

## CONJUGATE ALGEBRAIC NUMBERS CLOSE TO A SYMMETRIC SET

A. DUBICKAS

ABSTRACT. A new proof is presented for the Motzkin theorem saying that if a set consists of  $d - 1$  complex points and is symmetric relative to the real axis, then there exists a monic, irreducible, and integral polynomial of degree  $d$  whose roots are as close to each of these  $d - 1$  points as we wish. Unlike the earlier proofs, the new proof is efficient, i.e., it gives both an explicit construction of the polynomial in question and the location of its  $d$ th root.

### §1. INTRODUCTION

Let  $d \geq 2$  be an integer, and let  $\alpha$  be an algebraic integer of degree  $d$  over the field  $\mathbb{Q}$  of rational numbers. Many results are known about sets in the complex plane that contain (or do not contain) the number  $\alpha$  together with all its conjugate numbers. For instance, in [1, 3, 10, 11] intervals on the real axis were considered, and in [4, 5] sets on the plane were treated. Of course, the set of all numbers conjugate to an algebraic integer possesses natural arithmetic properties, and this implies certain restrictions on the disposition of such a set. Any such set is symmetric relative to the real axis, and the basic symmetric functions take integral values at the points of this set.

However, any symmetric set of  $d - 1$  points can be approximated by numbers conjugate to an algebraic integer of degree  $d$ . The Motzkin theorem has been known for more than fifty years; it states that if  $S = \{\lambda_1, \lambda_2, \dots, \lambda_{d-1}\}$  is a set of  $d - 1$  complex points symmetric relative to the real axis, then for any positive  $\varepsilon$  there exists an algebraic integer  $\alpha = \alpha_d$  of degree  $d$  such that the numbers  $\alpha_1, \alpha_2, \dots, \alpha_{d-1}$  conjugate to  $\alpha$  lie (respectively) in the  $\varepsilon$ -neighborhoods of the points  $\lambda_1, \lambda_2, \dots, \lambda_{d-1}$ . A usual proof of this fact employs the Kronecker joint approximation theorem (see, e.g., [9, pp. 49–51]). Such a proof is inefficient, since it gives no method for constructing the number  $\alpha$ , or rather, its minimal polynomial over the field of rational members. Neither the location of the  $d$ th conjugate, i.e., of  $\alpha$  itself, nor its magnitude becomes clear.

Our goal in this paper is to give a simple and *efficient* proof of the following theorem.

**Theorem.** *Let  $S = \{\lambda_1, \lambda_2, \dots, \lambda_{d-1}\}$  be a set of  $d - 1$  complex points that is symmetric relative to the real axis, and let*

$$u = \max\{1, |\lambda_1|, \dots, |\lambda_{d-1}|\}, \quad v = \min_{1 \leq i < j \leq d-1} |\lambda_i - \lambda_j|.$$

*Then, for every  $\varepsilon$  with  $0 < \varepsilon < 1$  and every even integer*

$$s \geq (2/\varepsilon)d^2(u/v)^{d-2} + du$$

*there exists an algebraic integer  $\alpha = \alpha_d$  of degree  $d$  such that, after proper reordering, the numbers  $\alpha_1, \alpha_2, \dots, \alpha_{d-1}$  conjugate to  $\alpha$  satisfy  $|\alpha_j - \lambda_j| < \varepsilon$ ,  $j = 1, \dots, d - 1$ . Moreover,*

---

2000 *Mathematics Subject Classification.* Primary 11D75, 11J25.

*Key words and phrases.* Integral polynomial, Eisenstein criterion, Salem numbers.

The work was supported in part by the Lithuanian Foundation for Research and Science.

the trace of  $\alpha$  is equal to  $s$ , and for  $\varepsilon < v/2$  the number  $\alpha_j$ ,  $j = 1, \dots, d-1$ , is real if and only if so is  $\lambda_j$ .

