BULL. AUSTRAL. MATH. SOC. 11R04, 11R16, 11R21, 11R32
VOL. 65 (2002) [439–447]

ON NUMBERS WHICH ARE DIFFERENCES OF TWO CONJUGATES OF AN ALGEBRAIC INTEGER

ARTŪRAS DUBICKAS

We investigate which numbers are expressible as differences of two conjugate algebraic integers. Our first main result shows that a cubic, whose minimal polynomial over the field of rational numbers has the form $x^3 + px + q$, can be written in such a way if p is divisible by 9. We also prove that every root of an integer is a difference of two conjugate algebraic integers, and, more generally, so is every algebraic integer whose minimal polynomial is of the form $f(x^e)$ with an integer $e \geqslant 2$.

1. INTRODUCTION

Let K be a number field, that is, a finite extension of the field of rational numbers $\mathbb{Q}$, and let $\mathbb{Z}_K$ be its ring of integers. (Recall that $a \in \mathbb{Z}_K$ if and only if $a \in K$ and its minimal polynomial over $\mathbb{Q}$, whose leading coefficient is equal to 1, has all other coefficients lying in the ring of integers $\mathbb{Z}$.) Assume that β is an algebraic number of degree d over the field K with conjugates $\beta_1 = \beta, \beta_2, \ldots, \beta_d$.

QUESTION 1. Which numbers β can be written as a difference $\alpha - \alpha'$ of two conjugates over K of an algebraic integer?

Recall that α is an *algebraic integer* if its minimal polynomial over $\mathbb{Q}$, whose leading coefficient is equal to 1, has all other coefficients lying in the ring $\mathbb{Z}$. Then its minimal polynomial over K, whose leading coefficient is 1, has all other coefficients in the ring $\mathbb{Z}_K$. Clearly, such β itself must be an algebraic integer. Furthermore, β must be expressible as a difference of two conjugates over K of an algebraic number.

The set of numbers which are differences of two conjugates over K was studied by the author and Smyth in [3]. It was shown that $\beta = \alpha - \alpha'$ with some α and α' conjugate over K if and only if there is an automorphism σ in the Galois group of $K(\beta_1, \ldots, \beta_d)/K$ of order n such that $\sum_{i=0}^{n-1} \sigma^i(\beta) = 0$. Then, setting $\alpha = \sum_{i=0}^{n-1} (n-i-1)\sigma^i(\beta)/n$, we indeed have $\beta = \alpha - \sigma(\alpha)$. (Compare with Hilbert's

Received 23rd October, 2001
I owe Question 1 to Chris Smyth. I would like to thank Andrzej Schinzel for his interest and a suggestion concerning the Cardano formulae. This research was partially supported by a grant from Lithuanian State Science and Studies Foundation.

Copyright Clearance Centre, Inc. Serial-fee code: 0004-9727/02 $A2.00+0.00.

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

Theorem 90 in its additive form. See, for example, [4] or [5, Chapter VIII, Section 6].) This implies that β can only be expressible as above if its *trace* over K, namely, the sum of *all* its conjugates over K is 0.

Of course, the answer to Question 1 depends on K. For example, $\sqrt{2}$ is not expressible as a difference of two conjugates over $\mathbb{Q}(\sqrt{2})$ of an algebraic number. However it is a difference of two conjugates over $\mathbb{Q}$ of an algebraic integer, say, $\alpha = (\sqrt{6}+\sqrt{2})/2$ and $\alpha' = (\sqrt{6}-\sqrt{2})/2$.

QUESTION 2. Is every algebraic integer which is expressible as a difference of two conjugates over K of an algebraic number also expressible as a difference of two conjugates over K of an algebraic integer?

The positive answer to Question 2 would immediately imply the following answer to Question 1: those β which are algebraic integers and which are differences of two conjugates over K of an algebraic number (the latter ones were described above).

2. RESULTS

For β of degree at most 3, the condition on its trace is not only necessary, but also sufficient (see [3]). It follows that every β of trace zero over K and of degree at most 3 over K is a difference of two conjugates over K. For $d = 1$, only $\beta = 0$ is of trace zero, and it is a difference of two zeroes. We begin with the following simple result.

