QUESTIONS D'EXAMEN RELATIVES AU COURS D'INTRODUCTION À LA THÉORIE DES NOMBRES

Les trois énoncés sont indépendants. Les documents ne sont pas autorisés.
On transcrira la lettre $\mathbf{p}$ *par* $\underline{p}$.

[TdN 1]

Soient p un nombre premier, et $K = \mathbf{F}_{p^2}$ le corps à p^2 éléments. On note α une racine du polynôme $P(T) = T^{p^2} - T - 1$ dans une clôture algébrique de K, et L le corps $K(\alpha)$.

1°/ On rappelle que le groupe cyclique $Aut(L/K)$ est engendré par l'automorphisme $\sigma : x \mapsto x^{p^2}$.

i) Déterminer les conjugués de α sur K, et en déduire le degré de α sur K.

ii) On pose $a = \alpha^p - \alpha$. Montrer que a appartient à K, et déterminer le polynôme minimal de α sur K.

2°/ Soit u un élément de K. Montrer que $T^p - T - u$ divise P dans $K[T]$ si et seulement si $u^p + u = 1$.

3°/ Donner la décomposition de P en facteurs irréductibles dans $K[T]$.

[TdN 2]

On considère les corps de nombres $K = \mathbf{Q}(\sqrt{-5})$ et $L = \mathbf{Q}(\sqrt{-5}, \sqrt{2})$, dont on désigne les anneaux d'entiers par $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\sqrt{-5}$ et $\mathcal{O}_L$.

1°/ Calculer la norme de l'idéal $\mathbf{p} = (2, 1 + \sqrt{-5})$ de $\mathcal{O}_K$. Montrer que $\mathbf{p}$ n'est pas principal, mais que son carré l'est.

2°/ Calculer le nombre de classes de K. (On rappelle que $M_K = (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|D_K|}$.)

3°/ Montrer que $\beta = \frac{1+\sqrt{-5}}{\sqrt{2}}$ est un entier de L, et que l'idéal $\mathbf{p}\mathcal{O}_L$ de $\mathcal{O}_L$ est principal. En déduire que pour tout idéal $\mathbf{a}$ de $\mathcal{O}_K$, l'idéal $\mathbf{a}\mathcal{O}_L$ de $\mathcal{O}_L$ est principal.

[TdN 3]

Soient $K \subset L$ deux corps de nombres, d'anneaux d'entiers $\mathcal{O}_K \subset \mathcal{O}_L$, et $\mathbf{p}$ un idéal premier de $\mathcal{O}_K$. On suppose que l'extension L/K est *galoisienne*, et on note G son groupe de Galois. On désigne par

$$\wp_1 = \wp \ , \ \wp_2 \ , \ ..., \ \wp_g$$

les idéaux premiers de $\mathcal{O}_L$ au-dessus de $\mathbf{p}$ (c'est-à-dire divisant $\mathbf{p}\mathcal{O}_L$), et par $D = D_{\wp} = \{\sigma \in G, \sigma\wp = \wp\}$ le sous-groupe de décomposition de G en $\wp$

1°/ On suppose ici que $g = 1$, et que $\mathbf{p}\mathcal{O}_L = \wp$. Montrer que G est un groupe cyclique.

2°/ On revient au cas général. On note $L^D = \{x \in L, \forall \sigma \in D, \sigma x = x\}$ le sous-corps de L fixé par D et $\mathcal{O}_D$ l'anneau des entiers de L^D .

i) Montrer que $[L^D : K] = g$.

ii) On considère l'idéal premier $\wp_D := \wp \cap \mathcal{O}_D$ de $\mathcal{O}_D$. Montrer que $\wp$ est le seul idéal premier de $\mathcal{O}_L$ au-dessus de $\wp_D$.

3°/ On suppose que $g \geq 2$, mais que pour toute extension M de K contenue dans L et distincte de L, l'anneau des entiers $\mathcal{O}_M$ de M possède un seul idéal premier $\wp_M$ au-dessus de $\mathbf{p}$.

i) Déterminer le corps L^D.

ii) Calculer l'indice de ramification e et le degré résiduel f de $\mathbf{p}$ dans L. En déduire qu'il n'existe en fait aucune extension M strictement comprise entre K et L.

iii) Montrer que G est un groupe cyclique d'ordre premier.

