(1) (a) $Cl(K)$ finite say order n

so $I^n = 1$ in $Cl(K)$

so $I^n = (a)$ principal.

what is $I\mathcal{O}_L$ where $L = K(\sqrt[n]{a})$?

$(I\mathcal{O}_L)^n = I^n \mathcal{O}_L = (a) = (\sqrt[n]{a})^n$

so by unique factorization of ideals

$\Rightarrow \quad I\mathcal{O}_L = (\sqrt[n]{a})$

(b) let $I_1 \cdots I_k$ be ideals representing the elements of $Cl(K)$.

L_i = ext of K st $I_i \mathcal{O}_{L_i}$ = principal works

then L = compositum of $L_1 \cdots L_k$

as $I_i \mathcal{O}_L = (I_i \mathcal{O}_{L_i})(\mathcal{O}_L)$ is principal $\forall i$

(2) (a) f reducible / $\mathbb{Q} \Leftrightarrow$ has rational root $\frac{p}{q}$

$p^3 - 3pq^2 + q^3 = 0 \quad \Rightarrow \quad p \mid q$ so $q \mid p$

only ± 1, but ± 1 not a root.

$f(\pm\infty) = \pm\infty$

$f(0) = 1$

$f(1) = -1$ ① so 3 real roots

already have $\mathcal{O}_K \subset \frac{1}{\operatorname{disc}(1,\alpha,\alpha^2)} \mathbb{Z}[\alpha]$ from class

so let's compute $\operatorname{disc}(1,\alpha,\alpha^2)$. if α,β,γ roots of f

then

$$\operatorname{disc}(1,\alpha,\alpha^2) = \det\left(\sigma(\alpha^i)\right)^2 = \begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix}^2$$

(σ: embedding)

$$= (\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2 = \text{disc of } f$$

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

so $\operatorname{disc}(f) = -3^3 + 2^2 \cdot 3^3 = 3^4$

so $\mathcal{O}_K \subset \frac{1}{3^4}\mathbb{Z}[\alpha]$

(b) $\alpha^3 - 3\alpha + 1 = 0$ so $\alpha^{-1} = 3 - \alpha^2 \in \mathcal{O}_K$.

$$f(X-2) = (X-2)^3 - 3(X-2) + 1$$
$$= X^3 - 6X^2 + 9X - 1 = g(X)$$

so $g(\alpha+2) = f(\alpha) = 0$

so $(\alpha+2)^3 - 6(\alpha+2)^2 + 9(\alpha+2) = 1$

so $(\alpha+2)^{-1} = (\alpha+2)^2 - 6(\alpha+2) + 9 \in \mathcal{O}_K$

$(\alpha+1)^3 = 3\alpha(\alpha+2) \Leftrightarrow \alpha^3 + 3\alpha^2 + 3\alpha + 1 = 3\alpha^2 + 6\alpha$

$\Leftrightarrow \alpha^3 + 1 = 3\alpha$ clear

so $(3)\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ $\quad \sum_{i=1}^{r} e_i f_i = 3$

but $\left((\alpha+1)^3\right) = \left(5\,\underbrace{\alpha(\alpha+1)}_{\text{units}}\right) = (3)$

so $(3)\mathcal{O}_K = (\alpha+1)^3 \mathcal{O}_K$ so $(\alpha+1)$ is prime

$r=1 \quad e=3 \quad f=1$

(c) let $\mathfrak{p} = (\alpha+1)$ so $(3) = \mathfrak{p}^3$

suffices to check $\mathcal{O}_K/(3)\mathcal{O}_K \cong \mathbb{Z}[\alpha]/(3)\mathbb{Z}[\alpha]$

$\mathcal{O}_K/(3)\mathcal{O}_K = \mathcal{O}_K/\mathfrak{p}^3\mathcal{O}_K$

and know from class $|\mathcal{O}_K/\mathfrak{p}^3\mathcal{O}_K| = |\mathcal{O}_K/\mathfrak{p}|^3$

