体論: 期末試験的なレポート問題

- 言うまでもないことだが、数値的な答だけでは十分ではない。論理的な説明がもっと大事である。
- とくに、「... は既約である。」と書く場合には、理由を添えると加点される。(本題に関係のないことを書いている場合を除く。)
- maxima などの数式処理ソフトを用いてもよいが、肝心なところは自分でチェックや証明をすること。(必須ではないがもし使った場合には使用ソフト名を挙げてください。)

問題 30.1. $a, b \in \mathbb{Z}$ とし、b は 平方数ではないものとする。次の各問いに答えなさい。

(1) $K = \mathbb{Q}[\sqrt{b}]$ の $\mathbb{Q}$ 上の 拡大次数を求めなさい。

[答] $X^2 - b$ は $\sqrt{b}$ を根に持つ、$X^2 - b$ が $\mathbb{Z}$ 上既約であることは容易に確かめられる。Gauss の補題により、 $X^2 - b$ は $\mathbb{Q}$ 上既約である。よって、$\sqrt{b}$ の最小多項式は $X^2 - b$ (2 次式) で、よって $[K : \mathbb{Q}] = 2$. (10)

---

(2) K の元 $a + \sqrt{b}$ が K の元の平方ならば、$(a^2 - b)$ は 平方数であることを示しなさい。

[答] $a + \sqrt{b} = (c + d\sqrt{b})^2$ と仮定すると、$\mathbb{Q}$ 上の共役を考えて $a - \sqrt{b} = (c - d\sqrt{b})^2$ であることがわかる。[(1) により $\mathbb{Q}$ 上の位数にの「共役をとる写像」が存在することにも注目。]

２つの等式の両辺を辺々掛け合わせて、$(a^2 - b) = (c^2 - d^2 b)^2$. したがって、$a^2 - b \in \mathbb{Q}^2$ である。(1) と同じ議論を使うことにより、$a^2 - b \in (\mathbb{Z})^2$ であることがわかる。(20)

☆注意☆: $\alpha = a + a_2\sqrt{b} \in K$ に対して、その $\mathbb{Q}$ 上の共役 $\bar{\alpha} = a - a_2\sqrt{b} \in K$ を考え、$\alpha\bar{\alpha}$ のことを $\alpha \in K$ の $\mathbb{Q}$ 上のノルムと呼ぶ。今回の解答例ではこれを $N(\alpha)$ で書くことにする。$N(\alpha) \in \mathbb{Q}$ であること、α に関して乗法的であること ($\forall \alpha, \beta \in K$ にたいして $N(\alpha\beta) = N(\alpha)N(\beta)$) に注意。一般のノルムの定義や性質の詳細については Milne の “Fields and Galois theory” でも参照のこと。

※以下の小問では a^2-b は平方数でないとする。※

(3) $\sqrt{a+\sqrt{b}}$ の $\mathbb{Q}$ 上の最小多項式 $m(X)$ を求めなさい。

[答] $m_0(X)=(X^2-a)^2-b$ は候補である。$M=\mathbb{Q}(\sqrt{a+\sqrt{b}})\subset\mathbb{Q}(\sqrt{b})$ とおく。(1) と同じ議論と (2) により、$[M:K]=2$. 従って $[M:\mathbb{Q}]=[M:K][K:\mathbb{Q}]=2\cdot 2=4$ がわかる。よって $m=m_0$ が求める答である。(20)

※ さらに以下の小問では a,b は互いに素で、$a^2-b\geq 2$ とする。 ※

問題が難しくなりすぎていたので

以下では必要なら (上の仮定のもとで) 「(あ) $\mathbb{Q}$ 上 $\sqrt{b}$, $\sqrt{a^2-b}$ は $\mathbb{Q}$ 上一次独立である」ことを証明なしに使ってもよい。(もちろん証明もつけていただいてもよいが。

