数理解析研究所講究録 1324 巻 2003 年 217-224

Quadratic reduction of multiplicative group and its applications

小川 裕之 (大阪大学大学院 理学研究科)

§1 序

乗法群の 2 次簡約化とは, 乗法群 $\mathbb{G}_{\mathrm{m}}$ を $\mathbb{P}^1-\{0,\infty\}$ とみなし, 体 k 上共役な α,β に対して, $\mathbb{P}^1$ 上の 1 次分数変換 $h: x\mapsto \frac{x-\alpha}{x-\beta}$ で $\mathbb{G}_{\mathrm{m}}$ を引き戻して得られる k 上の代数群 A^* のことを言う. $K=k(\alpha,\beta)$ は k の高々 2 次の拡大だが $K\neq k$ のとき, A^* の k-有理点全体のなす群 $A^*(k)$ の h よる像はノルム写像 $N_{K/k}: K^\times\to k^\times$ の核 $\ker N_{K/k}$ に等しい. A^* は, ノルム写像の核を下の体 k の言葉で記述する道具となり, 2-同種

$$(N_{K/k}, h^{-1}): K^\times\ni\xi\longmapsto(\xi\xi', h^{-1}(\xi/\xi'))\in k^\times\times A^*(k)$$

(ξ' は $\xi\in K$ の k 上の共役元) を得る. この 2-同種は, 複素平面の極座標変換

$$(|\cdot|,\arg): \mathbb{C}^\times\ni z=re^{i\theta}\longmapsto(r,\theta)\in\mathbb{R}^\times\times S^1$$

とよく似ている. 単位円 S^1 が $\mathbb{R}$ 上の群多様体なので, $K^\times$ の部分群としての $\ker N_{K/k}$ ではなく, $A^*(k)$ (k 上の群多様体の k-有理点のなす群) であることに意味がある. 複素数の場合にはノルム写像の平方根が通常の絶対値として $\mathbb{R}$ 上定義されるので極座標への座標変換 ($\mathbb{R}$ 上の群多様体としての同型) になったのだが, 一般の 2 次拡大 K/k では平方根が取れないので 2-同種にとどまり, 座標変換とは言えない. この多少の曖昧さはあっても, K で表現されていた整数論的性質を 2 次下の体 k の言葉で書くためのひとつの手段を与えたことになる. 直ちに思いつくのが Kummer 理論であろう. K を 1 の原始 N 乗根 ζ を含む体とする. このとき, "K 上の N 次巡回拡大体は, ある $a\in K^\times$ の N 乗根を添加 ($K(a^{1/N})$) して得られる" とか, "$\mathrm{Gal}(K(a^{1/N})/K)$ は $\langle a, K^{\times N}\rangle/K^{\times N}$ に同型である" とか. N が奇数の場合にだが, Kummer 理論として紹介してありそうなことのほとんどすべては, K の 2 次部分体 k (ζ は含まないが $\zeta+\bar{\zeta}$ を含む体) 上で A^* を使ったものに自然に拡張されることを, 本稿の 3 節でみる. 本稿とは異なった視点から, 小松亨氏も同様の結果 ([ko]) を得ている. 小松氏は, 橋本氏-三宅氏-陸名氏 ([HM], [HR]) の生成的巡回多項式のパラメータの空間の構造を詳しく調べ, その空間に加法演算を定義し, N が奇数の場合に Kummer 理論の類似を与えた ([Ko]). $N=3$ の場合には, Morton が Shanks の生成的 3 次巡回多項式に 2 次多項式写像のガロア理論 ([M1]) を使って Kummer 理論の類似を示した ([M2]) が, 煩雑で (簡明な) Kummer 理論の類似と思えない気がしないでもない. 橋本氏-三宅氏-陸名氏 ([HM], [HR]) の生成的巡回多項式は Shanks の 3 次巡回多項式を含んでいるので, 小松氏の結果は, Morton のものは真に含む形でより洗練された形で整理, 拡張したものと言える. また, もともと生成的巡回多項式をとっていたこともあり, パラメータを取り替えたときの巡回拡大体間の関係を調べるのが主要な議論となっっている. 本稿での立場, 方法はそれらとは異なる. k 上の代数群 A^* に関して Kummer 列を考え Hilbert 定理 90 の類似 (定理 3.1) を証明する. Kummer 理論で, 巡回拡大が Kummer

拡大になることの裏付け ("生成的" ということ) が Hilbert 定理 90 だったので, 本稿の立場では定理 3.1 が 3 節での最も重要な結果である. まだ完全なものはないが, 最終節で Kummer 理論以外にも幾つか応用について触れてみたい.

