HW 3

(1) (a) $\alpha \in \mathcal{O}_L$ integral $\Rightarrow$

$\sigma(\alpha)$ integral $\forall \sigma : L \hookrightarrow \mathbb{C}$ (same min poly)

$\sigma(P(x)) = P(\sigma(x))$ for $P \in \mathbb{Z}[x]$.

so min poly $\alpha / K = \prod_{\substack{\sigma: L \hookrightarrow \bar{K} \\ \sigma|_K = id}} (x - \sigma(\alpha))$

has coefficients in $\mathcal{O}_L \cap K = \mathcal{O}_K$.

(b) $\left(\mathfrak{p}, [\mathcal{O}_L : \mathcal{O}_K[\alpha]]\right) = 1$

$\Rightarrow \mathfrak{p}\mathcal{O}_L + \underbrace{[\mathcal{O}_L : \mathcal{O}_K[\alpha]]\mathcal{O}_L}_{\subset \mathcal{O}_K[\alpha]} = \mathcal{O}_L$.

so $\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L + \mathcal{O}_K[\alpha]$

$\mathfrak{p}\mathcal{O}_L \subset q_i$ so $\mathcal{O}_L = \mathcal{O}_K[\alpha] + q_i$

(c) say $P(x) \in \mathcal{O}_K[x]$ $P(x) \bmod \mathfrak{p} \in (\bar{g}_i(x))$

$\Rightarrow P(x) \in \mathfrak{p}\mathcal{O}_K[x] + g_i(x) \in (\mathfrak{p}, q_i)$

so injective. Surjective clear as $\mathcal{O}_K[x] \twoheadrightarrow k_{\mathfrak{p}}[x]$

(d) $\mathcal{O}_K[x] \xrightarrow{i} \mathcal{O}_K[\alpha] \xrightarrow{j} \mathcal{O}_K[\alpha] / \mathcal{O}_K[\alpha] \cap q_i$

$(x \longmapsto \alpha)$

$\cong (\mathcal{O}_K[\alpha] + q_i) / q_i$

$\cong \mathcal{O}_L / q_i$

for $j = q_i$ clearly so only need

$$i^{-1}(q_i) = (p, g_i(x))$$

ie $P(x) \in \mathcal{O}_K[x]$ $\quad P(\alpha) \in (p, g_i(\alpha))$

$$\iff P(x) \in (p, g_i(x))$$

which is clear

(e) $\mathcal{O}_L/q_i \hookleftarrow \mathcal{O}_K[x]/(p, g_i(x)) \cong \dfrac{k_p[x]}{(\bar{g}_i(x))}$

$\bar{g}_i$ irreducible so $(\bar{g}_i(x))$ prime ideal in $k_p[x]$

in fact maximal ideal

so $\mathcal{O}_L/q_i \hookleftarrow$ field

so $\mathcal{O}_L/q_i$ is either a field or 0

if q_i prime ideal then $\mathcal{O}_L/q_i \cong k_p[x]/\bar{g}_i(x)$ so $\dim_{\mathbb{F}_p}(\mathcal{O}_L/q_i) = \dim_{\mathbb{F}_p}^{k_p/\bar{q}_i} = \deg \bar{g}_i$

(f) $\bar{g}_i \bar{u} + \bar{g}_j \bar{v} = 1$ in $k_p[x]$

so $g_i u + g_j v = 1 + p[x]$ for some lifts u, v

so $1 \in p[x] + g_i(x) u(x) + g_j(x) v(x)$

$= (p, g_i(x)) + (p, g_j(x))$

$1 = q_i + q_j$

(g) $g_i(x) \in p[\alpha] + \bar{g}_i(\alpha)$ as cosets

so $\prod g_i(x)^{e_i} \in p[\alpha] + \prod \bar{g}_i(\alpha)^{e_i} = p[\alpha] + \bar{f}(\alpha)$

$= p[\alpha]$.

