Splitting fields for E_8-torsors

Burt Totaro

Several of the fundamental problems of algebra can be unified into the problem of classifying G-torsors over an arbitrary field k, for a linear algebraic group G. (A G-torsor can be defined as a principal G-bundle over Spec k, or as an algebraic variety over k with a free transitive action of G.) For example, $PGL(n)$-torsors are equivalent to central simple algebras, and torsors for the orthogonal group are equivalent to quadratic forms. See Serre [36] for a recent survey of the classification problem for G-torsors over a field.

The study of G-torsors is still in its early stages. Indeed, it is not completely known how complicated G-torsors can be, if we fix the type of the group but allow arbitrary base fields. Tits showed that there is a bound on how complicated they can be. For each split semisimple group G, there is an integer $d(G)$ depending only on the type of G, not on the field, such that every G-torsor over a field k becomes trivial over some finite extension E of k of degree dividing $d(G)$ [40]. For example, it is easy to see that one can take $d(G)$ to be the order of the Weyl group of G. But it is a fundamental problem to determine the best possible number $d(G)$ for each type of group. Tits found the optimal value of d for the simply connected split groups of exceptional type other than E_8: one can take $d(G_2) = 2$, $d(F_4) = 2\cdot 3 = 6$, $d(E_6) = 2\cdot 3 = 6$, and $d(E_7) = 2^2\cdot 3 = 12$ [40].

As in other problems, the group E_8 is far more difficult. Most of Tits's paper is devoted to the proof that one can take $d(E_8) = 2^9\cdot 3^3\cdot 5 = 69120$, which is much better than the easy result that one can take $d(E_8)$ to be the order of the Weyl group, $2^{14}\cdot 3^5\cdot 5^2\cdot 7 = 696,729,600$. (That is, Tits shows that every torsor for the split group E_8 over a field becomes trivial over some field extension of degree dividing $2^9\cdot 3^3\cdot 5$. Because E_8 has no center or outer automorphisms, it is equivalent to say, as Tits does, that every algebraic group of type E_8 over a field becomes split over some extension of degree dividing $2^9\cdot 3^3\cdot 5$.)

In this paper, we will show that we can take $d(E_8) = 2^6\cdot 3^2\cdot 5 = 2880$ (Theorem 0.1, below). The proof is completed at the end of section 7. It turns out that this result is optimal. Indeed, Grothendieck defined a topological invariant, the torsion index, for every split group G [22]. He showed that for a "versal" G-torsor over a field, the greatest common divisor of all degrees of splitting fields is the torsion index of G. I computed that the torsion index of E_8 is exactly $2^6\cdot 3^2\cdot 5$ [41], which implies the optimality of the following theorem.

2000 Mathematics Subject Classification. Primary 11E72; Secondary 14M17, 20G15.

Key words and phrases: torsors, Galois cohomology, splitting fields, homogeneous varieties, exceptional Lie groups, Rost invariant, maximal subgroups.

Theorem 0.1 *Every torsor for the split algebraic group E_8 over a field becomes trivial over some separable field extension of degree dividing $2^6 \cdot 3^2 \cdot 5 = 2880$. Equivalently, every algebraic group of type E_8 over a field becomes split over some separable field extension of degree dividing $2^6 \cdot 3^2 \cdot 5$.*

The field extension we construct will not be Galois. The fact that it is separable is nontrivial only if the base field is imperfect and of characteristic 2, 3, or 5. But the theorem is new even over fields of characteristic zero.

One interesting aspect of Theorem 0.1 is that it is relatively easy to show that every E_8-torsor over a field k can be split by some field extensions $K_1, K_2, \ldots$ such that gcd $[K_i : k]$ divides $2^6 \cdot 3^2 \cdot 5$. This follows from the fact that Grothendieck's torsion index of E_8 divides $2^6 \cdot 3^2 \cdot 5$, which is an easy topological calculation [41]. That is, if we think of an E_8-torsor as a homogeneous variety, it is relatively easy to show that every E_8-torsor over a field has a zero-cycle of degree dividing $2^6 \cdot 3^2 \cdot 5$, whereas Theorem 0.1 asserts that every E_8-torsor in fact has a closed point of degree dividing $2^6 \cdot 3^2 \cdot 5$. We can therefore think of Theorem 0.1 as one step toward a positive answer to the following general question in the arithmetic theory of homogeneous varieties.

Question 0.2 *Let k be a field, G a smooth connected linear algebraic group over k, and X a quasi-projective variety which is a homogeneous space for G. Suppose that there is a zero-cycle (not necessarily effective) of degree $d > 0$ on X. Then X has a closed point of degree dividing d, which moreover can be chosen to be etale (that is, separable) over k.*

See section 9 for the history of Question 0.2. We will give a positive answer to Question 0.2 for torsors over the split simply connected exceptional groups G_2, F_4, and E_6, as well as a partial result for E_7, in Theorem 5.1. We need the result for E_7 as part of the proof of Theorem 0.1 about E_8. The case $d = 1$ of Question 0.2 is already known for torsors under any split simple group except E_8, by Bayer-Lenstra [3] and Gille [18], Théorème C.

A big part of the proof of Theorem 0.1 involves an analysis of the subgroup structure of the Weyl group of E_8. The maximal subgroups of the Weyl group of E_8 were listed in the Atlas [14], and the list is reprinted in section 8, but I have not used the list in the proofs. The point is that the Atlas list was compiled using the classification of the finite simple groups, or at least of the simple groups of order less than two million or so, and it seems preferable not to use such a huge body of work when it can be avoided. I have therefore given a direct group-theoretic analysis of the subgroups of the Weyl group of E_8 for the purposes of this paper. The deepest tool used is Brauer's 1940s theory of blocks of defect one [7]. Using the Atlas list of maximal subgroups would shorten the paper, but not too much, because the paper requires a lot of further analysis of the subgroups, not only the maximal ones.

Although the proof does not require computer work, I found the group-theory program GAP convenient for calculations when needed [16]. Also, I would like to thank Jean-Louis Colliot-Thélène, Philippe Gille, and Jan Saxl for helpful discussions. The referee observed that the proof becomes much easier when the base field k is Hilbertian; see section 2 for details.

1 Notation

We follow Atlas notation in that one-letter names such as $S_{2a}(p^b)$, $U_a(p^b)$, and $L_a(p^b)$ are used for the finite groups PSp, PSU, and PSL that are simple for most values of the parameters. An integer a denotes the cyclic group of order a, and a^b denotes the product of b cyclic groups of order a. We write $A.B$ or sometimes AB for any group extension with normal subgroup A and quotient group B, while $A:B$ denotes a split extension. The notation a^{b+c} indicates an extension $a^b.a^c$; in particular, 2_+^{1+2n} denotes the extraspecial group of plus type, the central product of n copies of the dihedral group of order 8. The wreath product $A \wr S_n$ is the obvious split extension $A^n:S_n$. Finally, $[n]$ means an unspecified group of order n.

Much of our analysis is concerned with the action of the Weyl group $W(E_8)$ on the 240 roots which form the E_8 root system. A standard reference is Bourbaki [6]. In fact, we formulate the analysis in terms of the action of the quotient group $W(E_8)/\{\pm 1\}$ on the set R of 120 E_8 roots modulo sign. For calculations, it is useful to think of $W(E_8)/\{\pm 1\}$ as the orthogonal group of the 8-dimensional quadratic form $q = x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ over $\mathbf{F}_2$, and R as the set of vectors v in $(\mathbf{F}_2)^8$ with $q(v) = 1$, as mentioned in Bourbaki, exercise VI.4.1. We use the standard (but non-Atlas) notation $O_8^+(2)$ for this orthogonal group. Also, we write $G_1 = \Omega_8^+(2)$ for the simple subgroup of index 2 in the orthogonal group $O_8^+(2)$. In these terms, the orthogonal group $O_8^+(2)$ is an extension $G_1.2$, and the Weyl group of E_8 is an extension $2.G_1.2$.

2 First steps of the proof

This section explains the general shape of the proof, which is divided into cases depending on the structure of a maximal torus in a given algebraic group of type E_8.

Let E_8 denote the split group of type E_8 over a field k. The set $H^1(k, E_8)$ of isomorphism classes of E_8-torsors over k is naturally in bijection with the set of isomorphism classes of algebraic groups of type E_8 over k, because the group E_8 has no center or outer automorphisms. (To a given E_8-torsor we associate its automorphism group: this is an algebraic group of type E_8, not necessarily isomorphic to the split group E_8.) This explains the equivalence between the two statements of the theorem.

Given any E_8-torsor over k, let L be the corresponding group of type E_8 over k, and let T be a maximal torus in L defined over k. (Such a torus exists, by Chevalley, Rosenlicht, and Grothendieck; a reference is Borel-Springer [5], 7.10.) We want to show that L becomes split over an extension of k of degree dividing $2^6 \cdot 3^2 \cdot 5$. Let Φ be the set of roots of L relative to T, $|\Phi| = 240$, and let $R = \Phi/\{\pm 1\}$, $|R| = 120$. The Galois group $\mathrm{Gal}(k_s/k)$ acts on Φ through the Weyl group $W(E_8)$. We prefer to analyze the action of the Galois group on the smaller set R of roots modulo sign, where it acts through $G_1.2 = W(E_8)/\{\pm 1\}$. Let G be the image of the Galois group in $G_1.2$, which is well-defined up to conjugacy.

Definition 2.1 *A conjugacy class of subgroups G of $G_1.2 = W(E_8)/\{\pm 1\}$ is good if the following holds. Let L be any group of type E_8 over a field k which has a maximal torus T defined over k such that the image of the homomorphism $Gal(k_s/k) \to G_1.2$*

associated to T is conjugate to G. Then L splits over a separable extension of k of degree dividing $2^6 \cdot 3^2 \cdot 5$.

In these terms, Theorem 0.1 will follow from the statement that all subgroups G of $G_1.2$ are good. A big step in that direction is the following.

Lemma 2.2 *Let G be a subgroup of $G_1.2$ which has an orbit on R of order dividing* $120 = 2^3 \cdot 3 \cdot 5$. *Then G is good.*

Proof. We have to show that any group L of type E_8 over a field k with a maximal torus T such that the associated homomorphism of the Galois group $\text{Gal}(k_s/k)$ to $G_1.2$ has image G must split over an extension of k of degree dividing $2^6 \cdot 3^2 \cdot 5$. We are given that some element $\{\pm x\}$ of R has orbit under the Galois group of order dividing $2^3 \cdot 3 \cdot 5$. We can make a separable extension k_1/k of degree equal to this orbit size, hence dividing $2^3 \cdot 3 \cdot 5$, so that $\text{Gal}(k_s/k_1)$ fixes the element $\{\pm x\}$ of R. The roots $\{\pm x\}$ form a subsystem of type A_1 in the E_8 root system. So $\text{Gal}(k_s/k_1)$ also preserves the orthogonal complement of $\{\pm x\}$ in the E_8 root lattice, which is a subsystem of type E_7. Equivalently, the group L over k_1 has a subgroup of type $A_1 \times E_7$ which contains the given torus.

