JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Florent JOUVE, Emmanuel KOWALSKI et David ZYWINA

An explicit integral polynomial whose splitting field has Galois group $W(\mathbf{E}_8)$

Tome 20, nº 3 (2008), p. 761-782.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_3_761_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 761-782

An explicit integral polynomial whose splitting field has Galois group $W(\mathrm{E}_8)$

par Florent JOUVE, Emmanuel KOWALSKI et David ZYWINA

Pour les* 60 *ans de Henri Cohen

Résumé. En utilisant le principe selon lequel le polynôme caractéristique de matrices obtenues comme éléments d'un groupe réductif $\mathbf{G}$ sur $\mathbf{Q}$ a typiquement un corps de décomposition dont le groupe de Galois est le groupe de Weyl de $\mathbf{G}$, 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 $\mathbf{E}_8$.

Abstract. Using the principle that characteristic polynomials of matrices obtained from elements of a reductive group $\mathbf{G}$ over $\mathbf{Q}$ typically have splitting field with Galois group isomorphic to the Weyl group of $\mathbf{G}$, 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 $\mathbf{E}_8$.

1. Introduction

The goal of this paper is to give a concrete explicit example of a polynomial $P \in \mathbf{Z}[T]$ such that the Galois group of the splitting field of P is isomorphic to the group $W(\mathbf{E}_8)$, the Weyl group of the exceptional algebraic group $\mathbf{E}_8$ (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 $\mathbf{F}_2$; 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 $\mathbf{Q}(t)$ which are isomorphic to the root lattice $\mathbf{E}_8$ (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

Manuscrit reçu le 10 janvier 2008.

E.K. supported by the A.N.R through the ARITHMATRICS project.

Mots clefs. Inverse Galois problem, Weyl group, exceptional algebraic group, random walk on finite group, characteristic polynomial.

survey of Shioda [20], or the paper [16] of Nuzhin, as well as [3, §2.2] or [25, Th. 2]).

Theorem 1.1. *Let $P \in \mathbf{Z}[T]$ 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 $\mathbf{Q}$ is isomorphic to $W(\mathbf{E}_8)$.*

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 $\mathbf{G}/\mathbf{Q}$ is a (split) connected reductive algebraic group given as a $\mathbf{Q}$-subgroup of $GL(r)$ for some $r \geqslant 1$, via an injective $\mathbf{Q}$-homomorphism

$$\mathbf{G} \xrightarrow{i} GL(r),$$

and if $g \in \mathbf{G}(\mathbf{Q})$ 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 $W(\mathbf{G})$ of $\mathbf{G}$. 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 $\mathbf{E}_8$) determined the Galois group of $\det(T - \mathrm{ad}(X))$ for a "general" X in a simple Lie algebra over $\mathbf{C}$ (compare also with [20, §8.4, last paragraph], where the same characteristic polynomial for $\mathfrak{e}_8$ 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 $SL(r, \mathbf{Z})$ ($r \geqslant 2$, so that $\mathbf{G} = SL(r)$, and i is the tautological embedding in $GL(r)$) or $Sp(2g, \mathbf{Z})$ ($g \geqslant 1$, so that $\mathbf{G} = Sp(2g)$ and i corresponds to the standard embedding in $GL(2g)$): when k is large, the steps of the walk ξ_j being independently chosen uniformly at random among the elements of a fixed finite generating set of $\mathbf{G}(\mathbf{Z})$, the probability that the splitting field of $\det(T-g)$ has Galois group different from $W(\mathbf{G})$ is exponentially small in terms of k.

We do not take up the full details of this approach here for the exceptional group $\mathbf{E}_8/\mathbf{Q}$, 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 $W(\mathbf{E}_8)$, and it turns out (which we didn't quite expect) that it is possible to check that it is not a proper subgroup of $W(\mathbf{E}_8)$.

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

```
www.math.ethz.ch/~kowalski/e8pol.gp
www.math.ethz.ch/~kowalski/e8pol.mgm
```

two short files containing definitions of the polynomial above in GP/Pari and Magma, respectively. Loading either will define the variable `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

$$2^{3640}\cdot 3^{300}\cdot 5^{30}\cdot 73^{28}\cdot 109^{2}\cdot 113^{4}\cdot 131^{4}\cdot 331^{28}\cdot 419^{28}$$
$$\cdot\, 1033^{4}\cdot 1103^{57}\cdot 3307^{28}\cdot 4649^{4}\cdot 11467^{4}\cdot 629569^{4}\cdot 87087881^{4}\cdot 508141873^{2}$$
$$\cdot 8321263487^{28}\cdot 58276913161^{2}\cdot 126454995466730813^{4}\cdot 202992518210175167^{57}$$
$$\cdot\, 16443577117231488733333^{28}\cdot 175205913903379470245930652970 57^{2},$$

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., $\mathbf{Q}[T]/(P)$, not its splitting field) is

$$1103^{57}\cdot 202992518210175167^{57}\approx 8.9777\cdot 10^{1159}.$$

It was also possible to find a polynomial $\tilde{Q}\in\mathbf{Q}[T]$ with (slightly) smaller coefficients such that $\mathbf{Q}[T]/(\tilde{Q})\simeq\mathbf{Q}[T]/(Q)$ (by using the `polredabs` function), which is available upon request.

We also remark, as pointed out by the referee, that the splitting field of the polynomial Q over the quadratic field $k/\mathbf{Q}$ generated by the discriminant of P gives a realization of the orthogonal group $O_8^{+}(2)$ over k. It is in fact known that this group admits realizations as Galois group over $\mathbf{Q}$ (see [14, Th. 7.11, Th. 10.3 (g)] for this result), but we do not know if explicit polynomials have been constructed in that case.

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 $\mathfrak{S}_n$, $n \geqslant 1$, being the case $R = \{1, \ldots, n\}$. We denote by $\mathbf{F}_q$ 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, `polred`) with the polynomial P, etc, and for explanations of the corresponding functions and algorithms in Pari/GP; also, thanks to S. Garibaldi for explaining why the computation with GAP coincides with the one with Magma (see Appendix A).

