Canad. Math. Bull. Vol. **49** (2), 2006 pp. 196–202

Another Proof of Totaro's Theorem on E_8-Torsors

Vladimir Chernousov

Abstract. We give a short proof of Totaro's theorem that every E_8-torsor over a field k becomes trivial over a finite separable extension of k of degree dividing $d(E_8) = 2^6 3^2 5$.

1 Introduction

In the paper we give a short proof of the following theorem due to B. Totaro [7].

Theorem 1.1 *Let k be an arbitrary field. Then every E_8-torsor defined over k becomes trivial over a finite separable extension of k of degree dividing $d(E_8) = 2^6 3^2 5$.*

Note that in a second paper on E_8-torsors [8], Totaro showed that the bound $2^6 3^2 5$ is exact, *i.e.,* there is an E_8-torsor that cannot be split by an extension whose degree is a proper divisor of $2^6 3^2 5$.

The original proof of Theorem 1.1 is based on an analysis of the subgroup structure of the Weyl group of type E_8, Brauer's theory of blocks, Aschbacher's theorem on the maximal subgroups of the classical groups over finite fields, and the classification of solvable primitive linear groups. Moreover, some of the computations in [7] were made with the aid of a computer. The aim of the present paper is to simplify the proof. Eventually, following the Totaro's main idea on considering Galois orbits in the corresponding root system $\Sigma(E_8)$, we give a short straightforward proof of Theorem 1.1.

2 Generic Case and Possible Bad Cases

Let G_0 be a split group of type E_8 over k. Let $\xi \in Z^1(k, G_0)$, and let $G = {}^{\xi}G_0$ be the corresponding twisted group. Consider a maximal k-defined torus $T \subset G$. Let E/k be a minimal finite extension splitting T. The extension E/k is necessarily Galois, and its Galois group Γ acts in a natural way on the root system $\Sigma = \Sigma(G, T)$ of G with respect to T. This gives rise to a canonical embedding $\Gamma \hookrightarrow W$ where $W = W(E_8)$ is the corresponding Weyl group. If we choose a base of Σ, then the action of Γ on Σ induces an action of Γ on the set $R = \Sigma/(\pm 1)$. This set has 120 elements and we always choose positive roots as representatives of the elements of R.

The case of "generic" E_8-torsors is easy.

Received by the editors May 12, 2005; revised November 30, 2005.
Supported by the Canada Research Chairs Program, and by NSERC's Grant G121210944
AMS subject classification: Primary: 11E72; secondary: 14M17, 20G15.

Lemma 2.1 *Assume that Γ has an orbit on R of size dividing $120 = 2^3 \cdot 3 \cdot 5$. Then there is a finite separable extension L/k of degree dividing $d(E_8)$ such that G splits over L.*

Proof Let $\alpha \in R$ be such that $|\Gamma(\alpha)|$ divides 120. Let $\mathrm{Stab}_\Gamma(\alpha)$ be the stabilizer of α in Γ, and consider the subfield $L_1 \subset E$ corresponding to $\mathrm{Stab}_\Gamma(\alpha)$. Taking an extension L_2/L_1 of degree 2 if necessary, we may assume that Σ has a root α stable with respect to an (absolute) Galois group of L_2. The centralizer Σ' of α in Σ is the subsystem of type E_7 which is stable with respect to the Galois group of L_2. If $H \subset G$ is the subgroup in G of type E_7 corresponding to Σ', then H is L_2-defined and, by a result of Tits [6], splits over a separable extension L_3/L_2 of degree dividing $2^2 3$. Clearly L_3 also splits G, and $[L_3 : k] = [L_3 : L_2][L_2 : L_1][L_1 : k]$ divides $(2^2 3)2(120) = 2^6 3^2 5$, as required. ■

If Σ contains a proper subroot system stable with respect to Γ, then using known results on groups of classical types and Tits results [6] on splitting fields of groups of types G_2, F_4, E_6, E_7, it is easy to conclude that G splits over a finite separable extension of k of degree dividing $d(E_8)$. Thus, we may henceforth assume without loss of generality that Σ does not contain root subsystems stable with respect to Γ. In this case, possible "bad" orbit decompositions are given by the following:

Lemma 2.2 ([7, Lemma 4.1]) *If Γ has no orbits on R of size dividing 120, then the orbit sizes of Γ are either*

(a) 64 + (multiples of 7 summing to 56)*;*
(b) 50 + (multiples of 7 summing to 70)*;*
(c) 45 + (multiples of 25 summing to 75)*;*
(d) 36 + (multiples of 7 summing to 84) *or*
(e) (multiples of 16 summing to 48) + (multiples of 9 summing to 72).