$\mathcal{O}_K/\mathfrak{p} = k_{\mathfrak{p}}$ and $[k_{\mathfrak{p}} : \mathbb{F}_3] = f = 1$

so $|\mathcal{O}_K/\mathfrak{p}^3| = 3^3$

Also $\mathbb{Z}[\alpha]/(3)\mathcal{O}_K \cap \mathbb{Z}[\alpha] \leftarrow \mathbb{Z}[\alpha]/(3)\mathbb{Z}[\alpha]$

and the latter is $\cong \mathbb{Z}[x]/(3, x^3-3x+1)$

$\cong \mathbb{F}_3[x]/(x^3-3x+1)$

$\cong \mathbb{F}_3[x]/(x+1)^3 \cong \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3$

the two cardinalities are the same

$\mathcal{O}_K/(3) \hookleftarrow \mathbb{Z}[\alpha]/(3)\mathcal{O}_K \cap \mathbb{Z}[\alpha]$ is injective

so they are isomorphic. $\square$.

(d) let $\mathcal{O}_K = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$

and $e_i = \frac{f_i}{3^{n_i}} \in \frac{1}{3^4}\mathbb{Z}[\alpha]$ w/ n_1, n_2, n_3 minimal

ordered st $n_1 \geq n_2 \geq n_3$ and if $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$

then $n_1 > 0$.

But then

$e_1 \in \mathcal{O}_K = \mathbb{Z}[\alpha] + (3)\mathcal{O}_K$

so $\exists\ a, b, c \in \mathbb{Z}$ such that

$u \in \mathbb{Z}[\alpha]$

$$e_1 = u + 3 \cdot \left(\frac{a}{}e_1 + b e_2 + c e_3\right)$$

$$\frac{f_1}{3^{n_1}} = u + 3\left(\frac{a f_1}{3^{n_1}} + \frac{b f_2}{3^m} + \frac{c f_3}{3^{n_3}}\right)$$

so $\frac{f_1}{3} = 3^{n_1 - 1}u + a f_1 + b f_2 3^{n_1 - n_2} + c f_3 3^{n_1 - n_3}$

$\in \mathbb{Z}[\alpha]$

$(n_1 \geq 1)$

contradicting the minimality of n_1.

(Otherwise $e_1 = \frac{f_1}{3^{n_1}} = \frac{f_1'}{3^{n_1 - 1}}$ w/ $f_1' = \frac{f_1}{3} \in \mathbb{Z}[\alpha]$)

(e) $n = 3$ $r = 3$ (3 real roots) $s = 0$ $\operatorname{disc}(K) = \operatorname{disc}(1, \alpha, \alpha^2) = 3^4$

so Minkowski bound

$$\lambda = \frac{n!}{n^n}\left(\frac{\pi}{4}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

$$= \frac{3!}{3^3} \sqrt{3^4} = 2$$

Thus every $[I] \in Cl(K)$

contains some $I \in [I]$ st $\|I\| = 1$ or 2

$\|I\|=1 \Rightarrow I = \mathcal{O}_K$

$\|I\|=2 \Rightarrow I \mid (2)\mathcal{O}_K$.

$2 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ so

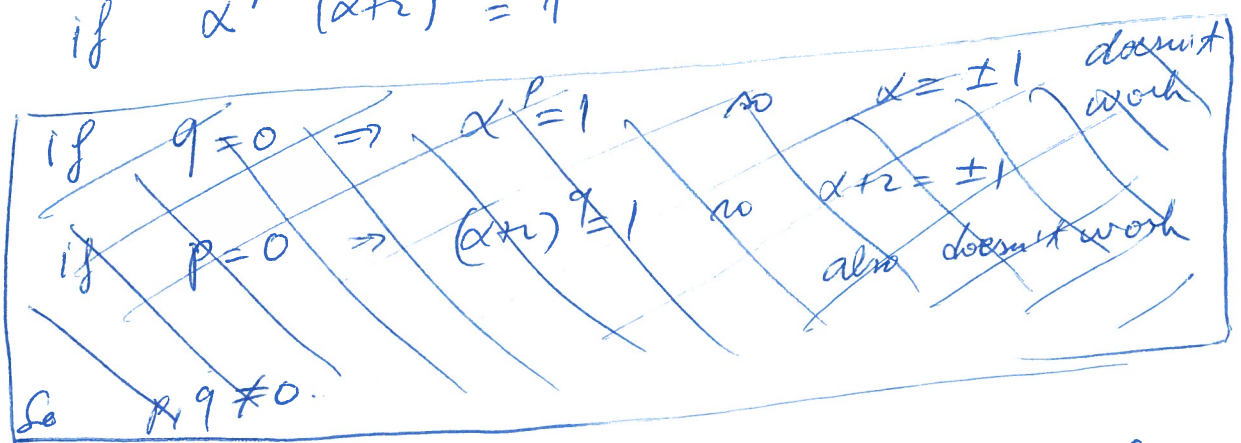
$f(x) \bmod 2 = X^3+X+1$ irreducible / $\mathbb{F}_2[X]$

