XVII
Motifs d'Artin de dimension 2

1. Déterminant et parité

Soit K un corps de nombres. Soit $\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbf{C})$ une représentation. Le *déterminant* $\det(\rho)$ de ρ est alors un caractère

$$\mathrm{Gal}(\bar{K}/K) \to \mathbf{C}^\times.$$

C'est une représentation de dimension 1, qui est donc décrite par la théorie du corps de classe.

Soit v une place finie de K telle que l'image par ρ d'un sous-groupe d'inertie en v est triviale. Le facteur d'Euler en v de $L(\rho, s)$ est alors

$$L_v(\rho, s) = \frac{1}{1 - \mathrm{Tr}(\rho(\mathrm{Frob}_v))|\mathcal{P}_v|^{-s} + \det(\rho(\mathrm{Frob}_v))|\mathcal{P}_v|^{-2s}},$$

où Tr est la trace.

Soit v une place réelle de K. Soit $c_v \in \mathrm{Gal}(\bar{K}/K)$ une conjugaison complexe (bien définie à conjugaison près). Comme $\rho(c_v)$ est une involution, ses valeurs propres sont 1 ou -1. On dit que ρ est *impaire* en v si $\det(\rho)(c_v) = -1$, et qu'elle est *paire* en v sinon. Si $K = \mathbf{Q}$, il n'y a qu'une seule place à l'infini, si bien qu'il n'est pas nécessaire de la mentionner.

2. Représentations de dimension 2 réductibles

Soit $\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbf{C})$ une représentation galoisienne réductible. Comme toute représentation complexe d'un groupe fini est semi-simple, il existe deux caractères χ_1, χ_2 de $\mathrm{Gal}(\bar{K}/K)$ tel que ρ soit isomorphe à $\chi_1 \oplus \chi_2$. Il existe deux caractères du groupe des classes d'idèles $\mathbf{A}_K^\times/K^\times$ correspondant à χ_1 et χ_2. On a alors

$$\Lambda(\rho, s) = \Lambda(\chi_1, s)\Lambda(\chi_2, s).$$

Le conducteur N_ρ de ρ est égal au produit des conducteurs de χ_1 et χ_2. Pour toute place réelle v de K, on a $n_v^+(\rho) = n_v^+(\chi_1) + n_v^+(\chi_2)$. L'équation fonctionnelle de $\Lambda(\rho, .)$ se réduit au produit des équations fonctionnelles de $\Lambda(\chi_1, .)$ et $\Lambda(\chi_2, .)$.

Si $K = \mathbf{Q}$, χ_1 et χ_2 sont associés à des caractères de Dirichlet, encore noté χ_1 et χ_2 par abus de notations, si bien que $L(\rho, s)$ est un produit de fonctions L de Dirichlet. On a alors en développant le produit eulérien

$$L(\chi_1 \oplus \chi_2, s) = \sum_{n \geq 1} \frac{\sum_{d|n} \chi_1(d)\chi_2(n/d)}{n^s}.$$

3. Sous-groupes finis de $\mathrm{GL}_2(\mathbf{C})$

Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbf{C})$. Notons PG son image dans $\mathrm{PGL}_2(\mathbf{C}) = \mathrm{GL}_2(\mathbf{C})/Z$, où Z est le centre de $\mathrm{GL}_2(\mathbf{C})$ formé par les homothéties.

Théorème 1. — *Le groupe PG est de l'un des types suivants :*

(1) cyclique,

(2) isomorphe à un groupe diédral (cas diédral*),*

(3) isomorphe au groupe alterné A_4 (cas tétraédral*),*

(4) isomorphe au groupe symétrique S_4 (cas octaédral*),*

(5i) isomorphe au groupe alterné A_5 (cas icosaédral.*)*

Démonstration. — Notons que les groupes $\mathrm{PGL}_2(\mathbf{C})$ et $\mathrm{PSL}_2(\mathbf{C})$ sont isomorphes.

