数理で読み解く
石取りゲーム

連載◎第 7 回補足 (2009 年 10 月号)

佐藤文広
●立教大学理学部

ニム積と標数 2 の体

この補足では、J.H.Conway “On Numbers and Games” に従って定理 7.1, 7.2（連載第 7 回、10 月号）の証明を与えます。以下では、体論についての基本的な知識を仮定します。この部分は本連載の中でもっとも数学的予備知識を必要とする部分です。

命題 7b.1 ニム積について以下の等式が成り立つ。
(i) $a \overset{*}{\times} 0 = 0$, $a \overset{*}{\times} 1 = a$.
(ii) 交換法則： $a \overset{*}{\times} b = b \overset{*}{\times} a$.
(iii) $b \neq 0$ ならば, ニム積に関する消去則

$$a_1 \overset{*}{\times} b = a_2 \overset{*}{\times} b \quad \Longleftrightarrow a_1 = a_2$$

が成り立つ. とくに, $a, b \neq 0$ ならば, $a \overset{*}{\times} b \neq 0$ である.
(iv) 分配法則： $(a \overset{*}{+} b) \overset{*}{\times} c = a \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c$
(v) 結合法則： $(a \overset{*}{\times} b) \overset{*}{\times} c = a \overset{*}{\times} (b \overset{*}{\times} c)$

【証明】 以下では, 命題 3.7（連載第 3 回、6 月号）の証明と同様に, $\{a'\} = \{a' \mid 0 \leq a' < a\}$ のような略記法を用いる. また、$\overset{*}{=}$ はこの等号の成立において帰納法の仮定を用いていることを表す.

(i) $0'$ は存在しないから, $a \overset{*}{\times} 0 = 0 \overset{*}{\times} a = \mathrm{mex}(\emptyset) = 0$ である. これより, $a = b = c = 0$ のときには, 命題で主張されているその他の等式もすべて成り立つことに注意する. $1' = 0$ なので, $a \overset{*}{\times} 1 = \mathrm{mex}\{a' \overset{*}{\times} 1 \overset{*}{+} a \overset{*}{\times} 0 \overset{*}{+} a' \overset{*}{\times} 0\} \overset{*}{=} \mathrm{mex}\{a'\} = a$.

(ii) $a \overset{*}{\times} b = \mathrm{mex}\{a' \overset{*}{\times} b \overset{*}{+} a \overset{*}{\times} b' \overset{*}{+} a' \overset{*}{\times} b'\} \overset{*}{=} \mathrm{mex}\{b \overset{*}{\times} a' \overset{*}{+} b' \overset{*}{\times} a \overset{*}{+} b' \overset{*}{\times} a'\} = b \overset{*}{\times} a$.

(iii) $a_1 \neq a_2$ だとする. $a_1 < a_2$ としてよい. このとき, $a_2' = a_1$, $b' = 0$ とでき, $a_2' \overset{*}{\times} b \overset{*}{+} a_2 \overset{*}{\times} b' \overset{*}{+} a_2' \overset{*}{\times} b' = a_1 \overset{*}{\times} b$ となるから, $a_2 \overset{*}{\times} b = \mathrm{mex}\{a_2' \overset{*}{\times} b \overset{*}{+} a_2 \overset{*}{\times} b' \overset{*}{+} a_2' \overset{*}{\times} b'\} \neq a_1 \overset{*}{\times} b$ である.

(iv) 分配法則は

$$
\begin{aligned}
&(a \overset{*}{+} b) \overset{*}{\times} c \\
&\quad = \mathrm{mex}\{(a \overset{*}{+} b)' \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{+} b)' \overset{*}{\times} c'\} \\
&\quad \overset{(\spadesuit)}{=} \mathrm{mex}\{(a' \overset{*}{+} b) \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a' \overset{*}{+} b) \overset{*}{\times} c',\ (a \overset{*}{+} b') \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{+} b') \overset{*}{\times} c'\} \\
&\quad \overset{*}{=} \mathrm{mex}\{(a' \overset{*}{\times} c \overset{*}{+} a \overset{*}{\times} c' \overset{*}{+} a' \overset{*}{\times} c') \overset{*}{+} b \overset{*}{\times} c,\ a \overset{*}{\times} c \overset{*}{+} (b' \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c' \overset{*}{+} b' \overset{*}{\times} c')\} \\
&\quad \overset{(\heartsuit)}{=} \mathrm{mex}\{(a \overset{*}{\times} c)' \overset{*}{+} b \overset{*}{\times} c,\ a \overset{*}{\times} c \overset{*}{+} (b \overset{*}{\times} c)'\} \\
&\quad = a \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c
\end{aligned}
$$