so $\prod g_i(\alpha)^{e_i} \mathcal{O}_L \subset_{\mathfrak{P}} \mathcal{O}_L$ as $\prod g_i(\alpha)^{e_i} \in \mathfrak{P}$

$$\prod q_i^{e_i} = \prod (\mathfrak{P}, g_i(\alpha))^{e_i} \subset \left(\mathfrak{P}, \prod g_i(\alpha)^{e_i}\right). \subset \mathfrak{P}\mathcal{O}_L$$

$$\Rightarrow \mathfrak{P}Q \mid \mathfrak{P}\mathcal{O}_L + \prod g_i(\alpha)^{e_i}\mathcal{O}_L \mid \prod q_i^{e_i}$$

$$\Rightarrow \mathfrak{P}\mathcal{O}_L \mid \prod q_i^{e_i}$$

(b) say $q_1 \cdots q_s$ prime ideals

$q_{s+1} \cdots = \mathcal{O}_L$

$$\Rightarrow \mathfrak{P}\mathcal{O}_L = \prod_{i=1}^{s} q_i^{d_i} \mid \prod q_i^{e_i}$$

$$\Rightarrow d_i \le e_i \quad 1 \le i \le s$$

but $\sum_{i=1}^{s} d_i f_{q_i/\mathfrak{P}} = [L:K]$ (from claim)

$\wedge$

$d_i \le e_i$! $\forall i$

$\sum_{\text{all } i} e_i f_{q_i/\mathfrak{P}} = \sum e_i \cdot \deg \bar{g}_i(x) = \deg \bar{f} = [L:K]$

$\Rightarrow d_i = e_i \ \forall i$ and all q_i are prime ideals

Thus $\mathfrak{P}\mathcal{O}_L = \prod q_i^{e_i}$

$e_i =$ exponent of $\bar{g}_i$ in $\bar{f}$

$f_{q_i/\mathfrak{P}} = \deg \bar{g}_i$

D.

(2) (a) $d = [\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]] = \begin{cases} 1 & m \not\equiv 1 \ (4) \\ 2 & m \equiv 1 \ (4) \end{cases}$

$p \mid m$ odd $\Rightarrow p \nmid d$

$p \mid m$ $p = 2$ can only happen if $m \equiv 2 \ (4)$ in which case $d = 1$

so $p \nmid d$ and $p\mathcal{O}_K = (p, \sqrt{m})^2$

as $X^2 - m \equiv X^2 \pmod{p}$ Use Pr 1

(b) $m \equiv 3 \ (4)$ $d = 1$ so apply Pr 1

$X^2 - m \equiv X^2 - 1 \mod 2 \equiv (X+1)^2 \pmod 2$

so $2\mathcal{O}_K = \left(2, 1+\sqrt{m}\right)^2$

$m \equiv 1 \ (4)$ $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ $\alpha = \frac{1+\sqrt{m}}{2}$ min poly

$P(X) = X^2 - X - \frac{m-1}{4}$

if $m \equiv 1 \ (8)$

$m \equiv 5 \ (8)$

then $P(X) \equiv X^2 - X \pmod 2$

$P(X) \equiv X^2 - X - 1 \pmod 2$ irreducible

so $m \equiv 1 \ (8)$ $2\mathcal{O}_K = (2, \alpha)(2, \alpha - 1)$

$= \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$

if $m \equiv 5 \ (8)$ $2\mathcal{O}_K = (2)$.

(c) $p \nmid 2m \Rightarrow p \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]]$

so follows immediately from Problem 1.

