TWO VARIATIONS OF A THEOREM OF KRONECKER

ARTŪRAS DUBICKAS AND CHRIS SMYTH

ABSTRACT. We present two variations of Kronecker's classical result that every nonzero algebraic integer that lies with its conjugates in the closed unit disc is a root of unity. The first is an analogue for algebraic nonintegers, while the second is a several variable version of the result, valid over any field.

1 Introduction

In 1857 Leopold Kronecker published the following fundamental result.

Theorem K (Kronecker [K])**.** *Every nonzero algebraic integer that lies with its conjugates in the closed unit disc* $|z| \leqslant 1$ *is a root of unity.*

We refer to a set consisting of an algebraic number and its conjugates as a *conjugate set* of algebraic numbers. An obvious consequence of his result is that there are no conjugate sets of nonzero algebraic integers in the open unit disc $|z| < 1$. In this paper we present two variations of this result. Denote by $P_\alpha(z) \in \mathbb{Z}[z]$ the minimal polynomial of an algebraic number α, its roots being the conjugates of α. Let us call the (positive) leading coefficient of $P_\alpha(z)$ the *van*[1] *of* α. Thus algebraic integers have van 1; other algebraic numbers have van at least 2. The first result concerns algebraic numbers of fixed degree and van having conjugates of smallest possible maximum modulus.

Theorem 1. *Let* α *be an algebraic number of degree* d *and van* $v \geqslant 2$*. Write* $v = v_1^r$ *where* $r \in \mathbb{N}$ *and* v_1 *is not a proper power. Suppose that* α *lies with all its conjugates in the closed disc* $|z| \leqslant v^{-1/d}$*. Then* α *and all its conjugates lie on* $|z| = v^{-1/d}$*, and either*

(a) $P_\alpha(z) = vz^d - 1$ *with* $\gcd(r, d) = 1$*;*

(b) $P_\alpha(z) = vz^d + 1$ *with* $\gcd(r, d)$ *a power of* 2 *(including* 1*), and, when* $4|d$*, that* $4v$ *is not a* 4*th power;*
or

(c) d *is even, and* $P_\alpha(z) = z^{d/2} S(v^{1/s} z^{d/2s} + z^{-d/2s})$*, where* S *is the minimal polynomial of a nonzero totally real algebraic integer of degree* $s = \gcd(r, d/2)$ *lying with its conjugates in the interval* $(-2v^{1/2s}, 2v^{1/2s})$*.*

Thus this result gives the smallest closed disc containing any conjugate sets of algebraic numbers of van v and degree d, and finds all such sets in that disc. Note that for fixed v, d there are only finitely many polynomials S and so only finitely many α. Also note that when d is

2000 *Mathematics Subject Classification.* Primary 11R06; Secondary 12E05, 15A15.

[1]The portion of an army that is nearest the front.

even and $\gcd(r, d/2) = 1$ (for instance when v is not a proper power), then cases (b), (c) consist simply of the $P_\alpha(z) = vz^d - kz^{d/2} + 1$, where k is an integer with $|k| < 2\sqrt{v}$.

Case (b) of the theorem, when $\gcd(r, d) \neq 1$, is actually a special case of (c). It is included here for clarity.

As examples, we see that for $v = 3, d = 2$ we get the 8 minimal polynomials $3z^2 - 1$ and $3z^2 + kz + 1$ for $k \in \{0, \pm 1, \pm 2, \pm 3\}$ with their roots on $|z| = 3^{-1/2}$. For $v = 4, d = 4$, only case (c) of the theorem applies, and $S(z)$ is one of $z^2 - k$ (where $k = 2, 3, 5, 6, 7$), $z^2 + kz - 1$ (where $k = \pm 1, \pm 2$), $z^2 \pm 2z - 2$ or $z^2 \pm 3z + 1$, giving the 13 minimal polynomials $4z^4 \pm 2z^2 + 1$, $4z^4 \pm z^2 + 1$, $4z^4 - 3z^2 + 1$, and $4z^4 \pm az^3 + bz^2 \pm cz + 1$ with $(a, b, c) = (4, 3, 2), (2, 3, 1), (4, 2, 2)$ and $(6, 5, 3)$. All have their roots on $|z| = 4^{-1/4} = 2^{-1/2}$.

The main result of this paper is a several variable version of Kronecker's Theorem valid over any field, where, in this general situation, one cannot define discs or circles, there being no metric to make use of.

