An explicit integral polynomial whose splitting field has Galois group $W(E_8)$


<http://jtnb.cedram.org/item?id=JTNB_2008__20_3_761_0>
An explicit integral polynomial whose splitting field has Galois group $W(E_8)$

par Florent JOUVE, Emmanuel KOWALSKI et David ZYWINA

Résumé. En utilisant le principe selon lequel le polynôme caractéristique de matrices obtenues comme éléments d’un groupe réductif $G$ sur $\mathbb{Q}$ a typiquement un corps de décomposition dont le groupe de Galois est le groupe de Weyl de $G$, nous construisons un polynôme unitaire explicite de degré 240, à coefficients entiers, dont le corps de décomposition a pour groupe de Galois le groupe de Weyl du groupe exceptionnel de type $E_8$.

Abstract. Using the principle that characteristic polynomials of matrices obtained from elements of a reductive group $G$ over $\mathbb{Q}$ typically have splitting field with Galois group isomorphic to the Weyl group of $G$, we construct an explicit monic integral polynomial of degree 240 whose splitting field has Galois group the Weyl group of the exceptional group of type $E_8$.

1. Introduction

The goal of this paper is to give a concrete explicit example of a polynomial $P \in \mathbb{Z}[T]$ such that the Galois group of the splitting field of $P$ is isomorphic to the group $W(E_8)$, the Weyl group of the exceptional algebraic group $E_8$ (which is also, in Atlas notation [2, p. 85–87], the group $2 \cdot O^+_8(2) \cdot 2$, where $O^+_8(2)$ is the orthogonal group of the unique non-singular split quadratic form of rank 8 over $\mathbb{F}_2$; see Remark 2.5 below for more background on this group). It was motivated by the construction of such extensions by Várilly-Alvarado and Zywina [24] using the Galois action on Mordell-Weil lattices of some elliptic curves over $\mathbb{Q}(t)$ which are isomorphic to the root lattice $E_8$ (this leads in principle to infinitely many such polynomials, though they are not necessarily easy to write down), itself based on ideas of Shioda. The existence of such polynomials was already known from the solution of the inverse Galois problem for Weyl groups (see the
survey of Shioda [20], or the paper [16] of Nuzhin, as well as [3, §2.2] or [25, Th. 2]).

**Theorem 1.1.** Let $P \in \mathbb{Z}[T]$ be the monic polynomial of degree 240 given by $P(T) = T^{120}Q(T + T^{-1})$, where $Q$ is the monic polynomial of degree 120 described by Table 1 in Appendix B. Then the Galois group of the splitting field of $P$ over $\mathbb{Q}$ is isomorphic to $W(E_8)$.

In fact, as we will explain in Proposition 4.1, it is possible to generalize the construction to obtain infinitely many (linearly disjoint) examples. In another direction, although we used the Magma software [5] to construct $P$ (and partly to prove Theorem 1.1), we explain in Appendix A how it could be recovered (in principle) “by hand”, and in particular that it is quite simple from the point of view of the structure of reductive algebraic groups.

The basis of the construction is the following principle: if $G/\mathbb{Q}$ is a (split) connected reductive algebraic group given as a $\mathbb{Q}$-subgroup of $GL(r)$ for some $r \geq 1$, via an injective $\mathbb{Q}$-homomorphism

$$G \overset{\ i \ \longrightarrow \ GL(r),}$$

and if $g \in G(\mathbb{Q})$ is a “random” element, then the Galois group of the splitting field of $\det(T - i(g))$ (i.e., the characteristic polynomial of $g$, seen as a matrix through $i$) is typically isomorphic to the Weyl group $W(G)$ of $G$. Note that such a principle is in fact pretty close to some of the early methods used for the study of Lie groups (a “retour aux sources”), as explained in the historical notes in [6]; in particular, a long time before the Weyl group was defined in the current manner, É. Cartan (see [8], in particular pages 50 and following for the case of $E_8$) determined the Galois group of $\det(T - \text{ad}(X))$ for a “general” $X$ in a simple Lie algebra over $\mathbb{C}$ (compare also with [20, §8.4, last paragraph], where the same characteristic polynomial for $E_8$ is mentioned and related to the Mordell-Weil lattices; note those polynomials are not the same as the ones considered here, e.g., their roots satisfy many additive relations, whereas ours satisfy multiplicative relations, as explained in Remark 2.4).

This principle depends on stating what “random” means (and then on proving the statement!). This was done in [13, §7] for elements obtained by random walks

$$g = \xi_1 \cdots \xi_k$$

in either $SL(r, \mathbb{Z})$ ($r \geq 2$), so that $G = SL(r)$, and $i$ is the tautological embedding in $GL(r))$ or $Sp(2g, \mathbb{Z})$ ($g \geq 1$, so that $G = Sp(2g)$ and $i$ corresponds to the standard embedding in $GL(2g)$: when $k$ is large, the steps of the walk $\xi_j$ being independently chosen uniformly at random among the elements of a fixed finite generating set of $G(\mathbb{Z})$, the probability that
the splitting field of $\det(T - g)$ has Galois group different from $W(\mathbb{G})$ is exponentially small in terms of $k$.

We do not take up the full details of this approach here for the exceptional group $E_8/\mathbb{Q}$, though we will come back to this at a later time in greater generality. What we do is follow the principle to produce a candidate polynomial. We know that there is an a-priori embedding of its Galois group in $W(E_8)$, and it turns out (which we didn’t quite expect) that it is possible to check that it is not a proper subgroup of $W(E_8)$.

Remark 1.2. In order to allow easy checking, we have put on the web at the urls

\begin{itemize}
  \item www.math.ethz.ch/~kowalski/e8pol.gp
  \item www.math.ethz.ch/~kowalski/e8pol.mgm
\end{itemize}

two short files containing definitions of the polynomial above in GP/Pari and Magma, respectively. Loading either will define the variable \texttt{pol} to be the polynomial of the proposition.

By construction, $P$ is self-reciprocal (so all its roots are units). Its splitting field turns out to be totally real, and is a quadratic extension of the splitting field of $Q$. The discriminant of $P$ is of size about $10^{14952}$, and it is divisible by

$$2^{3640} \cdot 3^{300} \cdot 5^{30} \cdot 73^{28} \cdot 109^2 \cdot 113^4 \cdot 131^{28} \cdot 419^{28} \cdot 1033^4 \cdot 1103^{57} \cdot 3307^{28} \cdot 4649^4 \cdot 11467^4 \cdot 629569^4 \cdot 87087881^4 \cdot 508141873^2 \cdot 8321263487^{28} \cdot 58276913161^2 \cdot 126454995466730813^4 \cdot 202992518210175167^{57} \cdot 164435771172314887333^2 \cdot 17520591390337947024593065297057^2,$$

with the cofactor being a square. Clever use of Pari/GP [17] (as explained by K. Belabas) shows that the discriminant of the number field of degree 240 determined by $P$ (i.e., $\mathbb{Q}[T]/(P)$, not its splitting field) is

$$1103^{57} \cdot 202992518210175167^{57} \approx 8.9777 \cdot 10^{1159}.$$
Notation. As usual, $|X|$ denotes the cardinality of a set. For any finite set $R$, $\mathfrak{S}_R$ is the group of all permutations of $R$, with $\mathfrak{S}_n$, $n \geq 1$, being the case $R = \{1, \ldots, n\}$. We denote by $F_q$ a field with $q$ elements.