For any closed subgroup H of the split group E_8 over a field k, the set of isomorphism classes of pairs $H' \subset G'$ such that G' is a group of type E_8 over k and H' is a subgroup that becomes conjugate to $H \subset E_8$ over the algebraic closure can be identified with the set $H^1(k, \text{Aut}(H \subset E_8))$ of isomorphism classes of torsors for the group scheme $\text{Aut}(H \subset E_8)$ over k ([43], section 17.6, Theorem). Since E_8 has no outer automorphisms, this group scheme is the normalizer $N_{E_8}(H)$. We observe that the subgroup $H = (SL(2) \times E_7)/\mathbf{Z}/2$ of the split group E_8 is its own normalizer; this follows from the analogous calculation in the Weyl group of E_8, which can be found in Table 11 of Carter [11]. So, in the situation we have been considering, the isomorphism class of L over k_1 is determined by an element of $H^1(k_1, H)$.

Tits showed that any element of $H^1(k_1, H)$ can be killed by an extension of k_1 of degree dividing $2^3 \cdot 3$ ([40], Lemma 3). It is straightforward to check that the extension Tits constructs can be arranged to be separable (see the proof of Theorem 5.1 in this paper, for example). Thus the group L becomes split over a separable extension of k of degree dividing $(2^3 \cdot 3 \cdot 5)(2^3 \cdot 3) = 2^6 \cdot 3^2 \cdot 5$. QED (Lemma 2.2).

In particular, Lemma 2.2 shows that the theorem is true in the "generic" case where G is the whole group $G_1.2$, since then G acts transitively on the set R of order 120. Unfortunately, Theorem 0.1 cannot simply be reduced to this "generic" case. (Such a reduction would only show that every E_8-torsor over a field can be killed by a collection of field extensions K_i such that $\sum [K_i : k] = 2^6 \cdot 3^2 \cdot 5$.) At worst, one might have to prove the theorem separately for all possible subgroups G of $G_1.2$. In fact, I have written the proof to use as little case-by-case checking as I could arrange.

The referee pointed out that when the base field k is Hilbertian, such as any infinite field which is finitely generated over $\mathbf{Q}$ or over $\mathbf{F}_p$ (see Serre [34], 9.5, 9.6), then Theorem 0.1 can be proved much more easily. Indeed, we have just shown that whenever a group L of type E_8 over a field k contains a "generic" torus, meaning one such that that the Galois group of k maps onto the Weyl group of E_8, then L

splits over a separable field extension of degree dividing $2^6{\cdot}3^2{\cdot}5$. Let Y be the variety of maximal tori of L. Then the natural torus in the group $L \times_k k(Y)$ is "generic" in this sense. The variety Y is rational over k, by Grothendieck (see Borel-Springer [5], 7.9). For k Hilbertian, it follows that there is a k-point of Y such that the corresponding torus in L is "generic" in the same sense. Therefore, L is split by a separable extension of degree dividing $2^6{\cdot}3^2{\cdot}5$, proving Theorem 0.1 for k Hilbertian. Unfortunately, this seems not to help in proving Theorem 0.1 for arbitrary fields.

3 Subsystems of E_8

Lemma 3.1 *Any subgroup G of $G_1.2 = W(E_8)/\{\pm 1\}$ which preserves a nontrivial proper subsystem of the E_8 root system is good.*

We will usually just say "a subsystem" to mean a nontrivial proper subsystem. Equivalently, the statement means that any group L of type E_8 over a field k which has a reductive subgroup of maximal rank other than a maximal torus or the whole group must split over a separable extension of k of degree dividing $2^6{\cdot}3^2{\cdot}5$. This was in fact stated by Tits [40], Lemma 4, but proved there only for subsystems other than A_8 and D_8. Here A_8 is easy, but D_8 is not. (Also, Tits did not mention that the field extensions can be chosen to be separable, but that is clear from his proof in the cases he considers.)

More precisely, confirming the statement of Tits's Lemma 4, we will show that a group of type E_8 splits over an extension of degree dividing $2{\cdot}3^2$ if it has a subgroup of type A_8, or of degree dividing 2^6 if it has a subgroup of type D_8.

Proof. To complete Tits's proof, we only need to show that a subgroup $G \subset G_1.2$ which preserves an A_8 or D_8 subsystem of the E_8 root system is good. Equivalently, we have to show that a group L of type E_8 over a field k which has a subgroup of type A_8 or D_8 becomes split over a separable extension of degree dividing $2^6 \cdot 3^2 \cdot 5$. This is clear for A_8, because any group of type A_8 becomes split over a separable extension of degree dividing $2 \cdot 3^2$. Here 2 is to reduce to an inner form of $SL(9)/Z$ and 9 is to split the corresponding central simple algebra [40].

So suppose that we have a group L of type E_8 over a field k which has a subgroup of type D_8. Over the algebraic closure, such a subgroup is the semispin group $Ss(16)$, the quotient of the split simply connected group $Spin(16)$ by a subgroup $\mathbf{Z}/2$ of the center $(\mathbf{Z}/2)^2$ other than the one with quotient $SO(16)$. The subgroup $Ss(16)$ of the split group E_8 is its own normalizer, by the analogous calculation in the Weyl group in Carter [11], Table 11. So the isomorphism class of L over k together with its subgroup of type D_8 is described by an element of $H^1(k, Ss(16))$. We will show that any element of $H^1(k, Ss(16))$ splits in degree dividing 2^6, so in particular in degree dividing $2^6{\cdot}3^2{\cdot}5$. This proof will have the same structure as the whole proof for E_8 in this paper, though on a smaller scale.

Given an element of $H^1(k, Ss(16))$, we can look at the associated inner form M of $Ss(16)$ over k, and find a maximal torus T in M defined over k. Let G be the image of the homomorphism from $\mathrm{Gal}(k_s/k)$ to the Weyl group $W(D_8) = 2^7 : S_8$ associated to T. Consider the action of G on the set S of the 8 coordinate lines $\mathbf{R} \cdot e_i$, in the usual notation for the D_8 root system [6].

First suppose that G has an orbit of order dividing 8 on S. Then we can make a separable extension k_1 of k of degree dividing $2^3 = 8$ to make the Galois group fix an element of S. Equivalently, the Galois group $\mathrm{Gal}(k_s/k_1)$ preserves a D_7 subsystem of D_8. By making a further separable extension k_2/k_1 of degree dividing 2, we can split the 1-dimensional torus which is the centralizer of D_7 in $D_8 = Ss(16)$. What is left is an element of $H^1(k_2, Spin(14))$, which corresponds to a 14-dimensional quadratic form with trivial invariants in $H^1(k_2, \mathbf{Z}/2)$ and in $H^2(k_2, \mathbf{Z}/2)$. Pick a 2-dimensional subspace on which the associated symmetric bilinear form is nondegenerate; then, even in characteristic 2, all we need is a separable extension k_3/k_2 of degree dividing 2 to make this subspace isotropic, in other words to produce a 2-dimensional hyperbolic summand of our 14-dimensional form. What is left is an element of $H^1(k_3, Spin(12))$, or equivalently a 12-dimensional form with trivial invariants in H^1 and H^2. At this point we can apply Pfister's beautiful theorem that every 12-dimensional quadratic form with trivial invariants in H^1 and H^2 splits after a separable extension of degree dividing 2 [28]. (The proof was extended to characteristic 2 by Baeza [2], pp. 130-131.) Thus, if the subgroup $G \subset W(D_8)$ has an orbit on the set S of order dividing 8, then we have shown that the given element of $H^1(k, Ss(16))$ can be killed by some extension of degree dividing $2^3 \cdot 2 \cdot 2 \cdot 2 = 2^6$, as we want.

Otherwise, every orbit of G on S has order not dividing 8. It follows that G has orbit sizes $3 + 5 = 8$ on S. The situation now is much simpler than in the analogous situation for E_8, to be described in Lemma 4.1. Namely, by definition of S, G permutes 3 of the coordinate lines $\mathbf{R} \cdot e_i$ in $\mathbf{R}^8$ and also permutes the remaining 5 coordinate lines. This means that G preserves a $D_3 \times D_5$ subsystem of the D_8 root system, which makes things easy. Clearly G is contained in a subgroup of the form $2^7 : (S_3 \times S_5)$ in the Weyl group of D_8. First, make a extension k_1/k of degree dividing 2 to make the Galois group map into $(2^2 : S_3) \times (2^4 : S_5) = W(D_3 \times D_5)$. Then we have an element of $H^1(k_1, (Spin(6) \times Spin(10))/\mathbf{Z}/4)$, where $\mathbf{Z}/4$ injects into both factors. We use the exact sequence of Galois cohomology [35],

$$H^1(k_1, Spin(10)) \to H^1(k_1, (Spin(6) \times Spin(10))/\mathbf{Z}/4) \to H^1(k_1, Spin(6)/\mathbf{Z}/4).$$

We can make a separable extension k_2/k_1 of degree dividing $2^2 = 4$ to kill the image of our element in $H^1(k_1, Spin(6)/\mathbf{Z}/4) = H^1(k_1, SL(4)/\mathbf{Z}/4)$, so that the given element lifts to $H^1(k_2, Spin(10))$. By another result of Pfister's, every element of $H^1(k_2, Spin(10))$, corresponding to a 10-dimensional quadratic form with trivial invariants in $H^1(k_2, \mathbf{Z}/2)$ and $H^2(k_2, \mathbf{Z}/2)$, can be killed by some separable extension of degree dividing 2 [28]. Again, the proof was extended to characteristic 2 by Baeza [2], pp. 129-130. Thus, on the assumption that G has orbit sizes $3+5 = 8$ on S, we have split the given group of type D_8 by a separable extension of degree dividing $2 \cdot 2^2 \cdot 2 = 2^4$, so in particular dividing 2^6. This completes the proof that every element of $H^1(k, Ss(16))$ is killed by some separable extension of k of degree dividing 2^6. QED (Lemma 3.1)

4 Bad orbit decompositions

Lemma 4.1 *Let $G \subset G_1.2 = W(E_8)/\{\pm 1\}$ be a subgroup such that no orbit of G on R has order dividing 120. Then the orbit sizes of G on R are either*

$$\begin{gathered} 64 + (\textit{multiples of 7 summing to 56}), \\ 50 + (\textit{multiples of 7 summing to 70}), \\ 36 + (\textit{multiples of 7 summing to 84}), \\ 45 + (\textit{multiples of 25 summing to 75}), \;\; \textit{or} \\ (\textit{multiples of 16 summing to 48}) + (\textit{multiples of 9 summing to 72}). \end{gathered}$$

We call these the possible bad orbit decompositions.

Several of these bad orbit decompositions can actually occur, for suitable subgroups of $G_1.2$. The subgroup of $G_1.2$ which preserves a D_8 subsystem of the E_8 root system has orbit sizes $56 + 64$ on the set R of E_8 roots modulo sign, where the orbit of size 56 is the set of D_8 roots modulo sign. Likewise, the subgroup of $G_1.2$ preserving an A_8 subsystem has orbit sizes $36 + 84$ on R. The decomposition $48 + 72$ also occurs for some subgroups of $G_1.2$, which forces some proofs later to be more complex than one would like. (By Lemma 3.1, a subgroup of $G_1.2$ that preserves a subsystem of the E_8 root system must be good. But a subgroup with orbit sizes $48 + 72$ on R cannot preserve a subsystem, so we will have to show that all such subgroups are good by other methods.)

Proof. We know that all orbits have order dividing $|G_1.2| = 2^{13} \cdot 3^5 \cdot 5^2 \cdot 7$, and their sum is 120. It is convenient to compute that a Sylow 7-subgroup $\mathbf{Z}/7 \subset G_1.2$ has only one fixed point in R, so that all its other orbits have size 7. This calculation is made at the beginning of the proof of Lemma 7.1, for example. It follows that for any subgroup G of $G_1.2$ of order a multiple of 7, all orbits of G on R have order a multiple of 7 except for exactly one, which has order $\equiv 1 \pmod 7$. Combining this with the fact that all G-orbits have order dividing $|G_1.2| = 2^{13} \cdot 3^5 \cdot 5^2 \cdot 7$, we find that, if G has any orbits on R of order a multiple of 7, then all orbits of G are multiples of 7 except one which is either 36, 50, or 64. (We are assuming that no orbit of G has order dividing 120.)