§2 乗法群の 2 次簡約化

k を体, $\overline{k}$ を k の分離閉包, $\Omega/\overline{k}$ を万有体とする. $\alpha, \beta \in \overline{k}$ に対して, 一次分数変換

$$h = h_{\{\alpha,\beta\}} : \mathbb{P}^1 \ni x \mapsto \frac{x-\alpha}{x-\beta} \in \mathbb{P}^1$$

を考える. 万有体 Ω において, 乗法群 $\mathbb{G}_{\mathrm{m}}$ は $\mathbb{P}^1$ から 0 と ∞ を取ったもの ($\mathbb{P}^1 - \{0, \infty\}$) と (代数的集合として) 同一視できる. この意味でここでは以下, $\mathbb{G}_{\mathrm{m}} = \mathbb{P}^1 - \{0, \infty\}$ とし, $\mathbb{P}^1 - \{0, \infty\}$ にもこの同一視により $\mathbb{G}_{\mathrm{m}}$ から来る乗法群の構造を入れておく. $A^* = A^*_{\alpha,\beta} = h^{-1}(\mathbb{P}^1 - \{0, \infty\})$ とおく. $h^{-1}(0) = \alpha$, $h^{-1}(\infty) = \beta$ だから, A^* は代数的集合としては $\mathbb{P}^1 - \{\alpha, \beta\}$ で, $k\{\alpha, \beta\}$ $(= k(\alpha+\beta, \alpha\beta))$ 上定義される. $k\{\alpha, \beta\}$ は, $k(\alpha, \beta)$ の高々 2 次の部分体である. この A^* にも $\mathbb{G}_{\mathrm{m}} = \mathbb{P}^1 - \{0, \infty\}$ から来る乗法群の構造が入る. 実際, $a, b \in A^*(\Omega)$ に対して,

$$a \otimes b = h^{-1}(h(a)\,h(b)) \qquad a^{[-1]} = h^{-1}(1/h(a))$$

で乗法および inverse が定義される. 具体的に計算すると,

$$a \otimes b = \frac{ab - \alpha\beta}{a+b-(\alpha+\beta)} \qquad a^{[-1]} = (\alpha+\beta) - a$$

なので, この乗法も inverse もまた $k\{\alpha, \beta\}$ 上定義される. また $h^{-1}(1) = \infty$ だから, ∞ がこの乗法の単位元になる.

命題 2.1 $(A^*_{\alpha,\beta}, \otimes, .^{[-1]}, \infty)$ は $k\{\alpha, \beta\}$ 上定義された代数群になる. 更に A^* は $k(\alpha, \beta)$ 上では乗法群 $\mathbb{G}_{\mathrm{m}}$ に代数群として同型である.

整数 m について, $x \in A^*$ の m 乗を $x^{[m]}$ と書く. つまり $m > 0$ のとき $x^{[m]} = x \otimes x \otimes \cdots \otimes x$ (m 個の積), $m = 0$ のとき $x^{[0]} = 1_{A^*} = \infty$, $m < 0$ のとき $x^{[m]} = (x^{[-m]})^{[-1]}$ と定義する.

以下の議論では表だって出てこないが, $A = h^{-1}(|P^1 - \{\infty\}) = \mathbb{P}^1 - \{\beta\}$ に

$$a \oplus b = h^{-1}(h(a) + h(b))$$

で加法を定義 (零元は $h^{-1}(0) = \alpha$) することで, $k(\alpha, \beta)$ 上の可換代数 A が定義される. 次節の実 Kummer 理論での, Hilbert 定理 90 の類似の証明に必要となるがここでは触れないことにする. (cf. [O])

上で定義した代数群 $A^* = A^*_{\alpha,\beta}$ が k 上定義されるためには, $k\{\alpha, \beta\} = k$ でなければならない. $k\{\alpha, \beta\} = k$ なるとき, 組 $\{\alpha, \beta\}$ を k-有理的と呼ぶ. k-有理的であるための必要十分条件は, (1) α と β がともに k に属するか, (2) α が k 上 2 次の元で β がその共役であるかのいずれかである. 以下, $\{\alpha, \beta\}$ は特に断らない限り k-有理的とする. k-有理的組 $\{\alpha, \beta\}$ から k-代数群 A^* がたくさん得られる. それらはすべて閉体 $\overline{k}$ 上で乗法群 Gm に同型であるが,

命題 2.2 k-有理的な $\{\alpha_1, \beta_1\}$, $\{\alpha_2, \beta_2\}$ に対して, k 上の代数群 $A^*_{\alpha_1,\beta_1}$ と $A^*_{\alpha_1,\beta_1}$ が k-代数群として k 上同型であるための必要十分条件は, $k(\alpha_1, \beta_1) = k(\alpha_2, \beta_2)$ である.

先ほどの k-有理的組の分類と考え合わせると, A^* の k-同型類は k 上の 2 次拡大体に対応する.