For the convenience of the reader we give a sketch of the proof due to Totaro. It is based on the following result.

Lemma 2.3

(i) *A 7-Sylow subgroup of W has only one fixed point in R.*
(ii) *A 5-Sylow subgroup of W has 4 orbits of size 25 and 4 orbits of size 5 in R.*

Proof This is easy to check by direct inspection. ■

Proof of Lemma 2.2 Let us first assume that 7 divides $|\Gamma|$. Then, by Lemma 2.3, all orbits of Γ in R have sizes divisible by 7 except for one whose size is $\equiv 1$ modulo 7. The size of this exceptional orbit is either 36, 50 or 64, since by our assumption there is no orbit of size dividing 120. Thus, assuming that $|\Gamma|$ is a multiple of 7 we have cases (a), (b), and (d).

Assume next that $|\Gamma|$ is not divisible by 7, but divisible by 25. Since the sum of sizes of all orbits of Γ in R is 120, and sizes of orbits do not divide 120, we find, by Lemma 2.3, that all orbits of Γ have size divisible by 25 except for one whose size is 45. Hence we have case (c).

Finally, assume that the order of Γ is divisible by neither 7 nor 25. Recall that $|W| = 2^{14}3^5 5^2 7$. Since there is no orbit of Γ whose size divides 120, all of them have sizes a multiple of 16 or 9. The only way it can happen is case (e). ■

By [7, Lemma 6.1], cases (b) and (c) are impossible. By [7, Lemma 4.2], in case (a) the complementary subset to the orbit of size 64 forms a subsystem of type D_8. The remaining cases (d) and (e), which caused most of the complications in [7], will be dealt with in a simple fashion in the following two sections.

For later use, we need the following fact related to the Rost invariant for E_7. For the definition and properties of the Rost invariant R_G of an algebraic group G we refer to [4].

Proposition 2.4 *Let H_0 be a split simple simply-connected algebraic group of type E_7 defined over an arbitrary field K, and let*

$$R_{H_0}\colon H^1(K, H_0) \to H^3(K, \mathbb{Q}/\mathbb{Z}(2))$$

be the Rost invariant of H_0. Let $\xi \in H^1(K, H_0)$ be such that the 3-component of $R_{H_0}(\xi)$ is trivial. Then there is a separable extension L/K of degree dividing 4 such that ξ is trivial over L.

Proof By [6], there is a quasi-split subgroup $H' \subset H_0$ of type E_6 such that ξ is in the image of $H^1(K, H') \to H^1(K, H_0)$. Taking a proper quadratic extension E/K if necessary, we may assume that H' is split over E. One knows that for a split group H'_E of type E_6 the 2-component of $R_{H'}(\xi_E)$, where ξ_E is the image of ξ under the restriction map $H^1(K, H_0) \to H^1(E, H_0)$, is a symbol. Taking again a separable quadratic extension L/E killing this symbol, we may assume that the 2-component of $R_{H'}(\xi_L)$ is trivial over L. Then $\xi_L \in \operatorname{Ker} R_{H'}$. It remains to observe that $\operatorname{Ker} R_{H'} = 1$, by [3] (see also [2]). ■

3 An Orbit of Size 36

Let $R_1 \subset R$ be an orbit of Γ of size 36, and let $R_2 = R \setminus R_1$. Take a positive root $\alpha \in R_1$ and consider $\Gamma_1 = \operatorname{Stab}_\Gamma(\alpha)$. Note that in the definition of Γ_1, α is viewed as an element of R, but not of Σ. Let $E'_1 \subset E$ be the subfield corresponding to Γ_1. Taking a proper quadratic extension E_1/E'_1 if necessary, we may assume that α viewed as a root in Σ is stable with respect to an (absolute) Galois group of E_1. Since $|R_1| = 36$, the index $[E_1 : k]$ is either $2^2 3^2$ or $2^3 3^2$.