Corrigé

I.1^o/ i) Comme $K(\alpha)$ est séparable sur K, le degré de α sur K est égal au nombre de ses conjugués sur K. Comme L/K est galoisienne, les conjugués de α sur K sont tous de la forme $\sigma^i(\alpha)$, où $\sigma^i, i \in \mathbf{N}$, parcourt le groupe (cyclique) $Gal(L/K)$. Or $\sigma(\alpha) = \alpha^{p^2} = \alpha+1$, d'où $\sigma^i(\alpha) = \alpha + i$, qui ne sont distincts que pour $i = 0, ..., p-1$. Donc $[K(\alpha) : K] = p$.

ii) Puisque $\sigma(a) = (\alpha^p - \alpha)^{p^2} = \alpha^p - \alpha = a$, a appartient bien à K. Le polynôme $Q_a(T) := T^p - T - a \in K[T]$ étant de degré p et annulant α, c'est le polynôme minimal de α sur K.

2^o/ Si ce polynôme $Q_u(T)$ divise $P(T)$, toute racine β de Q_u est racine de P, donc d'après le 1^o/, $u = \beta^p - \beta$, qui vérifie $u^p + u = \beta^{p^2} - \beta = 1$. Inversément, $Q_u^p = P - Q_u - (u^p + u - 1)$, donc Q_u divise P si cette expression est nulle.

3^o/ Pour $u \neq v$, les polynômes Q_u et Q_v sont premiers entre eux, donc P est divisible par le produit des Q_a, où a parcourt l'ensemble R des racines dans K de l'equation $a^p + a = 1$. Or toute racine a dans K^{alg} de cette équation vérifie $a^{p^2} = -a^p + 1 = a$, donc appartient à K, et est simple. Ainsi R a p éléments, et par comparaison des degrés, $P = \Pi_{a \in R} Q_a$. On aurait aussi pu dire que P, qui est séparable, est le produit des polynômes minimaux distincts de ses racines dans K^{alg}, et conclure par le 1^o/.

II.1^o/ Comme $\mathcal{O}_K = \mathbf{Z}[T]/(T^2+5)$, et que $T^2 + 5 \equiv (T+1)^2$ (mod. 2), un lemme du cours entraîne que l'idéal $\mathbf{p} = (\sqrt{-5}+1, 2)$ de $\mathcal{O}_K$ est premier, et que $2\mathcal{O}_K = \mathbf{p}^2$. Cette relation se vérifie en fait facilement: $\mathbf{p}^2 = (4, 2(1+\sqrt{-5}, (1+\sqrt{-5})^2) = (2).(2, 1+\sqrt{-5}, \sqrt{-5}) = (2)$. Donc $2^2 = N_{K/\mathbf{Q}}(2) = (N_{K/\mathbf{Q}}(\mathbf{p}))^2$, et $N_{K/\mathbf{Q}}(\mathbf{p}) = 2$. (On aurait aussi pu dire : $N(\mathbf{p})$ divise $N(2) = 4$ et $N(\sqrt{-5}+1) = 6$, donc vaut 1 ou 2, donc 2 car $\mathbf{p}^2 \neq \mathcal{O}_K$.) De plus, $\mathbf{p}^2 = (2)$ est bien principal. Si $\mathbf{p}$ était principal, son générateur $x + y\sqrt{-5} \in \mathcal{O}_K$ aurait pour norme $\pm N_{K/\mathbf{Q}}(\mathbf{p}) = \pm 2 = x^2 + 5y^2$, ce qui n'est pas résoluble dans $\mathbf{Z}^2$.

2^o/ Toute classe d'idéaux de K est représentée par un idéal $\mathbf{a}$ de norme $\leq M_K$. Ici, $D_K = -4 \times 5$, donc $M_K = \frac{4}{\pi}\sqrt{5} < 3$ (en effet, $80 < 81 < 9\pi^2$). Comme tout idéal de norme 2 divise 2, donc vaut $\mathbf{p}$, qui n'est pas principal, le groupe des classes $Pic(\mathcal{O}_K)$ est d'ordre $h_K = 2$.