Acknowledgement. Many thanks are due to K. Belabas for help with performing numerical computations (discriminant, basis of the ring of integers, \texttt{polred}) with the polynomial $P$, etc, and for explanations of the corresponding functions and algorithms in \texttt{Pari/GP}; also, thanks to S. Garibaldi for explaining why the computation with \texttt{GAP} coincides with the one with \texttt{Magma} (see Appendix A).

2. A priori upper bound on the Galois group for $E_8$

Let $E_8/\mathbb{Q}$ be the split group of type $E_8$; it is a simple algebraic group over $\mathbb{Q}$ of rank 8 and dimension 248. For information on $E_8$ as a Lie group, we can refer to [1]; for $E_8$ as algebraic group, including proof of existence, abstract presentation, etc, see, e.g., [21, Ch. 9, Ch. 10, §17.5]. In Appendix A we also mention a few concrete details.

Contrary to classical groups such as $SL(n)$ or $Sp(2g)$ or orthogonal groups, which come with an “obvious” embedding in a group of matrices of size comparable with the rank (which is $n-1$ or $g$, respectively), the smallest faithful representation of $E_8$ is of dimension $248 = \dim E_8$. More precisely, this is the adjoint representation

$$\text{Ad} : E_8 \rightarrow GL(e_8)$$

where $e_8$ is the Lie algebra of $E_8$, the tangent space at the identity element with the Lie bracket arising from differentiation of commutators. This representation is defined over $\mathbb{Q}$ and given by

$$g \mapsto T_e(h \mapsto ghg^{-1}),$$

the differential at the identity element of the conjugation by $g$, see, e.g, [4, I.3.13]. The fact that $\text{Ad}$ is injective is because the center of $E_8$ is trivial (in general, the kernel of the adjoint representation is the center, in characteristic 0 at least).

Fix a maximal torus $T$ of $E_8$ that is defined over $\mathbb{Q}$ (but not necessarily split, so that $T$ is not necessarily isomorphic to $G_m^8$ over $\mathbb{Q}$, but only over some finite extension field; in fact, the case of interest will be when this field is large). Let $X(T) \simeq \mathbb{Z}'$ be the group of characters $\alpha : T \rightarrow G_m$ (not necessarily defined over $\mathbb{Q}$). For each $\alpha \in X(T)$, let

$$g_\alpha = \{X \in e_8 \mid \text{Ad}(t) \cdot X = \alpha(t)X, \text{ for all } t \in T\}$$

be the weight space for $\alpha$ in the adjoint representation. Let $R(T, E_8)$ be the set of non-trivial $\alpha \in X(T)$ with $g_\alpha \neq 0$; these are called the roots of $E_8$ with respect to $T$. 
Explicit $W(E_8)$ polynomial

Remark 2.1. It is customary, to view $X(T)$ as an additive group. In particular, for $\alpha \in R$, the inverse character $\alpha^{-1}$ is denoted $-\alpha$, and $\alpha_1 + \alpha_2$ is the character $t \mapsto \alpha_1(t)\alpha_2(t)$, etc.

The set $R(T, E_8)$ is an abstract root system in the space $V = X(T) \otimes \mathbb{Z}R$; cf. [6, Ch. 6] for definitions.

The structure theory of reductive groups (see, e.g., [4, 13.18]) shows that the space $g_\alpha$ is one dimensional for each root $\alpha \in R(T, E_8)$, and gives a direct sum decomposition

$$e_8 = t \oplus \bigoplus_{\alpha \in R(T, E_8)} g_\alpha,$$

where $t$ is the Lie algebra of $T$.

From this decomposition, we recover the fact that $|R(T, E_8)| = \dim E_8 - \dim T = 248 - 8 = 240$. The absolute Galois group of $\mathbb{Q}$ acts naturally on $X(T)$: for any $\alpha \in X(T)$ and $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma(\alpha)$ is the unique character of $T$ such that

$$\sigma(\alpha(t)) = (\sigma(\alpha))(\sigma(t))$$

for all $t \in T$. The set of roots $R(T, E_8)$ is stable under this action.

Finally, we recall that the Weyl group of $E_8$ with respect to $T$ is the finite quotient group $W(T, E_8) = N(T)/T$, where $N(T)$ is the normalizer of $T$ in $E_8$. Since all maximal tori of a connected linear algebraic group are conjugate (see, e.g., [21, Th. 6.4.1]), the Weyl group $W(T, E_8)$ is independent of the torus $T$ up to isomorphism. We will write $W(E_8)$ for this abstract group when the choice of torus is unimportant.

The group $W(T, E_8)$ acts on the roots by conjugation: for $w \in N(T)$, $\alpha \in R(T, E_8)$, let

$$(w \cdot \alpha)(t) = \alpha(w^{-1}tw),$$

which obviously depends only on the image of $w$ in $W(T, E_8)$. This action is faithful (for instance, because $R(T, E_8)$ generates the character group $X(T)$, and $T$ is its own centralizer, see [4, 13.17]).

We can now state the main result of this section.

**Proposition 2.2.** Fix a semisimple element $g \in E_8(\mathbb{Q})$, and let $T$ be any maximal torus of $E_8$ that contains $g$.

1. We have the factorization

$$\det(T - \text{Ad}(g)) = (T - 1)^8 \prod_{\alpha \in R(T, E_8)} (T - \alpha(g)).$$

---

1 It is precisely because the values of the roots $\alpha$ are the eigenvalues of matrices arising from the adjoint representation that the terminology root, which may seem confusing today, was introduced in the historical development of the theory of Lie and algebraic groups.
Define the polynomial \( P = \det(T - \text{Ad}(g))/(T - 1)^8 \in \mathbb{Q}[T] \), and let \( Z \subset \mathbb{Q} \) be the set of roots of \( P \). Assume that \( P \) is separable. Then the map

\[
\beta: \begin{cases} 
R(T, E_8) & \rightarrow Z \\
\alpha & \mapsto \alpha(g)
\end{cases}
\]

is a bijection which respects the respective \( \text{Gal}(\mathbb{Q}/\mathbb{Q}) \)-actions.

Let \( K \) be the splitting field of \( P \), i.e., the extension of \( \mathbb{Q} \) generated by \( Z \). Assume that \( P \) is separable. Then the map (2.3)

\[
\phi_g: \text{Gal}(K/\mathbb{Q}) \hookrightarrow W(T, E_8)
\]

such that for all \( \sigma \in \text{Gal}(K/\mathbb{Q}) \) and \( \alpha \in R(T, E_8) \), we have

\[
\phi_g(\sigma) \cdot \alpha = \sigma(\alpha).
\]

**Proof.** Since \( g \) is semisimple, it does lie in a maximal torus \( T \) of \( G \) (see, e.g., [21, Th. 6.4.5 (ii)]), and we fix one such torus. The operator \( \text{Ad}(g) \) acts as the identity on \( t \) (since conjugation by \( g \) is trivial on \( T \)) and as multiplication by \( \alpha(g) \) on each \( g_{\alpha} \), for \( \alpha \in R(T, E_8) \). Therefore from (2.1), we deduce that

\[
\det(T - \text{Ad}(g)) = (T - 1)^8 \prod_{\alpha \in R(T, E_8)} (T - \alpha(g)).
\]

Thus \( P \), as defined in the statement of the proposition, is indeed a polynomial.

