Un théorème de Dedekind à propos de la ramification

Théorème 1 (Dedekind)**.** *Soit K un corps de nombres. Alors un nombre premier p ramifie en K si et seulement si p divise le discriminant Δ_K*

La preuve aura besoin de plusieurs piliers. On commence en introduisant quelques notations. Dans la suite, p est un nombre premier et $\mathfrak{O}$ est l'anneau des entiers de K. On écrit aussi $\overline{\mathfrak{O}}$ au lieu de $\mathfrak{O}/(p)$ et la réduction modulo p, c'est-à-dire, le morphisme $\mathfrak{O} \to \overline{\mathfrak{O}}$, sera notées par $\alpha \mapsto \overline{\alpha}$. On fixe aussi une décomposition de p en idéaux premiers deux-à-deux distincts :

$$\begin{aligned} p\mathfrak{O}_K &= \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \\ &= \mathfrak{p}_1^{e_1} \cap \cdots \cap \mathfrak{p}_r^{e_r}. \end{aligned}$$

(Comme vous avez vu au cours de Théorie de Nombres 1.)

Ramification et existence de nilpotents.— Comme $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathfrak{O}$ si $i \neq j$, le théorème Chinois garantit que

$$\begin{aligned} \pi : \overline{\mathfrak{O}} &\longrightarrow \mathfrak{O}/\mathfrak{p}_1^{e_1} \times \cdots \times \mathfrak{O}/\mathfrak{p}_r^{e_r}, \\ a + (p) &\longmapsto (a + \mathfrak{p}_1^{e_1}, \ldots, a + \mathfrak{p}_r^{e_r}) \end{aligned}$$

est un isomorphisme.

Lemme 2. *Le premier p ramifie si et seulement si l'anneau $\overline{\mathfrak{O}}$ possède un élément nilpotent non-nul.*

Démonstration. ($\Rightarrow$) On suppose $e_1 > 1$. Soit $x \in \mathfrak{p}_1^{e_1-1} \smallsetminus \mathfrak{p}_1^{e_1}$. Clairement $x^2 \in \mathfrak{p}_1^{e_1}$. L'élément

$$(x + \mathfrak{p}_1^{e_1}, 0 + \mathfrak{p}_2^{e_2} \ldots, 0 + \mathfrak{p}_r^{e_r}) \in \prod_i \mathfrak{O}/\mathfrak{p}_i^{e_i}$$

est nilpotent et non-nul.

($\Leftarrow$) Si p ne ramifie pas, alors π induit un isomorphisme entre $\overline{\mathfrak{O}}$ et un produit de *corps*. Clairement, un tel anneau n'a pas de nilpotents non-triviaux. $\square$

La preuve du Théorème suivra ainsi d'une compréhension de comment des propriétés de $\overline{\mathfrak{O}}$ se lisent sur la forme de la trace.

La trace et le discriminant.— On fixe un corps k. Dans la suite, on travaillera exclusivement avec des "k-algèbres finies", c'est-à-dire, des k-algèbres dont la dimension en tant que k-espace vectoriel est finie. Les résultats qui suivent seront appliqués au cas $k = \mathbb{F}_p$, $A = \overline{\mathfrak{O}}$ et $\mathfrak{O}/\mathfrak{p}_i^{e_i}$.

Définition 3. Soit A une k-algèbre finie.

1) Pour chaque élément $a \in A$, on définit la trace de a, notée $\mathrm{Tr}_A(a)$, comme étant la trace de l'application k-linéaire $A \to A$ donnée par $x \mapsto ax$.

2) La *forme de la trace* de A est la forme k-bilinéaire et symétrique $\tau_A : A \times A \to k$ définie par $\tau_A(x, y) = \mathrm{Tr}_A(xy)$.

Si A est une k-algèbre et $\{a_i\}$ et $\{b_i\}$ sont des bases de A, il est bien connu que

$$\det(\tau_A(b_i, b_j)) = \det(P)^2 \cdot \det(\tau_A(a_i, a_j)),$$

où P est la matrice de passage de $\{a_i\}$ à $\{b_i\}$. Ceci nous conduit à la construction suivante.

