SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ANNE PHILIPPE

Corps de fonctions rationnelles invariant par un groupe cyclique d'après R. Swan

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 10, p. 1-9

<http://www.numdam.org/item?id=STNG_1974-1975__4__A10_0>

Séminaire de Théorie des Nombres
Mars 1975
Grenoble

CORPS DE FONCTIONS RATIONNELLES INVARIANT PAR UN GROUPE CYCLIQUE D'APRES R. SWAN [6]

par Anne PHILIPPE

INTRODUCTION.

Soit k un corps et $x_1 \ldots x_p$, p indéterminées.

Le groupe symétrique S_p opère sur le corps $K = k(x_1 \ldots x_p)$. Pour tout sous-groupe G de S_p, on définit le sous-corps de K fixe par G, ou corps des fonctions rationnelles invariant par G, noté L. Si $G = S_p$, L est une extension transcendante pure de k.

Le problème posé par E. Noether est la question de savoir si pour tout sous-groupe G de S_p, L est une extension transcendante pure de k. Si la réponse est affirmative et si k est un corps de nombres, une application du théorème d'irréductibilité de Hilbert permet de réaliser G comme groupe de Galois d'une extension de k.

En particulier, la réponse est affirmative si k contient une racine primitive p^e de l'unité et car$k$ premier à p, et si G est cyclique permutant circulairement les x_i. [3] (dû à Masuda).

En 1969, Swan [6] a montré que, si G est un groupe cyclique d'ordre p, opérant transitivement sur les indéterminées $x_1 \ldots x_p$, le corps $L = \mathbb{Q}(x_1 \ldots x_p)^G$ n'est pas une extension transcendante pure de $\mathbb{Q}$ pour $p = 47$.

Reformulant le problème en termes de représentation de groupe, Lenstra l'a résolu, [2], pour un groupe G abélien et la représentation régulière.

§ 1. RESULTATS DE MASUDA [3].

Soit k un corps de nombres, $x_1 \ldots x_p$, p indéterminées, permutées circulairement par $s \in S_p$.

Soit G le groupe engendré par s. G opère sur K et on pose $L = K^G$. Si ζ est une racine primitive p^e de l'unité, $k' = k(\zeta)$, $L' = k'.L$ et $K' = k'.K$. Alors $L' = K'^G$.

Prenons pour base de K' sur k' les y_i définis par :

$$y_i = \sum_{j=1}^{j=p} \zeta^{ij} x_j \text{ , pour } i = 1 \ldots p .$$

Dans la suite, l'ensemble d'indices sera $\mathbb{Z}/p\mathbb{Z}$ noté $\{1,2,\ldots,p\}$ et on pose $c_{jk} = \dfrac{y_j y_k}{y_{j+k}}$ pour tous j et k dans $\mathbb{Z}/p\mathbb{Z}$. Soit M' le corps engendré sur k' par les c_{jk}. Montrons $M' = L'$.

Remarques :

1. s opère sur les y_i par $s(y_i) = \zeta^i y_i$.
2. $M' \subset L'$ car les c_{jk} sont fixes par s donc par G.
3. M' est engendré sur k' par les c_{1j}, avec $j \in \{1,2,\ldots,p\}$ car $c_{jk} = \dfrac{c_{1k} \times c_{1k+1} \times \cdots \times c_{1k+j-1}}{c_{11} \times c_{12} \times \cdots \times c_{1j-1}}$.
4. $M'(y_1) = K'$ car $y_j = \dfrac{y_1 y_{j-1}}{c_{1j-1}}$ pour $j \in \{2,\ldots,p\}$.

LEMME 1. $M' = L'$.

Preuve : Comme $y_1^p = c_{11} \times c_{12} \times \ldots \times c_{1p}$, $y_1^p \in M'$ d'où $[K' : M'] \leq p$. D'autre part $M' \subset L'$, donc $[K' : M'] \geq p$, d'où $[K' : M'] = [K' : L'] = p$. Comme $M' \subset L'$, $M' = L'$.

COROLLAIRE. L' est une extension transcendante pure de k' . Donc la question posée en introduction a une réponse affirmative si $k = k'$.

Remarque 5. M' contient les éléments de la forme $y_1^{-i} y_i$, pour $i \in \{1,2,\ldots,p\}$, qui sont fixes par s .

§ 2. ETUDE D'UN $\mathbb{Z}\pi$-MODULE.