Now we assume that \( P \) is separable. We first note that \( \alpha(g) \neq 1 \) for any \( \alpha \in R(T, E_8) \). To see this, we claim that for any \( \alpha \), we can find another root \( \alpha' \) such that \( \alpha'' = \alpha + \alpha' \) (in additive notation) is also in \( R(T, E_8) \). Then, since \( \alpha'(g) \neq \alpha''(g) \) by assumption, we obtain \( \alpha(g) \neq 1 \) as desired. From this, in turn, we deduce (see, e.g., [4, IV.12.2]) that \( g \) is regular and hence is contained in a *unique* maximal torus \( T \), which is necessarily defined over \( \mathbb{Q} \).

Now, to check the claim, one can look at the description of the root system in Remark 2.5, but this is in fact a general property of any root system \( R \) with Dynkin diagram containing no connected component which is a single point: given \( \alpha \in R \), one first chooses a system \( \Delta \) of simple roots such that \( \alpha \in \Delta \), and take \( \alpha' \) to be one of the simple roots which are not perpendicular to \( \alpha \) (which exists because of the assumption on the root system; in other words, \( \alpha \) and \( \alpha' \) are connected in the Dynkin diagram of the simple roots; e.g., for \( E_8 \), if \( \alpha \) corresponds to the vertex labelled 1 of the Dynkin diagram (2.5), one can take \( \alpha' \) the root labelled 3, etc). Then \( (\alpha, \alpha') \) are two simple roots for an irreducible root system of rank 2 contained in \( R \), and one can check that \( \alpha + \alpha' \in R \) using the classification of those (see, e.g., [21, 9.1.1]). For \( E_8 \) (or more generally if the Dynkin diagram of \( R \) has no multiple bond), one can also simply notice that \( s_{\alpha}(\alpha') = \alpha' + \alpha \), where \( s_{\alpha} \) is the reflection associated with \( \alpha \) (see, e.g., [21, 10.2.2]).
Coming back to \( P \), from the above factorization, we find that the map \( \beta \) is well-defined and surjective, and since \(|R(T, E_8)| = 240 = |Z|\), it is therefore bijective. For each \( \alpha \in R(T, E_8) \) and \( \sigma \in \text{Gal}(\overline{Q}/Q) \), we have

\[
\beta(\sigma(\alpha)) = \sigma(\alpha)(g) = \sigma(\alpha)(\sigma(g)) = \sigma(\alpha(g)),
\]

since \( g \in E_8(Q) \). The Galois group \( \text{Gal}(K/Q) \) acts faithfully on \( Z \) (the permutation action on the roots), so using \( \beta \), we find that \( \text{Gal}(K/Q) \) acts faithfully on \( R(T, E_8) \), and this induces an injective group homomorphism

\[
\phi_g : \text{Gal}(K/Q) \hookrightarrow \mathfrak{S}_{R(T,E_8)}.
\]

Since \( W(T, E_8) \) acts faithfully on \( R(T, E_8) \), we may naturally view \( W(T, E_8) \) as a subgroup of \( \mathfrak{S}_{R(T,E_8)} \). To conclude, it is thus sufficient to show that the image of \( \phi_g \) lies in this subgroup, or in other words, that for every \( \sigma \in \text{Gal}(K/Q) \), there exists \( w_\sigma \in W(T, E_8) \) such that

\[
\sigma(\alpha) = w_\sigma \cdot \alpha, \quad \text{for all } \alpha \in R(T, E_8).
\]

Fix a split torus \( T_0 \) of \( E_8 \) that is defined over \( Q \), which exists since we assumed that our group \( E_8 \) is split over \( Q \). Note that \( T_0 \) is split over \( K \) and that \( T \) is also. Indeed, to check this, it is equivalent to check that the action of \( \text{Gal}(\overline{Q}/K) \) on the character group of \( T \) is trivial (see, e.g., [21, Prop. 13.2.2]). For this, it suffices to show that the roots are invariant, since they generate \( X(T) \) (see, e.g., [21, 8.1.11], noting that \( E_8 \) is of adjoint type, or the description of the root system in Remark 2.5). But for any \( \sigma \in \text{Gal}(\overline{Q}/K) \), we have

\[
\beta(\sigma(\alpha)) = \sigma(\alpha)(g) = \sigma(\alpha)(\sigma(g)) = \sigma(\alpha(g)) = \alpha(g) = \beta(\alpha),
\]

and \( \sigma(\alpha) = \alpha \) follows from the injectivity of the map \( \beta \).

Now the fact that \( T \) and \( T_0 \) are both \( K \)-split implies that there exists \( x \in E_8(K) \) such that \( T = xT_0x^{-1} \), as proved, e.g., in [21, Th. 15.2.6]. Consider then any \( \sigma \in \text{Gal}(K/Q) \), and note that \( \sigma(x) \) makes sense since \( x \in E_8(K) \). Since both \( T \) and \( T_0 \) are defined over \( Q \), we have \( T = \sigma(x)T_0(\sigma(x))^{-1} \) and hence \( \sigma(x)x^{-1} \in N(T) \). Let \( w_\sigma \) be the element of \( W(T, E_8) \) represented by \( \sigma(x)x^{-1} \). We now claim that \( \sigma(\alpha) = w_\sigma \cdot \alpha \), for all \( \alpha \in R(T, E_8) \), which will finish the proof.

To see this, note that the Galois group \( \text{Gal}(K/Q) \) acts trivially on \( X(T_0) \) (because \( T_0 \) is split), and that we have an isomorphism

\[
\gamma : \begin{cases} T_0 & \rightarrow & T \\ t & \mapsto & xt(x^{-1}) \end{cases}
\]

which is defined over \( K \). For any \( \alpha \in R(T, E_8) \), we have

\[
\sigma(\alpha) = \sigma(\alpha \circ \gamma \circ \gamma^{-1}) = (\alpha \circ \gamma) \circ \sigma(\gamma)^{-1},
\]

and then, for all \( t \in T \), we obtain

\[
(\sigma(\alpha))(t) = \alpha(x\sigma(x)^{-1}t\sigma(x)x^{-1}) = \alpha((\sigma(x)x^{-1})^{-1}t(\sigma(x)x^{-1})),
\]

Explicit \( W(E_8) \) polynomial

767
which is the desired conclusion.

