XIV
Motifs d'Artin

1. Représentations de groupes

Soit G un groupe fini. Une *représentation complexe* de G sur un espace vectoriel complexe E est un morphisme de groupes $\rho : G \to \mathrm{GL}(E)$. On parle encore d'une *action linéaire* de G sur E. C'est la même notion que celle d'un $\mathbf{C}[G]$-module à gauche. Ainsi, parfois, ρ est oublié et on note $g.e$ pour $\rho(g)(e)$ (pour $g \in G$ et $e \in E$). Lorsque E est de dimension finie n, on dit que n est la *dimension* ou le *degré* de ρ.

Si ρ_1 et ρ_2 sont deux représentations de G sur E_1 et E_2. Un *morphisme* (resp. *isomorphisme*) de représentations de G est un morphisme (resp. isomorphisme) de $\mathbf{C}[G]$-modules $E_1 \to E_2$. On peut par ailleurs considérer la *somme* $\rho_1 \oplus \rho_2$ de ρ_1 et ρ_2 qui est une représentation sur $E_1 \oplus E_2$ donnée par $(\rho_1 \oplus \rho_2)(g) = \rho_1(g) \oplus \rho_2(g)$. De même, on peut considérer le produit tensoriel $\rho_1 \otimes_{\mathbf{C}} \rho_2$ qui fait opérer G sur $E_1 \otimes_{\mathbf{C}} E_2$.

Lorsque E ne possède pas de sous-espace distinct de $\{0\}$ et E stable par G (*i.e.* par $\rho(G)$), on dit que ρ est *irréductible*. Les représentations irréductibles de G sont en nombre fini à isomorphisme près. Le *caractère* de la représentation est la fonction $G \to \mathbf{C}$ qui à g associe $\mathrm{Tr}(\rho(g))$. (Cette notion contient comme cas particuliers les caractères de G définis comme morphismes de groupes $G \to \{z \in \mathbf{C}/|z| = 1\}$.) Attention au conflit de terminologie : un caractère désigne à la fois une représentation de dimension 1 à valeurs dans les nombres complexes de module 1 et un la trace d'une représentation. Une telle fonction est constante sur les classes de conjugaison de G. On appelle *fonctions centrales* sur G les fonctions $G \to \mathbf{C}$ constantes sur les classes de conjugaison. Un théorème de théorie des groupes affirme que toute fonction centrale sur G est combinaison linéaire complexe de caractères de représentations. Mieux encore cette combinaison linéaire est unique si on se restreint aux caractères de représentations irréductibles. Il en résulte que deux représentations de G ayant mêmes caractères sont isomorphes.

On note ρ^* la *représentation contragrédiente* de ρ. C'est la représentation sur l'espace dual de E qui à g associe l'endomorphisme $\rho^*(g)$ dual de $\rho(g^{-1})$. Son caractère est conjugué du caractère de ρ, puisque les valeurs propres de $\rho(g)$ sont des racines de l'unité, si bien que les valeurs propres de $\rho(g^{-1})$ sont inverses, et donc conjuguées, des valeurs propres de $\rho(g)$. Ainsi, si ρ est de dimension 1, ρ^* est la représentation $\bar{\rho}$, au sens de la conjugaison complexe des caractères de dimension 1.

Une représentation de G est fournie par la *représentation régulière* $\mathbf{C}[G]$ de G. L'élément $g \in G$ opère sur $\mathbf{C}[G]$ par multiplication à gauche par $[g]$ dans l'anneau en groupe $\mathbf{C}[G]$. Plus généralement, si G opère sur un ensemble fini X, on a une représentation de G sur $\mathbf{C}[X]$. Dans ses fondements, la théorie des représentations contient le théorème suivant, qui utilise implicitement que les représentations irréductibles de G sont en nombre fini, à isomorphisme près.