と示される. 最初の等号はニム積の定義、最後の等号はニム和の定義による。($\spadesuit$) の等号の成立を示す。補題 3.2 (i) により ($\spadesuit$) の右辺は左辺より大きいか等しい。もし等号が成り立たないとすると, 補題 3.2 (ii) により, $(a \overset{*}{+} b) \overset{*}{\times} c$ は

$$
\begin{gathered}
(a' \overset{*}{+} b) \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a' \overset{*}{+} b) \overset{*}{\times} c', \\
(a \overset{*}{+} b') \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{+} b') \overset{*}{\times} c'
\end{gathered}
$$

のいずれかに等しい.

$$
(a \overset{*}{+} b) \overset{*}{\times} c = (a' \overset{*}{+} b) \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a' \overset{*}{+} b) \overset{*}{\times} c'
$$

だったとする. ここで, $a \overset{*}{+} b > a' \overset{*}{+} b$ だとすると, $(a \overset{*}{+} b) \overset{*}{\times} c$ の定義と矛盾する. 一方, $a \overset{*}{+} b < a' \overset{*}{+} b$ だとすると, 上の式は

$$
(a' \overset{*}{+} b) \overset{*}{\times} c = (a \overset{*}{+} b) \overset{*}{\times} c \overset{*}{+} (a' \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c'
$$

と変形されるから, $(a' \overset{*}{+} b) \overset{*}{\times} c$ の定義と矛盾する.

$$
(a \overset{*}{+} b) \overset{*}{\times} c = (a \overset{*}{+} b') \overset{*}{\times} c \overset{*}{+} (a \overset{*}{+} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{+} b') \overset{*}{\times} c'
$$

の場合も同様に矛盾に導かれる. よって, ($\spadesuit$) の等号が示された.

次に ($\heartsuit$) の等号を示そう. やはり補題 3.2 (i) により ($\heartsuit$) の左辺は右辺より大きいか等しく、($\heartsuit$) が成り立たないとすると, 補題 3.2 (ii) により, $a \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c$ は

$$
\begin{gathered}
(a' \overset{*}{\times} c \overset{*}{+} a \overset{*}{\times} c' \overset{*}{+} a' \overset{*}{\times} c') \overset{*}{+} b \overset{*}{\times} c, \\
a \overset{*}{\times} c \overset{*}{+} (b' \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c' \overset{*}{+} b' \overset{*}{\times} c')
\end{gathered}
$$

のいずれかに等しい. もし, 前者に等しいならば

$$
a \overset{*}{\times} c = a' \overset{*}{\times} c \overset{*}{+} a \overset{*}{\times} c' \overset{*}{+} a' \overset{*}{\times} c'
$$

となり、$a \overset{*}{\times} c$ の定義に矛盾する．もし、後者に等しいならば

$$b \overset{*}{\times} c = b' \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c' \overset{*}{+} b' \overset{*}{\times} c'$$

となり、同様に矛盾に導かれる．よって, (♡) の等号が示された.