Remark 2.3. A different approach to Proposition 2.2 is sketched (for classical groups) in [13, App. E]. The one above is more direct and intrinsic, and is more amenable to generalizations, but we indicate the idea (which can be seen as more down-to-earth): given a (regular semisimple) $g \in E_8(Q)$, and a fixed split torus $T_0$, one considers the set

$$X_g = \{ t \in T_0 \mid t \text{ and } g \text{ are conjugate} \}.$$ 

This is a non-empty set because $g$ is semisimple, and one shows that the Weyl group (defined as $N(T_0)/T_0$) acts simply transitively by conjugation on $X_g$; an injection $\text{Gal}(K/Q) \to W(E_8)$ is then produced by fixing $t_0 \in X_g$ and mapping $\sigma$ to $w_{\sigma}$ such that $\sigma(t_0) = w_{\sigma}^{-1} \cdot t_0$. Another small computation then proves that the permutation of the set of zeros $Z$ obtained from a given $\sigma \in \text{Gal}(K/Q)$ is always conjugate to the permutation of $R(T_0, E_8)$ induced by $\sigma$.

Remark 2.4. Proposition 2.2 implies that the zeros of a polynomial $\det(T - \text{Ad}(g))$ satisfy many multiplicative relations; indeed, all the 240 zeros are contained in the multiplicative subgroup of $C^\times$ generated by the $\alpha(t)$ corresponding to eight simple roots $\alpha$ (see also [3] for this type of questions, and the next remark if the terminology is unfamiliar).

Remark 2.5. Here are some basic facts on $W(E_8)$ which can be useful to orient the reader. This group $W(E_8)$ is of order $696729600 = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$, and its simple Jordan-Hölder factors are $Z/2Z$, $Z/2Z$ and the simple group $D_4(F_2)$ (also sometimes denoted $PO^+_8(2)$, $D_4(2)$, $D_4^+(2)$, or $O^+_8(2)$ as in the Atlas of Finite Groups [2]), where $D_4$ is the split algebraic group of type $D_4$ of dimension 28; this composition series is essentially already computed by É. Cartan in [8, p. 50 and following], working on it as a subgroup of $S_{240}$ (a rather impressive performance). It can be presented as a Coxeter group (see [6, Chapter IV]) using eight generators $w_1, \ldots, w_8$, corresponding to a system of simple roots $\alpha_1, \ldots, \alpha_8 \in R$ (i.e., roots such that any $\alpha \in R$ can be either represented as integral combination of the $\alpha_i$ with non-negative coefficient, or its opposite $\alpha^{-1}$ can be written in this way, but not both), subject to relations

$$w_i^2 = 1 \quad (w_iw_j)^{m(i,j)} = 1, \quad 1 \leq i < j \leq 8,$$

where

$$m(i,j) = 3 \text{ if } (i,j) \in \{(1,3), (3,4), (2,4), (4,5), (5,6), (6,7), (7,8)\},$$
Explicit $W(E_8)$ polynomial

and $m(i, j) = 2$ otherwise. (This is encoded in the well-known Dynkin diagram

(2.5)

\begin{center}
\begin{tikzpicture}
\draw (0,0) -- (1,0) -- (2,0) -- (3,0) -- (4,0) -- (5,0) -- (6,0) -- (7,0) -- (8,0);
\filldraw (1,0) circle (2pt);
\filldraw (4,0) circle (2pt);
\filldraw (2,0) circle (2pt);
\end{tikzpicture}
\end{center}

where $m(i, j) = 3$ if and only if the vertices labelled $i$ and $j$ are joined by an edge.)

One can also define $W(E_8)$ as the automorphism group of the lattice $\Gamma_8 \subset \mathbb{Q}^8$ (of rank 8) generated by $(\frac{1}{2}, \ldots, \frac{1}{2})$ and the sublattice

$$\{(x_1, \ldots, x_8) \in \mathbb{Z}^8 \mid x_1 + \cdots + x_8 \equiv 0 \pmod{2}\},$$

with the standard bilinear form (see, e.g., [19, V.1.4.3] for some more discussion of this lattice, and also [1, §10], where the isomorphism $W(E_8) \simeq \text{Aut}(\Gamma_8)$ is proved; note many authors studying lattices write $E_8$ for the lattice instead of the group). In fact, in the identification of $W(T, E_8)$, for some maximal torus $T \subset E_8$, as $\text{Aut}(\Gamma_8)$, $\Gamma_8$ can be identified with the character group of $T$, and the roots $R$ are then interpreted as the 240 vectors in $\Gamma_8$ with squared-length 2, namely

$$\pm x_i \pm x_j, \quad 1 \leq i < j \leq 8,$$

$$\frac{1}{2}(\pm x_1 \pm x_2 \pm \cdots \pm x_8), \quad \text{with an even number of minus signs,}$$

the action of $W(E_8)$ on $R$ being the same as the action of the automorphism group. The lattice $\Gamma_8$ is generated by $R$, with a basis given for instance by the following eight roots

$$\frac{1}{2}(x_1 + x_2 - x_3 - x_4 - x_5 - x_6 - x_7 - x_8)$$

$$-x_2 + x_3, \quad x_2 + x_3, \quad -x_i + x_{i+1}, \quad \text{for } 3 \leq i \leq 7,$$

(which are therefore an example of system of simple roots); see, e.g., [1, p. 56].

\textbf{Remark 2.6.} See [20, §7] for explicit examples of polynomials whose splitting fields have Galois groups $W(E_6)$ and $W(E_7)$; they are much simpler, which can be expected, since $|W(E_6)| = 51840 = 2^7 \cdot 3^4 \cdot 5$ and $|W(E_7)| = 2903040 = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$. Moreover, these polynomials have degree 27, resp. 56, which is smaller than the degrees that would arise from the adjoint representations, namely $72 = 78 - 6$ and $126 = 133 - 7$ (this reflects the fact that there exist faithful representations of the groups $E_6$ and $E_7$ of simply-connected type in dimension 27 and 56).

There are very classical interpretations of the permutation representations of degree 27 and 56, $W(E_6)$ being the same as the group of automorphisms of the set of 27 lines on a smooth cubic surface, while the simple subgroup of index 2 in $W(E_7)$ is isomorphic to the group of automorphisms...
of the 28 bitangents on a smooth quartic curve (see e.g. [8, p. 43] for \(E_6\) and [8, p. 50] for \(E_7\)). The modern interpretation of these facts is related to the theory of del Pezzo surfaces (and hence to the viewpoint in [24]); for a readable account, see [15, Ch. IV].

From the (related) lattice point of view, 27 and 28 are the numbers of shortest vectors in the dual of the corresponding lattices, and the Weyl groups act by permuting them.

3. Construction of the example

The polynomial of Theorem 1.1 is constructed using Magma (version 2.13-9). We look at the split group \(E_8/\mathbb{Q}\), and the system of 16 “algebraic generators” given by Magma, which come from the Steinberg presentation of reductive algebraic groups. Precisely (see Appendix A for some more details and references), those are the generators \(x_i = x_{\alpha_i}(1), 1 \leq i \leq 8\), of the eight one-parameter unipotent root subgroups \(U_{\alpha_i}\) associated with the simple roots \(\alpha_i\) (see, e.g., [21, 8.1.1]), and the generators \(x_{8+i} = x_{-\alpha_i}(1), 1 \leq i \leq 8\), of the unipotent subgroups associated with the negative of the simple roots. The simple roots are numbered (by Magma) in the usual way described explicitly, for instance, in [6, Ch. VI, §4.10], and correspond with the vertices of the Dynkin diagram as in Remark 2.5.

