PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 1, 1965

ON ARITHMETIC PROPERTIES OF COEFFICIENTS OF RATIONAL FUNCTIONS

DAVID G. CANTOR

The purpose of this note is to prove the following generalization of a result of Polya:

THEOREM. **Let $\{a_n\}$ be a sequence of algebraic integers, and f a nonzero polynomial with complex coefficients. If $\sum_{n=0}^{\infty} f(n)a_n z^n$ is a rational function, then so is $\sum_{n=0}^{\infty} a_n z^n$.**

Polya [3] has proved that if $\sum_{n=0}^{\infty} na_n z^n$ is a rational function, then so is $\sum_{n=0}^{\infty} a_n z^n$. It follows immediately from Polya's result that if k is a rational integer and $\sum_{n=0}^{\infty} (n-k)a_n z^n$ is a rational function, then so is $\sum_{n=0}^{\infty} a_n z^n$. It is then easy to prove inductively, that if f is a polynomial with complex coefficients, all of whose roots are rational integers, and if $\sum_{n=0}^{\infty} f(n)a_n z^n$ is a rational function, then so is $\sum_{n=0}^{\infty} a_n z^n$.

Suppose K is an algebraic number field and $A \subset K$ is an ideal. If α and β are algebraic numbers in K, we say, as usual, that $\alpha \equiv \beta(A)$, if there exists a rational integer r, relatively prime to A, such that $r\alpha$ and $r\beta$ are algebraic integers and $(r\alpha - r\beta) \in A$. We say that A divides the numerator (denominator) of α if $\alpha \equiv 0(A)$ $((1/\alpha) \equiv 0(A))$. We denote the norm of the ideal A by NmA.

LEMMA 1. *Let K be an algebraic number field and $\alpha \in K$ an algebraic number. Then the set of those prime ideals of K which divide the numerator of some element of the sequence $\{k - \alpha : k = 1, 2, 3, \cdots\}$ is infinite.*

Proof. Suppose n is a rational integer such that $n\alpha$ is an algebraic integer, and suppose $P_1, P_2, \cdots, P_r$ are the only prime ideal divisors of the sequence $\{nk - n\alpha : k = 1, 2, 3, \cdots\}$. Now $Nm(nk - n\alpha)$ is a nonconstant polynomial $g(k)$ with rational integral coefficients. Hence for each rational integer k, there exist rational integers $s_1, s_2, \cdots, s_r$ such that $g(k) = \mp \prod_{i=1}^{r} (NmP_i)^{s_i}$. Thus there are only finitely many rational primes which divide some element of the sequence $\{g(k) : k = 1, 2, 3, \cdots\}$. But this is false [2, p. 82].

REMARK. A less elementary proof of Lemma 1 is obtained by observing that if P is a prime ideal with residue class degree 1, and not dividing the denominator of α, then there exists a rational integer

Received August 13, 1963.

n such that $n \equiv \alpha(P)$; since the set of such prime ideals has Dirichlet density 1, among all prime ideals, there are infinitely many of them.

LEMMA 2. *Suppose $\{a_n\}$ is a sequence of algebraic integers and α is an algebraic number. If $\sum_{n=0}^{\infty}(n-\alpha)a_n z^n$ is a rational function then so is $\sum_{n=0}^{\infty} a_n z^n$.*

Proof. Since $\sum_{n=0}^{\infty}(n-\alpha)a_n z^n$ is a rational function, there exist distinct nonzero algebraic numbers $\theta_1, \theta_2, \cdots, \theta_m$ and polynomials with algebraic coefficients $\lambda_1, \lambda_2, \cdots, \lambda_m$ such that

$$(1) \qquad (n-\alpha)a_n = \sum_{i=1}^{m} \lambda_i(n)\theta_i^n ,$$

for all $n \geqq n_0$, where n_0 is a rational integer. By replacing the sequence $\{a_n\}$ by the sequence $\{a_{n+n_0}\}$ if necessary, we may assume that (1) holds for all $n \geqq 0$. Let K be an algebraic number field which contains α, the coefficients of the λ_i, and the θ_i. Choose a rational integer k and a prime ideal $P \subset K$ such that P divides the numerator of $k-\alpha$ and does not divide the numerator or denominator of α, the θ_i, the differences $(\theta_i - \theta_j)\,(i \neq j)$, and the coefficients of the λ_i; by Lemma 1, there are infinitely many choices for the prime ideal P. Suppose that $NmP = p^f$ where p is a rational prime. We substitute $n = k + jp^f$ in (1), where j is a rational integer:

$$(k + jp^f - \alpha)a_n = \sum_{i=1}^{m} \lambda_i(k + jp^f)\theta_i^{k+jp^f} .$$

