For Tutors

MeBio　数学テキスト

$x^5 - 5x + 12 = 0$ について

—Galois 群，巾根表示，類体論，整数環—

Edited by kamei

目 次

第 1 章

きっかけと他の例

筆者は医歯学部進学予備校メビオで数学講師として勤務しています．過日同僚の新家英太郎さんに「$\mathbb{Q}$ 上 Galois 群が A_5 になる代数拡大の例は」と尋ねられ，いろいろ計算している途中で $f(x)=x^5-5x+12=0$ なる「興味深い」方程式が見つかりました．この方程式の分解体 K の Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$ は A_5 ではなく D_5 ですが，A_5 と異なり可解群ですから，種々の整数論的現象の例として非常に具体的な数値を示すことができます．その際，数式ソフトが非常に有効です．整数であることがわかっている数を小数計算した結果，十分に整数に近い小数が得られたならその数が決定できたことにするわけです．（もちろん数学としてはその正当性を再確認する必要があります.）

筆者が学生の頃は万人が容易に使える数式ソフトなどなく，電卓レベルで計算するか自分でプログラムを組むかぐらいしかなかったのですが，今回数式ソフトを使ってみてその威力に驚きました．本稿ではその活用の仕方も紹介したいと思います．計算には Maxima と Excel を多用しました．

本稿で行ってみたのは次の事項です.

- Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$ を決定する，（実は D_5）
- 2 次の部分体 F を決定する.
- $f(x)=0$ の一つの解を α とするとき，他の解を $F(\alpha)$ の元として表す.
- α を巾根表示する.
- K を F の類体とみて，対応する射線 $\mathfrak{m}$ と同型 $\mathrm{Gal}(K/F)\simeq A_{\mathfrak{m}}/H_{\mathfrak{m}}$ を決定する.
- $K/\mathbb{Q}$ で分岐する素数 2, 5 の素因子に対し，その分解群，惰性群，分岐群を決定する.
- F の絶対類体を決定する.
- 判別式 $D(E/\mathbb{Q})$, $D(K/\mathbb{Q})$ を決定する.
- 整数環 $\mathcal{O}_E$, $\mathcal{O}_K$ を決定する.

これらについては 2 章で見ることにして，この章では Galois 群が $\mathbb{Z}/5\mathbb{Z}$ になる例と A_5 になる例を一つずつ紹介しておきましょう.

§1　5 次巡回拡大

ζ を 1 の複素 11 乗根とする．つまり $\zeta=\exp\dfrac{2\pi i}{11}=\cos\dfrac{2\pi}{11}+i\sin\dfrac{2\pi}{11}$ である．この場合円分体 $\mathbb{Q}(\zeta)$ は $\mathbb{Q}$ 上 10 次の巡回拡大であり,

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\simeq(\mathbb{Z}/11\mathbb{Z})^\times\simeq\mathbb{Z}/10\mathbb{Z}=<\sigma>$$

ここで σ は $\sigma(\zeta)=\zeta^2$ で定義される自己同型である.（ 2 は $(\mathbb{Z}/11\mathbb{Z})^\times$ の原始根である.）

従って $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ の位数 2 の部分群 $<\sigma^5>$ に対応する体 K が $\mathbb{Q}$ 上 5 次の巡回拡大になっている.
$\sigma^5:\zeta\to\zeta^{2^5}=\zeta^{32}=\zeta^{-1}$ は複素共役写像なので $K=\mathbb{Q}(\zeta)\cap\mathbb{R}$ でもある.

$\alpha=\zeta+\zeta^{-1}=2\cos\dfrac{2\pi}{11}(\fallingdotseq 1.682507065662362)$ と置くと

$$\begin{aligned}
\beta &= \sigma(\alpha) = \zeta^2+\zeta^{-2} &&= 2\cos\frac{4\pi}{11} && (\fallingdotseq 0.83083002600377),\\
\gamma &= \sigma^2(\alpha) = \zeta^4+\zeta^{-4} &&= 2\cos\frac{6\pi}{11} && (\fallingdotseq -0.28462967654657),\\
\delta &= \sigma^3(\alpha) = \zeta^8+\zeta^{-8} &&= 2\cos\frac{8\pi}{11} && (\fallingdotseq -1.30972146789057),\\
\epsilon &= \sigma^4(\alpha) = \zeta^5+\zeta^{-5} &&= 2\cos\frac{10\pi}{11} && (\fallingdotseq -1.918985947228995)
\end{aligned}$$

が α のすべての共役元であり，

$$\begin{aligned}
\alpha+\beta+\gamma+\delta+\epsilon &= -1\\
\alpha\beta+\alpha\gamma+\alpha\delta+\alpha\epsilon+\beta\gamma+\beta\delta+\beta\epsilon+\gamma\delta+\gamma\epsilon+\delta\epsilon &= -4\\
\alpha\beta\gamma+\alpha\beta\delta+\alpha\beta\epsilon+\alpha\gamma\delta+\alpha\gamma\epsilon+\alpha\delta\epsilon+\beta\gamma\delta+\beta\gamma\epsilon+\beta\delta\epsilon+\gamma\delta\epsilon &= 3\\
\alpha\beta\gamma\delta+\alpha\beta\gamma\epsilon+\alpha\beta\delta\epsilon+\alpha\gamma\delta\epsilon+\beta\gamma\delta\epsilon &= 3\\
\alpha\beta\gamma\delta\epsilon &= -1
\end{aligned}$$

であることが，展開しても数値的に計算してもわかる．

解と係数の関係より α の $\mathbb{Q}$ 上の最小定義式は $x^5+x^4-4x^3-3x^2+3x+1=0$ である．（つまり $K \simeq \mathbb{Q}[x]/(x^5+x^4-4x^3-3x^2+3x+1)$ ということになる．）

Maxima では

```
float(expand((x-2*cos(2*%pi/11))*(x-2*cos(4*%pi/11))*(x-2*cos(6*%pi/11))
*(x-2*cos(8*%pi/11))*(x-2*cos(10*%pi/11))));
```

と入力すればよい．

```
x^5+1.0*x^4-4.0*x^3-2.999999999999999*x^2+3.0*x+1.0
```

という結果が出力される．

参考 1　α は $x^5+x^4-4x^3-3x^2+3x+1=0$ の解であるが，$\mathbb{Q}$ 上 5 次巡回拡大の元であるからこの方程式は巾根で解ける．実際，

$$\alpha = 2\cos\frac{2\pi}{11} = \frac{1}{5}\left[\begin{array}{l}
-1+\sqrt[5]{-\frac{11}{4}\left\{89+25\sqrt{5}+5\sqrt{178\sqrt{5}-410}\right\}}\\
+\sqrt[5]{-\frac{11}{4}\left\{89-25\sqrt{5}+5\sqrt{-178\sqrt{5}-410}\right\}}\\
+\sqrt[5]{-\frac{11}{4}\left\{89-25\sqrt{5}-5\sqrt{-178\sqrt{5}-410}\right\}}\\
+\sqrt[5]{-\frac{11}{4}\left\{89+25\sqrt{5}-5\sqrt{178\sqrt{5}-410}\right\}}
\end{array}\right]$$

（Kamei_HP:http://www1.kcn.ne.jp/~mkamei/math/11th_root.pdf）

参考 2　ちなみに $(\alpha-\beta)(\beta-\gamma)(\gamma-\delta)(\delta-\epsilon)(\epsilon-\alpha)=11$ で，これは素イデアル (11) が完全分岐することを表す．

参考 3　$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ の位数 5 の部分群 $<\sigma^2>$ に対応する $\mathbb{Q}(\zeta)$ の部分体を F とする．$\eta=\zeta+\zeta^4+\zeta^5+\zeta^9+\zeta^3$ とおくと $\sigma(\eta)=\zeta^2+\zeta^8+\zeta^{10}+\zeta^7+\zeta^6$ であり，$\eta+\sigma(\eta)=-1$, $\eta\sigma(\eta)=3$ なので，η の定義方程式は $x^2+x+3=0$

であり，$\eta = \dfrac{-1 \pm \sqrt{-11}}{2}$ であることがわかる．（実は $\eta = \dfrac{-1 + \sqrt{-11}}{2}$ である．）
従って $F = \mathbb{Q}(\eta) = \mathbb{Q}(\sqrt{-11})$ である．

§ 2　5 次交代群 A_5

$f(x)$ を $\mathbb{Q}$ 上既約な 5 次方程式とし，K をその分解体としよう．$G = \mathrm{Gal}(K/\mathbb{Q})$ は $f(x) = 0$ の 5 解の置換群として 5 次対称群 S_5 の部分群である．明らかに K は $\mathbb{Q}$ 上の 5 次拡大体を含む．K がさらに 3 次拡大体も含むとしよう．この場合 $|G| = 15,\ 30,\ 60,\ 120$ であるが，S_5 には位数 15 や 30 の部分群は存在しないので，$G = S_5$ または $G = A_5$ となる．

また，$f(x) = 0$ の 5 解を $\alpha,\ \beta,\ \gamma,\ \delta,\ \epsilon$ とすると，解の差積 $\left(= \pm\sqrt{D(f)}\right)$

$$(\alpha-\beta)(\alpha-\gamma)(\alpha-\delta)(\alpha-\epsilon)(\beta-\gamma)(\beta-\delta)(\beta-\epsilon)(\gamma-\delta)(\gamma-\epsilon)(\delta-\epsilon)$$

が有理数であれば $G \subset A_5$，そうでなければ $G \not\subset A_5$ ということになる．

問題 1–2–1　$f(x) = x^5 + 20x + 16$ とする．

(1)　$f(x)$ は $\mathbb{Z}/3\mathbb{Z}$ 上既約であることを示せ．

(2)　$f(x) = 0$ の判別式を求め，それが $\mathbb{Q}^2$ に含まれることを確認せよ．

(3)　$f(x)$ を $\mathbb{Z}/7\mathbb{Z}$ 上で因数分解せよ．

(4)　$f(x)$ の分解体 K の $\mathbb{Q}$ 上のガロア群 $G = \mathrm{Gal}(K/\mathbb{Q})$ は $G \simeq A_5$ であることを示せ．

問題 2–1 **の解答**

(1)　$f(x) = 0$ は $\mathbb{Z}/3\mathbb{Z}$ で解を持たない．つまり $f(x)$ の因数に一次式はない．また，$\mathbb{Z}/3\mathbb{Z}$ の 2 次の既約多項式は $x^2+1,\ x^2+x+2,\ x^2+2x+2$ の 3 つであるが，これらのいずれでも割り切れない．つまり 2 次の因数も持たない．従って既約である．

(2)　一般に $f(x)$ を n 次既約多項式とすると，$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f,\ f')$ である．（ここで $R(f,\ f')$ は $f(x)$ と $f'(x)$ の終結式 (resultant) を表す．）　$f(x) = x^5 + ax + b$ の場合に計算すると，$D(f) = 4^4a^5 + 5^5b^4$ である．$a = 20, b = 16$ を代入して $D(f) = 2^{16} \cdot 5^6 \in \mathbb{Q}^2$.

(3)　$x^5 + 20x + 16 \equiv (x+2)(x+3)(x^3+2x^2-2x-2) \pmod 7$

(4)　(1) より G は位数 5 の元を含む．(2) より $G \subset A_5$ である．(3) より G は位数 3 の元を含む．上に述べた事実により $G = A_5$ である．

■

この拡大を色々調べていて次の（ほぼ自明な）事実に気づきました．

問題 1–2–2　$f(x)$ を，最高次の係数が 1 である，整数係数の既約な 5 次方程式とする．$f(x) = 0$ の分解体 K のガロア群が $\mathrm{Gal}(K/\mathbb{Q}) \subset A_5$ であれば，$f(x) \pmod p$ は 2 次 $\times 3$ 次に因数分解されることはない．

従って $f(x) \pmod p$ が $\mathbb{Z}/p\mathbb{Z}$ に解を持たなければ，それは $\mathbb{F}_p$ 上既約な 5 次方程式ということになります．

第 2 章

$x^5 - 5x + 12 = 0$

この章では $x^5 - 5x + 12 = 0$ について調べていきます.

§ 1　$\mathrm{Gal}(K/\mathbb{Q}) = D_5$

問題 2–1–1　$\mathbb{Q}$ 上 $x^5 - 5x + 12 = 0$ の分解体を K とする．そのガロア群を $G = \mathrm{Gal}(K/\mathbb{Q})$ とする．

(1)　$G = D_5$ であることを示せ.

(2)　K に含まれる 2 次体 F が $F = \mathbb{Q}(\sqrt{-10})$ であることを示せ.

解答

(1)　$D(f) = 4^5 \cdot (-5)^5 + 5^5 \cdot 12^4 = 2^8 \cdot 5^5(81-1) = 2^{12} \cdot 5^6 \in \mathbb{Q}^2$ より $G \subset A_5$ である．また $\mathbb{Z}/7\mathbb{Z}$ で $f(x) = x^5 - 5x + 12 = 0$ は解を持たないので $f(x)$ は $\mathbb{Z}/7\mathbb{Z}$ 上既約である．（∵ 問題 1–2–2）従って $|G|$ は 5 の倍数である.
また複素数体で考えると $x^5 - 5x + 12 = 0$ の解は 1 実 4 虚であることがわかるので，$|G|$ は 2 の倍数である.
次に $x^5 - 5x + 12 = 0$ の 5 解を x_1，x_2，x_3，x_4，x_5 とし，次の 6 つの数を考える.

$$\begin{aligned}
y_1 &= (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2 \\
y_2 &= (x_1x_2 + x_2x_3 + x_3x_5 + x_5x_4 + x_4x_1 - x_1x_3 - x_3x_4 - x_4x_2 - x_2x_5 - x_5x_1)^2 \\
y_3 &= (x_1x_2 + x_2x_4 + x_4x_3 + x_3x_5 + x_5x_1 - x_1x_4 - x_4x_5 - x_5x_2 - x_2x_3 - x_3x_1)^2 \\
y_4 &= (x_1x_2 + x_2x_4 + x_4x_5 + x_5x_3 + x_3x_1 - x_1x_4 - x_4x_3 - x_3x_2 - x_2x_5 - x_5x_1)^2 \\
y_5 &= (x_1x_2 + x_2x_5 + x_5x_3 + x_3x_4 + x_4x_1 - x_1x_5 - x_5x_4 - x_4x_2 - x_2x_3 - x_3x_1)^2 \\
y_6 &= (x_1x_2 + x_2x_5 + x_5x_4 + x_4x_3 + x_3x_1 - x_1x_5 - x_5x_3 - x_3x_2 - x_2x_4 - x_4x_1)^2
\end{aligned}$$

この 6 つを解とする 6 次方程式 $(y-y_1)(y-y_2)(y-y_3)(y-y_4)(y-y_5)(y-y_6)$ を作る．この方程式は x_1〜x_5 に関する対称式なので，有理整数係数である．実際に計算すると

$$y^6 + 200y^5 + 22000y^4 + 1120000y^3 + 28000000y^2 - 66016000000y + 1600000000 = 0$$

となる．ところがこの方程式は $y = 100$ を解に持つ．そこで $y_1 = 100$ ということにすれば，G の 5–Sylow 群は $(x_1\ x_2\ x_3\ x_4\ x_5)$ で生成されるものに限られる．$G \subset A_5$ と合わせて $G = D_5$ がわかる.

(2)　$x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1 = 10$ としてよい．この場合 $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 5$, $x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1 = -5$ ということになる．これを利用して $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_4)^2(x_4-x_5)^2(x_5-x_1)^2 = -4000$ がわかる（はず！）.
$\sqrt{-4000} = 20\sqrt{-10}$ より $F = \mathbb{Q}(\sqrt{-10})$ がわかった（ことにしよう）.

■

実は，実際にはこの方法はとっていません．まず Maxima で $x^5-5x+12=0$ の複素数解を求めました.

入力：`to_poly_solve([x^5-5*x+12=0], [x]);`

出力：
```
%union([x=-1.842085934630922],
 [x=-1.709561043370329*%i-0.35185424082737],
 [x=1.272897223922499-0.71979868148386*%i],
 [x=0.71979868148386*%i+1.272897223922499],
 [x=1.709561043370329*%i-0.35185424082737])
```

この 5 解を $x1,\ x2,\ x3,\ x4,\ x5$ として覚えさせておきます.

入力：
```
x1:-1.84208593463092;
 x2:-0.35185424082737+1.70956104337032*%i;
 x3:1.27289722392249-0.71979868148386*%i;
 x4:1.27289722392249+0.71979868148386*%i;
 x5:-0.35185424082737-1.70956104337032*%i;
```

$x2$ と $x5$, $x3$ と $x4$ を複素共役にしておくことがポイントです．（$D_5 =< (x1,\ x2,\ x3,\ x4,\ x5),\ (x2,\ x5)(x3,\ x4) >$ となるようにしておきたいので.）

$(x1-x2)^2(x2-x3)^2(x3-x4)^2(x4-x5)^2(x5-x1)^2$ を計算します.

入力：`expand((x1-x2)^2*(x2-x3)^2*(x3-x4)^2*(x4-x5)^2*(x5-x1)^2);`

出力：`-2.3560921448092964*10^-13*%i-3999.999853697214`

これはもう -4000 で間違いないでしょう．（上の解答で「はず！」と書いたのはこのことです.）だめなら x3 と x4 を入れ替えてやり直してみます．それでもだめなら $G=D_5$ ではありません.