L'espace vectoriel $\mathbf{C}^2$ est muni d'un produit hermitien canonique $[.,.]$. Notons $\mathrm{SU}(2)$ le sous-groupe de $\mathrm{GL}_2(\mathbf{C})$ préservant ce produit hermitien. On a

$$\mathrm{SU}(2) = \{\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{C}) |\, |a|^2 + |b|^2 = 1\}.$$

Posons

$$V = \{\begin{pmatrix} x & \bar{y} \\ y & -x \end{pmatrix} \in \mathrm{M}_2(\mathbf{C}) | (x, y) \in \mathbf{R} \times \mathbf{C}\}.$$

C'est un espace euclidien pour la norme $h = \begin{pmatrix} x & \bar{y} \\ y & -x \end{pmatrix} \mapsto -\det(h) = x^2 + |y|^2$. On a alors un morphisme de groupes $\tau : \mathrm{SU}(2) \simeq \mathrm{SO}(V)$ donné par $g \mapsto (h \mapsto ghg^{-1})$. En effet l'application $(h \mapsto ghg^{-1})$ préserve la norme de V, puisque c'est un déterminant.

Lemme 1. — *Le morphisme de groupes τ est surjectif de noyau* $\{\pm I_2\}$.

Démonstration. — En effet, pour $t \in \mathbf{R}$, l'image de $\begin{pmatrix} e^{-it/2} & 0 \\ 0 & e^{it/2} \end{pmatrix} \in \mathrm{SU}(2)$ est, en identifiant V à $\mathbf{R} \times \mathbf{C}$, donnée par $(x, y) \mapsto (x, e^{it}y)$, qui est une rotation d'angle t et d'axe $\mathbf{R}(1, 0)$. Après conjugaison par $g \in SU(2)$, qui agit transitivement sur les droites de $\mathbf{C}^2$, on en déduit que toutes les rotations sont dans l'image τ.

Par ailleurs, le noyau de τ est le normalisateur de $\mathrm{SO}(V)$ dans $\mathrm{SU}(2)$. Soit $g \in \mathrm{Ker}(\tau)$. Alors g laisse fixe tout axe de rotation et donc toute droite de V. C'est donc une homothétie. On a donc $g \in \{\pm I_2\}$. Cela prouve le lemme.

Revenons à la démonstration du théorème. On a donc montré que les groupes $\mathrm{SU}(2)/\pm 1$ et $\mathrm{SO}(V)$ sont isomorphes. Munissons $\mathbf{C}^2$ du produit hermitien

$$(u, v) \mapsto [u, v]_G = \frac{1}{|\tilde{G}|} \sum_{g \in \tilde{G}} [gu, gv],$$

où $\tilde{G} = G \cap \mathrm{SL}_2(\mathbf{C})$. On vérifie qu'il s'agit bien d'un produit hermitien. Alors $\tilde{G}$ est formé de matrices spéciales unitaires pour ce produit. Tous les produits hermitiens se déduisent les uns des autres par action d'une matrice de $\mathrm{GL}_2(\mathbf{C})$: il existe $g_0 \in \mathrm{GL}_2(\mathbf{C})$ tel que pour tout $(u,v) \in \mathbf{C}^2$, on ait

$$[u,v]_G = [g_0u, g_0v].$$

Cela prouve qu'on a $\tilde{G} \subset g_0\mathrm{SU}(2)g_0^{-1}$. On s'est ramené à rechercher les sous-groupes finis de $\mathrm{SO}_3(\mathbf{R})$ puisqu'on a $PG \subset g_0\mathrm{SU}(2)g_0^{-1}/\pm 1 \simeq \mathrm{SU}(2)/\pm 1 \simeq \mathrm{SO}(V)$. On a montré que PG agit sur $\mathbf{S}^2$ la sphère unité de $\mathbf{R}^3$. Comme les images des éléments de PG sont de déterminant 1 dans $\mathrm{SO}(V)$, il agissent comme des rotations ou comme l'identité. En dehors du cas de l'identité, leurs points fixes sont situés sur l'axe de rotation.

Considérons l'ensemble de tous les points fixes sur la sphère $\mathbf{S}^2$. Posons $X = \cup_{g\in PG, g\notin\{\pm 1\}}(\mathbf{S}^2)^g$. Cet ensemble est constitué de paires de points antipodaux : les intersections des axes de rotation avec $\mathbf{S}^2$. L'ensemble X est fini puisque c'est la réunion finie d'ensembles X^g qui ont chacun deux éléments.

