XVIII
Tordues, relèvements, exemples

1. Torsion par un caractère

Soit K un corps de nombres. Soit $\bar{K}$ une clôture algébrique de K. Soit ρ : $\mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(E)$ un motif d'Artin, avec E espace vectoriel complexe de dimension finie n. Soit $\chi : \mathrm{Gal}(\bar{K}/K) \to \mathbf{C}^\times$ un caractère.

On a $\rho \otimes \chi : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(E)$ donnée par $\sigma \mapsto \rho(\sigma)\chi(\sigma)$. C'est la *tordue de ρ par le caractère χ*.

Notons $P\rho$ la *représentation projective* associée à ρ. C'est le morphisme de groupe $\mathrm{Gal}(\bar{K}/K) \to \mathrm{PGL}(E)$ déduit de ρ. Les représentations projectives $P\rho$ et $P(\rho \otimes \chi)$ sont identiques.

Soit v une place réelle de K. Notons $n_v^+ = n_v^+(\rho)$ la dimension de la partie invariante de E par une conjugaison complexe en v. Posons $n_v^- = n_v^-(\rho) = n - n_v^+$. On a alors $n_v^+(\rho \otimes \chi) = n_v^+(\rho)$ si l'image par χ d'une conjugaison complexe en v est 1 et $n_v^+(\rho \otimes \chi) = n_v^-(\rho)$ si l'image par χ d'une conjugaison complexe en v est -1.

Si v est une place finie non ramifiée pour χ, *i.e.* le noyau de χ contient un sous-groupe d'inertie I_v en v, on $\rho(I_v) = \rho \otimes \chi(I_v)$. On a alors

$$L_v(\rho \otimes \chi, s) = \det(1 - \rho(\mathrm{Frob}_v)\chi(\mathrm{Frob}_v)|\mathcal{P}_v|^{-s}|V^{I_v})^{-1}.$$

Si v est une place finie non ramifiée pour ρ, mais ramifiée pour χ, on a

$$L_v(\rho \otimes \chi, s) = 1.$$

En effet $\rho \otimes \chi(I_v)$ est composé de matrices diagonales, non toutes triviales, si bien que $V^{\rho\otimes\chi(I_v)} = 1$.

PROPOSITION 1. — *Si les conducteurs N_ρ de ρ et N_χ de χ sont premiers entre eux, on a*

$$N_{\rho\otimes\chi} = N_\rho N_\chi^n.$$

Démonstration. — On le vérifie place par place. C'est vrai pour les places finies étrangères à N_ρ et N_χ.

Si v est une place finie telle que $\mathcal{P}_v | N_\rho$ et $\mathcal{P}_v \nmid N_\chi$, les groupes de ramification de $\rho \otimes \chi$ sont ceux de ρ. Les valuations $\mathcal{P}_v$-adiques de $N_{\rho\otimes\chi}$ et N_ρ sont égales.

Si v est une place finie telle que $\mathcal{P}_v \nmid N_\rho$ et $\mathcal{P}_v | N_\chi$, on a $(\rho \otimes \chi)_{|I_v} = (1 \otimes \chi)_{|I_v} \simeq \chi^n$, si bien que la valuation $\mathcal{P}_v$-adique de $N_{\rho\otimes\chi}$ est la valuation $\mathcal{P}_v$-adique de N_χ multipliée par n.

Remarque . — Si v est une place ramifiée pour ρ et χ, on ne peut pas prédire $L_v(\rho\otimes\chi, s)$ simplement. Pour en prendre conscience, considérer le cas où ρ' est une représentation non ramifiée en v et où on a $\rho = \rho' \otimes \bar{\chi}$. On a alors $L_v(\rho, s) = 1$ et $L_v(\rho\otimes\chi, s) = L_v(\rho', s)$.

La représentation contragrédiente de $\rho\otimes\chi$ est $\rho^*\otimes\bar{\chi}$. L'équation fonctionnelle de $\Lambda(\rho\otimes\chi)$ prend alors la forme

$$\Lambda(\rho\otimes\chi, 1-s) = w_{\rho\otimes\chi}\Lambda(\rho^*\otimes\bar{\chi}, s).$$

On peut donner une recette pour $w_{\rho\otimes\chi}$ si les conducteurs de ρ et de χ sont premiers entre eux.