2. A priori upper bound on the Galois group for $\mathbf{E}_8$

Let $\mathbf{E}_8/\mathbf{Q}$ be the split group of type $\mathbf{E}_8$; it is a simple algebraic group over $\mathbf{Q}$ of rank 8 and dimension 248. For information on $\mathbf{E}_8$ as a Lie group, we can refer to [1]; for $\mathbf{E}_8$ 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 $\mathbf{E}_8$ is of dimension $248 = \dim \mathbf{E}_8$. More precisely, this is the adjoint representation

$$\mathrm{Ad} : \mathbf{E}_8 \to GL(\mathfrak{e}_8)$$

where $\mathfrak{e}_8$ is the Lie algebra of $\mathbf{E}_8$, the tangent space at the identity element with the Lie bracket arising from differentiation of commutators. This representation is defined over $\mathbf{Q}$ 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 Ad is injective is because the center of $\mathbf{E}_8$ is trivial (in general, the kernel of the adjoint representation is the center, in characteristic 0 at least).

Fix a maximal torus $\mathbf{T}$ of $\mathbf{E}_8$ that is defined over $\mathbf{Q}$ (but not necessarily split, so that $\mathbf{T}$ is not necessarily isomorphic to $\mathbf{G}_m^8$ over $\mathbf{Q}$, but only over some finite extension field; in fact, the case of interest will be when this field is large). Let $X(\mathbf{T}) \simeq \mathbf{Z}^r$ be the group of characters $\alpha \colon \mathbf{T} \to \mathbf{G}_m$ (not necessarily defined over $\mathbf{Q}$). For each $\alpha \in X(\mathbf{T})$, let

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{e}_8 \mid \mathrm{Ad}(t) \cdot X = \alpha(t)X, \text{ for all } t \in \mathbf{T}\}$$

be the weight space for α in the adjoint representation. Let $R(\mathbf{T}, \mathbf{E}_8)$ be the set of non-trivial $\alpha \in X(\mathbf{T})$ with $\mathfrak{g}_\alpha \neq 0$; these are called the *roots of* $\mathbf{E}_8$ *with respect to* $\mathbf{T}$.

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

The set $R(\mathbf{T}, \mathbf{E}_8)$ is an abstract root system in the space $V = X(\mathbf{T}) \otimes_{\mathbf{Z}} \mathbf{R}$; cf. [6, Ch. 6] for definitions.

The structure theory of reductive groups (see, e.g., [4, 13.18]) shows that the space $\mathfrak{g}_\alpha$ is one dimensional for each root $\alpha \in R(\mathbf{T}, \mathbf{E}_8)$, and gives a direct sum decomposition

$$\mathfrak{e}_8 = \mathfrak{t} \oplus \bigoplus_{\alpha \in R(\mathbf{T}, \mathbf{E}_8)} \mathfrak{g}_\alpha, \tag{2.1}$$

where $\mathfrak{t}$ is the Lie algebra of $\mathbf{T}$.

From this decomposition, we recover the fact that $|R(\mathbf{T}, \mathbf{E}_8)| = \dim \mathbf{E}_8 - \dim \mathbf{T} = 248 - 8 = 240$. The absolute Galois group of $\mathbf{Q}$ acts naturally on $X(\mathbf{T})$: for any $\alpha \in X(\mathbf{T})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $\sigma(\alpha)$ is the unique character of $\mathbf{T}$ such that

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

for all $t \in \mathbf{T}$. The set of roots $R(\mathbf{T}, \mathbf{E}_8)$ is stable under this action.

Finally, we recall that the *Weyl group of* $\mathbf{E}_8$ *with respect to* $\mathbf{T}$ is the finite quotient group $W(\mathbf{T}, \mathbf{E}_8) = N(\mathbf{T})/\mathbf{T}$, where $N(\mathbf{T})$ is the normalizer of $\mathbf{T}$ in $\mathbf{E}_8$. Since all maximal tori of a connected linear algebraic group are conjugate (see, e.g., [21, Th. 6.4.1]), the Weyl group $W(\mathbf{T}, \mathbf{E}_8)$ is independent of the torus $\mathbf{T}$ up to isomorphism. We will write $W(\mathbf{E}_8)$ for this abstract group when the choice of torus is unimportant.

The group $W(\mathbf{T}, \mathbf{E}_8)$ acts on the roots by conjugation: for $w \in N(\mathbf{T})$, $\alpha \in R(\mathbf{T}, \mathbf{E}_8)$, let

$$(w \cdot \alpha)(t) = \alpha(w^{-1}tw), \tag{2.2}$$

which obviously depends only on the image of w in $W(\mathbf{T}, \mathbf{E}_8)$. This action is faithful (for instance, because $R(\mathbf{T}, \mathbf{E}_8)$ generates the character group $X(\mathbf{T})$, and $\mathbf{T}$ 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 $g \in \mathbf{E}_8(\mathbf{Q})$, and let $\mathbf{T}$ be any maximal torus of $\mathbf{E}_8$ that contains g.*

(1) *We have the factorization*[1]

$$\det(T - \mathrm{Ad}(g)) = (T-1)^8 \prod_{\alpha \in R(\mathbf{T}, \mathbf{E}_8)} (T - \alpha(g)).$$

[1] It is precisely because the values of the roots α 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.

