

Werk

Titel: Sommes de Gauss et structure galoisienne des anneaux d'entiers

Autor: QUEYRUT, Jacques

PURL: https://resolver.sub.uni-goettingen.de/purl?320141322_0011 | log15

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

✉ info@digizeitschriften.de

SOMMES DE GAUSS ET
STRUCTURE GALOISIENNE DES ANNEAUX D'ENTRIERS

par

Jacques QUEYRUT

--:--:--

Soient $\mathbb{Z}$ l'anneau des entiers et $\mathbb{Q}$ son corps des fractions. On fixe une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$. Si N est une extension finie de $\mathbb{Q}$ incluse dans $\bar{\mathbb{Q}}$, on note G_N le groupe de Galois de $\bar{\mathbb{Q}}$ sur N et $\mathbb{Z}_N$ l'anneau des entiers de N .

Soit Γ un groupe fini.

On note $\mathcal{S}(\Gamma)$ l'ensemble des extensions finies N de $\mathbb{Q}$ telles que Γ soit isomorphe à un sous-groupe du groupe des $\mathbb{Q}$ -automorphismes de N . Si $N \in \mathcal{S}(\Gamma)$, $\mathbb{Z}_N$ a une structure de $\mathbb{Z}[\Gamma]$ -module de rang r défini.

THÉORÈME I. - Soient N et N' deux extensions finies de $\mathbb{Q}$ incluses dans $\bar{\mathbb{Q}}$. Soit Γ un groupe fini. On suppose que

- 1) N et N' appartiennent à $\mathcal{S}(\Gamma)$
- 2) $\mathbb{Z}_N$ et $\mathbb{Z}_{N'}$ sont des $\mathbb{Z}[\Gamma]$ -modules localement isomorphes.

Alors il existe un $\mathbb{Z}[\Gamma]$ -module X de type fini sans $\mathbb{Z}$ -torsion et un isomorphisme de $\mathbb{Z}[\Gamma]$ -module de $\mathbb{Z}_N \oplus X$ sur $\mathbb{Z}_{N'} \oplus X$.

Ce résultat peut aussi s'exprimer de la façon suivante : soit $G_{\oplus}(\mathbb{Z}[\Gamma])$ le groupe de Grothendieck de la catégorie des $\mathbb{Z}[\Gamma]$ -modules de type fini sans $\mathbb{Z}$ -torsion, modulo les suites exactes scindées (voir [Q1]) ; alors sous les hypothèses du théorème I, $[\mathbb{Z}_N] = [\mathbb{Z}_{N'}]$ dans $G_{\oplus}(\mathbb{Z}[\Gamma])$.

Ce résultat a été conjecturé et démontré dans un cas particulier par S.M.J. Wilson ([W]).

Dans le cas où $\mathbb{Z}_N$ est un $\mathbb{Z}[\Gamma]$ -module projectif (cas modéré), Fröhlich a démontré le résultat plus précis suivant :

THÉORÈME II (Fröhlich [F]). - Soit $N \in \mathcal{S}[\Gamma]$ telle que Γ ne contienne pas d'élément sauvagement ramifié dans N , alors $[\mathbb{Z}_N] = r[\mathbb{Z}[\Gamma]]$ dans $G_{\oplus}(\mathbb{Z}[\Gamma])$.

On est donc amené à étudier la structure locale des anneaux d'entiers et à déterminer le sous-groupe de $G_{\oplus}(\mathbb{Z}[\Gamma])$ engendré par l'ensemble des classes $[\mathbb{Z}_N]$, $N \in \mathcal{S}(\Gamma)$. Et plus précisément, on est conduit à déterminer le genre d'un anneau d'entier.