Observe that the number

$$\lambda = \lambda_d = s - \lambda_1 - \dots - \lambda_{d-1}$$

is real, because  $S$  is symmetric relative to the real axis. (Therefore, the set  $S \cup \{\lambda_d\}$  is symmetric.) Since the trace of  $\alpha$  equals  $s$ , it is easy to check that

$$|\alpha - \lambda| \leq |\alpha_1 - \lambda_1| + \dots + |\alpha_{d-1} - \lambda_{d-1}| < (d-1)\varepsilon,$$

so that  $\alpha$  is close to  $\lambda$ . It is also clear that if  $\varepsilon < v/2$ , then  $\alpha$  is real because, by the theorem, the number of complex (nonreal) numbers among  $\alpha_1, \dots, \alpha_{d-1}$  is even.

## §2. PROOF OF THE THEOREM

Let  $\lambda_d$  be defined as above, and let

$$\sigma_1 = \lambda_1 + \dots + \lambda_d = s, \quad \sigma_2 = \lambda_1\lambda_2 + \dots + \lambda_{d-1}\lambda_d, \quad \dots, \quad \sigma_d = \lambda_1\lambda_2 \dots \lambda_d$$

be the elementary symmetric functions of  $\lambda_1, \lambda_2, \dots, \lambda_d$ . Clearly, all numbers  $\sigma_2, \dots, \sigma_d$  are real. We put  $b_1 = \sigma_1 = s$ . Let  $b_2$  be an even number nearest to  $\sigma_2$ ,  $\dots$ , let  $b_{d-1}$  be an even number nearest to  $\sigma_{d-1}$ , and let  $b_d$  be a number of the form  $4k+2$ ,  $k \in \mathbb{Z}$ , nearest to  $\sigma_d$ . We claim that the polynomial

$$P(x) = x^d - b_1x^{d-1} + b_2x^{d-2} - \dots + (-1)^n b_n = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_d)$$

is as required.

Indeed,  $P(x)$  is irreducible over  $\mathbb{Q}$  by the Eisenstein criterion; therefore,  $\alpha$  is an algebraic integer of degree  $d$  and with trace  $s$ . As in [2], we note that if  $P'(\lambda_j) \neq 0$ , then  $P(x)$  has a root  $\alpha_j$  such that

$$|\alpha_j - \lambda_j| \leq d|P(\lambda_j)|/|P'(\lambda_j)|.$$

(Indeed, if  $\alpha_j$  is a root nearest to  $\lambda_j$ , then the modulus of the quantity

$$\frac{P'(\lambda_j)}{P(\lambda_j)} = \sum_{i=1}^d \frac{1}{\alpha_i - \lambda_j}$$

does not exceed  $d/|\alpha_j - \lambda_j|$ .) To obtain the inequalities  $|\alpha_j - \lambda_j| < \varepsilon$ , it suffices to show that

$$d|P(\lambda_j)| < \varepsilon|P'(\lambda_j)|$$

for  $j = 1, 2, \dots, d-1$ .

We write  $P(x) = F(x) + G(x)$ , where  $F(x) = (x - \lambda_1) \dots (x - \lambda_d)$  and

$$G(x) = (b_2 - \sigma_2)x^{d-2} - (b_3 - \sigma_3)x^{d-3} + \dots + (-1)^d(b_d - \sigma_d).$$

Clearly,  $P(\lambda_j) = G(\lambda_j)$ . By the choice of  $b_2, \dots, b_d$ , we have  $|b_j - \sigma_j| \leq 1$  for  $j = 2, 3, \dots, d-1$ , and  $|b_d - \sigma_d| \leq 2$ . Consequently,

$$|G(\lambda_j)| \leq |\lambda_j|^{d-2} + \dots + |\lambda_j| + 2 \leq du^{d-2},$$

whence  $d|P(\lambda_j)| \leq d^2u^{d-2}$ .

