Notre Dame Journal of Formal Logic
Volume XI, Number 4, October 1970

POLYNOMIALS WITH COMPUTABLE COEFFICIENTS

R. L. GOODSTEIN

In a recent article [1] I showed that the well known second Gauss proof of the fundamental theorem of algebra can be adapted to give a proof of the existence of a zero of a polynomial with algebraic-number coefficients which is finitist and constructivist in the strictest senses of these terms. The object of the present note is to show that this result yields an effective proof of the existence of a zero of a polynomial in which the leading coefficient is unity and the remaining coefficients are recursive real or complex numbers.

It is readily seen that there can be no constructive existence proof of the roots of a polynomial in which the leading coefficient is a (primitive) recursive real number; for let c_n be an arbitrary primitive recursive function which takes only the values 0, 1; let

$$\gamma_0 = c_0$$
$$\gamma_{n+1} = \begin{cases} c_{n+1}, \textit{if } (\forall r)\ (r \leq n \rightarrow c_r = 0) \\ 0, \textit{if } (\exists r)\ (r \leq n \ \&\ c_r = 1) \end{cases}$$

and let γ denote the recursive real number

$$\sum_{0 \leq r} \gamma_r \cdot (2^{-r})$$

(so that $\gamma = 0$ if $c_r = 0$ for all r, and $\gamma = 2^{-\rho}$ if ρ is the first value of r for which $c_r = 1$). Then the polynomial equation

$$\gamma x^2 - 2x - 1 = 0$$

has the root $x = -\frac{1}{2}$ if $\gamma = 0$, and two roots which are approximately $x = -\frac{1}{2}$ and $x = \frac{1}{2} + 2^{\rho+1}$ if $c_\rho = 1$. Thus if there is an effective procedure for determining even the integral parts of the roots of the equation, we could determine whether $c_n = 0$ for all n or not, and this is known to be impossible for arbitrary c_n.

Let a_i denote the recursively convergent recursive sequence of rational numbers (a_i^n), where for given p we may without loss of generality suppose that $|a_i^N - a_i^n| < 2^{-np}$ for $N \geq n$; let $\mathsf{P}(x)$ denote the polynomial

$$x^p + a_1 x^{p-1} + a_2 x^{p-2} + \ldots + a_p$$

Received July 26, 1969

and let $P_n(x)$ denote the polynomial

$$x^p + a_1^n x^{p-1} + a_2^n x^{p-2} + \ldots + a_p^n$$

with rational coefficients. Further, for each integral value of n let $\alpha_1^n, \alpha_2^n, \ldots, \alpha_p^n$ be the roots of $P_n(x)$ so that

$$P_n(x) = (x - \alpha_1^n)(x - \alpha_2^n) \ldots (x - \alpha_p^n)$$

We showed in [1] that there is an effective procedure for deciding whether an algebraic number is zero or not, and so an effective procedure for determining the minimum of two algebraic real numbers.

Define the sequence β_n as follows: let $\beta_1 = \alpha_1^1$; let β_2 be the α_i^2 of smallest index i, $1 \leq i \leq p$, such that $|\alpha_i^2 - \alpha_1^1|$ is minimum, and generally let β_{k+1} be the α_i^{k+1} of smallest index i such that $|\beta_k - \alpha_i^{k+1}|$ is minimum, (so that for each k there is a q such that $\beta_k = a_q^k$). Let μ_n denote the $\min|\alpha_i^{n+1} - \beta_n|$, $1 \leq i \leq p$. Furthermore, let A be an integral upper bound of all $|a_i^n|$, $i = 1, 2, \ldots, p$ and let $R = \max(2, 2A)$ so that, as may readily be seen, all the zero of all the polynomials $P_n(x)$ lie inside the circle $|x| = R$. Then if $|x| \leq R$, and $N > n$,

$$|P_N(x) - P_n(x)| \leq 2^{-np} \textstyle\sum_{i=0}^{p-1} R^i < R^p 2^{-np} \quad .$$

But

$$|P_{n+1}(\beta_n)| = |(\alpha_1^{n+1} - \beta_n)(\alpha_2^{n+1} - \beta_n) \ldots (\alpha_p^{n+1} - \beta_n)| \geq \mu_n^p$$

and

$$|P_{n+1}(\beta_n)| = |P_{n+1}(\beta_n) - P_n(\beta_n)| < R^p 2^{-np}$$

so that $\mu_n^p < R^p 2^{-np}$, whence $\mu_n < R2^{-n}$. But $|\beta_{n+1} - \beta_n| = \min|\alpha_i^{n+1} - \beta_n| = \mu_n$ and so $|\beta_{n+1} - \beta_n| < R2^{-n}$. It follows that for $N > n$,

$$|\beta_N - \beta_n| \; R2^{-(n-1)}$$

which proves that β_n is recursively convergent and determines a recursive real or complex number β, say. Now $P_n(x)$ is uniformly convergent to $P(x)$ for $|x| \leq R$ and $P_n(\beta_n) = 0$ for all n, and therefore β is zero of $P(x)$.

It will be observed that β is a computable number, and this is the most that the proof yields; if the coefficients of the polynomial $P(x)$ are primitive recursive numbers we cannot by these methods show that β is a primitive recursive (real or complex) number, for the zeros of the polynomial $P_n(x)$ are determined for each particular value of n, and not as functions of an integral variable n.

REFERENCE

[1] Goodstein, R. L., "A constructive form of the Second Gauss proof of the Fundamental Theorem of Algebra," *Constructive Aspects of the Fundamental Theorem of Algebra*, B. Dejon and P. Henrici (Eds.), Wiley, New York (1969).

University of Leicester
Leicester, England