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　$\mathbb{Z}$ が加法に関して群になることを示せ。$\mathbb{R}^*$ が乗法に関して群になることを示せ。

数の和・積の性質は既知とする。即ち和・積の結合法則等は成立を仮定する。

最初は $\mathbb{Z}$ が和に関して群をなすことを証明する。結合法則は既知としたので単位元だが，これは 0 がその性質を持つ。任意の整数 a に対し

$$a+0=0+a=a$$

が成立し，$0\in\mathbb{Z}$ なので単位元は存在する。$a\in\mathbb{Z}$ の逆元にあたるのが $-a$ であり，$a\in\mathbb{Z} \implies -a\in\mathbb{Z}$ なので任意の元 a に対し，a 逆元 $-a\in\mathbb{Z}$ が存在する。よって $\mathbb{Z}$ は和に関して群をなす。

次に $\mathbb{R}^*=\{\,x\in\mathbb{R}\mid x\neq 0\,\}$ を考える。演算は乗法である。結合法則は同様に既知とした。単位元は 1 がそれである，任意 $x\in\mathbb{R}^*$ に対し

$$x\cdot 1=1\cdot x=x$$

なので $1\in\mathbb{R}^*$ が単位元になる。x の逆元は $x\neq 0$ より $x'=\dfrac{1}{x}$ とおくと，$x'\in\mathbb{R}^*$ であり，

$$x\cdot x'=x'\cdot x=1$$

となるので逆元が存在する。

演習問題 1.4　次を示せ。ただし n 次行列 A,B,C に対し結合法則 [$(AB)C=A(BC)$] が成立することなど線型代数の知識は既知としてよい。

(1) $GL(2;\mathbb{R})$ および $GL(2;\mathbb{Q})$ が群になることを示せ。

(2) $M_n(\mathbb{Z})$ を成分が整数である n 次行列全体の集合とする。$GL(n;\mathbb{Z})=\{\,A\in M_n(\mathbb{Z})\mid \det A\neq 0\,\}$ とすると，行列の積という演算に関して $GL(2;\mathbb{Z})$ は群にならないことを示せ。

(1)　$M(\mathbb{R})$ 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

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

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。

(2) 積は入るが逆元が $\mathrm{GL}(2;\mathbb{Z})$ に存在しない。$A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ とすると $\det A = 4 \neq 0$ なので $A \in \mathrm{GL}(2;\mathbb{Z})$ である。A の逆元 A^{-1} は $A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ とならなければならない。しかし $\dfrac{1}{2} \notin \mathbb{Z}$ なので $A^{-1} \notin \mathrm{GL}(2;\mathbb{Z})$ である。よって群にはならない。

演習問題 1.5　S_n が群になることを証明せよ。

$\sigma \in S_n$ を $P_n = \{1, 2, \ldots, n\}$ から P_n への全単射と見る。

$$\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$$

積は合成写像である。数学序論で学んだように全単射と全単射の合成写像は全単射である。よって $\forall \sigma, \tau \in S_n$ に対し $\sigma \circ \tau \in S_n$ となる。

任意の元 $\sigma, \tau, \rho \in S_n$ と任意の $k \in P_n$ に対し

$$\begin{aligned} \sigma \circ (\tau \circ \rho)(k) &= \sigma(\tau \circ \rho(k)) = \sigma(\tau(\rho(k))) \\ &= \sigma \circ \tau(\rho(k)) = (\sigma \circ \tau) \circ \rho(k) \\ &= \big((\sigma \circ \tau) \circ \rho\big)(k) \end{aligned}$$

となるので $\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho$ となり，結合法則が成立する。id を恒等写像，即ち任意の $k \in P_n$ に対し $id(k) = k$ となる写像とすると $id \in S_n$ であり，任意の $\sigma \in S_n$ と任意の $k \in P_n$ に対し

$$\sigma \circ id(k) = \sigma(id(k)) = \sigma(k)$$
$$\mathrm{id} \circ \sigma(k) = id(\sigma(k)) = \sigma(k)$$

が成立するので $\sigma \circ id = id \circ \sigma = \sigma$ が成立する。よって id は単位元である。$\sigma \in S_n$ に対し σ は全単射なので逆写像 σ^{-1} が存在して $\sigma^{-1} \in S_n$ となる。このとき $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = id$ となるので σ^{-1} は逆元である。

演習問題 1.6　$m\mathbb{Z}$ が群になることを示せ。

数の和に関して結合法則の成立は既知とする。$\forall n_1, n_2 \in m\mathbb{Z}$ とすると，ある整数 $k_1, k_2 \in \mathbb{Z}$ が存在して $n_1 = mk_1, n_2 = mk_2$ となる。

$$n_1 + n_2 = mk_1 + mk_2 = m(k_1 + k_2)$$

であり，$k_1 + k_2 \in \mathbb{Z}$ なので $n_1 + n_2 \in m\mathbb{Z}$ となる。よって $m\mathbb{Z}$ において和が定義される。