On a immédiatement l'égalité des caractères

$$\det(\rho\otimes\chi) = \det(\rho)\chi^n.$$

Proposition 2. — *Si $n = 2$, la représentation contragrédiente de ρ est isomorphe à $\rho\otimes\det(\rho)^{-1}$. On a alors l'équation fonctionnelle*

$$\Lambda(\rho, 1-s) = w_{\rho\otimes\chi}\Lambda(\rho\otimes\det(\rho)^{-1}, s).$$

Démonstration. — C'est une conséquence de l'identité matricielle

$${}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}.$$

Si $n = 2$, et v est une place réelle de ρ est impaire en v si et seulement si $n_v^+(\rho) = 1$ et $n_v^-(\rho) = 1$, c'est-à-dire si et seulement si $n_v^+(\rho\otimes\chi) = 1$ et $n_v^-(\rho\otimes\chi) = 1$, si et seulement si $\rho\otimes\chi$ est impaire en v.

2. Exemples diédraux

Revenons sur la représentation $\rho : \mathrm{Gal}(M/\mathbf{Q}) \to S_3 \subset \mathrm{GL}_2(\mathbf{C})$, où M est le corps de décomposition du polynôme irréductible $X^3 - X - 1$ sur $\mathbf{Q}$. Le groupe de Galois $\mathrm{Gal}(M/\mathbf{Q})$ est d'ordre 6.

Ce polynôme est de discriminant -23, si bien que le seul nombre premier ramifié dans M est 23.

Le corps quadratique $\mathbf{Q}(\sqrt{-23})$ est l'unique corps quadratique contenu dans M. Le groupe $\mathrm{Gal}(M/\mathbf{Q}(\sqrt{-23}))$ est cyclique d'ordre 3.

L'extension $M|\mathbf{Q}(\sqrt{-23})$ est non ramifiée en dehors de 23. Montrons qu'elle est non ramifiée en l'unique idéal au dessus de 23. Comme le polynôme $X^3 - X - 1$ est congru à $(X-3)(X-10)^2$ modulo 23, l'extension $M|\mathbf{Q}$ n'est pas totalement ramifiée en 23. L'indice de ramification en 23 de $M|\mathbf{Q}$ n'est donc pas 6. Comme l'extension $\mathbf{Q}(\sqrt{-23})|\mathbf{Q}$ est totalement ramifiée en 23, et donc d'indice de ramification égal à 2, l'indice de ramification en 23 de $M|\mathbf{Q}$ est un diviseur pair de 6 qui n'est pas 6. C'est donc 2. Donc tout groupe d'inertie en 23 de $\mathrm{Gal}(M/\mathbf{Q})$ est d'ordre 2. L'indice de ramfication en l'unique idéal premier au dessus de 23 de l'extension $\mathrm{Gal}(M/\mathbf{Q}(\sqrt{-23}))$ est donc $2/2 = 1$, si bien que l'extension $M|\mathbf{Q}(\sqrt{-23})$ est non ramifiée en 23.

Comme c'est une extension abélienne partout non ramifiée et telle que toute place réelle de $\mathbf{Q}(\sqrt{-23})$ (il n'y en a pas, puisque c'est un corps quadratique imaginaire) reste réelle dans M, M est contenu dans le corps de classe de Hilbert H de $\mathbf{Q}(\sqrt{-23})$. On a donc un morphisme surjectif $\mathrm{Gal}(H/\mathbf{Q}(\sqrt{-23})) \to \mathrm{Gal}(M/\mathbf{Q}(\sqrt{-23}))$. Or, la loi de réciprocité d'Artin affirme que le groupe $\mathrm{Gal}(H/\mathbf{Q}(\sqrt{-23}))$ est isomorphe à $\mathcal{C}\ell(\mathbf{Q}(\sqrt{-23}))$, qui se trouve être cyclique d'ordre 3. Il en résulte que $H = M$. De plus, pour $\mathcal{Q}$ place finie de $\mathbf{Q}(\sqrt{-23})$, l'isomorphisme $\mathrm{Gal}(H/\mathbf{Q}(\sqrt{-23})) \simeq \mathcal{C}\ell(\mathbf{Q}(\sqrt{-23}))$ associe à $\mathrm{Frob}_{\mathcal{Q}}$ la classe de $\mathcal{Q}$ dans $\mathcal{C}\ell(\mathbf{Q}(\sqrt{-23}))$.

