Journal of Number Theory 88, 114–128 (2001)
doi:10.1006/jnth.2000.2607, available online at http://www.idealibrary.com on IDEAL®

Corps pythagoriciens, fermatiens et *P*-réduisants

Bruno Deschamps

Equipe de Théorie des Nombres, Faculté des Sciences et Techniques,
Université Jean Monnet, 23 rue du docteur Paul Michelon,
F42023 Saint-Etienne, Cedex 2, France
E-mail: Bruno.Deschamps@univ-st-etienne.fr

Communicated by M. Waldschmidt

Received November 29, 1999

Dans cet article, nous définissons et étudions la notion de corps P-réduisant qui généralise celle de corps pythagoricien. Nous montrons que si P désigne un polynôme absolument irréductible de $\mathbb{Q}(T_1, ..., T_n)[X]$, alors aucune extension finie et stricte de la clôture P-réduisante dans d'un corps K hilbertien de caractéristique 0 n'est P-réduisante. Dans une deuxième partie, nous regardons un cas particulier de corps P-réduisant: les corps ultra-n-fermatiens. Nous montrons que si p est un nombre premier impair et si K est un corps de caractéristique nulle contenant les racines p^2-ièmes de l'unité, alors le groupe de Galois, $Gal(K_p^{u-ferm}/K)$, (où K_p^{u-ferm} désigne la clôture ultra-p-fermatienne de K) est un pro-p-groupe sans torsion.

This paper is devoted to the notion of P-reducing field, which generalizes the notion of a Pytagorean field. We show that if P is an absolutely irreducible polynomial of $\mathbb{Q}(T_1, ..., T_n)[X]$, then there is no proper finite P-reducing extension of the P-reducing closure of an Hilbertian field of characteristic 0. In the second part, we study a particular case of P-reducing fields: ultra-n-Fermatian fields. We show that if p is an odd prime number and K is a field of characteristic 0 containing all the p^2th roots of unity, then the Galois groups, $Gal(K_p^{u-ferm}/K)$ (where K_p^{u-ferm} is the ultra-p-Fermation closure of K) is a torsion-free pro-p-group.

1. INTRODUCTION

L'objectif de cet article est de présenter la notion de corps P-réduisant, qui généralise assez largement celle de corps pythagoricien. Après quelques rappels sur les corps pythagoriciens et hilbertiens, nous présentons dans une première partie, la notion de corps P-réduisant qui apparaît pour la première fois dans [Des3] où nous montrions dans une annexe qu'aucune extension finie et stricte de $\mathbb{Q}^{pyth}$ (la clôture pythagoricienne de $\mathbb{Q}$) n'est pythagoricienne. Ce résultat, comme nous allons le voir, est en fait valable dans le cadre beaucoup plus général où l'on suppose juste K hilbertien. Si

0022-314X/01 $35.00

$P \in \mathbb{Q}[T_1, ..., T_n, X]$, on dit qu'un corps K est P-réduisant si pour toute spécialisation $(t_1, ..., t_n) \in K$, le polynôme $P(t_1, ..., t_n, X)$ se décompose totalement sur K. Nous montrons dans cette partie que si K désigne un corps hilbertien de caractéristique 0 et si P désigne un polynôme absolument irréductible sur $\mathbb{Q}[T_1, ..., T_n, X]$, alors aucune extension finie et stricte de la clôture P-réduisante de K (i.e. la plus petite extension algébrique P-réduisante de K) n'est P-réduisante. Les corps pythagoriciens étant un cas particulier des corps P-réduisants, nous obtenons alors le résultat annoncé précédemment.

Dans une deuxième partie, nous nous intéressons à un cas particulier de corps P-réduisant: les corps (ultra-)n-fermatiens. Ce sont les corps de caractéristique 0 qui vérifient $K^n = K^n + K^n$ (et qui possèdent les racines n-ièmes de l'unité). La notion de corps fermatien a été introduite et étudiée par Ribenboim (cf. [Rib2, Rib3]). Ribenboim s'est notamment intéressé à la "P-réduction" pour les polynômes $P = X^n - H(T_1, ..., T_n)$. Nous montrons une série de résultats arithmétiques concernant les corps ultra-n-fermatiens. En particulier, après avoir caractérisé sous certaines contraintes la propriété pour un corps d'être n-fermatien en regardant les extensions cycliques de K de degré divisant n (caractérisation qui représente un analogue au théorème de Diller et Dress), nous montrons que si p est un nombre premier impair et si K contient les racines p^2-ièmes de l'unité, alors le groupe de Galois, $Gal(K_p^{u-ferm}/K)$, (où K_p^{u-ferm} désigne la clôture ultra-p-fermatienne de K) est un pro-p-groupe sans torsion. Voici maintenant quelques rappels sur les corps pythagoriciens et hilbertiens dont nous aurons besoin dans la suite.

Corps pythagoriciens

DÉFINITION. Un corps K est dit pythagoricien, si toute somme de carrés d'éléments de K est encore un carré dans K.

Par récurrence immédiate, un corps est pythagoricien si et seulement si toute somme de deux carrés est encore un carré (i.e., $K^2 = K^2 + K^2$).

EXEMPLES.

- Tout corps K de caractéristique 2 est pythagoricien. En effet, on a $a^2 + b^2 = (a+b)^2$ pour tout $a, b \in K$.

- Tout corps K algébriquement clos est pythagoricien. En effet, si a et b sont deux éléments de K, une racine $\alpha \in K$ du polynôme $X^2 - a^2 - b^2$ vérifie bien $\alpha^2 = a^2 + b^2$.

