環論 (第 8 回)

8. 剰余環

今回は剰余環について解説する. まず, 例を挙げる. 整数全体を 3 で割った余りで分類する.

$$\{0+3n \mid n\in\mathbb{Z}\} = \{-3,0,3,6,...\},$$
$$\{1+3n \mid n\in\mathbb{Z}\} = \{-2,1,4,7,...\},$$
$$\{2+3n \mid n\in\mathbb{Z}\} = \{-1,2,5,8,...\}.$$

この各グループを $\mathbb{Z}$ の法 3 の剰余類と言う. 整数 $x\in\mathbb{Z}$ に対して,

$$x+3\mathbb{Z} = \{x+3n \mid n\in\mathbb{Z}\}$$

とおくと, 剰余類はそれぞれ

$$0+3\mathbb{Z} = \{3n \mid n\in\mathbb{Z}\},\quad 1+3\mathbb{Z} = \{1+3n \mid n\in\mathbb{Z}\},\quad 2+3\mathbb{Z} = \{2+3n \mid n\in\mathbb{Z}\}$$

と表せる. 剰余類全体の集合

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

を商集合と呼ぶ. この商集合に足し算と掛け算を次で定める.

$$\begin{aligned}(x+3\mathbb{Z})+(y+3\mathbb{Z}) &= (x+y)+3\mathbb{Z}\\ (x+3\mathbb{Z})\cdot(y+3\mathbb{Z}) &= (xy)+3\mathbb{Z}.\end{aligned}$$

この演算で $\mathbb{Z}/3\mathbb{Z}$ は可換環となる. 例えば,

$$\begin{aligned}(1+3\mathbb{Z})+(2+3\mathbb{Z}) &= (3+3\mathbb{Z}) = 0+3\mathbb{Z},\\ (2+3\mathbb{Z})\cdot(2+3\mathbb{Z}) &= (4+3\mathbb{Z}) = 1+3\mathbb{Z}\end{aligned}$$

のように計算できる.

一般的に可換環 A とそのイデアル I が与えられると, 上例のように新しい可換環 A/I を構成できる. これを A の I による剰余環という. 剰余環は非常に重要な概念であり, 数学の様々な対象が剰余環を用いて表現される. 今回は剰余環の構成と演算の計算方法について詳しくみる.

定義 8-1 (剰余類と商集合)

可換環 A のイデアル I を考える．$x \in A$ に対して集合

$$x + I = \{x + a \mid a \in I\}$$

を x **の属する剰余類**という．また剰余類全体を

$$A/I = \{x + I \mid x \in A\}$$

で表し, A **の** I **による商集合**という．

(補足)

(1) $0 + I$ は単に I と省略して書くこともある．

(2) $x + I$ を $\bar{x}$ と表すこともある．

(3) $0 \in I$ より $x \in x + I$ に注意する．特に

$$A = \bigcup_{x \in A} (x + I).$$

定理 8-1

可換環 A のイデアル I を考える．$x, y \in A$ に対して

(1) $x + I = y + I \iff x - y \in I.$

(2) $x + I = y + I \iff (x + I) \cap (y + I) \neq \phi.$

[証明]

(1) $x + I = y + I$ とする．$x \in x + I = y + I$ より $x = y + a$ $(a \in I)$ と表せるので,

$$x - y = a \in I.$$

逆に $x - y \in I$ と仮定する． このとき, $x - y = a$ $(a \in I)$ と表せる． $z \in x + I$ とすると, $z = x + b$ $(b \in I)$ と表せる．$a + b \in I$ より

$$z = x + b = y + (a + b) \in y + I.$$

従って $x + I \subseteq y + I$. 同様に $y + I \subseteq x + I$.

(2) $\Rightarrow$ は自明．$\Leftarrow$ を示す．仮定より $z \in (x + I) \cap (y + I)$ が取れる．このとき,

$$z = x + a = y + b \ (a, b \in I)$$

と表せるので $x-y=b-a\in I$. (1) より $x+I=y+I$.

$\square$

例題 8-1

(1) $\mathbb{Z}$ において $1+5\mathbb{Z}=11+5\mathbb{Z}$ を示せ.

(2) $\mathbb{C}[x]$ のイデアル $I=(x+1)$ に対して, $x^3+I=x+I$ を示せ.

[解答]
(1) $1-11=-10\in 5\mathbb{Z}$ より $1+5\mathbb{Z}=11+5\mathbb{Z}$.
(2) $x^3-x=x(x-1)(x+1)\in I$ より $x^3+I=x+I$.

$\square$

問題 8-1

(1) $\mathbb{C}[x]$ のイデアル $I=(x-1)$ に対して, $(x^2+1)+I=(x+1)+I$ を示せ.

