SPLITTING FIELDS OF G-VARIETIES

Z. REICHSTEIN AND B. YOUSSIN

Abstract. Let G be an algebraic group, X a generically free G-variety, and $K = k(X)^G$. A field extension L of K is called a splitting field of X if the image of the class of X under the natural map $H^1(K, G) \mapsto H^1(L, G)$ is trivial. If L/K is a (finite) Galois extension then $\mathrm{Gal}(L/K)$ is called a splitting group of X.

We prove a lower bound on the size of a splitting field of X in terms of fixed points of nontoral abelian subgroups of G. A similar result holds for splitting groups. We give a number of applications, including a new construction of noncrossed product division algebras.

Contents

1991 *Mathematics Subject Classification.* Primary: 14L30, 16K20, 20G10, 14E05. Secondary: 14E15.

Key words and phrases. Splitting field, splitting group, nontoral subgroup, algebraic group action, division algebra, noncrossed product, exceptional group.

Z. Reichstein was partially supported by NSF grant DMS-9801675.

1. Introduction

Let k be an algebraically closed field of characteristic zero, let K be a finitely generated field extension of k and let G is an algebraic group defined over k. Recall that elements of the non-abelian cohomology set $H^1(K, G)$ can be identified with (birational classes of) generically free G-varieties X such that $k(X)^G = K$ (see [Po, Section 1.3]). The set $H^1(K, G)$ has no group structure in general; however, $H^1(K, G)$ is equipped with a marked element, which we shall denote by 1. This element is represented by the "split" G-variety $X \simeq X_0 \times G$, where $k(X_0) = K$ and G acts by left multiplication on the second factor. A field extension L/K is said to be a splitting field for $u \in H^1(K, G)$ if $u \mapsto 1$ under the natural map $H^1(K, G) \longrightarrow H^1(L, G)$.

The nonabelian cohomology set $H^1(K, G)$ often allows a different interpretation: its elements can be identified with certain algebraic objects defined over K, e.g, quadratic forms if $G = O_n$, central simple algebras if $G = \mathrm{PGL}_n$, Cayley algebras, if $G = G_2$, etc. These objects may be viewed as "twisted forms" of a single "split" object. In such cases the above notion of a splitting field coincides with the usual one. We will review this interpretation of $H^1(K, G)$ in Section 3; see also [Se_4, Chapter III], [Se_2, Chapter X], [KMRT, Section 29] or [Re, Sections 6-8].

Recall that a subgroup of G is called *toral* if it lies in a torus in G. Our main results on splitting fields are Theorems 1.1 and 1.2.

Theorem 1.1. *Let X be a generically free primitive G-variety, $K = k(X)^G$, and let L/K be a splitting field for X. Suppose X has a smooth point fixed by a finite abelian p-subgroup H of G. Then $[L : K]$ is divisible by $[H : H_T]$ for some toral subgroup H_T of H.*

If X is a generically free primitive G-variety, $K = k(X)^G$, and L is a splitting field which is a (finite) Galois extension of K, then we shall refer to $\mathrm{Gal}(L/K)$ as a *splitting group* for X.

Theorem 1.2. *Let X be a generically free primitive G-variety and let A be a splitting group for X. Suppose X has a smooth point fixed by a finite abelian subgroup H of G. Then A contains an isomorphic copy of H/H_T for some toral subgroup H_T of H.*

Our proofs of Theorems 1.1 and 1.2 are based on the following results of [RY]: for any finite abelian subgroup H of G, the existence of a smooth H-fixed point on a (complete smooth) G-variety X is a birational invariant of X. Moreover, such points survive under dominant rational G-equivariant maps and under certain G-equivariant covers; see [RY, Section 5 and Appendix]. We review and further extend these results in Section 2; see Proposition 2.2 and Theorems 2.5, 2.6 and 2.7.

Informally speaking, Theorem 1.1 (respectively, Theorem 1.2) may be viewed as a "lower bound" on a splitting field (respectively, a splitting group) of X. In particular, if X is a vector space and G acts linearly on X then X has a smooth G-fixed point (namely, the origin) and, hence, in this case Theorem 1.1 (respectively, Theorem 1.2) can be applied to every finite abelian p-subgroup (respectively, subgroup) H of G. Of course, Theorems 1.1 and 1.2 are only of interest if H is nontoral, since otherwise H/H_T may be trivial.

Elementary finite abelian subgroups of algebraic groups have been extensively studied (see [BS], [Bor$_1$], [St], [Se$_5$]); a complete classification was obtained by Griess [Gri]. To the best of our knowledge, nonelementary finite abelian subgroups have not been classified. In Section 5 we apply Theorem 1.1 to a number of specific groups G, where we have sufficient information about the depth of certain nontoral subgroups (see Definition 4.5). In particular, for $G = E_8$ we give a new proof of a theorem of Serre; see Corollary 5.5. Note, however, that the examples we give in Section 5 are somewhat fragmentary, because we do not know any general results about the depth of finite abelian subgroups in exceptional groups. (Propositions 5.3 and 5.7 represent our best efforts in this direction; see also Corollary 4.10.) We hope that this question will attract the attention of group theorists in the future, and that a more complete picture will emerge.

"Upper bounds" on the degrees of splitting fields, i.e., results of the form "every G-variety can be split by a field extension of degree dividing $n(G)$", can be found in the paper [T$_2$] of Tits. For a discussion of these results, including a table of values for $n(G)$, see Remark 4.9.

