暗号の数理問題解説 #2

河野

演習問題 1.1　$A=\{a,b,c\}$ とする。A の 2 項演算は全部で何個存在するか?

有限集合 A の個数を $|A|$ で表す。次の命題を使用する。「A,B を有限集合とするとするとき，A から B への写像 $f:A\to B$ は全部で $|B|^{|A|}$ 個ある。」知らない人のために証明を書いておく。内容を理解している人は飛ばして演習問題の解説へ。$|A|=m$ とし，$A=\{a_1,a_2,\ldots,a_m\}$，$|B|=n$ とし，$B=\{b_1,b_2,\ldots,b_n\}$ としておく。写像を決めるためには元の行き先を決めればよい。a_1 の行き先 $f(a_1)$ は $b_1,b_2,\ldots,b_n$ の n 通りの可能性がある。a_2 の行き先 $f(a_2)$ は $b_1,b_2,\ldots,b_n$ の n 通りの可能性がある。以下同様に a_m の行き先 $f(a_m)$ は $b_1,b_2,\ldots,b_n$ の n 通りの可能性がある。よってすべての写像は

$$\underbrace{n\times n\times\cdots\times n}_{m\text{ 個}}$$

存在することが分かる。

$|A|=3$ なので $|A\times A|=3\times 3=9$ である。2 項演算は $A\times A$ から A への写像なので全部で 3^9 個存在する。

演習問題 1.2　$A=\{a,b\}$ とする。A の演算で結合律を満たすようなものをすべて列挙せよ。

場合分けをしていけばできるが，なるべく効率よく実行したい。$a\cdot a=a$ を $(1a)$ と書く。以下

$$\begin{array}{llll} a\cdot a=a & (1a) & a\cdot a=b & (1b)\\ a\cdot b=a & (2a) & a\cdot b=b & (2b)\\ b\cdot a=a & (3a) & b\cdot a=b & (3b)\\ b\cdot b=a & (4a) & b\cdot b=b & (4b) \end{array}$$

と書く。1 から 4 に対し a または b が指定されたものを演算表と呼ぶ。演算を 1 つ決めるには例えば $(1a)+(2b)+(3b)+(4a)$ のように 4 つのルールを決めればよい。$\overline{a}=b,\overline{b}=a$ とおく。ある演算 $(1x_1)+(2x_2)+(3x_3)+(4x_4)$ が結合律を満たしているとする。演算表において a と b をすべて入れ替えた演算も結合律を満たす。即ち $(4\overline{x_1})+(3\overline{x_2})+(2\overline{x_3})+(1\overline{x_4})$ も結合律をみたす。また演算表において $x\cdot y$ を $y\cdot x$ に入れ替えた演算も結合律を満たす。即ち $(1x_1)+(2x_3)+(3x_2)+(4x_2)$ も結合律を満たす。以上のことを踏まえで場合分けを実行する。

$(2a)+(3b)$ が選択されていて結合律が成立しているとする。即ち $a\cdot b=a$, $b\cdot a=b$ が成立している。$a\cdot a=(ab)a=a(ba)=ab=a$ より $(1a)$ が成立しなければならない。また $b\cdot b=(ba)b=b(ab)=ba=b$ より $(4b)$ が成立する。このときは $(1a)+(2a)+(3b)+(4b)$ で結合律をみたす。前に述べたことより $(1a)+(2b)+(3a)+(4b)$ も同様である。

次に $(2a)+(3a)$ を考える。このとき $(1a)+(2a)+(3a)+(4a)$ はすべての計算結果が a になるので結合律を満たす。$(1a)+(2a)+(3a)+(4b)$ は $a=0,b=1$ の例を考えれば分かるように結合律を満たす。よって $(1b)+(2b)+(3b)+(4b)$ および $(1a)+(2b)+(3b)+(4b)$ も結合律を満たす。よって残っているのは $(1b)+(2a)+(3a)$ の場合である。$(1b)+(2a)+(3a)+(4a)$ の場合は結合律を満

たせば $b = aa = (ba)a = b(aa) = bb = a$ となるので結合律はみたさない。$(1b)+(2a)+(3a)+(4b)$ の場合は結合律を満たす (各自チェックを)。よって $(1a)+(2b)+(3b)+(4a)$ も結合律を満たす。以上が結合律をみたす演算である。

演習問題 1.3　$GL(n;\mathbb{R})$ および $GL(n;\mathbb{C})$ が群になることを示せ。

$M(\mathbb{R})$ および $M(\mathbb{C})$ をそれぞれ成分が実数または複素数である n 次行列全体がつくる集合とする。n 次行列演算が定義されていることは，n 次行列と n 次行列の積が n 次行列になること，および成分が実数または複素数の行列の積はやはり成分が実数または複素数になることから従う。結合法則は線型代数で学んだように成立する。証明を一応書いておこう。$A = [a_{ij}], B = [b_{ij}], C = [c_{ij}]$ を $M(\mathbb{R})$ または $M(\mathbb{C})$ の元とすると

$$(AB)C = ([a_{ij}][b_{ij}])\,[c_i j] = \left[\sum_{s=1}^{n} a_{is}b_{sj}\right][c_{ij}] = \left[\sum_{t=1}^{n}\sum_{s=1}^{n}(a_{is}b_{st})c_{tj}\right]$$
$$= \left[\sum_{s=1}^{n}\sum_{t=1}^{n} a_{is}(b_{st}c_{tj})\right] = [a_{ij}]\left[\sum_{t=1}^{n} b_{it}c_{tj}\right] = A(BC)$$