命題 2.3 次の対応は 1 対 1 である.

$$\{A^*_{\alpha,\beta} \mid \{\alpha,\beta\} \text{ は } k\text{-有理的}\}/_{k\text{-同型}} \longrightarrow \{K/k \mid K \text{ は } k \text{ 上高々 2 次の拡大体}\}$$
$$A^*_{\alpha,\beta} \mapsto k(\alpha,\beta)$$

以下, 高々 2 次の拡大 K/k に対して, K/k に対応する A^* の k-同型類を A^*_K と書くことにする. すなわち, k-有理的組 $\{\alpha,\beta\}$ で $k(\alpha,\beta)=K$ なるもの (これを K/k-有理的組と呼ぶ) について, $A^*_{\alpha,\beta}$ の属する k-同型類を A^*_K とする.

定義 2.4 高々 2 次の拡大 K/k に対して, A^*_K を K/k に関する乗法群 $\mathbb{G}_m$ の 2 次簡約化と呼ぶ.

$K=k$ のときは, k-代数群 A^*_k は乗法群 $\mathbb{G}_m$ に他ならないので, k-有理点 $A^*(k)$ は体 k の乗法群 $k^\times$ と見なせる. K/k が 2 次の拡大の場合, K 上では A^*_k は乗法群 $\mathbb{G}_m$ に同型なので $A^*_K(K)$ は体 K の乗法群 $K\times$ と考えてよい. 残るは K/k が 2 次の拡大の場合の k-有理点であるが,

命題 2.5 K/k が 2 次の拡大のとき, k-代数群 A^*_K の k-有理点 $A^*_K(k)$ は, 集合としては 代表の取り方によらず $\mathbb{P}(k)$ に等しい. 群としては, ノルム写像 $N_K/k : K^\times \longrightarrow k^\times$ の核 $\ker N_{K/k}$ に同型である.

上の繰り返しになるが, 2 次簡約化 A^*_K の真の意味は, ノルム写像 $N_{K/k}$ の核を k 上の代数群として表現したものになっている. 複素平面における通常の極座標表示

$$\begin{array}{ccc} \mathbb{C}^\times & \longleftrightarrow & \mathbb{R}^\times \times S^1 \\ z & \longrightarrow & (|z|, \arg(z/|z|)) \\ re^{i\theta} & \longleftarrow & (r,\theta) \end{array}$$

で, S^1 が $\mathbb{R}$ 上の群多様体であることに注意するなら,

$$\begin{array}{ccc} K^\times & \longrightarrow & k^\times \times A^*_K(k) \\ \xi & \longrightarrow & (N_{K/k}(\xi), h^{-1}(\xi/\xi')) \end{array}$$

(ξ' は ξ の k 上の共役) が, 一般の代数拡大における極座標表示の類似と見なすことができる. ただし, 複素数, 実数の場合と異なり, 平方根をとることが出来ないので, "2-同種" で "座標" と呼ぶべきものではないのだが. これを眺めていると, Tate 曲線 $E_q=\mathbb{C}^\times/\langle q\rangle$ の拡張について余計な一言を付け加えそうになるがやめておく.

そもそもの名前の付け方が悪かったのだが, この節の最後として A^*_K の "reduction" について述べる. 通常の仕方で k-代数群 A^*_K の reduction を定義する. k を代数体, K/k を高々 2 次の拡大体とする. ν を k の素点とし, k_ν で k の ν に関する完備化とする. 埋め込み $\overline{k} \hookrightarrow \overline{k_\nu}$ を固定する. この埋め込みによる K の ν に関する完備化を K_ν とする. K/k は代数体の高々 2 次の拡大であるが, K_ν/k_ν は局所体の高々 2 次の拡大で, k-代数群 (の k-同型類) A^*_K と同様に k_ν-代数群 (の k_ν-同型類) $A^*_{K_\nu}$ が定義される. 埋め込み $\overline{k} \hookrightarrow \overline{k_\nu}$ は代数群の射 $A^*_K \longrightarrow A^*_{K_\nu}$ を引き起こす. 更に ν が有限素点の場合, k の ν に関する剰余類体を $\mathfrak{f}_\nu$, K の剰余類体を $\mathfrak{F}_\nu$ とおく.

定義 2.6 ν が A^*_K の良い素点 (a good place) であるとは, ある K/k-有理的組 $\{\alpha,\beta\}$ で, α,β ともに ν-整数で, $\nu(\alpha-\beta)=0$ なるものが存在するときを言う.

ν が $A^*_{K/k}$ の良い素点であるなら, 上の定義で取った K/k-有理的組 $\{\alpha,\beta\}$ について, $\overline{\alpha}=\alpha \mod \nu$, $\overline{\beta}=\beta \mod \nu$ とおくと, $\mathfrak{f}_\nu$ 上の代数群 $A^*_{\overline{\alpha},\overline{\beta}}$ が定義される. $\{\overline{\alpha},\overline{\beta}\}$ は $\mathfrak{F}_\nu/\mathfrak{f}_\nu$-有理的組であるので, $A^*_{\overline{\alpha},\overline{\beta}}$ の $\mathfrak{f}_\nu$-同型類として $A^*_{\mathfrak{F}_\nu}$ が定義される. $A^*_{\mathfrak{F}_\nu}$ を単に $\overline{A^*_K}$ と書いて, A^*_K の reduction mod ν と呼ぶ. つまり, ν が良い素点であるなら, 通常の reduction map mod ν が k-代数群 A^*_K の reduction mod ν $\overline{A^*_K}$ を引き起こす.