THÉORÈME 1. — *La représentation régulière de G est isomorphe à $\oplus_\tau \tau^{\oplus d_\tau}$, où τ parcourt les représentations complexes irréductibles de G à isomorphisme près, où on a noté d_τ la dimension de τ.*

Lorsque H est sous-groupe d'indice fini de G. Soit τ une représentation continue de H sur un espace vectoriel complexe F. On obtient une représentation de G par *induction de τ de H à G* en posant $E = F \otimes_{\mathbf{C}[H]} \mathbf{C}[G]$ (produit tensoriel de $\mathbf{C}[H]$-modules). En termes concrets, on choisit un système de représentants $(g_s)_{s\in S}$ de $H\backslash G$. On pose $E = F^S$ et on note, pour $s \in S$ et $e \in F$, e_s l'application qui à s associe e et à t associe 0 si $t \neq s$. On munit alors E d'une action linéaire de G par $g.e_s = \tau(h)(e_t)$ où $h \in H$ et $t \in S$ sont uniquement déterminés par l'identité $gs = ht$. On peut encore écrire $E = \oplus_s sF$, muni de l'action $\rho(g).sx = t\tau(h)(x)$ (avec les mêmes notations).

On note $\mathrm{Ind}_H^G(\tau)$ la représentation induite de τ de H à G. On s'intéresse tout particulièrement au cas où τ est de dimension 1, on a alors l'induite est dite *induite d'un caractère*. L'induction commute au passage à la contragrédiente. La représentation induite de la représentation de dimension 1 du sous-groupe trivial de G n'est autre que la représentation régulière de G.

Lorsque G est un quotient de G', une représentation de G' est obtenue en composant ρ avec le morphisme surjectif $G' \to G$. C'est l'*inflation* de G à G'. On la note $\mathrm{Inf}_G^{G'}$.

Puisque G est un groupe fini, son image par ρ est un sous-groupe fini de $\mathrm{GL}(E)$. Supposons E de dimension finie, il existe un corps de nombres F tel que l'image de ρ est contenue dans $\mathrm{GL}(E')$ où E' est un sous-F-espace vectoriel de E.

Toutes ces notions s'adaptent au cas où G est un groupe topologique. Il faut alors supposer que l'action est continue.

2. Représentations galoisiennes complexes d'image finie

Soit K un corps de nombres. Soit $\bar{K}$ une clôture algébrique de K. On s'intéresse aux représentations de dimension finie de $\mathrm{Gal}(\bar{K}/K)$ sur un espace vectoriel complexe, que l'on suppose continues, ce qui revient à dire que leurs images sont finies. On les appelle encore *motifs d'Artin*.

Soit ρ une telle représentation. Il existe $L|K$ une extension galoisienne finie telle que ρ se factorise par $G = \mathrm{Gal}(L/K)$.

Exemple 1. — Les premiers exemples sont fournis par les morphismes de groupes $G \to \mathbf{C}^\times$, qui sont les représentations de dimension 1.

Exemple 2. — Soit $P \in K[X]$. Soit L un corps de décomposition de P sur K. Le groupe $\mathrm{Gal}(L/K)$ opère sur l'ensemble R des racines de P. On a donc une représentation de $\mathrm{Gal}(L/K)$ sur $\mathbf{C}[R]$ par linéarité.

Exemple 3. — On a une version plus fine de l'exemple précédent. Soit T le sous-groupe du groupe des permutations R form par l'action de $\mathrm{Gal}(L/K)$. On obtient une représentation de G_K en combinant le morphisme $G_K \to T$ avec une représentation complexe de T. Considérons par exemple $P = X^3 - 3X + 1$. Le groupe de Galois de son corps de décomposition sur $\mathbf{Q}$ est le groupe symétrique $\mathcal{S}_3$. Ce groupe admet deux représentations

irréductibles de dimension 1 (représentation triviale et signature) et une représentation irréductible de dimension 2, qu'on peut utiliser.

Exemple 4. — Soit $L|K$ une extension Galoisienne. Le groupe G opère sur $\mathcal{O}_L^\times$, qui est un groupe de type fini. On obtient une représentation de G en considérant $\mathcal{O}_L^\times \otimes \mathbf{C}$.