(2) *Define the polynomial* $P = \det(T - \mathrm{Ad}(g))/(T-1)^8 \in \mathbf{Q}[T]$, *and let* $Z \subset \overline{\mathbf{Q}}$ *be the set of roots of* P. *Assume that* P *is separable. Then the map*

$$\beta \quad \begin{cases} R(\mathbf{T}, \mathbf{E}_8) & \rightarrow & Z \\ \alpha & \mapsto & \alpha(g) \end{cases} \tag{2.3}$$

is a bijection which respects the respective $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-actions.*

Let K *be the splitting field of* P, *i.e., the extension of* $\mathbf{Q}$ *generated by* Z. *Then the Galois action on* $R(\mathbf{T}, \mathbf{E}_8)$ *induces an injective homomorphism*

$$\phi_g\colon \mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow W(\mathbf{T}, \mathbf{E}_8)$$

such that for all $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ *and* $\alpha \in R(\mathbf{T}, \mathbf{E}_8)$, *we have*

$$\phi_g(\sigma) \cdot \alpha = \sigma(\alpha).$$

Proof. Since g is semisimple, it does lie in a maximal torus $\mathbf{T}$ of $\mathbf{G}$ (see, e.g., [21, Th. 6.4.5 (ii)]), and we fix one such torus. The operator $\mathrm{Ad}(g)$ acts as the identity on $\mathfrak{t}$ (since conjugation by g is trivial on $\mathbf{T}$) and as multiplication by $\alpha(g)$ on each $\mathfrak{g}_\alpha$, for $\alpha \in R(\mathbf{T}, \mathbf{E}_8)$. Therefore from (2.1), we deduce that

$$\det(T - \mathrm{Ad}(g)) = (T-1)^8 \prod_{\alpha \in R(\mathbf{T}, \mathbf{E}_8)} (T - \alpha(g)).$$

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 $\alpha \in R(\mathbf{T}, \mathbf{E}_8)$. To see this, we claim that for any α, we can find another root α' such that $\alpha'' = \alpha + \alpha'$ (in additive notation) is also in $R(\mathbf{T}, \mathbf{E}_8)$. 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 $\mathbf{T}$, which is necessarily defined over $\mathbf{Q}$.

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 Δ of simple roots such that $\alpha \in \Delta$, and take α' to be one of the simple roots which are not perpendicular to α (which exists because of the assumption on the root system; in other words, α and α' are connected in the Dynkin diagram of the simple roots; e.g., for $\mathbf{E}_8$, if α corresponds to the vertex labelled 1 of the Dynkin diagram (2.5), one can take α' the root labelled 3, etc). Then (α, α') 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 $\mathbf{E}_8$ (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_α is the reflection associated with α (see, e.g., [21, 10.2.2]).

Coming back to P, from the above factorization, we find that the map β is well-defined and surjective, and since $|R(\mathbf{T},\mathbf{E}_8)| = 240 = |Z|$, it is therefore bijective. For each $\alpha \in R(\mathbf{T},\mathbf{E}_8)$ and $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, we have

$$\beta(\sigma(\alpha)) = \sigma(\alpha)(g) = \sigma(\alpha)(\sigma(g)) = \sigma(\alpha(g)),$$

since $g \in \mathbf{E}_8(\mathbf{Q})$. The Galois group $\mathrm{Gal}(K/\mathbf{Q})$ acts faithfully on Z (the permutation action on the roots), so using β, we find that $\mathrm{Gal}(K/\mathbf{Q})$ acts faithfully on $R(\mathbf{T},\mathbf{E}_8)$, and this induces an injective group homomorphism

$$\phi_g\colon\ \mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow \mathfrak{S}_{R(\mathbf{T},\mathbf{E}_8)}.$$

Since $W(\mathbf{T},\mathbf{E}_8)$ acts faithfully on $R(\mathbf{T},\mathbf{E}_8)$, we may naturally view $W(\mathbf{T},\mathbf{E}_8)$ as a subgroup of $\mathfrak{S}_{R(\mathbf{T},\mathbf{E}_8)}$. To conclude, it is thus sufficient to show that the image of ϕ_g lies in this subgroup, or in other words, that for every $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$, there exists $w_\sigma \in W(\mathbf{T},\mathbf{E}_8)$ such that

$$\sigma(\alpha) = w_\sigma \cdot \alpha, \qquad \text{for all } \alpha \in R(\mathbf{T},\mathbf{E}_8).$$

Fix a split torus $\mathbf{T}_0$ of $\mathbf{E}_8$ that is defined over $\mathbf{Q}$, which exists since we assumed that our group $\mathbf{E}_8$ is split over $\mathbf{Q}$. Note that $\mathbf{T}_0$ is split over K and that $\mathbf{T}$ is also. Indeed, to check this, it is equivalent to check that the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/K)$ on the character group of $\mathbf{T}$ is trivial (see, e.g., [21, Prop. 13.2.2]). For this, it suffices to show that the roots are invariant, since they generate $X(\mathbf{T})$ (see, e.g., [21, 8.1.11], noting that $\mathbf{E}_8$ is of adjoint type, or the description of the root system in Remark 2.5). But for any $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/K)$, 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 β.

Now the fact that $\mathbf{T}$ and $\mathbf{T}_0$ are both K-split implies that there exists $x \in \mathbf{E}_8(K)$ such that $\mathbf{T} = x\mathbf{T}_0x^{-1}$, as proved, e.g., in [21, Th. 15.2.6]. Consider then any $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$, and note that $\sigma(x)$ makes sense since $x \in \mathbf{E}_8(K)$. Since both $\mathbf{T}$ and $\mathbf{T}_0$ are defined over $\mathbf{Q}$, we have $\mathbf{T} = \sigma(x)\mathbf{T}_0\sigma(x)^{-1}$ and hence $\sigma(x)x^{-1} \in N(\mathbf{T})$. Let w_σ be the element of $W(\mathbf{T},\mathbf{E}_8)$ represented by $\sigma(x)x^{-1}$. We now claim that $\sigma(\alpha) = w_\sigma \cdot \alpha$, for all $\alpha \in R(\mathbf{T},\mathbf{E}_8)$, which will finish the proof.

