2011年7月5日

定義の復習

$R \subset X \times X$ を同値関係とし、$x \in X$ とするとき、

$$[x] = \{y \mid y \in X,\ (x, y) \in R\}$$

を、(関係 R に関する、) x を含む同値類という。同値類全体の集合 $\{[x] \mid x \in X\}$ を関係 R による商集合といい、X/R と書く。R は同値関係なので、

$$(x, y) \in R \iff [x] = [y] \iff x \in [y] \iff y \in [x] \iff [x] \cap [y] \neq \emptyset.$$

$\mathbb{Z}$ の構成

$$\mathbb{N} = \{1, 2, 3, \dots\},$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$$

とし、$\mathbb{N}_0^2 = \mathbb{N}_0 \times \mathbb{N}_0$ 上の関係 R を次で定める。

$$R = \{((a, b), (c, d)) \in \mathbb{N}_0^2 \mid a + d = b + c\}$$

すると R は同値関係になる。R による商集合

$$\mathbb{N}_0^2/R = \{[a, b] \mid (a, b) \in \mathbb{N}_0^2\}$$

から $\mathbb{Z}$ への写像　f を

$$f([a, b]) = a - b$$

によって定める。f の定義は見かけ上同値類 $[a, b]$ の代表元 (a, b) の取り方に依存しているように見えるので、$[a, b] = [c, d]$ のとき $f([a, b]) = f([c, d])$ が示されないと f は写像になっていると言えない。実際、

$$[a, b] = [c, d] \implies ((a, b), (c, d)) \in R \implies a + d = b + c \implies a - b = c - d$$

なので、$f([a, b]) = f([c, d])$ が成り立つ。

このように、商集合を定義域とする写像の定義が見かけ上同値類の代表元の取り方に依存しているとき、その写像の値が実際には同値類の代表元の取り方に依存しないことを示すことを、「写像が well-defined である」ことを示す、という。上の写像 f は全単射でもある。

集合 X における二項演算 (binary operation) とは、$X \times X$ から X への写像のことである。例えば、$\mathbb{N}_0^2/R$ に演算 $+$ を次のように定義することができる。

$$+ : (\mathbb{N}_0^2/R) \times (\mathbb{N}_0^2/R) \to \mathbb{N}_0^2/R,\ +([a,b],[c,d]) = [a+c, b+d].$$

以後 $+([a,b],[c,d])$ を $[a,b]+[c,d]$ と書くことにする。この写像 $+$ は well-defined である。実際、$[a,b] = [a',b']$, $[c,d] = [c',d']$ とすると、$\alpha = a'-a = b'-b$, $\beta = c'-c = d'-d$ とおくことにより、$[a+c, b+d] = [a'+c', b'+d']$ が確かめられる。さらに、

$$f([a,b]+[c,d]) = f([a,b]) + f([c,d])$$

が成り立つ。ただし、右辺における $+$ は $\mathbb{Z}$ における通常の和である。

$\mathbb{Q}$ の構成

$$X = \{(a,b) \mid a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0\}$$

とおき、

$$R = \{((a,b),(c,d)) \mid ((a,b),(c,d)) \in X \times X,\ ad = bc\}$$

とおくと、R は X 上の同値関係になる。R による商集合

$$X/R = \{[a,b] \mid (a,b) \in X\}$$

から $\mathbb{Q}$ への写像　f を

$$f([a,b]) = \frac{a}{b}$$

によって定める。f は well-defined であることがわかり、また f は全単射でもある。

X/R に演算 $\times$ を次のように定義することができる。

$$\times : (X/R) \times (X/R) \to X/R,\ \times([a,b],[c,d]) = [ac, bd].$$

この写像 $\times$ は well-defined である。さらに、

$$f(\times([a,b],[c,d])) = f([a,b])f([c,d])$$

が成り立つ。ただし、右辺は $\mathbb{Q}$ における通常の積である。

X/R に演算 $+$ を次のように定義することができる。

$$+ : (X/R) \times (X/R) \to X/R,\ +([a,b],[c,d]) = [ad+bc, bd].$$

この写像 $+$ は well-defined である。さらに、

$$f(+([a,b],[c,d])) = f([a,b]) + f([c,d])$$

が成り立つ。ただし、右辺の $+$ は $\mathbb{Q}$ における通常の和である。

$\mathbb{Z}/m\mathbb{Z}$ の構成

m を正の整数とし、$a \in \mathbb{Z}$ が m で割り切れるとき $m|a$ と書く。

$$R = \{(a, b) \mid (a, b) \in \mathbb{Z} \times \mathbb{Z},\ m|(a - b)\}$$

とおくと、R は $\mathbb{Z}$ 上の同値関係になる。R による商集合

$$\mathbb{Z}/R = \{[a] \mid a \in \mathbb{Z}\}$$

を $\mathbb{Z}/m\mathbb{Z}$ とも書く。$\mathbb{Z}/m\mathbb{Z}$ に演算 $+$ を次のように定義することができる。

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ +([a], [b]) = [a + b].$$

この写像 $+$ は well-defined である。また、$\mathbb{Z}/m\mathbb{Z}$ に演算 $\times$ を次のように定義することができる。

$$\times : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ \times([a], [b]) = [ab].$$

この写像 $\times$ は well-defined である。

環の定義

集合 A に２つの演算 $+$（加法）, $\times$（乗法）が定義されていて、下記の性質が成り立つとき、A は環 (ring) であるという。

(1) $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$ （結合法則）

(2) $\forall a, b \in A,\ a + b = b + a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a + 0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a + b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b + c) = (a \times b) + (a \times c),\ (b + c) \times a = (b \times a) + (c \times a)$ （分配法則）

通常、「$\times$」は省略して書かない。また、a の加法に関する逆元（上記 (4) 参照）を $-a$ と書き、$a + (-b)$ を $a - b$ と書く（これで減法が定義されたことになる）。例えば、$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ などがそうである。$\mathbb{R}$ を成分とする n 次正方行列全体の集合も環になる。さらに、$\mathbb{Z}/m\mathbb{Z}$ も環になる。