Exemple 5. — Un exemple du même type que le précédent est fourni par le groupe $E(L)$ des points L-rationnels d'une courbe elliptique E sur K. Là encore, on obtient une représentation complexe en considérant $E(L) \otimes \mathbf{C}$.

En général, comme ρ est d'image finie, pour tout $\sigma \in G$, les valeurs propres de $\rho(\sigma)$ sont des racines de l'unité, qui sont *a fortiori* de module 1.

Si l'image (finie) de ρ est à conjugaison près contenue dans $GL_d(R)$, avec R sous-anneau de $\mathbf{C}$, on dit que R est un *anneau de coefficients* de ρ. En particulier le polynôme caractéristique de tout élément de l'image de ρ est à coefficients dans R. En particulier, si ρ est de dimension 1, et donc associée à un caractère χ, l'anneau $\mathbf{Z}[\chi]$ engendré par les valeurs de χ est un anneau de coefficients.

Par l'inflation, toutes les représentations galoisiennes sont des représentations de $\mathrm{Gal}(\bar{K}/K)$ (le groupe de Galois absolu de K) où $\bar{K}$ est une clôture algébrique de K. On doit imposer toutefois une condition de continuité, en munissant $\mathrm{Gal}(\bar{K}/K)$ de la topologie profinie. La topologie des espaces vectoriels sur $\mathbf{C}$ impose que la représentation se factorise par un groupe de Galois fini.

Si on admet des représentations galoisiennes sur des espaces vectoriels sur d'autres corps que $\mathbf{C}$, tel qu'un corps l-adique, on est amené à considérer des représentations qui ne se factorisent pas par des groupes de Galois finis.

3. Fonctions L

Soit ρ une représentation galoisienne complexe de dimension finie comme ci-dessus. Soit v une place finie de K. On dit que ρ est *non ramifiée* en v si $\rho(I_v)$ est trivial, où I_v est un groupe d'inertie en v de $\mathrm{Gal}(L/K)$. Dans ce cas, l'image d'une substitution de Frobenius Frob_v est définie à conjugaison près dans $\mathrm{Gal}(L/K)$, si bien que $\rho(\mathrm{Frob}_v)$ est définie à conjugaison près dans $\mathrm{GL}(E)$. Notez que, comme $\rho(\mathrm{Frob}_v)$ est d'ordre fini, il est diagonalisable. Le polynôme caractéristique de $\rho(\mathrm{Frob}_v)$ ne dépend que de v et pas du choix de Frob_v. Il détermine la classe de conjugaison de $\rho(\mathrm{Frob}_v)$ dans $\mathrm{GL}(E)$ et donc la restriction de ρ à un sous-groupe de décomposition en v, à isomorphisme près.

Lorsque v est éventuellement ramifiée, on peut considérer le sous-espace vectoriel E^{I_v} de E formé par les élément fixes par un sous-groupe d'inertie I_v. Dans ce cas, $\rho(\mathrm{Frob}_v)$ est défini à conjugaison près dans $\mathrm{GL}(E^{I_v})$. Ainsi on pose

$$P_v(X) = \det(1 - X\rho(\mathrm{Frob}_v); E^{I_v}) \in \mathbf{C}[X]$$

(on considère le déterminant de l'opérateur $1 - X\rho(\mathrm{Frob}_v)$ qui opère sur E^{I_v}). Noter le degré de P_v tend à diminuer lorsque I_v grandit. On peut même avoir $E^{I_v} = \{0\}$ et donc $P_v(X) = 1$. Ainsi, le polynôme $P_v(X)$ ne contient pas d'information sur $\rho(I_v)$.