implies $(2)\mathcal{O}_K$ is prime ideal so ~~[illegible]~~

$I = (2)\mathcal{O}_K$ is principal and so $Cl(K) = \{1\}$.

(f) ~~[illegible]~~ if $\zeta_n \in K \subset \mathbb{R}$ then $\zeta_n = \pm 1$

(g) if $\alpha^p (\alpha+2)^q = 1$ we need to show that $p=q=0$.



for any $\sigma : K \hookrightarrow \mathbb{C}$ get $\sigma(\alpha)^p (\sigma(\alpha)+2)^q = 1$

~~[illegible]~~

so deduce that $\alpha^p (\alpha+2)^q = 1$ (as $\alpha, \beta, \gamma \in \mathbb{R}$)

$\beta^p (\beta+2)^q = 1$

$\gamma^p (\gamma+2)^q = 1$

ordering $-2 < \alpha < -1 < 0 < \beta < 1 < \gamma < 2$ (easy to see)

it follows that

$\beta^p(\beta+1)^q = 1$ so if $p \geq 0$ then $q < 0$.

$0 < \beta < 1 \quad 2 < \beta$ can change signs to have this

$\gamma^p(\gamma+1)^q = 1$ so $\gamma^p = (\gamma+1)^{-q}$

so $p > -q$.

$\alpha^p(\alpha+1)^q = 1$

$-2 < \alpha < -1$ so $0 < \alpha+1 < 1$

$\alpha^{+p} = (\alpha+1)^{-q}$ $\qquad \alpha^p = \left(\frac{1}{\alpha+1}\right)^q > \left(\frac{1}{\alpha+1}\right)^{-p}$

so $\left(\alpha(\alpha+1)\right)^p > 1$. $\overset{p \geq 0}{\Longrightarrow}$

either $p = 0$ (can't be) or $|\alpha(\alpha+1)| > 1$.

but $\alpha(\alpha+1) = (\alpha+1)^2 - 1$

$-1 < \alpha+1 < 0$ so

$|\alpha(\alpha+1)| \in (0,1)$ Contradiction.

Finally $\frac{1}{\alpha+1} = (\alpha-1)^2$ so $\alpha+1$ and α cannot be a basis. Indeed if $\alpha - 1 = \alpha^p(\alpha+1)^q$ ($\alpha \in \mathcal{O}_K^\times$)

then $(\alpha-1)^{2q+1} = \alpha^p$. Again taking an automorphism we may assume α is any of the roots and taking $\alpha \in (0,1)$

would give $(\text{negative})^{\text{odd}} = \text{positive}$ contradiction.

(3) (a) $\operatorname{disc}(K) = \operatorname{disc} \mathbb{Z}[\sqrt[3]{7}] = \operatorname{disc}(1, \sqrt[3]{7}, \sqrt[3]{7^2})$

