

KS_3 の自己同型群 II

首 藤 武 史

§0 序

K を代数的閉体とし, p をその標数とする. A が K 上の有限次元多元環であるとき, この自己同型全体のなす群 $\text{Aut}(A)$ が代数群の構造を持つことはよく知られている. $p=0$ の場合にはこのリー環 $L(\text{Aut}(A))$ は自然に A の導分環 $\text{Der}(A)$ に一致することもよく知られている. しかしながら, $p>0$ の場合には一般にはこのことは成立しないことが簡単な例で示される. これに関して, 幾つかの例を計算して次のような予測をしている.

A の根基を保つ導分全体 $\text{der}(A)$ は $\text{Der}(A)$ の部分リー環で, これが $\text{Aut}(A)$ のリー環であろう.

前回の講演では, このことを示す例として, A が 3 次の対称群 S_3 の群環である場合の計算結果を報告した. 結果は以下の通りである.

$p \neq 2, 3$ のとき, $A \cong K \times K \times M_2(K)$. これから, $\text{Aut}(A) \cong S_2 \times \text{PGL}_2(K)$.

$p=2$ のとき, $A \cong K[x]/(x^2) \times M_2(K)$. これから, $\text{Aut}(A) \cong K^\times \times \text{PGL}_2(K)$.

$p=3$ のとき, $\dim \text{Aut}(A)=4$, $(\text{Aut}(A) : \text{Aut}(A)_0)=2$.

いずれの場合にも, $L(\text{Aut}(A))=\text{der}(A)$ が成立している.

ここで, $p=3$ の場合は, 代数群としての次元, 連結成分の個数はコンピュータ・ソフトウェアを利用して得た結論である.

今回, $p=3$ の場合に, A の自己準同型全体のなす空間 $\text{End}(A)$ を詳しく調べることで, 上記の結果をコンピュータに依らずに証明できたので, その概略を報告する.

ところで, 上記の結果のうち前者 2 つは, K は代数的閉体ではなく任意の体, 特に有限体, で成立する. 従って, $p=3$ の場合にも, 抽象群としてのまとめ方が望ましい. これについて §4 で言及する.

§§ 1, 2 では K は標数 3 の任意の体とし, §3 ではさらに代数的閉体とする. 代数多様体や代数群の基本的なことは [2] に従う.

§1 KS_3

3 次対称群 S_3 およびこの群環 (group algebra) について以下の議論に必要なことをまとめる.

S_3 は位数 6 の群で, 2 つの元 e_1, e_2 で生成され, 次の基本関係をもつ:

$$(1.1) \quad e_1^2=e_0, \quad e_2^2=e_0, \quad e_2e_1=(e_1e_2)^2$$

ここで, e_0 は S_3 の単位元である.

$$(1.2) \quad e_3 = e_1 e_2 e_1, \quad e_4 = e_1 e_2, \quad e_5 = e_2 e_1$$

とおけば,

$$S_3 = \{e_0, e_1, e_2, e_3, e_4, e_5\}$$

で, e_1, e_2, e_3 は位数 2 をもち, e_4, e_5 の位数は 3 である. $A_3 = \{e_0, e_4, e_5\}$ は正規部分群で, 3 次の交代群である.

K を標数 3 の任意の体とし, $A = KS_3$ を S_3 の K 上の群環とする. すなわち, A は S_3 の元を基底にもつ K 上の 6 次元ベクトル空間で, S_3 の積を線形に拡大することによって得られる K 上の多元環である. e_0 が単位元である. たびたびこれを 1 で表す.

A は直既約 (すなわち, A は多元環の直積では表されない) である. A の根基 (Jacobson radical) R は $\{e_1 - e_2, e_1 - e_3, e_0 - e_4, e_0 - e_5\}$ で張られる 4 次元のイデアルで,

$$A/R \cong K \times K.$$

§ 2 $\text{End}(A)$

A の 1 次変換 σ が, $\sigma(1)=1$ で, A の任意の 2 元 a, b に対して

$$(2.1) \quad \sigma(ab) = \sigma(a)\sigma(b)$$

を満たすとき, A の自己準同型と呼ばれる. これらの全体のなす集合を $\text{End}(A)$ で表す. これは 1 次変換の積 (合成) に関して閉じている.