(3) (a) $f(x) = \dfrac{x^p - 1}{x-1} \equiv \dfrac{(x-1)^p}{x-1} \equiv (x-1)^{p-1} \pmod p$

$N_{K/\mathbb{Q}}(1-\zeta_p) = p$ so $1-\zeta_p \mid p$ so by Problem 1

$$p\mathcal{O}_K = (p, 1-\zeta_p)^{p-1} = (1-\zeta_p)^{p-1}$$

$e \cdot f \cdot r = p-1 \qquad e = p-1$ so $f = 1$

(b) so $K/\mathbb{Q}$ is totally tamely ramified at p.

$$\mathbb{F}_p^{\times} = g^{\mathbb{Z}/(p-1)\mathbb{Z}} \qquad 1 = g^a$$

$$1^r = g^{a \cdot r} = 1 \iff a \cdot r = p-1$$

(c) $f(x)$ splits completely in $\mathbb{F}_{q^s}[x]$

$\iff$ primitive p^{th} roots of 1 are in $\mathbb{F}_{q^s}^{\times} \cong \mathbb{Z}/(q^s-1)\mathbb{Z}$

$\iff \exists\, \alpha \in \mathbb{Z}/(q^s-1)\mathbb{Z}$ of order p

$\iff p \mid q^s - 1$ (by Cauchy)

$\iff s \geq r$.

(d) Suppose $\bar{f}(x) \bmod q = \prod g_i(x)$

(already know q unramified in k $\quad q \neq p$

so all exponents are 1 as $\mathcal{O}_k = \mathbb{Z}[\zeta_p]$)

$\bar{g}_i(x)$ splits completely over $\mathbb{F}_q[x]/(\bar{g}_i(x))$

$\cong \mathbb{F}_{q^{\deg \bar{g}_i(x)}}$ and

so $\deg \bar{g}_i(x) \geq r$.

Reciprocally, if $f(x) = \prod (x - \alpha_i)$ $\alpha_i \in \mathbb{F}_{q^r}$ in $\mathbb{F}_{q^r}[x]$

then $f(x) = \prod \bar{g}_i(x)$ in $\mathbb{F}_q[x]$

where $\bar{g}_i(x)$ = min poly of α_i / $\mathbb{F}_q$ of degree r.

Thus $f \bmod q = \prod \bar{g}_i(x)$ $\quad \deg \bar{g}_i = r$

and so $q\,\mathcal{O}_K = \left(\prod_{i=1}^{\frac{p-1}{r}} q_i\right)$ $\quad f_{q_i/q} = r$

(5) (a) $\iff \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{15})} = \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}$

$\hookrightarrow \mathcal{D}^{-1}$

know $\mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})} = \mathbb{Z} + \mathbb{Z}\sqrt{3} + \mathbb{Z}\frac{1+\sqrt{5}}{2} + \mathbb{Z}\frac{3+\sqrt{15}}{2}$

so need to show that

$\mathcal{D}^{-1} = \{\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})} \mid \mathrm{Tr}_{\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}(\sqrt{15})}(\alpha \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}) \subset \mathcal{O}_{\mathbb{Q}(\sqrt{15})}\}$

$= \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}$

say $\alpha = a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \in \underbrace{\mathbb{Q}(\sqrt{3},\sqrt{5})}_{L}$ $\quad K = \mathbb{Q}(\sqrt{15})$

$Tr = Tr_{L/K}$

$Tr(\alpha) = 2a + 2d\sqrt{15}$

$Tr(\alpha\sqrt{3}) = 6b + 2c\sqrt{15}$

$Tr(\alpha\sqrt{5}) = 10c + 2b\sqrt{15}$

$Tr(\alpha\sqrt{15}) = 30d + 2a\sqrt{15}$

$\alpha \in \mathbb{Q}^\vee \iff Tr\left(\alpha \cdot \begin{matrix} 1 \\ \sqrt{3} \\ \frac{1+\sqrt{5}}{2} \\ \frac{\sqrt{3}+\sqrt{15}}{2} \end{matrix}\right) \in \mathcal{O}_{\mathbb{Q}(\sqrt{15})} = \mathbb{Z}[\sqrt{15}]$

