

行列による自由モノイド

hora-algebra

May 7, 2022

1 問題

二つの 2×2 行列 A_0, A_1 であって, A_0, A_1 を好きな順で好きな回数掛け合わせたとき, 積として出来上がった行列から掛けた順番と回数を復元できるようなものは, どんな体の上で存在するだろうか. この問題を二通りの (もちろん同値な) 方法で書いておく. 一つ目はモノイドの言葉を明示的に使った方法である.

Question 1.0.1. K を体とする. K 上の 2×2 正方行列と積の為すモノイド $M_2(K)$ が階数 2 の自由モノイドを部分モノイドとしてもつための K についての必要十分条件を求めよ.

二つ目はもう少し初等的な書き方である.

Question 1.0.2. K を体とする. K 上の 2×2 正方行列 A_0, A_1 であって, 次の条件を満たすものが存在するための K についての必要十分条件を求めよ.

条件 $0, 1$ からなる有限文字列の集合 $\coprod_{n=0}^{\infty} \{0, 1\}^n$ から $M_2(K)$ への写像 $\coprod_{n=0}^{\infty} \{0, 1\}^n \rightarrow M_2(K) : (i_1, \dots, i_n) \mapsto A_{i_1} \dots A_{i_n}$ が単射である

例を挙げておく.

Example 1.0.3 (有限体). K が有限体なら, $M_2(K)$ は有限集合なので条件を満たさない.

Example 1.0.4 (有限体の代数拡大). 上の例は少し一般化できる. K の標数が正 ($p > 0$) でさらに素体 $\mathbb{F}_p$ 上代数的だとする. このとき $M_2(K)$ の元 A_0, A_1 を任意にとると, A_0, A_1 の 8 つの成分で $\mathbb{F}_p$ 上生成される中間体 $\mathbb{F}_p \subset L \subset K$ は有限体である. 従って $M_2(L)$ は有限集合になり, A_0, A_1 は条件を満たさない. 従って K は条件を満たさない.

Example 1.0.5 (ユークリッドの互除法). 標数 0 の体 K について $A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

と $A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ は条件を満たす二つの行列になっている. 実際, 長さ 2 の縦ベクトル $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ に左から A_0, A_1 を掛けることを考える. A_0 を左からかけることは下の成分を上成分に足すことに対応し, A_1 を左からかけることは上の成

分を下成分に足すことに対応する. v に左から A_0, A_1 を好きな順番で好きな回数かけると, 互いに素な正整数の組が出来上がる. 逆に, ユークリッドの互除法を考えることにより, 全ての互いに素な正整数の組は v に A_0, A_1 を左から掛ける方法で一意的に実現できる. つまり, **互いに素な正整数の組と二文字の有限文字列は, ユークリッドの互除法により一対一に対応する**. 例えば, 00101 という有限文字列は $A_0 A_0 A_1 A_0 A_1 v = \begin{pmatrix} 13 \\ 5 \end{pmatrix}$ に対応する. 逆方向の対応の例として, $\begin{pmatrix} 19 \\ 27 \end{pmatrix}$ をユークリッドの互除法で“復号”する. 大きい方から小さい方を引くことを $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ になるまで繰り返し, 上から下を引くなら 0 を, 下から上を引くなら 1 を記録する.

$$\begin{pmatrix} 19 \\ 27 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 19 \\ 8 \end{pmatrix} \xrightarrow{0} \begin{pmatrix} 11 \\ 8 \end{pmatrix} \xrightarrow{0} \begin{pmatrix} 3 \\ 8 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 3 \\ 5 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \xrightarrow{0} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \xrightarrow{1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

となり, 文字列 1001101 と対応する. 体 K の標数が 0 なら全ての正整数は互いに相異なるので, K は条件を満たす.

Remark 1.0.6 (別の次数と階数). この問題では, 2×2 行列の中で階数 2 の自由モノイドを作ること考えているが, 一般に $n \times n$ 行列の中で階数 m の自由モノイドを作ること考え得る. しかし, $n, m \geq 2$ なら結果は $n = 2, m = 2$ の場合と同じになる. 例えば, 階数 m の自由モノイドはそもそも階数 2 の自由モノイドの部分モノイドである.

