No.: Date:

Number Fields 2011

1.) (a) Minkowski Bound: $\left(\frac{4}{\pi}\right) \cdot \frac{1}{2} \sqrt{\Delta(k)}$

$-17 \equiv 3 \pmod 4 \Rightarrow \mathcal{O}_k = \mathbb{Z}[\sqrt{-17}] \Rightarrow \Delta(k) = \Delta(t^2+17) = 4 \cdot 17.$

$\therefore \left(\frac{4}{\pi}\right) \cdot \frac{1}{2} \sqrt{4 \cdot 17} = \sqrt{\frac{16 \cdot 17}{\pi^2}} < \sqrt{272/9} < 6.$

$\therefore Cl_k$ is represented by norms with ideals ≤ 5. $\Rightarrow$ Generated by prime ideal factors of (2), (3), (5)

$[\mathcal{O}_k : \mathbb{Z}[\sqrt{-17}]] = 1$: Dedekind Criterion Valid on $p = 2, 3, 5$

$t^2+17 \equiv (t-1)^2 \pmod 2 \Rightarrow (2) = (2, \sqrt{-17}+1)^2$

$\equiv t^2+2t-1 \pmod 3 \Rightarrow (3) = (2, \sqrt{-17}+1)(2, \sqrt{-17}-1)$

$\equiv t^2+2 \pmod 5 \Rightarrow (5) =$ is prime.

$\alpha = (2, \sqrt{-17}+1)$, $\beta = (3, \sqrt{-17}+1)$: $Cl_k = \langle [\alpha], [\beta] \rangle$

$\beta^2 \cdot \alpha = \beta \cdot (6, 1+\sqrt{-17}) = (18, 3(1+\sqrt{-17}), (1+\sqrt{-17})^2)$

$= (18, 3(1+\sqrt{-17}), -16+2\sqrt{-17}) = (18, 3(1+\sqrt{-17}), 2(1+\sqrt{-17}))$

$= (18, 1+\sqrt{-17}) = (1+\sqrt{-17})$ as $1+\sqrt{-17} \mid 18 = N(1+\sqrt{-17})$

$\therefore [\alpha] = [\beta]^{-2} = [\beta]^4 = e$.

Claim: β^2 not principal

β^2 is of norm 9, $\beta^2 \neq (3)$ (We know the factorsation of (3)), $j \neq \beta^2$

If $\beta^2 = (x + y\sqrt{-17})$: $x, y \in \mathbb{Z}$

$x^2 + 17y^2 = 9 \Rightarrow y = 0$, $x = 3, -3$ (reject)

$\therefore \beta^2$ not principal $\Rightarrow$ ord $([\beta]) \neq 1, 2 \Rightarrow$ ord $([\beta]) = 4$

$\therefore Cl_k \cong C_4 = \langle [\beta] \rangle$ //

No.: Date:

(b) Work over K.:

$(y+\sqrt{-17})(y-\sqrt{-17}) = x^5$

If P is prime ideal, $P \mid (y \pm \sqrt{-17}) : 2\sqrt{-17} \in P \Rightarrow P \mid (2\sqrt{-17})$

But $N(P) \mid N(x)^5$: ✗

If $2 \mid N(P)$: $2 \mid x$

$\therefore y^2 + 17 = 2^5 \equiv 0 \pmod 4 \Rightarrow y^2 \equiv -1 \pmod 4$ (no sln).

If $17 \mid N(P)$: $17 \mid x \Rightarrow y^2 = x^5 - 17 \equiv 0 \pmod{17} \Rightarrow 17 \mid y$

$\therefore 17^2 \mid x^5 - x^5 = -17$ (reject)

$\therefore N(P) \mid N(2\sqrt{-17}) = 2^2 \cdot 17 \Rightarrow N(P) = 1 \Rightarrow$ No common factors between $(y \pm \sqrt{-17})$

$x^5 = P_1^{5k_1} \cdots P_n^{5k_n}$ (P_i are distinct prime ideals)

$(y+\sqrt{-17})$, $(y-\sqrt{-17})$ no shared factors $\Rightarrow$ (After rearranging $P_1 \cdots P_n$)

$(y+\sqrt{-17}) = P_1^{5k_1} \cdots P_r^{5k_r} = I^5$.

$\therefore$ ord $([I]) = 1$ or 5 (reject as $Cl_K \cong C_4 \Rightarrow$ No ekmat of order 5)

$\therefore I$ is principal

Dirichlet's Unit Theorem: $O_K^* \cong \mu \times \mathbb{Z}^*$

± 1 are the only ~~our~~ roots of unity in K.

$\therefore y+\sqrt{-17} = \pm(a+b\sqrt{-17})^5 = (\pm(a+b\sqrt{-17}))^5 = (\text{WLOG})\ (a+b\sqrt{-17})^5$

$(a, b \in \mathbb{Z})$

$\therefore y+\sqrt{-17} = a^5 + 5a^4 b\sqrt{-17} + 10a^3b^2(-17) + 10a^2b^3(-17)\sqrt{-17} + 5ab^4(17)^2 + b^5(17)^2\sqrt{-17}$

$\therefore 1 = 5a^4 b + 10a^2b^3(-17) + b^5(17)^2 \Rightarrow b \mid 1 \Rightarrow b = 1$ or -1

$b=1$: $1 = 5a^4 - 170a^2 + 17^2 = 1$ or -1

Consider mod 5: $17^2 = 2^2 = -1 \neq 1$ (reject 1)

No.: ..... Date: .....

(mod 17): $5a^4 \equiv 1 \pmod{17}$

$\therefore a^{4} \equiv 7 \pmod{17}$

But $7^4 \equiv (49)^2 \equiv (-2)^2 \equiv 4 \not\equiv 1 \pmod{17}$

$\therefore$ 7 is not a 4th power.

integral

$\therefore$ No solutions

2.1 $\forall x \in \mathcal{O}_K$: $x = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$.

$Tr(x) = 2a \in \mathbb{Z} \Rightarrow a = k/2$, $k \in \mathbb{Z}$

$N(x) = a^2 - d b^2 \in \mathbb{Z} \Rightarrow k^2 - 4d b^2 \in \mathbb{Z} \Rightarrow 4d b^2 \in \mathbb{Z}$

If $b = p/q$, $p, q \in \mathbb{Z}$, $q \in \mathbb{N}$ and $\gcd(p, q) = 1$:

$q^2 \mid 4d \Rightarrow$ (d is square free) $q = 1$ or 2

$\therefore b = \lambda/2$, $\lambda \in \mathbb{Z}$

$k^2 - d\lambda^2 \in 4\mathbb{Z}$

If $d \equiv 1 \pmod 4$: $k^2 \equiv \lambda^2 \pmod 4$ iff $k \equiv \lambda \pmod 2$

$\therefore x = n + m(1 + \sqrt{d})/2$, $n, m \in \mathbb{Z}$

If $d \equiv 2, 3 \pmod 4$: $k^2 \equiv 0 \pmod 4 \Rightarrow k \equiv 0 \pmod 2$ $\Rightarrow$ $d \neq$

$2\lambda^2 \equiv 0 \pmod 4 \Rightarrow \lambda \equiv 0 \pmod 2$

If $d \equiv 3 \pmod 4$: $k^2 \equiv -\lambda^2 \pmod 4 \Rightarrow k \equiv \lambda \pmod 2$, $k, \lambda \not\equiv 1 \pmod 4$

$\therefore k, \lambda \equiv 0 \pmod 2$

d square free $\Rightarrow$ $d \not\equiv 0 \pmod 4$

$\therefore$ If $d \equiv 1 \pmod 4$: $\mathcal{O}_K = \mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{d})\right]$

If $d \equiv 2, 3 \pmod 4$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$

No.: ..... Date: .....

(b) $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ as $t^3 - 2$ is irreducible (Eisenstein) and $2^{1/3}$ root of $t^3 - 2$.

$\mathbb{Q} \leq \mathbb{Q}(2^{2/3}) \leq \mathbb{Q}(2^{1/3}) : [\mathbb{Q}(2^{2/3}) : \mathbb{Q}] \mid [\mathbb{Q}(2^{1/3}) : \mathbb{Q}]$

$4^{1/3} = (2^{1/3})^2 \Rightarrow 4^{1/3} \in \mathbb{Q}(2^{1/3}) \Rightarrow \mathbb{Q}(4^{1/3}) \leq \mathbb{Q}(2^{1/3})$

$2^{1/3} = \frac{1}{2}(2^{2/3})^2 \Rightarrow \mathbb{Q}(2^{1/3}) \leq \mathbb{Q}(2^{2/3})$

$\therefore \mathbb{Q}(2^{1/3}) = \mathbb{Q}(4^{1/3})$

Let $\{1, 4^{1/3}, 4^{2/3}\}$ be a basis of $\mathbb{Q}(2^{1/3})$

$\{1, 2^{1/3}, 2^{2/3}\}$ is also a basis of $\mathbb{Q}(2^{1/3})$,

elements are integral

$$\begin{pmatrix} 1 \\ 2^{2/3} \\ 2^{4/3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2^{1/3} \\ 2^{2/3} \end{pmatrix}, \quad \left| \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} \right| = 2.$$

$\therefore \{1, 4^{1/3}, 4^{2/3}\}$ not integral as $\Delta(1, 4^{1/3}, 4^{2/3}) = 4\,\Delta(1, 2^{1/3}, 2^{2/3})$

$\therefore \Delta$ Not minimal

No.: Date:

4) (a) Consider : $\Phi : K \to \mathbb{R}^2$, $\Phi(a + b\sqrt{d}) = (a + b\sqrt{d},\ a - b\sqrt{d})$

$\Lambda = \Phi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^2$; $\text{Covol}(\Lambda) = |\Delta(\mathcal{O}_K)| = D$

Let $R(t) = [t, t] \times [D/t, D/t]$:

R is balanced convex, closed; & $|R(t)| = 4D = 2^2 \cdot \text{Covol}(\Lambda)$

$\therefore \exists\, \alpha \in \mathcal{O}_K$ s.t $\Phi(\alpha) \neq \in R$, $\alpha \neq 0$.

$\alpha \neq 0$: $\mathcal{O}_i(\alpha) \neq 0 \Rightarrow \Phi(\alpha)$ is not on x or y axis.

Pick $x_1 \in \mathcal{O}_K \setminus \{0\}$, s.t. $\Phi(x_1) \in R(1)$. :

Given $x_1, \dots x_n \in \mathcal{O}_K$ s.t. $\Phi(x_i) \in R(t_i)$ and

$|\mathcal{O}_1(x_1)| > \dots |\mathcal{O}_n(x_n)| > 0$:

Pick $t_{n+1} \in (0, |\mathcal{O}_n(x_n)|)$: $x_{n+1} \in \mathcal{O}_K \setminus \{0\}$ s.t. $\Phi(x_{n+1}) \in R(t_{n+1})$

$\therefore |\mathcal{O}_{n+1}(x_{n+1})| \in (0, |\mathcal{O}_1(x_n)|)$

$|N(x_n)| = \mathcal{O}_1(x_n) \cdot \mathcal{O}_2(x_n) \leq D$

Since $(|\mathcal{O}_1(x_n)|)_{n \geq 1}$ is decreasing, $(x_n)_{n \geq 1}$ is distinct

$\therefore \exists\, m \in [1, D] \cap \mathbb{N}$ s.t $\exists\, \infty$ x_n, $N(x_n) = m$

$|\mathcal{O}_K/(m)|$ finit $\Rightarrow \exists\, \infty$ x_n of norm m, x_n in the same $\mathcal{O}_K/(m)$ coset. $|N(x_n)| = m$.

By passing to a subsequence: We can WLOG :

$(x_n)_{n \geq 1}$ distinct, $N(x_n) = m$, $x_{n_1} - x_{n_2} \equiv 0 \pmod m$ $(n_i, n \in \mathbb{N})$

$|N[x_n/x_1]| = 1$

$x_n/x_1 = 1 + (x_n - x_1)/x_1$, $x_1 \mid m$, $m \mid x_n - x_1 \Rightarrow x_n/x_1 \in \mathcal{O}_K$

$\therefore x_n/x_1 \in \mathcal{O}_K^\times$

$\therefore$ We have found ∞ elements unit elements

No.: Date:

(b) If r is the # of real embeddings, s is the # of complex embedding pairs:

$$\mathcal{O}_K^\times \cong \mu \times \mathbb{Z}^{r+s-1}, \qquad \mu = \{ x \in \mathcal{O}_K : x \text{ is a root of unity} \}$$

(c) $N(8+3\sqrt{7}) = 1 \Rightarrow$ Valid unit. ; $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$

If $1 < a+b\sqrt{7} \leq 8+3\sqrt{7}$: $|a^2 - 7b^2| = 1$

$1 > |a-b\sqrt{7}| > 0$.

$\therefore 0 < 2a, 2b\sqrt{7} \leq 9+3\sqrt{7} \Rightarrow 0 < b \leq 3/2 + 9/2\sqrt{7}$

$\leq 3/2 + 9/4 < 4.$

If $b=1$: $a^2 - 7 \in \{\pm 1\}$
If $b=2$ $a^2 - 28 \in \{\pm 1\}$
} No solution in $\mathbb{Z}$

$\therefore$ $b=3$: $a^2 - 63 \in \{\pm 1\} \Rightarrow a = 8.$

$\therefore \varepsilon = 8+3\sqrt{7}$ is the unit with smallest magnitude, > 1.

$\therefore \varepsilon$ is fundamatal.

No.: Date:

Number Fields 2012

1.) (a) $x \in \mathcal{O}_K$: $x \in \mathcal{O}_K^\times$ iff $N(x) = 1$

If $K = \mathbb{Q}(\sqrt{d})$:

Case 1: $d < 0$.

$N(x + y\sqrt{d}) = x^2 - dy^2 = 1$, $|d| > 1 \Rightarrow y = 0 \Rightarrow x = \{1 \text{ or } -1$

$\therefore \mathcal{O}_K^\times / \{\pm 1\} = \{e\} \cong C_1$

Case 2: $d > 0$

Consider : $\phi : \mathcal{O}_K^\times \to (\mathbb{R}, +)$, $\phi(x) = \log(|x|)$

ϕ is a group homomorphism

Claim: $\mathrm{Im}(\phi)$ is discrete.

Fix $[-R, R] \subseteq \mathbb{R}$; $|\phi^{-1}([-R, R] \cap \mathrm{Im}(\phi))| \leq |\{x \in \mathcal{O}_K^\times : |x| \leq e^R\}|$

$\leq |\{x \in \mathcal{O}_K^\times : |x| \leq e^R\}| < \infty$ as $\mathcal{O}_K$ is a discrete group.

$\therefore \mathrm{Im}(\phi)$ is discrete.

If

$\therefore \exists$ ~~minimal~~ $x \in \mathcal{O}_K^\times$ s.t. $\phi(x) > 0$ is minimal

($\mathrm{Im}(\phi) \cap \overline{D}(0,1)$ is finite)

Claim: $\mathrm{Im}(\phi)$ generated by $\phi(x)$

$\forall y \in \mathcal{O}_K^\times$: $\log(|y|) = a \cdot \log(|x|) + R$, $0 \leq R < \log(|x|)$, $a \in \mathbb{Z}$

$\log(|y/x^a|) = R < \log(|x|) \Rightarrow R = 0$ ($\log(|x|)$ minimal)

$\therefore \log(|y|) = \log(|x^a|)$

$\therefore \mathrm{Im}(\phi)$ generated by $\phi(x)$

$\therefore \mathcal{O}_K^\times / \ker(\phi)$ ~~$\cong \mathbb{Z}$~~ is cyclic (generated by x)

No.: Date:

If no such x, $\Phi(x) > 0$: $\mathrm{Im}(x) = \{0\}$ $\therefore$ $\mathcal{O}_K^\times / \ker(\Phi) \cong C_1$

(a) If ~~$\Phi(x) = 1$~~ $\Phi(x) = 0$: $|x| = 1$; $x \in \mathbb{R}$ $\Rightarrow$ $x = 1$ or -1

$\therefore \ker(\Phi) = \{\pm 1\}$

$\therefore$ $\mathcal{O}_K^\times / \{\pm 1\} \cong C_1$ or $\mathbb{Z}$ (cyclic).

(b) $-3 < 0$: $\mathcal{O}_K \cong \mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$ $\Rightarrow$ 1 is a generator.

$K = \mathbb{Q}(\sqrt{11})$: $\alpha = 10 + 3\sqrt{11} > 1$; $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$

If $1 < a + b\sqrt{11} \leq \alpha$: $a^2 - 11b^2 = 1$ or -1

$1 > |a - b\sqrt{11}| \geq 0$

$\therefore 0 < 2a,\ 2b\sqrt{11} \leq 11 + 3\sqrt{11}$

$\therefore 0 < b \leq \sqrt{11}/2 + 3/2 < 4$

$\therefore b = 1, 2, 3$

If $b = 1$ or 2, no solutions of a. $\Rightarrow$ $b = 3$, $a = 10$

$\therefore \alpha$ is a generator.

(c) $N(\pm(10 + 3\sqrt{11})^n) = 1$ $\Rightarrow$ All units of norm 1 (no elemab of norm -1)

$\therefore n = -1$: No solutions

$4^2 - 11 \cdot (1)^2 = 5$ $\therefore$ $x = 4$, $y = 1$ is a solution

~~$(4)^2 - 11(1)^2 = (5)$~~ $\Rightarrow$ $(5) = (5, 4 - \sqrt{11})(5, 4 + \sqrt{11})$

$\therefore N(x + \sqrt{11} \cdot y) = 5$ $\Rightarrow$ $(x + \sqrt{11} \cdot y) = (5, 4 - \sqrt{11})$ or $(4 + \sqrt{11})$

$\therefore x + \sqrt{11}\, y = u \cdot (4 - \sqrt{11})$ or $u \cdot (4 + \sqrt{11})$, $u \in \mathcal{O}_K^\times$

$N(u) = 1$: All $u \in \mathcal{O}_K^\times$ will be valid.

No.: ..... Date: .....

Solution : $\left\{ (x, y) : x + \sqrt{11}\, y = \epsilon \left\{ \pm (4 * \pm \sqrt{11}) \cdot (10 + 3\sqrt{11})^n : n \in \mathbb{Z} \right\} \right\}$

Dedekind : $(2) = (2, \sqrt{11} + 1)^2$

$(7) = (7, \sqrt{11} + 2)(7, \sqrt{11} - 2)$

$\therefore$ $\exists$ 2 ideals of norm 14 : $(5 \pm \sqrt{11})$

$\therefore N(x + \sqrt{11} y) = 14 \Rightarrow (x + \sqrt{11} y) = (5 \pm \sqrt{11})$ or $(5 - \sqrt{11})$

$\therefore x + \sqrt{11} y = u \cdot (5 \pm \sqrt{11})$; $N(u) = 1 \Rightarrow$ all $u \in \mathcal{O}_K^\times$ works

$\therefore \left\{ (x, y) : x + \sqrt{11} y \in \left\{ \pm (10 + 3\sqrt{11})^n \cdot (5 \pm \sqrt{11}) : n \in \mathbb{N} \right\} \right\}$ ✓

2.) cal $\alpha = \frac{1 \pm \sqrt{1 - 48}}{2}$ (Pick +)

$\therefore K = \mathbb{Q}(\sqrt{-47})$: $-47 \equiv 1 \pmod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z}[\alpha]$

$\mathbb{Z}[\alpha] = \mathcal{O}_K \Rightarrow$ We can apply Dedekind Criterion to

$p = 2, 3$

$t^2 - t + 12 \equiv t(t-1) \pmod{2, 3}$

$\therefore (2) = (2, \alpha), (2, \alpha - 1)$

$(3) = (3, \alpha), (3, \alpha - 1)$

$N(\alpha) = \frac{1}{4}(1 + 47) = 12$

$N(\alpha + 2) = \frac{1}{4} N(5 + 2\sqrt{-47}) = \frac{1}{4}\{25 + 47\} = 18$

$(2, \alpha)^2 \cdot (3, \alpha) = (2, \alpha)\underbrace{(6, 2\alpha, 3\alpha, \alpha^2)}_{\text{Generates } \alpha} = (2, \alpha)(6, \alpha)$

$= (12, 2\alpha, 6\alpha, \alpha^2) = (12, 2\alpha, \alpha - 12) = (12, \alpha)$

$= (\alpha)$ as $\alpha \mid 12$.

No.: Date:

$(\alpha 2, \alpha) \cdot (3, \alpha-1)^2 = (2, \alpha+2)(3, \alpha+2)^2 = (3, \alpha+2) \cdot (6, \underbrace{3(\alpha+2), 2(\alpha+2)}_{\text{Generaks } \alpha+2}, (\alpha+2)^2)$

$= (3, \alpha+2) \cdot (6, 3+\alpha) = (18, 3(\alpha+2), \alpha^2+4\alpha+4) = (18, 3(\alpha+2), 5\alpha-8)$

$= (18, \underbrace{3(\alpha+2), 5\alpha+10}_{\gcd(3,5)=1}) = (18, \alpha+2) = (\alpha+2)$ as $\alpha+2 \mid 18$.