On considère la relation d'équivalence sur k définie par

$$x \sim y \quad \Leftrightarrow \quad y = xa^2 \text{ avec } a \in k^*.$$

L'ensemble quotient sera noté par k/k^{*2} : la multiplication de k induit une opération $k/k^{*2} \times k/k^{*2} \to k/k^{*2}$ qui donne à k/k^{*2} la structure d'un monoïde multiplicatif. Dans la suite, on abusera la notation et "0" désignera à la fois l'élément nul de k et sa classe dans k/k^{*2}.

Définition 4. Le discriminant de A, noté D_A, est l'élément de k/k^{*2} définie par

$$\det(\tau_A(a_i, a_j)),$$

où $\{a_i\}$ est une k-base arbitraire de A.

Remarques 5.

Exemple 6. Soit $k = \mathbb{Q}$ et K un corps de nombres ayant des plongements $\{\sigma_j : K \to \mathbb{C}\}_{j=1}^n$. On a vu dans les travaux dirigés que, si $\alpha_1, \ldots, \alpha_n$ est une $\mathbb{Q}$-base de K, alors

$$[\det(\sigma_i(\alpha_j))]^2 = \det(\tau_K(\alpha_i, \alpha_j)).$$

Si la base $\alpha_1, \ldots, \alpha_n$ est *de plus* une base entière de $\mathfrak{O}$, alors D_K est la classe de Δ_K dans $\mathbb{Q}/\mathbb{Q}^{*2}$.

Exemple 7. Soit $A = k[X]/(X^2)$. Si x note la classe de X, alors $1, x$ est une base et $\mathrm{Tr}(x) = 0$, comme un calcul simple montre. De plus, $\mathrm{Tr}(xy) = 0$ pour tout $y \in A$ car $\mathrm{Tr}(x(a + bx)) = a \cdot 0 + b\mathrm{Tr}(0) = 0$. Dans ce cas, τ_A est dégénérée, c'est-à-dire, le noyau $\mathrm{Ker}(\tau_A) = \{a \in A : \tau(a, b) = 0, \forall b \in A\}$ est non-nul.

De façon générale, soit A une k-algèbre finie et $a \in A$ un élément nilpotent : $a^n = 0$. Comme pour chaque $b \in A$ on a $(ab)^n = 0 \cdot b^n$, on constate que ab est aussi nilpotent. En utilisant que la trace d'un endomorphisme nilpotent est toujours nulle, on déduit que $\tau_A(a, -) : A \to k$ est la fonction partout nulle. En particulier, la forme bilinéaire τ_A est dégénérée et $D_A = 0$, ou, si D_A appartient à la classe de zéro.

Vue de la décomposition de $\overline{\mathfrak{O}}$ comme produit d'anneaux, l'étude du discriminant de la $\mathbb{F}_p$-algèbre $\overline{\mathfrak{O}}$ aura besoin du

Lemme 8. *Soient $A_1, \ldots, A_n$ des k-algèbres finies. Alors*

$$D_{A_1 \times \cdots \times A_n} = D_{A_1} \cdots D_{A_n}.$$

Démonstration. On fera la preuve dans le cas $n = 2$ parce que le cas général suit par récurrence. Soit $\{a'_i\}_{i=1}^{r_1}$ base de A_1. Soit $\{a''_i\}_{i=1}^{r_2}$ base de A_2. On définit pour $i \in \{1, \ldots, r_1 + r_2\}$:

$$\alpha_i = \begin{cases} (a'_i, 0), & \text{si } 1 \leqslant i \leqslant r_1, \\ (0, a''_{i-r_1}), & \text{si } r_1 + 1 \leqslant i \leqslant r_1 + r_2. \end{cases}$$

