(ii) For each n we consider the circle $x^2+y^2=R_n^2$ where

$$R_n^2 = 16n^6+4n^4+4n^2+1.$$

We can see that

$$\begin{aligned}16n^6+4n^4+4n^2+1 &= (4n^3-1)^2+(2n^2+2n)^2\\ &= (4n^3)^2+(2n^2+1)^2 = (4n^3+1)^2+(2n^2-2n)^2.\end{aligned}$$

The three lattice points

$$(4n^3-1,\ 2n^2+2n),\quad (4n^3,\ 2n^2+1),\quad (4n^3+1,\ 2n^2-2n)$$

are on an arc of length

$$R_n\left\{\arctan\frac{2n^2+2n}{4n^3-1}-\arctan\frac{2n^2-2n}{4n^3+1}\right\} = R_n\arctan\frac{16n^4+4n^2}{16n^6+4n^4-4n^2-1}$$
$$= 2\sqrt[3]{2}R_n^{1/3}+o(1)$$

and the theorem follows.

References

[1] J. Cilleruelo and A. Córdoba, *Trigonometric polynomials and lattice points*, Proc. Amer. Math. Soc., to appear.

[2] A. Zygmund, *A Cantor–Lebesgue theorem for double trigonometric series*, Studia Math. 43 (1972), 173–178.

DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE MADRID
28049 Madrid, España

Received on 17.5.1990
and in revised form on 27.7.1990 (2048)

ACTA ARITHMETICA
LIX.1 (1991)

Sur une classe d'extensions non ramifiées

par

A. MOVAHHEDI (Limoges)

Soient K un corps de nombres, θ un élément primitif de K sur $\boldsymbol{Q}$: $K=\boldsymbol{Q}(\theta)$. Notons φ le polynôme minimal de θ sur $\boldsymbol{Q}$. Supposons que le corps L de décomposition de φ soit une S_n-extension (1) de $\boldsymbol{Q}$. Alors Elstrodt, Grunewald et Mennicke [1] ont montré que si le discriminant $D(\varphi)$ du polynôme φ est sans facteur carré, la A_n-extension (2) $L/\boldsymbol{Q}(\sqrt{D(\varphi)})$ est non ramifiée en toutes les places finies. Yamamura [7] et Osada [4] ont généralisé ce résultat en montrant que la condition "le groupe de Galois $G(L/\boldsymbol{Q})$ est S_n" est une conséquence de l'hypothèse "$D(\varphi)$ est sans facteur carré". Enfin Nakagawa [3] a obtenu le même résultat en remplaçant l'hypothèse "$D(\varphi)$ est sans facteur carré" par l'hypothèse moins forte "le discriminant $D_{K/\boldsymbol{Q}}$ de l'extension $K/\boldsymbol{Q}$ est sans facteur carré", en retrouvant ainsi un théorème de Scholz [5] datant de 1937. Notre but est de généraliser ce résultat. Nous remarquons en particulier que, contrairement à ce que pourraient laisser penser les articles cités ci-dessus, le problème de la non-ramification de $L/\boldsymbol{Q}(\sqrt{D(\varphi)})$ est largement indépendant du groupe de Galois de $L/\boldsymbol{Q}$.

L'auteur remercie F. Laubie pour son aide dans la réalisation de ce travail.

Fixons d'abord quelques notations. Soient k un corps de nombres et K une extension finie de k de degré n. Soit $\{b_i\}_{1\leqslant i\leqslant n}$ une base de K/k. Le discriminant de cette base est un élément non nul de k dont la classe modulo k^{*2} est indépendante du choix de la base choisie. Ceci nous fournit donc une extension quadratique ou triviale F de k contenue dans la clôture normale L de K sur k.

Pour un idéal premier $\mathfrak{q}$ de K, on écrit $\mathfrak{q}=\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g}$ la décomposition de $\mathfrak{q}$ en produit de puissance d'idéaux premiers $\mathfrak{p}_i$ de K deux à deux distincts. On note f_i le degré résiduel de $\mathfrak{p}_i$ de sorte qu'on a $n=\sum_{i=1}^{g}e_if_i$.