To see this, note that the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ acts trivially on $X(\mathbf{T}_0)$ (because $\mathbf{T}_0$ is split), and that we have an isomorphism

$$\gamma \quad \begin{cases} \mathbf{T}_0 & \rightarrow & \mathbf{T} \\ t & \mapsto & xtx^{-1} \end{cases}$$

which is defined over K. For any $\alpha \in R(\mathbf{T},\mathbf{E}_8)$, we have

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

and then, for all $t \in \mathbf{T}$, we obtain

$$(\sigma(\alpha))(t) = \alpha(x\sigma(x)^{-1}t\sigma(x)x^{-1}) = \alpha\big((\sigma(x)x^{-1})^{-1}t(\sigma(x)x^{-1})\big), \tag{2.4}$$

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) $g \in \mathbf{E}_8(\mathbf{Q})$, and a fixed *split* torus $\mathbf{T}_0$, one considers the set

$$X_g = \{t \in \mathbf{T}_0 \mid t \text{ and } g \text{ are conjugate}\}.$$

This is a non-empty set because g is semisimple, and one shows that the Weyl group (defined as $N(\mathbf{T}_0)/\mathbf{T}_0$) acts simply transitively by conjugation on X_g; an injection $\mathrm{Gal}(K/\mathbf{Q}) \to W(\mathbf{E}_8)$ is then produced by fixing $t_0 \in X_g$ and mapping σ to w_σ 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 $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ is always conjugate to the permutation of $R(\mathbf{T}_0, \mathbf{E}_8)$ induced by σ.

Remark 2.4. Proposition 2.2 implies that the zeros of a polynomial $\det(T - \mathrm{Ad}(g))$ satisfy many multiplicative relations; indeed, all the 240 zeros are contained in the multiplicative subgroup of $\mathbf{C}^\times$ generated by the $\alpha(t)$ corresponding to eight simple roots α (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 $W(\mathbf{E}_8)$ which can be useful to orient the reader. This group $W(\mathbf{E}_8)$ is of order $696729600 = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$, and its simple Jordan-Hölder factors are $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$ and the simple group $D_4(\mathbf{F}_2)$ (also sometimes denoted $P\Omega_8^+(2)$, $D_4(2)$, $D_4^+(2)$, 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 $\mathfrak{S}_{240}$ (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 α_i with non-negative coefficient, or its opposite α^{-1} can be written in this way, but not both), subject to relations

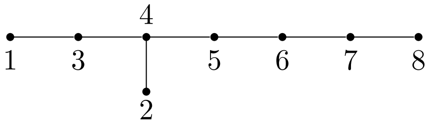
$$w_i^2 = 1 \qquad (w_i w_j)^{m(i,j)} = 1, \qquad 1 \leqslant i < j \leqslant 8,$$

where

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

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

(2.5)



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

One can also define $W(\mathbf{E}_8)$ as the automorphism group of the lattice $\Gamma_8 \subset \mathbf{Q}^8$ (of rank 8) generated by $(\frac{1}{2}, \ldots, \frac{1}{2})$ and the sublattice

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

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 $W(\mathbf{E}_8) \simeq \mathrm{Aut}(\Gamma_8)$ is proved; note many authors studying lattices write $\mathbf{E}_8$ for the lattice instead of the group). In fact, in the identification of $W(\mathbf{T}, \mathbf{E}_8)$, for some maximal torus $\mathbf{T} \subset \mathbf{E}_8$, as $\mathrm{Aut}(\Gamma_8)$, Γ_8 can be identified with the character group of $\mathbf{T}$, and the roots R are then interpreted as the 240 vectors in Γ_8 with squared-length 2, namely

$$\pm x_i \pm x_j, \qquad 1 \leqslant i < j \leqslant 8,$$
$$\tfrac{1}{2}(\pm x_1 \pm x_2 \pm \cdots \pm x_8), \qquad \text{with an even number of minus signs,}$$

the action of $W(\mathbf{E}_8)$ on R being the same as the action of the automorphism group. The lattice Γ_8 is generated by R, with a basis given for instance by the following eight roots

$$\tfrac{1}{2}(x_1 + x_2 - x_3 - x_4 - x_5 - x_6 - x_7 - x_8)$$
$$-x_2 + x_3, \quad x_2 + x_3, \quad -x_i + x_{i+1}, \text{ for } 3 \leqslant i \leqslant 7,$$

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

Remark 2.6. See [20, §7] for explicit examples of polynomials whose splitting fields have Galois groups $W(\mathbf{E}_6)$ and $W(\mathbf{E}_7)$; they are much simpler, which can be expected, since $|W(\mathbf{E}_6)| = 51840 = 2^7 \cdot 3^4 \cdot 5$ and $|W(\mathbf{E}_7)| = 2903040 = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$. 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 $\mathbf{E}_6$ and $\mathbf{E}_7$ 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 $\mathbf{E}_6$ and [8, p. 50] for $\mathbf{E}_7$). 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 $\mathbf{E}_8/\mathbf{Q}$, 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 $x_i = x_{\alpha_i}(1)$, $1 \leqslant i \leqslant 8$, of the eight one-parameter unipotent root subgroups U_{α_i} associated with the simple roots α_i (see, e.g., [21, 8.1.1]), and the generators $x_{8+i} = x_{-\alpha_i}(1)$, $1 \leqslant i \leqslant 8$, 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 $\mathbf{E}_8(\mathbf{Q})$ by taking the product of those sixteen generators x_i (in the order above) namely

$$g = x_1 \cdots x_{16} = x_{\alpha_1}(1) \cdots x_{\alpha_8}(1) x_{-\alpha_1}(1) \cdots x_{-\alpha_8}(1), \tag{3.1}$$

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 $\mathbf{E}_8$, we compute the matrix $m = \mathrm{Ad}(g)$ (which is in fact in $SL(248, \mathbf{Z})$; 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 $\det(T - m) \in \mathbf{Z}[T]$ 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] Note that we also checked that if we construct an element of $\mathbf{E}_8(\mathbf{Q})$ by taking the product of the i first generators (in the same order as above) with $1 \leqslant i \leqslant 15$, 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 $\mathbf{Q}$ (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 $Q \in \mathbf{Z}[T]$, 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 $\mathrm{Ad}(g)$ is diagonalizable, but this is clear because the minimal polynomial of $\mathrm{Ad}(g)$ 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 $W(\mathbf{E}_8)$. First, according to Proposition 2.2, we know that G can be identified with a subgroup of $W(\mathbf{E}_8)$, 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 $W(\mathbf{E}_8)$ as a subgroup of $\mathfrak{S}_{240}$ by permutations of the roots of $\mathbf{E}_8$.