Theorem 2. *Let F be any field, and $P(z_1, \dots, z_d) \in F[z_1, \dots, z_d]$ a polynomial satisfying $P(0, \dots, 0) \neq 0$. Suppose that $\mathbf{n}_j = (n_{j,1}, \dots, n_{j,d})$, $j = 1, 2, \dots,$ is a sequence of integer d-tuples satisfying $\lim_{j\to\infty} \min_{1\leqslant i\leqslant d} n_{j,i} = \infty$. Suppose too that there is a number ω in an algebraic closure of F such that $P(\omega^{n_{j,1}}, \dots, \omega^{n_{j,d}}) = 0$ for all j. Then ω is a root of unity.*

We remark that the condition $\lim_{j\to\infty} \min_{1\leqslant i\leqslant d} n_{j,i} = \infty$ is necessary, as otherwise we could take $F = \mathbb{Q}$, $P = 2 - z_1 + 2z_2 - z_3$, $\omega = \sqrt{2}$, $\mathbf{n}_j = (2, j, j + 2)$. The condition $P(0, \dots, 0) \neq 0$ is also necessary, as otherwise we could take $P = 2z_1 - z_2$, $\omega = 2$, $\mathbf{n}_j = (j, j + 1)$. Of course we in fact require only that $P(\omega^{n_{j,1}}, \dots, \omega^{n_{j,d}}) = 0$ for infinitely many j, as we can replace our sequence of integer d-tuples $\mathbf{n}_j$ by the corresponding subsequence for these j.

The case $d = 1$ of this theorem tells us that if $P(\omega^n) = 0$ for infinitely many n then ω is a root of unity. The proof of this is simple: as P has only finitely many roots, $\omega^n = \omega^{n'}$ for some $n \neq n'$, giving the result. It is also essentially the same as one proof of Kronecker's theorem: if α and its conjugates all have modulus at most 1 then so do all powers of α. However, there are only finitely many polynomials of a fixed degree having all their roots in $|z| \leqslant 1$, so that one such polynomial must have infinitely many powers of α as a root. Then the previous argument finishes the proof.

Other generalisations of Kronecker's theorem to polynomials in several variables have been given earlier, by Montgomery and Schinzel [MS], Boyd [B] and Smyth [Sm]. See also Schinzel [Sc, Section 3.4]. However Theorem 2 seems to be the first several variable generalisation that is valid over an arbitrary field.

2 Proof of Theorem 1

Our proof is an application of the following result of Robinson, concerning which circles $|z| = R$ contain conjugate sets of algebraic numbers.

Theorem R (Robinson [R, pp. 42–43])**.** *Let $R \geqslant 0$. The circle $|z| = R$ contains a conjugate set of algebraic numbers if and only if some integer power of R is rational.*

For such an R, let ℓ be the least integer such that $R^{2\ell}$ is rational. Then the minimal polynomial of an algebraic number lying with its conjugates on $|z| = R$ is the appropriate integer multiple of either

(i) $z^\ell \pm R^\ell$ *if* $R^\ell \in \mathbb{Q}$*;*
(ii) $z^{2\ell} - R^{2\ell}$ *if* $R^\ell \notin \mathbb{Q}$*;*
or of the form
(iii) $z^{\ell s} S(z^\ell + R^{2\ell}/z^\ell)$ *for some irreducible polynomial* $S \in \mathbb{Z}[x]$ *of degree* s *having all its zeros in the interval* $(-2R^\ell, 2R^\ell)$.

Conversely, each such polynomial is, up to an integer multiple, the minimal polynomial of a conjugate set of algebraic numbers lying on $|z| = R$.

Proof of Theorem 1. Since we are looking for α with minimal polynomial $vz^d + \cdots + v_0$ having all roots on $|z| = |v_0/v|^{1/d}$ with $|v_0/v|^{1/d}$ minimal for fixed v, d, we must take $v_0 = \pm 1$. But then $1/\alpha$ is an algebraic integer lying with its conjugates on $|z| = v^{1/d}$. It is such the minimal polynomials of such algebraic integers we use Robinson's result to specify, for $R = v^{1/d}$, and then take their reciprocal polynomials.

We have $R^{2\ell} = v_1^{2r\ell/d}$, so that $\ell = d/\gcd(2r, d)$. In case (i) we need $d = \ell$, so that $\gcd(2r, d) = 1$. In case (ii) we need $d = 2\ell$ so that $\gcd(2r, d) = 2$, and r odd so that $R^\ell \notin \mathbb{Q}$. Combining these results relating to $vz^d - 1$ (to be precise, to its reciprocal $z^d - v$) we get that $\gcd(r, d) = 1$ in case (a) of Theorem 1.