Lemme 2. — *On a*

$$2 - \frac{2}{|PG|} = \sum_{\omega\in PG\backslash X} (1 - \frac{|\omega|}{|PG|}).$$

Démonstration. — Par la formule de Burnside pour les points fixe d'un groupe agissant sur un ensemble, on a

$$\sum_{g\in PG} |X^g| = |\{(g,x) \in PG \times X | gx = x\}| = \sum_{x\in X} |\{g \in PG | gx = x\}| = \sum_{x\in X} \frac{|PG|}{|PG.x|}.$$

Cette dernière quantité est $|PG|$ multipliée par le nombre d'orbites. On en déduit

$$|PG\backslash X| = \frac{1}{|PG|} \sum_{g\in PG} |X^g|.$$

Séparons le cas où $g = 1$, on obtient

$$|PG\backslash X| = \frac{1}{|PG|}(|X^1| + \sum_{g\in PG, g\neq 1} |X^g|) = \frac{1}{|PG|}(|X| + 2(|PG| - 1)).$$

Comme on a $|X| = \sum_{\omega\in PG\backslash X} |\omega|$ et $|PG\backslash X| = \sum_{\omega\in PG\backslash X} |1|$, on a

$$2(1 - \frac{1}{|PG|}) = \sum_{\omega\in PG\backslash X} (1 - \frac{|\omega|}{|PG|}).$$

Cela prouve le lemme.

Revenons au théorème. On a donc $|PG\backslash X| = 2$ ou 3 puisqu'on a les inégalités

$$2 > 2(1 - \frac{1}{|PG|}) = \sum_{\omega\in PG\backslash X} (1 - \frac{|\omega|}{|PG|}) \geq |PG\backslash X| \times 1/2.$$

Lemme 3. — *Si $|PG\backslash X| = 2$, le groupe PG est cyclique.*
Démonstration. — Posons $PG\backslash X = \{\omega_1, \omega_2\}$. On a

$$2(1 - \frac{1}{|PG|}) = 1 - \frac{|\omega_1|}{|PG|} + 1 - \frac{|\omega_2|}{|PG|},$$

et donc $|\omega_1| + |\omega_2| = 2$. On a alors $|\omega_1| = |\omega_2| = 1$. Donc PG est formé de rotations d'axe NS, avec N et S points antipodaux, $\omega_1 = \{N\}$, $\omega_2 = \{S\}$. Un groupe de rotations qui fixent un axe est cyclique. Cela prouve le lemme.

Revenons au théorème. Il reste étudier le cas $|PG\backslash X| = 3$. Posons $X = \alpha \cup \beta \cup \gamma$ (union disjointe d'orbites sous PG) et $a = |PG|/|\alpha|$, $b = |PG|/|\beta|$ et $c = |PG|/|\gamma|$. Ce sont des nombres entiers ≥ 1 qui vérifient :

$$2(1 - \frac{1}{|PG|}) = 1 - \frac{1}{a} + 1 - \frac{1}{b} + 1 - \frac{1}{c}$$

et donc

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1 + \frac{2}{|PG|}.$$

Si $a = 1$, on a $\frac{1}{b} + \frac{1}{c} = \frac{2}{|PG|}$ et donc $|\gamma| + |\beta| = 2$. On trouve alors $|\gamma| = |\beta| = 1$ et PG est cyclique comme ci-dessus. En effet, γ et β sont des singletons de points antipodaux de $\mathbf{S}^2$ et

Supposons maintenant que $a > 1$, $b > 1$ et $c > 1$.

Lemme 4. — *Supposons $|PG\backslash X| = 3$ et $|c| \geq |b| \geq |a| > 1$. On est alors dans l'une des situations suivantes :*
(2) $(a, b, c) = (2, 2, c)$ *avec* $|PG| = 2c$
(3) $(a, b, c) = (2, 3, 3)$ *avec* $|PG| = 12$
(4) $(a, b, c) = (2, 3, 4)$ *avec* $|PG| = 24$
(5) $(a, b, c) = (2, 3, 5)$ *avec* $|PG| = 60$.
Démonstration. — On considère l'équation

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1 + \frac{2}{|PG|}.$$

Si $a \geq 3$, on a $1/a + 1/b + 1/c \leq 3 \times 1/3 = 1$. C'est absurde, donc on a $a = 2$.

