Liet. matem. rink., T. 42, spec. nr., 44–46

Polynomials with many roots on a circle

Artūras DUBICKAS (VU)
e-mail: arturas.dubickas@maf.vu.lt

Result

Let $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ be the fields of rational, real and complex numbers, respectively. We say that a field K is real (or, more generally, complex), if $K \subset \mathbb{R}$ (or, respectively, $K \subset \mathbb{C}$). In particular, every totally real number field is real. Our purpose is to give a self contained proof of the following theorem.

Theorem. *Let K be a real field. Suppose that the polynomial $f(z) \in K[z]$ is irreducible over K and has m distinct roots on the circle $|z| = r > 0$ at least one of which is real. Then $f(z) = g(z^m)$ for some $g(z) \in K[z]$.*

We begin with the following lemma.

Lemma. *Suppose that β, β', β'' are algebraic numbers conjugate over a complex field K satisfying $\beta^2 = \beta'\beta''$. Then β/β' is a root of unity.*

Proof of the lemma. Every complex number z can be written as $|z| \exp\{i \arg z\}$, where $-\pi < \arg z \leqslant \pi$. By Dirichlet's Theorem, there is a positive integer n such that $\gamma = \beta^n$ and its conjugates over K all have positive real parts. Of course, $\gamma^2 = \gamma'\gamma''$ with $\gamma, \gamma', \gamma''$ conjugate over K. Assume that $\gamma, \gamma', \gamma''$ are all distinct, for otherwise the result follows immediately. On applying the automorphism σ taking γ to its conjugate $\sigma(\gamma)$ over K with maximal modulus and (if there are several of these) maximal argument, we obtain that $\sigma(\gamma)^2 = \sigma(\gamma')\sigma(\gamma'')$. This is however impossible, because either the modulus or the argument of the number on the left–hand side is strictly greater than that on the right–hand side.

Proof of the theorem. Assume, without loss of generality, that $m \geqslant 2$. If the polynomial f has at least one complex root on $|z| = r$, say ζ, then its complex conjugate $\overline{\zeta}$ is also a root of f, because its coefficients are real. Hence $r^2 = \zeta\overline{\zeta}$. The product of all m roots of f on $|z| = r$ is therefore equal to $\pm r^m$. Since r or $-r$ is the root of f, it follows that $\alpha_1^m = \pm\alpha_1\alpha_2 \ldots \alpha_m$, where $\alpha_1, \ldots, \alpha_m$ are all m roots of f on $|z| = r$ with α_1 being the real root. Furthermore, by the lemma, every quotient α_j/α_1, where $1 \leqslant j \leqslant m$, is a root of unity. Hence every automorphism of the splitting field of f which maps α_1 to α_j permutes the elements of the set $\{\alpha_1, \ldots, \alpha_m\}$, giving $\alpha_1^m = \alpha_2^m = \ldots = \alpha_m^m$.

Since the quotients α_j/α_1, where $1 \leqslant j \leqslant m$, are all distinct, they must be m distinct roots of unity $\exp\{2\pi ij/m\}$, $j = 0, 1, \ldots, m-1$. Now, writing $\varepsilon = \exp\{2\pi i/m\}$ and $f(z) = \sum_{k=0}^{d} f_k z^k$, where $f_d \neq 0$, $f_0 \neq 0$, we deduce that

$$\begin{aligned} h(z) &= \frac{1}{m}\left(f(z) + f(\varepsilon z) + \ldots + f(\varepsilon^{m-1} z)\right) \\ &= \frac{1}{m}\sum_{k=0}^{d}(1^k + \varepsilon^k + \ldots + \varepsilon^{(m-1)k}) f_k z^k \end{aligned}$$

is $g(z^m)$ for some non-zero $g(z) \in K[z]$, because the sum $1^k + \varepsilon^k + \ldots + \varepsilon^{(m-1)k}$ is equal to m for k divisible by m and vanishes otherwise. Furthermore, $\deg h(z) \leqslant d$. On the other hand, this inequality cannot be strict, since $h(\alpha_1) = 0$ and f is irreducible which implies that h is divisible by f. It follows that $h(z) = f(z)$, because $h(0) = f(0) = f_0$. The proof of the theorem is completed, since $h(z) = g(z^m)$.