We then construct an element \(g\) in \(E_8(\mathbb{Q})\) by taking the product of those sixteen generators \(x_i\) (in the order above) namely

\[ g = x_1 \cdots x_{16} = x_{\alpha_1}(1) \cdots x_{\alpha_8}(1)x_{-\alpha_1}(1) \cdots x_{-\alpha_8}(1), \]

in terms of simple root subgroups; we think of this as a very simple random walk of length 16. Then using the adjoint representation of \(E_8\), we compute the matrix \(m = \text{Ad}(g)\) (which is in fact in \(SL(248, \mathbb{Z})\); in the basis given by Magma, it is a fairly sparse matrix, with only 6661 non-zero coefficients among the \(248^2 = 61540\) entries; the maximal absolute value among the coefficients is 16).\(^2\)

The characteristic polynomial \(\det(T - m) \in \mathbb{Z}[T]\) is divisible by \((T - 1)^8\) by Proposition 2.2, and the polynomial \(P\) of Theorem 1.1 is

\[ P = \det(T - m)(T - 1)^{-8}. \]

Here are the exact Magma commands to obtain this polynomial (in a few seconds, this speed depending on fast routines for computing characteristic polynomials of big integral matrices; neither GAP nor Pari/GP are currently able to do this computation as quickly):

\[^2\text{Note that we also checked that if we construct an element of }E_8(\mathbb{Q})\text{ by taking the product of the }i\text{ first generators (in the same order as above) with }1 \leq i \leq 15,\text{ then the resulting polynomial is not irreducible.}\]
A<T>:=PolynomialRing(RationalField());
E8:=GroupOfLieType("E8",RationalField());
gen:=AlgebraicGenerators(E8);
rho:=AdjointRepresentation(E8);
g:=Identity(E8); for i in gen do g:=g*i; end for;
m:=rho(g);
pol:=CharacteristicPolynomial(m) div (T -1)^8;

Any decent software package confirms that $P$ is at least irreducible over $\mathbb{Q}$ (in particular, its zeros are distinct, as required for the second part of Proposition 2.2). Because the roots of $P$ come in inverse pairs, it is possible to write $P = T^{120}Q(T + T^{-1})$ for a unique polynomial $Q \in \mathbb{Z}[T]$, which we did to shorten a bit the description of $P$ in Theorem 1.1. The irreducibility of $P$ also implies that $g$ is semisimple: indeed, it suffices to check that $\text{Ad}(g)$ is diagonalizable, but this is clear because the minimal polynomial of $\text{Ad}(g)$ has to be $(T - 1)P$, and 1 is not a zero of $P$.³

Now we prove that the splitting field $K$ of $P$ has Galois group $G$ isomorphic to $W(E_8)$. First, according to Proposition 2.2, we know that $G$ can be identified with a subgroup of $W(E_8)$, and that this identification is made in such a way that the action of $G$ by permutation of the zeros of $P$ in $K$ corresponds to the action of $W(E_8)$ as a subgroup of $S_{240}$ by permutations of the roots of $E_8$.

This last compatibility is crucial because of the following well-known fact of algebraic number theory: if $S \in \mathbb{Z}[T]$ is an irreducible monic polynomial of degree $d$ with splitting field $F/\mathbb{Q}$, $H$ the Galois group of $F/\mathbb{Q}$ seen as permutation group of the roots of $S$ in $F$, $p$ a prime number such that $S$ factors modulo $p$ in the form

$$S \pmod{p} = S_1 \cdots S_d,$$

where $S_i$ is the product of $n_i \geq 0$ distinct monic irreducible polynomials of degree $i$ in $\mathbb{F}_p[T]$, then $H \subset S_d$ contains a permutation with cycle type consisting of $n_1$ fixed points, $n_2$ disjoint transpositions, etc, and in general $n_i$ disjoint $i$-cycles.

We apply this to $P$ and $S_{240}$, with primes $p = 7$ and $p = 11$. We find (again, any decent software package will be able to factor $P$ modulo 7 and 11) that $P \pmod{7}$ is the product of 2 distinct irreducibles of degree 4, and 29 distinct irreducibles of degree 8, whereas $P \pmod{11}$ is the product of 16 distinct irreducible polynomials of degree 15. Hence $G \subset S_{240}$ contains elements of the type

$$g_8 = c_1^{(4)} c_2^{(4)} c_3^{(8)} \cdots c_{31}^{(8)}, \quad g_{15} = d_1^{(15)} \cdots d_{16}^{(15)}$$

where the $c_i^{(\ell)}$ (resp. $d_j^{(15)}$) are disjoint $\ell$-cycles (resp. disjoint 15-cycles).

³ If $g$ were not semisimple, we could also simply argue with its semisimple part, so this is not of great importance.
In both cases, Magma confirms that such conjugacy classes are unique in \( W(\mathbf{E}_8) \) (i.e., there is a single conjugacy class in \( W(\mathbf{E}_8) \) with the cycle structure of \( g_8 \) or \( g_{15} \) as permutation of \( R \)).

There are nine conjugacy classes of maximal subgroups in \( W(\mathbf{E}_8) \), which are known to Magma. Their indices in \( W(\mathbf{E}_8) \) are as follows:

\[
12096, 11200, 2025, 1575, 960, 135, 120, 2.
\]

Let \( M \) be any maximal subgroup; then Magma can also output a list of the cycle structures, in the permutation action on \( \mathcal{S}_R \cong \mathcal{S}_{240} \), of each conjugacy class of elements in \( M \) (of course, there are sometimes different conjugacy classes in a given \( M \) with the same cycle structure).

Now it turns out, by inspection, that none of the maximal subgroups of \( W(\mathbf{E}_8) \) contains elements with the two cycle structures given in (3.2), and this means that the group \( G = \text{Gal}(K/\mathbb{Q}) \) can not be a subgroup of any of them, and therefore we have \( G = W(\mathbf{E}_8) \).

More precisely, the subgroup of index 2 is unique and is the kernel of the restriction of the signature homomorphism \( \varepsilon \), which is a surjective homomorphism

\[
\varepsilon : W(\mathbf{E}_8) \hookrightarrow \mathcal{S}_{240} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z},
\]

such that \( \varepsilon(g_8) = (-1)^{31} = -1, \varepsilon(g_{15}) = 1 \). We see from this that \( G \) is not contained in \( \ker \varepsilon \), and hence the only thing to check to conclude that \( G = W(\mathbf{E}_8) \) is the fact that none of the maximal subgroups of index > 2 contains an element of the class \( g_{15} \).

This is what we deduced from Magma (but it would be interesting to have a more conceptual proof; it can also be checked in the Atlas of Finite Groups \([2]\), by reducing to the “big” simple quotient \( O_8^+(2) = (\ker \varepsilon)/(\text{center}) \), for which the maximal subgroups are listed “on paper”).

Here are the Magma commands which can be used to construct \( W(\mathbf{E}_8) \) and inspect the structure of its maximal subgroups:

```magma
W:= WeylGroup(E8); max:= MaximalSubgroups(W); for m in max do print("- - - -"); for c in ConjugacyClasses(m:subgroup) do print(CycleStructure(c[3])); end for; end for;
```

The url \url{www.math.ethz.ch/~kowalski/e8check.mgm} contains a Magma script that lists the maximal subgroups containing elements of each of the two conjugacy classes (though, as we observed, checking is only needed for \( g_{15} \)).