§ 2　共役元を $F[\alpha]$ の元として表す

問題 2–2–1　$\mathbb{Q}$ 上 $x^5-5x+12=0$ の分解体を K とする．$F=\mathbb{Q}(\sqrt{-10})$ とする．$x^5-5x+12=0$ の一つの解を α とすると，α の共役元は F の元として次のように表されることを示せ．（$\mathrm{Gal}(K/F)\simeq\mathbb{Z}/5\mathbb{Z} =< \sigma >$ とする.）

$$\beta=\sigma(\alpha)=\left(-\frac{1}{8}\alpha^4-\frac{1}{8}\alpha^3-\frac{1}{8}\alpha^2-\frac{1}{8}\alpha+\frac{1}{2}\right)+\left(\frac{1}{80}\alpha^4+\frac{3}{80}\alpha^3+\frac{9}{80}\alpha^2-\frac{13}{80}\alpha-\frac{1}{20}\right)\sqrt{-10}$$

$$\gamma=\sigma^2(\alpha)=\left(\frac{1}{8}\alpha^4+\frac{1}{8}\alpha^3+\frac{1}{8}\alpha^2-\frac{3}{8}\alpha-\frac{1}{2}\right)+\left(\frac{1}{40}\alpha^4+\frac{3}{40}\alpha^3-\frac{1}{40}\alpha^2-\frac{3}{40}\alpha-\frac{1}{10}\right)\sqrt{-10}$$

$$\delta=\sigma^3(\alpha)=\left(\frac{1}{8}\alpha^4+\frac{1}{8}\alpha^3+\frac{1}{8}\alpha^2-\frac{3}{8}\alpha-\frac{1}{2}\right)-\left(\frac{1}{40}\alpha^4+\frac{3}{40}\alpha^3-\frac{1}{40}\alpha^2-\frac{3}{40}\alpha-\frac{1}{10}\right)\sqrt{-10}$$

$$\epsilon=\sigma^4(\alpha)=\left(-\frac{1}{8}\alpha^4-\frac{1}{8}\alpha^3-\frac{1}{8}\alpha^2-\frac{1}{8}\alpha+\frac{1}{2}\right)-\left(\frac{1}{80}\alpha^4+\frac{3}{80}\alpha^3+\frac{9}{80}\alpha^2-\frac{13}{80}\alpha-\frac{1}{20}\right)\sqrt{-10}$$

■

（Maxima では $\alpha=x1,\ \beta=x2,\ \gamma=x3,\ \delta=x4,\ \epsilon=x5$ と表している.）

参考 4

$\beta=\sigma(\alpha)=\left(-\frac{1}{8}\alpha^4-\frac{1}{8}\alpha^3-\frac{1}{8}\alpha^2-\frac{1}{8}\alpha+\frac{1}{2}\right)+\left(\frac{1}{80}\alpha^4+\frac{3}{80}\alpha^3+\frac{9}{80}\alpha^2-\frac{13}{80}\alpha-\frac{1}{20}\right)\sqrt{-10}$ を $f(x)=x^5-5x+12$ に代入すると

$$f(\beta)=[\left(401\,i-5\sqrt{10}\right)a^{20}+\left(2415\,i+335\sqrt{10}\right)a^{19}+\left(8135\,i+3085\sqrt{10}\right)a^{18}+\left(8345\,i+9585\sqrt{10}\right)a^{17}$$
$$+\left(17935\sqrt{10}-15955\,i\right)a^{16}+\left(1135\sqrt{10}-28097\,i\right)a^{15}+\left(-16185\,i-44115\sqrt{10}\right)a^{14}+\left(235185\,i-74215\sqrt{10}\right)a^{13}$$
$$+\left(198495\,i-131915\sqrt{10}\right)a^{12}+\left(79285\sqrt{10}-212555\,i\right)a^{11}+\left(-297731\,i-14945\sqrt{10}\right)a^{10}$$

$+\left(243995\sqrt{10}-2152845\,i\right)\,a^9+\left(1233495\,i+703645\sqrt{10}\right)\,a^8+\left(1003965\,i-601555\sqrt{10}\right)\,a^7$
$+\left(1029365\,i+806695\sqrt{10}\right)\,a^6+\left(5818947\,i-1560485\sqrt{10}\right)\,a^5+\left(45738\,10^{\frac{3}{2}}-10555380\,i\right)\,a^4$
$+\left(471408\,10^{\frac{3}{2}}-8869920\,i\right)\,a^3+\left(218048\,10^{\frac{3}{2}}-13383040\,i\right)\,a^2+\left(26402560\,i+139648\,10^{\frac{3}{2}}\right)\,a$
$+7781376\,i+3113472\,10^{\frac{3}{2}}]/(3276800\sqrt{10})$

が得られる．この α の 20 次方程式は $\alpha^5-5\alpha+12$ で割り切れることが確かめられる．（β は確かに解である！）

問題 2–1–2 の解法

K を複素数体 $\mathbb{C}$ の部分体と考える．先ほど見たように $\mathbb{C}$ における $f(x)=x^5-5x+12=0$ の解は

$$\begin{aligned}
\alpha &= -1.84208593463092,\\
\beta &= -0.35185424082737+1.70956104337032i,\\
\gamma &= 1.27289722392249-0.71979868148386i,\\
\delta &= 1.27289722392249+0.71979868148386i,\\
\epsilon &= -0.35185424082737-1.70956104337032i
\end{aligned}$$

の 5 つである．$\mathrm{Gal}(K/F)$ の生成元を σ, 複素共役写像を τ とする．ただし $\sigma(\alpha)=\beta$ となるように σ を選ぶ．

二面体群の構造により $\tau^{-1}\sigma\tau=\sigma^4$ でなければならない．これより σ は $(\alpha\ \beta\ \gamma\ \delta\ \epsilon)$ または $(\alpha\ \beta\ \delta\ \gamma\ \epsilon)$ と決まる．γ と δ は複素共役であり $\tau=(\beta\ \epsilon)(\gamma\ \delta)$ である．

以下 $\sigma=(\alpha\ \beta\ \gamma\ \delta\ \epsilon)$ と仮定する．（これでうまくいかないときは γ と δ を入れ替えてやればよい.）

$\beta=\sigma(\alpha)=a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4$ としよう．（ただし $a,\ b,\ c,\ d,\ e\in F$ である.）この等式に σ を作用させると

$$\begin{aligned}
\beta &= \sigma(\alpha)=a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4\\
\gamma &= \sigma(\beta)=a+b\beta+c\beta^2+d\beta^3+e\beta^4\\
\delta &= \sigma(\gamma)=a+b\gamma+c\gamma^2+d\gamma^3+e\gamma^4\\
\epsilon &= \sigma(\delta)=a+b\delta+c\delta^2+d\delta^3+e\delta^4\\
\alpha &= \sigma(\epsilon)=a+b\epsilon+c\epsilon^2+d\epsilon^3+e\epsilon^4
\end{aligned}$$

これを行列表示する．

$$\begin{pmatrix}\beta\\ \gamma\\ \delta\\ \epsilon\\ \alpha\end{pmatrix}=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3&\alpha^4\\ 1&\beta&\beta^2&\beta^3&\beta^4\\ 1&\gamma&\gamma^2&\gamma^3&\gamma^4\\ 1&\delta&\delta^2&\delta^3&\delta^4\\ 1&\epsilon&\epsilon^2&\epsilon^3&\epsilon^4\end{pmatrix}\begin{pmatrix}a\\ b\\ c\\ d\\ e\end{pmatrix}$$

これより

$$\begin{pmatrix}a\\ b\\ c\\ d\\ e\end{pmatrix}=\begin{pmatrix}1&\alpha&\alpha^2&\alpha^3&\alpha^4\\ 1&\beta&\beta^2&\beta^3&\beta^4\\ 1&\gamma&\gamma^2&\gamma^3&\gamma^4\\ 1&\delta&\delta^2&\delta^3&\delta^4\\ 1&\epsilon&\epsilon^2&\epsilon^3&\epsilon^4\end{pmatrix}^{-1}\begin{pmatrix}\beta\\ \gamma\\ \delta\\ \epsilon\\ \alpha\end{pmatrix}$$

これを数式計算ソフトなどで数値的に解く．wxMaxima だと次のような結果が得られる．

$$\begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0.49999999592506-0.15811387901572i \\ -0.12499999289094-0.51387012206986i \\ -0.1250000064251+0.35575623898989i \\ -0.12499999676365+0.11858540949798i \\ -0.12500000085652+0.039528472287642i \end{pmatrix}$$

この結果を $\mathbb{Q}(\sqrt{-10})$ の元として表示するのは容易である.

$$\begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} 0.49999999592506-0.15811387901572i \\ -0.12499999289094-0.51387012206986i \\ -0.1250000064251+0.35575623898989i \\ -0.12499999676365+0.11858540949798i \\ -0.12500000085652+0.039528472287642i \end{pmatrix} = \begin{pmatrix} \frac{1}{2}-\frac{1}{20}\sqrt{-10} \\ -\frac{1}{8}-\frac{13}{80}\sqrt{-10} \\ -\frac{1}{8}+\frac{9}{80}\sqrt{-10} \\ -\frac{1}{8}+\frac{3}{80}\sqrt{-10} \\ -\frac{1}{8}+\frac{1}{80}\sqrt{-10} \end{pmatrix}$$

（結果的にこれは γ, δ の選択が正しかったことを意味する．選択を逆にしていれば $\mathbb{Q}(\sqrt{-10})$ の元と見なせない値が出てくる.）

Maxima では次の通り.

入力：
```
A:matrix([1,x1,x1^2,x1^3,x1^4],[1,x2,x2^2,x2^3,x2^4],
 [1,x3,x3^2,x3^3,x3^4],[1,x4,x4^2,x4^3,x4^4],[1,x5,x5^2,x5^3,x5^4]);
 B:matrix([x2],[x3],[x4],[x5],[x1]);
 expand(A^^(-1).B);
```
結果：
```
matrix([0.49999999592506-0.15811387901572*%i],
 [-0.51387012206986*%i-0.12499999289094],
 [0.35575623898989*%i-0.1250000064251],
 [0.11858540949798*%i-0.12499999676365],
 [0.039528472287642*%i-0.12500000085652])
```

虚数部分を $\sqrt{-10}$ の有理数倍に直すには多少手間がかかる.（電卓を使って $\sqrt{10} \fallingdotseq 3.1622$ で割るだけだが.）それが面倒なら，最初から K を $\mathbb{Q}$ 上の 10 次拡大として扱えばよい.

$\beta = \sigma(\alpha) = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\sqrt{-10} + g\alpha\sqrt{-10} + h\alpha^2\sqrt{-10} + j\alpha^3\sqrt{-10} + k\alpha^4\sqrt{-10}$ としよう．（ただし $a \sim k \in \mathbb{Q}$ である．i を使用していないことに注意！）この等式に σ を作用させると

$$\begin{aligned}
\beta &= \sigma(\alpha) = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\sqrt{-10} + g\alpha\sqrt{-10} + h\alpha^2\sqrt{-10} + j\alpha^3\sqrt{-10} + k\alpha^4\sqrt{-10} \\
\gamma &= \sigma(\beta) = a + b\beta + c\beta^2 + d\beta^3 + e\beta^4 + f\sqrt{-10} + g\beta\sqrt{-10} + h\beta^2\sqrt{-10} + j\beta^3\sqrt{-10} + k\beta^4\sqrt{-10} \\
\delta &= \sigma(\gamma) = a + b\gamma + c\gamma^2 + d\gamma^3 + e\gamma^4 + f\sqrt{-10} + g\gamma\sqrt{-10} + h\gamma^2\sqrt{-10} + j\gamma^3\sqrt{-10} + k\gamma^4\sqrt{-10} \\
\epsilon &= \sigma(\delta) = a + b\delta + c\delta^2 + d\delta^3 + e\delta^4 + f\sqrt{-10} + g\delta\sqrt{-10} + h\delta^2\sqrt{-10} + j\delta^3\sqrt{-10} + k\delta^4\sqrt{-10} \\
\alpha &= \sigma(\epsilon) = a + b\epsilon + c\epsilon^2 + d\epsilon^3 + e\epsilon^4 + f\sqrt{-10} + g\epsilon\sqrt{-10} + h\epsilon^2\sqrt{-10} + j\epsilon^3\sqrt{-10} + k\epsilon^4\sqrt{-10}
\end{aligned}$$

またこれら 5 式の複素共役をとると

$$\begin{aligned}
\epsilon &= \tau(\beta)=a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4-f\sqrt{-10}-g\alpha\sqrt{-10}-h\alpha^2\sqrt{-10}-j\alpha^3\sqrt{-10}-k\alpha^4\sqrt{-10}\\
\delta &= \tau(\gamma)=a+b\epsilon+c\epsilon^2+d\epsilon^3+e\epsilon^4-f\sqrt{-10}-g\epsilon\sqrt{-10}-h\epsilon^2\sqrt{-10}-j\epsilon^3\sqrt{-10}-k\epsilon^4\sqrt{-10}\\
\gamma &= \tau(\delta)=a+b\delta+c\delta^2+d\delta^3+e\delta^4-f\sqrt{-10}-g\delta\sqrt{-10}-h\delta^2\sqrt{-10}-j\delta^3\sqrt{-10}-k\delta^4\sqrt{-10}\\
\beta &= \tau(\epsilon)=a+b\gamma+c\gamma^2+d\gamma^3+e\gamma^4-f\sqrt{-10}-g\gamma\sqrt{-10}-h\gamma^2\sqrt{-10}-j\gamma^3\sqrt{-10}-k\gamma^4\sqrt{-10}\\
\alpha &= \tau(\alpha)=a+b\beta+c\beta^2+d\beta^3+e\beta^4-f\sqrt{-10}-g\beta\sqrt{-10}-h\beta^2\sqrt{-10}-j\beta^3\sqrt{-10}-k\beta^4\sqrt{-10}
\end{aligned}$$

行列表示して

$$\begin{pmatrix}\beta\\ \gamma\\ \delta\\ \epsilon\\ \alpha\\ \epsilon\\ \delta\\ \gamma\\ \beta\\ \alpha\end{pmatrix}=\begin{pmatrix}
1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \sqrt{-10} & \alpha\sqrt{-10} & \alpha^2\sqrt{-10} & \alpha^3\sqrt{-10} & \alpha^4\sqrt{-10}\\
1 & \beta & \beta^2 & \beta^3 & \beta^4 & \sqrt{-10} & \beta\sqrt{-10} & \beta^2\sqrt{-10} & \beta^3\sqrt{-10} & \beta^4\sqrt{-10}\\
1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \sqrt{-10} & \gamma\sqrt{-10} & \gamma^2\sqrt{-10} & \gamma^3\sqrt{-10} & \gamma^4\sqrt{-10}\\
1 & \delta & \delta^2 & \delta^3 & \delta^4 & \sqrt{-10} & \delta\sqrt{-10} & \delta^2\sqrt{-10} & \delta^3\sqrt{-10} & \delta^4\sqrt{-10}\\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \epsilon^4 & \sqrt{-10} & \epsilon\sqrt{-10} & \epsilon^2\sqrt{-10} & \epsilon^3\sqrt{-10} & \epsilon^4\sqrt{-10}\\
1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & -\sqrt{-10} & \alpha\sqrt{-10} & -\alpha^2\sqrt{-10} & -\alpha^3\sqrt{-10} & -\alpha^4\sqrt{-10}\\
1 & \epsilon & \epsilon^2 & \epsilon^3 & \epsilon^4 & -\sqrt{-10} & \epsilon\sqrt{-10} & -\epsilon^2\sqrt{-10} & -\epsilon^3\sqrt{-10} & -\epsilon^4\sqrt{-10}\\
1 & \delta & \delta^2 & \delta^3 & \delta^4 & -\sqrt{-10} & \delta\sqrt{-10} & -\delta^2\sqrt{-10} & -\delta^3\sqrt{-10} & -\delta^4\sqrt{-10}\\
1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & -\sqrt{-10} & \gamma\sqrt{-10} & -\gamma^2\sqrt{-10} & -\gamma^3\sqrt{-10} & -\gamma^4\sqrt{-10}\\
1 & \beta & \beta^2 & \beta^3 & \beta^4 & -\sqrt{-10} & \beta\sqrt{-10} & -\beta^2\sqrt{-10} & -\beta^3\sqrt{-10} & -\beta^4\sqrt{-10}
\end{pmatrix}\begin{pmatrix}a\\ b\\ c\\ d\\ e\\ f\\ g\\ h\\ j\\ k\end{pmatrix}$$

数値的に解くと次の結果が得られる.

$$\begin{pmatrix}a\\ b\\ c\\ d\\ e\\ f\\ g\\ h\\ j\\ k\end{pmatrix}\fallingdotseq\begin{pmatrix}
0.49999999592506-2.9143354396410359\times10^{-16}\,i\\
-0.12499999289094-1.3877787807814457\times10^{-17}\,i\\
-0.1250000064251-8.6736173798840355\times10^{-18}\,i\\
-0.12499999676365+4.8572257327350599\times10^{-17}\,i\\
-0.12500000085652+2.7755575615628914\times10^{-17}\,i\\
-0.049999998737397-5.2662502028650513\times10^{-17}\,i\\
-0.16250000072495+1.5085612560290513\times10^{-17}\,i\\
0.11250000070232+3.4971192753400734\times10^{-17}\,i\\
0.037499999127739+1.5771322222121898\times10^{-17}\,i\\
0.01250000048558-1.3714193236627737\times10^{-18}\,i
\end{pmatrix}\fallingdotseq\begin{pmatrix}\frac{1}{2}\\ -\frac{1}{8}\\ -\frac{1}{8}\\ -\frac{1}{8}\\ -\frac{1}{8}\\ -\frac{1}{20}\\ -\frac{13}{80}\\ \frac{9}{80}\\ \frac{3}{80}\\ \frac{1}{80}\end{pmatrix}$$

Maxima では次の通り.