$Tr(\alpha) = 2a + 2d\sqrt{15} \rightarrow 2a, 2d \in \mathbb{Z}$

$Tr(\alpha\sqrt{3}) = 6b + 2c\sqrt{15} \Rightarrow 6b, 2c \in \mathbb{Z}$

$Tr\left(\alpha\,\frac{1+\sqrt{5}}{2}\right) = Tr\left(\frac{\alpha}{2}\right) + Tr\left(\frac{\alpha\sqrt{5}}{2}\right) = a + d\sqrt{15} + 5c + b\sqrt{15}$ $\Rightarrow$ $a+5c,\ b+d \in \mathbb{Z}$

$Tr\left(\alpha\,\frac{\sqrt{3}+\sqrt{15}}{2}\right) = Tr\left(\frac{\alpha\sqrt{3}}{2}\right) + Tr\left(\frac{\alpha\sqrt{15}}{2}\right) = 3b + c\sqrt{15} + 15d + a\sqrt{15}$ $\Rightarrow$ $3b+15d \in \mathbb{Z}$, $a+c \in \mathbb{Z}$

So $a = \frac{A}{2}$ $\quad c = \frac{C}{2}$ $\quad d = \frac{D}{2}$ $\quad A, C, D \in \mathbb{Z}$.

$A + C$ even

$B + D$ even

$b = b + d - d \in \frac{1}{2}\mathbb{Z}$

$b = \frac{B}{2}$ $\quad B \in \mathbb{Z}$

so A, C even or A, C odd
B, D even or B, D odd

$$\frac{A + C\sqrt{5}}{2} = \begin{cases} \frac{A-1}{2} + \frac{C-1}{2}\sqrt{5} + \frac{1+\sqrt{5}}{2} & A, C \text{ odd} \\ \frac{A}{2} + \frac{C}{2}\sqrt{15} & A, C \text{ even} \end{cases}$$

$$\frac{B\sqrt{3}+D\sqrt{15}}{2} = \begin{cases} \frac{B}{2}\sqrt{3}+\frac{D}{2}\sqrt{15} & B,D \text{ even} \\ \frac{B-1}{2}\sqrt{3}+\frac{D-1}{2}\sqrt{15}+\frac{\sqrt{3}+\sqrt{15}}{2} & B,D \text{ odd} \end{cases}$$

thus $\alpha \in \mathbb{Z}\left[1, \sqrt{3}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{3}+\sqrt{15}}{2}\right] = \mathcal{O}_{\mathbb{Q}(\sqrt{3},\sqrt{5})}$

so $\mathcal{D}^{\vee}_{L/K} = \mathcal{O}_L \Rightarrow \mathcal{D}_{L/K} = \mathcal{O}_L$.

(7) (a). any $\alpha \in \mathcal{O}_L$ of the form

$$\alpha = \sum a_I \prod \alpha_i^{e_i}$$

so $V_m = \{ g \in G_{L/K} \mid g(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{m+1}} \ \forall \alpha \}$

$$\Leftrightarrow \quad g(\alpha_i) \equiv \alpha_i \pmod{\mathfrak{q}^{m+1}} \ \forall \ i$$

reciprocally $g(\sum a_I \prod \alpha_i^{e_i})$

$$= \sum a_I \prod g(\alpha_i)^{e_i} \equiv \sum a_I \prod \alpha_i^{e_i} \pmod{\mathfrak{q}^{m+1}}$$

(b) (i) $K = \mathbb{Q}(\sqrt{2+\sqrt{3}})$ splitting field of $(X^2-2)^2-3$

with roots $\pm\sqrt{2\pm\sqrt{3}}$

$\sqrt{2-\sqrt{3}} = \frac{1}{\sqrt{2+\sqrt{3}}}$ no roots $\pm\alpha, \pm\alpha^{-1}$

so $\alpha \in \mathcal{O}_K^{\times}$

(ii) $\sigma(\alpha) = \alpha^{-1}$ gives autom $\sigma(\pm\alpha^{\pm 1}) = \pm\alpha^{\mp 1}$