Since $p^f \equiv 0(P)$ and $k \equiv \alpha(P)$, we obtain

$$0 \equiv \sum_{i=1}^{m} \lambda_i(\alpha)\theta_i^k \theta_i^{jp^f}(P) .$$

But $\theta_i^{jp^f} \equiv \theta_i^j(P)$, hence

$$(2) \qquad \sum_{i=1}^{m} \lambda_i(\alpha)\theta_i^{k+j} \equiv 0(P) .$$

The m equations obtained from (2) by successively substituting $j = 0, 1, 2, \cdots, m-1$ are linear in the $\lambda_i(\alpha)$ and have as determinant $\prod_{i=1}^{m} \theta_i^k$ times the Vandermonde determinant det $\| \theta_i^j \|$, $1 \leqq i \leqq m$, $0 \leqq j \leqq m-1$, which is not $\equiv 0(P)$, since P does not divide any of the θ_i or the differences $(\theta_i - \theta_j)\,(i \neq j)$. Hence

$$(3) \qquad \lambda_i(\alpha) \equiv 0(P),\ 1 \leqq i \leqq m .$$

By Lemma 1, (3) is true for infinitely many prime ideals P, hence $\lambda_i(\alpha) = 0,\ 1 \leqq i \leqq m$. It follows that the polynomials $\lambda_i(n)$ are divisible by $n - \alpha$. Put $\mu_i(n) = \lambda_i(n)/(n - \alpha)$; $\mu_i(n)$ is a polynomial with algebraic coefficients. By (1)

$$a_n = \sum_{i=1}^{m} \mu_i(n)\theta_i^n .$$

Thus $\sum_{n=0}^{\infty} a_n z^n$ is a rational function.

LEMMA 3. *Suppose $\{a_n\}$ is a sequence of algebraic numbers and f is a nonzero polynomial with complex coefficients. If $\sum_{n=0}^{\infty} f(n)a_n z^n$ is a rational function, then there exists a nonzero polynomial g with algebraic coefficients snch that $\sum_{n=0}^{\infty} g(n)a_n z^n$ is a rational function.*

Proof. There exist distinct nonzero complex numbers $\theta_1, \theta_2, \cdots, \theta_m$ and nonzero polynomials with complex coefficients $\lambda_1, \lambda_2, \cdots, \lambda_m$ such that

$$f(n)a_n = \sum_{i=1}^{m} \lambda_i(n)\theta_i^n , \tag{4}$$

for all large n. Without loss of generality, we may assume that (4) holds for all $n \geqq 0$. In what follows, all fields are considered as subfields of the field of complex numbers. Denote by Ω the field of algebraic numbers, and by L the smallest field which contains Ω, the θ_i, and all of the coefficients of the polynomials $f, \lambda_1, \lambda_2, \cdots, \lambda_m$.