Alternatively, suppose that G has no orbits of order a multiple of 7, but that G has an orbit of order a multiple of 5^2. Then G has order a multiple of 5^2, so G contains a Sylow 5-subgroup of $G_1.2$. We compute, for example at the beginning of the proof of Lemma 6.1, that the orbits of a Sylow 5-subgroup of $G_1.2$ on R are 4 of order 25 and 4 of order 5. So all orbits of G on R have order which is a multiple of 5, and which divides $|G|$, while (we assume) not dividing $120 = 2^3 \cdot 3 \cdot 5$. The only way this can happen is for all orbits of G to have order a multiple of 25 except for one orbit of order 45.

Finally, suppose that G has no orbits of order a multiple of 7 or of 5^2. Since all orbits have order not dividing $2^3 \cdot 3 \cdot 5$, they all have orders a multiple of 16 or of 9. The only way this can happen is for G to have some orbits whose orders are multiples of 16, with total size 48, together with some orbits whose orders are multiples of 9, with total size 72. QED (Lemma 4.1)

The bad orbit decomposition $64 + (\text{multiples of 7 summing to 56}) = 120$ caused a lot of trouble in the first version of this paper. But it turns out that it can be handled very quickly, as follows.

Lemma 4.2 *For any subgroup G of $G_1.2$ which has an orbit of order 64 on R, the complementary subset of order 56 in R forms a subsystem of type D_8 in the E_8 root system. So G preserves a D_8 subsystem, and hence G is good.*

Proof. Let X_2 be a Sylow 2-subgroup of G. Since X_2 has odd index in G and 64 is a power of 2, X_2 must act transitively on the G-orbit of order 64. Let Y_2 be a Sylow 2-subgroup of $G_1.2$ containing X_2. Then all orbits of Y_2 on R have size a power of 2 at most 120, hence at most 64, and so the orbit of size 64 for X_2 is also an orbit for the larger group Y_2.

On the other hand, the subgroup $W(D_8)/\{\pm 1\}$ of $W(E_8)/\{\pm 1\} = G_1.2$ which preserves a D_8 subsystem has odd index (namely $3^3 \cdot 5 = 135$). So the Sylow 2-subgroup Y_2 of $G_1.2$ preserves a D_8 subsystem, consisting of 56 roots modulo sign. Since Y_2 has an orbit of size 64 on R, the complement of this orbit must be a D_8 subsystem. Since the original group G preserves the same set of order 64, G also preserves its complement, a D_8 subsystem. So G is good by Lemma 3.1. QED

5 Sharper results for E_7

The proof of Theorem 0.1 began with Lemma 2.2, which rests on Tits's theorem that every E_7-torsor is killed by some field extension of degree dividing 12. In the course of the proof of Theorem 0.1, in Lemma 6.2, we will need more precise information on the group E_7. Namely, we will give a positive answer to the general Question 0.2 for torsors under the simply connected split groups G_2, F_4, E_6 over any field, as well as a partial result for E_7. This is a fairly straightforward consequence of known results on these groups by Tits, Rost, Gille, Garibaldi, and others, although the proof for F_4-torsors in characteristic 2 requires some extra effort. We will use the result for E_7 to show that subgroups of $G_1.2 = W(E_8)/\{\pm 1\}$ whose 3-Sylow subgroup is small enough must be good.

Theorem 5.1 *Let G be a simply connected split group of type G_2, F_4, E_6, or E_7 over a field k. Then any element of $H^1(k, G)$ can be killed by some separable extension of degree dividing* 2, $2{\cdot}3 = 6$, $2{\cdot}3 = 6$, *or* $2^2{\cdot}3 = 12$, *respectively. Moreover, Question 0.2 has a positive answer for G-torsors when G is G_2, F_4, or E_6. For E_7, we have the following partial result on Question 0.2: any E_7-torsor which is killed by an extension of degree prime to 3 can be killed by a separable extension of degree dividing* $2^2 = 4$.

Corollary 5.2 *Any subgroup $G \subset G_1.2$ with an orbit on R of order dividing* $2^3{\cdot}3^2{\cdot}5$ *(not necessarily dividing* $2^3 \cdot 3 \cdot 5 = 120$*) and with* $\text{ord}_3|G| \leq 2$ *is good.*

Proof of Corollary 5.2. The corollary is true without the assumption on the order of G if G has an orbit on R of order dividing $2^3 \cdot 3 \cdot 5$, by Lemma 2.2. So we can assume that G has an orbit of order dividing $2^3 \cdot 3^2 \cdot 5$ but not $2^3 \cdot 3 \cdot 5$. It follows that $\text{ord}_3|G| = 2$. We can make a separable extension k_1/k of degree equal to the size of the given orbit, thus dividing $2^3{\cdot}3^2{\cdot}5$, so that $\text{Gal}(k_s/k_1)$ fixes a point of R. Equivalently, this Galois group preserves a subsystem of type $A_1 \times E_7$ of the E_8 root system. Moreover, since $\text{ord}_3|G| = 2$, the image H of $\text{Gal}(k_s/k_1)$ in $G_1.2$ has $\text{ord}_3|H| = 0$. Using Theorem 5.1, it follows that the subgroup of type $A_1 \times E_7$ in

L over k_1 becomes split over an extension of k_1 of degree dividing 2^3, rather than $2^3 \cdot 3$ as we have in general. Thus L splits over an extension of k of degree dividing $(2^3 \cdot 3^2 \cdot 5)(2^3) = 2^6 \cdot 3^2 \cdot 5$. QED (Corollary 5.2)

Before giving the proof of Theorem 5.1, let us state a consequence of the above result which will be used in the proof of Theorem 0.1.

Corollary 5.3 *Any subgroup $G \subset G_1.2$ with $ord_3|G| \leq 2$ and either $ord_5|G| \leq 1$ or $ord_7|G| = 0$ is good.*

Proof. If G has an orbit on R of order dividing 120, then G is good by Lemma 2.2. Otherwise, the set of orbit sizes of G on R is one of those listed in Lemma 4.1. If G has orbit sizes $64 +$ (multiples of 7 summing to 56), then G is good by Lemma 4.2. By our assumptions on the order of G, G cannot have orbit sizes $50 +$ (multiples of 7 summing to 70). The remaining possibilities for the orbit sizes of G on R are

$$36 + (\text{multiples of 7 summing to 84}),$$
$$45 + (\text{multiples of 25 summing to 75}), \text{ or}$$
$$(\text{multiples of 16 summing to 48}) + (\text{multiples of 9 summing to 72}).$$

In each of these cases, there is an orbit of size $9 \cdot 1$, $9 \cdot 2$, $9 \cdot 4 = 36$, $9 \cdot 5 = 45$, or $9 \cdot 8 = 72$, thus of order 3^2 times a divisor of $2^3 \cdot 5$. By Corollary 5.2, using that $\mathrm{ord}_3|G| \leq 2$, G is good. QED (Corollary 5.3).

Proof of Theorem 5.1. For any field k, any element of $H^1(k, G_2)$ can be killed by a separable extension of k of degree dividing 2. Equivalently, any octonion algebra over a field splits over such an extension. For example, this is clear from the identification of $H^1(k, G_2)$ with the set of isomorphism classes of 3-fold Pfister forms, which works even in characteristic 2: see Serre [36], completing the earlier works of Jacobson [23] and van der Blij and Springer [4]. It follows from the same result that any G_2-torsor over a field which is killed by an extension of odd degree is trivial, in view of Springer's theorem, the analogous statement for quadratic forms [38]. The proof of Springer's theorem was extended to characteristic 2 by Baeza [2], p. 119. This answers Question 0.2 for the split group G_2.

Tits's argument [40] shows that any element of $H^1(k, F_4)$ can be killed by a separable extension of degree dividing 2 followed by a separable extension of degree dividing 3. Moreover, the Rost invariant $H^1(k, F_4) \to H^3(k, \mathbf{Q}/\mathbf{Z}(2))$ has trivial kernel, by Rost [29] and (in characteristic 2 or 3, where the invariant takes values in Kato's modified version of Galois cohomology) Gille [19]. An F_4-torsor which can be killed by a field extension of degree prime to 2 and by an extension of degree prime to 3 clearly has trivial Rost invariant, and hence is trivial; this answers part of Question 0.2 for F_4.

We now solve the remaining cases of Question 0.2 for F_4. It is immediate from Tits's statement, above, that for any F_4-torsor over a field k, the 2-part of the Rost invariant is killed by a separable extension of degree dividing 2 (since the extension of degree dividing 3 that follows is injective on $H^3(\cdot, \mathbf{Z}/2(2))$). Now let X be any F_4-torsor which is killed by a field extension of degree prime to 3. Then the 3-part of the Rost invariant of X is 0, and the 2-part of the Rost invariant can be killed by a separable extension of degree dividing 2, so the above result of Rost and Gille implies that X itself is killed by this separable extension of degree dividing 2.

The last case of Question 0.2 for F_4 is that any F_4-torsor X which is killed by a field extension of odd degree can be killed by a separable extension of degree dividing 3. The hypothesis implies that the 2-part of the Rost invariant of X is 0. For k not of characteristic 2, Rost showed that, since the 2-part of the Rost invariant of X is 0, the 27-dimensional Jordan algebra J corresponding to X is a "first Tits construction" $J = J(A, \lambda)$ for some central simple algebra A of degree 3 over k and some $\lambda \in k^*$ ([25], Proposition 40.5). Then we can split A by a separable extension of k of degree dividing 3, which makes J split.

We need a different argument in characteristic 2, since the above theorem of Rost seems to be unknown in characteristic 2. To begin, let X be any F_4-torsor over a field k of characteristic 2. (Actually, the following argument works in any characteristic other than 3.) The F_4-torsor X is equivalent to the characteristic 2 version of a Jordan algebra, a "cubic norm structure" J of dimension 27 over k, as defined in [25], p. 520. By Petersson and Racine ([25], Theorem 39.19), which uses that the characteristic is not 3, every such algebra is a "second Tits construction" $J = J(B, \tau, u, \nu)$ for some quadratic etale algebra l/k, a central simple algebra B of degree 3 over l with a unitary involution τ, a hermitian element u of B with $N_B(u) = 1$, and an element ν of l^* with $N_{l/k}(\nu) = 1$, that is, $\tau(\nu) = \nu^{-1}$. The element ν determines an element L_ν of $H^1(k, \mu_{3[l]})$, where $\mu_{3[l]}$ denotes the twist of the $\text{Gal}(k_s/k)$-module μ_3 by the homomorphism $\text{Gal}(k_s/k) \to \{\pm 1\}$ corresponding to l/k, by identifying this group with the anti-invariant subgroup of $H^1(l, \mu_3) = l^*/(l^*)^3$. The point is that in this situation, we can define the 3-part of the Rost invariant of an F_4-torsor X as the product $g_2(B, \tau) \cdot L_\nu$, where $g_2(B, \tau)$ is the class of the algebra with involution (B, τ) in $H^2(k, \mu_{3[l]})$ and the product is in $H^3(k, \mu_3^{\otimes 2})$. This is the way Knus-Merkurkev-Rost-Tignol define the 3-part of the Rost invariant in characteristics not 2 or 3 (p. 537), but it also makes sense in characteristic 2. We have to check that this definition in characteristic 2 agrees with the Petersson-Racine definition of the 3-part of the Rost invariant [27], which will imply in particular that it is an invariant of the F_4-torsor X. It suffices to prove this equality after making the quadratic etale extension l/k, since we are considering 3-primary invariants. But over l, J becomes a first Tits construction, and in that case this definition is the same as Petersson-Racine's definition.

