Journal de Théorie des Nombres
de Bordeaux **17** (2005), 949–953

The cubics which are differences of two conjugates of an algebraic integer

par Toufik ZAIMI

Résumé. On montre qu'un entier algébrique cubique sur un corps de nombres K, de trace nulle est la différence de deux conjugués sur K d'un entier algébrique. On prouve aussi que si N est une extension cubique normale du corps des rationnels, alors tout entier de N de trace zéro est la différence de deux conjugués d'un entier de N si et seulement si la valuation 3−adique du discriminant de N est différente de 4.

Abstract. We show that a cubic algebraic integer over a number field K, with zero trace is a difference of two conjugates over K of an algebraic integer. We also prove that if N is a normal cubic extension of the field of rational numbers, then every integer of N with zero trace is a difference of two conjugates of an integer of N if and only if the 3−adic valuation of the discriminant of N is not 4.

1. Introduction

Let K be a number field, β an algebraic number with conjugates $\beta_1 = \beta, \beta_2, ..., \beta_d$ over K and $L = K(\beta_1, \beta_2, ..., \beta_d)$ the normal closure of the extension $K(\beta)/K$. In [2], Dubickas and Smyth have shown that β can be written $\beta = \alpha - \alpha'$, where α and α' are conjugates over K of an algebraic number, if and only if there is an element σ of the Galois group $G(L/K)$ of the extension L/K, of order n such that $\sum_{0\leq i\leq n-1} \sigma^i(\beta) = 0$. In this case $\beta = \alpha - \sigma(\alpha)$,where $\alpha = \sum_{0\leq i\leq n-1}(n-i-1)\sigma^i(\beta)/n$ is an element of L and the trace of β for the extension $K(\beta)/K$, namely $Tr_{K(\beta)/K}(\beta) = \beta_1 + \beta_2 + ... + \beta_d$, is 0. Furthermore, the condition on the trace of β to be 0 is also sufficient to express $\beta = \alpha - \alpha'$ with some α and α' conjugate over K of an algebraic number, when the extension $K(\beta)/K$ is normal (i. e. when $L = K(\beta)$) and its Galois group is cyclic (in this case we say that the extension $K(\beta)/K$ is cyclic) or when $d \leq 3$.

Manuscrit reçu le 20 décembre 2003.

Let D be a positive rational integer and $\mathcal{P}(D)$ the proposition : *For any number field K and for any algebraic integer β of degree $\leq D$ over K, if β is a difference of two conjugates over K of an algebraic number, then β is a difference of two conjugates over K of an algebraic integer.* In [1], Smyth asked whether $\mathcal{P}(D)$ is true for all values of D. It is clear that if $Tr_{K(\beta)/K}(\beta) = 0$ and $\beta \in \mathbb{Z}_K$,where $\mathbb{Z}_K$ is the ring of integers of K, then $\beta = 0 = 0 - 0$ and $\mathcal{P}(1)$ is true. For a quadratic extension $K(\beta)/K$, Dubickas showed that if $Tr_{K(\beta)/K}(\beta) = 0$, then β is a difference of two conjugates over K of an algebraic integer of degree ≤ 2 over $K(\beta)$ [1]. Hence, $\mathcal{P}(2)$ is true. In fact, Dubickas proved that if the minimal polynomial of the algebraic integer β over K, say $Irr(\beta, K)$, is of the form $P(x^m)$, where $P \in \mathbb{Z}_K[x]$ and m is a rational integer greater than 1, then β is a difference of two conjugates over K of an algebraic integer.

Consider now the assertion $\mathcal{P}_c(D)$: *For any number field K and for any algebraic integer β of degree $\leq D$ over K such that the extension $K(\beta)/K$ is cyclic, if $Tr_{K(\beta)/K}(\beta) = 0$, then β is a difference of two conjugates over K of an algebraic integer.*

The first aim of this note is to prove :

Theorem 1. *The assertions $\mathcal{P}(D)$ and $\mathcal{P}_c(D)$ are equivalent, and $\mathcal{P}(3)$ is true.*

Let $\mathbb{Q}$ be the field of rational numbers. In [5], the author showed that if the extension $N/\mathbb{Q}$ is normal with prime degree, then every integer of N with zero trace is a difference of two conjugates of an integer of N if and only if $Tr_{N/\mathbb{Q}}(\mathbb{Z}_N) = \mathbb{Z}_\mathbb{Q}$. It easy to check that if $N = \mathbb{Q}(\sqrt{m})$ is a quadratic field (m is a squarefree rational integer), then $Tr_{N/\mathbb{Q}}(\mathbb{Z}_N) = \mathbb{Z}_\mathbb{Q}$ if and only if $m \equiv 1[4]$. For the cubic fields we have :

