Lent 2024 **Number Fields – Example Sheet 1** P.P. Varjú

1. Find the minimal polynomials over $\mathbf{Q}$ of

$$(1+i)\sqrt{3}, \qquad i+\sqrt{3}, \qquad 2\cos(2\pi/7).$$

2. Which of the following are algebraic integers?

$$\sqrt{5}/\sqrt{2},\ (1+\sqrt{3})/2,\ (\sqrt{3}+\sqrt{7})/2,\ \frac{3+2\sqrt{6}}{1-\sqrt{6}},\ (1+\sqrt[3]{10}+\sqrt[3]{100})/3,\ 2\cos(2\pi/19).$$

3. Let f be a monic polynomial with algebraic integer coefficients. Prove that the roots of f are algebraic integers.

4. Let K be a number field. Show that every extension $L|K$ of degree 2 is of the form $L = K(\sqrt{\alpha})$ with $\alpha \in K^\times$, $\alpha \notin (K^\times)^2$. Show further that there is a isomorphism $K(\sqrt{\alpha}) \cong K(\sqrt{\beta})$ inducing the identity on K if and only if $\alpha/\beta \in (K^\times)^2$.

5. Let $m \neq 0, 1 \in \mathbf{Z}$ be square-free, and let $K = \mathbf{Q}(\sqrt{m})$. Prove that

$$\mathcal{O}_K = \begin{cases} \left\{a + b\cdot\frac{1+\sqrt{m}}{2} : a, b \in \mathbf{Z}\right\} & \text{if } m \equiv 1 \mod 4, \\ \{a + b\sqrt{m} : a, b \in \mathbf{Z}\} & \text{otherwise.} \end{cases}$$

6. Let $K = \mathbf{Q}(\theta)$ where θ is a root of $X^3 - 2X + 6$. Show that $[K : \mathbf{Q}] = 3$ and compute $N_{K|\mathbf{Q}}(\alpha)$ and $\mathrm{Tr}_{K|\mathbf{Q}}(\alpha)$ for $\alpha = n - \theta$, $n \in \mathbf{Z}$ and $\alpha = 1 - \theta^2, 1 - \theta^3$.

7. Let $d \in \mathbf{Z}_{\geq 1}$ and $\alpha_1, \ldots, \alpha_d \in \mathbf{C}$. Prove that

$$\det(\alpha_i^{j-1}) = \prod_{1\leq i<j\leq d} (\alpha_j - \alpha_i)$$

with both i and j in the determinant running through $1, \ldots, d$.

Let K be a number field of degree d, and let $\alpha \in K$. Conclude that

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{d-1}) = \prod_{1\leq i<j\leq d} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

If $K = \mathbf{Q}(\alpha)$, and f is the minimal polynomial of α, then conclude

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{d-1}) = (-1)^{d(d-1)/2}\mathbf{N}_{K|\mathbf{Q}}(f'(\alpha)).$$

8. Let $K = \mathbf{Q}(\delta)$ where $\delta = \sqrt[3]{m}$ and $m \neq 0, \pm 1$ is a square-free integer. Show that $\mathrm{disc}(1, \delta, \delta^2) = -27m^2$. By calculating the traces of θ, $\delta\theta$, $\delta^2\theta$, and the norm of θ, where $\theta = u + v\delta + w\delta^2$ with $u, v, w \in \mathbf{Q}$, show that the ring of integers $\mathcal{O}_K$ of K satisfies

$$\mathbf{Z}[\delta] \subset \mathcal{O}_K \subset \tfrac{1}{3}\mathbf{Z}[\delta].$$

9. Let $d \in \mathbf{Z}_{\geq 2}$, let $f(X) = X^d + aX + b$ with $a, b \in \mathbf{Q}$, and let $\theta \in \mathbf{C}$ be a root of f. Write down the matrix representing multiplication by $f'(\theta)$ with respect to the basis $1, \theta, \ldots, \theta^{d-1}$ for K. Hence show that

$$\mathrm{disc}(1, \theta, \ldots, \theta^{d-1}) = (-1)^{\binom{d}{2}}\big((1-d)^{d-1}a^d + d^d b^{d-1}\big).$$

10. Compute an integral basis for $\mathcal{O}_K$ in the cases $K = \mathbf{Q}[X]/(X^3 + X + 1)$ and $K = \mathbf{Q}[X]/(X^3 - X - 4)$.

11. Let $K = \mathbf{Q}(i, \sqrt{2})$. By computing the relative traces $\mathrm{Tr}_{K|k}(\theta)$ where k runs through the three quadratic subfields of K, show that the algebraic integers θ in K have the form $\frac{1}{2}(\alpha + \beta\sqrt{2})$, where $\alpha = a + ib$ and $\beta = c + id$ are Gaussian integers. By considering $N_{K|k}(\theta)$ where $k = \mathbf{Q}(i)$ show that

$$\begin{aligned} a^2 - b^2 - 2c^2 + 2d^2 &\equiv 0 \pmod 4, \\ ab - 2cd &\equiv 0 \pmod 2. \end{aligned}$$

Hence prove that an integral basis for $\mathcal{O}_K$ is $1, i, \sqrt{2}, \frac{1}{2}(1+i)\sqrt{2}$, and calculate the discriminant of K.

12. Let K be a quadratic field and $I \subset \mathcal{O}_K$ an ideal. Show that $I = (\alpha, \beta)$ for some $\alpha \in \mathbf{Z}$ and $\beta \in \mathcal{O}_K$. Let $c = \gcd(\alpha^2, \alpha \ \mathrm{Tr}_{K|\mathbf{Q}}\, \beta, N_{K|\mathbf{Q}}\beta)$. By computing the norm and trace show that $\frac{\alpha\beta}{c} \in \mathcal{O}_K$. Deduce that $(\alpha, \beta)(\alpha, \beta')$ is principal, where $\beta\beta' = N_{K|\mathbf{Q}}\beta$.