Cette étude a été faite complètement dans le cas particulier des extensions abéliennes de $\mathbb{Q}$ par Leopoldt qui a démontré le théorème suivant :

THÉORÈME III (Leopoldt [L]). - Soit N une extension abélienne de $\mathbb{Q}$ de groupe de Galois Γ ; $\mathbb{Z}_N$ est isomorphe à l'ordre de $\mathbb{Z}$ dans $\mathbb{Q}[\Gamma]$, noté $\mathcal{O}(\mathbb{Z}_N, \mathbb{Q}[\Gamma])$ est appelé ordre associé de $\mathbb{Z}_N$, défini par $\mathcal{O}(\mathbb{Z}_N, \mathbb{Q}[\Gamma]) = \{\lambda \in \mathbb{Q}[\Gamma], \lambda \mathbb{Z}_N \subset \mathbb{Z}_N\}$. L'ordre associé $\mathcal{O}(\mathbb{Z}_N, \mathbb{Q}[\Gamma])$ est engendré par $\mathbb{Z}[\Gamma]$ et les idempotents associés aux groupes supérieurs de ramifications.

Leopoldt montre de plus qu'une base de $\mathbb{Z}_N$ sur $\mathcal{O}(\mathbb{Z}_N, \mathbb{Q}[\Gamma])$ peut être construite à l'aide des sommes de Gauss associées aux caractères de Γ .

De nombreux contre-exemples dus à A.-M. Bergé, S.M.J. Wilson et J. Cougnard, montrent que le théorème 3 ne se généralise pas sous cette forme aux extensions quelconques de $\mathbb{Q}$ et aux groupes Γ -non abéliens.

1. - Sommes de Gauss galoisiennes

Soit K un corps de nombres. On note $\mathfrak{P}(\mathbb{Z}_K)$ l'ensemble des idéaux premiers de $\mathbb{Z}_K$. L'indication par un élément de $\mathfrak{P}(\mathbb{Z}_K)$ désignera la complétion.

Soit $J(K)$ le groupe des idèles de K ; on plonge K_p^* dans $J(K)$ pour tout $p \in \mathfrak{P}(\mathbb{Z}_K)$ et K^* dans la diagonale de $J(K)$.

La définition des sommes de Gauss galoisiennes fait intervenir la théorie du corps de classes. L'application d'Artin est normalisée de telle sorte que les Frobenius géométriques, que l'on note $F_{K,p}$, correspondent aux uniformisantes. La théorie du corps de classes donne donc un homomorphisme de $J(K)/K^*$ dans G_K^{ab} , le quotient de G_K par l'adhérence de son sous-groupe des commutateurs.

Pour la suite, on fixe un caractère additif non trivial ψ_K du groupe $A(K)/K$ dans $\mathbb{Q}^*$ où $A(K)$ est le groupe des adèles de K . On note $\psi_{K,p}$ sa restriction à K_p : $K_p \longrightarrow A(K)/K \xrightarrow{\psi} \mathbb{Q}^*$.

Soit d_p (ou d) un générateur de l'idéal $p^n \mathbb{Z}_{K,p}$ où n est le plus petit entier tel que : $\psi_{K,p}(p^{-n} \mathbb{Z}_{K,p}) = 1$.

L'idéal $p^n \mathbb{Z}_{K,p}$ est appelé conducteur de $\psi_{K,p}$.

DÉFINITION 1.1. - Soit ρ un caractère de G_K de dimension 1 ; on appelle somme de Gauss abélienne, l'élément $\tau_K^{ab}(\rho)$ de $\mathbb{Q}^*$ défini par

$$\tau_K^{ab}(\rho) = \prod_{p \in \mathfrak{P}(\mathbb{Z}_K)} \tau_{K,p}^{ab}(\rho) \text{ avec :}$$

$$\text{si } p \text{ est une place archimédienne } \tau_{K,p}^{ab}(\rho) = 1$$

$$\text{si } p \text{ est une place non archimédienne}$$

$$\tau_{K,p}^{ab}(\rho) = \sum_{x \in U_{K,p}^{(0)} / U_{K,p}^{(n)}} \rho_p(x/\gamma d_p)^{-1} \psi_{K,p}(x/\gamma d_p)$$

$$\text{où } U_{K,p}^{(0)} = (\mathbb{Z}_{K,p})^*, \quad U_{K,p}^{(n)} = 1 + p^n \mathbb{Z}_{K,p}.$$

$$\rho_p \text{ est la composée des applications } K_p^* \longrightarrow J(K)/K^* \longrightarrow G_K^{ab} \longrightarrow \mathbb{Q}^*.$$

n est égal au produit scalaire de ρ et du caractère d'Artin (c'est la valuation en p du conducteur de ρ).

