ON A THEOREM OF LATIMER AND MACDUFFEE

OLGA TAUSSKY

THE matrix solutions of an irreducible algebraic equation with integral coefficients were studied by Latimer and MacDuffee.[1] They considered matrices with rational integers as elements. If A is such a matrix, then all matrices of the "class" $S^{-1}AS$ will again be solutions if S is a matrix of determinant ± 1. On the other hand, in general all solutions cannot be derived in this way from one solution only. It was in fact shown that the number of classes of matrix solutions coincides with the number of different classes of ideals in the ring generated by an algebraic root of the same equation. Although this result is of interest in many different branches of mathematics it is not generally known. It seems particularly often required for periodic matrices.[2]

Latimer and MacDuffee actually dealt with the more general case when the equation was reducible. By restriction to irreducible equations only, a very simple proof can be obtained.

In what follows $f(x)=0$ is an irreducible algebraic equation of degree n with integral coefficients, α one of its algebraic roots, $A=(a_{ik})$ an $n \times n$ matrix with rational integers as elements which satisfies $f(x)=0$ and S is a matrix with rational integers as elements and determinant ± 1.

THEOREM 1. *The algebraic number α is a characteristic root of the matrix A and the components of the corresponding characteristic vector $(\alpha_1, \ldots, \alpha_n)$ can be chosen to form the basis of an ideal in the ring formed by the polynomials in α with rational integers as coefficients.*

Proof. Since $f(x)$ is assumed irreducible it follows that it is the characteristic and the minimum polynomial of A and that α is a characteristic root of A. Since in this case the characteristic roots of A are all simple, the corresponding characteristic vector is uniquely determined apart from a factor of proportionality. Since

$$\alpha(\alpha_1, \ldots, \alpha_n) = A(\alpha_1, \ldots, \alpha_n) \tag{1}$$

we may take for α_i the cofactor of the ith element in a fixed row of the deter-

Received July 20, 1948.

[1] C. G. Latimer and C. C. MacDuffee, "A Correspondence Between Classes of Ideals and Classes of Matrices," *Ann. of Math.*, vol. 34 (1933), 313-316. See also related work in A. Speiser, *Theorie der Gruppen* (Springer, 1937); B. L. van der Waerden, *Gruppen von linearen Transformationen* (Springer, 1935); H. Zassenhaus, "Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen," *Abh. Math. Sem. Hansischen Univ.*, vol. 12 (1938), 276-288.

[2] See e.g. R. P. Bambah and S. Chowla, "On Integer Roots of the Unit Matrix," *Proc. Nat. Inst. Sci. India*, vol. 13 (1937), 241-246.

https://doi.org/10.4153/CJM-1949-026-1 Published online by Cambridge University Press

minant $|a_{ik} - \alpha\delta_{ik}|$. This is a polynomial in α with rational integral coefficients. From (1) it follows that

$$\alpha^i(\alpha_1, \ldots, \alpha_n) = A^i(\alpha_1, \ldots, \alpha_n), \qquad (i = 0, \ldots, n-1).$$

Since the numbers $1, \alpha, \ldots, \alpha^{n-1}$ form a basis for the ring in question, it is proved that the set of numbers

$$a_1\alpha_1 + \ldots + a_n\alpha_n$$

where a_i are rational integers, forms an ideal.

THEOREM 2. *Two ideals determined (as in Theorem 1) from the same matrix A belong to the same ideal class.*

Proof. Since the elements of the basis of an ideal in Theorem 1 are uniquely determined apart from a common multiplier it follows that any two such ideals must be equivalent—as usual two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be equivalent or belong to the same class if two elements, α, β in the ring exist such that

$$\mathfrak{a}\alpha = \mathfrak{b}\beta.$$

THEOREM 3. *To every ideal $(\omega_1, \ldots, \omega_n)$ in the ring generated by α there corresponds a matrix X with rational integers as elements which satisfies $f(X) = 0$ and such that*

$$\alpha(\omega_1, \ldots, \omega_n) = X(\omega_1, \ldots, \omega_n).$$

Proof. Since $(\omega_1, \ldots, \omega_n)$ is an ideal there must exist a relation

$$\alpha(\omega_1, \ldots, \omega_n) = X(\omega_1, \ldots, \omega_n) \tag{2}$$

where X is a matrix with rational integral elements. From (2) follows

$$\alpha^i(\omega_1, \ldots, \omega_n) = X^i(\omega_1, \ldots, \omega_n), \qquad (i = 0, \ldots, n-1).$$

This implies

$$f(\alpha)(\omega_1, \ldots, \omega_n) = f(X)(\omega_1, \ldots, \omega_n) = 0.$$

Since $f(X)$ is also a matrix with rational elements and since the relations

$$f(X)(\omega_1^{(i)}, \ldots, \omega_n^{(i)}) = 0$$

hold in the fields generated by the conjugate roots of α and $|\omega_i^{(k)}| \neq 0$ it follows that

$$f(X) = 0.$$

THEOREM 4. *The matrix X in Theorem 3 is uniquely determined apart from a transformation SXS^{-1}.*

Proof. If a different basis for the ideal were chosen it would be of the form $S(\omega_1, \ldots, \omega_n)$ with $|S| = \pm 1$. There would then be a relation

$$\alpha S(\omega_1, \ldots, \omega_n) = YS(\omega_1, \ldots, \omega_n).$$

On the other hand, in virtue of (2)

$$\alpha S(\omega_1, \ldots, \omega_n) = SX(\omega_1, \ldots, \omega_n).$$

Hence by the argument used at the end of the proof of Theorem 3:

$$SX = YS \qquad \text{or}$$
$$Y = SXS^{-1}.$$

https://doi.org/10.4153/CJM-1949-026-1 Published online by Cambridge University Press

The Theorems 1–4 show that *there is a* 1-1 *correspondence between the classes of matrices and the ideal classes.*

It may be pointed out that the matrices S for which $SAS^{-1} = A$ play a role similar to the units in the algebraic number fields. Such a matrix is in fact a polynomial[3] in A, and since its determinant is ± 1 it is a unit in the field generated by A.

Institute for Numerical Analysis
National Bureau of Standards

[3] See e.g. J. H. M. Wedderburn, "Lectures on Matrices," *Amer. Math. Soc. Colloquium Publications,* vol. 17 (1934), 27.

https://doi.org/10.4153/CJM-1949-026-1 Published online by Cambridge University Press