The interest of this definition of the 3-primary Rost invariant in characteristic 2 is that any element of $H^1(k, M)$, where M is a Galois module which is isomorphic to $\mathbf{Z}/3$ as an abelian group, can be killed by a separable extension of k of degree dividing 3 (not a Galois extension, in general). Thus, the above definition shows that the 3-part of the Rost invariant of any F_4-torsor in characteristic 2 can be killed by an extension of degree dividing 3. We can now solve the last case of Question 0.2 for F_4-torsors. If X is an F_4-torsor in characteristic 2 which is killed by an extension of odd degree, then the 2-part of the Rost invariant is 0. We have just shown that the 3-part of the Rost invariant can be killed by an extension of degree dividing 3. Since the whole Rost invariant has trivial kernel, the F_4-torsor itself is killed by this extension of degree dividing 3. This completes the solution of Question 0.2 for F_4.

Write E_6 for the simply connected split group of type E_6 over k. Tits's proof in [40] shows that every element of $H^1(k, E_6)$ is killed by some separable extension of degree dividing 6. Moreover, the map $H^1(k, F_4) \to H^1(k, E_6)$ is surjective, and is compatible with the Rost invariants, by Garibaldi [17], 7.2. So Question 0.2 for E_6 follows from the above argument proving it for F_4.

For the results on E_7, we will need similar information about any quasi-split group E_6^2 of type E_6 over k. First, every element of $H^1(k, E_6^2)$ can be killed by a separable extension of degree dividing 12, since we can first split the group E_6^2 by a separable quadratic extension K/k and then split the resulting element of $H^1(K, E_6)$. Next, we need to prove a partial result on Question 0.2 for the quasi-split group E_6^2. Namely, we will show that an element x of $H^1(k, E_6^2)$ which is killed by an extension of degree prime to 3 is killed by a separable extension of degree dividing $2^2 = 4$. Indeed, the assumption implies that the 3-primary Rost invariant of x is zero. This remains true after we make a separable quadratic extension K/k to split the group E_6^2, and then we have an element of $H^1(K, E_6)$ whose 3-primary Rost invariant is zero. It follows that this element is killed by a separable extension of K of degree dividing 2. Thus the given element x of $H^1(k, E_6^2)$ is killed by a separable extension of degree dividing $2^2 = 4$, as claimed.

We now prove the last statement of the lemma, that an element x of $H^1(k, E_7)$ which is killed by an extension of degree prime to 3 can be killed by a separable extension of k of degree dividing $2^2 = 4$. The assumption implies that the 3-primary Rost invariant of x is zero. By Garibaldi [17], Proposition 3.6, x is the image of some element y of $H^1(k, E_6^2)$ for some quasi-split group E_6^2, possibly split, and the Rost invariants are compatible. So y also has 3-primary Rost invariant zero. By the argument above, y is killed by some separable extension of k of degree dividing $2^2 = 4$. So the same goes for x. QED

6 Subgroups with bad orbit decompositions

We now analyze in detail the subgroups of $G_1.2$ with bad orbit decompositions, as defined in Lemma 4.1. For the reasons mentioned in the introduction, we will not use the Atlas list of maximal subgroups of G_1, but the reader may wish to refer to it for convenience. It is given in section 8, along with some extra information about the action of the maximal subgroups on the set R of the 120 E_8 roots modulo sign.

Here are the easiest cases after Lemma 4.2.

Lemma 6.1 *No subgroup G of $G_1.2$ has orbit sizes $50+$(multiples of 7 summing to 70) or $45 +$ (multiples of 25 summing to 75) on R.*

Proof. Suppose that a subgroup G of $G_1.2$ has orbit sizes as above on R. Then 5^2 divides the order of G, so that, after conjugating G, we can assume that G contains a fixed Sylow 5-subgroup $X_5 = (\mathbf{Z}/5)^2$ of $G_1.2$. We can describe the orbits of X_5 on R explicitly, and then the orbits of G will have to be unions of some of the X_5-orbits.

To describe the action of the Sylow 5-subgroup X_5 on R, we think of the 8-dimensional quadratic space $(\mathbf{F}_2)^8$ of plus type (maximal Witt index) as the sum of two 4-dimensional spaces W_1 and W_2 of minus type. Explicitly, we can take W_1 and W_2 to be the $\mathbf{F}_2$-vector space of even subsets of $\{1, \dots, 5\}$, with addition the Boolean sum, and with the quadratic form $q(A) = (1/2)|A| \pmod 2$ and associated bilinear form $(A, B) = |A \cap B| \pmod 2$. (These quadratic forms were described by Griess [20], for example.) Then $X_5 = (\mathbf{Z}/5)^2$ acts by cyclic permutations on each summand of $(\mathbf{F}_2)^8 = W_1 \oplus W_2$. The orbits of X_5 on the set R of vectors $x \in (\mathbf{F}_2)^8$ with $q(x) = 1$ are 4 of size 5, the orbits of $(12, 0)$, $(13, 0)$, $(0, 12)$, and $(0, 13)$, and

4 of size 25, the orbits of $(12, 1234)$, $(13, 1234)$, $(1234, 12)$, and $(1234, 13)$. (Here we write 0 to mean the empty set, because it is the zero element in these vector spaces.) Write A_1, A_2, A_3, A_4 and B_1, B_2, B_3, B_4 for the X_5-orbits of size 5 and 25, respectively.

This construction exhibits an inclusion $S_5 \wr S_2 \subset G_1.2$. In particular, the normalizer of $X_5 \cong (\mathbf{Z}/5)^2$ in $G_1.2$ is at least its normalizer in $S_5 \wr S_2$, which has the form $(5:4) \wr S_2$. We see that the normalizer of X_5 in $G_1.2$ acts transitively on the 4 X_5-orbits B_i of size 25. Also, this normalizer has at most 2 orbits on the set of unordered pairs of X_5-orbits of size 25, the orbit of $B_1 \cup B_2$ (which also contains $B_3 \cup B_4$) and that of $B_2 \cup B_3$.

Suppose that the given group $G \subset G_1.2$ has orbit sizes 45+(multiples of 25 summing to 75) on R. Since G contains X_5, the G-orbit of size 45 must be the union of some X_5-orbit B_i of size 25 with all 4 X_5-orbits A_j of order 5. Since the normalizer of X_5 in $G_1.2$ acts transitively on the 4 sets B_i, we can assume after conjugating G that the G-orbit of size 45 is the union S of B_1 with all 4 sets A_j. Since G is contained in the orthogonal group $G_1.2 = O_8^+(2)$, it preserves the bilinear form on $R \subset (\mathbf{F}_2)^8$. But we compute that an element of B_1 is orthogonal to 21 points in S, while an element of A_1 is orthogonal to 29 points in S. So S cannot be a G-orbit. This contradiction shows that the given orbit sizes cannot occur.

Similarly, suppose that $G \subset G_1.2$ has orbit sizes 50+(multiples of 7 summing to 70) on R. Since G contains X_5, all G-orbits have order a multiple of 5. It follows that the G-orbits besides the one of order 50 have sizes either 70 or $35 + 35$. The G-orbit of order 50 must be the union $B_i \cup B_j$ for some $1 \leq i < j \leq 4$. By the above description of the normalizer of X_5, we can assume after conjugating G that the G-orbit of size 50 is either $B_1 \cup B_2$ or $B_2 \cup B_3$.

Suppose that the G-orbit of size 50 is $B_1 \cup B_2$. We compute that the orthogonal complement of an element of A_1 in $B_1 \cup B_2$ has order 20, while the orthogonal complement of an element of B_3 or B_4 in $B_1 \cup B_2$ has order 26. So there is no G-orbit in R containing both A_1 and a set B_i, which contradicts what we know about the orbit sizes.

Finally, suppose that the G-orbit of size 50 is $B_2 \cup B_3$. We compute that the orthogonal complement of an element of A_1 in $B_2 \cup B_3$ has order 20, while the orthogonal complement of an element of B_1 or B_4 in $B_2 \cup B_3$ has order 30. So, again, there is no G-orbit in R which contains both A_1 and a set B_i, which contradicts what we know about the orbit sizes. QED

The next more difficult orbit decomposition we need to consider is as follows.

Lemma 6.2 *Any subgroup $G \subset G_1.2$ with orbits on R of sizes (multiples of 16 summing to 48)+ (multiples of 9 summing to 72) has $\mathrm{ord}_3|G| \leq 2$ and hence is good.*

Proof. Clearly G has an orbit of size 16 or 48. Neither of these sizes is congruent to 0 or 1 modulo 7. So G cannot contain a Sylow 7-subgroup of $G_1.2$, since such a subgroup acts freely on R outside one point, as we observed in the proof of Lemma 4.1. That is, G has order of the form $2^a 3^b 5^c$. Thus, if we can show that the exponent of 3 in the order of G is at most 2, it will follow that G is good by Corollary 5.3.

Also, we can see easily that the exponent of 5 in the order of G is at most 1. The point is that the group $G_1.2$ acts transitively on the set R of size 120, where 120 is a multiple of 5, whereas G has an orbit of size not a multiple of 5. So the index of G in $G_1.2$ must be a multiple of 5. Since $G_1.2$ has order $2^{13}\cdot 3^5\cdot 5^2\cdot 7$, it follows that the exponent of 5 in the order of G is at most 1.

It seems natural to use Aschbacher's theorem on the maximal subgroups of the classical groups over finite fields, since the proof is elementary [1]. Namely, the theorem says that any subgroup of a classical group such as the orthogonal group $G_1.2 = O_8^+(2)$ is either contained in one of a list of "classical" proper subgroups, to be described in Lemma 6.4, or else is almost simple and absolutely irreducible on $(\mathbf{F}_2)^8$. (By definition, a group G is almost simple if there is a nonabelian simple group Y such that $Y \subset G \subset \text{Aut}(Y)$.) So an important step in this proof will be to analyze the case where G is almost simple. In fact, any subgroup G of $G_1.2$ which satisfies the hypotheses of Lemma 6.2 must be solvable, but we will not carry the argument to that point. We will merely assume now that G is almost simple, and derive a contradiction. We know that the simple subgroup Y of G has order $2^a\cdot 3^b\cdot 5$, where the exponent of 5 is 1 rather than 0 by Burnside's theorem that groups of order $p^a\cdot q^b$ are solvable.

Brauer showed in 1968 that any simple group of order $2^a\cdot 3^b\cdot 5$ is isomorphic to A_5 of order $2^2\cdot 3\cdot 5 = 60$, A_6 of order $2^3\cdot 3^2\cdot 5 = 360$, or $U_4(2) \cong \Omega_5(3)$ of order $2^6\cdot 3^4\cdot 5 = 25,920$ [8]. We prefer not to use this classification, but only the first lemma in Brauer's paper, which follows easily from his 1940s work on block theory: if G is a simple group of order $p^a\cdot q^b\cdot r$ with p, q, r distinct primes, then an r-Sylow subgroup of G is its own centralizer in G.

