SÉMINAIRE N. BOURBAKI

MICHEL KERVAIRE

Fractions rationnelles invariantes

Séminaire N. Bourbaki, 1975, exp. n° 445, p. 170-189

<http://www.numdam.org/item?id=SB_1973-1974__16__170_0>

© Association des collaborateurs de Nicolas Bourbaki, 1975, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
26e année, 1973/74, n° 445

445-01
Février 1974

FRACTIONS RATIONNELLES INVARIANTES

[d'après H. W. LENSTRA]

par Michel KERVAIRE

Problème 1. Soient k un corps, G un groupe fini et V une représentation de G sur k. Le groupe G opère sur $K = k(V)$, le corps des fractions de l'algèbre symétrique de V sur k. Soit K^G le corps fixe de G. L'extension K^G/k est-elle transcendante pure ?

Apparemment le problème est déjà classique à la fin du siècle dernier. Voir W. BURNSIDE [1], Chap. XVII. Cependant, le premier résultat un peu général date de 1915. E. FISCHER [3] démontre que la réponse est "oui" si $k = \mathbf{C}$ et G est abélien. Voir Prop. (1.1) ci-dessous. A cette époque, semble-t-il, on conjecture que la réponse est toujours affirmative. En 1969, R. SWAN [7] exhibe le premier contre-exemple avec $k = \mathbb{Q}$, G le groupe cyclique d'ordre 47 et V la représentation régulière. Les résultats de Swan sont étendus par V. E. VOSKRESENSKII [8] au cas d'un groupe cyclique d'ordre quelconque.

Ce rapport résume les travaux de H. W. LENSTRA [5] qui résolvent la question pour G abélien et k arbitraire, du moins dans le cas où V est la représentation régulière. Voir Théorème (4.1).

Dans le cas où G est non-abélien, on ne sait apparemment rien hormis quelques cas particuliers. Même pour $k = \mathbf{C}$. Il est par ailleurs remarquable d'observer que le problème analogue pour $k[V]$, l'algèbre symétrique de V, est résolu depuis longtemps. Voir C. CHEVALLEY [2] et G. C. SHEPHARD - J. A. TODD [6].

Dans toute la suite G est supposé abélien fini. On note e = exposant de G, le p.p.c.m. des ordres des éléments de G.

1. Corps des constantes assez gros

Le point de départ est le théorème de Fischer.

1.1 PROPOSITION.- Si le corps ℓ contient les racines e-ièmes de l'unité et si la caractéristique de ℓ ne divise pas e , alors $\ell(V)^G/\ell$ est pure pour toute représentation V de G .

Démonstration (Celle de Fischer, essentiellement.) V est somme directe de représentations de dimension 1 , i.e. il existe une ℓ-base $y_1,\dots,y_n$ de V telle que $\alpha.y_i = \chi_i(\alpha)y_i$ pour tout $\alpha \in G$, où les $\chi_i : G \to \ell^*$ sont des caractères de G .

On a $\ell(V) = \ell(y_1,\dots,y_n)$ et les $y_1,\dots,y_n$ sont algébriquement indépendants. Il en résulte que le sous-groupe Y du groupe multiplicatif L^* , $L = \ell(V)$, engendré par $y_1,\dots,y_n$ est abélien libre avec base $y_1,\dots,y_n$.

Soient X le groupe des caractères de G , i.e. $X = \mathrm{Hom}(G, \ell^*)$, et $\Phi : Y \to X$ l'homomorphisme donné par $\Phi(y_i) = \chi_i$. Il est clair que $I = \mathrm{Ker}\,\Phi$ est contenu dans le corps fixe L^G . En fait, $\ell(I)$ = corps des fractions de l'algèbre de groupe $\ell[I]$, est égal à L^G . En effet, $\ell[I] = \ell[Y]^G$ comme on le voit immédiatement et $L^G = \ell(Y)^G$ est corps des fractions de $\ell[Y]^G$. Comme I est sous-groupe du groupe abélien libre Y , il possède une $\mathbb{Z}$-base libre $z_1,\dots,z_n$ et $L^G = \ell(I) = \ell(z_1,\dots,z_n)$ est transcendant pur sur ℓ .

On va appliquer la Prop. (1.1) avec ℓ = le corps des racines de $X^e - 1$ sur k et V la représentation régulière de G , i.e. V admet pour base $\{x_\alpha \mid \alpha \in G\}$ et $\alpha.x_\beta = x_{\alpha\beta}$. On suppose donc provisoirement que la caractéristique de k ne divise pas e .

Soit $\pi = \mathrm{Gal}(\ell/k)$. On considère la suite exacte

$$1 \to I \to Y \xrightarrow{\Phi} X \to 1 ,$$

comme ci-dessus. On observe que

1) π opère sur X par $(\sigma\chi)(\alpha) = \sigma(\chi(\alpha)) \in \ell^*$, $\sigma \in \pi$, $\alpha \in G$.

2) Y admet pour base $\{y_\chi \mid \chi \in X\}$, où $y_\chi = \sum_{\alpha \in G} \chi(\alpha^{-1}) x_\alpha$, et π opère sur Y par $\sigma . y_\chi = y_{\sigma\chi}$.

3) $\Phi : Y \to X$ définie par $\Phi(y_\chi) = \chi$ est surjective et commute à l'action de π .

Par suite I se trouve muni d'une structure de $\mathbb{Z}[\pi]$-module. D'autre part, si $K = k(V) = k(x_\alpha \mid \alpha \in G)$, on a

$$k(V)^G = \ell(x_\alpha \mid \alpha \in G)^{G \times \pi} = \ell(I)^\pi \quad , \quad \text{et} \quad \ell^\pi = k .$$

On est donc amené à étudier le

Problème 2. Soient F un corps, π un groupe d'automorphismes de F et M un $\mathbb{Z}[\pi]$-module, $\mathbb{Z}$-libre, écrit multiplicativement. Soient $F[M]$ l'algèbre de groupe de M sur F et $F(M)$ son corps de fractions sur lequel π opère de façon évidente. L'extension $F(M)^\pi/F^\pi$ est-elle transcendante pure ?