$\therefore$ $(2) = (2, \alpha)(2, \alpha-1)$
$(3) = (3, \alpha)(3, \alpha-1)$
$(\alpha) = (2, \alpha)^2 \cdot (3, \alpha)$
$(\alpha+2) = (2, \alpha) \cdot (3, \alpha-1)^2$

Minkowski Bound: $\left(\frac{4}{\pi}\right) \cdot \frac{2!}{2^2} \sqrt{|\Delta|}$

$\Delta(O_k) = \text{Disc}(x^2 - x + 12) = 1 - 4 \cdot (12) = -47$

$\therefore \left(\frac{4}{\pi}\right) \cdot \sqrt{47} < \sqrt{\frac{188}{9}} < \sqrt{21} < 5.$

$\therefore$ All elemab of Cl_k has representative of norm ≤ 4.

$\Rightarrow Cl_k$ generaked by prime ideal factors of (2), (3)!

Let $\alpha = [(2, \alpha)]$, $\beta = [(3, \alpha)]$:

$\left.\begin{aligned} \alpha^2 \cdot \beta^0 &= e \\ \alpha \cdot \beta^{-2} &= e \end{aligned}\right\} \alpha = \beta^2, \quad \beta^5 = e.$

If β $(3, \alpha)$ is principal: $(3, \alpha) = (x + y\left(\frac{1+\sqrt{-47}}{2}\right)) \Rightarrow$

We have elemal of norm 3.

$(x + y/2)^2 + \frac{47}{4} \cdot y^2 = 3$

If $|y| \geq 1$: $LHS \geq \frac{47}{4} > 3$ (rej)

$\therefore y = 0 \Rightarrow x^2 = 3$ (no sln)

$\therefore \beta \neq e \Rightarrow \text{ord}(\beta) = 5.$

$\therefore Cl_k \cong C_5, \quad = \langle \beta \rangle$

No.: ..... Date: .....

Let $\omega = \frac{1}{2}(1+\sqrt{-47})$:

$$y^3+y+12 = (y+\omega)(y+\bar{\omega}) = 3X^5$$

Let $I = GCD((y+\omega),(y+\bar{\omega})) : (y+\omega), (y+\bar{\omega}) \in I$

$\omega - \bar{\omega} = \frac{1}{2}(1+\sqrt{-47} - (1-\sqrt{-47})) = \sqrt{-47} \Rightarrow I \mid (\sqrt{-47})$

$N((\sqrt{-47})) = 47$ is prime. $\therefore I = (1)$ or $(\sqrt{-47})$

If $I = (\sqrt{-47})$: $I^2 \parallel (y+\omega)(y+\bar{\omega}) \Rightarrow I^2 \mid (3X^5)$ (reject)

as $p \mid (3)(X)^5$, $p \nmid (3) \Rightarrow p^5 \mid (3x^5)$.

$\therefore I=(1)$

Let $\therefore (X)^5 = P_1^{5k_1} \cdots P_n^{5k_n}$, P_i are prime. :

$$\left.\begin{aligned}(y+\omega) &= P_1^5 \cdots P_r^5 \cdot J_1 \\ (y+\bar{\omega}) &= P_{r+1}^5 \cdots P_n^5 \cdot J_2\end{aligned}\right\} \; J_1 J_2 = 3$$

$3 \nmid y+\omega \Rightarrow J_1$, J_2 are the 2 factors of (3)

But $[P_1^5 \cdots P_r^5 J_1] \neq e$ (in CL_K) $\Rightarrow (y+\omega)$ not principal

$\therefore$ Contradiction

$\therefore$ No integral solutions

No.: ..... Date: .....

3.) (a) Let $x = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \in \mathcal{O}_K$: $a, b, c, d \in \mathbb{Q}$

$Tr_{K/\mathbb{Q}(\sqrt{p})}(x) = 2a + 2b\sqrt{p} \in \mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \mathbb{Z}[\sqrt{p}]$

$\therefore a, b \in \frac{1}{2}\cdot\mathbb{Z}$

$Tr_{K/\mathbb{Q}(\sqrt{q})}(x) = 2a + 2c\sqrt{q} \in \mathcal{O}_{\mathbb{Q}(\sqrt{q})} = \mathbb{Z}[\sqrt{q}]$

$\therefore a, c \in \frac{1}{2}\cdot\mathbb{Z}$

$Tr_{K/\mathbb{Q}(\sqrt{pq})}(x) = 2a + 2d\sqrt{pq} \in \mathcal{O}_{\mathbb{Q}(\sqrt{pq})} = \mathbb{Z}[\frac{1}{2}(1+\sqrt{pq})]$

$\therefore 2a, 2b \in \frac{1}{2}\mathbb{Z}$, $4a \equiv 4d \pmod 2$

$2a \in \mathbb{Z} \Rightarrow 4a \in 2\cdot\mathbb{Z} \Rightarrow 4d \in 2\cdot\mathbb{Z}$

$\therefore 2d \in \mathbb{Z}$

$\therefore x = \frac{1}{2}(a + b\sqrt{p}) + \frac{1}{2}\sqrt{q}(c + d\sqrt{p})$, $a, b, c, d \in \mathbb{Z}$

(b) $N_{K/\mathbb{Q}(\sqrt{qp})}(x) = \frac{1}{4}(a+b\sqrt{p})^2 - \frac{q}{4}(c+d\sqrt{p})^2 \in \mathbb{Z}[p]$

$\therefore a^2 + pb^2 - q(c^2 + pd^2) \equiv 0 \pmod 4 \Rightarrow a^2 - b^2 + c^2 - d^2 \equiv 0 \pmod 4$

$2ab - 2qcd \equiv 0 \pmod 4 \Rightarrow 2ab + 2cd \equiv 0 \pmod 4$

$\therefore ab + cd \equiv 0 \pmod 2$

If $c, d \equiv 0 \pmod 2$: $a^2 \equiv b^2 \pmod 4 \Rightarrow a \equiv b \pmod 2$

$ab + cd \equiv ab \pmod 2 \Rightarrow a$ or $b \equiv 0 \pmod 2$

$\therefore a \equiv b \equiv 0 \pmod 2$

If $c, d \equiv 1 \pmod 2$: $ab \equiv 1 \pmod 2 \Rightarrow a, b \equiv 1 \pmod 2$

If one of $c, d \equiv 0 \pmod 2$: $ab \equiv 0 \pmod 2 \Rightarrow$ at least 1 of $a, b \equiv 0 \pmod 2$

$a^2 - b^2 \equiv d^2 - c^2 \pmod 4 \Rightarrow a, b$ not both 0

If $c \equiv 0 \pmod 2$: $b \equiv 0 \pmod 2$

If $c \equiv 1 \pmod 2$: $b \equiv 1 \pmod 2$

No.: Date:

$\therefore\ b \equiv c \pmod 2, \quad a \equiv d \pmod 2$

$\therefore$ ~~Not~~ iff $\mathcal{O}_K \subseteq \mathbb{Z}\cdot\left\{1, \sqrt{p}, \frac{1+\sqrt{pq}}{2}, \frac{\sqrt{p}+\sqrt{q}}{2}\right\}$

$N\left(\frac{1+\sqrt{pq}}{2}\right) = \frac{1-(pq)}{4} \equiv 0 \pmod 4 \Rightarrow \frac{1+\sqrt{pq}}{2} \in \mathcal{O}_K$

~~$N\left(\frac{\sqrt{p}+\sqrt{q}}{2}\right) =$~~

~~$\alpha = \frac{\sqrt{p}+\sqrt{q}}{2} \Rightarrow \alpha^2 = \frac{p+q+2\sqrt{pq}}{4}$~~

$$\underbrace{\sqrt{p}\left(\frac{1+\sqrt{pq}}{2}\right)}_{\in \mathcal{O}_K} = \frac{\sqrt{p}+\sqrt{q}}{2} + \underbrace{\left(\frac{p-1}{2}\right)\cdot\sqrt{q}}_{\in \mathcal{O}_K}$$

$$\therefore \frac{\sqrt{p}+\sqrt{q}}{2} \in \mathcal{O}_K.$$

$$\therefore \mathcal{O}_K = \mathbb{Z}\cdot\left\{1, \sqrt{p}, \frac{1+\sqrt{pq}}{2}, \frac{\sqrt{p}+\sqrt{q}}{2}\right\}$$

$$\text{Disc}(1, \sqrt{p}, \sqrt{q}, \sqrt{pq}) = \det\begin{pmatrix} 1 & \sqrt{p} & \sqrt{q} & \sqrt{pq} \\ 1 & -\sqrt{p} & \sqrt{q} & -\sqrt{pq} \\ 1 & \sqrt{p} & -\sqrt{q} & -\sqrt{pq} \\ 1 & -\sqrt{p} & -\sqrt{q} & \sqrt{pq} \end{pmatrix} = pq \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix}$$

$$= pq \cdot 8 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} = -16pq \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$$= -16pq \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 16pq.$$

$\therefore \text{Disc} = 16^3 p^2 q^2 \qquad -(*)$

$\text{Disc}\left(1, \sqrt{p}, \frac{1+\sqrt{pq}}{2}, \frac{\sqrt{p}+\sqrt{q}}{2}\right) = \frac{1}{4^2}\cdot(*) = 16p^2q^2.$

No.: ..... Date: .....

No.: ..... Date: .....

Number Fields 2013

1.) (a) Let $\{\beta_1, \dots \beta_n\}$ be an integral basis:

$$\begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} = A \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \quad A \in GL_n(\mathbb{Z})$$

$\therefore \Delta(1, \alpha, \dots \alpha^{n-1}) = \det(A)^2 \cdot \Delta(\beta_1, \dots \beta_n)$

LHS = $\mathrm{Disc}(f)$: $\det(A)^2 \mid \mathrm{Disc}(f)$, $\mathrm{Disc}(f)$ is square-free

$\Rightarrow \det(A) = 1$ or -1

$\therefore \Delta(1, \alpha, \dots \alpha^{n-1}) = \Delta(\beta_1, \dots \beta_n) \Rightarrow \{1, \dots \alpha^{n-1}\}$ is an integral basis

(b) $(1-\alpha) = 3/\beta \Rightarrow \alpha = (\beta-3)/\beta$

$$\alpha^3 - 3\alpha - 25 = \frac{(\beta-3)^3}{\beta^3} - \frac{3(\beta-3)}{\beta} - 25 = 0$$

$$(\beta-3)^3 - 3(\beta-3)\cdot\beta^2 - 25\beta^3 = 0$$

$$(\beta-3)(\beta^2 - 6\beta + 9 - 3\beta^2) - 25\beta^3$$

$$= (\beta-3)(-2\beta^2 - 6\beta + 9) - 25\beta^3 = 0$$

$$\therefore 25\beta^3 + (\beta-3)(2\beta^2 + 6\beta - 9) = 27\beta^3 - 27\beta + 27 = 0.$$

$\therefore \beta^3 - \beta + 1 = 0$

$\therefore \beta$ root of $g(t) = t^3 - t + 1$

(mod 2): $t^3 + t + 1$ has no roots in $\mathbb{F}_2 \Rightarrow$ Irreducible in $\mathbb{F}_2$

$\Rightarrow$ Irreducible in $\mathbb{Z} \Rightarrow$ Irreducible over $\mathbb{Q}$

$\therefore g(t)$ is the minimal polynomial of β

$\Delta(1, \beta, \beta^2) = \mathrm{Disc}(g) = (-4)(-1)^2 - 27(1)^2 = 4 - 27 = -23$ is square free.

$\therefore \{1, \beta, \beta^2\}$ is an integral basis

$\therefore \Delta(k) = -23$

No.: Date:

$\Delta(1, \alpha, \alpha') = (-4)(-3)^3 - 27(25)^2$

$= -27\ (25^2 - 4 \cdot 3^3 \cdot 2^2) = -27 \cdot 27 \cdot 23.$

$= [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta(1, \beta, \beta')$

$\therefore\ [\mathcal{O}_K : \mathbb{Z}[\alpha]] = \sqrt{27}.$

2.) (a) Dirichlet Unit Theorem: Let K be a number field, r be the # of real embeddings of K in $\mathbb{C}$, s be the # of complex embedding pairs of K in $\mathbb{C}$

Let $\mu = \{x \in K : x \text{ is a root of unity}\}$:

$\mathcal{O}_K^{\times} \cong \mu \times \mathbb{Z}^{r+s-1}$

(b) Let $G = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$:

Define: $f_K(t) = \prod_{g \in G} (t - g(\alpha^k))$

$\forall\ h \in G:\ h \cdot f_K(t) = f_K(t) \Rightarrow f_K \in \mathbb{Q}[t]$

But $g(\alpha^k)$ are algebraic integers $\Rightarrow$ $g(\alpha)^k$ are integral

Since coefficients of f_K are sums / products of integral elements $\Rightarrow$ Coefficients are integral

$\therefore f_K(t) \in \mathbb{Z}[t]$

Coefficients of f_K are bounded by $A = \mathrm{Max}\left\{\binom{|G|}{i} : 0 \le i \le |G|\right\} \cdot \mathrm{Max}\{1, |g(\alpha)| : g \in G\}^{|G|}$.

$\therefore f_K$ Since there are finite degree $|G|$ polynomials in $\mathbb{Z}[t]$

No.: Date:

with coefficients bounded by A.

$\therefore \exists\ n_1 < n_2$ s.t. $f_{n_1} = f_{n_2}$

$\therefore \exists\ g \in G$ s.t. $\alpha^{n_1} = g(\alpha)^{n_2} = g(\alpha^{n_2})$

$\therefore$ ~~$g(\alpha) = \alpha^{n_1/n_2}$~~

$g(\alpha) = \alpha^{n_1/n_2}$

$\therefore g^{|G|}(\alpha) = \alpha = \alpha^{(n_1/n_2)|G|} \Rightarrow (\alpha^{n_2^{|G|} - n_1^{|G|}} - 1)\,\alpha^{n_1^{|G|}} = 0$

$\therefore \alpha^{n_2^{|G|} - n_1^{|G|}} = 1 \Rightarrow \alpha$ is a root of unity

$\alpha = 0$ or

Cor 4^{th} & 12^{th} cyclotomic polynomial : $t^4 - t^2 + 1 = f(t)$

$N_{K/k}(1 - \xi) = N_{K/k}(-1 \cdot \xi) = f(-1) = 1$

Let $\forall \in O_K^{\times}$: $G = Gal(K/\mathbb{Q})$ is abelian

$\therefore \forall g \in G$: $g(\tilde{\forall}) = \overline{g(\forall)} \Rightarrow |g(\forall/\tilde{\forall})| = 1$

$\therefore \forall/\tilde{\forall}$ is a root

Let $F = \mathbb{Q}(\sqrt{3})$; $O_F = \mathbb{Z}[\sqrt{3}]$

Dirichlet : $O_F^{\times} \cong \{\pm 1\} \times \mathbb{Z}^n$

$\alpha = 2 + \sqrt{3}$ is a >1 unit.

If $1 < a + b\sqrt{3} \leq \alpha$:

$1 > |a - b\sqrt{3}| > 0 \Rightarrow 0 < 2a,\ 2b\sqrt{3} \leq 3 + \sqrt{3}$

$\therefore 0 < 2ab \leq 1/2 + \sqrt{3}/2 \Rightarrow b = 1$

$a^2 - 3b^2 = 1$ or $-1 \Rightarrow a = 2$

$\therefore \alpha$ is a fundamental unit

No.: Date:

$N_{K/F}\left(\frac{1}{2}(1+\sqrt{3})\right) = \frac{1}{4}(3+1) = 1$

$N_{K/F}\left(\frac{1}{2}(1+\sqrt{3}+2)\right) = (1+\sqrt{3}/2)^2 + 1/4 = 1+\sqrt{3}+1 = 2+\sqrt{3}$. (unit in F)

$\therefore N_{K/\mathbb{Q}}(1+\zeta) = 1 \Rightarrow 1+\zeta$ is a unit in $\mathcal{O}_K^\times$

(Dirichlet). $\mathcal{O}_K^\times \cong \left\{ \omega^n \zeta^m : n \in \mathbb{N} \right\} \times \mathbb{Z}^{0+r-1}$

Let ε be a fundamental unit

$\therefore 1+\zeta = \varepsilon^a \cdot \omega^b \zeta^b$

$N(1+\zeta) = N(\varepsilon)^a \cdot N(\omega)^b = (2+\sqrt{3})^a$

$\therefore (2+\sqrt{3}) = N(\varepsilon)^a$

Since $2+\sqrt{3}$ is fundamental: $a = 1$

$\therefore \mathcal{O}_K^\times = \left\{ \cdot \zeta^a \cdot (1+\zeta)^b : a, b \in \mathbb{N} \right\}$

$(1+\zeta)^{12} = \sum_{k=0}^{12} \binom{12}{k} \zeta^{12-k}$; coefficient of ζ^r = coefficient of ζ^{12-r}.

$\therefore \overline{(1+\zeta)^{12}} = (1+\zeta) \Rightarrow 1+\zeta \in \mathbb{R}$

$\zeta(1+\zeta)^{10} = \sum_{k=1}^{11} \binom{10}{k-1} \zeta^{k+n}$ $\therefore$ Coefficient of ζ^r, ζ^{11-r} equal

$\therefore \in \mathbb{R}$

$\therefore \forall u \in \mathcal{O}_K^\times$, $\exists r \in [0, 11]$, $u \cdot (1+\zeta)^r \in K \cap \mathbb{R} = F$

$\therefore \mathcal{O}_K^\times = \left\{ (1+\zeta)^r u : u \in \mathcal{O}_F^\times, 0 \le r \le 11 \right\}$

($u \in \mathcal{O}_F^\times$, $r \in \mathbb{Z} \Rightarrow (1+\zeta)^r u \in \mathcal{O}_K^\times$)

$\therefore (2+\sqrt{3})$, $(1+\zeta)$ are fundamental units of F, K respectively

No.: Date:

4.) (a) Let K be a number field: $p \in \mathbb{N}$ be a prime, $\alpha \in \mathcal{O}_K$.
If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$: Let $f \in \mathbb{Z}[t]$ be min. poly. of α,
$\bar{f} \in \mathbb{F}_p[t]$ be $f \pmod p$

Let $\bar{f} = \prod_{i=1}^{r} \bar{g}_i^{e_i}$ be prime factorisation in $\mathbb{F}_p[t]$

$P_i = (p, g_i(\alpha))$ are prime ideals in $\mathcal{O}_K$,

$(p) = \prod_{i=1}^{r} P_i^{e_i}$

(b) $\mathcal{O}_K = \mathbb{Z}[\sqrt{65}]$: $f(t) = t^2 - 65$

$f(t) = (t-1)^2 \pmod 2 \Rightarrow (2) = (2, \sqrt{65}-1)^2$

$f(t) = t^2+1 \pmod 3$ (irreducible) $\Rightarrow (3)$ is prime

$f(t) = t^2 \pmod 5 \Rightarrow (5) = (5, \sqrt{65})^2$

(c) If $N(I) = 10$: Prime factorisation of I has 1 factor of (each) of norm 2, 5.

Since $\exists$ 1 ideal of 2, 5: $I = (2, \sqrt{65}-1)(5, \sqrt{65})$
$= (2, \sqrt{65}+5)(5, \sqrt{65}+5)$

$65 \equiv 1 \pmod 4$: $\omega = \frac{1}{2}(1+\sqrt{65})$

$\mathcal{O}_K = \mathbb{Z}[\omega]$, Minimum polynomial: $(2t-1)^2 = 65 \Rightarrow 4t^2 - 4t - 64$
$f(t) = t^2 - t - 16$

$\pmod 2$: $(t-1)t \pmod 2 \Rightarrow (2) = (2, \omega)(2, \omega-1)$

$(t^2 - t - 16) = t^2 - t - 1 \pmod 3 \Rightarrow (3)$ is prime.

$t^2 - t - 16 = t^2 + 4t + 4 = (t+2)^2 \pmod 5 \Rightarrow (5) = (5, 2+\omega)^2$

$\therefore$ If $N(I) = 10$, I is a product of a norm 2, 5 prime ideal

$\therefore I = (2, \omega)(5, 2+\omega)$ or $(2, \omega-1)(5; 2+\omega)$

No.: Date:

$(2, \omega)(5, \omega+2) = (10, \omega+2)$

$N(\omega+2) = \frac{1}{4} N(5+\sqrt{65}) = -10. \Rightarrow \omega+2 \mid 10$

$\therefore (2, \omega) \cdot (5, \omega+2) = (\omega+2)$ is principle

$(2, \omega-1)(5, \omega+2) = \overline{(2, \omega)} \cdot \overline{(5, \omega+2)} = (2+\bar{\omega})$

$= (2 + 1/2 - \sqrt{65}/2) = (-3-\omega) = (\omega-3)$

$\therefore$ All ideals of norm 10 is principal

(c) Minkowski Bound: $\frac{1}{2}\sqrt{|\Delta|}$; $\Delta = \text{Disc}(t^2-t-16)$

$= 1+64 = 65.$

$\therefore \sqrt{65/4} = \sqrt{16+1/4} < 5$

$\therefore Cl_K$ is represented by ideals of norm ≤ 4.

