GALOIS GROUPS ASSOCIATED WITH CM-FIELDS, SKEW-SYMMETRIC MATRICES AND ORTHOGONAL MATRICES

by S. D. COHEN and R. W. K. ODONI

(Received 19 September, 1988)

0. Introduction. The main aims of this paper are to provide a device for constructing large families of complex-multiplication (CM) fields, and to examine the Galois groups of some related field extensions. We recall that an algebraic number field $K$ (i.e. $[K:Q]<\infty$) is called a CM-field if it is totally complex but is quadratic over some totally real field (see Section 1). CM fields are important in algebraic geometry, since the ring of endomorphisms of a simple abelian variety defined over an algebraic number field is either $\mathbb{Z}$ or a $\mathbb{Z}$-order in a CM field. Moreover, CM fields figure prominently in classfield theory, since Shimura [15] has shown that “almost all” classfields over CM fields $K$ can be generated by means of division points on abelian varieties admitting $\mathbb{Z}$-orders in $K$ as their endomorphism rings. Shimura’s work can be regarded as a natural generalization of the classical method (due to Kronecker and H. Weber) of generating classfields of imaginary quadratic fields via division points on CM-elliptic curves.

The standard examples of CM fields are abelian over $\mathbb{Q}$: for example, $\mathbb{Q}(e^{2\pi i/n})$ ($n \geq 3$) or $\mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$ squarefree. We shall use properties of skew-symmetric matrices in order to generate CM fields not of the above type. The basic idea is to start with a totally real algebraic number field $F$ and adjoint to it finitely many non-zero eigenvalues of skew-symmetric matrices defined over $F$. In Section 1 we show that this process automatically yields CM fields; in fact, we shall also show that every CM field arises in this way (even taking $F = \mathbb{Q}$ for this purpose). This latter result is a consequence of results of F. Krakowski [9] on symmetric matrices and totally real algebraic numbers. We shall pay particular attention to associated Galois structures; the main effort in our paper is devoted to the calculation of Galois groups of characteristic polynomials of skew-symmetric matrices. In the first place we do this for “generic” skew-symmetric matrices, the underlying principle in operation here being the study of the branch points of associated covers of projective space (ramification), for which we refer, for example, to [6], [7] (although no familiarity with such is needed). Later we apply Hilbert’s irreducibility theorem to obtain results over algebraic number fields.

We begin in Section 1 with some standard results on CM fields and related Galois groups, and establish the characterisation of CM fields as “eigenfields” of skew-symmetric matrices over $\mathbb{Q}$. In Section 2 we define generic skew-symmetric matrices and state our result on the Galois groups of their characteristic polynomials (Theorem 1). An inductive approach to Theorem 1 itself by means of various specialisations was originally set out by the second author (and is briefly summarised in Section 6). On the other hand, very conveniently, existing work of the first author [3] (as we demonstrate in Section 3) exactly yields the analogue of Theorem 1 for a very particular specialisation involving just two indeterminates. This result (Theorem 1’) is, in effect, much stronger than Theorem 1 and might be of independent interest; nevertheless, Theorem 1 suffices for our purpose here. In Section 4, we derive analogous results for orthogonal matrices; the principal tool here is the (modified) Cayley transformation of skew-symmetric matrices into orthogonal matrices.

matrices. In Section 5 we apply Hilbert’s irreducibility theorem in conjunction with our earlier results in order to generate CM fields with prescribed Galois structure of certain types. We conclude by posing the question of the minimal size of a skew-symmetric matrix associated with a given CM field (via the procedure described in Section 1).

1. CM fields. Let \( \mathbb{Q} \) be the rational field, \( \mathbb{Z} \subset \mathbb{Q} \) the ring of integers and let \( \mathbb{R} \) and \( \mathbb{C} \) denote the real field and complex field respectively. Let \( \bar{\mathbb{Q}} \) be an algebraic closure of \( \mathbb{Q} \), which we regard as embedded in \( \mathbb{C} \). If \( \sigma \in \text{Aut} \mathbb{C}, \ z \in \mathbb{C}, \) we write \( z^{\sigma} \) for the image of \( z \) under \( \sigma \), and generally, put \( A^{\sigma} = \{ a^{\sigma} : a \in A \} \) when \( A \subseteq \mathbb{C}, \ \sigma \in \text{Aut} \mathbb{C} \). We always denote complex conjugation by \( x \in \text{Aut} \mathbb{C} \).

An (algebraic) number field \( K \) is a finite algebraic extension of \( \mathbb{Q} \). We call \( K \) a totally real (TR) field if \( K^{\sigma} \subseteq \mathbb{R} \) for all \( \sigma \in \text{Aut} \mathbb{C} \), and totally complex (TC) if \( K^{\sigma} \subseteq \mathbb{R} \) is false for all \( \sigma \in \text{Aut} \mathbb{C} \). The minimal extension of \( K \) which is Galois over \( \mathbb{Q} \) is denoted by \( \bar{\mathcal{K}} \). \( K \) is called a CM field if \( \bar{\mathcal{K}} \) is a TC field but \( [\bar{\mathcal{K}} : \mathbb{F}] = 2 \) for some TR field \( \mathbb{F} \).

The following proposition is, in principle, well-known; part of it is given in [10, Ch. 1], and we leave the proofs to the reader.

**Lemma 1.1.**

(i) Let \( K \) be a CM field; then \( \bar{\mathcal{K}} \) is also a CM field, and \( x (= \text{complex conjugation}) \) is central of order 2 in \( \text{Gal} \bar{\mathcal{K}}/\mathbb{Q} \).

(ii) Let \( L/\mathbb{Q} \) be a finite Galois extension. Then \( L \) is either a TR field or a TC field. Moreover \( L \) is a CM field if and only if \( x \) is central of order 2 in \( \text{Gal} L/\mathbb{Q} \). Let \( F \) be a subfield of \( L \) (Galois, CM), and let \( H = \text{Gal} L/F \). Then \( F \) is a TR field if and only if \( x \in H \), and \( F \) is a TC field if and only if \( x \notin H \).

(iii) Let \( E, F \) be TR fields, and let \( K, L \) be TC fields. Then \( EF \) is a TR field, and \( EK, KL \) are TC fields; if \( K \) and \( L \) are, moreover, CM fields, then \( EK \) and \( KL \) are also CM fields.

