Théorie des nombres II

Examen du 4 mars 2015 (durée : 2 heures)

Dans tous les exercices, F désignera un corps local dont le corps résiduel est de caractéristique p, $\mathfrak{p}_F$ l'idéal maximal, et k_F le corps résiduel.

EXERCICE 1. (4 points) — Si $x \in \mathbb{F}_p$, on note $[x] \in \mathbb{Z}_p$ son représentant multiplicatif.

i) Rappeler la définition de l'application [.]. Montrer que, si $x \in \mathbb{F}_p^\times$, alors $[x] \in \mathbb{Z}_p$ est l'unique racine $(p-1)$-ième de 1 qui est congrue à x modulo $p\mathbb{Z}_p$.

Si $x \in \mathbb{F}_p$, et $x^{p^{-n}}$ l'unique èlément solution de $X^{p^n} = x$, et si $\hat{x}_n$ est un relèvement (quelconque) dans $\mathbb{Z}_p$ de $x^{p^{-n}}$, alors la limite de la suite $((\hat{x}_n)^{p^n})$ existe dans $\mathbb{Z}_p$, qui est alors $[x]$. Notons que, comme $x^{p^{-n}} = x$ dans $\mathbb{F}_p$, on a en fait

$$[x] = \lim_{n\to\infty} \hat{x}^{p^n}$$

où $x \in \mathbb{Z}_p$ est un relèvement quelconque de x.
On a $[1] = 1$ $[xy] = [x][y]$, donc $[x]^{p-1} = [x^{p-1}] = 1$; de plus c'est clair que $[x]$ se réduit à x dans $\mathbb{F}_p$. L'unicité découle du lemme de Hensel.

Dans la suite de cet exercice, supposons $p = 5$.

ii) Ecrivons $[2] = 2 + \sum_{n\geq 1} a_n \cdot 5^n$ avec $a_n \in \{0, 1, 2, 3, 4\}$. Déterminer a_1, a_2.

Deux méthodes pour calculer $[x]$:

1. Puisque $[2] \equiv 2 \mod p$, on a $[2] = [2]^p[2] \equiv 2^p \mod p^2$. Comme $p = 5$, on trouve

$$[2] \equiv 2^5 = 32 = 2 + 5 + 5^2 \equiv 2 + 5 \mod 5^2;$$

puis, $(2+5)^5 = 2^5 + 5.5 \mod 5^3$, d'où $[2] = 2 + 5 + 2.5^2 \mod 5^3$.

2. Utiliser la méthode de Newton : soit $f(X) = X^4 - 1$, on a $f'(X) = 4X^3$ et $f'(2) = 32 \equiv 2 \mod 5$. Posons $x_0 = 2$, et

$$x_1 = 2 - \frac{f(2)}{f'(2)} \equiv 2 - \frac{15}{2} \equiv 2 + 5 \mod 5^2,$$

$$x_2 = 2 + 5 - \frac{f(2+5)}{f'(2)} \equiv 2 + 5 - \frac{1}{2} \cdot 5^2 \equiv 2 + 5 + 2 \cdot 5^2 \mod 5^3.$$

iii) Ecrivons $1 + [2] = \sum_{n\geq 0} [b_n] \cdot 5^n$. Déterminer $b_0, b_1 \in \mathbb{F}_5$.

D'après le cours, $1 + [2] = [1 + 2] + 5 \cdot [Q_1^+((1, 0, ...), (2, 0, ...))] \mod 5^2$, où

$$Q_1^+(X_i, Y_i) = X_1 + Y_1 + \frac{X_0 + Y_0 - (X_0^{p^{-1}} + Y_0^{p^{-1}})^p}{p} = X_1 + Y_1 - \Big(\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} X_0^{p^{-(p-i)}} Y_0^{p^{-i}}\Big).$$

En notant que $x^{p^{-1}} = x$ dans $\mathbb{F}_p$, on obtient (dans $\mathbb{F}_5$)

$$b_1 = 0 + 0 - \left(\frac{\binom{5}{1}}{5} \cdot 2 + \frac{\binom{5}{2}}{5} \cdot 2^2 + \frac{\binom{5}{3}}{5} \cdot 2^3 + \frac{\binom{5}{4}}{5} \cdot 2^4\right) = -(2 + 2 \cdot 2^2 + 2 \cdot 2^3 + 2^4) = 3.$$