- Le corps $\mathbf{C}$ des nombres constructible à la règle et aux compas est pythagoricien. Rappellons (cf. [Des1]) que $\mathbf{C}$ est la réunion des tours d'extensions quadratiques réelles de $\mathbb{Q}$. Par construction même de $\mathbf{C}$, si a

et b sont dans $\mathbf{C}$, alors $\sqrt{a^2+b^2}$ est dans $\mathbf{C}$, d'où le fait que $\mathbf{C}$ soit pythagoricien.

• Un corps réel clos (i.e. un corps K tel que $[\bar{K}:K]=2$) est pythagoricien. En effet, K vérifie $K=K^2\cup -K^2$ (cf. [Rib1]). En particulier (voir plus bas), la clôture totalement réelle d'un corps ordonné K (i.e. l'intersection de tous les corps réels clos contenant K, voir [Des2]) est un corps pythagoricien.

• Aucun corps de nombres n'est pythagoricien. En effect, si K est un corps de nombres, il existe un nombre premier p tel que $\sqrt{p}\notin K$; sinon, K contiendrait le corps $\mathbb{Q}(\sqrt{2},\sqrt{3},\ldots)$ qui est de dimension infinie sur $\mathbb{Q}$ (cf. [Des1]). Mais alors, comme $p=1^2+\cdots+1^2$ (p fois), K n'est pas pythagoricien.

Si $(K_i)_i$ désigne une famille de corps pythagoriciens, extensions algébriques d'un même corps, il est clair que $\bigcap_i K_i$ est un corps pythagoricien. Par suite, si K désigne un corps, parmi toutes ses extensions algébriques pythagoriciennes, il en existe une plus petite (l'intersection).

DÉFINITION. Soit K un corps. On appelle clôture pythagoricienne de K la plus petite extension algébrique pythagoricienne de K. On note ce corps K^{pyth}.

On peut construite le corps K^{pyth} en considérant la suite de corps $(K_n)_n$ définie ainsi:

$$K_0=K;\qquad \forall n\geqslant 0,\qquad K_{n+1}=K_n(\sqrt{\alpha^2+\beta^2})_{\alpha,\beta\in K_n}$$

On obtient K_{n+1} en adjoignant à K_n les éléments $\sqrt{\alpha^2+\beta^2}$ où α et β parcourent K_n. En particulier, toute somme de carrés d'éléments de K_n est un carré dans K_{n+1}. Il est alors clair que $K^{pyth}=\bigcup_{n\in\mathbb{N}} K_n$. On établit sans peine (cf. [Rib1]) que l'extension K^{pyth}/K est galoisienne; la construction de K^{pyth} prouve notamment que:

THÉORÈME. *Soit K un corps. Le groupe $Gal(K^{pyth}/K)$ est un pro-2-groupe.*

Les corps pythagoriciens présentent de très intéressantes propriétés arithmétiques, notamment la suivante:

THÉORÈME. *Si L/K est une extension telle que L soit pythagoricien et telle que $[L:K]<+\infty$, alors K est aussi pythagoricien.*

On obtient alors:

COROLLAIRE. • *Si K est un corps non pythagoricien, K^{pyth} ne possède aucune sous-extension stricte de degré fini (i.e. si $K\subset L\subset K^{pyth}$ et*

$[K^{pyth}: L] < +\infty$ *alors* $L = K^{pyth}$). *En particulier,* $\mathbb{Q}^{pyth}$ *ne possède aucun sous-corps* M, *autre que lui-même, tel que* $[\mathbb{Q}^{pyth}: M] < +\infty$.

• *Si* K *est un corps, le groupe de Galois,* $Gal(K^{pyth}/K)$, *est un pro-2-groupe sans torsion.*

Diller et Dress (cf. [DD]) ont donné une caractérisation des corps pythagoriciens ordonnables:

THÉORÈME. *Soir* K *un corps tel que* $-1 \notin K^2$. *Les propositions suivantes sont équivalentes*:

(i) K *est pythagoricien*;

(ii) K *ne possède pas d'extension cyclique de degré* 4.

Corps hilbertiens

DÉFINITION. Un corps K est dit hilbertien si, pour tout polynôme irréductible $P \in K(T_1, ..., T_n)[X]$, il existe une partie $V \subset K \times \cdots \times K$, Zariski-dense, telle que pour tout $(t_1, ..., t_n) \in V$, le polynôme spécialisé $P(t_1, ..., t_n, X) \in K[X]$ reste irréducible.

L'étude des corps hilbertiens a été très active ces dernières années. Elle a permis de caractériser certaines propriétés galoisiennes, en particulier en ce qui concerne la théorie inverse de Galois (voir [DeDe] pour plus de détail sur le sujet). Voici quelques exemples:

EXEMPLES.

• Tout corps de nombres est hilbertien. C'est le théorème initial dû à Hilbert.

• Tout corps de fractions $K(X)$ est un corps hilbertien (cf. [FJ]).

• Toute extension de type fini d'un corps hilbertien est hilbertienne (cf. [FJ]).

• Un corps algébriquement clos n'est jamais hilbertien.

