2012/09/24(Mon.)

1　分解群 (および惰性群) の計算

さまざまな $\mathbb{Q}$ の拡大体について, そのガロア群, 分解群 (場合により惰性群,Frobenius 写像) を計算する.
ここで, 分解群, 惰性群,Frobenius 写像の定義について確認する.
体の拡大 L/K と,L 上の素イデアル w,K 上の素イデアル v, が定義されているものとし, w は v の上にあるとする.
このとき, **分解群** (Decomposition Group) $D(L/K,w)$ は以下のように定義できる.

$$D(L/K,w)=\{\sigma\in \mathrm{Gal}(L/K):\sigma(w)=w\}$$

また素イデアル v,w に対する有限群をそれぞれ $\mathrm{GF}_v,\mathrm{GF}_w$ とおくと, 自然な全射

$$D(L/K,w)\longrightarrow \mathrm{Gal}(\mathrm{GF}_w/\mathrm{GF}_v),\sigma\mapsto(x\in\mathrm{GF}_w\mapsto\sigma(x)\in\mathrm{GF}_w)$$

が定義できる ($D(L/K,w)$ の定義より σ では GF_q は変わらない).
この全単射の写像の核を**惰性群** (Inertia Group) といい,$I(L/K,w)$ と表す. 準同型定理より,

$$D(L/K,w)/I(L/K,w)\simeq \mathrm{Gal}(\mathrm{GF}_w/\mathrm{GF}_v)$$

である. また直接的には,

$$I(L/K,w)=\{\sigma\in D(L/K,w):\forall a\in\mathbb{Z}_L,\sigma(a)\equiv a\pmod w)\}$$

である.
また,$\mathrm{Gal}(\mathrm{GF}_w/\mathrm{GF}_v)$ は巡回群であるが, その生成元の一つであり,

$$\sigma\in\mathrm{Gal}(\mathrm{GF}_w/\mathrm{GF}_v),\forall a\in\mathbb{Z}_L,\sigma(a)\equiv a^{|\mathrm{GF}_w|}\pmod w$$

を満たす σ を w の (数論的)**Frobenius 置換/写像**といい,

$$\left[\frac{L/K}{w}\right]$$

と表記する.
この定義からわかるように, アーベル拡大でない場合は, 分解群, 惰性群,Frobenius 写像は w の取り方によって異なる場合がある. また, ガロア群 $\mathrm{Gal}(L/K)$ の正規部分群になっているとは限らない.
$\mathrm{Gal}(L/K)$ の部分群 $D(L/K,w),I(L/K,w)$ に対応する L の部分体をそれぞれ L_D,L_I とすると,

$$\{1\}\subset I(L/K,w)\subset D(L/K,w)\subset\mathrm{Gal}(L/K)$$

なので,

$$L\supset L_I\supset L_D\supset K$$

である (それぞれの拡大はガロア拡大である保証はない).
また w の**相対次数**とは,$\mathrm{GF}_w/\mathrm{GF}_v$ の拡大次数, つまり $\log_{|\mathrm{GF}_v|}|\mathrm{GF}_w|$ を表す.

以下で素イデアル w の分岐の仕方を示す.(正の整数 e, f, g を使う)
(i)$L_D/K(g$ 次)
$v = P_0P_1\cdots$ という形に素イデアル分解できる (各 P_i は互いに共役であるとは限らない). このとき w が P_0 の上にあるとしてよい. そうすると $w = P_0^e$ が成り立っている. またこのとき P_0 の相対次数は 1 である.
(ii)$L_I/L_D(f$ 次)
P_0 は分解されない. そのため相対次数は 1 から f になる.
(iii)$L/L_I(e$ 次) P_0 は分岐し,w になる. 相対次数は f のままである.
以上からわかることだが,$|\mathrm{Gal}(L/K)| = [L : K] = efg$ である.

この文書の目的はあくまでも計算であるため, 詳しい解説は該当する文書に委ねよう.