Soit $\chi : \mathrm{Gal}(M/\mathbf{Q}(\sqrt{-23})) \to \mathbf{C}^\times$. Alors ρ est isomorphe à l'induite $\mathrm{Ind}_{\mathbf{Q}(\sqrt{-23})/\mathbf{Q}}\chi$.

Elle est impaire, puisque $\mathbf{Q}(\sqrt{-23})$ est imaginaire. Le conducteur de ρ est donné par la formule

$$N_\rho = \mathcal{D}_{\mathbf{Q}(\sqrt{-23})} \times N_\chi^2.$$

Or on a $N_\chi = 1$, car χ est non ramifié. De plus $\mathcal{D}_{\mathbf{Q}(\sqrt{-23})} = 23\mathbf{Z}$. De plus, on a $\chi_\sigma = \bar{\chi}$, car ρ est diédrale et irréductible.

On peut examiner de plus près les groupes de ramification en une place finie q. Si $q \neq 23$, on a $I_{23} = G_0 = \{1\}$. Si $q = 23$, on sait que G_1 est le 23-sous-groupe de Sylow de G_0. Mais G_0 est le sous-groupe d'inertie en 23, qui est d'ordre 2. Donc $G_1 = \{1\}$. Notons h_0 l'élément non trivial de G_0. Il est d'ordre 2. Déterminer les invariants de V sous G_0 revient à déterminer les invariants sous h_0. Alors $\rho(h_0)$ est une involution ayant pour valeurs propres 1 et -1. La dimension des invariants sous G_0 est donc 1. On retrouve bien que le conducteur de ρ en 23 est 23^n, où n est donné par la recette du conducteur, c'est-à-dire

$$n = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|}(\dim(E) - \dim(E^{G_i})) = 1.$$

Écrivons maintenant la fonction L complétée de ρ. L'image d'une conjugaison complexe par ρ est une involution de valeurs propres 1 et -1. On a donc en la place infinie v, $n_v^+ = 1$ et $n_v^- = 1$. Le facteur à l'infini est

$$\Gamma_{\mathbf{R}}(s)^{n_v^+}\Gamma_{\mathbf{R}}(s+1)^{n_v^-} = \Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{R}}(s+1) = \Gamma_{\mathbf{C}}(s).$$

On obtient donc

$$\Lambda(\rho, s) = \Lambda(\chi, s) = 23^{-s}2(2\pi)^{-s}\Gamma(s)L(\rho, s).$$

La représentation contragrédiente ρ^* de ρ est $\mathrm{Ind}_{\mathbf{Q}(\sqrt{-23})/\mathbf{Q}}\chi^*$, car la contragrédience commute à l'induction.

Le déterminant de ρ est le caractère quadratique $\delta : \mathrm{Gal}(\mathbf{Q}(\sqrt{-23})/\mathbf{Q}) \to \{-1, 1\}$ qui à Frob_q associe le symbole de Legendre $\left(\frac{-23}{q}\right)$. On a donc

$$\rho^* \simeq \rho \otimes \delta.$$

La représentation ρ que nous venons de décrire est la représentation irréductible de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ de conducteur minimal 23.

On peut construire une représentation de type diédrale paire de façon analogue. Soit M un corps de décomposition sur $\mathbf{Q}$ du polynôme X^3-4X-1 de discriminant 229 (nombre premier). Le corps M contient le corps quadratique réel $\mathbf{Q}(\sqrt{229})$, le fait que le corps est réel est la seule différence avec le cas précédent.

Le corps M est totalement réel (car toutes les racines complexes de $X^3 - 4X - 1$ sont réelles). L'extension $M|\mathbf{Q}(\sqrt{229})$ est partout non ramifiée. Ainsi le groupe de Galois $\mathrm{Gal}(M/\mathbf{Q}(\sqrt{229}))$ est un quotient de $\mathrm{Gal}(H/\mathbf{Q}(\sqrt{229}))$ où H est le corps de classe de Hilbert de $\mathbf{Q}(\sqrt{229})$).

Comme le groupe de classe $\mathcal{C}\ell(\mathbf{Q}(\sqrt{229}))$ est cyclique d'ordre 3, et que ce groupe est isomorphe à $\mathrm{Gal}(H/\mathbf{Q}(\sqrt{229}))$, il en résulte que $M = H$.