We shall show that  $\varepsilon|P'(\lambda_j)| > d^2u^{d-2}$ . As above,  $|G'(\lambda_j)| \leq (d-1)(d-2)u^{d-3}/2$ , which yields  $\varepsilon|G'(\lambda_j)| < d^2u^{d-2}$ . Next, we have

$$|F'(\lambda_j)| = \prod_{1 \leq i \leq d, i \neq j} |\lambda_j - \lambda_i|.$$

All factors except  $|\lambda_d - \lambda_j|$  are bounded below by  $v$ , and

$$|\lambda_d - \lambda_j| = |s - \lambda_1 - \dots - 2\lambda_j - \dots - \lambda_{d-1}| \geq s - du \geq (2/\varepsilon)d^2(u/v)^{d-2}.$$

Thus,  $|F'(\lambda_j)| \geq (2/\varepsilon)d^2(u/v)^{d-2}v^{d-2} = (2/\varepsilon)d^2u^{d-2}$ , which proves the inequality

$$\varepsilon|F'(\lambda_j)| \geq 2d^2u^{d-2}.$$

Since  $P'(\lambda_j) = F'(\lambda_j) + G'(\lambda_j)$ , we easily obtain

$$\varepsilon|P'(\lambda_j)| \geq \varepsilon|F'(\lambda_j)| - \varepsilon|G'(\lambda_j)| > 2d^2u^{d-2} - d^2u^{d-2} = d^2u^{d-2},$$

whence  $d|P(\lambda_j)| < \varepsilon|P'(\lambda_j)|$ .

Under the condition  $\varepsilon < v/2$ , the disks of radius  $\varepsilon$  centered at  $\lambda_1, \dots, \lambda_{d-1}$  are disjoint. If, say,  $\lambda_j$  is real ( $1 \leq j \leq d-1$ ), then so is  $\alpha_j$ . Indeed, otherwise, since  $\alpha = \alpha_d$  lies in none of the disks, while the numbers  $\alpha_j$  and  $\alpha_\ell = \bar{\alpha}_j \neq \alpha_j$  lie in one and the same disk, we see that at least one of the disks is empty, a contradiction.

### §3. APPLICATION TO SALEM NUMBERS

The idea of the above proof is based on the fact that near any polynomial  $F(x) = x^d - \sigma_1x^{d-1} + \dots + (-1)^d\sigma_d$  with real coefficients we can find an irreducible polynomial  $P(x) = x^d - b_1x^{d-1} + \dots + (-1)^db_d$ ; the word “near” means that  $H(F - P) \leq 2$ . In 1962, Turán conjectured that the height can be replaced by the length, i.e.,  $L(H - P) \leq c$  with an absolute (independent of  $d$ ) constant  $c$ . Although this conjecture has not been proved as yet, a result of Györy is known, saying that for any  $F(x) \in \mathbb{Z}[x]$  there is an irreducible polynomial of the form  $P(x) = F(x) + b$  with  $b \in \mathbb{Z}$  and  $|b| \leq c(d)$ , where  $c(d)$  is some explicit function of  $d$ . We shall use this result to present an application of our theorem.

Recall that an algebraic integer  $\beta > 1$  of degree  $d = 2m + 2$ ,  $m \in \mathbb{N}$ , is called a *Salem number* if the numbers conjugate to  $\beta$  are of the form

$$\beta^{-1}, e^{\phi_1\sqrt{-1}}, e^{-\phi_1\sqrt{-1}}, \dots, e^{\phi_m\sqrt{-1}}, e^{-\phi_m\sqrt{-1}},$$

where  $0 < \phi_1, \dots, \phi_m < \pi$ . We prove that for any  $0 < \xi_1 < \xi_2 < \dots < \xi_m < \pi$  there exists a Salem number  $\beta$  of degree  $d = 2m + 2$  such that the numbers conjugate to  $\beta$  have arguments as close to  $\xi_1, \xi_2, \dots, \xi_m$  as we wish and have any sufficiently large trace.