$= \operatorname{desc}$ minimal polynomial $x^3 - 7$

$= (-1)^{\binom{3}{2}} 3^3 (-7)^2 + (-1)^{\binom{2}{2}} 2^2 \cdot 0$

$= -3^3 \cdot 7^2$

$x^3 - 7 \bmod 3 \equiv (x-1)^3$ $\quad r=1, e=3, f=1$

so $(3)\mathcal{O}_K = (3, \sqrt[3]{7} - 1)^3$

totally ramified

$x^3 - 7 \bmod 7 \equiv x^3$ $\quad r=1, e=3, f=1$

$(7)\mathcal{O}_K = (7, \sqrt[3]{7})^3 = (\sqrt[3]{7})^3$

totally ramified

(b) seek primes p such that

$x^3 - 7 \bmod p$ factors as

(i) linear factors
(ii) linear × quadratic
(iii) irreducible

$\bmod 2 \equiv (x+1)(x^2+x+1)$

$\bmod 13$ irreducible as $x^3 - 7 \not\equiv 0 \pmod{13}$

To find example for (i) compute $\{n^3 - 7\}$

for $n = 1, 2, 3, \ldots, 20$, factor them

and pick p dividing three different $n^3 - 7$

and we quickly find 19 as p.

(c) Minkowski bound $r=1$, $s=1$

$$\frac{3!}{3^3}\frac{4}{\pi}\sqrt{3^3 7^2}$$

$$= \frac{56\sqrt{3}}{9\pi} \simeq 10.\ldots$$

so seek ideals $I \mid (p)\mathcal{O}_K$ $p = 2, 3, 5, 7$

and then every $[I] \in Cl_K$ will have representatives products of these prime ideals

$$(2)\mathcal{O}_K = \mathfrak{p}_2\mathfrak{q}_2 \qquad \mathfrak{p}_2 = (2, \sqrt[3]{7}+1) \quad \mathfrak{q}_2 = (2, \sqrt[3]{7}^2 + \sqrt[3]{7} + 1)$$

$$(3)\mathcal{O}_K = (3, \sqrt[3]{7})^3 = \mathfrak{p}_3^3$$

$$(5)\mathcal{O}_K = \mathfrak{p}_5\mathfrak{q}_5 \qquad \mathfrak{p}_5 = (5, 2+\sqrt[3]{7})$$

$$\mathfrak{q}_5 = (5, \sqrt[3]{7}^2 - 2\sqrt[3]{7} - 1)$$

$$(7)\mathcal{O}_K = \mathfrak{p}_7^3 = (\sqrt[3]{7})^3$$

In $Cl(K)$: $\mathfrak{p}_2\mathfrak{q}_2 = 1$

$\mathfrak{p}_3^3 = 1$ $\quad \mathfrak{p}_3 \neq 1$ as $\mathfrak{p}_3$ not principal

$\mathfrak{p}_5\mathfrak{q}_5 = 1$

$\mathfrak{p}_7 = 1$

so $Cl(K) = \langle \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5 \rangle$.

$\alpha = \sqrt[3]{7}$

$$\mathfrak{p}_2\mathfrak{p}_3 = (2, \alpha+1)(3, \alpha-1) = (6, 2\alpha+2, 3\alpha+3, \alpha^2-1)$$

$$= (6, 2\alpha-2, \alpha+5, \alpha^2-1) = (6, 2(\alpha-1), \alpha-1, \alpha^2-1)$$

$$= (6, \alpha-1)$$

but $N_{K/\mathbb{Q}}(\alpha-1) = 6$ so $\alpha - 1 \mid 6$

so $\mathfrak{p}_2\mathfrak{p}_3 = (\alpha-1) = 1$ in $Cl(K)$

Also

$$\mathfrak{p}_3 \cdot \mathfrak{p}_5 = (3, \alpha-1)(5, \alpha+2)$$

$$= (15, 5\alpha - 5, 3\alpha + 6, (\alpha-1)(\alpha+2))$$

$$= (15, 2\alpha - 11, 3\alpha + 6, (\alpha-1)(\alpha+2))$$

$$= (15, 2\alpha - 11, \alpha + 17, \text{—})$$

$$= (15, 2\alpha - 11, \alpha + 2, (\alpha-1)(\alpha+2))$$

$$= (15, \alpha + 2) \quad \Rightarrow \quad (\alpha+2) = 1 \text{ in } Cl(K)$$

$N_{K/\mathbb{Q}}(\alpha+2) = 15$ so

so $Cl(K) = \langle \mathfrak{p}_3 \rangle \cong \mathbb{Z}/3\mathbb{Z}$.