$\therefore$ Generated by prime ideal factors of $(2), (3)$

If $(5) = (x+y\omega) =$

$(5) = (x^2 + 2xy\omega + y^2\omega^2)$

$= (x^2 + 16y^2 + (2xy - y^2)\cdot\omega)$

Unit Group: $O_K^\times \cong \{\pm 1\} \times \mathbb{Z}^n$.

Try: $\alpha = 8 + \sqrt{65} = 7\beta + 2\omega.$

If $0 < x + y\omega \leq \alpha$: , $x, y \in \frac{1}{2}\cdot\mathbb{Z}$

$|\phi > |x - y\sqrt{65}| \geq 0.$

$\therefore 0 < 2x, 2y\sqrt{65} \leq 9 + \sqrt{65}$

$\therefore 1 \leq 2y \leq 1 + 9/\sqrt{65} < 3$

If $2y = 1$: $x^2 - 65/4 = 1$ or -1

$4\cdot(2x)^2 = 61$ or 69 (reject)

$\therefore 2y = 2$: $x = 8.$

$\therefore$ α is fundamental ; $N(\alpha) = -1$

If $(5, \omega+2)$ is principal

No.: Date:

$(5, \omega+2) = (A)$

$\therefore (5) = (A^2)$ $\therefore$ $\exists$ unit d_4 s.t $A^2 \cdot d^r = 5$ or -5.

$N(\pm 5) > 0$, $N(A)^2 > 0 \Rightarrow N(d)^r > 0 \Rightarrow r$ is even.

$\therefore A' = A d^{r/2}$, $A'^2 = 5$ or -5.

$A' = x + y/2 + y/2\sqrt{65}$:

~~$x^2 + xy + y^2/4 - 65\,y^2/4 = x^2 + xy - 16$~~

$(x + y/2)^2 + y^2/4 \cdot 65$

$x^2 + y^2\omega^2 + 2xy\omega = x^2 + y^2(-\omega + 16) + 2xy\omega$

$= x^2 + 16y^2 + (2xy - y^2)\omega = 5$ or -5.

If $y = 0$: $x^2 = 5$ or -5 (rej.)

$\therefore 2x = y$: $65y^2 = 5$ or -5 (rej.)

$\therefore (5, \omega+2)$ not principal

$(5, \omega+2) \cdot (2, \omega)$ principal $\Rightarrow (2, \omega)$ not principal

$\therefore Cl_k = \langle [(2, \omega)] \rangle$, $[(2, \omega)] \cdot [(5, \omega+2)] = e$.

$[(5, \omega+2)]$ order $2 \neq \Rightarrow$

$Cl_k \cong C_2$.

No.: ..... Date: .....

No.: Date:

Number Fields 2014

1.) (a) Let K be a number field: r be the # of real embeddings of K into $\mathbb{C}$, s be the # of pairs of non-real complex embeddings of K

Cl$_K$ elements have a representative of norm $\leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta|}$, $n = 2s + r$, $\Delta = \mathrm{Disc}(K)$

There are finit ideals of a $\mathcal{O}_K$ norm m ($m \in \mathbb{N}$) $\Rightarrow$ Cl$_K$ must be finite

(b) $-34 \equiv 2 \pmod 4$: $\mathcal{O}_K = \mathbb{Z}[\omega]$, $\omega = \sqrt{-34}$

$f(t) = t^2 + 34$ is the minimal polynomial of ω

$f(t) \equiv t^2 \pmod 2$

$\equiv t^2 + 1 \pmod 3$

$\equiv t^2 - 1 \equiv (t-1)(t+1) \pmod 5$

$\equiv (t-1)(t+1) \pmod 7$

Dedekind Criterion: $(2) = (2, \omega)^2$

(3) is prime

$(5) = (5, \omega - 1)(5, \omega + 1)$

$(7) = (7, \omega - 1)(7, \omega + 1)$

$(5, \omega+1) \cdot (7, \omega+1) = (35, \underbrace{5(\omega+1), 7(\omega+1)}_{\gcd(5,7) = 1}, (\omega+1)^2)$

$= (35, (\omega+1), (\omega+1)^2) = (\omega+1)$ ($\omega + 1 \mid 35 = N(\omega+1)$)

$(2, \omega) \cdot (5, \omega - 1)^2 = (2, \omega + 4) \cdot (5, \omega + 4)^2 = (5, \omega + 4)(10, \omega + 4)$

$= (50, 5(\omega+4), \omega^2 + 8\omega + 16) = (50, 5(\omega+4), 84 - 8\omega - 18)$

$= (50, \underbrace{5(\omega+4), 8\omega + 32}_{\gcd(5,8) = 1}) = (50, \omega + 4)$

$= (\omega + 4)$ as $\omega + 4 \mid 50 = N(\omega + 4)$

Minkowski Bound: $\left(\frac{4}{\pi}\right) \cdot \frac{1}{2}\sqrt{4 \times 34} \leq \sqrt{\frac{34 \times 16}{9}} \cdot 4 < 8$

$\therefore$ Cl$_K$ represented by elements of norm ≤ 7.

No.: Date:

$\therefore$ Cl_K generated by prime factors of (p) : $p = 2, 3, 5, 7$

$\alpha = (2, \omega)$, $\beta = (5, \omega - 1)$, $\gamma = (7, \omega + 1)$

$[\gamma] \cdot [\beta]^{-1} = e$ ($(\beta\gamma\omega)$ factorisation)

$[\alpha] \cdot [\beta]^2 = e \Rightarrow [\alpha] = [\beta]^{-2}$

$[\alpha]^2 = e$

$\therefore$ Cl_K generated by $[\beta]$, $[\beta]^4 = e$.

If β^2 is principal : $\beta^2 \neq (5)$, β^2 is an ideal of norm 25. , $\beta^2 = (x + y\omega)$

$x^2 + 34y^2 = 25 \Rightarrow |y| = 0 \Rightarrow x \in \{\pm 5\}$ (reject)

$\therefore$ $[\beta]^2 \neq e \Rightarrow Cl_K \cong C_4$, $|Cl_K| = 4$ ($Cl_K = \langle [\beta] \rangle$)

(a)

2.) (a) Let $\underline{P} \triangleleft \mathcal{O}_K$ be a prime $\Rightarrow \mathcal{O}_K / \underline{P}$ is a field.

Let $p = \text{char}(\mathcal{O}_K / \underline{P}) \in \mathbb{N}$: $p \in \underline{P}$ ($p \equiv 0$ in $\mathcal{O}_K / \underline{P}$)

$q \in \mathbb{N}$ prime,

If $q \in \underline{P}$: $q \equiv 0$ in $\mathcal{O}_K / \underline{P} \Rightarrow q \equiv 0 \pmod p$

$\therefore q = p$

$\therefore$ p is the unique prime in $\underline{P}$

~~Ramification~~ Let $(p) = \prod_{i=1}^{r} \underline{P}_i^{e_i}$ be prime ideal factorisation

$(e_1, \ldots e_r)$ are ~~the~~ ramification ~~index~~

$([\mathcal{O}_K / \underline{P}_i : \mathbb{F}_p])_{i=1,\ldots r}$ is the ~~residue class~~ degree.

For $\underline{P}_i$: e_i is the ramification index, $[\mathcal{O}_K / \underline{P}_i : \mathbb{F}_p] = f_i$ is the residue class degree

No.: Date:

Claim: $\sum_{i=1}^{r} e_i f_i = \deg [K : G]$

(Proof): $\mathcal{O}_K$ is a $\mathbb{Z}$-Module of dimension $[K : G]$

$\therefore |\mathcal{O}_K / p.\mathcal{O}_K| = p^{[K:G]}$

$(p) = \prod_{i=1}^{r} P_i^{e_i} \Rightarrow N((p)) = \prod_{i=1}^{r} N(P_i)^{e_i}$

Since $\mathcal{O}_K / P_i$ is a field extension of $\mathbb{F}_p$ of degree f_i,

$|\mathcal{O}_K / P_i| = p^{f_i}$

$\therefore N((p)) = p^{[\deg K : G]}$

$\prod_{i=1}^{r} N(P_i)^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i} = p^{\sum_{i=1}^{r} e_i f_i} \Rightarrow [K : G] = \sum_{i=1}^{r} e_i f_i$

(b) $t^n - 1 = \prod_{i=0}^{n-1} (t - \zeta^i) \Rightarrow f(t) = \prod_{i=1}^{n-1} (t - \zeta^i) = (t^n - 1)/(t - 1)$

$= \sum_{k=0}^{n-1} t^k$

$\therefore f(1) = \prod_{i=1}^{n-1} (1 - \zeta^i) = n$ - (*) $(\forall n \in \mathbb{N})$

$\zeta_n^p = \omega_q$ is a primative q root of unity, $\zeta^q = \omega_p$ is a primative p root of unity

If $n = pq$:

$(*) : p \cdot q = \prod_{i=1}^{q-1} \zeta_n^{p \cdot i} \cdot \prod_{j=1}^{p-1} \zeta_n^{q \cdot j} = n$

Claim: $\{ p, \dots (q-1)p \} \cap \{ q, \dots (p-1)q \} = \phi$.

If $a = pr = qs$: $p, q \mid a \Rightarrow pq \mid a$

But $a \in \{ 1, \dots pq-1 \}$ (contradiction)

$\therefore$ intersection $= \phi$

$\therefore 1 = \prod_{1 \le j \le n-1,\ p,q \nmid j} (1 - \zeta^j)$

No.: ..... Date: .....

$\Lambda = \{ k : 1 \le k < pq, \quad p, q \nmid k \}$; $1 \in \Lambda$

$\therefore \underbrace{(1-\xi)}_{\in \mathbb{Z}[\xi]} \cdot \underbrace{\prod_{r \in \Lambda \setminus \{1\}} (1-\xi^r)}_{\in \mathbb{Z}[\xi]} = 1 \quad \Rightarrow 1-\xi \in \mathbb{Z}[\xi]^\times$

(c) $(*)$: $P = \prod_{i=1}^{p-1} (1-\xi^i)$

$\forall\, i = 1, \dots p-1$: $1-\xi^i = 1 + \xi + \dots + \xi^{i-1} \Rightarrow 1-\xi \mid 1-\xi^i$

But $i = 1, \dots p-1 \Rightarrow \gcd(i, p) = 1$

$\therefore \exists\, a \in \mathbb{N},\ b \in \mathbb{Z}$ s.t $ai + bp = 1$

$\therefore \xi = \xi^{ai+bp} = \xi^{ai}$

$\therefore 1-\xi = 1-(\xi^i)^a = 1 + \xi^i + \dots \xi^{i(a-1)}$

$\therefore 1-\xi^i \mid 1-\xi$

$\therefore (1-\xi) = (1-\xi^i) \Rightarrow (P) = (1-\xi)^{p-1}$

Let $(1-\xi)$ factorise to $I_1 \dots I_r$, I_i are prime ideals

$\therefore (P) = \prod_{i=1}^{r} I_j^{p-1} = \left(\prod_{j=1}^{r} I_j \right)^{p-1}$

$\therefore$ If $\mathfrak{q} \trianglelefteq \mathcal{O}_K$ is prime, $\mathfrak{q} \mid (P) \Rightarrow \mathfrak{q} \in \{ I_1, \dots I_r \}$

$\therefore \mathfrak{q}^{p-1} \mid (P)$

$N((P)) = P^{[K:\mathbb{Q}]}$; $N(\mathfrak{q}) = P^a$, $a \ge 1$

$\therefore \underset{(p-1) \le}{a \cdot (p-1)} \le [K:\mathbb{Q}]$

But ξ root of $t^{p-1} + \dots + 1 \Rightarrow [K:\mathbb{Q}] \le p-1$

$\therefore$ Equality : $[K:\mathbb{Q}] = p-1$ ∎

No.: ..... Date: .....

4) (a) Let K be a number field: $\mathcal{O}_K$ be its integral ring.

$\Lambda = \{ \alpha_1, \dots \alpha_n \}$ its $\subseteq \mathcal{O}_K$ is an integral basis if

$\mathbb{Z} \cdot \Lambda = \mathcal{O}_K$ ✓

(b) Let $X \in K$ $\mathcal{O}_K = \mathbb{Q}(\sqrt{d})$: $X = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$

$[K : \mathbb{Q}] = 2$: Coefficient of min. poly. of X (over $\mathbb{Q}$)
determined by $Tr(X)$, $N(X)$

$\therefore X \in \mathcal{O}_K$ iff $Tr(X), N(X) \in \mathbb{Z}$

$Tr(X) = 2a \Rightarrow a = k_1/2$, $k_1 \in \mathbb{Z}$

$N(X) = a^2 - d b^2 \in \mathbb{Z}$

$\therefore k_1^2 - 4 d b^2 \in \mathbb{Z} \Rightarrow 4 d b^2 \in \mathbb{Z}$

Let $b = p/q$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $\gcd(p, q) = 1$:

$\therefore q^2 \mid 4 d p^2 \Rightarrow q^2 \mid 4d$; d is square free $\Rightarrow$

$q \mid 2 \Rightarrow q = 1$ or 2

$\therefore b = k_2/2$, $k_2 \in \mathbb{Z}$

$k_1^2 - d k_2^2 \equiv 0 \pmod 4$ iff

$(d \equiv 1 \pmod 4)$: $k_1^2 \equiv k_2^2 \pmod 4$ iff $k_1 \equiv k_2 \pmod 2$

$\therefore X \in \mathbb{Z} \cdot \{ 1, \frac{1}{2}(1 + \sqrt{d}) \}$

$(d \equiv 2, 3 \pmod 4)$: $k_1^2 \equiv 2 k_2^2 \pmod 4 \Rightarrow k_1 \equiv k_2 \equiv 0 \pmod 2$

$(d \equiv 3 \pmod 4)$: $k_1^2 \equiv -k_2^2 \pmod 4$ iff $k_1 \equiv k_2 \equiv 0 \pmod 2$

$\therefore d \equiv 1 \pmod 4$: $\mathcal{O}_K = \mathbb{Z} \cdot \{ 1, \frac{1}{2}(1 + \sqrt{d}) \}$

$\therefore d \equiv 2, 3 \pmod 4$: $\mathcal{O}_K = \mathbb{Z} \cdot \{ 1, \sqrt{d} \}$

No.: ..... Date: .....

(c) Dirichlet: $K = \mathbb{Q}(\sqrt{13})$, $\mathcal{O}_K^\times = \mu \times \mathbb{Z}^r$, μ are its the roots of units in K.

$K \subset \mathbb{R}$: $\mu = \{\pm 1\}$.

$\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1+\sqrt{13})]$

Fundamental Unit: Try $\alpha = 1+\omega$, $\omega = \frac{1}{2}(1+\sqrt{13})$

$N(\alpha) = (3/2)^2 - 13\cdot(1/4) = -1$ $\therefore$ Valid unit

If $1 < a+b\omega \leq \alpha$: $a, b \in \mathbb{Z}$

$1 > |a + b/2 - b/2\sqrt{13}| > 0$

$0 < 2a+b,\ b\sqrt{13} \leq 2 + 1/2 + \sqrt{13}/2$

$\therefore\ 0 < b \leq 1/2 + 5/2\sqrt{13} < 2.$

$\therefore$ ~~but~~ $0 < 2a < 3/2 + \sqrt{13}/2 \Rightarrow$ ~~$\Rightarrow$~~ $0 < a \leq 3/4 < \sqrt{13}/4$

$(a+1/2)^2 - 13/4 = 1$ or -1

$(2a+1)^2 = 17$ or $9 \Rightarrow 2a+1 \in \{\pm 3\}$

$a > 0$: $a = 1$.

$\therefore$ α is fundamental

(d) $X^2 + XY - 3Y^2 = N(X + Y\omega) = 17$

$\beta = 4 + \omega$, $N(\beta) = 17$ $\Rightarrow$ $(17) = (\beta)(\bar{\beta})$

Since $[K : \mathbb{Q}] = 2$, (17) have at most 2 prime ideal factors.

$\therefore$ (β), $(\bar{\beta})$ are the only ideals of norm 17.

$N((X+Y\omega)) = 17 \Rightarrow (X+Y\omega) = (\beta)$ or $(\bar{\beta})$

$\therefore$ $X + Y\omega = u\cdot\beta$ or $u\cdot\bar{\beta}$; $u \in \mathcal{O}_K^\times$

$N(X+Y\omega) = N(\beta) = N(\bar{\beta}) = 17 \Rightarrow N(u) = 1$

$\therefore$ $u = \pm\alpha^{2r}$, $r \in \mathbb{N}$ - (1)

$N(\beta\cdot u) = N(\bar{\beta}\cdot u) = 17$ for u of form (1)

$\therefore$ Solution: $\{(X,Y) \in \mathbb{Z}^2 :$ $X+\omega Y = \pm(1+\omega)^{2r}\cdot(4+\omega)$ or $\pm(1+\omega)^{2r}\cdot(4+\bar{\omega})$, $r \in \mathbb{Z}\}$

No.: Date:

Number Fields 2015

1.) (a) Let $f(t) = \sum_{k=0}^{n} c_k t^n$, $c_n = 1$:

Let $R = \mathbb{Z}[c_0, \dots c_{n-1}]$, $S = R(\alpha)$

$c_i \in O_k \Rightarrow c_i$ is integral over $\mathbb{Z} \Rightarrow$

$\therefore R/\mathbb{Z}$ is ~~an integral extension~~ $\Rightarrow$ Finitely generated extension

$\alpha \in S$ is integral over R as $f(\alpha) = 0$, $f \in R[t]$

$\therefore S/R$ is finitely generated $\Rightarrow S/\mathbb{Z}$ is finitely generated.

$\therefore \alpha \in S$ is integral over $\mathbb{Z}$: α is an algebraic integer.

If α is a root of h: α is a root of $h^n \in O_k[t]$

$\therefore \alpha$ is integral over $\mathbb{Z}$

Since h is monic: $h(t) = \prod_{a_i \in \text{Root}(h)} (t - a_i)$

$\therefore$ Coefficient of h is the symmetric polynomials of Root $(h) \Rightarrow$ sum/product of algebraic integer.

$\therefore$ Coefficients of h are algebraic integer

$\therefore h \in O_k[t]$

(b) $\text{Disc}(X^3 - X - 4) = (-1)(-1)^3 - 27(-4)^2 = 1 - 4 \times 27 = -107$ (prime)

Since $\Delta(1, \alpha, \alpha^2)$ is square-free :

$\{1, \alpha, \alpha^2\}$ is an integral basis.

No.: ..... Date: .....

2.) (a) Let $K = \mathbb{Q}(\sqrt{d}) : d \equiv 2, 3 \pmod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$

$\therefore \forall p \in \mathbb{N}$, p prime: Dedekind Criterion $\Rightarrow (p)$ = factorisation determined by $t^2 - d \pmod p$

$\therefore (p)$ is prime iff $t^2 - d$ is irreducible over $\mathbb{F}_p$

(b) $t^2 + 14 \equiv t^2 \pmod 2$

$t^2 + 14 \equiv t^2 - 1 \pmod 3$

Dedekind Criterion: $(2) = (2, \sqrt{-14})^2$

$(3) = (3, 1 + \sqrt{-14})(3, -1 + \sqrt{-14})$

Minkowski Bound: $(4/\pi)^1 \cdot 1/2 \sqrt{\Delta(K)}$ - (1)

$\Delta(K) = \operatorname{disc}(t^2 + 14) = -4 \cdot 14$

$(1) = (4/\pi)\sqrt{14} = \sqrt{14 \times 16/9} = \sqrt{160 + 64/9} = \sqrt{224/9} < \sqrt{25} = 5$

$\therefore Cl_K$ elements represented by ideals of norms < 2

$\therefore Cl_K$ generated by prime ideals of $(2), (3)$

$(2, \sqrt{-14})(3, -1 + \sqrt{-14})^2 = (2, 2 + \sqrt{-14})(3, 2 + \sqrt{-14})^2$

$= (3, 2 + \sqrt{-14})(6, \underbrace{3(2 + \sqrt{-14}), 2(2 + \sqrt{-14}), (2 + \sqrt{-14})^2}_{\text{Generates } 2 + \sqrt{-14}})$

$= (18, 3(2 + \sqrt{-14}), (2 + \sqrt{-14})^2) = (18, 3(2 + \sqrt{-14}), -10 + 4\sqrt{-14})$

$= (18, \underbrace{8 + 4\sqrt{-14}}_{4(2 + \sqrt{-14})}, 3(2 + \sqrt{-14})) = (18, 2 + \sqrt{-14}) = (2 + \sqrt{-14})$

as $2 + \sqrt{-14} \mid 18 = N(2 + \sqrt{-14})$

If $N((x + y\sqrt{-14})) = 2$: $(x, y \in \mathbb{Z})$ $x^2 + 14y^2 = 2 \Rightarrow y = 0 \Rightarrow$ (No sol. of x)

$\therefore (2, \sqrt{-14})$ is not principal

$Cl_K = \langle [(2, \sqrt{-14})], [(3, -1 + \sqrt{-14})] \rangle$; $[(2, \sqrt{-14})] = [(3, -1 + \sqrt{-14})]^2 \neq e$.