De manière générale, il est difficile de prévoir l'hilbertianité d'une extension infinie d'un corps hilbertien. Par exemple, la clôture totalement réelle de $\mathbb{Q}$, appelée plus généralement *le corps des nombres totalement réels* et noté $\mathbb{Q}^{tr}$ n'est pas un corps hilbertien, alors que $\mathbb{Q}^{tr}(\sqrt{-1})$ en est un (voir [Des2, DeDe]). Nous utiliserons dans cet article un très profond théorème dû à Weissauer (voir [FJ]) que voici:

THÉORÈME. *Soit* K *un corps hilbertien,* L/K *une extension galoisienne et* M/L *une extension finie et stricte. Le corps* M *est hilbertien.*

Ce théorème prouve, en particulier, que $\mathbb{Q}^{pyth}(\sqrt{-1})$ est hilbertien (puisque $\mathbb{Q}^{pyth}/\mathbb{Q}$ est galoisienne et que $\sqrt{-1} \notin \mathbb{Q}^{pyth}$) alors même que $\mathbb{Q}^{pyth}$ n'est pas hilbertien. En effet, un corps de caractéristique différente de 2, pythagoricien, n'est jamais hilbertien puisque le polynôme $P(X, T_1, T_2) = X^2 - T_1^2 - T_2^2$ (qui est visiblement irréductible) n'admet aucune spécialisation $T_1 = t_1$, $T_2 = t_2$ qui le laisse irréductible.

2. CORPS P-RÉDUISANTS

DÉFINITION. Soit n un entier positif et $P \in \mathbb{Q}[T_1, ..., T_n, X]$. Un corps K de caractéristique 0 est dit P-réduisant, si pour tout n-uplet $(t_1, ..., t_n) \in K^n$, les racines du polynôme $P(t_1, ..., t_n, X)$ sont dans K.

Il est évident que si K et L sont deux corps de caractéristique 0 isomorphes, alors, si K est P-réduisant, L l'est aussi. On a alors:

THÉORÈME–DÉFINITION. *Soit K un corps de caractéristique 0 et $(K_i)_{i \in I}$ une famille d'extensions algébriques de K, P-réduisantes. Le corps $L = \bigcap_{i \in I} K_i$ est un corps P-réduisant.*

En particulier, parmi les extensions algébriques P-réduisantes de K, il en existe une plus petite (pour l'inclusion) notée K_P et appelée clôture P-réduisante de K.

L'extension K_P/K est galoisienne.

Preuve. Si $(t_1, ..., t_n) \in L^n$, les racines $r_1, ..., r_k$ de $P(t_1, ..., t_n, X)$ sont dans chaque K_i, donc dans L.

Le corps K_P est alors obtenu en prenant l'intersection de toutes les extensions algébriques P-réduisantes de K (il existe au moins une telle extension puisque $\bar{K}$ est P-réduisant).

Soit $\sigma \in Gal(\bar{K}/K)$; le corps $\sigma^{-1}(K_P)$ est P-réduisant, donc $K_P \subset \sigma^{-1}(K_P)$; et ainsi $\sigma(K_P) \subset K_P$. L'extension K_P/K est donc normale. Comme K est supposé de caractéristique nulle, K_P/K est séparable. ∎

Comme pour les corps pythagoriciens, on peut construire la clôture P-réduisante d'un corps K. Pour cela, on pose $K_1 = K(\alpha_i)_i$ où α_i parcourt toutes les racines dans $\bar{K}$ des polynômes $P(t_1, ..., t_n, X)$ où $(t_1, ..., t_n)$ parcourt tous les n-uplets d'éléments de K. Ensuite, on pose $K_2 = K_1(\alpha_i)_i$ où α_i parcourt l'ensemble des racines dans $\bar{K}$ des polynômes $P(t_1, ..., t_n, X)$ et où $(t_1, ..., t_n)$ parcourt l'ensemble des n-uplets d'éléments de K_1. Ainsi de suite, on construit par récurrence une suite de corps $(K_n)_n$. Il est alors clair que $K_P = \bigcup_{n \in \mathbb{N}} K_n$.

EXEMPLES. (1) Si $n=0$ et $P\in\mathbb{Q}[X]$, alors K est P-réduisant si et seulement s'il contient le corps de décomposition C de P sur $\mathbb{Q}$. Ainsi, $\mathbb{Q}_P=C$.

(2) Si $P=X^2-T_1$, alors $\mathbb{Q}_P=\mathbf{C}(i)$ où $\mathbf{C}$ désigne le corps des nombres constructibles à la règle et au compas.

(3) Si $n\geqslant 2$ et $P=X^2-T_1^2-\cdots-T_n^2$, alors K est P-réduisant si et seulement si K est pythagoricien.

(4) Si K est algébriquement clos, alors K est P-réduisant pour tout P.

(5) Soit $n>1$ et $P_n(T_1, ..., T_n, X)=X^n+T_1X^{n-1}+\cdots+T_n$, on a

PROPOSITION. *Les propriétés suivantes sont équivalentes*:

(i) *K est P_n-réduisant,*

(ii) *Toute extension finie L/K a un degré $>n$.*

Preuve. Si K possède une extension de degré $d\leqslant n$, alors si M désigne son polynôme minimal, le polynôme $X^{n-d}M(X)$ est la spécialisation, pour un certain n-uplet, de $P_n(T_1, ..., T_n, X)$, qui, par conséquent, ne se décompose pas totalement sur K. Réciproquement, s'il existe un n-uplet $(t_1, ..., t_n)$ d'éléments de K pour lequel $P_n(t_1, ..., t_n, X)$ ne se décompose pas totalement, alors un de ses facteurs irréductibles engendre une extension de degré $d\leqslant n$ sur K. ∎

COROLLAIRE. *Un corps K est algébriquement clos si et seulement si K est P_n-réduisant pour tout $n\geqslant 1$.*

Si l'on pose $K_n=\mathbb{Q}_{P_n}$, les corps K_n sont alors galoisiens sur $\mathbb{Q}$ et on a $\mathbb{Q}=K_1\subset K_2\subset\cdots\subset K_n\subset\cdots$ et $\bar{\mathbb{Q}}=\varinjlim_{n\geqslant 1}K_n$. En effet, un corps K étant P_n-réduisant si et seulement s'il ne possède aucune extension stricte de degré $\leqslant n$, on a bien la suite d'inclusions. Soit maintenant $\alpha\in\bar{\mathbb{Q}}$, si n_0 désigne le degré du polynôme minimal de α sur $\mathbb{Q}$, alors $[K_{n_0}(\alpha):K_{n_0}]\leqslant n_0$ et donc $\alpha\in K_{n_0}$.

