数理解析研究所講究録
998巻 1997年 161-169

$GL(3)$ の ある種のガロア不変有限部分群の構造について

名古屋大学理学部　鈴木浩志（Hiroshi Suzuki）

K を、有理数体 $\mathbf{Q}$ 上 galois な体とし、その整数環を O_K とする。一般線形群 $GL(n, O_K)$ の有限部分群 G で K の $\mathbf{Q}$ 上の galois 群 $G(K/\mathbf{Q})$ の作用で安定なもの（$\sigma \in G(K/\mathbf{Q})$ について $\sigma(G) \subset G$ となるもの）を考える。

定義　O_K^n の標準的な基底で生成された $\mathbf{Z}$-部分加群 $\mathbf{Z}^n$ の直和分解 $\mathbf{Z}^n = \bigoplus_{j=1}^{k} L_j$ で、各 $g \in G$ について 1 のべき根 $\varepsilon_j(g)$ と置換 $s(g) \in \mathfrak{S}_k$ が存在して、全ての j について $\varepsilon_j(g) g L_j = L_{s(g)(j)}$ となるようなものが存在するとき、G は A-type であるという。

ここで、次の問題を考える。

問題　$GL(n, O_K)$ の有限部分群 G で $G(K/\mathbf{Q})$ の作用で安定なものは、全て A-type か？

G がべき零な場合（Y. Kitaoka and H. Suzuki [2]）、及び $n=2$ の場合（Y. Kitaoka [3]）には既に確かめられているので、ここでは、$n=3$ の場合に上が正しいことを確かめる。

まず、基本的な事柄についてまとめておく。

補題 1　K で 2 つ以上の $\mathbf{Q}$ の有限素点が分岐し、$\mathbf{Q}$ 上 galois な全ての真の中間体 F について $GL(n,F)\cap G \subset GL(n,O_{K\cap\mathbf{Q}^{ab}})$ が成り立っていれば、G は A-type である。（Y. Kitaoka [1], 補題 3。ここで、$\mathbf{Q}^{ab}$ は、有理数体の最大 abel 拡大。）

これをつかって、$[K:\mathbf{Q}]$ に関する帰納法をすれば、$K/\mathbf{Q}$ で分岐する $\mathbf{Q}$ の有限素点が唯ひとつ p のみな場合（$p\infty$-分岐と言うことにする）に帰着される。必要なら K に 1 の p べき根をつけて考えてもよい。以下 $K/\mathbf{Q}$ は、$p\infty$-分岐とする。(p は素数。)

補題 2　K が abel 体（$\mathbf{Q}$ 上 abel）なら A-type である。（Y. Kitaoka [1]、定理 1。）よって問題は、$G\subset GL(n,O_{K\cap\mathbf{Q}^{ab}})$ か？と同値である。

注意　たとえば $G(K/\mathbf{Q})$ がべき零で、p が奇数の場合はこの補題 2 と galois 群が巡回群であることからわかる。

$\mathfrak{p}$ を p の上の K の素因子とし、

$$\begin{aligned} G(\mathfrak{p}) &= \{g \in G\,;\, g \equiv 1(\mathfrak{p})\} \\ G(p) &= \langle G(\mathfrak{p})\,;\, \mathfrak{p} \mid p \rangle \end{aligned}$$

とおく。$G(p)(\mathfrak{p}) = G(\mathfrak{p})$ より、$G(p)(p) = G(p)$ である。$\mathfrak{p}$ が $\mathbf{Q}$ 上分解していなければ $G(\mathfrak{p}) = G(p)$ である。また、ある $\mathfrak{p} \mid p$ について $G(\mathfrak{p}) = G(p)$ なら、全ての $\mathfrak{p} \mid p$ についても $G(\mathfrak{p}) = G(p)$ である。$G(\mathfrak{p})$ は 有限 p-群である。さらに、$G(\mathfrak{p})$ は、G の正規部分群なので、$G(p)$ も 有限 p-群である。

補題 3　K が abel 体なら $T^{-1}G(p)T$ が diagonal となる $T \in GL(n, \mathbf{Z})$ がとれる。(Y. Kitaoka and H. Suzuki [2], 補題 1。)

注意　G が A-type なら、$G(\mathfrak{p}) = G(p)$ は 可換 p-群で、$GL(n, O_{K\cap\mathbf{Q}^{ab}})$ に含まれる。

補題 4　$G(\mathfrak{p}) = G(p) \subset GL(n, O_{K\cap\mathbf{Q}^{ab}})$ なら、G は A-type である。(Y. Kitaoka [3]、補題 1.8。)

