# FROM AMONG $n$ CONJUGATE ALGEBRAIC INTEGERS, $n-1$ CAN BE APPROXIMATELY GIVEN

TH. MOTZKIN

1. **Summary.** Given $n$ arbitrary complex numbers $z_1, \cdots, z_n$, it is easy to construct (see 6.2) an irreducible algebraic equation

$$\zeta^n + \alpha_1\zeta^{n-1} + \cdots + \alpha_n = 0$$

with complex rational coefficients $\alpha_\nu$, such that its $n$ roots $\zeta_1, \cdots, \zeta_n$ lie within assigned neighbourhoods of $z_1, \cdots, z_n$. If the numbers $z_1, \cdots, z_n$ are symmetric to the real axis, then there exists an equation with real rational coefficients whose roots are near $z_1, \cdots, z_n$. If, however, the coefficients $\alpha_\nu$ are required to be integers, then in sufficiently small neighbourhoods there will be no system $\zeta_1, \cdots, \zeta_n$, except possibly the system $z_1, \cdots, z_n$ itself, as follows immediately from the continuity of the coefficients as functions of the roots.

In this note we prove (Theorem 3.2) that for every $n-1$ given numbers $z_1, \cdots, z_{n-1}$, and every $\epsilon>0$, there exists an irreducible equation with complex integral coefficients $\alpha_1, \cdots, \alpha_n$ and with roots $\zeta_\nu$ such that $|\zeta_\nu - z_\nu| < \epsilon$ for $\nu = 1, \cdots, n-1$. The same is true (§5) for real integral coefficients provided that the numbers $z_1, \cdots, z_{n-1}$ are symmetric to the real axis. Some remarks on the possible location of the free root $\zeta_n$ are added (§4).

The proof of the main theorems employs the well known facts of the solubility of a system of linear Diophantine inequalities under certain conditions, and of the uniform continuity of the roots of an algebraic equation

$$b_0y^n + \cdots + b_n = 0$$

with general complex coefficients $b_\nu$, as functions of the ratios of these coefficients. A topological proof of the latter theorem is prefixed (§2); uniform continuity, and incidentally ordinary continuity, of the roots of an algebraic equation is exhibited as a consequence of the classical proposition of set theory that asserts the uniform continuity of every topological mapping of a compact space.[1]

2. **The theorem on uniform continuity.** 2.1. Every polynomial

$$z^n + a_1z^{n-1} + \cdots + a_n$$

corresponds to a point $a = (a_1, \cdots, a_n)$ of the complex affine $n$-space

Received by the editors June 17, 1946.

[1] For example Sierpiński, *General topology*, p. 99.

$A_n$. The system $(z_1, \cdots, z_n)$ of the roots of the polynomial can be considered as a point of the complex symmetric-affine $n$-space $Z_n$ that is obtained from the ordinary affine $n$-space by identifying points $(z_1, \cdots, z_n)$ that have the same coordinates $z_\nu$ in different order. Neither $A_n$ nor $Z_n$ is compact.

The closure of $A_1 = Z_1$ formed by adding the point $\infty$ is the complex projective one-space $B_1$. By allowing $z_\nu$ to take the value $\infty$, the space $Z_n$ is enlarged and becomes the symmetric-multiprojective space $Y_n$ that contains as points all the systems $(y_1, \cdots, y_n)$ of roots of equations $b_0 y^n + \cdots + b_n = 0$. The coefficients $b_0, \cdots, b_n$ are the coordinates of a point of the complex projective $n$-space $B_n$; to every point of $B_n$ there correspond infinitely many points of $A_{n+1}$ with normalized coordinates, that is, such that $\sum |b_\nu|^2 = 1$. Any two normalized representations of the same point of $B_n$ differ by a factor $\lambda$ with $|\lambda| = 1$.

The spaces $Y_n$ and $B_n$ are compact, and since the mapping of $y = (y_1, \cdots, y_n)$ on $b = (b_0, \cdots, b_n)$ is one-to-one, continuous, and defined for every $y$, this mapping is topological.

2.2. An appropriate metric of $B_n$ is obtained by defining the distance $\rho(b, b')$ between two points of $B_n$ as that between the two infinite subsets of $A_{n+1}$ corresponding to the two given points, that is, as the least $\rho$ for which there exist normalized representations of $b$ and $b'$ with $(\sum |b_\nu - b_\nu'|^2)^{1/2} = \rho$, or alternatively, $\max_\nu |b_\nu - b_\nu'| = \rho$.[2] The normalized representation of one of the points, say $b$, can be arbitrarily chosen when determining the distance; there follows at once $\rho(b, b') + \rho(b, b'') \geqq \rho(b', b'')$.