Lemma 3.1 *If the 3-component of $R_{G_0}([\xi])$ is trivial over E_1, then there is a separable extension E_2/k of degree dividing $2^5 3^2$ which kills ξ.*

Proof Let Σ' be the root subsystem of Σ consisting of roots orthogonal to α. Consider the subgroup H of G corresponding to Σ'. It has type E_7 and is defined over E_1 since α is. Since H contains a semisimple anisotropic E_1-kernel of G, by a result due to R. Steinberg (*cf.* [2, Theorem 3.2]), there is a cocycle $\xi_1 \in Z^1(E_1, H_0)$, where

$H_0 \subset G_0$ is a canonical E_1-split subgroup of type E_7, such that ξ is equivalent to ξ_1 over E_1. Note that $R_{G_0}(\xi) = R_{H_0}(\xi_1)$. Then, by Proposition 2.4, there is a separable extension E_2/E_1 of degree dividing 4 which kills ξ_1, and hence ξ. Its degree over k divides $4(2^3 3^2)$, as required. ■

By Lemma 3.1, we may henceforth assume without loss of generality that the 3-component of $R_{G_0}([\xi])$ is nontrivial over E_1.

Lemma 3.2 *Let $\beta \in R_2$. Then $|\Gamma_1(\beta)|$ is a multiple of 21.*

Proof Since Γ_1 contains a 7-Sylow subgroup of W, the size of $\Gamma_1(\beta)$ is divisible by 7 by Lemma 2.3(i). Assume that $|\Gamma_1(\beta)|$ is not divisible by 3. Take the extension E_2/E_1 of degree prime to 3 corresponding to the stabilizer $\Gamma_2 = \mathrm{Stab}_{\Gamma_1}(\beta)$. By a counting argument, there are at least two roots in R_2 different from β whose Γ_2-orbits have sizes not divisible by 3. Repeating the above construction 2 times, we can find a finite extension E/E_1 of degree prime to 3 with the property that an (absolute) Galois group of E stabilizers α and at least 3 roots in R_2. Then it follows from Tits' classification [5] that the E-rank of G is at most 5. Again, by Tits' classification, all simple groups which could appear in a semisimple E-anisotropic kernel of G have trivial 3-components of the Rost invariant, implying therefore that $R_{G_0}(\xi_E)$ has also trivial 3-component. On the other hand, since $[E : E_1]$ is prime to 3, the 3-component of $R_{G_0}(\xi_E)$ is still nontrivial — a contradiction. ■

Recall that we assumed that Σ has no subroot systems stable with respect to Γ; in particular we may assume that R_1 is not a subroot system. It follows that there is $\delta \in R_1$ such that either $\alpha + \delta$ or $\alpha - \delta$ is a root, call it $\beta = \alpha \pm \delta$, belonging to R_2. Since the size of $\Gamma_1(\beta)$ is divisible by 21, so is $|\Gamma_1(\delta)|$. Since R_1 consists of 36 elements, the size of $\Gamma_1(\delta)$, hence that of $\Gamma_1(\beta)$, is exactly 21.

Let $R_1' = \Gamma_1(\delta)$, $R_1'' = R_1 \setminus R_1'$, $R_2' = \Gamma_1(\beta)$, $R_2'' = R_2 \setminus R_2'$. Recall that we denote the subsystem of Σ of type E_7 consisting of all roots in Σ orthogonal to α by Σ'.