This last compatibility is crucial because of the following well-known fact of algebraic number theory: if $S \in \mathbf{Z}[T]$ is an irreducible monic polynomial of degree d with splitting field $F/\mathbf{Q}$, H the Galois group of $F/\mathbf{Q}$ 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 $n_i \geqslant 0$ distinct monic irreducible polynomials of degree i in $\mathbf{F}_p[T]$, then $H \subset \mathfrak{S}_d$ 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 $\mathfrak{S}_{240}$, 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 $G \subset \mathfrak{S}_{240}$ contains elements of the type

$$g_8 = c_1^{(4)} c_2^{(4)} c_3^{(8)} \cdots c_{31}^{(8)}, \qquad g_{15} = d_1^{(15)} \cdots d_{16}^{(15)} \tag{3.2}$$

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

$$12096, \quad 11200, \quad 2025, \quad 1575, \quad 1120, \quad 960, \quad 135, \quad 120, \quad 2.$$

Let M be any maximal subgroup; then Magma can also output a list of the cycle structures, in the permutation action on $\mathfrak{S}_R \simeq \mathfrak{S}_{240}$, 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 $G = \mathrm{Gal}(K/\mathbf{Q})$ 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 ε, which is a surjective homomorphism

$$\varepsilon \, : \, W(\mathbf{E}_8) \hookrightarrow \mathfrak{S}_{240} \to \mathbf{Z}/2\mathbf{Z},$$

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:

```
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 `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 $W(\mathbf{E}_8)$ (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 $W(\mathbf{E}_8)$, 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 $|W(\mathbf{E}_8)|/30$ (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 $L/\mathbf{Q}$ with Galois group $W(\mathbf{E}_8)$ 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 $|W(\mathbf{E}_8)|/16$ elements, and is the largest conjugacy class in $W(\mathbf{E}_8)$ (and, as we explained, any odd conjugacy class would have done just as well for our argument).[4]

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 $W(\mathbf{E}_8)$. Let $b = 1$ or 2, and let $c = w_1 \cdots w_8$ be a Coxeter element in $W(\mathbf{E}_8)$. Then any proper subgroup of $W(\mathbf{E}_8)$ 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.) □

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 $\mathbf{E}_8/\mathbf{Z}$ be a model of the split Chevalley group $\mathbf{E}_8$ defined over $\mathbf{Z}$, and let $S \subset \mathbf{E}_8(\mathbf{Z})$ 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 $\Gamma = \mathbf{E}_8(a_5)$ on p. 58.

$\mathbf{E}_8(\mathbf{Z})$. *Then*

$$(4.1)\quad \liminf_{k\to+\infty} \frac{1}{|S|^k}|\{(s_1,\ldots,s_k)\in S^k \mid \textit{the splitting field of}\\ \det(T-\mathrm{Ad}(s_1\cdots s_k)) \textit{ has Galois group } W(\mathbf{E}_8)\}| > 0.$$

In fact, there exist infinitely many $g\in\mathbf{E}_8(\mathbf{Z})$ for which the splitting fields of $\det(T-\mathrm{Ad}(g))$ *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 $\geqslant 1-C\exp(-ck)$ for some $c>0$, $C\geqslant 0$), but checking this would involve a deeper analysis of the finite groups $\mathbf{E}_8(\mathbf{F}_q)$, which we defer to another time.

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

Indeed, let $h_s\in\mathbf{E}_8(\mathbf{Q})$ be the semisimple part of h (see, e.g., [4, I.4.4]); we also have

$$Q=\det(T-\mathrm{Ad}(h_s))(T-1)^{-8}.$$

For $p=7$ and $p=11$, we have $Q\equiv P\,(\mathrm{mod}\,p)$, 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

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

Because the $\mathbf{E}_8(\mathbf{F}_p)$ are distinct non-abelian simple groups for all $p\geqslant 2$ (this is due to Chevalley [10]), the reduction map $\mathbf{E}_8(\mathbf{Z})\xrightarrow{\pi}H$ is surjective. Indeed, the individual reduction maps $\mathbf{E}_8(\mathbf{Z})\to\mathbf{E}_8(\mathbf{F}_p)$ are onto, because the algebraic generators $x_\alpha(1)$ in $\mathbf{E}_8(\mathbf{Z})$ associated with the roots of $\mathbf{E}_8$ (with respect to a split maximal torus) reduce to the corresponding generators of $\mathbf{E}_8(\mathbf{F}_p)$ (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 π (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 $G_1 \to G_2$).

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

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

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 $\mathbf{E}_8(\mathbf{F}_p) \to \mathbf{Z}/2\mathbf{Z}$).

It follows from the two observations above that the proposition holds with the precision that the liminf is $\geqslant |C||H|^{-1}$ (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 $L' \neq \mathbf{Q}$ of L which is totally split at all of p_1,. . . , 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 $g \equiv 1 \,(\mathrm{mod}\, p_j)$ for $1 \leqslant j \leqslant N$. Then any extension produced by random walk satisfying those conditions (or simply by lifting the congruence conditions to $g \in \mathbf{E}_8(\mathbf{Z})$) must be linearly disjoint from L, since it will be split at all the primes p_j. □

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 $\mathbf{E}_8^m/\mathbf{Q}$ the split group of type $\mathbf{E}_8$ over $\mathbf{Q}$ given by Magma. Associated with it are a maximal torus $\mathbf{T}^m \subset \mathbf{E}_8^m$, split over $\mathbf{Q}$, the set of roots R associated with $\mathbf{T}^m$, and a certain choice $\Delta \subset R$ of simple roots. Those are enumerated

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

as dictated by the Dynkin diagram: the roots α_i and α_j are not orthogonal, with respect to a $W(\mathbf{E}_8)$-invariant inner product on $X(\mathbf{T}^m) \otimes \mathbf{R}$, 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_α which is the image of a non-trivial homomorphism

$$x_\alpha : \mathbf{G}_a \to \mathbf{E}_8^m$$

which is defined over $\mathbf{Q}$ and such that

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

for $t \in \mathbf{T}^m$ and $u \in \mathbf{G}_a$. The generators giving $g \in \mathbf{E}_8^m(\mathbf{Q})$ in (3.1) are $x_i = x_{\alpha_i}(1)$ for $1 \leqslant i \leqslant 8$ and $x_{8+i} = x_{-\alpha_i}(1)$ for $1 \leqslant i \leqslant 8$.

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

$$\mathrm{Lie}(\mathbf{G}_a) \xrightarrow{dx_\alpha} \mathrm{Lie}(\mathbf{E}_8^m).$$

Define $e_\alpha = dx_\alpha(1) \in \mathrm{Lie}(\mathbf{E}_8^m)$; this is a generator of the root space $\mathfrak{g}_\alpha$ associated to α. Because the image of x_α is unipotent, $\mathrm{ad}(e_\alpha)$ is a nilpotent endomorphism of $\mathrm{Lie}(\mathbf{E}_8^m)$, where ad is the adjoint representation at the Lie algebra level (so that $\mathrm{ad}(X)$ maps Y to $[X, Y]$, where $[X, Y]$ is the Lie bracket). Then we have the formula

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

where the exponential, which can be interpreted by the usual power series as an exponential of matrix, is in fact a polynomial in $u\,\mathrm{ad}(e_\alpha)$ since $\mathrm{ad}(e_\alpha)$ is nilpotent (see (4.3) below). (This can be proved purely algebraically, but we may also extend scalars to $\mathbf{R}$, and see that both sides represent smooth functions of $u \in \mathbf{R}$ into $GL(\mathrm{Lie}(\mathbf{E}_8^m) \otimes \mathbf{R})$ which satisfy the same ordinary differential equation $\frac{dy}{du} = \mathrm{ad}(e_\alpha)y$ and which take the same value at 0).

Thus to compute $\mathrm{Ad}(g)$, it is enough to compute the endomorphisms $\mathrm{ad}(e_\alpha)$ for $\alpha \in R$. But since a basis of the Lie algebra is made of a basis (say $h_1, \dots, h_8$) of the Lie algebra of the torus $\mathbf{T}^m$, and the e_α for $\alpha \in R$, this amounts in turn to being able to compute the brackets $[e_\alpha, e_\beta]$ for α, $\beta \in R$ and $[e_\alpha, h_i]$ for all α 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 $c(\alpha, \beta) \in \mathbf{Q}^\times$. 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 $\mathbf{Z}$ (as is the case of $\mathbf{E}_8^m$), 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 α, $\beta \in R$ with $\alpha + \beta \in R$ and u, $v \in \mathbf{G}_a$ (the simple form of this relation is due to the fact that the root system of $\mathbf{E}_8$ 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 $\mathrm{ad}(e_\alpha)$ is nilpotent of order 2, so that (4.2) becomes

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

see, e.g., [21, 10.2.7] or [11, §3].

So the endomorphism $\mathrm{Ad}(g)$ 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* (α, β), 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 $\mathrm{Ad}(g)$, it suffices to describe the extraspecial structure constants in $\mathrm{Lie}(\mathbf{E}_8^m)$. *These are defined to all be* $+1$. This can be checked by the following Magma commands:

```
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 $\mathbf{E}_8$ of type E_8 over $\mathbf{Z}$, with split maximal torus $\mathbf{T}/\mathbf{Z}$ 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 $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_8) \in \{\pm 1\}^8$ of signs, and the possible elements g that can be obtained are, relative to a fixed group $\mathbf{E}_8/\mathbf{Z}$, of the form

$$g_{\boldsymbol{\varepsilon}} = x_{\alpha_1}(\varepsilon_1)\cdots x_{\alpha_8}(\varepsilon_8)x_{-\alpha_1}(\varepsilon_1)\cdots x_{-\alpha_8}(\varepsilon_8)$$

Now it turns out that there exists an element $t_{\boldsymbol{\varepsilon}} \in \mathbf{T}$, depending only on those signs, such that

$$x_{\alpha_i}(\varepsilon_i) = t_{\boldsymbol{\varepsilon}} x_{\alpha_i}(1) t_{\boldsymbol{\varepsilon}}^{-1}$$

for all simple roots α_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

$$x_{-\alpha_i}(\varepsilon_i) = t_{\boldsymbol{\varepsilon}} x_{-\alpha_i}(1) t_{\boldsymbol{\varepsilon}}^{-1}$$

and therefore we also have

$$g_{\boldsymbol{\varepsilon}} = t_{\boldsymbol{\varepsilon}} g t_{\boldsymbol{\varepsilon}}^{-1},$$