Dans toute la suite, nous supposons p premier et nous notons $p-1 = n$. π désigne un groupe d'ordre n , isomorphe à Aut $\mathbb{F}_p$, opérant sur K' comme suit : si T est un générateur de π , et t un générateur de $\mathbb{F}_p^*$,

$$T(\zeta) = \zeta^t \quad \text{et} \quad T(y_i) = y_{ti} \quad \text{pour tout} \quad i \in \{1,2,\ldots,p\}$$

π permute librement les y_i pour $i \in \{1,2,\ldots,p-1\}$ et laisse y_p fixe.

Le sous-groupe multiplicatif de K'^* engendré par $y_1,\ldots,y_{p-1}$, est noté H . Il est muni d'une structure de $\mathbb{Z}[\pi]$-module par l'opération de π définie ci-dessus et l'opération de $\mathbb{Z}$ est : $(n,y) \rightsquigarrow y^n$ pour tout $(n,y) \in \mathbb{Z} \times H$. H est un $\mathbb{Z}[\pi]$-module libre engendré par y_1 et isomorphe à $\mathbb{Z}[\pi]$ par ℓ :

$$\begin{array}{ccc} H & \xrightarrow{\ell} & \mathbb{Z}\pi \\ 1 & \longmapsto & 0 \\ y_1 & \longmapsto & 1 \end{array}$$

Soit M le sous-$\mathbb{Z}[\pi]$-module de H fixe par G : $M = H \cap L'$. D'après la remarque 5, M contient $y_1^{-i}y_i$, pour $i = 2,\ldots,p-1$, et M contient y_1^p. Ces éléments engendrent un sous-module H_1 de H, d'indice p dans H. Alors M ne peut être égal qu'à H ou à H_1. M ne peut être égal à H ; sinon L' serait contenu dans H, or y_p appartient à L' et y_p n'appartient pas à H.

Donc $M = H_1$. M est un sous-module d'indice p de H.

Soit I l'idéal de $\mathbb{Z}[\pi]$ engendré par p et par $T-r$, où r est le représentant de t appartenant à $\{1,\ldots,p-1\}$. I opère sur H par :

$$(T-r)y_1 = T(y_1)y_1^{-r} = y_r y_1^{-r} .$$

I est l'image de M par ℓ : $\ell(y_1^p) = p$ et $\ell(y_r y_1^{-r}) = T-t$. De plus, M est isomorphe à I comme $\mathbb{Z}[\pi]$-module.

APPLICATION.

PROPOSITION 1. *Le corps* L' *est engendré sur* k' *par* y_p *et* M. $L' = k'(M,y_p)$.

Preuve : D'après le lemme 1, $L' = k'(c_{11},\ldots,c_{1p})$. Or $y_1^{-i}y_i = c_{11} \times c_{12} \times \ldots \times c_{1i-1}$ pour $i = 2,3,\ldots,p-1$ et $y_1^p = c_{11} \times c_{12} \times \ldots \times c_{1p}$. M admet donc pour générateurs $c_{11}, c_{12}, \ldots, c_{1p-2}$ et $c_{1p-1} \times c_{1p}$. Comme $y_p = c_{1p}$, $L' = k'(M,y_p)$.

Alors pour un système quelconque de générateurs $m_1,\ldots,m_{p-1}$ de M, les m_i et y_p sont algébriquement indépendants.

§ 3. INVARIANT RELATIF A UN SOUS-ANNEAU DE L'.

a) On considère l'anneau $R = k'[y_p, m_1, m_1^{-1} \ldots m_{p-1}, m_{p-1}^{-1}]$. R vérifie les propriétés suivantes :

- P_1. R est un anneau factoriel.

En effet, $R = M^{-1}k'[y_1, m_1, \ldots, m_{p-1}]$. Or, un anneau de polynômes sur un anneau factoriel est factoriel, et pour toute partie multiplicative S d'un anneau A , A factoriel implique $S^{-1}A$ factoriel.

■ P_2 . $k' \subset R \subset L'$, L' est le corps des fractions de R , R est de type fini sur k' et R est stable par π .

■ P_3 . $U(R)/U(k')$ est un groupe abélien de type fini ($U(A)$ désignant le groupe des unités de l'anneau A).

En effet $U(R)/U(k')$ est isomorphe à M , ou I .

b) Supposons que L est une extension transcendante pure de k , de base $\{u_1, \ldots, u_p\}$. $L' = k'(u_1, \ldots, u_p)$ et l'anneau $R' = k'[u_1, \ldots, u_p]$ vérifie aussi les propriétés P_1 , P_2 , P_3 . De plus, $U(R')/U(k') = \{1\}$.