Lemma 3.3 *$\pm R_2''$ coincides with Σ'.*

Proof Since $(\alpha, \beta) = \pm 1$ and $(\alpha, \delta) = \pm 1$, the intersection of $\Sigma'/\pm 1$ with R_1' and R_2' is empty, hence

$$(\Sigma'/\pm 1) = ((\Sigma'/\pm 1) \cap R_1'') \cup ((\Sigma'/\pm 1) \cap R_2'').$$

The order of $(\Sigma'/\pm 1) \cap R_2''$ being Γ_1-stable is divisible by 21. Since R_1'' has order 16 and $|\Sigma'/\pm 1| = 63$, we have $(\Sigma'/\pm 1) \cap R_1'' = \varnothing$. ■

As a direct consequence of the above lemma we have

Corollary 3.4

(i) $(\alpha, \gamma) = \pm 1$, *if $\gamma \in R_1$ and $\gamma \neq \alpha$.*
(ii) $\alpha \pm \gamma_1 \in R_1''$, *if $\gamma_1 \in R_1''$.*

https://doi.org/10.4153/CMB-2006-020-5 Published online by Cambridge University Press

(iii) $(\gamma_1, \gamma_2) = \pm 1$, *if* $\gamma_1, \gamma_2 \in R_1$, $\gamma_1 \neq \gamma_2$.

Proof Properties (i) and (ii) are clear since $(\Sigma' / \pm 1) \subset R_2$. Property (iii) follows from (i), since α was an arbitrary root in R_1. ■

Lemma 3.5 *$\pm R_1''$ is a subroot system of Σ.*

Proof Let $\gamma \in R_1''$. We have to show that $\gamma \pm \gamma' \in R_1''$ for all $\gamma' \in R_2''$ different from γ. Arguing as above, we see that there exists a subset $R'_{1,\gamma}$ of R_1, with 21 elements, comprised of roots whose sum with γ is in R_2. By Corollary 3.4, the remaining 14 roots in $R_1 \setminus R'_{1,\gamma}$ have sum with γ in $R_1 \setminus R'_{1,\gamma}$. We will be finished if we show that $R'_{1,\gamma} = R'_1$.

Let $\delta \in R'_1$. By Corollary 3.4(iii), either $\gamma + \delta$ or $\gamma - \delta$ is a root. Call it β. Since $(\alpha, \beta) \equiv 0$ modulo 2, we have either $\alpha = \pm\beta$ or $\beta \in \Sigma' = R_2''$. The first case is impossible, since the Γ_1-orbits of δ and γ consist of 21 and at most 14 elements, respectively. Then $\beta \in R_2$, so that $\delta \in R'_{1,\gamma}$. ■

To finish the consideration of orbits of size 36, it remains to note that the subroot system R_1'' is Γ_1-stable, hence it has an automorphism of order 7. However the minimal simple root system having an automorphism of order 7 has type A_6 and consists of 42 elements.

4 An Orbit of Size a Multiple of 16

We start with an explicit description of a 3-Sylow subgroup of W, denoted below by Ψ, and its action on the root system Σ. Recall that $|\Psi| = 3^5$. Let $\Pi = \{\alpha_1, \dots, \alpha_8\}$ be a fixed basis of Σ. Here and below we label roots as in [1]. Consider the subroot system of type $E_6 \times A_2$ in Σ generated by $\Sigma_1 = \langle \alpha_1, \dots, \alpha_6 \rangle$ and $\Sigma_2 = \langle \alpha_8, -\alpha \rangle$ where α is the highest root of Σ^+. Comparing the orders of the Weyl groups of type E_6, A_2, E_8, we find that the direct product $\Psi = \Psi_1 \times \Psi_2$ of 3-Sylow subgroups Ψ_1 of $W(E_6)$ and Ψ_2 of $W(A_2)$ is a 3-Sylow subgroup of W.

Recall that Ψ_2 has order 3. As for Ψ_2, we choose the subgroup in $W(A_2)$ generated by the element e which takes α_8 into $-\alpha$ and $-\alpha$ into $-(\alpha_8 - \alpha)$.

The root system Σ_1 contains a subroot system Σ_3 of type $A_2 \times A_2 \times A_2$ generated by the roots $\langle \alpha_1, \alpha_3 \rangle$, $\langle \alpha_5, \alpha_6 \rangle$ and $\langle \alpha_2, -\beta \rangle$, respectively, where β is the positive root of maximal length in Σ_1 with respect to the basis $\alpha_1, \dots, \alpha_6$. Let $w_0, w_1 \in W(E_6)$ be the elements of maximal length with respect to the bases $\{\alpha_1, \dots, \alpha_6\}$ and $\{\alpha_1, \alpha_3, \alpha_4, \alpha_2, -\beta, \alpha_5\}$, respectively. Let $d = w_0 w_1$. It is easy to see that d has order 3 and takes the roots $\alpha_1, \alpha_3, \alpha_5, \alpha_6, \alpha_2, -\beta$ into $\alpha_6, \alpha_5, \alpha_2, -\beta, \alpha_3, \alpha_1$, respectively. Therefore d permutes the components of Σ_3 and their Weyl groups.