In particular the distance $\rho(y, y')$ between two points $y$ and $y'$ of $B_1 = Y_1$ is defined as the least $\rho$ with $(|z_1 - z_1'|^2 + |z_2 - z_2'|^2)^{1/2} = \rho$ for a suitable representation $y = z_1/z_2$, $y' = z_1'/z_2'$ with $|z_1|^2 + |z_2|^2 = |z_1'|^2 + |z_2'|^2 = 1$, or equivalently by use of the spherical distance.

In the same way a metric of $Y_n$ can be introduced by defining the distance $\rho(y, y')$ between two points of $Y_n$ as that of the sets of identified points, that is, as the least $\rho$ for which there exists a permutation $1', \cdots, n'$ of $1, \cdots, n$ such that all $\rho(y_\nu, y'_{\nu'}) \leqq \rho$.

With these definitions of distances in $B_n$ and $Y_n$, the theorem on the uniform continuity of every topological mapping of a compact space entails:

*If the distance between the coefficients of two polynomials of the same degree is less than $\epsilon$, the distance between their systems of roots is less than*

[2] Or by any other natural extension of a metric from one to more dimensions, in the sense of Th. Motzkin, *Sur le produit des espaces métriques*, Comptes Rendus du Congrès International des Mathématiciens Oslo 1936, vol. 2, p. 137.

*$\epsilon'$, and $\epsilon' \to 0$ for $\epsilon \to 0$.*[3]

The example of the polynomials $\epsilon z^n - 1$ and 1 shows that uniform convergence independently of the degree $n$ does not hold for the above distance; perhaps it holds for a similar definition in regard to $\sum (b_\nu z)^\nu = 0$.

3. **The theorem on approximation by conjugate integers.** 3.1. *For any given complex number $z$ and every $\epsilon > 0$ there exists a root $\zeta$ of an irreducible algebraic equation $\zeta^2 + \alpha_1 \zeta + \alpha_2 = 0$ with complex integer coefficients $\alpha_1$ and $\alpha_2$ such that $|\zeta - z| < \epsilon$.*

PROOF. The function $\alpha^{1/2}$ maps the parallels to the axes through complex integers into two orthogonal systems of equilateral hyperbolas. For integral $\alpha \to \infty$ their consecutive intersections become arbitrarily near to each other. The non-integral numbers $\zeta = \alpha^{1/2} - \alpha'$ with complex integral $\alpha$ and $\alpha'$ are therefore dense on the whole plane.

Alternatively, this theorem is a particular case of 3.2 and can be proved in the same way, every step of the proof becoming much simpler.

3.2. *For any $n-1$ given complex numbers*

$$z_1, \cdots, z_{n-1}$$

*and every $\epsilon > 0$ there exists a system*

$$\zeta_1, \cdots, \zeta_{n-1}$$

*of roots of an irreducible algebraic equation $\zeta^n + \alpha_1 \zeta^{n-1} + \cdots + \alpha_n = 0$ with complex integral coefficients $\alpha_\nu$ such that*

$$|\zeta_\nu - z_\nu| < \epsilon, \qquad \nu = 1, \cdots, n-1.$$

3.3. PROOF. The numbers $z_\nu$ are roots of an equation $z^{n-1} + a_1 z^{n-2} + \cdots + a_{n-1} = 0$ with general complex coefficients $a_\nu = c_{2\nu-1} + ic_{2\nu}$.

We assume the real numbers

$$1, c_1, \cdots, c_{2n-2}$$

to be rationally independent, that is, not to fulfill any homogeneous linear equation with coefficients that are rational and not all 0. If necessary we can achieve this independence by slightly changing the numbers $c_1, \cdots, c_{2n-2}$ one after the other, always avoiding the enu-

[3] With the same proof, the theorem on uniform continuity may be enunciated for polynomials with $n$ real roots, even before introducing complex numbers. Indeed, the theorem on uniform continuity and that on the existence of the roots of an algebraic equation (the "fundamental theorem of algebra") are independent of each other. For a topological proof of the "fundamental theorem," see W. L. Chow, Math. Ann. vol. 116 (1939) p. 463; for an elementary proof see Th. Motzkin and A. Ostrowski, Preuss. Akad. Wiss. Sitzungsber. 1933, p. 255.

merable set of values with a rational relation between them and the preceding numbers. Because of the continuity of the roots of an algebraic equation, the new roots $z_\nu$ are near to the old ones, so that numbers $\zeta_\nu$ near enough to the new roots $z_\nu$ are also near to the given ones.