THÉORÈME 1.2. - Il existe une unique application τ de $\bigcup_{K \subset \bar{\mathbb{Q}}} R(G_K)$ dans $\bar{\mathbb{Q}}^*$, où $R(G_K)$ désigne le groupe des caractères de G_K et où K parcourt l'ensemble des sous-extensions de $\bar{\mathbb{Q}}$ de degré fini sur $\mathbb{Q}$, vérifiant :

- 1) $\tau_K(\rho) = \prod_{p \in P(\mathbb{Z}_K)} \tau_{K,p}(\rho), \quad \forall \rho \in R(G_K), \quad \forall K \subset \bar{\mathbb{Q}},$
- 2) $\tau_{K,p}(\rho) \tau_{K,p}(\rho') = \tau_{K,p}(\rho + \rho'), \quad \forall \rho, \rho' \in R(G_K), \quad \forall K \subset \bar{\mathbb{Q}}, \quad \forall p \in P(\mathbb{Z}_K),$
- 3) si $\rho \in R(G_K)$ est de dimension 1, $\tau_{K,p}(\rho) = \tau_{K,p}^{ab}(\rho)$,
- 4) soit G_F un sous-groupe ouvert d'indice fini de G_K et soit $\rho \in R(G_F)$ de dimension 0, on note $\text{Ind}_F^K(\rho)$ le caractère de G_K induit par ρ ; on a

$$\tau_{K,p}(\text{Ind}_F^K(\rho)) = \prod_{p|p} \tau_{F,p}(\rho).$$

Démonstration. - Voir [D] ou [Ta].

PROPRIÉTÉS 1.3. - 1) Soit ψ_K un caractère additif non trivial de $A(K)/K$; il existe $a \in K^*$ tel que $\psi'_K(ax) = \psi_K(x)$, alors

$$\tau_{K,p}(\rho, \psi'_K) = (\det_\rho)_p(a) \tau_{K,p}(\rho, \psi_K).$$

Et par suite $\tau_K(\rho, \psi'_K) = \tau_K(\rho, \psi_K)$.

2) Soit $\text{Ver}_{K/\mathbb{Q}}$ le transfert de $G_{\mathbb{Q}}$ dans G_K ,

$$\forall g \in G_{\mathbb{Q}}, \quad g(\tau_K(g^{-1}(\rho))) = \tau_K(\rho) \det_\rho \circ \text{Ver}_{K/\mathbb{Q}}(g).$$

Soient Γ un groupe fini, et $N \in \mathcal{B}(\Gamma)$. Le groupe Γ est donc isomorphe au groupe $G_{N\Gamma}/G_N$. On en déduit donc un homomorphisme injectif de $R(\Gamma)$ dans $R(G_{N\Gamma})$. On note $\tau_{N,\Gamma}$ le composé des homomorphismes

$$R(\Gamma) \longrightarrow R(G_{N\Gamma}) \xrightarrow{\tau_{N\Gamma}} \bar{\mathbb{Q}}^*.$$

Il existe un unique isomorphisme, noté Det , de $\chi_1(\bar{\mathbb{Q}}[\Gamma])$ sur $\text{Hom}(R(\Gamma), \bar{\mathbb{Q}}^*)$ caractérisé par la propriété suivante : soit $a \in \bar{\mathbb{Q}}[\Gamma]^*$; soit $[\bar{\mathbb{Q}}[\Gamma], a] \in \chi_1(\bar{\mathbb{Q}}[\Gamma])$ où a désigne la multiplication par a ; soit $\rho \in R(\Gamma)$ le caractère d'une représentation $T : \Gamma \rightarrow \text{GL}_n(\bar{\mathbb{Q}})$; alors

$$\text{Det}_\rho([\bar{\mathbb{Q}}[\Gamma], a]) = \det\left(\sum_{\gamma \in \Gamma} a_\gamma T(\gamma)\right) \quad \text{si} \quad a = \sum_{\gamma \in \Gamma} a_\gamma \gamma \quad (\text{voir [Q 1]}).$$