Theorem 2. *Let N be a normal cubic extension of $\mathbb{Q}$. Then, every integer of N with zero trace is a difference of two conjugates of an integer of N if and only if the $3-$adic valuation of the discriminant of N is not 4.*

2. Proof of Theorem 1

First we prove that the propositions $\mathcal{P}(D)$ and $\mathcal{P}_c(D)$ are equivalent. It is clear that $\mathcal{P}(D)$ implies $\mathcal{P}_c(D)$, since by Hilbert's Theorem 90 [3] the condition $Tr_{K(\beta)/K}(\beta) = 0$ is sufficient to express $\beta = \alpha - \alpha'$ with some α and α' conjugate over K of an algebraic number. Conversely, let β be an algebraic integer of degree $\leq D$ over K and which is a difference of two conjugates over K of an algebraic number. By the above result of Dubickas and Smyth, and with the same notation, there is an element $\sigma \in G(L/K)$, of order n such that $\sum_{0\leq i \leq n-1} \sigma^i(\beta) = 0$. Let $< \sigma >$ be the cyclic subgroup of $G(L/K)$ generated by σ and $L^{<\sigma>} = \{x \in L, \sigma(x) = x\}$ the fixed field of $< \sigma >$. Then, $K \subset L^{<\sigma>} \subset L^{<\sigma>}(\beta) \subset L$, the degree of β over $L^{<\sigma>}$ is

$\leq D$ and by Artin's theorem [3], the Galois group of the normal extension $L/L^{<\sigma>}$ is $< \sigma >$. Hence, the extensions $L/L^{<\sigma>}$ and $L^{<\sigma>}(\beta)/L^{<\sigma>}$ are cyclic since their Galois groups are respectively $< \sigma >$ and a factor group of $< \sigma >$. Furthermore, the restrictions to the field $L^{<\sigma>}(\beta)$ of the elements of the group $< \sigma >$ belong to the Galois group of $L^{<\sigma>}(\beta)/L^{<\sigma>}$ and each element of $G(L^{<\sigma>}(\beta)/L^{<\sigma>})$ is a restriction of exactly d elements of the group $< \sigma >$, where d is the degree of $L/L^{<\sigma>}(\beta)$. It follows that

$$dTr_{L^{<\sigma>}(\beta)/L^{<\sigma>}}(\beta) = Tr_{L/L^{<\sigma>}}(\beta) = \sum_{0 \leq i \leq n-1} \sigma^i(\beta) = 0,$$

and β is a difference of two conjugates over $L^{<\sigma>}$ of an algebraic number. Assume now that $\mathcal{P}_c(D)$ is true. Then, β is difference of two conjugates over $L^{<\sigma>}$, and a fortiori over K, of an algebraic integer and so $\mathcal{P}(D)$ is true.

To prove that $\mathcal{P}(3)$ is true, it is sufficient to show that if β a cubic algebraic integer over a number field K with $Tr_{K(\beta)/K}(\beta) = 0$ and such that the extension $K(\beta)/K$ is cyclic, then β is a difference of two conjugates of an algebraic integer, since $\mathcal{P}(2)$ is true and the assertions $\mathcal{P}(3)$ and $\mathcal{P}_c(3)$ are equivalent. Let

$$Irr(\beta, K) = x^3 + px + q,$$

and let σ be a generator of $G(K(\beta)/K)$. Then, $p = Tr_{K(\beta)/K}(\beta\sigma(\beta))$ and the discriminant $disc(\beta)$ of the polynomial $Irr(\beta, K)$ satisfies

$$disc(\beta) = -4p^3 - 3^3q^2 = \delta^2,$$

where $\delta = (\beta - \sigma^2\beta)(\sigma\beta - \beta)(\sigma^2\beta - \sigma\beta) \in \mathbb{Z}_K$. Set $\gamma = \beta - \sigma^2(\beta)$. Then, γ is of degree 3 over K and

$$Irr(\gamma, K) = x^3 + 3px - \delta.$$

As the polynomial $-27t + x^3 + 3px - 26\delta$ is irreducible in the ring $K(\beta)[t, x]$, by Hilbert's irreducibility theorem [4], there is a rational integer s such that the polynomial $x^3 + 3px - (26\delta + 27s)$ is irreducible in $K(\beta)[x]$. Hence, if $\theta^3 + 3p\theta - (26\delta + 27s) = 0$, then

