ということになります。したがって、

$$\beta_{r+1} \equiv \beta_r + y \times 5^r \equiv \beta_r - \frac{\beta_r^2 + 1}{5^r} \times 5^r \equiv \beta_r - \beta_r^2 - 1 \,(\mathrm{mod}\, 5^{r+1})$$

となります。これを計算して、

$$\begin{aligned}\beta = (\quad \cdots &\mapsto [120813568]_{5^{12}} \mapsto [23157318]_{5^{11}} \mapsto [3626068]_{5^{10}} \mapsto [1672943]_{5^9} \mapsto [110443]_{5^8} \\ &\mapsto [32318]_{5^7} \mapsto [1068]_{5^6} \mapsto [1068]_{5^5} \mapsto [443]_{5^4} \mapsto [68]_{5^3} \mapsto [18]_{5^2} \mapsto [3]_5)\end{aligned}$$

となります。

## 6. $p$ 進数

5 節で得た合同方程式の系列 $(*)_r\,(r=1,2,3,\cdots)$ の 2 つの解の系列 $\alpha,\beta$ を、どのようにして方程式

$$x^2+1=0$$

の解と見ることができるか解説します。何をするかと言えば、数の方も系列化して、加法や乗法を持つ新しい数の集合を作ります。新たな数を 5 進数といいます。5 進数は、整数・有理数の実数への拡大とは異なる数の範囲の拡大になっています。次節で、5 進数の世界で方程式を解きます。$p=5$ として 5 という素数を使いますが、任意の素数 $p$ に対しても $p$ 進数が同様の方法で定義できます。

3 節で定めたように、$A_r$ を $5^r$ を法とする合同類全体の集合とします。集合 $\mathbb{Z}_5$ を

$$\mathbb{Z}_5=\left\{ ([a_r]_{5^r})_{r=1}^{\infty}\in\prod_{r=1}^{\infty}A_r \;\middle|\; \text{すべての } r \text{ に対して } a_{r+1}\equiv a_r \pmod{5^r} \right\}$$

と置きます。$\mathbb{Z}_5$ の各元を 5 進数といいます。$\mathbb{Z}_5$ に加法・減法と乗法を、

$$\begin{aligned} ([a_r]_{5^r})_{r=1}^{\infty}\pm([b_r]_{5^r})_{r=1}^{\infty} &= ([a_r\pm b_r]_{5^r})_{r=1}^{\infty}\\ ([a_r]_{5^r})_{r=1}^{\infty}\times([b_r]_{5^r})_{r=1}^{\infty} &= ([a_rb_r]_{5^r})_{r=1}^{\infty}\end{aligned}$$

と定めましょう。命題 3 (3 節の最後の部分) から、任意の $r$ に対して

$$\begin{aligned} a_{r+1}\pm b_{r+1} &\equiv a_r\pm b_r \pmod{5^r}\\ a_{r+1}b_{r+1} &\equiv a_rb_r \pmod{5^r}\end{aligned}$$

となるので、加法・減法と乗法は矛盾なく定義されます。この加法と乗法に関して $\mathbb{Z}_5$ は「環」になります。

整数全体 $\mathbb{Z}$ から $\mathbb{Z}_5$ への写像を

$$\begin{array}{ccccc} i & : & \mathbb{Z} & \to & \mathbb{Z}_5\\ & & a & \mapsto & ([a]_{5^r})_{r=1}^{\infty}\end{array}$$

と定めます。$i(a)$ はすべての成分が $a$ の代表する合同類という元です。$i$ は中への 1 対 1 写像です。実際、$a>b$ とすると、$r$ を十分大きくとれば $0<a-b<5^r$ となります。このとき、$a$ と $b$ を $5^r$ で割った余りが異なるので、$[a]_{5^r}\neq[b]_{5^r}$ となります。よって、$i(a)\neq i(b)$ です。さらに、定理 2 から

$$\begin{aligned} i(a\pm b) &= i(a)\pm i(b)\\ i(ab) &= i(a)\times i(b)\end{aligned}$$