DÉFINITION.- L'extension K/k est dite stablement pure s'il existe une extension pure E/K de génération finie, telle que E/k soit pure.

La question de savoir si toute extension stablement pure serait automatiquement pure est un vieux problème non-résolu de O. Zariski.

L'intérêt de cette notion est technique. On peut caractériser agréablement les $\mathbb{Z}[\pi]$-modules M pour lesquels $F(M)^\pi/F^\pi$ est stablement pure. ($\pi \subset \mathrm{Aut}(F)$.) D'autre part, on verra que dans la situation considérée, miracle : stablement pure = pure. Dans le cas général, le problème de Zariski reste ouvert.

2. Caractérisation des $\mathbb{Z}[\pi]$-modules M tels que $F(M)^\pi/F^\pi$ soit stablement pure

Dans ce numéro, π est un groupe fini, pas nécessairement abélien, d'automorphismes d'un corps F .

DÉFINITION.- Un $\mathbb{Z}[\pi]$-module S , $\mathbb{Z}$-libre, est appelé π-module de permutation s'il possède une $\mathbb{Z}$-base finie $b_1,\dots,b_n$ telle que tout élément de π permute $\{b_1,\dots,b_n\}$.

2.1 PROPOSITION.- Si S est un π-module de permutation, alors $F(S)^\pi/F^\pi$ est pure.

Démonstration. Soit $x_1,\dots,x_n$ une $\mathbb{Z}$-base de S permutée par π . Soit $V \subset F(S)$ l'espace vectoriel $V = Fx_1 + \dots + Fx_n$. On observe que π opère sur V . Cette action est semi-linéaire, i.e. $\sigma(\lambda x) = \sigma(\lambda).\sigma(x)$ pour $\sigma \in \pi$, $\lambda \in F$, $x \in V$. Dans ces conditions, on sait que V possède une F-base $z_1,\dots,z_n$ formée d'éléments invariants par π . Il est alors clair que $F(S)^\pi = F(z_1,\dots,z_n)^\pi = F^\pi(z_1,\dots,z_n)$ est pur sur F^π .

La proposition suivante est l'une des idées cruciales de Lenstra.

2.2 PROPOSITION.- Si S est facteur direct dans un π-module de permutation, et si

$$1 \to M \to N \to S \to 1$$

est une suite exacte de $\mathbb{Z}[\pi]$-modules, $\mathbb{Z}$-libres, alors

$$F(N) \cong F(M \times S) ,$$

par un $F\pi$-isomorphisme.

En particulier, $F(N)^\pi \cong F(M \times S)^\pi$ sur F^π .

Démonstration. On a une injection $N \hookrightarrow F(N)^*$ de groupes multiplicatifs

compatible avec l'action de π . Soit $F(M)^{\cdot}.N$ le sous-groupe de $F(N)^{\cdot}$ engendré par $F(M)^{\cdot}$ et N . C'est un sous π-module de $F(N)^{\cdot}$.

On a une projection de π-modules

$$f : F(M)^{\cdot}.N \to S$$

donnée par $f(u.y) = y \bmod. M$. Pour voir que f est bien définie, il suffit de voir que $F(M)^{\cdot} \cap N = M$. Ceci est immédiat. (Les éléments de N forment une F-base de $F[N]$.) En outre, f est visiblement surjective et son noyau est $F(M)^{\cdot}$. On a donc une suite exacte

$$1 \to F(M)^{\cdot} \to F(M)^{\cdot}.N \to S \to 1$$

de $\mathbb{Z}[\pi]$-modules.

2.3 LEMME.- Soit $1 \to A \to B \to S \to 1$ une suite exacte de $\mathbb{Z}[\pi]$-modules, avec S facteur direct dans un π-module de permutation. Supposons que pour tout sous-groupe $\pi' \subset \pi$ on ait $H^1(\pi', A) = 0$. Alors, $B \cong A \times S$ comme $\mathbb{Z}[\pi]$-modules.

L'application de ce lemme à la suite

$$1 \to F(M)^{\cdot} \to F(M)^{\cdot}.N \to S \to 1$$

fonctionne, car $H^1(\pi', F(M)^{\cdot}) = 0$ par Hilbert 90. Il en résulte

$$F(M)^{\cdot}.N \cong F(M)^{\cdot} \times S ,$$

d'où $F(N) \cong F(M \times S)$ par un $F\pi$-isomorphisme.

Reste à démontrer le lemme. Supposons d'abord que S soit un π-module de permutation. On se ramène immédiatement au cas où π opère transitivement sur une $\mathbb{Z}$-base $x_1, \ldots, x_n$ de S . Soit π' le groupe de stabilité de x_1 . La suite exacte de cohomologie

$$H^0(\pi', B) \to H^0(\pi', S) \to H^1(\pi', A) = 0$$

montre que $B^{\pi'} \to S^{\pi'}$ est surjectif. Il existe donc $y_1 \in B$ tel que $\sigma y_1 = y_1$ pour tout $\sigma \in \pi'$ et y_1 se projette sur $x_1 \in S$. On définit

$s : S \to B$ par $s(x_i) = \sigma_i y_1$, où $\sigma_i x_1 = x_i$. La classe de σ_i mod. π' est bien définie et $\sigma_i y_1$ ne dépend que de cette classe. Il est clair que s est une section.

Le résultat s'étend immédiatement au cas où S est seulement facteur direct dans un π-module de permutation.

Nous sommes maintenant en mesure de caractériser les $\mathbb{Z}[\pi]$-modules M tels que $F(M)^\pi/F^\pi$ soit stablement pure.

2.4 PROPOSITION.- Soient F un corps et π un groupe fini d'automorphismes de F . Soit M un $\mathbb{Z}[\pi]$-module, $\mathbb{Z}$-libre et de génération finie. Il y a équivalence entre

(i) $F(M)^\pi/F^\pi$ est stablement pure, et

(ii) il existe une suite exacte

$$1 \to M \to S_1 \to S_2 \to 1 ,$$

où S_1 , S_2 sont des π-modules de permutation.