(v) 結合法則は

$$\begin{aligned}
&(a \overset{*}{\times} b) \overset{*}{\times} c \\
&\quad = \mathrm{mex}\{(a \overset{*}{\times} b)' \overset{*}{\times} c \overset{*}{+} (a \overset{*}{\times} b) \overset{*}{\times} c' \overset{*}{+} (a \overset{*}{\times} b)' \overset{*}{\times} c'\} \\
&\quad \overset{(\clubsuit)}{=} \mathrm{mex}\{(a' \overset{*}{\times} b \overset{*}{+} a \overset{*}{\times} b' \overset{*}{+} a' \overset{*}{\times} b') \overset{*}{\times} c \overset{*}{+} (a \overset{*}{\times} b) \overset{*}{\times} c' \overset{*}{+} (a' \overset{*}{\times} b \overset{*}{+} a \overset{*}{\times} b' \overset{*}{+} a' \overset{*}{\times} b') \overset{*}{\times} c'\} \\
&\quad \overset{*}{=} \mathrm{mex}\{a \overset{*}{\times} (b' \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c' \overset{*}{+} b' \overset{*}{\times} c') \overset{*}{+} a' \overset{*}{\times} (b \overset{*}{\times} c) \overset{*}{+} a' \overset{*}{\times} (b' \overset{*}{\times} c \overset{*}{+} b \overset{*}{\times} c' \overset{*}{+} b' \overset{*}{\times} c')\} \\
&\quad \overset{(\diamondsuit)}{=} \mathrm{mex}\{a \overset{*}{\times} (b \overset{*}{\times} c)' \overset{*}{+} a' \overset{*}{\times} (b \overset{*}{\times} c) \overset{*}{+} a' \overset{*}{\times} (b \overset{*}{\times} c)'\} \\
&\quad = a \overset{*}{\times} (b \overset{*}{\times} c)
\end{aligned}$$

と示される．ここで, 最初の等号と最後の等号はニム積の定義による。(♣) の等号は, (iv) の証明中の (♠) の場合と同様である．(♢) は (♣) と全く同様である。 □

上の命題によって, 非負整数の集合 $\mathbb{N}$ はニム和・ニム積について標数 2 の整域をなすことが証明されました。定理 7.1 が主張するように， $\mathbb{N}$ はニム和・ニム積について体をなすのですが、より詳しく次の定理が成り立ちます.

定理 7b.2 （定理 7.1 の詳細版） 任意の $m \geq 0$ に対し，$K_m = \{0, 1, \ldots, 2^{2^m} - 1\}$ とおく．K_m は有限体（2^{2^m} 元体）をなし，K_{m+1} は K_m の 2 次拡大体で,

$$K_{m+1} = K_m \overset{*}{\times} 2^{2^m} \overset{*}{+} K_m$$

となる．また，2^{2^m} の体 K_m 上の定義方程式は,

$$x \overset{*}{\times} x \overset{*}{+} x \overset{*}{+} 2^{2^m - 1} = 0$$

で与えられる．従って，$\mathbb{N} = \bigcup_{m=0}^{\infty} K_m$ は標数 2 の素体 $K_0 = \{0, 1\}$ 上の無限次代数拡大体となる.

定理の証明の前に, 一つ補題を用意しておきます.

補題 7b.3 $\Delta \in \mathbb{N}$ に対し, $[\Delta] = \{0, 1, 2, \ldots, \Delta - 1\}$ とおく．もし, $[\Delta]$ がニム和・ニム積について体をなすならば,

$$\delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2 = \delta_1 \Delta + \delta_2 \quad (\delta_1, \delta_2 \in [\Delta])$$

が成り立つ．ここで, 右辺の演算は整数の通常の和, 積を考えている.

【証明】　$\delta_1 = 0$ ならば明らかに成り立っているから, δ_1, δ_2 に関する二重の帰納法で証明する.

$$\begin{aligned}(\delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2)' &= (\delta_1 \overset{*}{\times} \Delta)' \overset{*}{+} \delta_2,\ \delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2' \\ &= \delta_1' \overset{*}{\times} \Delta \overset{*}{+} \delta_1 \overset{*}{\times} \delta_3 \overset{*}{+} \delta_1' \overset{*}{\times} \delta_3 \overset{*}{+} \delta_2,\ \delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2' \quad (\delta_3 < \Delta) \\ &= \delta_1' \overset{*}{\times} \Delta \overset{*}{+} (\delta_1 \overset{*}{+} \delta_1') \overset{*}{\times} \delta_3 \overset{*}{+} \delta_2,\ \delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2'\end{aligned}$$

である. ここで, $\delta_1 > 0$ であり、したがって, $\delta_1 \overset{*}{+} \delta_1' \neq 0$ としてよいから, $[\Delta]$ が体をなすという仮定により, $\delta_1 \overset{*}{+} \delta_1'$ は可逆であり, $(\delta_1 \overset{*}{+} \delta_1') \overset{*}{\times} \delta_3 \overset{*}{+} \delta_2$ は Δ より小さい任意の元を表せる. したがって,

$$(\delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2)' = \delta_1' \overset{*}{\times} \Delta \overset{*}{+} \delta_3,\ \delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2'$$