Let a be an arbitrary element of order 3 in the Weyl group of the first component of Σ_3. Denote $b = dad^{-1}$ and $c = dbd^{-1}$. Clearly, a, b, c commute and d permutes them. Consider the subgroup Ψ_1 in $W(E_6)$ generated by a, b, c, d. Since Ψ_1 has order 3^4, it is a 3-Sylow subgroup of $W(E_6)$.

One easily checks that there are 4 orbits of Ψ on R which are as follows. The Ψ-orbit of α_7 consists of 81 elements in $\Sigma^+ \setminus \{\Sigma_1^+ \cup \Sigma_2^+\}$. The Ψ-orbit of α_1 consists of 9 elements and coincides with Σ_3^+. The Ψ-orbit of α_8 consists of 3 elements in $\Sigma_2^+ = \{\alpha_8, \alpha, \alpha - \alpha_8\}$. Lastly, the Ψ-orbit of α_4 consists of the remaining 27 elements in $\Sigma_1^+ \setminus \Sigma_3^+$.

We also need information about the stabilizer $\mathrm{Stab}_\Psi(\beta)$ of a root $\beta \in R$. It is easy to see that for each root $\beta \in \Psi(\alpha_7) = \Sigma^+ \setminus \{\Sigma_1^+ \cup \Sigma_2^+\}$ one has $\mathrm{Stab}_\Psi(\beta) \subset \langle a \rangle \cup \langle b \rangle \cup \langle c \rangle$. Furthermore, for each $\beta \in \Psi(\alpha_4)$, $\mathrm{Stab}_{\Psi_1}(\beta)$ has order 3 and is generated by an element of the form $da^{\epsilon_1} b^{\epsilon_2} c^{\epsilon_3}$ where ϵ_i is 0, 1 or 2.

Let R_1 and R_2 be unions of orbits of Γ whose sizes are divisible by 16 and 9 respectively. Let $\Gamma_3 \leq \Gamma$ be a 3-Sylow subgroup. Without loss of generality we may assume that Γ_3 is a subgroup of Ψ.

Lemma 4.1 $|\Gamma_3| \leq 3^3$.

Proof If $|\Gamma_3| = 3^5$, then $\Gamma_3 = \Psi$ and hence Γ_3 has the orbit $\Gamma_3(\alpha_7) = \Psi(\alpha_7)$ of size 81, which is impossible.

Assume that $|\Gamma_3| = 3^4 = 81$. Then Γ_3 is a normal subgroup in Ψ and hence Ψ acts in a natural way on Γ_3-orbits. Since Ψ has the orbit $\Psi(\alpha_7)$ of size 81, Γ_3 has at least three orbits of size 27. Since R_1 and R_2 contain at most one and two orbits of size 27 respectively, we find that Γ_3 has exactly 3 orbits of size 27 and their union is necessarily $\Sigma^+ \setminus \{\Sigma_1^+ \cup \Sigma_2^+\}$. It follows that for each $\beta \in \Sigma^+ \setminus \{\Sigma_1^+ \cup \Sigma_2^+\}$ we have $\mathrm{Stab}_\Psi(\beta) \subset \Gamma_3$ and this implies $\langle a, b, c \rangle \subset \Gamma_3$. But then the orbit $\Gamma_3(\alpha_4)$ contains at least 27 elements giving thus the fourth orbit of size 27 — a contradiction. ■

We are ready to finish the proof. Since $|\Gamma_3| \leq 27$, the Γ_3-orbits of roots in R_2 have sizes divisible by 9 or 27. Since $|R_2| = 72$, there is at least one $\beta \in R_2$ such that the size of its Γ_3-orbit is not divisible by 27. As in §3, consider $\Gamma' = \mathrm{Stab}_\Gamma(\beta)$ and let $E_1 \subset E$ be the subfield corresponding to Γ'. If the 3-component of $R_{G_0}(\xi)$ is trivial over E_1, then the same argument as in Lemma 3.1 completes the proof. Thus we may assume without loss of generality that $|\Gamma_3| = 27$, and that for each root $\beta \in R_2$, whose Γ_3-orbit has size divisible by 9 but not by 27, the 3-component of $R_{G_0}(\xi)$ is nontrivial over the corresponding field E_1.