In Sections 8 and 9 we apply Theorem 1.2, with $G = \mathrm{PGL}_n$, to the theory of central simple algebras. Recall that an element $\alpha \in H^1(K, \mathrm{PGL}_n)$ may be (functorially) identified with an n^2-dimensional central simple K-algebra D_α; see Example 3.1. In particular, L/K is a splitting field for α if and only if L is a splitting field for D_α, i.e., $D_\alpha \otimes_K L = M_n(L)$. Recall that D is an H-crossed product iff H is a splitting group for D and $|H| = \deg(D)$.

Let $\mathrm{UD}(n,k)$ be the universal division algebra of degree n, i.e., the division algebra generated by two generic matrices, $X = (x_{ij})$ and $Y = (y_{ij})$, in $\mathrm{M}_n(k(x_{ij}, y_{ij}))$. Here x_{ij}, y_{ij} are algebraically independent variables over k. If the reference to k is clear from the context, we shall write $\mathrm{UD}(n)$ in place of $\mathrm{UD}(n,k)$. A famous theorem of Amitsur asserts that $\mathrm{UD}(n)$ is not a crossed product if n is divisible by p^3 for some prime p.

As an application of Theorem 1.2 we will prove the following result.

Theorem 1.3. *Let $Z(p^r)$ be the center of the universal division algebra $\mathrm{UD}(p^r)$, let K be a field extension of $Z(p^r)$ and let $D = \mathrm{UD}(p^r) \otimes_{Z(p^r)} K$. Suppose p^e is the highest power of p dividing $[K : Z(p^r)]$, where e is a non-negative integer and $e \leq r-1$. If A is a splitting group for D then*

$$p^{2r-2e-2} \mid |A|\,.$$

In particular, if $r \geq 2e+3$ then D is a noncrossed product.

If $K = Z(p^r)$, i.e., $D = \mathrm{UD}(p^r)$, we recover a theorem of Amitsur and Tignol; see [TA_1, Theorem 7.3]. If $e = 0$, i.e., D is a prime-to-p extension of $\mathrm{UD}(p^r)$, we recover a theorem of Rowen and Saltman [RS, Theorem 2.1] to the effect that D is not a crossed product for any $r \geq 3$.

Abelian subgroups of PGL_n carry a natural skew-symmetric form and their nontoral subgroups are isotropic with respect to this form; see Section 7. Thus symplectic modules and their Lagrangian submodules, used by Tignol and Amitsur to prove [TA_1, Theorem 7.3], naturally arise in our setting; in particular, they will be used in the proof of Theorem 1.3 in Section 8.

It is likely that Theorem 1.3 can also be proved by an application of Amitsur's specialization technique, along the lines of [RS, Section 2] and that such a proof will go through in prime characteristic (assuming $p \not| \operatorname{char}(k)$). We believe that our approach, based on the fixed points of nontoral subgroups, is of independent interest; in particular, it shows that Theorem 1.3 remains true if $\mathrm{UD}(p^r)$ is replaced by any central simple algebra whose corresponding PGL_n-variety has points fixed by certain nontoral subgroups of PGL_n; see Remark 8.4.

As another application of Theorem 1.2 with $G = \mathrm{PGL}_n$, we construct a noncrossed product division algebra over a "small" function field. Since the time of Amitsur's original examples, two other noncrossed product constructions have appeared in the literature, due, respectively, to Jacob—Wadsworth [JW] and Brussel [Br]. Both of these examples have the property that their centers are "smaller" and easier to describe than the center of Amitsur's "generic" example, $\mathrm{UD}(p^r, k)$.

The problem we address here is one of constructing noncrossed product examples over "small" fields in the geometric setting, i.e., noncrossed products D with center K such that K is a function field over an algebraically closed base field k of characteristic 0. Moreover, we would like "the size of K", as measured by $\mathrm{trdeg}_k(K)$, to be as small as possible.

Note that $\mathrm{trdeg}_k(K)$ cannot be ≤ 1 by Tsen's theorem. Moreover, division algebras D with $\mathrm{trdeg}_k(K) = 2$ are conjectured to be cyclic. At the other extreme, if $D = \mathrm{UD}(n)$ is Amitsur's original noncrossed product example (with n divisible by p^3 for some prime p) then $\mathrm{trdeg}_k(K) = n^2 + 1$.

In this paper we prove the following theorem.

Theorem 1.4. *Let p be a prime, $r \geq 2$ be an integer, and k be an algebraically closed field of characteristic 0. Then there exists a division algebra D of degree p^r with center K, such that*

(a) K is a finitely generated extension of k of transcendence degree 6 *and*

(b) no prime-to-p extension of D is a crossed product.

The idea of the proof is as follows. We show (see Section 8) that it is enough to construct a smooth PGL_{p^r}-variety X with two points whose stabilizers are "incompatible" symplectic modules $(\mathbb{Z}/p^r\mathbb{Z})^2$ and $(\mathbb{Z}/p\mathbb{Z})^6$; such varieties are fairly easy to construct. The difficult part is to reduce the dimension of X/PGL_{p^r} to 6; this is done in Section 9. Our argument there is based on a resolution result for the fixed point loci of finite abelian subgroups (we show that the fixed-point set of a finite abelian subgroup H can be resolved in such way that it has a component of the minimal possible codimension, equal to $\operatorname{rank} H$; see Theorem 9.3) and on a form of Bertini's theorem in the equivariant setting (Theorem 9.7). We believe Theorems 9.3 and 9.7 are of independent interest.

A. R. Wadsworth has pointed out to us that Theorem 1.4 can be proved by modifying the arguments of [JW]. This approach, based on valuation theory, cohomology, and the Merkurjev—Suslin theorem, yields the desired result under the assumption that $p \not| \operatorname{char}(k)$.