$K/\mathbf{Q}$ は $p\infty$-分岐であるから、$G(p) \subset GL(n, O_{K^{ab}})$ なら、$G(\mathfrak{p}) = G(p)$ である。よって、G が、A-type でなければ、$G(p)$ も A-type ではない。よって、最小位数の反例は $G = G(p)$ となっている。

ここで、n に関する帰納法をしながら、最小位数の反例を探すことを考えれば、

補題 5　行列の大きさが $n-1$ 以下なら全て A-type であることが既に確かめられている場合、行列の大きさが n の時にも全て A-type であることを示すには、次の 3 つの場合のみを考えればよい。

1) G は基本 abel 群。$p\not| n$ なら $G \subset SL(n, O_K)$ としてよい。

2) $2 \neq p \mid n$、$K \ni \zeta_p$、$G \subset SL(n, O_K)$、$G^p = 1$ かつ $G^c = \langle \zeta_p \rangle$。

3) $p = 2 \mid n$、$G \subset SL(n, O_K)$ かつ $G^2 = G^c = \{\pm 1\}$。

この補題は、G を最小位数の反例としておいて、以下の順に確かめるとわかりやすい。

i)　$\Phi(G) = \Phi(G)(p)$。

ii)　$\Phi(G) \subset Z(G)$。

iii)　$\Phi(G)$ は scalar。

iv)　G が非可換なら、$\zeta_p \in K$ かつ $G^c = \langle \zeta_p \rangle$。

v)　G が非可換なら、$p \mid n$。$g \in G \backslash Z(G)$ について、固有多項式 $\varphi_g(X)$ は X^p の多項式。

vi)　G が可換または $p \neq 2$ なら、$G^p = 1$ としてよい。

vii)　$p\not| n$ なら、$SL(n, O_K) \supset G$ かつ G は基本 abel p-群としてよい。

viii)　$p \neq 2$ で G が非可換の場合、$G^c = \langle \zeta_p \rangle$、$G^p = 1$ かつ $G \subset SL(n, O_K)$ としてよい。

ix)　$p = 2$ で G が非可換な場合、$G^2 = G^c = \{\pm 1\}$ としてよい。

x)　ix) でさらに、$G \subset SL(n, O_K)$ としてよい。

(vi)–x) では、K に 1 の p べき根を添加して、G を、G と 1 の p べき根で生成される群の部分群と取りかえている。)

注意　$G(K/\mathbf{Q})$ がべき零で $p = 2$ の場合は、$G(K/\mathbf{Q})$ が 2-群なので、G は指数 2 の $G(K/\mathbf{Q})$-安定部分群を持つ。よって、この場合、G が四元数群 Q_8 となり容易に確かめることができる。

注意　$G(K/\mathbf{Q})$ が一般で $n = 2$ の場合も、G が四元数群の場合が問題になるが、$\mathbf{Q}(\sqrt{2})$、$\mathbf{Q}(\sqrt{-1})$、$\mathbf{Q}(\sqrt{-2})$ の類数が 1 であることに注意すると、G は指数 2 の $G(K/\mathbf{Q})$ 安定部分群を持つことがわかって、べき零の場合に帰着される。

そこで、上の補題を使って、$n = 3$ の場合を考える。

定理　$GL(3, O_K)$ の有限部分群で、$G(K/\mathbf{Q})$ の作用で安定なものは、すべて A-type である。

証明の概略　G が rank 2 の基本 abel p-群の場合、rank 3 の基本 abel 3-群の場合、及び位数 27 exponent 3 の非可換 3-群の場合が問題になる。

$p \geqq 5$ で、$SL(3, O_K) \supset G$ が rank 2 の基本 abel p-群の場合。

G を反例と仮定して、固有値が重複しない元の固有空間を Kv, Kv', Kv'' とする。$G(K/\mathbf{Q})$ の元は $\{Kv, Kv', Kv''\}$ に置換を引き起こす。固有値とそれに対する固有空間が決まれば行列はひとつに決まるので、$\mathrm{Im}\,(G(K/\mathbf{Q}) \to \mathrm{Aut}\,G) \longrightarrow \mathfrak{S}_3 \times G(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ は単射としてよい（$\mathfrak{S}_3$ は 3 次対称群）。ここで、$G(K/\mathbf{Q})$ が可換なら反例にはならないので、$G(K/\mathbf{Q}) \longrightarrow \mathfrak{S}_3$ 全射の場合だけが問題である。$p\infty$-分岐な 2 次体は $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ だけなので、$K_2 = \mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ とおくと、$\mathfrak{S}_3$-拡大は K_2 を含み、

$$G(K/\mathbf{Q}) \cong \mathfrak{S}_3 \times_{G(K_2/\mathbf{Q})} G(\mathbf{Q}(\zeta_p)/\mathbf{Q})$$