(d) $$\frac{1}{2 - \sqrt[3]{7}} = \frac{8 - 7}{2 - \sqrt[3]{7}} = 4 + 2\sqrt[3]{7} + \sqrt[3]{7}^2$$

(e) See end of solutions.

(4) (a) need to check that if $e_{\mathfrak{p}/p} > 1$ then $\mathfrak{p}^2$ is principal. But $(p)\mathcal{O}_K = \mathfrak{p}^2$ for every p which ramified in K.

(b) If $m \equiv 1, 2 \pmod 4$ then $\mathfrak{p} = (p, \sqrt{m})$ for every ramified prime if

$\mathfrak{p}_1 \cdots \mathfrak{p}_k$ is principal for $\mathfrak{p}_i \mid p_i$

then $\mathfrak{p}_1 \cdots \mathfrak{p}_k = (p_1 \cdots p_k, \sqrt{m}) = (n, \sqrt{m})$ is principal.

say $(n, \sqrt{m}) = (\alpha)$

$\Rightarrow \alpha \mid \sqrt{m}$ so $N_{K/\mathbb{Q}}(\alpha) \mid m$

if $N(\alpha) \neq m$ then $N(\alpha) < m$

so $\alpha = a + b\sqrt{m}$ $\quad N(\alpha) = a^2 + b^2 m$

$\Rightarrow b = 0$. But no integer divides $\sqrt{m}$

so $(n, \sqrt{m}) = (\sqrt{m}) \rightarrow \sqrt{m} \mid n$

so $m \mid n$ as n is square free.

Thus only $\mathfrak{p}_1 \cdots \mathfrak{p}_k = \prod_{\mathfrak{p} \mid p} \mathfrak{p} \in \ker \phi$.

If $m \equiv 3 \ (4)$ then

$$\left.\begin{aligned} p\mathcal{O}_K &= (p, \sqrt{m})^2 \quad p \mid m \\ 2\mathcal{O}_K &= (2, 1+\sqrt{m})^2 \end{aligned}\right\} \text{ all ramify.}$$

as before $(n, \sqrt{m})$ is not principal unless $m \mid n$

Suppose $n \mid m$ $n \neq m$. n odd. Can $(2, 1+\sqrt{m})(n, \sqrt{m})$ be principal?

$$(2, 1+\sqrt{m})(n, \sqrt{m}) = (2n, n + n\sqrt{m}, 2\sqrt{m}, m + \sqrt{m})$$

$$= (2n, n+\sqrt{m}, 2\sqrt{m}, m - \sqrt{m})$$

$m = m'n$, n odd $\qquad \frac{m+n}{2n} = \frac{m'+1}{2} n \in \mathbb{Z}$.

so

$$= (2n, n+\sqrt{m}, 2\sqrt{m}) = (2n, n+\sqrt{m})$$
$$= (2\sqrt{m}, n+\sqrt{m})$$

If $(2\sqrt{m}, n+\sqrt{m}) = (\alpha)$

$\Rightarrow \alpha \mid 2\sqrt{m}$ and so $\alpha \notin \mathbb{Z}$

$\alpha = a+b\sqrt{m} \qquad b \neq 0$

so $a^2+b^2|m| \mid 4|m| \Rightarrow |b| \leq 2$

so $b = \pm 1$ or ± 2

if ± 2 then $\alpha = \pm 2\sqrt{m}$

but $2\sqrt{m} \nmid n+\sqrt{m}$ ($2\sqrt{m}(x+y\sqrt{m})$ $= 2ym + 2x\sqrt{m} \neq n+\sqrt{m}$)

so $b = \pm 1$ and

$$a^2+|m| = \frac{4|m|}{k} \qquad k = 1, 2, 3, 4.$$

ie $$a^2+|m| = \begin{cases} 4|m| \\ 2|m| \\ \frac{4|m|}{3} \\ |m| \end{cases}$$

so $$a^2 = \begin{cases} 3|m| & \leftarrow \text{only if } m \equiv -3 \not\equiv 3 \pmod 4 \text{ so never} \\ |m| & \leftarrow \text{never} \\ |m|/3 & \leftarrow \text{only if } m \equiv -3 \not\equiv 3 \pmod 4 \\ 0 \end{cases}$$

so α can only be $\pm\sqrt{m}$ but $\pm\sqrt{m} \nmid n+\sqrt{m}$

if $n \neq m$.