Suivant Artin, on pose le *produit eulérien* :

$$L(\rho, s) = \prod_v \frac{1}{P_v(|\mathcal{P}_v|^{-s})}$$

où v parcourt les places finies de K. C'est la *fonction L d'Artin* de ρ. Il est essentiel de noter que le facteur en la place v ne dépend que de la restriction de ρ à un groupe de décomposition en v. La représentation ne dépend que de la classe d'isomorphie de ρ, et donc que de la fonction centrale définie par la trace de ρ. Puisque toute fonction centrale $G \to \mathbf{C}$ est combinaison linéaire de traces de représentations de la forme $\sum_i \lambda_i \mathrm{Tr}(\rho_i)$, une fonction de cette forme admet comme fonction L le produit $\prod_i L(\rho_i, s)^{\lambda_i}$, au moins lorsque $\lambda_i \in \mathbf{Z}$ pour tout i. On peut définir une fonction L d'Artin pour toute telle fonction centrale sur G, en particulier pour les caractères des représentations.

Lorsque ρ est de dimension 1, elle se factorise par une le groupe de Galois G d'une extension L/K abélienne. C'est ainsi un caractère de G. Ainsi on peut invoquer la théorie du corps de classe pour identifier G à un quotient d'un groupe de classe de rayon (ou à un groupe de classe d'idèle). Il existe un caractère de Hecke $\chi : \mathbf{A}_K^\times / K^\times$ d'image finie tel que, pour tout idéal premier $\mathcal{P}$ de $\mathcal{O}_K$ non ramifié dans $L|K$, on a $\rho(\mathrm{Frob}_\mathcal{P}) = \chi(\pi_\mathcal{P})$ où $\pi_\mathcal{P}$ est un l'idèle dont toutes les composantes sont 1, sauf celle en la place $\mathcal{P}$, où on a une uniformisante de $\mathcal{P}$. On a ainsi

$$L(\rho, s) = L(\chi, s)$$

(les facteurs en les places ramifiées valent 1). Ainsi on retrouve les fonctions L de Hecke d'image finie. En particulier, lorsque ρ est la représentation triviale de dimension 1, on retrouve la fonction ζ_K de Dedekind de K.

Un autre cas particulier réside dans le cas où l'extension L/K est l'extension cyclotomique $\mathbf{Q}(\mu_n)/\mathbf{Q}$ engendrée par une racine primitive n-ème de l'unité. On identifie le groupe de Galois de l'extension à $(\mathbf{Z}/n\mathbf{Z})^\times$. Ainsi, ρ s'identifie à un caractère de Dirichlet χ, puisque l'image de la substitution de Frobenius en p est la classe de p modulo n. Ainsi on retrouve une fonction L de Dirichlet.

4. Un exemple

Considérons le polynôme $T^3 - T - 1$, qui est irréductible sur $\mathbf{Q}$. Soit L un corps de décomposition de ce polynôme. Le groupe de Galois de $L|K$ est isomorphe au groupe symétrique S_3, lequel opère sur les sommet d'un triangle équilatéral centré en l'origine du plan. On a donc une représentation $\rho : \mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$. Plus précisément, un corps de coefficients de ρ est l'anneau $\mathbf{Z}[e^{2i\pi/3}]$. Le polynôme caractéristique de l'identité est $(X-1)^2$. Le polynôme caractéristique de l'image par ρ d'une transposition de S_3 est $X^2 - 1$. Le polynôme caractéristique de l'image par ρ d'un cycle d'ordre 3 est $X^2 + X + 1$.

Le polynôme $T^3 - T - 1$ a pour discriminant -23, si bien qu'on a une extension intermédiaire $\mathbf{Q}(\sqrt{-23})$ contenue dans L. L'extension $L|\mathbf{Q}$ est non ramifiée en dehors de 23.

Débutons notre étude locale en 23. Notons I_{23} un sous-groupe d'inertie en 23 de $\mathrm{Gal}(L/\mathbf{Q})$. Comme l'extension $\mathbf{Q}(\sqrt{-23})|\mathbf{Q}$ est totalement ramifiée en 23, et que

l'extension $L|\mathbf{Q}(\sqrt{-23})$ est non ramifiée en l'unique idéal au dessus de 23, le groupe $\rho(I_{23})$ est d'ordre pair mais I_{23} n'est pas égal à G. Donc le groupe $\rho(I_{23})$ est d'ordre 2, et a pour éléments l'identité et une symétrie par rapport à une droite. La dimension de l'espace $I^{\rho(I_{23})}$ des invariants de $\mathbf{C}^2$ sous I_{23} est donc égal à 1.