命題 2.7 ν が K/k で不分岐で, 2 を割らないならば, ν は A^*_K の良い素点である.

§3 実 Kummer 理論

全節で定義した "乗法群の 2 次簡約化" の簡単な応用を述べる.

N を正の奇数とし, ζ を 1 の原始 N 乗根, $w=\zeta+\overline{\zeta}$ とする. 体 k として, $w\in k$ なるものをとり, $K=k(\zeta)$ とおく. 以下, $A^*=A_K^*$ と略記しする. 通常言う Kummer 理論は, 1 の原始 N 乗根を含む円分体 $\mathbb{Q}(\zeta)$ 上の N 次巡回拡大を $\mathbb{Q}(\zeta)$ の乗法群で記述する理論であるが, $\mathbb{Q}(\zeta)$ の最大実部分体 $\mathbb{Q}(\zeta+\overline{\zeta})$ 上の N 次巡回拡大を乗法群の 2 次簡約化 A^* で記述するのがここでの目標である.

$\eta=h^{-1}(\zeta)\in A^*$ とおく. $\zeta\in\ker N_{K/k}$ なので, η は k-有理点 ($\eta\in A^*(k)=\mathbb{P}^1(k)$) で, $\langle\eta\rangle$ は A^* の N 等分点のなす群に一致する ($A^*[N]=\langle\eta\rangle$). この G_k ($=\mathrm{Gal}(\overline{k}/k)$) 加群の完全列

$$1_{A^*}\longrightarrow A^*[N]\,(=\langle\eta\rangle)\longrightarrow A^*(\overline{k})\xrightarrow{[N]}A^*(\overline{k})\longrightarrow 1_{A^*}$$

長完全列をとると

$$\begin{aligned}1\longrightarrow H^0(\mathrm{G}_k,\langle\eta\rangle)\longrightarrow H^0(\mathrm{G}_k,A^*(\overline{k}))\xrightarrow{[N]}H^0(\mathrm{G}_k,A^*(\overline{k}))\\ \xrightarrow{\delta}H^1(\mathrm{G}_k,\langle\eta\rangle)\longrightarrow H^1(\mathrm{G}_k,A^*(\overline{k}))\xrightarrow{[N]}H^1(\mathrm{G}_k,A^*(\overline{k}))\end{aligned}$$

(δ は連結準同型). 従って N-Kummer 列

$$1\longrightarrow A^*(k)/A^*(k)^{[N]}\xrightarrow{\delta}H^1(\mathrm{G}_k,\langle\eta\rangle)\longrightarrow H^1(\mathrm{G}_k,A^*(\overline{k}))[N]\longrightarrow 1$$

を得る. ここで Hilbert 定理 90 の類似である次の定理が成り立つ.

定理 3.1 $H^1(\mathrm{G}_k,A^*(\overline{k}))[N]=\{1\}$

連結準同型 δ を具体的に書き下して,

系 3.2

$$\begin{array}{ccc}\delta:A^*(k)/A^*(k)^{[N]}&\xrightarrow{\sim}&H^1(\mathrm{G}_k,\langle\eta\rangle)\\ a&\longmapsto&\text{“}\sigma\mapsto\alpha^\sigma\oplus\alpha^{[-1]}\text{”}\end{array}$$

は同型写像である. ただし, $\alpha\in A^*(\overline{k})\subset\mathbb{P}^1(\overline{k})$ は, $\alpha^{[N]}=a$ なるものとする.

当初の目的 (実円分体上の Kummer 理論) には達したのだが, ここで得たものをより古典的 (より初等的 ?) に書き下してみたい. 理解を深めるするために, あるいは具体的な応用のために.

k はこれまでの様に $w=\zeta+\overline{\zeta}$ (ζ は 1 の原始 N-乗根) を含む体とする. $a\in A^*(k)$ に対して, k 上の方程式 $x^{[N]}=a$ の最小分解体を k_a とおく. k_a は "a の N 乗根の体" だから, Kummer 理論として自然に話をすすめればよい.

命題 3.3 k_a は k 上の巡回拡大体で, 拡大次数は N を割りきる.

命題 3.4 $x_a^{[N]}=a$ なる $x_a\in\overline{k}$ をとる. このとき, k_a は k 上 x_a を添加した体である. また, 任意の $\sigma\in\mathrm{Gal}(k_a/k)$ に対して, $\sigma(x_a)=\eta^{[j]}\otimes x_a$ (for $0\le\exists j<N$) が成り立つ.