THÉORÈME 1. *Supposons $F\neq k$ et $\mathfrak{q}$ ramifié dans K/k.*

1) *Dans le cas où $\mathfrak{q}$ ne divise pas 2, pour que l'extension L/F soit non*

(1) Par S_n-extension nous entendons une extension galoisienne dont le groupe de Galois est le groupe symétrique S_n de degré n.

(2) A_n est le sous-groupe alterné de S_n.

ramifiée en $\mathfrak{q}$ *il faut et il suffit que la valuation* $\mathfrak{q}$*-adique* $v_{\mathfrak{q}}(D_{K/k})$ *du discriminant* $D_{K/k}$ *soit un entier impair égal à la somme* $\sum_{e_i pair} f_i$.

2) *Dans le cas où* $\mathfrak{q}$ *divise* 2, *et où* $v_{\mathfrak{q}}(D_{K/k})$ *est un entier impair, pour que l'extension* L/F *soit non ramifiée en* $\mathfrak{q}$ *il faut qu'on ait*

$$v_{\mathfrak{q}}(D_{K/k}) = (2v_{\mathfrak{q}}(2)+1)\sum_{e_i pair} f_i.$$

(*Cette condition étant également suffisante lorsque* K *contient* F.)

Démonstration. L'extension L/F est non ramifiée en $\mathfrak{q}$ si et seulement s'il en est de même de l'extension KF/F. En effet, dans le cas $F \not\subset K$, le corps L est la clôture normale de KF sur F; et dans le cas contraire ($F \subset K$), F est contenu dans chaque conjugué K' de K sur k et les extensions K'/F et K/F sont ramifiées ou non ramifiées simultanément.

Supposons que $v_{\mathfrak{q}}(D_{K/k})$ soit un entier impair. Le corps F peut alors s'écrire $F = K(\sqrt{\delta})$, où δ est un élément sans facteur carré de K de valuation $\mathfrak{q}$-adique 1. Notons $\mathfrak{p}$ l'idéal premier de F au-dessus de $\mathfrak{q}$. Nous avons $\mathfrak{q} = \mathfrak{p}^2$ dans F. L'anneau des entiers du complété de F en $\mathfrak{p}$, considéré comme algèbre sur l'anneau des entiers du complété de k en $\mathfrak{q}$, est engendré par $\sqrt{\delta}$ ([6], ch. III, § 6, lemme 3). D'où

$$v_{\mathfrak{q}}(D_{F/k}) = v_{\mathfrak{q}}(4\delta) = 2v_{\mathfrak{q}}(2)+1.$$

Considérons d'abord le cas $F \not\subset K$. Supposons que l'extension KF/F soit non ramifiée en $\mathfrak{q}$. Alors chaque e_i est inférieur ou égal à 2, et de plus les idéaux premiers $\mathfrak{p}_i$ de K au-dessus de $\mathfrak{q}$ pour lesquels e_i vaut 2 ne se ramifient pas dans le composé KF. Donc les $\mathfrak{p}_i$ avec $e_i = 1$ sont exactement les diviseurs de $\mathfrak{q}$ qui se ramifient dans KF/K. D'où

$$v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) = \sum_{e_i=1} f_i v_{\mathfrak{p}_i}(D_{KF/K}),$$

où $N_{K/k}$ désigne la norme relative de l'extension K/k. Or, pour tout i avec $e_i = 1$, nous avons

$$v_{\mathfrak{p}_i}(D_{KF/K}) = 2v_{\mathfrak{p}_i}(2)+1 = 2v_{\mathfrak{q}}(2)+1$$

comme pour l'extension F/k, d'où

$$v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) = \sum_{e_i=1} (2v_{\mathfrak{q}}(2)+1) f_i.$$

D'autre part la formule de transitivité du discriminant ([6], ch. III, § 4, prop. 8) nous donne

$$v_{\mathfrak{q}}(N_{F/k}(D_{KF/F})) + v_{\mathfrak{q}}(D_{F/k}^n) = v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) + v_{\mathfrak{q}}(D_{K/k}^2),$$

soit

$$n(2v_{\mathfrak{q}}(2)+1) = \sum_{e_i=1} (2v_{\mathfrak{q}}(2)+1) f_i + 2v_{\mathfrak{q}}(D_{K/k}),$$

soit encore

$$2v_{\mathfrak{q}}(D_{K/k}) = (2v_{\mathfrak{q}}(2)+1)(n - \sum_{e_i=1} f_i) = (2v_{\mathfrak{q}}(2)+1) \sum_{e_i=2} 2f_i.$$

