B3.4 Algebraic Number Theory, Hilary 2020

Exercises 1

Q 1. Show that the polynomial $X^3 - X - 1 = 0$ is irreducible. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $X^3 - X - 1 = 0$. Express $\beta = \frac{1}{\alpha+1}$ as an element of $\mathbb{Q}[\alpha]$. Is β an algebraic integer?

Q 2. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and let $\alpha = \sqrt{2} + \sqrt{3}$.

(i) What is the degree $[K : \mathbb{Q}]$?

(ii) What are the conjugates of α?

(iii) Show that $K = \mathbb{Q}(\alpha)$.

(iv) Compute $\mathbf{N}_{K/\mathbb{Q}}(\alpha)$.

(v) Find the minimal polynomial of α.

(vi) Is $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$? (*Hint: consider numbers of the form* $a\sqrt{2} + b\sqrt{6}$).

Q 3. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = 2^{1/3}$. Evaluate $\mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \alpha^2)$.

Q 4. Let $K = \mathbb{Q}(\sqrt{d})$, $d < 0$ squarefree, be an imaginary quadratic field. Write $u(d)$ for the number of units in $\mathcal{O}_K$. What are the possible values of $u(d)$, and for which fields are these values attained?

Q 5. Suppose that β is a root of $X^3 + pX + q = 0$, where $X^3 + pX + q$ is an irreducible polynomial in $\mathbb{Z}[X]$, and let $K = \mathbb{Q}(\beta)$. Compute $\mathrm{tr}_{K/\mathbb{Q}}(\beta^i)$ for $i = 0, 1, \ldots, 4$. Deduce that $\mathrm{disc}_{K/\mathbb{Q}}(1, \beta, \beta^2) = -4p^3 - 27q^2$. Hence, give an example of a cubic number field K such that $\mathcal{O}_K$ has a power integral basis.

Q 6. Let $f(X) = X^3 - X^2 - 2X - 8$.

(i) Show that f is irreducible over $\mathbb{Q}$.

(ii) Let α be a root of f and let $K = \mathbb{Q}(\alpha)$. Show that $\frac{1}{2}\alpha(\alpha + 1) \in \mathcal{O}_K$. (*Hint: you might want to first show that* $4/\alpha \in \mathcal{O}_K$.)

(iii) Calculate $\mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \frac{1}{2}\alpha(\alpha+1))$, and hence conclude that e_1, e_2, e_3 is an integral basis for $\mathcal{O}_K$, where $e_1 = 1$, $e_2 = \alpha$ and $e_3 = \frac{1}{2}\alpha(\alpha + 1)$. (*Hint:* you may want to use the result of Question 5.)

Q 7. Suppose that $[K : \mathbb{Q}] = n$, and that, of the n embeddings $\sigma_i : K \to \mathbb{C}$, r_1 of them are real and there are r_2 complex conjugate pairs, where $r_1 + 2r_2 = n$. Show that the sign of Δ_K is $(-1)^{r_2}$.

Q 8. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = 2^{1/3}$. Show that $1, \alpha, \alpha^2$ is an integral basis for $\mathcal{O}_K$, and hence evaluate Δ_K (you may use the result of Question 3).

Q 9. Let $K = \mathbb{Q}(\sqrt{2})$.

(i) Show that if u is a unit in $\mathcal{O}_K$ other than ± 1 then precisely one of the units $\pm u^{\pm 1}$ is *positive*, that is to say is $a + b\sqrt{2}$ with $a, b > 0$. Show that the positive units are precisely those strictly bigger than 1.

(ii) Find the smallest positive unit u.

(iii) Show that the positive units are precisely $u, u^2, u^3, \dots$.

(iv) Hence, describe how to find all positive solutions $(x_i, y_i) \in \mathbb{N}^2$ to Pell's equation $x_i^2 - 2y_i^2 = 1$.

(v) Supposing these are listed in order $x_1 < x_2 < x_3 < \dots$ of increasing size, find a recurrence relation expressing x_n in terms of x_{n-1} and x_{n-2} for $n \geqslant 3$.

ben.green@maths.ox.ac.uk