OBSERVATION. *Given a number field K, suppose that β is an algebraic integer and $-\beta$ is its conjugate over K. Then β can be written as a difference of two conjugates over K of an algebraic integer.*

PROOF: Let β be of degree d over K. Choose $m \in \mathbb{Z}$ such that $\alpha = \beta/2 + \sqrt{(\beta/2)^2 - m}$ is of degree $2d$ over K. Then α is an algebraic integer, since so is β. Also, $-\beta/2 + \sqrt{(\beta/2)^2 - m}$ is conjugate to α over K. Their difference is β which completes the proof. □

The answers to the above questions for quadratic numbers now follow, since every quadratic number β of trace 0 has $-\beta$ as its other conjugate.

COROLLARY 1. *For every number field K, a quadratic over K algebraic integer β, whose minimal polynomial over K is $x^2 + px + q$, can be written as a difference of two conjugates over K of an algebraic integer if and only if $p = 0$.*

If, for instance, $K = \mathbb{Q}$ and $\beta = \sqrt{2}$, then, choosing $m = -1$, we have the above example with $\alpha = (\sqrt{6}+\sqrt{2})/2$ being the root of the irreducible over $\mathbb{Q}$ polynomial $x^4 - 4x^2 + 1$. Can the real cubic root of 2 be expressed in a similar way?

Before we answer this question, consider the simplest case of cubics which are expressible as differences of conjugate algebraic integers. Let β be a cubic algebraic

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

integer over a number field K of trace 0 with minimal polynomial x^3+px+q over K. Here, $p, q \in \mathbb{Z}_K$, and so does the discriminant of β,

$$\Delta = \big((\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)\big)^2 = -4p^3-27q^2.$$

Set $\gamma = \gamma_1 = \beta_1 - \beta_3$. It has at least two other conjugates over K, $\gamma_2 = \beta_2 - \beta_1$ and $\gamma_3 = \beta_3 - \beta_2$, since the Galois group of $K(\beta_1, \beta_2, \beta_3)/K$ contains the 3-cycle (123). Clearly, every such β of trace 0 is expressible as $\alpha - \alpha'$ with algebraic integers $\alpha = \gamma_1/3$ and $\alpha' = \gamma_2/3$ conjugate over K provided that $\gamma/3 \in \mathbb{Z}_K$. The minimal polynomial for $\gamma/3$ over K is either $x^3 + px/3 - \ell/27$, if $\ell = \gamma_1\gamma_2\gamma_3 = \sqrt{\Delta} \in K$, or $\big(x^3+px/3\big)^2 - \Delta/729$, if $\ell = \sqrt{\Delta} \notin K$. In both cases, $\gamma/3 \in \mathbb{Z}_K$ if and only if $\Delta/729 \in \mathbb{Z}_K$.

The discriminant of the polynomial x^3-2 is equal to 108. It is not divisible by 729. Nevertheless, $2^{1/3}$ is a difference of two conjugate integers, even units. One can check that $2^{1/3}$ is a difference of two roots of an irreducible over $\mathbb{Q}$ polynomial

$$x^{18} - 6x^{15} + 7x^{12} + 4x^9 + 115x^6 + 2x^3 + 1.$$

This shows that the construction of α might be nontrivial even for cubic β. We now are in the position to state the main results of this paper. Below, $\Delta = -4p^3 - 27q^2$.

THEOREM 1. *Let K be a number field, and let β be a cubic algebraic integer over K whose minimal polynomial over K is x^3+px+q. If $p/9 \in \mathbb{Z}_K$, then β can be written as a difference of two conjugates over K of an algebraic integer. Furthermore, the latter number can be chosen to be of degree 9, if $\sqrt{\Delta} \in K$, and 18 otherwise.*

Note that $\sqrt{\Delta} \in K$ if the Galois group of $K(\beta_1, \beta_2, \beta_3)/K$ is cyclic (of order 3), and $\sqrt{\Delta} \notin K$, if the Galois group is S_3 (of order 6).