Throughout this paper we shall work over a fixed base field k which will be assumed to be algebraically closed and of characteristic zero. The assumption that k should be algebraically closed is usually not essential: generally speaking, the problems we wish to consider (such as constructing noncrossed products or proving lower estimates on the size of splitting fields) can only become harder after passing to the algebraic closure. The characteristic zero assumption is more serious, since most of our proofs ultimately rely on canonical resolution of singularities (via Proposition 2.2 and Theorem 2.5).

Acknowledgements

We would like to thank D. J. Saltman, J.-P. Serre, and A. R. Wadsworth for helpful discussions.

2. G-varieties

Preliminaries. A G-variety X is an algebraic variety with a G-action. Here G, X and all other algebraic objects in this paper are assumed to be defined over a fixed base field k. Unless otherwise specified, we shall assume that k is algebraically closed and of characteristic 0. The G-action on X is given by a morphism $G \times X \longrightarrow X$. If the reference to the action is clear from the context, we shall write gx for the image of (g, x) under this map. Given $x \in X$, the stabilizer of x is defined as $\{g \in G \mid gx = x\}$; we will denote this subgroup of G by $\operatorname{Stab}_G(x)$ or simply $\operatorname{Stab}(x)$ if the reference to G is clear from the context.

By a morphism $X \longrightarrow Y$ of G-varieties, we shall mean a G-equivariant morphism from X to Y. The same goes for rational morphism, isomorphism, birational morphism, etc., of G-varieties.

A G-variety X is called *primitive* if G transitively permutes the irreducible components if X. Equivalently, X is primitive iff $k(X)^G$ is a field. Note that an irreducible G-variety is necessarily primitive and that the converse holds if G is a connected group.

If X is a G-variety then any variety Y with $k(Y) = k(X)^G$ is called a rational quotient variety for X; we will often write $Y = X/G$. Note that X/G is only defined up to birational isomorphism and that X is a primitive G-variety iff X/G is irreducible. The inclusion $k(Y) = k(X)^G \hookrightarrow k(X)$ induces the rational quotient map $\pi \colon X \dashrightarrow X/G$. By a theorem of Rosenlicht $\pi^{-1}(y)$ is a single G-orbit for y in general position in X/G (see [Ro_1, Theorem 2], [Ro_2]).

A G-variety X is called *generically free* if $\operatorname{Stab}(x) = \{1\}$ for x in general position in X. We will usually consider G-varieties that are both primitive and generically free. Up to birational isomorphism, a primitive generically free G-variety may be viewed as a principal G-bundle over X/G and thus represents a class in $H^1(K, G)$, where $K = k(X)^G$; see [Po, Section 1.3]. We shall return to this connection in Section 3.

It is often convenient to have a concrete (biregular) model for X/G. If G is a finite group then, under rather mild assumptions on X, we have such a model in the form of a *geometric quotient*, which we shall denote by $X//G$. Here the quotient map $\pi\colon X \longrightarrow X//G$ is regular and each fiber of this map is a single G-orbit. For a precise definition and a detailed discussion of the geometric quotient we refer the reader to [PV, Section 4.2].

Lemma 2.1. *Let G be a finite group and X be a normal quasiprojective G-variety. Then*

(a) *X is covered by affine open G-invariant subsets.*

(b) *There exists a geometric quotient map $\pi\colon X \longrightarrow X//G$.*

(c) *Moreover, if X is projective then so is $X//G$.*

Proof. (a) By a theorem of Kambayashi, we may assume without loss of generality that $X \subset \mathbb{P}(V)$, where V is a finite-dimensional vector space, and G-acts linearly on X, via a representation $G \longrightarrow \mathrm{GL}(V)$; see [Ka, Theorem 2.5] or [PV, Theorem 1.7].

We want to show that every $x \in X$ has an affine G-invariant neighborhood in X. To construct this neighborhood, choose a homogeneous polynomial $h \in k[V]$ such that $h(gx) \neq 0$ for every $g \in G$ but $h(y) = 0$ for every $y \in \overline{X} - X$. After replacing h by the product of g^*h over all $g \in G$, we may assume h is G-invariant. Now $\{z \in \overline{X} \mid h(z) \neq 0\}$ is a desired affine G-invariant neighborhood of x.

(b) Follows from part (a) and [PV, Theorem 4.14].

(c) See [PV, Theorem 4.16]. □

The variety X_L. Let X be a generically free primitive G-variety, let $K = k(X)^G$ and let $cl(X)$ be the class of X in $H^1(K, G)$. Suppose L is a finitely generated field extension of K. Then X_L is defined as the G-variety representing the image of $cl(X)$ under the natural map $H^1(K, G) \longrightarrow H^1(L, G)$. In other words, $cl(X) \mapsto cl(X_L)$ under this map.

To construct X_L explicitly, let $Y \dashrightarrow X/G$ be a rational map such that $k(Y)/k(X/G)$ is precisely the extension L/K. Note that such a rational map exists because L is finitely generated over K and, hence, over k. Now we set $X_L = Y \times_{X/G} X$, where the G-action on X_L is induced from the G-action on X; cf. [Re, Section 2.6].

We emphasize that X_L is only defined up to birational isomorphism (of G-varieties). We we will often want to work with a specific model for X_L which is smooth or projective or has "small" stabilizers (or all of the above). The existence of such models is guaranteed by Proposition 2.2 and Theorem 2.5.

Smooth projective models for G-varieties.