入力：
```
i:sqrt(-10);
C:matrix(
[1,x1,x1^2,x1^3,x1^4,i,x1*i,x1^2*i,x1^3*i,x1^4*i],
[1,x2,x2^2,x2^3,x2^4,i,x2*i,x2^2*i,x2^3*i,x2^4*i],
[1,x3,x3^2,x3^3,x3^4,i,x3*i,x3^2*i,x3^3*i,x3^4*i],
[1,x4,x4^2,x4^3,x4^4,i,x4*i,x4^2*i,x4^3*i,x4^4*i],
```

```
[1,x5,x5^2,x5^3,x5^4,i,x5*i,x5^2*i,x5^3*i,x5^4*i],
[1,x1,x1^2,x1^3,x1^4,-i,-x1*i,-x1^2*i,-x1^3*i,-x1^4*i],
[1,x5,x5^2,x5^3,x5^4,-i,-x5*i,-x5^2*i,-x5^3*i,-x5^4*i],
[1,x4,x4^2,x4^3,x4^4,-i,-x4*i,-x4^2*i,-x4^3*i,-x4^4*i],
[1,x3,x3^2,x3^3,x3^4,-i,-x3*i,-x3^2*i,-x3^3*i,-x3^4*i],
[1,x2,x2^2,x2^3,x2^4,-i,-x2*i,-x2^2*i,-x2^3*i,-x2^4*i]
);
D:matrix([x2],[x3],[x4],[x5],[x1],[x5],[x4],[x3],[x2],[x1]);
float(expand(C^^(-1).D));
```

出力：
```
matrix([0.49999999592506-2.914335439641035 9*10^-16*%i],
[-1.3877787807814457*10^-17*%i-0.12499999289094],
[-8.6736173798840355*10^-18*%i-0.1250000064251],
[4.8572257327350599*10^-17*%i-0.12499999676365],
[2.7755575615628914*10^-17*%i-0.12500000085652],
[-5.2662502028650513*10^-17*%i-0.049999998737397],
[1.5085612560290513*10^-17*%i-0.16250000072495],
[3.4971192753400734*10^-17*%i+0.11250000070232],
[1.5771322222121901*10^-17*%i+0.037499999127739],
[0.01250000048558-1.3714193236627739*10^-18*%i])
```

γ, δ, ϵ も同様にして α で表記することができる．$\beta = g(\alpha)$ を使って $\gamma = g(g(\alpha))$ として求めてもよい．

入力：
```
f(a):=(-a^4-a^3-a^2-a+4)/8+(a^4+3*a^3+9*a^2-13*a-4)*sqrt(10)*%i/80;
ratsimp(expand(remainder(f(f(a)),a^5-5*a+12)));
```

出力：
```
((2*%i+sqrt(10))*a^4+(6*%i+sqrt(10))*a^3+(sqrt(10)-2*%i)*a^2+(-6*%i-3*sqrt(10))*a
-8*%i-4*sqrt(10))/(8*sqrt(10))
```

§ 3　α の巾根表示

$\mathrm{Gal}(K/\mathbb{Q}) = D_5$ は可解群であるから，$x^5 - 5x + 12 = 0$ の解は巾根による表示ができるはずである．それを実行してみて次の結果を得た．この結果が数値的に正しいことは Excel などで容易に確認できる．試してみてください．

問題 2–3–1　　$x^5 - 5x + 12 = 0$ の実数解 α は

$$\alpha = -\frac{\sqrt{5}}{5}\left\{\left(50+25\sqrt{5}+15\sqrt{25+11\sqrt{5}}\right)^{\frac{1}{5}} + \left(50+25\sqrt{5}-15\sqrt{25+11\sqrt{5}}\right)^{\frac{1}{5}}\right.$$
$$\left. + \left(50-25\sqrt{5}+15\sqrt{25-11\sqrt{5}}\right)^{\frac{1}{5}} + \left(50-25\sqrt{5}-15\sqrt{25-11\sqrt{5}}\right)^{\frac{1}{5}}\right\}$$

と表される．（5 乗根は，実数になるようにとるものとする．）

解法

5 乗根を考えるときは $\mathbb{Q}(\zeta)$ (ζ は 1 の虚数 5 乗根) を含む体上で Kummer 拡大として考えないといけない．$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times = <\rho>$ とする．ただし $\rho(\zeta) = \zeta^2$ である．

合成体 $L = K(\zeta) = K \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta)$ で $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ であるから，σ, $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ は $\mathbb{Q}(\zeta)$ には自明に働くものとし，$\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ は K には自明に働くものとする．（τ は L においては複素共役

ではない.)　その場合 $\mathrm{Gal}(K/\mathbb{Q}(\zeta,\ \sqrt{-10}))\simeq(\mathbb{Z}/5\mathbb{Z})=<\sigma>$ と見なせる.

$\xi_1=\alpha+\beta\zeta+\gamma\zeta^2+\delta\zeta^3+\epsilon\zeta^4$ とする.

$$\begin{aligned}\sigma(\xi_1)&=\beta+\gamma\zeta+\delta\zeta^2+\epsilon\zeta^3+\alpha\zeta^4=\zeta^4\xi_1\\ \sigma^2(\xi_1)&=\gamma+\delta\zeta+\epsilon\zeta^2+\alpha\zeta^3+\beta\zeta^4=\zeta^3\xi_1\\ \sigma^3(\xi_1)&=\delta+\epsilon\zeta+\alpha\zeta^2+\beta\zeta^3+\gamma\zeta^4=\zeta^2\xi_1\\ \sigma^4(\xi_1)&=\epsilon+\alpha\zeta+\beta\zeta^2+\gamma\zeta^3+\delta\zeta^4=\zeta\xi_1\end{aligned}$$

なので，ξ_1 の $\mathbb{Q}(\zeta,\sqrt{-10})$ 上の定義方程式は $x^5-{\xi_1}^5=0$ である．つまり $p={\xi_1}^5\in\mathbb{Q}(\zeta,\sqrt{-10})$ である．$p={\xi_1}^5\fallingdotseq-11825.3969776668$ であることが計算できる．

ξ_1 の K 上の共役根

$$\begin{aligned}\xi_3=\rho(\xi_1)&=\alpha+\beta\zeta^2+\gamma\zeta^4+\delta\zeta+\epsilon\zeta^3\\ \xi_2=\rho(\xi_1)&=\alpha+\beta\zeta^4+\gamma\zeta^3+\delta\zeta^2+\epsilon\zeta\\ \xi_4=\rho(\xi_1)&=\alpha+\beta\zeta^3+\gamma\zeta+\delta\zeta^4+\epsilon\zeta^2\end{aligned}$$

に関しても $q={\xi_2}^5,\ r={\xi_3}^5,\ s={\xi_4}^5\in\mathbb{Q}(\zeta,\sqrt{-10})$ であり，$q\fallingdotseq-14.77267873205662,\ r\fallingdotseq-862.396670,\ s\fallingdotseq 202.5666600975$ であることが計算できる．

入力：
```
z:float(cos(2*%pi/5)+%i*sin(2*%pi/5));
p1:float(expand((x1+x2*z+x3*z^2+x4*z^3+x5*z^4)^5));
p2:float(expand((x1+x2*z^4+x3*z^3+x4*z^2+x5*z)^5));
p3:float(expand((x1+x2*z^2+x3*z^4+x4*z+x5*z^3)^5));
p4:float(expand((x1+x2*z^3+x3*z+x4*z^4+x5*z^2)^5));
```
出力：
```
0.95105651629515*%i+0.30901699437495
6.0364841916384809*10^-12*%i-11825.39697766701
-1.4357171605926014*10^-14*%i-14.77267873205694
-2.4772845069178972*10^-13*%i-862.3966700885505
202.5666600975604-1.5548718446744785*10^-13*%i
```

$(p=p1,\ q=p2,\ r=p3,\ s=p4$ とおいた.)

すべて実数なので，$\mathbb{Q}(\zeta,\sqrt{-10})\cap\mathbb{R}=\mathbb{Q}(\sqrt{5},\sqrt{5+\sqrt{5}})$ の元になっているはずである（後出).

$$\begin{aligned}p+q+r+s&=-12500=-2^2\times5^5\\ pq+pr+ps+qr+qs+rs&=7812500=2^2\times5^9,\\ pqr+pqs+prs+qrs&=1953125000=2^2\times5^{12},\\ pqrs&=-30517578125=5^{15}\end{aligned}$$

より $p,\ q,\ r,\ s$ は $x^4+12500x^2-7812500x^2-1953125000x-30517578125=0$ の 4 解であるが，$p+q$ と $r+s$ が $\mathbb{Q}(\sqrt{5})$ 上共役であることを考慮すると $p+q=-6250-2500\sqrt{5},\ r+s=-6250+2500\sqrt{5}$ であることに気づく．また，pq と rs が $\mathbb{Q}(\sqrt{5})$ 上共役であることを考慮すると $pq=78125\sqrt{5},\ rs=-78125\sqrt{5}$ であることに気づく．

$p,\ q$ は $x^2+(6250+2500\sqrt{5})x+78125\sqrt{5}=0$ の解なので，

$$\begin{aligned}p&=-(3125+1250\sqrt{5})-\sqrt{(3125+1250\sqrt{5})^2-78125\sqrt{5}}=-25\sqrt{5}\left\{50+25\sqrt{5}+15\sqrt{25+11\sqrt{5}}\right\}\\ q&=-(3125+1250\sqrt{5})+\sqrt{(3125+1250\sqrt{5})^2-78125\sqrt{5}}=-25\sqrt{5}\left\{50+25\sqrt{5}-15\sqrt{25+11\sqrt{5}}\right\}\end{aligned}$$

同様にして

$$r = -25\sqrt{5}\left\{50 - 25\sqrt{5} + 15\sqrt{25 - 11\sqrt{5}}\right\}$$
$$s = -25\sqrt{5}\left\{50 - 25\sqrt{5} - 15\sqrt{25 - 11\sqrt{5}}\right\}$$

も得る．ξ_1，ξ_2，ξ_3，ξ_4 は実数なので，それぞれ $p^{\frac{1}{5}}, q^{\frac{1}{5}}, r^{\frac{1}{5}}, s^{\frac{1}{5}}$ である．(5 乗根は実数をとればよい．)

$$\xi_1 + \xi_2 + \xi_3 + \xi_4 = 4\alpha + (\beta + \gamma + \delta + \epsilon)(\zeta^2 + \zeta^3 + \zeta^4) = 4\alpha - (\beta + \gamma + \delta + \epsilon) = 5\alpha$$

なのだから

$$\alpha = \frac{\xi_1 + \xi_2 + \xi_3 + \xi_4}{5} = \frac{1}{5}\left(p^{\frac{1}{5}} + q^{\frac{1}{5}} + r^{\frac{1}{5}} + s^{\frac{1}{5}}\right)$$

となり，問題の結果を得る． ■

実 4 次体 $\mathbb{Q}(\zeta, \sqrt{-10}) \cap \mathbb{R} = \mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}})$ について．

$\mathbb{Q}(\zeta, \sqrt{-10}) \cap \mathbb{R} = \mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}})$ であることを示しておこう．

$$\begin{tikzcd}
 & & \mathbb{Q}(\sqrt{-10}, \zeta) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
 & \mathbb{Q}(\sqrt{-10}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & M \arrow[d, dash] & \mathbb{Q}(\zeta) \arrow[dl, dash] \\
\mathbb{Q}(\sqrt{-10}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash] & \\
 & \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & \{e\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
 & <\rho^2> \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & <\tau\rho^2> \arrow[d, dash] & <\tau> \arrow[dl, dash] \\
<\rho> \arrow[dr, dash] & <\tau\rho> \arrow[d, dash] & <\tau, \rho^2> \arrow[dl, dash] & \\
 & <\tau, \rho> & &
\end{tikzcd}$$

$\mathrm{Gal}(\mathbb{Q}(\sqrt{-10})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} =< \tau >$, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} =< \rho >$ より $\mathrm{Gal}(\mathbb{Q}(\zeta, \sqrt{-10})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ である．この場合の部分体とガロア群の対応は図のようになっている．$\mathbb{Q}(\sqrt{-10}, \sqrt{5})$, $\mathbb{Q}(\zeta)$ ともに実ではないので，最大実部分体は $< \tau\rho^2 >$ に対応する部分体 M でなければならない．この M を具体的に書きたい．

背反方程式 $\zeta\ 4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ を ζ^2 で割り，$\left(\zeta + \frac{1}{\zeta}\right)^2 + \left(\zeta + \frac{1}{\zeta}\right) - 2 = 0$ と変形した上で解くと $\zeta + \frac{1}{\zeta} = \frac{-1+\sqrt{5}}{2}$ を得る．これは $2\cos\frac{2\pi}{5}$ の値である．これを $\zeta^2 - \frac{-1+\sqrt{5}}{2}\zeta + 1 = 0$ と変形して解くと $\zeta = \frac{-1 + \sqrt{5} + \sqrt{10 + 2\sqrt{5}}i}{4}$ となる．これは $\frac{\sqrt{10+2\sqrt{5}}}{4} = \sin\frac{2\pi}{5}$ を意味する．

従って $\sqrt{10 + 2\sqrt{5}}i \in \mathbb{Q}(\zeta, \sqrt{-10})$ であり，この数は純虚数である．一方 $\sqrt{2}i \in \mathbb{Q}(\zeta, \sqrt{-10})$ でもあり，この数も純虚数なので $\frac{\sqrt{10+2\sqrt{5}}i}{\sqrt{2}i} = \sqrt{5+\sqrt{5}} \in \mathbb{Q}(\zeta, \sqrt{-10})$，しかもこの数は実数なので，$\sqrt{5+\sqrt{5}} \in M$ とわかる．$\sqrt{5+\sqrt{5}} \notin \mathbb{Q}(\sqrt{5})$ は明らかなので，$M = \mathbb{Q}(\sqrt{5+\sqrt{5}})$ といえる． ■

これによると $p = {\xi_1}^5 = -25\sqrt{5}\left\{50 + 25\sqrt{5} + 15\sqrt{25 + 11\sqrt{5}}\right\} \in \mathbb{Q}(\sqrt{5+\sqrt{5}})$ であるから，$\sqrt{25 + 11\sqrt{5}}$ の部分が $\sqrt{5+\sqrt{5}}$ の整式としてかけるはずである．これについては次の通り．

$$\sqrt{25 + 11\sqrt{5}} = \frac{3+\sqrt{5}}{2}\sqrt{5+\sqrt{5}}$$

$\mathbb{Q}(\sqrt{5})$ の基本単数が $\epsilon = \frac{1+\sqrt{5}}{2}$ であることを使って導くことができる．

問題 2–3–1 の別のアプローチ

$\eta=\sqrt{5+\sqrt{5}}$ とすると $M=\mathbb{Q}(\eta)$ の $\mathbb{Q}$ 上の基底として $1,\ \eta,\ \eta^2,\ \eta^3$ がとれる．$p=a+b\eta+c\eta^2+d\eta^3$ $(a,\ b,\ c,\ d\in\mathbb{Q})$ とおいて，共役 4 式で行列表示すれば $a,\ b,\ c,\ d$ を求めることができる．
$\eta_1=\eta=\sqrt{5+\sqrt{5}}, \eta_2=\sqrt{5-\sqrt{5}}, \eta_3=-\sqrt{5+\sqrt{5}}, \eta_4=-\sqrt{5-\sqrt{5}}$ としよう．

$$\begin{pmatrix} a\\ b\\ c\\ d\end{pmatrix}=\begin{pmatrix}1 & \eta_1 & {\eta_1}^2 & {\eta_1}^3\\ 1 & \eta_2 & {\eta_2}^2 & {\eta_2}^3\\ 1 & \eta_3 & {\eta_3}^2 & {\eta_3}^3\\ 1 & \eta_4 & {\eta_4}^2 & {\eta_4}^3\end{pmatrix}^{-1}\begin{pmatrix} p\\ s\\ q\\ r\end{pmatrix}\fallingdotseq\begin{pmatrix}3124.999948700116\\ 1874.999955502734\\ -1249.999973055091\\ -562.4999865392979\end{pmatrix}\fallingdotseq\begin{pmatrix}3125\\ 1875\\ -1250\\ -562.5\end{pmatrix}$$

