Some remarks on the modular isomorphism problem

千葉大学・大学院理学研究院　櫻井　太朗 *
Taro Sakurai
Graduate School of Science,
Chiba University

序文

標数 $p > 0$ の素体 $\mathbb{F}_p$ と有限 p 群 G が与えられたとき，モジュラー群多元環 $\mathbb{F}_pG$ が定義される．この構成に関して次のような素朴な問いが考えられる*1.

問題. 有限 p 群はモジュラー群多元環から決定されるか？つまり有限 p 群 G と H が与えられたとき

$$\mathbb{F}_pG \cong \mathbb{F}_pH \implies G \cong H$$

が成立するか？

これは**モジュラー同型問題** (modular isomorphism problem) と呼ばれ，提起されてから既に半世紀以上が経過しているが，未解決のままである（[11, Introduction]，特に [4, 7, 12] を参照）．本稿では [11] において導入した判定法に関する紹介をする．講演では主に判定法とその証明について解説し，どのようにモジュラー同型問題へ適用するのかについてほとんど触れなかったが，この判定法から Deskins [3] や Passi-Sehgal [10] による結果に対する別証明を与えることができる [11]．本稿では（一般論は [11] に譲ることにして）四元数群 Q_8 の場合を具体的に記述する．小さな例を通して判定法がどのように適用されるのかを見て取ってもらいたい．

1　判定法

定義 1.1 ([11, Definition 1.4])**.** 有限群 G の同型類を $[G]$ で表す．同型類の集合 M は

$$[G] \times [H] = [G \times H]$$

を演算とする可換モノイドである．このグロタンディーク群を $K(M)$ とおき，その局所化を $L(M) = \mathbb{Q} \otimes_{\mathbb{Z}} K(M)$ とおく．このとき M は $L(M)$ の部分モノイドと同一視できる．有限可換環

* `https://orcid.org/0000-0003-0608-1852`
*1 ここで $\mathbb{F}_3C_4 \cong \mathrm{Mat}_2(\mathbb{F}_3) \cong \mathbb{F}_3V_4$ のような例はいくらでも作れることに注意．ここで V_4 は Klein の四元群.

R に対して，$L(M)$ の部分空間 $S(R)$ を

$$S(R) = \sum_A \mathbb{Q}[A^*]$$

で定める．ここで和は R 上の有限多元環 A の代表系を渡り，A^* は A の乗法群を表す．このとき $[K] \in S(R)$ がすべての部分群 $K \le G$ に対して成立するならば，有限群 G は R **上遺伝的** (hereditary over R) であるという．

定義から遺伝的な有限群は部分群に関して閉じている．

例 1.2. 位数 q の巡回群を C_q で表す．位数 2 の巡回群 C_2 は $(\mathbb{F}_2C_2)^* \cong C_2$，つまり

$$[C_2] = [(\mathbb{F}_2C_2)^*] \in S(\mathbb{F}_2)$$

ゆえ $\mathbb{F}_2$ 上遺伝的である．また位数 4 の巡回群 C_4 も $(\mathbb{F}_2C_4)^* \cong C_4 \times C_2$ ゆえ

$$[C_4] = [(\mathbb{F}_2C_4)^*] - [C_2] = [(\mathbb{F}_2C_4)^*] - [(\mathbb{F}_2C_2)^*] \in S(\mathbb{F}_2)$$

なので，再帰的に $\mathbb{F}_2$ 上遺伝的である．

遺伝的な有限群は群多元環から決定できるというのが，新たな判定法（同型問題が肯定的に解決できるための十分条件）である．

判定法 1.3 ([11, Criterion 1.6])**.** 有限群 G と H に対して，G が有限可換環 R 上遺伝的かつ $RG \cong RH$ ならば $G \cong H$ である．

