Algebraic Number Theory
Example Sheet 2

Hand in the answers to questions 4, 6, 8. Deadline 2pm Thursday, Week 5.

0. Let $d \in \mathbb{Q}$ be a non-cube and let $\zeta = \exp(2\pi i/3)$. Show that the map
$$\tau \; : \; \mathbb{Q}(\sqrt[3]{d}) \to \mathbb{Q}(\zeta\sqrt[3]{d})$$
given by
$$\tau(a + b\sqrt[3]{d} + c\sqrt[3]{d}^2) = a + b\zeta\sqrt[3]{d} + c\zeta^2\sqrt[3]{d}^2$$
is an isomorphism of fields. [1]

1. (i) Let d be a non-square and $K = \mathbb{Q}(\sqrt{d})$. Describe the embedddings σ_1, $\sigma_2 : K \hookrightarrow \mathbb{C}$. What is the signature of K? Are $\sigma_1(K)$ and $\sigma_2(K)$ different?
   (ii) Let d be a non-cube and $K = \mathbb{Q}(\sqrt[3]{d})$. Describe the embeddings σ_1, σ_2, $\sigma_3 : K \hookrightarrow \mathbb{C}$. What is the signature of K? Are the $\sigma_j(K)$ different?

2. Let $\sigma : \mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{C}$ be given by $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$. Explicitly write down the embeddings $\tau : \mathbb{Q}(\sqrt{5}, \sqrt{6}) \hookrightarrow \mathbb{C}$ that extend σ.

3. Which integers $-10 \le D \le 10$ are discriminants of quadratic fields?

4. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 2X - 2$. Compute an integral basis for $\mathcal{O}_K$. What is Δ_K?

5. Suppose $f = X^3 + bX + c \in \mathbb{Q}[X]$ is irreducible and let θ be a root. Let $K = \mathbb{Q}(\theta)$. Show that
$$\Delta(1, \theta, \theta^2) = -4b^3 - 27c^2.$$
Memorise this formula! You're expected to quote it when needed.

6. Let θ be as in Q4. Show carefully [2] that $\mathbb{Q}(\theta) \ne \mathbb{Q}(\sqrt[3]{d})$ for any non-cube d. Thus not all cubic fields are of the form $\mathbb{Q}(\sqrt[3]{d})$.

7. Let $\theta = \sqrt[3]{10}$. Show that $(1 + \theta + \theta^2)/3$ is an algebraic integer. Compute an integral basis for $K = \mathbb{Q}(\theta)$. What is Δ_K? (The answer is -300).

8. Let p be an odd prime and let $\zeta = \exp(2\pi i/p)$. Recall that this has minimal polynomial
$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \frac{X^p - 1}{X - 1}.$$
   (i) Write down a basis for $\mathbb{Q}(\zeta)/\mathbb{Q}$.

[1] **Hint:** If you try to do this by simply using the definition of an isomorphism then you just make a mess. Instead look at your lecture notes and find a lemma that gives you this.

[2] **Hint:** Let $\eta = \sqrt[3]{d}$ and suppose $K = \mathbb{Q}(\eta)$. Then $1, \theta, \theta^2$ and $1, \eta, \eta^2$ are both $\mathbb{Q}$-bases for K. What do we know about the ratio $\Delta(1, \theta, \theta^2)/\Delta(1, \eta, \eta^2)$?

(ii) Explain why the conjugates of ζ are

$$\zeta_1 = \zeta, \quad \zeta_2 = \zeta^2, \quad \zeta_3 = \zeta^3, \ldots, \quad \zeta_{p-1} = \zeta^{p-1}.$$

(iii) Compute the following:

$$\mathrm{Trace}(\zeta^j), \qquad \mathrm{Norm}(\zeta^j), \qquad \mathrm{Norm}(\zeta^j - 1)$$

for $j \in \mathbb{Z}$.

(iv) Show that

$$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = \prod_{1 \le i < j \le p-1} (\zeta_i - \zeta_j)^2 = (-1)^{(p-1)/2} \cdot \prod_{\substack{1 \le i, j \le p-1, \\ i \ne j}} (\zeta_i - \zeta_j).$$

(v) Show that [3]

$$\Phi'(\zeta_i) = \prod_{\substack{1 \le j \le p-1, \\ j \ne i}} (\zeta_i - \zeta_j)$$

and thus

$$\prod_{i \ne j} (\zeta_i - \zeta_j) = \prod_{i=1}^{p-1} \Phi'(\zeta_i) = \mathrm{Norm}_{K/\mathbb{Q}}(\Phi'(\zeta)).$$

(vi) By differentiating the identity

$$(X - 1)\Phi(X) = X^p - 1$$

show that $\Phi'(\zeta) = p\zeta^{p-1}/(\zeta - 1)$.

(vii) Deduce that

$$\Delta(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{(p-1)/2} p^{p-2}.$$

(viii) Show that $1, \zeta, \ldots, \zeta^{p-2}$ is an integral basis for $\mathcal{O}_K$. What is the discriminant Δ_K?

9. Let K be a number field. We say that K is **totally real** if all its embeddings are real. Show that if K is totally real then the discriminant Δ_K is positive.

10. Let K be a number field and let $\alpha \in \mathcal{O}_K$. Let $I = (\alpha)$ be the principal ideal of $\mathcal{O}_K$ generated by α. Write I^+ for I viewed as an additive subgroup of $\mathcal{O}_K^+$. Compute $\Delta(I^+)$ in terms of Δ_K and $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)$.

11. For this exercise you might need to revise the definition of a **unit** and of the **unit group** of a ring. This exercise is about the units and unit groups of $\mathcal{O}_K$ with K a number field.
   (i) Show that $\alpha \in \mathcal{O}_K$ is a unit if and only if $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.
   (ii) Show that $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$. Deduce that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.
   (iii) Let $K = \mathbb{Q}(\sqrt{d})$ where d is a squarefree negative integer. Determine the possibilities for the unit group of $\mathcal{O}_K$. You should have different answers for $d = -1$, $d = -3$ and $d \ne -1, -3$.

---

[3]**Hint:** Start with the identity $\Phi(X) = \prod_{i=1}^{p-1}(X - \zeta_i)$ and differentiate both sides, employing the product rule.

12. Let ω be an algebraic integer.
    (i) Show that some conjugate of ω has absolute value ≥ 1.
    (ii) Suppose further that $\mathrm{Norm}(\omega) = 1$. Show that that some conjugate has absolute value ≤ 1.
    (iii) (Hard!) With the help of (ii), show that $X^n + X + 3$ is irreducible over $\mathbb{Q}$ for all $n \geq 2$.

13. Let γ be an algebraic integer which is real and > 1. Suppose all other conjugates of γ have absolute value < 1. Show that $\mathrm{Trace}(\gamma^n) - \gamma^n \to 0$ as $n \to \infty$.

14. Let, for $n \geq 1$,
$$M_n = (1 + \sqrt{2})^n + (1 - \sqrt{2})^n.$$
Show (without expanding brackets) that $M_n \in \mathbb{Z}$, and that moreover it is the nearest integer of $(1 + \sqrt{2})^n$.