Proposition 2.2. *Every G-variety is birationally isomorphic to a smooth projective G-variety.*

Proof. Let X be a G-variety. By [RY, Proposition 7.1], X is birationally isomorphic to a complete G-variety. (Note that the proof of [RY, Proposition 7.1] is based on Sumihiro's equivariant completion theorem.) Thus we may assume without loss of generality that X is complete.

Now by [Ka, Theorem 2.5] there exists a projective representation $G \hookrightarrow \mathrm{PGL}(V)$ and a closed G-invariant subvariety X' of $\mathbb{P}(V)$ such that X and X' are birationally isomorphic as G-varieties. After replacing X by X', we may assume X is projective. Now apply the canonical resolution of singularities theorem (see either [V, Theorem 7.6.1] or [BM, Theorem 13.2]) to X to construct a smooth projective model. $\square$

Definition 2.3. We shall call an algebraic group H *Levi-commutative* if H is a semidirect product of a diagonalizable group D and a unipotent group U, where $U \triangleleft H$ is the unipotent radical of the identity component H_0 of H.

We shall denote $U = R_u(H_0)$.

Lemma 2.4. *Let H be an algebraic group and let H_0 be the identity component of H. The following conditions are equivalent.*

(i) H is Levi-commutative,

(ii) $H/R_u(H_0)$ is commutative,

(iii) every reductive subgroup of H is commutative, and

(iv) every linear representation of H has 1-dimensional H-invariant subspace.

Proof. The equivalence of (i), (ii) and (iii) follows from the Levi decomposition theorem (see [OV, Section 6.4]). The equivalence of (i) and (iv) is proved in [RY, Lemma A.1]. $\square$

Theorem 2.5. *Let X be a G-variety. Then there exists a sequence of blowups*

$$X_n \longrightarrow X_{n-1} \longrightarrow \ldots \longrightarrow X_0 = X$$

such that X_n is smooth and $\mathrm{Stab}(x)$ *is Levi-commutative for every $x \in X_n$.*

Proof. See [RY, Theorem 1.1]. $\square$

Going up and going down.

Theorem 2.6 (Going down)**.** *Let H be a Levi-commutative group (see Definition 2.3) and let $X \dashrightarrow Y$ be a rational map of H-varieties. Suppose Y is complete and X has a smooth point fixed by H. Then Y has a smooth point fixed by H.*

Proof. See [RY, Propositions 5.3 and A.2]. $\square$

Theorem 2.7 (Going up)**.** *Let H be a finite abelian group of prime power order p^n and let $f\colon X \dashrightarrow Y$ be a dominant rational map of H-varieties. Suppose*

(i) Y is irreducible,

(ii) X is complete,

(iii) $\dim(X) = \dim(Y)$ *and f is dominant,*

(iv) H has a smooth fixed point in Y, and

(v) $\deg(f)$ *is not divisible by p^{e+1}.*

Then there exists a subgroup H' of H such that $|H'| \geq p^{n-e}$ and

(a) H' has a fixed point in X.

(b) Moreover, if $X \dashrightarrow Z$ is a rational map of complete H-varieties then H' has a fixed point in Z.

This theorem is a generalization of [RY, Propositions 5.5 and A.4], where e is assumed to be 0. Our proof below is based on an argument of Kollár and Szabó; cf. [RY, Proposition A.4]. Our applications will only use (a); however, part (b) is needed for the inductive argument.

A convenient way to visualize the setting of Theorem 2.7 is by means of the diagram

$$\begin{tikzcd} X \arrow[r, dashed, "h"] \arrow[d, "f"'] & Z \\ Y & \end{tikzcd}$$

If $e = 0$ the theorem allows us to lift an H-fixed point from Y to X, then transport it to Z. (A similar but slightly weaker statement is true if $e \geq 1$.) We will make use of such diagrams in the proof.

Proof. The proof is by induction on $d = \dim Y$. If $\dim Y = 0$ then Y is a point, X is a set of $\deg(X/Y)$ points, and the desired result follows from a simple counting argument.

To perform the induction step, we assume that the theorem holds whenever $\dim(Y) \leq d-1$. Let $y \in Y$ be a smooth fixed point, $B_y(Y)$ be the blowup of Y at y, and $Y' \subset B_yY$ be the exceptional divisor. Note that H acts linearly on $Y' = \mathbb{P}^{\dim(Y)-1}$ and, hence, has a fixed point in Y'; see Lemma 2.4(iv). This fixed point will be smooth because every point of Y' is smooth.

Let $X = \bigcup_i X_i$ be the decomposition of X into irreducible components. It is enough to find the required fixed point in one of the components X_i which is mapped dominantly onto Y; thus, we may assume that all X_i are mapped dominantly onto Y.

It follows that each map $X_i \dashrightarrow B_yY$ is dominant; let $\overline{X}_i$ be the normalization of B_yY in the field of rational functions on X_i, $\overline{X}$ be the disjoint union of all $\overline{X}_i$ (in other words, $\overline{X}$ is the normalization of B_yY in the ring $k(X) = \bigoplus_i k(X_i)$), and $\overline{f} : \overline{X} \longrightarrow B_yY$ be the natural morphism. Clearly, H acts on $\overline{X}$ and $\overline{f}$ is H-equivariant. Each $\overline{X}_i$, it is birationally isomorphic to X_i. Together these birational isomorphisms yield an H-equivariant birational isomorphism $\overline{X} \dashrightarrow X$.

Let $F_1, F_2, \ldots \subset \overline{X}$ be the divisors lying over Y'. Note that even though $\overline{X}$ is not necessarily complete, each F_i is complete since it is mapped finitely to a complete variety Y'.