Examinons maintenant les autres places. Soit q un nombre premier distinct de 23. Soit Frob_q une substitution de Frobenius dans $\mathrm{Gal}(L/K)$. Notons $P_q(X)$ le polynôme caractéristique de $\rho(\mathrm{Frob}_q)$. On est dans l'un des cas suivants :

Un 3-cycle de S_3 si et seulement si le polynôme $T^3 - T - 1$ est sans racine sur le corps fini $\mathbf{F}_q$. Notons T_3 l'ensemble des nombres premiers q de ce type. On a alors

$$P_q(X) = X^2 + X + 1.$$

Une transposition de S_3 si et seulement si le polynôme $T^3 - T - 1$ a une unique racine dans le corps fini $\mathbf{F}_q$. Notons T_2 l'ensemble des nombres premiers q de ce type. On a alors

$$P_q(X) = X^2 - 1.$$

L'identité de S_3 si et seulement si le polynôme $T^3 - T - 1$ est scindé sur le corps fini $\mathbf{F}_q$. Notons T_1 l'ensemble des nombres premiers q de ce type. On a alors

$$P_q(X) = (X - 1)^2.$$

Finalement, la fonction L de ρ est donnée par

$$L(\rho, s) = \frac{1}{1 - 23^{-s}} \prod_{q \in T_1} \frac{1}{1 - 2q^{-s} + q^{-2s}} \prod_{q \in T_2} \frac{1}{1 - q^{-2s}} \prod_{q \in T_3} \frac{1}{1 + q^{-s} + q^{-2s}}.$$

5. Quelques propriétés élémentaires

La fonction L d'une représentation galoisienne pour l'extension $L|K$ est invariante par inflation, c'est-à-dire qu'elle ne change pas si on remplace L par un corps plus grand. Voyons ce qu'est la fonction L d'une somme de représentations.

Proposition 1. — *Soient ρ_1 et ρ_2 des représentations galoisiennes complexes. On a*

$$L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s) L(\rho_2, s).$$

Démonstration. — On démontre cela facteur par facteur. L'identité repose entièrement sur le fait que le polynôme caractéristique d'une somme directe d'endomorphismes est le produit des polynômes caractéristiques de ces endomorphismes.

Observer qu'on ne peut pas donner de formule simple pour $L(\rho_1 \otimes \rho_2, s)$ en terme des fonctions L de ρ_1 et ρ_2.

Proposition 2. — *Soit $L|K$ une extension galoisienne finie de groupe de Galois G. Notons ρ_R la représentation régulière de G. On a*

$$\zeta_L(s) = L(\rho_R, s).$$

Démonstration. — Cette identité se vérifie facteur par facteur. Nous allons la montrer seulement pour les facteur non ramifié dans $L|K$ (voir proposition 3 pour se ramener au cas non ramifié). Soit $\mathcal{Q}$ un idéal premier de K non ramifié dans L. Considérons le facteur suivant de ζ_L : $\prod_{\mathcal{P}|\mathcal{Q}} \frac{1}{1-|\mathcal{P}|^{-s}}$ où $\mathcal{P}$ parcourt les idéaux premier de L au dessus de $\mathcal{Q}$. Il y a $g_{\mathcal{Q}}$ tels idéaux $\mathcal{P}$. On a $|G| = g_{\mathcal{Q}} f_{\mathcal{Q}}$, où $f_{\mathcal{Q}}$ est le degré résiduel, puisque $\mathcal{Q}$ est non ramifié. Ainsi, on obtient

$$\prod_{\mathcal{P}|\mathcal{Q}} \frac{1}{1-|\mathcal{P}|^{-s}} = (\frac{1}{1-|\mathcal{Q}|^{-s}})^{g_{\mathcal{Q}}}.$$