Si $b \geq 4$, on a $1/a + 1/b + 1/c \leq 1/2 + 1/4 + 1/4 = 1$. C'est absurde, donc on a $b \leq 3$.

Si $a = 2$ et $b = 3$, on a $1/a + 1/b + 1/c \leq 1/2 + 1/3 + 1/c$ et donc $c \leq 5$.

On retrouve les cas annoncés. Cela prouve le lemme.

Revenons au théorème. Tous les cas annoncés dans le lemme se produisent.

Le cas $(2, 2, c)$ est celui des isométries d'un polygone régulier à c sommets situés sur l'équateur de $\mathbf{S}^2$.

Le cas $(2, 2, 3)$ est celui des isométries d'un tétraèdre régulier inscrit dans $\mathbf{S}^2$.

Le cas $(2, 3, 3)$ est celui des isométries d'un octaèdre régulier inscrit dans $\mathbf{S}^2$.

Le cas $(2,3,5)$ est celui des isométries d'un icosaèdre régulier inscrit dans $\mathbf{S}^2$.

Il reste à voir pourquoi dans le type (a,b,c), γ est l'ensemble des sommets d'un polyèdre régulier, β est l'ensemble des centres des faces, α est l'ensemble des milieux des arêtes.

Les divers isomorphismes avec le groupe diédral D_c, le groupe alterné A_4, le groupe symétrique S_4 et le groupe alterné A_5 sont classiques. Cela achève de prouver le théorème.

Remarque 1. — 1) Parmi ces groupes, seul le cas icosaédral donne lieu au cas d'un groupe G non résoluble.

2) On peut envisager de trouver des extensions galoisiennes ayant pour groupe de Galois le groupe trouvé.

3) Si PG est cyclique, le groupe G est abélien. Alors $\mathbf{C}^2$ est un G-module réductible.

4) Si PG n'est pas cyclique, G n'est pas abélien et $\mathbf{C}^2$ est un G-module irréductible.

5) Le premier cas à étudier est le cas diédral. Soit G tel que PG est isomorphe au groupe diédral D_n. Alors G admet un sous-groupe d'indice 2 dont l'image dans PG est $C_n \subset D_n$ cyclique d'ordre n.

4. Induites de caractères

Soit K un corps de nombres. Soit $\bar{K}$ une clôture algébrique de K. Soit L une extension quadratique de K contenue dans $\bar{K}$, qui est une clôture algébrique de K.

Soit $\chi : \mathrm{Gal}(\bar{K}/L) \to \mathbf{C}^\times$ un caractère d'ordre fini. Alors on pose

$$\rho = \mathrm{Ind}_{\mathrm{Gal}(\bar{K}/L)}^{\mathrm{Gal}(\bar{K}/K)} \chi = \mathrm{Ind}_{L/K} \chi.$$

Rappelons qu'on a

$$\Lambda(\rho, s) = \Lambda(\chi, s).$$

Soit σ l'élément non trivial de $\mathrm{Gal}(L/K)$. Soit $\tilde{\sigma}$ un prolongement à $\mathrm{Gal}(\bar{K}/K)$. Alors χ admet un *caractère conjugué* $\chi_\sigma : \mathrm{Gal}(\bar{K}/L) \to \mathbf{C}^\times$ donné par

$$\chi_\sigma(\tau) = \chi(\tilde{\sigma}\tau\tilde{\sigma}^{-1})$$

qui est bien défini car $\mathrm{Gal}(\bar{K}/L)$ est d'indice 2 dans $\mathrm{Gal}(\bar{K}/K)$ et donc normal.