これより $p=3125+1875\eta-1250\eta^2-\dfrac{1125}{2}\eta^3$ が得られる．

入力：
```
m1:float(expand(sqrt(5+sqrt(5))));
m2:float(expand(sqrt(5-sqrt(5))));
m3:float(expand(-sqrt(5+sqrt(5))));
m4:float(expand(-sqrt(5-sqrt(5))));
E:matrix([1,m1,m1^2,m1^3],[1,m2,m2^2,m2^3],[1,m3,m3^2,m3^3],[1,m4,m4^2,m4^3]);
F:matrix([p1],[p4],[p2],[p3]);
float(expand(E^^(-1).F));
```
出力：
```
matrix([3124.999948628592-2.1871478927161307*10^-12*%i],
[1874.999955545879-6.5021237791705725*10^-13*%i],
[7.1837514778689194*10^-13*%i-1249.999973045221],
[2.452860552504883*10^-13*%i-562.4999865452656])
```

$$\begin{aligned}
& 3125+1875\eta-1250\eta^2-\frac{1125}{2}\eta^3\\
= & \ 3125+1875\sqrt{5+\sqrt{5}}-1250(5+\sqrt{5})-\frac{1125}{2}(5+\sqrt{5})\sqrt{5+\sqrt{5}}\\
= & \ -3125-1250\sqrt{5}+\frac{1875-1125\sqrt{5}}{2}\sqrt{5+\sqrt{5}}
\end{aligned}$$

より最初に得た結果と一致することが確認される．

§ 4 Artin symbol $\left(\dfrac{K/F}{\mathfrak{p}}\right)$

K/F は Abel 拡大だから F の類体である．従ってある法 $\mathfrak{m}$ に対するイデアル群 $H_{\mathfrak{m}}$ に対して同型 $\mathrm{Gal}(K/F)\simeq A_{\mathfrak{m}}/H_{\mathfrak{m}}$ が成り立つはずである．この $\mathfrak{m}$ と $H_{\mathfrak{m}}$ を見ておきたい．（極端に簡単ではない類体論の実例として，無意義ではないと思われる．）

p を $F/\mathbb{Q}$ で分解する素数とする．分解する条件は

$$p \text{ は } F/\mathbb{Q} \text{ で分解} \iff \left(\frac{-10}{p}\right)=1 \iff p\equiv 1,\ 7,\ 9,\ 11,\ 13,\ 19,\ 23,\ 37 \pmod{40}$$

このような素数 p の素因子 $\mathfrak{p}$ に対する Artin symbol $\left(\dfrac{K/F}{\mathfrak{p}}\right)$ の値を，多く計算してみよう．$\beta, \gamma, \delta, \epsilon$ が $F[\alpha]$ の元として表されているので，Frobenius 置換の結果がどの元と一致するかを見るのは数式ソフトを使えば容易で

ある．多くの結果から $A_{\mathfrak{m}} \to \mathrm{Gal}(K/F)$ の kernel $H_{\mathfrak{m}}$ が見えてくる．

例 1 ：$(7,\ 2+\sqrt{-10})$

$F=\mathbb{Q}(\sqrt{-10})$ では素イデアル (7) は $(7)=\mathfrak{p}_1\mathfrak{p}_2$ と分解される．ここで $\mathfrak{p}_1=(7,\ 2+\sqrt{-10}),\mathfrak{p}_2=(7,\ 2-\sqrt{-10})$．従って　$\bmod \mathfrak{p}_1$ では $\sqrt{-10}\equiv -2$ であり，

$$\begin{aligned}
\beta &\equiv (-\alpha^4-\alpha^3-\alpha^2-\alpha+4)-2(5\alpha^4+\alpha^3+3\alpha^2+5\alpha+1)\equiv 3\alpha^4+4\alpha^3-4\alpha+2\\
\gamma &\equiv (\alpha^4+\alpha^3+\alpha^2-3\alpha+4)-2(3\alpha^4+2\alpha^3-3\alpha^2-2\alpha+2)\equiv 2\alpha^4-3\alpha^3+\alpha-1\\
\delta &\equiv (\alpha^4+\alpha^3+\alpha^2-3\alpha+4)+2(3\alpha^4+2\alpha^3-3\alpha^2-2\alpha+2)\equiv -2\alpha^3+2\alpha^2\\
\epsilon &\equiv (-\alpha^4-\alpha^3-\alpha^2-\alpha+4)+2(5\alpha^4+\alpha^3+3\alpha^2+5\alpha+1)\equiv 2\alpha^4+\alpha^3-2\alpha^2+2\alpha-1
\end{aligned}$$

一方 $\mathbb{F}_7[x]$ で $x^5-5x+12$ は既約であるから，$\mathfrak{p}_1$ は $\mathcal{O}_K$ においても素イデアルであり，$\mathcal{O}_K/\mathfrak{p}_1\simeq\mathbb{F}_{7^5}$ は $\mathcal{O}_F/\mathfrak{p}_1\simeq\mathbb{F}_7$ の 5 次拡大である．$\mathrm{Gal}(\mathbb{F}_{7^5}/\mathbb{F}_7)$ は Frobenius 置換 $\tau: x\mapsto x^7$ で生成される．

従って α の τ による共役は

$$\begin{aligned}
\tau(\alpha) &\equiv \alpha^7\equiv -2\alpha^3+2\alpha^2\equiv\delta\equiv\sigma^3(\alpha)\\
\tau^2(\alpha) &\equiv 3\alpha^4+4\alpha^3-4\alpha+2\equiv\beta\equiv\sigma(\alpha)\\
\tau^3(\alpha) &\equiv 2\alpha^4+\alpha^3-2\alpha^2+2\alpha-1\equiv\epsilon\equiv\sigma^4(\alpha)\\
\tau^4(\alpha) &\equiv 2\alpha^4-3\alpha^3+\alpha-1\equiv\gamma\equiv\sigma^2(\alpha)
\end{aligned}$$

であることが確かめられる．つまり $\left(\dfrac{K/F}{\mathfrak{p}_1}\right)=\sigma^3$ である．共役をとって $\left(\dfrac{K/F}{\mathfrak{p}_2}\right)=\sigma^2$ であることもわかる．

例 2 ：$\mathfrak{q}_1=(11,\ 1+\sqrt{-10})$

$\mathcal{O}_K/\mathfrak{q}_1\simeq\mathbb{F}_{11^5}$ は $\mathcal{O}_F/\mathfrak{q}_1\simeq\mathbb{F}_{11}$ の 5 次拡大である．$\mathrm{Gal}(\mathbb{F}_{11^5}/\mathbb{F}_{11})$ は Frobenius 置換 $: x\mapsto x^{11}$ で生成される．この Frobenius 置換は σ に一致する．$\left(\left(\dfrac{K/F}{\mathfrak{q}_1}\right)=\sigma,\ \left(\dfrac{K/F}{\mathfrak{q}_2}\right)=\sigma^4\right)$

例 3 ：$\mathfrak{r}_1=(13,\ 4+\sqrt{-10})$

$\mathcal{O}_K/\mathfrak{r}_1\simeq\mathbb{F}_{13^5}$ は $\mathcal{O}_F/\mathfrak{r}_1\simeq\mathbb{F}_{13}$ の 5 次拡大である．$\mathrm{Gal}(\mathbb{F}_{13^5}/\mathbb{F}_{13})$ は Frobenius 置換 $: x\mapsto x^{13}$ で生成される．この Frobenius 置換は σ^4 に一致する．$\left(\left(\dfrac{K/F}{\mathfrak{r}_1}\right)=\sigma^4,\ \left(\dfrac{K/F}{\mathfrak{r}_2}\right)=\sigma\right)$

例 4 ：(3)

平方剰余記号 $\left(\dfrac{-10}{3}\right)=\left(\dfrac{2}{3}\right)=-1$ より $F/\mathbb{Q}$ では (3) は remain prime である．Frobenius 置換は $x\mapsto x^9$ であるが，$x^9\equiv x\ (\bmod 3,\ x^5-5x+12)$ より $\left(\dfrac{K/F}{(3)}\right)=e$．これは (3) が K/F で完全分解することを意味する．実際

$$x^5-5x+12\equiv x\left(x-1-\sqrt{-10}\right)\left(x-1+\sqrt{-10}\right)\left(x+1-\sqrt{-10}\right)\left(x+1+\sqrt{-10}\right)$$

例 5 ：$\mathfrak{s}_1=(3+\sqrt{-10})$

$\mathcal{O}_K/(3+\sqrt{-10}) \simeq \mathbb{F}_{19^5}$ は $\mathcal{O}_F/(3+\sqrt{-10}) \simeq \mathbb{F}_{19}$ の 5 次拡大である．Gal($\mathbb{F}_{19^5}/\mathbb{F}_{19}$) は Frobenius 置換 : $x \mapsto x^{19}$ で生成される．この Frobenius 置換は σ^2 に一致する．$\left(\left(\dfrac{K/F}{\mathfrak{s}_1}\right)=\sigma^2,\ \left(\dfrac{K/F}{\mathfrak{s}_2}\right)=\sigma^3\right)$

反省

最初はこの方法で，多数の $\pmod{\mathfrak{p}}$ に関する α の共役元の表示を集めれば，mod をとらない標数 0 での表示が見えてくるはずと思っていましたが，挫折しました．K の整数環を $\mathcal{O}_F[\alpha]$ と思い込んでいたために，β の表記の係数が $\pmod{\mathfrak{p}}$ を増やすたびに大きくなっていってしまったのです．理由に気づかずかなり悩みましたが，まさか分数係数のせいだとは思いませんでした．分数係数とわかっていれば，この方法でも解にたどり着けたかもしれません．

最初に判別式をとった時点で，D が異常に 2 でよく割れることから整数環がもっと小さいことに気づいておくべきでした．

その他の p に対する Artin symbol の値も調べてみたのが次の表である．

素数 p	素イデアル $\mathfrak{p}$	Frob(α)	$\left(\dfrac{K/F}{\mathfrak{p}}\right)$
7	$(7,\ 2+\sqrt{-10})$	$a^7 \equiv 5a^3+2a^2$	σ^3
11	$(1+\sqrt{-10})$	$a^{11} \equiv 3a^3+a^2+a$	σ
13	$(13,\ 4+\sqrt{-10})$	$a^{13} \equiv 10a^4+a^3+8a+12$	σ^4
19	$(3+\sqrt{-10})$	$a^{19} \equiv a^4+17a^3+4a^2+16a+15$	σ^2
23	$(23,\ 6+\sqrt{-10})$	$9\alpha^4+10\alpha^3+13\alpha^2+2\alpha+10$	σ
37	$(37,\ 8+\sqrt{-10})$	$36\alpha^4+6\alpha^3+29\alpha^2+3\alpha+4$	σ^2
41	$(1+2\sqrt{-10})$	$16\alpha^4+17\alpha^3+15\alpha^2+34\alpha+18$	σ^2
47	$(47,\ 15+\sqrt{-10})$	$32\alpha^4+14\alpha^3+7\alpha^2+17\alpha+13$	σ
53	$(53,\ 19+\sqrt{-10})$	$50\alpha^4+4\alpha^3+43\alpha^2+9\alpha+12$	σ^2
59	$(7+\sqrt{-10})$	$18\alpha^4+39\alpha^3+56\alpha^2+5\alpha+46$	σ^3
89	$(7+2\sqrt{-10})$	$46\alpha^4+27\alpha^3+59\alpha^2+x+83$	σ
103	$(103,\ 14+\sqrt{-10})$	$67\alpha^4+21\alpha^3+89\alpha^2+80\alpha+41$	σ^4
127	$(127,\ 25+\sqrt{-10})$	α	e
131	$(11+\sqrt{-10})$	$116\alpha^4+119\alpha^3+128\alpha^2+95\alpha+60$	σ
139	$(7-3\sqrt{-10})$	$114\alpha^4+99\alpha^3+54\alpha^2+80\alpha+100$	σ
157	$(157,\ 33+\sqrt{-10})$	α	e
167	$(167,\ 18+\sqrt{-10})$	$79\alpha^4+28\alpha^3+130\alpha^2+97\alpha+18$	σ^2
173	$(173,\ 63+\sqrt{-10})$	$19\alpha^4+100\alpha^3+111\alpha^2+116\alpha+97$	σ^3
179	$(13+\sqrt{-10})$	$143\alpha^4+26\alpha^3+81\alpha^2+108\alpha+144$	σ^2
197	$(197,\ 37+\sqrt{-10})$	α	e
211	$(11+3\sqrt{-10})$	$60\alpha^4+127\alpha^3+204\alpha^2+31\alpha+182$	σ^3
223	$(223,\ 92+\sqrt{-10})$	α	e
241	$(9-4\sqrt{-10})$	$97\alpha^4+231\alpha^3+151\alpha^2+123\alpha+94$	σ^4
251	$(1+5\sqrt{-10})$	α	e
263	$(263,\ 76+\sqrt{-10})$	$110\alpha^4+x^3+219\alpha^2+196\alpha+86$	σ^2

$\mathfrak{p}=(127,\ 25+\sqrt{-10})$ は単項ではないが，K/F で完全分解する．実際
$x^5-5x+12 \equiv (x-4)(x-34)(x-46)(x-62)(x-108) \pmod{127}$ が確かめられる．$(157,\ 33+\sqrt{-10})$, $(197,\ 37+\sqrt{-10})$, $(223,\ 92+\sqrt{-10})$ も同様に完全分解する．

また 251 の素因子 $(1+5\sqrt{-10})$ は単項であってなおかつ K/F で完全分解する．このような素数の特徴付けを

後で問題にしておいた．

さて，これらのデータを元に Artin map の kernel となるイデアル群を見つけたい．

$\mathcal{O}_F$ の類数は 2 である．表を利用して，拡大 K/F に対応するイデアル群 H に含まれる単項イデアルをあげてみると，

- そのまま単項素イデアルである素数
  $(3),\ (17),\ (29),\ (31),\ (43),\ (61),\ (67),\ (71),\ (73),\ (79),\ (83),\ (97),\ \cdots.$
- $F/\mathbb{Q}$ では分解するが，$\left(\dfrac{K/F}{(p)}\right) = \left(\dfrac{K/F}{\mathfrak{p}}\right)\left(\dfrac{K/F}{\bar{\mathfrak{p}}}\right) = e$ となってしまう素数
  $(7),\ (11),\ (13),\ (19),\ (23),\ (37),\ (41),\ (47),\ (53),\ (59),\ (89),\ (103),\ \cdots$
- 表から $\left(\dfrac{K/F}{\mathfrak{p}}\right)\left(\dfrac{K/F}{\mathfrak{q}}\right) = e$ となる 組み合わせを選んでできる単項イデアル

$\mathfrak{p}$	$\mathfrak{q}$	$\mathfrak{pq}$	$\left(\frac{K/F}{\mathfrak{p}}\right)$	$\left(\frac{K/F}{\mathfrak{q}}\right)$
$(7,\ 2+\sqrt{-10})$	$(37,\ 8+\sqrt{-10})$	$(3+5\sqrt{-10})$	σ^3	σ^2
$(7,\ 2+\sqrt{-10})$	$(53,\ 19+\sqrt{-10})$	$(11-5\sqrt{-10})$	σ^3	σ^2
$(7,\ 2+\sqrt{-10})$	$(167,\ 18+\sqrt{-10})$	$(13+10\sqrt{-10})$	σ^3	σ^2
$(7,\ 2+\sqrt{-10})$	$(173,\ 63-\sqrt{-10})$	$(31+5\sqrt{-10})$	σ^3	σ^2
$(7,\ 2+\sqrt{-10})$	$(263,\ 76+\sqrt{-10})$	$(29-10\sqrt{-10})$	σ^3	σ^2
$(13,\ 4+\sqrt{-10})$	$(23,\ 6+\sqrt{-10})$	$(7+5\sqrt{-10})$	σ^4	σ
$(13,\ 4+\sqrt{-10})$	$(47,\ 15+\sqrt{-10})$	$(19-5\sqrt{-10})$	σ^4	σ
$(13,\ 4+\sqrt{-10})$	$(103,\ 14-\sqrt{-10})$	$(33+5\sqrt{-10})$	σ^4	σ
$(23,\ 6+\sqrt{-10})$	$(47,\ 15-\sqrt{-10})$	$(9-10\sqrt{-10})$	σ	σ^4
$(23,\ 6+\sqrt{-10})$	$(103,\ 14+\sqrt{-10})$	$(37+10\sqrt{-10})$	σ	σ^4
$(37,\ 8+\sqrt{-10})$	$(53,\ 19-\sqrt{-10})$	$(31-10\sqrt{-10})$	σ^2	σ^3
$(37,\ 8+\sqrt{-10})$	$(167,\ 18-\sqrt{-10})$	$(77+5\sqrt{-10})$	σ^2	σ^3
$(37,\ 8+\sqrt{-10})$	$(173,\ 63+\sqrt{-10})$	$(49+20\sqrt{-10})$	σ^2	σ^3
$(37,\ 8+\sqrt{-10})$	$(263,\ 76-\sqrt{-10})$	$(59-25\sqrt{-10})$	σ^2	σ^3
$(47,\ 15+\sqrt{-10})$	$(103,\ 14+\sqrt{-10})$	$(29-20\sqrt{-10})$	σ	σ^4
$(53,\ 19+\sqrt{-10})$	$(167,\ 18-\sqrt{-10})$	$(51+25\sqrt{-10})$	σ^2	σ^3
$(53,\ 19+\sqrt{-10})$	$(173,\ 63+\sqrt{-10})$	$(13-30\sqrt{-10})$	σ^2	σ^3
$(53,\ 19+\sqrt{-10})$	$(263,\ 76-\sqrt{-10})$	$(117-5\sqrt{-10})$	σ^2	σ^3
$(167,\ 18+\sqrt{-10})$	$(173,\ 63+\sqrt{-10})$	$(129+35\sqrt{-10})$	σ^2	σ^3
$(167,\ 18+\sqrt{-10})$	$(263,\ 76-\sqrt{-10})$	$(89-60\sqrt{-10})$	σ^2	σ^3
$(173,\ 63+\sqrt{-10})$	$(263,\ 76+\sqrt{-10})$	$(57-65\sqrt{-10})$	σ^3	σ^3