となります。通常は $i$ を省いて、単に $a$ と書きます。

**定理 5.** $a=(\cdots\mapsto[a_{r+1}]_{5^{r+1}}\mapsto[a_r]_{5^r}\mapsto[a_{r-1}]_{5^{r-1}}\mapsto\cdots\mapsto[a_3]_{5^3}\mapsto[a_2]_{5^2}\mapsto[a_1]_5)$ を $\mathbb{Z}_5$ の元とする。

任意の正の整数 $r$ に対して

$$\begin{gathered} a_r\equiv c_1+c_2\times5+c_3\times5^2+\cdots+c_{r-1}\times5^{r-2}+c_r\times5^{r-1}\pmod{5^r}\\ c_r\in\{0,1,2,3,4\}\end{gathered}$$

を満たす無限数列 $\{c_r\}_{r=1}^{\infty}$ がただ一つ存在して、$a$ は収束する無限級数の極限として

$$a=c_1+c_2\times5+c_3\times5^2+\cdots+c_r\times5^{r-1}+c_{r+1}\times5^r+\cdots$$

と一意的に表わされる (5 進展開)。さらに、任意の正の整数 $r$ に対して、ある整数 $b$ が存在して

$$a-b=c'_{r+1}\times5^r+c'_{r+2}\times5^{r+1}+c'_{r+3}\times5^{r+2}+\cdots\quad(c'_s\in\{0,1,2,3,4\})$$

となる。(この性質を $\mathbb{Z}_5$ の中での整数の稠蜜性 (ちゅうみつせい) といいます。)

逆に、無限数列 $\{c_r\}_{r=1}^{\infty}$ から無限級数が上のように定まり、その極限として $\mathbb{Z}_5$ の元が定まる。

定理 5 の証明の概略を書きます。$([a_r]_{5^r})_{r=1}^{\infty}$ に対して、$\{c_r\}_{r=1}^{\infty}$ を次のように帰納的に定めます。

$$c_1 \equiv a_1 \,(\mathrm{mod}\, 5)$$

となる整数 $c_1 \in \{0,1,2,3,4\}$ をとります。$c_1, \cdots, c_r$ が決まっているとすると

$$a_{r+1} \equiv a_r \equiv c_1 + c_2 \times 5 + c_3 \times 5^2 + \cdots + c_{r-1} \times 5^{r-2} + c_r \times 5^{r-1} \,(\mathrm{mod}\, 5^r)$$

なので、

$$a_{r+1} - (c_1 + c_2 \times 5 + c_3 \times 5^2 + \cdots + c_{r-1} \times 5^{r-2} + c_r \times 5^{r-1}) \equiv c_{r+1} \times 5^r \,(\mathrm{mod}\, 5^{r+1})$$

を満たす整数 $c_{r+1} \in \{0,1,2,3,4\}$ がただ一つ決まります。

収束の意味ですが、$\mathbb{Z}_5$ の中では

$$n \to 0 \quad \text{のとき} \quad p^n \to 0$$

が成り立ちます。無限数列 $\{c_r\}_{r=1}^{\infty}$ から逆の手順をたどると整数列 $\{a_r\}_{r=1}^{\infty}$ が

$$a_r = c_1 + c_2 \times 5 + c_3 \times 5^2 + \cdots + c_{r-1} \times 5^{r-2} + c_r \times 5^{r-1}$$

で定義され、この $\{a_r\}_{r=1}^{\infty}$ を用いて

$$a = (\cdots \mapsto [a_{r+1}]_{5^{r+1}} \mapsto [a_r]_{5^r} \mapsto [a_{r-1}]_{5^{r-1}} \mapsto \cdots \mapsto [a_3]_{5^3} \mapsto [a_2]_{5^2} \mapsto [a_1]_5)$$

と $\mathbb{Z}_5$ の中の元が定まります。収束することは、任意の正の整数 $r$ に対して

$$a - a_r = c_{r+1} \times 5^r + c_{r+2} \times 5^{r+1} + c_{r+3} \times 5^{r+2} + \cdots$$

