Solutions

Problem 1 :

1) $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$, $\alpha = \frac{\sqrt{3}+\sqrt{7}}{2} \in K$

α is a root of $X^2 - \sqrt{3}X - 1$ (we follow the hint)

Indeed, $\alpha^2 - \sqrt{3}\alpha - 1 = \left(\frac{10+2\sqrt{3}\sqrt{7}}{4}\right) - \sqrt{3}\,\frac{\sqrt{3}+\sqrt{7}}{2} - 1 =$

$$= \frac{5+\sqrt{3}\sqrt{7}}{2} - \frac{3+\sqrt{3}\sqrt{7}}{2} - \frac{2}{2} = \frac{5+\sqrt{3}\sqrt{7} - 3 - \sqrt{3}\sqrt{7} - 2}{2} = 0$$

It follows that α is integral over $\mathbb{Z}[\sqrt{3}]$

($X^2 - \sqrt{3}X - 1$ is monic with coeff. in $\mathbb{Z}[\sqrt{3}]$)

But $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{3}]$ is integral $\Rightarrow$ α is integral over $\mathbb{Z}$.

2)

$$N_{\mathbb{Q}}^{L}(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha) = \alpha\, \sigma_1(\alpha)\, \sigma_2(\alpha)\, (\sigma_1 \circ \sigma_2)(\alpha) =$$

$$= \underbrace{\frac{\sqrt{3}+\sqrt{5}}{2} \quad \frac{-\sqrt{3}+\sqrt{5}}{2}} \cdot \underbrace{\frac{\sqrt{3}-\sqrt{5}}{2} \quad \frac{-\sqrt{3}-\sqrt{5}}{2}} =$$

use $(x-y)(x+y) = x^2 - y^2$

$$= \frac{5-3}{4} \cdot -\frac{3-5}{4} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin \mathbb{Z} \Rightarrow$$ α is not integral $/\mathbb{Z}$.

Problem 2

1)

$$\deg(\underset{\uparrow}{X^3}-X-1)=3$$

monic + no roots in $\mathbb{Z}$ $\Rightarrow$ irreducible over $\mathbb{Z}$ and also over $\mathbb{Q}$.

2) ~~Let~~ $1,\alpha,\alpha^2$ is a $\mathbb{Q}$-basis of K

Let $\beta\in K$ denote $\varphi_\beta: K\longrightarrow K$, $x\longmapsto\beta x$ and M_β = matrix of β with respect to the $\mathbb{Q}$-basis $1,\alpha,\alpha^2$

Then $\mathrm{Tr}^K_{\mathbb{Q}}(\beta)=\mathrm{Tr}^{\cancel{K}}_{\cancel{\mathbb{Q}}}(M_\beta)$

- $\varphi_\alpha(1)=\alpha$
  $\varphi_\alpha(\alpha)=\alpha^2$
  $\varphi_\alpha(\alpha^2)=\alpha^3\underset{\uparrow}{=}\alpha+1$

  since α is a root of X^3-X-1

$$\Rightarrow M_\alpha=\begin{array}{c|ccc} & \alpha & \alpha^2 & \alpha^3=\alpha+1\\ \hline 1 & 0 & 0 & 1\\ \alpha & 1 & 0 & 1\\ \alpha^2 & 0 & 1 & 0\end{array}\rightsquigarrow \mathrm{Tr}^K_{\mathbb{Q}}(\alpha)=\mathrm{Tr}(M_\alpha)=0$$

Another argument: $K=\mathbb{Q}(\alpha)$, ~~an~~ then

X^3-X-1 = min and also characteristic polynomial of $\alpha/\mathbb{Q}$

$=X^3-\mathrm{Tr}(\alpha)X^2+\dots$ $\Rightarrow$ $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha)=0$

- Similarly:

$$M_{\alpha^2}=\begin{array}{c|ccc} & \alpha^2 & \alpha^3 & \alpha^4=\alpha^3\cdot\alpha=\alpha^2+\alpha\\ \hline 1 & 0 & 1 & 0\\ \alpha & 0 & 1 & 1\\ \alpha^2 & 1 & 0 & 1\end{array}\Rightarrow \mathrm{Tr}^K_{\mathbb{Q}}(\alpha^2)=2$$

- $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha^3)=\mathrm{Tr}^K_{\mathbb{Q}}(\alpha+1)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(1)=0+3=3$

- $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha^4)=\mathrm{Tr}^K_{\mathbb{Q}}(\alpha^2+\alpha)=\mathrm{Tr}(\alpha^2)+\mathrm{Tr}(\alpha)=2+0=2$