Seconde méthode : c'est clair que $b_0 = 1 + 2 = 3$, donc $1 + [2] = [3] + [b_1] \cdot 5 \mod 5^2$ et $b_1 5 \equiv 1 + [2] - [3] \mod 5^2$. Comme dans ii), on vérifie que $[3] = 3 + 3 \cdot 5 \mod 5^2$, donc

$$1 + [2] - [3] \equiv 1 + (2 + 5) - (3 + 3 \cdot 5) \mod 5^2 = 3 \cdot 5 \mod 5^2$$

EXERCICE 2. (4 points) — Soient K, K' deux extensions finies de F d'indice de ramification e, e'. Supposons que K/F est modérément ramifiée et que e divise e'. Montrer que la composée KK' est non ramifiée sur K'.

(i) Se ramener au cas où K/F est totalement ramifiée. Soit $K_0 \subset K$ la sous-extension non ramifiée maximale de F contenue dans K. Alors, d'après le cours, K_0K' est non ramifiée sur K'. Ainsi, pour montrer que KK' est non ramifiée sur K', il suffit de montrer que KK' est non ramifiée sur K_0K'. En remplaçant F par K_0 (et K' par K_0K'), on peut supposer que K/F est totalement ramifiée.

(ii) Comme K/F est totalement ramifiée et modérément ramifiée, il existe une uniformisante π_K de K telle que $\pi_K^e := \pi_F \in \mathcal{O}_F$; on a de plus $KK' = K'(\pi_K)$. Notons $v_{K'}$ la valuation normalisée sur K', étendue de manière unique à KK'. Soit $\pi_{K'}$ une uniformisante de K', alors $u := \pi_K^e/\pi_{K'}^{e'}$ appartient à $\mathcal{O}_{K'}^\times$, car $v_{K'}(\pi_K^e) = v_{K'}(\pi_F) = e'$. D'autre part, par hypothèse $e|e'$; si on pose $t := \pi_K/\pi_{K'}^{e'/e}$, alors $t^e = u$ et $KK' = K'(t)$ (car $\pi_{K'} \in K'$).

(iii) On peut maintenant conclure que KK' est non ramifiée sur K, d'après le cours. En effet, soit $P(X)$ le polynôme minimal de t sur K' ; alors $P(X)|(X^e - u)$. En particulier, $\overline{P}(X) \in k_{K'}[X]$ est séparable, et irréductible par le lemme de Hensel. Puisque $t \in KK'$, on en déduit que

$$[k_{KK'} : k_{K'}] \geq \deg \overline{P} = \deg P = [KK' : K']$$

d'où le résultat.

EXERCICE 3. (6 points) Soit ζ_p une racine primitive p-ième de 1. Posons $F = \mathbb{Q}_p(\zeta_p)$ et $K = F(\alpha)$, où $\alpha \in \overline{\mathbb{Q}_p}$ est une racine de l'équation $X^p = 1 - p$.

i) Montrer que l'extension $K/\mathbb{Q}_p$ est galoisienne, totalement ramifiée de degré $p(p-1)$. Donner une uniformisante de K.

Comme α est racine de $X^p - (1-p) = 0$, $\alpha - 1$ est racine de l'équation $(X+1)^p - (1-p) = 0$, soit

$$X^p + \binom{p}{1} X^{p-1} + \cdots \binom{p}{1} X + p = 0,$$

qui est un polynôme d'Eisenstein dans $\mathbb{Q}_p[X]$. Donc $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\alpha - 1)$ est totalement ramifiée sur $\mathbb{Q}_p$ de degré p, avec $\alpha - 1$ une uniformisante. Soit v_p la valuation sur K normalisée par $v_p(p) = 1$, alors $v_p(\alpha - 1) = 1/p$.