が $\mathbb{Z}_5$ の中で $5^r$ で割り切れるということからわかります。

**例.** $\mathbb{Z}_5$ の中では $1 + 5 + 5^2 + 5^3 + \cdots = \dfrac{1}{1-5} = -\dfrac{1}{4}$ となる。

証明：実際、正の整数 $r \leqq s$ に対して

$$(1-5)(1 + 5 + 5^2 + \cdots + 5^{s-1}) = 1 + 5^s \equiv 1 \,(\mathrm{mod}\, 5^r)$$

となるので、$r \to \infty$ とするとよい。 □

少し、不思議な感じがしますね。実数の世界では、無限級数

$$1 + t + t^2 + t^3 + t^4 + \cdots$$

は、$|t| < 1$ のときのみ収束し、その極限が $\dfrac{1}{1-t}$ となるのでした。

5 進数の世界では、実数の世界では収束しえない無限級数が収束します。これは、整数・有理数から実数を作る作り方と 5 進数を作る作り方が違うからです。整数・有理数はまばらにあり、隙間を敷き詰める (稠密性) というイメージは同じなのですが、何が近い数かということが違うのです。その違いを表にまとめると

| 実数 | 「通常の意味」での大きさが 0 に近い |
|---|---|
| 5 進数 | 大きな 5 のべきで割れるほど 0 に近い |

となります。

## 7. 方程式 $x^2+1=0$ の 5 進数における解

5 節で存在を示した合同方程式の系 $(*)_r\,(r=1,2,3,\cdots)$ の解からできた合同類の系 $\alpha,\beta$ を考えます。$\alpha=([\alpha_r]_{5^r})_{r=1}^{\infty}$ とおくと、定理 4 から

$$\alpha_{r+1}\ \equiv\ \alpha_r\,(\mathrm{mod}\,5^r)$$

となるので、$\mathbb{Z}_5$ の元になります。$\beta$ についても同様です。

$\alpha^2+1$ を計算してみましょう。定理 4 から

$$\alpha_r^2+1\ \equiv\ 0\,(\mathrm{mod}\,5^r)$$

が各正の整数 $r$ に対して成り立つので、$\mathbb{Z}_5$ における加法と乗法の定義から

$$\alpha^2+1=0$$

となります。同様に $\beta^2+1=0$ となります。したがって、次の定理が成り立ちます。解が 2 つしかないことは、解の系が 2 つのみであることに従います。

**定理 6.** 方程式 $x^2+1=0$ は $\mathbb{Z}_5$ の中で解 $x=\alpha,\beta$ を持つ。また、解はこの 2 つのみである。

ここからは付け足しです。素数 $p$ を動かすと次のようになります。

$$\text{方程式 } x^2+1=0 \text{ が } \mathbb{Z}_p \text{ の中で解ける } \Leftrightarrow\ p\ \equiv\ 1\,(\mathrm{mod}\,4)$$

$p$ が小さいときに、合同方程式の系として $\mathbb{Z}_p$ の元が定まることを確認してみましょう。

最後にもう一言だけ加えます。自然現象は、種々の物事が絡み合ってとても複雑ですが、一つ一つを取り上げるととてもシンプルで、整数上の幾何学によって記述されるものが多々あります。それらの現象を解析するにあたり、実数・複素数のみでなく、合同類や $p$ 進数を用いて考えるとより本質的なものが見えてくることがよくあります。現代整数論は、そういう現象を扱う数学でもあります。

もっと詳しく知りたい方は、

山本芳彦 著「数論入門 1, 2」 岩波講座「現代数学への入門」

を読むことをお薦めします。整数論全般への入門書です。その一部として、整数の合同やその類とそれを用いた計算などが解説されています。コンピュータを用いた具体的な計算などとても楽しい本です。

少し専門的になりますが

加藤和也・黒川重信・斎藤毅 著「数論 1」 岩波講座「現代数学の基礎」
J.P. セール 著・彌永昌吉 訳 「数論講義」 岩波書店

などが入門書に続く文献です。$p$ 進数の整数論を取り上げています。