We turn to the problem of constructing CM fields.

**Lemma 1.2.** Suppose that \( F \) is a TR field and that \( \lambda \in \bar{\mathcal{Q}} \) is such that \( \lambda^2 \) is a totally negative real number. Then \( F(\lambda) \) is a CM field. More generally, if \( \lambda_1, \ldots, \lambda_n \) are zeros of \( g(x^2) \), where \( g(x) \) is a totally negative polynomial over \( F \), then \( F(\lambda_1, \ldots, \lambda_n) \) is a CM field.

**Proof.** Clearly \( \lambda \) is purely imaginary, \( F(\lambda^2) \) is a TR field and \( F(\lambda) \) a TC field because \( 0 \neq \lambda^\sigma \in i\mathbb{R} \) for all \( \sigma \in \text{Aut} \mathbb{C} \). For the last part use Lemma 1.1(iii).

The relevance of skew symmetric matrices \( S \) over \( F \) now becomes apparent because, by considering also their transposes, such matrices have characteristic polynomials of the form \( x^2g(x^2) \) where \( g \) is non-constant (provided \( S \) is non-zero) and totally negative.

**Corollary 1.2A.** Let \( F \) be a TR field, and let \( S \) be a non-zero \( n \times n \) skew-symmetric matrix over \( F \) (\( n \geq 2 \)). Then \( S \) has a non-zero eigenvalue \( \lambda \), and \( F(\lambda) \) is a CM field. More generally, if \( \lambda_1, \ldots, \lambda_n \) are non-zero eigenvalues of skew-symmetric matrices over \( F \), then \( F(\lambda_1, \ldots, \lambda_n) \) is a CM field.

Significantly, Lemma 1.2 and its corollary have strong converses which we now derive from the following general result.
Lemma 1.3. Let $K$ be an imaginary quadratic extension of a real algebraic number field $F$. Then for some $\lambda$ in $K$, $K = \mathbb{Q}(\lambda)$ and $F = \mathbb{Q}(\lambda^2)$. ($\lambda$ is purely imaginary and $\lambda^2$ is a negative real number.)

Proof. We have $F = \mathbb{Q}(\theta)$ and $K = F(\sqrt{1-\alpha})$, where $\theta$ is real and $\alpha$ is a positive number in $F$. $F$ has finitely many subfields; hence there exist distinct integers $i$, $j$, $k$ (whose size could easily be bounded in terms of $\deg \mathbb{Q}(\theta)$) such that

$$\mathbb{Q}(\alpha \beta^2_i) = \mathbb{Q}(\alpha \beta^2_j) = \mathbb{Q}(\alpha \beta^2_k) = E \text{ (say)} \subseteq F,$$

where $\beta_i = \theta + (r/\alpha) \not\in F$. Then

$$2(i - j)(j - k)(k - i)\theta = (i^2 - k^2)(\alpha \beta^2_i - \alpha \beta^2_j) - (i^2 - j^2)(\alpha \beta^2_j - \alpha \beta^2_k) \in E$$

and so actually $E = F$. Now set $\beta = \beta_i$ and $\lambda = \beta \sqrt{1-\alpha}$. It follows that

$$\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\theta) = \mathbb{Q}(\alpha \beta^2) = \mathbb{Q}(\lambda^2) \subseteq \mathbb{Q}(\lambda) \subseteq K.$$ 

In particular, $\sqrt{1-\alpha} = \lambda/\beta \not\in \mathbb{Q}(\lambda)$ and so $K = \mathbb{Q}(\lambda)$, which completes the proof.

Corollary 1.3A. Let $K$ be a CM-field. Then in $K$ there is a $\lambda$ such that $K = \mathbb{Q}(\lambda)$, $K \cap \mathbb{R} = \mathbb{Q}(\lambda^2)$ and $\lambda^2$ is totally negative, i.e. $\lambda$ is totally imaginary.

Corollary 1.3B. A number field $K$ is a CM field if and only if there is a rational skew-symmetric matrix $S$, and a non-zero eigenvalue $\lambda$ of $S$, such that $K = \mathbb{Q}(\lambda)$.

Proof. The "if" part is a special case of Corollary 1.2A. To prove the "only if" part, we quote a result of Krakowski [9, p. 237]: if $\mu \in \mathbb{Q}$ is totally imaginary, there is a rational skew-symmetric $S$ such that $\det(\mu I - S) = 0$. If $K$ is a CM field we choose $\lambda$ as in Corollary 1.3A and put $\mu = \lambda$.

We now briefly consider the structure of $\text{Gal } K/\mathbb{Q}$ when $K$ is a CM-field. The fact that $\tau$ is a central involution in $\text{Gal } K/\mathbb{Q}$ imposes a strong constraint on the structure of this group. This is best understood in terms of wreath-products of permutation groups [12, Section 4]. As it happens we shall only need to consider the wreath product $S_n[S_2]$ where $S_k$ is the symmetric group on $k$ symbols. Now $S_n[S_2]$ has a simple concrete interpretation in terms of subgroups of $S_{2n}$, which can be described in various equivalent ways. First, we partition the set of symbols $\{1, \ldots, 2n\}$ into $n$ disjoint pairs $\{a_1, a_2\}, \ldots, \{a_{2n-1}, a_{2n}\}$ in arbitrary fashion. We then consider the set of all $\sigma \in S_{2n}$ such that the image of each pair $\{a_{2j-1}, a_{2j}\}$ is again a pair $\{a_{2k-1}, a_{2k}\}$. These $\sigma$ form a subgroup of $S_{2n}$ which is isomorphic to $S_n[S_2]$; we call it a concrete $S_n[S_2]$ in $S_{2n}$, and denote it by $CS_n[S_2]$. Equivalently $CS_n[S_2]$ is the centraliser in $S_{2n}$ of the permutation $(a_1, a_2) \ldots (a_{2n-1}, a_{2n})$, a fixed-point-free involution. If we replace the above pair-partition by another, the effect is merely to conjugate the corresponding $CS_n[S_2]$ by some member of $S_{2n}$. Moreover, since $(a_1, a_2)$ belongs to at least one $CS_n[S_2]$, the latter is not contained in the alternating subgroup $A_{2n}$ of $S_{2n}$. We denote the interaction by $CS_n[S_2] \cap A_{2n}$; it is unambiguous (up to conjugacy), since $A_{2n} \not\subset S_{2n}$.