so that all $\mathrm{Ad}(g_{\boldsymbol{\varepsilon}})$ 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 (α_1, α_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 `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:

```
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 $P(T) = T^{120}Q(T + T^{-1})$.

i	Coefficient of T^i
0	3655878949839679228545604211066587948352691620258015814553812701089947720863540976 89969
1	−111887646713137430521048522604623538676037567802415981673883117751446056784102628673 32448
2	169253696238399029559192135798369681596869020592118579039666548219126339368278708130365896
3	−16871599202625244945718248910288337200396954706370569562234622933721635292901264313045 85100
4	1246653887056935042811751248267463873819259839102822551011387643367102984812116623425278 4168
5	−728269471566973634550357234234269718903249223813147727033376925804090972820095648612223 15768
6	350331529672673601609711561533019721386090515420775351136161318553244630344247566318282845504
7	−14272385656156168368749660272808498929314673919470833506310980085795474519493655121654 45324548
8	5026354438587350042393019188859322619309223067912455590765316222074769006654715395492167534064
9	−155432426927478900309456519584687287930281384244483880523448845411524214762868901602816 06087912
10	427277228565865779631258585803103025992527144045229019252972643856542811647037266340733 63638112
11	−105456673870095173711703163143669727224697814378273599459423442778596360012854640538260794921080
12	2356078170957551993688581901498998788561639785155614314554514031315579148073619500168566 03119900
13	−47977014926490760959163686706653014844472931786280060863293713860842703218461074385521942 8626708
14	8956356231730618036002268513122117723125049324189333060863836161565482619496880145245313 33153508
15	−154047255579008975439206165268927893225750575885319436650783952332966645396351518807147 8275995640
16	2451788710586871745589664228861539890944914421283328064352160762645878635406460765371848 464480340
17	−362464050590163818800969733785795448347338510958993087294955818455198791118078136004279 0583083604
18	4994024072126951505126399098824620904652453895567294295762673834554854694248727868906577 016537540
19	−643172163767297376425355955402812975260885947008068224064040462754133173117395768803620 0659035092
20	7763241468623979545008124501105553771540039037756350364261700519310257100760280299151055 542732492
21	−880294288038149938824565107025927387257133887019890682471629876658527691483055582491983 2373777496
22	9397428905594516743427299464872348062738848222907978714295289389671821494398632421489330 984834096
23	−946292186183823150423264818068356620906068754285022275683057287389641532183482378880535 2470036944
24	9004042910145318452280462187844950546979429562212010153159452511976316511237893389182144 564071816
25	−810846677744797335062514386602088914590500178148403323330317275066290660350225763504076 3697120800
26	6920877993691644199503325490868076639226322468228894863452356759758353696538512384603684 679212236
27	−560639328665035505063244531239254564807748541293508639942701501322245511542334255066822 9228526380
28	4315552971543918712292689802749919612866096319783016002162626109826378082792279094813015 908629560
29	−316014729294557396162558442409771792037022575765028248339068240881582156544353211741934 3460827840
30	2203660581121260808668034624515265900353324373444058449372337614106044024846226145678411 752103944
31	−146474434330301954627390006617178873947302542253746672774019261577648194577466136187467 6553542888
32	9288377473519001398475109115392192916668808364926009603017616124822122796867853489711716 33827678
33	−562380987452023460657841067338702972535374341028182139165378619782789496619429231331416 465467136
34	3253562358249063049142624469761767965717648564566862798075574363173492775248044152062079 43829668
35	−179980581397996318804833400684252642822685183748168637880480218232713417673333008007141 832612656

i	Coefficient of T^i
36	9525935867334281196257737496802434411675952819111819733090199405595351818530196193805 8278687152
37	−48268244673830087725415910980532812904398769665363772047167723957702501678922709545345961314952
38	234273924423789017503549587022927279662075047491837233574212898698021943326496853314859833886 76
39	−108971632948360818020237402059192217045820451216730854407095238357971163734840158379497214857 60
40	485994548142665239365793298212340464805181935176940059580638204419718778857670107595552266514 8
41	−207904128957238188098185113751724325074533022345668006765764345172812939612009330482688553934 4
42	853451569340348395409517113261975739247889854460920295141494937564435136719739663763259170648
43	−336306101614439964957860525247000005857956841159545332435837005318322034194039653447757128580
44	127254544703467199806219784585607568957868365018715949880037719179469076397221511835490064520
45	−462513445436078725971009739400886709161830468766141323966244222113226702229254328026033487 64
46	161512294492144957540705013169282480803014705921259955731537933170586664304161702674650796 92
47	−542029623005368774096118086613218322931921280426756960985724517219069956301030304591136894 4
48	174852399601581920712250367205397380175980711632905661966371645419876989206678590265255487 8
49	−542294947655157376138526043814456732351589519118047194151659330168304308215153590486208844
50	16172935862088003197127926697747570755437801676229023800089356728255453102074455907437 6324
51	−463869188986237217474698810030204172145668502650535114507992237066598963813957909597438 04
52	127970514991628963984407217790237967249843252959160147960396289318424659483438948451113 80
53	−339607312911272821833933753671469772432925174574219450636495000879436980094241090515213 6
54	867027209473064571745438316617176614625159965185956598478937806132721701397948869458900
55	−2129628759047661568080539580329073335769500461656257746776672519047876556437575051763 24
56	503278855324158938804831557853490712538077311727477732074515210312526717326322303889 78
57	−114434386671879085433515709868765791761107474903381192451953508881502960550169755820 04
58	250350476312666500501758912665916562918380129128192524357871217146209977184961925474 4
59	−52695894494490726849363910367787731695418436441898266807943892019318841189964356850 8
60	1067150515924383289306892390046542535455737217194513600401686577404531899409151923 14
61	−207907799103357938654714576353578331631541129515160808807303957647355120130256527 96