単位元は $E = [\delta_{ij}]$ である。ここで δ_{ij} はクロネッカーのデルタである。$EE = E$ なので E は正則行列である。よって $E \in GL(n;\mathbb{R})$ および $E \in GL(n;\mathbb{C})$ となる。また $A, B \in GL(n;\mathbb{R})$ のとき逆行列 A^{-1} および B^{-1} が存在する。このとき $A^{-1} \in GL(n;\mathbb{R})$ である。$(AB) = B^{-1}A^{-1}$ なので AB の逆行列も存在する。よって $AB \in GL(n;\mathbb{R})$ である。以上により $GL(n;\mathbb{R})$ は群になる。$GL(n;\mathbb{C})$ についても同様に証明できる。

演習問題 1.4

(1) $A = \{a, b\}$ とする。A 結合律を満たす演算のうち，a を単位元とするものをすべて列挙せよ。

(2) A の結合律を満たし，a を単位元とする演算の中で群となる演算は何通りか？

(3) $G = \{\, e, a, b, c \,\}$ を 4 個の元からなる集合とする。G 上の演算で群になるものをすべて列挙せよ。ただし e は単位元とする。

(4) $A_n = \{a_1, \cdots, a_n\}$ を n 個の要素から成る集合とする。A_n には何通りの 2 項演算が定義可能か？

(5) $SL(n;\mathbb{K})$ が $GL(n;\mathbb{K})$ の部分群であることを示せ。

(6) 命題 1.16 を証明せよ。

(1)　演習問題 1.2 の解説中の記号を使う。a が単位元になるためには $aa = a, ab = b, ba = b$ が成立する必要がある。即ち $(1a)+(2b)+(3b)$ が必要である。これを満たすのは $(1a)+(2b)+(3b)+(4a)$ と $(1a)+(2b)+(3b)+(4b)$ である。
(2)　前問の結果より可能性は 2 通りである。$(1a)+(2b)+(3b)+(4b)$ が群演算を定義すると仮定する。$bb = b$ の両辺に b の逆元 b^{-1} をかけると $b = ba = b(bb^{-1}) = (bb)b^{-1} = bb^{-1} = a$ となり矛盾よって $(1a)+(2b)+(3b)+(4b)$ は群にならない。$(1a)+(2b)+(3b)+(4a)$ が群になることのチェックは各自にまかせる。

(3) 最初に次が成立することに注意する。「$xy = x \implies y = e$ および $xy = y \implies x = e$」群なので逆元を左または右からかけることで示される。

次の 2 つの場合に分ける。

(A) $x \neq e$ (単位元) となる x で $x^2 \neq e$ を満たす元が存在する。

(B) 任意の $x \neq e$ に対し $x^2 = e$ となる。

(A) の場合 $x^3 \neq e$ が成立することを示す。$x^3 = e$ が成立するとする。e, x, x^2 は異なる G の元なのでこれ以外の元 y が G には存在する。このとき最初に述べたことより $xy \neq x$ かつ $xy \neq y$ が成立する。$xy = e$ のとき $y = x^{-1} = x^{-1}e = x^{-1}x^3 = x^2$ となり矛盾。$xy = x^2$ のとき $x = y$ となり矛盾。よって $x^3 \neq e$ である。以上により $G = \left\{ e, x, x^2, x^3 \right\}$ となることが分かる。a, b, c との関係は $(x, x^2, x^3) = (a, b, c)$ または $(a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$ の 6 通りがある。

次に (B) のとき $a^2 = b^2 = e$ が成立している。このとき $ab \neq a$ かつ $ab \neq b$ である。$ab = e$ が成立すると，$a = b^{-1} = b^{-1}e = b^{-1}b^2 = b$ となり矛盾。よって $ab = c$ である。この場合演算は一意的に決まる。

(4) $|A| = n$，$|A \times A| = n^2$ である。演習問題 1.1 の解説で述べたことから 2 項演算は全部で n^{n^2} ある。

(5) H が G の部分群であることを示すためには命題 1.15 または命題 1.16 の条件を満たすことをチェックすればよい。ここでは命題 1.15 を用いる。線型代数で学んだ行列式の性質 $|AB| = |A|\,|B|$ (ここで $|A|$ は行列 A の行列式) を使う。