Lemma 1.4. Let $F$ be any field of characteristic $0$, let $g(x) \in F[x]$ have degree $n \geq 1$, and suppose that $g(x^2)$ has $2n$ distinct zeros (in $\bar{F}$, the algebraic closure of $F$). Then
Gal \( g(x^2) / F \) can be injected into a \( CS_n[S_2] \) in \( S_{2n} \). It can be injected into \( CS_n[S_2] \cap A_{2n} \) if and only if the discriminant of \( g(x^2) \) is a square in \( F \).

Proof. The last assertion follows immediately from the first on using standard elementary Galois theory. (The injections referred to in the statements of the theorem are injections of permutation groups on the \( 2n \) zeros of \( g(x^2) \)). Suppose \( g(x^2) \) has \( 2n \) distinct zeros. Then \( g(x) \) has \( n \) (distinct) zeros \( \beta_1, \ldots, \beta_n \), and we may label the zeros \( \alpha \) of \( g(x^2) \) with double subscripts in such a way that \( \alpha_{i2} = -\alpha_{i1} \) and \( \alpha_{i1}^2 = \alpha_{i2}^2 = \beta_i \) for \( i = 1, \ldots, n \). It is then immediately clear that every \( \sigma \in Gal g(x^2) / F \), regarded as a permutation of the \( \alpha_{ij} \), lies in the \( CS_n[S_2] \) corresponding to the centraliser of \( (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{n1}, \alpha_{n2}) \); the lemma is proved.

We shall now apply Lemma 1.4 to CM fields; we show that, if \( K \) is a CM field with \([K : Q] = 2n\), then \( Gal \hat{K} / Q \) can be injected into \( CS_n[S_2] \). In fact we give two proofs; the first is (implicitly) longer, but also yields the characterisation of CM fields as “eigenfields” of rational skew-symmetric matrices.

**Lemma 1.5.** If \( K \) is a CM field and \([K : Q] = 2n\), \( Gal \hat{K} / Q \) can be (permutation-) injected into a \( CS_n[S_2] \) in \( S_{2n} \).

First proof. We choose \( \lambda \) as in Lemma 1.3 and take \( g(x) \in Q[x] \) to be the minimum polynomial of \( \lambda^2 \) over \( Q \). Then \( Gal \hat{K} / Q \) is (permutation-) isomorphic to \( Gal g(x^2) / Q \) acting on the conjugates of \( \lambda \) over \( Q \), and we can apply Lemma 1.4.

Second proof. We regard \( Gal \hat{K} / Q \) as a group of permutations of the \( 2n \) conjugates of \( \theta \) over \( Q \), where \( K = Q(\theta) \). This yields a faithful representation \( f \) of \( Gal \hat{K} / Q \) into \( S_{2n} \). Since \( \tau \) fixes no conjugate of \( \theta \), \( f(\tau) \) is a fixed-point-free involution, i.e. consists of the product of \( n \) disjoint transpositions in \( S_{2n} \). Moreover, \( f(\tau) \) is central in \( f(Gal \hat{K} / Q) \), so that \( f(Gal \hat{K} / Q) \) is contained in the centraliser of \( f(\tau) \) in \( S_{2n} \), which is a \( CS_n[S_2] \), as required.

2. Generic skew-symmetric matrices. Let \( F \) be any field of characteristic 0, and let \( n \geq 1 \). We choose \( n(n - 1)/2 \), quantities \( t_{ij} \) (\( 1 \leq i < j \leq n \)) which are algebraically independent over \( F \), define \( t_{ji} \) to be \((-t_{ij}) \) if \( 1 \leq i < j \leq n \), and form the matrix \( \Sigma_n \) whose \((i, j)\) entry is \( t_{ij} \). We call \( \Sigma_n \) a generic skew-symmetric \( n \times n \) matrix over \( F \). Let \( x \) be a further indeterminate; we put \( f_n(x) = \det(x \Sigma_n - \Sigma_n) \). Our aim is to calculate the Galois group \( \Gamma_n(F) \) of \( f_n(x) \) over the field \( F_n \) obtained from \( F \) by adjoining the entries of \( \Sigma_n \). It is obvious (see below) that \( \Gamma_n(F) \) is well-defined, \( f_n \) being irreducible.

Next we observe that, by transposing \( x \Sigma_n - \Sigma_n \), we have

\[
f_{2n}(x) = g_{2n}(x^2), \quad f_{2n+1}(x) = x g_{2n+1}(x^2),
\]

where \( g_m(x) \) is \( x \)-monic in \( Z[x, \ldots, t_{ij}, \ldots] \) of degree \([m/2]\). Because of (2.1), it is occasionally convenient to use \( f_m \) etc. to denote either \( f_{2n} \) or \( f_{2n+1} \) in which case \( n = [m/2] \). For example, \( \deg g_m = n \) and defining \( G_m(F) \) as \( Gal g_m(x)/F_m \), we have \( G_m(F) \subseteq S_n \). We shall prove

**Theorem 1.** Let \( F \) be any field of characteristic 0. Then, for any \( n \geq 1 \),

\[
\begin{align*}
(i) & \quad \Gamma_{2n}(F) \equiv \begin{cases} CS_n[S_2] \cap A_{2n}, & \text{if } \sqrt{-1} \in F \text{ or } n \text{ is even}; \\ CS_n[S_2], & \text{if } \sqrt{-1} \notin F \text{ and } n \text{ is odd}; \end{cases} \\
(ii) & \quad \Gamma_{2n+1}(F) \equiv CS_n[S_2].
\end{align*}
\]
Theorem 1, of course, contains the assertion that $G_m(F) = S_n$. Granted this, we quote from Lemma 5 of [3] (see also Lemma 4 of [5]) the following relevant result, using $\Delta(g)$ for the discriminant of $g$ and $v(g)$ for $(-1)^{\deg g(0)}$.

**Lemma 2.1.** Let $g(x)$ be a monic polynomial of degree $n$ over $F$, a field of characteristic 0. Suppose that

(i) $\text{Gal}(g(x)/F) \cong S_n$,

(ii) $\Delta(g) \neq v(g) \times (\text{square in } F)$,

(iii) $\text{Gal}(g(x^2)/E \notin C_2$, where $E$ is the splitting field of $g$ and $C_2$ is a cyclic group of order 2. Then

$$\text{Gal}(g(x^2)/F = \begin{cases} \text{CS}_n[S_2] \cap A_{2n}, & \text{if } v(g) \text{ is a square in } F, \\ \text{CS}_n[S_2], & \text{otherwise.} \end{cases}$$

The conclusions of Lemma 2.1 and Theorem 1 (in particular (2.2)) are tied by the following simple fact concerning the generic polynomial $g_{2n}$.