$\therefore \operatorname{ord}([(3, -1 + \sqrt{-14})]) = 4$, $Cl_K = \langle [(3, -1 + \sqrt{-14})] \rangle \cong C_4$

No.: Date:

4) (a) Let $r = |\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})|$, $n = |\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})|$,

$s = \frac{1}{2}(n-r)$ (# of non-real embeddings $\hookrightarrow \mathbb{C}$)

$\mu = \{ x \in K : x \text{ is a root of unity} \}$

$$\mathcal{O}_K^{\times} \cong \mu \times \mathbb{Z}^{r+s-1}$$

If $K = \mathbb{Q}(\sqrt{d})$:

(Embedding)

If $d < 0$: $\sqrt{-d} \to \pm\sqrt{-d}$ (non-real)

$\therefore s = 1, \ r = 0.$

$\therefore$ If $\mathcal{O}_K^{\times} = \{ x \in K : x \text{ is a root of unity} \}$

If $d > 0$: ($K \subseteq$ If $\mathbb{R}$); All embeddings are real: $\sqrt{d} \to \pm\sqrt{d} \in \mathbb{R}$

$\therefore$ If $r = 2, \ s = 0.$

Since $K \subseteq \mathbb{R}$: ± 1 are the only roots of unity

$$\mathcal{O}_K^{\times} \cong \{\pm 1\} \times \mathbb{Z}$$

(b) ε is a fundamental unit if $\varepsilon > 1$, smallest unit that is > 1

Try $d = 5 + \sqrt{26}$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{26}]$ as $26 \equiv \vec{0} \pmod 2$

If $1 < a + b\sqrt{26} \leq d$: $a, b \in \mathbb{Z}$, $a^2 - 26b^2 \in \{\pm 1\}$

$\therefore 1 > |a - b\sqrt{26}| \geq 0$:

$\therefore 0 < 2a, \ 2b\sqrt{26} \leq 6 + \sqrt{26}$

$\therefore 0 < b \leq 3/\sqrt{26} + 1/2 \leq 1/3 + 3/5 < 2.$

$\therefore b = 1$: $a^2 - 26 \in \{\pm 1\} \Rightarrow (a > 0) \ a = 5.$

$\therefore d$ is fundamental

No.: Date:

Norms of ideal 10:

Dedekind Criterion: $\mathcal{O}_K = \mathbb{Z}[\sqrt{26}]$

$t^2 - 26 \equiv t^2 \pmod 2$
$\equiv (t-1)(t+1) \pmod 5$

$(2) = (2, \sqrt{26})^2$
$(5) = (5, \sqrt{26}-1)(5, \sqrt{26}+1)$

$\therefore \exists$ 2 ideals of norm 10: $(2, \sqrt{26})(5, \sqrt{26}-1) = (2, \sqrt{26}+4)\cdot(5, \sqrt{26}+4)$

$= (4+\sqrt{26})$

$(2, \sqrt{26})\cdot(5, \sqrt{26}+1) = (2, \sqrt{26}+6)(5, \sqrt{26}+6)$

$= (6+\sqrt{26})$

$\therefore N(x + \sqrt{26}y) \in \{\pm 10\}$ iff $(x+\sqrt{26}y) = (4+\sqrt{26})$ or $(6+\sqrt{26})$

iff $x + \sqrt{26}y = u\cdot(4+\sqrt{26})$ or $u\cdot(6+\sqrt{26})$, $u \in \mathcal{O}_K^*$

$\therefore$ Solutions:

$\{(x,y) \in \mathbb{Z}^2 : x + \sqrt{26}y = \in \{\pm(5+\sqrt{26})^n(4+\sqrt{26}), \pm(5+\sqrt{26})^n(6+\sqrt{26}) : n \in \mathbb{Z}\}\}$

No.: Date:

Number Fields 2017

1) (a) Let $\text{Root}(f) = \{ \alpha_1, \dots \alpha_n \}$

$$\text{Disc}(f) = (-1)^{\binom{n}{2}} \prod_{\substack{1 \le i,j \le n \\ i \ne j}} (\alpha_i - \alpha_j)$$

$$f(t) = \prod_{i=1}^{n} (t - \alpha_i) \qquad \text{(Assume } f \text{ monic, else not true)}$$

$$f'(t) = \sum_{i=1}^{n} \prod_{j \ne i} (t - \alpha_j) \; : \; f'(\alpha_i) = \prod_{j:\, j \ne i} (\alpha_i - \alpha_j)$$

If f is irreducible: $N_{G(\alpha)/G}(f'(\alpha_1)) = \prod_{i=1}^{n} f'(\alpha_i)$

$$\therefore \text{Disc}(f) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} \prod_{j \ne i} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} N_{G(\alpha_1)/G}(f'(\alpha_1))$$

(b) Let A, B be formal variables:

$$f(t) = t^n + At + B \in G(A,B)[t]$$

Gauss Lemma: f is irreducible iff f irreducible over $\mathbb{Z}[A,B][t]$

$f = t \cdot A + (t^n + B)$, ~~gcd $t \mid t^n + B$~~ $= t, t^n + B$ coprime over $\mathbb{Z}[B][t]$; f linear in A $=$ f irreducible over $\mathbb{Z}[A,B][t]$

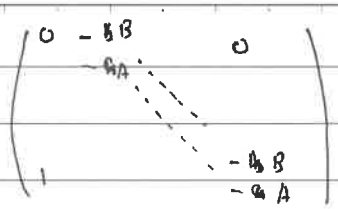
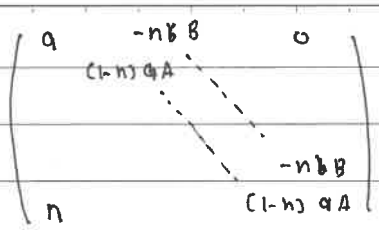
$\therefore$ f irreducible.

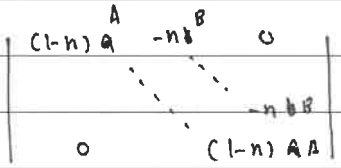
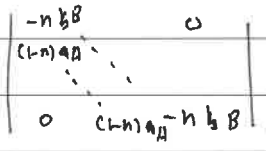
$$\therefore \text{Disc}(f) = (-1)^{\binom{n}{2}} N_{G(\alpha)/G}(f'(\alpha))$$

$f'(\alpha)$ action on $G \cdot \{ 1, \dots \alpha^{n-1} \}$

$f'(t) = nt^{n-1} + a$

No.: Date:

$A \otimes I_n + n$  $=$ 

Det: $\otimes A$  $+n(-1)^{n-1}$ 

$= A \otimes^n (1-n)^{n-1} + n(-1)^{n-1} (-1)^{n-1} (n \otimes B)^{n-1}$

$\therefore$ Disc $(f) = (-1)^{\binom{n}{2}} \left((-1)^{n-1} (1-n)^{n-1} A^n + n^n \cdot B^{n-1} \right)$

Sub: $A \to a$, $B \to a$

Disc $(t^n + at + b) = (-1)^{\binom{n}{2}} \left((1-n)^{n-1} A^n + n^n B^{n-1} \right)$ //

cc! $(\mathbb{F}_2)$: f has no roots

If $f(x) = (x^2 + ax + b)(x^2 + cx + d)$, $bd = 1 \Rightarrow b = d = 1$

$a + c = 0$
$ad + bc = a + c = 1$ } No solution

$\therefore$ f irreducible over $\mathbb{F}_2 \Rightarrow$ irreducible over $\mathbb{A} \otimes \mathbb{Z}$
$\Rightarrow$ irreducible over $\mathbb{Q}$

Disc $(f) = +\left((-3)^3 - 4^4 \right) = 256 - 27 = 227$ is prime.

$\therefore \Delta(1, \alpha, \ldots \alpha^3)$ is square free (α root of f)

$\therefore \{1, \ldots \alpha^3\}$ is an integral basis

$\therefore \mathcal{O}_K = \mathbb{Z}[\alpha]$ //

No.: Date:

2.) (a) $\varepsilon \in \mathcal{O}_K^\times$ is fundamental if $\varepsilon > 1$, ε is minimal of elements in $\mathcal{O}_K^\times > 1$.

If $1 < a + b\sqrt{6} \leq 5 + 2\sqrt{6}$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ as $K = \mathbb{Q}(\sqrt{6})$ as $6 \equiv 2 \pmod 4$

$a, b \in \mathbb{Z}$, $|a^2 - 6b^2| = 1$;

$\therefore 1 > |a - b\sqrt{6}| > 0$.

$\therefore 0 < 2a,\ 2b\sqrt{6} \leq 6 + 2\sqrt{6} \Rightarrow 0 < b \leq \frac{3}{\sqrt{6}} + 1 < 3$

$\therefore b = 1$ or 2.

If $b = 1$: $a^2 - 6 = 1$ or -1 (reject)

If $b = 2$: $a^2 - 24 = 1$ or $-1 \Rightarrow a = 5$.

$\therefore 5 + 2\sqrt{6}$ is a fundamental unit.

(b) $-55 \equiv 1 \pmod 4$; Let $\omega = \frac{1}{2}(1 + \sqrt{-55})$, $K = \mathbb{Q}(\sqrt{-55})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$

Disc(K): $4\omega^2 - 4\omega + 1 + 55 = 0 \Rightarrow \omega^2 - \omega + 14 = 0$

$\therefore$ Disc$(1, \omega) = 1 \cdot -4 \cdot 14 = -55$

$\therefore$ Disc$(K) = -55$.

Minkowski Bound: $\left(\frac{4}{\pi}\right) \cdot \left(\frac{1}{2}\right) \sqrt{|-55|} = \sqrt{55 \cdot \frac{4}{\pi^2}} < \sqrt{\frac{220}{9}} < 5$.

$\therefore Cl_K$ elements represented by ideals of norm ≤ 4.

$\therefore Cl_K$ generated by prime ideal factors of (2), (3)

Dedekind Criterion: $t^2 - t + 14 \equiv t(t-1) \pmod 2$

$t^2 - t + 14 \equiv t^2 - t - 1 \pmod 3$ (irreducible)

$\therefore Cl_K = \langle (d) \rangle$, $d = (2, \omega + 1) = (2, \omega + 1)$

No.: Date:

$(d)^2 = (2, \omega+3)^2 = (4, 2(\omega+3), \omega^2+6\omega+9) = (4, 2(\omega+3), 7\omega-5)$

$= (4, 2(\omega+3), 7\omega-5-4\cdot\omega+3\cdot 4) = (4, 2(\omega+3), 3(\omega+3))$

Generate $\omega+3$

$= (4, \omega+3)$

$(4, \omega+3)\cdot(2, \omega+3) = (8, 2(\omega+3), \omega^2+6\omega+9) = (8, 2(\omega+3), 7\omega-5)$

$= (8, 2\omega+6, \omega-5-8)$

$(2, \omega+1)^2 = (4, 2(\omega+1), \omega^2+2\omega+1) = (4, 2(\omega+1), 3\omega-13)$

$= (4, 2(\omega+1), 3(\omega+1)) = (4, (\omega+1))$

$(2, \omega+1)^4 = (16, 4(\omega+1), 3\omega-13) = (16, 4(\omega+1), 3(\omega+1)) = (16, \omega+1)$

$= (\omega+1)$ as $\omega+1 \mid 16 = N(\omega+1)$

If $(2, \omega+1)^2$ is principal: $\exists x, y \in \mathbb{Z}$ s.t.

$N(x+y\omega) = 4$

$\therefore (x+y/2)^2 + 55/4\, y^2 = 4 \Rightarrow (2x+y)^2 + 55y^2 = 16$

$\therefore y = 0 \Rightarrow x = \pm 2.$

But $(2, \omega+1)^2 \neq (2) \Rightarrow$ reject $(x, y) = (\pm 2, 0)$

$\therefore (2, \omega+1)$ not principal $\Rightarrow \mathrm{ord}([(2, \omega+1)]) \neq 1, 2.$

$\therefore (2, \omega+1)^4 = (\omega+1) \Rightarrow \mathrm{ord}([(2, \omega+1)]) = 4.$

$\therefore Cl_k = \langle [d] \rangle \cong C_4$ //

No.: Date:

4) (a) Let $(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ be prime ideal factorisation of (p)

$\mathfrak{p}$ is inert if (p) is prime; $\mathfrak{p}$ splits completely if $e_1 = \dots = e_r = 1$;

$\mathfrak{p}$ ramified if $\exists\, e_i$ s.t. $e_i > 1$

(a) If (2) split completely:

Dedekind Criterion: Let $f \in \mathbb{Z}[t]$ be minimal polynomial of α.

$f \pmod p$ must factorise into $[K:\mathbb{Q}]$ distinct factors $\Rightarrow$

$\exists\, [K:\mathbb{Q}]$ distinct roots of $f \pmod p$ in $\mathbb{F}_2$

$\therefore [K:\mathbb{Q}] \leq |\mathbb{F}_2| = 2 < [K:\mathbb{Q}]$ (contradiction)

$\therefore (2)$ will not split completely

(b) If $d \equiv 2, 3 \pmod 4$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$: $\sqrt{d}$ minimal polynomial $= t^2 - d$

If $p \mid d$: $t^2 - d \equiv t^2$ or $(t-1)^2 \pmod 2$

$\therefore (2)$ 2 ramifies

If $d \equiv 1 \pmod 4$: $\omega = \frac{1}{2}(1 + \sqrt{d})$

$4\omega^2 - 4\omega + 1 = d \Rightarrow \omega^2 - \omega + \frac{1-d}{4} \ni \omega$

If $d \equiv 1 \pmod 8$: $\frac{1-d}{4} \equiv 0 \pmod 2$

$\therefore (2) = (2, \omega) \cdot (2, \omega - 1)$ $\Rightarrow$ Splits completely.

If $d \equiv 5 \pmod 8$: $\frac{1-d}{4} \equiv 1 \pmod 2$.

$t^2 + t + 1$ is irreducible in $\mathbb{F}_2$ $\Rightarrow$ (2) is inert.

No.: ..... Date: .....

No.: Date:

Number Fields 2017

1.) (a) Let $\alpha \in \underset{\sim}{\alpha}$, $\alpha \neq 0$: f be minimal polynomial of α.

$f(x) = \sum_{k=0}^{n} a_k x^k$ is irreducible; $f \nmid t$ as $\alpha \neq 0$.

$\therefore a_0 \overset{a_0 a_n}{a_k} = 0 \Rightarrow t \mid f$ (reject)

$a_k \; a_0 = \sum_{k=1}^{n} -a_k \alpha^k \in \underset{\sim}{\alpha}$ ($\alpha \in \underset{\sim}{\alpha}$)

$\therefore a_0 \in \mathbb{Z} \cap \underset{\sim}{\alpha} \Rightarrow \neq \phi$ ($\mathbb{Z} \cap \underset{\sim}{\alpha}$)

(b) Since $\exists\, m \in \mathbb{Z} \cap \underset{\sim}{\alpha}$, $m \neq 0$: $(m) \subseteq \underset{\sim}{\alpha}$

$\therefore \left| \mathcal{O}_L/(m) \right| \geq \left| \mathcal{O}_L/\underset{\sim}{\alpha} \right|$, $m^{[L:G]} = \left| \mathcal{O}_L/(m) \right| \geq \left| \mathcal{O}_L/\underset{\sim}{\alpha} \right|$

$\Rightarrow \left| \mathcal{O}_L/\underset{\sim}{\alpha} \right| < \infty$ (Finite)

Since $\underset{\sim}{\alpha} \triangleleft \mathcal{O}_L$: $\mathcal{O}_L/\underset{\sim}{\alpha}$ is a ring $\Rightarrow$ + structure operation forms an finite abelian group.

(c) Let $\underset{\sim}{\alpha} = \mathbb{Z} \cdot \{ \alpha_1, \ldots \alpha_n \}$:

A_{ij} be defined as: $x \alpha_j = \sum_{i=1}^{n} A_{ij} \alpha_i$

$A_{ij} \in \mathbb{Z}$ as $x \cdot \underset{\sim}{\alpha} \subseteq \underset{\sim}{\alpha} = \mathbb{Z} \cdot \{ \alpha_1, \ldots \alpha_n \}$

$\therefore$ x-multiplication is represented by matrix A, Cayley Hamilton Theorem $\Rightarrow \alpha_x$ is a root of $\det(A - tI)$, α_x is linear map of x-multiplication

$\therefore x$ is a root of $\det(A - tI) \cdot (-1)^{[L:G]}$ (monic polynomial in $\mathbb{Z}[t]$) $\Rightarrow x$ is integral

$\therefore x \in \mathcal{O}_L$

No.: ..... Date: .....

(d) $(b, \alpha)(b, \bar{\alpha}) = (b^2, b\alpha, b\bar{\alpha}, N(\alpha))$

$= (b^2, b\alpha, b \cdot Tr(\alpha), N(\alpha))$

Let $c = gcd(b^2, b\,Tr(\alpha), N(\alpha))$: $c \in (b, \alpha)\cdot(b, \bar{\alpha})$

$N(b\alpha/c) = \frac{b^2}{c}\frac{N(\alpha)}{c} \in \mathbb{Z}$

$Tr(b\alpha/c) = b/c \cdot Tr(\alpha) = \frac{1}{c} \cdot b\,Tr(\alpha) \in \mathbb{Z}$

$[L : G] = 2 \Rightarrow b\alpha/c \in \mathcal{O}_L$

$\therefore b\alpha \in (c) \Rightarrow (b, \alpha)(b, \bar{\alpha}) = (c)$ ✱

2.) (a) $\Phi : \mathcal{O}_L^{\times} \to \mathbb{R}^{r+s}$; $\sigma_1, \dots \sigma_r$, be real embeddings

$\sigma_{r+1}, \dots \sigma_{r+s}$ be representative of each complex embedding pair.

$\Phi(x) = (\log(|\sigma_1(x)|), \dots \log(|\sigma_r(x)|), 2\log(|\sigma_{r+1}(x)|), \dots 2\log(|\sigma_{r+s}(x)|))$

$a, b \in (0, \infty)$:

1 $\log(ab) = \log(a) + \log(b) \Rightarrow \Phi$ is a homomorphism

But $x \in \mathcal{O}_L^{\times}$: $N(x) = 1 \Rightarrow \sum_{i=1}^{r+s} \Phi(x)_i = 0$.

$\therefore Im(\Phi) \leq \cong$ Subgroup of $\mathbb{R}^{r+s-1}$

If $\Phi(x) = 0$: $\forall \sigma \in G = Hom_{\mathbb{Q}}(L, \mathbb{C})$, $|\sigma(x)| = 1$

Claim: x is a root of unity.

$f_k(t) = \prod_{g \in G} (t - g(x)^k)$

$\forall g \in G$: $g \cdot f_k = f_k \Rightarrow f_k \in G[t]$

Since coefficients of f are sum / product of alg. integers, coefficients are integral

No.: Date:

$\therefore f_k \in \mathbb{Z}[t]$

Let $M = \max\left\{ \binom{|G|}{i} : 0 \le i \le |G| \right\}$: Coefficients of f_k are symmetric polynomials in $(g(X^k))_{g \in G}$

$\therefore$ Bounded in magnitude by M

Since $\exists$ finitely distinct $f \in \mathbb{Z}[t]$ of degree $|G|$, coefficients bounded in magnitude by M:

$\exists\ k_1 < k_2$ s.t. ~~$f(k_1)$~~ $= f_{k_1} = f_{k_2}$

$\therefore X^{k_1} = G(X^{k_2}) \Rightarrow G(X) = X^{k_1/k_2}$

$G^{|G|} = id : X = X^{(k_1/k_2)^n} \Rightarrow X^{k_2^n - k_1^n} = 1$

$\therefore X$ is a root of unity.

$\therefore \ker(\Phi) = \{ x \in \mathcal{O}_L : x \text{ is a root of unity} \}$ is finite.

Consider: $\mathcal{O}_L^{\times} \xrightarrow[\Phi_1]{} \mathcal{O}_L \xrightarrow[L]{} \mathbb{R}^{r+s}$

$\Phi_1(x) = x, \quad L(x) = (\log(|\sigma_1(x)|), \dots \log(|\sigma_r(x)|), 2\log(|\sigma_{r+1}(x)|), \dots 2\log(|\sigma_{r+s}(x)|))$

$\therefore \Phi = L \cdot \Phi_1$

Claim : $\mathrm{Im}(\Phi)$ is discrete.

If $K \subseteq \mathbb{R}^{r+s}$ is cone-compact: $\Phi^{-1}(K) = \Phi_1^{-1} \cdot (L^{-1}(K))$

$\mathcal{O}_L$ is discrete : $L(\mathcal{O}_L)$ discrete $\Rightarrow L^{-1}(K)$ is ~~discrete~~ finite.

$\therefore \Phi^{-1}(K)$ is discrete.