Therefore $\ker \Phi = \bigoplus_{\substack{p/p \\ p \mid m}} P$.

(c) If $I \in Cl(K)[2]$

$I = \prod q_i^{a_i}$ such that $q_i \mid p_i$

then $[I]$ contains a representative where

the q_i that appear are

- $q_i \mid p_i$ ramified and $a_i = 1$
- $p_i = q_i \bar{q}_i$ and only one of q_i and $\bar{q}_i$ appears.

Indeed, if p_i is unramified then q_i is principal and if $p_i = q_i \bar{q}_i$ and q_i and $\bar{q}_i$ both appear then $q_i^a \bar{q}_i^{-b} \overset{\text{say } a \geq b}{=\!=} (p_i)^b q_i^{a-b} = q_i^{a-b}$ in $Cl(K)$.

So $I = \prod_{P/p \text{ ramified}} P^{0 \text{ or } 1} \cdot \prod_{p_i = q_i \bar{q}_i} q_i^{a_i}$

if $I^2 = \prod_{p_i = q_i \bar{q}_i} q_i^{2a_i}$ is principal $= (\alpha)$

then $|N_{K/\mathbb{Q}}(\alpha)| = \|(\alpha)\| = \prod \|q_i\|^{2a_i}$

but $\|q_i\| = p_i^{f q_i/p_i} = p_i$ $\left(\sum_{i=1}^{2} ef = 2 \text{ so } e=f=1 \right)$

so $\|(\alpha)\| = \prod p_i^{2a_i} = \|(\prod p_i^{a_i})\|$

so $\left\| \left(\alpha / \prod p_i^{a_i} \right) \right\| = 1 \rightarrow (\alpha) = \left(\prod p_i^{a_i} \right)$

then

$$\prod q_i^{2a_i} = \prod (p_i)^{a_i} = \prod q_i^{a_i} \bar{q}_i^{a_i}$$

contradicting unique factorization unless $a_i = 0$.

so $I = \prod_{q_i / \mathfrak{P} \text{ ramified}} q_i^{0 \text{ or } 1}$

so Φ is surjective

(d) $|\mathcal{O}(K)[2]| = \dfrac{\left| \bigoplus_{\mathfrak{P}/p \text{ ramified}} \mathbb{Z}/2\mathbb{Z} \; \mathfrak{P} \right|}{|\ker = \mathbb{Z}/2\mathbb{Z}|} = 2^{M-1}$

(5) (a) by Problem 1 of Pset 3

p splits in $\mathcal{O}_K$ as $x^n - 2$ splits mod $\mathbb{F}_p$

if $x^n - 2 \bmod p$ splits completely

$\Rightarrow$ $\exists$ n^{th} roots of 2 in $\mathbb{F}_p^\times$ so

$2 = \alpha_i^n$ so $\left(\alpha_i / \alpha_j \right)^n = 1$ in $\mathbb{F}_p^\times$

$i = 1, \ldots, n$ $i \neq j$

so $n \mid p-1$

$2^{\frac{p-1}{n}} = \alpha^{p-1} = 1 \pmod p$

(b) $n \mid p-1$ so $\mathbb{Z}/n\mathbb{Z} \twoheadleftarrow \mathbb{Z}/(p-1)\mathbb{Z}$

$\cong \mathbb{F}_p^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$

so $\exists$ unique $F \subset \mathbb{Q}(\zeta_p)$ $[F:\mathbb{Q}] = n$.

and $F/\mathbb{Q}$ is Galois with $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$

$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/F) = \mathbb{Z}/\left(\frac{p-1}{n}\right)\mathbb{Z} \subset \mathbb{F}_p^\times$