Note that in this possible "bad" case we have that $\mathrm{Stab}_{\Gamma_3}(\beta)$, being a group of order 3, is a 3-Sylow subgroup of Γ'. By arguing as in Lemma 3.2, we may therefore additionally assume that a nontrivial $x \in \mathrm{Stab}_{\Gamma_3}(\beta)$ has at most 3 invariant positive roots with respect to the canonical action of $\Gamma_3 \subset W$ on Σ. In particular, this assumption implies that for each root in $R_2 \cap (\Sigma^+ \setminus \{\Sigma_1^+ \cup \Sigma_2^+\})$ its Γ_3-orbit has size 27, hence that β with the above property is in Σ_1^+. We also have $e \notin \Gamma_3$, since each root in Σ_1 is stable with respect to e.

Consider the canonical morphism

$$f\colon \Psi \to \Psi/\langle e \rangle \simeq \Psi_1 = \langle a, b, c, d \rangle.$$

Since $e \notin \Gamma_3$, the image $f(\Gamma_3)$ has order 27, hence it is a normal subgroup in Ψ_1. As in Lemma 4.1, we find that Ψ_1 acts on Γ_3-orbits of Γ_3 on Σ_1^+. Thus $\Sigma_1^+ \setminus \Sigma_3^+$, being a unique Ψ_1-orbit of size 27, is a disjoint union of 3 Γ_3-orbits of size 9. Then for each root $\beta \in \Sigma_1^+ \setminus \Sigma_3^+$, $\mathrm{Stab}_{\Psi_1}(\beta)$, being a group of order 3, is contained in Γ_3. However it is easy to see that all such stabilizers generate Ψ_2, whose order is 3^4. This contradicts our assumption that $|\Gamma_3| = 27$.

Acknowledgements Work on the present paper started in 2002 at the Centre Bernoulli, E.P.F.L., Lausanne, and continued at Bielefeld University in 2003. The author thanks both centres for their hospitality and their stimulating atmosphere. The author would also like to thank Forschergruppe "Spektrale Analysis, asymptotische Verteilungen und stochastische Dynamik" for its support.

References

[1] N. Bourbaki, *Éléments de mathématique.* In: Groupes et algèbres de Lie, Ch. 4–6. Masson, Paris, 1981.

[2] V. Chernousov, *The kernel of the Rost invariant, Serre's Conjecture II and the Hasse principle for quasi-split groups* $^{3,6}D_4, E_6, E_7$. Math. Ann. **326**(2003), 297–330.

[3] R. S. Garibaldi, *The Rost invariant has trivial kernel for quasi-split groups of low rank.* Comment. Math. Helv. **76**(2001), no. 4, 684–711.

[4] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological Invariants in Galois Cohomology.* University Lecture Series 28, American Mathematical Society, Providence, RI, 2003.

[5] J. Tits, *Classification of algebraic semisimple groups.* In: Algebraic Groups and Discontinuous Subgroups, Proc. Symp. Pure Math. 9, 1966, pp. 33–62.

[6] ———, *Sur les degrés des extensions de corps déployant les groupes algébriques simples.* C. R. Acad. Sci. Paris Sr. I Math. **315**(1992), no. 11, 1131–1138.

[7] B. Totaro, *Splitting fields for E_8-torsors.* Duke Math. J. **121**(2004), no. 3, 425–455.

[8] ———, *The torsion index of E_8 and other groups.* Duke Math. J. **129**(2005), no. 2, 219–248.

Department of Mathematical Sciences
University of Alberta
Edmonton AB
T6G 2G1
e-mail: chernous@math.ualberta.ca