

CORRIGÉ de l'EXAMEN du 20 février 2026

I

Soit K un corps de nombres. Soit $\rho : \text{Gal}(\bar{K}/K) \rightarrow \text{GL}_2(\mathbf{C})$ un motif d'Artin irréductible, qui se factorise par le groupe fini $G = \text{Gal}(L/K)$. On suppose que ρ est isomorphe à sa contrédiente ρ^* . Notons $\epsilon : \text{Gal}(\bar{K}/K) \rightarrow \mathbf{C}^\times$ le déterminant de ρ . Posons $H = \{h \in G \mid \det(\rho(h)) = 1\}$.

1. Rappeler le lien entre ρ , ρ^* et ϵ .

On a ρ^* isomorphe à $\rho \otimes \bar{\epsilon}$.

2. Montrer que ϵ est un caractère trivial ou quadratique.

Comme ρ est isomorphe à ρ^* , les déterminants sont isomorphes. On a donc $\epsilon = \bar{\epsilon}$. Ainsi ϵ prend des valeurs réelles et donc dans $\{-1, 1\}$.

3. Montrer que tout $g \in G$ satisfait $\det(\rho(g)) = 1$ ou $\text{tr}(\rho(g)) = 0$.

D'après 1, ρ et $\rho \otimes \bar{\epsilon}$ sont isomorphes. En particulier, on a $\text{tr}(\rho(g)) = \text{tr}(\rho(g)\epsilon(g)) = \text{tr}(\rho(g))\epsilon(g)$ et donc $\text{tr}(\rho(g))(1 - \epsilon(g)) = 0$.

4. Montrer que si $g \in G$, et $g \notin H$, on a $\rho(g)$ d'ordre 2. Si $G - H$ est non vide, en déduire que pour tout $g_0 \in G - H$ et $h \in H$, on a $\rho(g_0 h g_0) = \rho(h^{-1})$, puis que $\rho(H)$ est abélien.

Si $g \in G - H$, on a $\epsilon(g) \neq 1$ et donc $\epsilon(g) = -1$, et $\text{tr}(\rho(g)) = 0$. Le polynôme caractéristique de $\rho(g)$ est donc $X^2 - 1$ si bien que $\rho(g)$ est d'ordre 2. Alors H est d'indice 2 dans G . On a $\rho(g_0 h g_0 h g_0)$ d'ordre 2 et donc $\rho(g_0 h g_0) = \rho(h^{-1})$. L'application $x \mapsto x^{-1}$ est alors un automorphisme de $\rho(H)$, si bien que $\rho(H)$ est abélien.

5. Si ϵ est quadratique, l'image de ρ dans $\text{PGL}_2(\mathbf{C})$ est-elle isomorphe à un groupe cyclique, diédral, tétraédral ($\mathcal{A}_4$), octaédral ($\mathcal{S}_4$), ou icosaédral ($\mathcal{A}_5$) ?

Comme ρ est irréductible, le cas cyclique est exclu. Comme H est d'indice 2 dans G et est envoyé injectivement dans $\text{PGL}_2(\mathbf{C})$, la moitié au moins des éléments de l'image de ρ dans $\text{PGL}_2(\mathbf{C})$ est d'ordre 2. Cet état de fait est compatible avec le seul cas diédral.

6. Si ϵ est quadratique, montrer qu'il existe une extension quadratique $E|K$ et un caractère $\chi : \text{Gal}(\bar{K}/E) \rightarrow \mathbf{C}^\times$, tel que ρ est isomorphe à la représentation induite de E à K de χ .

On a vu que G admet un sous-groupe H d'indice 2 et abélien. Notons E le sous-corps de L fixé par H . C'est une extension quadratique de K . Comme H est abélien, $\rho(H)$ est formé de matrices simultanément diagonalisables de valeurs propres des racines de l'unité. C'est donc un groupe cyclique. Soit (e_1, e_2) une base de diagonalisation pour $\rho(H)$. Alors la projection sur la droite dirigée par e_1 fournit le caractère χ cherché (si on choisit e_2 , on obtient le caractère inverse). On vérifie que ρ est induite de χ .