Finalement on obtient

$$v_{\mathfrak{q}}(D_{K/k}) = (2v_{\mathfrak{q}}(2)+1) \sum_{e_i \text{ pair}} f_i.$$

Réciproquement, supposons que $v_{\mathfrak{q}}(D_{K/k})$ soit un entier impair égal à $\sum_{e_i \text{pair}} f_i$, et que $\mathfrak{q}$ ne divise pas 2. Partons de l'inégalité $n \geqslant \sum_{e_i \text{impair}} f_i + 2\sum_{e_i \text{pair}} f_i$. Par la théorie de Kummer les idéaux $\mathfrak{p}_i$ de K au-dessus de $\mathfrak{q}$ qui se ramifient dans l'extension quadratique KF/K sont exactement ceux dont l'indice de ramification e_i est impair. D'où $v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) = \sum_{e_i \text{impair}} f_i$. L'inégalité précédente s'écrit donc $n \geqslant v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) + 2v_{\mathfrak{q}}(D_{K/k})$. Comme de plus $v_{\mathfrak{q}}(D_{K/k})$ est supposé impair, on a $v_{\mathfrak{q}}(D_{F/k}) = 1$. Ainsi en appliquant deux fois la formule de transitivité du discriminant on obtient

$$v_{\mathfrak{q}}(N_{F/k}(D_{KF/F})) = v_{\mathfrak{q}}(N_{K/k}(D_{KF/K})) + v_{\mathfrak{q}}(D_{K/k}^2) - v_{\mathfrak{q}}(D_{F/k}^n) \leqslant 0,$$

ce qui signifie bien que KF/F est non ramifiée en $\mathfrak{q}$.

Considérons maintenant le cas $F \subset K$. Comme $\mathfrak{q}$ divise $D_{K/k}$, pour que l'extension K/F soit non ramifiée en $\mathfrak{q}$ il faut et il suffit que $\mathfrak{q}$ se ramifie dans F, et que pour tout i, on ait $e_i = 2$. Si $\mathfrak{q}$ ne divise pas 2, cette dernière condition équivaut à $v_{\mathfrak{q}}(D_{K/k})$ est un entier impair égal à $\sum_{e_i \text{pair}} f_i$. Si $\mathfrak{q}$ divise 2, alors puisque par hypothèse $v_{\mathfrak{q}}(D_{K/k})$ est impair, $v_{\mathfrak{q}}(D_{F/k}) = 2v_{\mathfrak{q}}(2)+1$. Donc pour que K/F soit non ramifiée en $\mathfrak{q}$ il faut et il suffit que l'on ait

$$v_{\mathfrak{q}}(D_{K/k}) = \frac{n}{2} v_{\mathfrak{q}}(D_{F/k}) = (2v_{\mathfrak{q}}(2)+1) \sum_{e_i \text{pair}} f_i.$$

Exemple. Soient $k = \boldsymbol{Q}(\sqrt{79})$ et $K = H(\theta)$, où H est le corps de classes de Hilbert de k, et où θ est une racine du polynôme $X^3 + X + 1$. Alors $D_{K/k} = \mathfrak{q}^3$, où $\mathfrak{q}$ est l'idéal premier de k au-dessus de 31. De plus, la décomposition de $\mathfrak{q}$ dans K est donnée par $\mathfrak{q} = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$ avec $f_i = 1$ pour $i = 1, 2, 3, \ldots, 6$. Ainsi la clôture normale $L = k(\sqrt{-31})$ de K sur k est une extension abélienne non ramifiée de $F = k(\sqrt{-31})$ de degré 9.

Indépendamment du résultat précédent concernant la non ramification de l'extension L/F, on peut se demander s'il existe des conditions suffisantes portant sur le discriminant $D_{K/k}$ pour que le groupe de Galois $G(L/k)$ soit le groupe symétrique S_n tout entier.

