

CORRIGÉ de l'examen du 18 février 2025

I

Soit $\rho : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{C})$ une représentation d'image finie, irréductible, impaire, de conducteur N . On note P (majuscule de la lettre ρ) l'application $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}(\text{M}_2(\mathbf{C}))$ qui à σ associe $M \mapsto \rho(\sigma)M\rho(\sigma)^{-1}$. C'est la *représentation adjointe* de ρ .

Soit p un nombre premier. Si p est non ramifié pour ρ , on note α_p et β_p les valeurs propres de $\rho(\phi_p)$, où ϕ_p est une substitution de Frobenius en p . Ainsi le polynôme caractéristique de $\rho(\phi_p)$ est $X^2 - a_p X + a_{p,p}$, avec $a_p = \alpha_p + \beta_p$ et $a_{p,p} = \alpha_p \beta_p$.

À partir de la question 6, on suppose qu'en tout nombre premier q divisant N , l'image par ρ d'un sous-groupe d'inertie I_q en q a un vecteur fixe v non nul dans $\mathbf{C}^2$, et que $\rho(I_q)$ est cyclique d'ordre premier à q . Notons a_q la trace de $\rho(\phi_q)$ agissant sur $\mathbf{C}v$.

1. Montrer que P est d'image finie.

C'est évident puisque ρ est d'image finie.

2. Supposons ρ non ramifiée en p .

2.a. Montrer que P est non ramifiée en p .

Soit σ dans un groupe d'inertie en p . On a $\rho(\sigma) = 1$ et donc $P(\sigma) = 1$ et donc P non ramifiée en p .

2.b. Montrer que les valeurs propres de $P(\phi_p)$ sont α_p/β_p , β_p/α_p , 1 et 1.

Les valeurs propres de $P(\phi_p)$ sont les valeurs propres de $\rho(\phi_p) \otimes \rho^*(\phi_p)$, c'est-à-dire les rapports des valeurs propres de $\rho(\phi_p)$ et de $\rho^*(\phi_p)$. On trouve bien α_p/β_p , β_p/α_p , $\alpha_p/\alpha_p = 1$, $\beta_p/\beta_p = 1$.

2.c. En déduire le facteur d'Euler en p de $L(P, s)$ en termes de a_p et $a_{p,p}$.

On utilise les relations $a_p = \alpha_p + \beta_p$ et $a_{p,p} = \alpha_p \beta_p$. On a donc $\alpha_p^2 + \beta_p^2 = a_p^2 - 2a_{p,p}$.

Le polynôme caractéristique de $P(\phi_p)$ est donc $(X - 1)^2(X - \alpha_p/\beta_p)(X - \beta_p/\alpha_p) = (X - 1)^2(X^2 - (\alpha_p^2 + \beta_p^2)(\alpha_p \beta_p)^{-1}X + 1) = (X - 1)^2(X^2 - (a_p^2 a_{p,p} - 2)X + 1)$. On utilise la relation $\bar{a}_p = a_p \bar{a}_{p,p}$. On trouve que le polynôme caractéristique est $(X - 1)^2((X + 1)^2 - |a_p|^2 X) = X^4 - |a_p|^2 X^3 + 2(|a_p|^2 - 1)X^2 - |a_p|^2 X + 1$. Ainsi le facteur d'Euler en p est $L_p(s) = (p^{-s} - 1)^2((p^{-s} + 1)^2 - |a_p|^2 p^{-s})^{-1}$.

3.a. Quelles sont les valeurs propres avec multiplicité de $P(\phi_\infty)$, où ϕ_∞ est une conjugaison complexe ?

Ce sont les rapports des valeurs propres de $\rho(\phi_\infty)$. On trouve 1 et -1 tous deux avec la multiplicité 2.

3.b. En déduire le facteur à l'infini $L_\infty(P, s)$.

On trouve $\Gamma_{\mathbf{R}}(s)^2 \Gamma_{\mathbf{R}}(s + 1)^2 = \Gamma_{\mathbf{C}}(s)^2$.

4. Soit $\psi : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathbf{C}^\times$ un caractère. Montrer que $\rho \otimes \psi$ et ρ ont même représentation adjointe.

C'est immédiat puisque $\rho(\sigma)\psi(\sigma)I_2 M \psi(\sigma)^{-1} I_2 \rho(\sigma)^{-1} = \rho(\sigma)M\rho(\sigma)^{-1}$.

5. Y a-t-il des cas où P est non ramifiée en p et ρ est ramifiée en p ?

Supposons que $\rho = \rho_0 \otimes \psi$ avec ρ_0 non ramifiée en p et ψ caractère ramifié en p . Alors P n'est pas ramifiée en p et ρ est ramifiée en p , puisque ψ est ramifié en p .

