京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学
KYOTO UNIVERSITY

| | |
|---|---|
| Title | 虚2次体の第2p-類体のガロア群について(代数的整数論における最近の話題) |
| Author(s) | 三宅, 克哉 |
| Citation | 数理解析研究所講究録 (1992), 797: 132-140 |
| Issue Date | 1992-08 |
| URL | http://hdl.handle.net/2433/82773 |
| Right | |
| Type | Departmental Bulletin Paper |
| Textversion | publisher |

Kyoto University

数理解析研究所講究録
797巻 1992年 132-140


# 虚2次体の第2 $p$-類体のガロア群について

名古屋大教養　三宅克哉 (Katsuya MIYAKE)

**1**．まず奇素数 $p$ を定める．虚2次体 $k$ についてそのヒルベルト $p$-類体を $k'$，第2 $p$-類体を $k''$ とし，$k''/k$ のガロア群を $G$ と現わす．このノウトでは，主として $k$ の $p$-類群 の $p$-ランクが 2の場合の $G$の構造を検討する．従って特に $k$ の単数は $\pm 1$ である．ひとつには単数が少ないことも影響して，大雑把に言って虚2次体の類数は一般に大きいのだが，さらに $G$ のサイズにも同様の傾向を見ることが出来る．以下では，特にイデアルのカピチュレイションについての虚2次体の特性に注目して，群論的にこれを検討する．

**2**．特に $p$-類群の $p$-ランクが2の場合について報告するが，一般の虚2次体に関して，我々の $G$ は次の著しい性質を持っている：

（A） $G$ の正規部分群 $H$ で剰余群 $G/H$ が巡回群になるものについては，指数 $[\mathrm{Ker}\, V_{G\to H} : [G,G]]$ は必ず指数 $[G:H]$ と一致する；ただし $V_{G\to H} : G \to H/[H,H]$ は $G$ の $H$ への移送写像 (transfer)で ある．

また第2類体 $k''$ は有理数体 $\mathbb{Q}$ 上のガロア拡大であるから，$G$ は次の性質を合わせ持つ：

（Ｂ） $G$ の位数 2 の自己同型写像 $\varphi$ で，$G$ の各元 $g$ に対して $g^{\varphi+1} \in [G, G]$ となるものが存在する．

条件（Ａ）の二 つの指数のうち ，初めのものが 後者で割り切れ ることはヒルベルトの定理 94 として良く知られており，最近になって鈴木 [Su] が一般の場合（剰余群 $G/H$ がアーベル群になるもの）につ いてこれを証明した ． 特に $G$ 自身 がアーベル群であるときは，（Ａ）が成り立 つための 必要十 分条件は $G$ が巡回 群であることである．また例えばメ タサイクリク群について は（Ｂ）は 成り立たない．乱暴な言い方をするとして，James [Ja] は位数が $p^6$ を越えない $p$-群を分類し，約 500 種類を あげているが，そのうち，2 元で生成され，（Ａ）と（Ｂ）の両方を満たすものは，8 種類しかない．

最近，次の形の $p$-群で，（ 1）$m = n = 2$，（2）$\mu = 1 \le \nu$，もしくは（3）$\mu = \nu = 2$ である場合に，（Ａ）と（Ｂ）を満たすものをすべ て決定した（詳細は 三宅 [M1] 参照のこと）；ただし，$m, n, \mu, \nu$ は正整数であって，$m \le p^{\mu} - 1$, $n \le p^{\nu} - 1$, $\mu \le \nu$ を満たす：

$$G = < a, b, c_{i,1}, c_{1,j} \mid 1 \le i \le m, 1 \le j \le n >,$$

$$[a, b] = c_{1,1},$$

$$[c_{i,1}, a] = c_{i+1,1}, \quad [c_{i+1,1}, b] = 1, \quad 1 \le i \le m, \quad c_{m+1,1} = 1,$$

$$[c_{1,j}, b] = c_{1,j+1}, \quad [c_{1,j+1}, a] = 1, \quad 1 \le j \le n, \quad c_{1,n+1} = 1,$$

$$a^{p^{\mu}} = \prod_{i,j} c_{i,j}^{q_{i,j}}, \quad b^{p^{\nu}} = \prod_{i,j} c_{i,j}^{r_{i,j}},$$

$$q_{i,j}, r_{i,j} \in \mathbb{Z}, \quad 1 \le i \le m, \ 1 \le j \le n, \ (i-1)(j-1) = 0,$$

$$c_{i,1}^{p^{\mu - t(i)}} = c_{1,j}^{p^{\min\{\mu, \nu - t(j)\}}} = 1, \quad 1 \le i \le m, \ 1 \le j \le n,$$

（ただし $t(i)$ は $p^{t(i)} \leq i < p^{t(i)+1}$ を満たす整数）.