3.4. We also assume the numbers $z_\nu$, and every subset of them, not to be a system of roots of an algebraic equation with complex integral coefficients. Otherwise replace the $z_\nu$ by $z_\nu\lambda$ with a suitable real rational $\lambda$ near 1. This does not affect the above property of rational independence, since the $a_\nu$ are only multiplied by real rational factors.

Then the existence of a system $\zeta_1, \cdots, \zeta_n$ of roots of an algebraic equation with complex integral coefficients entails its irreducibility for sufficiently small $\epsilon$. For if there existed a sequence of reducible systems with $\epsilon \rightarrow 0$, then infinitely many of them would have a subsystem belonging to the same indices $\nu < n$. Passing to the limit, the corresponding $z_\nu$ would form a system of roots of an algebraic equation with complex integral coefficients.

3.5. Now if there exist complex integers $\alpha_1, \cdots, \alpha_n$ such that

$$\left| (\alpha_{\nu+1} - a_\nu\alpha_1) - (a_{\nu+1} - a_\nu a_1) \right| < \epsilon_1, \qquad \nu = 1, \cdots, n-1,$$

where $a_n = 0$, put $a_1 - \alpha_1 = z_n$. Then the coefficients $\alpha_{\nu+1}$ of $\zeta^n + \alpha_1\zeta^{n-1} + \cdots + \alpha_n$ differ from those

$$a'_{\nu+1} = a_{\nu+1} - a_\nu z_n = a_{\nu+1} - a_\nu a_1 + a_\nu\alpha_1$$

of $(z - z_n)(z^{n-1} + a_1 z^{n-2} + \cdots + a_{n-1})$ by less than $\epsilon_1$, and the coefficient of $z^{n-1}$ is $a_1' = \alpha_1$ in both polynomials. Hence the distance between the points $(1, \alpha_1, \cdots, \alpha_n)$ and $(1, a_1', \cdots, a_n')$ in complex projective $n$-space is less than $\epsilon_2$, and $\epsilon_2 \rightarrow 0$ for $\epsilon_1 \rightarrow 0$. By the theorem on the uniform continuity of the roots of algebraic equations, the roots $\zeta_1, \cdots, \zeta_n$ and $z_1, \cdots, z_n$ may be so arranged that the spherical distance (or distance as defined in 2.2) between corresponding roots is less than $\epsilon_3$, and $\epsilon_3 \rightarrow 0$ for $\epsilon_2 \rightarrow 0$. Hence $|\zeta_\nu - z_\nu| < \epsilon$, $\nu = 1, \cdots, n-1$, and $\epsilon \rightarrow 0$ for $\epsilon_3 \rightarrow 0$.

Since $a_1' = \alpha_1$, we have $\zeta_1 + \cdots + \zeta_n = z_1 + \cdots + z_n$, whence $|\zeta_n - z_n| < (n-1)\epsilon$.

3.6. Now a theorem of Kronecker[4] states that, for rationally independent real $1, c_1, c_2, \cdots$, arbitrary real $d_1, d_2, \cdots$, and $\epsilon_1 > 0$, there are real integers $\alpha_1 > 0, \gamma_1, \gamma_2, \cdots$ such that $|\alpha_1 c_\mu - \gamma_\mu - d_\mu| < \epsilon_1$, $\mu = 1, 2, \cdots$. Taking $d_1, d_2, \cdots$ as the real and imaginary parts of $a_1 a_\nu - a_{\nu+1}$, we see that the Diophantine inequalities at the beginning

[4] For example Hardy-Wright, *Theory of numbers*, p. 370, Theorem 442.

of 3.5 can be solved for complex integers $\alpha_1>0$, $\alpha_2=\gamma_1+i\gamma_2, \cdots$. This completes the proof of 3.2.

For a given $\alpha_1$ there is at most one solution, if $\epsilon_1\leqq 1/2$.