Clairement, $\alpha_1, \ldots, \alpha_{r_1+r_2}$ est une base de $A_1 \times A_2$. Si $i \in \{1, \ldots, r_1\}$ et $j \in \{r_1+1, \ldots, r_1+r_2\}$ on a $\alpha_i \alpha_j = 0$. De même, $\alpha_i \alpha_j = 0$ si $i \in \{r_1 + 1, \ldots, r_1 + r_2\}$ et $j \in \{1, \ldots, r_1\}$. Ensuite, si $i, j \in \{1, \ldots, r_1\}$, on a $\alpha_i \alpha_j = (a'_i a'_j, 0)$ et si $i, j \in \{r_1 + 1, \ldots, r_1 + r_2\}$, alors $\alpha_i \alpha_j = (0, a''_{j-r_1} a''_{j-r_1})$. Il est facile de voir que la matrice $\tau_{A_1 \times A_2}(\alpha_i, \alpha_j)$ est ainsi

$$\begin{pmatrix} \tau_{A_1}(a'_i, a'_j) & O \\ O & \tau_{A_2}(a''_i, a''_j) \end{pmatrix},$$

et l'égalité $D_{A_1 \times A_2} = D_{A_1} \cdot D_{A_2}$ suit d'une formule bien connue sur les déterminants. $\square$

La trace et le discriminant d'un corps fini.— Soit E une extension de degré n de $\mathbb{F}_p$; il s'agit d'une $\mathbb{F}_p$-algèbre finie. On souhaite montrer

Proposition 9. *Le discriminant D_E est non-nul.*

Dans la suite, $F : E \to E$ est l'automorphisme de Frobenius définit par $F(\alpha) = \alpha^p$. Pour chaque $\alpha \in E$, on désigne par $\mathscr{F}_\alpha$ l'ensemble $\{F^\nu(\alpha) : \nu \in \mathbb{N}\}$. (Par définition $F^0 = \mathrm{id}$ et $F^{-\nu}$ est l'inverse de F^ν.) La preuve de la Proposition 9 est une conséquence de la

Proposition 10. $\mathrm{Tr}_E = \displaystyle\sum_{i=0}^{n-1} F^i$.

Démonstration. La preuve se fait en plusieurs étapes.
Étape 1. Soit $\alpha \in E^*$ tel que $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$. Alors $\mathscr{F}_\alpha = \{F^i(\alpha) : i = 0, \ldots, m-1\}$, et cet ensemble a précisément m éléments.

Clairement $\#\mathbb{F}_p(\alpha)^\times = p^m - 1$, d'où $\alpha^{p^m} - \alpha = 0$. Donc $\mathscr{F}_\alpha = \{F^i(\alpha), : i = 0, 1, \ldots, m-1\}$. Ensuite, si $F^i(\alpha) = F^j(\alpha)$ pour $0 \leqslant i < j \leqslant m-1$, alors $F^h(\alpha) = \alpha$ pour $h \leqslant m - 1$. Par conséquent, tout élément de $\mathbb{F}_p(\alpha)$ est racine de $X^{p^h} - X$: en effet,

$$\begin{aligned} F^h \sum_j b_j \alpha^j &= \sum_j b_j [F^h(\alpha)]^j \\ &= \sum b_j \alpha^j. \end{aligned}.$$

D'où $\#\mathbb{F}_p(\alpha) \leqslant p^h$, ce qui est impossible.

Étape 2. Soit $\alpha \in E^*$ comme dans l'étape précédente. Alors $(X-\alpha)\cdots(X-F^{m-1}(\alpha))$ est le polynôme minimal de α (sur $\mathbb{F}_p$).

Comme

$$\Pi_\alpha(\alpha^{p^i}) = \Pi_\alpha(\alpha)^{p^i},$$

on déduit que

$$\mathscr{F}_\alpha \subset \{\text{racines de } \Pi_\alpha\}$$

Or, Π_α n'a pas plus de m racines et la conclusion suit aussitôt.

Étape 3. Conclusion.