3)

$$D^{K}_{\mathbb{Q}}(1,\alpha,\alpha^2) \underset{def}{\overset{\uparrow}{=}} \det\left(\mathrm{TR}(\alpha^i\alpha^j)\right)_{0\le i,j\le 2} =$$

$$= \det\begin{pmatrix} Tr(1) & Tr(\alpha) & Tr(\alpha^2) \\ Tr(\alpha) & Tr(\alpha^2) & Tr(\alpha^3) \\ Tr(\alpha^2) & Tr(\alpha^3) & Tr(\alpha^4) \end{pmatrix} = \det\begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} =$$

$$\underset{\text{Laplace formula for 1. line}}{=} 3\cdot\begin{vmatrix} 2 & 3 \\ 3 & 2 \end{vmatrix} + 2\begin{vmatrix} 0 & 2 \\ 2 & 3 \end{vmatrix} = 3(4-9) + 2(-4) =$$

$$= -15 - 8 = -23$$

Rk One can also compute $D^K_{\mathbb{Q}}(1,\alpha,\alpha^2)$ using the formula from Ex 3, Sheet 3

4) $1, \alpha, \alpha^2 \in \mathcal{O}_K$, $d_K = D^K_{\mathbb{Q}}\underbrace{(x_1, x_2, x_3)}_{\mathbb{Z}\text{-basis of } \mathcal{O}_K}$

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \underset{M_3(\mathbb{Z})}{\underset{\in}{A}} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \Rightarrow -23 = \underbrace{(\det A)^2}_{\text{square in } \mathbb{Z}} \cdot d_K$$

Since, -23 is <u>square free</u> $\Rightarrow \det A = \pm 1$

$\Rightarrow$ A is invertible in $M_3(\mathbb{Z}) \Rightarrow 1, \alpha, \alpha^2$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

(This was discussed many times in lecture/exercises)

5) From lecture and question (4) we know that

23 ramifies in K.

Write prime decomposition $23\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$

From lecture we know $3 = [K:\mathbb{Q}] = \sum_{i=1}^{r} e_i f_i$

Assume $f_i \ge 2$ for some i, ~~then $e_i f_i \ge 2$~~

note that $e_i = 1$ (otherwise $e_i f_i \ge 4 > 3$)

$\hookrightarrow$ there is another j with $e_j > 1$, then $e_j \ge 2$

We get $3 \ge e_i f_i + e_j f_j \ge 2 + 2 = 4$ ↯

6) $\alpha^3-\alpha-1=0 \Rightarrow \cancel{\alpha^3+}\ 1=\alpha^3-\alpha=\alpha(\alpha^2-1)=\alpha(\alpha-1)\underline{(\alpha+1)}$

$\Rightarrow \alpha+1\in\mathcal{O}_K^*$

<u>Rk</u>: One can also compute that $N^K_{\mathbb{Q}}(\alpha+1)=1$

7) $K\subseteq\mathbb{R} \Rightarrow \mu(K)=\{\pm 1\}$.

X^3-X-1 has 2 complex and one real root $\Rightarrow r_2=1,\ r_1=1$

Theorem from the lecture implies that $\mathcal{O}_K^*\simeq\mu(K)\oplus\mathbb{Z}^{r_1+r_2-1}$

$\simeq\mu(K)\oplus\mathbb{Z}$

Let $\varepsilon\in\mathcal{O}_K^*$ be a fundamental unit (generator of $\mathbb{Z}$)

Then every unit we can uniquely write $\pm\varepsilon^l$ where $l\in\mathbb{Z}$

Then $(\alpha+1)=\pm\varepsilon^l$
and where $l,k\neq 0$, since $\alpha+1\neq\pm1$
$u=\pm\varepsilon^k$ $u\neq\pm1$

Then take $n=2k$, $m=2l$, we get

$(\alpha+1)^n=\varepsilon^{2lk}=u^{2m}$

Problem 3

1) $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}] = \mathbb{Z}[X]/_{X^2-10}$

prime ideal in $\mathcal{O}_K$ ↓

$\mathcal{O}_K/_{2\mathcal{O}_K} \simeq \mathbb{Z}/_2[X]/_{X^2} \overset{\text{Lecture}}{\Rightarrow} 2\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p} = (2, \sqrt{10})$

