Corrigé de l'examen du 19 mai 2011
"Cohomologie galoisienne et théorie des nombres"

Université Paris-Sud (D. Harari)

Exercice 1 : Vrai ou faux ?

a) C'est faux. Prenons en effet $i = 1$ et $M = \mathbf{Q}/\mathbf{Z}$. Alors $H^1(\Gamma_K, \mathbf{Q}/\mathbf{Z})$ est le dual du groupe de Galois abélien Γ_K^{ab} de Γ_K, qui est un groupe profini infini (il est isomorphe au complété profini de K^*). Ce dual ne peut être fini, sinon Γ_K^{ab} serait fini (comme on l'a vu encours, l'assertion est par contre vraie si M est supposé fini).

b) C'est faux. Prenons $k = \mathbf{R}$, qui n'est même pas de dimension cohomologique finie. Pour $r = 3$, on a alors $H^3(\mathbf{R}, \mathbf{Z}) = H^1(\mathbf{R}, \mathbf{Z})$ par 2-périodicité de la cohomologie du groupe de Galois absolu de $\mathbf{R}$ (qui est un groupe cyclique d'ordre 2). Or $H^1(\mathbf{R}, \mathbf{Z}) = 0$ puisque $\mathbf{Z}$ n'a pas de sous-groupe fini non trivial.

c) C'est vrai. Comme M est de type fini, on peut trouver un sous-groupe ouvert distingué U de G tel que U agisse trivialement sur M. On a alors $H^1(U, M) = 0$ car le U-module M est isomorphe à $\mathbf{Z}^r$ pour un certain entier r (il est de type fini et sans torsion) et $H^1(U, \mathbf{Z}^r) = 0$ parce que $\mathbf{Z}^r$ n'a pas de sous-groupe fini non trivial (donc il n'y a pas d'homomorphisme continu non trivial de U dans $\mathbf{Z}^r$). Maintenant la suite exacte de restriction-inflation identifie $H^1(G, M)$ avec $H^1(G/U, M)$, qui est fini via le corollaire 1.25 puisque G/U est fini.

d) C'est vrai. On sait que $\mathrm{scd}_p(G) = \mathrm{scd}_p(G_p)$, où G_p est un p-Sylow de G. L'hypothèse que p divise l'ordre de G donne que G_p est un pro-p-groupe non trivial (via la proposition 3.5.a), il admet donc un quotient G_p/U par un sous-groupe ouvert distingué U, tel que $P := G_p/U$ soit un p-groupe fini. Comme un tel groupe est résoluble, son abélianisé A est un p-groupe abélien non trivial. Alors $H^2(G_p, \mathbf{Z}) = H^1(G_p, \mathbf{Q}/\mathbf{Z})$ contient $H^1(P, \mathbf{Q}/\mathbf{Z}) = H^1(A, \mathbf{Q}/\mathbf{Z})$ dont la p-torsion est non triviale (elle s'identifie à A/pA et A est somme directe de groupes de la forme $\mathbf{Z}/p^r\mathbf{Z}$).

Exercice 2 : Modules divisibles.

1. Comme la multiplication par n est surjective dans M, on a une suite exacte de G-modules :

$$0 \to M[n] \to M \stackrel{\cdot n}{\to} M \to 0$$

et il suffit alors de lui appliquer la suite exacte longue de cohomologie.

2. Ici $M[n]$ est fini car il est isomorphe à μ_n^m, où μ_n est le groupe des racines n-ièmes de l'unité dans $\overline{K}^*$. On en déduit que $H^i(G, M[n])$ est fini via le corollaire 5.12. D'après 1., $H^i(G, M)[n]$ est également fini (noter que $(\overline{K}^*)^m$ est bien divisible).

3. On note que $H^1(L, M)$ est nul car par hypothèse il est égal au groupe $H^1(L, (\overline{K}^*)^m)$ et on peut appliquer Hilbert 90. Par restriction-inflation on obtient alors

$$H^1(G, M) = H^1(\mathrm{Gal}\,(L/K), N)$$

où N est le sous-module de M constitué des invariants sous $\mathrm{Gal}\,(\overline{K}/L)$. Soit n le cardinal de $\mathrm{Gal}\,(L/K)$, on obtient que $H^1(G, M) = H^1(G, M)[n]$ par le corollaire 1.24, et ce dernier groupe est fini d'après 2.

Exercice 3 : Normes locales et globales.

1. C'est une conséquence immédiate du théorème 7.7., qui découle lui-même de Tate-Nakayama.

2. Posons $G = \mathrm{Gal}\,(F/k)$. D'après le théorème 8.9., on a une injection $H^2(G, F^*) \to H^2(G, I_F)$ dont le conoyau est fini. D'autre part $H^2(G, I_F)$ est isomorphe à $\bigoplus_{v \in \Omega_k} H^2(G_v, F_v^*)$, où $G_v \simeq \mathrm{Gal}\,(F_v/k_v)$ est le groupe de décomposition en v (formule (10) après la proposition 8.3.). Maintenant comme G (et donc aussi G_v) est cyclique, on a $H^2(G, F^*) = \widehat{H}^0(G, F^*)$ et $H^2(G_v, F_v^*) = \widehat{H}^0(G_v, F_v^*)$, ce qui donne le résultat.