1.1 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$

$L = \mathbb{Q}(\zeta_8)$ とおく. また, ζ_8 は,1 の 8 乗根のうち, 偏角が正で最小のものとする.(つまり

$$\zeta_8 = \frac{1+\sqrt{-1}}{\sqrt{2}}$$

である.)
ζ_8 の最小多項式 $f(x)$ は,

$$f(x) = (x^8 - 1)/(x^4 - 1) = x^4 + 1$$

である. この拡大は円分拡大 (cyclotomic extension) と呼ばれている (1 のべき乗根を添加しているため). またこの拡大はガロア拡大であり, そのガロア群は

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$$

(ただし,

$$\sigma : \zeta_8 \mapsto \zeta_8^3, \sqrt{2} \mapsto -\sqrt{2}, \sqrt{-1} \mapsto -\sqrt{-1}$$
$$\tau : \zeta_8 \mapsto \zeta_8^5, \sqrt{2} \mapsto -\sqrt{2}, \sqrt{-1} \mapsto \sqrt{-1}$$

である.)
円分拡大であるため, また位数が 4(有理素数の 2 乗) であるため,$\mathrm{Gal}(L/\mathbb{Q})$ は可換群になる.
L の整数環を $\mathbb{Z}_L$ と書くと, (計算省略)$\mathbb{Z}_L = \mathbb{Z}[\zeta_8]$ なので, 任意の (有理) 素数 p に対して $p \nmid (\mathbb{Z}_L : \mathbb{Z}[\zeta_8])$ $(= 1)$ が成立する. よってすべての (有理) 素数 p に対して, 多項式の $\mathrm{mod}p$ での因数分解によってイデアル $p\mathbb{Z}[\zeta_8]$ の分解ができる.

1.1.1 $p = 2$ の場合

$$x^4 + 1 \equiv (x+1)^4 \pmod 2$$

より,

$$(2) = (2, \zeta_8 + 1)^4$$

と分解できる.($\mathfrak{P}_0 = (2, \zeta_8 + 1)$ とおく)
これからわかるように,(2) の上にある素イデアルは $\mathfrak{P}_0$ しかないため, 共役はすべて $\mathfrak{P}_0$ に一致する. よって

$$D(L/\mathbb{Q}, \mathfrak{P}_0) = \mathrm{Gal}(L/\mathbb{Q})$$

である. また

$$\mathrm{GF}(\mathfrak{P}_0) \simeq \mathrm{GF}(2) \simeq \mathbb{Z}/2\mathbb{Z}$$

であるため,$\mathfrak{P}_0$ の相対次数は 1 である. よって

$$I(L/\mathbb{Q}, \mathfrak{P}_0) = D(L/\mathbb{Q}, \mathfrak{P}_0)$$

である. Frobenius 写像は単位元 1 以外にはありえない.

1.1.2 $p = 5$ のとき

$$x^4 + 1 \equiv (x^2 + 2)(x^2 + 3) \pmod 5$$

より,

$$(2) = (5, \zeta_8^2 + 2)(5, \zeta_8^2 + 3)$$

と分解できる.($\mathfrak{P}_1 = (5, \zeta_8^2 + 2), \mathfrak{P}_2 = (5, \zeta_8^2 + 3)$ とおく)
σ, τ による作用は

$$\begin{aligned}
\sigma(\mathfrak{P}_1) &= (5, -\zeta_8^2 + 2) = (5, \zeta_8^2 + 3) = \mathfrak{P}_2 \\
\sigma(\mathfrak{P}_2) &= (5, -\zeta_8^2 + 3) = (5, \zeta_8^2 + 2) = \mathfrak{P}_1 \\
\tau(\mathfrak{P}_1) &= \mathfrak{P}_1 \\
\tau(\mathfrak{P}_2) &= \mathfrak{P}_2
\end{aligned}$$

よって,$\mathfrak{P}_1$ ないし $\mathfrak{P}_2$(アーベル拡大なのでどちらでも同じ) の分解群は

$$D(L/\mathbb{Q}, \mathfrak{P}_1) = \{1, \tau\} = \langle \tau \rangle$$

それに対応する中間体は

$$L_D = \mathbb{Q}(i)$$

事実,(5) は $L_D = \mathbb{Q}(i)$ で,

$$(5) = (i + 2)(i - 2)$$

と分解する.
$\mathfrak{P}_1$ の指数は 1 なので,L/L_I の拡大次数も 1, よって $L_I = L$ である.($I = \{1\}$ である.)
Frobenius 写像は τ である.