Ainsi, si on note $G_n=Gal(K_n/\mathbb{Q})$, on a $Gal(\bar{\mathbb{Q}}/\mathbb{Q})=\varprojlim_{n\geqslant 1}G_n$.

Par définition même des corps hilbertiens, on a la proposition suivante:

PROPOSITION. *Soit $P\in\mathbb{Q}[T_1, ..., T_n, X]$ un polynôme de degré en X plus grand que 1 et absolument irréductible. Si K est un corps P-réduisant, K ne peut pas être hilbertien.*

Preuve. Le polynôme P étant irréductible sur K, si K était hilbertien, alors il existerait un n-uplet $(t_1, ..., t_n)\in K^n$ tel que $P(t_1, ..., t_n, X)$ soit irréductible sur K. Comme ce dernier polynôme est de degré plus grand que 1, cela contredirait alors le fait que K est P-réduisant. ∎

Cette proposition nous permet alors de donner le résultat sur les extensions finies des clôtures P-réduisantes des corps hilbertiens que nous annoncions dans l'introduction.

THÉORÈME. *Soit $P \in \mathbb{Q}[T_1, ..., T_n, X]$ un polynôme absolument irréductible de degré en X plus grand que* 1. *Si K est un corps hilbertien, alors $[K_P : K] = +\infty$ et aucune extension finie et stricte de K_P n'est P-réduisante. En particulier, si L est un corps P-réduisant et si $L \neq \mathbb{Q}_p$ alors $[L : \mathbb{Q}_p] = +\infty$.*

Preuve. Le corps K_P n'est pas hilbertienne; comme toutes les extensions finies de K sont des corps hilbertiens, on a $[K_P : K] = +\infty$. Par application du théorème de Weissauer, K_P/K étant galoisien et K étant hilbertien, toutes les extensions finies et strictes de K_P sont hilbertiennes et ne peuvent être P-réduisantes. ∎

On en déduit donc:

COROLLAIRE. *Si K désigne un corps hilbertien de caractéristique $\neq 2$, alors aucune extension finie et stricte de K^{pyth} n'est pythagoricienne.*

Preuve. Le polynôme $X^2 - T_1^2 - T_2^2$ est visiblement absolument irréductible sur $K(T_1, T_2)[X]$ quand K n'est pas de caractéristique 2. L'application du théorème de Weissauer prouve alors le corollaire. ∎

Remarques. • Ce corollaire avait déjà été établi le cas $K = \mathbb{Q}$.

• Le cas de la caractéristique 2 est pathologique. En effet, en caractéristique 2 tout corps est pythagoricien et il existe des corps de caractéristique 2 hilbertiens. Par exemple $\mathbb{F}_2(T)$.

On peut s'intéresser à la réciproque du théorème 1: *une extension algébrique de $\mathbb{Q}$ qui n'est pas hilbertienne est-elle nécessairement P-réduisante pour un polynôme P absolument irréductible et de degré en X plus grand que* 1?

Pierre Dèbes et Dan Haran viennent d'apporter récemment une réponse négative à cette question. Ils montrent dans leur article [DH] que, pour tout nombre premier $p > 2$, le corps K_{p^∞} construit de la manière suivante: *Soit la suite de corps $(K_n)_n$ définie par, $K_0 = \mathbb{Q}$, $K_1 = K_0(\sqrt[p]{\alpha})_{(\alpha \in K_0, \alpha \geqslant 0)}$ et pour tout $n \geqslant 1$, $K_{n+1} = K_n(\sqrt[p]{\alpha})_{(\alpha \in K_n, \alpha \geqslant 0)}$. On pose alors $K_{p^\infty} = \bigcup_{n \in \mathbb{N}} K_n$.* est un corps non hilbertien qui n'est P-réduisant pour aucun P. A ce propos, ils montrent que ces corps sont RG-hilbertiens,[1] ceci constituant un nouvel exemple de corps RG-hilbertien et non hilbertien (le premier exemple d'un tel corps avait été donné par Fried et Völklein). Cet exemple est

[1] Un corps K est dit RG-hilbertien s'il vérifie la propriété de Hilbert uniquement pour les polynômes absolument irréductibles.

intéressant, car les corps K_{p^∞} ne sont pas PAC[2] (on consultera [DH, FJ] pour plus de détails sur les propriétés *RG*-hilbertien et PAC). Dans [DH], Dèbes et Haran donnent aussi une caractérisation arithmétique des corps P-réduisants pour un P donné. Nous renvoyons le lecteur à cet article pour plus de détails.

3. CORPS FERMATIENS

Dans tout ce qui suit, on désigne par K^n l'ensemble des puissances n-ièmes des éléments d'un corps K. Tous les corps considérés dans cette partie seront commutatifs et de caractéristique nulle.