D'après P_3 , $U(R)/U(k')$ est un $\mathbb{Z}\pi$-module de type fini. $U(R)/U(k')$ permet de définir <u>un invariant</u> $\alpha(k', L', \pi)$ <u>pour tout anneau</u> R <u>vérifiant</u> P_1, P_2, P_3 , <u>et</u> π <u>étant un sous-groupe fini de</u> Aut L' .

LEMME 2. <u>Si</u> $a \in R^{\pi}$ <u>et</u> $a \neq 0$, R <u>vérifie</u> P_2 <u>implique</u> $R[a^{-1}]$ <u>vérifie</u> P_2 .

<u>Si, de plus</u>, R <u>vérifie</u> P_1 <u>et</u> P_2 , <u>alors</u> $R[a^{-1}]$ <u>aussi, et on a une suite exacte</u> :

$$0 \to U(R) \to U(R[a^{-1}]) \to S \to 0 \qquad (1)$$

<u>où</u> S <u>est un</u> $\mathbb{Z}[\pi]$<u>-module, libre comme groupe abélien, dont une base est permutée par</u> π .

<u>On appelle</u> S <u>un</u> $\mathbb{Z}\pi$<u>-module de permutations</u>.

<u>Preuve</u> : a se décompose dans R en $a = u p_1^{\nu_1}, \ldots, p_v^{\nu_v}$; comme $a \in R^{\pi}$, pour tout $\sigma \in \pi$, $\sigma a = a$, donc σ permute les p_i . On prend pour S le $\mathbb{Z}[\pi]$-module engendré par une base $e_1, \ldots, e_v$, dans laquelle π opère comme sur les p_i . Définissons un homomorphisme de

$U(R[a^{-1}])$ dans S : l'image de $x \in U(R[a^{-1}])$ est $\sum_{i=1}^{i=v} \mathrm{ord}_{p_i}(x)e_i$. Si $\lambda_1,\ldots,\lambda_v$ et ν sont des entiers positifs, l'image des $a^{-\nu}p_1^{\lambda_1},\ldots,p_v^{\lambda_v}$ est $\sum_{i=1}^{i=v}(\lambda_i-\nu\nu_i)e_i$, donc l'application est surjective. Le noyau est formé des $a^{-\nu}x$ tels que $\mathrm{ord}_{p_i}(x) = \mathrm{ord}_{p_i}(a^\nu)$, i.e. tels que a^ν divise x ; alors $a^{-\nu}x \in R$ et son inverse aussi. Donc le noyau est $U(R)$.

On en déduit que :

$$0 \to U(R)/U(k') \to U(R[a^{-1}])/U(k') \to S \to 0 \tag{2}$$

est aussi une suite exacte de $\mathbb{Z}\pi$-modules. On posera $\overline{U}(R) = U(R)/U(k')$.

LEMME 3. Si R et R' vérifient P_2 , il existe $a \in R^\pi$ et $a' \in R'^\pi$ tels que $R[a^{-1}] = R'[a'^{-1}]$.

Preuve : Il suffit de se ramener à $R \subset R'$, en utilisant le corps des fractions commun L' .

Des $\mathbb{Z}[\pi]$-modules, on se ramène à des A-modules, où A est un anneau de Dedekind. Précisément, η désigne une racine primitive n^e de l'unité, et $A = \mathbb{Z}[\eta]$ est l'anneau des entiers de $\mathbb{Q}(\eta)$.

Soit Φ_n le polynôme minimal de η et Φ l'idéal de $\mathbb{Z}[\pi]$ engendré par $\Phi_n(T)$. Alors $\mathbb{Z}[\pi]/\Phi \simeq \mathbb{Z}[\eta] = A$. A tout $\mathbb{Z}[\pi]$-module N est associé le A-module $N^\Phi = \mathrm{Hom}_{\mathbb{Z}\pi}(A,N) \simeq \{x \in N \ ; \ \Phi x = 0\}$.

De la suite exacte (2), on déduit une suite exacte de A-modules :

LEMME 4. $$0 \to \overline{U}(R)^\Phi \to \overline{U}(R[a^{-1}])^\Phi \to S^\Phi \to 0 \tag{3}$$
est une suite exacte, et S^Φ est un A-module libre.

Preuve : cf. lemme 9 [6].

Alors le A-module $\overline{U}(R)^{\Phi}$ est défini à un facteur direct libre près, en fonction de k', de L' et de l'action de π, indépendamment de R.