II

On reprend les notations de I. On suppose maintenant que ϵ est quadratique.

1. Notons $L(\rho, s) = \sum_I a_I / |I|^s$ la fonction L de ρ développée comme série de Dirichlet indexée par les idéaux de $\mathcal{O}_K$. Montrer qu'on a $a_I \in \mathbf{R}$ pour tout idéal I .

Par développement du produit eulérien, il suffit de prouver cela pour $I = \mathcal{P}$ premier. Si $\mathcal{P}$ est non ramifié dans L , $a_{\mathcal{P}}$ est la trace de l'image par d'une substitution de Frobenius $\text{Frob}_{\mathcal{P}}$, et donc nul (si $\epsilon(\text{Frob}_{\mathcal{P}}) = -1$) ou réel (si $\epsilon(\text{Frob}_{\mathcal{P}}) = 1$). Si $\mathcal{P}$ est premier et ramifié dans L , tout élément g du groupe d'inertie en I admet un vecteur fixe sous $\rho(g)$. Si $g \in H$, on a $\epsilon(g) = 1$ et donc $\rho(g)$ a pour seule valeur propre 1, et $\rho(g) = 1$ ce qui est absurde car $\mathcal{P}$ est ramifié. On a donc $\rho(g) \notin H$. Le groupe d'inertie est normal dans le groupe de décomposition, et le quotient est cyclique, si bien le groupe de décomposition en $\mathcal{P}$ ne peut être que d'ordre 2 ou 4. Ainsi la substitution de Frobenius ne peut avoir pour valeur propre que ± 1 , d'où $a_{\mathcal{P}} \in \mathbf{R}$.

2. Montrer que $L(\rho, s) = L(\chi, s)$.

Puisque ρ est induite de χ , c'est une conséquence immédiate de la formule qui exprime la fonction L des motifs d'Artin induits.

3. Montrer que la fonction L complétée $\Lambda(\rho, s)$ est holomorphe sur $\mathbf{C}$.

On a $\Lambda(\rho, s) = \Lambda(\chi, s)$. Or la fonction $\Lambda(\chi, s)$ satisfait la conjecture d'Artin puisque c'est une fonction L complétée abélienne.

4. Montrer que $\Lambda(\rho, s) = \Lambda(\rho, 1 - s)$ ou $\Lambda(\rho, s) = -\Lambda(\rho, 1 - s)$ pour tout $s \in \mathbf{C}$.

Par l'équation fonctionnelle, il existe $w \in \mathbf{C}$ tel que $\Lambda(\rho, s) = w\Lambda(\rho, 1 - s)$, puisque ρ et ρ^* sont isomorphes. On a donc $\Lambda(\rho, s) = w^2\Lambda(\rho, s)$ et donc $w = 1$ ou $w = -1$.

5. Montrer que $L(\rho, s)$ est un nombre réel > 0 si s est un nombre réel > 1 .

La fonction $L(\rho, s)$ est donnée par un produit eulérien de fonctions holomorphes jamais nulles qui converge uniformément sur tout compact pour $\Re(s) > 1$. Ce produit eulérien ne s'annule donc pas. C'est une fonction continue sur $]1, +\infty[$. Elle tend vers 1 lorsque s tend vers $+\infty$. Ainsi, elle est > 0 sur $]1, +\infty[$.

6. Supposons que $\Lambda(\rho, 1/2) \neq 0$. Montrer que $\Lambda(\rho, s)$ réel > 0 si s est un nombre réel < 0 .

Comme $\Lambda(\rho, 1/2) = w\Lambda(\rho, 1/2)$, on a nécessairement $w = 1$. Donc, on a $\Lambda(\rho, s) = \Lambda(\rho, 1 - s)$. Il suffit d'utiliser la question précédente.

III

On reprend les notations de **I** et **II**. On suppose que ϵ est quadratique, que $K = \mathbf{Q}$ et qu'il existe une forme modulaire primitive $f \in S_1(N)$ de q -développement $\sum_{n \geq 1} a_n q^n$ et telle que $L(f, s) = L(\rho, s)$. Notons W_N l'opérateur d'Atkin-Lehner sur $S_1(N)$.