DÉFINITION. Soient K un corps et n un entier naturel non nul. On dit que K est:

- n-fermatien si toute somme de puissances n-ièmes d'éléments de K est encore une puissance n-ième dans K. (i.e. $K^n = K^n + K^n$.)
- ultra-n-fermatien si K est $(X^n - T_1^n - T_2^n)$-réduisant.

On a alors:

LEMME 1. *Soient K un corps commutatif et n un entier naturel non nul. Les propriétés suivantes sont équivalentes*:

(i) *K est ultra-n-fermatien.*

(ii) *K est n-fermatien et contient les racines n-ièmes de l'unité.*

Nous allons focaliser notre attention sur la notion de corps *ultra-n-fermatien*, celle-ci étant un cas particulier de la notion de corps P-réduisant. En particulier, on pourra parler de *clôture ultra-n-fermartienne* d'un corps, alors que la notion de *clôture n-fermatienne* n'est pas naturelle. En effet, on peut parler de clôture n-fermatienne d'un corps K en prenant une extension algébrique n-fermatienne de K minimale pour l'inclusion, mais il n'y a alors pas unicité de cette clôture. Par exemple, pour $n=3$ notons pour un nombre réel α, $\sqrt[3]{\alpha}$ la racine réelle de $X^3 - \alpha$. Considérons la suite de corps $(K_n)_n$ définie par

$$K_0 = \mathbb{Q}; \qquad K_{n+1} = K_n(\sqrt[3]{a^3 + b^3})_{a,\, b \in K_n}.$$

Le corps $K = \bigcup_n K_n$ est alors une clôture 3-fermatienne de $\mathbb{Q}$ qui n'est visiblement pas la clôture ultra-3-fermatienne de $\mathbb{Q}$ puisque $K \subset \mathbb{R}$ (on

[2] Un corps K est dit (P)seudo-(A)lgébriquement-(C) los si toute variété irréductible, lisse et définie sur K possède un point K-rationnel.

appellerait ce corps la *clôture 3-fermatienne réelle* de $\mathbb{Q}$). On peut, grâce, à l'axiome du choix, décrire d'autres clôtures 3-fermatiennes de $\mathbb{Q}$.

THÉORÈME 2. *Soient K un corps et n un entier naturel non nul. Il y a équivalence entre les propositions suivantes:*

(i) *K est ultra-n-fermatien et $-1 \in K^n$;*

(ii) *K est $(X^n - T)$-réduisant;*

(iii) *K contient les racines n-ièmes de l'unité et $K = K^n$;*

(iv) *K contient les racines n-ièmes de l'unité et l'application $x \mapsto x^n$ est une surjection de K sur lui-même.*

Preuve. (i) $\Rightarrow$ (iii). Par le lemme 1, on sait déjà que K contient les racines n-ièmes de l'unité. Reste à montrer que $K = K^n$. Soit $\alpha \in K$; considérons pour $i = 0, ..., n$, les équations

$$(E_i) \qquad (\alpha + i)^n = \sum_{k=0}^{n} C_n^k i^{n-k} \alpha^k.$$

On regarde ces équations comme un système linéaire, d'inconnues α^k. Considérons alors les deux déterminants suivants:

$$\Delta = \begin{vmatrix} C_n^0 0^n & C_n^1 0^{n-1} & C_n^2 0^{n-2} & \cdots & \cdots & 1 \\ C_n^0 1^n & C_n^1 1^{n-1} & C_n^2 1^{n-2} & \cdots & \cdots & C_n^n 1^0 \\ C_n^0 2^n & C_n^1 2^{n-1} & C_n^2 2^{n-2} & \cdots & \cdots & C_n^n 2^0 \\ \vdots & & & & & \vdots \\ \vdots & & & & & \vdots \\ C_n^0 n^n & C_n^1 n^{n-1} & C_n^2 n^{n-2} & \cdots & \cdots & C_n^n n^0 \end{vmatrix}$$

et

$$\Sigma = \begin{vmatrix} C_n^0 0^n & (\alpha+0)^n & C_n^2 0^{n-2} & \cdots & \cdots & 1 \\ C_n^0 1^n & (\alpha+1)^n & C_n^2 1^{n-2} & \cdots & \cdots & C_n^n 1^0 \\ C_n^0 2^n & (\alpha+2)^n & C_n^2 2^{n-2} & \cdots & \cdots & C_n^n 2^0 \\ \vdots & & & & & \vdots \\ \vdots & & & & & \vdots \\ C_n^0 n^n & (\alpha+n)^n & C_n^2 n^{n-2} & \cdots & \cdots & C_n^n n^0 \end{vmatrix}$$

Puisque K est n-fermatien et que -1 est une puissance n-ième dans K, toute somme (resp. différence, resp. produit, resp. rapport) d'éléments de K^n est encore dans K^n. Ainsi, tout déterminant à coefficients dans K^n est

élément de K^n. En remarquant que, pour tout entier $m \in \mathbb{N}$, on a $m = 1^n + \cdots + 1^n$ (m fois), on voit immédiatement que $\mathbb{N} \subset K^n$ et que, par suite Δ et Σ sont dans K^n. Maintenant, $\Delta = (-1)^{n+1} V(1, ..., n) \prod_{k=0}^{n} C_n^k$ où $V(1, ..., n)$ est le déterminant de Vandermonde associé au n-uplet $(1, ..., n)$. Ainsi, $V \neq 0$ et en appliquant la règle de Cramer, on trouve

$$\alpha = \frac{\Sigma}{\Delta} \in K^n$$

par suite $K = K^n$. Notons au passage que cette méthode nous permet de trouver des formules explicites pour écrire un élément de K comme somme de puissances n-ièmes. Par exemple, pour:

- $n = 2$, on a

$$\alpha = (\alpha + 1)^2 + \left(i\left(\frac{\alpha}{2} + 1\right)\right)^2 + \left(i\frac{\sqrt{3}}{2}\alpha\right)^2$$

(qui n'est pas la formule la plus simple car il est bien connu que $\alpha = (\frac{\alpha+1}{2})^2 + (i\frac{\alpha-1}{2})^2$).

