Feuille 3 : Lemme de Hensel, discriminant

Exercice 1 Soit K un corps ultramétrique complet de valeur absolue $|\cdot|$. On note R son anneau de valuation. Soit $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ de degré $n \geq 0$ tel que $a_0 a_n \neq 0$.

1. Si f est irréductible, montrer que
$$\max_{0 \leq i \leq n} |a_i| = \max\{|a_0|, |a_n|\}.$$
2. En déduire que si f est irréductible, unitaire, tel que $a_0 \in R$, alors $f \in R[X]$.

Exercice 2 (Lemme de Hensel, variante)
Soit K un corps ultramétrique complet de valeur absolue $|\cdot|$. On note R son anneau de valuation. Soient $f \in R[X]$ et $\alpha_0 \in R$ tel que $|f(\alpha_0)| < |f'(\alpha_0)|^2$. Pour $i \geq 0$, on introduit la suite
$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)} \quad \text{et on pose} \quad c := \frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2}.$$
1. Montrer que pour tout $i \geq 0$, on a
$$\left| \frac{f(\alpha_i)}{f'(\alpha_i)^2} \right| < c^{2^i}.$$
2. En déduire que la suite (α_i) converge dans R vers une racine α de f, et que de plus, on a
$$|\alpha - \alpha_0| \leq c < 1.$$
3. En déduire que si $|f'(\alpha_0)| = 1$ et $|f(\alpha_0)| < 1$, alors f admet une racine α dans R.

Exercice 3 (Extensions quadratiques de $\mathbb{Q}_2$)
1. Soient K un corps de caractéristique différente de 2 et $\alpha, \beta \in K - K^2$. Montrer que
$$K[\sqrt{\alpha}] = K[\sqrt{\beta}] \iff \exists x \in K^* \ \ \alpha = x^2 \beta.$$
2. Soit $x = 2^n u$ un élément de $\mathbb{Q}_2^*$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_2^\times$ une unité 2-adique. Montrer que $x \in \mathbb{Q}_2^{*2}$ si et seulement si n est pair et $u = 1 \mod 8\mathbb{Z}_2$.
3. En déduire les extensions quadratiques de $\mathbb{Q}_2$.

Exercice 4 (Autres applications de Hensel)
1. Soient ℓ, p deux nombres premiers. Montrer que le corps $\mathbb{Q}_\ell$ est isomorphe au corps $\mathbb{Q}_p$ si et seulement si $\ell = p$.
2. Soit $u \in \mathbb{Q}_p^*$. Montrer que
$$u \in \mathbb{Z}_p^\times \iff \text{il existe une infinité d'entiers } n \text{ tels que } u^{p-1} \in \mathbb{Q}_p^{*n}.$$
3. En déduire que si φ est un endomorphisme de corps de $\mathbb{Q}_p$ alors en notant v_p la valuation p-adique, on a : $\forall x \in \mathbb{Q}_p$, $v_p(\varphi(x)) = v_p(x)$.
4. En déduire que le seul endomorphisme de corps de $\mathbb{Q}_p$ est l'identité.

Exercice 5 Soit A l'algèbre des polynômes de $\mathbb{C}[t]$ dont le coefficient de degré 1 est nul. Montrer que A est une algèbre intègre de type fini sur $\mathbb{C}$. Détermniner son corps des fractions et sa clotûre intégrale.

Exercice 6 (Norme et Trace)
Soient $A \subset B$ des anneaux intègres avec B un A-module libre de rang n. L'élément $\beta \in B$ définit par multiplication une application linéaire $B \to B,\ x \mapsto \beta x$. Le déterminant (resp. la trace) de cette application linéaire est noté $\mathrm{Nm}_{B/A}\beta$ (resp. $\mathrm{Tr}_{B/A}\beta$).

1. Observer que $\mathrm{Nm}_{B/A}\beta\beta' = \mathrm{Nm}_{B/A}\beta \mathrm{Nm}_{B/A}\beta'$.
2. Soient L/K une extension galoisienne de corps de degré n et $y \in L$. Soient $f(X)$ le polynôme minimal de y sur K et $y_1 = y, y_2, \ldots, y_m$ les racines de $f(X)$. Montrer que
$$\mathrm{Tr}_{L/K}\, y = r(y_1 + \cdots + y_m), \quad \mathrm{Nm}_{L/K}\, y = (y_1 \cdots y_m)^r$$
où $r = [L : K[y]] = n/m$ (on pourra commencer par traiter le cas $r = 1$).
3. En déduire que si L/K est séparable de degré n et si $\{\sigma_1, \ldots, \sigma_n\}$ sont les différents K-plongements de L dans une clôture algébrique de L/K, alors, on a
$$\forall y \in L, \quad \mathrm{Tr}_{L/K}\, y = \sum_{i=1}^{n} \sigma_i(y) \quad \text{et} \quad \mathrm{Nm}_{L/K}(y) = \prod_{i=1}^{n} \sigma_i(y).$$