$\therefore \mathrm{Im}(\Phi)$ is a discrete subgroup of $\mathbb{R}^{s+r}$ $\{ x \in \mathbb{R}^{s+r} : \sum x_i = 0 \}$

$\cong \mathbb{R}^{r+s-1}$

No.: Date:

(b1) $\mathcal{O}_k^\times \cong \{\pm 1\} \times \mathbb{Z}$ (Dirichlet Unit Theorem)

If $x \in \mathcal{O}_k^\times$, $N(x) = 1$ or -1; If $N(x) = -1$:

$\exists\, a, b, c \in \mathbb{Z}$ s.t $a^2 - d b^2 = -c^2$, $c \neq 0$.

(mod p): $(a/c)^2 = -1 \pmod p \Rightarrow -1$ is a square.

But $p \equiv 3 \pmod 4 \Rightarrow -1$ is not a square.

$\therefore$ Contradiction

$\therefore N(x) = 1$

Pick $k = \mathbb{Q}(\sqrt{2})$:

$N(1+\sqrt{2}) = 1^2 - 2 = -1$ ✱

No.: Date:

4.) (a) Claim: $K = \mathbb{Q}(\sqrt{d})$, d square-free; $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$.
$= \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ if $d \equiv 1 \pmod 4$

Let $x = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$:

$Tr(x) = 2a + 0 \Rightarrow a \in \frac{1}{2}\cdot\mathbb{Z}$

$N(x) = a^2 - d b^2$

$\therefore 4d b^2 \in \mathbb{Z}$; $b = p/q$, $\gcd(p,q) = 1 \Rightarrow$

$q^2 \mid 4d$; (d square-free) $\Rightarrow q^2 \mid 4$ $\therefore q = 1$ or 2.

i. $\therefore 4a^2 - 4d b^2 \equiv 0 \pmod 4$

If $d \equiv 1 \pmod 4$: $(2a) \equiv (2b) \pmod 4$ $\therefore k_1 + k_2 \cdot \frac{1}{2}(1+\sqrt{d})$

If $d \equiv 2, 3 \pmod 4$: $(2a) \equiv 0 \pmod 4 \Rightarrow (2b) \equiv 0 \pmod 4$

$(2a) \equiv 1 \pmod 4 \Rightarrow d\cdot(2b)^2 \equiv 1 \pmod 4$ (reject)

$\therefore k_1 + k_2\sqrt{d}$.

(b) Let $x \in \mathcal{O}_L$, $x = a_1 + b_1\sqrt{2} + c_1\sqrt{\delta} + d_1\sqrt{2\delta}$, $2\delta \equiv 2 \pmod 4$

$Tr_{L/\mathbb{Q}(\sqrt{2})}(x) = 2a_1 + 2b_1\sqrt{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$

$\therefore a_1, b_1 \in \frac{1}{2}\cdot\mathbb{Z}$

$Tr_{L/\mathbb{Q}(\sqrt{\delta})}(x) = 2a_1 + 2c_1\sqrt{\delta}$; $\delta \equiv 3 \pmod 4 \Rightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{\delta})} = \mathbb{Z}[\sqrt{\delta}]$

$\therefore a_1, c_1 \in \frac{1}{2}\mathbb{Z}$

$Tr_{L/\mathbb{Q}(\sqrt{2\delta})}(x) = 2a_1 + 2d_1\sqrt{2\delta} \in \mathcal{O}_{\mathbb{Q}(\sqrt{2\delta})} = \mathbb{Z}[\sqrt{2\delta}]$

$\therefore d_1 \in \frac{1}{2}\mathbb{Z}$

Let $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, $d = 2d_1$

$N_{L/\mathbb{Q}(\delta)}(x) = (a_1 + c_1\sqrt{\delta})^2 - 2(b_1 + d_1\sqrt{2\delta})^2$

$= (a_1^2 + \delta c_1^2 - 2b_1^2 - 2d_1\sqrt{2}(*\delta)) + 2a_1c_1\sqrt{\delta} - 4b_1d_1\sqrt{(2\delta)}$

$\in \mathcal{O}_{\mathbb{Q}(\delta)}$

No.: ..... Date: .....

$\therefore$ ~~$a_1^2 + 8c_1$~~ $a^2 + 8c^2 - 2(b^2 + 8d^2) \equiv 0 \pmod 4$

$2ac \cdot 8 - 4bd \equiv 0 \pmod 4$

$\therefore ac \equiv 0 \pmod 2$

$a^2 - 8c^2 \equiv 2(b^2 + 8d^2) \pmod 4$

$2 \mid a^2 - c^2 \Rightarrow a \equiv c \pmod 2 \Rightarrow a \equiv c \equiv 0 \pmod 2$

$\therefore b^2 - d^2 \equiv 0 \pmod 2 \Rightarrow b \equiv d \pmod 2$

$\therefore \chi = a + c\sqrt{8} + b\sqrt{2} + d \cdot \frac{1}{2}(b + \sqrt{2}) \cdot (1 + \sqrt{d})$

$\therefore \{1, \sqrt{2}, \sqrt{8}, \frac{1}{2}(\sqrt{2} + \sqrt{28})\}$ is an integral basis

(b) Minkowski Bound: $(4/\pi) \cdot \frac{1}{2}\sqrt{|\Delta|}$ $\quad (4/\pi)\sqrt{14} \leq \sqrt{\frac{224}{9}} < \sqrt{25}$

$|\Delta| = 4 \cdot 14$

$\therefore$ Suffice to consider ideals of norms ≤ 4

$\therefore Cl_K$ generated by prime ideal factors of (2) (3)

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$: $t^2 + 14 \equiv t^2 \pmod 2$

$\equiv t^2 - 1 \pmod 3$

$\therefore (2) = (2, \sqrt{-14})^2$

$(3) = (3, 1 + \sqrt{-14})(3, \sqrt{-14} - 1)$

$(3, \sqrt{-14} + 2)^2 \cdot (2, \sqrt{-14} + 2) = (3, \sqrt{-14} + 2)(6, 2 + \sqrt{-14})$

$= (18, 3(2 + \sqrt{-14}), 18 + 4\sqrt{-14}) = (18, \underbrace{3(2 + \sqrt{-14})}_{\text{generates } 2 + \sqrt{-14}}, 8 + 4\sqrt{-14})$

$= (18, 2 + \sqrt{-14}) = (2 + \sqrt{-14})$ $\quad (N(2 + \sqrt{-14}) = 18 \Rightarrow 18 \in (2 + \sqrt{-14}))$

$Cl_K = \langle \underbrace{(2, \sqrt{-14})}_{\alpha}, \underbrace{(3, \sqrt{-14} - 1)}_{\beta} \rangle$

$\alpha^2 \beta^2 = (2 + \sqrt{-14}) \Rightarrow [\alpha] = [\beta]^{-2}$ $\therefore$ $[\beta]^4 = e$.

No.: Date:

$N(\beta') = 9$: $\beta' \neq (3)$

If $x^2 + 14y^2 = 9$, $x, y \in \mathbb{Z}$: ($\mathcal{O}_{\mathbb{Q}(\sqrt{-14})} = \mathbb{Z}[\sqrt{-14}]$)

$|y| = 0 \Rightarrow x = 3$ or -3 (reject)

$\therefore$ β' not principal $\Rightarrow$ ord $([\beta]) = 4$

$\therefore$ $Cl \cong C_4 = \langle [\beta] \rangle$ //

No.: ..... Date: .....

No.: Date:

Number Fields 2018

1.) (a) Let q be a prime, $q \mid n^2+n+m$:

Min. polynomial of $\omega = \frac{1}{2}(1+\sqrt{-p})$: $f(t) = t^2 - t + m$.

$\therefore f(-n) \equiv 0 \pmod q$

$\mathcal{O}_L = \mathbb{Z}[\omega]$: Dedekind's Criterion $\Rightarrow (q) = (q, \omega+n)\cdot(q, n+\bar{\omega})$

$\therefore (q, \omega+n)\cdot(q, \bar{\omega}+n) \mid (n^2+n+m) = (n+\omega)\cdot(n+\bar{\omega})$

Since $(q, \omega+n)$, $(q, \bar{\omega}+n)$ are prime ideals, one of them must be a factor of $(n+\omega)$

$\therefore$ ~~$q \le N((q, \omega+n)) = N((q, \bar{\omega}+n)) \mid N((n+\omega)) = n^2+n+m$~~

Suppose $q < m$: Since class group is trivial, $(q, \omega+n) = (x+y\omega)$

$x, y \in \mathbb{Z}$

$\therefore q = N((x+y\omega)) = (x+y/2)^2 + p\,y^2/4 \quad -(1)$

If $|y| \ge 1$: $(1) \ge p/4 = m - 1/4 \Rightarrow q \ge m$ (reject)

$\therefore y = 0 \Rightarrow q = x^2$ (reject, q is prime)

$\therefore q \ge m$.

But if n^2+n+m is composite, $\exists$ prime factor $\le \sqrt{n^2+n+m} < m$

$\therefore n^2+n+m$ is prime.

(b) Minkowski Bound: $\mathrm{Disc}(L) = \mathrm{Disc}(t^2-t+41) = 1-4(41) = -163$

$$\left(\frac{\pi 4}{4\pi}\right)\cdot\frac{1}{2}\sqrt{163} = \left(\frac{\pi 4}{4\pi}\right)\sqrt{40+3/4} = \sqrt{\frac{163\times 4}{\pi^2}} < \sqrt{\frac{652}{9}\,\frac{652}{}}$$

$$= \sqrt{72+4/9} < 9$$

$\therefore$ Suffice to consider ideals of norms $\le 8 \Rightarrow$ Suffice to consider ~~idea~~ prime ideal factors of ~~the~~ (2), (3), (5), (7)

No.: Date:

$\omega = \frac{1}{2}(1+\sqrt{-163})$:

$\mathbb{Z}[\omega] = \mathcal{O}_L$: (Dedekind) $t^2-t+41 \equiv t^2+t+1$ irreducible mod 2)

$\equiv t^2-t-1$ irreducible mod 3)

$\equiv t^2-t+1$ irreducible mod 5)

$\equiv t^2-t-1$ irreducible mod 7)

$\therefore \mathcal{O}_K(p)$ is prime for $p = 2, 3, 5, 7$.

$\therefore Cl_K = \langle (p) : p \in \{2,3,5,7\} \rangle$ is trivial.

2.) (a) $[L : \mathbb{Q}(\omega)]$ = degree of minimal polynomial of ω over $\mathbb{Q}$

Let $f(t) = \frac{t^p-1}{t-1} = \sum_{k=0}^{p-1} t^k \doteq \frac{(s+1)^p-1}{s} = \sum_{k=1}^{p} \binom{p}{k} s^{p-1}$

Since $p \mid \binom{p}{1}, \dots \binom{p}{p-1}$, $p \nmid \binom{p}{p} = 1$, $p^2 \nmid \binom{p}{1} = p$:

Eisenstein criterion $\Rightarrow$ f is irreducible over S $\Rightarrow$ irreducible over t.

$\therefore f$ is the minimal polynomial of ω $\Rightarrow$ $[L : \mathbb{Q}(\omega)] = \deg(f) = p-1$.

(b) $\mathrm{Disc}(1, \dots \omega^{p-2}) = \mathrm{Disc}(\text{Min. poly of } \omega) = (-1)^{\binom{p-1}{2}} N_{L/\mathbb{Q}}(f'(\omega))$

$f'(t) = \frac{(t-1)\cdot p t^{p-1} - (t^p-1)}{(t-1)^2}$; $f'(\omega) = \frac{p\omega^{p-1}}{\omega-1} = \frac{-p}{\omega(1-\omega)}$

$N(p) = p^{p-1}$

$N(\omega) = (-1)^{p-1}$.

$N(1-\omega) = f(1) = p$

$\mathrm{Disc}(1, \dots \omega^{p-2}) = (-1)^{\binom{p-1}{2}} p^{p-1}/p$

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

No.: Date:

(c) $L = \mathbb{Q}(\omega)$, $K = \mathbb{Q}(\sqrt{5}) = L \cap \mathbb{R}$

Let $u \in L$ be a unit: We know $(p) = \prod_{k=1}^{p-1} (1-\omega^k) = (1-\omega)^{p-1}$

$\mathcal{O}_L/(1-\omega) \cong \mathbb{F}_p$

Let σ be complex conjugation map: $\sigma \cdot (1-\omega) = (1-\omega^{-1}) = (1-\omega)$

$\therefore \sigma$ defines an automorphism on $\mathcal{O}_L/(1-\omega) = \{0, \dots p-1\}$

$\therefore \sigma$ acts trivially

Since Galois group of L is abelian: $\forall\ \phi \in Gal(L/\mathbb{Q})$,

$\phi(\overline{x}) = \overline{\phi(x)}$

$\therefore |\phi(u/\bar{u})| = 1 \quad (\forall \phi \in Gal(L/\mathbb{Q})) \Rightarrow u/\bar{u}$ is a root of unity in $\mathbb{Q}(\omega) \Rightarrow u/\bar{u} = (-1)^b \omega^{2k}$, $b, k \in \mathbb{Z}$

But $u \equiv \bar{u} \pmod{1-\omega}$: $u = \bar{u}(-1)^b \omega^{2k} \equiv \bar{u}(-1)^b \equiv (-1)^b u$

$\therefore u(1 \pm (-1)^b) \equiv 0 \pmod{1-p}$

u is a unit $\Rightarrow u \neq 0$ in $\mathcal{O}_L/(1-\omega) \Rightarrow 1 + (-1)^b \equiv 0$

$\therefore b$ is not a odd.

$u = \bar{u} \cdot \omega^{2k} \Rightarrow \overline{u\omega^{-k}} = \bar{u}\omega^k = u\omega^{-k}$.

$\therefore u\omega^{-k} \in \mathcal{O}_K^\times$

Dirichlet: $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbb{Z}^n$

~~Let $\varepsilon = 2+\sqrt{5}$ ... If $1 < a+b(\frac{1}{2}(1+\sqrt{5}$~~

Let $d = \frac{1}{2}(1+\sqrt{5})$: $d > 1$, d is a unit.

If $1 < x + d \cdot y \leq d$, $x, y \in \mathbb{Z}$:

$1 > |(x + y/2) - y/2\sqrt{5}| > 0$

$\therefore 0 < 2x+y, \ \sqrt{5}y \leq 3/2 + \sqrt{5}/2$.

No.: Date:

$\therefore y = 1, \quad x = u$

α is a fundamental unit

$\therefore u \cdot \omega^{-k} \in \{ \pm \alpha^n : n \in \mathbb{Z} \}$

$\therefore u \in \{ \pm \omega^k \alpha^n : k, n \in \mathbb{Z} \} \subseteq \mathcal{O}_L^\times$

$\therefore \mathcal{O}_L^\times = \{ \pm \omega^k \alpha \left(\frac{1+\sqrt{5}}{2} \right)^n : k, n \in \mathbb{Z} \}$ //

4.) (a) $N(C_m) = m^n$ ~~deg~~ $[L:\mathbb{Q}]$

$f(t) = \sum_{k=0}^{n-1} t^k \quad \therefore f(1) = n = \prod_{k=1}^{n-1} (1 - \sqrt[n]{m}^k)$

$\therefore$ 6 $N(C_m) = m^{[L:\mathbb{Q}]} = N((\alpha)^n) = N((\alpha))^n$.

$\alpha = \zeta_n \sqrt[n]{m}$.

Let $m = p_1 \dots p_k$, $p_i \in \mathbb{N}$ are distinct primes

$C_m = (C_{m^{1/n}})^n$: If $q \in \mathbb{N}$ is prime, $q^* \mid N(C_{m^{1/n}})$:

$q^{*n} \mid N(C_m) = (p_1^* \dots p_k)^{\text{deg}\,[L:\mathbb{Q}]}$

WLOG: $(q = p_1) \quad \therefore n \leq [L:\mathbb{Q}]$

But $m^{1/n}$ root of $t^n - m$ $\quad [L:\mathbb{Q}] \leq n$

$\therefore [L:\mathbb{Q}] = n$.

(b)

No.: ..... Date: .....

Claim: $Tr(m^{i/n}) = 0$ for $i = 1, \dots n-1$

Consider G basis: $\{1, \beta_0, \dots \beta_{n-1}\}$ of L

$m^{i/n}$ matrix: $A_{ij} = 1_{i=j+r \pmod n}$ ∃ 0 - Trace

$Tr(1) = n$.

$\therefore$ Pick $\beta_i^* = \beta_{n-i} / nm$

$Tr(\beta_i \cdot \beta_j^*) = \frac{1}{nm} Tr(\beta_i \cdot \beta_{n-j}) = \frac{1}{nm} Tr(\beta_{n-j+i}) = 0$

as $n-j+i \not\equiv 0 \pmod n$ for $0 \le i, j \le n-1$

(b) Let $\beta = m^{1/n}$: $Tr(\beta^r) = m^{\lfloor r/n \rfloor} \cdot 1_{r \equiv 0 \pmod n}$

If $r \not\equiv 0 \pmod n$: $\beta^r = \beta^{\lfloor r/n \rfloor \cdot n} \cdot \beta^k$, $0 \le k \le n-1$

If $0 \le r \le n-1$: Consider β^r action on $\{1, \dots \beta^{n-1}\}$:

Matrix representation: $\begin{pmatrix} 0 & & & m \\ \vdots & & \iddots & \\ 0 & \iddots & & \\ 1 & & & 0 \end{pmatrix}$ has 0 trace if $r \neq 0$, n trace if $r = 0$

$\begin{pmatrix} O_{n-r,r} & m \cdot I_{n-r} \\ I_r & O_{r,n-r} \end{pmatrix}$

Let $\beta = m^{1/n}$: $0 \le r < n$

β^r action on $\{1, \dots \beta^{n-1}\}$ represented by matrix:

$\begin{pmatrix} O_{n-r,r} & mI_{n-r} \\ I_{r,r} & O_{r,n-r} \end{pmatrix}$

$\therefore Tr(\beta^r) = 1_{r=0} \cdot n$

Pick $\beta_k^* = \beta_{n-k} / nm$:

No.: Date:

$Tr(\beta_i \cdot \beta_{n-i}/nm) = Tr(\beta_0)/nm = 1$

If $i \neq j$: $Tr(\beta_i \cdot \beta_{n-j}/nm) = 1/nm \cdot \underbrace{Tr(\beta_{n-j+i})}_{m^{\lfloor n-j+i \rfloor} \cdot Tr(\beta^r),\ 0<r<n.}$

$= 0.$

$\therefore$ Dual Basis.

Let $x = \sum_{k=0}^{n-1} a_k \cdot \beta^k \in \mathcal{O}_L$: $a_k \in \mathbb{Q}$

$Tr(x \cdot \beta^{n-i}) = \sum a_k \cdot nm \in \mathbb{Z}$ as $x \cdot \beta^{n-i} \in \mathcal{O}_L$

$\therefore a_k \in 1/nm\ \mathbb{Z}$

Valid $\forall k$: $x \in 1/nm\ \mathbb{Z}[\beta]$

cor If $n = m = p$: $\forall x \in \mathcal{O}_L$, $x = \sum_{k=0}^{n-1} a_k \beta^k$, $a_k \cdot p^r \in \mathbb{Z}$

Pf If $a_k \in \mathbb{Z}$ $(\forall k)$, $x \in \mathbb{Z}[\beta]$

Else: Pick k minimal s.t. $a_k \notin \mathbb{Z}$

$$\underbrace{x \cdot \beta^{(n-1)-k}}_{\in \mathcal{O}_L} = \underbrace{\sum_{r=0}^{k-1} a_r \beta^{r+(n-1)}}_{\in \mathcal{O}_L} + a_k \beta^{n-1} + \underbrace{\sum_{r>k} a_r \cdot \beta p \cdot \beta^{r-k}}_{\in \mathcal{O}_L}$$

$\therefore a_k \beta^{n-1} \in \mathcal{O}_L$

$N(a_k \beta^{n-1}) = a_k^p \cdot N(\sqrt{-p}^{1/p})^{p-1} = a_k^p \cdot (-1)^{\frac{p-1}{2}(p-1)} p^{\frac{p-1}{2}} \in \mathbb{Z}$

$\therefore$ If $a_k \in 1/p\ \mathbb{Z} \setminus \mathbb{Z}$: $p^{p-1} a_k^p \notin \mathbb{Z}$ (contradiction)

$\therefore x \in \mathbb{Z}[\beta] \Rightarrow \mathcal{O}_L = \mathbb{Z}[\beta]$

No.: Date:

Number Fields 2019

1.) (a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$

(b) Dirichlet's Unit Theorem: Let K be a number field; r, s be the number of real / complex pairs of embeddings into $\mathbb{C}$

Let $\mu = \{ x \in \mathcal{O}_K : x \text{ is a root of unity} \}$:

$$\mathcal{O}_K^{\times} \cong \mu \times \mathbb{Z}^{r+s-1}$$

If $K = \mathbb{Q}(\sqrt{2})$: $K \subseteq \mathbb{R} \Rightarrow \pm 1$ are the only roots of unity

$r=1, s=1 \Rightarrow \mathcal{O}_K^{\times} \cong \{\pm 1\} \times \mathbb{Z}$

Let ε be a fundamental unit: By taking $\pm$, we can WLOG $\varepsilon > 0$; By changing to $1/\varepsilon$, we can WLOG $\varepsilon > 1$.