(c) $p \neq 2$ so 2 is unramified in $\mathbb{Q}(\zeta_p)$ and F

so $D_{q/2} \cong \mathrm{Gal}(k_q/\mathbb{F}_2) = \langle \mathrm{Frob}_{q/2} \rangle$

$\downarrow$ $\downarrow$

$D_{p/2} \cong \mathrm{Gal}(k_p/\mathbb{F}_2) = \langle \mathrm{Frob}_{p/2} \rangle$

$\mathrm{Frob}_{p/2}(x) = x^2$ so $\mathrm{Frob}_{p/2}$ = image of $\mathrm{Frob}_{q/2}$

$\mathrm{Frob}_{q/2}(x) = x^2$

From class $\mathrm{Frob}_{q/2} \in D_{q/2} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$

is $2 \in (\mathbb{Z}/p\mathbb{Z})^\times$

But if $\mathbb{F}_p^\times = \langle g \rangle$

then $2 = g^{n \cdot k}$ where $\alpha = g^k$ so

$2 \in \langle g^n \rangle \cong \mathbb{Z}/\frac{p-1}{n}\mathbb{Z}$

so image of 2 in $\mathbb{Z}/n\mathbb{Z} = \dfrac{(\mathbb{Z}/p\mathbb{Z})^\times}{\mathbb{Z}/\frac{p-1}{n}\mathbb{Z}}$ is 1

so $\mathrm{Frob}_{\mathfrak{P}/2} = 1$ —

(d) Thus $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_2) = \langle \mathrm{Frob}_{\mathfrak{P}/2} \rangle = 1$

so $f_{\mathfrak{P}/2} = 1$ and also $e_{\mathfrak{P}/2} = 1$

$\Rightarrow$ 2 splits completely in F.

(e) $\mathbb{Z}[X_1 \dots X_m] \xrightarrow{i} \mathcal{O}_F = \mathbb{Z}[\alpha_1 \dots \alpha_m] \longrightarrow \mathcal{O}_F/\mathfrak{P}$ (112) $\mathbb{F}_2$

$X_i \longmapsto \alpha_i$

has kernel $i^{-1}(\mathfrak{P})$ which are all distinct as the $\mathfrak{P}$ are distinct.

(f) X_i maps to 0 or 1 and if $\pi(X_i) = e_i$

then $\pi(P(X_1 \dots X_m)) = P(e_1 \dots e_m) \bmod 2$

so π uniquely defined by $X_i \mapsto 0$ or 1.

Thus have 2^m quotients with kernel $(X_i \mid X_i \mapsto 0)$.

so $2^m \geq n \Rightarrow m \geq \lceil \log_2(n) \rceil$

3(e) (i) say $O_K^\times$ = rank 1 has free part generated by $u > 1$ (if $u < 1$ take u^{-1})

$$\sigma(u) = re^{i\theta} \qquad \bar{\sigma}(u) = re^{-i\theta}$$

$$1 = N_{K/\mathbb{Q}}(u) = u\,\sigma(u)\bar{\sigma}(u) = ur^2 \quad \text{so} \quad u = r^{-2}$$

(ii) $\operatorname{disc}(1, u, u^2) =$

$$\begin{vmatrix} 1 & 1 & 1 \\ r^{-2} & re^{i\theta} & re^{-i\theta} \\ r^{-4} & r^2e^{2i\theta} & r^2e^{-2i\theta} \end{vmatrix}^2$$

$$= \begin{vmatrix} 1 & 2 & 1 \\ u & 2r\cos\theta & re^{-i\theta} \\ u^2 & 2r^2\cos(2\theta) & r^2e^{2i\theta} \end{vmatrix}^2 = 4 \begin{vmatrix} 1 & 1 & 1 \\ u & r\cos\theta & re^{i\theta} \\ u^2 & r^2\cos 2\theta & r^2e^{-2i\theta} \end{vmatrix}^2$$

$$= 4 \begin{vmatrix} 1 & 1 & 0 \\ u & r\cos\theta & -ir\sin\theta \\ u^2 & r^2\cos 2\theta & -ir^2\sin 2\theta \end{vmatrix}^2$$