4. **Situation of the remaining root $\zeta_n$.** 4.1. *For every $N>0$ there is an $\epsilon(N)>0$ such that for $\epsilon<\epsilon(N)$ either $|\zeta_n|>N$ or $\zeta_\nu=z_\nu$, $\nu=1, \cdots, n-1$.*

PROOF. There exists either no value $\zeta$ with $|\zeta|\leqq N$ such that $z_1, \cdots, z_{n-1}, \zeta$ are the roots of an algebraic equation of degree $n$ with complex integral coefficients, or one value, or (for the roots $z_1, \cdots, z_{n-1}$ of an algebraic equation of degree $n-1$ with complex integral coefficients) every complex integer $\zeta$ with $|\zeta|\leqq N$ is appropriate; at any rate the number of the possible $\zeta$ is finite. For a given $\zeta$, a system $\zeta_\nu$ close enough to the numbers $z_1, \cdots, z_{n-1}, \zeta$ must coincide with them; let $\epsilon_0$ be a distance ensuring coincidence for every $\zeta$. Now if there existed for every $\epsilon'=1, 1/2, 1/3, \cdots$ values $\zeta_n$ with $|\zeta_n|\leqq N$ and $|\zeta_n-\zeta|\geqq\epsilon'$ for every possible $\zeta$, then a subsequence of these $\zeta_n$ would converge to a new $\zeta$. Hence no such $\zeta_n$ exists for a certain $\epsilon'$; then we may put $\epsilon(N)=\min(\epsilon', \epsilon_0)$.

4.2. There exist, however, values $\zeta_n$ near any given direction. More precisely:

*The numbers $\zeta_1, \cdots, \zeta_n$ may be required to have their sum in a given half strip that contains a complex integer; or, what is less, $\zeta_n$ may be required to be within a given angle with arbitrary vertex and arbitrarily small aperture.*[5]

PROOF. The second part of the theorem follows immediately from the first part. Indeed, since every angle contains a half strip with infinitely many complex integers, the sum $-\alpha_1$ may be required to be within a given angle. Hence the same is true for $z_n=a_1-\alpha_1$ and, by the inequality $|\zeta_n-z_n|<(n-1)\epsilon$ at the end of 3.5, for $\zeta_n$.

To prove the first contention, we remember that by 3.5, it is enough to show that the complex integer $\alpha_1$ can be determined such that the numbers $a_\nu\alpha_1$ are, mod integers, near given numbers. If the given half strip contains an integer ray $\gamma+\delta x$, $x>0$, we put $\alpha_1=\gamma+\delta\alpha'$, $\alpha'=1, 2, \cdots$. The Diophantine inequalities for $\alpha', \alpha_2, \alpha_3, \cdots$ are soluble, as in 3.6, if 1 and the real and imaginary parts of the numbers $a_\nu\delta$ are rationally independent. Now every rational relation between them might be written as an equation $\sum\delta_\nu a_\nu\delta+\delta'=c$ with complex rational $\delta_\nu$ and $\delta'$ and real $c$; putting $\delta_\nu\delta=\delta_\nu'$, this would become a

[5] A strip between, but not including, two parallel straight lines is divided by a nonparallel line into two half strips. A strip or half strip contains infinitely many complex integers either if it contains an integral ray (half straight line through two complex integers) or if its direction is irrational; otherwise it contains no complex integer.

similar relation for the numbers $a_\nu$. But the real and imaginary part of these numbers, and 1, have been supposed to be rationally independent.

On the other hand, if the given half strip has an irrational direction, that is, if it contains a ray $x+(cx+c')i$ with variable real $x>N$ (or $x<N$) and given real $c'$ and real irrational $c$, then the imaginary part $\gamma'$ of $\alpha_1=\gamma+i\gamma'$ is required to be near $c\gamma+c'$. Hence the numbers $c\gamma$, $a_\nu(1+ic)\gamma$ have to be, mod integers, near given numbers, for a $\gamma>N$ (or $\gamma<N$). Such numbers exist provided that 1, $c$, and the real and imaginary parts of $a_1(1+ic), \cdots, a_{n-1}(1+ic)$ are rationally independent, which can be attained, as in 3.3, by small changes of the numbers $a_\nu$.

5. **The approximation theorem for real coefficients.** 5.1. *For any given numbers $z_1, \cdots, z_{n-1}$ that are symmetric to the real axis and every $\epsilon>0$ there exists a system $\zeta_1, \cdots, \zeta_n$ of roots of an algebraic equation $\zeta^n+\alpha_1\zeta^{n-1}+ \cdots +\alpha_n=0$ with real integral coefficients $\alpha_\nu$ such that $|\zeta_\nu-z_\nu|<\epsilon$ for all $\nu\leqq n-1$.*

*Moreover, $\zeta_\nu$ may be required to be real if the corresponding $z_\nu$ is real, and $\zeta_n$ may be required to be on a given real ray.*

The proof is as in the general case. The real numbers $z_\nu$ can be changed a little so as to be different from each other; then the symmetry of the corresponding roots $\zeta_\nu$ will compel these roots to be real. This change should be effectuated before the displacement ensuring that the numbers $1, a_1, \cdots, a_{n-1}$ are rationally independent and that the $z_\nu$ have no subset which is the system of roots of an algebraic equation with real integral coefficients. The latter condition entails irreducibility, the former the solubility of the Diophantine inequalities for real integral $\alpha_\nu$ and $\alpha_1$ on the given ray, whence the theorem.