1. Supposons $W_N(f) \neq if$. Montrer l'annulation en $s = 1/2$ du prolongement analytique de $s \mapsto \int_0^\infty f(iy)y^{s-1} dy$.

On a $\Lambda(f, s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(f, s) = N^{s/2} \int_0^\infty f(iy)y^s dy/y$. On a $W_N(f) = wif$. On a donc $w \neq 1$ et donc $0 = \Lambda(\rho, 1/2) = \Lambda(f, 1/2)$ et donc le prolongement analytique de $s \mapsto \int_0^\infty f(iy)y^{s-1} dy$ s'annule en $s = 1/2$.

2. Montrer que la densité analytique de l'ensemble des nombres premiers p tels que $a_p = 0$ vaut $1/2$.

Si p est non-ramifié pour ρ , ce qui n'exclut qu'un nombre fini de premier, le nombre a_p est le p -ème coefficient du q -développement de f . C'est donc aussi le p -ème coefficient de la série de Dirichlet $L(f, s)$, qui est aussi la trace de $\rho(\text{Frob}_p)$. Cette trace est nulle si et seulement si $\text{Frob}_p \notin H$. Or H est un sous-groupe d'indice 2 de G , si bien que, par le théorème de densité de Chebotarev, la densité est $1/2$.

3. Comment calculer numériquement de façon approchée $\Lambda(\rho, 1/2)$ à partir de N , de la valeur propre de W_N et des coefficients a_n ? (Une esquisse suffit.)

Ce calcul pose problème en raison de la convergence de $\int_0^\infty f(iy)y^{-1/2} dy$ en $y = 0$. On écrit $\Lambda(\rho, s) = N^{s/2} \int_0^\infty f(iy)y^{-s} dy = N^{s/2} (\int_0^{N^{-1/2}} f(iy)y^{-s} dy + \int_{N^{-1/2}}^\infty f(iy)y^{-s} dy)$. Le calcul de l'autre intégrale utilise la relation $W_N(f) = iw f$ et donc permet le changement de variable $y \mapsto 1/(Ny)$, si bien qu'on a $\Lambda(\rho, 1/2) = 2N^{1/4} (\int_{N^{-1/2}}^\infty f(iy)y^{-1/2} dy)$ qui converge sans problème. On peut développer suivant le q -développement de f , les termes décroissent exponentiellement rapidement vers 0.

IV

Soit L le corps de décomposition sur $\mathbf{Q}$ du polynôme $X^4 - X - 1$. Noter que discriminant de ce polynôme est -283 , que l'anneau des entiers de $\mathbf{Q}(\sqrt{-283})$ est l'anneau $\mathbf{Z}[(1 + \sqrt{-283})/2]$, que le nombre de classe de $\mathbf{Q}(\sqrt{-283})$ est égal à 3, que le groupe de Galois $\text{Gal}(L/\mathbf{Q})$ s'identifie au groupe symétrique $\mathcal{S}_4$ via son action sur les racines de $X^4 - X - 1$, que ce polynôme admet une unique racine double modulo 283.

On identifie le groupe symétrique $\mathcal{S}_4$ à un sous-groupe de $\text{PGL}_2(\mathbf{C})$. On a donc une représentation projective $\tilde{\rho} : \text{Gal}(L/\mathbf{Q}) \rightarrow \text{PGL}_2(\mathbf{C})$.

Posons $M = L(\sqrt{4 - 7x^2})$, où x est une racine de $X^4 - X - 1$. Le calcul de la norme $N_{\mathbf{Q}(x)|\mathbf{Q}}(4 - 7x^2)$ donne $-7^2 \cdot 283$.

On admet que $M|\mathbf{Q}$ est galoisienne et que $\tilde{\rho}$ se relève en une représentation $\rho : \text{Gal}(M/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{C})$.

