Indag. Mathem., N.S., 17 (1), 31–36 March 27, 2006

Additive Hilbert's Theorem 90 in the ring of algebraic integers

by Artūras Dubickas

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania

Communicated by Prof. R. Tijdeman at the meeting of March 21, 2005

ABSTRACT

For a number field K, we give a complete characterization of algebraic numbers which can be expressed by a difference of two K-conjugate algebraic integers. These turn out to be the algebraic integers whose Galois group contains an element acting as a cycle on some collection of conjugates which sum to zero. Hence there are no algebraic integers which can be written as a difference of two conjugate algebraic numbers but cannot be written as a difference of two conjugate algebraic integers. A generalization of the construction to a commutative ring is also given. Furthermore, we show that for $n \geqslant 3$ there exist algebraic integers which can be written as a linear form in n K-conjugate algebraic numbers but cannot be written by the same linear form in K-conjugate algebraic integers.

1. INTRODUCTION

A classical additive (multiplicative) form of Hilbert's Theorem 90 states that, given a finite cyclic Galois extension F/K generated by σ, an element $\beta \in F$ has trace zero (norm 1) with respect to the extension F/K iff $\beta = \alpha - \sigma(\alpha)$ ($\beta = \alpha/\sigma(\alpha)$) for some $\alpha \in F$ (see, e.g., p. 290 and p. 288 in [9] or [7]). Noncommutative versions of Hilbert's Theorem 90 for division rings were given in [8] and, among other things, in [10].

In [5] we considered a variation of Hilbert's Theorem 90 without any restrictions on α, namely, given a field K, describe algebraic over K numbers β which can

MSC: 11R04, 11R09, 11R32, 13B25

Key words and phrases: Conjugate algebraic integers, Galois group, Hilbert's Theorem 90

E-mail: arturas.dubickas@maf.vu.lt (A. Dubickas).

be written as $\alpha - \alpha'$ (or α/α') with arbitrary K-conjugate numbers α and α'. The purpose of this paper is to give a complete characterization of algebraic integers expressible by a difference of two K-conjugate numbers which may be viewed as an arithmetical version of our variation of additive Hilbert's Theorem 90. (Partial results on this and similar problems were earlier obtained by the author [2] and T. Zaimi [14–16].)

Let K be a number field. Given an algebraic number β of degree d over K, we denote by G the Galois group of the normal closure of $K(\beta)$ over K. We prove the following theorem.

Theorem. *An algebraic number β can be written as a difference $\alpha - \alpha'$ of two K-conjugate numbers α and α' if and only if there is an element in G acting as a permutation group on conjugates of β which acts as an s-cycle on certain collection of s conjugates which sum to zero. Furthermore, if β is an algebraic integer then α too can be chosen to be an algebraic integer of degree at most $s|G|$ over K.*

Most important here is the second part of the statement, as the first part is a very slight variation of Hilbert's Theorem 90 in its classical form and was proved in [5]. (Necessity: write $\beta = \alpha - \tau(\alpha)$, where τ is an automorphism of the Galois closure of $K(\alpha, \beta)$ over K which maps α to α', act by the cyclic group generated by τ, and the result follows easily for any K of characteristic zero, by adding all obtained equalities. Sufficiency: defining α by $\sum_{i=1}^{s}(1 - i/s)\sigma^{i-1}(\beta)$, where $\sigma^{s}(\beta) = \beta$, and using $\sum_{i=1}^{s}\sigma^{i-1}(\beta) = 0$ we have $\alpha - \sigma(\alpha) = \beta$ for every field of characteristic zero.) It was the second, multiplicative, part on numbers which can be represented as α/α' in which we actually required K to be an algebraic number field. The answer turned out to be the same with 'sum to zero' being replaced by 'multiply to a root of unity', where the proof of sufficiency is not straightforward.