6. Montrer que le conducteur de P est N^2 .

Les seuls nombres premiers qui divisent le conducteur de P sont ceux qui divisent N . Pour q diviseur premier de N , puisque $\rho(I_q)$ est d'ordre premier à q , on a que l'inertie est modérée. On a donc $G_1 = \{0\}$. Soit $g = \rho(\sigma)$ un générateur de $\rho(I_q)$. Soit w un vecteur propre de g avec $g(w) = \lambda w$, et $\lambda \neq 1$. Alors (v, w) est une base de $\mathbf{C}^2$. Notons (v^*, w^*) la base duale. Le produit tensoriel de ces deux bases donne une base de vecteurs propres pour $P(\sigma)$ de $M_2(\mathbf{C})$. Les valeurs propres de $P(\sigma)$ sont $1, 1, \lambda$ et $\bar{\lambda}$. Ainsi, l'espace $V^{G_0} = V^{I_q}$ a dimension 2. Donc l'exposant en q du conducteur de ρ est 2 pour tout diviseur premier q de N . Le conducteur de P est bien N^2 .

7. En déduire $\Lambda(P, s)$ (fonction $L(P, s)$ complétée).

Il reste à déterminer les facteurs d'Euler en q pour q diviseur premier de N . On vient de voir que le sous-espace invariant par le sous-groupe d'inertie en q est de dimension 2. Avec les notations ci-dessus, $P(\phi_q)$ opère trivialement sur la partie fixée par l'inertie. On a donc, pour tout $q|N$, $L_q(P, s) = (1 - q^{-s})^2$. On a donc $\Lambda(P, s) = N^{-s} \Gamma_{\mathbf{C}}(s) \prod_p L_p(s)$.

8.a. Notons $M_2^0(\mathbf{C}) = \{M \in M_2(\mathbf{C}) / \text{tr}(M) = 0\}$. Montrer que $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ stabilise $M_2^0(\mathbf{C})$ et agit trivialement sur un supplémentaire. Notons P^0 la représentation déduite de P par restriction à $M_2^0(\mathbf{C})$.

On a $M_2(\mathbf{C}) = M_2^0(\mathbf{C}) \oplus \mathbf{C}I_2$. Chaque terme est stable puisque la trace est invariante par conjugaison et que les matrices scalaires commutent universellement.

8.b. En déduire que $L(P, s) = L(P^0, s)\zeta(s)$, où ζ est la fonction zêta de Riemann.

Puisque la fonction L d'une somme directe est le produit des fonctions L , il suffit de prouver que la fonction L de la représentation déduite de P par restriction au matrices scalaire est $\zeta(s)$. C'est évident puisque cette dernière représentation est triviale de dimension 1.

8.c. Montrer que P est isomorphe à P^* (sa contragrédiente).

C'est une propriété des représentations adjointes. On peut le montrer en constatant que ρ^* est isomorphe à $\rho \otimes \bar{\epsilon}$, où ϵ est le caractère obtenu comme déterminant de ρ , ce qui est particulier aux représentations de dimension 2. Donc ρ et ρ^* ont même représentation adjointe. Or la représentation adjointe de ρ^* est P^* .

9. Soit K une extension quadratique de $\mathbf{Q}$. Supposons que ρ est induite d'un caractère ξ de $\text{Gal}(\bar{K}/K)$.

9.a. Montrer que P est isomorphe à $\text{Ind}_{K/\mathbf{Q}} 1 \oplus \text{Ind}_{K/\mathbf{Q}}(\xi/\xi')$, où ξ' est le caractère de $\text{Gal}(\bar{K}/K)$ donné par $\xi'(\sigma) = \xi(\tau\sigma\tau^{-1})$, avec $\tau \in \text{Gal}(\mathbf{Q}/\mathbf{Q}) - \text{Gal}(\bar{K}/K)$.

Noter que c'est un énoncé purement algébrique. Comme la contragrédience commute à l'induction, P s'identifie à $\text{Ind}_{K/\mathbf{Q}} \xi \otimes \text{Ind}_{K/\mathbf{Q}} \bar{\xi}$. Comme $\{1, \tau\}$ est un système de représentants de $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})/\text{Gal}(\bar{K}/K)$, on a une base (e_1, e_τ) de l'induite de ξ . La base duale (e_1^*, e_τ^*) donne une base de l'induite de ξ' . On obtient une base de $M_2(\mathbf{C})$ comme produit tensoriel de ces deux bases. Alors le sous-espace E engendré par $\{e_1 \otimes e_1^*, e_\tau \otimes e_\tau^*\}$ est stable par $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, dont l'action se factorise par $\text{Gal}(K/\mathbf{Q})$. Alors τ échange les deux vecteurs de la base, si bien que E est la représentation régulière de $\text{Gal}(K/\mathbf{Q})$ et est donc isomorphe à $\text{Ind}_{K/\mathbf{Q}} 1$. Le sous-espace F de base $\{e_1 \otimes e_\tau^*, e_\tau \otimes e_1^*\}$ vérifie des

propriétés analogues. Il s'identifie à $\text{Ind}_{K/\mathbf{Q}}(\xi/\xi')$.

9.b. Montrer que $L(P, s) = \zeta_K(s) L(\xi/\xi', s)$, où ζ_K est la fonction zêta de Dedekind de K .