**Remark 3.1.** Here are some remarks about this proof, which go in the direction of making the objects and arguments more intrinsic and independent
of an a priori knowledge of the list of maximal subgroups of $W(E_8)$ (it’s not clear if it is reasonable to hope for such a proof...). First of all, the conjugacy class of order 15 is particularly symmetric, and we can also prove its uniqueness by pure thought. Indeed, it corresponds to the regular class of order 15 in $W(E_8)$, as defined by Springer [22], and Springer proved that there is at most one regular conjugacy class of a given order in the Weyl group for an irreducible root system (see [22], in particular Theorem 4.1, Proposition 4.10 and Table 3 in §5.4). Even more precisely, $g_{15}$ is the class of the square of the Coxeter elements (e.g., [6, Ch. V, §6] for the basic properties of the Coxeter element).

Finding the two classes above so easily is somewhat surprising, but it is not such amazing luck. First, the size of $g_{15}$ is $|W(E_8)|/30$ (again, this can be deduced from Springer’s work [22, Cor. 4.3, 4.4] without invoking any computer check), so by the Chebotarev density theorem, an extension $L/Q$ with Galois group $W(E_8)$ may be expected to lead to this conjugacy class for roughly three percent of the primes, which is not negligible. The class $g_8$, though less symmetric, is even less surprising from this point of view: it contains no less than $|W(E_8)|/16$ elements, and is the largest conjugacy class in $W(E_8)$ (and, as we explained, any odd conjugacy class would have done just as well for our argument).

We state formally the observation we used on subgroups containing $g_{15}$, as it may prove to be useful for later reference:

**Lemma 3.2.** Let $w_1, \ldots, w_8$ be simple reflections generating $W(E_8)$. Let $b = 1$ or 2, and let $c = w_1 \cdots w_8$ be a Coxeter element in $W(E_8)$. Then any proper subgroup of $W(E_8)$ containing an element conjugate to $c^b$ is contained in the index 2 subgroup $\ker \varepsilon$.

**Proof.** We mentioned that the case $b = 2$ is checked unenlighteningly using Magma, and then the case $b = 1$ follows since a proper subgroup containing a conjugate of $c$ contains also a conjugate of $c^2$. (Note that by [22, Prop. 4.7], if $b$ is coprime with 30, resp. 15, then $c^b$ is conjugate to $c$, resp. $c^2$, so the lemma holds in fact for any $b$ coprime with 15.) \[\square\]

**4. Infinitely many extensions**

In this section, we show that the construction of the specific polynomial $P$ also leads easily to infinitely many examples.

**Proposition 4.1.** Let $E_8/Z$ be a model of the split Chevalley group $E_8$ defined over $Z$, and let $S \subset E_8(Z)$ be a symmetric finite generating set for

---

4 There are 112 conjugacy classes altogether, which are also described explicitly by Carter in [9]; in his notation, $g_8$ is the class with $\Gamma = A''_7$ on p. 56 of loc. cit., while $g_{15}$ is the class with $\Gamma = E_8(a_5)$ on p. 58.
Then
\[
\liminf_{k \to +\infty} \frac{1}{|S|^k} \left| \{(s_1, \ldots, s_k) \in S^k \mid \text{the splitting field of} \right. \\
\det(T - \text{Ad}(s_1 \cdots s_k)) \text{ has Galois group } W(\mathbf{E}_8) \left. \right| > 0.
\]

In fact, there exist infinitely many \(g \in \mathbf{E}_8(\mathbb{Z})\) for which the splitting fields of \(\det(T - \text{Ad}(g))\) are linearly disjoint and have Galois group isomorphic to \(W(\mathbf{E}_8)\).

As explained before, one can expect a much stronger result (the left-hand side of (4.1) should be \(\geq 1 - C \exp(-ck)\) for some \(c > 0, C \geq 0\)), but checking this would involve a deeper analysis of the finite groups \(\mathbf{E}_8(\mathbb{F}_q)\), which we defer to another time.

Proof. First of all, the fact that \(\mathbf{E}_8(\mathbb{Z})\) is finitely generated (hence \(S\) exists) is a standard property of Chevalley groups.

Let \(g\) be the element of \(\mathbf{E}_8\) in the proof of Theorem 1.1; it turns out that \(g \in \mathbf{E}_8(\mathbb{Z})\) (this is clear from (3.1) and the fact that Magma constructs a group defined over \(\mathbb{Z}\)). Let \(P = \det(T - \text{Ad}(g))(T - 1)^{-8}\). Now, we claim that for any \(h \in \mathbf{E}_8(\mathbb{Z})\), if \(h\) is conjugate to \(g\) modulo \(p\) for \(p = 7\) and \(p = 11\) (where congruences refer to the reduction maps \(\mathbf{E}_8(\mathbb{Z}) \to \mathbf{E}_8(\mathbb{F}_p)\), or to congruences of matrices after applying \(\text{Ad}\), and conjugation is in \(\mathbf{E}_8(\mathbb{F}_p)\)), then the Galois group of the splitting field of \(Q = \det(T - \text{Ad}(h))(T - 1)^{-8}\) must be \(W(\mathbf{E}_8)\).

Indeed, let \(h_s \in \mathbf{E}_8(\mathbb{Q})\) be the semisimple part of \(h\) (see, e.g., [4, I.4.4]); we also have
\[
Q = \det(T - \text{Ad}(h_s))(T - 1)^{-8}.
\]

For \(p = 7\) and \(p = 11\), we have \(Q \equiv P \pmod{p}\), and since \(P\) has distinct roots modulo 11, not including 1 \(\in \mathbf{F}_{11}\) (it has only irreducible factors of degree 15), these conditions imply that \(h_s\) must be regular semisimple, and that \(Q\) has distinct roots.

Finally, the Galois group of the splitting field of \(Q\) will contain elements of the same conjugacy classes \(g_8\) and \(g_{15}\) discussed in the proof of Theorem 1.1, and hence by Proposition 2.2, it will have to be isomorphic to \(W(\mathbf{E}_8)\).

Now let \(H = \mathbf{E}_8(\mathbb{F}_7) \times \mathbf{E}_8(\mathbb{F}_{11})\).

Because the \(\mathbf{E}_8(\mathbb{F}_p)\) are distinct non-abelian simple groups for all \(p \geq 2\) (this is due to Chevalley [10]), the reduction map \(\mathbf{E}_8(\mathbb{Z}) \overset{\pi}{\longrightarrow} H\) is surjective. Indeed, the individual reduction maps \(\mathbf{E}_8(\mathbb{Z}) \to \mathbf{E}_8(\mathbb{F}_p)\) are onto, because the algebraic generators \(x_\alpha(1)\) in \(\mathbf{E}_8(\mathbb{Z})\) associated with the roots of \(\mathbf{E}_8\) (with respect to a split maximal torus) reduce to the corresponding generators of \(\mathbf{E}_8(\mathbb{F}_p)\) (see, e.g., [23, §6] for the fact that the elements \(x_\alpha(1)\) generate the group of rational points of a simple split Chevalley group
over a prime field; this can also be checked for \( p = 7, 11 \) with Magma’s `Generators()` command, and one can apply the classical Goursat lemma to the image of \( \pi \) (a proper subgroup of \( G_1 \times G_2 \), where \( G_i \) are non-abelian simple groups, which surjects to \( G_1 \) and \( G_2 \), is the graph of an isomorphism \( G_1 \rightarrow G_2 \)).