With an additional arithmetical condition on β (to be an algebraic integer) the roles of additive and multiplicative settings are in some sense reversed. In [2] we proved that if a unit β can be written as α/α' with K-conjugate numbers α and α', then α can be chosen to be a unit too. The method similar to that in [5] was used. However the additive setting is more difficult. In general, the question whether every algebraic integer β which can be written as a difference of two K-conjugate algebraic numbers can be also written as a difference of two K-conjugate algebraic integers was posed by C.J. Smyth. We could not settle this problem in [2] and obtained only partial results for cubic integers instead. T. Zaimi [14–16] also considered this and similar problems. The above theorem answers this question in the affirmative. Note that the general upper bound $s|G|$ for the degree of α coincides with that obtained in Theorem 1 [2] for some special cubic algebraic integers. Since $s \leqslant d$ and $|G| \leqslant d!$, the degree of the algebraic integer α over K whose existence is claimed by the theorem will always be at most $dd!$. On the other hand, it is at least $\sqrt{d}$.

The proof of the theorem is given in Section 2, where we also give a generalization of the construction to an integral domain A whose quotient field K satisfies certain mild assumption concerning irreducibility of polynomials. The construction is in some sense a lifting of the pair of K-conjugate algebraic numbers α, α' whose difference $\alpha - \alpha'$ is an algebraic integer to the pair of K-conjugate algebraic integers $\gamma + \alpha$, $\gamma + \alpha'$. There are however certain limits beyond which this argument cannot be extended. For instance, in [4] we considered the numbers β which can be represented by a linear form $k_1\alpha_1 + \cdots + k_n\alpha_n$ in K-conjugate $\alpha_1, \dots, \alpha_n$, where $k_1, \dots, k_n \in K$ add to zero. A natural extension of the theorem from $n = 2$ to $n \geqslant 3$ would be the following. If an algebraic integer β can be written as a linear form $k_1\alpha_1 + \cdots + k_n\alpha_n$ in K-conjugate algebraic numbers $\alpha_1, \dots, \alpha_n$, where $k_1, \dots, k_n \in \mathcal{O}_K$ (the ring of integers of K), then $\alpha = \alpha_1$ can be chosen to be an algebraic integer too. (Of course, except for $k_1 + \cdots + k_n = 0$, one has to assume some additional condition on the greatest common divisor of $k_1, \dots, k_n$, like, for example, the only algebraic integers ζ for which we have $\zeta^{-1}k_1, \dots, \zeta^{-1}k_n \in \mathcal{O}_K$ are units.) We prove however that such extension of the theorem is not true for any $n > 2$. Setting $k_1 = k_2 = 1, k_3 = -2, k_4 = \cdots = k_n = 0$, in Section 3 we will give an example of the algebraic integer β which can be written as a linear form in K-conjugate algebraic numbers, but cannot be written by the same form in K-conjugate algebraic integers.

2. LIFTING

Proof of the Theorem. Let $\sigma \in G$ be an automorphism which acts as the s-cycle on conjugates of the algebraic integer β adding to zero $\sum_{i=1}^{s} \sigma^{i-1}(\beta) = 0$. Set $\alpha = \sum_{i=1}^{s}(1 - i/s)\sigma^{i-1}(\beta)$. Then $\alpha - \sigma(\alpha) = \beta$. Write

$$F(X, Y) = (X + \alpha)(X + \sigma(\alpha) \cdots \big(X + \sigma^{s-1}(\alpha)\big) - Y.$$