これは**随伴** $\mathrm{Hom}(RG, A) \cong \mathrm{Hom}(G, A^*)$ と**準同型の数え上げ**（Lovász [8, 9] による組合せ論的な手法）を使って証明される．判定法を適用するには，どのような有限群が遺伝的であるかを知ることが肝要である．少なくとも準正則群（定義 1.4）と呼ばれる群の同値類は適当な条件の下で $S(R)$ の元であり（補題 1.5），これを用いて四元数群 Q_8 のような場合にはモジュラー同型問題が肯定的に解決できる．

定義 1.4. 可換環 R 上の非単位的な（＝必ずしも単位元を持つとは限らない）多元環 A に対し，**準乗法** (quasi-multiplication) を

$$x \circ y = x + y + xy$$

で定める．元 $x \in A$ がこの演算に関して正則である，つまり $x \circ y = 0 = y \circ x$ であるような元 $y \in A$ が存在するとき，x は**準正則** (quasi-regular) であるという．多元環 A の準正則元全体のなす群を**準正則群** (quasi-regular group) といい，記号 $Q(A)$ で表す．多元環 A のすべての元が準正則であるとき，A は**準正則**であるという．

単位的な多元環 A に対しては同型 $Q(A) \to A^*$，$x \mapsto 1 + x$ が存在する．つまり，準正則群とは乗法群の非単位的な多元環への拡張である．単位元の添加を考えることにより，次の補題が示せる．

補題 1.5 ([11, Lemma 2.4])**.** 有限可換環 R 上の非単位的な有限準正則多元環 A の準正則群 $Q(A)$ に対し，$[Q(A)] \in S(R)$ が成立する．

ここまでをまとめると，$S(R)$ に関連する遺伝的という性質を導入して，同型問題の判定法を述べ，適当な準正則群の同型類は $S(R)$ の元であることを紹介した．四元数群 Q_8 の場合にモジュラー同型問題をこの手法で解決しようとすると，例 1.2 で真部分群は $\mathbb{F}_2$ 上遺伝的であることは見たので，後は $[Q_8] \in S(\mathbb{F}_2)$ を示せばよい．ところが巡回群のようにモジュラー群多元環の乗法群を考えるのはうまくいかない．乗法群 $(\mathbb{F}_2 Q_8)^*$ は

```
gap> g := QuaternionGroup(8);;
gap> a := GroupRing(GF(2), g);;
gap> u := Units(a);; GroupId(u);
[ 128, 178 ]
gap> Size(DirectFactorsOfGroup(u));
1
```

ゆえ直既約で Q_8 を部分群としては含むが，直積因子には含まないからだ [5]．ある多元環の準正則群を考えることで上手く $[Q_8] \in S(\mathbb{F}_2)$ が示せることを最後に見る．

2 四元数群

四元数群を

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm i \cdot j\} = \{\, (-1)^k \cdot i^a \cdot j^b \mid 0 \le k, a, b < 2 \,\}$$

と書く．いま四元数群 $A = Q_8$ 上に新たな演算を

$$\begin{aligned} x + y &= x \cdot y \cdot m(x,y)^{-1} \\ x \times y &= m(x,y) \end{aligned} \tag{2.1}$$

で定める [1, 2, 6]．ここで $m\colon Q_8 \times Q_8 \to Z(Q_8)$ は元 $x = (-1)^k \cdot i^a \cdot j^b$ と $y = (-1)^\ell \cdot i^c \cdot j^d$ に対して

$$m(x,y) = (-1)^{ac+bd+ad} \tag{2.2}$$

によって定義される写像である．これらの演算によって $A = Q_8$ は $\mathbb{F}_2$ の非単位的な多元環になる！さらに準乗法は

$$\begin{aligned} x \circ y &= x + y + x \times y \\ &= x \cdot y \cdot m(x,y)^{-1} + m(x,y) \\ &= x \cdot y \cdot m(x \cdot y \cdot m(x,y)^{-1}, m(x,y)) \\ &= x \cdot y \end{aligned}$$

