June 20, 2022

NUMBER THEORY I, 20/6/2022

Each question is 4 points (each complete exercise 8 points; total 32 points).

Exercise 1. (1) Find an integral basis and the discriminant of $K = \mathbb{Q}[\sqrt{7}]$.

(2) Let $\mathcal{O}_K$ be the ring of algebraic integers of K. Show that, for the euclidean topology of the real numbers $\mathbb{R}$, the point $0 \in \mathbb{R}$ is an accumulation point for the set $\mathcal{O}_K$ (*i.e.* for each real number $\epsilon > 0$, there exists $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, such that $\alpha \in (-\epsilon, \epsilon)$).

Exercise 2. (1) Let p be an odd prime and $\mathbb{Q}(\zeta_p)$ the p-th cyclotomic field, where ζ_p is a primitive p-th root of unity. In the ring of integers $\mathbb{Z}[\zeta_p]$ of $\mathbb{Q}(\zeta_p)$, show that $\alpha \in \mathbb{Z}[\zeta_p]$ is a unit if and only if $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha) = \pm 1$, where $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha)$ is the norm of α.

(2) Find the fundamental unit of the field $K = \mathbb{Q}[\sqrt{7}]$.

Exercise 3. Let $K = \mathbb{Q}[\sqrt{7}]$ and write $\mathcal{O}_K$ for its ring of algebraic integers. Show that the class number of K is equal to 1 in the following two steps.

(1) Show that $2 = \mathfrak{p}^2$ is ramified K and the prime ideal $\mathfrak{p}$ is principal. [Hint: look at the factorisation $2 = (3+\sqrt{7})(3-\sqrt{7})$ and show that the two ideals $(3+\sqrt{7})$ and $(3-\sqrt{7})$ are equal; for this last step, compute the quotient $\frac{3+\sqrt{7}}{3-\sqrt{7}}$.]

(2) Calculate the Hasse bound of K and conclude.

Exercise 4. (1) Find a prime number number ℓ_1 which is split and a prime number ℓ_2 which is inert in the quadratic field $\mathbb{Q}[\sqrt{7}]$

(2) Let $p \geq 5$ be a prime number. Prove that 3 is a square modulo p if and only if $p \equiv \pm 1 \pmod{12}$. [Hint: Use Gauss quadratic reciprocity law, and observe that a odd prime number $p \neq 3$ must be congruent to 1, 5, 7 or 11 modulo 12.]]