The group H acts on the set $\{F_i\}$. Let $\mathcal{F}_j$ denote the H-orbits in $\{F_i\}$. Choose a divisor $F_j^* \in \mathcal{F}_j$ in each orbit. By the ramification formula (see, e.g., [L, Corollary XII.6.2]),

$$\deg(X/Y) = \sum_j |\mathcal{F}_j| \cdot \deg(F_j^*/E) \cdot e(\overline{f}, F_j^*)\,,$$

where $e(\overline{f}, F_j^*)$ denotes the ramification index of $\overline{f}$ at the generic point of F_j^*. Since $\deg(X/Y)$ is not divisible by p^{e+1}, $|\mathcal{F}_j| \cdot \deg(F_j^*/E)$ is not divisible by p^{e+1} for some j. For this j, set $X' = HF_j^* = \bigcup_{F_i \in \mathcal{F}_j} F_i$; this variety is complete since each F_i is complete. Let $f' \colon X' \longrightarrow Y'$ be the restriction of $\overline{f} \colon \overline{X} \longrightarrow B_z(Y)$ to X'; the degree of f' is equal to $|\mathcal{F}_j| \cdot \deg(F_j^*/E)$, and hence, is not divisible by p^{e+1}. Let $h' \colon X' \dashrightarrow X$ be the restriction of $\overline{X} \dashrightarrow X$ to X'. Note that h' is well-defined, since $\overline{X}$ is normal, X is complete, and X' is a divisor in $\overline{X}$.

By our construction, $\dim(Y') = d - 1$ and conditions (i)–(v) hold for the map $f'\colon X' \dashrightarrow Y'$. Applying the induction assumption to the diagram

$$\begin{tikzcd} X' \arrow[r, dashed, "h'"] \arrow[d, "f'"'] & X \\ Y' & \end{tikzcd}$$

we prove part (a). Applying the induction assumption to the diagram

$$\begin{tikzcd} X' \arrow[r, dashed, "h'"] \arrow[d, "f'"'] & X \arrow[r, dashed, "h"] & Z \\ Y' & & \end{tikzcd}$$

we prove part (b). $\square$

Remark 2.8. Theorems 2.6 and 2.7 are valid over an algebraically closed field of arbitrary characteristic; the proofs given above are characteristic-free.

3. Two interpretations of H^1

Let A be a finite-dimensional algebra over k. We do not assume that A is commutative, associative or has an identity element. Let K is a field extension of k. We shall say that a K-algebra B is of type A if $B_{\overline{K}} \simeq A_{\overline{K}}$, where $\overline{K}$ is the algebraic closure of K. (Here, as usual, $B_{\overline{K}} \stackrel{\text{def}}{=} B \otimes_K \overline{K}$ and $A_{\overline{K}} \stackrel{\text{def}}{=} A \otimes_k \overline{K}$.)

Let $G = \mathrm{Aut}_k(A)$. It is easy to see that G is a closed subgroup of $\mathrm{GL}_{\dim(A)}$; thus it is an algebraic group. We now have the following bijections.

$$\begin{array}{ccc} H^1(K,G) & \longleftrightarrow & \left\{ \begin{array}{l} \text{Birational isomorphism classes} \\ \text{of primitive generically free} \\ G\text{-varieties } X \text{ with } k(X)^G = K \end{array} \right\} \\ \updownarrow & & \\ \{K\text{-algebras of type } A\} & & \end{array}$$

The horizontal correspondence is described in [Po, Section 1.3]; the vertical one in [Se$_2$, Section X.2] or [KMRT, Proposition 29.1]. Note that the above diagram is functorial in K and that the correspondences in it are bijections of pointed sets: the identity elements of $H^1(K,G)$ corresponds to the "split" algebra A_K and to the "split" variety $X = X_0 \times G$, where $k(X_0)^G = K$; see Definition 4.1.

In this paper we shall be primarily interested in passing back and forth between G-varieties and algebras of type A. In other words, we would like to construct an explicit correspondence $X \mapsto B$ which completes the triangle in the above diagram. Given a generically free primitive G-variety X with $k(X)^G = K$, we define $B = RMaps_G(X, A)$. Here $RMaps_G(X, A)$ is the set of G-equivariant rational maps $X \dashrightarrow A$, where we view A as a k-vector space with a G-action. The k-algebra structure on A gives rise to a K-algebra structure on B via

$$(f_1 + f_2)(x) \stackrel{\text{def}}{=} f_1(x) + f_2(x) \ ,$$
$$(f_1 f_2)(x) \stackrel{\text{def}}{=} f_1(x) f_2(x) \ ,$$
$$(\alpha f_2)(x) \stackrel{\text{def}}{=} \alpha(x) f_1(x) \ .$$

Here $f_1, f_2 \in RMaps_G(X, A)$, $\alpha \in K$, x is an element of X in general position, and the operations in the right hand sides of the above formulas are performed in A. The correspondence $X \mapsto RMaps_G(X, V)$ completes the triangle in the above diagram; see [Re, Proposition 8.6 and Lemma 12.3].

Example 3.1. $A = \mathrm{M}_n(k)$ is the algebra of $n \times n$-matrices over k. By a theorem of Wedderburn, B is a K-algebra of type M_n if and only if B is a central simple K-algebra; see e.g., [KMRT, Theorem 1.1] or [Se$_2$, X.5, Proposition 7].