That is enough to show that the simple subgroup Y of the almost simple group G inside $G_1.2$ cannot have an orbit on R of order 48. Indeed, by Brauer's lemma, a Sylow 5-subgroup $P \cong \mathbf{Z}/5$ in Y is its own centralizer, so the normalizer has order $5c$ for some c dividing 4. If H is any subgroup of Y of index not a multiple of 5, then H is conjugate to a subgroup containing the Sylow 5-subgroup P of Y, and the normalizer of P in H has order $5d$ for some d dividing c. By Sylow's theorem that $[Y : N_Y(P)] \equiv 1 \pmod{p}$, applied to Y and H, it follows that the index of H in Y is congruent mod 5 to c/d, thus to 1, 2, or 4. Thus Y has no subgroup of index $\equiv 3 \pmod{5}$. In particular, Y cannot have an orbit in R of order 48.

With a little more effort, let us show that Y does not have an orbit in R of size 24 on which it acts primitively. We will use the following lemma from Wielandt's book [44]:

Lemma 6.3 *Let G be a primitive permutation group of degree n. Let $H \subset G$ be the stabilizer of a point, with orbit sizes $n = 1 + n_2 + \cdots + n_r$, $1 \leq n_2 \leq \cdots \leq n_r$. If $n_r > 1$, then $(n_i, n_r) \neq 1$ for all $2 \leq i \leq r$.*

Now suppose that the simple group Y has an orbit S in R of size 24 on which it acts primitively. Let H be the stabilizer in Y of a point in S. Since $24 \equiv 4 \pmod{5}$, the argument using Sylow's theorem shows that all subgroups of H have index congruent to 0 or 1 modulo 5. Since H has order $2^c\cdot 3^d\cdot 5$, the H-orbit sizes not a multiple of 5 must be 1, 6, or 16. If there is an H-orbit of size 16, then this must be the biggest H-orbit on S. By Lemma 6.3, all H-orbit sizes in S except the one H-orbit of size 1 have a common factor with 16, thus are even, which is a contradiction since S has size 24. We know there is only one H-orbit on S of size 1 because the Y-action on S is primitive, so the only possible H-orbit sizes on 24 are $24 = 1 + 5 + 6 + 6 + 6$. This also contradicts Lemma 6.3, since 5 and 6 are relatively prime. Thus we have shown that Y does not have an orbit in R of size 24 on which it acts primitively.

We know that the almost simple group G has an orbit of size 16 or 48. Choose one such orbit. Since the simple group Y is a normal subgroup of G, its orbits on the given G-orbit are permuted transitively by G; in particular, they all have the same size. This size is greater than 1, that is, Y does not act trivially on the G-orbit of size 16 or 48. To see that, we use that an element of order 5 in $G_1.2$, which Y must contain, fixes at most 10 points in R, as we see from the action of the Sylow 5-subgroup $(\mathbf{Z}/5)^2$ of G_1 on R, which is described in the proof of Lemma 6.1. So the simple group Y is a subgroup of S_n for some divisor n of 48 between 2 and 48. But we have shown that Y does not have an orbit of size 48, and that if it has an orbit of size 24 then it does not act primitively. It follows that the simple group Y, of order $2^a \cdot 3^b \cdot 5$, is isomorphic to a primitive subgroup of S_d for some divisor d of 48 between 2 and 16. It seems reasonable to use the list of primitive subgroups of S_n for $n \leq 20$ worked out in the period 1893–1912 by F. N. Cole, G. A. Miller, and others (see Sims [37] for a table of the results). We find that $d = 6$ and Y is isomorphic to A_5 or A_6.

The outer automorphism group of Y has order 2 for $Y \cong A_5$ or 4 for $Y \cong A_6$. Since $Y \subset G \subset \mathrm{Aut}(Y)$, the exponent of 2 in the order of G is at most 3 if $Y \cong A_5$, contradicting the fact that G has an orbit in R of size 16 or 48. So $Y \cong A_6$. By the above calculation that $d = 6$, a Y-orbit inside the given G-orbit must have order 6, 12, or 24 (not 48, as we have shown), and the stabilizer of a point must be contained in an index-6 subgroup of A_6. But an index-6 subgroup of A_6 is isomorphic to A_5, which has no subgroup of index 2 or 4. So the Y-orbits inside the given G-orbit must have size 6. Since the outer automorphism group of Y has order only 4, the G-orbit containing this Y-orbit has order dividing 24, which contradicts the fact that this G-orbit has size 16 or 48. Thus we have reached a contradiction from the assumption that the group G with an orbit of size 16 or 48 on R is almost simple.

We now apply Aschbacher's theorem, in the case of the orthogonal group $G_1.2 = O_8^+(2)$. The statement is as follows. Here I have followed Kleidman and Liebeck's Table 3.5.E [24], p. 73, for a detailed description of the subgroups involved. In particular, that table shows that some of the subgroups in Aschbacher's list are contained in others, and therefore can be omitted from the following statement.

Lemma 6.4 *Every subgroup G of the orthogonal group $G_1.2 = O_8^+(2)$ is either almost simple and absolutely irreducible on $(\mathbf{F}_2)^8$, or is conjugate to a subgroup of one of the following subgroups, which we call the classical subgroups of $G_1.2$.*

(1) Reducible subgroups: the stabilizer P_i of an i-dimensional isotropic subspace of $(\mathbf{F}_2)^8$, for $i = 1$, 2, or 4, where $P_1 \cong 2^6{:}S_8$, $P_2 \cong 2_+^{1+8}{:}(S_3)^3.2$, and $P_4 \cong 2^6{:}A_8$; the stabilizer $O_2^-(2) \times O_6^-(2)$ of a 2-dimensional nondegenerate subspace of minus type, which is isomorphic to $(3 \times U_4(2)){:}[2^2]$; and the stabilizer $S_6(2).2$ of a non-isotropic line.

(2) Imprimitive subgroups: $O_4^-(2) \wr S_2$, which is isomorphic to $(A_5)^2{:}[2^3]$, $O_2^-(2) \wr S_4$, which is isomorphic to $S_3 \wr S_4$, and $L_4(2).2$, which is isomorphic to S_8.

(3) Non-absolutely irreducible subgroups: $(3 \times U_4(2)){:}2$ and $O_4^+(4).2$, which is isomorphic to $(A_5)^2{:}2^2$.

It may be helpful to compare these "classical" subgroups of $G_1.2$ with the list of all maximal subgroups of G_1 given in section 8.

Several of these subgroups cannot contain the given group G, with orbit sizes (multiples of 16 summing to 48) + (multiples of 9 summing to 72) on R, because they have a small orbit on R. Namely, $P_1 \cong 2^6 : S_8$, which we can also view as the stabilizer in $G_1.2$ of a D_8 subsystem of the E_8 root system, has orbit sizes $56+64$ on R, which implies with some care that G cannot be a subgroup of P_1. The next subgroup $P_2 \cong 2_+^{1+8}:(S_3)^3.2$, which is the stabilizer of a $(D_4)^2$ subsystem, has orbit sizes $24+96$, so cannot contain G. The group $O_2^-(2) \times O_6^-(2)$ is the stabilizer of an $A_2 \times E_6$ subsystem, and has orbit sizes $3 + 36 + 81$, so cannot contain G. The group $S_6(2).2$ is the stabilizer of an $A_1 \times E_7$ subsystem, and has orbit sizes $1 + 63 + 56$ on R, so does not contain G. The group $O_4^-(2) \wr S_2$ is the stabilizer of an $(A_4)^2$ subsystem, and has orbit sizes $20+100$, so does not contain G. The group $O_2^-(2) \wr S_4$ is the stabilizer of an $(A_2)^4$ subsystem, and has orbit sizes $12 + 108$ on R, so does not contain G.

The remaining classical subgroups act transitively on the set R of order 120. Several of them have 3-adic order at most 2, so that Lemma 6.2 is proved if G is contained in one of those subgroups. This applies to the subgroups $P_4 \cong 2^6 : A_8$, $L_4(2).2 \cong S_8$, and $O_4^+(4).2 \cong (A_5)^2 : 2^2$. The only remaining possibility is that G is contained in the classical subgroup $(3 \times U_4(2)):2$, which has order $2^7 {\cdot} 3^5 {\cdot} 5$. Since this subgroup acts transitively on R, of size 120, while its subgroup G has some orbit sizes which are not multiples of 5, the index of G in $(3 \times U_4(2)):2$ is a multiple of 5. That means that G has order $2^a {\cdot} 3^b$ and hence is solvable.

We can assume that the representation of G on $(\mathbf{F}_2)^8$ is irreducible and primitive; otherwise G would be contained in one of the classical subgroups of types (1) or (2) in $O_8^+(2)$, and we would already know that $\mathrm{ord}_3|G| \leq 2$. By Jordan and Suprunenko's analysis of solvable linear groups [39], since G is a primitive solvable subgroup of $GL_8(2)$, it must be contained in the normalizer of $\mathbf{F}_{2^8}^*$ in $GL_8(2)$, which is isomorphic to $255:8$. This group has $\mathrm{ord}_3|G| = 1$, and so we have proved that $\mathrm{ord}_3|G| \leq 2$ in all cases. QED

7 Orbit size 36

This section analyzes the bad orbit decomposition which turns out to be the hardest. This will complete the proof of Theorem 0.1, in view of Lemma 4.1.

Lemma 7.1 *For any subgroup G of $G_1.2$ with orbits on R of sizes*

$$36 + (\textit{multiples of 7 summing to 84}),$$

the G-orbit of order 36 is an A_8 subsystem of the E_8 root system. It follows that G is good.

Proof. Once we know that G preserves an A_8 subsystem, it is good by Lemma 3.1. So the problem is to show that the G-orbit of size 36 is an A_8 subsystem. It suffices to prove this when G is contained in G_1. If not, then $G \cap G_1$ is a subgroup of index 2 in G, so its orbits on R have the form either $36 +$ (multiples of 7) again or $18 + 18 +$ (multiples of 7). But the latter case cannot occur, by Lemma 4.1. So $G \cap G_1$ also satisfies the hypothesis of the lemma. Thus we can assume that $G \subset G_1$ from now on.

Another easy initial observation is that the exponent of 5 in the order of G is at most 1. Indeed, the group $G_1.2$ acts transitively on the set R of size 120, whereas G has an orbit on R of size not a multiple of 5, so the index of G in $G_1.2$ must be a multiple of 5. That is, the exponent of 5 in the order of G is at most 1.

It is clear that 7 divides the order of G, so that G contains a Sylow 7-subgroup $X_7 \cong \mathbf{Z}/7 \subset G_1$. We compute that the normalizer of this subgroup in G_1 is the affine group $7{:}6$. The proof of Lemma 7.1 will be divided into two parts, depending on how big the normalizer of X_7 in G is. The bigger this normalizer is, the fewer possibilities there are for what the G-orbit of size 36 can be, and we can look at all the possibilities. On the other hand, the smaller the normalizer of X_7 in G, the more the structure of G as an abstract group is restricted, as we will see later using Brauer's character theory. When the normalizer of X_7 in G is as big as possible, namely $7 : 6$, Feit [15] was able to use Brauer's character theory to describe the possible simple subgroups G of G_1, but only with the aid of computer calculations which are not described in detail.

There is some choice in where to draw the line between the two parts of the proof. I have decided to use the elementary approach, looking at the possible G-orbits in R, when G contains the subgroup $7{:}3$ of index 2 in the normalizer $7{:}6$ of G in G_1. Thus, under that assumption, we will now prove that the G-orbit of size 36 is an A_8 subsystem of the E_8 root system.

