2012年6月12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

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

を考えると、写像 $g : \mathbb{R}[x]/(x^2+1) \to \mathbb{C}$, $g([f(x)]) = f(\sqrt{-1})$ が定義できて、これは全単射であり、しかも $[f_1(x)], [f_2(x)] \in \mathbb{R}[x]/(x^2+1)$ に対して

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

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 $g : A \to B$ が存在して、$\forall a, b \in A$,

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

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 $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ 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。