EXAMEN

THÉORIE DES NOMBRES M2

Documents admis : notes de cours. Le soin de la rédaction compte dans la note. Dans tout l'examen, $p \neq 2$, K est une extension finie de $\mathbf{Q}_p$ et π est une uniformisante de $\mathcal{O}_K$.

1. Un calcul de H^1

Soit X un espace de Banach sur $\mathbf{Q}_p$ muni d'une action continue (et $\mathbf{Q}_p$-linéaire) du groupe $\mathbf{Z}_p$ et soit g un générateur topologique de $\mathbf{Z}_p$ (par exemple $g = 1$).

1.1. Montrer que l'application $H^1(\mathbf{Z}_p, X) \to X/(1-g)$ qui à la classe $\overline{c}$ d'un cocycle associe l'image de $c(g)$ dans $X/(1-g)$ est bien définie et injective.

Soit $F_n = \mathbf{Q}_p(\zeta_{p^n})$ et $F_\infty = \cup_{n\geq 1} F_n$ et $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, de sorte que si $n \geq 1$, alors Γ_n est isomorphe à $\mathbf{Z}_p$. On note g_n un générateur topologique de Γ_n. Pour $k \geq 1$, on pose $F^*_{n,k} = \oplus_{j=1, p\nmid j}^{p^k-1} \zeta_{p^{n+k}}^j \cdot F_n$. Soit $R_n : \widehat{F}_\infty \to F_n$ la trace normalisée de Tate et $X_n = \ker(R_n)$.

1.2. Montrer que $F_{n+k} = F_n \oplus F^*_{n,1} \oplus \cdots \oplus F^*_{n,k}$ et que $X_n \cap F_{n+k} = F^*_{n,1} \oplus \cdots \oplus F^*_{n,k}$.

1.3. Si $x = \sum_{j=1,p\nmid j}^{p^k-1} x_j \cdot \zeta_{p^{n+k}}^j \in F^*_{n,k}$, montrer qu'il existe $a \in \mathbf{Z}_p^\times$, dépendant du choix de g_n, tel que $x = (1 - g_n^{p^{k-1}}) \sum_j x_j \cdot \zeta_{p^{n+k}}^j/(1-\zeta_p^{aj})$.

1.4. En déduire que $1 - g_n : F^*_{n,k} \to F^*_{n,k}$ est bijective, et qu'il existe une constante C indépendante de k telle que $|(1-g_n)^{-1}(x)| \leq C|x|$ si $x \in F^*_{n,k}$.

1.5. Montrer que $1 - g_n : X_n \to X_n$ est bijective.

1.6. Montrer que $H^1(\Gamma_n, \widehat{F}_\infty)$ est un F_n-espace vectoriel de dimension ≤ 1.

Si $x \in \mathbf{Z}_p^\times$, on peut écrire $x = x_0 \cdot (1 + py)$ avec $x_0^{p-1} = 1$ et $y \in \mathbf{Z}_p$. On pose alors $\log_p(x) = \log_p(1+py) = \sum_{n\geq 1} (-1)^{n-1}(py)^n/n$, de sorte que $\log_p : (\mathbf{Z}_p^\times, \times) \to (\mathbf{Z}_p, +)$ est un morphisme de groupes.

1.7. Montrer que $H^1(\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p), \mathbf{C}_p)$ est un $\mathbf{Q}_p$-espace vectoriel de dimension 1, engendré par la classe du cocycle $g \mapsto \log_p \chi_{\mathrm{cyc}}(g)$.

2. Séries formelles commutant pour la composition

Dans ce problème, on s'intéresse aux séries formelles $f(X) \in \mathcal{O}_K[\![X]\!]$ telles que $f(0) = 0$. Si f est une telle série et si $n \geq 1$, on note $f^{\circ n} = f \circ \cdots \circ f$ la série f composée avec elle-même n fois. Soit $\mathbf{P}$ l'ensemble des $f(X) = \sum_{i \geq 1} a_i X^i \in \mathcal{O}_K[\![X]\!]$ telles que $a_1 \in \mathfrak{m}_K$, $a_1 \neq 0$ et telles qu'il existe $i \geq 2$ avec $a_i \notin \mathfrak{m}_K$.

2.1. Montrer que si $f \in \mathbf{P}$ et $z \in \mathfrak{m}_{\mathbf{C}_p}$ avec $z \neq 0$, alors $|f(z)| < |z|$.

Si $f \in \mathbf{P}$, soit $\Lambda_n(f) = \{z \in \mathfrak{m}_{\mathbf{C}_p} \text{ tels que } f^{\circ n}(z) = 0\}$, et $\Lambda(f) = \cup_{n \geq 1} \Lambda_n(f)$.

2.2. Montrer que $\Lambda_n(f)$ est fini pour tout $n \geq 1$, et que $\Lambda(f)$ est infini.

2.3. Montrer que si f, $g \in \mathbf{P}$ vérifient $f \circ g = g \circ f$, alors $\Lambda(f) = \Lambda(g)$.

Soit $\mathbf{U}$ l'ensemble des $u(X) = \sum_{i \geq 1} a_i X^i \in \mathcal{O}_K[\![X]\!]$ telles que $a_1 \in \mathcal{O}_K^\times$ et a_1 n'est pas une racine de 1. Si $u \in \mathbf{U}$, soit $\Lambda_n(u) = \{z \in \mathfrak{m}_{\mathbf{C}_p} \text{ tels que } u^{\circ n}(z) = z\}$ et $\Lambda(u) = \cup_{n \geq 1} \Lambda_n(u)$.

2.4. Montrer que si u, $v \in \mathbf{U}$ vérifient $u \circ v = v \circ u$, alors $\Lambda(u) = \Lambda(v)$.

2.5. Montrer que si $f \in \mathbf{P}$ et $u \in \mathbf{U}$ vérifient $u \circ f = f \circ u$, alors $\Lambda(f) = \Lambda(u)$.

On suppose désormais que $u(X) = X + \pi^r \alpha(X)$ avec $r \geq 1$ et $\alpha(X) \in \mathcal{O}_K[\![X]\!]$.

2.6. Montrer que $u^{\circ p}(X) = X + p\pi^r \alpha(X) + \pi^{2r} \beta(X)$ avec $\beta(X) \in \mathcal{O}_K[\![X]\!]$.

2.7. En déduire que si $s \geq 1$ et k est assez grand, alors $u^{\circ p^k}(X) \equiv X \bmod \pi^s$.

2.8. Montrer que si $r \geq \mathrm{val}_\pi(p) + 1$ et $k \geq 0$, alors $u^{\circ p^k}(X) \equiv X + p^k \pi^r \alpha(X) \bmod p^k \pi^{r+1}$.

2.9. Montrer que le cardinal de $\Lambda_{p^k}(u)$ est borné indépendamment de $k \geq 0$.

2.10. Montrer que l'on peut étendre par continuité la définition de $u^{\circ m}$ à tout $m \in \mathbf{Z}_p$.

2.11. Montrer que $\Lambda(u) = \cup_{k \geq 0} \Lambda_{p^k}(u)$, puis que $\Lambda(u)$ est fini.

2.12. Montrer que si $u \in \mathbf{U}$ et si $u(X) \equiv X \mod \pi$, alors il n'existe pas de $f \in \mathbf{P}$ telle que $f \circ u = u \circ f$.