命題 3.5 $a,\ a'\in A^*(k)$ とする. $k_a=k_{a'}$ であるための必要十分条件は, $\langle a,A^*(k)^{[N]}\rangle=\langle a',A^*(k)^{[N]}\rangle$ である.

命題 3.6 $\mathrm{Gal}(k_a/k)\simeq\langle a,A^*(k)^{[N]}\rangle/A^*(k)^{[N]}$

$A^*(k)$ の部分群 A で $A^*(k)^{[N]}$ を含み, $A^*(k)^{[N]}$ 上指数有限のもの $(A^*(k)^{[N]} < A < A^*(k))$ をとる. $k_A = \prod_{a \in A} k_a$ とおく. このとき, 上の命題より

命題 3.7 A, A' は $A^*(k)^{[N]}$ 上指数有限の $A^a st(k)$ の部分群とする. $k_A = K_{A'}$ となるための必要十分条件は, $A = A'$ である.

命題 3.8 k_A は k 上有限次アーベル拡大体で, $\mathrm{Gal}(k_A/k) \simeq A/A^*(k)^{[N]}$

でもって定理.

定理 3.9 L を k 上のアーベル拡大体で, ガロア群の巾指数が N を割り切るとする. このとき $A^*(k)^{[N]}$ を指数有限な部分群として含む $A^*(k)$ の部分群 A があって $(A^*(k)^{[N]} < A < A^*(k))$, $L = k_A$ と書ける.

(体の理論として) Kummer 理論になりました.

例 3.10 k_a/k の定義方程式 $f(x, a) = x^{[N]} - a = 0$ を幾つか計算してみる. 式の表示としてはすでに最も簡単な形になっているが, 既に良く知られているものとの比較もかねて, x の有理式 (多項式) として書き下してみる.

(1) $N = 3$ のとき

$\alpha = \zeta$, $\beta = \overline{\zeta}$ ととり, 代数群 $A^*_{\zeta,\overline{\zeta}}$ で $x^{[3]}$ を計算すると

$$x^{[3]} = \frac{x^3 - 3x - 1}{3x(x+1)}$$

よって

$$f(x, a) = \frac{x^3 - 3ax^2 - 3(a+1)x - 1}{3x(x+1)}$$

この分子は Shanks' symplest cubic と呼ばれるもので, 確かに 3 次巡回拡大体をすべて生成する. 分母は, $\eta = h^{-1}(\zeta) = -1$, $\eta^{[2]} = 0$ だから, $A^*[3] = \langle \eta \rangle = \{\infty, -1, 0\}$. つまり A^* の 3 等分多項式である.

α, β は k 上 $k(\zeta)$ を生成するものならどれでもよいのだが, 例えば α, β を $X^2 - (n+1)X + (n^2 - n + 1)$ (判別式は $-3(n-1)^2$) の根とし, $a = n^2/3$ ととれば, $f(x, a)$ の分子は Washington の 3 次巡回多項式 $x^3 - n^2x^2 + (n^3 - 2n^2 + 3n - 3)x + 1$ で, 分母は $A^*_{\alpha,\beta}$ の 3 等分多項式 $3(x-1)(x-n)$ にである.

α, β を $X^2 - (n^3 - n^2 - 1)X + (n^6 + n^5 + n^4 - 2n^3 - n^2 + 1) = 0$ (判別式は $-3(n^3 + n^2 - 1)^2$) の根とし, $a = -n(n^3 - 3)/3$ ととれば, $f(x, a)$ の分子は $x^3 + n(n^3 - 3)x^2 - (n^7 + 2n^6 + 3n^5 - n^4 - 3n^3 - 3n^2 + 3n + 3)x - 1$ で, 分母は $A^*_{\alpha,\beta}$ の 3 等分多項式 $3(x + n^2)(x - n^3 + 1)$ にである.

α, β を $X^2 - (n+1)^2X + (n^4 + n^3 + 3n^2 + n + 1) = 0$ (判別式は $-3(n^2+1)^2$) の根とし, $a = (n^3 + 2n^2 + 3n + 3)/3$ ととれば, $f(x, a)$ の分子は $x^3 - (n^3 + 2n^2 + 3n + 3)x^2 + n(n^2 + n + 3)(n^2 + 2)x + 1$ (岸康弘氏 [Ki]) で, 分母は $A^*_{\alpha,\beta}$ の 3 等分多項式 $3(x-n)(x-n^2-n-1)$ になる.