Remark 1.0.7 (群として). 今回の問題では, モノイドの元として関係式を持たない二つの行列を考えているが, (仮に考えている行列が正則だったとしても) 群の元として関係式を持たないわけではない. 例えば, ユークリッドの互除法の例で挙げた標数 0 の体 K についての $A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ と $A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ が生成する群は (自由群ではなく) $SL_2(\mathbb{Z})$ である. 余談だが, 代わりに $B_0 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ と $B_1 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ を考えれば自由群を生成する. この SL_2 の部分自由群は Sanov 部分群と呼ばれている.

2 解答

実は, Remark 1.0.4 で挙げた体以外全ての体は条件を満たす, というのが結論である.

Proposition 2.0.1 (解答). 体 K についての求めている条件は, 以下のどちらかを満たすことである.

- K の標数は 0 である.
- K の標数は正 $p > 0$ であり, さらに K は素体 $\mathbb{F}_p$ 上超越的である.

証明の基本的なアイデアは、文字列の多項式への encoding である。安直に encoding するなら、文字列 00101 を多項式 $0x^4 + 0x^3 + 1x^2 + 0x^1 + 1x^0 (= x^2 + 1)$ へ変換したくなる。しかしこれでは先頭の 0 の分情報が落ちてしまうので、長さ n の文字列には x^n を足して考えてみる (文字列の先頭に 1 を追加してから変換すると言っても同じことである)。例えば、文字列 00101 は長さが 5 なので $x^5 + 0x^4 + 0x^3 + 1x^2 + 0x^1 + 1x^0 (= x^5 + x^2 + 1)$ を対応させる。この対応が情報を損なわないような状況を考えてみるのが次のメモリの定義である¹。

Definition 2.0.2 (メモリ). 体 K について、 $x \in K$ がメモリであるとは、写像 $\coprod_{n=0}^{\infty} \{0, 1\}^n \rightarrow K : (i_1, \dots, i_n) \mapsto x^n + \sum_{k=0}^n i_k x^{n-k}$ が単射であることをいう。

Informal に言い換えれば、メモリとは係数が 0 か 1 のみのモニック多項式 $f(z) \in K[z]$ に対して、 $z = x$ を代入した値 $f(x) \in K$ のみから $f(z)$ を復元できるような $x \in K$ のことである。

Example 2.0.3 (2 進数表記). 体 K の標数が 0 なら、2 進数表記を考えることで $2 \in K$ はメモリである。

Example 2.0.4. K の標数は正 $p > 0$ であり²、さらに K は素体 $\mathbb{F}_p$ 上超越的であるとすると、この時、 $\mathbb{F}_p$ 上超越的な元 $x \in K$ を一つ取れば、 x は K のメモリである。

では、Proposition 2.0.1 の証明に移る。

Proof. ここまでの具体例によれば、体 K がメモリ $x \in K$ を持てば条件を満たすことを証明すればいい。実はこのとき $A_0 = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ と $A_1 = \begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix}$ は条件を満たす二つの行列になっている。実際、 x の多項式 $f(x)$ について $\begin{pmatrix} f(x) \\ 1 \end{pmatrix}$ に左から A_0 を掛けると $\begin{pmatrix} xf(x) \\ 1 \end{pmatrix}$ になり左から A_1 を掛けると $\begin{pmatrix} xf(x) + 1 \\ 1 \end{pmatrix}$ になることを用いれば、長さ 2 の縦ベクトル $v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ に左から A_0, A_1 を掛けることで A_0, A_1 が条件を満たすことを確認できる.. $\square$

この証明では本質的には、 $(x$ を掛けたり、 $)x$ を掛けた後に 1 を足すという K 上 1 次元アフィン変換を使おうとしている。2 × 2 行列の話に書き換えるために 1 次元アフィン変換を 2 次元の線形変換へ加工したものが $(A_0$ と) A_1 である。

¹この問題のために定義した安直な概念で、数学的な自然さは (少なくとも 2022/05 の私から見れば) 全く感じられない対象である。

²正標数であることはこの具体例では使っていない