By Hilbert's irreducibility theorem [6] (see p. 298 in [11] and a nice special case [1]), there exist $t \in \mathbb{N}$ such that $F(X, t)$ is irreducible in $L[X]$, where L is the normal closure of $K(\beta)$ over K. (Of course, L is also the normal closure of $K(\alpha)$ over K.) Let t be one of these, and let S be the set of s roots of the equation $F(X, t) = 0$. Then $\gamma \in S$ is of degree s over L with S being its conjugate set. Take an arbitrary automorphism of the normal closure of $L(\gamma)$ over K which takes α to $\sigma(\alpha)$. The key observation is that it maps the equation $F(X, t) = 0$ to itself, so, in particular, S to S. Suppose that this automorphism maps γ to γ'. Then $\gamma + \alpha$ and $\gamma' + \sigma(\alpha)$ are conjugate over K. However γ and γ' are conjugate over L, hence so are $\gamma + \sigma(\alpha)$ and $\gamma' + \sigma(\alpha)$. It follows that the latter two are conjugate over its subfield K. Since $\gamma + \alpha$ and $\gamma' + \sigma(\alpha)$ are K-conjugate, we conclude that $\gamma + \alpha$ and $\gamma + \sigma(\alpha)$ are K-conjugate. Their difference is $(\gamma + \alpha) - (\gamma + \sigma(\alpha)) = \alpha - \sigma(\alpha) = \beta$, so it remains to show that $\gamma + \alpha$ is an algebraic integer of degree at most $s|G|$ over K. Indeed, $\gamma + \alpha$ is a root of the monic polynomial

$$\begin{aligned} F(X - \alpha, t) &= X\big(X + \sigma(\alpha) - \alpha\big) \cdots \big(X + \sigma^{s-1}(\alpha) - \alpha\big) - t \\ &= X(X - \beta)\big(X - \beta - \sigma(\beta)\big) \cdots \\ &\quad \big(X - \beta - \sigma(\beta) - \cdots - \sigma^{s-2}(\beta)\big) - t \end{aligned}$$

of degree s which is irreducible in $L[X]$ (because so is $F(X,t)$) and whose coefficients are algebraic integers. Thus $\gamma+\alpha$ is an algebraic integer and its degree over K is $\leqslant s[L:K]=s|G|$, which completes the proof of the theorem. □

In principle, the above proof is not entirely constructive, but relying on some effective version of Hilbert's irreducibility theorem (see, e.g., [11]) it is effective. So a bound for the height of $\gamma+\alpha$ can be given in terms of d and the height of β only. However, for 'most' β already the polynomial $F(X,1)$ (with $t=1$) is irreducible in $L\{X\}$, so a corresponding γ can be found from the equation $F(X,1)=0$.

Let A be an *integral domain*, namely, a commutative ring that has an identity element and has no divisors of 0. Suppose that its quotient field K has the following property: for every polynomial $Q(X)\in L[X]$, where L/K is a finite Galois extension, there exists a monic polynomial $P(X)\in A[X]$, not a constant, such that $P(Q(X))$ is irreducible in $L[X]$. Recall that an element ω is called *integral* over A if it is a root of a monic polynomial in $A[X]$ (see p. 335 in [9]).

Proposition. *With the above conditions on A and K, assume that α and α' are K-conjugate. If $\alpha-\alpha'$ is integral over A then there is a number γ, algebraic over K, such that $\gamma+\alpha$ and $\gamma+\alpha'$ are integral over A and K-conjugate.*

Proof. There is no loss of generality to assume that $\alpha\neq\alpha'$ for otherwise the claim is trivial. Set $Q(X)=(X+\alpha)(X+\sigma(\alpha))\cdots(X+\sigma^{s-1}(\alpha))$, where σ is an automorphism of the Galois closure L of $K(\alpha)$ over K mapping α to α'. Here, $\sigma^{s}(\alpha)=\alpha$. Define γ as an arbitrary root of $P(Q(X))=0$, where $P(X)\in A[X]$ is the monic polynomial for which $P(Q(X))$ is irreducible in $L[X]$. Since $\alpha-\sigma(\alpha)$ is integral over A, so are also its conjugates $\sigma^{j-1}(\alpha)-\sigma^{j}(\alpha)$, $j=2,\dots,s-1$, and so are their sums $\alpha-\sigma^{j}(\alpha)$, $j=1,\dots,s-1$. The coefficients of the polynomial $Q(X-\alpha)=X(X+\sigma(\alpha)-\alpha)\cdots(X+\sigma^{s-1}(\alpha)-\alpha)$ are therefore integral over A, hence so are the coefficients of $P(Q(X-\alpha))$. If follows that $\gamma+\alpha$ is integral over A. Furthermore, by the same argument as in the proof of the theorem, $\gamma+\alpha$ and $\gamma+\sigma(\alpha)$ are K-conjugate, which completes the proof of the proposition. □

