SÉMINAIRE N. BOURBAKI

JACQUES MARTINET

Un contre-exemple à une conjecture d'E. Noether

Séminaire N. Bourbaki, 1971, exp. n° 372, p. 145-154

<http://www.numdam.org/item?id=SB_1969-1970__12__145_0>

Séminaire BOURBAKI
22e année, 1969/70, n° 372 Février 1970

UN CONTRE-EXEMPLE A UNE CONJECTURE D'E. NOETHER

d'après R. SWAN

par Jacques MARTINET

Soit k un corps, et $x_1,\dots,x_n$ n indéterminées ; notons K le corps $k(x_1,\dots,x_n)$. Le groupe symétrique S_n sur n lettres opère sur K . A tout sous-groupe G de S_n , la théorie de Galois associe le corps $L = K^G$ des éléments de K fixes par G . Il est bien connu que lorsque $G = S_n$, L est une extension transcendante pure de K (L/k est engendrée par les fonctions symétriques des x_i). E. Noether [7] a conjecturé que L était toujours une extension transcendante pure de k , quel que soit le sous-groupe G considéré : si cette conjecture était vraie, on pourrait alors prouver en utilisant le théorème d'irréductibilité de Hilbert, que, lorsque le corps de base k est un corps de nombres, tout groupe fini peut être réalisé comme groupe de Galois d'une extension galoisienne de k .

En fait, il n'y a eu que peu de résultats dans cette direction. La raison en est que la conjecture est fausse. Swan [10] a donné le contre-exemple suivant :

THÉORÈME 1.- *Soit* $\mathbb{Q}$ *le corps des rationnels,* $x_1,\dots,x_n$ n *indéterminées,* $K = \mathbb{Q}(x_1,\dots,x_n)$, G *le groupe cyclique d'ordre* n *opérant transitivement sur les indéterminées* $x_1,\dots,x_n$, *et* L *le sous-corps de* K *fixe par* G . *Pour* $n = 47$, L *n'est pas une extension transcendante pure de* $\mathbb{Q}$.

1. Résultats sur le problème de Noether.

Nous considérons un corps k, le corps $K = k(x_1,\ldots,x_n)$, sur lequel S_n opère de façon naturelle, et un sous-groupe G de S_n. Les résultats les plus anciens sont dus à Noether [7] et Seidelmann [9].

Si k est de caractéristique 0, pour $n = 3$ ou 4, K^G est une extension transcendante pure de k, quel que soit le sous-groupe G de S_n. Masuda [5], [6], a étudié le cas du sous-groupe cyclique G de S_n permutant circulairement $x_1,\ldots,x_n$. Il obtient les résultats suivants :

On suppose que la caractéristique de k ne divise pas n. Alors, $L = K^G$ est une extension transcendante pure de k pour $n = 2, 3, 4, 5, 6, 7, 11$, et, quel que soit n, lorsque k contient les racines n-ièmes de l'unité. (On a un résultat analogue si n est premier et égal à la caractéristique de k. Cf. Kuniyoshi [2].)

Chevalley [1] a montré que K^G est une extension transcendante pure de k lorsque k est de caractéristique 0 et G un groupe fini engendré par des réflexions.

Pour donner d'autres résultats, il est commode d'adopter une autre présentation. Donnons-nous un corps k, un k-espace vectoriel de dimension finie V, et une représentation ρ de G dans $\mathrm{Aut}(V)$. Le groupe G opère *via* ρ sur l'algèbre symétrique de V, qui s'identifie, par le choix d'une base $v_1,\ldots,v_n$ de V, à l'algèbre $k[v_1,\ldots,v_n]$. Le groupe G opère alors sur le corps des fractions $k(V)$ de l'algèbre symétrique de V, en permutant les v_i. Réciproquement, étant donnée une extension $K = k(x_1,\ldots,x_n)$ de k et un groupe G permutant les x_i, on peut trouver un k-espace vectoriel V, une représen-

tation ρ de G dans $Aut(V)$ et un isomorphisme d'extensions de $k(V)$ sur $k(x_1,\ldots,x_n)$ compatible avec les opérations de G .

Avec ces notations, on a les résultats suivants :

Si G est un groupe abélien fini d'exposant e , et k un corps dont la caractéristique ne divise pas e , contenant les racines e-ièmes de l'unité, $k(V)^G$ est une extension transcendante pure de k pour toute représentation ρ de G dans $Aut(V)$ (Pittie [8], et aussi Kuyk et Mullender [4] dans le cas de la représentation régulière).