Théorème 2. *Supposons qu'il n'y a pas de corps entre* K *et* k, *et qu'il existe un idéal premier* $\mathfrak{q}$ *de* K *verifiant* $v_{\mathfrak{q}}(D_{K/k}) = 1$. *Alors le groupe de Galois* $G(L/k)$ *est égal à* S_n.

Démonstration. Soit θ un élément primitif de K sur k: $K = k(\theta)$. Désignons par $\varphi(X)$ le polynôme minimal de θ sur k. Soient $\theta_1 = \theta, \theta_2, \ldots, \theta_n$

les conjugués de θ sur k: $L = k(\theta_1, \ldots, \theta_n)$. Le groupe de Galois $G = G(L/k)$ est ainsi un groupe de permutations transitif de degré n. Soit $\mathfrak{P}$ un idéal premier de L ramifié dans L/k. Notons $\mathfrak{p}$ (resp. $\mathfrak{q}$) la trace de cet idéal premier sur K (resp. k): $\mathfrak{p} = \mathfrak{P} \cap K$ et $\mathfrak{q} = \mathfrak{P} \cap k$. Si $v_{\mathfrak{q}}(D_{K/k}) = 1$, alors la décomposition de $\mathfrak{q}$ en produit d'idéaux premiers (deux à deux distincts) de K est de la forme $\mathfrak{q} = \mathfrak{p}_1^2 \mathfrak{p}_2 \ldots \mathfrak{p}_g$. Quitte à remplacer $\mathfrak{P}$ par l'un de ses conjugués on peut supposer que $\mathfrak{p}_1 = \mathfrak{p}$. Chacun des $\mathfrak{p}_i$ correspond à un facteur irréductible du polynôme $\varphi(X)$ regardé dans l'anneau $k_{\mathfrak{q}}[X]$: $\varphi(X) = \varphi_1(X)\varphi_2(X) \ldots \varphi_g(X)$. où $\varphi_1(X)$ est le polynôme minimal de $\theta \in K_{\mathfrak{p}_1}$ sur $k_{\mathfrak{q}}$. Comme les $\varphi_i(X)$ pour $i \geqslant 2$ fournissent des extensions non ramifiées de $k_{\mathfrak{q}}$, le groupe d'inertie de $\mathfrak{P}$ dans L/k est un groupe d'ordre deux (=degré de $\varphi_1(X)$) engendré par la transposition définie par les deux racines du polynôme $\varphi_1(X)$. Nous venons ainsi de voir que sous l'hypothèse $v_{\mathfrak{q}}(D_{K/k}) = 1$, le groupe de Galois $G(L/k)$ contient une transposition.

Par ailleurs, l'hypothèse "Il n'y a pas de corps entre K et k" équivaut à "le groupe $G(L/K)$ d'isotropie de θ dans G est un sous-groupe maximal de G". Or G étant transitif, cette dernière propriété équivaut à la primitivité de G. Ainsi, sous les hypothèses du théorème 2, le groupe G est un groupe primitif contenant une transposition. Le théorème 2 découle alors du résultat suivant dû à C. Jordan ([2], Théorèmes sur les groupes primitifs, pp. 285–286):

Soit G un groupe primitif de degré n. Si G contient une transposition, alors G est le groupe symétrique S_n tout entier.

EXEMPLES. 1. Soient $n \leqslant p$ deux nombres premiers. Alors le groupe de Galois du polynôme $\varphi(X) = X^n + X^2 + p$ est le groupe symétrique S_n. En effet, le discriminant du polynôme φ est $D(\varphi) = (-1)^{(n-1)/2} p\,(n^n p^{n-2} + 4(n-2)^{n-2})$, de sorte que $v_p(D(\varphi)) = 1$. Comme de plus φ est un polynôme irréductible de degré premier, le théorème précédent s'applique.

2. Soit $\varphi(X) = X^{2n} + X^2 + p$, où p est un nombre premier impair ne divisant pas $n-1$. Alors φ est un polynôme irréductible de discriminant $D(\varphi) = (-1)^n 2^{2n} p\,[n^n p^{n-1} + (-1)^{n-1}(n-1)^{n-1}]^2$. Donc $v_p(D(\varphi)) = 1$. Cet exemple montre que dans le théorème précédent la condition $v_{\mathfrak{q}}(D_K) = 1$, pour un idéal premier $\mathfrak{q}$ de k, n'entraîne pas qu'il n'y a pas de corps entre K et k.