この表の $\mathfrak{pq}$ の欄に書かれた数の作る単項イデアルが，類体 K/F に対応するイデアル群 H に含まれることになる．

これらよりこの拡大の法が $\mathfrak{m} = (10)$ であり，$H = H_{\mathfrak{m}} \supset \{a + 5b\sqrt{-10} \mid a$ は奇数, b は整数 $\}$ が予想される．（本当は $\mathfrak{m} = (5)$ なのだが．後出） ただしこれだけでは同型 $\mathrm{Gal}(K/F) \simeq A_{\mathfrak{m}}/H_{\mathfrak{m}}$ の正体はわからない．

$\left(\dfrac{K/F}{\mathfrak{pq}}\right) \neq e$ となる単項イデアルも調べてみる．

$\mathfrak{p}$	$\mathfrak{q}$	$\mathfrak{pq}$	$\left(\dfrac{K/F}{\mathfrak{p}}\right)$	$\left(\dfrac{K/F}{\mathfrak{q}}\right)$	$\left(\dfrac{K/F}{\mathfrak{pq}}\right)$
$(7,\ 2+\sqrt{-10})$	$(7,\ 2+\sqrt{-10})$	$(3-2\sqrt{-10})$	σ^3	σ^3	σ
$(7,\ 2+\sqrt{-10})$	$(13,\ 4+\sqrt{-10})$	$(1-3\sqrt{-10})$	σ^3	σ^4	σ^2
$(7,\ 2+\sqrt{-10})$	$(13,\ 4-\sqrt{-10})$	$(9+\sqrt{-10})$	σ^3	σ	σ^4
$(7,\ 2+\sqrt{-10})$	$(23,\ 6-\sqrt{-10})$	$(11+2\sqrt{-10})$	σ^3	σ^4	σ^2
$(7,\ 2+\sqrt{-10})$	$(37,\ 8-\sqrt{-10})$	$(13+3\sqrt{-10})$	σ^3	σ^3	σ
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

このあたりでだいたい見当がつく．$n=a+b\sqrt{-10}$ を 10 と素な $\mathcal{O}_F$ の元とする．ここで a は 5 と素な奇数である，（b は有理整数というだけで，制限はない．）このとき $m\equiv a^{-1}b \pmod 5$ であれば，$\left(\dfrac{K/F}{(n)}\right)=\sigma^m$ となっているのである．

$n_1=a+b\sqrt{-10}$, $n_2=c+d\sqrt{-10}$ のとき $n_1n_2=(ac-10bd)+(ad+bc)\sqrt{-10}$ であるが，
$(ac-10bd)^{-1}(ad+bc)\equiv a^{-1}c^{-1}(ad+bc)\equiv c^{-1}d+a^{-1}b \pmod 5$ であるから，確かに準同型になっている．

単項でないイデアル $\mathfrak{n}$ については，単項イデアル $\mathfrak{n}^2$ の像が決まるので，$\left(\dfrac{K/F}{\mathfrak{n}}\right)$ が確定する．

注意　実は (2) の素因子 $(2,\ \sqrt{-10})$ は K/F では分岐しない．従って $\mathfrak{m}=(5)$ であって，$\left(\dfrac{K/F}{(2,\ \sqrt{-10})}\right)=e$ である．

§ 5　F の絶対類体

F の類数は 2 である．$\mathcal{O}_F$ のイデアルは単項とは限らない．$\mathcal{O}_F$ の素イデアル $\mathfrak{p}$ が単項であるかどうかを調べるために，F の絶対類体を求めておきたい．

虚二次体の絶対類体は，考えている虚二次体に各イデアル類の J 不変量を添加して得られる．それらの値は虚二次体上共役である．そこで Maxima で J 不変量を求めようと思ったのだが，組み込み関数や公開されているパッケージがなかったので，近似計算する関数を入力した．それは上半平面 $\mathfrak{H}$ の複素数 τ（modular 変換してなるべく虚部 $\mathrm{Im}(\tau)$ を大きくしておく）に対して $q=\exp(2\pi i\tau)$ とおいて，

$$\begin{aligned}
J(\tau) \;=\; & \frac{1}{q}+744+196884q+21493760q^2+864299970q^3+20245856256q^4+333202640600q^5 \\
&+4252023300096q^6+44656994071935q^7+401490886656000q^8+3176440229784420q^9 \\
&+22567393309593600q^{10}+146211911499519294q^{11}+874313719685775360q^{12} \\
&+4872010111798142520q^{13}+25497827389410525184q^{14}+126142916465781843075q^{15} \\
&+\cdots\cdots
\end{aligned}$$

と q 展開したものである．計算結果は

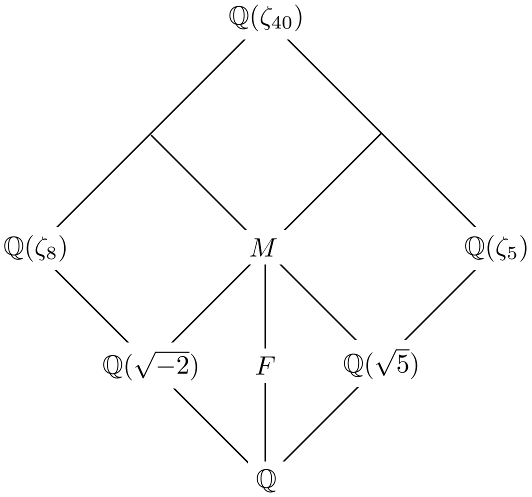
$$\begin{aligned}
J(\mathcal{O}_F) &= J(\sqrt{-10}) &&= 425671414.61878961 \quad (=\mu \text{ とおく}) \\
J((2,\sqrt{-10})) &= J\left(\frac{\sqrt{-10}}{2}\right) &&= 21385.38121041633 \quad (=\nu \text{ とおく})
\end{aligned}$$

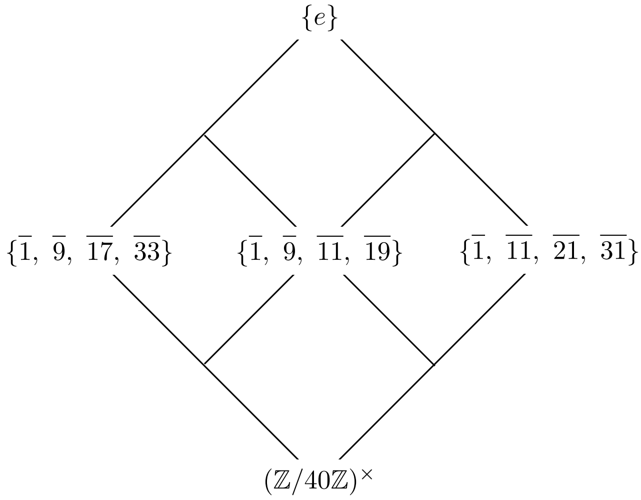
となった．

$\mu+\nu=425692800.00009$, $\mu\nu=9103145472000.002$ より正確な値は $\mu+\nu=425692800=(2^6\cdot3^3\cdot5)\times49270$, $\mu\nu=9103145472000=(2^6\cdot3^3\cdot5)^2\times121945$, であろうと予想すると，$\mu=(2^6\cdot3^3\cdot5)\times(24635+11016\sqrt{5})$,

$\mu=(2^6\cdot 3^3\cdot 5)\times(24635-11016\sqrt{5})$ と計算され，$F=\mathbb{Q}(\sqrt{-10})$ の絶対類体が $M=\mathbb{Q}(\sqrt{-10},\sqrt{5})$ であることがほぼ確実となる．（これは実際に確認できる．）

ところで $M=\mathbb{Q}(\sqrt{-10},\sqrt{5})=\mathbb{Q}(\sqrt{-2},\sqrt{5})$ であり，$\mathbb{Q}(\sqrt{-2})\subset\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\sqrt{5})\subset\mathbb{Q}(\zeta_5)$ であるから M は $\mathbb{Q}(\zeta_8,\zeta_5)=\mathbb{Q}(\zeta_{40})$ の部分体である．つまり，これらの体はすべて $\mathbb{Q}(\zeta_{40})/\mathbb{Q}$ の Galois 群 $(\mathbb{Z}/40\mathbb{Z})^\times$ で統制される．下図は M の位置を表す部分体，部分群の包含関係図である．（必要なところしか書いていない．）





$\sqrt{-2}=\zeta_8+{\zeta_8}^3$ であるから $\mathbb{Q}\left(\sqrt{-2}\right)$ は $\{\overline{1},\ \overline{3}\}\subset\mathrm{Gal}\left(\mathbb{Q}(\zeta_8)/\mathbb{Q}\right)=(\mathbb{Z}/8\mathbb{Z})^\times$ に対応する．
$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{40})/\mathbb{Q}\right)=(\mathbb{Z}/40\mathbb{Z})^\times$ の部分集合としては $\{\overline{1},\ \overline{3},\ \overline{9},\ \overline{11},\ \overline{17},\ \overline{19},\ \overline{27},\ \overline{33}\}$ である．

$\sqrt{5}=2\left(\zeta_5+{\zeta_5}^4\right)+1$ であるから $\mathbb{Q}\left(\sqrt{5}\right)$ は $\{\overline{1},\ \overline{4}\}\subset\mathrm{Gal}\left(\mathbb{Q}(\zeta_5)/\mathbb{Q}\right)=(\mathbb{Z}/5\mathbb{Z})^\times$ に対応する．
$\mathrm{Gal}\left(\mathbb{Q}(\zeta_{40})/\mathbb{Q}\right)=(\mathbb{Z}/40\mathbb{Z})^\times$ の部分集合としては $\{\overline{1},\ \overline{9},\ \overline{11},\ \overline{19},\ \overline{21},\ \overline{29},\ \overline{31},\ \overline{39}\}$ である．

これらより $M=\mathbb{Q}(\sqrt{-2},\ \sqrt{5})$ に対応するガロア群は $\{\overline{1},\ \overline{9},\ \overline{11},\ \overline{19}\}$ であることがわかった．

問題 2–5–1　p を素数とする．次を示せ．

(1)　$p=a^2+10b^2$ となる整数 $a,\ b$ が存在する $\iff p\equiv 1,\ 9,\ 11,\ 19 \pmod{40}$

(2)　$p=a^2+250b^2$ となる整数 $a,\ b$ が存在する
$\iff p\equiv 1,\ 9,\ 11,\ 19 \pmod{40}$ かつ $x^5-5x+12\equiv 0 \pmod{p}$ が解を持つ．

解答

(1)　$F/\mathbb{Q}$ で分岐する素数 2, 5 が a^2+10b^2 と表されないのは明らかである．そこで p は $F/\mathbb{Q}$ で不分岐であるとしてよい．すると

$$
\begin{aligned}
&p=a^2+10b^2 \text{ となる整数 } a,\ b \text{ が存在する}\\
\iff\ & p=(a+b\sqrt{-10})(a-b\sqrt{-10})\\
\iff\ & p \text{ は } F/\mathbb{Q} \text{ で } (p)=\mathfrak{p}\overline{\mathfrak{p}} \text{ と分解し，かつ } \mathfrak{p} \text{ は } F \text{ において単項}\\
\iff\ & p \text{ は } M/\mathbb{Q} \text{ で完全分解}\\
\iff\ & \mathrm{Gal}\left(\mathbb{Q}(\zeta_{40})/\mathbb{Q}\right)=(\mathbb{Z}/40\mathbb{Z})^\times \text{ とした場合}, \overline{p} \text{ が } M \text{ に対応する部分群に含まれる}\\
\iff\ & p\equiv 1,\ 9,\ 11,\ 19 \pmod{40}
\end{aligned}
$$

(2)　$p=(a+5b\sqrt{-10})(a-5b\sqrt{-10})$ と分解される条件である．(1) の条件に加えて，$\mathfrak{p}=(a+5b\sqrt{-10})$ がイデアル群 H に含まれる条件が加わったわけだが，これは先ほど見たように $\mathfrak{p}$ が K/F で完全分解することと同値である．つまり $x^5-5x+12\equiv 0 \pmod{p}$ が何らの拡大も起こさず，一次素因子 5 つの積に因数分解されることを意味する．

§ 6　$|\mathcal{O}_E : \mathbb{Z}[\alpha]|$ と $|\mathcal{O}_K : \mathcal{O}_F[\alpha]|$ の決定

$\mathcal{O}_F[\alpha]$ は $\mathcal{O}_K$ の真部分集合であった．そこで $\mathcal{O}_K$ を決定しておきたい．そのために．これら整環とその整閉包である整数環との，加群としての index $|\mathcal{O}_K : \mathcal{O}_F[\alpha]|$ を調べておこう．

§1 において $f(x) = x^5 - 5x + 12 = 0$ について $D(f) = 2^{12} \cdot 5^6$ であることを見たので，(2), (5) の素因子の挙動を調べ本当の相対判別式 $D(K/F)$ が決定できれば，この問題は解決する．

$E = \mathbb{Q}(\alpha)$ とおく．$E \subset \mathbb{R}$ と思ってもよい．E は $\mathbb{Q}$ 上 5 次拡大であるが，Galois 拡大ではない．$\mathcal{O}_K$ を決定する際には，先に $\mathcal{O}_E$ を決定しておくことになる．従って $|\mathcal{O}_E : \mathbb{Z}[\alpha]|$ も同時に調べることにする．

K/F は 5 次巡回拡大だから，F の素イデアル $\mathfrak{p}$ は K/F では

(i)　完全分解する．$\big(\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5,\ N_{K/F}\mathfrak{P}_i = \mathfrak{p}\big)$,

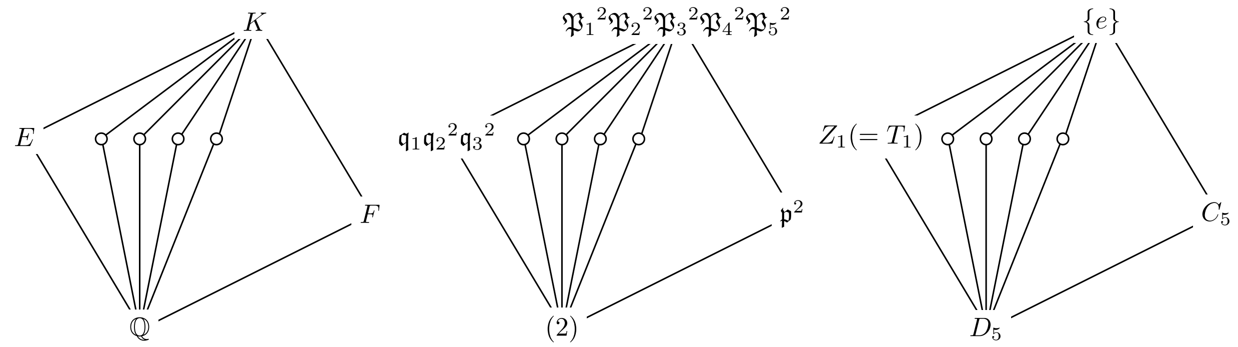
(ii)　完全分岐する，$\big(\mathfrak{p} = \mathfrak{P}^5,\ N_{K/F}\mathfrak{P} = \mathfrak{p}\big)$,

(ii)　素イデアルである，$\big(\mathfrak{p} = \mathfrak{P},\ N_{K/F}\mathfrak{P} = \mathfrak{p}^5\big)$

の 3 通りしかない．$F/\mathbb{Q}$ で分岐しない素数 ($p \neq 2,\ 5$) の素因子に関しては前節で類体論的に (i), (iii) を決定した．そこで $p = 2,\ 5$ について考えよう．

(2)–成分について

$F/\mathbb{Q}$ においては $(2) = \mathfrak{p}^2$ $\big(\mathfrak{p} = (2,\ \sqrt{-10})\big)$ と分岐する．一方 $f(x) \equiv x(x+1)^4 \pmod 2$ だから，$E/\mathbb{Q}$ においては (2) は少なくとも 2 つ以上の素イデアルに分解する．この場合 K/F では (ii), (iii) ではあり得ず (i) の完全分解ということになる．従って相対判別式 $D(K/F)$ は (2) の素因子を持たず，射線 $\mathfrak{m}$ は (2) と素である．§4 で $\mathfrak{m} = (10)$ と述べたのは最善ではなかった．正しくは $\mathfrak{m} = (5)$ であり，$\left(\dfrac{K/F}{\mathfrak{p}}\right) = e$ である．（実際に完全分解している．）



