Problem sheet 2 Solutions

Problem 1

Let N be the largest number such that N^2 divides $\Delta[1, \sqrt{d}]$. As we evaluate

$$\Delta[1, \sqrt{d}] = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d,$$

we get $N = 2$. Following the algorithm given in the proof of Theorem 3.21, it suffices to check if $\frac{1}{2}$, $\frac{\sqrt{d}}{2}$, and $\frac{1+\sqrt{d}}{2}$ are algebraic integers or not. The minimal polynomials of $\frac{1}{2}$ and $\frac{\sqrt{d}}{2}$ are $2x-1$ and $4x^2-d$, respectively, hence $\frac{1}{2}$ and $\frac{\sqrt{d}}{2}$ are not algebraic integer. By straightforward computation one can also check that the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is $4x^2-4x-(d-1)$ if $d \not\equiv 1(\text{mod}4)$ and $x^2-x-\frac{d-1}{4}$ if $d \equiv 1(\text{mod}4)$.

If $d \not\equiv 1(\text{mod}4)$, then none of $\frac{1}{2}$, $\frac{\sqrt{d}}{2}$, and $\frac{1+\sqrt{d}}{2}$ is an algebraic integer, hence $\{1, \sqrt{d}\}$ is an integral basis. If $d \equiv 1(\text{mod}4)$, then $\frac{1+\sqrt{d}}{2}$ is an algebraic integer and we also have

$$\det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = d.$$

Since d is square-free, $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis.

Problem 2

It suffices to show that $\{1, \alpha, \alpha^2\}$ is an integral basis of $\mathcal{O}_k$. Let $\sigma_1, \sigma_2, \sigma_3$ be the complex embeddings of K and denote $\theta_i = \sigma_i(\alpha)$ for $i = 1, 2, 3$. We also denote $s_1 = \theta_1 + \theta_2 + \theta_3$, $s_2 = \theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1$, and $s_3 = \theta_1\theta_2\theta_3$. We have

$$s_1 = 0, \quad s_2 = 2, \quad s_3 = -1$$

by Vieta's formulas. We now evaluate $\Delta[1, \alpha, \alpha^2]$ using Proposition 2.39:

$$\begin{aligned}
\Delta[1, \alpha, \alpha^2] &= (-1)^{\frac{3\dot{2}}{2}} N_{K/\mathbb{Q}}(Df(\theta)) = -N_{K/\mathbb{Q}}(3\alpha^2+2) \\
&\quad - \prod_{i=1}^{3} \sigma_i(3\alpha^2+2) = -\prod_{i=1}^{3}(3\sigma_i(\alpha)^2+2) = -(3\theta_1^2+2)(3\theta_2^2+2)(3\theta_3^2+2) \\
&= -27\theta_1^2\theta_2^2\theta_3^2 - 18(\theta_1^2\theta_2^2+\theta_2^2\theta_3^2+\theta_3^2\theta_1^2) - 12(\theta_1^2+\theta_2^2+\theta_3^2) - 8 \\
&= -27s_3^2 - 18(s_2^2-2s_1s_3) - 12(s_1^2-2s_2) - 8 = -59.
\end{aligned}$$

Note that $\Delta[1, \alpha, \alpha^2] = -59$ is square-free. By Corollary 3.22, $\{1, \alpha, \alpha^2\}$ is an integral basis of $\mathcal{O}_k$, hence $\mathcal{O}_k = \mathbb{Z}[\alpha]$.

Problem 3

As $\theta_1, \cdots, \theta_n$ is an integral basis of K and $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$, there exist $d_{ij} \in \mathbb{Z}$ for $1 \leq i, j \leq n$ such that

$$\alpha_i = \sum_{j=1}^{n} d_{ij}\theta_j.$$

Let D be the integral matrix given by $D = (d_{ij})_{1 \leq i,j \leq n}$. By Proposition 2.32, we have

$$\Delta[\alpha_1, \cdots, \alpha_n] = \det(D)^2 \Delta[\theta_1, \cdots, \theta_n]. \tag{1}$$

If $\Delta[\alpha_1, \cdots, \alpha_n] = \Delta[\theta_1, \cdots, \theta_n]$, then $\det D = \pm 1$, hence D^{-1} is an integral matrix. We may write $D^{-1} = (f_{ij})_{1 \leq i,j \leq n}$, where $f_{ij} \in \mathbb{Z}$. It follows that $\theta_i = \sum_{j=1}^{n} f_{ij}\alpha_j$ for $1 \leq i \leq n$. Any elements in $\mathcal{O}_K$ is expressed by a $\mathbb{Z}$-linear combination of $\theta_1, \cdots, \theta_n$, hence $\mathbb{Z}$-linear combination of $\alpha_1, \cdots, \alpha_n$. Thus, $\alpha_1, \cdots, \alpha_n$ is an integral basis of K.

Conversely, suppose that $\alpha_1, \cdots, \alpha_n$ is an integral basis of K. As both of $\{\theta_1, \cdots, \theta_n\}$ and $\{\alpha_1, \cdots, \alpha_n\}$ are integral bases, there exist $F = (f_{ij})_{1 \leq i,j \leq n}$ with $f_{ij} \in \mathbb{Z}$ such that $\theta_i = \sum_{j=1}^{n} f_{ij}\alpha_j$. Then by Proposition 2.32 we have

$$\Delta[\theta_1, \cdots, \theta_n] = \det(F)^2 \Delta[\alpha_1, \cdots, \alpha_n]. \tag{2}$$

Note that $\det(D), \det(F) \in \mathbb{Z}$. Combining (1) and (2), we conclude that $\Delta[\theta_1, \cdots, \theta_n] = \Delta[\alpha_1, \cdots, \alpha_n]$.

Problem 4

The minimal polynomial of $3^{\frac{1}{3}}$ is $f(t) = t^3 - 3$. This is a special case of Example 3.31 for $p = 3$.

Problem 5

(a) Let L be the Galois closure of K over $\mathbb{Q}$. For an element τ of the Galois group of L and a complex embedding σ of K, $\tau \circ \sigma$ is also a complex embedding of K. It follows that τ induces a permutation of $\{\sigma_1, \cdots, \sigma_n\}$.

If the permutation induced by τ is even, then we have $\tau P = P$ and $\tau N = N$. If the permutation is odd, then we have $\tau P = N$ and $\tau N = P$. In either cases, τ fixes $P + N$ and PN. To sum up, $P + N$ and PN are fixed

by every elements of the Galois group of L, hence they are rational. On the other hand, they are also algebraic integers. Therefore, $P+N$ and PN are integers.

(b) Observe that $\det(\sigma_i(x_j))_{1\leq i,j\leq n} = P - N$. It follows that

$$\Delta[x_1, \cdots, x_n] = \big(\det(\sigma_i(x_j))_{1\leq i,j\leq n}\big)^2 = (P-N)^2 = (P+N)^2 - 4PN.$$

Since we have $P+N, PN \in \mathbb{Z}$ from (a), $\Delta[x_1, \cdots, x_n] \equiv 1 (\mathrm{mod} 4)$.