Notons $t = \zeta_p - 1$, qui est une uniformisante de F d'après le cours ; on a $v_p(t) = 1/(p-1)$. Par conséquent, on a

$$v_p\left(\frac{t}{\alpha - 1}\right) = \frac{1}{p-1} - \frac{1}{p} = \frac{1}{p(p-1)}.$$

En particulier, $e(K/\mathbb{Q}_p) \geq p(p-1)$. D'autre part, c'est clair que $[K:\mathbb{Q}_p] = [K:F][F:\mathbb{Q}_p] \leq p(p-1)$, donc

$$[K:\mathbb{Q}_p] = e(K/\mathbb{Q}_p) = p(p-1),$$

et que $K/\mathbb{Q}_p$ est totalement ramifiée avec $\frac{t}{\alpha-1}$ une uniformisante.

Pour voir que $K/\mathbb{Q}_p$ est galoisienne, il suffit de noter que si $\sigma : K \to \overline{\mathbb{Q}_p}$ est un prolongement, alors $(\frac{\sigma\alpha}{\alpha})^p = 1$, donc $\sigma\alpha = \zeta_p^s\alpha$ avec $0 \leq s \leq p-1$ et $\frac{\sigma\alpha}{\alpha} \in K$.

ii) Déterminer les sous-groupes de ramification $(G_i)_{i\in\mathbb{N}}$ de $G = \mathrm{Gal}(K/\mathbb{Q}_p)$.

L'extension $K/\mathbb{Q}_p$ étant totalement ramifiée, on a $G_{-1} = G_0 = G$. Puis $[F:\mathbb{Q}_p] = p-1$ est premier à p, on a $G_1 = H := \mathrm{Gal}(K/F)$. Soit $\sigma \in G_1$ et $\sigma \neq 1$. Alors σ fixe ζ_p, et en posant $\sigma\alpha = \zeta_p^s\alpha$ avec $1 \leq s \leq p-1$, on obtient

$$\sigma(\frac{t}{\alpha-1}) - \frac{t}{\alpha-1} = \frac{t}{\zeta_p^s\alpha - 1} - \frac{t}{\alpha-1} = \frac{t\alpha(1-\zeta_p^s)}{(\zeta_p^s\alpha-1)(\alpha-1)},$$

dont la valuation (pour v_p) est $\frac{2}{p(p-1)}$, car

$$v_p(\alpha) = 0, \quad v_p(t) = v_p(\zeta_p^s - 1) = \frac{1}{p-1}, \quad v_p(\zeta_p^s\alpha - 1) = v_p(\alpha-1) = \frac{1}{p}.$$

On en déduit que

$$i_K(\sigma) = 2.$$

C'est-à-dire, $G_1 = H$ et $G_i = \{1\}$ si $i \geq 2$.

iii) Calculer les fonctions $\varphi_{K/\mathbb{Q}_p}$ et $\psi_{K/\mathbb{Q}_p}$.

La fonction $\varphi_{K/\mathbb{Q}_p}$ est donnée par

$$\varphi_{K/\mathbb{Q}_p}(x) = \int_0^x \frac{1}{[G_0:G_u]}du = \begin{cases} x & \text{si } -1 \leq x \leq 0 \\ x/(p-1) & \text{si } 0 \leq x \leq 1 \\ 1/(p-1) + (x-1)/p(p-1) & \text{si } x \geq 1 \end{cases}$$

et la fonction $\psi_{K/\mathbb{Q}_p}$:

$$\psi_{K/\mathbb{Q}_p}(x) = \begin{cases} x & \text{si } -1 \leq x \leq 0 \\ (p-1)x & \text{si } 0 \leq x \leq 1 \\ p(p-1)x - p + 1 & \text{si } x \geq 1. \end{cases}$$

EXERCICE 4. (6 points) — Considérons le polynôme $P(X) = X^p - X - \frac{1}{p} \in \mathbb{Q}_p[X]$.

i) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}_p[X]$.