Remarks

1. The theorem for $K = \mathbb{Q}$ and for f having no roots outside the circle $|z| \leqslant r$ was proved by D.W. Boyd [1]. In R. Ferguson's paper [4] the condition of maximality of the circle was dropped out giving the theorem as stated for $K = \mathbb{Q}$. However the latter paper contains a clumsy proof of the lemma combined with some incorrect reasoning like "since both polynomials are monic" (see pg. 224 in [4]) which is not the case. The above proof follows the argument given in [4]. The replacement of $\mathbb{Q}$ by the arbitrary real field K makes no difference.

2. The lemma was first proved by C.J. Smyth [6]. The above proof is a simplified version of that given in [6] (see also Lemma 2 in [3]). A more general (algebraic) version of the lemma in which K is an arbitrary field of characteristic zero and more conjugates are involved was considered by the author in Theorem 4 of [2]. (Algebraic means that for an arbitrary field of characteristic zero neither Dirichlet's Theorem nor the arguments like "map γ to the conjugate of largest argument" can be applied.)

3. The condition on one of the roots to be real cannot be omitted. This is shown by the existence of numbers having all d roots on the circle $|z| = r$, but $f(z) \neq f_d z^d + f_0$. One can take, for instance, $K = \mathbb{Q}$, $d = p - 1$, where p is an odd prime, and $f(z) = z^{p-1} + \ldots + z + 1$. All monic irreducible polynomials with integer coefficients having roots on $|z| = r$ were characterized by R.M. Robinson [5]. The author and C.J. Smyth [3] described all polynomials with integer coefficients having all roots on two circles centered at the origin.

4. The theorem can be proved for every formally real field K. Recall that K is formally real, if -1 cannot be expressed as $\sum k_j^2$, where $k_j \in K$. Every such field is of characteristic zero. It contains a unique extension R which is formally real and which has no formally real extensions other than R itself. Also, $R(i)$, where i stands for a root of

$z^2 + 1 = 0$, is algebraically closed field (see, for instance, B.L. van der Waerden's book [7]). Then R and $R(i)$ play the roles of $\mathbb{R}$ and $\mathbb{C}$.

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

References

[1] D.W. Boyd, Irreducible polynomials with many roots of maximal modulus, *Acta Arith.*, **68**, 85–88 (1994).
[2] A. Dubickas, On the degree of a linear form in conjugates of an algebraic number, *Illinois J. Math.* (to appear).
[3] A. Dubickas, C.J. Smyth, On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles, *Proc. Edinburgh Math. Soc.*, **44**, 1–17 (2001).
[4] R. Ferguson, Irreducible polynomials with many roots of equal modulus, *Acta Arith.*, **78**, 221–225 (1997).
[5] R.M. Robinson, Conjugate algebraic integers on a circle, *Math. Zeitschr.*, **110**, 41–45 (1969).
[6] C.J. Smyth, Conjugate algebraic numbers on conics, *Acta Arith.*, **40**, 333–346 (1982).
[7] B.L. van der Waerden, *Algebra*, Springer–Verlag, Berlin, New York (1971).

Daugianariai, turintys daug šaknų ant apskritimo

A. Dubickas

Tegul K yra realusis laukas. Įrodome, kad kiekvienas neredukuojamas virš $K[z]$ daugianaris, turintis m šaknų ant apskritimo, kurio centras yra koordinačių pradžios taške, bent viena iš kurių yra reali, gali būti išreikštas kaip $g(z^m)$ su tam tikru $g(z) \in K[z]$.