La surjectivité de l'application $a \mapsto [\bar{Q}[\Gamma], a]$ de $\bar{Q}[\Gamma]^*$ dans $\kappa_1(\bar{Q}[\Gamma])$ donne la proposition suivante :

PROPOSITION 1.4. - Il existe $\alpha_{N, \Gamma} \in \bar{Q}[\Gamma]^*$ tel que

$$\tau_{N, \Gamma} = \text{Det}([\bar{Q}[\Gamma], \alpha_{N, \Gamma}]).$$

2. - Groupe de Grothendieck relatif

Soient R un anneau de Dedekind de corps des fractions K et A une K -algèbre semi-simple de dimension finie sur K , séparable.

Soit $\mathcal{O}$ un ordre de R dans A .

On note $\mathcal{C}(\mathcal{O})$ la catégorie des $\mathcal{O}$ -modules de type fini sans R -torsion.

On fixe une clôture séparable de K ; on pose $\bar{A} = \bar{K} \otimes_K A$.

On associe à $\mathcal{C}(\mathcal{O})$ la catégorie, notée $\bar{\mathcal{C}}'(\mathcal{O})$, suivante :

- les objets de $\bar{\mathcal{C}}'(\mathcal{O})$ sont les triplets (M, α, N) où M et N sont des objets de $\mathcal{C}$ et α est un $\bar{A}$ -automorphisme de $\bar{K} \otimes_R M$ sur $\bar{K} \otimes_R N$

- un morphisme de (M, α, N) dans (M', α', N') est un couple (f, g) de $\mathcal{O}$ -homomorphismes de M dans M' et de N dans N' respectivement tels que $\alpha' \circ f_{\bar{K}} = g_{\bar{K}} \circ \alpha$ où $f_{\bar{K}}$ et $g_{\bar{K}}$ proviennent de f et g par extension des scalaires à $\bar{K}$.

DÉFINITION 2.1. - On appelle groupe de Grothendieck relatif de la catégorie $\mathcal{C}(\mathcal{O})$ le quotient du groupe abélien libre engendré par les classes d'isomorphismes des objets de $\bar{\mathcal{C}}'(\mathcal{O})$ par le sous-groupe engendré par les éléments de la forme

$$(M, \beta \alpha, P) - (M, \alpha, N) - (M, \beta, P)$$

et

$$(M \oplus M', \alpha \oplus \alpha', N \oplus N') - (M, \alpha, N) - (M', \alpha', N') .$$

On note $\bar{G}_{\oplus, \text{rel}}(\mathcal{O})$ ce groupe et on note $[M, \alpha, N]$ la classe d'un élément (M, α, N) dans ce groupe.

10-06

THÉOREME 2.2. - La suite suivante est exacte

$$\chi_1(\bar{A}) \xrightarrow{\delta} \bar{Q}_{\oplus, \text{rel}}(\mathcal{O}) \xrightarrow{\nu} Q_{\oplus}(\mathcal{O}) \xrightarrow{\varepsilon} \chi_0(\bar{A})$$

où les applications δ, ν, ε sont définies de la façon suivante :

$$\varepsilon : [M] \longrightarrow [\bar{K} \otimes_R M]$$

$$\nu : [M, \alpha, N] \longrightarrow [N] - [M]$$

δ : soit V un $\bar{A}$ -module ; il existe un $\bar{A}$ -module W et un $\mathcal{O}$ -module M tel que $\bar{K} \otimes_R M = V \oplus W$; δ associe à $[V, \alpha]$ l'élément $[M, \alpha \oplus \text{Id}, M]$, qui ne dépend pas du choix de M et W .

Le groupe G_K de Galois de $\bar{K}$ sur K , opère sur $\bar{Q}_{\oplus, \text{rel}}(A)$. On note $\mathfrak{R}_{\Phi}(\mathcal{O})$ le sous-groupe de $\bar{Q}_{\oplus, \text{rel}}(\mathcal{O})$ engendré par les éléments dont l'image par extension des scalaires à K dans $\bar{Q}_{\oplus, \text{rel}}(A)$ est de torsion et fixe par G_K .