THEOREM 2. *Let K be a number field, and let $e \geqslant 2$ be an integer. Assume that β is an algebraic integer whose minimal polynomial over K is of the form $f(x^e)$, where $f(x) \in \mathbb{Z}_K[x]$. Then β can be written as a difference of two conjugates over K of an algebraic integer.*

In particular, if $x^e - q$, where $e \geqslant 2$, is irreducible over $\mathbb{Q}$, then $q^{1/e}$ is a difference of conjugate algebraic integers. (The conditions on $q \in K$ under which the polynomial $x^e - q$ is irreducible over an arbitrary field K can be found in [**5**, Chapter VIII, Section 9].)

COROLLARY 2. *If $e \geqslant 2$ is a positive integer, $q \in \mathbb{Z}$ and $q^{1/e}$ has degree e over $\mathbb{Q}$, then $q^{1/e}$ can be written as a difference of two conjugates over $\mathbb{Q}$ of an algebraic integer.*

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

3. Proof of Theorem 1

Let $\gamma = \gamma_1 = \beta_1 - \beta_3$ be as in Section 2. Since $\gamma_1 + \gamma_3 + \gamma_3 = 0$,

$$\gamma_1\gamma_2 + \gamma_1\gamma_3 + \gamma_2\gamma_3 = 3(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) = 3p,$$

and $\gamma_1\gamma_2\gamma_3 = \ell = \sqrt{\Delta}$, we deduce that γ is a root of $x^3 + 3px - \ell = 0$. The idea of the proof is to look at the action of the group G of the Galois extension $K(\beta_1, \beta_2, \beta_3)/K$ on the number

$$\alpha = \gamma/3 + (m - \ell/27)^{1/3}.$$

The Galois group G is cyclic if and only if $\ell \in \mathbb{Z}_K$. Then γ is of degree 3 over K. Otherwise, G is S_3 and γ is of degree 6 over K. Choose $m \in \mathbb{Z}$ such that α is of degree 9 or 18 over K, respectively. Clearly, $\alpha' = \gamma_2/3 + (m - \ell/27)^{1/3}$ is among the conjugates of α over K, so that $\alpha - \alpha' = (\beta_1 - \beta_3 - \beta_2 + \beta_1)/3 = \beta_1 = \beta$. Since $\ell = \gamma^3 + 3p\gamma$, the minimal polynomial of α over $K(\gamma)$ is

$$x^3 - \gamma x^2 + \gamma^2 x/3 + p\gamma/9 - m.$$

Thus α is an algebraic integer if $\gamma^2/3$ is an algebraic integer and, in addition to this, $p/9 \in \mathbb{Z}_K$. We shall show that the second condition automatically implies the first one.

Note the minimal polynomial of $\gamma^2/3$ over K is

$$x^3 + 2px^2 + p^2x - \Delta/27.$$

Indeed, this follows from the equality $\Delta = \ell^2 = \left(\gamma^3 + 3p\gamma\right)^2 = 27\left(\gamma^2/3 + p\right)^2(\gamma^2/3)$ and from the fact that the numbers $\gamma_1^2, \gamma_2^2, \gamma_3^2$ are distinct. (Clearly, $\gamma_1 \neq -\gamma_2$. Also, $\gamma_1 \neq \gamma_2$, since, by [**6**, Lemma 1], the equality $2\beta_1 = \beta_2 + \beta_3$ is impossible.) Notice that $\Delta/27 = -108(p/9)^3 - q^2 \in \mathbb{Z}_K$, because $p/9$ and q are both in $\mathbb{Z}_K$. This completes the proof, since the condition $p/9 \in \mathbb{Z}_K$ implies that $\gamma^2/3$ is an algebraic integer.

Remark. Formally, Lemma 5 of [**6**] is given for $K = \mathbb{Q}$ only, but the argument (map to the largest conjugate) remains the same for every K which is a subfield of the field of complex numbers, including number fields. More generally, the equality $q_1\beta_1 = q_2\beta_2 + \ldots q_n\beta_n$ with *distinct* algebraic numbers $\beta_1, \ldots, \beta_n$, $n \geqslant 3$, conjugate over an arbitrary field K of characteristic 0 is impossible, if $q_1, \ldots, q_n$ are nonzero integers such that $|q_1| \geqslant |q_2| + \cdots + |q_n|$. See [**2**, Theorem 4], where such an argument could not be used, and thus an algebraic proof was given.