For $vz^d + 1$, (i) gives that $\gcd(2r, d) = 1$. In fact, there are other pairs (v, d) for which $vz^d + 1$ is irreducible. (These are in fact particular instances of (iii), as we show below.) Clearly, if (r, d) has an odd factor > 1 then $vz^d + 1$ is reducible. Otherwise, by Capelli's 1898 Theorem (see [Sc, Theorem 19, p. 92]), it is irreducible, unless $4|d$ and $4v$ is a 4th power. (The exceptional case comes from the factorization $\frac{1}{4}u^4 + 1 = (\frac{1}{2}u^2 + u + 1)(\frac{1}{2}u^2 - u + 1)$.) This proves (b).

Now consider case (iii). First note that S must be monic, in order that $z^{\ell s} S(z^\ell + R^{2\ell}/z^\ell)$, as the minimal polynomial of $1/\alpha$, is monic. We have $d = 2\ell s$ and $R^{2\ell} = v_1^{2r\ell/d} = v_1^{\ell(r/h)/(d/2h)}$, where $h = \gcd(r, d/2)$. Hence $\ell = d/2h$, giving $h = s$, and case (c) follows.

Finally, we show how the cases of $vz^d + 1$ irreducible, not covered by (ii), in fact come from (iii). Consider the nth Chebyshev polynomial of the first kind, $T_n(X)$, defined by $T_n(Z + Z^{-1}) = Z^n + Z^{-n}$, which is monic of degree n, with integer coefficients. On replacing Z by $\sqrt{u}Z$ we have that

$$\begin{aligned} u^n Z^n + Z^{-n} &= u^{n/2} T_n\left(\frac{uZ + Z^{-1}}{\sqrt{u}}\right) \\ &= S(uZ + Z^{-1}), \end{aligned}$$

where $S(X) = u^{n/2} T_n(X/\sqrt{u})$ is of degree n. Since T_n is even for n even, and odd for n odd, S is, for $u \in \mathbb{N}$, also monic with integer coefficients. Hence $u^n Z^{2n} + 1 = Z^n S(uZ + Z^{-1})$. Now put $n = \gcd(r, d/2)$, $u = v^{1/n}$ and $Z = z^{d/2n}$. Then $vz^d + 1 = z^{d/2} S(v^{1/n} z^{d/2n} + z^{-d/2n})$, where S has all its roots in $(-2v^{1/2n}, 2v^{1/2n})$. (Recall that n is a power of 2 here, which is just as well, since these are the only values of n for which T_n, and so S, is irreducible.)

□

3 Proof of Theorem 2

Since $\omega \neq 0$, the result for F a finite field is immediate. The proof for other fields is in two parts. We first prove it for $F = \mathbb{Q}$, and then reduce the general case to this case, or to the case of F a finite field.

For $F = \mathbb{Q}$ the proof is also quite simple. Let L be a finite extension of $\mathbb{Q}$ containing ω. Now if $|\omega|_{\mathfrak{p}} = 1$ for all valuations $|.|_{\mathfrak{p}}$ of L then, by Theorem K, ω is a root of unity. Thus, by the product rule, if ω were not a root of unity, then it could be embedded in some completion $L_{\mathfrak{p}}$ of L for which $|\omega|_{\mathfrak{p}} < 1$. But then $|P(\omega^{n_{j,1}}, \dots, \omega^{n_{j,d}})|_{\mathfrak{p}} \to |P(0, \dots, 0)|_{\mathfrak{p}} \neq 0$ as $j \to \infty$, a contradiction.

We now consider the general case. First of all, by replacing F by $F(\omega)$ we may assume that $\omega \in F$. For each j the polynomial $P(z^{n_{j,1}}, \dots, z^{n_{j,d}})$ can be written as a polynomial $Q_j(z) = \sum_{k=0}^{K_j} a_{j,k} z^{m_{j,k}}$, where the K_j do not exceed the number of nonzero coefficients of P, and the $m_{j,k}$ are distinct. Also $m_{j,0} = 0$, while the other $m_{j,k}$, being linear forms with positive coefficients in some of the $n_{j,1}, \dots, n_{j,d}$, satisfy $\min_{1 \leqslant k \leqslant K_j} m_{j,k} \to \infty$ as $j \to \infty$. By replacing the sequence $\{Q_j\}$ by a subsequence, we can assume that all the K_j are equal, to K say, and that the $a_{j,k}$, being sums of certain nonzero coefficients of P, do not depend on j. So we will write $Q_j(z) = \sum_{k=0}^{K} a_k z^{m_{j,k}}$. Note that $a_0 \neq 0$. Further, some permutation of the indices $1, \dots, K$ will put the exponents $m_{j,1}, \dots, m_{j,K}$ in ascending order. By again taking a subsequence we can assume that the same permutation works for all j, and then, by relabelling the $m_{j,k}$, that they are strictly increasing:

$$0 = m_{j,0} < m_{j,1} < \cdots < m_{j,K}.$$

We know too, from the assumption in the statement of the theorem, that $m_{j,1} \to \infty$ as $j \to \infty$, and that $Q_j(\omega) = 0$ for $j \in \mathbb{N}$.

Next, we claim that we may assume that for $k = 0, 1, \dots, K-1$ the sequence of differences $m_{j,k+1} - m_{j,k}$ tends monotonically to infinity as $j \to \infty$. We already know that this sequence is unbounded for $k = 0$. The following algorithm achieves this for other k.

(1) Initialize: $k := 0$.
(2) In the case of $\{m_{j,k+1} - m_{j,k}\}_{j \in \mathbb{N}}$ bounded: replace $\{Q_j\}$ by a subsequence with $u = m_{j,k+1} - m_{j,k}$ constant, and put $Q_j := Q_j + a_{k+1}\omega^u z^{m_{j,k}} - a_{k+1} z^{m_{j,k+1}}$ and $K := K-1$.
In the case of $\{m_{j,k+1} - m_{j,k}\}_{j \in \mathbb{N}}$ unbounded: replace $\{Q_j\}$ by a subsequence with $m_{j,k+1} - m_{j,k}$ monotonically increasing.
(3) $k := k+1$. If $k \geqslant K$ then STOP. Else go to (2).

We also need to assume that the differences $(m_{j,K} - m_{j,K-1}) - (m_{j-1,K} - m_{j-1,K-1})$ tend to infinity with j. This can also be achieved by taking a suitable subsequence of the Q_j's. Note that all of these monotonicity properties are preserved under replacement of the sequence $\{Q_j\}_{j \in \mathbb{N}}$ by any infinite subsequence of itself.

If $K = 1$, then $Q_1(\omega) = Q_2(\omega) = 0$ gives $\omega^{m_{2,1} - m_{1,1}} = 1$, which proves the theorem. Thus we can suppose that $K \geqslant 2$. We now consider the $\infty \times (K+1)$ matrix whose rows are the vectors $\mathbf{v}_j = (z^{m_{j,K}}, z^{m_{j,K-1}}, \dots, z^{m_{j,2}}, z^{m_{j,1}}, 1)$ for $j \in \mathbb{N}$. By the definition of Q_j, we see that $Q_j(z) = \mathbf{v}_j(a_K, a_{K-1}, \ldots, a_0)^T$ at $z = \omega$ is 0, so the determinant of any $K+1$ vectors $\mathbf{v}_j$ vanishes at $z = \omega$. Every such determinant is a polynomial in z with coefficients in the prime subfield of F, isomorphic to $\mathbb{Q}$ or to some finite field $\mathbb{F}_p$. We will show that an infinite sequence of $(K+1)$-tuples of $\mathbf{v}_j$'s can be chosen, whose determinants can be used to apply the theorem, which we have already proved for the prime field.

Let us consider the determinant of $K+1$ vectors $\mathbf{v}_j$. For convenience we shall simply call a typical determinant $D_i(z)$, with rows $\mathbf{v}_\ell$, where ℓ runs over a set I_i of $K+1$ integers to be chosen later such that i is the smallest element in I_i. Associate to $\mathbf{v}_\ell$ its vector of exponents $\mathbf{m}_\ell = (m_{\ell,K}, m_{\ell,K-1}, \ldots, m_{\ell,1}, 0)$. Then a typical term in $D_i(z)$ will be of the form $\pm z^m$, where $m = m_\sigma$ is a sum of the entries of a vector $\mathbf{m}_\sigma = (m_{u,\sigma(K)}, m_{v,\sigma(K-1)}, \ldots, m_{q,\sigma(1)}, m_{i,\sigma(0)})$ for some permutation σ of $\{0, 1, \ldots, K\}$, where $I_i = \{i < q < \cdots < v < u\}$. We now order all such vectors lexicographically, so that the largest vectors are those with largest first component, and so on. Then we impose conditions on the $\mathbf{m}_\ell$'s that we are going to choose from all the $\mathbf{m}_j$'s (or, equivalently, the conditions on the set I_i), so that the lexicographic ordering on the $\mathbf{m}_\sigma$ corresponds to the usual ordering on the exponents m_σ. The conditions we impose are as follows: for each $\ell \in I_i$ except for $\ell = i$ the differences $m_{\ell,k} - m_{\ell,k-1}$, where $k = K, K-1, \ldots, 2, 1$, are all greater than $\sum_{t \in I_i, i \leqslant t < \ell} m_{t,K}$. It is routine to verify that this ensures that the orderings correspond. These conditions can be arranged by choosing the $\mathbf{m}_\ell$'s to be a suitable set of $K+1$ vectors $\mathbf{m}_j$ from the sequence of all $\mathbf{m}_j$'s, made possible by the monotonically increasing property of the $m_{j,k} - m_{j,k-1}$ for increasing j.