La loi de réciprocité d'Artin affirme que, pour $\mathcal{Q}$ place finie de $\mathbf{Q}(\sqrt{229})$, l'image de $\mathrm{Frob}_{\mathcal{Q}} \in \mathrm{Gal}(H/\mathbf{Q}(\sqrt{229}))$ dans $\mathcal{C}\ell(\mathbf{Q}(\sqrt{229}))$ est la classe de $\mathcal{Q}$.

On a un caractère $\chi : \mathrm{Gal}(H/\mathbf{Q}(\sqrt{229})) \to \mathbf{C}^\times$ d'ordre 3. Posons $\rho = \mathrm{Ind}_{\mathbf{Q}(\sqrt{229})/\mathbf{Q}}\chi$. C'est une représentation paire puisque M est totalement réel.

Comme M est totalement réel, l'image par ρ d'une conjugaison complexe en l'unique place à l'infini v est triviale. On a $n_v^+ = 2$ et $n_v^- = 0$ Ainsi le facteur à l'infini de $\Lambda(\rho, s)$ est $\Gamma_{\mathbf{R}}(s)^2$. On a donc

$$\Lambda(\rho, s) = 229^{-s}\pi^{-s}\Gamma(s/2)^2 L(\rho, s).$$

Il n'est pas difficile de systématiser ces constructions d'exemples diédraux. Il suffit de choisir une extension quadratique $K(\sqrt{a})$ de K. On peut considérer un caractère χ d'un groupe des classes, ou plus généralement de classe de rayon, de $K(\sqrt{a})$. L'induite de $K(\sqrt{a})$ à K de χ fournit alors une représentation diédrale.

3. Relèvement de représentations projectives

Soit $\tilde{\rho} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{PGL}(E)$ une représentation projective de $\mathrm{Gal}(\bar{K}/K)$. Existe-t-il $\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(E)$ telle que $P\rho = \tilde{\rho}$?

On dit alors que ρ est un *relèvement* de $\tilde{\rho}$.

Proposition 3. — *Soient ρ_1 et ρ_2 des relèvements de $\tilde{\rho}$. Il existe un caractère χ : $\mathrm{Gal}(\bar{K}/K) \to \mathbf{C}^\times$ tel que $\rho_2 = \rho_1 \otimes \chi$.*

Démonstration. — Il résulte de la suite exacte

$$1 \to \mathbf{C}^\times \to \mathrm{GL}(E) \to \mathrm{PGL}(E) \to 1,$$

que ρ_1 et ρ_2 sont en rapport un morphisme à valeurs dans $\mathbf{C}^\times$.

Comme on a la suite exacte

$$1 \to \mathbf{C}^\times \to \mathrm{GL}(E) \to \mathrm{PGL}(E) \to 1,$$

la question du relèvement d'une représentation projective d'un groupe G résulte de la nullité du groupe $\mathrm{H}^2(G, \mathbf{C}^\times)$, où G opère trivialement sur $\mathbf{C}^\times$.

Théorème 4 (Tate). — *Si k est un corps p-adique ou $\mathbf{R}$ ou un corps de nombres, de clôture algébrique $\bar{k}$, on a*

$$\mathrm{H}^2(\mathrm{Gal}(\bar{k}/k), \mathbf{C}^\times) = 0.$$

La démonstration de Tate est nullement évidente et repose sur la théorie du corps de classe.

Corollaire . — *La représentation projective $\tilde{\rho}$ admet un relèvement.*

Mais cela ne donne par une construction pour le relèvement ρ. On souhaite que ρ soit non ramifiée en dehors d'un nombre fini de places.

Alternativement, on peut prescrire une collection de relèvements locaux $(\rho_{v|D_v})_{v\in\Omega_K}$ et chercher un relèvement global ρ tel que pour toute place finie v, on ait

$$\rho_{|I_v} = \rho_{v|I_v},$$

où D_v est un groupe de décomposition en v, et I_v le sous-groupe d'inertie de D_v.

Théorème 5 (Tate). — *Soit $(\rho_{v|D_v})_{v\in\Omega_K}$ tel que ρ_v soit une représentation $D_v \to \mathrm{GL}(V)$ qui soit un relèvement de $\tilde{\rho}_{|D_v}$. Supposons que $\rho_v(I_v) = \{1\}$ pour presque toute place finie v. Alors il existe un relèvement ρ de $\tilde{\rho}$ tel que pour toute place finie v de K on ait*

$$\rho_{|I_v} = \rho_{v|I_v},$$

où D_v est un groupe de décomposition en v, et I_v le sous-groupe d'inertie de D_v.

