Problem sheet 8 Solutions

Problem 1

(a) Let $\alpha = 2^{\frac{1}{3}}$. The minimal polynomial of α is $f(x) = x^3 - 2$. Let $\sigma_1, \sigma_2, \sigma_3$ be the complex embeddings of K and let $\alpha_i = \sigma_i(\alpha)$ for $i = 1, 2, 3$. We also write

$$s_1 = \sum_{i=1}^{3} \alpha_i, \quad s_2 = \sum_{i \neq j} \alpha_i \alpha_j, \quad s_3 = \prod_{i=1}^{3} \alpha_i.$$

By Vieta's formulas we get $s_1 = 0$, $s_2 = 0$, and $s_3 = 2$.

We will show that $1, \alpha, \alpha^2$ is an integral basis of K. By Corollary 2.42, we have $\Delta[1, \alpha, \alpha^2] = -108 = -2^2 3^3$. Note that the largest integer N such that $N^2 | \Delta[1, \alpha, \alpha^2]$ is 6. Hence, it is sufficient to prove that for $a_0, a_1, a_2 \in \{0, 1, 2, 3, 4, 5\}$

$$\theta = \frac{1}{6} \sum_{j=0}^{2} a_j \alpha^j$$

is an algebraic integer only if $a_j = 0$ for all $j = 0, 1, 2$.

If θ is an algebraic integer, then

$$\begin{aligned}
N(\theta) = \prod_{i=1}^{3} \sigma_i(\theta) &= \frac{1}{6^3} \prod_{i=1}^{3} (a_0 + a_1 \alpha_i + a_2 \alpha_i^2) \\
&= \frac{1}{6^3} \{a_0^3 + a_1^3 s_3 + a_2^3 s_3^2 + a_0^2 a_1 s_1 + a_0 a_1^2 s_2 + a_0^2 a_2 (s_1^2 - 2 s_2) \\
&\quad + a_0 a_2^2 (s_2^2 - s_1 s_3) + a_1^2 a_2 s_1 s_3 + a_1 a_2^2 s_2 s_3 + a_0 a_1 a_2 (s_2^2 - 3 s_3)\} \\
&= \frac{a_0^3 + 2a_1^3 + 4a_2^3 - 6 a_0 a_1 a_2}{6^3}
\end{aligned}$$

is also an integer. One can check that $a_0^3 + 2a_1^3 + 4a_2^3 - 6a_0 a_1 a_2$ is divisible by 6^3 only if $a_0 = a_1 = a_2 = 0$, hence $1, \alpha, \alpha^2$ is an integral basis of K.

(b) For $K = \mathbb{Q}(2^{\frac{1}{3}})$ we have $d = 3$, $r = 3$, and $s = 0$. We calculate the Minkowski bound:

$$c = \frac{d!}{d^d} \sqrt{|\Delta|} = \frac{3!}{3^3} \sqrt{108} \approx 2.309.$$

The only rational prime $\leq c$ is 2. Note that $\langle 2 \rangle = \mathfrak{p}^3$, where $\mathfrak{p} = \langle 2^{\frac{1}{3}} \rangle$. As $\mathfrak{p}$ is principal, $\mathrm{Cl}(K)$ is trivial.

Problem 2

(a) Let $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Since

$$(x-1)f(x) = x^p - 1 = (x-1)(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}),$$

we obtain the identity $f(x) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1})$. It follows that

$$N(1-\zeta) = \prod_{i=1}^{p-1}(1-\zeta^i) = f(1) = p.$$

Thus, $\langle 1-\zeta\rangle$ is a prime ideal as $N(1-\zeta)$ is prime.

(b) Note that $f(x)$ is the minimal polynomial of ζ and we have

$$f(x) \equiv (x-1)^{p-1} (\text{mod } p).$$

By Dedekind's criterion (Theorem 4.73), $\langle p\rangle = \mathfrak{p}^{p-1}$, where $\mathfrak{p} = \langle 1-\zeta, p\rangle$. Indeed, we have $\mathfrak{p} = \langle 1-\zeta\rangle$ as $1-\zeta | f(1) = p$. It follows from $\langle p\rangle = \langle 1-\zeta\rangle^{p-1} = \langle (1-\zeta)^{p-1}\rangle$ that there exists $u \in O_F^\times$ such that $p = u(1-\zeta)^{p-1}$.

(c) Let G be the group of roots of unity in O_F. As the degree of $e^{\frac{2\pi i}{n}}$ goes to infinity as $n \to \infty$, G is a finite abelian group. Let $e^{\frac{2\pi m_1 i}{n_1}}, \cdots, e^{\frac{2\pi m_k i}{n_k}}$, where $\gcd(m_i, n_i) = 1$, be generators of G. Observe that these generate $e^{\frac{2\pi i}{N}}$, where N is the largest common multiple of $n_1, \cdots, n_k$. It follows that G is indeed a cyclic group. Let $\zeta_N = e^{\frac{2\pi i}{N}}$ be a generator of G. Since ζ_N generates ζ, we have $p|N$. On the other hand, it follows from $\zeta_N \in O_F$ that $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta)$, hence $\phi(N) = [\mathbb{Q}(\zeta_N) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(p) = p-1$. Elementary number theory implies that N is either p or $2p$. Therefore, $G = \{\pm\zeta^s : s \in \mathbb{Z}\}$.

(d) The argument in (b) still works even if we replace ζ with ζ^r for r coprime to p. We thus have $\langle p\rangle = \langle (1-\zeta^r)^{p-1}\rangle = \langle (1-\zeta^s)^{p-1}\rangle$ for r, s coprime to p. It follows that $\langle 1-\zeta^r\rangle = \langle 1-\zeta^s\rangle$, hence there exists $u \in O_F^\times$ such that $1-\zeta^r = u(1-\zeta^s)$.

Problem 3

Let $s_1, \cdots, s_n$ be the elementary symmetric polynomials in n variables. Let $\sigma_1, \cdots, \sigma_n$ be the complex embeddings and denote $\alpha_i = \sigma_i(\alpha)$ for $i = 1, \cdots, n$. If $|\alpha_i| \le N$ for all i, then $|s_k(\alpha_1, \cdots, \alpha_n)| \le 2^n N^n$ for any $1 \le k \le n$. In particular, there are only finitely many integral polynomials $x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ satisfying this bound. It implies that there are only finitely many α with conjugates of bounded complex absolute value.