We now see that $\mathbf{m}_\ell$ can be chosen so that the m_σ are all distinct. Hence $D_i(z)$ is a sum of $r := (K+1)!$ terms $\pm z^m$, equalling, in descending order of exponents, $\pm z^{m_1} \pm \cdots \pm z^{m_{r-1}} \pm z^{m_r}$, where

$$\begin{aligned} m_1 &= m_{u,K} + m_{v,K-1} + \cdots + m_{q,1} + m_{i,0}, \\ m_{r-1} &= m_{q,K} + m_{i,K-1} + \cdots + m_{v,1} + m_{u,0}, \\ m_r &= m_{i,K} + m_{q,K-1} + \cdots + m_{v,1} + m_{u,0}. \end{aligned}$$

Hence $m_{r-1} - m_r = (m_{q,K} - m_{q,K-1}) - (m_{i,K} - m_{i,K-1})$. Note that we have constructed not one but infinitely many collections $m_1 > \cdots > m_{r-1} > m_r$ and infinitely many polynomials $D_i(z) = \pm z^{m_1} \pm \cdots \pm z^{m_{r-1}} \pm z^{m_r}$ vanishing at $z = \omega$. The fact that the differences

$$(m_{j,K} - m_{j,K-1}) - (m_{j-1,K} - m_{j-1,K-1})$$

tend to infinity with j ensures that $m_{r-1} - m_r$ tends to infinity with i. Dividing $D_i(z)$ by z^{m_r}, it is easy see that we are back to the same problem for the field $F = \mathbb{Q}$ or $F = \mathbb{F}_p$ with $P(z_1, z_2, \ldots, z_{r-1}) = \pm z_1 \pm z_2 \pm \cdots \pm z_{r-1} \pm 1$ and with $n_i = m_i - m_r$ for $i = 1, 2, \ldots, r-1$ (because $n_{r-1} = m_{r-1} - m_r$ is the smallest component of the vector $(n_1, n_2, \ldots, n_{r-1})$, and $n_{r-1} \to \infty$ as $i \to \infty$), which we have already solved. This completes the proof.

REFERENCES

[B] Boyd, David W.: Kronecker's theorem and Lehmer's problem for polynomials in several variables, J. Number Theory **13** (1981), 116–121.

[K] Kronecker, Leopold.: Zwei sätse über Gleichungen mit ganzzahligen Coefficienten, J. Reine Angew. Math. **53** (1857), 173–175. See also Werke. Vol. 1, 103–108, Chelsea Publishing Co., New York, 1968.

[MS] Montgomery, H. L.; Schinzel, A.: Some arithmetic properties of polynomials in several variables, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 195–203. Academic Press, London, 1977.

[R] Robinson, Raphael M.: Conjugate algebraic integers on a circle, Math. Z. **110** (1969), 41–51.

[Sc] Schinzel, A.: Polynomials with special regard to reducibility. Encyclopedia of Mathematics and its Applications, **77**. Cambridge University Press, Cambridge, 2000.

[Sm] Smyth, C. J.: A Kronecker-type theorem for complex polynomials in several variables, Canad. Math. Bull. **24**(1981), 447–452. Addenda and errata: **25** (1982), 504.

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

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

SCHOOL OF MATHEMATICS, UNIVERSITY OF EDINBURGH, JAMES CLERK MAXWELL BUILDING, KING'S BUILDINGS, MAYFIELD ROAD, EDINBURGH EH9 3JZ, SCOTLAND, U.K.

E-mail address: c.smyth@ed.ac.uk