Démonstration. (i) $\Rightarrow$ (ii). Supposons d'abord que $F(M)^\pi/F^\pi$ est pure. Il existe $x_1,\ldots,x_n \in F(M)^\pi$ tels que $F(M)^\pi = F^\pi(x_1,\ldots,x_n)$. On considère $R_1 = F[x_1,\ldots,x_n]$ et $R_2 = F[M]$ qui sont des anneaux factoriels stables par π .

D'après un premier lemme de Swan ([7], Lemma 8), il existe $a_1 \in R_1^\pi$ et $a_2 \in R_2^\pi$ tels que $R_1[a_1^{-1}] = R_2[a_2^{-1}]$, $= R$ disons. Un autre lemme de Swan ([7], Lemma 7) fournit des suites exactes

$$1 \to U(R_1) \to U(R) \to S_1 \to 1 ,$$

$$1 \to U(R_2) \to U(R) \to S_2 \to 1 ,$$

où S_1 , S_2 sont des π-modules de permutation, et où $U(R_1)$, $U(R_2)$, $U(R)$ sont les groupes d'éléments inversibles dans R_1 , R_2 , R . Voir aussi [9].

On a $U(R_1) = F^*$, $U(R_2) = F^* . M$. On obtient donc la suite exacte

$$1 \to M \to S_1 \to S_2 \to 1 .$$

Maintenant, si $F(M)^\pi/F^\pi$ est seulement stablement pure, il existe un π-module trivial (donc de permutation) M_o tel que $F(M)^\pi(M_o)/F^\pi$ soit pure. On a $F(M)^\pi(M_o) = F(M \times M_o)^\pi$, d'où une suite exacte

$$1 \to M \times M_o \to S_1 \to S_2 \to 1 ,$$

avec S_1, S_2 des π-modules de permutation. On en tire les suites

$$1 \to M \to S_1 \to S_1/M \to 1 ,$$

et $$1 \to M_o \to S_1/M \to S_2 \to 1 .$$

Dans la deuxième suite, on a $H^1(\pi', M_o) = 0$ pour tout sous-groupe π' de π et S_2 est un π-module de permutation. D'après le lemme ci-dessus, $S_1/M \cong M_o \times S_2$ est donc un π-module de permutation.

(ii) $\Rightarrow$ (i). En vertu de la Prop. (2.2), on a

$$F(S_1)^\pi \cong F(M \times S_2)^\pi .$$

L'assertion en résulte immédiatement en appliquant deux fois la Prop. (2.1).

Résumé : Avec les notations du n° 1, $k(x_\alpha \mid \alpha \in G)^G = \ell(I)^\pi$ est donc stablement pure sur $k = \ell^\pi$ si et seulement si il existe une suite

$$1 \to I \to S_1 \to S_2 \to 1$$

exacte, où S_1, S_2 sont des π-modules de permutation.

Il s'agit de traduire cette information en critère "calculable".

3. Un cas particulier

La clef de cette traduction sera donnée par l'examen d'un cas particulier : Soit ρ un quotient cyclique de $\pi \subset \mathrm{Aut}(F)$. On note A_ρ l'ordre maximal dans $\mathbb{Q}\rho$. C'est aussi un $\mathbb{Z}[\rho]$-module, donc un $\mathbb{Z}[\pi]$-module via $\pi \to \rho$.

3.1 PROPOSITION.- Soit P un $\mathbb{Z}[\rho]$-module projectif de type fini. On regarde

A_ρ , P , $A_\rho \otimes P$ comme $\mathbb{Z}[\pi]$-modules via $\pi \to \rho$. Alors, il existe un $F\pi$-isomorphisme $F(P) \cong F(A_\rho \otimes P)$.

Evidemment pas induit par l'inclusion. (Produits tensoriels sur $\mathbb{Z}[\pi]$.)

Démonstration. Soient r l'ordre de ρ et

$$X^r - 1 = \prod_{i=1}^{t} f_i(X) = \prod_{j=1}^{t+1} g_j(X)$$

deux décompositions de $X^r - 1$ en produits de polynômes unitaires $f_i(X)$, $g_j(X) \in \mathbb{Z}[X]$, satisfaisant aux conditions :

(a) $f_i(X) = g_i(X)$ pour $i = 1,\dots,t-1$,

(b) $f_t(X) = g_t(X).g_{t+1}(X)$, et

(c) $g_{t+1}(X) = X^d - 1$, où d divise r .

Soit τ un générateur de ρ . On a la suite exacte

$$0 \to P/g_t(\tau)P \xrightarrow{g_{t+1}(\tau)} P/f_t(\tau)P \to P/g_{t+1}(\tau)P \to 0$$

où l'injectivité de la première flèche résulte de l'hypothèse P projectif. On se ramène à une vérification pour $P = \mathbb{Z}[\rho]$.

Or, $P/g_{t+1}(\tau)P = P/(\tau^d - 1)P = \mathbb{Z}[\rho_d] \otimes_{\mathbb{Z}\rho} P$, où ρ_d est cyclique d'ordre d et $\mathbb{Z}[\rho_d]$ un $\mathbb{Z}[\pi]$-module via la surjection $\pi \to \rho \to \rho_d$. Ainsi, $P/g_{t+1}(\tau)P$ est facteur direct dans un module $\mathbb{Z}[\rho_d] \otimes_{\mathbb{Z}\rho} (\mathbb{Z}\rho)^N = (\mathbb{Z}[\rho_d])^N$, visiblement π-module de permutation.

On applique la Prop. (2.2) au corps $F = \ell(\prod_{i=1}^{t-1} P/f_i(\tau)P)$, ce qui donne $F(P/f_t(\tau)P) \cong F(P/g_t(\tau)P \times P/g_{t+1}(\tau)P)$, i.e.

$$\ell(\prod_{i=1}^{t} P/f_i(\tau)P) \cong \ell(\prod_{j=1}^{t+1} P/g_j(\tau)P) ,$$

par un $\ell\pi$-isomorphisme.