となる. この右辺に帰納法の仮定を用いれば,

$$(\delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2)' = \delta_1'\Delta + \delta_3,\ \delta_1\Delta + \delta_2'$$

となり, 右辺は $\delta_1\Delta + \delta_2$ より小さい任意の $\mathbb{N}$ の元を表せる. よって,

$$\delta_1 \overset{*}{\times} \Delta \overset{*}{+} \delta_2 = \delta_1\Delta + \delta_2$$

が成り立つ. □

【定理の証明】　K_m に関する主張を m についての数学的帰納法で証明しよう. $K_0 = \{0, 1\}$, $K_1 = \{0, 1, 2, 3\}$ であり, $\overset{*}{\times}$ の積表（連載第 7 回、10 月号、第 2 節）を見れば, K_0, K_1 が体となっていることは容易に確認できる. また, $2 \overset{*}{\times} 2 = 3 = 2 \overset{*}{+} 1$ である, $m \geq 1$ とし, K_m が体で $x = 2^{2^{m-1}}$ が $x \overset{*}{\times} x \overset{*}{+} x \overset{*}{+} 2^{2^{m-1}-1} = 0$ を満たしていると仮定する. このとき, $x = 2^{2^m}$ が

$$(\sharp) \qquad x \overset{*}{\times} x \overset{*}{+} x \overset{*}{+} 2^{2^m-1} = 0$$

を満たすことを示せばよい. もし, $x = 2^{2^m}$ に対し $(\sharp)$ が成り立っていれば, $K_m(2^{2^m})$ は K_m の二次拡大体で

$$K_m(2^{2m}) = \left\{ \delta_1 \overset{*}{\times} 2^{2^m} + \delta_2 \;\middle|\; \delta_1, \delta_2 \in K_m \right\}$$

であり, 補題 7b.3 により, 右辺の集合は

$$\left\{ \delta_1 \overset{*}{\times} 2^{2^m} \overset{*}{+} \delta_2 \;\middle|\; \delta_1, \delta_2 \in K_m \right\} = \left\{ \delta_1 2^{2^m} + \delta_2 \;\middle|\; \delta_1, \delta_2 < 2^{2^m} \right\} = [2^{2^m}] = K_{m+1}$$

となり, K_{m+1} が体であることがわかる. そこで, $(\sharp)$ を証明しよう.

$$(2^{2^m} \overset{*}{\times} 2^{2^m})' = \delta_1 \overset{*}{\times} 2^{2^m} \overset{*}{+} 2^{2^m} \overset{*}{\times} \delta_2 \overset{*}{+} \delta_1 \overset{*}{\times} \delta_2 = (\delta_1 \overset{*}{+} \delta_2) \overset{*}{\times} 2^{2^m} \overset{*}{+} \delta_1 \overset{*}{\times} \delta_2 \quad (\delta_1, \delta_2 < 2^{2^m})$$

したがって, $\alpha_1 \overset{*}{\times} 2^{2^m} \overset{*}{+} \alpha_2 = \alpha_1 2^{2^m} + \alpha_2$ $(\alpha_1, \alpha_2 < 2^{2^m})$ が $(2^{2^m} \overset{*}{\times} 2^{2^m})'$ の中に現れるには, $x \overset{*}{\times} x \overset{*}{+} \alpha_1 \overset{*}{\times} x \overset{*}{+} \alpha_2 = 0$ が K_m において解を持つことが必要十分である. 下の補題により, K_m で解を持たないような最初の α_1, α_2 は $\alpha_1 = 1$, $\alpha_2 = 2^{2^m-1}$ である. したがって, $2^{2^m} \overset{*}{\times} 2^{2^m} = 2^{2^m} + 2^{2^m-1}$ となる. □

補題 7b.4 K_m は体であり、$2^{2^{m-1}} \overset{*}{\times} 2^{2^{m-1}} = 2^{2^{m-1}} + 2^{2^{m-1}-1}$ が成り立つことがすでに証明されているとする. このとき,

(i) $x^2 + a = 0$ $(a \in K_m)$ は常に唯一つの解を持つ.

