《教科書 **問 4.10** および **問 16.10** に関する補足》

(2019 年 1 月 15 日)

「代数学 5 及び 6」で使用してゐる text **例 4.8**, **問 4.10** の $f(x) = x^8 - 24x^6 + 108x^4 - 144x^2 + 36$ は $\alpha = \sqrt{6 + 3\sqrt{2} + 2\sqrt{3} + 2\sqrt{6}}$ についての $\mathrm{irr}(\alpha, \mathbb{Q}, x)$ であることを証明したい. $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ が 8 次拡大であることを示せばよい. しかるに $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ であることは容易にわかるが, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$ を示さうとすれば, 結局 $f(x)$ の $\mathbb{Q}$ 上の既約性を示さねばならない. 通常なら, 適当な素数 p で還元して $f(x) \bmod p$ の既約性を示せばよいが, この場合は, いかなる素数 p に関しても $f(x) \bmod p$ は因数分解されて,

1 次式 8 個の積の型 $\cdots \frac{1}{8}$, 2 次式 4 つの積の型 $\cdots \frac{1}{8}$, 4 次式 2 つの積の型 $\cdots \frac{6}{8}$

の割合で因数分解される (Tschebotarev の密度定理). ゆゑに Eisenstein の判定法などは利用できない. しかし, 以下の様にすれば証明できる.

```
/*
  The field extension over the rationals generate by
     a = sqrt (6+3*sqrt(2)+2*sqrt(3)+2*sqrt(6)
  is Galois.  irr(a,Q,x) = f=x^8-24*x^6+108*x^4-144*x^2+36;
  This program shows it is indeed irreducible.
*/

factor(Mod(f,5))
> [Mod(1, 5)*x^4 + Mod(2, 5)*x^2 + Mod(3, 5) 1]
> [Mod(1, 5)*x^4 + Mod(4, 5)*x^2 + Mod(2, 5) 1]
factor(Mod(f,11))
> [Mod(1, 11)*x^4 + Mod(1, 11)*x^2 + Mod(6, 11) 1]
> [Mod(1, 11)*x^4 + Mod(8, 11)*x^2 + Mod(6, 11) 1]

\\ mod 5 や mod 11 でこの多項式になる様な Z 上の多項式が存在しないことを示せばよい.
{
for(i=1,2,
   for(j=1,2,
             b=factor(Mod(f,5))[i,1];
             c=factor(Mod(f,11))[j,1];
             print(chinese(b,c));
      )
   )};
/*
これらの解はそれぞれ
  Mod(1, 55)*x^4 + Mod(12, 55)*x^2 + Mod(28, 55)
  Mod(1, 55)*x^4 + Mod(52, 55)*x^2 + Mod(28, 55)
  Mod(1, 55)*x^4 + Mod(34, 55)*x^2 + Mod(17, 55)
  Mod(1, 55)*x^4 + Mod(19, 55)*x^2 + Mod(17, 55)
となるが, 定数項は 36 の約数でなければならないので, 探してゐる多項式は存在し得ない.
*/
```

《 教科書 **例 4.8** の拡大の Galois 群の元の計算 》

1. まづ $\boxed{\mathrm{id} = \sigma_0^+}$ である. さらに

$$\boxed{\sigma = \sigma_1^+} : \alpha \mapsto \alpha_1, \qquad \boxed{\tau = \sigma_2^+} : \alpha \mapsto \alpha_2$$