となり，元の演算と一致する．よって，すべての元は準乗法に関しても正則なので A は準正則であり，補題 1.5 より $[Q_8] = [Q(A)] \in S(\mathbb{F}_2)$ を得る．したがって，例 1.2 と合わせると Q_8 は $\mathbb{F}_2$ 上遺伝的であり，判定法 1.3 より四元数群 $G = Q_8$ に関してはモジュラー同型問題を肯定的に解決できることが確かめられた．序文で言及した Deskins [3] や Passi-Sehgal [10] による結果も，基本的には上と同じような方針により別証明を与えることができる．

跋文

講演後に飛田明彦氏からのコメントへ返答する中で「$\mathbb{F}_p$ 上遺伝的でない有限 p 群の具体例を知らない」と述べた．たとえ小さな群であっても，大きな多元環の乗法群に直積因子として現れ，その正規補群も多元環の乗法群として実現される可能性が否定できないところに難しさ（と柔軟さ）があると感じている．読者諸賢が具体例や遺伝的な群である必要条件などを発見されたときには，ご教示頂ければありがたい．

謝辞

「有限群のコホモロジー論とその周辺」において講演の機会を与えて頂いた，世話人の飛田明彦氏（埼玉大学）と亀子正喜氏（芝浦工業大学）には大変お世話になりました．ここに感謝の意を表します．

参考文献

[1] J. C. Ault and J. F. Watters, 'Circle groups of nilpotent rings', *Amer. Math. Monthly* 80 (1973) 48–52, doi:10.2307/2319260, MR 316493, Zbl 0251.16009.

[2] A. A. Bovdi, 'On circle groups of nilpotent rings of characteristic 2', *Period. Math. Hungar.* 32 (1996) 31–34, doi:10.1007/BF01879729, MR 1407906, Zbl 0858.16028.

[3] W. E. Deskins, 'Finite abelian groups with isomorphic group algebras', *Duke Math. J.* 23 (1956) 35–40, doi:10.1215/S0012-7094-56-02304-3, MR 77535, Zbl 0075.23905.

[4] B. Eick and A. Konovalov, 'The modular isomorphism problem for the groups of order 512', *Groups St Andrews 2009 in Bath. Vol. 2* (Cambridge University Press, Cambridge, 2011) 375–383, doi:10.1017/CBO9780511842474.005, MR 2858869, Zbl 1231.20002.

[5] The GAP Group, GAP — groups, algorithms, and programming, (2019) version 4.10.1. http://www.gap-system.org.

[6] R. Gilmer and D. Roselle, 'Complements and comments', *Amer. Math. Monthly* 80 (1973) 1116–1118, doi:10.2307/2318547, MR 327413.

[7] M. Hertweck and M. Soriano 'On the modular isomorphism problem: groups of order 2^6', *Groups, rings and algebras*, Contemp. Math. 420 (American Mathematical

Society, Providence, RI, 2006) 177–213, doi:10.1090/conm/420/07976, MR 2279240, Zbl 1120.20005.

[8] L. Lovász, 'Operations with structures', *Acta Math. Acad. Sci. Hung.* 18 (1967) 321–328, doi:10.1007/BF02280291, MR 214529, Zbl 0174.01401.

[9] L. Lovász, 'Direct product in locally finite categories', *Acta Sci. Math.* (*Szeged*) 33 (1972) 319–322, MR 327865, Zbl 0251.18004.

[10] I. B. S. Passi and S. K. Sehgal, 'Isomorphism of modular group algebras', *Math. Z.* 129 (1972) 65–73, doi:10.1007/BF01229543, MR 311752, Zbl 0234.20003.

[11] T. Sakurai, 'The isomorphism problem for group algebras: a criterion', Preprint, 2019, arXiv:1901.09939v3.

[12] R. Sandling, 'The isomorphism problem for group rings: a survey', *Orders and their applications*, Lecture Notes in Math. 1142 (Springer, Berlin, 1985) 256–288, doi:10.1007/BFb0074806, MR 812504, Zbl 0565.20005.