(2) $N = 5$ のとき

$\alpha = \zeta$, $\beta = \overline{\zeta}$ ととり, 上と同様に代数群 $A^*_{\zeta,\overline{\zeta}}$ で $x^{[5]}$ を計算して, 結局

$$f(x, a) = \frac{x^5 - 5ax^4 + 10w(a - 1 - w)x^3 - 10w(a+1)x^2 - 5(a-w)x - 1}{5x(x - 1 - w)(x-1)(x-w)}$$

$\eta = h^{-1}(\zeta) = -1$, $\eta^{[2]} = 0$, $\eta^{[3]} = w$, $\eta^{[4]} = w+1$ なので, 分母は $A^*[5]$ の 5 等分多項式である. $\eta^{[2]} = 0$ に注意して分子をよく見ると, x^4 の係数に $a-0$ が, x^3 の係数に $a-0^{[1]}$ が, x^2 の係数に $a-0^{[2]}$ が, x の係数に $a-0^{[3]}$ が現れている.

(3) 一般の奇数 N について

$f(x,a)$ の分子は x の monic N 次式で, 定数項は -1, x^{N-j} $(j=1,\cdots,N-1)$ の係数は, $(-1)^j {}_N C_j\,(a-0^{[j]}) \times$ (w の有理式としての $0^{[j]}$ の分母). $f(x,a)$ の分母は $N\prod_{j=1}^{N-1}(x-0^{[j]})$, $A^*[N]$ の N 等分多項式.

N が偶数の場合も含めて, $W\,(=\zeta+\bar{\zeta})$ を含む体上の N 次巡回拡大体の定義方程式については, ガロアの逆問題の立場から, 橋本喜一朗氏, 三宅克哉氏, 陸名雄一氏 (N が奇数の場合 [HM], N が偶数の場合 [HR]) によりすでに与えられている. 上で $\alpha=\zeta$, $\beta=\bar{\zeta}$ とおいて具体的に計算した, k_a の定義方程式 $x^{[N]}=a$ は, 橋本氏-三宅氏の式 ([HM]) そのものである. ここでの話は方程式を得ると言う立場からは何も新しいことは無いのだが, Kummer 理論として自然に導くことができたことで, 数論への応用が見えてくると思う.

Morton ([M2]) は, Shanks の 3 次巡回多項式 $x^3-ax^2-(a-3)x-1$ がパラメータ a について, 同じ体を表わす 2 つの a の間に一次分数変換で移りあう関係のあることを示し, 1 の原始 3 乗根を含まない場合に Kummer 理論の類似と思うことができると述べている. 命題 3.5 はより洗練された形でのその拡張と言うこともできる. $N=3$ の場合に限定して命題 3.5 を Morton の言い方に習うと,

系 3.11 $N=3$ とする. a をパラメータとする Shanks の 3 次巡回多項式 $g(x,a)=x^3-3ax^2-3(a+1)x-1$ について, $g(x,a)$ と $g(x,a')$ が k 上同じ 3 次巡回拡大体を生成するための必要十分条件は, ある $c\in k$ で a' が $\frac{(c^3-3c-1)a-3c(c+1)}{3c(c+1)a+c^3+3c^2-1}$ ($a\otimes c^{[3]}$ のこと) か $\frac{(c^3-3c-1)a-c^3+3c^2+6c+1}{3c(c+1)a-c^3-6c^2-3c+1}$ ($a^{[-1]}\otimes c^{[3]}$ のこと) に等しくなるようなものが存在する.

そもそも Morton は, 2 次多項式写像の繰り返し (iteration) のガロア群について研究していた. ([M1]) 3 次巡回体の場合, そのガロア群 σ による生成元 x の像 x^σ は x の 2 次多項式で書けるので, Shanks の 3 次巡回多項式で与えられた 3 次巡回体を Morton の 2 次巡回多項式の繰り返しのガロア群の立場から調べたのが, この系である. 元々の Morton の定式化も証明も, 煩雑で, たくさんの計算に頼ったやや冗長なものに思える. Chapman は Morton の証明を簡略化したが ([C]), それでも数式処理を必要とするようなものとなっている.

先ほども述べたが, 円分体の最大実部分体 $\mathbb{Q}(\zeta+\bar{\zeta})$ 上の N 次巡回拡大を生成する巡回多項式は, 橋本氏, 三宅氏, 陸名氏によって与えられている. 小松亨氏 ([Ko]) は, その多項式が同じ体を生成するためのパラメータの関係を調べるために, パラメータの空間に加法演算を定義し加法群の構造を持つことを示した. 小松氏の加法群, 加法演算は本稿の代数群の k-有理点 $A^*_{\zeta,\bar{\zeta}}(k)$, 群演算 $\otimes$ と同じもので, 本稿とは微妙に異なる部分もあるが本質的に同じ結果を得ている. 小松氏の研究は上で触れた Morton のアプローチによく似ているが, Morton のものより定式化, 証明ともに遥かに洗練されている. 小松氏の場合は, 生成的巡回多項式から始めたため, 本稿の定理 3.9 (巡回拡大体の生成定理) にあたるものは証明する必要のないものであった. 裏をかえせば, 本稿の定理 3.9 は, (N が奇数の場合にだが) 橋本氏-三宅氏の巡回多項式が生成的であることの Kummer 理論からの自然な説明を与えたことになっている.