$\tau(\alpha) = -\alpha$ gives autom $\sigma(\pm\alpha^{\pm 1}) = \mp\alpha^{\pm 1}$

and any auton takes α to $\pm\alpha^{\pm 1}$

$\alpha \mapsto \alpha$ id

$\alpha \mapsto \alpha^{-1}$ σ

$\alpha \mapsto -\alpha$ τ

$\alpha \mapsto -\alpha^{-1}$ $\sigma\tau$

so $Gal(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$

(iii) by Problem 1 as $\mathcal{O}_K = \mathbb{Z}[\alpha]$

need to factor $(x^2-2)^2 - 3 \mod 3$

$= (x^2-2)^2 \pmod 3$

and x^2-2 is irreducible

so $(3) = \left(3, \left(\sqrt{2+\sqrt{3}}\right)^2 - 2\right)^2 = (3, \sqrt{3})^2$

$= (\sqrt{3})^2$

$1(\alpha) - \alpha = 0$

$\sigma(\alpha) - \alpha = \alpha^{-1} - \alpha = \frac{1-\alpha^2}{\alpha} = \frac{1-(2+\sqrt{3})}{\alpha}$

$= (\sqrt{3}-1) \cdot \alpha^{-1}$

$\tau(\alpha) - \alpha = -\alpha - \alpha = -2\alpha$

$\sigma\tau(\alpha) - \alpha = -\frac{1}{\alpha} - \alpha = -\frac{1+\alpha^2}{\alpha} = -(3+\sqrt{3})\alpha^{-1}$

$= -\sqrt{3}(\sqrt{3}+1)\alpha^{-1}$

so $(\sqrt{3})^n \mid 1(\alpha) - \alpha \quad \forall n$

$\sqrt{3} \nmid (\sqrt{3}-1)\alpha^{-1}$

$\sqrt{3} \nmid -2\alpha$

$\sqrt{3} \mid -\sqrt{3}(\sqrt{3}+1)\alpha^{-1}$

$\sqrt{3}^2 \nmid$

so $I_{\sqrt{3}/3} = \{1, \sigma\tau\}$

$P_{\sqrt{3}/3} = \{1\}$

(iv) factor $(x^2-2)^2 - 3 \mod 2$

$$x^4 - 1 = -(x+1)^4 \pmod 2$$

so $2\mathcal{O}_K = \left(2, \sqrt{2+\sqrt{3}}+1\right)^4 = \mathfrak{q}^4$

$= (2, \alpha+1)^4$

again compute $\sigma(\alpha) - \alpha = (\sqrt{3}-1)\alpha^{-1}$

$\tau(\alpha) - \alpha = -2\alpha$

$\sigma\tau(\alpha) - \alpha = -\sqrt{3}(\sqrt{3}-1)\alpha^{-1}$

so $v_{\mathfrak{q}}(\tau(\alpha)-\alpha) = v_{\mathfrak{q}}(\mathfrak{q}^4) = 4.$

and $v_{\mathfrak{q}}(\sigma(\alpha)-\alpha) = v_{\mathfrak{q}}(\sigma\tau(\alpha)-\alpha)$

as $\mathfrak{q} + \sqrt{3}.$

and $v_{\mathfrak{q}}(\sigma(\alpha)-\alpha) = v_{\mathfrak{q}}(\sqrt{3}-1)$

$(\sqrt{3}-1)(\sqrt{3}+1) = 2$ and $\sigma((\sqrt{3}+1)) = (\sqrt{3}-1)$ as ideals

so $v_{\mathfrak{q}}(\sqrt{3}-1) = \frac{v_{\mathfrak{q}}(2)}{2} = 2$

So $I_{\mathfrak{q}/2} = \{1, \sigma, \tau, \sigma\tau$ and $v_{\mathfrak{q}}(g(\alpha)-\alpha) \geq 1\}$

$P_{\mathfrak{q}/2}$ $v_{\mathfrak{q}}(\ ) \geq 2\}$

$$V_2 = V_3 = \{ g \in G_{LK} \mid v_q(g(\alpha) - \alpha) \geq 4 \}$$

$$= \{1, \sigma\tau\}$$

$$V_m = \{1\} \qquad m > 3.$$