その結果，総計 13 タイプの群が得られたが，（1）の場合が 3 種，（2）が 7 種，（3）が 3 種である．また James [Ja] のものはすべて（1）の場合に属する．これら 13 タイプへの分類は，$m$，$n$，$\mu$，$\nu$，$p=3$ ないし $p>3$ の組合せと $q_{i,j}$，$r_{i,j}$ が満たすべき条件（主として mod $p$ での合同関係）の形状による．顕著と思われることとしては，例えば，この形の $G$ が（A）と（B）を満たすためには，$m \geq 2$ かつ $n \geq 2$ で，しかも $m=2$ もしくは $n=2$ のいずれかが成り立たなければならない．

**3**．第 1 節の記号のもとで，さらに $K$ を $k$ の不分岐アーベル $p$-拡大とし，対応する $G$ の部分群を $H$ とする．また $K$ の $p$-類群を単に $C(K)$ と書く．類体論のアルティン写像によって，$C(k)$ と $C(K)$ はそれぞれ $G/[G,G]$ と $H/[H,H]$ に同型である．一方，$k$ のイデアルを自然に持ち上げて $K$ のイデアルと見ることにより，準同型写像

$$j_{K/k}: C(k) \to C(K)$$

が定義される；これがアルティン写像によって $G$ から $H$ への移送写像（から得られる準同型写像）

$$\overline{V}_{G\to H}: G/[G,G] \to H/[H,H]$$

と対応する．よって，$\mathrm{Ker}\, j_{K/k}$ の位数は条件（A）の指数

$$[\mathrm{Ker}\, V_{G\to H} : [G,G]]$$

と一致する．もう一方の指数 $[G:H]$ は拡大次数 $[K:k]$ である．

特に $K/k$ が不分岐巡回拡大であるときには，次の等式が良く知られ

ている：

$$|\mathrm{Ker}\, j_{K/k}| = [K : k] \cdot [E_k : \mathrm{N}_{K/k}(E_K)]\ ;$$

ここで $E_k$，$E_K$ は，それぞれ，$k$，$K$ の単数群であり，$\mathrm{N}_{K/k}$ は $K/k$ のノルム写像である．ところが，我々の場合，$E_k = \{\pm 1\}$ である．しかも $[K : k]$ は奇素数の冪であるから，最後の指数 $[E_k : \mathrm{N}_{K/k}(E_K)]$ は1に等しい．従って等式 $|\mathrm{Ker}\, j_{K/k}| = [K : k]$ が成り立ち，条件（A）が確認された．

**Proposition 1**. 虚2次体 $k$ の奇数次の不分岐巡回拡大 $K$ については等式 $|\mathrm{Ker}\, j_{K/k}| = [K : k]$ が成り立つ．

**Remark**. 実2次体についてはこのようなことは一般には成り立たない．Heider & Schmithals [HS] によれば，判別式 $d_k$ が 100000 未満の実2次体 $k$ で 3-イデアル類群が (3, 3)-タイプのもの，$d_k$ = 32009, 42817, 62501, 72329, 94639，のいずれについても，4箇ある不分岐巡回拡大のうちの3箇で $k$ の 3-イデアル類群全体が単項化し，特に $d_k$ = 62501 についてはすべての不分岐巡回拡大でそうなっている．また実2次体 $k$ でこの Proposition が成り立つような ものは，自明なもの以外はまだ知られていない．（一般に有限次代数体で，すべての奇素数 $p$ についてそのイデアル類群の $p$-ランクが1であるものについては，この Proposition が成り立つ．）[註)] また虚2次体 $k$ で，その 3-イデアル類群が (3, 3)-タイプのものは，$|d_k|$ が小さいものいから順に，$d_k$ = -3896, -4027, -6583, -8751, -9748, -12067, … と続く．

註）草稿にあったミスを岩澤先生が指摘してくださった．謝意を記す．

**4**．条件（B）に ついても触れておこう．明らかに $k^{\infty}$ は $\mathbb{Q}$ 上ガロア拡大である．したがって，その群 $\mathrm{Gal}(k^{\infty}/\mathbb{Q})$ の 2-シロウ群の位数は 2 である；そこで位数 2 の元 $\rho$ を取り，それによる $\mathrm{Gal}(k^{\infty}/\mathbb{Q})$ の内部自己同型写像を考えれば，正規 部分群 $G=\mathrm{Gal}(k^{\infty}/k)$ の 自己同型写像 $\varphi$ が得られる．イデアル類群 $C(k)$ と $G/[G,G]$ の 同型を与えるアルティン写像は，この $\varphi$ が $G/[G,G]$ 上に引き起こす作用と $\rho$ の $C(k)$ への自然な作用とを対応させるから，条件（B）は次の命題から直ちに従う：

