2013年6月11日

イデアルと剰余環（復習）

可換環 A の空でない部分集合 I がイデアルとは、

(i) $\forall a \in I, \forall b \in I, a + b \in I$

(ii) $\forall a \in A, \forall b \in I, ab \in I$

が成り立つときをいう。I が A のイデアルならば

$$R = \{(a, b) \mid a \in A,\ b \in A,\ a - b \in I\}.$$

は A 上の同値関係になる。商集合 A/R を A/I と書く。A/I に演算 $+, \times$ を次のように定義することができる。

$$\begin{aligned} + : A/I \times A/I \to A/I, &\quad + ([a], [b]) = [a + b], \\ \times : A/I \times A/I \to A/I, &\quad \times ([a], [b]) = [ab]. \end{aligned}$$

これらの写像 $+, \times$ は well-defined であり、これらの演算により A/I は環になる。

複素数の構成

$A = \mathbb{R}[x]$ のイデアル

$$I = (x^2 + 1) = \{f(x)(x^2 + 1) \mid f(x) \in \mathbb{R}[x]\}$$

を考える。$\forall [f(x)] \in A/I$ (ただし $f(x) \in A$) に対して、$f(x)$ を $x^2 + 1$ で割った商を $q(x) \in A$, 余りを $a + bx$ $(a, b \in \mathbb{R})$ とおくと、

$$f(x) = (x^2 + 1)q(x) + a + bx$$

ここで、$(x^2 + 1)q(x) \in I$ だから、同値関係 R の定義より $[f(x)] = [a + bx]$ となる。したがって

$$A/I = \{[a + bx] \mid a, b \in \mathbb{R}\}.$$

また、$a, b, a', b' \in \mathbb{R}$ に対して、

$$\begin{aligned} [a + bx] = [a' + b'x] &\iff (a + bx) - (a' + b'x) \in I \\ &\iff (a - a') + (b - b')x \text{ は } x^2 + 1 \text{ で割り切れる} \\ &\iff a - a' = b - b' = 0 \\ &\iff a = a',\ b = b' \end{aligned}$$

である。さらに、A/I における和は

$$[a+bx]+[a'+b'x]=[(a+bx)+(a'+b'x)]=[(a+a')+(b+b')x]$$

であり、積は

$$\begin{aligned}[a+bx][a'+b'x]&=[(a+bx)(a'+b'x)]\\&=[aa'+(ab'+ba')x+bb'x^2]\\&=[aa'+(ab'+ba')x+bb'(x^2+1)-bb']\\&=[aa'-bb'+(ab'+ba')x]\end{aligned}$$

となるので、これは複素数における和と積

$$\begin{aligned}(a+bi)+(a'+b'i)&=(a+a')+(b+b')i,\\(a+bi)(a'+b'i)&=(aa'-bb')+(ab'+ba')i\end{aligned}$$

と同じ形をしている。つまり、複素数は、A/I の元 $[a+bx]$ を $a+bi$ と略記したものと考えることができる。厳密には、全単射 $\varphi : A/I \to \mathbb{C}$, $\varphi([f(x)])=f(\sqrt{-1})$ が定義できて、しかも $[f_1(x)],[f_2(x)]\in\mathbb{R}[x]/(x^2+1)$ に対して

$$\begin{aligned}\varphi([f_1(x)]+[f_2(x)])&=\varphi([f_1(x)])+\varphi([f_2(x)]),\\\varphi([f_1(x)]\times[f_2(x)])&=\varphi([f_1(x)])\varphi([f_2(x)])\end{aligned}$$

ただし右辺は $\mathbb{C}$ における和と積である。

一般に A,B を 2 つの環とするとき、ある全単射 $\varphi : A\to B$ が存在して、$\forall a,b\in A$,

$$\begin{aligned}\varphi(a+b)&=\varphi(a)+\varphi(b),\\\varphi(ab)&=\varphi(a)\varphi(b),\\\varphi(1_A)&=1_B\end{aligned}$$

となるとき、A と B は同型であるといい、$A\cong B$ と書く。ただし、1_A は A の単位元、1_B は B の単位元を表す。上のことは $A/I\cong\mathbb{C}$ となることを示している。

$(\mathbb{Z}/3\mathbb{Z}[x])/(x^2+1)$ の構成

同様のことを $\mathbb{R}$ の代わりに $\mathbb{Z}/3\mathbb{Z}$ でやってみる。$A = \mathbb{Z}/3\mathbb{Z}[x]$ のイデアル $I = (x^2+1)$ を考え、同値関係

$$R = \{(a, b) \mid a \in A,\ b \in A,\ a - b \in I\}.$$

による商集合 A/R (A/I とも書く) に上と同様に演算を入れる。$\mathbb{Z}/3\mathbb{Z}$ は 3 個の同値類 $[0], [1], [2]$ からなるので、A/I は以下の 9 個の同値類からなる：

$$[[0]], [[1]], [[2]], [[1]x], [[1]x + [1]], [[1]x + [2]], [[2]x], [[2]x + [1]], [[2]x + [2]]$$

これらを簡単に

$$0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$$

と書くことにする。加法は例えば、A において

$$\begin{aligned}&(x + 2) + (2x + 2) = ([1]x + [2]) + ([2]x + [2]) = ([1] + [2])x + ([2] + [2])\\&= [1 + 2]x + [2 + 2] = [0]x + [1] = [1] = 1\end{aligned}$$

というように計算するので、A/I においては $[x + 2] + [2x + 2] = [1]$ となる。

乗法は例えば、A において

$$\begin{aligned}&(x + 2)(2x + 2) = ([1]x + [2]) \times ([2]x + [2]) = [1][2]x^2 + ([1][2] + [2][2])x + [2][2]\\&= [2]x^2 + [2 + 4]x + [4] = [2]x^2 + [1] = 2x^2 + 1\end{aligned}$$

というように計算するので、A/I においては $[x+2]\times[2x+2] = [2x^2+1] = [2(x^2+1)+2] = [2]$ となる。