Astérisque

ANDRZEJ SCHINZEL

Les extensions pures et les résidus des puissances

Astérisque, tome 24-25 (1975), p. 69-74

<http://www.numdam.org/item?id=AST_1975__24-25__69_0>

Société Mathématique de France
Astérisque 24-25 (1975)

LES EXTENSIONS PURES ET LES RÉSIDUS DES PUISSANCES

par

Andrzej SCHINZEL

-:-:-:-

Par une extension pure d'un corps K je comprends le corps $K(\xi_1, \dots, \xi_k)$, où $\xi_i^{n_i} = \alpha_i \in K$. Dans le cas où $k = 1$ et K contient une racine primitive n-ième de l'unité de la théorie de ces extensions est due à Kummer. Mais le premier résultat général démontré sans la dernière hypothèse est à mon avis le théorème suivant de Capelli.

La condition nécessaire et suffisante pour qu'une extension pure $K(\xi)$ soit de degré n est que $\alpha \neq \beta^p$, $p \mid n$ et si $4 \mid n$, $\alpha \neq -4\beta^4$, $\beta \in K$.

Capelli lui-même a démontré son théorème seulement pour des corps algébriques mais l'extension au cas général ne présente pas de difficulté. Le cas $k > 1$ sous l'hypothèse kummerienne a été envisagée par Hasse et sans cette hypothèse par Besicovitch. Leurs résultats sont contenus dans le théorème suivant de Mordell (1953).

Si K contient des racines primitives de l'unité de degrés $n_1, \dots, n_k$ où k et les nombres $\xi_1, \dots, \xi_k$ sont réels ; alors l'extension $K(\xi_1, \dots, \xi_k)$ est de degré $n_1 \dots n_k$ si et seulement si $\xi_1^{X_1} \dots \xi_k^{X_k} \in K$ entraîne $X_1 \equiv 0 \mod n_i$ $(1 \leq i \leq k)$.

Ce théorème a été récemment généralisé par Siegel dans son travail qui vient de paraître aux Acta Arithmetica et plus encore par Kneser dans un travail qui va paraître au même Journal. Le résultat de Kneser est le suivant :

Pour que le degré d'une extension pure séparable $[K(\xi_1, \dots, \xi_k) : K]$ soit égal à l'indice $[K^* < \xi_1, \dots, \xi_k > : K^*]$ il faut et il suffit que pour tout nombre premier p

$$\zeta_p \in K^* < \xi_1, \dots, \xi_k > \longrightarrow \zeta_p \in K$$

et

$$1 + \zeta_4 \in K^* < \xi_1, \dots, \xi_k > \longrightarrow \zeta_4 \in K$$

où ζ_q est une racine primitive de l'unité de degré q.

En utilisant le résultat de Kneser, je viens de démontrer le théorème suivant :

THÉORÈME 1. - Pour qu'une extension pure séparable $K(\xi_1, \dots, \xi_k)$ soit de degré $n_1 \dots n_k$ il faut et il suffit que pour tout nombre premier p l'égalité

$$\prod_{p \mid n_i} \alpha_i^{X_i} = \gamma^p \quad \text{entraîne} \quad X_i \equiv 0 \pmod p \quad (1 \leq i \leq k)$$

et les conditions $\prod_{p \mid n_i} \alpha_i^{X_i} = -4\gamma^4$, $n_i X_i \equiv 0 \pmod 4$ $(1 \leq i \leq k)$ entraînent $X_i \equiv 0 \mod 4$ $(1 \leq i \leq k)$ (où γ désigne un élément de K).

C'est une généralisation simultanée du théorème de Capelli et de celui de Mordell, mais au contraire du théorème de Capelli la condition de séparabilité ne

peut être ici enlevée.

La question naturelle s'impose quand il y a des éléments $\xi_1, \ldots, \xi_k$ tels que $\xi_i^{n_i} = \alpha_i$ et

$$[K(\xi_1, \ldots, \xi_k) : K] = [K^* < \xi_1, \ldots, \xi_k > : K^*] .$$

Une condition nécessaire et suffisante simple n'existe probablement pas mais j'ai démontré que la condition suivante suffit : $\zeta_4 \in K$ ou bien si $n_i X_i \equiv 0 \pmod 4$ $(1 \leq i \leq k)$ alors $\prod \alpha_i^{X_i} \neq -\gamma^4$ et $-4\gamma^4$, $\gamma \in K$.

D'autre part il est possible de donner une condition nécessaire et suffisante pour le phénomène suivant :

Les nombres naturels $n_1, \ldots, n_k$, n et les éléments $\alpha_1, \ldots, \alpha_k$, β de K^* étant donnés, n divisible par n_i mais non divisible par la caractéristique de K et chaque corps $K(\xi_1, \ldots, \xi_k)$ où $\xi_i^{n_i} = \alpha_i$ contient au moins un η avec $\eta^n = \beta$.