Let α be a unit, $\alpha > 1$ and $|\alpha|$ minimal:

If $\alpha = \varepsilon^r$: $|\alpha| = |\varepsilon|^r \Rightarrow |\varepsilon| \leq |\alpha|$, equality iff $r = 1$

$\therefore \alpha = \varepsilon$ ✓

Try: $1+\sqrt{2}$; $N(1+\sqrt{2}) = 1-2 = -1 \Rightarrow 1+\sqrt{2} \in \mathcal{O}_K^{\times}$

If $1 < a + b\sqrt{2} \leq 1+\sqrt{2}$, $a, b \in \mathbb{Z}$ and $a^2 - 2b^2 \in \{\pm 1\}$:

$1 > |a - b\sqrt{2}| > 0$

$$\therefore 0 < 2a,\ 2b\sqrt{2} \leq 2 + \sqrt{2} \Rightarrow \begin{cases} 0 < a \leq 1 + 1/\sqrt{2} \Rightarrow a = 1 \\ 0 < b \leq 1/\sqrt{2} + 1/2 \Rightarrow b = 1 \end{cases}$$

$\therefore 1+\sqrt{2}$ is a generator.

$$\mathcal{O}_K^{\times} = \{ \pm (1+\sqrt{2})^n : n \in \mathbb{Z} \}$$

No.: ..... Date: .....

(c) $N(3+\sqrt{2}) = 9-2 = 7$.

$\therefore N((3+\sqrt{2})) = 7$ ($\Rightarrow P$ is prime)

$\therefore \mathcal{O}_K/p \cong \mathbb{F}_7$; $\mathbb{F}_7^\times \cong C_6$

$-1 \equiv 6 \pmod{P}$ as $\mathrm{char}(\mathcal{O}_K/p) = 7$.

$1+\sqrt{2} \equiv -2 \equiv 5 \pmod{P}$

We want: $(-1)^a \cdot \varepsilon^b \in G$ iff $(6)^a \cdot 5^b \equiv 1 \pmod 7$

$1 \to 5 \to 25 \equiv 4 \to 20 \equiv 6 \to 30 \equiv 2 \to 3 \to 1$

$\varepsilon^b \equiv 1$ $\varepsilon^b \equiv -1$ iff $b \equiv 3 \pmod 6$, $b \not\equiv 6 \pmod 7$

$\varepsilon^b \equiv 1$ iff $b \equiv 6 \pmod 6$

$\therefore G = \{\pm \varepsilon^{3k} : k \in \mathbb{Z}\} = \{(-1)^a (-\varepsilon^3)^k : k \in \mathbb{Z}\}$

is cyclic, generated by $-\varepsilon^3$

No.: ..... Date: .....

2.) (a) Let r, s be the # of real / complex pairs embedding into $\mathbb{C}$ (of L).

Minkowski's Upper Bound: $\left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \sqrt{|\mathrm{Disc}(L)|}$

(b) Min. polynomial of ω: $(2\omega - 1)^2 + 4\omega^2 - 4\omega + 1 = -47$

$\therefore \omega^2 - \omega + 12 = 0$

$f(t) = t^2 - t + 12.$

$N(\omega) = \frac{1}{4}(1 + 47) = 12 = 2^2 \cdot 3$

$N(2+\omega) = \frac{1}{4}\{25 + 47\} = 18 = 2 \cdot 3^2$

Factorise : (2), (3)

Since $\mathbb{Z}[\omega] = \mathcal{O}_K$: $[\mathcal{O}_K : \mathbb{Z}[\omega]] = 1$ is coprime to $2, 3$.

Dedekind Criterion: $(\mathrm{mod}\ 2)$ $f \equiv t(t-1) \Rightarrow (2) = (2, \omega)(2, \omega - 1)$

$(\mathrm{mod}\ 3)$ $f \equiv t(t-1) \Rightarrow (3) = (3, \omega)(3, \omega - 1)$

$(2, \omega)^2 = (4, 2\omega, \omega^2) = (4, 2\omega, \omega - 12) = (4, \omega)$

$(2, \omega)^3 \cdot (3, \omega) = (12, 3\omega, 4\omega, \omega^2) = (12, \omega) = (\omega)$ as $\omega \mid 12\ (= N(\omega))$

$\therefore (\omega) = (2, \omega)^3 \cdot (3, \omega)$

$(2, \omega) = (2, \omega + 2)$, $(3, \omega - 1) = (3, \omega + 2)$

$(3, \omega+2)^2 = (9, 3\omega + 6, \omega^2 + 4\omega + 4) = (9, 3\omega + 6, 5\omega - 8)$

$= (9, 3\omega + 6, (6\omega + 12) - (5\omega - 8) - 18) = (9, 3\omega + 6, \omega + 2) = (9, \omega + 2)$

$\therefore (3, \omega+2)^3 \mid (\omega + 2)$
$(2, \omega+2) \mid (\omega + 2)$
$\Big\} \quad (2, \omega+2)(3, \omega+2)^2 \mid (\omega + 2)$

By comparing norms: $(\omega+2) = (2, \omega+2) \cdot (3, \omega+2)^2$.

No.: ..... Date: .....

(c) Minkowski Bound: $r = 0, \quad S = 1$

$$\left(\frac{4}{\pi}\right) \cdot \frac{2!}{2^2} \cdot \sqrt{D_L}$$

Since $\mathcal{O}_{K_L} = \mathbb{Z}[\omega]$: $D_L = \text{Disc}(f) = -47$

$$\therefore \left(\frac{2}{\pi}\right) \cdot \sqrt{47} < \frac{2}{3} \cdot 7 < 5.$$

$\therefore$ It suffice to consider ideals of norm ≤ 4 $\Rightarrow$ Ideals generated by prime ideal factor of 2, 3.

Let $\alpha = [(2, \omega)]$, $\beta = [(3, \omega)]$: $\alpha^2 \cdot \beta = e$

$\alpha \cdot \beta^{-2} = e \Rightarrow \alpha = \beta^2$ $\Big\}$ $\beta^5 = e$.

$\therefore$ Class group generated by β, $\text{ord}([\beta]) = 1$ or 5:

If β is principal: $\beta = (x + y\omega)$, $x, y \in \mathbb{Z}$

$N(\beta) = 3 = x^2 (x + y/2)^2 + y^2/4 \cdot 47$

$\therefore$ ~~$12 = 4x^2 + 4xy + 48y^2$~~ ~~$3 = x^2 + xy + 12y^2$~~

If $|y| \geq 2$: RHS $\geq 49/4 \cdot 47 > 3$ reject!

If $|y| = 0$: $3 = x^2$ reject!

$|y| = 1$: $x^2 + xy + 12 = 3$

$\therefore x^2 + x = -9$

$x^2 - x = -9$ $\Big\}$ no int. solution

$\therefore \text{ord}(\beta) = 5$

$\therefore |Cl_L| = 5, \quad Cl_L \cong C_5.$

No.: Date:

4.) (a) Claim: $\mathbb{Z}[t]/(P, g(t)) \cong \mathbb{F}_p[t]/(g(t))$ (Ring isomorphism)

Consider $\Phi : \mathbb{Z}[t] \to \mathbb{F}_p[t]/(g(t))$;

Φ is a surjective ring homomorphism; If $\overset{h}{\$} \in \ker(\Phi)$:

$g(t) \mid \bar{h}$ ($\bar{h}$ is $h \pmod p$)

$\therefore \bar{h} = g(t) \cdot \varphi(t)$ (in $\mathbb{F}_p$)

$\therefore p \mid h - g(t)\cdot\varphi(t) \Rightarrow h \in \mathbb{Z}[t]\cdot(P, \varphi(t)\, g(t))$

Since $(P, g(t)) \subseteq \ker(\Phi)$: $\ker(\Phi) = (P, g(t))$

1st isomorphism: $\mathbb{Z}[t]/(P, g(t)) \cong \mathbb{F}_p[t]/(g(t))$

Claim: $\mathbb{Z}[\overset{t}{\alpha}]/(P, g(t)) \cong \mathbb{Z}[\alpha]/(P, g(\alpha))$

$\overline{\Phi} : \mathbb{Z}[t] \to \mathbb{Z}[\alpha]/(P, g(\alpha))$, $\overline{\Phi}(h(t)) = h(\alpha)$

is a surjective ring homomorphism

$h \in \ker(\overline{\Phi})$: $\exists \varphi$ s.t. $p \mid h(\alpha) - \varphi(\alpha)\cdot g(\alpha)$

$\therefore h(t) \in$

~~$\mathbb{Z}[t]/(f) \overset{\Phi}{\cong} \mathbb{Z}[\alpha]$~~

$\mathbb{Z}[\alpha] \overset{\Phi}{\cong} \mathbb{Z}[t]/(P, g(t))$

$\therefore \Phi(P) = P$

$\Phi(g(\alpha)) = g(t)$

$\mathbb{Z}[\alpha]/(P, g(\alpha)) \cong \mathbb{Z}[t]/(f)/(P, g(t))$

$\mathbb{Z}[\alpha]/(P, g(\alpha)) \cong \mathbb{Z}[t]/(f)\,/\,\mathbb{Z}[t]\cdot(P, g(\overset{t}{\alpha}))/(f)$ ($g \mid f$ over $\mathbb{F}_p$ $\Rightarrow f \in (P, g(t))$)

$\cong \mathbb{Z}[t]/(P, g(t))$

No.: Date:

$\mathbb{Z}[\alpha] = \mathcal{O}_L \Rightarrow \mathbb{F}_p[t]/(g_i) \cong \mathcal{O}_L/P_i$, $N(P_i) = p^{\deg(g_i)}$

$\prod_{i=1}^{r} P_i^{e_i} \subseteq (P, \prod_{i=1}^{r} g_i^{e_i}(\alpha)) = (P, \bar{f}(\alpha)) = (P)$

But $p^n = N((p)) = p^{\sum_{i=1}^{r} \deg(P_i)\cdot e_i} = N(\prod_{i=1}^{r} P_i^{e_i})$

$\therefore (P) = \prod_{i=1}^{r} P_i^{e_i}$, $N(P_i) = p^{\deg(g_i)}$ ✓

(b) If $\mathcal{O}_K = \mathbb{Z}[\alpha]$: Let f be minimal polynomial of α.

$\bar{f} = f \pmod p$, $\bar{f} = \prod_{i=1}^{r} P_i^{e_i} g_i^{e_i} \pmod p$

Dedekind: $(P) = \prod_{i=1}^{r} (P, g_i(\alpha))^{e_i} \Rightarrow e_1 = \dots = e_r = 1$

$N(P_i) = p \Rightarrow \deg(g_i) = 1 \Rightarrow r = n$

$\therefore \bar{f}$ factorises as n distinct factors $\Rightarrow \exists$ n distinct roots of $\bar{f}$ in $\mathbb{F}_p$; $n > |\mathbb{F}_p| = p \Rightarrow$ Contradiction

$\therefore \forall \alpha \in \mathcal{O}_K$, $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$.

No.: ..... Date: .....

Number Fields 2020

1.) (a) Minkowski Theorem: Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. If $S \subseteq \mathbb{R}^n$ is measurable ~~and~~, $\mathrm{Vol}(S) > \mathrm{Covol}(\Lambda)$:

~~$\mathrm{Vol}(S) \geq \mathrm{Covol}(\Lambda)$~~

$\exists\, x, y \in S$ s.t. $x \neq y$, $x - y \in \Lambda$

If S is symmetric, balanced convex around 0:

$\mathrm{Vol}(S) > 2^n \mathrm{Covol}(\Lambda)$ OR ($\mathrm{Vol}(S) \geq 2^n \mathrm{Covol}(\Lambda)$ $\wedge$ S closed)

$\Rightarrow S \cap \Lambda \neq \{0\}$

(b) Let $\Phi : K \to \mathbb{R}^2$, $\Phi(a + b\sqrt{d}) = (a, b\sqrt{d})$

Fix $I \triangleleft \mathcal{O}_K$:

Claim: $\mathrm{Covol}(\Phi(I)) = \frac{1}{2} N(I) \cdot \sqrt{\Delta}$, $\Delta = |\mathrm{Disc}(\mathcal{O}_K)|$

Let $I = \mathbb{Z} \cdot [x_1, x_2]$, $x_i = a_i + b_i\sqrt{-d}$.

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \\ b_1\sqrt{d} & b_2\sqrt{d} \end{pmatrix} = \begin{pmatrix} \sigma_1(x_1) & \sigma_2(x_1) \\ \sigma_2(x_1) & \sigma_2(x_2) \end{pmatrix} = A$$

$\det(A)^2 = \Delta(x_1, x_2) = N(I)^2 \cdot \Delta$ ~~Δ~~ $\mathrm{Disc}(\mathcal{O}_K)$

But $|\det(A)|^2 = 2^2 \begin{vmatrix} a_1 & a_2 \\ b_1\sqrt{d} & b_2\sqrt{d} \end{vmatrix}^2$

$\therefore \mathrm{Covol}(\Lambda) = \frac{1}{2}|\det(A)| = \frac{1}{2} N(I) \cdot \sqrt{\Delta}$

Pick r s.t. $\pi r^2 = \frac{1}{2} N(I) \cdot \sqrt{\Delta} \cdot 2^2$

r^2

$\therefore \exists\, \alpha \in \bar{D}(0, r) \cap \Phi(I)$, $\alpha \neq 0$: $(\alpha) = I \cdot J$, $N((\alpha)) \leq r^2$

$N(\alpha) =$

$\therefore N(I) \cdot N(J) \leq r^2 \leq \left(\frac{4}{\pi}\right) \cdot \frac{1}{2} \sqrt{\Delta}\, N(I)$

$\therefore \forall I \triangleleft \mathcal{O}_K$, $[I]^{-1}$ has ~~norm~~ a ~~representative with norm~~ $\leq \left(\frac{2}{\pi}\right)\sqrt{\Delta}$

4 If $d \not\equiv 3 \pmod 4$: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ $\Rightarrow \sqrt{\Delta} = \sqrt{4d^2} = 2d \cdot \sqrt{d}$

$\therefore N(\alpha) \leq \frac{4}{\pi}\sqrt{d} \cdot N(I)$

No.: Date:

∴ Since $C(a) = I \cdot J$: $\forall\ [I] \in Cl_K$, $[I]^{-1}$ has representative with norm $\leq 4\sqrt{|d|}/\pi$

∴ Cl_K represented ~~generated~~ by ideals of norm $\leq 4\sqrt{|d|}/\pi$

If $N(\mathfrak{a}) = M$: $\left| \mathcal{O}_K / \mathfrak{a} \right| = M \Rightarrow M \in \mathfrak{a}$ (Lagrange)

∴ $\mathfrak{a} \mid (M) \Rightarrow$ Finite # of ideals $\mathfrak{a}$, $N(\mathfrak{a}) = M$

∴ Cl_K have finite elements (each element has representative with norm $\leq 4\sqrt{|d|}/\pi$)

(c) $4\sqrt{22}/\pi \not< 4\cdot 5/8$ ~~4.5/8~~ $\Rightarrow 4 \cdot 5/3 \Rightarrow$ Consider elements of norm ≤ 6.

Dedekind: $\mathcal{O}_K = \mathbb{Z}[\sqrt{-22}]$

$t^2 + 22 \equiv (t)^2 \pmod 2$

$\equiv (t^2+1) \pmod 3$

$\equiv t^2 + 2 \pmod 5$

∴ (5) is prime ; $(2) = (2, \sqrt{-22})^2$, ~~$(3) = (3, \sqrt{-22}) \cdot (3, \sqrt{-22}+1)$~~

(3) is prime.

If $(2, \sqrt{-22}) = (a + b\sqrt{-22})$: $a^2 + 22b^2 = 2 \Rightarrow b = 0$, no sln. of a.

∴ $(2, \sqrt{-22})$ not principal

∴ $Cl_K = \{ e, [(2, \sqrt{-22})] \} \cong C_2$

If $y^3 = (X - \sqrt{-22})(X + \sqrt{-22})$

Let $I \mid (X \pm \sqrt{-22})$: $X \pm \sqrt{-22} \in I \Rightarrow 2X,\ 2\sqrt{-22} \in I$

∴ $I \mid (2\sqrt{-22})$

But $2 \mid y \Rightarrow 2 \mid x^3 \Rightarrow 4 \mid y^3 - x^3 = 22$ (reject)

No.: Date:

$11 \mid y \Rightarrow 11 \mid y^3 - 22 \Rightarrow 11 \mid x^3 \Rightarrow 11 \mid x \Rightarrow 11^3 \mid y^3 - x^3 = 22$ (objection)

$N(I) \mid N(y)^3 \Rightarrow N(I)$ has no factor of 2, 11

$\therefore I = (1)$

$y^3 = P_1^3 \cdots P_r^3$ (P_i distinct prime ideals) $\Rightarrow$

$(x + \sqrt{-22}) = (\text{WLOG}) \; P_1^3 \cdots P_s^3$

$\therefore$ ord $[P_1 \cdots P_s] = 1$ or 3

$|Cl_k| = 2 \Rightarrow$ order $\neq 3$. $\therefore (x + \sqrt{-22}) = (a + b\sqrt{-22})^3$

$\therefore x + \sqrt{-22} = u \cdot (a + b\sqrt{-22})^3, \; a, b \in \mathbb{Z}$

But $\mathcal{O}_k^\times \cong \mu \times \mathbb{Z}^0$; $[\mathbb{Q}(\sqrt{-22}) : \mathbb{Q}] = 2 \Rightarrow$

$\therefore$ If $\omega \in k$ is a n-primative root of unity : $\varphi(n) \mid 2$

$\therefore n = 3$ or 1

No.: Date:

If $x, y \in \mathbb{Z}$: $x^3 (x - \sqrt{-22})(x + \sqrt{-22}) = y^3$

Let I be a prime ideal : $I \mid (x \pm \sqrt{-22})$

$\therefore 2x,\ 2\sqrt{-22} \in I \Rightarrow I \mid (2\sqrt{-22}) \Rightarrow N(I) \mid 88.$

But $N(I) \mid N(y) = y^2$: If $q \mid y$, $q = 2$ or 11,

$q \mid y \Rightarrow q \mid y^3 - 22 \Rightarrow q \mid x^2 \Rightarrow q \mid x \Rightarrow q^2 \mid y^3 - x^3 = 22$ (reject)

$\therefore 2, 11 \nmid N(I) \Rightarrow N(I) = 1$

$(y^3) = P_1^{3k_1} \dots P_r^{3k_r}$ (P_i are distinct prime ideals)

$\therefore$ (WLOG) $(x + \sqrt{-22}) = P_1^{3k_1} \dots P_s^{3k_s} = I^3$

If I not principal: ord $[I] = 3$ (rejects, as $Cl_K \cong C_2 \Rightarrow$ No order 3 elements)

$\therefore x + \sqrt{-22} = u \cdot (a + b\sqrt{-22})^3$, $u \in \mathcal{O}_K^\times$

$\mathcal{O}_K^\times \cong \mu \times \mathbb{Z}^{s+t-1}$; $\{\pm 1\}$ are on the only roots of unity in $\mathcal{O}_K$

$\therefore \pm 1 = (\pm 1)^3 \Rightarrow x + \sqrt{-22} = (a + b\sqrt{-22})^3$ ($a, b \in \mathbb{Z}$)

$= a^3 + 3a^2 b\sqrt{-22} - 66ab^2 + (-22)b^3\sqrt{-22}$

$\therefore x = a^3 - 66ab^2$

$+1 = 3a^2 b - 22b^3 \Rightarrow b = 1$ or -1

$\therefore 3a^2 - 22 = 1$ or $-1 \Rightarrow 3a^2 = 23$ or 21 (no solutions)

$\therefore$ No integer solutions

No.: Date:

2.) (a) $\mathrm{Disc}(\alpha_1, \dots \alpha_n) = |\mathrm{Det}(G_i(\alpha_j))|$, $\mathrm{Hom}_G(K, \mathbb{C}) = \{G_1, \dots G_n\}$

$\Delta(\alpha_1, \dots \alpha_n) = 0$ iff $\mathrm{Det}(G_i(\alpha_j)) = 0$ iff $A = (G_i(\alpha_j))$

linearly dependent iff $\exists\ \underline{\lambda}$ s.t. $(\forall i)\ G_i(\sum \lambda_j \alpha_j) = 0$, $\underline{\lambda} \neq \underline{0}$

iff $\exists\ \underline{\lambda}$ s.t. $\sum \lambda_j \alpha_j = 0$, $\underline{\lambda} \neq 0$

We use:

$(1)\ G_1(x) = \dots = G_n(x) = 0 \Rightarrow x = 0$

$\therefore$ $\mathrm{Disc}(\alpha_1, \dots \alpha_n) = 0$ iff $\{\alpha_1, \dots \alpha_n\}$ are linearly independent

iff $\{\alpha_1, \dots \alpha_n\}$ is a basis ($\dim_G(K) = n$)

(b) $N((p)) = p^n$

Since $(P, \alpha) \overset{?}{=} (p)$: $(P, \alpha) \mid (p) \Rightarrow N((P, \alpha)) \mid p^n$

$(P, \alpha)^n = \left(\binom{n}{k} p^{n-k} \alpha^k : 0 \leq k \leq n \right) = I$

$p \cdot \alpha \in I$, $\alpha^n \in I$;

$0 = \alpha^n + p\alpha \cdot (*) + a_0 \Rightarrow a_0 \in I$.