Note that $\mathrm{Aut}_k(A) = \mathrm{PGL}_n$. Thus, if K is a finitely generated field extension of k, every central simple K-algebra B of degree n is of the form $RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n(k))$ for some generically free irreducible PGL_n-variety X with $k(X)^G = K$. Moreover, the G-variety X is uniquely determined up to birational isomorphism. For example, if $B = \mathrm{UD}(n)$ is the universal division algebra of degree n generated by two generic matrices then $B = RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n(k))$, where $X = \mathrm{M}_n(k) \times \mathrm{M}_n(k)$ and PGL_n acts on X by simultaneous conjugation. This description of $\mathrm{UD}(n)$ is due to Procesi; see [Pr, Theorem 2.1].

Example 3.2. $A = \mathbf{O}$ is the 8-dimensional split Cayley algebra (otherwise known as the split octonion algebra). Then $\mathrm{Aut}(\mathbf{O})$ is the exceptional group G_2. By a theorem of Zorn, B is a K-algebra of type $\mathbf{O}$ if and only if B is a Cayley algebra over K. Cayley algebras are thus in natural 1—1 correspondence with generically free irreducible G_2-varieties; see [Re, Remark 11.4], [Se$_3$, Section 8.1], [KMRT, Proposition 33.24].

Example 3.3. A is the 27-dimensional (split) Albert algebra (otherwise known as an exceptional simple Jordan algebra) defined over k. Then $\mathrm{Aut}(A)$ is the exceptional group F_4. Algebras of type A are precisely the Albert algebras, i.e., a 27-dimensional exceptional simple Jordan algebras; see e.g., [KMRT, p. 517], [Se$_3$, Section 9].

Remark 3.4. The results of this section remain valid if the algebra A is replaced by a more general algebraic object consisting of a vector space with a tensor on it. Such objects are called structured spaces in [Re]. We refer the reader there for details; see also [KMRT, Section 29].

4. Splitting fields

Definition 4.1. Let G be an algebraic group and X be a primitive generically free G-variety, $K = k(X)^G$ and $cl(X) =$ the class of X in $H^1(K, G)$. We will say that X is *split* if X is birationally isomorphic to $X/G \times G$ (as a G-variety). Equivalently, X is split if there exists a rational section $X/G \dashrightarrow X$ or, if $cl(X) = 1$; see, e.g., [Po, 1.4.1].

A field extension L of K is called a *splitting field* of X if X_L is split. Equivalently, L is a splitting field if the image of $cl(X)$ under the natural map $H^1(K, G) \longrightarrow H^1(L, G)$ is trivial.

Remark 4.2. Recall that an algebraic group G is called *special* if every generically free G-variety is split. Special groups were studied by Serre [Se_1] and classified by Grothendieck [Gro, Theorem 3]; see also [PV, Theorem 2.8]. In particular, GL_n, SL_n, Sp_{2n}, and the additive group $\mathrm{G_a}$ are special. Moreover, it is easy to see that if N is a normal subgroup of G and both N, G/N are special, then so is G. In particular, every connected solvable group is special; cf. [PV, Section 2.6].

Split G-varieties.

Lemma 4.3. *Let G be an algebraic group, let X be a split G-variety and let H be a Levi-commutative subgroup of G (see Definition 2.3). If H has a smooth fixed point in X then*

(a) H is contained in a Borel subgroup of G. Moreover,

(b) if H is diagonalizable then it is contained in a maximal torus of G.

Proof. Since X is split, it is birationally isomorphic to $X_0 \times G$, where X_0 is a projective variety (a projective model for X/G). Let B is a Borel subgroup of G. Consider the rational G-equivariant map

$$X \simeq X_0 \times G \dashrightarrow X_0 \times G/B .$$

Since $X_0 \times G/B$ is a complete variety, the Going Down Theorem 2.6 tells us that H fixes a point of $X_0 \times G/B$. Consequently, H is contained is a conjugate of B, and part (a) follows. Part (b) is immediate from part (a) and [Bor_2, Theorem 10.6(5)]. □

Remark 4.4. Note that our proof of Lemma 4.3 relies only on the Going Down Theorem and not on Proposition 2.2. In particular, Lemma 4.3 is valid in arbitrary characteristic; see Remark 2.8.

Proof of Theorem 1.1. Consider the natural projection map $X_L \dashrightarrow X$ of G-varieties. Here L is a splitting field for X, i.e., X_L is split. By Proposition 2.2, we may assume without loss of generality that X_L is smooth and projective. Let p^e be the maximal power of p dividing $[L : K] = \deg(X_L/X)$. By the Going Up Theorem 2.7(a), there exists a point $y \in X_L$ and a subgroup H' of H such that (i) $[H : H']$ divides p^e and (ii) $H' \subset \mathrm{Stab}(y)$. Now (i) says that $[H : H']$ divides $[L : K]$ and (ii), in combination with Lemma 4.3(b), says that H' is toral. □

Nontoral subgroups.

Definition 4.5. Let G be an algebraic group and let H be an abelian p-subgroup of G. The *depth* of H is defined as the smallest integer i such that H has a toral subgroup of index p^i.

Recall that a prime number p is called a *torsion prime* for G if G has a nontoral abelian p-subgroup H, i.e., an abelian p-subgroup H of depth ≥ 1. Following [Se_5, 1.3] we will denote the set of torsion primes for G by $Tors(G)$.

Remark 4.6. Torsion primes have been extensively studied; see [Bor_1], [SS], [St], [Se_5]. In particular, $Tors(G) = Tors(G')$ if G' is a derived subgroup of G; see [Se_5, 1.3.2]. If $f\colon \overline{G} \longrightarrow G$ is the universal cover of G then $Tors(G)$ is the union of $Tors(\overline{G})$ and the set of prime divisors of $\mathrm{Ker}(f)$; see [Se_5, 1.3.3].

