ON THE DIAGONAL FORM OF REAL SYMMETRIC MATRICES

BY

F. D. VELDKAMP

(Communicated by Prof. T. A. Springer at the meeting of January 27, 1973)

Introduction

In numerical mathematics one would like to have some kind of algorithm which brings a real or complex matrix in diagonal or triangular form by means of rational operations and taking arbitrary n-th roots. For arbitrary matrices such an algorithm cannot exist, since it would imply the characteristic polynomial always to be solvable by radicals, which is not the case in general by the Abel-Ruffini theorem. One might ask the same question for the diagonal form of real symmetric matrices. In this note we show the answer in this case to be negative either, by producing real symmetric matrices whose characteristic polynomials are not solvable.

The problem has been suggested by A. van der Sluis in a discussion with the author.

1. Lemma. *Let $l_0 \supset k_0$ be a Galois extension of commutative fields whose Galois group G_0 is isomorphic to either S_n or A_n with $n>4$, $k \supset k_0$ an extension made by successive adjunction of square roots, $l=l_0k$ a common extension of l_0 and k generated by these two fields. Then $l \supset k$ is a Galois extension with Galois group isomorphic to either S_n or A_n.*

Proof. l_0 is the splitting field over k_0 of a separable polynomial, hence so is l over k, i.e., l is Galois over k. Clearly $l \neq k$, for otherwise $l_0 \subseteq k$, which is impossible since $[l_0 : k_0]=n!$ or $\frac{1}{2}n!$, and $[k : k_0]$ is a power of 2. Let G denote the Galois group of l over k. Any $\sigma \in G$ leaves l_0 invariant as a whole, since l_0 is normal over k_0; the restriction of σ to l_0 will be called σ_0. Obviously $\sigma \mapsto \sigma_0$ is an injective homomorphism of G into G_0; let H denote the image of G under this homomorphism, so $G \cong H$. If we can show H to be normal in G, it follows that $H=S_n$ or A_n by the simplicity of A_n.

We have a tower of extensions

$$k_0 \subset k_1 \subset k_2 \subset \ldots \subset k_t = k$$

with $k_i = k_{i-1}(\alpha_i)$, $\alpha_i^2 \in k_{i-1}$. So we also have

$$l_0 \subseteq l_0 k_1 \subseteq l_0 k_2 \subseteq \ldots \subseteq l_0 k_t = l,$$

with $l_0k_i = l_0k_{i-1}(\alpha_i)$. Any $\tau_0 \in G$ can be extended step by step to an automorphism of $l_0k_1, l_0k_2, \ldots, l$ over k_0 which leaves each of the fields $k_1, k_2, \ldots, k_t = k$ invariant as a whole. That is, we can find an automorphism τ of l over k_0 which leaves both k and l_0 invariant as a whole, and such that the restriction of τ to l_0 is τ_0. For $\sigma \in G$, the k_0-automorphism $\tau\sigma\tau^{-1}$ of l induces the identity on k, hence belongs to G. Therefore $\tau_0\sigma_0\tau_0^{-1} \in H$, which shows that $H \lhd G_0$.

Remark. The above argument, of course, works under much weaker assumptions. If G_0 has a simple normal subgroup G_0', and k is obtained from k_0 by a series of successive normal extensions, then either $G=1$ or G is isomorphic to a subgroup H of G_0 with $G_0' \subseteq H \subseteq G_0$.

2. Consider the following situation. Let k_0 be a subfield of the reals, $f \in k_0[X]$ a polynomial of degree $n > 4$ whose splitting field l_0 over k_0 is also contained in the reals and such that the Galois group G_0 of l_0 over k_0 is isomorphic to either S_n or A_n.

Let $A\colon k_0^n \to k_0^n$ be any linear transformation having f as its characteristic polynomial, e.g.,

$$A = \begin{pmatrix} 0 & 0 & & 0 & -u_n \\ 1 & 0 & \cdots & \vdots & \vdots \\ 0 & 1 & & & \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & 0 & -u_2 \\ 0 & 0 & & 1 & -u_1 \end{pmatrix}$$

if $f = X^n + u_1X^{n-1} + \ldots + u_{n-1}X + u_n$. There are n distinct roots of f in l, say $\lambda_1, \ldots, \lambda_n$.