Cette condition est donnée dans le résumé de ma conférence. Je viens d'obtenir le résultat plus précis que voici :

THÉORÈME 2. - Pour tous nombres naturels $n_1, \ldots, n_k$ et tous éléments $\alpha_1, \ldots, \alpha_k$ de K^* il existe des éléments $\xi_1, \ldots, \xi_k$ tels que $\xi_i^{n_i} = \alpha_i$ et que pour tout n divisible par $n_1, \ldots, n_k$ mais non divisible par la caractéristique de K pour tout $\beta \in K$: si $K(\xi_1, \ldots, \xi_k)$ contient un η avec $\eta^n = \beta$ alors au moins une des trois conditions suivantes est satisfaite pour des éléments γ et δ convenables de K

(i) $\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} = \gamma^n$,

(ii) $n \not\equiv 0 \pmod{2^\tau}$, $\overline{\prod_{2|n_i}} \alpha_i^{\ell_i} = -\delta^2$ et $\beta \overline{\prod_{i=1}^{k}} \alpha_i^{q_i n/n_i} = \gamma^n$,

(iii) $n \equiv 0 \pmod{2^\tau}$, $\overline{\prod_{2|n_i}} \alpha_i^{\ell_i} = -\delta^2$ et

$$\beta \overline{\prod_{i=1}^{k}} \alpha_i^{q_i n/n_i} = (-1)^{n/2^\tau} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$$

où τ est le plus grand entier naturel tel que $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$ s'il en existe un, $\tau = \infty$ dans le cas contraire.

Inversement, si une des conditions ci-dessus est satisfaite, alors chaque corps $K(\xi_1, \dots, \xi_k)$ où $\xi_i^{n_i} = \alpha_i$ contient au moins un η avec $\eta^n = \beta$.

Ce théorème généralise le résultat classique concernant les corps kummériens ainsi qu'un résultat récent de Gerst concernant le cas $K = Q$, $k = 1$.

Après avoir cité Gerst, je dois passer aux résidus des puissances. Déjà, en 1934, Trost a démontré que si la congruence $X^n \equiv a \pmod{p}$ est résoluble pour tous nombres premiers p alors $a = b^n$ ou bien $n \equiv 0 \mod 8$ et $a = 2^{n/2} b^n$. Ce théorème a été retrouvé par Aukeny et Rogers en 1951 et deux années plus tard généralisé par Flanders aux corps algébriques. D'après le théorème de Flanders, si $X^n \equiv \alpha \pmod{\mathfrak{P}}$ est résoluble pour tous les idéaux premiers d'un corps K, alors $\alpha = \beta^n$ ou bien $n \equiv 0 \pmod{2^{\tau+1}}$ et $\alpha = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$.

Gerst, dans le travail déjà cité, a généralisé le résultat de Trost dans une direction différente : il a démontré que si les congruences $X^n \equiv a \pmod{p}$ et $x^n \equiv b \pmod{p}$ sont simultanément résolubles ou non-résolubles, alors $b a^r = c^n$ ou bien $n \equiv 0 \mod 8$ et $b a^r = 2^{n/2} c^n$.

Or, je viens de démontrer la généralisation simultanée des résultats de Flanders et de Gerst.

THÉORÈME 3 - Soit n divisible par n_i $(1 \leq i \leq k)$, $\alpha_1, \ldots, \alpha_k$, $\beta \in K^*$. La résolubilité des congruences $X^{n_i} \equiv \alpha_i \pmod{\mathfrak{P}}$ entraîne la résolubilité de la congruence $X^n \equiv \beta \pmod{\mathfrak{P}}$ pour tous les idéaux premiers $\mathfrak{P}$ d'un corps algébrique K si et seulement si l'une au moins des quatre conditions suivantes est satisfaite pour des éléments γ, δ de K convenables : (i), (ii),

$$\text{(iii')} \quad n \equiv 2^\tau \bmod 2^{\tau+1}, \quad \prod_{2 \mid n_i} \alpha_i^{\ell_i} = -\delta^2,$$

$$\beta \prod_{i=1}^{i=k} \alpha_i^{q_i n/n_i} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$$

$$\text{(iv)} \quad n \equiv 0 \bmod 2^{\tau+1}, \quad \beta \prod_{i=1}^{i=k} \alpha_i^{q_i n/n_i} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n .$$

Ce théorème a des conséquences pour les congruences exponentielles dont j'ai parlé à Oberwolfach, donc je ne les mentionne pas ici.

-:-:-:-

BIBLIOGRAPHIE

[1] E. ARTIN and J. TATE. - Class field theory. New York-Amsterdam 1967, p. 93-97.

[2] A. CAPELLI. - Sulla riduttibilità della funzione $x^n - A$ in un campo qualunque di rationalità. Math. Ann. 54 (1901), p. 602-603.

[3] M. FLANDERS. - Generalization of a theorem of Ankeny and Rogers. Ann. of Math. 57 (1953), p. 392-400.

[4] I. GERST. - On the theory of n th power residues and a conjecture of Kronecker. Acta Arith. 17 (1970), p. 121-139.

[5] H. HASSE. - Bericht über neuere Untersuchungen und Probleme aud der Theorie der algebraischen Zahlkörper, vol. 2, Würzburg 1965, p. 42.

[6] H. B. MANN. - Introduction to algebraic number theory. Columbus, Ohio, 1955, p. 145-158.

[7] L. J. MORDELL. - On the linear independence of algebraic numbers. Pacific J. Math. 3 (1953), p. 625-630.

[8] A. SCHINZEL. - A refinement of a theorem of Gerst on power residues. Acta Arith. 17 (1970), p. 161-168.

[9] C. L. SIEGEL. - Algebraische Abhängigkeit von Wurzeln. Acta Arith. 21 (1972), p. 59-64.

[10] E. TROST. - Zur Theorie der Potenzreste. Niew Archief Wisk 18 (1934), p. 58-61.

-:-:-:-

Andrzej SCHINZEL
Institut Mathématique de
l'Académie Polonaise des
Sciences
BRZOZOWA 12 m 24
00286 VARSOVIE