Indeed, first we apply the theorem to the real numbers

$$\lambda_1 = 2 \cos \xi_1, \lambda_2 = 2 \cos \xi_2, \dots, \lambda_m = 2 \cos \xi_m,$$

but instead of an even trace  $s$  we now choose any sufficiently large trace  $s$ , and employ the Györy result in place of the Eisenstein criterion. (The inequality  $s \geq (2/\varepsilon)d^2(u/v)^{d-2} + du$  is replaced with  $s \geq (2c(m)/\varepsilon)m^2(u/v)^{m-2} + mu$ , where  $c(m)$  is the constant determined in [6].) As a result, we obtain a number  $\alpha > 2$  of degree  $m + 1$  and with trace  $s$ . We claim that  $\beta = (\alpha + \sqrt{\alpha^2 - 4})/2$  is the required Salem number.

Indeed, if  $P(x)$  is the minimal polynomial for  $\alpha$  over  $\mathbb{Q}$ , then  $\beta$  is a root of the polynomial  $Q(x) = P(x + 1/x)x^{m+1}$  of degree  $d = 2m + 2$ . The latter polynomial is irreducible over  $\mathbb{Q}$ , because otherwise it is divisible by some cyclotomic polynomial, which contradicts the irreducibility of  $P(x)$ . Thus,  $Q(x)$  determines a Salem number.

Let  $\beta_j = e^{\phi_j\sqrt{-1}} = (\alpha_j + \sqrt{\alpha_j^2 - 4})/2$ , where  $j = 1, \dots, m$ . The identity

$$|2 \cos \xi_j - \alpha_j| = 4|\sin((\xi_j - \phi_j)/2) \sin((\xi_j + \phi_j)/2)|$$

shows that the arguments of the numbers  $\beta_1, \beta_2, \dots, \beta_m$  are close to  $\xi_1, \xi_2, \dots, \xi_m$  within any prescribed accuracy. Since the polynomials  $Q(x)$  and  $P(x)$  have the same trace, this completes the proof.

Recently, McKee and Smyth [7] proved that Salem numbers may have any integral trace if the degree of numbers is allowed to grow (is not fixed).

## REFERENCES

- [1] A. Dubickas, *On intervals containing full sets of conjugates of algebraic integers*, Acta Arith. **91** (1999), 379–386. MR1736019 (2000i:11161)
- [2] ———, *The Remak height for units*, Acta Math. Hungar. **97** (2002), 1–13. MR1932792 (2003k:11159)
- [3] V. Ennola, *Conjugate algebraic integers in an interval*, Proc. Amer. Math. Soc. **53** (1975), 259–261. MR0382219 (52:3104)
- [4] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **17** (1923), 228–249.
- [5] M. Fekete and G. Szegő, *On algebraic equations with integral coefficients whose roots belong to a given point set*, Math. Z. **63** (1955), 158–172. MR0072941 (17:355a)
- [6] K. Györy, *On the irreducibility of neighbouring polynomials*, Acta Arith. **67** (1994), 283–294. MR1292740 (95h:11114)
- [7] J. McKee and C. J. Smyth, *There are Salem numbers of every trace*, Bull. London Math. Soc. **37** (2005), 25–36.
- [8] Th. Motzkin, *From among  $n$  conjugate algebraic integers,  $n - 1$  can be approximately given*, Bull. Amer. Math. Soc. **53** (1947), 156–162. MR0019653 (8:443f)
- [9] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Monogr. Mat., vol. 57, PWN, Warsaw, 1974. MR0347767 (50:268)
- [10] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, Studies in Mathematical Analysis and Related Topics, Stanford Univ. Press, Stanford, CA, 1962, pp. 305–315. MR0144892 (26:2433)
- [11] ———, *Intervals containing infinitely many sets of conjugate algebraic units*, Ann. of Math. (2) **80** (1964), 411–428. MR0175881 (31:157)

MATHEMATICS AND INFORMATICS DEPARTMENT, VILNIUS UNIVERSITY, NAUGARDUKO 24, VILNIUS 03225, LITHUANIA

*E-mail address:* arturas.dubickas@maf.vu.lt

Received 22/NOV/2003

Translated by A. PLOTKIN