

商加群について

N が R -加群 M の部分加群であるとき, $m \equiv m' \pmod{N} \stackrel{\text{def}}{\iff} m - m' \in N$ と定義するとこれは同値関係になる. また商集合 $M/\equiv$ に加法, スカラー倍を

$$\begin{aligned} \text{加法} \quad [m] + [m'] &:= [m + m'] \\ \text{スカラー倍} \quad a[m] &:= [am] \end{aligned}$$

と定義すると, これは well-defined であり, $M/\equiv$ は R -加群になる. これを M の N による商加群といい M/N と表す.

・ $\equiv$ が同値関係であること.

(反射律) $\forall m \in M$ に対して, $m - m = 0 \in N$. したがって $m \equiv m \pmod{N}$.

(対称律) $m \equiv m' \pmod{N}$ とすると $m - m' \in N$ よって $m' - m = -(m - m') \in N$ であるので, $m' \equiv m \pmod{N}$.

(推移律) $m_1 \equiv m_2 \pmod{N}$ かつ $m_2 \equiv m_3 \pmod{N}$ とする. このとき $m_1 - m_2 \in N$ かつ $m_2 - m_3 \in N$. よって $m_1 - m_3 = (m_1 - m_2) + (m_2 - m_3) \in N$. すなわち $m_1 \equiv m_3 \pmod{N}$.

・ 加法の well-definedness

$[m_1] = [m'_1], [m_2] = [m'_2]$ とする. このとき $m_1 - m'_1 \in N$ かつ $m_2 - m'_2 \in N$ であるので, $(m_1 + m_2) - (m'_1 + m'_2) = (m_1 - m'_1) + (m_2 - m'_2) \in N$. すなわち $[m_1 + m_2] = [m'_1 + m'_2]$ である.

・ スカラー倍の well-definedness

$[m] = [m']$ とする. このとき $m - m' \in N$ であるので $\forall a \in R$ に対して $am - am' = a(m - m') \in N$. すなわち $[am] = [am']$.

・ M/N が R -加群になることは省略. (加法, スカラー倍が M の加法, スカラー倍で定義されていることから簡単に示される.)

Remark. $\mathbb{Z}/n\mathbb{Z}$ について.

n の倍数全体を $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ と書くことにすれば, これは $\mathbb{Z}$ の部分加群になることが簡単に解かる. n を法とした合同関係は

$$\begin{aligned} z \equiv w \pmod{n} &\stackrel{\text{def}}{\iff} z - w \text{ は } n \text{ の倍数} \\ &\iff z - w \in n\mathbb{Z} \end{aligned}$$

であるので, $\mathbb{Z}/n\mathbb{Z}$ (の加法群) は $\mathbb{Z}$ の $n\mathbb{Z}$ による商加群に他ならない.

したがって, $\mathbb{Z}/n\mathbb{Z}$ の環構造を調べるには, 積の well-definedness のみチェックすればよい. (環になること, 乗法単位元は $[1]$ であることなどは簡単に示せる.)

$[z] = [z'], [w] = [w']$ とする. このとき $\exists k, l \in \mathbb{Z}$ があって $z - z' = nk, w - w' = nl$ と出来る. $zw - z'w' = zw - zw' + zw' - z'w' = z(w - w') + (z - z')w = z(nl) + (nk)w' = n(zl + kw')$ であるので, $[zw] = [z'w']$.

また,

「 m と n が互いに素」である必要十分条件は「 $\exists a, b \in \mathbb{Z}$ が存在して $am + bn = 1$ とできる」こと

であったのを思い出そう. n が素数ならば, 「 n の倍数以外の $\forall m$ に対して m は n と互いに素になるので, $1 = am + bn$ となる $\exists a, b \in \mathbb{Z}$ が存在する」. これを $\mathbb{Z}/n\mathbb{Z}$ の言葉に翻訳すると, 「 $\forall [m] \in \mathbb{Z}/n\mathbb{Z}, [m] \neq [0]$ に対して, $[1] = [a][m] + [b][n] = [a][m]$ となる $[a], [b]$ が存在する」となる. これは $[a]$ が $[m]$ の乗法逆元であること.