For simply connected simple groups the torsion primes are given by the following table:

Type of G	$Tors(G)$
A_n or C_n	$\emptyset$
B_n $(n \geq 3)$, D_n $(n \geq 4)$ or G_2	$\{2\}$
F_4, E_6, or E_7	$\{2, 3\}$
E_8	$\{2, 3, 5\}$

For details see [Bor$_1$, Proposition 4.4], [St, Corollary 1.13] or [Se$_5$, 1.3.3].

Using the terminology of Definition 4.5, we can rephrase Theorem 1.1 as follows.

Theorem 4.7. *Let G be an algebraic group, H be a finite abelian p-subgroup of G of depth d, X be a generically free G-variety and $K = k(X)^G$. If X has a smooth H-fixed point and L/K is a splitting field of X then $p^d \mid [L:K]$.*

In particular, if $X = V$ is a generically free linear representation of G then $[L:K]$ is divisible by every torsion prime of G. $\square$

Let G be an algebraic group and let S be a special subgroup containing G. (For example, S can be taken to be GL_n, SL_n or Sp_{2n}.) We shall view S as a G-variety with respect to the left multiplication action; it is easy to see that this variety is generically free.

Corollary 4.8. *Let G be an algebraic group, H be a finite abelian p-subgroup of G of depth d and S be a special group containing G, as above. Suppose $K = k(S)^G$ and L/K is a splitting field for S (as a G-variety). Then $p^d \mid [L:K]$.*

Proof. Let $\overline{S}$ be a smooth projective model of S (as an S-variety); see Proposition 2.2. Let V be a generically free linear representation of S. Since S is special, V is split as an S-variety. Thus there exists an S-equivariant dominant rational map $f\colon V \dashrightarrow S \simeq \overline{S}$. Since $G \subset S$, we can view $f\colon V \dashrightarrow \overline{S}$ as a dominant rational map of G-varieties. Since V has a H-fixed point, the Going Down Theorem 2.6 tells us that so does $\overline{S}$. Applying Theorem 4.7 to the smooth variety $X = \overline{S}$, we conclude that $p^d \mid [L:K]$, as claimed. $\square$

Remark 4.9. Let G be a simple group. A theorem of Tits asserts that every G-variety X can be split by an extension L/K, where $K = k(X)^G$ and every prime factor of $[L:K]$ lies in $Tors(G)$; see [Se$_3$, 2.3]. This gives a partial converse to Theorem 4.7.

More precisely, the results of [T_2] show that every G-variety can be split by an extension of degree dividing $n(G)$, where $n(G)$ is given by the following table.

Type	Simply Connected	Not Simply Connected
A_n	1	$n+1$
B_n	$2^{\sup(1,n-4)}$	2^n
C_n	1	$2^{v_2(n)+1}$
D_n	$2^{\sup(1,n-5)}$	$2^{v_2(n)+n}$
G_2	2	–
F_4	6	–
E_6	6	$2\cdot 3^4$
E_7	12	$2^5\cdot 3$
E_8	$2^7\cdot 3^3\cdot 5$	–

Here G is an almost simple group of the indicated type (recall that G is almost simple if the center $Z(G)$ is finite and $G/Z(G)$ is simple) and $v_2(m)$ denotes the highest power of 2 dividing m.

Note that the terminology of [T_2] is somewhat different from ours. A primitive G-variety X corresponds to a group of inner type over $k(X)^G$ (and if G is simply connected, then of strongly inner type). With these conventions, the entries for all group types other than E_8 come directly from [T_2, Proposition A1] or from [T_2, Propositions 1 and 2].

Our entry for E_8 follows from [T_2, Corollaire 2] and the fact that $n(G)$ may be taken to be the degree of a splitting field for one particular "generic" E_8-variety; see [T_1, Proposition 8]. (Recall that we are working in characteristic zero.) In fact [T_2, Corollaire 2] implies that $n(E_8)$ may be taken to be one of the numbers $2^7\cdot 3\cdot 5$, $2^6\cdot 3^2\cdot 5$ or $2^4\cdot 3^3\cdot 5$ (it is not currently known which one). The entry for $n(E_8)$ in our table is the least common multiple of these three numbers.

Combining the above-mentioned results of [T_2] with Theorem 4.7, we obtain the following upper bound on the depth of abelian p-subgroups of quasi-simple algebraic groups.

Corollary 4.10. *Let G be an almost simple algebraic group and let H be a finite abelian p-subgroup of G of depth d (not necessarily elementary). Then p^d divides the number $n(G)$ given in Remark 4.9.* □

5. Examples

In this section we illustrate Theorem 1.1 for several classes of groups. The application of Theorem 1.1 to the case $G = \mathrm{PGL}_n$ will come up later, after we discuss the nontoral subgroups of PGL_n in Section 7; see Lemma 8.1 below.

Orthogonal groups: splitting fields of quadratic forms. Let K be a finitely generated field extension of k. Recall that quadratic forms q over K are in 1—1 correspondence with primitive generically free O_n-varieties X such that $k(X)^{O_n} = K$; see [Se$_4$, III. Appendix 2.2] or [KMRT, Section 29E]. In particular, a field extension L/K splits the form if and only if it splits the corresponding variety.

Proposition 5.1. Let $q = <a_1, \ldots, a_n>$ be a quadratic form over K. Then

(a) there exists a splitting field L for q such that L/K is a Galois extension with $\mathrm{Gal}(L/K) = (\mathbb{Z}/2\mathbb{Z})^l$ for some $l \le [\frac{n+1}{2}]$.

