BULLETIN 13 (2), 1970

THE ORDER OF ALGEBRAIC LINEAR TRANSFORMATIONS

BY
RANDEE PUTZ

In this paper we extend the results of an earlier note [1].

DEFINITION. Let E be an extension field of the rationals. A vector $v=(b_1, \ldots, b_n)$ in E^n is *algebraic* if each coordinate b_i is algebraic over the rationals. A linear transformation $T: E^n \to E^n$ is *algebraic* if $T(v)$ is an algebraic vector for every algebraic vector v.

DEFINITION. The *degree* of an algebraic linear transformation T, denoted by $\deg T$, is the minimum of $[K: Q]$ taken over all finite algebraic extensions K of the rationals Q such that $T: K^n \to K^n$.

REMARK. Clearly if (a_{ij}) is the matrix representation of the algebraic linear transformation T, the degree of T is the degree over the rationals of the algebraic extension generated by the algebraic numbers a_{ij}.

DEFINITION. Let $\mathfrak{A}$ denote the algebra over the rationals of algebraic linear transformations $T: E^n \to E^n$. For T in $\mathfrak{A}$, T has *order m*, if $T^m=I$ (the identity transformation) and m is the smallest integer q for which $T^q=I$.

THEOREM. *Let T belong to $\mathfrak{A}$ the algebra of algebraic linear transformations. If T has order m then*

$$m \leq e^C(\log (n \deg T+1))(1+1/\log^2 (n \deg T+1))(n \deg T)^{\pi(n \deg T+1)}$$

where $\pi(t)$ denotes the number of primes less than t, C is Euler's constant, and an approximate value for e^C is, $e^C=1.78107\,24179\,90198$.

REMARK. If the extension field E is algebraic over the rationals of degree q, then replacing $\deg T$ by q in the inequality in the theorem yields a uniform bound on the order of algebraic linear transformations of E^n onto E^n.

Proof of the Theorem. Let K be the finite algebraic extension of the rationals such that $T: K^n \to K^n$ and $\deg T=[K: Q]$. Since K is a vector space over the rationals of dimension $\deg T$, let $v \to v_Q$ denote the linear isomorphism over the rationals, Q, of vectors v in K^n and vectors v_Q in Q^r, where $r=n \deg T$. The linear transformation $T: K^n \to K^n$ yields a linear transformation over Q, denoted by $T_Q: Q^r \to Q^r$, defined by $T_Q(v_Q)=(T(v))_Q$.

One easily establishes that for any two linear transformations $S, T: K^n \to K^n$ we have $(ST)_Q=S_QT_Q$. By induction we see that if the transformation T has order m

then the transformation T_Q has order m. Our result then follows immediately from the following theorem which appears in [1].

THEOREM. *If* $L: Q^r \to Q^r$ *is a linear transformation of order* m *then*

$$m \leq e^C(\log (r+1))(1+1/\log^2(r+1))r^{\pi(r+1)}.$$

REFERENCE

1. Randee Putz, *An estimate for the order of rational matrices*, Canad. Math. Bull. **10** (1967), 459–461.

TEMPLE UNIVERSITY,
PHILADELPHIA, PENNSYLVANIA

https://doi.org/10.4153/CMB-1970-055-x Published online by Cambridge University Press