とおく. 教科書の**例 4.8** (p.5, $\ell.-6$) で述べた様に

$$\alpha\sigma(\alpha) = \alpha\alpha_1 = \sqrt{6}, \tag{1}$$

$$\alpha\tau(\alpha) = \alpha\alpha_2 = (1+\sqrt{2}\,)\sqrt{6}, \tag{2}$$

$$\alpha\alpha_3 = 3\sqrt{2} + 2\sqrt{3}. \tag{3}$$

2. $\sigma(\sqrt{2}\,) = -\sqrt{2}$, $\sigma(\sqrt{3}\,) = \sqrt{3}$, $\sigma(\sqrt{6}\,) = -\sqrt{6}$, $\tau(\sqrt{2}\,) = \sqrt{2}$, ... $(\sigma\tau)(\alpha^2) = {\alpha_3}^2$. $(\tau\sigma)(\alpha^2) = {\alpha_3}^2$. 教科書, **例 4.8** の β を使へば

$$\sigma(\beta) = \beta_1 = 3\sqrt{2} + 2\sqrt{3} - 2\sqrt{6},$$

がわかる. 4.8 にある計算と同じことを繰り返へせば

$$\frac{(\beta_1 - \frac{{\beta_1}^2 - 54}{12})^2 - 8}{4} = \sqrt{3} \in L$$

等がわかり,

$$\sigma(\sqrt{2}\,) = -\sqrt{2},\ \sigma(\sqrt{3}\,) = \sqrt{3}$$

を得る.

3. $\sigma(\alpha)\,\sigma(\alpha_2) = (1-\sqrt{2}\,)(-\sqrt{6}\,) > 0$, $\sigma(\alpha) = \alpha_1 > 0$ より $\sigma(\alpha_2) > 0$.

4. 次に

$$\tau^2 = \sigma^2 \ : \ \alpha \mapsto -\alpha \tag{4}$$

つまり $\boxed{\tau^2 = \sigma^2 = \sigma_0^-}$ であることを示さう. まづ (1) に σ を施せば

$$\sigma(\alpha)\sigma^2(\alpha) = \sigma(\sqrt{6}) = -\sqrt{6} = -\alpha\alpha_1 = -\alpha\sigma(\alpha).$$

より $\sigma^2(\alpha) = -\alpha$. また (2) に τ を施せば, $\tau(\alpha)\tau^2(\alpha) = -\tau((1+\sqrt{2})\sqrt{6}) = -(1+\sqrt{2})\sqrt{6} = -\alpha\alpha_2 = -\alpha\,\tau(\alpha)$ より $\tau^2(\alpha) = -\alpha$ だから. このことから $\sigma^4 = \tau^4 = \mathrm{id}$ で σ, τ の位数はともに 4 である.

5. よつて $\sigma^3(\alpha) = \sigma(-\alpha) = -\alpha_1 = \sigma_1^-(\alpha)$ でがわかる. つまり $\boxed{\sigma^3 = \sigma_1^-}$.
同様に $\boxed{\tau\sigma^2 = \tau^3 = \sigma_2^-}$ である.

6. $\boxed{\sigma\tau = \sigma_3^+}$. なぜなら, まづ $\sigma(\alpha_2)^2 = \sigma({\alpha_2}^2) = {\alpha_3}^2$ より $\sigma(\alpha_2) = \pm\alpha_3$ で, $\alpha_2 = \tau(\alpha)$ だから $(\sigma\tau)(\alpha) = \pm\alpha_3$. $\sigma(\alpha_2) > 0$ より $(\sigma\tau)(\alpha) = \sigma_3(\alpha)$. つまり $\sigma\tau = \sigma_3^+$.

7. (3) に $\tau\sigma$ を施せば (4) より $(\tau\sigma)(\alpha)\,\alpha = -3\sqrt{2} - 2\sqrt{3} = -\alpha\alpha_3$. ゆゑに $(\tau\sigma)(\alpha) = -\alpha_3 = (\sigma\tau)(-\alpha) = (\sigma\tau\sigma^2)(\alpha)$. とくに $\boxed{\tau\sigma = \sigma_3^- = \sigma\tau^3}$ であり $\sigma\tau\sigma = \tau$. これに $\sigma^2 = \tau^2$ を右から掛ければ $\sigma\tau\sigma^{-1} = \tau^3 = \tau^{-1}$ がわかり, $\sigma\tau = \tau^3\sigma = \tau\tau^2\sigma = \tau\sigma^2\sigma = \tau\sigma^3$ を得る. 同じく, 左から掛ければ $\sigma^{-1}\tau\sigma = \tau^3 = \tau^{-1}$ などの関係式が得られる.