$0 = m0 \in m\mathbb{Z}$ なので $m\mathbb{Z}$ に単位元は存在する。

n を $m\mathbb{Z}$ の任意の元とすると，ある整数 $k \in \mathbb{Z}$ が存在して $n = mk$ と書ける。このとき $-k \in \mathbb{Z}$ なので $-n = m(-k) \in m\mathbb{Z}$ となる。$n + (-n) = (-n) + n = 0$ なので $-n$ は逆元である。逆元も存在するので $m\mathbb{Z}$ は群になる。

演習問題 1.7　$SL(2;\mathbb{Z})$ が群になることを示せ。

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}(2;\mathbb{Z})$ とすると $a,b,c,d,p,q,r,s \in \mathbb{Z}$ であり，$\det A = \det B = 1$ である。

$$AB = \begin{pmatrix} ap+br & aq+bs \\ cp+rd & cq+ds \end{pmatrix}$$

なので AB の成分は整数である。また $\det(AB) = \det A \det B = 1 \cdot 1 = 1$ なので $AB \in \mathrm{SL}(2;\mathbb{Z})$ である。行列の積に関して結合法則が成立するのはすでに線形代数で学んでおり，演習問題 1.4 でも一般の場合に証明してあるが，$n = 2$ の場合具体的に証明を書いておく。A, B を前のもの $C = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ とすると

$$\begin{aligned} A(BC) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} px+qz & py+qw \\ rx+sz & ry+sw \end{pmatrix} \\ &= \begin{pmatrix} a(px+qz)+b(rx+sz) & a(py+qw)+b(ry+sw) \\ c(px+qz)+d(rx+sz) & c(py+qw)+d(ry+sw) \end{pmatrix} \\ &= \begin{pmatrix} (ap+br)x+(aq+bs)z & (ap+br)y+(aq+bs)w \\ (cp+dr)x+(cq+ds)z & (cp+dr)y+(cq+ds)w \end{pmatrix} \\ &= \begin{pmatrix} ap+br & aq+bs \\ cp+rd & cq+ds \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} \\ &= (AB)\,C \end{aligned}$$

$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ とすると $1, 0 \in \mathbb{Z}$ であり $\det E = 1$ なので $E \in \mathrm{SL}(2;\mathbb{Z})$ である。$AE = EA = A$ が成立するので E は $\mathrm{SL}(2;\mathbb{Z})$ の単位元である。$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対し $A^{-1} = \dfrac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ となるのが $A \in \mathrm{SL}(2;\mathbb{Z})$ より $a,b,c,d \in \mathbb{Z}$ であり，$\det A = 1$ である。このとき $-b, -c \in \mathbb{Z}$ なので $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathrm{SL}(2;\mathbb{Z})$ となる。$AA^{-1} = A^{-1}A = E$ なので A の逆元も $\mathrm{SL}(2;\mathbb{Z})$ に存在する。

演習問題 *1.8　$SL(n;\mathbb{Z})$ が群になることを示せ。

積が $\mathrm{SL}(n;\mathbb{Z})$ に入るのは $\mathrm{SL}(2;\mathbb{Z})$ と同様に証明できる。結合法則は演習問題 1.4 で示してある。$E = (\delta_{ij})$ (δ_{ij} はクロネッカーのデルタ) とすると $EA = AE = A$ となるは線形代数で学んだが一応書いておく。

$$AE = (a_{ij})(\delta_{ij}) = \left(\sum_{s=1}^{n} a_{is}\delta_{sj}\right) = (a_{ij}) = A$$

$$EA = (\delta_{ij})(a_{ij}) = \left(\sum_{s=1}^{n} \delta_{is}a_{sj}\right) = (a_{ij}) = A$$

$1, 0 \in \mathbb{Z}$ かつ $\det E = 1$ なので $E \in \mathrm{SL}(n;\mathbb{Z})$ であり，E は単位元である。

線型代数で学んだように $A^{-1} = \dfrac{1}{\det A}\widetilde{A}$ である。ここで $\widetilde{A}$ は余因子行列である。今 $A \in \mathrm{SL}(2;\mathbb{Z})$ なので $\det A = 1$，よって $A^{-1} = \widetilde{A}$ である。余因子は成分の積と和で書かれるので整数である。よって $\widetilde{A}$ の成分は整数である。また $AA^{-1} = E$ より $\det A \det A^{-1} = \det E = 1$ なので $\det A^{-1} = 1$ である。よって $A^{-1} \in \mathrm{SL}(2;\mathbb{Z})$ である。

演習問題 1.9　命題 1.15 を証明せよ。

命題 1.15 を示すためには

$$\text{命題 1.14 の (1) かつ (2)} \iff \text{命題 1.15 の } (*)$$

を示せばよい。

命題 1.14 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 1.15 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 1.10

(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) $A = \{a, b, c\}$ 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，$A \times A$ の部分集合 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)　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 1.11　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) $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m + n \text{ は 5 で割り切れる}\}$

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

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

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 $1 \cdot 1 = 1$ 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。