(2) 可換環 $A=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$ のイデアル $I=(2,\ 1+\sqrt{-5})$ に対して次を示せ.

$$(10+3\sqrt{-5})+I=(3+2\sqrt{-5})+I.$$

例題 8-2
　$f(x)\in\mathbb{C}[x]\setminus\{0\}$ に対して $\mathbb{C}[x]$ のイデアル $I=(f(x))$ を考える. $g(x),h(x)\in\mathbb{C}[x]$ に対して次の同値を示せ.

$$g(x)+I=h(x)+I \iff g(x) \text{ と } h(x) \text{ を } f(x) \text{ で割った余りは等しい.}$$

特に

$$g(x)+I=r(x)+I,\quad \deg r(x)<\deg f(x)$$

のとき, $g(x)$ を $f(x)$ で割った余りは $r(x)$ である.

※ つまり, $\mathbb{C}[x]/I$ は $\mathbb{C}[x]$ を $f(x)$ で割った余りでグループ分けしたものと考えられる.

[証明]
割り算の原理より

$$\begin{aligned} g(x) &= q_1(x)f(x)+r_1(x) \quad (q_1(x),r_1(x)\in\mathbb{C}[x],\ \deg r_1(x)<\deg f(x)), \\ h(x) &= q_2(x)f(x)+r_2(x) \quad (q_2(x),r_2(x)\in\mathbb{C}[x],\ \deg r_2(x)<\deg f(x)) \end{aligned}$$

と表せる. $g(x)+I=h(x)+I$ と仮定する. $g(x)-h(x)\in I$ より

$$r_1(x)-r_2(x)=(g(x)-h(x))+f(x)(q_2(x)-q_1(x))\in I=(f(x)).$$

$\deg(r_1(x)-r_2(x)) < \deg f(x)$ より $r_1(x)=r_2(x)$.

逆に $r_1(x)=r_2(x)$ と仮定すると

$$g(x)-h(x)=f(x)(q_1(x)-q_2(x)) \in I.$$

よって $g(x)+I=h(x)+I$.

□

問題 8-2　自然数 n に対して $\mathbb{Z}$ のイデアル $n\mathbb{Z}$ を考える．$a,b \in \mathbb{Z}$ に対して次の同値を示せ.

$$a+n\mathbb{Z}=b+n\mathbb{Z} \iff a \text{ と } b \text{ を } n \text{ で割った余りは等しい}.$$

定義 8-2 (完全代表系)

可換環 A のイデアル I を考える．A の部分集合 R が次の 2 条件を満たすとき, A/I **の完全代表系**という.

(1) $A/I=\{x+I \mid x \in R\}$.

(2) $x+I=y+I \ (x,y \in R) \Rightarrow x=y$.

完全代表系は A/I の各剰余類から一つずつ元を取ってできる集合である.

例題 8-3

自然数 n に対して, $\mathbb{Z}/n\mathbb{Z}$ の完全代表系は $R=\{0,1,2,...,n-1\}$ で与えられる.

[証明]

(1) $a+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ とする．このとき,

$$a=qn+r \quad (q,r \in \mathbb{Z}, \quad 0 \le r \le n-1)$$

と表せる．$a-r=qn \in n\mathbb{Z}$ より

$$a+n\mathbb{Z}=r+n\mathbb{Z} \in \{r+n\mathbb{Z} \mid r \in R\}.$$

よって $\mathbb{Z}/n\mathbb{Z} \subseteq \{x+n\mathbb{Z} \mid x \in R\}$ であり, 逆の包含は明らかなので

$$\mathbb{Z}/n\mathbb{Z}=\{x+n\mathbb{Z} \mid x \in R\}.$$

(2) $a+n\mathbb{Z}=b+n\mathbb{Z}\ (a,b \in R)$ とする．このとき,

$$a-b \in n\mathbb{Z}, \qquad -(n-1) \le a-b \le n-1$$

なので $a=b$.

以上 (1), (2) より R は $\mathbb{Z}/n\mathbb{Z}$ の完全代表系である.

$\square$

問題 8-3 $A = \mathbb{C}[x]$ のイデアル $I = (x^2)$ を考える. 次の集合 R は A/I の完全代表系であることを示せ.

$$R = \{a + bx \mid a, b \in \mathbb{C}\}.$$

定理 8-2

可換環 A とそのイデアル I を考える. 商集合 A/I に対して

$$\begin{aligned} (x+I)+(y+I) &= (x+y)+I, \quad &\text{(eq1)} \\ (x+I)\cdot(y+I) &= xy+I \quad &\text{(eq2)} \end{aligned}$$

により足し算と掛け算を定義する.

(1) 演算 (eq1), (eq2) は well-defined である.

(2) この演算により A/I は可換環をなし, さらに

$$0_{A/I} = 0_A + I, \qquad 1_{A/I} = 1_A + I.$$

可換環 A/I を **A の I による剰余環**という.