- $n = 3$, on a

$$\alpha = \left(\frac{-\alpha - 3}{\sqrt[3]{18}}\right)^3 + (\sqrt[3]{2/9}\,(\alpha + 2))^3 + (-\sqrt[3]{5/18}\,(\alpha + 1))^3 + \left(\frac{\alpha}{\sqrt[3]{9}}\right)^3.$$

(iii) $\Rightarrow$ (iv). Immédiat.

(iv) $\Rightarrow$ (ii). Soit $t \in K$; d'après le (iv), il existe $x \in K$ tel que $t = x^n$. Les racines de $X^n - t$ sont alors les $\xi_n x$, où ξ_n décrit l'ensemble des racines n-ièmes de l'unité (qui sont dans K par hypothèse). Donc $X^n - t$ est totalement décomposé dans K.

(ii) $\Rightarrow$ (i). Soient t_1, $t_2 \in K$; posons $t = t_1^n + t_2^n$. Par hypothèse, le polynôme $X^n - t_1^n - t_2^n = X^n - t$ est complètement décomposé dans K, donc K est $(X^n - T_1^n - T_2^n)$-réduisant. Le choix $t = -1$, montre que $-1 \in K^n$. ∎

COROLLAIRE 1. • *Soient $m > 1$ et $n > 1$ deux entiers tels que m divise n. Si un corps K est ultra-n-fermatien et si $-1 \in K^n$ alors K est ultra-m-fermatien et $-1 \in K^m$.*

• *Soit $n > 1$ un entier naturel et $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. Il y a équivalence entre les propositions suivantes:*

(i) *K est ultra-n-fermatien et $-1 \in K^n$,*

(ii) *pour tout $i = 1, ..., r$, K est ultra-$p_i^{\alpha_i}$-fermatien et $-1 \in K^{p_i^{\alpha_i}}$*

(iii) *pour tout* $i=1, ..., r$ *et tout* $\beta_i \geqslant 1$, K *est ultra-*$p_i^{\beta_i}$*-fermatien et* $-1 \in K^{p_i^{\beta_i}}$.

Preuve. • D'après le théorème 2, on a $K=K^n$ et $\xi_n \in K$ (où ξ_n désigne une racine primitive n-ième de l'unité). Si $n=am$ avec $a \in \mathbb{N}$, alors $K^a \subset K$ donc $K=K^n=K^{am} \subset K^m$ et par suite $K=K^m$. De plus, $\xi_m=\xi_n^a \in K$ est une racine primitive m-ième de l'unité; donc K est ultra-m-fermatien et $-1 \in K^m$.

• (i) $\Rightarrow$ (iii). D'après le théorème 2, on a $K=K^n$ et $\xi_n \in K$ (où ξ_n désigne une racine primitive n-ième de l'unité). Soit p un nombre premier divisant n. On a $K=(K^{n/p})^p \subset K^p$, donc $K=K^p$. Par récurrence, on obtient $K=K^{p^\alpha}$ pour tout $\alpha \in \mathbb{N}$. La racine $\xi_p=\xi_n^{n/p}$ est primitive p-ième de l'unité, mais comme $\xi_p \in K=K^p$, il existe $\xi_{p^2} \in K$ tel que $\xi_{p^2}^p=\xi_p$. La racine ξ_{p^2} est alors primitive p^2-ième de l'unité. Par récurrence, on en déduit que, pour tout $\alpha \in \mathbb{N}$, K contient une racine primitive p^α-ième de l'unité. Le théorème 2 assure alors que K est ultra-p^α-fermation et que $-1 \in K^{p^\alpha}$.

(iii) $\Rightarrow$ (ii). Immédiat.

(ii) $\Rightarrow$ (i). D'après le théorème 2, on a pour tout $i=1, ..., r$, $K=K^{p_i^{\alpha_i}}$ et $\xi_{p_i^{\alpha_i}} \in K$ (où $\xi_{p_i^{\alpha_i}}$ désigne une racine primitive $p_i^{\alpha_i}$-ième de l'unité). Comme $K=K^{p_1^{\alpha_1}}=(K^{p_1^{\alpha_1}})^{p_2^{\alpha_2}}=K^{p_1^{\alpha_1}p_2^{\alpha_2}}$, on voit, par récurrence, que $K=K^{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}=K^n$. Maintenant, la racine $\xi_n=\xi_{p_i^{\alpha_n}}\cdots\xi_{p_i^{\alpha_n}} \in K$ est primitive n-ième de l'unité; on en déduit par le théorème 2 que K est ultra-n-fermation et que $-1 \in K^n$. ∎

Ce corollaire va nous permettre de caractériser les corps ultra-n-fermatiens en regardant leurs extensions cycliques (ce qui constitue, en quelque sorte, l'analogue du théorème de Diller et Dress pour les corps ultra-n-fermatiens):

THÉORÈME 3. *Soient* K *un corps et* $n>1$ *un entier naturel. Il y a équivalence entre les propositions suivantes*:

(i) K *est ultra-n-fermatien et* $-1 \in K^n$;

(ii) *Pour tout nombre premier* p *divisant* n, K *contient les racines* p*-ièmes de l'unité et, pour tout entier* $\alpha \in \mathbb{N}/\{0\}$, K *ne possède pas d'extension cyclique de degré* p^α.