$A.B \in SL(n;\mathbb{K})$ に対し $|A| = 1, |B| = 1$ が成立している。このとき $|AB| = |A|\,|B| = 1 \cdot 1 = 1$ なので $A \in SL(n;\mathbb{K})$ となる。また $|A| = 1$ のとき逆行列 A^{-1} が存在して $AA^{-1} = E$ が成立する。$|E| = 1$ なので $1 = |E| = |AA^{-1}| = |A|\,|A^{-1}] = 1 \cdot |A^{-1}] = |A^{-1}]$ より $A^{-1} \in SL(n;\mathbb{K})$ となる。

(6) 命題 1.16 を示すためには

$$\text{命題 1.15 の (1) かつ (2)} \iff \text{命題 1.16 の } (*)$$

を示せばよい。

命題 1.15 の (1) かつ (2) が成立しているとする。このとき H の任意の元 a, b に対し (2) より $b^{-1} \in H$ が成立する。a と b^{-1} に (2) を適用すると $ab^{-1} \in H$ となり $(*)$ が成立する。

命題 1.16 の $(*)$ が成立しているとする。H の任意の元 a を考える。このとき $e = aa^{-1} \in H$ である。e と a に $(*)$ を用いると $a^{-1} = ea^{-1} \in H$ となり (2) が成立する。H の任意の元を a, b とする。今示したことより $b^{-1} \in H$ である。a と b^{-1} に $(*)$ を適用すると $ab = a\left(b^{-1}\right)^{-1} \in H$ となり (1) が成立する。

演習問題 1.5

(1) $A = \{ a, b, c \}$ とする。A 上の 2 項関係は何種類存在するか答えよ。

(2) $A = \{ a_1, a_2, \ldots, a_n \}$ とする。A 上の 2 項関係は何種類存在するか答えよ。

(3) $A = \{ a, b, c \}$ 上の 2 項関係で同値関係になるものは何種類あるか答えよ。またそれぞれに対し完全代表系を 1 つ選べ。

(1) A 上の 2 項関係は $A \times A$ の部分集合 R を指定することなので，R の個数だけ関係が存在する。$|A \times A| = 9$ なのでこの個数は 2^9 である。ここで集合 A が $|A| = n$ のとき A の部分集合は全部で 2^n 個あるということを用いた。

(2) $|A| = n$ だから 2^{n^2} 個である。
(3) 関係をすべて列挙するのは一般に難しいが，同値関係の場合同値類分割と対応することに注意する。即ち A のグループへの分割が 1 つあると同値関係が 1 つ定まる。逆に同値関係が 1 つあるとグループへの分割が 1 つ定まる。この対応は一対一である。グループへの分割は (1) $A_1 = \{a, b, c\}$，(2) $A_1 = \{a, b\}, A_2 = \{c\}$，(3) $A_1 = \{a, c\}, A_2 = \{b\}$，(4) $A_1 = \{b, c\}, A_2 = \{a\}$，(5) $A_1 = \{a\}, A_2 = \{b\}, A_3 = \{c\}$ の 5 通りがある。よって同値関係も 5 種類存在する。

演習問題 1.6　整数 $\mathbb{Z}$ 上の関係 R が同値関係になるかどうか調べよ。同値関係になるときは証明し，そうでないときは反例をあげよ。また同値関係になるときは完全代表系を 1 つ選べ。

(1) $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m + n \text{ は } 5 \text{ で割り切れる}\}$

(2) $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m - n \text{ は } 5 \text{ で割り切れる}\}$

(3) $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid mn \text{ は } 5 \text{ で割り切れる}\}$

反射律，対称律，推移律の 3 つが成立するかどうかを調べればよい。関係を '$\sim$' で書く。
(1) $1 \in \mathbb{Z}$ とすると $1 + 1$ は 5 で割り切れないので $1 \not\sim 1$ である。反射律が成立しない。よって同値関係ではない。
(2) 任意の $n \in \mathbb{Z}$ に対し $n - n = 0$ は 5 で割り切れる。よって $n \sim n$ である。反射律は成立する。任意の $m, n \in \mathbb{Z}$ に対し $m \sim n$ が成立しているとする。よってある整数 k が存在して $m - n = 5k$ と書ける。このとき $n - m = 5(-k)$ となるので $n \sim m$ となる。対称律も成立している。任意の $\ell, m, n \in \mathbb{Z}$ に対し $\ell \sim m$ かつ $m \sim n$ が成立しているとする。このとき整数 $k_1, k_2 \in \mathbb{Z}$ が存在して $\ell - m = 5k_1$ かつ $m - n = 5k_2$ となっている。このとき $\ell - n = (\ell - m) + (m - n) = 5k_1 + 5k_2 = 5(k_1 + k_2)$ となる。$k_1 + k_2 \in \mathbb{Z}$ なので $\ell \sim n$ となる。よって推移律も成立している。よって同値関係である。
(3) $1 \in \mathbb{Z}$ に対し $a \cdot 1 = 1$ は 5 で割り切れないので $1 \not\sim 1$ である反射律が成立しない。よって同値関係ではない。