HW1

1). $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$.

else $\sqrt{m} = a+b\sqrt{n} \Rightarrow m = a^2+b^2n+2ab\sqrt{n}$

$\Rightarrow \sqrt{m} \in \mathbb{Q}$ so $\mathbb{Q}(\sqrt{m},\sqrt{n})/\mathbb{Q}(\sqrt{n})$ is quadratic with $\sqrt{m} \mapsto \pm\sqrt{m}$ as embeddings so the formulae follow

2). (a) L/K $Tr_{L/K}, N_{L/K} : O_L \to O_K$

$Tr_{K/\mathbb{Q}(\sqrt{m})} (a+b\sqrt{m}+c\sqrt{n}+d\sqrt{mn}) = 2a+2b\sqrt{m}$

$/\mathbb{Q}(\sqrt{n})$ $= 2a+2c\sqrt{n}$

$/\mathbb{Q}(\sqrt{mn})$ $= 2a+2d\sqrt{n}$

$\in O_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z}[\sqrt{m}]$ so ~~the result~~ it follows that every $\alpha \in O_K$ of the form $\frac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{mn}}{2}$

$a,b,c,d \in \mathbb{Z}$.

$N_{K/\mathbb{Q}(\sqrt{n})}(\alpha) = \frac{a^2-b^2m+c^2n-d^2mn+2(ac-bdm)\sqrt{n}}{4}$

$\in O_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$

so $a^2-b^2m+c^2n-d^2mn \equiv 0 \ (4)$

$ac-bdm \equiv 0 \pmod 2$

$m \equiv 2$
$n \equiv 3 \equiv -1$ so $ac \equiv 0 \pmod 2$

$a^2-2b^2-c^2+2d^2 \equiv 0 \pmod 4$

so a and c have the same parity thus even and so $2b^2 \equiv 2d^2 \pmod 4$ so b, d same parity

so $$\alpha = \frac{a}{2} + \frac{c}{2}\sqrt{n} + \begin{cases} \frac{b}{2}\sqrt{m} + \frac{d}{2}\sqrt{mn} & b, d \text{ even} \\ \frac{b-1}{2}\sqrt{m} + \frac{d-1}{2}\sqrt{mn} + \frac{\sqrt{m}+\sqrt{mn}}{2} & b, d \text{ odd} \end{cases}$$

(b) as before
$$2a + 2b\sqrt{m} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$
$$2a + 2c\sqrt{m} \in \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$$
$$2a + 2d\sqrt{mn} \in \mathbb{Z}\left[\frac{1+\sqrt{mn}}{2}\right]$$

(i) so $\alpha \in \mathcal{O}_K$ of the form $\dfrac{a+b\sqrt{m}+c\sqrt{n}+d\sqrt{mn}}{4}$ $a, b, c, d \in \mathbb{Z}$

with $\dfrac{a+b\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$
$$\parallel$$
$$p + q\frac{1+\sqrt{m}}{2} = \frac{2p+q+q\sqrt{m}}{2}$$

so a & b same parity.

Similarly a, b, c, d same parity.

(ii) $$\beta = \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{mn}}{4}$$

$$(4\beta - 1 - \sqrt{m})^2 = n(1+\sqrt{m})^2 = n(1+2\sqrt{m}+m)$$
$$(4\beta-1)^2 - 2(4\beta-1)\sqrt{m} + m$$

$$(4\beta-1)^2 + m - n(m+1) = (2(4\beta-1)+2n)\sqrt{m}$$

so β has min poly
$$\left((4X-1)^2 + m - n(m+1)\right)^2 = m\left(2(4X-1)+2n\right)^2$$
need this monic poly (after dividing by 16) to be in $\mathbb{Z}[X]$.

So work mod 16 and show get 0.

$$(4X-1)^2 \equiv -8X+1$$

so check $\left(-8X+1+m-n(m+1)\right)^2 \equiv m\left(8X-2+2n\right)^2$

$$\left(-8X+\underbrace{(m+1)(1-n)}_{\text{divisible by }4}\right)^2 \qquad m\left(8X+\underbrace{2(n-1)}_{\text{divisible by }4}\right)^2$$

so mod 16 get $4^2 \equiv 4^2$

$0 \equiv 0$

Thus $\beta \in \mathcal{O}_K$.