Preuve. *non*(ii) $\Rightarrow$ *non*(i). Supposons que K contienne les racins n-ièmes de l'unité (sinon, d'après le théorème 2 on a *non*(i) immédiatement). En particulier, K contient les racines p-ièmes de l'unité pour tout premier p divisant n. Soient p un nombre premier divisant n, α un entier non nul et L/K une extension cyclique de degré p^α. Quitte à considérer une sous-extension de L/K, on peut supposer que $\alpha=1$. Comme K contient les racines

p-ièmes de l'unité, L/K est kummérienne et par suite, il existe $\omega \in K$ tel que $L = K(\sqrt[p]{\omega})$. En particulier, $K \neq K^p$, ce qui signifie, d'après le théorème 2 que K n'est pas ultra-p-fermatien ou que $-1 \notin K^p$. Dans ce cas, d'après le corollaire 1, K n'est pas ultra-n-fermatien ou $-1 \notin K^n$.

non(i) $\Rightarrow$ *non*(ii). Supposons que K contienne une racine primitive p-ième de l'unité, ξ_p, pour tout p premier divisant n. D'après le corollaire 1, il existe p divisant n et $\alpha \in \mathbb{N}/\{0\}$ tels que K ne soit pas ultra-p^α-fermatien ou $-1 \notin K^{p^\alpha}$.

Si $-1 \notin K^{p^\alpha}$, alors $p = 2$ et donc $-1 \notin K^2$. L'extension $K(\sqrt{-1})/K$ est cyclique de degré 2. Supposons maintenant que $-1 \notin K^{p^\alpha}$; K n'est donc pas ultra-p^α-fermatien et comme $-1 \in K^p$, par le corollaire 1, K n'est pas ultra-p-fermatien. Comme $\xi_p \in K$, on a $K \neq K^p$. Soit alors $\omega \in K/K^p$; l'extension $K(\sqrt[p]{\omega})/K$ est cyclique (c'est une extension kummérienne) et elle est de degré p. En effet, $\sqrt[p]{\omega}$ annule le polynôme $X^p - \omega$; il suffit donc de vérifier que ce dernier est irréductible sur K. Soir ξ_p une racine primitive p-ième de l'unité. Dans $\bar{K}[X]$ on a $X^p - \omega = \prod_{k=1}^{p} (X - \xi_p^k \sqrt[p]{\omega})$; si $H(X) \in K[X]$ divise $X^p - \omega$ dans $K[X]$, alors son terme constant est de la forme $\xi_p^r \omega^{s/p}$ avec $s \leqslant p$. Supposons que $s \neq 0$, p, alors, comme p est premier, s est premier avec p et d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $up + vs = 1$. Mais alors $\omega^{(u+vs/p)} = \omega^{1/p} \in K$, ce qui est absurde. ∎

On obtient alors comme corollaire, cette propriété analogue à celle des corps pythagoriciens:

COROLLAIRE 2. *Soient $n \in \mathbb{N}/\{0\}$, L un corps ultra-n-fermatien et K un sous-corps de L. On suppose que*

- $-1 \in K^{n^2}$,
- *K contient les racines n^2-ièmes de l'unité.*

Alors, si $[L : K] < +\infty$, le corps K est ultra-n-fermatien.

Preuve. Supposons que K ne soit pas ultra-n-fermatien et considérons alors deux corps K_1 et L_1 tels que:

- $K \subset K_1 \subset L_1 \subset L$,
- L_1/K_1 ne possède aucune extension intermédiaire,
- L_1 soit ultra-n-fermatien et K_1 non ultra-n-fermatien.

(Un tel couple de corps (K_1, L_1) existe bien car l'extension L/K étant séparable, elle possède un nombre fini d'extensions intermédiaires).

Par hypothèse, $-1 \in K_1^n$ et K_1 contient les racines n-ièmes de l'unité, donc d'après le théorème 3, il existe un nombre premier p divisant n et un entier $\alpha \in \mathbb{N}/\{0\}$ tel que K_1 possède une extension cyclique de degré p^α, donc en particulier une extension cyclique de degré p. Mais K_1 ne peut pas posséder d'extension cyclique de degré p^2 car, comme K_1 contient les racines p^2-ièmes de l'unité, une telle extension serait kummérienne et il existerait $\omega \in K_1/K_1^{p^2}$ tel que $K_1(\sqrt[p^2]{\omega})$ soit cyclique de degré p^2. Alors comme $\omega \in L_1$ et que $L_1^{p^2} = L_1$ (théorème 2) on aurait $K_1(\sqrt[p^2]{\omega}) \subset L_1$ et il existerait une extension intermédiaire à l'extension L_1/K_1, ce qui est absurde.