(ii) $\phi : K_m \to K_m$ を $\phi(x) = x \overset{*}{\times} x \overset{*}{+} x$ と定義すると, ϕ は加法群の準同型で,

$$\mathrm{Ker}(\phi) = \{0, 1\}, \quad \mathrm{Im}(\phi) = \{0, 1, \ldots, 2^{2^m-1} - 1\}$$

である.

【証明】 (i) は、標数 2 の有限体の一般的性質である. ($x \mapsto x^2$ が $K_m^\times$ の自己同型を与えているから.)

(ii) 標数 2 であるから, ϕ が加法群の準同型となることは容易にわかる. また, $\mathrm{Ker}(\phi)$ は 2 次方程式の解集合であるから位数は 2 であり, $\{0, 1\}$ に一致することも容易にわかる. 最後に $\mathrm{Im}(\phi)$ についての主張を m に関する帰納法で示そう. K_m の元 α は $\alpha = \alpha_1 2^{2^{m-1}} + \alpha_2$ $(\alpha_1, \alpha_2 < 2^{2^{m-1}})$ と書くことができる. ここで, 補題 7b.3 により, 和・積は通常の整数の和・積として考えても, ニム和・ニム積として考えてもよいことに注意する. このとき,

$$\begin{aligned}
\alpha \overset{*}{\times} \alpha \overset{*}{+} \alpha &= (\alpha_1 \overset{*}{\times} \alpha_1 \overset{*}{\times} 2^{2^{m-1}} \overset{*}{\times} 2^{2^{m-1}} \overset{*}{+} \alpha_2 \overset{*}{\times} \alpha_2) \overset{*}{+} \alpha_1 \overset{*}{\times} 2^{2^{m-1}} \overset{*}{+} \alpha_2 \\
&= (\alpha_1 \overset{*}{\times} \alpha_1 \overset{*}{\times} (2^{2^{m-1}} \overset{*}{+} 2^{2^{m-1}-1}) \overset{*}{+} \alpha_2 \overset{*}{\times} \alpha_2) \overset{*}{+} \alpha_1 \overset{*}{\times} 2^{2^{m-1}} \overset{*}{+} \alpha_2 \\
&= \phi(\alpha_1) \overset{*}{\times} 2^{2^{m-1}} \overset{*}{+} \alpha_1 \overset{*}{\times} \alpha_1 \overset{*}{\times} 2^{2^{m-1}-1} \overset{*}{+} \phi(\alpha_2)
\end{aligned}$$

ここで, 帰納法の仮定により, $\phi(\alpha_1), \phi(\alpha_2) < 2^{2^{m-2}}$ であり, 補題 7b.3 により,

$$\phi(\alpha_1) \overset{*}{\times} 2^{2^{m-1}} = \phi(\alpha_1) 2^{2^{m-1}} < 2^{2^{m-2}} \cdot 2^{2^{m-1}} = 2^{2^{m-2}+2^{m-1}} < 2^{2^m-1},$$

$$\alpha_1 \overset{*}{\times} \alpha_1 \overset{*}{\times} 2^{2^{m-1}-1} < 2^{2^{m-1}} \overset{*}{\times} 2^{2^{m-1}-1} = 2^{2^m-1}, \quad \phi(\alpha_2) < 2^{2^{m-2}}$$

となるから, $\phi(\alpha) < 2^{2^m-1}$ である. $|\mathrm{Im}(\phi)| = 2^{2^m-1}$ だから, $\mathrm{Im}(\phi) = \{0, 1, \ldots, 2^{2^m-1} - 1\}$ であることが分かる. □

定理 7.2 は以上の議論に実質的には含まれています。

定理 7.2 ニム積について、次の等式が成立する。

$$\delta_1 \overset{*}{\times} 2^{2^m} \overset{*}{+} \delta_2 = \delta_1 2^{2^m} + \delta_2 \quad (\delta_1, \delta_2 < 2^{2^m}),$$

$$2^{2^m} \overset{*}{\times} 2^{2^m} = 2^{2^m} + 2^{2^m-1}, \quad 2^{2^m} \overset{*}{\times} 2^{2^n} = 2^{2^m+2^n} \ (m \neq n)$$

【証明】 第 1、第 3 の等式は、K_m が体をなすこと（定理 7b.2）より、補題 7b.3 から従う。第 2 の等式は、定理 7b.2 で与えられた $x = 2^{2^m}$ の体 K_m 上の定義方程式そのものである。 □