We need to describe the action of the Sylow 7-subgroup $X_7 \cong \mathbf{Z}/7$ of G_1 on R explicitly. Think of $(\mathbf{F}_2)^8$ as the set of even subsets of $\{1, \ldots, 9\}$, with addition the Boolean sum, and with the quadratic form $q(A) = (1/2)|A| \pmod 2$ and associated bilinear form $(A, B) = |A \cap B| \pmod 2$, as in the proof of Lemma 6.1; this quadratic form is indeed the 8-dimensional form of plus type over $\mathbf{F}_2$. This description exhibits an inclusion of the symmetric group S_9 into the orthogonal group $G_1.2 = O_8^+(2)$. Then $X_7 \cong \mathbf{Z}/7$ acts on $(\mathbf{F}_2)^8$ by cyclically permuting the numbers $\{1, \ldots, 7\}$. We see that X_7 acts freely on the set R of 120 vectors $x \in (\mathbf{F}_2)^8$ with $q(x) = 1$ outside the single point $89 \in R$. Also, the whole symmetric group S_9 has 2 orbits on R, the 36 2-element subsets of $\{1, \ldots, 9\}$ and the 84 6-element subsets of $\{1, \ldots, 9\}$. In terms of root systems, the S_9-orbit of size 36 is an A_8 subsystem of the E_8 root system R.

The normalizer $7{:}6$ of X_7 in G_1 is contained in $A_9 \subset G_1$ (and also in $S_7 \times S_2 \subset S_9$). Its subgroup $7 : 3$ of index 2 can be described as the normalizer of X_7 in the alternating group $A_7 \subset A_9 \subset G_1$.

Now let $G \subset G_1$ be any subgroup which contains $7{:}3 \subset G_1$, and which has orbit sizes $36 +$ (multiples of 7 summing to 84) on R. Then the G-orbit S of size 36 must be a union of some of the orbits of $7{:}3$. We will therefore list the orbits $T_1, \ldots, T_{10}$ of the group $7{:}3$ on the set R, using the notation above for elements of R. The left column of the table shows which pairs of orbits of $7{:}3$ are switched by the action of $7{:}6 \subset A_9$.

	Orbit	Element of orbit	Size of orbit
	T_1	89	1
	T_2	123456	7
⌈	T_3	18	7
⌊	T_4	19	7
⌈	T_5	123589	7
⌊	T_6	123689	7
	T_7	12	21
	T_8	123489	21
⌈	T_9	123458	21
⌊	T_{10}	123459	21

For each of these orbits T_i in R, the ith row of the following table lists the number of elements of each of the sets T_j which are orthogonal to a given element of T_i. Here we are viewing R as the set of non-isotropic vectors in $(\mathbf{F}_2)^8$. This table will be needed in the following calculation. (Or rather, part of it will; it would be enough to compute the first 5 rows of this table, or even less, by waiting to compute entries in this table until they are needed in the following calculation.)

	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}
T_1	1	7	0	0	7	7	21	21	0	0
T_2	1	1	1	1	3	3	15	9	15	15
T_3	0	1	1	6	4	4	15	12	15	6
T_4	0	1	6	1	4	4	15	12	6	15
T_5	1	3	4	4	7	3	9	9	12	12
T_6	1	3	4	4	3	7	9	9	12	12
T_7	1	5	5	5	3	3	9	13	12	12
T_8	1	3	4	4	3	3	9	13	12	12
T_9	0	5	5	2	4	4	11	12	11	10
T_{10}	0	5	2	5	4	4	11	12	10	11

The union of $7{:}3$-orbits $T_1 \cup T_3 \cup T_4 \cup T_7$ in R, of size $1+7+7+21 = 36$, is the A_8 subsystem of the E_8 root system described earlier. We will now show that the G-orbit S of size 36 can only be that set. Apart from the set $T_1 \cup T_3 \cup T_4 \cup T_7$, there are 40 unions of $7{:}3$-orbits with total order 36. The quotient group $(7{:}6)/(7{:}3) \cong \mathbf{Z}/2$ acts on this set of 40 subsets of R, with 22 orbits. We now list 22 subsets of R, choosing one out of each orbit under conjugation by the bigger group $7{:}6$. To prove that each of these sets S cannot be an orbit of a subgroup G of the orthogonal group $G_1.2 = O_8^+(2)$, we will exhibit two elements of S which are orthogonal to *different* numbers of elements of S. In the following table, say in the first row, "1567" denotes the subset $S = T_1 \cup T_5 \cup T_6 \cup T_7$ of order $1 + 7 + 7 + 21 = 36$ in R, and the row indicates that an element of T_1 is orthogonal to 36 elements of S, while an element of T_5 is orthogonal to 20 elements of S. These numbers are easy to check using the previous table.

1567	1	36	5	20
1348	1	22	3	19
1568	1	36	5	20
123456	1	22	2	10
1237	1	29	2	18
1257	1	36	2	20
1357	1	29	3	20
1367	1	29	3	20
1238	1	29	2	12
1258	1	36	2	14
1358	1	29	3	17
1368	1	29	3	17
1239	1	8	2	18
1249	1	8	2	18
1259	1	15	2	20
1269	1	15	2	20
1349	1	1	3	22
1359	1	8	3	20
1369	1	8	3	20
1459	1	8	3	20
1469	1	8	4	11
1569	1	15	5	23

Thus we have shown that the G-orbit of size 36 in R must be an A_8 subsystem of the E_8 root system when G contains the group $7:3$. For G containing only a smaller subgroup of the normalizer $7:6$ of a Sylow 7-subgroup in G_1, the number of cases to be considered in a similar approach would grow enough that the work would require a computer. We therefore turn to a more theoretical approach based on Aschbacher's theorem (Lemma 6.4). In this method, the main problem is to prove Lemma 7.1 when G is almost simple and absolutely irreducible on $(\mathbf{F}_2)^8$. We now assume that. Thus there is a simple group Y such that $Y \subset G \subset \mathrm{Aut}(Y)$. Since the order of G has the form $2^a\cdot 3^b\cdot 5^c\cdot 7^d$ with $c, d \leq 1$, the order of Y has the same form.

We know that G contains a Sylow 7-subgroup $X_7 \cong \mathbf{Z}/7$ of G_1. The subgroup X_7 is its own centralizer in G_1, and therefore also in G. A first step is to show that 7 divides the order of the simple subgroup Y, rather than the order of G/Y. This has various proofs, depending on how much group theory we want to use; here is a proof using the old (1893–1912) classification of primitive groups of degree at most 20. Suppose that 7 divides the order of G/Y. Let H be the inverse image in G of a Sylow 7-subgroup, isomorphic to $\mathbf{Z}/7$, in G/Y. Then the orbits of H on the complement in R of the G-orbit of size 36 have orders which are multiples of 7 summing to 84. The simple subgroup Y must act nontrivially on one of these orbits, since the subset of R fixed by a nontrivial element of G_1, being the intersection of R with a proper linear subspace of $(\mathbf{F}_2)^8$, must have size less than 84. Choose an H-orbit of size $7a$ on which Y acts nontrivially, where we have $a \leq 12$. Then the stabilizer of a point is a subgroup of index $7a$ in H, hence a subgroup of index a in Y. Since Y acts nontrivially on this orbit, this stabilizer must be a proper subgroup of Y, of index at most 12. It follows that the simple group Y is a primitive subgroup of S_n for some $n \leq 12$. Also, we know that the order of Y is divisible only by the primes 2, 3, and 5. By the list of primitive groups of degrees at most 12 [37], the simple group Y must be isomorphic to A_5 or A_6. In these cases, the outer automorphism group of Y has order 2 or 4, contradicting the fact that 7 divides the order of G. It follows that, in fact, 7 must divide the order of the simple group Y.

At this point, we know that the order of the simple group Y has the form $2^a 3^b 5^c 7$ with $c \leq 1$. The Sylow 7-subgroup $X_7 \cong \mathbf{Z}/7$ in Y acts freely on R outside one point, since it is a Sylow 7-subgroup of G_1. In particular, we deduce a weak result which we will need later: Y does not act trivially on the G-orbit of size 36.

The normalizer of X_7 in Y is a subgroup of the normalizer $7{:}6$ of X_7 in G_1, so it is isomorphic to one of $7{:}6$, $7{:}3$, $7{:}2$, or 7. We can assume that $N_Y(X_7)$ is not of the form $7{:}3$ or $7{:}6$, since we have already proved Lemma 7.1 in those cases. Also, $N_Y(X_7)$ cannot be equal to X_7; by Burnside [10], p. 327, that would imply that the Sylow subgroup X_7 had a normal p-complement in Y, contradicting simplicity of Y. It follows that $N_Y(7)$ has the form $7{:}2$.

At this point, we bring in our most advanced tool, Brauer's 1940s theory of groups Y whose order is divisible by a prime p to the first order [7]. This method is more powerful when the normalizer of a Sylow p-subgroup $X_p \cong \mathbf{Z}/p$ is small. Given a prime number p which divides the order of G to the first order, Brauer's theory divides the irreducible complex characters of Y into blocks. Every block consists either of a single character of degree a multiple of p or of some set of characters of degree not a multiple of p. If the Sylow subgroup X_p is its own centralizer in Y, as we know for the simple group Y we have been considering (with $p = 7$), then the principal block $B_0(p)$ (the one containing the trivial character 1) is the only block containing characters of degree not a multiple of p. Without any assumption on the centralizer, the quotient $N_Y(X_p)/C_Y(X_p)$ has order m for some m dividing $p - 1$. Then the principal block consists of m "non-exceptional" characters $\chi_1 = 1, \chi_2, \ldots, \chi_m$ and $t := (p-1)/m$ "exceptional" characters $\chi_0^{(j)}$, $j = 1, \ldots, t$. The exceptional characters all have the same degree x_0. There are signs $\delta_i = \pm 1$, $i = 1, \ldots, m$, such that the degrees x_i of the non-exceptional characters χ_i satisfy $\delta_i x_i \equiv 1 \pmod{p}$. Also, there is a sign $\delta_0 = \pm 1$ such that $\delta_0 x_0 \equiv -m \pmod{p}$. The following powerful "degree equation" holds:

$$\sum_{i=1}^{m} \delta_i x_i + \delta_0 x_0 = 0.$$

Finally, suppose that a degree appears in $B_0(p)$ which is a power of another prime r and which is greater than 1. Then the highest power of r which divides the order of G divides the sum of some set of the integers $\delta_i x_i$ with $0 \leq i \leq m$ which are multiples of r, including the given power of r, by [9], p. 94.

We apply these results to our simple group $Y \subset G$, with $p = 7$. As explained above, we have $N_Y(7) \cong 7{:}2$. So the principal block $B_0(7)$ of Y consists of 2 non-exceptional characters $\chi_1 = 1$ and χ_2, of degrees $x_1 = 1$ and x_2, and 3 exceptional characters $\chi_0^{(j)}$ of some degree x_0. There are signs δ_2 and δ_0 such that $\delta_2 x_2 \equiv 1 \pmod{7}$ and $\delta_0 x_0 \equiv -2 \equiv 5 \pmod{7}$, and we have the degree equation

$$1 + \delta_2 x_2 + \delta_0 x_0 = 0.$$

Moreover, the degree of each irreducible character divides the order of the group Y. These characters are in the principal block, so their degrees are also prime to 7. It follows that the degrees x_2 and x_0 have the form $2^a \cdot 3^b \cdot 5^c$ with $c \leq 1$. It is elementary to check (see Lehmer [26] for a much more general result) that the only solutions to this diophantine problem are $(x_2, x_0) = (1,2)$, $(6,5)$, $(8,9)$, or $(15,16)$.