We embed k_0^n in l_0^n, and extend A linearly to l_0^n. The Galois group G_0 operates coordinatewise on l_0^n:

$$\sigma(\xi_1, \ldots, \xi_n) = (\sigma\xi_1, \ldots, \sigma\xi_n) \text{ for } \sigma \in G_0,\ \xi_i \in l_0.$$

Corresponding to the eigenvalue λ_1 we choose an eigenvector e_1 of A in l_0^n whose coordinates are rational functions of λ_1. If $\sigma\lambda_1 = \lambda_i$ for $\sigma \in G_0$, then clearly $e_i = \sigma e_1$ is an eigenvector with eigenvalue λ_i, and e_i does not depend on σ such that $\sigma\lambda_1 = \lambda_i$. The vectors $e_1, \ldots, e_n$ form a basis of l_0^n. We choose a positive definite inner product $(\ ,\ )$ in l_0^n for which $e_1, \ldots, e_n$ form an orthonormal basis. Clearly, A is symmetric with respect to $(\ ,\ )$. Since every $\sigma \in G_0$ permutes $e_1, \ldots, e_n$, we have

$$(\sigma x, \sigma y) = \sigma(x, y) \text{ for } x, y \in l_0^n,$$

so, in particular,

$$\sigma(x, y) = (x, y) \text{ for } x, y \in k_0^n,$$

i.e., $(x, y) \in k_0$ for x and $y \in k_0^n$. Take an orthogonal basis $a_1, \ldots, a_n \in k_0^n$. Choose $\alpha_i \in \mathbf{R}$ with $\alpha_i^2 = (a_i, a_i)$ and take $k = k_0(\alpha_1, \ldots, \alpha_n)$, $l = l_0 k$. Then l is the splitting field of f over k, with Galois group $G \cong S_n$ or A_n by the lemma. In k^n we can find an orthonormal basis, viz., $\alpha_1^{-1}a_1, \ldots, \alpha_n^{-1}a_n$. With respect to this basis the extension of A to k^n is represented by a symmetric matrix.

3. A polynomial f as in the previous section can easily be found. Choose, for instance, real numbers $t_1, \ldots, t_n$ which are algebraically independent over the rationals, and take

$$f = (X - t_1) \ldots (X - t_n) = X^n + u_1 X^{n-1} + \ldots + u_{n-1}X + u_n.$$

For the ground field we must take $k_0 = \mathbf{Q}(u_1, \ldots, u_n)$, whereas $l_0 = \mathbf{Q}(t_1, \ldots, t_n)$ is a splitting field of f. As is well known, the Galois group of l_0 over k_0 is S_n in this case.

One can even find polynomials

$$f = X^n + a_1 X^{n-1} + \ldots + a_{n-1}X + a_n$$

with rational coefficients $a_1, \ldots, a_n$, hence $k_0 = \mathbf{Q}$, splitting field $l_0 \subseteq \mathbf{R}$ and Galois group S_n. This was shown in [1]. The argument is as follows. Take any polynomial g with rational coefficients which has n distinct real roots, say

$$g = X^n + b_1 X^{n-1} + \ldots + b_{n-1}X + b_n.$$

From Sturm's theorem (cf. [2], p. 280, or [4], p. 304) it follows that any polynomial

$$f = X^n + a_1 X^{n-1} + \ldots + a_{n-1}X + a_n$$

with real $a_1, \ldots, a_n$ such that all $|b_i - a_i|$ are sufficiently small has n distinct real roots. Let $c_0, c_1, \ldots, c_n$ be certain integers, $c_0 \neq 0$, and take $a_i = c_0^{-1}c_i$ for $i = 1, \ldots, n$. If $c_0, \ldots, c_n$ satisfy certain congruences, the Galois group of the splitting field of f over $\mathbf{Q}$ is S_n (cf. [3], § 61). Moreover, $c_0, \ldots, c_n$ can be chosen so that $a_1, \ldots, a_n$ are near enough to $b_1, \ldots, b_n$, hence f has n distinct real roots.

The result of sections 2 and 3 are summarized in the following

PROPOSITION. *For $n > 4$ there exist symmetric matrices with entries in a subfield k of the reals such that the splitting field l over k of the characteristic polynomial f of such a matrix has Galois group either S_n or A_n. One can even find such a matrix with $k = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i^2 \in \mathbf{Q}$ for $i = 1, \ldots, n$, and such that f has coefficients in $\mathbf{Q}$.*

Mathematical Institute
University of Utrecht

BIBLIOGRAPHY

1. BAUER, M., Ganzzahlige Gleichungen ohne Affekt. Math. Ann. **64**, 325–327 (1907).
2. JACOBSON, N., Lectures in abstract algebra **III**. Van Nostrand, Princeton (1964).
3. WAERDEN, B. L. VAN DER, Algebra **I**, 6e Aufl. Springer Verlag, Berlin etc. (1964).
4. WEBER, H., Lehrbuch der Algebra **I**, 2e Aufl. Vieweg und Sohn, Braunschweig (1912).