1. Montrer que l'extension $M|\mathbf{Q}(\sqrt{-283})$ est partout non ramifiée.

On a $\mathbf{Q}(\sqrt{-283}) \subset L$, par la théorie du discriminant. L'extension $L|\mathbf{Q}$ est non ramifiée en dehors de 283. L'indice de ramification de 283 dans L est égal à 2, car $X^4 - X - 1$ possède une unique racine double modulo 283. Comme l'indice de ramification de 283 dans $\mathbf{Q}(\sqrt{-283})$ est égal à 2. L'extension $L|\mathbf{Q}$ est non ramifiée en l'unique premier au dessus de 283. Il reste à voir que l'extension $M|L$ est partout non ramifiée. Au vu de la norme de $4 - 7x^2$, elle est non ramifiée en dehors de 7 et 283. Comme cette norme est un carré dans les complétés de $\mathbf{Q}(\sqrt{-283})$, l'extension $M|L$ est partout non ramifiée.

2. Montrer que le conducteur de ρ est 283.

C'est une puissance de 283, puisque ρ est non ramifiée en dehors de 283. On vient de voir que l'indice de ramification en 283 de $M|\mathbf{Q}$ est 2. L'image par ρ d'un sous-groupe d'inertie I_{283} en 283 est d'ordre 2, et son image dans $\mathcal{S}_4 \subset \text{PGL}_2(\mathbf{C})$ est aussi d'ordre 2. Donc l'élément non trivial de $\rho(I_{283})$ a pour valeur propre 1 et -1 . Donc le sous-espace de $\mathbf{C}^2$ invariant par $\rho(I_{283})$ est de dimension 1. Comme la ramification est modérée, puisque 283 ne divise pas l'ordre de $\text{Im}(\rho)$, les groupes de ramification supérieure G_i sont triviaux pour $i > 0$. Le conducteur local en 283 est donc 1. Le conducteur global est $283^1 = 283$.

3. Montrer que ρ est impaire.

Le polynôme $X^4 - X - 1$ possède deux racines réelles. Ainsi la conjugaison complexe ϕ possède deux points fixes parmi les racines, et échange les deux autres racines. Ainsi $\tilde{\rho}(\phi)$ est d'ordre 2. Donc $\rho(\phi)$ est d'ordre 2, mais n'est pas $-I_2$. Donc ses valeurs propres sont 1 et -1 , et son déterminant est -1 .

4. Montrer que $\det(\rho)$ est le caractère quadratique $\epsilon : \text{Gal}(\mathbf{Q}(\sqrt{-283})/\mathbf{Q}) \rightarrow \{-1, 1\}$.

Le déterminant de ρ est un caractère non ramifié en dehors de 283. Il est non trivial par la question précédente. De plus $\det(\rho)$ se factorise par G (puisque le déterminant de la matrice $-I_2$ est 1). Le noyau de $\det(\rho)$ correspond à un quotient abélien $\mathcal{S}_4$. Le seul quotient abélien de $\mathcal{S}_4$ est le quotient par le sous-groupe alterné. Donc le noyau de $\det(\rho)$ est trivial sur le sous-corps de L invariant par le groupe alterné. Ce sous-corps est $\mathbf{Q}(\sqrt{-283})$ par la théorie du discriminant. Comme $\mathbf{Q}(\sqrt{-283})$ est le sous-corps de L fixé par le sous-groupe alterné de $\mathcal{S}_4$, $\epsilon(\rho(g))$ n'est autre que la signature de g .

5. À isomorphisme près, ρ est-il le seul relèvement de $\tilde{\rho}$ de conducteur 283 ?

Tout relèvement de ρ est de la forme $\rho \otimes \chi$, où χ est un caractère de $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, qui est non ramifié en dehors de 283. Pour que le conducteur soit 283, il faut et il suffit que la dimension de $(\mathbf{C}^2)^{\rho \otimes \chi(I_{283})}$ soit 1. Cela revient à dire que la restriction de χ à I_{283} est 1 ou $\bar{\epsilon} = \epsilon$. On a donc $\rho \otimes \epsilon$ comme alternative à ρ . Or $\rho \otimes \epsilon$ est la contragrédiente de ρ , qui n'est pas isomorphe à ρ (par exemple : elle n'est pas de type diédral).