The case $(x_2, x_0) = (1,2)$ cannot occur: since Y is simple, it cannot have another 1-dimensional character besides the trivial character. If $(x_2, x_0) = (6,5)$, then Y has a unique 5-dimensional character. It follows that all algebraic conjugates of this character are equal; that is, this character must take rational values. By Schur [33], a finite subgroup of $GL_n(\mathbf{C})$ such that the associated character takes rational values has order divisible only by primes at most $n+1$. This is a contradiction in the case at hand, since 7 divides the order of Y.

If $(x_2, x_0) = (8,9)$, then the above result of Brauer's on the group order implies that Y has order $2^3{\cdot}3^2{\cdot}5^c{\cdot}7$ for some $c \leq 1$. By Sylow's theorem that $[Y : N_Y(7)] \equiv 1 \pmod 7$, since $N_Y(7) \cong 7{:}2$, Y must have order $2^3{\cdot}3^2{\cdot}7 = 504$. By Cole [12], a simple group Y of this order is isomorphic to $L_2(8) = PGL(2, \mathbf{F}_8)$. Since this group has trivial Schur multiplier, it lifts to a subgroup of $2.G_1 = W(E_8)' \subset GL(8, \mathbf{Q})$. Since Y is absolutely irreducible on $(\mathbf{F}_2)^8$, this lifted 8-dimensional representation of Y over $\mathbf{Q}$ is also absolutely irreducible. The character degrees we have computed imply that this is the unique 8-dimensional irreducible representation of Y. In particular, it must be isomorphic to the permutation character of $L_2(8)$ acting on $\mathbf{P}^1(\mathbf{F}_8)$ minus the trivial character. So the lifted 8-dimensional representation of Y factors through the symmetric group $S_9 \subset GL(8, \mathbf{Q})$. Reducing modulo 2, we find that the given representation of Y on $(\mathbf{F}_2)^8$ also factors through the standard representation of S_9 on $(\mathbf{F}_2)^8$. Since Y acts irreducibly on $(\mathbf{F}_2)^8$, it is elementary to check that it preserves at most one nonzero quadratic form on $(\mathbf{F}_2)^8$. So $Y \subset G_1.2 = O_8^+(2)$ is conjugate in $O_8^+(2)$ to a subgroup of $S_9 \subset O_8^+(2)$. That is, Y preserves an A_8 subsystem of the E_8 root system. Since $Y = PGL(2, \mathbf{F}_8)$ is a triply transitive subgroup of S_9, we can check from the explicit description earlier of the S_9-orbit S of size 36 in R that Y acts transitively on S. The other Y-orbits on R must have order a multiple of 7, and so the almost simple group G which normalizes Y must preserve the set S, which is an A_8 subsystem. Lemma 7.1 is proved in this case, where $(x_2, x_0) = (8,9)$.

Next, suppose $(x_2, x_0) = (15,16)$. We derive a contradiction in this case. Since Y has a character of degree 15, 5 divides the order of Y, in fact exactly once because we know that $\mathrm{ord}_5|Y| \leq 1$. The characters of Y have degrees 1, 15, 16, and possibly some multiples of 7. Consider the principal 5-block. It consists of 1, possibly the character of degree 16, and possibly some characters of degree a multiple of 7. There is no way the degree equation for $B_0(5)$ can be satisfied, as we see by looking at it modulo 7.

That completes the proof of Lemma 7.1 for all almost simple groups G in G_1. By Aschbacher's theorem, Lemma 6.4, it remains to prove the lemma for subgroups G of one of the classical subgroups of $G_1.2$.

Several of the classical subgroups of $G_1.2$ cannot contain a group G with orbit sizes $36 +$ (multiples of 7 summing to 84) because they have a small orbit on R. This applies to the parabolic subgroup P_2, with orbit sizes $24 + 96 = 120$ on R, to $O_2^-(2) \times O_6^-(2)$, with orbit sizes $3 + 36 + 81$, to $S_6(2).2$, with orbit sizes $1 + 63 + 56$, to $O_4^-(2) \wr S_2$, with orbits $20 + 100$, and to $O_2^-(2) \wr S_4$, with orbits $12 + 108$.

Some of the other classical subgroups of $G_1.2$ have order not a multiple of 7, so they cannot contain G. This applies to $(3 \times U_4(2)) : 2$, of order $2^7 \cdot 3^5 \cdot 5$, and $O_4^+(4).2 \cong (A_5)^2 : 2^2$, of order $2^6 \cdot 3^2 \cdot 5^2$.

So G must be contained in one of the remaining classical subgroups from the list in Lemma 6.4: $P_1 \cong 2^6 : S_8$, $P_4 \cong 2^6 : A_8$, or $L_4(2).2 \cong S_8$. These groups all have $\mathrm{ord}_3 \leq 2$ and $\mathrm{ord}_5 \leq 1$, so it is clear that G is good in these cases by Corollary 5.3. But it is not hard to prove the stronger statement of Lemma 7.1, that G preserves an A_8 subsystem.

To prove that, consider the image Q of G in S_8, which all three classical groups we are considering map to. The kernel is a 2-group. Since G has an orbit on R of size 36 and another orbit of size a multiple of 7, the order of G is a multiple of $3^2 \cdot 7$, and so is the order of $Q \subset S_8$. By the list of primitive permutation groups of degrees at most 8 [37], it follows that the image of Q in S_8 contains A_7. In particular, Q contains the normalizer of a Sylow 7-subgroup in A_7, which is isomorphic to $7 : 3$. Since G maps onto Q with kernel a 2-group, the subgroup $7 : 3 \subset Q$ lifts to a subgroup of G. Thus the normalizer of a Sylow 7-subgroup in G is at least $7 : 3$. It follows from the first part of this proof that the G-orbit of size 36 is an A_8 subsystem. Lemma 7.1 is proved. QED

Lemmas 2.2, 4.1, 4.2, 6.1, 6.2, and 7.1 together imply that all subgroups of $G_1.2 = W(E_8)/\{\pm 1\}$ are good. As explained in section 2, this statement implies Theorem 0.1. QED

8 Maximal subgroups of G_1

Although we have proved Theorem 0.1 without using the Atlas table of maximal subgroups of $G_1 = \Omega_8^+(\mathbf{F}_2) = W(E_8)'/\{\pm 1\}$, this table does help to see how the various subgroups we encountered fit together, so we print it here [14]. See section 1 for the notation used in this table. I have added some extra information to the Atlas table: the orbit sizes of each group on the set R (of the E_8 roots modulo sign, or equivalently of the non-isotropic vectors in $(\mathbf{F}_2)^8$), and the subsystem of the E_8 root system preserved by a given group, if any.

Conjugacy classes of maximal subgroups of $G_1 = \Omega_8^+(2) = W(E_8)'/\{\pm 1\}$

$[G_1 : H_i]$	$\lvert H_i\rvert$		Orbits on R	Description	Subsystem
$120 = 2^3{\cdot}3{\cdot}5$	$2^9{\cdot}3^4{\cdot}5{\cdot}7$	H_1	$1+63+56$	$S_6(2)$	$A_1 \times E_7$
$120 = 2^3{\cdot}3{\cdot}5$	$2^9{\cdot}3^4{\cdot}5{\cdot}7$	H_2	120	$S_6(2)$	
$120 = 2^3{\cdot}3{\cdot}5$	$2^9{\cdot}3^4{\cdot}5{\cdot}7$	H_3	120	$S_6(2)$	
$135 = 3^3{\cdot}5$	$2^{12}{\cdot}3^2{\cdot}5{\cdot}7$	H_4	$56+64$	$2^6 : A_8$	D_8
$135 = 3^3{\cdot}5$	$2^{12}{\cdot}3^2{\cdot}5{\cdot}7$	H_5	120	$2^6 : A_8$	
$135 = 3^3{\cdot}5$	$2^{12}{\cdot}3^2{\cdot}5{\cdot}7$	H_6	120	$2^6 : A_8$	
$960 = 2^6{\cdot}3{\cdot}5$	$2^6{\cdot}3^4{\cdot}5{\cdot}7$	H_7	$36+84$	A_9	A_8
$960 = 2^6{\cdot}3{\cdot}5$	$2^6{\cdot}3^4{\cdot}5{\cdot}7$	H_8	120	A_9	
$960 = 2^6{\cdot}3{\cdot}5$	$2^6{\cdot}3^4{\cdot}5{\cdot}7$	H_9	120	A_9	
$1120 = 2^5{\cdot}5{\cdot}7$	$2^7{\cdot}3^5{\cdot}5$	H_{10}	$3+36+81$	$(3 \times U_4(2)) : 2$	$A_2 \times E_6$
$1120 = 2^5{\cdot}5{\cdot}7$	$2^7{\cdot}3^5{\cdot}5$	H_{11}	120	$(3 \times U_4(2)) : 2$	
$1120 = 2^5{\cdot}5{\cdot}7$	$2^7{\cdot}3^5{\cdot}5$	H_{12}	120	$(3 \times U_4(2)) : 2$	
$1575 = 3^2{\cdot}5^2{\cdot}7$	$2^{12}{\cdot}3^3$	H_{13}	$24+96$	$2_+^{1+8} : (S_3)^3$	$(D_4)^2$
$11200 = 2^6{\cdot}5^2{\cdot}7$	$2^6{\cdot}3^5$	H_{14}	$12+108$	$(3^4 : 2^3).S_4$	$(A_2)^4$
$12096 = 2^6{\cdot}3^3{\cdot}7$	$2^6{\cdot}3^2{\cdot}5^2$	H_{15}	$20+100$	$(A_5)^2 : 2^2$	$(A_4)^2$
$12096 = 2^6{\cdot}3^3{\cdot}7$	$2^6{\cdot}3^2{\cdot}5^2$	H_{16}	120	$(A_5)^2 : 2^2$	
$12096 = 2^6{\cdot}3^3{\cdot}7$	$2^6{\cdot}3^2{\cdot}5^2$	H_{17}	120	$(A_5)^2 : 2^2$	

The pairs of subgroups H_2 and H_3, H_5 and H_6, H_8 and H_9, H_{11} and H_{12}, and H_{16} and H_{17} become conjugate in $G_1.2 = O_8^+(2)$. All the other subgroups H_i of G_1 have index 2 in their normalizers in $G_1.2$. Also, all the triples of isomorphic groups in the above table become conjugate in the famous "triality" automorphism group $\mathrm{Aut}(G_1) = G_1.S_3$. As a result, the table shows that all maximal subgroups of G_1 are conjugate in $\mathrm{Aut}(G_1)$ to subgroups that preserve a subsystem of the E_8 root system. Unfortunately, for the purpose of analyzing algebraic groups of type E_8 as in this paper, that is not as good as actually preserving a subsystem.