念のため (あ) を証明しておこう、次のことを言えばよい。

命題 30.1. $[\mathbb{Q}(\sqrt{b},\sqrt{a^2-b}):\mathbb{Q}]=4$

証明. $\mathbb{Q}(\sqrt{a^2-b}):K])=2$ を示せば十分。a^2-b が　K の元 $x+y\sqrt{b}$ $(x,y\in\mathbb{Q})$ の平方なら、

$$x^2+by^2+2xy\sqrt{b}=a^2-b$$

$\sqrt{b}$ は ((1) により) $\mathbb{Q}$ 上二次の元であるから、

$$x^2+by^2=a^2-b \text{ and } 2xy=0.$$

第二式より、$x=0$ か $y=0$ でなければならないが、

(a) $x=0$ のとき 第一式から $x^2=a^2-b$ だが、仮定と (1) と同様のガウスの補題の議論によりこれは無理。

(b) $y=0$ のとき、第一式から $(by)^2=b(a^2-b)$ がでてくるが、上の仮定により $b(a^2-b)$ は平方数ではありえない。($\gcd(b,a^2-b)=\gcd(a^2,b)$ で、結局 b と a^2-b とは互いに素であるから。)

□

(4) $m(X)$ の最小分解体を L とおく。L および $[L:\mathbb{Q}]$ を求めなさい。

[答] $A=\sqrt{a+\sqrt{b}}$ $B=\sqrt{a-\sqrt{b}}$ とおくと、$m_0(X)=(X-A)(X+A)(X-B)(X-B)$ であるから、

$L=\mathbb{Q}(A,B)=\mathbb{Q}(\sqrt{a+\sqrt{b}},\sqrt{a-\sqrt{b}})$ である。$[L:\mathbb{Q}]=8$ であることを示そう。$A^2-a=\sqrt{b}, AB=\sqrt{a^2-b}$ であるから、$L\supset\mathbb{Q}(\sqrt{b},\sqrt{a^2-b})$.

(Claim:) $$A\notin\mathbb{Q}((\sqrt{b},\sqrt{a^2-b})$$

Claim の証明:$\gamma_0=a+\sqrt{b}\in K$,$c=a^2-b\in\mathbb{Q}$ とおく。K の 元 α,β が $(\alpha+\beta\sqrt{c})^2=\gamma_0=a+\sqrt{b}$ を満たしたとすると、$\alpha^2=\gamma_0$ or $c\beta^2=\gamma^0$ ☆で言及したノルムの議論を用いて $N(\alpha)^2=N(\gamma_0)$ or $N(\beta)^2N(c)=N(\gamma_0)$ を満たさ泣けばいけないが、現在の状況ではいずれも無理である。

よって L は $\mathbb{Q}(A,B)$ の真の拡大体で、2 次拡大。だから $[L:\mathbb{Q}]=[L:\mathbb{Q}(A,B)][\mathbb{Q}(A,B):\mathbb{Q}]=4\cdot2=8.$ (10)

---

(5) L の $\mathbb{Q}$ 上のガロア群 G をもとめよ。
[答] 位数 8 の群をキチンと同定せねばならない。生成元と関係式でやるのがよい。答は 2 面数群 D_4 である。(20)

(6) L の部分体をすべて求めなさい。
[答] 全部やって (20)

次ページに (5),(6) についてもう少し詳しく書こう。いろいろなやり方があるので手順の詳細は省く。

$g :\in G = \mathrm{Gal}(L/\mathbb{Q})$ に対して、

$$g(\sqrt{a+\sqrt{b}}) = \epsilon_g \sqrt{a+\eta_g\sqrt{b}}$$
$$g(\sqrt{a-\sqrt{b}}) = \rho_g \sqrt{a+\pi_g\sqrt{b}}$$

となる $\{\epsilon_g, \eta_g, \rho_g, \pi_g\} \in \{\pm 1\}$ が存在する。上の式を辺々二乗すれば $\eta_g = -\pi_g$ であることがわかるから、

$$\begin{cases} g(\sqrt{a+\sqrt{b}}) = \epsilon_g \sqrt{a+\eta_g\sqrt{b}} \\ g(\sqrt{a-\sqrt{b}}) = \rho_g \sqrt{a-\eta_g\sqrt{b}} \end{cases}$$

逆に $g \in G$ は $\{\epsilon_g, \eta_g, \rho_g\}$ を決めると一意に決まるから、$g = g_{\epsilon,\eta,\rho}$ と書こう。つまり、

$$\begin{cases} g_{\epsilon,\eta,\rho}(\sqrt{a+\sqrt{b}}) = \epsilon\sqrt{a+\eta\sqrt{b}}, \\ g_{\epsilon,\eta,\rho}(\sqrt{a-\sqrt{b}}) = \rho\sqrt{a-\eta\sqrt{b}}. \end{cases}$$