**Lemma 2.2.** $v(g_{2n}) = (-1)^n P_{2n}^2$, where $P_{2n} \in \mathbb{Z}[t_2, \ldots, t_{ij}, \ldots]$.

**Proof.** $g_{2n}(0) = f_{2n}(0) = \det(-\Sigma_{2n}) = P_{2n}^2$, where $P_{2n}$ is the Pfaffian [8, vol. 1, 334–336, 400].

As stated in the Introduction, we take advantage of previous work [3] to prove a much stronger analogue of Theorem 1 for a certain specialisation of $f_m$ involving just two indeterminates $t$ and $u$. Of course, it implies Theorem 1 itself, although, for (2.2), a further application of Lemma 2.1 and 2.2 is necessary.

3. Reduction to two indeterminates. Take the specialisation of $\Sigma_n$ which is zero away from the super and sub-diagonals and has super-diagonal $\{t, u, 1, \ldots, 1\}$, where $t$ and $u$ are independent indeterminates. Thus, formally, if $1 \leq i \leq j \leq n$, then $t_{ij} = 0$ unless $j = i + 1$ in which case

$$t_{i,i+1} = \begin{cases} t, & \text{if } i = 1, \\ u, & \text{if } i = 2, \\ 1, & \text{if } 3 \leq i \leq n - 1. \end{cases}$$

**In this section only** we assume the above specialisation has been accomplished in reference to the polynomials $f_n(x)$ and $g_n(x)$ etc. However, for clarity, on some occasions these will be denoted by $f_n(x; t, u)$ and $g_n(x; t, u)$. Similarly, $\Gamma_n(F; t, u)$ will denote $\text{Gal}(f_n(x; t, u)/F(t, u))$ etc.

We define $f_0(x) = g_0(x) = 1$ and note that

$$f_1(x) = x, \quad g_1(x) = 1;$$

$$f_2(x) = x^2 + t^2, \quad g_2(x) = x + t^2;$$

$$f_3(x) = x(x^2 + t^2 + u^2), \quad g_3(x) = x + t^2 + u^2.$$ (3.1)

More generally, expanding by the first row of the defining determinant, we have

**Lemma 3.1.** $f_n(x; t, u) = x f_{n-1}(x; u, 1) + t^2 f_{n-2}(x; 1, 1), n \geq 2$.

**Corollary 3.1A.** (i) $g_n$ and $g_{n-1}$ are co-prime for all $n \geq 1$,

(ii) $g_{2n}(0) = t^2, \quad g_{2n+1}(0) = nt^2 + u^2$.

**Proof.** By induction.
Writing \( g_n^*(x) \) for \( g_n(x; 1, 1) \) and \( T = t^2, \ U = u^2, \ V = nT + U \), we obtain the following by a second application of Lemma 3.1.

**Lemma 3.2.** For \( n \geq 2 \),

\[(i) \quad g_{2n}^*(x) = xg_{2n-2}^*(x) + Tg_{2n-2}^*(x) + Uxg_{2n-3}^*(x); \]
\[(ii) \quad g_{2n+1}^*(x) = xg_{2n-1}^*(x) + Tg_{2n-1}^*(x) + Ug_{2n-2}^*(x); \]
\[(iii) \quad = xg_{2n-1}^*(x) + Tg_{2n-1}^*(x) + Vg_{2n-2}^*(x), \]

where \( \hat{g}_{2n-1}^*(x) = g_{2n-1}^*(x) - ng_{2n-2}^*(x) \), whence \( \hat{g}_{2n-1}(0) = 0 \).

With Lemma 3.2 in mind, we now describe a more general context which is, however, merely a special case of work covered in [3] (and also developed in [4]).

First assume that \( F \) is an algebraically closed field of characteristic 0 and \( t_1 \) and \( t_2 \) are indeterminates. Let \( h(x) = h_0(x) + t_1h_1(x) + t_2h_2(x) \in F[x, t_1, t_2] \) where \( h_0, h_1, h_2 \) are relatively prime polynomials (i.e. \( (h_1, h_2, h_3) = 1 \)), linearly independent over \( F \) and such that \( n = \deg h_0 > \max(\deg h_1, \deg h_2) \). Suppose also that they are not “totally composite” [3, p. 148], which simply means that they are not all functions of the same non-linear rational function. Finally, suppose that, for all pairs \((\alpha, \beta)\) of \( F \), the (polynomial) highest common factor of \( h_0(x) + \alpha h_1(x) \) and \( h_1(x) + \beta h_2(x) \) is square-free. (All of this ensures that, in one sense, all branch points of \( h \) are “simple”, see [6, Example 1]). The key to the results we now state is a correspondence between elements of (say) Gal \( h(x)/F(t_1, t_2) \) (as permutations of the zeros of \( h \)) and specialisations \( h_0(x) + a_1h_1(x) + a_2h_2(x) \) which have repeated factors; specifically a cycle of length \( s \) in an automorphism is associated with a zero of multiplicity \( s \) in a polynomial—in particular, simple branching relates to transpositions. For other recent applications of such ideas in number fields, see [13], [14].

**Lemma 3.3.** With \( h \) as above

\[(i) \quad \text{Gal } h(x)/F(t_1, t_2) \cong S_n. \]
\[(ii) \quad \text{Suppose also that } x \parallel h_0(x) \text{ and } h_1(0) = 0. \text{ Then}\]
\[\quad \text{Gal } h(x^2)/F(t_1, t_2) \cong CS_n[S_2]. \]

**Proof.** (i) follows from Lemma 7–9 of [3] via the route that the Galois group is a transitive group generated by transpositions. Because \( (h_0, h_1) \) is also square-free (by hypothesis), Lemma 9 of [3] additionally yields the fact that \( h_0(x) + a_1h_1(x) \) is square-free for some \( a_1 \in F \). Indeed, with the extra presupposition for (ii), we can assume that \( x \parallel h_0(x) + a_1h_1(x) \) which means that \( h_0(x^2) + a_1h_1(x^2) \) is also square-free apart from a factor \( x^2 \). By the construction employed in the proof of Lemma 6(iii) of [3] we obtain in \( \text{Gal } h(x^2)/E \) (\( E \) being the splitting field of \( h(x) \) over \( F(t_1, t_2) \)) a transposition \((\alpha, -\alpha)\) affecting simply a single pair \( \pm \alpha \) of zeros of \( h(x^2) \). By the transitivity of \( G = \text{Gal } h(x^2)/F(t_1, t_2) \), the group generated by all such transpositions is \( C_2^2 \); hence \( G \) is an extension of \( C_2 \) by \( S_n \) (by (i)) which yields (ii).

