# INTRODUCTION À LA THÉORIE ALGÉBRIQUE DES NOMBRES

**TN 1** Set $f_n(X) = X^n - X + 1$.

(1) Show that $\mathrm{disc}(f_n) = \pm(n^n - (n-1)^{n-1})$.

(2) Suppose $n = p$ is prime. Then show that $f_p$ is irreducible in $\mathbb{F}_p[X]$. [hint : prove that no root of $f_p$ belongs to $\mathbb{F}_{p^i}$ for $i < p$.]

(3) Now, let $n = 5$ and put $K := \mathbb{Q}[X]/(f_5)$.

(a) Show that $\mathcal{O}_K = \mathbb{Z}[X]/(f_5)$ [hint : $2869 = 19 \times 151$].

(b) Decompose (2) as a product of prime ideals of $\mathcal{O}_K$ and provide generators of each factor.

(c) Determine $r_1$ and $r_2$. Then prove that $M_K\sqrt{|D_K|} < 4$.

(d) Prove that in fact $\mathcal{O}_K$ is principal.

**TN 2**

Let $K$ be a number field of degree $n$ and discriminant $D_K \in \mathbb{Z}$.

(1) Let $\sigma : K \hookrightarrow \mathbb{C}$ be a complex embedding.

(a) Assume $\sigma(K) \subset \mathbb{R}$. Show that there exists $\alpha \in \mathcal{O}_K$ non zero such that
– $|\sigma(\alpha)| \leqslant 2\sqrt{|D_K|}$, and
– $|\sigma'(\alpha)| < 1$ for any other $\sigma' : K \hookrightarrow \mathbb{C}$ distinct from $\sigma$.

(b) Assume $\sigma(K) \not\subset \mathbb{R}$. Show that there exists $\alpha \in \mathcal{O}_K$ non zero such that
– $|\Im(\sigma(\alpha))| \leqslant \sqrt{|D_K|}$ and $|\Re(\sigma(\alpha))| < 2$, and
– $|\sigma'(\alpha)| < 1$ for any embedding $\sigma' : K \hookrightarrow \mathbb{C}$ not conjugate to $\sigma$.

(2) In both cases, prove that $|\sigma(\alpha)| > 1$. Then prove that $K = \mathbb{Q}(\alpha)$.

(3) Show that the coefficients of $f_\alpha$ are bounded above by $2n!\sqrt{|D_K|}$ and deduce that there are finitely many number fields of given discriminant and degree.

(4) Prove that there are finitely many number fields of given discriminant.

**TN 3** Let $p$ be prime number. We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and we denote by $|.|$ the $p$-adic absolute value on $\overline{\mathbb{Q}}_p$.

(1) Let $n > 1$ be an integer. Compute the degree of $\mathbb{Q}_p(\zeta_n)$ over $\mathbb{Q}_p$, where $\zeta_n$ is a primitive $n^{\text{th}}$ root of unity in $\overline{\mathbb{Q}}_p$.

(2) Let $F, E$ be finite extensions of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$. Assume $E$ is a *totally ramified* extension of $F$, of degree $n$ *prime to* $p$. We will prove that there is a uniformizer $\varpi$ of $\mathcal{O}_F$ such that $E$ is generated by some $n^{\text{th}}$-root of $\varpi$.

(a) We start with a uniformizer $\beta$ of $\mathcal{O}_E$. Show that $\beta^n$ is of the form $\varpi_0 u$ for some uniformizer $\varpi_0$ of $\mathcal{O}_F$ and some unit $u \in \mathcal{O}_E^\times$.

(b) Show that there is a unit $u_0 \in \mathcal{O}_F^\times$ such that $|u - u_0| < 1$ and then, exhibit a uniformizer $\varpi$ of $\mathcal{O}_F$ such that $|\beta^n - \varpi| < |\varpi|$.

(c) Let $\alpha_1, \cdots, \alpha_n$ denote the $n^{th}$-roots of $\varpi$ in $\overline{\mathbb{Q}}_p$. Show that for $i \neq j$ we have $|\alpha_i - \alpha_j| = |\alpha_i| = |\alpha_j| = |\varpi|^{1/n}$. [this is where we use that $n$ is prime to $p$]

(d) Prove that there is a unique index $i$ such that $|\beta - \alpha_i| < |\varpi|^{1/n}$ and then conclude.