(c) $\alpha - d\cdot\beta = \dfrac{a-d+(b-d)\sqrt{m}+(c-d)\sqrt{n}}{4} = \dfrac{r+s\sqrt{m}+t\sqrt{n}}{2}$

$r = \frac{a-d}{2}$ $\quad s = \frac{b-d}{2}$ $\quad t = \frac{c-d}{2} \in \mathbb{Z}$

$\alpha - d\cdot\beta - s\left(\frac{1+\sqrt{m}}{2}\right) - t\left(\frac{1+\sqrt{n}}{2}\right) = \frac{r-s-t}{2} \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$

so $r+s+t$ is even

so $\alpha = d\cdot\dfrac{1+\sqrt{m}+\sqrt{n}+\sqrt{mn}}{4} + s\,\dfrac{1+\sqrt{m}}{2} + t\,\dfrac{1+\sqrt{n}}{2} + \underbrace{\dfrac{r-s-t}{2}}_{\in\mathbb{Z}}$

qed.

(3). embeddings given by $\sqrt[3]{m} \mapsto \sqrt[3]{m},\ \zeta\sqrt[3]{m},\ \zeta^2\sqrt[3]{m}$

(a) so $\mathrm{Tr}\left(a+b\sqrt[3]{m}+c\sqrt[3]{m^2}\right) = 3a$

N as in the formula (I used SAGE, see site)

(b) $\delta = \dfrac{1+\sqrt[3]{m}+\sqrt[3]{m^2}}{3}$ $\qquad (3\delta-1)^3 = m(1+\sqrt[3]{m})^3$

$$= m\left(1+3\sqrt[3]{m}+3\sqrt[3]{m^2}+m\right)$$

$$= m\Big(m+1+3\big(\underbrace{\sqrt[3]{m}+\sqrt[3]{m^2}}_{3\delta-1}\big)\Big)$$

so $(3\delta-1)^3 = m(m+1)+3m(3\delta-1)$

$$27\delta^3-27\delta^2+9\delta-1 = m^2-2m+9m\delta$$

$$\delta^3-\delta^2+\delta\left(\frac{1-m}{3}\right)-\frac{(m-1)^2}{27}=0$$

$9 \mid m-1$ so this min poly $\in \mathbb{Z}[x]$.

(c) $\alpha = a+b\sqrt[3]{m}+c\sqrt[3]{m^2} \in \mathcal{O}_K$

$Tr_{K/\mathbb{Q}}(\alpha) = 3a \in \mathbb{Z}$

$Tr_{K/\mathbb{Q}}(\alpha\sqrt[3]{m}) = 3mc \in \mathbb{Z}$

$Tr(\alpha\sqrt[3]{m^2}) = 3mb) \in \mathbb{Z}$

so $\alpha = \dfrac{am+b\sqrt[3]{m}+c\sqrt[3]{m^2}}{3m}$ $\quad a,b,c\in\mathbb{Z}$

$$N_{K/\mathbb{Q}}(\alpha) = \frac{a^3m^3+b^3m+c^3m^2-3abcm^2}{27m^3} \in \mathbb{Z}$$

so $a^3m^2+b^3+c^3m-3abcm \in 27m^2\mathbb{Z}$

so $m \mid b^3$. m is sq free so $m \mid b$

and if $b = m\cdot b'$ get

$a^3m+b'^3m^2+c^3-3ab'cm \in 27m\mathbb{Z}$

so $m \mid c^3 \Rightarrow m \mid c$

so $\alpha = \dfrac{r + s\sqrt[3]{m} + t\sqrt[3]{m^2}}{3}$ $\quad r, s, t \in \mathbb{Z}$

(d) $\alpha - t\delta = \dfrac{r - t \;\; + (s-t)\sqrt[3]{m}}{3}$

min poly of $X = \dfrac{u + v\sqrt[3]{m}}{3}$ is

$$(3X - u)^3 = v^3 m$$

so $27X^3 - 27X^2u + 9Xu^2 - u^3 - v^3 m = 0$

$\in 27\mathbb{Z}[X] \iff 3 \mid u^2$ so $3 \mid u$

and $27 \mid u^3 + v^3 m$ so $27 \mid v^3 m$

$3 \mid u \Rightarrow 27 \mid u^3$

$3 \nmid m$ so $3 \mid v$

Thus $\alpha - t\delta \in O_K \Rightarrow \alpha - t\delta \in \mathbb{Z}[\sqrt[3]{m}]$

and so $\alpha \in \mathbb{Z}[\sqrt[3]{m}, \delta]$ as desired

(4). disc $f = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$

(a) $f' = nX^{n-1} + p$ $\quad f'(\alpha_i) = n\alpha_i^{n-1} + p$

$\alpha_i^n + p\alpha_i + q = 0$ so $\alpha_i^{n-1} = -p - \dfrac{q}{\alpha_i}$

so disc $f = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \left(\underbrace{n\left(-p - \frac{q}{\alpha_i}\right)} + p \right)$