62	389654199032008714559471645042246040997828759908228369348595230936592531800564450 0
63	−702441672053715648053554868151235620650214741238958432207947706491608211081312400
64	1217906293933626045443575891235974362526065587434348152620030439238974641211671 97
65	−2030635580590105083790184697265677341875656504546886367341254017221033727190234 0
66	325535050744221658893783581460068090820432376928395696152502323845143954494176 0
67	−501690059905683053720524741882157670117822132733245580070161190249583644847028
68	74312275258414477271317122327593160444507387370961124773453087824921327894416
69	−105774044552554697411433629650216722277821240463565285096519771099359926394 28
70	1446398328284711960698545660047973219044522333438207563556095761539846607256
71	−18996519559050912030516397229000562937779126459948317675246839823376324948 4
72	2395601606233371786554667702145256282431920936576436901814215375170795202 8
73	−289985551626442948970636214886713556047689046356649602477631682246768366 4
74	33683359931378850055967918177671604721038854040218043765411928833939374 0
75	−375298365252837471053718557231692477567001299095281572400242500019987 88
76	40095301522358096876408276723413584658915952975974783012918981896548 76
77	−4105698127153604390158533973705945471705454874276359364145000450306 52
78	402777959739174351157626462973173436172052725677862304851719105106 52
79	−37837685520390896825866186396558769421033223562235974202642793967 24
80	3402079879563275038788272504572633282653178303001597198949832063 82
81	−292611555142706202080178448650519443403040217103863047031171452 00
82	24061104052487871662441632140265623428786778657344129161332003 36
83	−189038373443757680942334919469355568250711998730640952299841492
84	1418110193908767337519222117327697897398825159577109946991124 8
85	−1015059691711179211122508131842675818892409168967000131556504
86	69273982784497519473037155287005412956159996851830481504940
87	−450400516357602205079555654456891807312822870560468341485 6
88	2787449227655635121225928531761051239369669339337567800 06
89	−164058105747109239189586690501948230652679960650804944 20
90	917373448095043315139701983319126630369060417226308240
91	−486851807313964339634743399521135795497971849034569 32
92	244940373686195276450219431395448163046462191337736 2
93	−116683889096980060401747351223521809696783299718096
94	5256318681823135646376194757383743386905542401984
95	−223594517259941108513934941256272336603486583080
96	8967837569963007481063656618084357384523513289

i	Coefficient of T^i
97	−338566611781299224336234061335519673555729968
98	12010206026853145744238047620715510383030860
99	−399536336273091783248772485529679824619372
100	12437443190985072692004053616601920326304
101	−361454027338752388080364343617032962704
102	9781270532352502601151919455054150468
103	−245758896101673421544480044149574716
104	5714846913247894902773082359642858
105	−122552946275635592994659815458660
106	2413849634493902632445738578404
107	−43467840407415668458306853984
108	711884504814065975117065754
109	−10538669572997700747046736
110	140021126816597308605612
111	−1655565532193307303324
112	17242140511966984109
113	−156184748605164508
114	1211012431626440
115	−7871527038772
116	41688975082
117	−172657460
118	524076
119	−1036
120	1

References

[1] J. F. Adams, *Lectures on exceptional Lie groups.* Chicago Lectures in Math., Univ. Chicago Press, 1996.

[2] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups; Maximal subgroups and ordinary characters for simple groups*, with computational assistance from J. G. Thackray, Oxford University Press, 1985.

[3] N. Berry, A. Dubickas, N. Elkies, B. Poonen and C. J. Smyth, *The conjugate dimension of algebraic numbers.* Quart. J. Math. **55** (2004), 237–252.

[4] A. Borel, *Linear algebraic groups*, 2nd edition. GTM **126**, Springer 1991.

[5] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system, I. The user language.* J. Symbolic Comput., **24** (1997), 235–265; also `http://magma.maths.usyd.edu.au/magma/`

[6] N. Bourbaki, *Groupes et algèbres de Lie*, Chapitres 4, 5, 6. Hermann, 1968.

[7] N. Bourbaki, *Groupes et algèbres de Lie*, Chapitres 7, 8. Hermann, 1975.

[8] É. Cartan, *Sur la réduction à sa forme canonique de la structure d'un groupe de transformations fini et continu.* Amer J. Math. **18** (1896), 1–46 (=Oeuvres Complètes, t. I_1, 293–353).

[9] R.W. Carter, *Conjugacy classes in the Weyl group.* Compositio Math. **25** (1972), 1–59.

[10] C. Chevalley, *Sur certains groupes simples.* Tôhoku Math. J. **7** (1955), 14–66.

[11] A. Cohen, S. Murray and D.E. Taylor, *Computing in groups of Lie type.* Math. Comp. **73**, Number 247, 1477–1498.

[12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.9*, 2007, `www.gap-system.org`

[13] E. Kowalski, *The large sieve and its applications: arithmetic geometry, random walks and discrete groups.* Cambridge Tracts in Math. **175**, Cambridge Univ. Press, 2008.

[14] G. Malle and B.H. Matzat, *Inverse Galois theory.* Springer Monographs in Math., 1999.

[15] Y.I Manin, *Cubic forms: algebra, geometry, arithmetic.* North Holland Math. Library 4, 2nd ed., 1988.

[16] Ya. N. Nuzhin, *Weyl groups as Galois groups of a regular extension of the field* $\mathbf{Q}$, (Russian). Algebra i Logika **34** (1995), no. 3, 311–315, 364; translation in Algebra and Logic **34** (1995), no. 3, 169–172.

[17] PARI/GP, version `2.4.2`, Bordeaux, 2007, `http://pari.math.u-bordeaux.fr/`.

[18] L. Saloff-Coste, *Random walks on finite groups.* In "Probability on discrete structures", 263–346, Encyclopaedia Math. Sci., **110**, Springer 2004.

[19] J-P. Serre, *Cours d'arithmétique.* PUF 1988.

[20] T. Shioda, *Theory of Mordell-Weil lattices.* In Proceedings of ICM 1990 (Kyoto), Vol. I (473–489), Springer, 1991.

[21] T.A. SPRINGER, *Linear algebraic groups*, 2nd edition, Progr. Math. **9**, Birkhaüser 1998.

[22] T.A. SPRINGER, *Regular elements of finite reflection groups.* Invent. math. **25** (1974), 159–198.

[23] R. STEINBERG, *Lectures on Chevalley groups.* Yale Univ. Lecture Notes, 1967.

[24] A. VÁRILLY-ALVARADO and D. ZYWINA, *Arithmetic E_8 lattices with maximal Galois action.* To appear in LMS J. Comput. Math.

[25] V.E. VOSKRESENSKII, *Maximal tori without effect in semisimple algebraic groups* (Russian). Matematicheskie Zametki, Vol. **44** (1988), 309–318; English translation: Mathematical Notes **44**, 651–655.

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