$$= -4 \begin{vmatrix} 1 & 1 & 0 \\ u & r\cos\theta & r\sin\theta \\ u^2 & r^2\cos 2\theta & r^2\sin 2\theta \end{vmatrix}^2$$

$$= -4 \left(\begin{vmatrix} r\cos\theta & r\sin\theta \\ r^2\cos 2\theta & r^2\sin 2\theta \end{vmatrix} - \begin{vmatrix} u & r\sin\theta \\ u^2 & r^2\sin 2\theta \end{vmatrix} \right)^2$$

$$= -4 \left(r^3 \underbrace{(\cos\theta \sin 2\theta - \cos 2\theta \sin\theta)}_{\sin\theta} - (\sin 2\theta - r^{-3}\sin\theta) \right)^2$$

$$= -4 \left((r^3 + r^{-3})\sin\theta - \underbrace{\sin 2\theta}_{2\sin\theta\cos\theta} \right)^2 =$$

$$= -4\sin^2\theta \left(r^3 + r^{-3} - 2\cos^2\theta \right)^2$$

$c = \cos\theta \qquad x = r^3 + r^{-3}$

$$|\mathrm{disc}(u)| = 4\sin^2\theta\,(r^3 + r^{-3} - 2\cos^2\theta)^2$$

$$= 4(1-c^2)(x-2c)^2$$

$$f(x) = (4-c^2)(x-2c)^2 - x^2$$

$$= -c^2x^2 - 4c(1-c^2)x + 4c^2(1-c^2)$$

If $A<0$: $\quad AX^2+BX+C \le \dfrac{4AC-B^2}{4A}$

so $\quad f(x) \le \dfrac{-16c^4(1-c^2) - 16c^2(1-c^2)^2}{-4c^2}$

$$= 4c^2(1-c^2) + 4(1-c^2)^2$$

$$= 4c^2 - 4c^4 + 4 - 8c^2 + 4c^4 = 4\sin^2\theta$$

so

$$|\mathrm{disc}(u)| \le 4\underbrace{(r^3+r^{-3})}_{x}^2 + 4^2\sin^2\theta \le$$

$$\le 4(r^6 + 2 + r^{-6}) + 4^2$$

$$\le 4(u^3 + u^{-3} + 6).$$

(iii) $\quad u^3 + u^{-3} + 6 \ge \dfrac{|\mathrm{disc}(u)|}{4}$

so $\quad u^3 \ge \dfrac{|\mathrm{disc}(u)|}{4} - u^{-3} - 6 \quad (u>1) \quad > \dfrac{|\mathrm{disc}(u)|}{4} - 7$

~~If u generates the [illegible] part of $\mathcal{O}_K^\times$~~

$$\operatorname{disc}(1, u, u^2) = \operatorname{disc} \mathbb{Z}[u] = \operatorname{disc}(K)\,[\mathcal{O}_K : \mathbb{Z}[u]]^2$$

so $\quad u^3 > \dfrac{|\operatorname{disc}(K)|}{4} - 7$

$\operatorname{disc}(K) = -1323 \quad$ so $\quad u^3 > 323.75$

$2 - \sqrt[3]{7} = \alpha \cdot u^{-k} \qquad |\alpha| = 1$ ↑ root of unity

so $\quad 2 - \sqrt[3]{7} = \pm u^{-k}$ (2 − ∛7 > 0)

so $\quad 2 - \sqrt[3]{7} = u^{-k} \quad k > 0.$ (2 − ∛7 < 1)

so $\quad u^k = \dfrac{1}{2 - \sqrt[3]{7}} > 323.75$ $\qquad k \geq 3$

so $\quad -\ln(2 - \sqrt[3]{7}) > \dfrac{k}{3} \ln(323.75)$

so $\quad 1 \leq k < \doteq \dfrac{3 \ln(2 - \sqrt[3]{7})}{\ln(323.75)} \approx 1.26$

so $\quad k = 1 \quad$ and so $\quad 2 - \sqrt[3]{7} = u^{-1}$

generates the free part of $\mathcal{O}_K^\times$