$$Irr(\theta, K(\beta)) = x^3 + 3px - (26\delta + 27s) = Irr(\theta, K),$$

since $Irr(\theta, K(\beta)) \in K[x]$. Set $\alpha = \frac{\gamma}{3} + \frac{\theta}{3}$. Then, $\frac{\sigma(\gamma)}{3} + \frac{\theta}{3}$ is a conjugate of α over $K(\beta)$ (and a fortiori over K) and

$$\beta = \frac{\gamma}{3} + \frac{\theta}{3} - (\frac{\sigma(\gamma)}{3} + \frac{\theta}{3}).$$

From the relations $(\frac{\theta}{3})^3 + \frac{p}{3}(\frac{\theta}{3}) - \frac{26\delta+27s}{27} = 0$ and $(\frac{\gamma}{3})^3 + \frac{p}{3}(\frac{\gamma}{3}) = \frac{\delta}{27}$, we obtain that α is a root of the polynomial

$$x^3 - \gamma x^2 + (\frac{\gamma^2 + p}{3})x - (\delta + s) \in K(\beta)[X]$$

and α is an algebraic integer (of degree ≤ 3 over $K(\beta)$) provided $\frac{\gamma^2+p}{3} \in \mathbb{Z}_{K(\beta)}$. A short computation shows that from the relation $\gamma(\gamma^2+3p)=\delta$, we have $Irr(\frac{\gamma^2}{3},K)=x^3+2px^2+p^2x-\frac{disc(\beta)}{27}$ and $\frac{\gamma^2+p}{3}$ is a root of the polynomial $x^3+px^2+q^2$ whose coefficients are integers of K. □

Remark 1. It follows from the proof of Theorem 1, that if β is a cubic algebraic integer over a number field K with zero trace, then β is a difference of two conjugates over K of an algebraic integer of degree ≤ 3 over $K(\beta)$. The following example shows that the constant 3 in the last sentence is the best possible. Set $K=\mathbb{Q}$ and $Irr(\beta,\mathbb{Q})=x^3-3x-1$. Then, $disc(\beta)=3^4$ and the extension $\mathbb{Q}(\beta)/\mathbb{Q}$ is normal, since β^2-2 is also a root of $Irr(\beta,\mathbb{Q})$. By Theorem 3 of [5], β is not a difference of two conjugates of an integer of $\mathbb{Q}(\beta)$ (the 3−adic valuation of $disc(\beta)$ is 4) and if $\beta=\alpha-\alpha'$, where α is an algebraic integer of degree 2 over $\mathbb{Q}(\beta)$ and α' is a conjugate of α over $\mathbb{Q}(\beta)$, then there exists an element τ of the group $G(\mathbb{Q}(\beta,\alpha)/\mathbb{Q}(\beta))$ such that $\tau(\beta)=\beta$, $\tau(\alpha)=\alpha'$, $\tau(\alpha')=\alpha$ and $\beta=\tau(\alpha-\alpha')=\alpha'-\alpha=-\beta$.

Remark 2. With the notation of the proof of Theorem 1 (the second part) we have: *Let β be a cubic algebraic integer over K with zero trace and such that the extension $K(\beta)/K$ is cyclic. Then, β is a difference of two conjugates of an integer of $K(\beta)$, if and only if there exists $a\in\mathbb{Z}_K$ such that the two numbers $\frac{a^2+p}{3}$ and $\frac{a^3+3pa+\delta}{27}$ are integers of K.* Indeed, suppose that $\beta=\alpha-\sigma(\alpha)$, where $\alpha\in\mathbb{Z}_{K(\beta)}$ (if $\beta=\alpha-\sigma^2(\alpha)$, then $\beta=\alpha+\sigma(\alpha)-\sigma(\alpha+\sigma(\alpha))$). Then, $\alpha-\sigma(\alpha)=\frac{\gamma}{3}-\sigma(\frac{\gamma}{3})$, $\alpha-\frac{\gamma}{3}=\sigma(\alpha-\frac{\gamma}{3})$, $\alpha-\frac{\gamma}{3}\in K$ and there exists an integer a of K such that $3\alpha-\gamma=a$. Hence, $\frac{\gamma+a}{3}=\alpha\in\mathbb{Z}_{K(\beta)}$, $Irr(\frac{\gamma+a}{3},K)=x^3-ax^2+\frac{a^2+p}{3}x-\frac{a^3+3pa+\delta}{27}\in\mathbb{Z}_K[X]$ and so the numbers $\frac{a^2+p}{3}$ and $\frac{a^3+3pa+\delta}{27}$ are integers of K. The converse is trivial, since $\beta=\frac{\gamma}{3}-\sigma(\frac{\gamma}{3})=\frac{\gamma+a}{3}-\sigma(\frac{\gamma+a}{3})$ for all integers a of K. It follows in particular when $\frac{disc(\beta)}{3^6}\in\mathbb{Z}_K$, that β is a difference of two conjugates of an integer of $K(\beta)$ $(a=0)$. Note finally that for the case where $K=\mathbb{Q}$ a more explicit condition was obtained in [5].