Par ailleurs, pour R représentation régulière de G, et $g \in G$ d'ordre f, le polynôme caractéristique de $R(g)$ est $(X^f - 1)^{|G|/f}$. Ainsi, le polynôme caractéristique de $\mathrm{Frob}_{\mathcal{P}}$ est $(X^{f_{\mathcal{Q}}} - 1)^{g_{\mathcal{Q}}}$. On obtient ainsi l'identité

$$\prod_{\mathcal{P}|\mathcal{Q}} \frac{1}{1-|\mathcal{P}|^{-s}} = \frac{1}{P_{\mathcal{Q}}(|\mathcal{Q}|^{-s})},$$

où $P_{\mathcal{Q}}(X) = (1 - X^{f_{\mathcal{Q}}})^{g_{\mathcal{Q}}}$. C'est précisément ce que nous voulions démontrer.

Corollaire . — *Soit $L|K$ une extension galoisienne finie de groupe de Galois G. On a*

$$\zeta_L(s) = \zeta_K(s) \prod_{\rho} L(\rho, s)^{d_\rho},$$

où ρ parcourt, à isomorphisme près, les représentations irréductibles, distinctes de 1*, de G, et où d_ρ est la dimension de ρ.*
Démonstration. — Il résulte du théorème 1 que la représentation régulière de G a pour fonction L :

$$\prod_{\rho} L(\rho, s)^{d_\rho}$$

où ρ parcourt, à isomorphisme près, toutes les représentations irréductibles de G. C'est le membre de droite dans l'énoncé du corollaire, puisque la représention irréductible triviale est de degré 1.

Le corollaire suggère une relation entre les zéros de ζ_K et ceux de ζ_L.

Conjecture (Dedekind). — Si $L|K$ est une extension finie quelconque, la fonction $x \mapsto \zeta_L(s)/\zeta_K(s)$ est entière.

Cette conjecture est démontrée si $L|K$ est Galoisienne. Cela suggère que les facteurs $L(\rho, s)$ admettent un prolongement méromorphe, voire holomorphe à $\mathbf{C}$. C'est l'objet de la conjecture d'Artin.

6. Facteurs d'Euler en les places infinies

Soient $L|K$ une extension galoisienne finie de groupe de Galois G. Soit ρ un motif d'Artin $\mathrm{Gal}(L/K) \to \mathrm{GL}_V$, avec V de dimension n.

Dans notre définition de $L(\rho, s)$, il manque à ce produit eulérien des facteurs correspondant aux places ramifiées et aux places infinies.

On peut étudier les places infinies comme suit. Rappelons les fonctions

$$\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\Gamma(s/2)$$

et

$$\Gamma_{\mathbf{C}}(s) = 2(2\pi)^{-s}\Gamma(s).$$

Soit $v \in \Omega_{K,\infty}$. Soit $w \in \Omega_{L,\infty}$ au dessus de v. Le groupe $\mathrm{Gal}(L_w/K_v)$ est trivial ou d'ordre 2. Dans ce dernier cas, v est réelle, et l'élément d'ordre deux, s'il existe, est la *conjugaison complexe* en w. Il ne dépend que de v à conjugaison près. On pose

$$n_v^+ = \dim(V^{\mathrm{Gal}(L_w/K_v)})$$

et

$$n_v^- = n - n_v^+.$$

Si v est une place réelle, on pose

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

Si v est une place complexe non réelle, on pose

$$L_v(\rho, s) = \Gamma_{\mathbf{C}}(s)^n.$$

On pose alors

$$\Lambda^{\mathrm{nr}}(\rho, s) = \prod_{v \in \Omega_K} L_v(\rho, s).$$

On vérifie facilement que la proposition 2 est encore valable si on remplace $L(\rho, s)$ par $\Lambda^{\mathrm{nr}}(\rho, s)$. Il reste à ajouter des facteurs tenant compte plus pleinement des places ramifiées dans L.