3. D'après 1. et 2., il suffit de voir que l'extension F_v/k_v est de degré au moins 2 pour une infinité de places v de k, ce qui résulte du théorème de Cebotarev.

Exercice 4 : Corps de nombres.

1. a) La suite exacte

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

reste exacte quand on tensorise par M au-dessus de $\mathbf{Z}$, car en tant que groupe abélien M est isomorphe à $\mathbf{Z}^r$ (donc plat sur $\mathbf{Z}$) pour un certain entier r. On a donc une suite exacte de G_k-modules

$$0 \to M \to M \otimes_{\mathbf{Z}} \mathbf{Q} \to M \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z} \to 0$$

mais $M \otimes_{\mathbf{Z}} \mathbf{Q}$ est uniquement divisible (comme groupe abélien il est isomorphe à $\mathbf{Q}^r$), ce qui implique $H^{i-1}(k, M \otimes_{\mathbf{Z}} \mathbf{Q}) = 0$ pour $i > 1$ (corollaire 1.26). On obtient alors le résultat avec la suite exacte longue de cohomologie.

b) C'est immédiat vu qu'avec les notations ci-dessus, ce G_k-module est isomorphe comme groupe abélien à $(\mathbf{Z}/n\mathbf{Z})^r$.

c) On utilise a), qui est également valable (avec la même preuve) si on remplace k par k_v. On est donc ramené à montrer que l'application naturelle

$$H^{r-1}(k, M \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z}) \to \bigoplus_{v \in \Omega_{\mathbf{R}}} H^{r-1}(k_v, M \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z})$$

est un isomorphisme. Comme $M \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z}$ est la limite inductive des $M \otimes_{\mathbf{Z}} \mathbf{Z}/n$ ($\varinjlim$ commute avec $\otimes_{\mathbf{Z}}$), il suffit de vérifier ce résultat en remplaçant $M \otimes_{\mathbf{Z}} \mathbf{Q}/\mathbf{Z}$) par $M \otimes_{\mathbf{Z}} \mathbf{Z}/n$. Ceci est une conséquence du théorème de Poitou-Tate puisque par hypothèse $(r-1) \geq 3$ et $M \otimes_{\mathbf{Z}} \mathbf{Z}/n$ est fini d'après b).

2. a) Comme M est de tye fini, il existe un sous-groupe ouvert distingué U de G_k qui agit trivialement sur M. On peut alors voir M comme un module de type fini sur l'anneau $\mathbf{Z}[G_k/U]$, ce qui fait que M s'écrit comme un quotient d'un G_k-module de la forme $P = \mathbf{Z}[G_k/U]^s$ avec s entier positif. Le noyau N de la surjection canonique $P \to M$ est alors de type fini et sans torsion car c'est un sous-groupe de P (qui est de type fini et sans torsion). Enfin, comme on l'a vu en cours, le G_k-module $\mathbf{Z}[G_k/U]$ est isomorphe à l'induit $I_{G_k}^U(\mathbf{Z})$.

b) On sait déjà d'après 1)c) que $\theta^r(P)$ et $\theta^r(N)$ sont des isomorphismes pour tout $r \geq 4$ car P et N sont de type fini et sans torsion. Or on a un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccccc}
H^r(k,N) & \longrightarrow & H^r(k,P) & \longrightarrow & H^r(k,M) & \longrightarrow & H^{r+1}(k,N) & \longrightarrow & H^{r+1}(k,P) \\
\downarrow{\scriptstyle \theta^r(N)} & & \downarrow{\scriptstyle \theta^r(P)} & & \downarrow{\scriptstyle \theta^r(M)} & & \downarrow{\scriptstyle \theta^{r+1}(N)} & & \downarrow{\scriptstyle \theta^{r+1}(P)} \\
\bigoplus_v H^r(k_v,N) & \longrightarrow & \bigoplus_v H^r(k_v,P) & \longrightarrow & \bigoplus_v H^r(k_v,M) & \longrightarrow & \bigoplus_v H^{r+1}(k_v,N) & \longrightarrow & \bigoplus_v H^{r+1}(k_v,P)
\end{array}$$

(où, dans les sommes directes, v décrit $\Omega_{\mathbf{R}}$). On conclut alors avec le lemme des cinq.

c) Le corollaire 9.10. dit que $H^3(k,\mathbf{Z}) = 0$ et pour v réelle, on a aussi $H^3(k_v,\mathbf{Z}) = H^1(k_v,\mathbf{Z}) = 0$. Ainsi $\theta^3(\mathbf{Z})$ a une source et un but nuls; il en va donc de même de $\theta^3(P)$ via le lemme de Shapiro. On obtient alors le résultat par chasse au diagramme en écrivant le diagramme précédent pour $r = 3$.