$N(\mathfrak{p}) = 2 = \cancel{\deg}\ 2^{\deg X}$

$\mathcal{O}_K/_{3\mathcal{O}_K} \simeq \mathbb{Z}/_3[X]/_{\underbrace{(X^2-10) \bmod 3}_{X^2-1=(X-1)(X+1)}} \Longrightarrow 3\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$, $\mathfrak{q}_1 = (3, \sqrt{10}-1)$, $\mathfrak{q}_2 = (3, \sqrt{10}+1)$ prime ideals in $\mathcal{O}_K$

$N(\mathfrak{q}_1) = N(\mathfrak{q}_2) = 3$

2) If $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ with $N(\mathfrak{p}) = 2$

Then $N(\mathfrak{p}) = |\mathcal{O}_K/_{\mathfrak{p}}| = 2 \Rightarrow 2 \cdot \bar{1} = \bar{0}$ in $\mathcal{O}_K/_{\mathfrak{p}} \Rightarrow 2 \in \mathfrak{p}$

$\Rightarrow 2\mathcal{O}_K \subseteq \mathfrak{p} \Rightarrow \mathfrak{p}$ ~~a~~ is a prime factor in the decomp. of $2\mathcal{O}_K$

$\Longrightarrow$ there is only one such ideal.
by (1)

Assume $\mathfrak{p}$ is princip~~ab~~le, that is $\mathfrak{p} = (\underbrace{a + \sqrt{10}b}_{\in \mathcal{O}_K})$, $a, b \in \mathbb{Z}$

~~Comparing~~ Then $|N^K_{\mathbb{Q}}(a + \sqrt{10}b)| = N(\mathfrak{p}) = 2$

$$\overset{\shortparallel}{|a^2 - 10b^2|}$$

We get $a^2 - 10b^2 = \pm 2$ (~~∄~~ no solutions in $\mathbb{Z}$, since no solutions mod 5 $a^2 \not\equiv \pm 2 \bmod 5$) ↯

3) $\mathfrak{p}$ is not principle $\Rightarrow \bar{\mathfrak{p}} \neq \bar{1}$ in $C(\mathcal{O}_K)$

$\mathfrak{p}^2 = \underbrace{2\mathcal{O}_K}_{\text{principle}} \Rightarrow \bar{\mathfrak{p}}^2 = \bar{1}$ in $C(\mathcal{O}_K) \Rightarrow \operatorname{ord} \bar{\mathfrak{p}} = 2$ in $C(\mathcal{O}_K)$

4) $r_2 = 0$, $n = 2$, $d_K = 4 \cdot 10$ $\quad \left(\frac{4}{\pi}\right)^{\cancel{a}} \cancel{m}\ \frac{2!}{2^2}\sqrt{4 \cdot 10} = \sqrt{10} < 4$ (but > 3).

5) From the Lecture (and question 1) we know that $C(\mathcal{O}_K) = \{\bar{1}, \bar{\mathfrak{p}}, \bar{\mathfrak{q}}_1, \bar{\mathfrak{q}}_2\}$

$\bar{\mathfrak{p}} \neq \bar{1}$, and $\bar{\mathfrak{p}}^2 = \bar{1}$. Also $\mathfrak{q}_1\mathfrak{q}_2 = 3\mathcal{O}_K \Rightarrow \bar{\mathfrak{q}}_1\bar{\mathfrak{q}}_2 = \bar{1} \Rightarrow \bar{\mathfrak{q}}_2 = \bar{\mathfrak{q}}_1^{-1}$

$$N((2+\sqrt{10})\mathcal{O}_K) = |N^K_{\mathbb{Q}}(2+\sqrt{10})| = 6$$

Write $(2+\sqrt{10})\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdot\ldots\cdot\mathfrak{p}_r^{e_r}$ in $\mathcal{O}_K$

Then by taking norms:

$$6 = N(\mathfrak{p}_1)^{e_1}\cdot\ldots\cdot N(\mathfrak{p}_r)^{e_r}$$

Since $N(\mathfrak{p}_i)$ is always a power of prime number

$\Rightarrow N(\mathfrak{p}_i) = 2$ or 3 (all such $\mathfrak{p}_i$ are from question (1))

It follows, $\underline{(2+\sqrt{10})\mathcal{O}_K = \mathfrak{p}\cdot\mathfrak{q}_i}$, where $i = 1$ or 2.

Anyway $\bar{\mathfrak{p}}\bar{\mathfrak{q}}_i = \bar{1}$ in $C(\mathcal{O}_K) \underset{\substack{\uparrow\\ \text{ord}\,\bar{\mathfrak{p}}=2}}{\Rightarrow} \bar{\mathfrak{q}}_i = \bar{\mathfrak{p}}^{-1} = \bar{\mathfrak{p}}$

and $\bar{\mathfrak{q}}_i^{-1} = \bar{\mathfrak{p}}$

Hence $\bar{\mathfrak{q}}_1 = \bar{\mathfrak{q}}_2 = \bar{\mathfrak{p}} \Rightarrow C(\mathcal{O}_K) = \{\bar{1}, \bar{\mathfrak{p}}\} \simeq \mathbb{Z}/2$.