$p^n \in I$, $\gcd(p^n, a_0) = p \Rightarrow p \in I$

$p \mid \binom{n}{k} p^{n-k} \alpha^k$ for $0 \leq k \leq n-1$

$p \mid \alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j$

$\Big\} \ I = (p)$

$\therefore N((P, \alpha)) = p$ $\Rightarrow$ (P, α) is $\Rightarrow$ (P, α) must be prime,

$(p) = P^n$

If $\alpha \in P^2$: $\rightarrow 0 \equiv \alpha^n + \sum_{j=0}^{n-1} \alpha^j \cdot a_j \equiv a_0 \pmod{P^2}$

$p^2 \in P^2 \Rightarrow \gcd(a_0, P^2) = p \in P^2$

$\therefore \alpha, p \in P^2 \Rightarrow p \subseteq P^2 \Rightarrow P^2 \mid p$ (reject)

$\therefore \alpha \notin P^2$

No.: Date:

(ii) Suppose $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$: $\exists\ \beta = \sum_{r=0}^{n-1} b_r \alpha^r$ s.t.

$b_0, \dots b_r$ not all $\in \mathbb{Z}$, $pb_0, \dots pb_r \in \mathbb{Z}$.

Pick smallest s s.t. $b_s \notin \mathbb{Z}$

$$\beta \cdot \alpha^{(n-1)-s} = \underbrace{\sum_{r=0}^{s-1} b_r \alpha^{r+(n-1)-s}}_{\in \mathbb{Z}[\alpha]} + b_s \alpha^{n-1} + \sum_{r>s} b_r \alpha^{(n-1)-s+r}$$

$r > s \Rightarrow n-1-s+r \geq n \Rightarrow p \mid \alpha^{(n-1)-s+r} = \sum_{r>s} b_r \alpha^{(n-1)-s+r} \in \mathbb{Z}[\alpha]$

$\therefore b_s \alpha^{n-1} \in \mathcal{O}_K$, $b_s = r/p$, $\gcd(r,p) = 1$

$N(r/p\ \alpha^{n-1}) = (-1)^{n(n-1)} r^{pn}/p^n \cdot a_0^{n-1} \notin \mathbb{Z}$ as $p \nmid r^n$, $p^{n-1} \parallel a_0^{n-1}$

$\therefore$ Contradiction

$\therefore p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ (p prime to $|\mathcal{O}_K/\mathbb{Z}[\alpha]|$)

(iii) $\mathrm{Disc}(1, \alpha, \alpha^2) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta(\mathcal{O}_K)$

$LHS = -4 \cdot 3^3 - 3^2 \cdot 27 = -3^3 \{12 + 37\} = -(3^3 \cdot 7) \cdot 13$

$3 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$, $\Rightarrow [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mid 13$

$\therefore [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$

$\therefore \mathcal{O}_K = \mathbb{Z}[\alpha]$ #

No.: Date:

4.) (a) Let $G = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$:

If $\forall \sigma \in G, \sigma(x) = x : x \in \mathbb{Q}$.

Let $f_m(t) = \prod_{i=1}^{n} (t - \sigma_i(\alpha)^m) : \forall \sigma \in G, \sigma(f_m) = f_m$

$\Rightarrow f_m \in \mathbb{Q}[t]$.

But coefficients of f_m are sum/products of algebraic integers $\Rightarrow f_m \in \mathbb{Z}[t]$

Let $a = \mathrm{Max}\left\{ \binom{n}{i} : 0 \le i \le n \right\}$: $\therefore$ There are finitely many polynomials in $\mathbb{Z}[t]$ with coefficients $\in [-a, a]$ and $\deg(f) \le n$.

Let there be $M-1$ such polynomials.

If $|\sigma_i(\alpha)| < 1+\varepsilon$: Coefficients of f_m are symmetric polynomials in $\sigma_i(\alpha)^m \Rightarrow |\text{Coefficient}| \le (1+\varepsilon)^{nm} \binom{n}{} a$

Pick ε s.t. $(1+\varepsilon)^{n \cdot M} < a+1/a$. ; $\varepsilon > 0$:

$\therefore$ For $f_1, \ldots f_M$, all coefficients are in $[-a, a] \Rightarrow$

$\exists f_{m_1} = f_{m_2}, \quad m_1 < m_2$.

$\therefore \sigma_i(\alpha)^{m_2} = \alpha^{m_1} \Rightarrow \sigma_i(\alpha) = \alpha^{m_1/m_2}$

$\sigma_i^{|G|} = \sigma_i^n = id : \alpha = \alpha^{(m_1/m_2)^n} \Rightarrow \alpha^{m_1^n} = \alpha^{m_2^n}$

$\therefore \alpha^{m_2^n - m_1^n} = 1 \Rightarrow \alpha$ is a root of unity

($|\sigma_i(\alpha)| = 1$ works under as $1 < 1+\varepsilon$) $\therefore \alpha$ is a root of unity

Pick $c < 1+\varepsilon$: $|\sigma_i(\alpha)| < c \ (\forall i) \Rightarrow \alpha$ is a root of unity

No.: Date:

Let K be a number field:

(b) Dirichlet Unit: Let r be the # of real embeddings, s be the # of complex pairs of embeddings

μ be the roots of unity; ~~(b) If L is~~

$$\mathcal{O}_K^\times \cong \mu \times \mathbb{Z}^{r+s-1}$$

(c) $K \subseteq \mathbb{R}$: $\mu = \{\pm 1\}$

Let $\mathcal{O}_K^\times = \{\pm 1\} \times \{\varepsilon^n : n \in \mathbb{Z}\}$: If $\varepsilon < 0$, replace with $-\varepsilon$.

$\therefore$ (WLOG): $\varepsilon > 0$

If $\varepsilon < 1$, replace with $1/\varepsilon$: WLOG, $\varepsilon > 1$

If $\varepsilon = 1$, ε is not a generator $\Rightarrow$ $\varepsilon > 1$

If $\alpha > 1$: $\alpha = \pm \varepsilon^N \Rightarrow$ WLOG $\alpha = \varepsilon^N$ $(\alpha > 0)$

$|\alpha| = |\varepsilon|^N > 1 \Rightarrow N \geq 0$.

$\therefore |\alpha| = |\varepsilon|^N \geq |\varepsilon|$ WLOG $= \varepsilon$ $\therefore$ ε is the smallest >1 element; $\mathcal{O}_K = \{\pm \varepsilon^n : n \in \mathbb{Z}\}$

Let $\alpha = 10 + 3\sqrt{11} > 1$: WLOG $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$

If $\exists\ 1 < a + b\sqrt{11} \leq 10 + 3\sqrt{11}$: $a, b \in \mathbb{Z}$, $a^2 - 11b^2 \in \{\pm 1\}$

$1 > \underbrace{|1/a + b\sqrt{11}|}_{|a - b\sqrt{11}|} > 0$.

$\therefore 0 < 2a,\ 2b\sqrt{11} \leq 11 + 3\sqrt{11} \Rightarrow 0 < b \leq \sqrt{11}/2 + 3/2 < 2 + 3/2$

$\therefore 1 \leq b \leq 3$

$b = 1$: $a^2 - 11 \in \{\pm 1\}$ (reject)

$b = 2$: $a^2 - 44 \in \{\pm 1\}$ (reject)

$b = 3$: $a^2 - 99 \in \{\pm 1\} \Rightarrow a^2 = 99 + 1 \Rightarrow a = 10$.

$\therefore$ α has minimal ~~ma~~ size $\Rightarrow$ $\mathcal{O}_K = \{\pm(10 + 3\sqrt{11})^n : n \in \mathbb{Z}\}$

No.: ..... Date: .....

Number Fields 20201

1.) (a) $f(t) = t^3 - 5t + 8$

If f is reducible over $\mathbb{Q}$: Gauss Lemma $\Rightarrow$ reducible over $\mathbb{Z}$

$\Rightarrow \exists$ root in $\mathbb{Z}$ (x)

$5x - x^3 = 8 \Rightarrow x \mid 8 \Rightarrow x \in \{0, \pm 1, \pm 2, \pm 4, \pm 8\}$

We can verify none of them are roots. $\therefore$ f must be irreducible. $\therefore [K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] =$ deg (Min. poly of α)

$=$ deg $(f) = 3$.

(b) β act on $\mathbb{Q}(1, \alpha, \alpha^2)$: $\alpha \cdot \beta = \frac{1}{2}(\alpha^2 + 5\alpha - 8)$

$\alpha^2 \cdot \beta = \beta \frac{1}{2}(5\alpha - 8 + 5\alpha^2 - 8\alpha) = \frac{1}{2}(5\alpha^2 - 3\alpha - 8$

M: $\begin{pmatrix} 0 & -4 & -4 \\ 1/2 & 5/2 & -3/2 \\ 1/2 & 1/2 & 5/2 \end{pmatrix}$

$\det(M - tI) = \begin{vmatrix} -t & -4 & -4 \\ -1/2 & 5/2 - t & -3/2 \\ 1/2 & 1/2 & 5/2 - t \end{vmatrix} = (-t)\left((5/2 - t)^2 + 3/4\right) + 4\left(\left(-\frac{1}{2}\right)(5/2 - t) + 3/4\right) - 4\left(-1/4 - \frac{1}{2}(5/2 - t)\right)$

$= (-t)(t^2 - 5t + 7) + 4((2t - 5) + 3) + (1 + (5 - 2t)) \in \mathbb{Z}[t]$

β root of $-\det(M - tI)$, (monic in t^3) $\Rightarrow$ β is an algebraic integer.

$\Delta(1, \alpha, \alpha^2) = -4 \cdot 307$

$\begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1/2 \\ 0 & 0 & 1/2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} \Rightarrow \Delta(1, \alpha, \beta) = 1/4 \cdot \Delta(1, \alpha, \alpha^2) = -307$

$\Delta(1, \alpha, \beta) = [\mathcal{O}_K : \mathbb{Z}[\alpha, \beta]]^2 \cdot \Delta(\mathcal{O}_K)$

$\therefore [\mathcal{O}_K : \mathbb{Z}[\alpha, \beta]]^2 \mid -307$ (non-square) $\Rightarrow$

$[\mathcal{O}_K : \mathbb{Z}[\alpha, \beta]] = 1$

$\therefore \Delta(1, \alpha, \beta) = \Delta(\mathcal{O}_K) \Rightarrow \mathcal{O}_K = \mathbb{Z}[1, \alpha, \beta]$

No.: Date:

(c) $[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 = 4 \Rightarrow [\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2$ is coprime to 3.

Dedekind criterion:

$f(t) = t^3 - 5t + 8 = t^3 + t + 2 = (t+1)(t^2 - t + 2)$

$\therefore (3) = (3, 3+\alpha) \cdot (3, \alpha^2 - \alpha + 2)$

$N(1+\alpha) = (-1)^3 N(-1-\alpha) = -f(-1) = -\{-1+5+8\} = -12.$

$\therefore N(\beta) = \frac{1}{8} N(\alpha) \cdot N(1+\alpha) = 12 = N((\beta))$

$\therefore$ (Prime factorisation of (β)): $(\beta) = P_1 \dots P_r$.

We must have $N(P_i) = 2$ or 4 for some i

If (2) is prime: No ideals of norm 2, 4.

$\therefore$ Contradiction $\Rightarrow$ (2) is not prime

No.: Date:

2.) (a) $\alpha \in K$ is algebraic if $\exists\, f \in \mathbb{Z}[t]$, $f \neq 0$ s.t. $f(\alpha) = 0$

Let α be algebraic, $\alpha \neq 0$: Pick $f \in \mathbb{Z}[t]$, f irreducible s.t.

$$f(t) = \sum_{k=0}^{n} a_k t^k, \quad a_n \neq 0 \text{ and } f(\alpha) = 0$$

~~If $a_0 = 0$: $t \mid f(t)$; $\alpha \neq 0 \Rightarrow f(\alpha) \neq 0$, $\deg(f) > 1$.~~

~~$\therefore$ Contr~~

@ $\alpha \neq 0$: $\deg(f) > 1$

If $a_0 = 0$: $t \mid f(t) \Rightarrow f$ reducible (reject).

$\therefore a_0 = -\sum_{k=1}^{n} a_k \alpha^k \Rightarrow \beta \neq 0$; $\beta = \sum_{k=1}^{n} -a_k \alpha^{k-1} \in \mathbb{Z}[\beta]$

$\therefore \alpha\beta = a_0 \in \mathbb{Z} \setminus \{0\}$ ($\beta \in \mathbb{Z}[\alpha]$) $\lightning$

(b) Fix $x \in k = \mathrm{Frac}(R)$: $\exists\, \alpha, \beta \in R$ s.t. $x = \alpha/\beta$, $\beta \neq 0$

(a) $\Rightarrow \exists\, r \in \mathbb{Z}[\beta]$ s.t. $\beta \cdot r \in \mathbb{Z} \setminus \{0\}$

By picking $-r$ if necessary, we can WLOG $\beta \cdot r \in \mathbb{N}$

$\therefore x = \alpha \cdot r / \beta \cdot r$, $\beta \cdot r \in \mathbb{N}$.

Since $r \in \mathbb{Z}[\beta] \subseteq R$, $\alpha \in R$: R closed wrt $+, \cdot \Rightarrow \alpha r \in R$

$\therefore \exists\, r \in R,\ m \in \mathbb{N}$ s.t. $x = r/m$ $\lightning$

(c) $\mathcal{O}_K$ is a finitely generated, free $\mathbb{Z}$-module of rank $n = [\mathcal{O}_K : \mathbb{Q}]$

$\mathbb{Z}$ is an Euclidean Domain: Any submodule of a Finitely generated free $\mathbb{Z}$-module is finitely generated, free $\mathbb{Z}$-module.

Since $R \leq \mathcal{O}_K$: $1 \in R \Rightarrow \mathbb{Z} \subseteq R \Rightarrow R$ is a $\mathbb{Z}$-module $\Rightarrow$ R is a sub-module of $\mathcal{O}_K$.

By applying Smith-Normal Form: $\exists$ Basis over $\mathbb{Z}$ of $\mathcal{O}_K$: $\{ d_1 \dots d_n \}$ s.t. $R = \mathbb{Z} \cdot \{ d_1 d_1, \dots d_r d_r \}$, $d_i \mid d_{i+1}$

But If $r < n$: $d_{r+1} = {}^{\#}X/m$, $x \in R$, $m \in \mathbb{N}$

But $\forall y \in \mathbb{Z}\cdot\{d_1 d_1, \dots d_r d_r\}$, $y \neq d_{r+1} \cdot m \cdot d_{r+1}$ as

element in $\mathcal{O}_K$ uniquely written as $\sum_{i=1}^{n} z_i d_i + \dots + z_n d_n$.

$\therefore$ Contradiction $\Rightarrow r = n$.

$\therefore$ R is a free $\mathbb{Z}$-module of rank n as well

$$|\mathcal{O}_K/R| = \left|\mathbb{Z}\cdot\{d_1, \dots d_n\}/\mathbb{Z}\cdot\{d_1 d_1, \dots d_n d_n\}\right| = d_1 \dots d_n < \infty$$

If $I \trianglelefteq R$: I is a $\mathbb{Z}$-submodule of R

$\therefore$ $\exists$ Basis of R $\cdot\{z_1, \dots z_n\}$

s.t $R = \mathbb{Z}\cdot\{\beta_1, \dots \beta_n\}$, $I = \mathbb{Z}\cdot\{e_1\beta_1, \dots e_r\beta_r\}$

Pick $x \in I$, $x \neq 0$: $\exists\ \tilde{x} \in \mathbb{Z}[x]$ s.t $x\cdot\tilde{x} \in \mathbb{Z}\setminus\{0\} = M$

$\tilde{x} \in \mathbb{Z}[x] \subseteq R \Rightarrow x\cdot\tilde{x} \in I \Rightarrow I \geq (x\cdot\tilde{x})$

$\therefore$

$$|R/I| \leq |R/(x\cdot\tilde{x})| = M^n < \infty \quad \therefore [R:I] < \infty$$

If $\mathcal{O}_K = \mathbb{Z}\cdot\{d_1, \dots d_n\}$, $R = \mathbb{Z}\cdot\{d_1 d_1, \dots, d_n d_n\}$:

$$d_n\cdot\mathcal{O}_K = \mathbb{Z}\cdot\{d_n d_1, \dots d_n d_n\} = \mathbb{Z}\{{}^{d_n}/_{d_1}\cdot d_1 d_1, \dots {}^{d_n}/_{d_n}\cdot d_n d_n\}$$

$\therefore$ $d_n\cdot\mathcal{O}_K \trianglelefteq R$

(d) $I = J = d_n\cdot\mathcal{O}_K$: $[R:I] = [R:J] = \prod_{k=1}^{n} {}^{d_n}/_{d_k}$

$I\cdot J = d_n^2\mathcal{O}_K = \mathbb{Z}\cdot\{d_n^2 d_1, \dots d_n^2 d_n\} \Rightarrow [R:IJ] = \prod_{k=1}^{n} {}^{d_n^2}/_{d_k}$

Equality: $d_1 \dots d_n = 1 \Rightarrow d_1 = \dots = d_n = 1 \Rightarrow R = \mathcal{O}_K$ #

No.: ..... Date: .....

4.) (a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{30}]$; $f(t) = t^2 - 30$ is the minimal polynomial of $\sqrt{30}$

Minkowski Bound: $\frac{1}{2}\sqrt{|d_K|}$; $d_K = -4 \cdot (-30) = 120$

$\therefore \frac{1}{2}\sqrt{120} = \sqrt{30} < 6.$

$\therefore$ Cl_K represented by ideals of norms 2, 3, 4, 5 $\Rightarrow$

prime ideal factors of $(2), (3), (5)$

($\mathcal{O}_K = \mathbb{Z}[\sqrt{30}]$) Apply Dedekind's Criterion:

$t^2 - 30 \equiv t^2 \pmod{2,3,5}$

$\therefore (p) = (p, \sqrt{30})$ $(p = 2, 3, 5)$

$\alpha = (2, \sqrt{30})$, $\beta = (3, \sqrt{30})$, $\gamma = (5, \sqrt{30})$

$\alpha \cdot \beta \cdot \gamma = (6, \sqrt{30})(5, \sqrt{30}) = (\sqrt{30})$

$\alpha \cdot \beta = (2, \sqrt{30}+6)(3, \sqrt{30}+6) = (\sqrt{30}+6)$

$\therefore Cl_K = \langle [\alpha] \rangle$

If α is principal: $(2, \sqrt{30}) = (a + b\sqrt{30})$ $\#$, $a, b \in \mathbb{Z}$ $\Rightarrow$

$a^2 - b^2 \cdot 30 = 2$ or -2

$\pmod 5$: $a^2 \equiv \pm 2 \pmod 5$ $\#$; No solutions $\Rightarrow$ $(2, \sqrt{30})$ not principal

$\therefore |Cl_K| = 2$, $Cl_K = \langle [\alpha] \rangle \cong C_2$

Dirichlet Unit Theorem: $\mathcal{O}_K^\times \cong \mu \times \mathbb{Z}$, $\mu = \{\text{roots of unity in } \mathcal{O}_K\}$

$= \{\pm 1\}$ as $\mathcal{O}_K \subseteq \mathbb{R}$

If ε is smallest >1 elemal of $\mathcal{O}_K^\times$, ε is a fundamental unit.

Try $10 + 3\sqrt{11}$: If $1 < a + b\sqrt{11} \leq 10 + 3\sqrt{11}$:

$1 \# > |a - b\sqrt{11}| \geq 0$ $\Rightarrow$ $0 < 2a,\ 2b\sqrt{11} \leq 11 + 3\sqrt{11}$

$\therefore b \leq \sqrt{11}/2 + 3/2 \leq 3/2 + \sqrt{3} < 4$

If $b = 1, 2$: $a^2 - 11b^2 \in \{\pm 1\}$ (no solution)

No.: Date:

$b = 3 \Rightarrow a = 10$. $\therefore$ $\varepsilon = 10 + 3\sqrt{11}$ is a fundamental unit.