Posons

$$Q(X) = (-p)X^pP(\frac{1}{X}) = (-p)X^p(\frac{1}{X^p} - \frac{1}{X} - \frac{1}{p}) = X^p + pX^{p-1} - p$$

qui est un polynôme d'Eisenstein, donc irréductible dans $\mathbb{Q}_p[X]$. Ainsi $X^pP(\frac{1}{X})$ est aussi irréductible et de même pour $P(X)$. En effet, si on avait $P(X) = P_1(X)P_2(X)$, alors

$$X^pP(\frac{1}{X}) = [X^{\deg P_1}P_1(\frac{1}{X})][X^{\deg P_2}P_2(\frac{1}{X})].$$

ii) Soit α une racine de $P(X)$ dans $\overline{\mathbb{Q}_p}$ et posons $F = \mathbb{Q}_p(\alpha)$. Montrer que $F/\mathbb{Q}_p$ est une extension galoisienne, i.e. F contient toutes les racines de $P(X)$.

Soit α' une autre racine de $P(X)$, différente de α. Alors

$$\alpha'^p - \alpha' = \alpha^p - \alpha = 1/p.$$

On en déduit que $\alpha'^p - \alpha^p = \alpha' - \alpha$, puis (car $\alpha' \neq \alpha$)

$$\alpha'^{p-1} + \alpha'^{p-2}\alpha + \cdots + \alpha^{p-1} = 1.$$

Posons $\zeta = \frac{\alpha'}{\alpha}$, alors (en divisant par α^{p-1})

$$\zeta^{p-1} + \zeta^{p-2} + \cdots + 1 - \frac{1}{\alpha^{p-1}} = 0.$$

Notons que $\frac{1}{\alpha^{p-1}} \in \mathcal{O}_F$, le polynôme $R(X) := X^{p-1} + X^{p-2} + \cdots + X + (1 - \frac{1}{\alpha^{p-1}})$ appartient à $\mathcal{O}_F[X]$, dont la réduction modulo $\mathfrak{p}_F$ est

$$\overline{R}(X) = X^{p-1} + \cdots + X + 1 \in k_F[X].$$

C'est un polynôme séparable, et $\overline{R}(1) = 1 + 1 + \cdots + 1 = p = 0$ dans k_F. Le lemme de Hensel permet de conclure que $\zeta \in \mathcal{O}_F$, donc $\alpha' = \zeta\alpha \in F$.

iii) Soit $\mathfrak{D}_{F/\mathbb{Q}_p}$ la différente. Déterminer $v_F(\mathfrak{D}_{F/\mathbb{Q}_p})$, où v_F désigne la valuation normalisée sur F.

Posons $\beta = \frac{1}{\alpha}$, alors β est racine de $Q(X)$, qui est d'Eisenstein. Donc $F/\mathbb{Q}_p$ est totalement ramifiée de degré p et $\mathcal{O}_F = \mathbb{Z}_p[\beta]$. D'après le cours, on sait que

$$v_F(\mathfrak{D}_{F/\mathbb{Q}_p}) = v_F(Q'(\beta)) = v_F(p\beta^{p-1} + p(p-1)\beta^{p-2}).$$

Les deux termes dans la somme ont différentes validations et celle du seconde est la plus petite, on obtient

$$v_F(\mathfrak{D}_{F/\mathbb{Q}_p}) = v_F(p) + p - 2 = 2p - 2.$$

iv) Déterminer le sous-groupe $N_{F/\mathbb{Q}_p}(F^\times)$ de $\mathbb{Q}_p^\times$.

D'après le cours, comme $F/\mathbb{Q}_p$ est abélienne, on a $|\mathbb{Q}_p^\times / N(F^\times)| = [F : \mathbb{Q}_p] = p$. D'autre part, $N_{F/\mathbb{Q}_p}(\beta) = -p$. Il reste à déterminer $N_{F/\mathbb{Q}_p}(\mathcal{O}_F^\times)$, qui est un sous-groupe de $\mathbb{Z}_p^\times$ d'indice p. Puisque $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ et $1 + p\mathbb{Z}_p$ est (topologiquement) cyclique, on en déduit

$$N_{F/\mathbb{Q}_p}(\mathcal{O}_F^\times) = \mu_{p-1} \times (1 + p^2\mathbb{Z}_p)$$

et

$$N_{F/\mathbb{Q}_p}(F^\times) = (-p)^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p^2\mathbb{Z}_p) = p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p^2\mathbb{Z}_p).$$