On a $P = P/(\tau^r - 1)P$, et $A_\rho \otimes P = \prod_{d|r} P/\Phi_d(\tau)P$, où r est l'ordre de

ρ et $\Phi_d \in \mathbf{Z}[X]$ est le polynôme cyclotomique évident.

La Prop. (3:1) est donc ramenée à voir qu'il existe une suite (finie) de décompositions $\prod_{i=1}^{t} f_i(X)$ de $X^r - 1$ qui débute avec $X^r - 1$ et se termine par $\prod_{d|r} \Phi_d(X)$, et telle que deux décompositions successives de cette suite satisfassent aux conditions (a), (b), (c) décrites ci-dessus. C'est un lemme combinatoire sur les ensembles ordonnés. Soit E l'ensemble des diviseurs de r ordonné par divisibilité. A une famille $\{E_1,\dots,E_t\}$ de sous-ensembles disjoints de E, dont la réunion est E, on associe la décomposition $\prod_{i=1}^{t} f_i(X)$, où $f_i(X) = \prod_{d \in E_i} \Phi_d(X) \in Z[X]$. Comme $X^d - 1 = \prod_{\delta|d} \Phi_\delta(X)$, on est amené au

3.2 LEMME.- Soient E un ensemble ordonné fini et F l'ensemble des familles $\{E_1,\dots,E_t\}$ de sous-ensembles non-vides disjoints de E. Pour $x \in E$, soit $S(x) = \{z \in E \mid z \leq x\}$. On considère dans F la relation d'équivalence engendrée par

$$\{E_1,\dots,E_{t-1}, E_t \cup S(X)\} \sim_E \{E_1,\dots,E_t, S(X)\},$$

si $E_t \cap S(X) = \emptyset$. Alors, tous les éléments $\{E_1,\dots,E_t\} \in F$ avec $E = \bigcup_{i=1}^{t} E_i$ sont équivalents.

En particulier, la famille $\{E\}$ qui dans l'exemple correspond à la décomposition triviale $X^r - 1$ de $X^r - 1$ est équivalente à la famille $\{\{d\}_{d \in E}\}$ qui correspond à $X^r - 1 = \prod_{d|r} \Phi_d(X)$. Il est clair par ailleurs que la relation $\sim_E$ correspond exactement aux conditions (a), (b), (c) ci-dessus.

Démonstration. (Issue d'une discussion avec Siegfried.) Soit $a \in E$. Posons $E' = S(a)$. Pour tout $y \in E'$, on a $S_E(y) = S_{E'}(y)$. Il en résulte que l'équivalence des familles dans E' équivaut à l'équivalence dans F. On écrira donc $\sim$ au lieu de $\sim_E$ ou $\sim_{E'}$.

On suppose par récurrence sur le cardinal de l'ensemble que toutes les décompositions de $S(a)$, $a \in E$, sont équivalentes si $S(a) \neq E$.

Soit $\{E_1,\ldots,E_t\} \in F$ avec $E = \bigcup_i E_i$. On va démontrer que si la longueur $t <$ Card E , il existe une famille équivalente et de longueur plus grande.

Un élément $x \in E$ est isolé dans $\{E_1,\ldots,E_t\}$ s'il est seul dans le E_i qui le contient. Il existe un $a \in E$, non-isolé dans $\{E_1,\ldots,E_t\}$ et tel que tout $x \in S(a)$, $x \neq a$, soit isolé. Soit $S(a) = \{a, x_1,\ldots,x_n\}$. On peut écrire

$$\{E_1,\ldots,E_t\} = \{E_1,\ldots,E_s, \{x_1\},\ldots, \{x_n\}\} ,$$

et supposer $a \in E_s$. Evidemment, $S(a) \neq E$. Je dis que

$$\{E_s \cup S(a)\} \sim \{E_s, \{x_1\},\ldots, \{x_n\}\} .$$

En effet, soit

$$\{A_1,\ldots,A_{r-1}, A_r \cup S(y)\} \sim \{A_1,\ldots,A_r, S(y)\}$$

une équivalence élémentaire dans une chaîne allant de $\{S(a)\}$ à $\{\{a\}, \{x_1\},\ldots, \{x_n\}\}$. Hypothèse de récurrence. Nécessairement, a est dans l'un des A_i . Recette : Remplacer A_j par $A'_j = A_j$ si $j \neq i$, $A'_i = E_s \cup A_i$. On obtient l'équivalence élémentaire

$$\{A'_1,\ldots, A'_{r-1}, A'_r \cup S(y)\} \sim \{A'_1,\ldots, A'_r, S(y)\} ,$$

car $E_s - \{a\}$ est disjoint de tous les ensembles en vue.

La recette fournit l'équivalence

$$\{E_s \cup S(a)\} \sim \{E_s, \{x_1\},\ldots, \{x_n\}\} .$$

On a donc

$$\begin{aligned} \{E_1,\ldots,E_t\} &= \{E_1,\ldots,E_s, \{x_1\},\ldots, \{x_n\}\} \\ &\sim \{E_1,\ldots,E_{s-1}, E_s \cup S(a)\} \\ &\sim \{E_1,\ldots,E_{s-1}, E_s - \{a\}, S(a)\} , \end{aligned}$$

par la définition de l'équivalence, et

$$\sim \{E_1,\ldots,E_{s-1}, E_s - \{a\}, \{a\}, \{x_1\},\ldots, \{x_n\}\} ,$$

car $\{S(a)\} \sim \{\{a\}, \{x_1\}, \ldots, \{x_n\}\}$.

On a $t = s + n$ et la nouvelle famille est de longueur $s + n + 1$.

4. Le théorème

On décompose $G = \prod_q (\mathbb{Z}/q\mathbb{Z})^{n(q)}$, où q parcourt les puissances de nombres premiers. Soient e l'exposant de G , ℓ le corps des racines sur k de $X^e - 1$ et $\pi = \mathrm{Gal}(\ell/k)$. Soient $\zeta_e \in \ell$ une racine primitive e-ième de 1 , $\zeta_q = \zeta_e^{e/q}$, et $\varphi_q : \pi \to U(\mathbb{Z}/q\mathbb{Z})$ définie par $\varphi_q(\sigma) = s$, si $\sigma(\zeta_q) = \zeta_q^s$.