Of course, the Theorem is a corollary to the Proposition with K being a number field, $A=\mathcal{O}_K$, $\alpha=\sum_{i=1}^{s}(1-i/s)\sigma^{i-1}(\beta)$, $P(X)=X-t$.

3. EXAMPLE

Take two distinct primes p and p' such that $\sqrt{p},\sqrt{p'},\sqrt{pp'}\notin K$, where K is a number field. Set $\beta=\sqrt{p}+\sqrt{p'}+\sqrt{pp'}$ which is clearly an algebraic integer. Then, as in [4], we see that $\beta=\alpha_1+\alpha_2-2\alpha_3$ with $\alpha_1=(-2\sqrt{p}+\sqrt{p'}+2\sqrt{pp'})/4$ and its K-conjugates

$$\alpha_2=\left(2\sqrt{p}+\sqrt{p'}-2\sqrt{pp'}\right)/4,\qquad \alpha_3=\left(-2\sqrt{p}-\sqrt{p'}-2\sqrt{pp'}\right)/4.$$

We claim that β cannot be written in the form $\omega+\omega_2-2\omega_3$ with ω_2,ω_3 being K-conjugate to an algebraic integer ω. Suppose that $\beta=\omega+\omega_2-2\omega_3$. Let F be the Galois closure of $K(\omega)$ over K. Then (see the proof of Theorem 1 in [4]) F as a linear space over K can be written as $F = \mathcal{L}(\beta) \oplus U$ for some linear space U, where $\mathcal{L}(\beta)$ is the linear space spanned by the conjugates of β and where $\oplus$ stands for the direct sum. Write $\omega = \eta + \gamma$ with $\eta \in \mathcal{L}(\beta)$, $\gamma \in U$. It follows that

$$\beta = \omega + \omega_2 - 2\omega_3 = \eta + \eta_2 - 2\eta_3 + \gamma + \gamma_2 - 2\gamma_3,$$

where η_2, η_3 are K-conjugate to η and γ_2, γ_3 are K-conjugate to γ. So $\beta = \eta + \eta_2 - 2\eta_3$ and $\gamma + \gamma_2 - 2\gamma_3 = 0$. The latter equality is impossible, unless $\gamma = \gamma_2 = \gamma_3$ (see, e.g., [12,13] and [3] for such results). The Galois group of β over K is the Klein 4-group, generated by two automorphisms $\sqrt{p} \to -\sqrt{p}$ and $\sqrt{p'} \to -\sqrt{p'}$. Note that $\mathcal{L}(\beta) = \langle \sqrt{p}, \sqrt{p'}, \sqrt{pp'} \rangle$. Writing $\eta = x_1\sqrt{p} + x_2\sqrt{p'} + x_3\sqrt{pp'}$ with $x_1, x_2, x_3 \in K$ and applying three automorphisms different from identity we obtain three remaining conjugates of η

$$-x_1\sqrt{p} + x_2\sqrt{p'} - x_3\sqrt{pp'}, \qquad x_1\sqrt{p} - x_2\sqrt{p'} - x_3\sqrt{pp'},$$
$$-x_1\sqrt{p} - x_2\sqrt{p'} + x_3\sqrt{pp'}.$$