(b) Subgroup: Let $T_1 = \{ x \in K^\times : x \text{ is totally } +ve \}$

$x, y \in T_1$: $G_i(x/y) = G_i(x)/G_i(y) > 0 \Rightarrow xy^{-1} \in T_1$

$\therefore T_1 \leq K^\times \Rightarrow T_1$ is a subgroup

Consider $\Phi : K^\times \to \{\pm 1\}^2$, $\Phi(x) = (\operatorname{sgn}(G_1(x)), \operatorname{sgn}(G_2(x)))$

Φ is a (mult.) homomorphism;

Surjective: $\Phi(-1) = (-1, -1)$, $\Phi(\sqrt{30}) = (1, -1)$, $\Phi(-\sqrt{30}) = (-1, 1)$

($G_1(a + b\sqrt{30}) = a + b\sqrt{30}$, $G_2(a + b\sqrt{30}) = a - b\sqrt{30}$)

$T_1 = \ker(\Phi)$

$\therefore$ (1st isomorphism) $K^\times / T_1 \cong C_2 \times C_2 \Rightarrow [K^\times : T_1] = 4$.

$\therefore$ Index 4 subgroup

(c) Equivalence Relation:

$I \sim I$: $I = (\pm 1) \cdot 1 \cdot I$

If $I \sim J$: $I = \alpha \cdot J \Rightarrow J = 1/\alpha \cdot I$; $\alpha \in T_1 \Rightarrow 1/\alpha \in T_1$

$\therefore J \sim I$

If $I \sim J$, $J \sim K$: $I = \alpha_1 J$, $J = \alpha_2 K \Rightarrow I = (\alpha_1 \cdot \alpha_2) \cdot K$, $\alpha_1 \cdot \alpha_2 \in T_1$

$\therefore I \sim K$. $\therefore$ Equivalence Relation

Group Structure:

$[I] \cdot [J] = [I \cdot J]$

(Well defined): If $I_1 = \alpha_1 I_2$, $J_1 = \alpha_2 J_2$ $\Rightarrow$ $I_1 \cdot J_1 = \alpha_1 \alpha_2 I_2 J_2$, $\alpha_1 \alpha_2 \in T$

$\therefore [I_1 \cdot J_1] = [I_2 \cdot J_2]$

$\because$ Commutative

$\therefore$ Operation is clearly closed; Associative, (ideal mult. is associative and commutative)

Identity: (1), $[I] \cdot [(1)] = [(1)] \cdot [I] = [I]$ $(\forall\, I)$

No.: Date:

Inverse : $\forall\ I,\quad I^{-1} = \mathfrak{a}\,\frac{1}{n}\cdot J$ for some ideal J.

$\therefore\ [I^{-1}]\cdot[J] = [J\cdot][I] = [\tfrac{1}{n}(1)] = [(1)]$ as $\tfrac{1}{n} \in T$.

$\therefore$ Valid Group structure.

Let ~~A be an equivalence class~~ in $\approx$, $I \overset{*}{\approx} J$ iff

$I = (\alpha)\cdot J,\quad \alpha \in K^{\times}$

If $I \sim J$: $I \approx J$;

$\therefore$ Each equivalence class of $\approx$ relation splits into equivalence classes of $\sim$

If $I = \alpha\cdot J$, $G_i(\alpha) < 0$: $-\alpha J = \alpha J$, $-\alpha \in T$

$G_1(\alpha)\cdot G_2(\alpha) < 0$, $G_2(\alpha) > 0$: $-\alpha J = \alpha J$,

$G_1(-\alpha) > 0$, $G_2(\alpha) < 0$.

$\therefore [I]_{\approx}$ Splits into at most 2 $\sim$ classes

Fix $\alpha \in K$, $\mathcal{O}_K^*$ s.t. $G_1(\alpha) > 0$, $G_2(\alpha) < 0$;

$[I]_{\approx}$ is a single $\sim$ class iff $I \sim J$, $J = \alpha\cdot I$, α

$G_1(\alpha) > 0$, $G_2(\alpha) < 0$.

iff $\exists\ \beta \in T$, $J = \beta\cdot I = \alpha I$ iff $\exists\ \beta \in T$, (β/α) is unit.

If $\exists\ \varepsilon \in \mathcal{O}_K^{\times}$, $N(\varepsilon) = G_1(\varepsilon)\,G_2(\varepsilon) = -1 < 0$.

$\therefore$ If $I = \alpha J$, $G_1(\alpha) > 0$, $G_2(\alpha) < 0$: $I = (-\varepsilon)\cdot\alpha J$

$G_i(-\varepsilon\alpha) > 0$.

$\therefore [I]_{\approx}$ is a single $\sim$ class.

$\therefore$ Order of group $= h_K$

Else If $G_1(\alpha) > 0$, $G_2(\alpha) < 0$: $I = \alpha J \sim J \Rightarrow I = \beta\cdot J$,

$\beta \in T$.

$\therefore \alpha/\beta \in \mathcal{O}_K^{\times}$, as $(\alpha/\beta)\cdot J = I$

$G_1(\alpha/\beta) > 0$, $G_2(\alpha/\beta) < 0$

$\therefore N(\alpha/\beta) < 0 \Rightarrow = -1$

No.: ..... Date: .....

(else $2 h_K$)

Order of group $= h_K$ iff $\exists$ element in $\mathcal{O}_K^\times$ of norm -1

iff $N(\varepsilon) = -1$ (ε is fundamental)

* $N(\pm \varepsilon^n) = N(\varepsilon)^n$ *

No.: Date:

Number Fields 2022

1.) (a) Let $K = \mathbb{Q}(\alpha)$, $f \in \mathbb{Z}[t]$ is the minimal polynomial of α.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = n$; Let $\Lambda = \text{Root}(f, \mathbb{C})$, $|\Lambda| = n$ as $\text{Char}(\mathbb{Q}) = 0 \Rightarrow f$ is separable.

$\forall \Phi \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$: Φ fixes $\mathbb{Q} \Rightarrow \Phi$ determined by $\Phi(\alpha)$

$f(\Phi(\alpha)) = \Phi(f(\alpha)) = 0 \Rightarrow \Phi(\alpha) \in \Lambda$

$\therefore$ At most n such embeddings

$\forall \beta \in \Lambda$: Define $\Phi(P(\alpha)) = P(\beta)$

(Well defined): $P_1(\alpha) = P_2(\alpha) \Rightarrow f \mid P_1 - P_2$

$\therefore P_1(\beta)$ equal

$\therefore \Phi \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \Rightarrow$ Precisely n such embeddings.

(b) Let $\{ d_1, \dots d_n \}$ be an integral basis of $\mathcal{O}_K$:

$d_K = \det(\sigma_i(d_j))^2$, $G = \text{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{ \sigma_1, \dots \sigma_n \}$

Let $\sigma_1, \dots \sigma_r$ be real embeddings; $(\sigma_{r+1}, \sigma_{r+s}) \dots (\sigma_{r+s-1}, \sigma_{r+2s})$ be complex embeddings pair.

Let $\det(\overline{(\sigma_i(d_j))}) = \det(\overline{(\sigma_i(d_j))}) \cdot (-1)^s$ as conjugation swaps exactly s pairs of rows.

$\therefore$ If s is odd: $\det(\overline{\sigma_i(d_j)}) = -\det(\sigma_i(d_j)) \Rightarrow \det(\sigma_i(d_j)) \in i\cdot\mathbb{R}$

If s is even: $\det(\overline{\sigma_i(d_j)}) = \det(\sigma_i(d_j)) \Rightarrow \det(\sigma_i(d_j)) \in \mathbb{R}$

$\therefore d_K < 0$ if s is odd

> 0 if s is even

No.: Date:

(b) $f(x) = X^3 + 2X^2 + 1$

(mod 3): f irreducible in $\mathbb{F}_3 \Rightarrow$ Irreducible in $\mathbb{Z} \Rightarrow$ Irreducible in G

$\text{Disc}(f) = (-1)^3 N_{L/G}(f'(\theta))$

$f'(\theta) = 3\theta^2 + 4\theta = \theta(3\theta+4) = (-3)\cdot\theta(-4/3 - \theta)$

$\therefore N(f'(\theta)) = (-3)^3 \cdot \underbrace{N(\theta)}_{(-1)} \underbrace{N(-4/3 - \theta)}_{f(-4/3)}$

$= 3^3 \cdot \left\{ (-4/3)^3 + 2(-4/3)^2 + 1 \right\}$

$= -64 + 6\times 16 + 27 = 59$ is square free.

$\Delta(1, \theta, \theta') = \text{Disc}(f) \Rightarrow$

$\therefore \{1, \theta, \theta^2\}$ must be an integral basis.

(c) If $\sigma_j \in \text{Hom}_G(k, \mathbb{C})$, $\bar{\sigma}_j(\alpha) = \overline{\sigma_j(\alpha)}$ be its conjugate.

If $\sigma_j(\alpha) \in \mathbb{R}$: $|\sigma_j(\alpha)| = 1 \Rightarrow \sigma_j(\alpha) = 1$ or $-1 \Rightarrow \alpha = 1$ or -1

$\therefore |N_{k/G}(\alpha)| = 1$

Else: $\forall\, \sigma_j \notin \mathbb{R}$; $G(\sigma_j(\alpha) + \overline{\sigma_j(\alpha)}) \neq G(\sigma_j(\alpha))$

Let $\alpha_j = \sigma_j(\alpha)$: $G \leq \underbrace{G(\alpha_j + \bar{\alpha}_j)}_{F} \leq \underbrace{G(\alpha_j, \bar{\alpha}_j)}_{M}$

$\because \alpha_j$ root of $t^2 - (\alpha_j + \bar{\alpha}_j)t + |\alpha_j|^2 \in F[t]$

$\therefore N_{F(\alpha_j)/F}(\alpha_j) = 1$

$\therefore \left(N_{G(\alpha_j)/G}(\alpha_j)\right)^{[F(\alpha_j):G(\alpha_j)]} = N_{F(\alpha_j)/G}(\alpha_j)$

$= 1$

$\therefore N_{G(\alpha)/G}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = N_{G(\alpha_j)/G}(\alpha_j) \Rightarrow |N_{G(\alpha)/G}(\alpha)| = 1$

(*)

No.: Date:

If $\alpha \in \mathcal{O}_K$: $|N(\alpha)| = 1$ iff $\alpha \in \mathcal{O}_K^\times$

$\therefore$ If $|\sigma_j(\alpha)| = 1$ for some j : $N(\alpha) = 1$ or -1 $\Rightarrow$ $N(\alpha) \in \mathcal{O}_K^\times$

($1/\alpha = \sigma_1(\alpha) \cdot \underbrace{\prod_{i=2}^{n} \sigma_i(\alpha)}_{\text{integral}}$ $\Rightarrow$ $1/\alpha \in \mathcal{O}_K^\times$)

$= 1/\sigma_1(\alpha) \in K$ $\&$ $\sigma_1 \in$

(iii) Let $\alpha = (3+4i)/5$, $K = \mathbb{Q}(i)$

$\sigma_i(\alpha) \in \left\{ (3 \pm 4i)/5 \right\}$; $\left| (3 \pm 4i)/5 \right| = 1$

But $\mathrm{Tr}(\alpha) = 6/5 \notin \mathbb{Z}$ $\Rightarrow$ $\alpha \in K \setminus \mathcal{O}_K$.

2) (a) If $I = \prod_{i=1}^{k} P_i^{m_i}$: $P_i^{m_i} \mid I$; iff $I \subseteq P_i^{m_i}$

$\therefore I \subseteq \bigcap_{i=1}^{k} P_i^{m_i} \Rightarrow \bigcap_{i=1}^{k} P_i^{m_i} \mid I$

But $\forall i$, $P_i^{m_i} \supseteq \bigcap_{i=1}^{k} P_i^{m_i} \Rightarrow P_i^{m_i} \mid \bigcap_{i=1}^{k} P_i^{m_i}$

$\therefore I \mid \bigcap_{i=1}^{k} P_i^{m_i} \Rightarrow I = \bigcap_{i=1}^{k} P_i^{m_i}$

Claim: $\Phi : \mathcal{O}_K/I \to \prod_{i=1}^{k} \mathcal{O}_K/P_i^{m_i}$, $\Phi(x) = (x, \dots x)$ is a ring homomorphism

(Well defined): If $x \sim y$ $x_1 - x_2 \in I$: $x_1 - x_2 \in P_i^{m_i} \Rightarrow \Phi(x_1) = \Phi(x_2)$

Φ is a ring homomorphism.

No.: Date:

(Injective) $\Phi(x) = 0 \Leftrightarrow x \in p_i^{m_i}$ $(1 \le i \le r) \Leftrightarrow x \in \bigcap_{i=1}^{r} p_i^{m_i}$

$\therefore x \in I$ $\ker(\Phi) = I \Rightarrow$ Map is injective.

(Surjective): For each i, $p_i^{m_i} + \prod_{j:j\neq i} p_j^{m_j} = (1)$

Fix $a \in p_i^{m_i}$, $b \in \prod_{j\neq i} p_j^{m_j}$ s.t. $a+b = (1)$

$\Phi(b)_i : b \equiv b+a \equiv 1 \pmod{p_i^{m_i}}$

$\Phi(b)_j \ (j\neq i) : b \equiv 0 \pmod{p_j^{m_j}}$

$\therefore \Phi(b) = e_i$

Since $\{e_1, \dots e_n\}$ generates $\prod_{i=1}^{n} O_K/p_i^{m_i}$: Φ is surjective

$\therefore$ Ring Isomorphism.

(b) Let $I' = \prod_{i=1}^{r} p_i^{m_i+1}$: Pick $x_i \in p_i^{m_i} \setminus p_i^{m_i+1}$.

$\nexists y$ s.t. $y + I' = (x_i + p_i^{m_i+1})_{i=1,\dots r}$.

If $y \in p_i \cdot I$: $y \in \bigcap p_i^{m_i+1} \supseteq p_i \cdot I$ $\therefore$ Contradiction

$y - x_i \in p_i^{m_i+1} \subseteq p_i^{m_i} \Rightarrow y \in p_i^{m_i}$ $(x_i \in p_i^{m_i})$

$\therefore y \in \bigcap_{i=1}^{m} p_i^{m_i} = I$.

Given ideal I: Pick $\alpha \in I$, $\alpha \notin p_i I$ $(\forall i = 1 \dots r)$,

where I has prime factorisation $\prod_{i=1}^{r} p_i^{e_i}$

Consider factorisation of (α): $p_i^{e_i} \| (\alpha)$ $(i=1,\dots r)$ $\Rightarrow (\alpha) = \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{j=1}^{s} q_j^{f_j}$

No.: Date:

Let $I' = \prod_{j=1}^{s} q_j^{f_j}$ (q_j are prime ideals, distinct from $P_1, \dots P_r$)

$I' + I = (1)$ (No common factors)

$I \cdot I' = (\alpha)$ is principal.

By a similar argument, we can pick $\beta \in I$ s.t.

$\beta \notin q_i I$ $(1 \le i \le s)$; $I \subseteq (\beta) \Rightarrow \prod_{i=1}^{r} P_i^{e_i} \mid N(\beta)$

$\therefore GCD((\beta), (\alpha)) = \prod_{i=1}^{r} P_i^{e_i} = I$

$\therefore (\beta) + (\alpha) = I \Rightarrow I = (\alpha, \beta)$ //

(b) Dedekind Criterion: Let K be a number field, $\alpha \in O_K$, $p \in \mathbb{N}$ be a prime

If $p \nmid [O_K : \mathbb{Z}[\alpha]]$: Let $f \in \mathbb{Z}[t]$ be min. poly. of α.

$\bar{f}$ be $f \pmod p$; $\bar{f} = \prod_{i=1}^{r} \bar{g}_i^{e_i}$ be prime factorisation in $\mathbb{F}_p[t]$

$(p) = \prod_{i=1}^{r} (p, g_i(\alpha))^{e_i}$

Let $\alpha = \sqrt{d}$: $[O_K : \mathbb{Z}[\alpha]] = 1$ or 2, coprime to any odd prime p.

No.: Date:

$\therefore$ ~~$t^2 - d \equiv t^2$ or $(t+1)^2 \pmod p$~~

$t^2 - d \equiv t^2 \pmod p$ if $p \mid d$. $\Rightarrow (p) = (p, \sqrt{d})^2$

$\equiv t^2 - d \pmod p$ if d is not a square $\Rightarrow (p)$ is prime

$\equiv (t - \sqrt{d})(t + \sqrt{d}) \pmod p$ if d is a square $\Rightarrow$

$(p) = (p, p - \sqrt{d})(p, p + \sqrt{d})$

~~$\therefore$ (p)~~

If p ramifies : (p is odd) $p \mid d$.

$\alpha \in \mathcal{O}_k = \mathbb{Z}[\sqrt{d}] \Rightarrow \alpha = x + y \cdot \sqrt{d}$

$\therefore -1 = x^2 - d y^2 \equiv 0 \pmod p$

$\therefore -1$ is a square in $\mathbb{F}_p$ (reject) as $\mathbb{F}_p^\times \cong C_{p-1}$,

$4 \nmid C_{p-1} \Rightarrow$ No element of order 4.

$\therefore$ p will not ramify.

No.: Date:

4) (a) Let $\Lambda = \{$ all fractional ideals in $K\}$:

Define: $I \sim J$ iff $\exists\, \alpha \in K$ s.t. $I = \alpha \cdot J$

$\sim$ is an equivalence relation; ideal classes are equivalence classes of Λ wrt $\sim$ relation

Since Define $[I] \cdot [J] = [I \cdot J]$:

(Well defined): $I \sim I' = \alpha_1 I_1$, $J = \beta_1 I \cdot J_1$ $\Big\}$ $IJ = \alpha_1 \beta_1 I_1 J_1$ $\therefore [IJ] = [I_1 J_1]$

Operation is closed; & Associative / Commutative inherited from fractional ideal multiplication

$[I] \cdot [(1)] = [(1)] \cdot [I] = [I]$ (unit)

We know all fractional ideals are invertible. $\Rightarrow$ Inverse exists

$\therefore \Lambda / \sim$ is an abelian group (wrt $\cdot$ operation)

(b) $\forall\, J \in$ Cl$_K$: Pick I s.t. $[I \cdot J] = e$.

Pick $\alpha \in I$ s.t. $N((\alpha)) = |N(\alpha)| \leq C_K\, N(I)$

($N(I) \cdot N(I')$)

$\therefore N(I') \in \leq C_K\, N(I)$

But $[I] \cdot [I'] = e \Rightarrow [I'] = [J]$

$\therefore$ Any J represented by ideal of norm $\leq C_K$.

$\therefore$ Cl$_K = \{ [I]: N(I) \in \{1, \dots \lfloor C_K \rfloor\} \}$

Fix n: If $N(I) = n$: $n \in (I) \Rightarrow (I) \mid (n)$

Since $\therefore (I)$ is a factor of $(n) \Rightarrow$ Finite choices of (I)

$\therefore$ Cl$_K = \bigcup_{r=1}^{\lfloor C_K \rfloor} \{ [\text{no. } I]: N(I) = r \}$ is finite.

No.: Date:

(c) $-33 \equiv 3 \pmod 4 \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{-33}]$; $\omega = \sqrt{-33}$

$|\text{Disc}| = 4 \cdot 33|$; Minkowski Bound $= \left(\frac{4}{\pi}\right)\sqrt{33} < \sqrt{33} < 4/3 \cdot 6 = 8$

$\therefore$ Cl$_K$ generated by prime factors of $(2), (3), (5), (7)$

$f(t) = t^2 + 33$

Dedekind: $(2) = (2, \omega+1)^2$ ($f \equiv (t+1)^2 \pmod 2$)

$(3) = (3, \omega)^2$ ($f \equiv (t)^2 \pmod 3$)

$(5) = (5)$ (inert) ($f \equiv t^2 + 3$ (inert) $\pmod{5!}$)

$(7) = (t-3)(t-4)\,(7, \omega-3)\,(7, \omega-4)$ ($f \equiv (t-3)(t-4) \pmod 7$)

$(2, \omega+1)(3, \omega+3)(7, \omega+3) = (42, \omega+3) = (\omega+3)$ ($\omega+3 \mid 42 = N(\omega+3)$)

$\therefore$ Cl$_K = \langle \alpha, \beta \rangle$, $\alpha = [(3, \omega)]$, $\beta = (7, \omega+3)$

$\alpha\beta$ $[\alpha]^2 = e$.

$(7, \omega+4)^2 = (49, 7(\omega+4), \underbrace{\omega^2 + 8\omega + 16}_{8\omega - 17}) = (49, 7(\omega+4), 8\omega - 17 + 49)$

$= (49, \omega+4) = (\omega+4)$ as $\omega+4 \mid 49 = N(\omega+4)$

$\therefore \beta^{-2} = e \Rightarrow \beta^2 = e$.

($x, y \in \mathbb{Z}$)

If $x^2 + 33y^2 = \pm k$, $k = 3, 7, 21$: (trick $-x$)

LHS $\geq 33y^2 \Rightarrow y = 0$

$x^2 = k$ has no solution

$\therefore$ α, β, $\alpha\beta$ (ideals of norm 3, 7, 21) are not principal

$\Rightarrow \alpha\beta \neq \alpha, \beta$

$\therefore$ Cl$_K = \{e, \alpha, \beta, \alpha\beta\} \cong C_2 \times C_2$.