Si de plus $K = \mathbf{Q}$, ρ est unique à isomorphisme près.

Démonstration. — Soit $\rho_0 : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(E)$ telle que $P\rho_0 = \tilde{\rho}$. Soit v une place finie de K. Il existe $\chi_v : D_v \to \mathbf{C}^\times$ tel que $\rho_v = \rho_{0|D_v} \otimes \chi_v$. On a χ_v non ramifié, *i.e.* $\chi_v(I_v) = 1$, pour presque tout v.

Par la théorie du corps de classe local, χ_v s'identifie à un caractère ϕ_v de $K_v^\times$, qui s'annule sur $\mathcal{O}_v^\times$ lorsque χ_v est non ramifié. Lorsque χ_v est ramifié, $\chi_{v|I_v}$ s'identifie à la restriction à $\mathcal{O}_v^\times$ de ϕ_v. Il existe $n_v \geq 0$ tel que ϕ_v s'annule sur ${U_v}^{(n_v)}$. Considérons le cycle arithmétique $\mathcal{M} = \prod_v \mathcal{P}_v^{n_v}$, avec $n_v = 0$ si v est une place infinie. On a la suite exacte de groupes finis

$$1 \to \prod_v (\mathcal{O}_v^\times / U_v^{(n_v)}) \to \mathcal{C}\ell(K)^{\mathcal{M}} \to \mathcal{C}\ell(K) \to 1.$$

Le produit $\prod_v \chi_v$ définit un caractère de $\prod_v (\mathcal{O}_v^\times / U_v^{n_v})$, que l'on peut étendre en un caractère du groupe des classes de rayon $\mathcal{C}\ell(K)^{\mathcal{M}}$. Comme on a morphisme surjectif de groupes $\mathbf{A}_K^\times \to \mathcal{C}\ell(K)^{\mathcal{M}}$, on obtient un caractère ϕ du groupe des classes d'idèles $\mathbf{A}_K^\times$, dont la restriction à $\mathcal{O}_v^\times$ coïcide avec ϕ_v.

Par la théorie du corps de classe global, il existe un caractère $\chi : \mathrm{Gal}(\bar{K}/K) \to \mathbf{C}^\times$ tel que $\chi_{|D_v} = \chi_v$. Considérons $\rho_0 \otimes \chi$. C'est un relèvement de $\tilde{\rho}$. On a bien $(\rho_0 \otimes \chi)_{|I_v} = \rho_{0|I_v} \otimes \chi_{v|I_v} = \rho_{v|I_v}$.

Supposons $K = \mathbf{Q}$. Montrons l'unicité de ρ. On peut reprendre l'argument ci-dessus et utiliser la trivialité du groupe des classes de $\mathbf{Q}$, ou, de façon alternative, raisonner directement comme suit. Soit ρ' un autre relèvement de $\tilde{\rho}$ satisfaisant les conditions prescrites. Il existe un caractère χ de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ tel que ρ' est isomorphe à $\rho \otimes \chi$. Comme ρ et ρ' coïncident sur I_v pour toute place finie v, on a $\chi(I_v) = \{1\}$ pour toute place finie v. Ainsi χ est partout non ramifié. Mais comme $\mathbf{Q}$ n'admet pas d'extension non ramifiée, on a $\chi = 1$. Donc ρ et ρ' sont isomorphes.

4. Exemples polyédraux

Les exemples de motifs d'Artin de dimension 2 non diédraux ne se laissent pas construire aussi simplement que les exemples diédraux.

Exemple trouvé par Tate sans ordinateur. Soit M le corps de décomposition du polynôme $X^4 + 3X^2 - 7X + 3$, qui est irréductible, sur $\mathbf{Q}$. L'extension $M|\mathbf{Q}$ est non ramifiée en dehors de $\{7, 19\}$. Son groupe de Galois est isomorphe au groupe alterné A_4. On a donc une représentation projective $\tilde{\rho} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(M/\mathbf{Q}) \to A_4 \subset \mathrm{PGL}_2(\mathbf{C})$. Alors $\tilde{\rho}$ admet un relèvement à $\mathrm{GL}_2(\mathbf{C})$ de conducteur 133 de type tétraédral.