1.2 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

$L := \mathbb{Q}(\sqrt[3]{2}, \omega), M := \mathbb{Q}(\sqrt[3]{2})$ とおく.
$p = 5$ を M 上で素イデアル分解する.
$x^3 - 2 \equiv (x + 2)(x^2 - 2x + 4) \pmod 5$ より,

$$5\mathbb{Z}_M = (5, \sqrt[3]{2} + 2)(5, \sqrt[3]{4} - 2\sqrt[3]{2} + 4)$$

である.($\mathfrak{p}_0 = (5, \sqrt[3]{2}+2), \mathfrak{p}_1 = (5, \sqrt[3]{4}-2\sqrt[3]{2}+4)$ とおく)
$\mathfrak{p}_0$ と共役なイデアルは M 内には $\mathfrak{p}_0$ しか存在しないことに注意せよ.
今度は L 上で考える.

$$\theta = \sqrt[3]{2} - \omega$$

とおくと,θ の最小多項式は

$$g(x) = x^6 - 3x^5 + 6x^4 - 11x^3 + 12x^2 + 3x + 1$$

である. $(\mathbb{Z}_L : \mathbb{Z}[\theta]) = 3^5$ より,$p = 5$ は多項式の因数分解によって素イデアル分解ができる. 詳しい計算は後で行うが,

$$g(x) \equiv (x^2 - 2x - 2)(x^2 + 2x - 2)(x^2 + 2x - 1) \pmod 5$$

なので,

$$5\mathbb{Z}_L = (5, \theta^2 - 2\theta - 2)(5, \theta^2 + 2\theta - 2)(5, \theta^2 + 2\theta - 1)$$

である. (

$$\mathfrak{P}_2 = (5, \theta^2 - 2\theta - 2), \mathfrak{P}_3 = (5, \theta^2 + 2\theta - 2), \mathfrak{P}_4 = (5, \theta^2 + 2\theta - 1)$$

とおく.)
$\mathfrak{P}_2$ は $\mathfrak{p}_0$ の上にあり,$\mathfrak{p}_0 = \mathfrak{P}_2 \cap M$ が成り立っている.
ここで,$L/\mathbb{Q}$ のガロア群を求めると,

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

となる (ただし

$$\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \omega \mapsto \omega,$$
$$\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega \mapsto \omega^2$$

である). $\mathfrak{P}_2$ は τ で不変なので, また $1, \tau$ 以外の置換は $\mathfrak{P}_2$ を不変に保たないため,

$$D(L/\mathbb{Q}, \mathfrak{P}_2) = \{1, \tau\}, L_D = \mathbb{Q}(\sqrt[3]{2}) = M$$

(ここで,$D(L/\mathbb{Q}, \mathfrak{P}_2)$ は $\mathrm{Gal}(L/\mathbb{Q})$ の正規部分群になっていないことに注意すること.)
$\mathrm{Gal}(L/\mathbb{Q})$ の位数 2 の部分群は

$$\{1, \tau\}, \{1, \sigma\tau\}, \{1, \sigma^2\tau\}$$

の 3 個あるため, 素イデアル $\mathfrak{P}_2, \mathfrak{P}_3.\mathfrak{P}_4$, および中間体 $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}\omega), \mathbb{Q}(\sqrt[3]{2}\omega^2)$ に (順不同で) 対応していることが推測できる.
なお, どの場合についても惰性群は $\{1\}$ である. また,Frobenius 写像はそれぞれの群に含まれる 1 以外の元 $(\tau, \sigma\tau, \sigma^2\tau)$ 以外にはありえない.