Lemme 5. — *Le caractère χ_σ est indépendant du choix de $\tilde{\sigma}$.*
Démonstration. — Soit $\tilde{\sigma}'$ un prolongement de σ à $\mathrm{Gal}(\bar{K}/K)$. On a

$$\chi(\tilde{\sigma}\tau\tilde{\sigma}^{-1})/\chi(\tilde{\sigma}'\tau\tilde{\sigma}'^{-1}) = \chi(\tilde{\sigma}\tau\tilde{\sigma}^{-1}\tilde{\sigma}'\tau^{-1}\tilde{\sigma}'^{-1}).$$

On écrit

$$\tilde{\sigma}\tau\tilde{\sigma}^{-1}\tilde{\sigma}'\tau^{-1}\tilde{\sigma}'^{-1} = (\tilde{\sigma}\tau\tilde{\sigma}^{-1})(\tilde{\sigma}'\tilde{\sigma}^{-1})(\tilde{\sigma}\tau^{-1}\tilde{\sigma}^{-1})(\tilde{\sigma}\tilde{\sigma}'^{-1})$$

où les quatre facteurs entre parenthèses sont dans $\mathrm{Gal}(\bar{K}/L)$, et sont deux paires d'inverses, si bien que le produit de leurs images par χ vaut 1. Cela prouve le lemme.

Soit G un groupe. Soit H un sous-groupe. Rappelons que l'induite ρ de H à G d'un caractère χ d'un sous-groupe H d'un groupe G peut être décrite ainsi. Soit $(g_s)_{s\in S}$ un système de représentants de G/H. Considérons l'espace vectoriel de base $(g_s)_{s\in S}$. Soit $\tau \in G$. Posons $\rho(\tau)g_s = \chi(g_r^{-1}\tau g_s)g_r$, avec $r \in S$ uniquement déterminé tel que $g_r^{-1}\tau g_s \in H$. On peut vérifier qu'il s'agit d'une représentation, *i.e.* que $\rho(\tau\tau') = \rho(\tau)\rho(\tau')$. En effet, on a pour tout $s \in S$ et $r, t \in S$ appropriés : $\rho(\tau\tau')g_s = \chi(g_r^{-1}\tau\tau' g_s)g_r = \chi(g_r^{-1}\tau g_t g_t^{-1}\tau' g_s)g_r = \chi(g_r^{-1}\tau g_t)\chi(g_t^{-1}\tau' g_s)g_r = \chi(g_t^{-1}\tau' g_s)\rho(\tau)g_t = \rho(\tau)\chi(g_t^{-1}\tau' g_s)g_t = \rho(\tau)\rho(\tau')g_s$.

Soit $S = \{1, \tilde{\sigma}\}$ un système de représentants de $\mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$. On peut noter 1, $\tilde{\sigma}$ la base de la représentation induite.

Soit E le $\mathbf{C}$-espace vectoriel de base $(1, \tilde{\sigma})$. Soit $\tau \in \mathrm{Gal}(\bar{K}/K)$.

Si $\tau \in \mathrm{Gal}(\bar{K}/L)$, on a $\rho(\tau)1 = \chi(\tau)1$, $\rho(\tau)\tilde{\sigma} = \chi(\tilde{\sigma}^{-1}\tau\tilde{\sigma})\tilde{\sigma}$. On a donc

$$\rho(\tau) = \begin{pmatrix} \chi(\tau) & 0 \\ 0 & \chi_\sigma(\tau) \end{pmatrix}.$$

Si $\tau \notin \mathrm{Gal}(\bar{K}/L)$, on a $\tau = \tilde{\sigma}(\tilde{\sigma}^{-1}\tau)$ avec $(\tilde{\sigma}^{-1}\tau) \in \mathrm{Gal}(\bar{K}/L)$. On a $\rho(\tau)1 = \chi(\tilde{\sigma}^{-1}\tau)\tilde{\sigma}$ et $\rho(\tau).\tilde{\sigma} = \chi(\tau\tilde{\sigma})1$. On a donc

$$\rho(\tau) = \begin{pmatrix} 0 & \chi(\tau\tilde{\sigma}) \\ \chi(\tilde{\sigma}^{-1}\tau) & 0 \end{pmatrix}.$$

Proposition 2. — *Les assertions suivantes sont équivalentes.*

(i) ρ est irréductible.

(ii) ρ est diédrale.

(iii) On a $\chi \neq \chi_\sigma$.