4. Proof of Theorem 2

If e is even, then the theorem follows immediately, by our observation. Assume that e is divisible by an odd prime P. Let ε be the primitive Pth root of unity. We

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

shall show first that there is a $\sigma \in G = G\big(K(\beta_1, \dots, \beta_d)/K\big)$ such that $\sigma(\beta) = \beta\varepsilon$ and $\sigma(\varepsilon) = \varepsilon$.

Indeed, take an arbitrary $\sigma_1 \in G$ which maps β to its conjugate $\beta\varepsilon$. Assume that $\sigma_1(\varepsilon) = \varepsilon^\ell$, where $1 < \ell \leqslant P-1$. Let j be the smallest positive integer such that $\ell^j \equiv 1 (\mathrm{mod}\, P)$. Then σ_1^j maps β to $\beta\varepsilon^{(\ell+1)^{j-1}}$ and ε to ε. It follows that we can take σ to be a power of σ_1^j, if $\ell \neq P-1$. The alternative case, $\ell = P-1$, can only happen for $P > 3$. Consider an automorphism $\sigma_2 \in G$ which maps β to its other conjugate $\beta\varepsilon^2$. If now $\sigma_2(\varepsilon) = \varepsilon^s$ with s in the range $1 \leqslant s < P-1$, then we can apply the above argument. Alternatively, $\sigma_2(\varepsilon) = \varepsilon^{P-1}$, but then the automorphism $\sigma_1\sigma_2$ maps β to $\beta\varepsilon^{P-1}$ and ε to ε. Clearly, there is a power of $\sigma_1\sigma_2$, which maps β to $\beta\varepsilon$ and ε to ε.

Set

$$\gamma = \gamma_1 = \beta\big(P - 1 + (P-2)\varepsilon + (P-3)\varepsilon^2 + \cdots + \varepsilon^{P-2}\big) = P\beta/(1-\varepsilon),$$

and $\gamma_i = \sigma^i(\gamma) = \gamma\varepsilon^{i-1}$ for $i = 2, 3, \dots, P$. Now, $\gamma_1, \dots, \gamma_P$, are all roots of the polynomial $x^P - \big(P\beta/(1-\varepsilon)\big)^P$. Assume that γ is of degree D over K. We choose $m \in \mathbb{Z}$ in such a way that

$$\alpha = \gamma/P + \big(m - (\gamma/P)^P\big)^{1/P}$$

is of degree PD over K. Then, as above, $\alpha' = \gamma_2/P + \big(m - (\gamma/P)^P\big)^{1/P}$ is conjugate to α over K and $\alpha - \alpha' = \big(\gamma - \sigma(\gamma)\big)/P = \beta$, using $\gamma/P = \beta/(1-\varepsilon)$. Also, α is a root of the polynomial

$$x^P - \sum_{j=1}^{P-1} (-1)^j \Big(\frac{\beta}{1-\varepsilon}\Big)^j \binom{P}{j} x^{P-j} - m.$$

It remains to prove that α is an algebraic integer. Clearly, so are β and $m \in \mathbb{Z}$. Since every binomial coefficient is divisible by P, it suffices to show that $P/(1-\varepsilon)^j$ is an algebraic integer for every $j = 1, \dots, P-1$. This will be the case if $P/(1-\varepsilon)^{P-1}$ is an algebraic integer, because so is $1-\varepsilon$ and its natural powers. The product of the conjugates of $P/(1-\varepsilon)^{P-1}$ over $\mathbb{Q}$ is equal 1, thus, equivalently, it suffices to show that $(1-\varepsilon)^{P-1}/P$ is an algebraic integer. This is exactly the case, because the coefficients of the polynomial

$$h(x) = (1-x)^{P-1} - 1 - x - \cdots - x^{P-1} = \sum_{j=1}^{P-2} (-1)^j \left(\binom{P-1}{j} + (-1)^{j-1} \right) x^j$$

are all divisible by P (check this for j even and odd)! Since $h(\varepsilon)/P = (1-\varepsilon)^{P-1}/P$, and ε itself is an algebraic integer, the proof is completed.

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

5. Similar questions

It is somewhat surprising that both questions are very easy to answer if we replace the word "difference" by one of the words "sum" or "product". In fact, *every* algebraic number β is a sum of two *distinct* conjugates α and α' over K. (Just take them both as roots of an irreducible over $K(\beta)$ polynomial $x^2 - \beta x + m$ with nonzero $m \in \mathbb{Z}$.) Similarly, by taking α and α' as roots of some irreducible over $K(\beta)$ polynomial $x^2 + mx + \beta$, where $m \in \mathbb{Z}$, we see that *every* nonzero algebraic number β is a product of two *distinct* conjugates α and α' over K, whereas zero is only expressible as the product of two zeroes (see also [**1**, Section 3]). In both cases, we can positively answer to the second question, because the numbers α and α' are algebraic integers provided that so is β.

With the word "difference" being replaced by the word "quotient", it was shown in [**3**] that a nonzero β is equal to α/α' with some α and α' conjugate over K if and only if there is an automorphism σ in the Galois group of $K(\beta_1, \ldots, \beta_d)/K$ of order n such that $\prod_{i=0}^{n-1} \sigma^i(\beta)$ is a root of unity. *Every* such β is also a quotient of two conjugates over K of an algebraic integer. (Just write $\beta = \alpha/\alpha' = (m\alpha)/(m\alpha')$ with some nonzero $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.) In order to ask the "right" questions for the "quotient" case, we replace the words "algebraic integer" by the word "unit". Recall that β is a *unit* if both β and $1/\beta$ are algebraic integers.

Question 1′. Which numbers β can be written as a quotient α/α' of two conjugates over K of a unit?

Question 2′. Is every unit which is expressible as a quotient of two conjugates over K of an algebraic number also expressible as a quotient of two conjugates over K of a unit?

The answer to Question 2′ is positive. This follows from the next theorem which also answers Question 1′, because β which are quotients of two units are units themselves.

Theorem 3. *Given a number field K, a unit β is expressible as a quotient of two conjugates over K of a unit if and only if there is an automorphism σ in the Galois group of the normal extension of $K(\beta)$ over K of order n such that $\prod_{i=0}^{n-1} \sigma^i(\beta)$ is a root of unity.*

Proof: The necessity of the condition follows from [**3**, Theorem 1.1]. In order to prove that the condition is also sufficient, we set

$$\gamma = \prod_{i=0}^{n-1} \left(\sigma^i(\beta)\right)^{n-i-1}.$$

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

Then $\gamma/\sigma(\gamma) = \beta^n/\theta$, where $\theta = \prod_{i=0}^{n-1} \sigma^i(\beta)$ is a root of unity. Among the conjugates of $\gamma^{1/n}$ over K there is at least one number of the form $\rho\sigma(\gamma)^{1/n}$, where $\rho^n = 1$. We have that $\gamma^{1/n}/\left(\rho\sigma(\gamma)^{1/n}\right) = \mu\beta$, where μ is a root of unity. Furthermore, $\gamma^{1/n}$ is a unit, since so is β. It suffices to show that, given arbitrary, say ℓth, root of unity μ and a unit β, which is a quotient of two conjugate over K units α and α', the number $\mu\beta$ is also expressible by a similar quotient.

Set $\delta = \alpha\omega$, where $\omega = \left(m + \sqrt{m^2 - 1}\right)^{1/\ell}$. As in [**3**, Lemma 3.1], given arbitrary extension of K, say L, which contains the numbers α and α', there is an $m \in \mathbb{Z}$ such that α and α' are conjugate over $K(\omega)$ and the degree of ω over L is 2ℓ (or, equivalently, the polynomial $1 - 2mx^\ell + x^{2\ell}$ is irreducible over L). Let L be the normal closure of $K(\alpha, \mu_\ell)$ over K. Here, μ_ℓ is the primitive ℓth root of unity. Note that $L(\omega)$ is the Galois extension over L and so it is over K, because L/K is normal. Then there is an automorphism σ of the Galois group of $L(\omega)/K$ such that $\sigma(\alpha) = \alpha'$ and $\sigma(\omega) = \mu^{-1}\omega$. (We can take σ as a composition of an automorphism taking ω to ω and α to α' and an automorphism fixing L and taking ω to $\mu^{-1}\omega$.) It follows that δ and $\sigma(\delta)$ are conjugate over K, and

$$\frac{\delta}{\sigma(\delta)} = \frac{\alpha\omega}{\alpha'\mu^{-1}\omega} = \frac{\mu\alpha}{\alpha'} = \mu\beta.$$

Moreover, $\delta = \alpha\omega$ is a unit, because so are α and ω. □

6. Speculations concerning possible generalisation

Let σ be an automorphism in the Galois group of $K(\beta_1, \ldots, \beta_d)/K$ which maps $(\beta_1, \beta_2, \ldots \beta_n)$ to $(\beta_n, \beta_1, \ldots, \beta_{n-1})$, where $\beta_1 + \cdots + \beta_n = 0$, and every β_i with $i > n$ to some β_j with $j = j(i) > n$. We know that only such β are differences of two conjugates over K of an algebraic number. Setting

$$\gamma = (n-1)\beta_1 + (n-2)\beta_2 + \cdots + \beta_{n-1},$$

we can simply choose $\alpha = \gamma/n$ and $\alpha' = \sigma(\alpha)$ in order that $\alpha - \alpha' = \beta$. Clearly, α already is an algebraic integer if so is γ/n. If α is not an algebraic integer, we can still obtain one from it by adding another algebraic number δ so that $\alpha + \delta$ is an algebraic integer and $N_\alpha \cap N_\delta = K$. (Given a field K and an algebraic number α, by N_α we denote the normal extension of $K(\alpha)$ over K.) This would immediately imply the positive answer to Question 2. Indeed, setting G_1 and G_2 for the Galois groups of N_α/K and N_δ/K, respectively, we have that the Galois group of $N_\alpha N_\delta/K$ is $G_1 \times G_2$ (see [**5**, Chapter VIII, Section 1]). In case if $K = \mathbb{Q}$ and $\alpha = \sqrt{1/2}$, we took

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

$\delta = \sqrt{3/2}$. Then, the respective normal extensions are $N_\alpha = \mathbb{Q}(\sqrt{2})$, $N_\delta = \mathbb{Q}(\sqrt{6})$ whose intersection is $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{6}) = \mathbb{Q}$.

However this is, in general, impossible. On applying the automorphisms which map α to their conjugates and δ to itself, we conclude that all differences between conjugates of α must be algebraic integers. In case if $K = \mathbb{Q}$ and $\beta_1 = 2^{1/3}$, $\beta_2 = 2^{1/3}\varepsilon$, $\beta_3 = 2^{1/3}\varepsilon^2$, where ε is the complex root of $\varepsilon^3 = 1$, the Galois group of $N_\beta/\mathbb{Q}$ is S_3. The difference between $\alpha = (2\beta_1 + \beta_2)/3$ and its conjugate $(2\beta_2 + \beta_1)/3$ is not an algebraic integer, so that, in principle, it is impossible choose δ, as required. We still managed to show that $2^{1/3}$ is a difference of two conjugate algebraic integers, using $\delta = \left(1 - 2(\varepsilon - \varepsilon^2)/9\right)^{1/3}$ such that $\alpha + \delta$ is an algebraic integer and $N_\alpha \cap N_\delta = \mathbb{Q}(\sqrt{-3})$ is not too big.

The method described in Sections 3 and 4 can be generalised to algebraic numbers of arbitrary degree. If say β is of degree $d = 4$, and the 4-cycle (1234) belongs to the Galois group of N_β/K, we can set $\gamma = \gamma_1 = 3\beta_1 + 2\beta_2 + \beta_3$ and, using $\gamma_1 + \cdots + \gamma_4 = 0$, compute r', p' and q' such that $\gamma_1, \ldots, \gamma_4$ are all roots of the polynomial $x^4 + r'x^2 + p'x + q'$. Here, r', p', q' depend on the coefficients r, p, q of the minimal polynomial for β, say $x^4 + rx^2 + px + q$. Setting

$$\alpha = \gamma/4 + (m - q'/256)^{1/4}$$

with appropriate $m \in \mathbb{Z}$, we see that β is a difference of α and its conjugate $\alpha' = \gamma_2/4 + (m - q'/256)^{1/4}$. Now, α is a root of the polynomial

$$x^4 - \gamma x^3 + 3\gamma^2 x^2/8 - \gamma^3 x/16 - m - \left(r'\gamma^2 + p'\gamma\right)/256.$$

It is not difficult to see that we shall get some advantage by demanding that $3\gamma^2/8$, $\gamma^3/16$ and $\left(r'\gamma^2 + p'\gamma\right)/256$ are all algebraic integers compared to the trivial method (in which we ask the number $\gamma/4$ to be an algebraic integer). This is however too technical for this paper.

At first glance, it may seem that the condition $p/9 \in \mathbb{Z}_K$ may be easily replaced by the weaker condition $p/3 \in \mathbb{Z}_K$. A cubic which is the root of the polynomial $x^3 + px + q$, by the Cardano formulae, is equal to say $\zeta + \omega$, where

$$\zeta^3 = -q/2 + \sqrt{p^3/27 + q^2/4}, \quad \omega^3 = -q/2 - \sqrt{p^3/27 + q^2/4}.$$

Both ζ and ω are roots of the equation $x^6 + qx^3 - (p/3)^3 = 0$. Assume, for simplicity, that the polynomial $x^6 + qx^3 - (p/3)^3$ is irreducible over K. If $p/3 \in \mathbb{Z}_K$, then ζ and ω are both algebraic integers. Furthermore, by Theorem 2, $\zeta = \alpha - \alpha'$ and $\omega = \gamma - \gamma'$, where α and γ are algebraic integers, α and α' are conjugate over K (and so are γ and γ'). Assume that $L = K\left(\varepsilon, \sqrt{p^3/27 + q^2/4}\right)$ is of maximal degree 4 over K. Then,

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press

as in Theorem 2, α and γ can be chosen to be of degree 9 over L, and thus of degree 36 over K. Clearly, $\alpha+\gamma$ and $\alpha'+\gamma'$ are conjugate over K if they are of maximal degree 324 over K. However, if α and γ are chosen as in Theorem 2, the degree of $\alpha+\gamma$ is only 108 (which is too small)! One has to be cautious in constructing examples via sums: for instance, $\sqrt{2}+\sqrt{6}$ and $\sqrt{3}$ are both differences of two conjugates over $\mathbb{Q}$ of algebraic integers (see Section 1 and Observation), but their sum, $\sqrt{2}+\sqrt{3}+\sqrt{6}$, is not expressible by a difference of two conjugates over $\mathbb{Q}$ (see [3]).

References

[1] A. Dubickas, 'The Remak height for units', *Acta Math. Hungar.* (to appear).

[2] A. Dubickas, 'On the degree of a linear form in conjugates of an algebraic number', *Illinois J. Math.* (to appear).

[3] A. Dubickas and C.J. Smyth, 'Variations on the theme of Hilbert's Theorem 90', *Glasgow Math. J.* (to appear).

[4] D. Hilbert, 'Die Theorie der algebraischen Zahlkörper', *Jahresber. Deutsch. Math.-Verein* **4** (1897), 175–546. English translation by I.T. Adamson: *The theory of algebraic number fields,* (Springer–Verlag, Berlin, 1998).

[5] S. Lang, *Algebra* (Addison–Wesley Publishing, Reading, Mass., 1965).

[6] C.J. Smyth, 'Conjugate algebraic numbers on conics', *Acta Arith.* **40** (1982), 333–346.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius 2600
Lithuania
e-mail: arturas.dubickas@maf.vu.lt

https://doi.org/10.1017/S0004972700020487 Published online by Cambridge University Press