Then it is a standard fact about random walks on finite groups (“convergence to the invariant distribution of reversible, aperiodic, irreducible, finite Markov chains”) that we have

\[
\lim_{k \to +\infty} \frac{1}{|S|^k} \left| \{(s_1, \ldots, s_k) \in S^k \mid \pi(s_1 \cdots s_k) \in H \text{ is conjugate to } (g \pmod{7}, g \pmod{11}) \in H \} \right| = \frac{|C|}{|H|},
\]

where \( C \subset H \) is the conjugacy class of \( (g, g) \) (see the discussion in [18, Th. 2.1, §2.2] and [13, Chapter 7]; in our case, the aperiodicity follows from the symmetry of \( S \), and the fact that there is no non-trivial homomorphism \( E_8(F_p) \rightarrow \mathbb{Z}/2\mathbb{Z} \).

It follows from the two observations above that the proposition holds with the precision that the liminf is \( \geq |C||H|^{-1} \) (which, however, is very small, roughly \( 10^{-15} \)).

The final remark follows quite easily from this, although one has to be careful that different elements \( g \) may lead either to the same polynomials or to splitting fields which are not linearly disjoint. To check quickly the simple statement that we can find infinitely many such fields, assume by contradiction there are only finitely many, and let \( L \) be the compositum of those extensions. Let \( p_1, \ldots, p_N > 11 \) be a finite list of primes such that there is no subextension \( L' \neq \mathbb{Q} \) of \( L \) which is totally split at all of \( p_1, \ldots, p_N \) (such a finite list exists since there are only finite many subfields of \( L \)). We can reproduce the arguments above with additional conditions \( g \equiv 1 \pmod{p_j} \) for \( 1 \leq j \leq N \). Then any extension produced by random walk satisfying those conditions (or simply by lifting the congruence conditions to \( g \in E_8(\mathbb{Z}) \)) must be linearly disjoint from \( L \), since it will be split at all the primes \( p_j \).

\[\square\]

**Appendix A: intrinsic characterization of the polynomial**

We now build on (3.1) to explain in detail how the definition (and computation) of \( P \) may be phrased in such a way that it does not depend on any choice or implementation detail in Magma’s code (which may, in particular, vary from version to version). So, in principle, it would be possible to compute \( P \) by hand using only printed references (such as [23] or [11]). More practically, other programs can be used to check the computation.
To make things clearer, we denote here by $E_8^m/Q$ the split group of type $E_8$ over $Q$ given by Magma. Associated with it are a maximal torus $T^m \subset E_8^m$, split over $Q$, the set of roots $R$ associated with $T^m$, and a certain choice $\Delta \subset R$ of simple roots. Those are enumerated

$$\Delta = \{\alpha_1, \ldots, \alpha_8\}$$

as dictated by the Dynkin diagram: the roots $\alpha_i$ and $\alpha_j$ are not orthogonal, with respect to a $W(E_8)$-invariant inner product on $X(T^m) \otimes \mathbb{R}$, if and only if the vertices $i$ and $j$ of the Dynkin diagram are connected.

For each $\alpha \in R$, there is a one-parameter unipotent root subgroup $U_\alpha$ which is the image of a non-trivial homomorphism

$$x_\alpha : \mathbb{G}_a \to E_8^m$$

which is defined over $Q$ and such that

$$t^{-1}x_\alpha(u)t = x_\alpha(\alpha(t)u)$$

for $t \in T^m$ and $u \in \mathbb{G}_a$. The generators giving $g \in E_8^m(Q)$ in (3.1) are $x_i = x_{\alpha_i}(1)$ for $1 \leq i \leq 8$ and $x_{8+i} = x_{-\alpha_i}(1)$ for $1 \leq i \leq 8$.

To compute $\text{Ad}(g)$, since $\text{Ad}$ is an homomorphism, one needs to compute $\text{Ad}(x_\alpha(u))$ for $\alpha \in R$ and $u \in Q$. Now we have an induced map between Lie algebras

$$\text{Lie(}G_a) \xrightarrow{dx_\alpha} \text{Lie}(E_8^m).$$

Define $e_\alpha = dx_\alpha(1) \in \text{Lie}(E_8^m)$; this is a generator of the root space $g_\alpha$ associated to $\alpha$. Because the image of $x_\alpha$ is unipotent, $\text{ad}(e_\alpha)$ is a nilpotent endomorphism of $\text{Lie}(E_8^m)$, where $\text{ad}$ is the adjoint representation at the Lie algebra level (so that $\text{ad}(X)$ maps $Y$ to $[X,Y]$, where $[X,Y]$ is the Lie bracket). Then we have the formula

$$(4.2) \quad \text{Ad}(x_\alpha(u)) = \exp(u \text{ad}(e_\alpha)),$$

where the exponential, which can be interpreted by the usual power series as an exponential of matrix, is in fact a polynomial in $u \text{ad}(e_\alpha)$ since $\text{ad}(e_\alpha)$ is nilpotent (see (4.3) below). (This can be proved purely algebraically, but we may also extend scalars to $\mathbb{R}$, and see that both sides represent smooth functions of $u \in \mathbb{R}$ into $GL(\text{Lie}(E_8^m) \otimes \mathbb{R})$ which satisfy the same ordinary differential equation $\frac{dy}{du} = \text{ad}(e_\alpha)y$ and which take the same value at 0).

Thus to compute $\text{Ad}(g)$, it is enough to compute the endomorphisms $\text{ad}(e_\alpha)$ for $\alpha \in R$. But since a basis of the Lie algebra is made of a basis (say $h_1, \ldots, h_8$) of the Lie algebra of the torus $T^m$, and the $e_\alpha$ for $\alpha \in R$, this amounts in turn to being able to compute the brackets $[e_\alpha, e_\beta]$ for $\alpha, \beta \in R$ and $[e_\alpha, h_i]$ for all $\alpha$ and $i$. 

It turns out that those brackets are explicitly known and depend only on the “abstract” root system $R$ except for

$$[e_{\alpha}, e_{\beta}] = c(\alpha, \beta)e_{\alpha+\beta}$$

where $c(\alpha, \beta) \in Q^\times$. Those $c(\alpha, \beta)$ are known as the structure constants for the Lie algebra; in fact, when the group comes from a group scheme defined over $\mathbb{Z}$ (as is the case of $E_8^m$), we have $c(\alpha, \beta) \in \{\pm 1\}$. At the level of the group, the structure constants occur in the commutator relations

$$[x_{\alpha}(u), x_{\beta}(v)] = x_{\alpha+\beta}(c(\alpha, \beta)uv)$$

for $\alpha, \beta \in R$ with $\alpha + \beta \in R$ and $u, v \in G_a$ (the simple form of this relation is due to the fact that the root system of $E_8$ is an example of simply laced root system, see, e.g., [21, §10.2]).