Démonstration. — On a vu que ρ est réductible si et seulement si $P\mathrm{Im}(\rho)$ est cyclique. Alors $\mathrm{Im}(\rho)$ est cyclique ou diédrale. Les deux premières conditions sont donc équivalentes.

La représentation est irréductible si et seulement si ρ est produit d'une homothétie et d'une symétrie. Il faut pour cela que $\chi(\tilde{\sigma}^{-1}\tau) = \chi(\tau\tilde{\sigma})$, c'est-à-dire $\chi = \chi_\sigma$. Cela prouve la proposition.

Notons $N\chi$ le conducteur de χ. Alors le conducteur de ρ est

$$N_\rho = \mathcal{D}_L N_{L/K}(N_\chi).$$

Soit v une place réelle de K. Soit $c_v \in \mathrm{Gal}(\bar{K}/K)$ une conjugaison complexe correspondante (bien définie à conjugaison près). S'il y a une seule place w de L au dessus de v, on a $L_w = \mathbf{C}$.

Sinon, il y a deux places w et w', qui sont réelles, de L au dessus de v. Notons f_w et $f_{w'}$ des conjugaisons complexes correspondantes de $\mathrm{Gal}(\bar{K}/L$.

Proposition 3. — *La représentation induite ρ est impaire en v si et seulement si l'une des conditions suivantes est vérifiée :*

(i) Il y a une place complexe w de L au dessus de v.

(ii) Il y a deux places w et w', qui sont réelles, de L au dessus de v, et on a $\chi(f_w)\chi(f_{w'}) = -1$ (on dit que χ est de signature $(-1, 1)$*).*
Démonstration. — Au vu de la description de l'induite donnée ci-dessus, on a, dans le cas (i), on a $c_v \notin \mathrm{Gal}(\bar{K}/L)$ et donc

$$\rho(\tau) = \begin{pmatrix} 0 & \chi(c_v\tilde{\sigma}) \\ \chi(c_v^{-1}\tilde{\sigma}) & 0 \end{pmatrix},$$

qui a pour déterminant -1.

Dans le cas (ii), on a $f_{w'} = \tilde{\sigma} f_w \tilde{\sigma}^{-1}$ et donc

$$\rho(c_v) = \begin{pmatrix} \chi(f_w) & 0 \\ 0 & \chi(f_{w'}) \end{pmatrix},$$

qui a pour déterminant $\chi(f_w)\chi(f_{w'})$, d'où la condition annoncée.

Proposition 4. — *Si l'image de ρ dans* $\mathrm{PGL}_2(\mathbf{C})$ *est le groupe diédral D_n, alors n est l'ordre de $\chi^{-1}\chi_\sigma$.*
Démonstration. — Dans ce cas le sous-groupe cyclique C_n d'ordre n de D_n est l'image de $\rho(\mathrm{Gal}(\bar{K}/L))$ dans $\mathrm{PGL}_2(\mathbf{C})$. Mais dans $\mathrm{PGL}_2(\mathbf{C})$, on a, pour $\tau \in \mathrm{Gal}(\bar{K}/L)$,

$$\rho(\tau) = \begin{pmatrix} \chi(\tau) & 0 \\ 0 & \chi_\sigma(\tau) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & (\chi_\sigma\chi^{-1})(\tau) \end{pmatrix}.$$

Donc n est l'ordre de $\chi^{-1}\chi_\sigma$.

Remarque . — Soit $\epsilon : \mathrm{Gal}(L/K) \to \{\pm 1\}$ le caractère quadratique. Si $\tau \in \mathrm{Gal}(\bar{K}/L)$, on a

$$\det(\rho)(\tau) = (\chi\chi_\sigma)(\tau).$$

Si $\tau \notin \mathrm{Gal}(\bar{K}/L)$, on a

$$\det(\rho)(\tau) = -\chi(\tilde{\sigma}\tau)\chi_\sigma(\tilde{\sigma}\tau).$$

Donc si $\chi_\sigma = \bar{\chi}$, on a $\det(\rho) = \epsilon$. C'est toujours le cas si χ est d'ordre 3, $\chi \neq 1$ et ρ irréductible.