We apply Lemma 3.3 to the situation of Lemma 3.2; note however that, in stating further results, we no longer assume that \( F \) is algebraically closed. We also recall the notation \( n = [m/2], \ T = t^2, \ U = u^2, \ V = nT + U \).

**Corollary 3.3A.**

\[(i) \quad \text{Gal } f_m(x; t, u)/F(T, U) \cong CS_n[S_2], \ m \geq 1. \]
\[(ii) \quad \Delta(g_m) \text{ in } F[T, U] \text{ has even degree in } T \text{ and in } U. \]
Proof. Using (3.1) the results are evident if \( m \leq 3 \) so assume \( m \geq 4 \) (i.e. \( n \geq 2 \)). Because the Galois group of \( f_m \) cannot be larger than \( CS_n[S_2] \), the validity of the theorem for a given field \( F \) is implied by applying it to \( \tilde{F} \). Hence we can also suppose that \( F \) is algebraically closed.

For \( m = 2n \) and with reference to (3.2), take \( h_0(x) = xg_{2n-2}^*(x) \), \( h_1(x) = xg_{2n-3}^*(x) \) and \( h_2(x) = g_{2n-2}^*(x) \). Then, by Corollary 3.1A(i), all the hypotheses of Lemma 3.2 are satisfied; in particular, the highest common factor of \( h_0(x) + \alpha h_2(x) \) and \( h_1(x) + \beta h_2(x) \) has degree 1 at most. Thus (i) follows from Lemma 3.3(iii).

For \( m = 2n + 1 \) we similarly use (3.4) to prove that

\[
\text{Gal}_{m}(x; t, u)/F(T, U) = \text{Gal}_{m}(x; t, u)/F(T, U) = CS_n[S_2].
\]

Again, from (3.3), \( \Delta(g_{2n+1}) \) has degree \((n - 1)\) in each of \( T \) and \( U \).

**Theorem 1'**. The conclusions of Theorem 1 are valid when \( \Gamma_m(F) \) is replaced by \( \Gamma_m(F; t, u) \).

**Proof.** Again by (3.1) we can suppose that \( m \geq 4 \) (i.e. \( n \geq 2 \)).

\( F(t, u) \) is a normal extension of \( F(T, U) \) of degree 4 with quadratic subfields \( F(T, u) \), \( F(t, U) \) and \( F(T, tu) \).

Let \( E \) be the splitting field of \( g_m \) over \( F(T, U) \). Then, by the theorem of natural irrationalities,

\[
G = G_m(F; t, u) = \text{Gal}_{m}(x)/F(t, u) \cap E,
\]

a normal subgroup of \( \text{Gal}_{m}(x)/F(T, U) = S_n \). Hence \( G \), if not \( S_n \), must be \( A_n \). However, the latter would imply that \( F(t, u) \cap E \) is one of the above-mentioned quadratic subfields of \( F(t, u) \) which could only be the case if \( \Delta(g_m) = WA_2(T, U) \), where \( A(T, U) \in F(T, U) \) and \( W = T, U \) or \( TU \). But this is impossible (even if \( F \) were replaced by its algebraic closure \( \tilde{F} \)) by Corollary 3.3A(ii).

Now let \( K \) be the splitting field of \( g(x^2) \) over \( F(T, U) \). Then

\[
\Gamma_m(F; t, u) = \text{Gal}_{m}(x^2)/K \cap F(t, u)
\]

and the result, at least for \( n \geq 4 \), can be derived by considering degrees from Lemma 2.1. Alternatively, argue as follows. By Corollary 3.3A(i) the only normal extensions of \( F(T, U) \) between \( K \) and \( E \) are \( K \), \( E \) and \( E(\alpha_1, \ldots, \alpha_n) \), where \( \alpha_1, \ldots, \alpha_n \) are the zeros of \( g_m(x) \), the last field corresponding to the group \( CS_n[S_2] \cap A_{2n} \). The desired result is thus clear from Lemma 2.1 and Corollary 3.3A(ii) provided \( E(t, u) \subseteq E(\alpha_1, \ldots, \alpha_n) \).

Otherwise, necessarily \( E(t, u) = K \) which implies that \( \deg[K, E] = 4 \) and \( n = 2 \). But then \( E(t) \) and \( E(u) \) are distinct normal extensions of \( F(T, U) \) between \( E \) and \( K \), contradicting the above. The proof is complete.

4. **Generic orthogonal matrices.** Our first task in this section is to give a suitable definition of generic orthogonal matrices. Let \( F \) be any field of characteristic \( \neq 2 \), and let \( M_n(F) \) be the set of all \( n \times n \) matrices over \( F \). It might seem possible to define a matrix \( U \in M_n(K) \) (\( K \) a suitable extension of \( F \)) to be “generic orthogonal” over \( F \) if its entries are “maximally algebraically independent”, subject to the conditions \( U^T U = U U^T = I_n \). Unfortunately, this approach makes it difficult to prove results about \( \det(x I_n - U) \), \( U \)
“generic orthogonal”. We shall therefore adopt a different approach, based on Cayley’s transformation [8, vol. 1, p. 352]. We begin with a short sequence of simple lemmas which, in principle, are well known, their fairly routine proofs in some cases being left as exercises for the reader. Until after Lemma 4.5 we shall take $F$ arbitrary of characteristic $\neq 2$.

**Lemma 4.1.** Let $n \geq 1$, and let $\Omega$ be an orthogonal matrix in $M_n(F)$; we put $u(x) = \det(xI_n - \Omega)$, where $x$ is an indeterminate over $F$. Suppose that $u(x) = (x + 1)^k(x - 1)^l v(x)$, where $v(\pm 1) \neq 0$. Then

(i) $\det \Omega = (-1)^{l-k} = (-1)^{n-l-k}$, so that $n - l - k = 2t$, where $0 \leq t \in \mathbb{Z}$;

(ii) $v(x) = x^{2t} v(x^{-1})$, with $v(x)$ monic of degree $2t$.