Soit Q l'ensemble des q divisant e , tels que

1) q est premier à la caractéristique de k ,

2) $\mathrm{Im}\{\varphi_q : \pi \to U(\mathbb{Z}/q\mathbb{Z})\}$ est cyclique,

3) si $q = 0 \mod. 4$, alors $\varphi_q(\pi) \neq \{+1, -1\}$.

Si γ est un groupe cyclique d'ordre c , on notera $R_\gamma = \mathbb{Z}[\gamma]/(\Phi_c(\tau_\gamma))$, où Φ_c est le c-ième polynôme cyclotomique. R_γ est indépendant du choix de τ_γ et $R_\gamma \cong \mathbb{Z}[\varepsilon_\gamma]$, où $\varepsilon_\gamma = e^{2\pi i/c}$, mais l'isomorphisme donné par $\tau_\gamma \to \varepsilon_\gamma$ dépend du choix de τ_γ .

Soit Q_γ l'ensemble des $q \in Q$ pour lesquels $\pi \to \gamma$ se factorise en $\pi \xrightarrow{\varphi_q} \rho_q \to \gamma$. ($\rho_q = \pi/\mathrm{Ker}\,\varphi_q$.) Pour tout $q \in Q_\gamma$, soit $\tau_q \in \rho_q$ un générateur de ρ_q se projetant sur τ_γ . On définit $t_q \in \mathbb{Z}$ par $\varphi_q(\tau_q) = t_q \mod. q$, et

$$\underline{a}_\gamma = \prod_{q \in Q_\gamma} (\tau_\gamma - t_q, q)^{n(q)} ,$$

un idéal de R_γ .

Remarque.- La description des $\underline{a}_\gamma$ dans les notes de Lenstra est légèrement différente, ce qui exige encore une reformulation. Je me borne à la description ci-dessus ; c'est celle qui apparaît naturellement dans la démonstration.

4.1 THÉORÈME.- Soit $V = k[G]$ la représentation régulière de G sur k. Les trois propriétés suivantes sont équivalentes :

(i) $k(V)^G/k$ est pure,

(ii) $k(V)^G/k$ est stablement pure,

(iii) on a simultanément les deux conditions :

(1) pour tout γ, l'idéal $\mathfrak{a}_\gamma$ de $R_\gamma \cong \mathbb{Z}[\varepsilon_\gamma]$ est principal, et

(2) si $\mathrm{caract}(k) \neq 2$, alors $k(\zeta_{2^{r(G)}})/k$ est cyclique, où $2^{r(G)}$ est la plus grande puissance de 2 divisant l'exposant de G.

Dans ce numéro, on suppose provisoirement que la caractéristique de k ne divise pas l'ordre de G. On se débarrassera de cette hypothèse au n° 6.

La première étape consiste à remplacer le π-module I (notations du n° 1) par un sous-module $J \subset I$ tel que I/J soit un π-module de permutation.

Définition de J. Soit $G = \prod_q (\mathbb{Z}/q\mathbb{Z})^{n(q)}$. On découpe l'ensemble des q divisant e en 3 morceaux.

$q \in Q$ ssi $\varphi_q(\pi)$ est cyclique, et si $q \equiv 0 \bmod 4$, $\varphi_q(\pi) \neq \{+1, -1\}$.

$q \in C$ ssi $q \equiv 0 \bmod 4$, et $\varphi_q(\pi) = \{+1, -1\}$.

$q \in D$ ssi $\varphi_q(\pi)$ n'est pas cyclique.

On observe que $D = \emptyset$ ssi la condition (2) du théorème est satisfaite. On pose $\rho_q = \pi/\mathrm{Ker}\,\varphi_q$.

Pour $q \in Q \cup C$, on définit $Z_q = \mathbb{Z}[\rho_q]$ et $\Phi_q : Z_q \to \mathbb{Z}/q\mathbb{Z}$ est l'extension $\mathbb{Z}$-linéaire de φ_q.

Pour $q \in D$, on écrit $\mathbb{Z}/q\mathbb{Z} - \{0\}$ multiplicativement $= \{u, u^2, \ldots, u^{q-1}\}$ et on prend $Z_q = \mathbb{Z}$-module libre sur $\mathbb{Z}/q\mathbb{Z} - \{0\}$, avec $\Phi_q : Z_q \to \mathbb{Z}/q\mathbb{Z}$ $\mathbb{Z}$-linéaire tel que $\Phi_q(u^s) = s$.

Dans les deux cas, π opère de façon évidente sur Z_q et $\mathbb{Z}/q\mathbb{Z}$, et Φ_q commute à l'action de π. On définit J_q par la suite exacte

$$0 \to J_q \to Z_q \xrightarrow{q} \mathbb{Z}/q\mathbb{Z} \to 0 .$$

Pour $q \in Q$, les J_q vont être $\mathbb{Z}[\rho_q]$-projectifs. On pourra les traiter à l'aide de (3.1), ce qui fournira la condition (1) du théorème. Les q dans C se révèleront inoffensifs. Ceux de D donneront la condition (2).

On pose $J = \prod_q (J_q)^{n(q)}$, $Z = \prod_q (Z_q)^{n(q)}$. On a un diagramme

$$\begin{array}{ccccccccc} 0 & \to & J & \to & Z & \to & \prod_q (\mathbb{Z}/q\mathbb{Z})^{n(q)} & \to & 0 \\ & & \downarrow f_o & & \downarrow f & & \| & & \\ 1 & \to & I & \to & Y & \to & X & \to & 1 . \end{array}$$

En effet, la décomposition de G fournit une identification $X = \prod_q (\mathbb{Z}/q\mathbb{Z})^{n(q)}$. Si $\alpha_{i,q}$ est le générateur du i-ième facteur $\mathbb{Z}/q\mathbb{Z}$, $i = 1,\ldots,n(q)$ qui correspond à $1 \in \mathbb{Z}/q\mathbb{Z}$, on l'envoie sur $\chi_{i,q} \in X$ défini par $\chi_{i,q}(\alpha_{i,q}) = \zeta_q$, $\chi_{i,q}(\alpha_{j,q'}) = 1$ pour $\alpha_{j,q'} \neq \alpha_{i,q}$.