Now, solving the linear system $1 = x_1 - x_1 - 2x_1$, $1 = x_2 + x_2 + 2x_2$, $1 = x_3 - x_3 + 2x_3$ obtained from $\beta = \eta + \eta_2 - 2\eta_3$, where η_2 and η_3 are, respectively, first and second numbers in the list, we get $x_1 = -1/2$, $x_2 = 1/4$, $x_3 = 1/2$. Since $\gamma_2 = \gamma_3 = \gamma$, this implies that $\omega = \gamma + (-2\sqrt{p} + \sqrt{p'} + 2\sqrt{pp'})/4$, $\omega_2 = \gamma + (2\sqrt{p} + \sqrt{p'} - 2\sqrt{pp'})/4$, $\omega_3 = \gamma + (-2\sqrt{p} - \sqrt{p'} - 2\sqrt{pp'})/4$. However then ω is not an algebraic integer, because $\omega - \omega_3 = \sqrt{pp'} + \sqrt{p'}/2$ is not. Note that all three numbers $\omega, \omega_2, \omega_3$ must be distinct, for otherwise either β or $\beta/2$ is a difference of two K-conjugate numbers, which is impossible, by the first part of the theorem, because none of the sums of two distinct conjugates of β is equal to zero. Hence η, η_2, η_3 must be distinct. This leaves the five cases, namely, when η_2 and η_3 are, respectively, second and first, first and third, third and first, second and third, third and second numbers in the above list of three. Each of these can be easily dealt with in the same manner. For example, with η_2, η_3 being the third and the first numbers, we get $x_1 = 1/2$, $x_2 = -1/2$, $x_3 = 1/4$. Then ω is not an algebraic integer, because $\omega - \omega_3 = \sqrt{p} + \sqrt{pp'}/2$ is not. Likewise, a contradiction is obtained in all five cases. Consequently, there is no algebraic integer ω for which $\omega + \omega_2 - 2\omega_3 = \sqrt{p} + \sqrt{p'} + \sqrt{pp'} = \beta$ (although there exists such algebraic number $\omega = (-2\sqrt{p} + \sqrt{p'} + 2\sqrt{pp'})/4$).

ACKNOWLEDGEMENT

The research was partially supported by the Lithuanian State Science and Studies Foundation.

REFERENCES

[1] Cavachi M. – On a special case of Hilbert's irreducibility theorem, J. Number Theory **82** (2000) 96–99.

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

[3] Dubickas A. – On the degree of a linear form in conjugates of an algebraic number, Illinois J. Math. **46** (2002) 571–585.

[4] Dubickas A. – Additive relations with conjugate algebraic numbers, Acta Arith. **107** (2003) 35–43.

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

[6] Hilbert D. – Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten, J. Reine Angew. Math. **110** (1892) 104–129.

[7] Houston E.G. – A linear algebra approach to cyclic extensions in Galois theory, Amer. Math. Monthly **100** (1993) 64–66.

[8] Lam T.Y., Leroy A. – Hilbert 90 Theorems over division rings, Trans. Amer. Math. Soc. **345** (1994) 595–622.

[9] Lang S. – Algebra, third ed., Grad. Texts in Math., vol. 211, Springer-Verlag, New York, Berlin, 2002.

[10] Nuss P. – Noncommutative descent and non-abelian cohomology, K-Theory **12** (1997) 23–74.

[11] Schinzel A. – Polynomials with special regard to reducibility, Encyclopedia of Mathematics and Its Applications, vol. 77, Cambridge Univ. Press, Cambridge, 2000.

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

[13] Smyth C.J. – Additive and multiplicative relations connecting conjugate algebraic numbers, J. Number Theory **23** (1986) 243–254.

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

[15] Zaimi T. – On the integer form of the Additive Hilbert's Theorem 90, J. Linear Algebra and Appl. **390** (2004) 175–181.

[16] Zaimi T. – The cubics which are differences of two conjugates of an algebraic integer, J. Théor. des Nombres de Bordeaux, submitted for publication.

(Received February 2005)