**Proposition 2**（鈴木 ）．相対 2 次拡大 $k/k_0$ が与えられたとし，その自明でない自己同型写像を $\rho$ とする．もし $k$ のイデアル類 $c$ の位数が奇数であり，しかも $k_0$ の類数と素であれば， $c^{\rho}=c^{-1}$ である．

証明は容易である．実際，$c$ の位数 が奇数であるから，巡回群 $\langle c\rangle$ のなかに $c=a^2$ と なる元 $a$ がある ．したがって $c = a^{1+\rho}\cdot a^{1-\rho}$ と表わされる．ところが $a^{1+\rho}$ は $k_0$ のイデアル類 から来ており，位数についての仮定から， $a^{1+\rho}=1$ である．よって $c^{1+\rho}=1$ は明らかである．

**Proposition 3**．もし $G$ が条件（B）を満たすならば，各 $g\in[G,G]$ に対して $g^{\varphi}\equiv g \bmod [G,[G,G]]$ で ある．したがって $G$ はメタサイクリクではありえない．

証明．前半については，特に $g=[a,b]$，$a,b\in G-[G,G]$，の 場合を見れば十分である；剰余群 $G/[G,[G,G]]$ で は $[G,G]$ は中心に入るか

ら，これは明らかであろう．後半については，剰余群 $G/[G,[G,G]]$ がもしメタサイクリクであるならば，適当に $a \in G-[G,G]$ を選んで $\langle a \rangle \cdot [G,[G,G]]$ が $[G,G]$ を含むように出来るから，前半により，$G$ が条件（B）を満たすことはない．

**5**．虚2次体 $k$ のイデアル $p$-類群 $C(k)$ が巡回群であるときは，そのシュア・マルティプライアは消える；したがってその $p$-類体 $k'$ には $k$ 上での本質的な中心拡大が存在せず，$k$ の第2 $p$-類体 $k''$ は $k'$ に潰れてしまう．しかし $C(k)$ の $p$-ランクが2になると $k'/k$ の自明でない中心拡大が存在する．しかも前節で見たように，$G=\mathrm{Gal}(k''/k)$ は二つの条件（A）と（B）を満たし，アーベル群でもメタサイクリク群でもありえない．（これはすでに野村 [No] が示すところである．）さらにこの場合，第2節で述べたように $m=1$ でも $n=1$ でもありえない；よって $[G,G]=\mathrm{Gal}(k''/k')$ の，したがって $C(k')$ の $p$-ランクは少なくとも3以上である．

**Proposition 4**. 虚2次体 $k$ のイデアル $p$-類群 $C(k)$ の $p$-ランクが2であれば，そのヒルベルト $p$-類体 $k'$ のイデアル $p$-類群 $C(k')$ の $p$-ランクは少なくとも3以上である．

**6**．一般に有限次代数的数体 $k$ のイデアルは，ヒルベルトの類体にまで持ち上げればすべて単項イデアルになることは良く知られている；単項化定理である．特に $p$-イデアル類群に注目するならば，ヒルベルト $p$-類体をとれば十分である．しかし上で Heider & Schmithals [HS] に

よる実2次体の例で見たように，ヒルベルト $p$-類体までいかなくてもすでにその真部分体で $p$-イデアル類群全体が単項化する場合がある；（岩澤 [Iw], Cremona & Odoni [CO], 中野 [Na] 等参照）．特に虚2次体でこのような例を見つけることは，上の Proposition 1 のみならず，歴史的にも興味深い．実際，クロネッカーは，楕円関数の虚数乗法に注目して，イデアル類群と単項化定理との関連で虚2次体の「類体」にあたるものを発見し，単項化定理が成り立つ最小の不分岐アーベル拡大として「絶対類体」を構想した．

このような虚2次体の例はまだ知られていないが，$k$ がそうであるための必要十分条件は

（C）$G=\mathrm{Gal}(k''/k)$ の部分群 $N$ で，交換子群 $[G,G]$ $(=\mathrm{Gal}(k''/k'))$ を真部分群として含み，移送写像 $V_{G\to N}: G \to N/[N,N]$ が自明なものになってしまうものが存在する