PROPOSITION 2.3. - Supposons que K est un corps de nombres et que A est une algèbre de groupe $K[\Gamma]$. Il existe une suite exacte :

$$\begin{aligned} \text{Hom}_{G_K, \Phi} (R(\Gamma), J(\bar{K})) / \text{Kom}_{G_K}^+ (R(\Gamma), U(\bar{K})) &\xrightarrow{\Delta} \mathfrak{R}_{\Phi}(\mathbb{Z}_K[\Gamma]) \\ &\longrightarrow \bigoplus_{p \in \mathfrak{P}(\mathbb{Z}_K)} Q_{\oplus}(\mathbb{Z}_{K, p}[\Gamma]) \end{aligned}$$

où $R(\Gamma)$ désigne le groupe des caractères de Γ à valeurs dans $\bar{\mathbb{Q}}$

$U(\bar{K})$ est le groupe des idèles unités de $\bar{K}$

$\mathfrak{P}(\mathbb{Z}_K)$ l'ensemble des idéaux premiers de $\mathbb{Z}_K$

$\Phi = \text{Hom}(G_K, \text{Det}(K[\Gamma]^*))$

$\text{Hom}_{G_K, \Phi} (R(\Gamma), J(K)) = \{f \in \text{Hom}(R(\Gamma), J(\bar{K})), \forall \phi \in \Phi, g f(g^{-1}(\chi)) = \phi(g) f(\chi)\}$

$\text{Hom}_{G_K}^+ (R(\Gamma), U(K)) = \{f \in \text{Hom}_{G_K} (R(\Gamma), J(K)), f(\chi)_p \text{ réel et positif pour toute place réelle } p \text{ de } K \text{ et tout caractère symplectique de } \Gamma\}$

Pour $N \in \mathcal{S}(\Gamma)$, on note encore $\tau_{N, \Gamma}$ la classe dans $\text{Hom}_{G_{\mathbb{Q}, \Phi}}(R(\Gamma), J(K)) / \text{Hom}_{G_{\mathbb{Q}}}^+(R(\Gamma), U(K))$ de l'application $\tau_{N, \Gamma}$ définie par le théorème 1.2.

Si $\tau_{N, \Gamma} = \text{Det}(\alpha_{N, \Gamma})$ (proposition 3.4), on a $\Delta(\tau_{N, \Gamma}) = [\mathbb{Z}[\Gamma], \alpha_{N, \Gamma}, \mathbb{Z}[\Gamma]]$.

Pour simplifier la suite de l'exposition, on suppose que $K = \mathbb{Q}$. Soit $N \in \mathcal{S}(\Gamma)$ telle que $N^\Gamma = \mathbb{Q}$.

On construit à partir de l'application trace une forme hermitienne à valeurs dans $\mathbb{Q}[\Gamma]$ pour l'involution définie à partir de l'application $\gamma \mapsto \gamma^{-1}$ (notée $\lambda \mapsto \bar{\lambda}$) de la façon suivante

$$\forall x, y \in N \quad \text{Tr}_{N/\mathbb{Q}}(x, y) = \sum_{\gamma \in \Gamma} \text{tr}_{N/\mathbb{Q}}(x \gamma(y)) \gamma.$$

Soit $T_{\mathbb{Q}, \Gamma}$ l'application de $\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} N$ dans $\bar{\mathbb{Q}}[\Gamma]$ définie par

$$T_{\mathbb{Q}, \Gamma}(k \otimes n) = k \sum_{\gamma \in \Gamma} \gamma(n) \gamma^{-1}.$$

PROPOSITION 2.4. - 1) L'application $T_{\mathbb{Q}, \Gamma}$ est une isométrie de $\bar{\mathbb{Q}} \otimes_{\mathbb{Q}} N$ dans $\bar{\mathbb{Q}}[\Gamma]$ munis respectivement des formes hermitiennes obtenues par extension des scalaires à $\bar{K}$ à partir de $\text{Tr}_{N/\mathbb{Q}}$ et de la forme hermitienne canonique $(\lambda, \mu) \mapsto \lambda \bar{\mu}$.