$\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5$ において $\mathfrak{P}_1$ の分解体を E と思ってよい．この場合 $E/\mathbb{Q}$ における分解の様子は
$(2) = \mathfrak{q}_1{\mathfrak{q}_2}^2{\mathfrak{q}_3}^2$, $\mathfrak{q}_1 = {\mathfrak{P}_1}^2$, $\mathfrak{q}_2 = \mathfrak{P}_2\mathfrak{P}_3$, $\mathfrak{q}_3 = \mathfrak{P}_4\mathfrak{P}_5$ のように表されることが容易にわかる．

一般に，代数体の拡大 L/M における共役差積の p 成分を $\mathfrak{d}(L/M,\ p)$ と書くことにしよう．
K/F で $\mathfrak{p}$ は不分岐だから $\mathfrak{d}(K/F,\ 2) = (1)$ である．また $\mathfrak{d}(F/\mathbb{Q},\ 2) = \mathfrak{p}^3$ であることは周知である．
共役差積の連鎖律より $\mathfrak{d}(K/\mathbb{Q},\ 2) = \mathfrak{d}(K/F,\ 2)\mathfrak{d}(F/\mathbb{Q},\ 2) = \mathfrak{p}^3 = {\mathfrak{P}_1}^3{\mathfrak{P}_2}^3{\mathfrak{P}_3}^3{\mathfrak{P}_4}^3{\mathfrak{P}_5}^3$ であることが従う．

これを E 経由の連鎖律 $\mathfrak{d}(K/\mathbb{Q},\ 2) = \mathfrak{d}(K/E,\ 2)\mathfrak{d}(E/\mathbb{Q},\ 2)$ で考える．K/E では $\mathfrak{P}_1$ のみが分岐するので，$\mathfrak{d}(K/E,\ 2) = {\mathfrak{P}_1}^{n_1}$ となるはずである．$E/\mathbb{Q}$ では $\mathfrak{q}_2$, $\mathfrak{q}_3$ が分岐するので，$\mathfrak{d}(E/\mathbb{Q},\ 2) = {\mathfrak{q}_2}^{n_2}{\mathfrak{q}_3}^{n_3} = {\mathfrak{P}_2}^{n_2}{\mathfrak{P}_3}^{n_2}{\mathfrak{P}_4}^{n_3}{\mathfrak{P}_4}^{n_3}$ のように表されるはずである．これより $n_1 = n_2 = n_3 = 3$ が得られる．

すると $\mathfrak{d}(E/\mathbb{Q},\ 2) = {\mathfrak{q}_2}^3{\mathfrak{q}_3}^3$ のノルムをとって $E/\mathbb{Q}$ の相対判別式 (の 2 巾成分) は $D(E/\mathbb{Q},\ 2) = N_{E/\mathbb{Q}}({\mathfrak{q}_2}^3{\mathfrak{q}_3}^3) = 2^6$ となる．$D(f) = 2^{12} \cdot 5^6$ と比較して $|\mathcal{O}_E : \mathbb{Z}[\alpha]| = 2^3 \times 5^m$ であることがわかった．つまり整数環 $\mathcal{O}_E$ を得るためには（2 巾に関しては）$\mathbb{Z}[\alpha]$ の基底を絞って 8 倍に広げないといけない．

次に $|\mathcal{O}_K:\mathcal{O}_F[\alpha]|$ の (2) 成分を考える．$D(f)=2^{12}\cdot 5^2$ なので，行列式で考えると

$$\begin{aligned}
&\Delta(\mathcal{O}_F[\alpha])\\
=\ &\Delta(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\sqrt{-10},\alpha\sqrt{-10},\alpha^2\sqrt{-10},\alpha^3\sqrt{-10},\alpha^4\sqrt{-10})\\
=\ &\Delta(1,\alpha,\alpha^2,\alpha^3,\alpha^4)^2(-2\sqrt{-10})^5\\
=\ &D(f)(-2\sqrt{-10})^5
\end{aligned}$$

これより $D(\mathcal{O}_F[\alpha])=\Delta(\mathcal{O}_F[\alpha])^2=(2^{39}\cdot 5^9)$ が得られる．

それに対し $\mathfrak{d}(K/\mathbb{Q},2)=\mathfrak{d}(K/F,2)\cdot\mathfrak{d}(F/\mathbb{Q},2)=\mathcal{O}_K\cdot\mathfrak{p}^3=\mathfrak{p}^3$ であり，

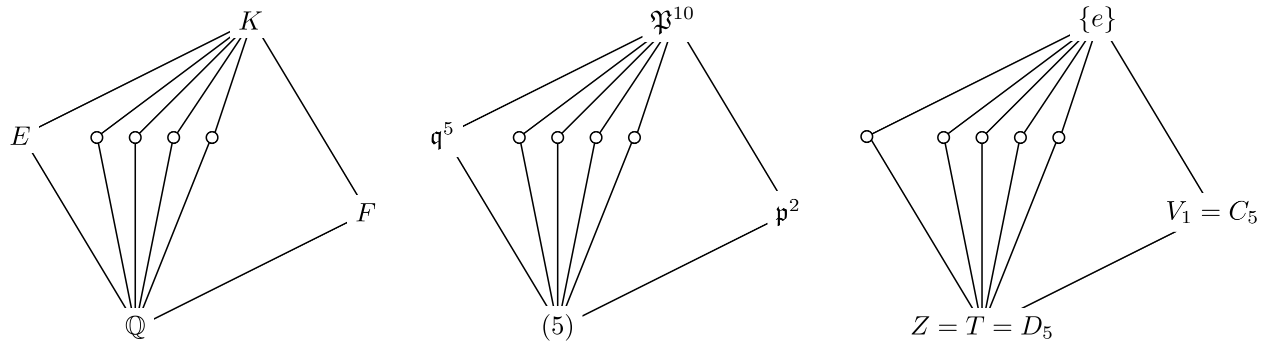
$$D(K/\mathbb{Q},2)=N_{K/\mathbb{Q}}\mathfrak{d}(K/\mathbb{Q},2)=N_{K/\mathbb{Q}}\mathfrak{p}^3=\mathfrak{p}^{30}=(2^{15})$$

であるから $|\mathcal{O}_K:\mathcal{O}_F[\alpha]|=2^{12}\times 5^{m'}$ がわかる．つまりこちらは（2 巾に関しては）$2^{12}=4096$ 倍に広げる必要がある．

(5)–成分について

次に (5) の分岐を考える．上の $\mathfrak{p},\mathfrak{P},\mathfrak{q}$ などの定義はリセットして，(5) の素因子のために使うことにする．$f(x)=x^5-5x+12$ に $x=y+3$ を代入すると，$f(y+3)=y^5+15\,y^4+90\,y^3+270\,y^2+400\,y+240$ となり，これは素数 5 に関する Eisenstein 方程式となっている．従って $|\mathcal{O}_E:\mathbb{Z}[\alpha]|$ は 5 の因子を持たない．さらに $\pi=\alpha+3$ とおくと π は $\mathcal{O}_{E,\mathfrak{q}}\subset E_{\mathfrak{q}}$ の素元であり，$\mathcal{O}_{E,\mathfrak{q}}=\mathbb{Z}_5[\pi]$ であって，$\mathrm{ord}_5\pi=\dfrac{1}{5}$ ということになる．（ただし $\mathfrak{q}=(5,\ \pi)$ とおいた．）結論として $|\mathcal{O}_E:\mathbb{Z}[\alpha]|=2^3$ ということになる．

このように $f(x)=x^5-5x+12\equiv(x+3)^5\equiv\pi^5 \pmod 5$ により (5) は $E/\mathbb{Q}$ で完全分岐する．つまり $(5)=\mathfrak{q}^5$ である．(5) は $F/\mathbb{Q}$ でも完全分岐するので，それを $(5)=\mathfrak{p}^2$ と書くと，$K/\mathbb{Q}$ では $(5)=\mathfrak{P}^{10}$ と完全分岐することがわかる．



局所体上では $\mathcal{O}_{E,\mathfrak{q}}=\mathbb{Z}_5[\pi]$ だから $D(E/\mathbb{Q},5)=D(f,5)=(5^6)$ である．実際これは $\mathfrak{d}(E/\mathbb{Q},5)=(f'(\alpha),5)$ $=(5\pi^4+60\pi^3+270\pi^2+540\pi+400,5)=(\pi)^6$ であることからも導かれる．

$\left(\mathrm{ord}_5 5\pi^4=\dfrac{9}{5},\ \mathrm{ord}_5 60\pi^3=\dfrac{8}{5},\ \mathrm{ord}_5 270\pi^2=\dfrac{7}{5},\ \mathrm{ord}_5 540\pi=\dfrac{6}{5},\ \mathrm{ord}_5 400=2\ \text{である！}\right)$

共役差積の連鎖律より $\mathfrak{d}(K/\mathbb{Q},5)=\mathfrak{d}(K/E,5)\cdot\mathfrak{d}(E/\mathbb{Q},\ 5)=\mathfrak{P}\cdot\mathfrak{q}^6=\mathfrak{P}^{13}$ が導かれる．$\mathfrak{d}(K/\mathbb{Q},\ 5)=\mathfrak{d}(K/F,\ 5)\mathfrak{d}(F/\mathbb{Q},\ 5)$ において $\mathfrak{d}(F/\mathbb{Q},\ 5)=\mathfrak{p}=\mathfrak{P}^5$ だから $\mathfrak{d}(K/F,\ 5)=\mathfrak{P}^8$ であることがわかった．これは共役差積の指数に関する Dedekind の定理

$$\mathfrak{d}(K/F,\ 5)=\mathfrak{P}^{(e-1)+(v_1-1)+(v_2-1)+\cdots}\quad(e:\text{分岐指数},\ v_i:\text{第}\ i\ \text{分岐群}\ V_i\ \text{の位数})$$

において $e=5,\ v_1=5,\ v_2=v_3=\cdots=1$ を意味する．つまり $T=D_5,\ V_1=C_5,\ V_2=\{e\}$ である．

もしも $\mathcal{O}_{K,\mathfrak{P}}=\mathcal{O}_{F,\mathfrak{p}}[\pi]$ なのであれば $\mathfrak{d}(K/F,\ 5)=\mathfrak{P}^{12}$ のはずであるから，(5) 成分に関しても整数環はもう少し大きい．相対判別式でいうと $D(K/F,\ 5)=N_{K/F}\mathfrak{P}^8=\mathfrak{p}^8=5^4$ で，$D(f,\ 5)$ と 5^2 の開きがあるから，$|\mathcal{O}_K:\mathcal{O}_F[\alpha]|=(2^6\times 5)^2=2^{12}\times 5^2$ とわかる．

補足　$\mathfrak{d}(E/\mathbb{Q},5)=\mathfrak{q}^6$ であること，および第 2 分岐群 $V_2=\{e\}$ であることは，直接調べることもできる．それについて述べておく．(5) の分岐を調べたいのだから，$f(x)=x^5-5x+12=0$ の解 α よりも $\mathcal{O}_{E,\mathfrak{q}}$ の素元 $\pi=\alpha-3$ を使った方がよい．π の共役元は

$$\begin{aligned}
\pi_1=\sigma\pi &\quad =\beta-3 &&= \frac{-\pi^4-13\pi^3-64\pi^2-142\pi-140}{8}+\frac{\pi^4+15\pi^3+90\pi^2+230\pi+200}{80}\sqrt{-10}\\
\pi_2=\sigma^2\pi &\quad =\gamma-3 &&= \frac{\pi^4+13\pi^3+64\pi^2+138\pi+100}{8}+\frac{\pi^4+15\pi^3+80\pi^2+180\pi+140}{40}\sqrt{-10}\\
\pi_3=\sigma^3\pi &\quad =\delta-3 &&= \frac{\pi^4+13\pi^3+64\pi^2+138\pi+100}{8}-\frac{\pi^4+15\pi^3+80\pi^2+180\pi+140}{40}\sqrt{-10}\\
\pi_4=\sigma^4\pi &\quad =\epsilon-3 &&= \frac{-\pi^4-13\pi^3-64\pi^2-142\pi-140}{8}-\frac{\pi^4+15\pi^3+90\pi^2+230\pi+200}{80}\sqrt{-10}
\end{aligned}$$

$\mathrm{ord}_5\pi=\dfrac{1}{5}$, $\mathrm{ord}_5\sqrt{-10}=\dfrac{1}{2}$ より計算すると，すべて $\pi=\pi^1$ の有理数倍の項の order が $\dfrac{1}{5}$ で一番小さいことが確認できる．しかるに

$$\pi_1-\pi=\frac{-\pi^4-13\pi^3-64\pi^2-150\pi-140}{8}+\frac{\pi^4+15\pi^3+90\pi^2+230\pi+200}{80}\sqrt{-10}$$

では $\dfrac{\pi^4}{80}\sqrt{-10}$ の項の order が $\dfrac{4}{5}-1+\dfrac{1}{2}=\dfrac{3}{10}$ で最小であることが確認できる．$\mathrm{ord}_5(\pi_4-\pi)=\dfrac{3}{10}$ も同様である．また

$$\pi_2-\pi=\frac{\pi^4+13\pi^3+64\pi^2+130\pi+100}{8}-\frac{\pi^4+15\pi^3+80\pi^2+180\pi+140}{40}\sqrt{-10}$$

では $\dfrac{\pi^4}{80}\sqrt{-10}$ の項の order が $\dfrac{4}{5}-1+\dfrac{1}{2}=\dfrac{3}{10}$ で最小であることが確認できる．$\mathrm{ord}_5(\pi_3-\pi)=\dfrac{3}{10}$ も同様である．

従って $\mathrm{ord}_5(\pi_1-\pi)(\pi_2-\pi)(\pi_3-\pi)(\pi_4-\pi)=\dfrac{6}{5}$ となる．

§ 7　$\mathcal{O}_E$ の決定

§6 で $|\mathcal{O}_E:\mathbb{Z}[\alpha]|=2^3$ であることを見た．$\mathcal{O}_E$ を実際に決定しよう．$E/\mathbb{Q}$ の基底として

$$\alpha^4,\ \alpha^3,\ \alpha^2,\ \alpha,\ 1$$

をとる．$R_0=\mathbb{Z}[\alpha]=\mathbb{Z}\alpha^4+\mathbb{Z}\alpha^3+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1$ とおく．見当をつけて当たってみると，$\phi=\dfrac{\alpha^4+\alpha^3+\alpha^2+\alpha}{4}$, $\psi=\dfrac{\alpha^3+\alpha}{2}$ が整数であることがすぐにわかる．（実際 $\phi^5-5\phi^4+15\phi-35\phi^2+50\phi-30=0$, $\psi^5-5\psi^3+30\psi^2-50\psi+60=0$）従って $\mathcal{O}_E=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1$ であることがわかる．

しかしこれでは整数環をたまたま見つけただけのことであって，確実に構成する手順とはならない．そこを考えてみた．

まず十分大きい 2 巾を法として $x^5-5x+12$ を因数分解する．例えば次のような結果が得られる．

$$x^5-5x+12\equiv(x-28)(x^2-38x+81)(x^2+66x+11)\pmod{128}$$

第 2 因子，第 3 因子は $\pmod{128}$ で解を持たないので $\mathbb{Q}_2$ 上既約である．この因数分解は Hensel の補題より $x^5 - 5x + 12$ の $\mathbb{Q}_2$ における因数分解に延長される．$E/\mathbb{Q}$ において $(2) = \mathfrak{q}_1\mathfrak{q}_2{}^2\mathfrak{q}_3{}^2$ であること，もしくは $\mathcal{O}_{E,2} = \mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_2 \simeq \mathcal{O}_{E,\mathfrak{q}_1} \oplus \mathcal{O}_{E,\mathfrak{q}_2} \oplus \mathcal{O}_{E,\mathfrak{q}_3} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}]$ であることに対応している．この同型写像を h とおく．$h : \mathcal{O}_{E,2} \to \mathbb{Z}_2 \oplus \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}]$.

$$x^2 - 38x + 81 \equiv (x-19)^2 - 280 \equiv (x-19)^2 + 1000 \equiv (x - 19 - 10\sqrt{-10})(x - 19 + 10\sqrt{-10}) \pmod{128},$$
$$x^2 + 66x + 11 \equiv (x+33)^2 - 1078 \equiv (x+33)^2 + 2250 \equiv (x + 33 - 15\sqrt{-10})(x + 33 + 15\sqrt{-10}) \pmod{128},$$

$\mathcal{O}_{E,2} \supset \mathbb{Z}_2[\alpha] \supset 8\mathcal{O}_{E,2}$ は分かっているので，α の $\mathcal{O}_{E,2}/8\mathcal{O}_{E,2}$ における像を決定すればよい．

$$\mathcal{O}_{E,2}/8\mathcal{O}_{E,2} \simeq \mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/8\mathbb{Z})\,[\sqrt{-10}] \oplus (\mathbb{Z}/8\mathbb{Z})\,[\sqrt{-10}] \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$$