群 S_3 の基本関係 (1.1) より,

(2.2) A の部分集合 $\{e_1, e_2\}$ から, A への写像 f が

$$f(e_1)^2 = 1, \quad f(e_2)^2 = 1, \quad f(e_2)f(e_1) = (f(e_1)f(e_2))^2$$

をみたすとき, f は一意的に A の自己準同型に拡張される. 最後の等式は

$$f(e_1)f(e_2)f(e_1) = f(e_2)f(e_1)f(e_2)$$

で置き換えてもよい.

実際, (1.2) より, $f(e_3) = f(e_1)f(e_2)f(e_1)$, $f(e_4) = f(e_1)f(e_2)$, $f(e_5) = f(e_2)f(e_1)$ と定義すればよい.

$A \times A$ の部分集合 B を次のように定義する：

$$(2.3) \quad B = \{(a, b) \in A \times A \mid a^2 = 1, b^2 = 1, aba = bab\}$$

A の自己準同型 f が (2.2) の各式を満たすことは明らかであるから、(2.2) より、

(2.4) 写像 $f \mapsto (f(e_1), f(e_2))$ は $\text{End}(A)$ から B への全単射である。

$\text{Aut}(A) = \text{End}(A) \cap \text{GL}(A)$ であるから、

(2.5) (2.4)で、 (a, b) に対応する A の自己準同型を σ とするとき、 σ が A の自己同型であるための必要純分条件は

$$\{1, a, b, aba, ab, ba\}$$

が 1 次独立であることである。

B を具体的にするために、まず、 A の位数 2 の元を調べる。 $a \in A$ が $a^2 = 1$ であるとする。 $a = \sum_{i=0}^5 x_i e_i$ とおく。 S_3 の乗積表により、 $x_0, x_1, \dots, x_5$ がみたす関係式を求め整理すると次の結果を得る。

(2.6) $a = \sum_{i=0}^5 x_i e_i$ のとき、 $a^2 = 1$ となるための必要十分条件は次の (i) または (ii) が成り立つことである：

$$(i) \quad x_0 = \pm 1, x_i = 0 \quad (i = 1, \dots, 5)$$

$$(ii) \quad x_0 = 0, x_1 + x_2 + x_3 = \pm 1, x_4 + x_5 = 0, x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$$

すなわち、

$$\{a \in A \mid a^2 = 1\}$$

$$= \{\pm e_0\} \cup \{x_1 e_2 + x_2 e_2 + x_3 e_3 + x_4(e_4 - e_5) \mid x_1 + x_2 + x_3 = \pm 1, x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$$

次に、 a, b が $a^2 = 1, b^2 = 1$ をみたすとき、 $(a, b) \in B$ となる条件を求める。まず次のことは容易に分かる。

(2.7) $a \in A$ とする。

$$(i) \quad (\pm e_0, a) \in B \Leftrightarrow a = \pm e_0 \quad (\text{復号同順})$$

$$(ii) \quad (a, \pm e_0) \in B \Leftrightarrow a = \pm e_0 \quad (\text{復号同順})$$

そこで、 A の部分集合 D^+ と D^- を次のように定義する：

$$D^+ = \{x_1 e_1 + x_2 e_2 + x_3 e_3 + x_4(e_4 - e_5) \mid x_1 + x_2 + x_3 = 1, x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$$

$$D^- = \{x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5) \mid x_1 + x_2 + x_3 = -1, x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$$

(2.8) $(a, b) \neq (\pm e_0, \pm e_0)$ とする. このとき,

$$(a, b) \in B \Leftrightarrow a, b \in D^+ \text{ または } a, b \in D^-.$$

証明の概略. 必要性. $\pi : A \rightarrow A/R$ を標準写像とする. §1 の議論より,

$$\pi(x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5)) = (x_1 + x_2 + x_3)\pi(e_1), \pi(e_1) \neq 0$$

仮定より $a, b \in D^+ \cup D^-$ で, $\pi(a) = \pi(b)$. これから $a, b \in D^+$ または $a, b \in D^-$ が分かる.