On prend f $\mathbb{Z}$-linéaire et définie comme suit. Cas $Q \cup C$: Si $\sigma \in \rho_{i,q} \subset \mathbb{Z}[\rho_{i,q}]$, i-ième copie de $\mathbb{Z}[\rho_q]$ dans Z_q, $q \in Q \cup C$, et $\varphi_q(\sigma) = s$, on pose $f(\sigma) = y_{\chi_{i,q}}^{s}$. Cas D : Si $\sigma = u_i^s$ dans la i-ième copie de Z_q, $q \in D$, alors $f(\sigma) = y_{\chi_{i,q}}^{s}$.

Observer que Z est écrit additivement, tandis que Y est un $\mathbb{Z}$-module multiplicatif.

f est une application de π-modules et le diagramme commute. ($f_o = f|J$.) Ceci résulte de la formule $\sigma\chi_{i,q} = \chi_{i,q}^{s}$, $i = 1,\ldots,n(q)$, si $\varphi_q(\sigma) = s \in U(\mathbb{Z}/q\mathbb{Z})$.

De plus $\mathrm{Coker}\, f_o = \mathrm{Coker}\, f$. Or, $\mathrm{Coker}\, f$ est un π-module de permutation. En effet, l'image de f a pour $\mathbb{Z}$-base les y_χ avec

$$\chi \in X_o = \{x_{i,q}^s \mid s \in \mathrm{Im}\, \varphi_q \text{ , si } q \in Q \cup C \text{ , et } s \neq 0 \text{ , si } q \in D\} .$$

L'ensemble X_o est stable par π et forme une sous $\mathbb{Z}$-base de la base $\{y_\chi\}$ de Y permutée par π .

4.2 COROLLAIRE.- Si $\ell(J)^\pi/\ell^\pi$ est pure, $\ell(I)^\pi/\ell^\pi$ l'est aussi. Si $\ell(I)^\pi/\ell^\pi$ est stablement pure, $\ell(J)^\pi/\ell^\pi$ l'est aussi.

Conséquence immédiate de (2.2) et (2.1) appliquées à $F = \ell$ et $F = \ell(J)$ respectivement.

Encore deux propositions.

4.3 PROPOSITION.- Soit $F \supset \ell$ un corps avec action de π prolongeant l'action sur ℓ . Soit $q \in C$, i.e. $q = 2^f$, $f \geq 2$, et $\varphi_q(\pi) = \{+1 , -1\}$. Alors, $F(J_q)^\pi/F^\pi$ est pure.

Démonstration. $J_q \subset \mathbb{Z}[\rho_q]$ est engendré par $\tau_q + 1$ et 2^f , où τ_q est l'élément non-trivial de ρ_q , et $\tau_q(\tau_q + 1) = \tau_q + 1$, $\tau_q(2^f) = 2^f(\tau_q + 1) - 2^f$. Donc, en notation multiplicative, J_q est le groupe abélien libre sur la $\mathbb{Z}$-base x_1 , x_2 et

$$\tau_q . x_1 = x_1 \quad , \quad \tau_q . x_2 = x_1^q x_2^{-1} .$$

Par définition de φ_q , on a $\tau_q(\zeta_q) = \zeta_q^{-1}$. Soit $\gamma = \zeta_q^{2^{f-2}}$, alors $\tau_q(\gamma) = -\gamma$. On considère

$$z_1 = x_1 \quad , \text{ et } \quad z_2 = \gamma . \frac{x_1^{-q/2} x_2 - 1}{x_1^{-q/2} x_2 + 1} .$$

On vérifie immédiatement que z_1 , z_2 sont invariants par π , et $F(x_1 , x_2) = F(z_1 , z_2)$. Donc $F(J_q)^\pi = F(x_1 , x_2)^\pi = F(z_1 , z_2)^\pi = F^\pi(z_1 , z_2)$ qui est pur sur F^π .

4.4 PROPOSITION.- Pour $q \in Q$, i.e. $\varphi_q(\pi)$ cyclique, et si $q = 0 \mod 4$, $\varphi_q(\pi) \neq \{+1, -1\}$, le $\mathbb{Z}[\rho_q]$-module J_q est projectif (de rang 1).

Démonstration. Soient τ_q un générateur de ρ_q et t_q un entier tel que $\varphi_q(\tau_q) = t_q \mod q\mathbb{Z}$. Le $\mathbb{Z}[\rho_q]$-module J_q est engendré par $\tau_q - t_q$ et q . Soit $f : \mathbb{Z}[\rho_q]e_1 + \mathbb{Z}[\rho_q]e_2 \to J_q$ défini par

$$f(e_1) = \tau_q - t_q \quad , \quad f(e_2) = q \ .$$

On va construire une section. Il est équivalent de construire un endomorphisme s de $\mathbb{Z}[\rho_q]e_1 + \mathbb{Z}[\rho_q]e_2$ tel que $\operatorname{Ker} f \subset \operatorname{Ker} s$ et $fs = f$. Soit r l'ordre de ρ_q . Il est facile de voir que t_q peut être choisi tel que $(t_q^r - 1)/q$ soit premier à q excepté justement si $q = 0 \mod 4$ et $\varphi_q(\rho_q) = \{+1, -1\}$. Soient alors $\alpha , \beta \in \mathbb{Z}$ tels que $\alpha.(t_q^r - 1)/q + \beta.q = 1$. On pose

$$s(e_1) = (1 - \beta q)e_1 + \beta(\tau_q - t_q)e_2 \ ,$$

$$s(e_2) = -(\tau_q^{r-1} + \tau_q^{r-2}t_q + \ldots + t_q^{r-1})\alpha e_1 + \beta q e_2 \ .$$

On vérifie sans difficulté que $fs = f$ et $\operatorname{Ker} f \subset \operatorname{Ker} s$. (On utilise que $\tau_q - t_q$ n'est pas diviseur de zéro dans $\mathbb{Z}[\rho_q]$.)