[証明]

(1) 足し算のみ示す. 示すことは,

$$x_1 + I = x_2 + I,\ \ y_1 + I = y_2 + I \Rightarrow (x_1 + y_1) + I = (x_2 + y_2) + I.$$

$x_1 + I = x_2 + I$, $y_1 + I = y_2 + I$ より,

$$x_1 - x_2 \in I, \quad y_1 - y_2 \in I.$$

従って

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) \in I.$$

よって $(x_1 + y_1) + I = (x_2 + y_2) + I$.

(2) A/I が可換環であることは A が可換環であることから導かれる. 例えば, A/I の分配法則 (定義 1-1 の (3-1)) について考える.

$$\begin{aligned} (x+I)\cdot\{(y+I)+(z+I)\} &= (x+I)\cdot((y+z)+I) \\ &= x\cdot(y+z)+I \\ &= (x\cdot y + x\cdot z)+I \quad (\because A \text{ の分配法則}) \\ &= (x\cdot y+I)+(x\cdot z+I) \\ &= (x+I)\cdot(y+I)+(x+I)\cdot(z+I). \end{aligned}$$

よって A/I で分配法則が成り立つ.

$\square$

問題 8-4

(1) 演算 (eq2) が well-defined であることを示せ.

(2) 定理 8-2 の状況で $1_{A/I} = 1_A + I$ を示せ.

例題 8-4
可換環 $\mathbb{Z}/7\mathbb{Z}$ において考える.

(1) $\overline{15 \cdot 16 \cdot 17}$ を計算せよ.

(2) $(\bar{2})^{30}$ を計算せよ.

(3) $(\bar{5})^{-1}$ を計算せよ.

(4) $\mathbb{Z}/7\mathbb{Z}$ は体であることを示せ.

ここで, $\bar{x} = x + 7\mathbb{Z}$ である.

[解答]
(1) について.

$$\overline{15 \cdot 16 \cdot 17} = \overline{15} \cdot \overline{16} \cdot \overline{17} = \bar{1} \cdot \bar{2} \cdot \bar{3} = \bar{6}.$$

(2) $(\bar{2})^3 = \bar{8} = \bar{1}$ より,

$$(\bar{2})^{30} = \{(\bar{2})^3\}^{10} = (\bar{1})^{10} = \bar{1}.$$

(3) $\bar{5} \cdot \bar{3} = \overline{15} = \bar{1}$ より $(\bar{5})^{-1} = \bar{3}$.

(4) まず,

$$\bar{1} \cdot \bar{1} = \bar{1}, \quad \bar{2} \cdot \bar{4} = \bar{1}, \quad \bar{3} \cdot \bar{5} = \bar{1}, \quad \bar{6} \cdot \bar{6} = \bar{1}.$$

よって $\mathbb{Z}/7\mathbb{Z} \setminus \{\bar{0}\}$ の全て元は可逆元なので $\mathbb{Z}/7\mathbb{Z}$ は体である.

$\square$

問題 8-5 可換環 $\mathbb{Z}/22\mathbb{Z}$ において考える.

(1) $(\overline{23})^3 + (\overline{49})^3$ を計算せよ.

(2) $(\bar{5})^{-1}$ を計算せよ.

(3) $\mathbb{Z}/22\mathbb{Z}$ は整域ではないとことを示せ. 従って $\mathbb{Z}/22\mathbb{Z}$ は体でもない (定理 2-2).

例題 8-5

$A = \mathbb{R}[x]$ とそのイデアル $I = (x^2+1)$ を考える.

(1) A/I の完全代表系は $\{a + bx \mid a, b \in \mathbb{R}\}$ であることを示せ.

(2) A/I は体である.

※ 後の授業で A/I が $\mathbb{C}$ と同型 (=環構造が同じ) であることを示す. A/I の元 $\bar{x}$ が $\mathbb{C}$ における $\sqrt{-1}$ に対応する.

[証明]

(1) 問題 8-3 と同様.

(2) $\overline{f(x)} \in A/I \setminus \{\bar{0}\}$ とする. (1) より

$$\overline{f(x)} = \overline{a+bx} \ \ (a, b \in \mathbb{R})$$

と表せる. $\overline{f(x)} \neq \bar{0}$ より, $a \neq 0$ または $b \neq 0$. 特に $a^2 + b^2 \neq 0$. ここで

$$g(x) = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} \cdot x$$

とおくと,

$$\overline{f(x)} \cdot \overline{g(x)} = \overline{\frac{a^2}{a^2+b^2}} + \overline{\frac{-b^2}{a^2+b^2}} \cdot (\overline{x})^2.$$

$I = (x^2+1)$ より $(\bar{x})^2 = \overline{-1}$. よって

$$\overline{f(x)} \cdot \overline{g(x)} = \overline{1}.$$

従って $\overline{f(x)} \in (A/I)^{\times}$. よって A/I は体である.

$\square$