Note in passing that the other brackets imply in particular that $\text{ad}(e_{\alpha})$ is nilpotent of order 2, so that (4.2) becomes

$$(4.3) \quad \text{Ad}(x_{\alpha}(u)) = \exp(u \text{ad}(e_{\alpha})) = \text{Id} + u \text{ad}(e_{\alpha}) + \frac{u^2}{2} \text{ad}(e_{\alpha})^2,$$

see, e.g., [21, 10.2.7] or [11, §3].

So the endomorphism $\text{Ad}(g)$ is easily computable from the knowledge of the structure constants. However, matters are somewhat complicated from then on by the fact that there is no absolutely canonical choice of the $c(\alpha, \beta)$. Still, as described for instance in [11, §2.3, §3], once a certain total order has been put on the root system, there exists a certain set of extraspecial pairs $(\alpha, \beta)$, precisely 112 of them, for which $c(\alpha, \beta)$ can be chosen arbitrarily in $\{\pm 1\}$, and then all other structure constants are uniquely determined.

Thus to describe unambiguously our endomorphism $\text{Ad}(g)$, it suffices to describe the extraspecial structure constants in $\text{Lie}(E_8^m)$. These are defined to all be $+1$. This can be checked by the following Magma commands:

```magma
L:= LieAlgebra( GroupOfLieType("E8", RationalField())); ExtraspecialSigns( RootDatum(L));
```

This already provides a way to construct from scratch, in principle, the polynomial $P$ of Theorem 1.1. However, there is an even stronger “uniqueness” feature, which was explained to us by Skip Garibaldi: for any choice of generators $x_{\alpha}(1)$ of the unipotent root subgroups (of a split group $E_8$ of type $E_8$ over $\mathbb{Z}$, with split maximal torus $T/\mathbb{Z}$ and simple roots $\Delta = \{\alpha_1, \ldots, \alpha_8\}$), determining the generators $x_i$ as above, the element

$$g = x_1 \cdots x_8 x_9 \cdots x_{16}$$

has the same characteristic polynomial. The point is that the elements $x_i$ are determined up to sign from the choice of the simple roots, hence the possible changes are determined by a vector $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_8) \in \{\pm 1\}^8$ of
signs, and the possible elements \( g \) that can be obtained are, relative to a fixed group \( \mathbf{E}_8/\mathbb{Z} \), of the form

\[
g_\varepsilon = x_{\alpha_1}(\varepsilon_1) \cdots x_{\alpha_8}(\varepsilon_8)x_{-\alpha_1}(\varepsilon_1) \cdots x_{-\alpha_8}(\varepsilon_8)
\]

Now it turns out that there exists an element \( t_\varepsilon \in T \), depending only on those signs, such that

\[
x_{\alpha_i}(\varepsilon_i) = t_\varepsilon x_{\alpha_i}(1)t_\varepsilon^{-1}
\]

for all simple roots \( \alpha_i \) (this follows, e.g., from [7, VIII.5.2, Cor. 3]). Then a simple computation (which can be done in \( SL(2) \), because it only concerns a root and its negative) shows that we also have

\[
x_{-\alpha_i}(\varepsilon_i) = t_\varepsilon x_{-\alpha_i}(1)t_\varepsilon^{-1}
\]

and therefore we also have

\[
g_\varepsilon = t_\varepsilon g t_\varepsilon^{-1},
\]

so that all \( \text{Ad}(g_\varepsilon) \) are conjugate and have the same characteristic polynomial.

We implemented this strategy using the GAP system [12], version 4.4.9, which knows about Lie algebras (but not algebraic groups), and has different structure constants than those of Magma (for instance, there is an extraspecial pair \( (\alpha_1, \alpha_3) \), and \( [e_{\alpha_1}, e_{\alpha_3}] = e_{\alpha_1+\alpha_3} \) for Magma, while \( [e_{\alpha_1}, e_{\alpha_3}] = -e_{\alpha_1+\alpha_3} \) for GAP). The recipe above, as it should, leads to a matrix with the same polynomial \( P \) as in Theorem 1.1 (note that the \texttt{CharacteristicPolynomial} function in GAP is not up to the task of computing \( P \) from the matrix in a reasonable amount of time, so we did this last check using Magma again, though one could also check modulo sufficiently many small primes to ensure the result by the Chinese Remainder Theorem). Here are the commands to produce this matrix:

```plaintext
L:=SimpleLieAlgebra("E",8,Rationals);
d:=[[]; for i in [1..248] do
    Append(d,[AdjointMatrix(Basis(L),Basis(L)[i])]);
od;
a:=[[];
am:=[[];
for i in [1..8] do
    a[i]:=IdentityMat(248)+d[i]+1/2*d[i]*d[i];
    am[i]:=IdentityMat(248)+d[120+i]+1/2*d[120+i]*d[120+i];
od;
m:=a[1]*a[2]*a[3]*a[4]*a[5]*a[6]*a[7]*a[8];
m:=m*am[1]*am[2]*am[3]*am[4]*am[5]*am[6]*am[7]*am[8];
```

Since GAP is Open Source, this computation can (or could) be checked in complete detail, guaranteeing the correctness of Theorem 1.1.
Appendix B: coefficient table

We conclude with an Appendix listing the table of coefficients of the polynomial $Q$ such that $P(T) = T^{120}Q(T - 1)$.
Explicit $W(E_8)$ polynomial

\[
\begin{array}{l}
\text{Coefficient of } T^i \\
\hline
97 & -3359560611781299224362340611346519673555729968 \\
98 & 120102062685314574423847620715510383030860 \\
99 & -399536336273091783248772485529679824619372 \\
100 & 12437443190985072692904053616601290526304 \\
101 & -36145402733875238808364434617032962704 \\
102 & 9781270532352502601151919455054150468 \\
103 & -2457588961016734215444804414937416 \\
104 & 5714846913247894902773082359642858 \\
105 & -122552946275635592994659815458660 \\
106 & 2413849634493902632445738578404 \\
107 & -43467840407415668458306853984 \\
108 & 711884504814065975117065754 \\
109 & -1053866957297700747046736 \\
110 & 14921126816597308603612 \\
111 & -16556653219330730324 \\
112 & 17244140511966984109 \\
113 & -156184734805164508 \\
114 & 1211012431626440 \\
115 & -7871527038772 \\
116 & 416889750481 \\
117 & -17257460 \\
118 & 524076 \\
119 & -1036 \\
120 & 1 \\
\end{array}
\]

References


Florent Jouve, Emmanuel Kowalski, David Zywina


Florent Jouve
Dept. of Mathematics, The University of Texas at Austin
1 University Station C1200
Austin, TX, 78712, USA.
E-mail: jouve@math.utexas.edu

Emmanuel Kowalski
ETH Zürich – DMATH
Rämistrasse 101
8092 Zürich, Switzerland
E-mail: kowalski@math.ethz.ch

David Zywina
Department of Mathematics, University of Pennsylvania
Philadelphia, PA 19104-6395, USA
E-mail: zywina@math.upenn.edu