この節の最後に, N 次巡回拡大 k_a/k における素イデアルの分解について簡単に触れておく. $\mathfrak{p}$ を k の $2N$ を割らない素イデアルとする. 命題 2.6 より $\mathfrak{p}$ は A^*_K の良い素点であるので, K/k-有

理的組 $\{\alpha, \beta\}$ があって, $\mathfrak{p} \nmid (\alpha-\zeta)^2$. ここで $d_{\alpha,\beta}(x) = (x-\alpha)(x-\beta)$ とおく. $a \in A^*_{\alpha,\beta}(k)$ とする.

命題 3.12 $a' = a \otimes h^{-1}_{\alpha,\beta}(-1)$ $(h^{-1}_{\alpha,\beta}(-1) = (\alpha+\beta)/2)$ とおく. このとき a か a' の少なくとも一方は $\mathfrak{p}$-整数である.

今 N は奇数だから $h^{-1}_{\alpha,\beta}(-1) \in A^*(k)^{[N]}$. 従って $k_a = k_{a'}$ である. 必要なら a と a' を取り替えて a は $\mathfrak{p}$-整数とする.

命題 3.13 $\mathfrak{p}$ が $d_{\alpha,\beta}(a)$ を割りきらないとする. このとき $\mathfrak{p}$ は k_a/k で不分岐で, 相対次数 $f_{\mathfrak{p}}(k_a/k)$ は $\bar{a}^f \in \overline{A^*_K}(\mathcal{O}/\mathfrak{p})^{[N]}$ なる最小の正の整数 f に等しい.

§4 応用 (?), 問題 (?)

代数群 A^*_K は, k 上の 2 次拡大体 K の乗法群で書かれたものを, k の言葉で
の最初の使い方として,

前節で円分体の最大実部分体の上で Kummer 理論が展開できることをみた. 数論の中での Kummer 理論の使われ方を考えれば, 前節の応用として多くのものを考えることができる. まだたいした結果は得られていないので寝言に等しいが, いくつか挙げてみる.

"3 を法とした, 2 次体の類数"
"$\mathbb{Q}(\sqrt{5})$ に関する鏡映"
"楕円曲線の 3-decent (Mordell-Weil rank の計算)"
"有限体上のガロア群 (Frobenius) についてのちょっと変った考え方"
"K/k を CM 拡大とする. K を CM にもつ k 上のアーベル多様体 A/k について"
"K を実 2 次体 $(k = \mathbb{Q})$ とする. K での連分数展開を $\mathbb{Q}$ の言葉で考える"
"K/k を CM でない 2 次拡大とする. K と k の単数群 (の自由部分) の差の部分の求め方"
"Tata 曲線. 2 次拡大 K/k について, $(q \in K^\times$ をうまくとって$)$ $K^\times/\langle q\rangle$ が k-構造をもつ"

…… あまりにひどいので, "$\mathbb{Q}(\sqrt{5})$ に関する鏡映" とは, どういったことを考えたいのか以下に触れる.

ζ を 1 の原始 5 乗根, $w = \zeta + \bar{\zeta}$ $(w^2 + w - 1 = 0)$, $A^* = A^*_{\zeta,\bar{\zeta}}$ ($\mathbb{Q}(w)$ 上の代数群) とおく, $K = \mathbb{Q}(\sqrt{d})$ を 2 次体とする. $K(w)$ は $\mathbb{Q}$ 上 (2, 2) 型ガロア拡大なので, K の他に $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{5})$, $K' = \mathbb{Q}(\sqrt{5\,D})$ を 2 次の部分体にもつ. K 上の 5 次巡回拡大 L をとる. $L(w)/K$ は 10 次巡回拡大で, $L(w)/K(w)$ は 5 次巡回拡大. 今 $K(w) \ni w = \zeta + \bar{\zeta}$ だから, 前節の実 Kummer 理論より, ある $a \in A^*(K(w))$ があって $L(w) = K(w)(a^{[1/5]})$ (a の 5 分体) となる. L は $K(w)(a^{[1/5]})$ の唯一つの 2 次部分体である. $L(w)$ の $\mathbb{Q}$ 上のガロア閉包を調べたい. $L(w)/K$ はガロアだったので, $L(w)$ の K' 上のガロア閉包を求めればよい. a の K' 上の共役元を a' とおく. $\mathbb{Q}(w)/\mathbb{Q}$ の共役写像は $K(w)/K'$ の共役写像を制限したもので, $\mathbb{Q}(w)$ 上の代数群 $(A^*, \otimes)$ をこの共役写像でうつしたものを $(A^{*\prime}, \otimes')$ とする. $a \in A^*(K(w))$ の共役 a' を $A^{*\prime}(K(w))$ の元と思って ($A^{*\prime}(K(w))$ は集合としては $A^*(K(w))$ と同じ) a' の 5 分体 $K(w)(a'^{[1/5]'})$ を考えると, $K(w)(a'^{[1/5]'})$ は K' 上の $L(w)$ の唯一の共役体である. A^* も $A^{*\prime}$ も 2 次拡大 $\mathbb{Q}(\zeta)/\mathbb{Q}(w)$ に関する $\mathbb{G}_{\mathrm{m}}$ の reduction だから $\mathbb{Q}(w)$ 上同型である. 実際 $A^{*\prime} \ni x \longmapsto (w+1)\,(x+1) \in A^*$ で, $K(w)(a'^{[1/5]'}) = K(w)(((w+1)(a'+1))^{[1/5]})$ $((w+1)(a'+1) \in A^*(K(w))$ の 5 分体) が従う. よって