Si G et H sont deux groupes finis, et si $\rho : G \to Aut(V)$ et $\sigma : H \to Aut(W)$ sont deux représentations telles que $k(V)^G$ et $k(W)^H$ sont des extensions transcendantes pures de k , alors $k(V \oplus W)^{G \times H}$ est encore une extension transcendante pure de k .

Signalons enfin que Pittie obtient des résultats dans le cas d'une représentation d'un groupe fini G dans $Aut(V)$ qui est induite par une représentation de degré 1 d'un sous-groupe distingué de G .

On trouvera une bibliographie sur le problème de Noether dans [4].

2. Invariants attachés à une extension.

Nous considérons un corps K , un groupe fini H d'automorphismes de K , et un sous-corps k de K , stable par H , tel que K soit une extension de type fini de k .

Nous dirons qu'un $\underline{\underline{Z}}[H]$-module P est un module de permutation si P est libre de type fini sur $\underline{\underline{Z}}$, et possède une base permutée par H . Soit $G_o(H)$ le groupe de Grothendieck de la catégorie des $\underline{\underline{Z}}[H]$-modules de type fini, et $P(H)$ le sous-groupe de $G_o(H)$ engendré par les modules de permutation. Nous allons

attacher au triplet (k, K, H) un invariant à valeur dans le groupe quotient $G_o(H)/P(H)$, que nous noterons $Sw(H)$. Pour cela, nous supposerons qu'il existe un sous-anneau A de K possédant les propriétés suivantes :

P_1 Le corps des fractions de A est K.

P_2 A est une k-algèbre de type fini.

P_3 A est stable par H.

P_4 A est factoriel.

P_5 A^*/k^* est un groupe abélien de type fini (on note A^* le groupe des unités de A).

THÉORÈME 2.- L'image de A^*/k^* dans $Sw(H)$ ne dépend pas du choix de l'anneau A (soumis aux conditions P_1 à P_5).

Indication pour la démonstration (cf. Swan [10]).

Soit $a \in A^H$, $a \neq 0$, et soit $B = A[a^{-1}]$. Il est clair que B vérifie les propriétés P_1 à P_4. On prouve l'existence d'une suite exacte $0 \to A^*/k^* \to B^*/k^* \to P \to 0$, où P est le module de permutation, combinaison linéaire formelle des idéaux principaux Ap_i de A, les p_i étant des éléments irréductibles de A, deux à deux non associés, parcourant l'ensemble des diviseurs de a. Il est alors clair que B vérifie P_5, et que A^*/k^* et B^*/k^* ont même image dans $Sw(H)$. Si maintenant A et A' sont deux anneaux vérifiant les propriétés P_1 à P_5, on montre qu'on peut trouver $a \in A^H$ et $a' \in A'^H$, tels que $A[a^{-1}]^* = A'[a'^{-1}]^*$, ce qui achève la démonstration du théorème.

Passons maintenant au cas d'un groupe H cyclique d'ordre n. Soit $\underline{O}$ un anneau de Dedekind et M un $\underline{O}$-module de type fini. On peut écrire M sous la forme $T \oplus P$ où T est un module de torsion et P un module projectif. Le module

P est isomorphe à la somme directe d'un module libre et d'un idéal I de $\underline{O}$; soit J l'idéal de $\underline{O}$, produit des idéaux premiers de $\underline{O}$ associés à une suite de Jordan-Hölder de T. On définit la classe de M, en abrégé c(M), comme étant la classe de l'idéal IJ^{-1} si $I \neq 0$, et la classe de J^{-1} si $I = 0$ (Bourbaki, Algèbre commutative, chapitre VII, § 4, n° 7). Soit σ un générateur de H et soit Φ le n-ième polynôme cyclotomique. L'anneau quotient $\underline{O} = \underline{\underline{Z}}[H]/(\Phi(\sigma))$ est isomorphe à l'anneau des entiers du corps des racines n-ièmes de l'unité ; c'est donc un anneau de Dedekind. Pour tout $\underline{\underline{Z}}[H]$-module M, notons M^{Φ} le sous-module formé des éléments de M annulés par $\Phi(\sigma)$; ce dernier module est muni naturellement d'une structure de $\underline{O}$-module.

Avec les notations ci-dessus, on peut énoncer le :

THÉORÈME 3.- La classe d'idéaux $c((A^*/k^*)^{\Phi})$ ne dépend pas du choix de l'anneau A vérifiant les propriétés P_1 à P_5.