十分性. $a = x_1e_1 + x_2e_2 + x_3e_3 + x_4(e_4 - e_5)$, $b = y_1e_1 + y_2e_2 + y_3e_3 + y_4(e_4 - e_5)$ が条件をみたすとする. このとき, aba を計算すると, 文字 x, y について対称であることが分かる. このことは $aba = bab$ を意味する.

(2.7) および (2.8) より,

$$(2.9) \quad B = \{(e_0, e_0)\} \cup \{(-e_0, -e_0)\} \cup (D^+ \times D^+) \cup (D^- \times D^-).$$

§3 Aut(A)

この節では K は代数的閉体であるとする. A を底 $\{e_0, \dots, e_5\}$ により 6 次元アファイン空間 K^6 と同一視する. A の 1 次変換全体の空間を $E(A)$ で表す. これは, K 上の 6 次正方形行列の全体であるから, 36 次元アファイン空間とみなされる. $A, A \times A$ および, $E(A)$ は Zariski 位相により位相空間である. A の正則な 1 次変換全体のなす群 $GL(A)$ は $E(A)$ の開集合である. (2.1) は座標の間の多項式関係を意味するから, $End(A)$ は $E(A)$ の閉集合, $Aut(A) = GL(A) \cap End(A)$ は $End(A)$ の開集合である.

(3.1) B は $A \times A$ の閉集合で, 写像 (2.4) は $End(A)$ から B への代数多様体の同型でもある.

実際, $f(e_1), f(e_2)$ はそれぞれ f の表現行列の第 1 列, 第 2 列である (列は第 0 列から数える) からこれは多項式写像であり, (1.2) より逆写像も多項式写像である.

(3.2) D^+, D^- はともに $A (=K^6)$ の閉部分集合で, 既約な 2 次元代数多様体である.

証明の概略. これらは明らかに K^4 の代数多様体に同型である. さらに, アファイン座標変換を利用して K^3 に埋め込むことができる. この像は, 1 つの既約多項式で定義され, 従って, K^3 の既約な超局面に同型である. これから, 2 次元の既約代数多様体であることが分かる.

(3.3) (1) $\sigma \in \text{Aut}(A)$ に対して, A の 1 次変換 σ' を次のように決める:

$$\sigma'(e_i) = -\sigma(e_i) \quad (i=1, 2, 3), \quad \sigma'(e_i) = \sigma(e_i) \quad (i=0, 4, 5)$$

このとき, σ' は A の自己同型である, すなわち, $\sigma' \in \text{Aut}(A)$.

(2) $\varepsilon = (id_A)'$ とおく. これは A の自己同型である: $\varepsilon \in \text{Aut}(A)$.

証明. (1) σ は A の自己同型だから, 容易に $\sigma' \in \text{Aut}(A)$ も分かる.

(2) $id_A \in \text{Aut}(A)$ であるから $\varepsilon = (id_A)' \in \text{Aut}(A)$.

(2.4) および (3.1) によって, $\text{End}(A)$ と B を同一視する. このとき,

$$(3.4) \quad \text{Aut}(A) \cap (D^+ \times D^+) \neq \phi, \quad \text{Aut}(A) \cap (D^- \times D^-) \neq \phi$$

実際, $id_A \in \text{Aut}(A) \cap (D^+ \times D^+)$, $\varepsilon \in \text{Aut}(A) \cap (D^- \times D^-)$.

(e_0, e_0) , $(-e_0, -e_0) \notin \text{Aut}(A)$ であるから, (2.8) より,

$$(3.5) \quad \text{Aut}(A) = (\text{Aut}(A) \cap (D^+ \times D^+)) \cup (\text{Aut}(A) \cap (D^- \times D^-))$$

右辺は $\text{Aut}(A)$ の既約成分への分解である. 従って,

- (i) $\dim \text{Aut}(A) = 4$,
- (ii) $\text{Aut}(A)_0 = \text{Aut}(A) \cap (D^+ \times D^+)$,
- (iii) $(\text{Aut}(A) : \text{Aut}(A)_0) = 2$.

実際, (3.2) より $D^+ \times D^+$, $D^- \times D^-$ は 4 次元の既約な代数多様体で, $\text{Aut}(A)$ との共通部分は稠密であるから, それぞれ既約である. $\dim D^\pm = 2$ より, (i) が成り立つ. (3.4) の議論より, $\text{Aut}(A) \cap (D^+ \times D^+)$ は単位元を含む $\text{Aut}(A)$ の既約成分である. すなわち, (ii). さらにこれから (iii) が従う.

§4 有限体の場合

A の内部自己同型群を $\text{Int}(A)$ で表す. これは $\text{Aut}(A)$ の閉正規部分群で連結である. 従って, $\text{Int}(A) \subset \text{Aut}(A)_0$ が成り立ち, 前回の講演で次の代数群の完全系列があることを報告した [3, Remark]:

$$(4.1) \quad \{1\} \rightarrow \text{Int}(A) \rightarrow \text{Aut}(A)_0 \rightarrow K^\times \rightarrow \{1\}$$

これらの群はいずれも素体上で定義されているので, k が K の部分体であるとき, k 有理点の系列

$$(4.2) \quad \{1\} \rightarrow \text{Int}(A)(k) \rightarrow \text{Aut}(A)_0(k) \rightarrow k^\times \rightarrow \{1\}$$

も完全ではないかと思われる．これが 0 系列であることは明らかである．問題は $\text{Aut}(A)_0(k) \rightarrow k^\times$ が全射であることである． k が有限体の場合，[1] (16.5) よりこの写像は全射であることが分かる．従って (4.2) は完全系列である．

k を有限体とし，元の個数が $|k|=3^m$ とする． S_3 の k 係数の群環を改めて A とおく．このとき，(4.2) は次の系列を意味する：

$$(4.3) \quad \{1\} \rightarrow \text{Int}(A) \rightarrow \text{Aut}(A)_0 \rightarrow k^\times \rightarrow \{1\}$$

ここで， D^+ を (2.7) の直後に定義した A の部分集合として，

$$(4.4) \quad \text{Aut}(A)_0 = \text{Aut}(A) \cap (D^+ \times D^+) = \text{GL}(A) \cap (D^+ \times D^+)$$

とおく．これは $\text{Aut}(A)$ の指数 2 の正規部分群である．

$\text{Int}(A) \cong A^\times / Z(A)^\times$ であるから，この右辺の群の位数を計算すると，

$$(4.5) \quad |\text{Int}(A)| = (3^m - 1) \cdot 3^{2m}$$

が分かる． $|k^\times| = 3^m - 1$ であり，(4.3) が完全系列であることから $\text{Aut}(A)_0$ の位数は $(3^m - 1)^2 \cdot 3^{2m}$ であることが分かる．これから従って，

$$(4.6) \quad |\text{Aut}(A)| = 2 \cdot (3^m - 1)^2 \cdot 3^{2m}$$

が分かる．

k の標数が 3 以外の場合には，序文に述べた結果から計算出来る．すべてをまとめると次のようになる．

(4.7) k を位数 p^m をもつ有限体とし， A を k 係数の S_3 の群環とする． A の自己同型群 $\text{Aut}(A)$ の位数は

- (i) $p \neq 2, 3$ の場合， $|\text{Aut}(A)| = 2 \cdot p^m \cdot (p^{2m} - 1)$
- (ii) $p = 2$ の場合， $|\text{Aut}(A)| = (2^m - 1) \cdot 2^m \cdot (2^{2m} - 1)$
- (iii) $p = 3$ の場合， $|\text{Aut}(A)| = 2 \cdot (3^m - 1)^2 \cdot 3^{2m}$

参考文献

- [1] A. Borel, Linear Algebraic Groups Second Enlarged Edition, G.T.M. **126**, Springer-Verlag, 1991.
- [2] J. E. Humphreys, Linear algebraic groups, G. T. M. **21**, Springer-Verlag, 1975.
- [3] 太田友明・首藤武史, KS3 の自己同型群, Proceedings of Summer Seminar on Lie Algebras and Related Topics, **26**, 26–29 (2010).