3. Proof of Theorem 2

With the notation of the proof of Theorem 1 (the second part) and $K=\mathbb{Q}$, let N be a cubic normal extension of $\mathbb{Q}$ with discriminant Δ and let v be the 3−adic valuation. Suppose that every non-zero integer β of N with zero trace is a difference of two conjugates of an integer of N. Then, $N=\mathbb{Q}(\beta)$ and by Theorem 3 of [5], $v(disc(\beta))\neq 4$. Assume also $v(\Delta)=4$. Then, $v(disc(\beta))>4$ and hence $v(disc(\beta))\geq 6$, since $\frac{disc(\beta)}{\Delta}\in\mathbb{Z}_{\mathbb{Q}}$ and $disc(\beta)$ is a square of a rational integer. It follows that $\frac{\gamma}{3}$ is an algebraic integer, since its minimal polynomial over $\mathbb{Q}$ is $x^3 + \frac{p}{3}x - \frac{\delta}{27} \in \mathbb{Z}_{\mathbb{Q}}[X]$ and β can be written $\beta = \alpha - \sigma(\alpha)$, where $\alpha = \frac{\gamma}{3}$ is an integer of N with zero trace. Thus, $v(disc(\alpha)) \geq 6$ and there is an integer η of N with zero trace, such that $\alpha = \eta - \sigma(\eta)$. It follows that $\beta = \eta - \sigma(\eta) - \sigma(\eta - \sigma(\eta)) = \eta - 2\sigma(\eta) + \sigma^2(\eta) = -3\sigma(\eta)$ and $\frac{\beta}{3}$ is also an integer of N with zero trace. The last relation leads to a contradiction since in this case $\frac{\beta}{3^n} \in \mathbb{Z}_N$ for all positive rational integers n. Conversely, suppose $v(\Delta) \neq 4$. Assume also that there exists an integer β of N with zero trace which is not a difference of two conjugates of an integer of N. Then, $N = \mathbb{Q}(\beta)$ and by Theorem 1 of [5], we have $Tr_{N/\mathbb{Q}}(\mathbb{Z}_N) = 3\mathbb{Z}$, since $Tr_{N/\mathbb{Q}}(1) = 3$ and $Tr_{N/\mathbb{Q}}(\mathbb{Z}_N)$ is an ideal of $\mathbb{Z}$. If $\{e_1, e_2, e_3\}$ is an integral basis of N, then from the relation $\Delta = \det(Tr(e_i e_j))$, we obtain $v(\Delta) \geq 3$ and hence $v(\Delta) \geq 6$, since Δ is a square of a rational integer. The last inequality leads to a contradiction as in this case we have $v(disc(\beta)) \geq 6$ and $\beta = \frac{\gamma}{3} - \sigma(\frac{\gamma}{3})$ where $\frac{\gamma}{3} \in \mathbb{Z}_N$. $\square$

This work is partially supported by the research center (N^o Math/1419/20).

References

[1] A. Dubickas, *On numbers which are differences of two conjugates of an algebraic integer.* Bull. Austral. Math. Soc. **65** (2002), 439–447.

[2] A. Dubickas, C. J. Smyth, *Variations on the theme of Hilbert's Theorem 90.* Glasg. Math. J. **44** (2002), 435–441.

[3] S. Lang, *Algebra.* Addison-Wesley Publishing, Reading Mass. 1965.

[4] A. Schinzel, *Selected Topics on polynomials.* University of Michigan, Ann Arbor, 1982.

[5] T. Zaimi, *On numbers which are differences of two conjugates over $\mathbb{Q}$ of an algebraic integer.* Bull. Austral. Math. Soc. **68** (2003), 233–242.

Toufik Zaimi
King Saud University
Dept. of Mathematics P. O. Box 2455
Riyadh 11451, Saudi Arabia
E-mail : zaimitou@ksu.edu.sa