である。

K_6 を K に含まれる唯一の $\mathfrak{S}_3$-拡大、K_3 を K_6 に含まれる 3 次体のうち Kv' と Kv'' の互換に対応するものとする。$v = {}^t(v_1, v_2, v_3) \in O_{K_3}^3$ ととれば、v' と v'' は v の共役である。v を O_{K_3} の integral basis を使って表せば、$\det P = \pm[O_{K_3} : \mathbf{Z}v_1 + \mathbf{Z}v_2 + \mathbf{Z}v_3]\sqrt{d_{K_3/\mathbf{Q}}}$ であることがわかる。（ここで、$d_{K_3/\mathbf{Q}}$ は K_3 の discriminant。）

また、$K_6/\mathbf{Q}$ は $p\infty$-分岐であるが、$p \geqq 5$ なので、K_6/K_2 で p の

上の素点は完全分解していなければなない。よって、

$$P\begin{pmatrix} \zeta_p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1}, P\begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_p & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1}, P\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_p \end{pmatrix}P^{-1}$$

の成分が O_K の元であることから

$$P\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}P^{-1}, P\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}P^{-1}, P\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1}$$

の成分も O_K の元でなければならないことがわかる。逆行列を具体的に書いて計算してみれば、

$$\det P \mid [O_{K_3} : (v_1, v_2, v_3)_{O_{K_3}}]$$

でなければならないことがわかる。先の式と比べると、K_3 の discriminant が 1 でなければならなくなって矛盾する。よってこの場合反例は存在しない。

注意　問題から G の成分が整数という条件を外して、$GL(n, K)$ の有限部分群で galois 群の作用で安定なものを考えると、$GL(n, K \cap \mathbf{Q}^{ab})$ に入らないものは、いくらでもあることがわかる。実際、galois でない n 次体の integral basis を縦に並べたベクトルをひとつ作り、その共役を横に並べてできる n 次正方行列を用いて、1 のべき根が並んだ対角行列の群を逆変換すればよい。基礎体が有理数体の条件を外した場合も同様にして、G が基礎体の abel 拡大に入らないことが、基礎体によってはおこりうることもわかる。

$p=3$ で G が可換の場合。

$G \not\subset SL(3,O_K)$ の時は、$G \cap SL(3,O_K)$ を考えればすぐわかる。それ以外の場合つまり、G が $G \subset SL(3,O_K)$ となる rank 2 の基本 abel 3-群の場合は、$p \geqq 5$ の場合と同様にして変換行列を考えると、反例となるはずの G の固有値が重複しない元 g は、

$$g \in \sqrt[3]{3}^{-1} GL(3,\mathbf{Q}) \cap GL(3,O_K)$$

でなければならないことがわかるが、成分の付値を考えれば、これはおこりえない。

$p=2$ の場合は、$\mathbf{Q}(\sqrt{2})$、$\mathbf{Q}(\sqrt{-1})$ および $\mathbf{Q}(\sqrt{-2})$ の類数が 1 であることを使えば、$G(K/\mathbf{Q})$ を可換としてよいことが確かめられる。

最後に $p=3$ で G が位数 27 exponent 3 の非可換 3-群の場合を考える。

$G(K/\mathbf{Q}) \subset \mathrm{Aut}\, G$ としてよい。$G(K/\mathbf{Q})$ がべき零なら反例はないので、それ以外の $\mathrm{Aut}\, G$ の部分群を、G が指数 3 の安定部分群を持つ場合と持たない場合に分ける。持たない場合、$\mathbf{Q}(\zeta_3)$、$\mathbf{Q}(\zeta_9)^+$、$\mathbf{Q}(\zeta_9)$ および、$\mathbf{Q}(\zeta_3, \sqrt[3]{3})$ の類数が 1 であることに注意すると、$\mathrm{Aut}\, G$ の部分群を galois 群 $G(K/\mathbf{Q})$ として実現する体 K が存在しないことがわかる。持つ場合には、3 が $K/\mathbf{Q}$ で完全分岐であることを確かめられる。そこで補題 3 を使って、指数 3 の安定部分群を対角化しておくと、

反例となるはずの G は、

$$\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}$$

という形の元を持たなければならなくなり、$G(\mathfrak{p}) = G$ と矛盾する。

以上で、$n = 3$ の場合も、全て A-type であることがわかる。

参考文献

[1] Y. Kitaoka, Finite arithmetic subgroups of GL_n ,III, Proc. Indian Acad. Sci. **104**(1994), 201–206.

[2] Y. Kitaoka and H. Suzuki, Finite arithmetic subgroups of GL_n, IV, Nagoya Math. J. **142**(1996), 183–188.

[3] Y. Kitaoka, Finite arithmetic subgroups of GL_n, V, to appear.