On en déduit donc que, pour tout $\omega \in K_1$, le polynôme $X^{p^2} - \omega$ est réductible dans $K_1[X]$. Soit ξ_{p^2} une racine primitive p^2-ième de l'unité; en écrivant:

$$X^{p^2} - \omega = \prod_{k=1}^{p^2} (X - \xi_{p^2}^k \sqrt[p^2]{\omega})$$

on en déduit qu'il existe un entier m tel que $0 < m < p^2$ et $\omega^{m/p^2} \in K_1$ (c'est le coefficient constant, à une racine p^2-ième de l'unité près, d'un polynôme de $K_1[X]$ divisant $X^{p^2} - \omega$). Si $m = p$, alors $\sqrt[p]{\omega} \in K_1$. Si $m \neq p$, alors m est premier avec p^2 et, par Bézout, il existe des entiers rationnels u et v tels que $up^2 + vm = 1$. On en déduit que $\omega^{1/p^2} = \omega^{u + vm/p^2} \in K_1$ et, par suite, que $\sqrt[p]{\omega} \in K_1$. Ainsi $K_1 = K_1^p$ et comme K_1 contient les racines p-ièmes de l'unité, K_1 n'a pas d'extension cyclique de degré p (car elle serait kummérienne), ce qui est absurde. ∎

Notons que le corollaire précédent n'a aucune chance de rester vrai si l'on ne prend pas quelques précautions sur l'existence de racines de l'unité dans K (penser à $\mathbb{R}$ et $\mathbb{C}$ par exemple). Pour finir, intéressons-nous à la clôture ultra-n-fermatienne d'un corps K (i.e. la clôture P-réduisante de K pour $P = X^n - T_1^n - T_2^n$) que nous noterons K_n^{u-ferm}:

THÉORÈME 4. *Soient $n \in \mathbb{N}/\{0\}$ et K un corps hilbertien. Alors $[K_n^{u-ferm} : K] = +\infty$ et aucune extension finie stricte de K_n^{u-ferm} n'est ultra-n-fermatienne.*

Preuve. Le polynôme $X^n - T_1^n - T_2^n$ est visiblement absolument irréductible dans $\mathbb{Q}(T_1, T_2)[X]$, donc reste irréductible sur tout corps de caractéristique 0. Si $[K_n^{u-ferm} : K] < +\infty$, alors K_n^{u-ferm} est hilbertien ce qui est en contradiction avec le fait que $X^n - T_1^n - T_2^n$ se décompose pour tout spécialisation $T_1 = t_1 \in K$, $T_2 = t_2 \in K$. Le fait qu'aucune extension finie stricte de K_n^{u-ferm} ne soit ultra-n-fermatienne vient immédiatement du théorème 1. ∎

Ribenboim avait déjà montré ce résultat dans le cas des corps de nombres. Remarquons que le corollaire 2 permet de donner un autre catégorie de corps K tels que $[K_n^{u-ferm} : K] = +\infty$. On a en effet:

PROPOSITION 1. *Soient $n \in \mathbb{N}/\{0\}$ et K un corps. On suppose que*

- $-1 \in K^{n^2}$,
- *K contient les racines n^2-ièmes de l'unité.*

Alors, si K n'est pas ultra-n-fermatien, $[K_n^{u-ferm} : K] = +\infty$.

On obtient alors une structure pour $Gal(K_p^{u-ferm}/K)$ analogue à celle, de $Gal(K^{pyth}/K)$ présentée dans l'introduction:

THÉORÈME 5. *Soient p un nombre premier impair et K un corps contenant une racine primitive p^2-ième de l'unité. Le groupe de Galois de l'extension K_p^{u-ferm}/K est un pro-p-groupe sans torsion.*

Preuve. Le groupe $Gal(K_p^{u-ferm}/K)$ est clairement sans torsion (c'est la traduction du corollaire 2, la condition $-1 \in K^{p^2}$ étant immédiatement vérifiée). Dans un corps M contenant les racines p-ièmes de l'unité, un polynôme $X^p - \alpha$ est, soit irréductible, soit totalement décomposé (même argument que dans la preuve du théorème 3). Considérons alors les corps L tels qu'il existe une suite finie $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ telle que pour tout $i = 0, \ldots, n-1$, $K_{i+1} = K_i(\sqrt[p]{\alpha^2 + \beta^p})$ pour un certain couple $\alpha, \beta \in K_i$. L'extension L/K est finie et galoisienne, son groupe de Galois est visiblement un p-groupe et comme K_p^{u-ferm} est la limite inductive de ces extensions L/K (par la construction de la clôture P-réduisante vue au paragraphe 2), on en déduit que $Gal(K_p^{u-ferm}/K)$ est la limite projective de p-groupes, c'est-à-dire un pro-p-groupe. ∎

RÉFÉRENCES

[DeDe] P. Dèbes et B. Deschamps, The inverse Galois problem over large fields, *dans* "Geometric Galois Action, II" London Math. Soc., Lecture Note Ser., Vol. 243, pp. 119–138, Cambridge Univ. Press, Cambridge, UK, 1997.

[Des1] B. Deschamps, "Problème d'arithmétique des corps et de théorie de Galois," Hermann, Paris, 1998.

[Des2] B. Deschamps, Clôture totalement réelle des corps de nombres ordonnables, *Manuscripta Math.* **100** (1999), 291–304.

[Des3] B. Deschamps, "Aspects de la théorie inverse de Galois," thèse de doctorat, Université Lille, 1997.

[DD] J. Diller et A. Dress, Zur Galoistheorie pythagoreischer Körper, *Ach. Math.* (1965), 148–152.

[DH] P. Dèbes et D. Haran, Almost Hilbertian fields, *Acta Arith.* **83** (1999), 269–287.

[FJ] M. Fried et M. Jarden, "Field Arithmetic," Springer-Verlag, New York, 1986.
[Rib1] P. Ribenboim, "Arithmétique des Corps," Hermann, Paris, 1973.
[Rib2] P. Ribenboim, Pythagorean and Fermatian fields, *Ist. Naz. Atta Mat. Sympos. Math.* **15** (1975), 583–593.
[Rib3] P. Ribenboim, Polynomials whose values are powers, *J. Reine Angew. Math.* **268–269** (1974), 34–40.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium