Bull. Austral. Math. Soc. 11R04, 11R16, 11R32
Vol. 68 (2003) [233–242]

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

T. Zaimi

We continue the investigation started by A. Dubickas of the numbers which are differences of two conjugates of an algebraic integer over the field Q of rational numbers. Mainly, we show that the cubic algebraic integers over Q with zero trace satisfy this property and we give a characterisation for those for which this property holds in their normal closure. We also prove that if a normal extension K/Q is of prime degree, then every integer of K with zero trace is a difference of two conjugates of an algebraic integer in K if and only if there exists an integer of K with trace 1.

1. Introduction

Let L be a number field, that is a finite extension of the field Q of rational numbers, and let K be a subfield of L. Then, the extension L/K is said to be normal if there exists $\theta \in L$ all of whose conjugates over K belong to L. In this case the set $G(L/K)$ of the $K-$embeddings of L in the complex field has a group structure and is called the Galois group of the extension L/K. A normal extension is said to be cyclic if its Galois group is cyclic.

Let $\theta \in L$, then the trace of θ over K, namely $r_{L/K}(\theta) = \sum_{\tau \in G(L/K)} \tau(\theta)$, is an element of K. In particular if $\theta \in Z_L$, where Z_L is the ring of the integers of the field L, then $r_{L/K}(\theta) \in Z_K$.

The additive form of Hilbert's Theorem 90 ([3]), asserts that if the extension L/K is cyclic, then every element $\theta \in L$ satisfying $r_{L/K}(\theta) = 0$, can be written as $\theta = \alpha - \sigma(\alpha)$, where $\alpha \in L$ and σ is a generator of $G(L/K)$. A natural question arises immediately. For which cyclic extensions L/K, can we write every integer β of L satisfying $r_{L/K}(\beta) = 0$ in the form $\beta = \alpha - \sigma(\alpha)$, where $\alpha \in Z_L$? The next result gives a partial answer to this question.

Theorem 1. *Let L/K be a normal extension of degree d, where d is inert in Z_K. Then, every integer β of the field L satisfying $r_{L/K}(\beta) = 0$, is a difference of two conjugates of an algebraic integer in L if and only if $r_{L/K}(Z_L) = Z_K$.*

Received 10th February, 2003

In fact the question above is in a certain sense due to Smyth [**1**]. He asks whether an algebraic integer which is a difference of two conjugates over K of an algebraic number, is a difference of two conjugates over K of an algebraic integer.

In [**2**], Dubickas and Smyth, have shown that a number θ is a difference of two conjugates over K of an algebraic number if and only if there exists an element τ in the Galois group of the normal closure of the extension $K(\theta)/K$ (the normal closure of the extension $K(\theta)/K$ is the smallest normal extension of K containing θ) such that $\theta+\tau(\theta)+\cdots+\tau^{n-1}(\theta)=0$, where n is the order of τ.

Recently ([**1**]), Dubickas proved that an algebraic integer β whose minimal polynomial over K, say $\mathrm{Irr}\,(\beta,K)$, is of the form

$$\mathrm{Irr}\,(\beta,K)=P(x^n),$$

where $P\in Z_K[X]$ and n is a rational integer greater than 1, is a difference of two conjugates over K of an algebraic integer. He also showed that the same property holds when

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

provided $p/9\in Z_K$. For this last case, the next theorem shows that the condition $p/9\in Z_K$ is not necessary when $K=Q$.

Theorem 2. *Let β be a cubic algebraic integer over Q. If $r_{Q(\beta)/Q}(\beta)=0$, then β is a difference of two conjugates of an algebraic integer of degree $\leqslant 3$ over the field $Q(\beta,\beta')$, where β' is a conjugate of β and $\beta'\neq\beta$.*

Let v be the 3-adic valuation function on the set $Z_Q:=Z$ (if $k\in Z$, then $v(k)$ is the greatest rational integer such that $k/(3^{v(k)})\in Z$). The following result gives a characterisation of the cubic algebraic integers over Q which are differences of two conjugates of an integer of the field $Q(\beta,\beta')$.

Theorem 3. *Let β be a cubic algebraic integer over Q and let $\mathrm{disc}\,(\beta)$ be the discriminant of $\mathrm{Irr}\,(\beta,Q):=x^3+px+q$. Then, β is a difference of two conjugates of an integer of the field $Q(\beta,\beta')$ if and only if $v(\mathrm{disc}\,(\beta))\notin\{4,5\}$, provided $v(\mathrm{disc}\,(\beta))\neq 3$ or there exists $\varepsilon\in\{-1,1\}$ such that $v(m+3p+\varepsilon l)\geqslant 3$ (respectively, such that $v(m+12p+8\varepsilon l)\geqslant 3$), where m is a squarefree rational integer, $l\in Z$, $l^2m=\mathrm{disc}\,(\beta)$ and $m\equiv 2,3[4]$ (respectively and $m\equiv 1[4]$), when $v(\mathrm{disc}\,(\beta))=3$.*

2. Proof of Theorem 1

Let L/K be a cyclic extension of degree $d\geqslant 2$ and let σ be a generator of $G(L/K)$. Set $\Lambda=\{\beta\in Z_L,\ r_{L/K}(\beta)=0\}$ and $D=\{\alpha-\sigma^m(\alpha),\ \alpha\in Z_L$ and $m\in Z\}$. It is clear that $D\subset\Lambda$ and if $r(Z_L)=Z_K$ (along the proof of Theorem 1, r means $r_{L/K}$), then there exists an element $e \in Z_L$ satisfying $r(e) = 1$. It follows (as in the proof of Hilbert's Theorem [**3**, p. 215]) that if $\beta \in \Lambda$, then

$$\beta = \alpha - \sigma(\alpha),$$

where

$$\alpha = \sum_{0 \leqslant k \leqslant d-2} \Big(\sum_{0 \leqslant i \leqslant k} \sigma^i(\beta) \Big) \sigma^k(e) \in Z_L.$$

Conversely, suppose $D = \Lambda$. Note first that $r(Z_L)$ is an ideal of Z_K and contains the ideal $r(Z_K) = dZ_K$. Suppose that $r(Z_L) \neq Z_K$. Then, $r(Z_L) = dZ_K$, since dZ_K is a prime ideal. We shall prove that $\beta/d \in \Lambda$, whenever $\beta \in \Lambda$. This leads to a contradiction, since in this case $\beta/d^n \in \Lambda \subset Z_L$ for all positive rational integers n. Let us now prove the following lemmas.

Lemma 1. *Let $\beta \in \Lambda$. Then there exists $\beta_1 \in \Lambda$ such that $\beta = \beta_1 - \sigma(\beta_1)$.*

Proof: Let $\beta \in \Lambda$. Then, there exist an element $\alpha \in Z_L$ and a positive rational integer m such that $\beta = \alpha - \sigma^m(\alpha)$, since $\Lambda = D$. Set $\eta = \sum_{0 \leqslant i \leqslant m-1} \sigma^i(\alpha)$ and $\beta_1 = \eta - \big(r(\eta)\big)/d$. Then, $r(\beta_1) = 0$, $\beta_1 \in Z_L$ and

$$\beta = \eta - \sigma(\eta) = \eta - \frac{r(\eta)}{d} - \sigma\big(\eta - \frac{r(\eta)}{d}\big) = \beta_1 - \sigma(\beta_1). \qquad \square$$

Lemma 2. *Let $\beta \in \Lambda$. Then, for every non-negative rational integer n, there exists $\beta_n \in \Lambda$ such that $\beta = \sum_{0 \leqslant k \leqslant n} (-1)^k C_k^n \sigma^k(\beta_n)$.*

Proof: We apply induction on n. Letting $\beta_0 = \beta$, we obtain the result for $n = 0$. Assume now that $\beta = \sum_{0 \leqslant k \leqslant n} (-1)^k C_k^n \sigma^k(\beta_n)$, where n is a non-negative rational integer and $\beta_n \in \Lambda$. Then, by Lemma 1, there exists $\beta_{n+1} \in \Lambda$ such that $\beta_n = \beta_{n+1} - \sigma(\beta_{n+1})$ and

$$\begin{aligned}
\beta &= \sum_{0 \leqslant k \leqslant n} (-1)^k C_k^n \sigma^k\big(\beta_{n+1} - \sigma(\beta_{n+1})\big) \\
&= C_0^n \beta_{n+1} + \sum_{1 \leqslant k \leqslant n} (-1)^k \big(C_k^n + C_{k-1}^n\big) \sigma^k(\beta_{n+1}) + (-1)^{n+1} C_n^n \sigma^{n+1}(\beta_{n+1}) \\
&= \sum_{0 \leqslant k \leqslant n+1} (-1)^k C_k^{n+1} \sigma^k(\beta_{n+1}).
\end{aligned} \qquad \square$$

Lemma 3. *Let $\beta \in \Lambda$. Then, $\sum_{0 \leqslant k \leqslant d-2} (d-1-k)\sigma^k(\beta) \in d\Lambda$.*

Proof: Let $\beta \in \Lambda$. Then, by Lemma 1, there exits $\alpha \in \Lambda$ such that $\beta = \alpha - \sigma(\alpha)$ and $\sum_{0 \leqslant k \leqslant d-2} (d-1-k)\sigma^k(\beta) = d\alpha \in d\Lambda$. $\square$

https://doi.org/10.1017/S000497270003762X Published online by Cambridge University Press

Returning to the proof of Theorem 1 and let $x_k = (d-1-k)+(-1)^k C_k^{d-2}$, where $0 \leqslant k \leqslant d-2$. Then, $x_0/d = 1$, $x_1/d = 0$ and for $k \geqslant 2$, $x_k/d \in Z$, since $k < d$ and

$$x_k = \frac{d-1-k}{k!}\big(k! + (-1)^k(d-2)(d-3)\dots(d-k)\big) = \frac{d(d-1-k)P(d)}{k!},$$

where P is a polynomial with rational integer coefficients.

Let now $\beta \in \Lambda$. Then, by Lemma 2, there exists $\alpha \in \Lambda$ such that

$$\beta = \sum_{0 \leqslant k \leqslant d-2} (-1)^k C_k^{d-2} \sigma^k(\alpha).$$

It follows by Lemma 3, that the number

$$\sum_{0 \leqslant k \leqslant d-2} x_k \sigma^k(\alpha) - \beta = \sum_{0 \leqslant k \leqslant d-2} \Big(x_k - (-1)^k C_k^{d-2}\Big)\sigma^k(\alpha)$$

is an element of the set $d\Lambda$. Furthermore, $\sum_{0 \leqslant k \leqslant d-2} x_k \sigma^k(\alpha) \in d\Lambda$, as $x_k/d \in Z$ for all $0 \leqslant k \leqslant d-2$ and $r\Bigg(\sum_{0 \leqslant k \leqslant d-2} x_k \sigma^k(\alpha)\Bigg) = 0$. Hence, $\beta \in d\Lambda$, since the sum of two elements of the set $d\Lambda$ belongs to $d\Lambda$ (if $\zeta = \theta - \sigma^m(\theta)$, where $\theta \in Z_L$ and m is a positive rational integer, then $\zeta = \eta - \sigma(\eta)$, where $\eta = \sum_{0 \leqslant i \leqslant m-1} \sigma^i(\theta)$. Hence, the sum of two elements of $\Lambda = D$ belongs to Λ).

REMARK. The proof of Theorem 1 can not be applied for a cyclic extension L/Q of degree 4, since in this case the condition $\Lambda = D$ does not imply $r_{L/Q}(Z_L) = 4Z$. Indeed, Let $Q(\sqrt{m})$ (m is a squarefree rational integer), be the unique quadratic field contained in L. Then, $\sqrt{m} = \alpha - \sigma\alpha$, where $\alpha \in Z_L$ and from the equalities $\sigma(\sqrt{m}) = -\sqrt{m} = \sigma(\alpha - \sigma\alpha) = \sigma\alpha - \sigma^2\alpha$ we obtain $\sqrt{m} = \alpha - \sigma\alpha = -(\sigma\alpha - \sigma^2\alpha)$ and $\alpha \in Q(\sqrt{m})$, as $\alpha = \sigma^2\alpha$. Hence, $m \equiv 1[4]$ and $r_{L/Q}(Z_L) = tZ$ where $t \in \{1, 2\}$, since $r_{L/Q}(1+\sqrt{m})/2 = 2$.

3. Proof of Theorem 2 and Theorem 3

First we show some results which can be used for the case where β is a cubic algebraic integer over a number field K. Set $\operatorname{Irr}(\beta, K) := x^3 + px + q$ and let L be the normal closure of the extension $K(\beta)/K$. Then, the group $G(L/K)$ is isomorphic to the symmetric group on three letters (respectively is cyclic of order 3) when $L \neq K(\beta)$ (respectively when $L = K(\beta)$). Fix an element σ in $G(L/K)$ of order 3, then $L = K\big(\beta, \sigma(\beta)\big)$,

$$r_{K(\beta)/K}(\theta) = \theta + \sigma(\theta) + \sigma^2(\theta),$$

where θ is any element of the field $K(\beta)$,

$$(1) \qquad p = r_{K(\beta)/K}\big(\sigma(\beta)\sigma^2(\beta)\big) = \beta\sigma(\beta) + \sigma(\beta)\sigma^2(\beta) + \sigma^2(\beta)\beta$$

and

$$(2) \qquad \operatorname{disc}(\beta) = \big((\beta - \sigma\beta)(\beta - \sigma^2\beta)(\sigma\beta - \sigma^2\beta)\big)^2 = -4p^3 - 3^3q^2.$$

Recall by Galois theory, that the field L contains three cubic extensions of K and only one quadratic extension of K, namely $K\big(\sqrt{\operatorname{disc}(\beta)}\big)$. The field $K\big(\sqrt{\operatorname{disc}(\beta)}\big)$ is the set of elements of L which are fix under the action of the automorphism σ (respectively Recall that the set of the elements of L which are fix under the action of σ is the field K). Note also that if $\beta = \theta - \tau(\theta)$, where $\theta \in Z_L$ and $\tau \in G(L/K)$, then there exists $\alpha \in Z_L$ such that $\beta = \alpha - \sigma(\alpha)$ and $K(\alpha) = L$. Indeed, if τ is of order 2, then $\tau(\beta) = \tau(\theta) - \theta = -\beta$ is a conjugate of β and if $\tau = \sigma^2$, then $\beta = \theta - \sigma^2(\theta) = \theta + \sigma(\theta) - \sigma\big(\theta + \sigma(\theta)\big)$. The equality $K(\alpha) = L$ is clear, since all the cubic extensions of K in L, namely $K(\beta)$, $K\big(\sigma(\beta)\big)$ and $K\big(\sigma^2(\beta)\big)$, are not normal over K (respectively since the only subfields of L containing K are L and K).

Let $\gamma := \beta - \sigma^2(\beta)$. Then, γ is of degree 6 (respectively of degree 3) over K and

$$\operatorname{Irr}\Big(\gamma, K\big(\sqrt{\operatorname{disc}(\beta)}\big)\Big) = x^3 + 3px - \delta,$$

where $\delta = (\beta - \sigma^2\beta)(\sigma\beta - \beta)(\sigma^2\beta - \sigma\beta)$ and satisfies $\delta^2 = \operatorname{disc}(\beta)$ (if $L = K(\beta)$, then $K\big(\sqrt{\operatorname{disc}(\beta)}\big) = K$). Hence,

$$\operatorname{Irr}\Big(\frac{\gamma}{3}, K\big(\sqrt{\operatorname{disc}(\beta)}\big)\Big) = x^3 + \frac{p}{3}x - \frac{\delta}{3^3}$$

and the next result follows.

Lemma 4. *If $\big(\operatorname{disc}(\beta)\big)/3^6 \in Z_K$, then β is a difference of two conjugates of an integer of the field L.*

Proof: From the last equality and the relation (2), we obtain that $\gamma/3 \in Z_L$, when $\big(\operatorname{disc}(\beta)\big)/3^6 \in Z_K$. Then, the result is immediate, since $(\gamma/3) - \sigma(\gamma/3) = \big(\beta - \sigma^2\beta/3\big) - \sigma\big(\beta - \sigma^2\beta/3\big) = \beta$. ∎

The proof of Theorem 2 is a trivial corollary of the next two lemmas.

Lemma 5. *Let $N_{K/Q}(p)$ be the norm over Q of the integer p of the field K. If $v\big(N_{K/Q}(p)\big) = 0$, then β is a difference of two conjugates (over K) of an integer of L.*

Proof: Note first that the algebraic integer $\big(N_{K/Q}(p)\big)/(p)\sigma(\beta)\sigma^2(\beta)$ belongs to the field $K(\beta)$. By (1), we have

$$r_{K(\beta)/K}\Big(\frac{N_{K/Q}(p)}{p}\sigma(\beta)\sigma^2(\beta)\Big) = \frac{N_{K/Q}(p)}{p} r_{K(\beta)/K}\big(\sigma(\beta)\sigma^2(\beta)\big) = N_{K/Q}(p).$$

Set $N_{K/Q}(p) = \pm 1 + 3k$, where $k \in Z$ and $\eta = \pm\Big(\big(N_{K/Q}(p)\big)/(p)\sigma(\beta)\sigma^2(\beta) - k\Big)$. Then, $\eta \in Z_{K(\beta)}$, $r_{K(\beta)/K}(\eta) = 1$ and

$$\beta = \alpha - \sigma(\alpha),$$

where

$$\alpha = \eta\beta + \beta\sigma(\eta) + \sigma(\beta)\sigma(\eta) \in Z_L.$$

Lemma 6. *If $p/3 \in Z_K$, then β is a difference of two conjugates over K of an algebraic integer with degree $\leqslant 18$ (respectively with degree $\leqslant 9$) over K.*

Proof: Consider the polynomial

$$-27t + x^3 + 3px - 26\delta,$$

in the two variables t and x and with coefficients in L. This polynomial is irreducible and by Hilbert's irreducibility Theorem [**4**, p. 179], there exists $s \in Z$ such that the polynomial $x^3 + 3px - (26\delta + 27s)$ is irreducible over L. Hence, if $\theta^3 + 3p\theta - (26\delta + 27s) = 0$, then

$$\operatorname{Irr}(\theta, L) = x^3 + 3px - (26\delta + 27s) = \operatorname{Irr}\Big(\theta, K\big(\sqrt{\operatorname{disc}(\beta)}\big)\Big),$$

since $\operatorname{Irr}(\theta, L) \in K\big(\sqrt{\operatorname{disc}(\beta)}\big)[x]$. Furthermore, if $\alpha = \gamma/3 + \theta/3$, then $\big(\sigma(\gamma)\big)/3 + \theta/3$ is a conjugate of α over L (and a fortiori over K) and

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

From the relation

$$\Big(\frac{\theta}{3}\Big)^3 + \frac{p}{3}\Big(\frac{\theta}{3}\Big) - \frac{26\delta + 27s}{27} = 0,$$

we obtain that α is a root of the polynomial

$$x^3 - \gamma x^2 + \Big(\frac{\gamma^2}{3} + \frac{p}{3}\Big)x - (\delta + s),$$

since $\gamma^3 + 3p\gamma = \delta$. Hence, α is an algebraic integer provided $\gamma^2/3 \in Z_L$. In fact (as in the proof of [**1**, Theorem 1]), the condition $p/3 \in Z_K$ implies $\gamma^2/3 \in Z_L$. Indeed, by (2), we have $\big(\operatorname{disc}(\beta)\big)/27 \in Z_K$ and from the relation $\gamma\big(\gamma^2 + 3p\big) = \delta$, we obtain that $\gamma^2/3$ is a root of the polynomial $x^3 + 2px^2 + p^2x - \big(\operatorname{disc}(\beta)\big)/27 \in Z_K[x]$. Note finally that from the relations $K(\alpha) \subset K(\gamma, \theta)$ and $K\big(\sqrt{\operatorname{disc}(\beta)}\big) \subset K(\gamma) = L \subset L(\theta) = K(\gamma, \theta)$, we deduce that α is of degree $\leqslant 18$ (respectively of degree $\leqslant 9$) over K. $\square$

PROOF OF THEOREM 3: With the notation above and $K = Q$, it is clear by the relation (2) and Lemma 5, that β is a difference of two conjugates of an integer of the field L, when $v(\mathrm{disc}(\beta)) = 0$. Note also, if $v(\mathrm{disc}(\beta)) \neq 0$, then by the relation (2), we have $v(p) \geqslant 1$ and $v(\mathrm{disc}(\beta)) \geqslant 3$. Hence, if $v(\mathrm{disc}(\beta)) \notin \{3,4,5\}$, then $v(\mathrm{disc}(\beta)) \geqslant 6$ and by Lemma 4, β is a difference of two conjugates of an integer of the field L.

Conversely (the case $v(\mathrm{disc}(\beta)) = 3$ will be treated separately at the end of the proof), suppose that $\beta = \alpha - \sigma(\alpha)$,where $\alpha \in Z_L$ and set $\delta := l\sqrt{m}$, where $l \in Z$ and m is a squarefree rational integer (respectively and set $m = 1$). Then, $Q\left(\sqrt{\mathrm{disc}(\beta)}\right) = Q(\sqrt{m})$.

The relation (1) together with the equality $\beta = \alpha - \sigma(\alpha)$, yields

$$p - 3w = u^2, \tag{3}$$

where the algebraic integers $w = \alpha\sigma(\alpha) + \sigma(\alpha)\sigma^2(\alpha) + \sigma^2(\alpha)\alpha$ and

$$u = \alpha + \sigma(\alpha) + \sigma^2(\alpha)$$

belong to the field $Q(\sqrt{m})$, since they are fix under the action σ. Next we need the following result.

LEMMA 7. *With the notation above and if $\beta = \alpha - \sigma(\alpha)$, where $\alpha \in Z_L$ and satisfies $(\alpha + \sigma(\alpha) + \sigma^2(\alpha))/3 \in Z_L$, then $v(\mathrm{disc}(\beta)) \geqslant 6$.*

PROOF: Let $s = (\alpha + \sigma(\alpha) + \sigma^2(\alpha))/3$. Then, $\sigma(s) = s$, $s \in Z_{Q(\sqrt{m})}$ and $\beta = \theta - \sigma(\theta)$, where $\theta = \alpha - s \in Z_L$ and satisfies $\theta + \sigma(\theta) + \sigma^2(\theta) = 0$. Hence,

$$\beta - \sigma\beta = \theta - \sigma(\theta) - \sigma(\theta - \sigma(\theta)) = -3\sigma(\theta)$$

and $v(\mathrm{disc}(\beta)) \geqslant 6$, since the algebraic integer $(\theta\sigma(\theta)\sigma^2(\theta))^2 = (\mathrm{disc}(\beta))/3^6$ is a rational.

Let us continue the proof of Theorem 3 and suppose that $v(p) \geqslant 1$. If $v(p) = 0$, then $v(\mathrm{disc}(\beta)) = 0$. It follows by (3) that $u^2/3 \in Z_{Q(\sqrt{m})}$ (respectively $u^2/3 \in Z_{Q(\sqrt{m})} = Z$, $u/3 \in Z$ and $v(\mathrm{disc}(\beta)) \geqslant 6$, by Lemma 7. This ends the proof of Theorem 3, since $\mathrm{disc}(\beta)$ is a square of a rational integer). $\square$

Assume now that $m \equiv 2,3[4]$ (respectively $m \equiv 1[4]$). To simplify the computation in what follows, especially when $v(\mathrm{disc}(\beta)) = 3$,we shall use the following lemma.

LEMMA 8. *With the notation above. Then, $\beta = \alpha - \sigma(\alpha)$ for some $\alpha \in Z_L$ if and only if there exist a and $b \in \{-1,0,1\}$ such that*

$$\frac{\gamma + a + b\sqrt{m}}{3} \in Z_L \left(\text{respectively such that } \frac{\gamma + a + b(1+\sqrt{m}/2)}{3} \in Z_L\right).$$

https://doi.org/10.1017/S000497270003762X Published online by Cambridge University Press

In this case we can choose α *so that* $\alpha+\sigma(\alpha)+\sigma^2(\alpha)=a+b\sqrt{m}$ *(respectively so that* $\alpha+\sigma(\alpha)+\sigma^2(\alpha)=a+b(1+\sqrt{m})/2$*).*

PROOF: Suppose that $\beta=\alpha-\sigma(\alpha)$, where $\alpha\in Z_L$. Then, the algebraic number $\theta=\alpha-\gamma/3$ belongs to the field $Q(\sqrt{m})$, since $\beta=\gamma/3-\sigma(\gamma/3)$ and $\theta=\sigma(\theta)$. Furthermore,

$$3\theta=\theta+\sigma(\theta)+\sigma^2(\theta)=\alpha+\sigma(\alpha)+\sigma^2(\alpha).$$

Set (as above) $u=\alpha+\sigma(\alpha)+\sigma^2(\alpha)$. Then, $u\in Z_{Q(\sqrt{m})}$ and $(\gamma+u)/3=(\gamma+3\theta)/3=\alpha\in Z_L$. Writing $u=a_0+b_0\sqrt{m}$ (respectively $u=a_0+b_0(1+\sqrt{m})/2$), $a_0=a+3a_1$ and $b_0=b+3b_1$, where a_0, b_0,a_1 and $b_1\in Z$, and a and $b\in\{-1,0,1\}$, we obtain the first implication. The second one follows from the equalities $\beta=(\gamma/3)-\sigma(\gamma/3)=(\gamma+u)/3-\sigma\big((\gamma+u)/3\big)$, where $u=a+b\sqrt{m}$ (respectively, where $u=a+b(1+\sqrt{m})/2$), since $\sigma(u)=u$.

Note that Lemma 8 is also true when the extension $Q(\beta)/Q$ is normal: $\beta=\alpha-\sigma(\alpha)$ for some $\alpha\in Z_{Q(\beta)}$ if and only if one of the three algebraic numbers $(\gamma+u)/3$, where $u\in\{-1,0,1\}$, is an algebraic integer. At a first glance Theorem 3 seems to be an easy corollary of Lemma 8, however using only this lemma the proof needs a non trivial computation.

Let us end the proof of Theorem 3. From the relation $\big((\gamma+u/3)-u/3\big)^3+p/3\big((\gamma+u)/3-u/3\big)=(l\sqrt{m})/3^3$, we obtain

$$\operatorname{Irr}\Big(\frac{\gamma+u}{3},Q\big(\sqrt{m}\big)\Big)=x^3-ux^2+\Big(\frac{u^2}{3}+\frac{p}{3}\Big)x-\frac{3pu+u^3+l\sqrt{m}}{3^3}.$$

It follows by Lemma 8 that

$$\frac{u^2}{3}\in Z_{Q(\sqrt{m})} \tag{4}$$

and

$$\frac{3pu+u^3+l\sqrt{m}}{3^3}\in Z_{Q(\sqrt{m})}. \tag{5}$$

Set $u:=a+b\sqrt{m}$ (respectively $u=a+b(1+\sqrt{m})/2$), where a and $b\in Z$. Then, the relation (4) can also be written

$$v\big(a^2+b^2m\big)\geqslant 1 \text{ and } v(2ab)\geqslant 1$$
$$\big(\text{respectively } v\big(A(2a-b)+mb^2\big)\geqslant 1,\ \text{and } v(Ab)\geqslant 1,\ \text{where } A=2a+b\big).$$

It follows when $v(m)=0$ that $v(a)\geqslant 1$ and $v(b)\geqslant 1$ (respectively $v(b)\geqslant 1$ and $v(a)\geqslant 1$). Hence, $u/3\in Z_L$ and by Lemma 7, $v\big(\operatorname{disc}(\beta)\big)\geqslant 6$.

Suppose now $v(m) = 1$ and write the relation (5)

$$v\big(a^3 + 3amb^2 + 3pa\big) \geqslant 3$$
$$\text{(5.1)} \quad \big(\text{respectively } v\big(A^3 + 3Amb^2 + 12Ap - \big(b^3m + 3A^2b + 12bp + 8l\big)\big) \geqslant 3\big)$$

and

$$v\big(b^3m + 3ba^2 + 3bp + l\big) \geqslant 3$$
$$\text{(5.2)} \quad \big(\text{respectively } v\big(b^3m + 3A^2b + 12bp + 8l\big) \geqslant 3\big).$$

Then, by (5.1) we have $v(a) \geqslant 1$ (respectively $v(A) \geqslant 1$). Furthermore, by (5.2) we obtain $v\big(b^3m\big) \geqslant 2$ and $v(b) \geqslant 1$ (respectively $v\big(b^3m\big) \geqslant 2$, $v(b) \geqslant 1$ and $v(a) \geqslant 1$), when $v(l) \geqslant 2$. Hence, $u/3 \in Z_L$ and by Lemma 7, $v\big(\operatorname{disc}(\beta)\big) \geqslant 6$.

It remains now to consider the case where $v(l) = v(m) = 1$ (or where $v\big(\operatorname{disc}(\beta)\big) = 3$). A short computation shows that the relations (5.1), (4) and $v(a) \geqslant 1$ are all equivalent (respectively the relations (4) and $v(A) \geqslant 1$ are equivalent. Furthermore, (5.1) together with (4) implies (5.2)).

Hence, by Lemma 8, $\beta = \alpha - \sigma(\alpha)$ for some $\alpha \in Z_L$ if and only if there exist a and $b \in \{-1, 0, 1\}$ satisfying the relations $v(a) \geqslant 1$ and (5.2) (respectively, the relations $v(2a + b) \geqslant 1$ and (5.1)). It follows that $a = 0$, $b = \pm 1$ (if $b = 0$, then $v(l) > 1$). (Respectively, it follows that $a = b = \pm 1$ (if $a = b = 0$, then $v(l) > 1$)) and $\beta = \alpha - \sigma(\alpha)$ where $\alpha \in Z_L$ if and only if one of the two relations

$$v(m + 3p \pm l) \geqslant 3 \quad (\text{respectively } v(m + 12p \pm 8l) \geqslant 3),$$

holds.

Note finally, if $\operatorname{Irr}(\beta, Q) = x^3 + 3x + 6$, then $\operatorname{disc}(\beta) = -3^3 2^3 5$, $m = -30$, $l = \pm 6$ and $m + 3p + l \in \{-27, -15\}$. Hence, β is a difference of two conjugates (over $Q\big(\sqrt{-30}\big)$) of an algebraic integer $\alpha \in L$ with $\operatorname{Irr}\big(\alpha, Q\big(\sqrt{-30}\big)\big) = x^3 - \sqrt{-30}x^2 - 9x + \sqrt{-30}$ ($a = 0$, $b = 1$ and $u = \sqrt{-30}$). However, if $\operatorname{Irr}(\beta, Q) = x^3 + 3x + 2$, then $\operatorname{disc}(\beta) = -3^3 2^3$, $m = -6$, $l = \pm 6$, $m + 3p + l \in \{-3, 9\}$ and β is not a difference of two conjugates of an integer of the field L. (Respectively, note finally that at least one of these inequalities holds (respectively, that these inequalities does not hold) infinitely many times. Indeed, let r be a prime rational integer greater than 3 and let $n \in \{r, 2r, 4r\}$ and satisfies (respectively and does not satisfy) $n \equiv \varepsilon_1[9]$, where $\varepsilon_1 \in \{-1, 1\}$. Then, $v(n) = 0$ and n is not a cube of a rational integer. Set $\operatorname{Irr}(\beta, Q) := x^3 - n$. Then, $\operatorname{disc}(\beta) = -27n^2$, $m = -3$, $l = 3\varepsilon_2 n$, where $\varepsilon_2 \in \{-1, 1\}$, and $v(m + 8\varepsilon l) \geqslant 3$, where ε satisfies $\varepsilon\varepsilon_1\varepsilon_2 = -1$ (respectively and $v(m + 8\varepsilon l) < 3$, where $\varepsilon \in \{-1, 1\}$). This ends the proof of Theorem 3. ∎

References

[1] A. Dubickas, 'On numbers which are differences of two conjugates of an algebraic integer', *Bull. Austral. Math. Soc.* **65** (2002), 439–477.

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

[3] S. Lang, *Algebra* (Addison-Wesley Publishing, Reading, MA, 1965).

[4] A. Schinzel, *Selected topics on polynomials* (University of Michigan, Ann Arbor, MI, 1982).

King Saud University
Deptartment of Mathematics
PO Box 2455
Riyadh 11451
Saudi Arabia