Another way:

$$6\mathcal{O}_K = \underset{\mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2}{2\mathcal{O}_K\cdot 3\mathcal{O}_K} \underset{\substack{\uparrow\\ \text{since } 6=-(2+\sqrt{10})(2-\sqrt{10})}}{\subseteq} \overbrace{(2+\sqrt{10})\mathcal{O}_K}^{\text{of norm}=6} \Longrightarrow (2+\sqrt{10})\mathcal{O}_K = \mathfrak{p}\mathfrak{q}_i$$

Problem 4

1) Recall that every $x \in K$ we can uniquely write as
$x = u\pi^n$, $u \in A^*$, π uniformizer in A, $n \in \mathbb{Z}$
Moreover, $x \in A \iff n \geq 0$
$x \in A^* \iff n = 0$
$x \notin A \iff n < 0$ (In particular, if $\overset{n<0}{x = u\pi^n \notin A}$, then $x^{-1} = u^{-1}\underset{-n>0}{\pi^{-n}} \in A$)

Assume $\mathcal{O}_K \not\subset A$, then $\exists\, x \in \mathcal{O}_K$ but $x \notin A$.

$x \in \mathcal{O}_K \Rightarrow (*)\ x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$ in K for some $a_i \in \mathbb{Z}$

If $x \notin A$, then $x^{-1} \in A$

Multiplying $(*)$ by $(x^{-1})^{n-1} = x^{-(n-1)} \in A$ we get

$$x + a_{n-1} + a_{n-2}x^{-1} + \dots + a_1 x^{-(n-2)} + a_0 x^{-(n-1)} = 0$$

$$\Rightarrow \quad A \not\ni x = -a_{n-1} - a_{n-2}x^{-1} - \dots - a_1 x^{-(n-2)} - a_0 x^{-(n-1)} \in A \quad ↯$$

(note that $\mathbb{Z} \subset A$, since $1 \in A$).

2) Let $\mathcal{O}_K \xhookrightarrow[\varphi]{} A$, then $\mathfrak{p} := \varphi^{-1}(\mathfrak{m}) = \mathfrak{m} \cap \mathcal{O}_K \in \operatorname{Spec} \mathcal{O}_K$.

& Let $0 \neq x \in \mathfrak{m}$

Since K is the fraction field of $\mathcal{O}_K$ we can write $x = \frac{a}{b}$, where $a, b \in \mathcal{O}_K$. Hence $0 \neq bx \in \mathfrak{m} \cap \mathcal{O}_K = \mathfrak{p}$

It follows that $\mathfrak{p} \neq 0$.

3) $(\mathcal{O}_K)_\mathfrak{p} = \left\{ \frac{a}{s} \mid s, a \in \mathcal{O}_K,\ s \notin \mathfrak{p} \right\} \subset K$

$s \in \mathcal{O}_K \subset A$, and $s \notin \mathfrak{p} \Rightarrow s \notin \mathfrak{m}$ (as an element in A)

$\xRightarrow[\text{A loc}]{\text{A local}}\ s \in A^* \Rightarrow \frac{1}{s} \in A \Rightarrow a \cdot \frac{1}{s} \in A \Rightarrow (\mathcal{O}_K)_\mathfrak{p} \subset A$

4) From the lecture we know that $(\mathcal{O}_K)_\mathfrak{p}$ is dvr with uniformizer $t \in \mathcal{O}_K$.
Assume $(\mathcal{O}_K)_\mathfrak{p} \subsetneq A$. Then $\exists\, x \in A$ such that $x \notin \mathcal{O}_K$.
$x \notin \mathcal{O}_K \Longrightarrow x^{-1} \in \mathcal{O}_K \subset A \Rightarrow x^{-1} \in A \xRightarrow[\text{since also } x \in A]{} x \in A^*$
Either for x or x^{-1} (both are in A^*) we have $= \varpi t^n$, $n > 0$, $\varpi \in \mathcal{O}_K^*$
$\varpi t^n \in A^* \Rightarrow t \in A^* \xRightarrow[\text{since } t^{-1} \in A]{} K = \operatorname{Frac}((\mathcal{O}_K)_\mathfrak{p}) = A$. Contradiction, since A is not a field