6. Soit p un nombre premier $\neq 283$. Soit N_p le nombre de racines $X^4 - X - 1$ dans le corps fini $\mathbf{F}_p$. Montrer que si $N_p = 4$, il existe $n, m \in \mathbf{Z}$ tels que $p = n^2 + nm + 71m^2$.

Si $N_p = 4$, on a $\tilde{\rho}(\text{Frob}_p) = 1$, et donc p est totalement décomposé dans L , et a fortiori dans $\text{Gal}(\mathbf{Q}(\sqrt{-283})/\mathbf{Q})$. Donc p est totalement décomposé dans une extension abélienne non ramifiée de degré 3 de $\mathbf{Q}(\sqrt{-283})$, et donc dans le corps de classe de Hilbert de $\mathbf{Q}(\sqrt{-283})$, puisque le groupe de classes de $\mathbf{Q}(\sqrt{-283})$ est cyclique d'ordre 3. Donc les idéaux au dessus de p dans $\mathbf{Q}(\sqrt{-283})$ sont principaux. Comme l'anneau des entiers de $\mathbf{Q}(\sqrt{-283})$ est $\mathbf{Z}[(1 + \sqrt{-283})/2]$, il existe $n, m \in \mathbf{Z}$ tels que $p = (n + m(1 + \sqrt{-283})/2)(n + m(1 - \sqrt{-283})/2)$ et donc $p = n^2 + nm + 71m^2$.

7. Montrer que si $N_p = 4$, le facteur d'Euler en p de $L(\rho, s)$ est $L_p(\rho, s) = (1 \pm p^{-s})^{-2}$.

Dans ce cas, on a $\tilde{\rho}(\text{Frob}_p) = 1$ et donc $\rho(\text{Frob}_p) = \pm 1$. Le polynôme caractéristique de $\rho(\text{Frob}_p)$ est donc $(X \pm 1)^2$. On peut préciser le signe en examinant si $4 - 7x^2$ est un carré modulo p lorsque x est une racine de $X^4 - X - 1$ modulo p .

8. Suivant la factorisation de $X^4 - X - 1$ modulo p , donner autant que possible le facteur d'Euler en p de $L(\rho, s)$.

Rappelons que $\epsilon(\rho(g))$ est la signature de $g \in \mathcal{S}_4$.

Si $X^4 - X - 1$ est scindé voir ci-dessus.

Si $X^4 - X - 1$ admet un facteur irréductible de degré 3, $\tilde{\rho}(\text{Frob}_p)$ est un 3-cycle de $\mathcal{S}_4$. Alors $\rho(\text{Frob}_p)$ est d'ordre 3 ou 6 et de déterminant 1. Son polynôme caractéristique est donc $X^2 \pm X + 1$.

Si $X^4 - X - 1$ admet deux facteurs irréductibles de degré 2, $\tilde{\rho}(\text{Frob}_p)$ est une double transposition de $\mathcal{S}_4$. Alors $\rho(\text{Frob}_p)$ est d'ordre 2 ou 4 et de déterminant 1, si bien que son polynôme caractéristique est $X^2 + 1$.

Si $X^4 - X - 1$ admet un facteur irréductible de degré 2 et deux facteurs de degré 1, $\tilde{\rho}(\text{Frob}_p)$ est une transposition de $\mathcal{S}_4$. Alors $\rho(\text{Frob}_p)$ est d'ordre 2 ou 4 et de déterminant -1 . Ainsi son polynôme caractéristique est $X^2 - 1$.

Si $X^4 - X - 1$ est irréductible, $\tilde{\rho}(\text{Frob}_p)$ est un 4-cycle de $\mathcal{S}_4$. Alors $\rho(\text{Frob}_p)$ est d'ordre 4 ou 8 et de déterminant -1 . Son polynôme caractéristique est $X^2 + 1$ ou $X^2 \pm \sqrt{-2}X - 1$.

On peut préciser les signes en examinant $4 - 7x^2$ pour x racine de $X^4 - X - 1$.

Pour des compléments, voir J-P. Serre : *On a Theorem of Jordan*, Bulletin (New Series) of the American Mathematical Society, Volume 40, Number 4, Pages 429-440.