個数の関係から、$\{g_{\epsilon,\eta,\rho}; \epsilon, \eta, \rho \in \{\pm 1\}\}$ の 8 つがちょうど G の元である。

$$g_{\epsilon,\eta,\rho}(\sqrt{b}) = \eta\sqrt{b}$$
$$g_{\epsilon,\eta,\rho}(\sqrt{a^2-b}) = \epsilon\rho\sqrt{a^2-b}$$

に注意しておこう。

$$\sigma = g_{-1,-1,1}, \quad \tau = g_{1,-1,1}$$

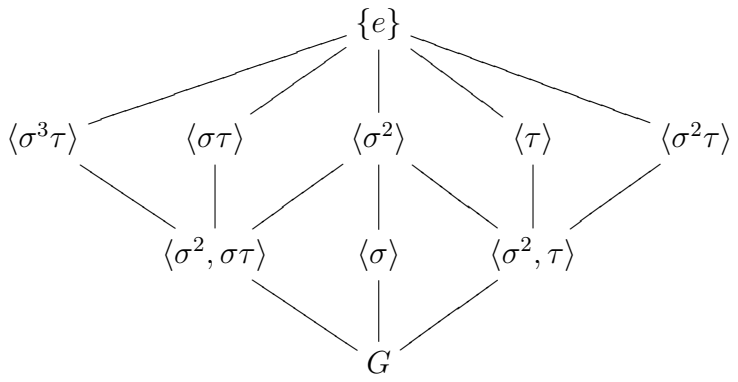
と置けば、σ は位数 4 の元, τ は 2 面体群 D_4

$$\sigma^4 = e, \quad \tau^2 = e, \quad \tau\sigma\tau^{-1} = \tau^{-1}$$

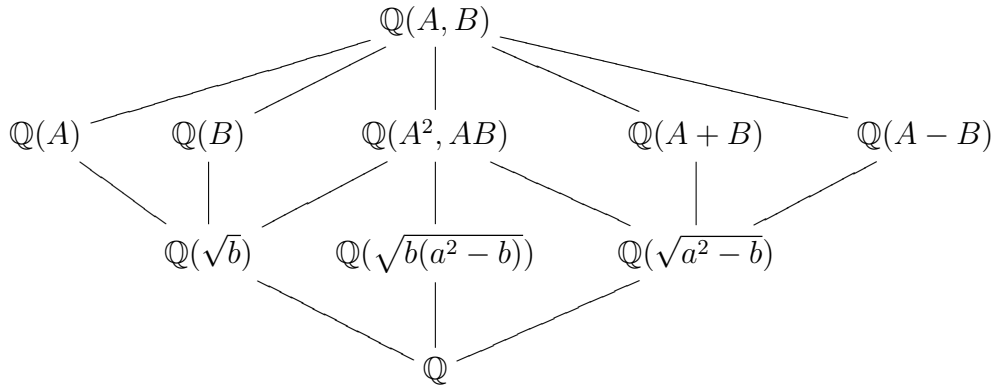
であることがわかる。$A = \sqrt{a+\sqrt{b}}, \qquad B = \sqrt{a-\sqrt{b}}$ の言葉で言えば、

$$\sigma(A) = -B, \sigma(B) = A, \tau(A) = B, \tau(B) = A.$$

D_4 の部分群をすべて求める。オイラーラグランジュの定理により、部分群の位数は 8 の約数である。それらがどういう体に対応するかは次ページのハッセ図を参照のこと。ハッセ図という言葉は本講義中には使わなかったし、解答中必須というわけではありません。意味はググってください。



対応する中間体のハッセ図は以下の通り。



注意:

$$A=\sqrt{a+\sqrt{b}},\quad B=\sqrt{a-\sqrt{b}}.$$
$$A^2=a+\sqrt{b},\quad B^2=a-\sqrt{b},\quad AB=\sqrt{a^2-b}$$

$$\mathbb{Q}(A^2,AB)=\mathbb{Q}(\sqrt{b},\sqrt{a^2-b})$$

$$(A\pm B)^2=A^2+B^2\pm 2AB=2a\pm\sqrt{a^2-b}$$

により $\mathbb{Q}(A\pm B)$ は $\mathbb{Q}(\sqrt{a^2-b})$ の 2 次拡大体であることがわかる。