Problem set 4 – Math 699 – Algebraic number theory

(1) In class, we determined an integral basis for $K = \mathbf{Q}(m^{1/3})$ for $m \not\equiv \pm 1 \pmod 9$ cubefree. In this exercise, you will determine an integral basis when $m \equiv \pm 1 \pmod 9$. In class, we proceeded rather neatly, but this won't work so well here. Recall that we let $\alpha = m^{1/3}$ and $m = ab^2$, where ab is squarefree and $(a, b) = 1$. Throughout, $m \equiv \pm 1 \pmod 9$.

(a) Let $\mu = r + s\alpha + t\alpha^2$ be an arbitrary element of K. Show that

$$\operatorname{tr}(\mu) = 3r$$

and

$$\mathcal{N}(\mu) = r^3 + s^3 m + t^3 m^2 - 3rstm.$$

(b) Let $\nu = \frac{1 \pm \alpha + \alpha^2}{3}$. Show that $\nu \in \mathcal{O}_K$. (Hint: what is its minimal polynomial?

(c) Since $\nu \notin \mathbf{Z}[\alpha]$, conclude that $3 \mid \operatorname{ind}(\alpha)$. From class, this implies that $\operatorname{ind}(\alpha) = 3b$.

(d) Conclude that $\nu, \alpha, \alpha^2/b$ is an integral basis of K. (Hint: what is the determinant of the change of basis matrix from this set to $1, \alpha, \alpha^2$?)

(e) I like integral bases that have the number 1 in them. Show that $1, \nu, \alpha^2/b$ is an integral basis of K.

(2) How much of the argument we used in class to determine the ring of integers for $\mathbf{Q}(m^{1/3})$ when $m \not\equiv \pm 1 \pmod 9$ goes through with $\mathbf{Q}$ adjoin a root of $x^n - m$? What conditions on m make it simpler? What if n is prime? What if m is squarefree or cubefree rather than simply mth power free?[1]

(3) Let K and L be number fields with $K \subseteq L$. Show that $\mathcal{N}_{K/\mathbf{Q}} \circ \mathcal{N}_{L/K} = \mathcal{N}_{L/\mathbf{Q}}$ and $\operatorname{tr}_{K/\mathbf{Q}} \circ \operatorname{tr}_{L/K} = \operatorname{tr}_{L/\mathbf{Q}}$.

(4) (a) Let α be an algebraic number and let f_α be its minimal polynomial, so that $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are its roots. Show that

$$\Delta(f_\alpha) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'_\alpha(\alpha_i).$$

[1] Integral bases for pure quartic fields are given in Takeo Funakura, *On integral bases of pure quartic fields*, Mathematical Journal of Okayama University **57** (1984), no. 1, pp. 27–41.

(b) Let α be an algebraic number and suppose $f_\alpha(x) = x^n + ax + b$. Show that $\Delta(f_\alpha) = (-1)^{\binom{n}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1})$.

(5) (Stickelberger's criterion) If K be a number field, then $\Delta(K) \equiv 0, 1 \pmod 4$. Prove this. (Hint: Recall that if $A = (a_{ij})$ is an $n \times n$ matrix, then

$$\det(A) = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{1,\tau(1)} a_{2,\tau(2)} \cdots a_{n,\tau(n)}.$$

For the matrix $A = (\sigma_i(\alpha_j))$ appearing in the definition of $\Delta(K)$, write $A = E - O$ where E is the sum of even permutations and O is the sum over odd permutations (with the $\operatorname{sgn}(\tau)$ factor removed). Now what?)

(6) (Brill's theorem) It follows from the previous assignment that a number field K of degree n has n embeddings into $\mathbf{C}$. These n embeddings consist of r_1 embeddings into $\mathbf{R}$ and r_2 pairs of complex conjugate embeddings into $\mathbf{C}$ that don't land inside $\mathbf{R}$. The pair (r_1, r_2) is called the *signature* of K. Show that the sign of $\Delta(K)$ is $(-1)^{r_2}$. (Hint: Compare the matrix $(\sigma_i(\alpha_j))$ (whose determinant-squared is the discriminant) to its complex conjugate).

(7) Let $K/\mathbf{Q}$ be a degree 4 extension with Galois group $V_4 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

(a) Draw the subgroup diagram for V_4 and the corresponding intermediate field diagram for $K/\mathbf{Q}$.

(b) Let $K_m = \mathbf{Q}(\sqrt{m})$, $K_n = \mathbf{Q}(\sqrt{n})$, and $K_r = \mathbf{Q}(\sqrt{r})$ (m, n, r, squarefree) denote the three quadratic intermediate extensions of $K/\mathbf{Q}$. Show that $K_r = \mathbf{Q}(\sqrt{mn})$ and that $r = m_1 n_1$, where $m_1 = m/g, n_1 = n/g$, where $g = \gcd(m, n)$.

(c) Since the congruence classes of m, n, r mod 4 affect $\mathcal{O}_{K_m}, \mathcal{O}_{K_n}, \mathcal{O}_{K_r}$, they affect $\mathcal{O}_K$. In the rest of this exercise, you will determine $\mathcal{O}_K$ when $(m, n) \equiv (2, 3) \pmod 4$.[2] Let $\alpha = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{r}$ denote an arbitrary element of K. What are its conjugates? By taking its trace down to K_m, K_n, and K_r, show that if $\alpha \in \mathcal{O}_K$, then $2a, 2b, 2c, 2d \in \mathbf{Z}$.

(d) By taking the norm of $\alpha = \frac{1}{2}(a' + b'\sqrt{m} + c'\sqrt{n} + d'\sqrt{r})$ ($a', b', c', d' \in \mathbf{Z}$) down to K_n, show that $a' \equiv c' \equiv 0 \pmod 2$ and $b' \equiv d' \pmod 2$ in order for α to be in $\mathcal{O}_K$.

(e) Conversely, suppose $\alpha = \frac{1}{2}(a' + b'\sqrt{m} + c'\sqrt{n} + d'\sqrt{r})$ ($a', b', c', d' \in \mathbf{Z}$) with $a' \equiv c' \equiv 0 \pmod 2$ and $b' \equiv d' \pmod 2$. Show that $\alpha \in \mathcal{O}_K$. (Hint: compute the minimal polynomial of α over K_n.

[2]For the remaining cases see Kenneth Williams, *Integers of biquadratic fields*, Canadian Mathematical Bulletin **13** (1970), no. 4, pp. 519–526.

(f) Conclude that $1, \sqrt{m}, \sqrt{n}, \dfrac{\sqrt{m}+\sqrt{r}}{2}$ is an integral basis of $\mathcal{O}_K$.

(g) Compute the discriminant of K.