ÉNS Lyon
2017-2018

Number Theory
M1

Exercise sheet 1
Number fields

Exercise 1.

Let $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

(a) Find $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$.

(b) Give the values of all different embeddings $K \hookrightarrow \mathbb{C}$ at $\sqrt{2}$ and $\sqrt{3}$, and the trace and norm of $\sqrt{2}$ and $\sqrt{3}$ over $\mathbb{Q}$.

Exercise 2. [Norm on a number field]

Let K be a number field.

(a) For every $\alpha \in K$, prove that $\alpha = 0 \iff N_{K/\mathbb{Q}}(\alpha) = 0$. If $\alpha \in \mathcal{O}_K$, prove that $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Is it an equivalence ?

(b) Prove that the units of $\mathcal{O}_K$ are exactly the $\alpha \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

(c) Prove that for $\alpha \in \mathcal{O}_K$, if $N_{K/\mathbb{Q}}(\alpha)$ is a prime number, then α is irreducible in $\mathcal{O}_K$. Is it an equivalence ?

Exercise 3. [Discriminant]

(a) For $P \in \mathbb{Q}[X]$ irreducible of degree d and α a root of P, $K = \mathbb{Q}(\alpha)$, prove that

$$\mathrm{disc}(1, \alpha, \cdots, \alpha^{d-1}) = (-1)^{d(d-1)/2} N_{K/\mathbb{Q}}(P'(\alpha)).$$

(b) Let $d \in \mathbb{Z} \backslash \{0, 1\}$ and $K = \mathbb{Q}(\sqrt{d})$. Compute $\mathrm{disc}(1, \sqrt{d})$.

(c) For $P = X^3 + aX + b \in \mathbb{Q}[X]$ irreducible on $\mathbb{Q}$ and α a root of P, compute $\mathrm{disc}(1, \alpha, \alpha^2)$.

Exercise 4. [Taussky's theorem]

Let K be a number field of degree n.

We denote by $(\alpha_1, \cdots, \alpha_n)$ a basis of K over $\mathbb{Q}$, and by $\sigma_1, \cdots, \sigma_n$ the embeddings $K \hookrightarrow \mathbb{C}$, numbered so that the r first ones are the real embeddings and for every $i \in \{r+1, \cdots, r+s\}$, $\overline{\sigma_i} = \sigma_{i+s}$.

(a) Recall the proof of the matrix equality

$$(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))_{i,j} = {}^t M M, \quad M = (\sigma_i(\alpha_j))_{i,j}.$$

(b) Prove there is an invertible matrix $R \in M_n(\mathbb{R})$ such that the $r+s$ first rows of RM are real and the s last ones are pure imaginary.

(c) Define D the diagonal matrix whose first $r+s$ diagonal coefficients are 1 and the last s coefficients are i. Prove that DRM is real, and deduce that ${}^t MM$ is congruent (over $\mathbb{R}$) to $D^{-1t}R^{-1}R^{-1}D^{-1}$.

(d) Prove that $D^{-1t}R^{-1}R^{-1}D^{-1}$ is of the shape

$$\begin{pmatrix} B_1 & 0 \\ 0 & -B_2 \end{pmatrix}$$

with B_1 and B_2 positive definite real symmetric matrices of respective sizes $r+s$ and s.

(e) Prove that the signature of the trace forme over K is $(r+s, s)$. What is the sign of the discriminant of K ?

Exercise 5. [Diophantine approximation]

(a) For any $x \in \mathbb{R}$ and any integer $M \geq 1$, use the pigeonhole principle to prove that there exists $(p, q) \in \mathbb{Z}^2$ with $1 \leq q \leq M$ such that $|qx - p| < 1/M$.

(b) Use it to prove that for any $x \notin \mathbb{Q}$, there are infinitely many rational numbers p/q such that $|x - p/q| < 1/q^2$ (Dirichlet's approximation theorem).

(c) Prove that the number $\sum_{k=0}^{+\infty} 1/2^{k!}$ is transcendental.