ただし 2 つめの同型 j は $j\left(a,\ b + c\sqrt{-10},\ d + e\sqrt{-10}\right) = (a,\ b,\ c,\ d,\ e)$ で与えられるものとする．1 つめの同型は $h \pmod 8$ であるが，h で表すことにする．これにより

$$\begin{aligned}
&j(h(1)) &&= j(1,\ 1,\ 1) &&= j(1,\ 1,\ 1) &&= (1,\ 1,\ 0,\ 1,\ 0)\\
&j(h(\alpha)) &&= j(28,\ 19 + 10\sqrt{-10},\ -33 + 15\sqrt{-10}) &&= j(4,\ 3 + 2\sqrt{-10},\ -1 - \sqrt{-10}) &&= (4,\ 3,\ 2,\ -1,\ -1)\\
&j(h(\alpha^2)) &&= j(16,\ -31 + 12\sqrt{-10},\ -9 + 2\sqrt{-10}) &&= j(0,\ 1 + 4\sqrt{-10},\ -1 + 2\sqrt{-10}) &&= (0,\ 1,\ 4,\ -1,\ 2)\\
&j(h(\alpha^3)) &&= j(0,\ -77 + 14\sqrt{-10},\ 21 - \sqrt{-10}) &&= j(0,\ 3 + 6\sqrt{-10},\ 5 - \sqrt{-10}) &&= (0,\ 3,\ 6,\ 5,\ -1)\\
&j(h(\alpha^4)) &&= j(0,\ -111 + 24\sqrt{-10},\ -15 - 4\sqrt{-10}) &&= j(0,\ 1,\ 1 + 4\sqrt{-10}) &&= (0,\ 1,\ 0,\ 1,\ 4)
\end{aligned}$$

この 5 つのベクトルでは $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ は生成されない．実際

$$\det \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 4 & 3 & 2 & -1 & -1 \\ 0 & 1 & 4 & -1 & 2 \\ 0 & 3 & 6 & 5 & -1 \\ 0 & 1 & 0 & 1 & 4 \end{pmatrix} = 40$$

であるから，2 巾因子を見て index 8 になっていることが確認される．$(\mathbb{Z}/8\mathbb{Z})^5$ 全体を生成するには $j(h(\alpha + \alpha^2 + \alpha^3 + \alpha^4)) = (4,\ 8,\ 12,\ 4,\ 4) \in 4(\mathbb{Z}/8\mathbb{Z})^5$, $j(h(\alpha + \alpha^3)) = (4,\ 6,\ 8,\ 4,\ -2) \in 2(\mathbb{Z}/8\mathbb{Z})^5$ より $\phi = \dfrac{\alpha^4 + \alpha^3 + \alpha^2 + \alpha}{4}$, $\psi = \dfrac{\alpha^3 + \alpha}{2}$ を追加すればよいことがわかる．一般的にこのように作った数は (2) 以外の素因子に関しては整数でないかもしれないが，その場合は適当に奇数倍してやって整数にすればよい．今の場合は作り方から（整数を 4, 2 で割っているだけなので）そのようなことは起こらない．

注意　$j(h(\alpha + \alpha^2 + \alpha^3 + \alpha^4)) = (4,\ 8,\ 12,\ 4,\ 4)$ だからといって $j\left(h\left(\dfrac{\alpha + \alpha^2 + \alpha^3 + \alpha^4}{4}\right)\right) = (1,\ 2,\ 3,\ 1,\ 1)$ な訳ではもちろんない．実際に計算すると $j\left(h\left(\dfrac{\alpha + \alpha^2 + \alpha^3 + \alpha^4}{4}\right)\right) = (3,\ 6,\ -1,\ -1,\ 1)$ になっている．

§ 8　$\mathcal{O}_K$ の決定 1；2 巾の除去

§6 で $|\mathcal{O}_K : \mathcal{O}_F[\alpha]| = 2^{12} \times 5^2$ であることを見た．$\mathcal{O}_K$ を実際に決定しよう．

やはりこの場合も 2 成分を見るためには最終的には局所化して考えるのがよいのだが，まずは大きく絞り込んでいこう．

$K/\mathbb{Q}$ の基底として $\alpha^4,\ \alpha^3,\ \alpha^2,\ \alpha,\ 1,\ \alpha^4\sqrt{-10},\ \alpha^3\sqrt{-10},\ \alpha^2\sqrt{-10},\ \alpha\sqrt{-10},\ \sqrt{-10}$ をとる．

$$\mathcal{O}_F[\alpha] = \mathbb{Z}\alpha^4 + \mathbb{Z}\alpha^3 + \mathbb{Z}\alpha^2 + \mathbb{Z}\alpha + \mathbb{Z}1 + \mathbb{Z}\alpha^4\sqrt{-10} + \mathbb{Z}\alpha^3\sqrt{-10} + \mathbb{Z}\alpha^2\sqrt{-10} + \mathbb{Z}\alpha\sqrt{-10} + \mathbb{Z}\sqrt{-10}$$

となっている．$\mathcal{O}_F[\alpha]=R_0$ とおく．$|\mathcal{O}_K:R_0|=2^{12}\times 5^2$ である．

§7 で見たように，$\phi=\dfrac{\alpha^4+\alpha^3+\alpha^2+\alpha}{4}$, $\psi=\dfrac{\alpha^3+\alpha}{2}$ とすると $\mathcal{O}_E=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1$ なので，

$$R_1=R_0[\phi,\ \psi]=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1+\mathbb{Z}\phi\sqrt{-10}+\mathbb{Z}\psi\sqrt{-10}+\mathbb{Z}\alpha^2\sqrt{-10}+\mathbb{Z}\alpha\sqrt{-10}+\mathbb{Z}\sqrt{-10}$$

とすれば，$\mathcal{O}_K\supset R_1\supset R_0$ であって，$|R_1:R_0|=2^6$ より $|\mathcal{O}_K:R_1|=2^6\times 5^2$ まで絞り込める．

次に $\beta=\sigma(\alpha)$ も整数であることに注意する．

$$\begin{aligned}
\beta &= \frac{-\alpha^4-\alpha^3-\alpha^2-\alpha+4}{8}+\frac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{80}\sqrt{-10}\\
&= \frac{-4\phi+4}{8}+\frac{4\phi+2\alpha^3+8\alpha^2-14\alpha-4}{80}\sqrt{-10}\\
&= \frac{-\phi+1}{2}+\frac{4\phi+4\psi+8\alpha^2-16\alpha-4}{80}\sqrt{-10}\\
&= \frac{-\phi+1}{2}+\frac{\phi+\psi+2\alpha^2-4\alpha-1}{20}\sqrt{-10}
\end{aligned}$$

$20\beta=10(-\phi+1)+(\phi+\psi+2\alpha^2-4\alpha-1)\sqrt{-10}$ であるから，β を付け加え，$\sqrt{-10}$ の代わりに β を基底に採用する．

$$R_2=R_1[\beta]=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1+\mathbb{Z}\phi\sqrt{-10}+\mathbb{Z}\psi\sqrt{-10}+\mathbb{Z}\alpha^2\sqrt{-10}+\mathbb{Z}\alpha\sqrt{-10}+\mathbb{Z}\beta$$

$\mathcal{O}_K\supset R_2\supset R_1$ であって，$|R_2:R_1|=20$ より $|\mathcal{O}_K:R_2|=2^4\times 5$ がわかる．

今度は $\gamma=\sigma^2(\alpha)$ が整数であることに注意する．

$$\begin{aligned}
\gamma &= \frac{\alpha^4+\alpha^3+\alpha^2-3\alpha-4}{8}+\frac{\alpha^4+3\alpha^3-\alpha^2-3\alpha-4}{40}\sqrt{-10}\\
&= \frac{4\phi-4\alpha-4}{8}+\frac{4\phi+2\alpha^3-2\alpha^2-4\alpha-4}{40}\sqrt{-10}\\
&= \frac{\phi-\alpha-1}{2}+\frac{4\phi+4\psi-2\alpha^2-6\alpha-4}{40}\sqrt{-10}\\
&= \frac{\phi-\alpha-1}{2}+\frac{2\phi+2\psi-\alpha^2-3\alpha}{20}\sqrt{-10}-\frac{1}{10}\{-20\beta-10\phi+10+(\phi+\psi+2\alpha^2-4\alpha)\sqrt{-10}\}\\
&= \frac{\phi-\alpha-1}{2}+\frac{2\phi+2\psi-\alpha^2-3\alpha-2\phi-2\psi-4\alpha^2+8\alpha}{20}\sqrt{-10}+2\beta+\phi-1\\
&= \frac{3\phi-\alpha-3}{2}+2\beta+\frac{-5\alpha^2+5\alpha}{20}\sqrt{-10}\\
&= \frac{3\phi-\alpha-3}{2}+2\beta+\frac{-\alpha^2+\alpha}{4}\sqrt{-10}
\end{aligned}$$

$4\gamma=6\phi-2\alpha-6+8\beta+(-\alpha^2+\alpha)\sqrt{-10}$ であるから，γ を付け加え，$\alpha^2\sqrt{-10}$ の代わりに γ を基底に採用する．

$$R_3=R_2[\gamma]=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1+\mathbb{Z}\phi\sqrt{-10}+\mathbb{Z}\psi\sqrt{-10}+\mathbb{Z}\gamma+\mathbb{Z}\alpha\sqrt{-10}+\mathbb{Z}\beta$$

$\mathcal{O}_K\supset R_3\supset R_2$ であって，$|R_3:R_2|=4$ より $|\mathcal{O}_K:R_3|=2^2\times 5$ まで絞り込める．

$\delta\in R_3, \epsilon\in R_3$ であるから，この方法ではこれ以上環を広げられない．そこでこれらを局所化して考える．

$$
\begin{aligned}
\mathcal{O}_{K,2} &\simeq \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_2 \\
&\simeq O_{K,\ \mathfrak{P}_1} \oplus O_{K,\ \mathfrak{P}_1} \oplus O_{K,\ \mathfrak{P}_1} \oplus O_{K,\ \mathfrak{P}_1} \oplus O_{K,\ \mathfrak{P}_1} \\
&\simeq \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}] \oplus \mathbb{Z}_2[\sqrt{-10}]
\end{aligned}
$$

先に述べたように

$$
\begin{aligned}
& x^5-5x+12 \\
\equiv\ & (x-28)\left(x-19-10\sqrt{-10}\right)\left(x-19+10\sqrt{-10}\right)\left(x+33-15\sqrt{-10}\right)\left(x+33+15\sqrt{-10}\right) \pmod{128}
\end{aligned}
$$

であるから，$\alpha \equiv 28 \pmod{{\mathfrak{P}_1}^{14}}$ とすると（ $(128) = (\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5)^{14}$ である）

$$
\begin{aligned}
\beta &= \frac{-\alpha^4-\alpha^3-\alpha^2-\alpha+4}{8} + \frac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{80}\sqrt{-10} \\
&\equiv -79677+8590\sqrt{-10} \pmod{{\mathfrak{P}_1}^6} \\
&\equiv 3-2\sqrt{-10} \pmod{{\mathfrak{P}_1}^6}
\end{aligned}
$$

β 自体も $x^5-5x+12=0$ の解だから，因数分解の結果と見比べて $\beta \equiv 19-10\sqrt{-10} \pmod{{\mathfrak{P}_1}^{14}}$ でなければならない．同様にして $\gamma \equiv -33+15\sqrt{-10} \pmod{{\mathfrak{P}_1}^{14}}$, $\delta \equiv -33-15\sqrt{-10} \pmod{{\mathfrak{P}_1}^{14}}$, $\epsilon \equiv 19+10\sqrt{-10} \pmod{{\mathfrak{P}_1}^{14}}$ であることがわかる．

$4\mathcal{O}_{K,2} \subset R_3 \otimes_{\mathbb{Z}} \mathbb{Z}_2$ は分かっているので，次の同型で各基底の像を調べよう．$(\mathbb{Z}/4\mathbb{Z})[\sqrt{-10}]$ を $\overline{R}$ と書くことにする．

$$
\begin{array}{ccccccccccccc}
\mathcal{O}_{K,2}/4\mathcal{O}_{K,2} & \simeq & & \overline{R} & \oplus & \overline{R} & \oplus & \overline{R} & \oplus & \overline{R} & \oplus & \overline{R} & \\
1 & \mapsto & (& 1+0\sqrt{-10} & , & 1+0\sqrt{-10} & , & 1+0\sqrt{-10} & , & 1+0\sqrt{-10} & , & 1+0\sqrt{-10} &) \\
\alpha & \mapsto & (& 0+0\sqrt{-10} & , & 3+2\sqrt{-10} & , & 3+3\sqrt{-10} & , & 3+1\sqrt{-10} & , & 3+2\sqrt{-10} &) \\
\alpha^2 & \mapsto & (& 0+0\sqrt{-10} & , & 1+0\sqrt{-10} & , & 3+2\sqrt{-10} & , & 3+2\sqrt{-10} & , & 1+0\sqrt{-10} &) \\
\alpha\sqrt{-10} & \mapsto & (& 0+0\sqrt{-10} & , & 0+3\sqrt{-10} & , & 2+3\sqrt{-10} & , & 2+3\sqrt{-10} & , & 0+3\sqrt{-10} &) \\
\beta & \mapsto & (& 3+2\sqrt{-10} & , & 3+3\sqrt{-10} & , & 3+1\sqrt{-10} & , & 3+2\sqrt{-10} & , & 0+0\sqrt{-10} &) \\
\gamma & \mapsto & (& 3+3\sqrt{-10} & , & 3+1\sqrt{-10} & , & 3+2\sqrt{-10} & , & 0+0\sqrt{-10} & , & 3+2\sqrt{-10} &) \\
\phi & \mapsto & (& 3+0\sqrt{-10} & , & 2+1\sqrt{-10} & , & 3+1\sqrt{-10} & , & 3+3\sqrt{-10} & , & 2+3\sqrt{-10} &) \\
\psi & \mapsto & (& 2+0\sqrt{-10} & , & 3+0\sqrt{-10} & , & 2+3\sqrt{-10} & , & 2+1\sqrt{-10} & , & 3+0\sqrt{-10} &) \\
\phi\sqrt{-10} & \mapsto & (& 0+3\sqrt{-10} & , & 2+2\sqrt{-10} & , & 2+3\sqrt{-10} & , & 2+3\sqrt{-10} & , & 2+2\sqrt{-10} &) \\
\psi\sqrt{-10} & \mapsto & (& 0+2\sqrt{-10} & , & 0+3\sqrt{-10} & , & 2+2\sqrt{-10} & , & 2+2\sqrt{-10} & , & 0+3\sqrt{-10} &)
\end{array}
$$

これを行列化する．

$$
M = \begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 3 & 2 & 3 & 3 & 3 & 1 & 3 & 2 \\
0 & 0 & 1 & 0 & 3 & 2 & 3 & 2 & 1 & 0 \\
0 & 0 & 0 & 3 & 2 & 3 & 2 & 3 & 0 & 3 \\
3 & 2 & 3 & 3 & 3 & 1 & 3 & 2 & 0 & 0 \\
3 & 3 & 3 & 1 & 3 & 2 & 0 & 0 & 3 & 2 \\
3 & 0 & 2 & 1 & 3 & 1 & 3 & 3 & 2 & 3 \\
2 & 0 & 3 & 0 & 2 & 3 & 2 & 1 & 3 & 0 \\
0 & 3 & 2 & 2 & 2 & 3 & 2 & 3 & 2 & 2 \\
0 & 2 & 0 & 3 & 2 & 2 & 2 & 2 & 0 & 3
\end{pmatrix}
$$

$\det M=-5508\equiv 0 \pmod 4$ だからこれらの基底は $\mathcal{O}_{K,2}/4\mathcal{O}_{K,2}$ を生成していない．掃き出し法でこの行列を上三角行列に整形していこう．例えば

$$N_1=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0\\-3&0&0&0&1&0&0&0&0&0\\-3&0&0&0&0&1&0&0&0&0\\-3&0&0&0&0&0&1&0&0&0\\-2&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&0&1\end{pmatrix}$$

を左からかけると

$$N_1M=\begin{pmatrix}1&0&1&0&1&0&1&0&1&0\\0&0&3&2&3&3&3&1&3&2\\0&0&1&0&3&2&3&2&1&0\\0&0&0&3&2&3&2&3&0&3\\0&2&0&3&0&1&0&2&-3&0\\0&3&0&1&0&2&-3&0&0&2\\0&0&-1&1&0&1&0&3&-1&3\\0&0&1&0&0&3&0&1&1&0\\0&3&2&2&2&3&2&3&2&2\\0&2&0&3&2&2&2&2&0&3\end{pmatrix}$$

となるが，これは ${}^t\left(1,\ \alpha,\ \alpha^2,\ \alpha\sqrt{-10},\ \beta-3,\ \gamma-3,\ \phi-3,\ \psi-2,\ \phi\sqrt{-10},\ \psi\sqrt{-10}\right)$ の行列表示を表している．この操作を繰り返すと，

$$N=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0\\0&0&0&0&-1&1&0&0&0&0\\0&0&1&0&0&0&0&0&0&0\\-3&0&1&0&0&0&1&0&0&0\\-13&0&1&-1&0&0&3&2&0&0\\-41&0&2&-3&0&0&9&7&0&0\\-340&0&18&-28&3&-3&76&56&1&0\\561&-2&-28&47&-3&4&-128&-90&-2&0\\1095&-3&-55&91&-6&8&-249&-177&-4&0\\2821&-8&-142&234&-16&20&-641&-455&-10&1\end{pmatrix}$$