Nous sommes maintenant en mesure de démontrer le théorème modulo quelques lemmes cohomologiques qui feront l'objet du n° 5.

(i) $\Rightarrow$ (ii) est trivial.

(ii) $\Rightarrow$ (iii). Par hypothèse et (4.2), $\ell(J)^\pi/\ell^\pi$ est stablement pure. Soient P , Γ , Δ les produits $\prod_q (J_q)^{n(q)}$, où q parcourt les ensembles Q , C , D respectivement. On a $J = P \times \Gamma \times \Delta$. D'après (4.3), $\ell(J)^\pi/\ell(P \times \Delta)^\pi$ est pure. Donc $\ell(P \times \Delta)^\pi/\ell^\pi$ est stablement pure. On a donc une suite exacte

$$1 \to P \times \Delta \to S_1 \to S_2 \to 1 \ ,$$

avec S_1 , S_2 des π-modules de permutation. (Critère (2.4).)

Comme $H^1(\pi', P \rtimes \Delta) = 0$ pour tout sous-groupe $\pi' \subset \pi$ d'après (5.2) et (5.3), on peut appliquer le lemme (2.3), et

$$P \times \Delta \times S_2 \cong S_1 .$$

Si D était non-vide, il existerait, d'après (5.3), un sous-groupe $\pi' \subset \pi$ tel que $\hat{H}^{-1}(\pi', \Delta) \neq 0$. Or, $\hat{H}^{-1}(\pi', P) = \hat{H}^{-1}(\pi', S) = 0$ par (5.1) et (5.2). Donc, $D = \emptyset$. C'est la condition (2) de (iii).

En outre,

$$P \times S_2 \cong S_1 .$$

Pour la suite du paragraphe. si H est un groupe abélien, on note $H_o = H/\mathrm{Tors}(H)$.

Soient γ un quotient cyclique de π , et $R_\gamma \cong \mathbb{Z}[\varepsilon_\gamma]$ regardé comme π-module. Il est facile de voir que $(R_\gamma \otimes S)_o$ est R-libre pour tout π-module de permutation S . En effet, si $S = \mathbb{Z}[\pi/\pi']$, on a $(R_\gamma \otimes S)_o = R_\gamma$ ou 0 suivant que $\pi \to \gamma$ se factorise ou non par $\pi \to \pi/\pi'$. Il en résulte que $(R_\gamma \otimes P)_o$ est stablement R_γ-libre, donc libre car R_γ est anneau de Dedekind. On a

$$(R_\gamma \otimes J_q)_o \cong (\tau_\gamma - t_q , q) \quad \text{ou} \quad 0$$

suivant que $\pi \to \gamma$ se factorise ou non par $\varphi_q : \pi \to \rho_q$. Donc, $(R_\gamma \otimes P)_o \cong \prod_{q \in Q_\gamma} (\tau_\gamma - t_q , q)^{n(q)}$. Il en résulte que l'idéal $\underline{a}_\gamma$ est principal et la condition (2) de (iii) est satisfaite.

(iii) $\Rightarrow$ (i). Comme $D = \emptyset$ par hypothèse, on a $J = P \times \Gamma$. Puisque $\ell(I)^\pi/\ell(J)^\pi$ et $\ell(P \times \Gamma)^\pi/\ell(P)^\pi$ sont pures par (4.2) et (4.4), il suffit de démontrer que $\ell(P)^\pi/\ell^\pi$ est pure.

Soit $P_q = (J_q)^{n(q)}$. C'est un $\mathbb{Z}[\rho_q]$-module projectif. Pour tout quotient cyclique γ de π , on a

$$\prod_{q \in Q_\gamma} R_\gamma \otimes P_q \cong \prod_{q \in Q_\gamma} R_\gamma \otimes (\mathbb{Z}[\rho_q])^{n(q)}$$

par hypothèse. Donc, puisque $A_\rho = \prod_\gamma R_\gamma$, produit étendu aux quotients de ρ ,

$$\ell(P) = \ell(\prod_q P_q) \cong \ell(\prod_q \prod_\gamma R_\gamma \otimes P_q) \qquad \text{par Prop. (3.1),}$$

où le produit est étendu aux quotients γ de ρ_q ,

$$\cong \ell(\prod_\gamma \prod_{q \in Q_\gamma} R_\gamma \otimes P_q) \cong \ell(\prod_\gamma \prod_{q \in Q_\gamma} R_\gamma \otimes (\mathbb{Z}[\rho_q])^{n(q)})$$

$$\cong \ell(\prod_q \prod_\gamma R_\gamma \otimes (\mathbb{Z}[\rho_q])^{n(q)}) \cong \ell(\prod_q (\mathbb{Z}[\rho_q])^{n(q)}) \ .$$

Or, $\prod_q (\mathbb{Z}[\rho_q])^{n(q)}$ est un π-module de permutation. Donc $\ell(P)^\pi/\ell^\pi$ est pure.

5. Lemmes de cohomologie

5.1 LEMME.- Soit S un π-module de permutation. Pour tout sous-groupe $\pi' \subset \pi$, on a

$$H^1(\pi', S) = \hat{H}^{-1}(\pi', S) = 0 \ .$$

Démonstration. On se ramène immédiatement au cas où π opère transitivement sur une $\mathbb{Z}$-base de S et $\pi' = \pi$. Pour tout entier positif, on a la suite exacte $0 \to S \xrightarrow{m} S \to S/mS \to 0$. On constate que $S^\pi \to (S/mS)^\pi$ est surjectif, donc la multiplication par m sur $H^1(\pi, S)$ est injective. Or, cette multiplication est nulle pour $m = Car(\pi)$. On obtient $\hat{H}^{-1}(\pi, S) = 0$ par calcul direct.