$= (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \dfrac{p(n-1)}{\alpha_i} \left(-\dfrac{nq}{p(n-1)} - \alpha_i \right)$

$\prod \alpha_i = (-1)^n q$ so

$$\operatorname{disc}(f) = (-1)^{\binom{n}{2}+n} \frac{p^n (n-1)^n}{q} f\left(-\frac{nq}{p(n-1)}\right)$$

$$= (-1)^{\binom{n}{2}+n} \frac{p^n (n-1)^n}{q}\left(\left(-\frac{nq}{p(n-1)}\right)^n + \underbrace{\cancel{p}\left(-\frac{nq}{\cancel{p}(n-1)}\right)+q}_{-\frac{q}{n-1}}\right)$$

$$= (-1)^{\binom{n}{2}} \frac{p^n (n-1)^n}{q}\,\frac{n^n q^n}{p^n (n-1)^n} - (-1)^{\binom{n}{2}+n} \frac{p^n (n-1)^n}{q}\,\frac{q}{n-1}$$

$$= (-1)^{\binom{n}{2}} n^n q^{n-1} + (-1)^{\binom{n-1}{2}} (n-1)^{n-1} p^n$$

(b) $$\operatorname{Tr}_{K/\mathbb{Q}}(\zeta_p^i) = \sum_{j=1}^{p-1} (\zeta_p^j)^i = -1 + \sum_{j=0}^{p-1} (\zeta_p^i)^j$$

$$= \begin{cases} -1 + \dfrac{(\zeta_p^i)^p - 1}{\zeta_p^i - 1} = 0 & i \neq 0 \\ p-1 & i = 0 \end{cases}$$

so $$\operatorname{disc}(K) = \det\left(\left(\zeta_p^i, \zeta_p^j\right)\right)_{i,j=0\ldots p-2} = \det\left(\operatorname{Tr}(\zeta_p^{i+j})\right)$$

$$= \underbrace{\begin{vmatrix} p-1 & -1 & -1 & \cdots & -1 \\ -1 & -1 & -1 & \cdots & -1 \\ -1 & & & & p-1 \\ -1 & & -1 & ⋰ & \\ \vdots & & ⋰ & -1 & \\ -1 & -1 & p-1 & & \end{vmatrix}}_{(p-2)\times(p-2)} = \begin{vmatrix} p-1 & -1 & -1 & \cdots & -1 \\ -p & 0 & 0 & \cdots & 0 \\ -p & & 0 & \cdots & p \\ -p & & 0 & ⋰ & \\ \vdots & & ⋰ & 0 & \\ -p & 0 & p & & \end{vmatrix}$$

$$= p \begin{vmatrix} -1 & \cdots & -1 \\ 0 & & p \\ \vdots & \iddots & \\ 0 & p & \end{vmatrix} = p \begin{vmatrix} -1 & 0 & \cdots & 0 \\ 0 & 0 & & p \\ \vdots & & \iddots & 0 \\ 0 & p & & \end{vmatrix}$$

$$= -p \underbrace{\begin{vmatrix} & & p \\ & \iddots & \\ p & & \end{vmatrix}}_{\text{reshuffle}} = -p \cdot (-1)^{\binom{p-3}{2}} \underbrace{\begin{vmatrix} p & & \\ & \ddots & \\ & & p \end{vmatrix}}_{(p-3)\times(p-3)}$$

$$= (-1)^{\binom{p-3}{2}+1} p^{p-2}$$

$$\binom{p-3}{2} + 1 = \frac{(p-3)(p-4)}{2} + 1 \equiv \frac{p-1}{2} \mod 2$$

clear $p > 2$

$$\sqrt{\operatorname{disc}(K)} = \prod_{i<j} (\alpha_i - \alpha_j) \in K \quad \text{always}$$

so $\sqrt{(-1)^{\frac{p-1}{2}} p^{p-2}} \in K$

$$\|$$

$$p^{\frac{p-3}{2}} \sqrt{(-1)^{\frac{p-1}{2}} p} \in K$$

q.e.d.