に対して

$$NM = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -2 & 0 & 1 & -3 & -2 & 3 & 2 \\ 0 & 0 & 1 & 0 & 3 & 2 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 & 3 & 5 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 8 & 1 & 10 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 25 & 0 & 29 & 0 & 18 \\ 0 & 0 & 0 & 0 & 0 & 196 & 9 & 245 & -9 & 140 \\ 0 & 0 & 0 & 0 & 0 & -320 & -12 & -403 & 9 & -243 \\ 0 & 0 & 0 & 0 & 0 & -628 & -24 & -788 & 18 & -472 \\ 0 & 0 & 0 & 0 & 0 & -1616 & -60 & -2028 & 48 & -1214 \end{pmatrix}$$

これを mod 4 で考えると

$$NM \equiv \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 & 1 & 1 & 2 & 3 & 2 \\ 0 & 0 & 1 & 0 & 3 & 2 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 3 & 3 & 3 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

この行列の 9 行目は

$$1095 - 3\alpha - 55\alpha^2 + 91\alpha\sqrt{-10} - 6\beta + 8\gamma - 249\phi - 177\psi - 4\phi\sqrt{-10} \in 2\mathcal{O}_K$$

を意味する．もう少し整理すると

$$\begin{aligned} & 1095 - 3\alpha - 55\alpha^2 + 91\alpha\sqrt{-10} - 6\beta + 8\gamma - 249\phi - 177\psi - 4\phi\sqrt{-10} \in 2\mathcal{O}_K \\ \iff & 1 + \alpha + \alpha^2 + \alpha\sqrt{-10} + \phi - \psi \in 2\mathcal{O}_K \\ \iff & \frac{1 + \alpha + \alpha^2 + \alpha\sqrt{-10} + \phi - \psi}{2} \in \mathcal{O}_K \\ \iff & \frac{1 + \alpha + \alpha^2 + \alpha\sqrt{-10} + \dfrac{\alpha^4 + \alpha^3 + \alpha^2 + \alpha}{4} - \dfrac{\alpha^3 + \alpha}{2}}{2} \in \mathcal{O}_K \\ \iff & \frac{\alpha^4 - \alpha^3 + 5\alpha^2 + 3\alpha + 4 + 4\alpha\sqrt{-10}}{8} \in \mathcal{O}_K \end{aligned}$$

ついに新しい整数が見つかった！ この整数を χ とおく．念のため χ が整数であることを確かめておこう．

入力：
```
x1:-1.84208593463092;
x2:-0.35185424082737+1.70956104337032*%i;
x3:1.27289722392249-0.71979868148386*%i;
x4:1.27289722392249+0.71979868148386*%i;
x5:-0.35185424082737-1.70956104337032*%i;
y1:float(expand((x1^4-x1^3+5*x1^2+3*x1+4+4*x1*sqrt(10)*%i)/8));
y2:float(expand((x2^4-x2^3+5*x2^2+3*x2+4+4*x2*sqrt(10)*%i)/8));
y3:float(expand((x3^4-x3^3+5*x3^2+3*x3+4+4*x3*sqrt(10)*%i)/8));
```

```
y4:float(expand((x4^4-x4^3+5*x4^2+3*x4+4+4*x4*sqrt(10)*%i)/8));
y5:float(expand((x5^4-x5^3+5*x5^2+3*x5+4+4*x5*sqrt(10)*%i)/8));
float(expand((x-y1)*(x-y2)*(x-y3)*(x-y4)*(x-y5)));
```

出力：
```
x^5-4.989966620945027*10^-8*%i*x^4-4.999999800373159*x^4+15.81138776179206*%i*x^3
+4.999999685109708*x^3-31.62277501506436*%i*x^2+44.99999891008485*x^2
-15.81138709910382*%i*x-249.9999924974333*x+31.6227690563274*%i+435.9999839449914
```

この出力は χ が $x^5-5x^4+(5+5\sqrt{-10})x^3+(45-10\sqrt{-10})x^2-(250+5\sqrt{-10})x+436+10\sqrt{-10}=0$ の解であることを意味する．χ は確かに整数である．$2\chi=1+\alpha+\alpha^2+\alpha\sqrt{-10}+\phi-\psi$ であるから，χ を付け加え，$\alpha\sqrt{-10}$ の代わりに χ を基底に採用する．

同様にして行列 NM の 10 行目からは整数

$$\xi=\frac{1+\phi-\psi+\psi\sqrt{-10}}{2}=\frac{\alpha^4-\alpha^3+\alpha^2-\alpha+4+(2\alpha^3+2\alpha)\sqrt{-10}}{8}$$

が得られる．この ξ は

$$x^5-5x^4+(20+5\sqrt{-10})x^3+(80-40\sqrt{-10})x^2-(360+20\sqrt{-10})x-288+160\sqrt{-10}=0$$

の解である．$2\xi=1+\phi-\psi+\psi\sqrt{-10}$ であるから，ξ を付け加え，$\psi\sqrt{-10}$ の代わりに ξ を基底に採用する．

以上より $R_4=R_3[\chi,\ \xi]$ とおくと，$\mathcal{O}_K\supset R_4\supset R_3$ であって，$|R_4:R_3|=4$ より $|\mathcal{O}_K:R_4|=5$ がわかる．

$$R_4=\mathbb{Z}\phi+\mathbb{Z}\psi+\mathbb{Z}\alpha^2+\mathbb{Z}\alpha+\mathbb{Z}1+\mathbb{Z}\phi\sqrt{-10}+\mathbb{Z}\xi+\mathbb{Z}\gamma+\mathbb{Z}\chi+\mathbb{Z}\beta$$

§ 9　$\mathcal{O}_K$ の決定 2；5 巾の除去

$|\mathcal{O}_K:\mathcal{O}_F[\alpha]|=2^{12}\times 5^2$ であった．$\beta=\dfrac{-\alpha^4-\alpha^3-\alpha^2-\alpha+4}{8}+\dfrac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{80}\sqrt{-10}$ を付け加えることにより $|\mathcal{O}_K:\mathcal{O}_F[\alpha,\ \beta]|=2^8\times 5$ とできるのだが，ここでは β の添加は考えないことにする．

$K/\mathbb{Q}$ で (5) は $(5)=\mathfrak{P}^{10}$ と完全分岐する．この場合は $\mathrm{ord}_5\varpi=\dfrac{1}{10}$ なる $\varpi\in K$ をとれば $\mathcal{O}_{K,\mathfrak{P}}=\mathbb{Z}_5[\varpi]$ である．（この右辺は ϖ で生成される環を表す．）
もしくは $\varpi_0,\ \varpi_1,\ \cdots,\ \varpi_9\in K$ が $\mathrm{ord}_5\varpi_k=\dfrac{k}{10}$ $(k=0,\ 1,\ 2,\ \cdots,\ 9)$ を満たすなら $\mathcal{O}_{K,\mathfrak{P}}=\oplus_{k=0}^{9}\mathbb{Z}_5\varpi_k$ となるといってもよい．（この右辺は $\{\varpi_k\}$ で生成される加群を表す．）
ところが $\mathbb{Z}_5[\alpha,\ \sqrt{-10}]=\mathbb{Z}_5[\alpha-3,\ \sqrt{-10}]=\mathbb{Z}_5[\pi,\ \sqrt{-10}]$ （ただし $\pi=\alpha-3$ ）において，加群としての基底が

$$\begin{aligned}&\mathbb{Z}_5[\alpha,\ \sqrt{-10}]\\ =\ &\mathbb{Z}_5 1+\mathbb{Z}_5\pi+\mathbb{Z}_5\pi^2+\mathbb{Z}_5\pi^3+\mathbb{Z}_5\pi^4+\mathbb{Z}_5\sqrt{-10}+\mathbb{Z}_5\pi\sqrt{-10}+\mathbb{Z}_5\pi^2\sqrt{-10}+\mathbb{Z}_5\pi^3\sqrt{-10}+\mathbb{Z}_5\pi^4\sqrt{-10}\end{aligned}$$

のようにとれるが，$\mathrm{ord}_5\pi=\dfrac{1}{5}$, $\mathrm{ord}_5\sqrt{-10}=\dfrac{1}{2}$ であるから，

$$\mathrm{ord}_5 1=\frac{0}{10},\ \mathrm{ord}_5\pi=\frac{2}{10},\ \mathrm{ord}_5\pi^2=\frac{4}{10},\ \mathrm{ord}_5\pi^3=\frac{6}{10},\ \mathrm{ord}_5\pi^4=\frac{8}{10},$$
$$\mathrm{ord}_5\sqrt{-10}=\frac{5}{10},\ \mathrm{ord}_5\pi\sqrt{-10}=\frac{7}{10},\ \mathrm{ord}_5\pi^2\sqrt{-10}=\frac{9}{10},\ \mathrm{ord}_5\pi^3\sqrt{-10}=\frac{11}{10},\ \mathrm{ord}_5\pi^4\sqrt{-10}=\frac{13}{10}$$

となって，これらは $\mathcal{O}_{K,\mathfrak{P}}$ の基底をなしていない．しかし $\pi^3\sqrt{-10}$ の代わりに $\dfrac{\pi^3\sqrt{-10}}{5}$, $\pi^4\sqrt{-10}$ の代わりに $\dfrac{\pi^4\sqrt{-10}}{5}$ をとれば，$\mathrm{ord}_5\dfrac{\pi^3\sqrt{-10}}{5}=\dfrac{1}{10}$, $\mathrm{ord}_5\dfrac{\pi^4\sqrt{-10}}{5}=\dfrac{3}{10}$ となって，$\mathcal{O}_{K,\mathfrak{P}}$ の基底をなす．

$$\frac{\pi^3\sqrt{-10}}{5}=\frac{(\alpha-3)^3\sqrt{-10}}{5}=\frac{(\alpha^3-9\alpha^2+27\alpha-27)\sqrt{-10}}{5}$$
$$\frac{\pi^4\sqrt{-10}}{5}=\frac{(\alpha-3)^4\sqrt{-10}}{5}=\frac{(\alpha^4-12\alpha^3+54\alpha^2-108\alpha+81)\sqrt{-10}}{5}$$

なので，mod $\mathbb{Z}[\alpha]$ で係数を小さくして $\varphi_1=\dfrac{(\alpha^3+\alpha^2+2\alpha-2)\sqrt{-10}}{5}$, $\varphi_2=\dfrac{(\alpha^4-2\alpha^3-\alpha^2+2\alpha+1)\sqrt{-10}}{5}$ とおく，φ_1，φ_2 は (5) 以外の素因子を分母に持つことはないので，K の整数である．実際に φ_1 は

$$x^5+2\sqrt{-10}x^4-20x^3-40\sqrt{-10}x^2+320x+128=0$$

の解であり，φ_2 は

$$x^5-5\sqrt{-10}x^4-220x^3+620\sqrt{-10}x^2+900x-1620\sqrt{-10}=0$$

の解である．以上より

$$\begin{aligned}\mathcal{O}_{K,\mathfrak{P}} &= \mathbb{Z}_5 1+\mathbb{Z}_5\pi+\mathbb{Z}_5\pi^2+\mathbb{Z}_5\pi^3+\mathbb{Z}_5\pi^4+\mathbb{Z}_5\sqrt{-10}+\mathbb{Z}_5\pi\sqrt{-10}+\mathbb{Z}_5\pi^2\sqrt{-10}+\mathbb{Z}_5\frac{\pi^3\sqrt{-10}}{5}+\mathbb{Z}_5\frac{\pi^4\sqrt{-10}}{5}\\ &= \mathbb{Z}_5 1+\mathbb{Z}_5\alpha+\mathbb{Z}_5\alpha^2+\mathbb{Z}_5\alpha^3+\mathbb{Z}_5\alpha^4+\mathbb{Z}_5\sqrt{-10}+\mathbb{Z}_5\alpha\sqrt{-10}+\mathbb{Z}_5\alpha^2\sqrt{-10}+\mathbb{Z}_5\varphi_1+\mathbb{Z}_5\varphi_2\end{aligned}$$

とわかった．

注意　$\beta=\dfrac{-\alpha^4-\alpha^3-\alpha^2-\alpha+4}{8}+\dfrac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{80}\sqrt{-10}$ に対しては

$$\begin{aligned}&16\beta-\varphi_2\\ =\ &-2\alpha^4-2\alpha^3-2\alpha^2-2\alpha+8+\frac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{5}\sqrt{-10}-\frac{\alpha^4-2\alpha^3-\alpha^2+2\alpha+1}{5}\sqrt{-10}\\ =\ &-2\alpha^4-2\alpha^3-2\alpha^2-2\alpha+8+(\alpha^3+2\alpha^2-3\alpha-1)\sqrt{-10}\\ \in\ &\mathcal{O}_F[\alpha]\end{aligned}$$

の関係があるので $\mathcal{O}_{K,\mathfrak{P}}=\mathbb{Z}_5[\alpha,\ \varphi_1,\ \varphi_2]=\mathbb{Z}_5[\alpha,\ \varphi_1,\ \beta]$ といってもよい．

$|\mathcal{O}_K:R_4|=5$ だったから，$\mathcal{O}_K=R_4[\varphi_1]$ がわかった．R_4 の基底で表現すると

$$\varphi_1=\frac{(\alpha^3+\alpha^2+2\alpha-2)\sqrt{-10}}{5}=\frac{-8-6\alpha^2+12\xi+6\psi-2\phi\sqrt{-10}-4\phi+12\gamma+16\beta}{5}$$

であるから R_4 に $\varphi_1/2$ を付け加え，$\phi\sqrt{-10}$ の代わりに $\varphi_1/2$ を基底に採用すると，整数環 $\mathcal{O}_K$ になる．

結論 $\mathcal{O}_K = \mathbb{Z}1 + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \mathbb{Z}\phi + \mathbb{Z}\psi + \mathbb{Z}\varphi_1/2 + \mathbb{Z}\xi + \mathbb{Z}\gamma + \mathbb{Z}\chi + \mathbb{Z}\beta$ である．ここで,

$$
\begin{aligned}
\phi &= \frac{\alpha^4+\alpha^3+\alpha^2+\alpha}{4} \\
\psi &= \frac{\alpha^3+\alpha}{2} \\
\beta &= \frac{-\alpha^4-\alpha^3-\alpha^2-\alpha+4}{8} + \frac{\alpha^4+3\alpha^3+9\alpha^2-13\alpha-4}{80}\sqrt{-10} \\
\gamma &= \frac{\alpha^4+\alpha^3+\alpha^2-3\alpha-4}{8} + \frac{\alpha^4+3\alpha^3-\alpha^2-3\alpha-4}{40}\sqrt{-10} \\
\chi &= \frac{\alpha^4-\alpha^3+5\alpha^2+3\alpha+4+4\alpha\sqrt{-10}}{8} \\
\xi &= \frac{\alpha^4-\alpha^3+\alpha^2-\alpha+4}{8} + \frac{2\alpha^3+2\alpha}{8}\sqrt{-10} \\
\varphi_1/2 &= \frac{\alpha^3+\alpha^2+2\alpha-2}{10}\sqrt{-10}
\end{aligned}
$$

■

実際次のように行列表示すると,（行列部分を M とおいて） $\det M = \dfrac{1}{102400} = \dfrac{1}{2^{12}\cdot 5^2}$ である．

$$
\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \phi \\ \psi \\ \varphi_1/2 \\ \xi \\ \gamma \\ \chi \\ \beta \end{pmatrix}
=
\begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & \frac{1}{10} & \frac{1}{5} & -\frac{1}{5} \\
\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{2} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{3}{8} & -\frac{1}{2} & \frac{1}{40} & \frac{3}{40} & -\frac{1}{40} & -\frac{3}{40} & -\frac{1}{10} \\
\frac{1}{8} & -\frac{1}{8} & \frac{5}{8} & \frac{3}{8} & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & 0 \\
-\frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{2} & \frac{1}{80} & \frac{3}{80} & \frac{9}{80} & -\frac{13}{80} & -\frac{1}{20}
\end{pmatrix}
\begin{pmatrix} \alpha^4 \\ \alpha^3 \\ \alpha^2 \\ \alpha \\ 1 \\ \alpha^4\sqrt{-10} \\ \alpha^3\sqrt{-10} \\ \alpha^2\sqrt{-10} \\ \alpha\sqrt{-10} \\ \sqrt{-10} \end{pmatrix}
$$

逆に表示すると

$$
\begin{pmatrix} \alpha^4 \\ \alpha^3 \\ \alpha^2 \\ \alpha \\ 1 \\ \alpha^4\sqrt{-10} \\ \alpha^3\sqrt{-10} \\ \alpha^2\sqrt{-10} \\ \alpha\sqrt{-10} \\ \sqrt{-10} \end{pmatrix}
=
\begin{pmatrix}
0 & 0 & -1 & 4 & -2 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-7 & 3 & -11 & -11 & 9 & -20 & -4 & 28 & 22 & 24 \\
-1 & 1 & 1 & -1 & 1 & 0 & 4 & 0 & -2 & 0 \\
-7 & -3 & -1 & 5 & 1 & 0 & 0 & -4 & 2 & 8 \\
-1 & -1 & -1 & -1 & 1 & 0 & 0 & 0 & 2 & 0 \\
-5 & -2 & -1 & 1 & 2 & -5 & 2 & -2 & 2 & 4
\end{pmatrix}
\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \phi \\ \psi \\ \varphi_1/2 \\ \xi \\ \gamma \\ \chi \\ \beta \end{pmatrix}
$$

となり，この行列の determinant は $102400 = 2^{12}\cdot 5^2$ である．