5. Notions de trace et norme ; quelques sujets d'examen

Rappel de cours sur trace et norme :

1. Si $K \to L \to M$ est une suite d'extensions de degrés finis telle que $[M : L] = n$ alors pour tout $x \in L$,
$$\mathrm{Tr}_{M/K}(x) = n\mathrm{Tr}_{L/K}(x) \text{ et } \mathrm{N}_{M/K}(x) = (\mathrm{N}_{L/K}(x))^n.$$
2. Si $P = X^n + a_{n-1}X^{n-1} + ... + a_0$ est le polynôme minimal de x sur K alors :
$$\mathrm{Tr}_{K(x)/K}(x) = -a_{n-1} \text{ et } \mathrm{N}_{K(x)/K}(x) = (-1)^n a_0.$$
3. Si L/K est une extension galoisienne de degré fini et de groupe G alors pour tout $x \in L$:
$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x) \text{ et } \mathrm{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$
4. Si L/K est une extension galoisienne de degré fini alors il existe un élément u de L tel que $\mathrm{Tr}_{L/K}(u) \neq 0$.
5. **Théorème d'Hilbert :** Si L/K est une extension galoisienne **cyclique** de groupe $\langle\sigma\rangle$, alors pour tout élément $u \in L$:
   (a) $\mathrm{N}_{L/K}(u) = 1$ si et seulement s'il existe $v \in L$ tel que $u = v(\sigma(v))^{-1}$
   (b) $\mathrm{Tr}_{L/K}(u) = 0$ si et seulement s'il existe $v \in L$ tel que $u = v - \sigma(v)$.

Exercice 5.1 (Sept. 2001) Soit K un corps de caractéristique positive p. Soit L une extension galoisienne cyclique de degré p de K. On note σ un générateur du groupe de Galois de L/K.

1. Prouver qu'il existe $\alpha \in L$ tel que $\mathrm{Tr}_{L/K}(\alpha) = 1$.
2. Montrer qu'il existe $\beta \in L$ tel que $\beta - \sigma(\beta) = \alpha^p - \alpha$.
3. En déduire que le polynôme $X^p - X - \beta$ n'a pas de racine dans L. *(*Indication : Soit θ racine de ce polynôme dans L, montrer que $\omega = \theta - \sigma(\theta) - \alpha \in \mathbb{F}_p \subset K$ et calculer la trace dans L/K de ω pour obtenir une contradiction.*)*

Exercice 5.2 (Juin 2001) Soit $f(X) = X^4 - 4X - 2$. On pose $G = \mathrm{Gal}_{\mathbb{Q}}(f)$.

1. Montrer que f est irréductible sur $\mathbb{Q}$.
2. Prouver que f a exactement deux racines réelles. En déduire que G contient une transposition.
3. Déduire de la factorisation de f modulo 3 que G contient un 3-cycle.
4. Prouver que $G \simeq S_4$.
5. Soit θ une racine de f. Calculer la matrice de la multiplication par $f'(\theta)$ sur la base $\{1, \theta, \theta^2, \theta^3\}$ de $\mathbb{Q}(\theta)$. Puis, calculer $\mathrm{N}_{\mathbb{Q}(\theta)/\mathbb{Q}}(f'(\theta))$ et en déduire le discriminant de f.
6. Soit K le corps des racines de f. Montrer que K contient un unique sous-corps de degré 2 sur $\mathbb{Q}$, et que ce corps est $\mathbb{Q}(\sqrt{-35})$.

Exercice 5.3 (Septembre 98) Soit Ω un corps algébriquement clos de caractéristique nulle. Soit K un sous-corps de Ω tel que l'extension Ω/K est de degré fini. Le but de cet exercice est de montrer que $\Omega = K(i)$.

1. Expliquer pourquoi Ω/K est galoisienne.

On pose i une racine de $X^2 + 1$ dans Ω. On pose $G = \mathrm{Gal}(\Omega/K(i))$. On suppose que G n'est pas trivial et on pose p un nombre premier divisant l'ordre de G.

2. Montrer qu'il existe un sous-corps L de Ω tel que $K(i) \subset L$ et Ω/L est une extension galoisienne de degré p.
3. Montrer que les racines p-èmes de l'unité sont dans L. En déduire que $\Omega = L(\alpha)$ où α est racine du polynôme irréductible $X^p - a \in L[X]$.
4. Soit $\theta \in \Omega$ tel que $\theta^p = \alpha$.
   a. Justifier l'existence de θ.
   b. Calculer $\mathrm{N}_{\Omega/L}(\alpha)$, puis $\mathrm{N}_{\Omega/L}(\theta)$.
   c. En déduire une contradiction. Conclure.

Exercice 5.4 (Avril 2001) Soit

$$P(X) = X^6 + (3 - 2\pi)X^4 + \pi X^3 + (3 - 2\pi)X^2 + 1 \in K[X]$$

où $K = \mathbb{Q}(\pi)$. Le but de cet exercice est de calculer le groupe de Galois $G = \mathrm{Gal}_K(P)$.

1. Montrer qu'il existe $Q(X) \in K[X]$ avec :
$$P(X) = X^3 Q(X + 1/X).$$
2. Montrer que $Q(X)$ est irréductible sur K. On note $H = \mathrm{Gal}_K(Q)$. En déduire que 3 divise l'ordre de H.
3. Montrer que le discriminant de Q n'est pas un carré dans K. *(*Admis : le discriminant de $X^3 + aX + b$ est $-4a^3 - 27b^2$.*)*
   En déduire que $H \simeq S_3$.
4. a. Montrer que Q a trois racines réelles α_1, α_2, α_3, vérifiant les inégalités suivantes :
$$\alpha_1 < -2 < 0 < \alpha_2 < 2 < \alpha_3.$$
   b. Notons β_i une racine de $X^2 - \alpha_i X + 1$ avec $i = 1, 2, 3$. Calculer α_i en fonction de la racine β_i. Montrer que les racines de P sont données par les β_i, β_i^{-1} avec $i = 1, 2, 3$.
   c. Soit L le corps des racines de P sur K, et M le corps des racines de Q sur K. Prouver que L/M est Galois, $N = \mathrm{Gal}(L/M)$ est distingué dans G, puis finalement
$$G/N \simeq H.$$
5. a. Montrer que β_1 et β_3 sont réelles. En déduire que $\beta_2 \notin M(\beta_1, \beta_3)$.
   b. Déduire de l'action de H sur les α_i, que $\beta_i \notin M(\beta_j, \beta_k)$ pour $\{i, j, k\} = \{1, 2, 3\}$.
   c. En déduire que $[L : M] = 8$.
   d. Montrer qu'il existe trois éléments $\sigma_i \in N$, $i = 1, 2, 3$, avec pour tout i et tout $j \neq i$:
$$\sigma_i(\beta_j) = \beta_j \quad \text{et} \quad \sigma_i(\beta_i) = \beta_i^{-1}.$$
   e. Prouver que $N = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle$.
6. En déduire que le groupe G est isomorphe à
$$(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$$
   où l'action de S_3 est donnée par la permutation des coordonnées.