5.2. Rational independence as required for this proof can also be attained by a simultaneous translation, according to the lemma:

*For every finite set $z_1, \cdots, z_{n-1}$ that is symmetric to the real axis and every $\epsilon>0$ there exists an $\epsilon'$ with $0<\epsilon'<\epsilon$ such that the coefficients $1, a_1', \cdots, a_{n-1}'$ of the equation with the roots $z_1+\epsilon', \cdots, z_{n-1}+\epsilon'$ are rationally independent.*

Proof. Otherwise, for every $\epsilon'$, there would hold a rational relation with coefficients not all 0. The set of rational relations being enumerable, and the set of $\epsilon'$ between 0 and $\epsilon$ not, there would exist a relation holding for infinitely many $\epsilon'$. Since the $a_\nu'$ are polynomials in $\epsilon'$, this relation belongs to every $\epsilon'$. But such a relation between the coefficients $a(\epsilon), a'(\epsilon), \cdots, a^{(n-1)}(\epsilon)/(n-1)!$ of $1, z, \cdots, z^{n-1}$ in a polynomial $a(z+\epsilon)$ cannot exist, since $a(\epsilon), \cdots, a^{(n-1)}(\epsilon)$ are of degree $n-1, \cdots, 0$.

**6. Miscellaneous remarks.** 6.1. Let $\beta(\eta)=\beta_0\eta^n+\beta_1\eta^{n-1}+\cdots+\beta_n$ have complex integral coefficients $\beta_\nu$, and let $q$ be a complex integer.

*The polynomial $p\beta(\eta)+q$, where $p$ is a complex prime not dividing $q\beta_0$, is irreducible.*[6]

Proof. Otherwise $p\beta(\eta)+q=\beta'(\eta)\beta''(\eta)$. The product of the highest powers in $\beta'(\eta)$ and $\beta''(\eta)$ with coefficients not divisible by $p$ is $q$ (mod $p$), hence these powers are constants. The highest coefficients of $\beta'(\eta)$ and $\beta''(\eta)$ would therefore be divisible by $p$, and $p\beta_0$ by $p^2$.

6.2. *In the proximity of every given n numbers $z_1, \cdots, z_n$ there are systems of roots of an irreducible equation of degree n with complex rational coefficients.*

Proof. A polynomial $\beta(\eta)$ with (for example rational) roots near the given numbers is easily found. The roots of $p\beta(\eta)+1$ are near to those of $\beta(\eta)$ if $p$ is large, because of the continuity of the roots of an algebraic equation as functions of the coefficients, so that a sufficiently large complex prime $p$ not dividing $\beta_0$ will do (6.1).

If the given numbers are symmetric to the real axis, the polynomials $\beta(\eta)$ and $p\beta(\eta)+1$ may be assumed to be real. If we want the roots near the real $z_\nu$ to be real, coinciding real $z_\nu$ are first separated as in 5.1.

6.3. *The roots of irreducible equations of a given degree $n\geqq 2$ with complex integral coefficients are dense on the whole plane.*

Proof. This immediate consequence of Theorem 3.2 on systems $n-1$ of whose numbers are approximately given follows already from 3.1, without reference to 3.2. This is trivial for $n=2$. Even the existence of a polynomial $\alpha(\zeta)$ of degree 2 with one root near a given number $z$, whose coefficients are divisible by a complex prime $p$, follows by means of multiplication by $p$ of a system of two conjugate algebraic integers one of which is near $z/p$ (or also, if 3.1 is proved in the same way as 3.2, from the solubility of the Diophantine inequalities for $\alpha_\nu$ divisible by $p$). But if $n>2$, then $\alpha(\zeta)\alpha'(\zeta)+p$—where $\alpha'(\zeta)$ is a polynomial of degree $n-2$ with large coefficients divisible by $p$—has two of its roots near to those of $\alpha(\zeta)$, and is irreducible by Eisenstein's rule.

Likewise Theorem 5.1 implies that the roots of irreducible equations of a given degree $n\geqq 3$ with real rational coefficients are dense on the whole plane, while for $n=2$ they are dense only on the real axis.

University of Jerusalem

[6] This is Eisenstein's rule, after putting $\zeta=1/\eta$, cf. van der Waerden, *Moderne Algebra*, vol. 1, p. 77.