問 16.10.0. p.2 の説明を, 詳細を省いてゐる箇所のすべてを補へ.
（または質問を提示せよ）.

問 16.10.1. $\sigma\tau = \tau\sigma^3$ であることを示せ.

問 16.10.2. $(\tau\sigma)^2(\alpha) = -\alpha$ であることを示せ.

問 16.10.3. $i = 1, 2, 3$ について, $\sigma^2(\alpha_i) = \tau^2(\alpha_i) = (\tau\sigma)^2(\alpha_i) = -\alpha_i$ であることを示せ.

問 16.10.4. 以上に基き, $G = \{\, 1,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \tau\sigma,\ \tau\sigma^2,\ \tau\sigma^3 \,\}$ の演算表を作れ :

左＼右	1	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
1								
σ								
σ^2								
σ^3								
τ								
$\tau\sigma$								
$\tau\sigma^2$								
$\tau\sigma^3$								

問 16.10.5. 上記の G の元を $\sigma = j, \tau = i, \tau\sigma = k$, $\sigma^2 = \tau^2 = (\tau\sigma)^2 = -1$ と書けば, $\sigma^3 = -j$, $\tau\sigma^2 = -i$, $\tau\sigma^3 = -k$ と書けて,

$$G = \{\, 1,\ i,\ j,\ k,\ -1,\ -i,\ -j,\ -k \,\},$$
$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i$$

となり, 覚え易くなる. これを 四元数群 と呼ぶ [1].

[1] 四元群とは別のものなので注意されたし.

《 **定理 16.1** (Galois の基本定理 1) の確認 》

定理 16.1 (Galois の基本定理 1) に述べられてゐる対応を, この場合について記述すれば, 以下の様になる.

$\mathscr{F}(L/K)$ は以下の全体	$\mathscr{G}(G)$ は以下の全体
$L = \mathbb{Q}(\alpha)$	$G^L = \{\, \sigma_0^+ \,\} = \{\, \mathrm{id} \,\} = \{1\},$
$= \mathbb{Q}(\alpha_1)$	$G^{K_1} = \{\, \sigma_0^+,\ \sigma_0^-,\ \sigma_2^+,\ \sigma_2^- \,\} = \{\, 1,\ \tau,\ \tau^2,\ \tau^3 \,\} = \langle \tau \rangle,$
$= \mathbb{Q}(\alpha_2)$	$G^{K_2} = \{\, \sigma_0^+,\ \sigma_0^-,\ \sigma_1^+,\ \sigma_1^- \,\} = \{\, 1,\ \sigma,\ \sigma^2,\ \sigma^3 \,\} = \langle \sigma \rangle,$
$= \mathbb{Q}(\alpha_3),$	$G^{K_{12}} = \{\, \sigma_0^+,\ \sigma_0^-,\ \sigma_3^+,\ \sigma_3^- \,\} = \{\, 1,\ \sigma\tau,\ \tau^2,\ \sigma^3\tau \,\} = \langle \sigma\tau \rangle,$
$M = \mathbb{Q}(\sqrt{2}, \sqrt{3}\,),$	$G^M = \{\, \sigma_0^+,\ \sigma_0^- \,\} = \{\, 1,\ \sigma^2 (= \tau^2) \,\} = \langle \sigma^2 \rangle,$
$K_1 = \mathbb{Q}(\sqrt{2}\,),$	$G^K = G.$
$K_2 = \mathbb{Q}(\sqrt{3}\,),$	
$K_{12} = \mathbb{Q}(\sqrt{6}\,),$	
$K = \mathbb{Q}.$