5.2 LEMME.- Si ρ_q est un quotient de π et J_q un $\mathbb{Z}[\rho_q]$-module projectif, on a

$$H^1(\pi', J_q) = \hat{H}^{-1}(\pi', J_q) = 0$$

pour tout sous-groupe π' de π .

Démonstration. J_q est facteur direct dans un $\mathbb{Z}[\rho_q]$-module libre, lequel est un π-module de permutation.

5.3 LEMME.- Supposons $\varphi_q : \pi \to U(\mathbb{Z}/q\mathbb{Z})$ à image non-cyclique. Alors, $H^1(\pi', J_q) = 0$ pour tout sous-groupe π' de π, et il existe un sous-groupe π' de π tel que $\hat{H}^{-1}(\pi', J_q) \neq 0$.

Démonstration. Pour la première assertion, on considère la suite exacte $0 \to J_q \to Z_q \to \mathbb{Z}/q\mathbb{Z} \to 0$. On constate que $Z_q^{\pi'} \to (\mathbb{Z}/q\mathbb{Z})^{\pi'}$ est surjectif pour tout $\pi' \subset \pi$, et $H^1(\pi', Z_q) = 0$ car Z_q est un π-module de permutation.

Pour la deuxième, on observe que $\varphi_q(\pi)$ contient le groupe à 4 éléments engendré par -1 et $5^{q/8}$. Soit π' son image réciproque par φ_q. On écrit $\mathbb{Z}/q\mathbb{Z} - \{0\} = \{u, u^2, \ldots, u^{q-1}\}$. Un calcul direct montre que $\hat{H}^{-1}(\pi', J_q)$ est cyclique d'ordre 2 engendré par la classe de $u - u^{1+q/2} - 2^{q/4}(u - u^{q-1})$.

6. Compléments

6.1 PROPOSITION.- Soient $W \subset V$ deux représentations fidèles du groupe fini G sur le corps k. Alors, $k(V)^G/k(W)^G$ est pure.

Démonstration. Soit $x_1, \ldots, x_d \in V$ une k-base de V mod. W. On considère dans $k(V)$ le $k(W)$-espace vectoriel $U = k(W).1 + k(W)x_1 + \ldots + k(W)x_d$. C'est un espace de dimension $d + 1$ car $x_1, \ldots, x_d$ sont algébriquement indépendants sur $k(W)$. Le groupe fini G opère semi-linéairement sur U et fidèlement sur $k(W)$. Il existe donc une $k(W)$-base b de U invariante par G. On peut prendre $b = \{1, z_1, \ldots, z_d\}$, et

$$k(V)^G = k(W)(U)^G = k(W)(z_1, \ldots, z_d)^G = k(W)^G(z_1, \ldots, z_d)$$

qui est pur sur $k(W)^G$.

6.2 COROLLAIRE.- Soit G abélien fini, $G = G_o \times P$, où P est un p-groupe et G_o est d'ordre premier à p. Soient k un corps de caractéristique p et

V , resp. V_o , les représentations régulières de G , resp. G_o , sur k . Alors $k(V)^G/k$ est pure si et seulement si $k(V_o)^{G_o}/k$ est pure.

Démonstration. On envoie V_o dans V par $x_\alpha \to \sum_{\gamma \in P} x_{\gamma\alpha}$ pour tout $\alpha \in G_o$. On a les inclusions $k(V_o)^{G_o} \subset k(V)^G \subset k(V)^{G_o}$. L'extension $k(V)^{G_o}/k(V_o)^{G_o}$ est pure par 6.1. Un théorème de Gaschütz [4] dit alors que $k(V)^G = (k(V)^{G_o})^P$ est pur sur $k(V_o)^{G_o}$.

Ainsi, $k(V_o)^{G_o}/k$ pure entraîne $k(V)^G/k$ pure.

Réciproquement, si $k(V)^G/k$ est (stablement) pure, alors $k(V_o)^{G_o}/k$ est stablement pure, et par le théorème (4.1) pour G_o d'ordre premier à caract(k) on conclut que $k(V_o)^{G_o}/k$ est pure.

On a donc le théorème (4.1) en général.

Pour les autres représentations, on a seulement un résultat partiel.

6.3 COROLLAIRE.- On suppose de nouveau caract(k) première à l'ordre de G . Soient V_1 une représentation fidèle de G et V la représentation régulière. Alors $k(V_1)^G/k$ est stablement pure ssi $k(V)^G/k$ est (stablement) pure.

Démonstration. Il existe une représentation fidèle W de G telle que $W \subset V_1$ et $W \subset V$. Il suffit de prendre pour W la somme des facteurs irréductibles de V_1 , pris chacun une fois exactement. On applique (6.1) aux deux inclusions $W \subset V_1$ et $W \subset V$.

BIBLIOGRAPHIE

[1] W. BURNSIDE - Theory of groups of finite order, Dover Publications, Inc. 1955.

[2] C. CHEVALLEY - Invariants of finite groups generated by reflections, Amer. J. Math., 77 (1955), 778-782.

[3] E. FISCHER - Die Isomorphie der Invariantenkörper der endlichen Abelschen Gruppen linearer Transformationen, Nachr. Königl. Ges. Wiss., Göttingen (1915), 77-80.

[4] W. GASCHÜTZ - Fixkörper von p-Automorphismengruppen rein transzendenter Körpererweiterungen von p-Charakteristik, Math. Zeitschrift, 71 (1959), 466-468.

[5] H. W. LENSTRA - Rational functions invariant under a finite abelian group, Notes polycopiées, Amsterdam (1972).

[6] G. C. SHEPHARD - J. A. TODD - Finite unitary reflection groups, Can. J. Math., 6 (1954), 274-304.

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

[8] V. E. VOSKRESENSKII - On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $Q(x_1,\ldots,x_n)$, Izv. Akad. Nauk SSSR, Ser. Mat., 34 (1970), 366-375. [English translation : Math. USSR - Izv., 4 (1970), 371-380.]

[9] J. MARTINET - Un contre-exemple à une conjecture d'E. Noether (d'après R. Swan), Sém. Bourbaki n° 372, 10 p., Lecture Notes in Math. 180, Springer-Verlag 1971.