Compte tenu du théorème 2, il suffit de démontrer le :

LEMME.- a) Si P est un module de permutation, P^{Φ} est libre sur $\underline{O}$.

b) Pour toute suite exacte $0 \to M \to N \to P \to 0$, où P est un module de permutation, N^{Φ} est isomorphe à la somme directe $M^{\Phi} \oplus P^{\Phi}$ (et, par conséquent, $c(M^{\Phi}) = c(N^{\Phi})$).

On trouvera une démonstration très élégante de ce lemme dans Swan ([10], lemme 9).

Notation. La classe du module $(A^*/k^*)^{\Phi}$, qui ne dépend que des corps k, K et du groupe H, sera notée $\alpha(k, K, H)$.

3. Un contre-exemple.

Nous nous donnons un nombre premier p , un corps k , dont la caractéristique n'est pas divisible par p , et nous posons $K = k(x_1,\ldots,x_p)$. Pour un corps L , on notera L' l'extension de L obtenue par adjonction des racines p-ièmes de l'unité. Nous faisons l'hypothèse que $[k' : k] = p - 1$. Soit G le groupe cyclique d'ordre p , qui opère sur K en permutant circulairement $x_1,\ldots,x_p$, et soit $L = K^G$. Il est clair que $[K' : K] = [L' : L] = p - 1$. Nous notons H le groupe de Galois de K'/K , canoniquement isomorphe par restriction aux groupes de Galois de L'/L et k'/k .

PROPOSITION 1.- Si L/k est une extension transcendante pure, alors $\alpha(k' , L' , H) = 1$.

En effet, on peut écrire $L = k(y_1,\ldots,y_p)$, où les y_i sont algébriquement indépendants sur k . Prenons $A = k'[y_1,\ldots,y_p]$. L'anneau A vérifie les conditions P_1 à P_5. Comme A^*/k'^* est réduit à l'élément neutre, $\alpha(k' , L' , H) = 1$.

Il n'y a plus maintenant qu'à calculer effectivement $\alpha(k' , L' , H)$. Pour cela, nous nous donnons une racine primitive p-ième ω de l'unité et formons les expressions (résolvantes de Lagrange) $y_i = \sum_{j=1}^{p} \omega^{-ij} x_j$, pour $i = 0,1,\ldots,p-1$. Le groupe H laisse fixe y_o ; le sous-$\underline{\underline{Z}}$-module M' de K'^* de base $y_1,\ldots,y_p$ est libre sur $\underline{\underline{Z}}[H]$, étant engendré sur cet anneau par y_1 .

Masuda [6] considère alors le sous-module M de M' défini par $M = M' \cap L'^*$. Il est facile de déterminer M explicitement : si σ est le générateur de G pour lequel $\sigma x_i = x_{i+1}$ $(i \bmod p)$, alors $\sigma y_i = \omega^i y_i$. Par

conséquent, y_1^p et $y_1^{-i}y_i$ sont les éléments de M ; ils engendrent un sous-module d'indice p de M', qui ne peut donc être que M. Cela prouve en outre que M est un sous-module d'indice p de M'.

Donnons-nous une $\underline{\underline{Z}}$-base $m_1,\ldots,m_{p-1}$ de M, et soit A l'anneau $k'[y_o, m_1, \ldots, m_{p-1}, m_1^{-1}, \ldots, m_{p-1}^{-1}]$. On vérifie que le corps des fractions de A est L', en remarquant que $K' = k'(M', y_o) = k'(M, y_o)(y_1)$ a un degré sur L' au plus égal à p. L'anneau A vérifie donc les conditions P_1 à P_5, le $\underline{\underline{Z}}[H]$-module A^*/k'^* n'étant autre que M. Par conséquent, $\alpha(k', L', H) = c(M^\Phi)$. La suite exacte $0 \to M^\Phi \to M'^\Phi \to M'^\Phi/M^\Phi \to 0$ montre que $\alpha(k', c', H) = c(M'^\Phi/M^\Phi)^{-1}$. On vérifie que M^Φ est un sous-$\underline{O}$-module d'indice p de M'^Φ, d'où l'on déduit que le $\underline{O}$-module M'^Φ/M^Φ est isomorphe à un quotient $\underline{\underline{Z}}[\zeta]/\mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier de $\underline{\underline{Z}}[\zeta]$ au-dessus de p, ζ désignant une racine primitive $(p-1)$-ième de l'unité. Il suffit maintenant de prouver que $\mathfrak{p}$ n'est pas principal lorsque $p = 47$ pour obtenir un contre-exemple à la conjecture de Noether.