3^o/ $\beta^2 = -2 + \sqrt{-5}$, donc β est entier sur $\mathcal{O}_K$, donc aussi sur $\mathbf{Z}$, et appartient à $\mathcal{O}_L$. Dans ces conditions $\mathbf{p}\mathcal{O}_L = (\sqrt{2}).\mathbf{b}_L$, où $\mathbf{b}_L$ est l'idéal de $\mathcal{O}_L$ engendré par $(\sqrt{2}, \beta)$. Mais $N_{L/\mathbf{Q}}(\sqrt{2}) = 4, N_{L/\mathbf{Q}}(\beta) = 9$, donc $N_{L/\mathbf{Q}}(\mathbf{b})$, qui divise 4 et 9, vaut 1, et $\mathbf{b}_L = \mathcal{O}_L$. Ainsi, $\mathbf{p}\mathcal{O}_L = \sqrt{2}\mathcal{O}_L$ est principal. (Autre méthode: $\mathbf{p}_L^2 = 2\mathcal{O}_L = (\sqrt{2}\mathcal{O}_L)^2$, donc $\mathbf{p}_L = \sqrt{2}\mathcal{O}_L$ puisque $Div(\mathcal{O}_L)$ est un groupe abélien sans torsion.) Tout idéal $\mathbf{a}$ de $\mathcal{O}_K$ étant de la forme $(\alpha).\mathbf{p}^n$ avec $\alpha \in K^*, n = 0$ ou 1, l'ideal $\mathbf{a}\mathcal{O}_L$ est de la forme $(\alpha\sqrt{2}^n)\mathcal{O}_L$, $n = 0$ ou 1. Dans chaque cas, on a nécessairement $\alpha\sqrt{2}^n \in \mathcal{O}_L$, donc $\mathbf{a}\mathcal{O}_L$ est principal .

III.1^o/ Puisqu'il n'y a qu'un idéal $\wp$ de $\mathcal{O}_L$ au-dessus de $\mathbf{p}$, tous les éléments de G vérifient $\sigma\wp = \wp$, et $D_\wp$ remplit tout G. De plus, $\wp$ est non ramifié sur $\mathbf{p}$, donc le sous-groupe d'inertie $I_\wp$ de $D_\wp$ est trivial, et $D_\wp = D_\wp/I_\wp$. Mais ce dernier groupe est isomorphe au groupe de Galois de l'extension résiduelle $\ell_\wp/k_\mathbf{p}$, où $\ell_\wp = \mathcal{O}_L/\wp, k_\mathbf{p} = \mathcal{O}_K/\mathbf{p}$, et celui-ci est cyclique (puisqu'il s'agit de corps finis). Donc $G \simeq Gal(\ell_\wp/k_\mathbf{p})$ est cyclique.

2^o/ i) D'après la théorie de Galois, L/L^D est une extension galoisienne, de groupe de Galois $D = D_\wp$. Donc $[L : L^D] = |D| = ef = n/g$, et $[L^D : L] = n/[L : L^D] = g$.

ii) $\wp$ est l'un des idéaux de $\mathcal{O}_L$ au-dessus de $\wp_D$, et les idéaux de $\mathcal{O}_L$ au-dessus de $\wp_D$ sont permutés par le groupe de Galois $Gal(L/L^D)$. Puisque ce groupe coïncide avec $D = D_\wp$, dont tous les éléments envoient $\wp$ sur lui-même, c'est que $\wp$ est le seul idéal de $\mathcal{O}_L$ au-dessus de $\wp_D$.

3^o/ i) Montrons par l'absurde que $L^D = L$. Sinon, L^D est une extension intermédiaire strictement incluse dans L. L'idéal $\wp_D = \wp \cap \mathcal{O}_D$ de $\mathcal{O}_D$ est au-dessus de $\mathbf{p} = \wp \cap \mathcal{O}_K$ (puisqu'il le contient), et l'hypothèse faite sur les extensions intermédiaires strictes dit que c'est le seul. Mais d'après 2^o/, $\wp$ est le seul idéal de $\mathcal{O}_L$ au-dessus de $\wp_D$, donc aussi le seul idéal de $\mathcal{O}_L$ au-dessus de $\mathbf{p}$. Ceci contredit l'hypothèse $g > 1$.

ii) Puisque $g = [L^D : K] = [L : K] = efg$, on a: $e = f = 1$, et $\mathbf{p}\mathcal{O}_L = \wp_1 ... \wp_g$, où chaque extension résiduelle $\ell_{\wp_i}/k_\mathbf{p}$ est triviale. Il en est donc de même (indices de ramifications et degrés résiduels des g_M idéaux premiers de $\mathcal{O}_M$ au-dessus de $\mathbf{p}$ tous égaux à 1) pour chaque extension intermédiaire M, dont le degré $[M : K]$ est alors égal à g_M. L'hypothèse impose ainsi $[M : K] = 1$ si $M \neq L$.

iii) D'après la question précédente et la théorie de Galois, le groupe G n'admet aucun sous-groupe propre. Il est donc cyclique d'ordre premier.