Since L is finitely generated over Ω, it has a finite transcendence basis $x_1, x_2, \cdots, x_r$. Each of the θ_i, the coefficients of the λ_i, and the coefficients of f satisfies an irreducible polynomial equation whose coefficients are elements of $\Omega[x_1, x_2, \cdots, x_r]$. Let $h_1, h_2, \cdots, h_s$ be all of the nonzero coefficients of these polynomials; $h_1, h_2, \cdots, h_s$ are polynomials in $x_1, x_2, \cdots, x_r$ with coefficients in Ω. Since there are only finitely many such polynomials, there exist algebraic numbers $\xi_1, \xi_2, \cdots, \xi_r$ such that $h(\xi_1, \xi_2, \cdots, \xi_r) \neq 0, 1 \leqq i \leqq s$. The map $x_i \rightarrow \xi_i$ gives rise to a homomorphism of the ring $\Omega[x_1, x_2, \cdots, x_r]$ onto Ω, which is the identity on Ω. By the extension of place theorem [1, p. 8], this homomorphism can be extended to a place $\varphi : L \rightarrow \Omega$, which is the identity on Ω. If $\alpha \in L$, we denote by $\bar{\alpha}$ the image of α under φ and if b is a polynomial, $b(n) = \sum_{i=1}^{t} b_i n^i$ with coefficients $b_i \in L$, we denote by $\bar{b}$ the polynomial with $\bar{b}(n) = \sum_{i=1}^{t} \bar{b}_i n^i$. The θ_i and the coefficients of $f, \lambda_1, \lambda_2, \cdots, \lambda_m$ satisfy nonconstant polynomials $g_1, g_2, \cdots, g_v$ with nonzero constant term; the nonzero coefficients of these polynomials are the h_j. Under the place φ the h_j go into finite nonzero algebraic numbers $\bar{h}_j$. Hence the polynomial $\bar{g}_k$ has the same degree as g_k, all of its terms are finite, and its constant term is not zero $(1 \leqq k \leqq v)$. The $\bar{\theta}_i$ and the coefficients of $\bar{f}, \bar{\lambda}_1, \bar{\lambda}_2, \cdots, \bar{\lambda}_r$ are roots of these polynomials; hence the $\bar{\theta}_i$ are finite, nonzero algebraic numbers, and the $\bar{f}, \bar{\lambda}_1, \bar{\lambda}_2, \cdots, \bar{\lambda}_m$ are nonzero polynomials, with finite, algebraic coefficients. Applying the place φ to both terms in (4), and putting $\bar{f} = g$, yields, since $\bar{a}_n = a_n$

$$g(n)a_n = \sum_{i=1}^{m} \bar{\lambda}_i(n)\bar{\theta}_i^n .$$

Hence

$$\sum_{n=0}^{\infty} g(n)a_n z^n = \sum_{n=0}^{\infty} \sum_{i=1}^{m} \bar{\lambda}_i(n)\bar{\theta}_i^n z^n$$

is a rational function, and g is a nonzero polynomial with algebraic coefficients.

Proof of theorem. By Lemma 3, we may assume that f has algebraic integer coefficients. Let α be a root of f and $g(n) = f(n)/(n - \alpha)$; by the lemma of Gause, $g(n)$ is a polynomial with algebraically integral coefficients. Put $b_n = g(n)a_n$; $\{b_n\}$ is a sequence of algebraic integers and $\sum_{n=0}^{\infty}(n - \alpha)b_n z^n$ is a rational function. By Lemma 2, so is $\sum_{n=0}^{\infty} b_n z^n$. Proceeding inductively, on the degree of f, we see that $\sum_{n=0}^{\infty} a_n z^n$ is a rational function.

REMARK. By the Remark following Lemma 1, one can replace, in the theorem, the requirement that the a_n be integers, by the requirement that the set of prime ideal divisors of the denominators of the a_n has Dirichlet density less than 1 among all prime ideals.

Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$, where the a_n are rational integers. Polya's theorem then asserts that if $f'(z)$ is a rational function, so is $f(z)$. The corresponding assertion of our generalization of Polya's theorem is: Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$ be a power series with algebraically integral coefficients. If there exists a nonzero differential operator L, of the form $L = \sum_{i=0}^{r} c_i(zd/dz)^i$ (c_i complex numbers), such that Lf is a rational function, then so is $f(z)$.

REFERENCES

1. S. Lang, *Introduction to algebraic geometry*, New York, 1958.
2. T. Nagell, *Introduction to number theory*, New York, 1958.
3. G. Polya, *Arithmetische Eigenschaften der Reihenentwicklungen*, J. Reine u. angew. Math., **151** (1921), 1-31.

INSTITUTE FOR DEFENSE ANALYSES
UNIVERSITY OF WASHINGTON