命題 4.1 $a \in A^*(K(w))$ の $K(w)$ 上の 5 分点の体 $L(w) = K(w)(a^{[1/5]})$ が $\mathbb{Q}$ 上ガロアであるための必要十分条件は, $\langle a, A^*(K(w))^{[5]}\rangle = \langle (w+1)(a'+1), A^*(K(w))^{[5]}\rangle$ である.

命題 4.2 (i) $L(w)$ が $\mathbb{Q}$ 上ガロア拡大のとき, $L(w)/\mathbb{Q}$ のガロア群は $\mathbb{Z}/2\mathbb{Z} \times D_5$ に同型である. ここで D_5 は位数 10 の 2 面体群.
(ii) $L(w)$ が $\mathbb{Q}$ 上ガロア拡大でないとき, $L(w)$ の $\mathbb{Q}$ 上のガロア閉包は 100 次体で, そのガロア群は $\mathbb{Z}/2\mathbb{Z} \times ((\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z})$ に同型である.

今, K の類数が 5 で丁度 1 回だけ割れるとする. L を K 上の唯一の不分岐 5 次巡回拡大とすると, $L(w)$ は $\mathbb{Q}$ 上ガロア拡大でなければならない. 従って $L(w) = K(w)(a^{[1/5]})$ なる $a \in A^*(K(w))$ は上の命題の関係式を満たさねばならない. a を K' の整数論を使って与えることができたなら, $\mathbb{Q}(w)$ をはさんで K のイデアル類群の 5-part を K' の整数論で記述すると言う意味での "鏡映" を得たことになるのだが, これはなかなかうまくいかない.

例えば $a \in A^*(K(w))$ を $a \in K'$ から選ぶと, 大概の場合 a の 5 分点の体 $K(w)(a^{[1/5]}$ は $\mathbb{Q}$ 上ガロアでなくなる. (a を $a \in K'$ から選ぶことが重要なのではなく, K' の整数論から構成する良い方法を考えればよい.) 上で調べたガロア群の構造より $K(w)(a^{[1/5]})/K$ はガロア拡大 (10 次巡回拡大) になる. 唯一の K 上 5 次中間体を L とおく ($K(w)(a^{[1/5]}) = L(w)$ となる). K の判別式 D が 5 で割れているとし ($K(w)/K$ は不分岐), a をうまく選んで $L(w)/K(w)$ が不分岐になるようにとれたなら, L/K は不分岐 5 次巡回拡大になるので K の類数は 5 で割れる. $L(w)/\mathbb{Q}$ はガロア拡大でないので, 結局 K の類数は 25 で割れることになる.

参考文献

[C] R. J. Chapman, *Automorphism polynomials in cyclic cubic extensions*, J. Number Theory 61 (1996), no. 2, 283-291.

[HM] K. Hashimoto, K. Miyake, *Inverse Galois problem for dihedral groups*, "Number theory and its applications (Kyoto 1997)", 165-181, Dev. Math. **2**, Kluwer Acad. Publ., Dordrecht, 1999.

[HR] K. Hashimoto, Y. Rikuna, *On generic famiries of cyclic polynomials with even degree*, Manuscripta Math. **107** (2002), no. 3, 283-288.

[Ki] Y. Kishi, 基本単数を根に持つ 3 次巡回多項式の族について, 日本数学会 2001 年度秋期総合分科会, 九州大学

[Ko] T. Komatsu, *On a generic polynomial and abelian extensions*, preprint.

[M1] P. Morton, *Arithmetic properties of periodic points of quadratic maps*, Acta Arith. **62** (1992), 343-372.

[M2] ———, *Characterizing cyclic cubic extensoins by automorphism polynomials*, J. Number Theory **49** (1994), no. 2, 183-208.

[O] H. Ogawa, *Quadratic reduction of multiplicative group and its applications to numver theory*, preprint.

[S] D. Dhanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137-1152.

[W] L. C. Washington, *A family of cubic fields and zeros of 3-adis L-functions*, J. Number Theory **63** (1997), no. 2, 408-417.