Exercice 7 (Discriminant)
Soient $A \subset B$ des anneaux avec B libre de rang m comme A-module. Soit $\{\beta_1, \ldots, \beta_m\}$ des éléments de B. Le *discriminant de la famille* $\{\beta_1, \ldots, \beta_m\}$ est
$$\mathrm{disc}(\{\beta_1, \ldots, \beta_m\}) := \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j)).$$

1. Montrer que si l'on pose $\mathrm{disc}(B/A) := \mathrm{disc}(\{\text{base de } B/A\})$ on obtient un élément bien défini de $A/(A^\times)^2$.
   Dans le cas particulier où $A = \mathbb{Z}$ et B l'anneau d'entiers $\mathcal{O}_K$ d'un corps de nombres K, le discriminant $\mathrm{disc}(B/\mathbb{Z})$ est un élément bien défini de $\mathbb{Z}$, que l'on appelle *discriminant absolu de* $K/\mathbb{Q}$ et que l'on note $d_{K/\mathbb{Q}}$ ou $d_{\mathcal{O}_K/\mathbb{Z}}$ ou même d_K.
2. Supposons $A = \mathbb{Z}$. Soit N le sous-A-module de B engendré par $\{\gamma_1, \ldots, \gamma_m\}$. Montrer que si le module N est d'indice fini dans B alors
$$\mathrm{disc}(\{\gamma_1, \ldots, \gamma_m\}) = (B : N)^2 \,\mathrm{disc}(B/\mathbb{Z})$$
3. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n avec α un entier algébrique (justifier...). Montrer que si $d = \mathrm{disc}(1, x, \ldots, x^{n-1})$ on a
$$\mathbb{Z}[x] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x].$$

4. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n avec α un entier algébrique. Montrer que si $\mathrm{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\})$ est sans facteur carré, alors

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \quad \text{et} \quad d_K = \mathrm{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\}).$$

5. Soit L/K une extension finie séparable de degré n. Soit $\sigma_1, \ldots, \sigma_n$ les K-homomorphismes distincts de L dans une clôture algébrique de L. Alors pour toute base $\beta_1, \ldots, \beta_n$ de L sur K, montrer que

$$\mathrm{disc}(\beta_1, \ldots, \beta_n) = \det(\sigma_i \beta_j)^2.$$

6. Soit $L = K[\beta]$ et $f(X)$ le polynôme minimal de β sur K. Supposons que $f(X)$ se factorise sous la forme $f(X) = \Pi(X - \beta_i)$ sur une clotûre algébrique de L. Montrer que

$$\mathrm{disc}(1, \beta, \ldots, \beta^{n-1}) = \prod_{i<j} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} \, \mathrm{Nm}_{L/K}(f'(\beta)).$$

   Ce nombre est appelé le *discriminant de* f et noté $\mathrm{disc}(f)$. On pourrait également le définir comme le résultant de f et f'.

Exercice 8 (Applications)
Soient k un corps, $a, b \in k$, $n \in \mathbb{N}\backslash\{0, 1\}$ et $P = X^n + aX + b$. On suppose que P est irréductible et **séparable**.

1. Montrer que

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1} a^n\right).$$

2. Cas particulier où $n = 2$ et $n = 3$.
3. On suppose $n = 3$. Soit x une racine de P dans une clôture algébrique $\overline{k}$ de k et K le corps de décomposition de $k(x)$ dans $\overline{k}$. Montrer que le groupe de Galois $\mathrm{Gal}(K/k)$ est soit isomorphe au groupe symétrique S_3 soit au groupe alterné A_3 et que

$$k(x) = K \iff [K : k] = 3 \iff \mathrm{disc}(P) \text{ est un carré dans } k.$$

4. Déterminer l'anneau des entiers de $\mathbb{Q}[x]$ où x est une racine du polynôme $X^3 - X - 1$ et le groupe de Galois de son corps de décomposition.
5. Calculer le discriminant d'une extension quadratique de $\mathbb{Q}$.