Dans ce cas, $\underline{\underline{Z}}[\zeta]$ est la clôture intégrale de $\underline{\underline{Z}}$ dans le corps k' des racines 23-ièmes de l'unité. Ce corps contient le corps quadratique $\mathbb{Q}(\sqrt{-23})$, dont l'anneau des entiers est formé des éléments de la forme $\frac{x + y\sqrt{-23}}{2}$, x et y étant des entiers rationnels de même parité. Si $\mathfrak{p}$ était principal, sa norme relativement à $\mathbb{Q}(\sqrt{-23})$, serait encore un idéal principal (α). On en déduirait une égalité de la forme $(\alpha) = (\frac{x + y\sqrt{-23}}{2})$, d'où, en prenant la norme relativement à $\mathbb{Q}$, l'égalité $47 = \frac{x^2 + 23y^2}{4}$, x et y étant des entiers de même parité. Un petit nombre d'essais montre qu'une telle égalité est impossible.

4. Descente galoisienne.

Le $\underline{\underline{Z}}[H]$-module M que nous avons utilisé est projectif de rang 1 . Masuda [6] prouve que, lorsque M est libre sur $\underline{\underline{Z}}[H]$, L est une extension transcendante pure de k . Malheureusement, on ne possède pas d'invariants commodes permettant de caractériser les $\underline{\underline{Z}}[H]$-modules libres parmi ceux qui sont projectifs (sauf dans le cas où H est cyclique d'ordre premier, mais ce cas ne se rencontre dans notre problème que lorsque $p = 3$). De plus, on ne sait pas si la condition que M soit libre sur $\underline{\underline{Z}}[H]$ est nécessaire pour que K/k soit transcendante pure ; l'invariant $\alpha(k', K', H)$ de Swan ne fournit qu'une réciproque partielle au résultat de Masuda.

Pittie [8] a tenté de systématiser l'étude précédente. On se donne un corps de base k , et une extension galoisienne de degré fini k' de k , dont le groupe de Galois est noté H .

Soit alors L une extension de type fini de k , de degré de transcendance n , telle que k soit algébriquement clos dans L , et soit L' le corps composé de k' et L .

Problème.- Supposant que L'/k' est transcendante pure, donner des conditions portant sur le triplet (k', L', H) pour qu'il en soit de même de L/k .

Limitons-nous au cas où k est de caractéristique 0 .

Pour faire cette étude, Pittie définit ce qu'il appelle un module de Masuda associé au triplet (k', L', H) : c'est un sous-$\underline{\underline{Z}}[H]$-module de L'^* vérifiant les conditions :

a) M est un $\underline{\underline{Z}}$-module libre de rang n ;

b) M possède une $\underline{\underline{Z}}$-base qui est une base de transcendance de L'/k' .

THÉORÈME 4.- Supposons H abélien et L'/k' transcendante pure. Alors, L est une extension transcendante pure de k si et seulement si il existe un module de Masuda pour le triplet (k', L', H) qui soit un $\underline{\underline{Z}}[H]$-module de permutation.

On peut montrer l'existence d'un module de Masuda pour (k', L', H) chaque fois que k' contient les racines e-ièmes de l'unité, e désignant l'exposant de H .

Ces résultats suggèrent l'utilisation du groupe Sw(H) pour trouver des invariants permettant de tester si une extension L/k est transcendante pure. Actuellement, on ne possède pas de résultats précis dans ce sens.

BIBLIOGRAPHIE

[1] C. CHEVALLEY - Invariants of finite groups generated by reflections, Am. Journal of Math., 77 (1955), p. 778-782.

[2] H. KUNIYOSHI - On a problem of Chevalley, Nagoya Math. Journal, 8 (1955), p. 65-67.

[3] W. KUYK - On a theorem of E. Noether, Proc. Kon. Ned. Acad. Wet., Ser. A, 67 (1964), p. 32-39.

[4] W. KUYK and P. MULLENDER - On the invariants of finite abelian groups, Proc. Kon. Ned. Acad. Wet., Ser. A, 66 (1963), n° 2, p. 232-237.

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

[6] K. MASUDA - Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariants, J. Math. Soc. Japan, 20 (1968), n° 2, p. 223-232.

[7] E. NOETHER - Gleichungen mit vorgeschriebener Gruppe, Math. Ann., 78 (1916), p. 221-229.

[8] Harsh Vardhan PITTIE - Group actions and algebraic K-theory, Thèse, Université de Princeton (Décembre 1969).

[9] F. SEIDELMANN - Die Gesamtheit der kub und biquadr. Gleichungen mit Affekt bei beliebigem Rationalitätsbereich, diss., Erlangen, (1916).

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