2012年6月5日

$\mathbb{Z}/m\mathbb{Z}$ 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。$a, b \in \mathbb{Z}$ に対して、$m|(a-b)$ のとき

$$a \equiv b \pmod{m}$$

と書き、a と b は m を法として合同である、という。このような式を合同式という。

$$\begin{aligned}
&[a] = [a'],\ [b] = [b'] \\
&\Longrightarrow\ m|(a-a'),\ m|(b-b') \\
&\Longrightarrow\ m|((a-a')+(b-b')) \\
&\Longrightarrow\ m|((a+b)-(a'+b')) \\
&\Longrightarrow\ [a+b] = [a'+b']
\end{aligned}$$

環 A において

$$\forall a \in A,\ a0 = 0a = 0$$

実際、$a0$ の、加法に関する逆元を b とおくと、

$$\begin{aligned}
0 &= a0 + b \\
&= a(0+0) + b \\
&= (a0 + a0) + b \\
&= a0 + (a0 + b) \\
&= a0 + 0 \\
&= a0.
\end{aligned}$$

$$\sum_{n=0}^{\infty} f(n)x^n = f(0) + f(1)x + f(2)x^2 + \cdots$$

と書いてみて、$f, g \in A^{\mathbb{N}_0}$ の積を考えてみると、多項式の展開となっている。