La fonction L est invariante par induction (avec changement de corps), si bien que $L(\text{Ind}_{K/\mathbf{Q}} 1, s) = L(1, s) = \zeta_K(s)$, idem pour l'autre facteur.

9.c. En déduire que $\Lambda(P, s)$ a un pôle simple en $s = 1$?

La fonction ζ_K a un pôle simple en $s = 1$. Comme ρ est irréductible, on a $\xi \neq \xi'$, si bien que $\xi/\xi' \neq 1$. Ainsi, $L(\xi/\xi', s)$ n'a pas de pôle ni zéro en $s = 1$. On a bien un pôle simple.

9.d. Quel est l'ordre d'annulation de $\Lambda(P, s)$ en $s = 0$?

Comme P est isomorphe à P^* , on a une équation fonctionnelle reliant $\Lambda(P, s)$ à $\Lambda(P, 1-s)$. Ainsi $\Lambda(P, 1-s)$ a un pôle simple en $s = 0$.

II

Supposons que ρ est attachée à une forme modulaire primitive parabolique f de poids 1 et niveau N . On note $\sum_{n \geq 1} a_n q^n$ le q -développement de f . Soit p un nombre premier ne divisant pas N . On a alors $L(\rho, s) = L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s}$.

1. Montrer que la série formelle $\sum_{r \geq 0} a_{p^r} X^r$ vaut $1/[(1 - \alpha_p X)(1 - \beta_p X)]$.

Comme $L(f, s) = L(\rho, s)$, on a $L_p(f, s) = L_p(\rho, s) = 1/[1 - \alpha_p p^{-s}][1 - \beta_p p^{-s}]$. Or, puisque f est primitive $L_p(f, s) = \sum_{r=0}^{\infty} a_{p^r} p^{-rs}$. On obtient le résultat en posant $X = p^{-s}$.

2. En déduire qu'on a, pour r entier ≥ 0 , $a_{p^r} = \sum_{i=0}^r \alpha_p^i \beta_p^{r-i}$.

Cela résulte de la formule $1/[(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})] = \sum_{i=0}^{\infty} \alpha_p^i p^{-is} (\sum_{j=0}^{\infty} \beta_p^j p^{-js})$ et du développement de ce dernier produit.

3. Exprimer $\sum_{r \geq 0} |a_{p^r}|^2 X^r$ comme une fraction rationnelle en X .

On a $|a_{p^r}|^2 = \sum_{i,j=0}^r \alpha_p^i \beta_p^{r-i} \bar{\alpha}_p^j \bar{\beta}_p^{r-j} = \sum_{i,j=0}^r (\alpha_p/\beta_p)^i (\beta_p/\alpha_p)^j = (1 - \lambda^{r+1})(1 - \lambda^{-r-1})/[(1 - \lambda)(1 - \lambda^{-1})]$, en posant $\lambda = \alpha_p/\beta_p$. On s'est ramené à des calculs de séries géométriques. On trouve $\sum_{r \geq 0} |a_{p^r}|^2 X^r = (1 + X)/[(1 - X)(1 - \alpha_p \bar{\beta}_p X)(1 - \beta_p \bar{\alpha}_p X)]$.

4. Comparer le facteur d'Euler en p de $L(P, s)$ et $\sum_{r \geq 0} |a_{p^r}|^2 p^{-rs}$.

On a $\sum_{r \geq 0} |a_{p^r}|^2 p^{-rs} = (1 + p^{-s})(1 - p^{-s}) L_p(P, s) = (1 - p^{-2s}) L_p(P, s)$.

5. Quel est le lien entre $L(P, s)$ et $\sum_{n=1}^{\infty} |a_n|^2 n^{-s}$?

Pour n et m premiers entre eux, on a $a_{nm} = a_n a_m$, puisque f est primitive, et donc $|a_{nm}|^2 = |a_n|^2 |a_m|^2$. On a donc $\sum_{n=1}^{\infty} |a_n|^2 n^{-s} = \prod_p (\sum_{r=0}^{\infty} |a_{p^r}|^2 p^{-rs})$. On peut donc comparer facteur par facteur, ce qui donne, aux facteurs correspondant aux nombres premiers divisant N près, l'égalité $L(P, s) = \sum_{n=1}^{\infty} |a_n|^2 n^{-s} \zeta(2s)$, mais il faut examiner les facteurs indéterminés pour $q|N$.

Si q est un nombre premier qui divise N , on a $L_q(P, s) = 1/(1 - q^{-s})^2$. Par ailleurs, on a $\sum_{r \geq 0} |a_{q^r}|^2 q^{-rs} = 1/(1 - q^{-s})$.

On obtient finalement

$$L(P, s) = \left(\sum_{n=1}^{\infty} |a_n|^2 n^{-s} \right) \zeta(2s) \prod_{q|N} \frac{(1 - q^{-s})(1 - q^{-2s})}{(1 - q^{-s})^2} = \left(\sum_{n=1}^{\infty} |a_n|^2 n^{-s} \right) \zeta(2s) \prod_{q|N} (1 + q^{-s}).$$