3. Soit $\varphi(X) = X^5 - 10X^3 - 5X^2 + 5X - 1$. Alors $\varphi(X)$ est un polynôme irréductible sur $\boldsymbol{Q}$ avec $D(\varphi) = 2^2 5^5 17^2$. Soit $K := \boldsymbol{Q}(\theta)$ où θ est une racine de φ. Alors 5 se ramifie totalement dans K, de sorte que $v_5(D_{K/\boldsymbol{Q}}) = 5$. Par ailleurs, puisque $\varphi(X)$ est, modulo 11, le produit de deux polynômes irréductibles de degré 2 et 3 respectivement: $\varphi(X) \equiv (X^2+9)(X^3+3X+6)$, le groupe de Galois de φ est le groupe symétrique S_5. Cet exemple montre que la réciproque du théorème 2 est fausse.

En combinant les résultat précédents, on obtient immédiatement le

THÉORÈME 3. *Supposons que*

(i) *Il n'y a pas de corps entre K et k.*

(ii) *Il existe $\mathfrak{q}$ idéal premier de k avec $v_{\mathfrak{q}}(D_{K/k}) = 1$.*

(iii) *$D_{K/k}$ est premier à 2 et pour tout idéal premier $\mathfrak{q}$ divisant $D_{K/k}$, $v_{\mathfrak{q}}(D_{K/k})$ est un entier impair égal à la somme $\sum_{e_i \text{pair}} f_i$.*

Alors, il vient $G(L/k) \simeq S_n$, et L/F est une A_n-extension non ramifiée en toutes les places finies.

EXEMPLE. Soit $k = \boldsymbol{Q}(\mu_5)$ le corps obtenu en adjoignant à $\boldsymbol{Q}$ les racines $5^{\text{èmes}}$ de l'unité. Soit $K = k(\theta)$ où θ est une racine du polynôme $\varphi(X) = X^7 + X^4 + 2X^3 + 2X^2 + X + 2$. Le discriminant $D_{K/k}$ de l'extension K/k est l'idéal de k engendré par l'entier $d = 3^3 \cdot 7 \cdot 241 \cdot 2447$. On voit sans difficulté que les hypothèses du théorème 3 sont vérifiées. Donc le groupe de Galois du corps L des racines du polynôme φ sur $\boldsymbol{Q}(\mu_5)$ est le groupe symétrique S_7, et L est une A_7-extension non ramifiée de $\boldsymbol{Q}(\mu_5, \sqrt{-d})$.

Du théorème précédent, on tire sans difficulté le corollaire suivant (dû à Scholz [5]):

COROLLAIRE. *Prenons $k = \boldsymbol{Q}$. Supposons que $D_{K/k}$ soit sans facteur carré. Alors il suit $G(L/k) \simeq S_n$, et L/F est une A_n-extension non ramifiée en les places finies.*

Références

[1] J. Elstrodt, F. Grunewald and J. Mennicke, *On unramified A_n-extensions of quadratic number fields*, Glasgow Math. J. 27(1985), 31–37.

[2] C. Jordan, *Oeuvres*, Tome I, Gauthier-Villars, Paris 1961.

[3] J. Nakagawa, *On the Galois group of a number field with square free discriminant*, Comment. Math. Univ. St. Paul 37(1)(1988), 95–98.

[4] H. Osada, *The Galois groups of the polynomials $X^n + aX^1 + b$*, J. Number Theory 25(1987), 230–238.

[5] A. Scholz, *Lösung der Aufgabe 208*, Jahresber. Deutsch. Math.-Verein. 47(1937), 47.

[6] J. P. Serre, *Corps locaux*, 2ème édition, Hermann, Paris 1968.

[7] K. Yamamura, *On unramified Galois extensions of real quadratic number fields*, Osaka J. Math. 23(1986), 471–478.

FACULTÉ DES SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
123, Av. Albert Thomas
87060 Limoges Cedex
France

Reçu le 6.6.1990 (2054)