Or, tout module de type fini sur un anneau de Dedekind est somme directe d'un module de torsion et d'un module projectif P. La classe $[P]$ de P dans le groupe $\Gamma(A)$ des classes de A-modules projectifs de type fini modulo les A-modules libres de type fini ([1], [4]) est un invariant, relativement à R. Calculons-le dans les cas (a) et (b).

Cas a). I est un idéal de $\mathbb{Z}[\pi]$ d'indice fini premier à l'ordre de π. Il en résulte ([5], Prop. 7.1) que I est un $\mathbb{Z}[\pi]$-module projectif, et I^{Φ} est sans torsion. Donc, dans ce cas, P est isomorphe à I^{Φ}.

Cas b). $\overline{U}(R')$ est trivial, $\overline{U}(R')^{\Phi}$ également. Sa classe dans $\Gamma(A)$ est notée $[0]$.

D'après le théorème de Chevalley, si $[I^{\Phi}] = [0]$, alors I^{Φ} est un idéal principal de A. D'où :

PROPOSITION 2. *Si L est une extension transcendante pure de k, l'idéal I^{Φ} est principal.*

§ 4. NON-PRINCIPALITE DE L'IDEAL I^{Φ}.

L'homomorphisme surjectif d'anneaux $\varphi : \mathbb{Z}[\pi] \to \mathbb{Z}[\eta]$, défini par $\varphi(T) = \eta$, donne, pour image de I, l'idéal J, engendré par p et $\eta - r$. Le noyau de l'application $I \to J$ est ΦI et J est isomorphe à I^{Φ}. De plus, J est un idéal de norme p ([6], § 1). On a le résultat suivant :

PROPOSITION 3. *Soit A l'anneau des entiers de $\mathbb{Q}(\eta)$, où η est une racine primitive n^{e} de l'unité et soit J un idéal de A de norme p premier, tel que n divise $p-1$. Alors J n'est pas principal pour les couples $(n,p) = (23,47)$ ou $(46,47)$.*

Preuve : Supposons $J = Aa$, pour $a \in A$.

$N(J) = \pm N_{\mathbb{Q}(\eta)/\mathbb{Q}}(a)$. Soit E une sous-extension de $\mathbb{Q}(\eta)$ contenant $\mathbb{Q}$, et $\theta = N_{\mathbb{Q}(z)/E}(a)$. θ vérifie $N_{E/\mathbb{Q}}(\theta) = \pm p$.

Prenons pour E un sous-corps quadratique imaginaire de $\mathbb{Q}(\eta)$. Il est de la forme $\mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$, sans facteur carré, d divise n , $d \neq 1$ et de plus si n ou $n/2$ est impair, $d \equiv 1(4)$, ou si 4 divise n mais 8 ne divise pas n , d impair. Ici, $n = 23$ ou 46 , donc on est dans le premier cas, et $d = -23$. Il existerait $\theta = \dfrac{2\alpha + \beta(\sqrt{-23}+1)}{2}$ tel que $N(\theta) = p = 47$. Ce qui est impossible, d'où la non-principalité de J .

Il résulte des propositions 2 et 3 le théorème suivant :

Soit k un corps de nombres, $x_1,\ldots,x_p$ des indéterminées, et G un groupe cyclique d'ordre p permutant circulairement les x_i . Le corps $L = k(x_1,\ldots,x_p)^G$ n'est pas une extension transcendante pure de k pour $p = 47$.

Il n'est pas nécessaire que k soit un corps de nombres : il suffit que $[k(\zeta) : k] = p - 1$, pour une racine primitive p^e de l'unité ζ . Le résultat de Lenstra [2] généralise la méthode de Swan : il étudie la principalité de produits d'idéaux du type de I .

BIBLIOGRAPHIE

[1] DOCK SANG RIM - Modules over finite groups. Annals of Math. 69, n° 3, (1959).

[2] H.W. LENSTRA - Rational functions invariant under a finite abelian group. Inventiones math. 25, 299-325, (1974).

[3] K. MASUDA - On a problem of Chevalley. Nagoya Math.J. 8, 59-63, (1955).

[4] J.P. SERRE - Modules projectifs et espaces fibrés à fibre vectorielle. Séminaire Dubreil (1968) Paris.

[5] R. SWAN - Induced reprentations and projective modules. Annals of Math. 71, 552-578 (1960).

[6] R. SWAN - Invariant rational functions and a problem of Steenrod. Inventiones Math. 7, 148-158 (1969).

-:-:-:-