(iii) there is a polynomial $w(x) \in F[x]$, with $\deg w(x) = t$, such that $u(x)$ and $w(x^2)$ have the same splitting field over $F$.

**Proof.** (iii) Factorise $v(x)$ into linear factors over the algebraic closure $\bar{F}$ of $F$; by hypothesis $v(\pm 1) \neq 0$ and so $v(x) = \prod_{j \in s} (x - a_j)^{e_j}$, where $\sum_{j \in s} e_j = 2t$ and no $a_j = \pm 1$. Let $y$ be an indeterminate over $\bar{F}$. Then

$$(1 - y)^{2t} \frac{(1 + y)}{1 - y} = A \prod_{j \in s} \left( y + \frac{1 + a_j}{1 - a_j} \right)^{e_j},$$

where $0 \neq A \in \bar{F}$; hence $(1 - y)^{2t} v(1 + y/1 - y) = w^*(y) \in F[y]$, with $\deg w^*(y) = 2t$. Finally, (ii) implies that $w^*(y) = w^*(-y)$, so that $w^*(y) = w(y^2)$, where $w(y) \in F[y]$ and $\deg w(y) = t$; this clearly proves the lemma.

**Lemma 4.2.** Let $\Omega \in M_n(F)$ be orthogonal, and suppose that $\det(\Omega + I_n) \neq 0$. Then $\det \Omega = +1$, and there is a unique skew-symmetric $S \in M_n(F)$ such that $\det(I_n \pm S) \neq 0$ and $\Omega = (I_n - S)^{-1}(I_n + S) = (I_n + S)(I_n - S)^{-1}$.

**Remark.** When $F$ has characteristic 0 this is the basis of “Cayley’s transformation”.

**Lemma 4.3.** Let $\Omega \in M_n(F)$ be orthogonal, and let $\mathbb{E}_n$ be the set of all diagonal $E$ in $M_n(F)$ with each (diagonal) entry equal to $\pm 1$. Then, for at least one $E \in \mathbb{E}_n$, there is a skew-symmetric $S \in M_n(F)$ such that $\det(I_n \pm S) \neq 0$ and $\Omega = (I_n - S)^{-1}(I_n + S) = (I_n + S)(I_n - S)^{-1}$. Moreover, $S$ is uniquely determined by $E$.

**Proof.** A simple induction on $n$ shows that, given $A \in M_n(F)$, there is at least one $E \in \mathbb{E}_n$ such that $\det(A + E) \neq 0$. In particular, there is an $E \in \mathbb{E}_n$ such that $\det(\Omega + E) \neq 0$. Then $\det(E \Omega + I_n) \neq 0$, while $E \Omega$ is orthogonal. The lemma now follows from Lemma 4.2.

We are now in a position to define generic orthogonal matrices over $F$. Let $\Sigma_n$ be the generic $n \times n$ skew-symmetric matrix over $F$, and let $E \in \mathbb{E}_n$. We put $\Omega(E, n) = E(I_n + \Sigma_n)(I_n - \Sigma_n)^{-1}$; it is clearly well-defined since $\det(I_n - \Sigma_n)$ specialises to 1 if $\Sigma_n$ is specialised to 0; the $\Omega(E, n)$ ($E \in \mathbb{E}_n$) are called generic $n \times n$ orthogonal matrices over $F$; our aim is to study the Galois group of $\det(xI_n - \Omega(E, n))$ over $F_n$ of Section 2. To determine this group we need two more simple lemmas.

**Lemma 4.4.** For every $E \in \mathbb{E}_n$ we have

(i) $\text{rank}(\Omega(E, n) + I_n) = n - \frac{1}{2}(1 - \det E)$;

(ii) $\text{rank}(\Omega(E, n) - I_n) = n - \frac{1}{2}(1 - \det(-E))$. 

LEMMA 4.5. Let \( E \in \mathbb{E}_n \), and let \( \det E = 1 \). Then there is a unique skew-symmetric \( S \) in \( M_n(F_n) \) such that \( \Omega(E, n) = E(I_n + \Sigma_n)(I_n - \Sigma_n) = (I_n + S)(I_n - S) \), and there is an \( F \)-automorphism of \( F_n \) sending \( \Sigma_n \) to \( S \).

Proof. By Lemma 4.5, \( \mathrm{rank} \ (\Omega(E, n) + I_n) = n \). Hence, by Lemma 4.4, \( \Omega(E, n) = (I_n + S)(I_n - S)^{-1} = (I_n - S)^{-1}(I_n + S) \), where \( S \) is unique (and in fact \( S = \Psi(\Sigma_n) \) and \( \Sigma_n = \Psi(S) \), where \( \Psi(X) = \{E(U_n + X) + X - I_n\}^{-1}(E(I_n + X) + I_n - X) \) for all suitable \( X \in M_n(F_n) \). Hence \( F_n \) coincides with \( F \) (entries of \( S \)), the superdiagonal entries of \( S \) are algebraically independent over \( F \), and there is an \( F \)-automorphism of \( F_n \) sending \( \Sigma_n \) to \( S \).

We are now in a position to determine the Galois group of \( \mathrm{det}(xI_n - \Omega(E, n)) \) over \( F_n \). We assume from now onwards that \( F \) has characteristic 0. Let \( \Gamma_n(F) \), \( f_n \) be as in Section 2 (for \( n \geq 1 \)), with \( \Gamma_0(F) \) defined to be the trivial group. We show that the Galois group under discussion can be expressed in terms of \( \Gamma_n(F) \) (for which Theorem 1 furnishes an explicit description).