ことである．我々の分類表のなかにはこれを満たすものがある（[M1], Proposition 14 参照）．

**Proposition 5.** 我々の群 $G$ で（1）$m=n=2$，または（2）$\mu=1 \le \nu$ の場合，三条件（A），（B），（C）をすべて満たすのは次のものである：

$$\mu=1,\ \nu=2,\ p\ge 3,\ m=2,\ n=p+1,$$

$$q_{1,j}=r_{1,j}=0 \quad (1\le j\le n-1),$$

$$r_{2,1}\equiv 0,\quad q_{2,1}\cdot r_{1,n}\not\equiv 0 \mod p.$$

特に $|G|=p^{p+5}$ であり，$G/[G,G]$ のタイプは $(p, p^2)$ である．

**7**. 上記では[M1]との関係もあって，特に $C(k)$ の $p$-ランクが2の場合を述べた．最後に筆者の [M2] で得られた最新の結果を紹介しておこう．一般に $C(k)$ の $p$-ランク $r$ が2以上であるとし，$C(k)$ の自分自身との交代積を $C(k)\wedge C(k)$ とする．良く知られているように，これは $C(k)$ のシュア・マルティプライアと同一視できる．野村 [No] をもとに，数学的帰納法によって次の定理が得られる．

**Theorem 1**. 上記の記号のもとで，$k$ は実または虚の2次体とし，$C(k)$ の $p$-ランク $r$ が2以上であるとする．このとき $C(k')$ の $p$-ランクは少なくとも $r(r-1)/2$ 以上 である．しかも $k'/k$ の最大不分岐中心拡大 $K$ のガロア群 $\mathrm{Gal}(K/k)$ は次の群 $D$ と同型であり，$\mathrm{Gal}(K/k')$ は $C(k)\wedge C(k)$ と同型である：

$$D=\langle a_i, c_{ij} \mid i=1,\dots,r,\ \ j=i+1,\dots,r\rangle,$$

$$a_i^{\varepsilon(i)} = c_{ij}^{\varepsilon(i)} = 1,\ \ i=1,\dots,r,\ \ j=i+1,\dots,r,$$

$$[a_i, a_j] = c_{ij},\ \ 1\le i<j\le r,$$

$$[a_i, c_{m,n}] = 1,\ \ i=1,\dots,r,\ \ 1\le m<n\le r;$$

ただしアーベル群 $C(k)$ のタイプは

$$(\varepsilon(1),\dots,\varepsilon(r)),\qquad p\le\varepsilon(1)\le\dots\le\varepsilon(r),$$

であるとする．

虚2次体の場合は，条件（A）によってさらに強いことが言える．

**Theorem 2**. 上記の記号のもとで，$k$ は虚2次体で，$C(k)$ の $p$-ランク $r$ が2以上であるとする．このとき $C(k')$ の $p$-ランクは少なくとも

$r^2-1$ 以上であり，$p$-類数 $|C(k')|$ についても次の不等式が成り立つ：

$$|C(k')| \geq |C(k) \wedge C(k)| \cdot \prod_{i=1}^{r} [C(k) : C(k)^{\varepsilon(i)}]/\varepsilon(i)$$

$$= |C(k) \wedge C(k)|^3.$$

## 文 献


[CO] J.E. Cremona and R.W.K. Odoni. A Generalization of a result of Iwasawa on the Capitulation Problem, Math. Proc. Camb. Phil. Soc. 107 (1990), 1-3.

[HS] F.-P. Heider und B. Schmithals. Zur Kapitulation der Idealklassen in unverzw eigten primzyklischen Erw e iterungen, Jour. reine angew. Math. 336 (1982), 1-25.

[Iw] K. Iwasawa. A Note on Capitulation Problem for Number Fields I, II; I, Proc. Japan Acad. 65, Ser.A,(1989), 59-61; II, ibid.,183-186.

[Ja] R. James. The Groups of Order $p^6$ ($p$ an Odd Prime), Math. of Computation 34, no.150 (1980), 613-637.

[M1] K. Miyake. Some $p$-Groups with two Generators which satisfy Certain Conditions arising from Arithmetic in Imaginary Quadratic Fields, Preprint Series 1991, N o.13, Coll.Gen. Educ., Nagoya Univ., 41pp. Submitted to Tôhoku Mathematical Journal.

[M2] _____. On the Ideal Class Groups of the $p$-Class Fields of Quadratic Number Fields, Preprint Series 1992, No.2, Coll. Gen. Educ., Nagoya Univ.

[Na] S. Nakano. 2次体上の単項化問題，当シムポジウムでの講演，(1991).

[No] A. Nomura. On the Existence of Unramified $p$-Extension, Osaka J. Math. 28 (1991), 55-62.

[Su] H. Suzuki. A Generalization of Hilbert's Theorem 94, Nagoya Math. J. 121 (1991), 161-169.