Also, by the Atlas, the whole group $G_1.2 = O_8^+(2) = W(E_8)/\{\pm 1\}$ has 9 conjugacy classes of maximal subgroups: G_1, $H_1.2$, $H_4.2$, $H_7.2$, $H_{10}.2$, $H_{13}.2$, $H_{14}.2$, $H_{15}.2$, and one "novelty", $Y \cong 2^{3+6} : (L_3(2) \times 2)$, which has index $2025 = 3^4{\cdot}5^2$ in $G_1.2$ and order $2^{13}3{\cdot}7$. (By definition, a novelty is a maximal subgroup of $G_1.2$ which is not G_1 and whose intersection with G_1 is not maximal in G_1.) As it happens, 8 of the 9 maximal subgroups of $G_1.2$, all of those other than G_1, are equal to the subgroup preserving a certain subsystem of the E_8 root system. These subsystems have type, respectively, $A_1 \times E_7$, D_8, A_8, $A_2 \times E_6$, $(D_4)^2$, $(A_2)^4$, $(A_4)^2$, and (corresponding to the novelty) $(A_1)^8$. The Atlas mentions some of these facts, but not all; one also has to check that the subgroups of $G_1.2$ preserving the subsystems A_8, $(D_4)^2$, and $(A_1)^8$ are the indicated maximal subgroups, for example using Carter's Table 11 [11], which describes the subgroup of $W(E_8)$ preserving each subsystem of the E_8 root system.

9 History of Question 0.2

Question 0.2 unifies several known properties of quadratic forms and division algebras. We recall the statement: a quasi-projective homogeneous variety X over a field with a zero-cycle (not necessarily effective) of degree $d > 0$ should have a closed point of degree dividing d. When $d = 1$ and X is a projective homogeneous variety, the question was formulated by Veisfeiler in 1969 [42]. He also formulates the analogous question about splitting fields for semisimple groups, which amounts to taking X to be a torsor for $\mathrm{Aut}(G)$ with G is a split group. Veisfeiler claimed to solve these problems for the split groups G_2, F_4, E_6, and E_7, but the proofs for F_4, E_6, and E_7 are incorrect. Question 0.2 for $d = 1$, X is a G-torsor, and G is the split group F_4, E_6, or E_7 follows from the results of Rost and others for F_4, and was proved by Gille for E_6 and E_7 [18].

When X is a G-torsor, $d = 1$, and G is absolutely simple, Question 0.2 (for all inner twists of G) is equivalent to Serre's Question 2 [36]: the map $H^1(k, G) \to \prod H^1(K_i, G)$ should be injective when $K_1, K_2, \dots$ is a set of finite extension fields of k such that gcd $[K_i : k] = 1$. For example, when $G = O(q)$ for a quadratic form q (although this is not a connected group), Question 2 follows from Springer's theorem that two quadratic forms which become isomorphic over a field extension of odd degree are in fact isomorphic [38]. Bayer-Lenstra proved analogous results for all the classical groups [3]. Also, Sansuc gave a positive solution to Question 2 for arbitrary connected linear algebraic groups over a number field [32], building upon the Kneser-Harder-Chernousov proof of the Hasse principle for simply connected groups over a number field.

Colliot-Thélène suggested the generalization of Question 0.2, still in the case $d = 1$, to arbitrary quasi-projective homogeneous spaces X. That is, if X has a zero-cycle of degree 1, then X should have a rational point. For X a quadric, this is equivalent to Springer's theorem that a quadratic form which becomes isotropic over a field extension of odd degree is isotropic [38]. Colliot-Thélène and Coray showed that zero-cycles of degree 1 need not imply the existence of rational points for rational varieties X other than homogeneous varieties, in particular for conic bundles over $\mathbf{P}^1_k$ with k a p-adic field [13].

Almost all the evidence for Question 0.2, including the present paper, is concerned with the case where X is either a projective homogeneous variety or a torsor. Gille observed that the question for general quasi-projective homogeneous varieties may be too optimistic, as the following example indicates. Let p be a prime number, $G = PGL(p)$, and $H = (G_m)^{p-1}.\mathbf{Z}/p \subset G$. Let A be a central simple algebra of degree p over a field k, and let X be the corresponding G-torsor. The automorphism group of X as a G-torsor is a twisted form G' of G. The algebra A is said to be cyclic if it is trivial or has a splitting field which is cyclic of degree p over k [30]. It is elementary that A is cyclic if and only if the G-torsor X comes from some H-torsor over k, or equivalently if and only if the quotient variety $H\backslash X$ has a k-point. Here $H\backslash X$ is a homogeneous variety for the twisted group G'. We know that any central simple algebra A of degree p becomes trivial and hence cyclic over some field extension of degree 1 or p, and it also becomes cyclic over some field extension of degree prime to p (corresponding to the subgroup $\mathbf{Z}/p \subset S_p$). Therefore the homogeneous variety $H\backslash X$ always has a closed point of degree dividing p and another of degree prime to p, and so it has a zero-cycle of degree 1. Thus a positive answer to Question 0.2 would imply that $H\backslash X$ always has a k-point, in other words that every central simple algebra of prime degree is cyclic. But this is a major open problem on division algebras, and some people expect a negative answer (see Rowen [31], for example).

Finally, we turn to Question 0.2 for general positive integers d rather than $d = 1$. There is less evidence for the question in the case of general d, even if we assume that X is a torsor, but there is some evidence. For example, the question has a positive answer for $PGL(n)$-torsors, and also (equivalently) for Severi-Brauer varieties. That is, if a central simple algebra splits over extension fields of degrees $a_1, a_2, \dots$, then it is isomorphic to a matrix algebra over a division algebra of dimension m dividing $\gcd(a_1, a_2, \dots)$, and therefore it splits over an extension field of degree m, which can be chosen to be separable over k. Both steps here are basic results in the theory of central simple algebras, proved by Schur for fields of characteristic zero and by Noether for arbitrary fields. A reference is [30], Theorems 7.2.3 and 7.1.12. Also, we have proved Question 0.2 for principal homogeneous spaces under the split simply connected exceptional groups G_2, F_4, and E_6, as well as a partial result for E_7, in Theorem 5.1.

It seems inevitable that in answering Question 0.2, the case of E_8 will be particularly difficult and will have to be considered separately.

References

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.* **76** (1984), 469–514.

[2] R. Baeza. *Quadratic forms over semilocal rings.* Lecture Notes in Mathematics **655**, Springer (1978).

[3] E. Bayer-Fluckiger and H. Lenstra. Forms in odd degree extensions and self-dual normal bases. *Am. J. Math.* **112** (1990), 359–373.

[4] F. van der Blij and T. Springer. The arithmetics of octaves and of the group G_2. *Indag. Math.* **21** (1959), 406–418.

[5] A. Borel and T. Springer. Rationality properties of linear algebraic groups. II. *Tohoku Math. J.* **20** (1968), 443–497.

[6] N. Bourbaki. *Groupes et algèbres de Lie, Chapitres 4, 5 et 6.* Masson (1981).

[7] R. Brauer. On groups whose order contains a prime number to the first power. I, II. *Amer. J. Math.* **64** (1942), 401–420, 421–440.

[8] R. Brauer. On simple groups of order $5 \cdot 3^a \cdot 2^b$. *Collected papers*, v. 2, 421–470. MIT (1980).

[9] R. Brauer. Über endliche lineare Gruppen von Primzahlgrad. *Math. Ann.* **169** (1967), 73–96.

[10] W. Burnside. *Theory of groups of finite order*, 2nd edition. Cambridge (1911).

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

[12] F. Cole. Simple groups as far as order 660. *Amer. J. Math.* **15** (1893), 303–315.

[13] J.-L. Colliot-Thélène and D. Coray. L'équivalence rationnelle sur les points fermés des surfaces rationnelles fibrées en coniques. *Comp. Math.* **39** (1979), 301–332.

[14] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson. *An atlas of finite groups.* Oxford (1985).

[15] W. Feit. On finite linear groups in dimension at most 10. *Proceedings of the conference on finite groups* (Utah, 1975), ed. W.R. Scott and F. Gross, 397–407. Academic Press (1976).

[16] The GAP Group. *GAP – groups, algorithms, and programming, Version 4.2.* Aachen, St Andrews (2000). http://www-gap.dcs.st-and.ac.uk/gap

[17] R. S. Garibaldi. The Rost invariant has trivial kernel for quasi-split groups of low rank. *Comment. Math. Helv.* **76** (2001), 684–711.

[18] P. Gille. La R-équivalence sur les groupes algébriques réductifs définis sur un corps global. *Publ. Math. IHES* **86** (1997), 199–235.

[19] P. Gille. Invariants cohomologiques de Rost en caractéristique positive. *K-Theory* **21** (2000), 57–100.

[20] R. Griess. Elementary abelian p-subgroups of algebraic groups. *Geom. Ded.* **39** (1991), 253–305.

[21] D. Gorenstein. *Finite groups*, 2nd edition. Chelsea (1980).

[22] A. Grothendieck. Torsion homologique et sections rationnelles. *Séminaire Chevalley, Anneaux de Chow et applications,* exposé no. 5. Paris (1958).

[23] N. Jacobson. Composition algebras and their automorphisms. *Rend. Circ. Mat. Palermo* **7** (1958), 55-80.

[24] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups.* LMS Lecture Notes **129**, Cambridge (1990).

[25] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol. *The book of involutions.* American Mathematical Society (1998).

[26] D. Lehmer. On a problem of Störmer. *Illinois J. Math.* **8** (1964), 57–79.

[27] H. Petersson and M. Racine. An elementary approach to the Serre-Rost invariant of Albert algebras. *Indag. Math.* **7** (1996), 343–365.

[28] A. Pfister. Quadratische Formen in beliebigen Körpern. *Invent. Math.* **1** (1966), 116–132.

[29] M. Rost. A (mod 3) invariant for exceptional Jordan algebras. *C. R. Acad. Sci. Paris Sér. I Math.* **313** (1991), 823-827.

[30] L. Rowen. *Ring theory,* Volume II. Academic Press (1988).

[31] L. Rowen. Are p-algebras having cyclic quadratic extensions necessarily cyclic? *J. Alg.* **215** (1999), 205–228.

[32] J.-J. Sansuc. Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *J. Reine Angew. Math.* **327** (1981), 12–80.

[33] I. Schur. Über eine Klasse von endlichen Gruppen linearer Substitutionen. *Sitz. der Preussischen Akad. Berlin* (1905), 77–91; *Gesammelte Abhandlungen*, v. 1, 128–142, Springer (1973).

[34] J.-P. Serre. Lectures on the Mordell-Weil theorem. Vieweg (1990).

[35] J.-P. Serre. Cohomologie galoisienne. Lecture Notes in Mathematics **5**, 5th edition, Springer (1994).

[36] J.-P. Serre. Cohomologie galoisienne: progrès et problèmes. Séminaire Bourbaki 1993/94, no. 783, *Astérisque* **227** (1995), 229–257.

[37] C. Sims. Computational methods in the study of permutation groups. *Computational problems in modern algebra*, ed. J. Leech, 169–183. Pergamon (1970).

[38] T. Springer. Sur les formes quadratiques d'indice zéro. *C. R. Acad. Sci. Paris Sér. I Math.* **234** (1952), 1517-1519.

[39] D. Suprunenko. *Soluble and nilpotent linear groups.* American Mathematical Society (1963).

[40] J. Tits. Sur les degrés des extensions de corps déployant les groupes algébriques simples. *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), 1131–1138.

[41] B. Totaro. The torsion index of E_8 and other groups. Preprint (2003).

[42] B. Veisfeiler. Certain properties of singular semisimple algebraic groups over non-closed fields. *Trudy Moskov. Mat. Obshch.* **20** (1969), 111–136. English translation: *Transactions of the Moscow Mathematical Society for the year 1969 (vol. 20)*, 109–134, American Mathematical Society (1971).

[43] W. Waterhouse. *Introduction to affine group schemes.* Springer (1979).

[44] H. Wielandt. *Finite permutation groups.* Academic Press (1964).

DPMMS, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, England

b.totaro@dpmms.cam.ac.uk