THEOREM 2. Let \( u(E, n, x) = \det(xI_n - \Omega(E, n)) \in F_n[x] \). Then \( u(E, n, x) \) has \( n \) distinct zeros. Moreover, if \( H(E, n, F) = \mathrm{Gal} u(E, n, x)/F_n \), then

\[
H(E, n, F) \cong \begin{cases} \Gamma_{n-1}(F), & \text{provided } n \text{ is even and } \det E = -1, \\ \Gamma_n(F), & \text{otherwise.} \end{cases}
\]

Proof. First suppose that \( \det E = 1 \). Using Lemma 4.5 we have

\[
u(E, n, x) = \det(xI_n - (I_n + S)(I_n - S)^{-1}),
\]

where \( S \) is the image of \( \Sigma_n \) under some \( F \)-automorphism of \( F_n \). Hence it suffices to assume that \( E = I_n \) and \( S = \Sigma_n \). We have

\[
u(I, n, x) = \det(xI_n - (I_n + \Sigma_n)(I_n - \Sigma_n)^{-1})
\]

\[
= \det(I_n - \Sigma_n)^{-1} \det((x-1)I_n - (x+1)\Sigma_n) = \det(I_n - \Sigma_n)^{-1}(1+x)^{f_n}\left(\frac{x-1}{x+1}\right).
\]

This shows that \( u(E, n, x) \) has \( n \) distinct zeros when \( \det E = 1 \), and that \( H(E, n, F) \equiv \Gamma_n(F) \), as required in (4.2).

We suppose that \( \det E = -1 \). If \( n = 0 \), then \( k = l = 1 \), \( t = 0 \) in Lemma 4.1 (with \( n = 2 \) and \( \Omega = \Omega(E, 2) \)). Hence \( u(E, 2, x) = x^2 - 1 \) and \( H(E, 2, F) \) is trivial. If \( n \geq 1 \), then \( E = ((-1) \oplus I_{2n+1})D \), where \( D \in \mathbb{E}_{2n+2} \) and \( \det D = 1 \). Applying Lemma 4.5 with \( D \) in place of \( E \), we see that the first argument will yield (4.1) for all \( E \in \mathbb{E}_{2n+2} \) with \( \det E = -1 \), once it is proved with \( E = E_0 = ((-1) \oplus I_{2n+1}) \).

Applying Lemmas 4.1 and 4.4 with \( \Omega = \Omega(E_0, 2n + 2) \) we have \( k = l = 1 \), \( t = n \), and
We specialise \( u(E_0, 2n+2, x) \) into 
\[
(x - 1)\det(l_{2n+1} - \Sigma_{2n+1})^{-1}(1 + x)^{2n+1}f_{2n+1}\left(\frac{x - 1}{1 + x}\right),
\]
which has 2n + 2 distinct zeros. It also has Galois group \( S_n[S_2] \) over \( F_{2n+1} \), by Theorem 1(ii). It follows that \( v(x) \) has 2n distinct zeros. Hence \( w(x) \) of Lemma 4.1 has \( n \) distinct zeros, \( w(x^2) \) has 2n distinct zeros, and \( \text{Gal} w(x^2)/F_{2n+2} \) can be injected in \( S_n[S_2] \), by Lemma 1.4. But we have just seen that some specialisation of \( v(x) \) has Galois group \( S_n[S_2] \) and it follows immediately that \( \text{Gal} v(x)/F_{2n+2} \equiv S_n[S_2] \equiv \Gamma_n(F) \). The theorem is completely proved.

5. Applications to CM fields. In this section \( F \) always denotes a TR field, in the sense of Section 1. Let \( k \in \mathbb{N} \); we choose \( n(1), \ldots, n(k) \in \mathbb{N} \), each \( \geq 2 \), and put 
\[
n = \sum_{i=k} n(i).\]
We choose a generic \( \Sigma_n \) over \( C \), specialising it to the form \( \Sigma^* = \bigoplus_{i \in k} \Sigma_n(i) \) (in disjoint sets of indeterminates). We propose to calculate \( G = \text{Gal}(\det(x\Sigma - \Sigma^*)/F_n) \) and \( \hat{G} = \text{Gal}(\det(x\Sigma - \Sigma^*)/F_n(V^\perp)) \), with \( F_n \) as in Section 2. Let \( A = \{i; 1 \leq i \leq k, n(i) \notin 2 + 4\mathbb{Z}\} \) and \( B = \{i; 1 \leq i \leq k, i \notin A\} \). We write \( \Sigma^*_A = \bigoplus_{i \in A} \Sigma_n(i) \), and \( \hat{G}_A \) (resp. \( \hat{G}_B \)) for the Galois group of \( \det(x\Sigma - \Sigma^*_A) \) over \( F_n \) (resp. \( F_n(V^\perp) \)), with analogous definitions for \( G_B \) (resp. \( \hat{G}_B \)). By Theorems 1–3 it is clear that \( G = \hat{G}_A \times \hat{G}_B \) and \( G_A \equiv \hat{G}_A \times G_B \), since the splitting field of \( \det(x\Sigma - \Sigma^*_A) \) over \( F_n \) cannot contain \( V^\perp \). Moreover, \( \hat{G}_C \equiv \prod_{i \in C} \text{Gal}(\det(x\Sigma - \Sigma_n(i))/F_n(V^\perp)) \) whenever \( C \subseteq \{1, \ldots, k\} \); thus the structure of \( \hat{G} \) is clear from Theorems 1–3. It only remains to calculate \( \hat{G}_B \); clearly \( \hat{G}_B = \{1\} \) if \( B = \emptyset \), so that we can ignore this case.

Let \( Z \) be the splitting field of \( \det(x\Sigma - \Sigma^*_B) \) over \( F_n \), where \( B \neq \emptyset \). Then, by Theorem 1(i), \( F_n(V^\perp) \subseteq Z \). It follows that \( (G_B : \hat{G}_B) = 2 \). We assert that \( G_B \equiv \hat{G}_B \times C_2 \). (\( C_2 \) cyclic of order 2).

To prove this, for each \( i \in B \), let \( \pm \alpha_{1(i)}, \ldots, \pm \alpha_{n(i)}(i) \) be the zeros of \( \det(x\Sigma - \Sigma_n(i)) \) (cf. Lemma 1.4) and \( E_i \) be the field \( F_n(\alpha_{1(i)}, \ldots, \alpha_{n(i)}(i)) \) so that, by Lemma 2.2, \( \det(x\Sigma - \Sigma_n(i)) \) has splitting field \( E_i(V^\perp) \). Define \( E \) to be the compositum of the \( E_i \), \( i \in B \). Then \( Z = E(V^\perp) \) and 
\[
\text{Gal} Z/E \equiv \text{Gal} F_n(V^\perp)/F_n \equiv C_2.\]
Hence \( G_B \) is the split extension of \( \text{Gal}(Z/F_n(V^\perp)) \) by \( C_2 \), as required.