Soit M le corps de décomposition du polynôme $X^4 - X^3 + 5X^2 - 7X + 12$, qui est irréductible, sur $\mathbf{Q}$. L'extension $M|\mathbf{Q}$ est non ramifiée en dehors de $\{2, 37\}$. Son groupe de Galois est isomorphe au groupe symétrique S_4. On a donc une représentation projective $\tilde{\rho} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(M/\mathbf{Q}) \to S_4 \subset \mathrm{PGL}_2(\mathbf{C})$. Alors $\tilde{\rho}$ admet un relèvement à $\mathrm{GL}_2(\mathbf{C})$ de conducteur $148 = 2^2 \times 37$ de type octaédral.

Exemple trouvé par Buhler. Soit M le corps de décomposition du corps $X^5 + 10X^3 - 10X^2 + 35X - 18$. L'extension $M|\mathbf{Q}$ est non ramifiée en dehors de $\{2, 5\}$. Son groupe de Galois est isomorphe au groupe alterné A_5. $\tilde{\rho} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(M/\mathbf{Q}) \to A_5 \subset \mathrm{PGL}_2(\mathbf{C})$. Alors $\tilde{\rho}$ admet un relèvement à $\mathrm{GL}_2(\mathbf{C})$ de conducteur $800 = 2^5 \times 5^2$ de type icosaédral. Cette représentation a donné lieu à la première vérification de la conjecture d'Artin pour une représentation qui ne se factorise pas par le groupe de Galois d'une extension résoluble.

5. Retour sur $X^3 - X - 1$

L'anneau des entiers du corps quadratique $\mathbf{Q}(\sqrt{-23})$ est $\mathcal{O}_{\mathbf{Q}(\sqrt{-23})} = \mathbf{Z} + \mathbf{Z}\frac{1+\sqrt{-23}}{2}$. Soit $\chi : \mathcal{C}\ell(\mathbf{Q}(\sqrt{-23})) \to \mathbf{C}^\times$ d'ordre 3. Il lui correspond un caractère, encore noté χ par abus, du groupe de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\sqrt{-23}))$ par la théorie du corps de classe. Considérons encore la représentation induite $\rho = \mathrm{Ind}_{\mathbf{Q}(\sqrt{-23})/\mathbf{Q}}\chi$. Cette représentation se factorise par le groupe de Galois du corps de décomposition L du polynôme $X^3 - X - 1$. On a

$$L(\rho, s) = L(\chi, s) = \prod_{\mathcal{Q}} \frac{1}{\chi(\mathcal{Q})|\mathcal{Q}|^{-s}} = \sum_{I} \frac{\chi(I)}{|I|^s},$$

où $\mathcal{Q}$ parcourt les idéaux premiers de $\mathbf{Q}(\sqrt{-23})$ et I les idéaux entiers de $\mathbf{Q}(\sqrt{-23})$.

Pour p nombre premier, notons N_p le nombre de racines de $X^3 - X - 1$ dans le corps fini $\mathbf{F}_p$. Si $p = 23$, on a $N_p = 2$.

On a $N_p = 1$ si et seulement si p est inerte dans $\mathbf{Q}(\sqrt{-23})$ c'est-à-dire si et seulement si le symbole de Legendre $\left(\frac{-23}{p}\right)$ vaut -1.

On a $N_p = 0$ ou 3 sinon et alors p est décomposé dans $\mathbf{Q}(\sqrt{-23})$. Posons alors $p\mathcal{O}_{\mathbf{Q}(\sqrt{-23})} = \mathcal{Q}\bar{\mathcal{Q}}$.

On a $N_p = 3$ si et seulement si $\mathrm{Frob}_p = 1$ dans $\mathrm{Gal}(L/\mathbf{Q})$, c'est-à-dire si et seulement si $\mathrm{Frob}_{\mathcal{Q}} = 1$ dans $\mathrm{Gal}(L/\mathbf{Q}(\sqrt{-23}))$, c'est-à-dire si et seulement si la classe de $\mathcal{Q}$ dans $\mathcal{C}\ell(\mathbf{Q}(\sqrt{-23})$ est triviale c'est-à-dire si et seulement si l'idéal $\mathcal{Q}$ est principal. C'est le cas si et seulement si il existe n, $m \in \mathbf{Z}$ tels que $\mathcal{Q} = (n + m\frac{1+\sqrt{-23}}{2})\mathcal{O}_{\mathbf{Q}(\sqrt{-23})}$, c'est-à-dire $p = (n + m\frac{1+\sqrt{-23}}{2})(n + m\frac{1-\sqrt{-23}}{2}) = n^2 + nm + 6m^2$.