Soient $m = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ et $d = n/m$. Les racines de Π_α sont $\alpha, F(\alpha), \dots, F^{m-1}(\alpha)$. Donc, $\chi_{E/\mathbb{F}_p,\alpha} = (X-\alpha)^d \cdots (X - F^{m-1}(\alpha))^d$ et par conséquent

$$\mathrm{Tr}_E(\alpha) = d \sum_{i=0}^{m-1} F^i(\alpha).$$

De l'autre côté,

$$\sum_{i=0}^{n-1} F^i(\alpha) = \sum_{i=0}^{m-1} + \sum_{i=m}^{2m-1} + \cdots + \sum_{i=(d-1)m}^{dm-1}.$$

En utilisant que $F^m(\alpha) = \alpha$ (puisque $\alpha^{p^m-1} = 1$) et donc que $F^{hm}(\alpha) = \alpha$ pour tout $h \in \mathbb{N}$, on voit que $\displaystyle\sum_{i=hm}^{hm+m-1} F^i(\alpha) = \sum_{i=0}^{m-1} F^i(\alpha)$ et on arrive à $\displaystyle\sum_{i=0}^{n-1} F^i(\alpha) = d \sum_{i=0}^{m-1} F^i(\alpha) =$ $\mathrm{Tr}_E(\alpha)$. □

Preuve de la Proposition 9. Soit $\alpha \in E^*$ tel que $\mathrm{Tr}_E(\alpha\beta) = 0$ pour tout β. Donc, pour chaque $\gamma \in E$, on a $\mathrm{Tr}_E(\gamma) = \mathrm{Tr}_E(\alpha \cdot \gamma/\alpha) = 0$. Mais ceci implique que chaque $\gamma \in E$ est racine du polynôme $P = X^{p^{n-1}} + \cdots + 1$. Ceci est impossible car $\#E = p^n$ tandis que $\deg P = p^{n-1}$. □

Preuve du théorème.— On fixe une base entière $\{\omega_1, \dots, \omega_n\}$ de K.

Lemme 11. *(1) L'ensemble $\{\overline{\omega}_1, \dots, \overline{\omega}_n\}$ est une base de $\overline{\mathfrak{O}}$ en tant que $\mathbb{F}_p$-espace vectoriel.*

(2) Si $x \in \mathfrak{O}$ se réduit sur $\overline{x} \in \overline{\mathfrak{O}}$, alors $\mathrm{Tr}_K(x)$ se réduit sur $\mathrm{Tr}_{\overline{\mathfrak{O}}}(\overline{x})$.

(3) La classe de Δ_K modulo p, un élément de $\mathbb{F}_p$, induit sur $\mathbb{F}_p/\mathbb{F}_p^{*2}$, le discriminant $D_{\overline{\mathfrak{O}}}$.

Démonstration. (1) Facile.

(2) Si $x \cdot \omega_j = \sum_i x_{ij}\omega_i$ alors $\overline{x} \cdot \overline{\omega}_j = \sum_{i=1}^n \overline{x}_{ij} \cdot \overline{\omega}_i$ et la formule suit aussitôt.

(3) Par définition, $D_{\overline{\mathfrak{O}}} = \det(\mathrm{Tr}_{\overline{\mathfrak{O}}}(\overline{\omega}_i\overline{\omega}_j))$. D'après (2), $\mathrm{Tr}_{\overline{\mathfrak{O}}}(\overline{\omega}_i\overline{\omega}_j) = \overline{\mathrm{Tr}_K(\omega_i\omega_j)}$. En prenant le déterminant, on obtient la formule souhaitée. □

Preuve du Théorème 1. On suppose que p ramifie. Il suit que $\overline{\mathfrak{O}}$ possède un nilpotent non-nul. Or, $\overline{\mathfrak{O}}$ est une $\mathbb{F}_p$-algèbre finie et d'après l'exemple 7, le discriminant $D_{\overline{\mathfrak{O}}}$ vaut 0. D'après le Lemme 11, la classe du discriminant Δ_K modulo p est nulle, c'est-à-dire, $p \mid \Delta_K$.

On suppose que $p \mid \Delta_K$, qui signifie que la classe de Δ_K est nulle dans $\mathbb{F}_p$. D'après le Lemme 11-(3), $D_{\overline{\mathfrak{O}}} = 0$. D'après le Lemme 8, on peut supposer $D_{\mathfrak{O}/\mathfrak{p}_1^{e_1}} = 0$. Donc $\mathfrak{O}/\mathfrak{p}_1^{e_1}$ ne peut pas être un corps fini (sinon cela contredirait la Proposition 9). Ceci signifie que $e_1 > 1$. $\square$