2) $[\mathbb{Z}_N, T_{\mathbb{Q}, \Gamma}, M]$ appartient à $\mathfrak{N}_{\Phi}(\mathbb{Z}[\Gamma])$ pour tout sous-module M de $\mathbb{Q}[\Gamma]$.

THÉORÈME I'. - Sous les hypothèses du théorème I, on a

$$[\mathbb{Z}_N, T_{\mathbb{Q}, \Gamma}, \mathbb{Z}[\Gamma]] = [\mathbb{Z}_{N'}, T_{\mathbb{Q}, \Gamma}, \mathbb{Z}[\Gamma]]$$

dans $\bar{\mathbb{Q}}_{\oplus, \text{rel}}(\mathbb{Z}[\Gamma])$.

Pour tout χ de $R(\Gamma)$, on note $W_{N/\mathbb{Q}}$ la constante de l'équation fonctionnelle des séries L d'Artin associées au caractère χ .

On note $W'_{N/\mathbb{Q}}$ l'élément de $\text{Hom}_{G_{\mathbb{Q}}} (R(\Gamma), J(\mathbb{Q}))$ construit de la façon suivante

- pour tout caractère χ irréductible et non symplectique de Γ , on pose

$$W'_{N/\mathbb{Q}}(\chi) = 1,$$

- pour tout caractère χ irréductible et symplectique de Γ , on définit les composantes locales de $W'_{N/K}(\chi)$ par

$$\begin{aligned} W'_{N/\mathbb{Q}}(\chi)_p &= 1 & \forall p \in p(\mathbb{Z}) \\ W'_{N/\mathbb{Q}}(\chi)_{p_\infty} &= W'_{N/\mathbb{Q}}(\chi^{w^{-1}}) & \forall w \in G_{\mathbb{Q}} \end{aligned}$$

où p_∞ désigne une place infinie de $\bar{\mathbb{Q}}$.

THÉORÈME II'. - Sous les hypothèses du théorème II

$$[\mathbb{Z}_N, T_{\mathbb{Q}, \Gamma}, \mathbb{Z}[\Gamma]] = \Delta(\tau_{N, \Gamma} \cdot W'_{N/\mathbb{Q}})$$

THÉORÈME III'. - Sous les hypothèses du théorème III

$$[\mathcal{B}_{N/\mathbb{Q}}^{-1}, T_{\mathbb{Q}, \Gamma}, \mathcal{O}(\mathbb{Z}_N, \mathbb{Q}[\Gamma])] = \Delta(\tau_{N, \Gamma})$$

où $\mathcal{B}_N^{-1}$ désigne la codifférente de N sur $\mathbb{Q}$.

-:-:-:-

RÉFÉRENCES

- [D] P. DELIGNE, Les constantes des équations fonctionnelles des fonctions L , Modular functions of one variable II, Lecture notes in Math. 349, Springer Verlag (1973).
- [F] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions, J. reine angew. Math. 286-287 (1976), 380-439.
- [L] H. W. LEOPOLDT, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine angew. Math. 201 (1959), 119-149
- [Q1] J. QUEYRUT, S-groupes des classes d'un ordre arithmétique, J. of Algebra vol. 76, n° 1 (1982), 234-260.
- [Q2] J. QUEYRUT, Structure galoisienne des anneaux d'entiers d'extensions sauvagement ramifiées, I, Annales Institut Fourier XXXI, 3 (1981), 3-35.
- [Ta] J. TATE, Local constants in Algebraic Number fields, A. Fröhlich éd., Academic Press, London 1977.

[W] S. WILSON, Extensions with identical wild ramification, Sémin. de Th.
des Nombres de Bordeaux (1980-1981).

(texte reçu le 1^{er} avril 1982)

-:-:-:-

Jacques QUEYRUT
U.E.R. de Mathématiques
et d'Informatique de
l'Université de Bordeaux I
F 33405 TALENCE CEDEX