Un calcul analogue montre que $N_p = 0$ si et seulement si il existe n, $m \in \mathbf{Z}$ tels que $p = 2n^2 + nm + 3m^2$.

Remarque . — Cela peut être exprimé dans le langage des formes quadratiques dû à Gauss. Notons Q l'ensemble des formes quadratiques $(x, y) \mapsto ax^2 + bxy + cy^2$ de discriminant $\Delta = b^2 - 4ac = -23$. On définit une relation d'équivalence $\simeq$ sur Q par $q \simeq q'$ si et seulement $q'((x, y)) = q((x, y)M)$ avec $M \in \mathrm{SL}_2(\mathbf{Z})$. Alors $Q/\simeq$ s'identifie à $\mathcal{C}\ell(\mathbf{Q}(\sqrt{-23}))$ par $ax^2 + bxy + cy^2 = a(x - \tau y)(x - \bar{\tau} y) \mapsto$ la classe de $I = \mathbf{Z} + \mathbf{Z}\tau$. Un système de représentants de $Q/\simeq$ est formé de $x^2 + xy + 6y^2$, $2x^2 + xy + 3y^2$ et $2x^2 - xy + y^2$.

Rappelons qu'on a

$$L(\rho, s) = \frac{1}{23^{-s}} \prod_{p, N_p=1} \frac{1}{1 - p^{-2s}} \prod_{p, N_p=0} \frac{1}{1 + p^{-s} + p^{-2s}} \prod_{p, N_p=3} \frac{1}{1 - 2p^{-s} + p^{-2s}}.$$

Posons alors

$$L(\rho, s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

avec, pour p premier $\neq 23$, $a_p = 0$ si $N_p = 1$, $a_p = 1$ si $N_p = 0$, $a_p = -2$ si $N_p = 3$. Ainsi, si p est premier, a_p est le p-ème coefficient de la série

$$\frac{1}{2}\Big(\sum_{m,n\in\mathbf{Z}} q^{m^2+nm+6n^2} - \sum_{m,n\in\mathbf{Z}} q^{2m^2+nm+3n^2}\Big).$$

Cette formule pour a_p est vraie si p n'est pas seulement un nombre premier mais tout entier ≥ 1.

On a par ailleurs la constatation numérique (voir ci-dessous)

$$\sum_{n=1}^{\infty} a_n q^n = q \prod_{m=1}^{\infty} (1 - q^m)(1 - q^{23m}) = \eta(z)\eta(23z),$$

où $q = e^{2i\pi z}$ et $\eta(z) = q^{1/24} \prod_{m=1}^{\infty}(1 - q^m)$.

On a $\eta(z)^{24} = q \prod_{m=1}^{\infty}(1 - q^m)^{24}$, qui est une forme modulaire de poids 12, notée Δ et auquel le nom de Ramanujan est souvent associé.

Donc η est une forme modulaire de poids 1/2 (à une racine 12-ème près). De même $z \mapsto \eta(23z)$ est une forme modulaire de poids 1/2 pour le groupe de congruence $\Gamma_1(23)$ (à une racine 12-ème près).

Donc $z \mapsto \eta(z)\eta(23z) \sum_{n=1}^{\infty} a_n q^n$ est une forme modulaire de poids 1 pour le groupe $\Gamma_1(23)$.

Ce lien entre motifs d'Artin et formes modulaires n'est pas un accident numérique mais l'illustration d'un phénomène général.

Remarque . — La démonstration de la constatation numérique suit le schéma suivant. Il faut savoir qu'à un scalaire près il n'y a qu'une seule forme modulaire parabolique de poids 1 pour $\Gamma_1(23)$, ce qui n'est pas évident. On peut montrer que les deux membres de la constatation numériques sont de telles formes modulaires. Comme leurs coefficients de degré 1 sont égaux, elles sont égales.