We are now in a position to generate a large class of CM fields, Galois over \( F \), with Galois group \( G \) (as above). For, putting \( t = \sum_{i=k} \frac{1}{2}n(i)\{n(i) - 1\} \), and, applying Hilbert’s irreducibility theorem [8, Ch. 9], there is a Hilbert set \( \mathcal{H} \) in \( F' \) such that, when the entries of \( \Sigma^* \) (suitably ordered) are specialised into \( \mathcal{H} \), the resulting specialised matrix \( \Sigma^{**} \) satisfies \( \text{Gal}(\det(x\Sigma - \Sigma^{**}))/F \equiv G \). It is clear from the construction that this procedure yields an infinite number of distinct CM fields, since we can argue as follows. Choose a \( \Sigma^{**} \) over \( F \) such that \( \text{Gal}(\det(x\Sigma - \Sigma^{**}))/F \equiv G \). Now choose a \( \Sigma^{***} \) over \( F \) such that \( \text{Gal}(\det(x\Sigma - \Sigma^{***}))/Z_1 \equiv G \), where \( Z_1 \) is the splitting field of \( \det(x\Sigma - \Sigma^{***}) \) over \( F \). If \( Z_2 \) is the splitting field of \( \det(x\Sigma - \Sigma^{***}) \) over \( Z_1 \), we choose a \( \Sigma^{**} \) over \( F \) such that \( \text{Gal}(\det(x\Sigma - \Sigma^{**}))/Z_2 \equiv G \), and repeat this process indefinitely. The splitting fields \( W_i \) of \( \det(x\Sigma - \Sigma^{***}) \) over \( F \) are pairwise linearly disjoint over \( F(V^\perp) \), and this gives the
desired result. (Alternatively, we could obtain this on replacing $k$ by $Nk$ ($N$ arbitrarily large in $\mathbb{N}$), and making appropriate specialisations of $\Sigma_{NK}$).

In principle, the same type of construction could be applied with generic orthogonal matrices in place of $\Sigma_n$; we leave the details to the reader as the results are ultimately equivalent to those obtained from $\Sigma_n$.

6. Further remarks. Because of its wholly elementary nature and of the interest of the underlying group theory, there is merit in sketching the original direct inductive proof of Theorem 1.

In the main it suffices to consider the even case. By specialising $\Sigma_{2n+2}$ as

$$\Sigma_{2n+2} \mapsto \left( \begin{array}{c|c} \Sigma_2 & O \\ \hline O & \Sigma_{2n} \end{array} \right) = \Sigma_2 \oplus \Sigma_{2n}$$

(in disjoint sets of variables), we see that $\Gamma_{2n+2}(F)$ contains a copy of $\Gamma_2(F) \times \Gamma_{2n}(F) \cong \Gamma_{2n}(F)$.

To begin with, the above inclusion can be harnessed with the classical theorem [2, Section 161] that, for $n \neq 6$, a transitive subgroup of $S_n$ containing a copy of $S_{n-1}$ must indeed be $S_n$, to prove by induction that $G_{2n}(F) \cong S_n$. (As for the exceptional case, $G_{12}(F) \cong S_6$ since, in addition, obvious alternative specialisations yield copies of $S_4 \times S_2$ and $S_3 \times S_3$ in $G_{12}(F)$).

The remaining claims of Theorem 1 (even case) can similarly be derived by means of Lemma 2.1 applied to $g_{2n}(x)$. Clearly, if condition (iii) is valid for $g_{2n}$, then the Galois group $H = \text{Gal}(g_{2n}(x^2)/E)$ referred to there is not “very small” (i.e. in $C_2$) and so, by induction, (iii) also holds for $g_{2n+2}(x)$. To get the induction started, values of $n \leq 4$ require more detailed information on $H$ obtained from further specialisations.

Finally, Theorem 1 for odd integers, can be deduced as follows. By (2.1) and Corollary 3.1A(ii), $\Gamma_{2n+1}(F)$ can be injected into, $S_{2n}$ but not $A_{2n}$, while specialising $\Sigma_{2n+1}$ as $(0) \oplus \Sigma_{2n}$ yields $\Gamma_{2n}(F)$ as a subgroup.

We conclude with a question raised in conversation with A. W. Chatters (Bristol). Suppose that $K = \mathbb{Q}(\lambda)$ is a CM-field (as in Corollary 1.3A), of absolute degree $2n$, say. We know from Corollary 1.3B that some skew-symmetric rational matrix $S$ possesses $\lambda$ as an eigenvalue. How small (in terms of $n$) can $S$ be, i.e. how few rows can $S$ have? We note that, in this sense, Krakowski’s method is not efficient, yielding an $S$ with about $9^n$ rows. By comparison, for a TR-field $F = \mathbb{Q}(\theta)$ of absolute degree $n$, we deduce from Bender [1] that $\theta$ is an eigenvalue of a symmetric rational matrix $A$ with $n$ rows ($n$ odd) or $n + 1$ rows ($n$ even).

In fact, we can employ Bender’s result in our situation in which $K$ is the CM-field $\mathbb{Q}(\lambda)$ (as above). Let $\theta = \lambda \sqrt{-1}$, so that $F = \mathbb{Q}(\theta)$ is a TR field of absolute degree $n(\sqrt{-1} \in K)$ or $2n(\sqrt{-1} \notin K)$. It tells us that there is a rational symmetric matrix with $m$ rows and eigenvalue $\theta$ with

$$m = \begin{cases} n, & \text{if } n \text{ is odd and } \sqrt{-1} \in K, \\ n + 1, & \text{if } n \text{ is even and } \sqrt{-1} \in K, \\ 2n + 1, & \text{if } \sqrt{-1} \notin K. \end{cases}$$
It follows that \( S = A \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \) (tensor product) is a rational skew-symmetric matrix with eigenvalue \( \lambda \) and \( p = 2m \) rows. Here, in the most favourable case (when \( n \) is odd and \( \sqrt{-1} \in K \)), \( p = 2n = \text{deg} K \), while, in the worst case (when \( \sqrt{-1} \notin K \)), \( p = 4n + 2 \). We suspect that the general upper bound \( p \leq 4n + 2 \) is not best possible and leave its improvement as an open problem.

REFERENCES