(b) Suppose $a_1, \ldots, a_n$ are algebraically independent variables over k, $K = k(a_1, \ldots, a_n)$ and L/K is a splitting field for q. Then $[L : K]$ is divisible by $2^{[\frac{n+1}{2}]}$.

Proof. (a) Suppose $n = 2m$ is even. Let

$$L = K(\sqrt{-a_2/a_1}, \ldots, \sqrt{-a_{2m}/a_{2m-1}})\,.$$

Note that L is a Galois extension of K and $\mathrm{Gal}(L/K) = (\mathbb{Z}/2\mathbb{Z})^l$ for some $l \le m$. Moreover, since $<a_{2i-1}, a_{2i}> \simeq <a_{2i-1}, -a_{2i-1}>$ for $i = 1, \ldots, m$,

$$q \simeq <a_1, -a_1> \oplus \cdots \oplus <a_{2m-1}, -a_{2m-1}> \simeq 0$$

in the Witt ring of L. This shows that q splits over L.

If $n = 2m + 1$ is odd then a similar argument shows that

$$L = k(\sqrt{-a_2/a_1}, \ldots, \sqrt{-a_{2m}/a_{2m-1}}, \sqrt{a_{2m+1}})$$

is a splitting field for q with $\mathrm{Gal}(L/K) = (\mathbb{Z}/2\mathbb{Z})^l$ and $l \le m + 1$.

(b) Consider the O_n-variety $X = \mathrm{M}_n$, with O_n acting (linearly) on X by left multiplication. Recall that $k(X)^{O_n} = k(b_{ij} \mid 1 \le i \le j \le n)$, where $b_{ij}(x)$ is the dot product of the ith and the jth columns of the matrix $x \in \mathrm{M}_n$; see, e.g., [DC, Section 2.10] or [Re, Lemma 6.4]. Note that since $\dim(X/O_n) = \dim(X) - \dim(O_n) = \frac{n(n+1)}{2}$, the generators b_{ij} are algebraically independent over k. The quadratic form corresponding to X is the "generic form" $q_X = \sum_{i \le j} b_{ij} x_i x_j$ defined over $k(b_{ij})$. Let Y be the subvariety of X consisting of $n \times n$-matrices with mutually orthogonal columns. Then Y is irreducible (see [Re, Example 3.10]) and the quadratic form corresponding to Y is the "generic diagonal" form $q = \sum_{i=1}^n a_i x_i^2$ which appears in the statement of part (b). Here $a_i = b_{ii}$ and q is defined over $K = k(a_1, \ldots, a_n)$. We can now view the usual orthogonalization process in k^n as an O_n-equivariant rational map $f\colon X \dashrightarrow Y$. That is, we view a matrix $x \in \mathrm{M}_n$ as a collection of n column vectors. To construct $f(x) \in Y$, we apply the orthogonalization process to this collection; the resulting n mutually orthogonal vectors form the columns of $f(x)$ (see [Re, Example 3.10] for details).

Note that the point $0_{n\times n}$ is a smooth point of X fixed by all of O_n; here $0_{n\times n}$ is the $n \times n$ zero matrix. Let Y' be a smooth projective model of Y (see Proposition 2.2); we can thus think of f as an O_n-equivariant rational map $X \dashrightarrow Y'$. Let $H \simeq (\mathbb{Z}/2\mathbb{Z})^n$ be the diagonal subgroup of O_n. By the Going Down Theorem 2.6, Y' has an H-fixed point. This point is smooth because every point of Y' is smooth. Since L splits q, it splits the O_n-variety Y or, equivalently, the O_n-variety Y'. Thus Theorem 4.7 tells us that $2^d \mid [L : K]$, where d is the depth of H. Since the dimension of any maximal torus in O_n is $[\frac{n}{2}]$, $d \ge n - [\frac{n}{2}] = [\frac{n+1}{2}]$, as claimed. □

The same argument with the group SO_n in place of O_n yields the following variant of Proposition 5.1. Note that elements $H^1(K, SO_n)$ represent equivalence classes of quadratic forms of determinant 1; cf. [Re, Example 8.4(b)] or [KMRT, (29.29)].

Proposition 5.2. Let $K = k(a_1, \dots, a_n)$, $q = <a_1, \dots, a_n>$ be a quadratic form of determinant 1 over K. Then

(a) there exists a splitting field L for q such that L/K is a Galois extension with $\mathrm{Gal}(L/K) = (\mathbb{Z}/2\mathbb{Z})^l$ for some $l \le [\frac{n-1}{2}]$.

(b) Suppose $a_1, \dots, a_{n-1}$ are algebraically independent variables over k, $a_n = (a_1 \dots a_{n-1})^{-1}$, and L/K is a splitting field for q. Then $[L:K] \ge 2^{[\frac{n-1}{2}]}$. $\square$

Exceptional groups G_2, F_4, $3E_6$ and $2E_7$. Let V be a generically free linear representation of G, let $K = k(V)^G$ and let L/K be a splitting field of V. Theorem 4.7 tells us that $[L:K]$ is divisible by 2 if $G = G_2$ and by 6 if $G = F_4$, $3E_6$ or $2E_7$. (Here $3E_6$ and $2E_7$ denote the simply connected groups of type E_6 and E_7 respectively.) If $G = G_2$, F_4 or $3E_6$ then this result is sharp. In other words, V can be split by L/K such that $[L:K]$ equals 2, if $G = G_2$ and 6, if $G = F_4$ or $3E_6$; see Remark 4.9.

Exceptional group E_8. Recall that by a theorem of Adams [Ad] E_8 has two maximal elementary abelian 2-subgroups (up to conjugacy): $D(T)$ of rank 9 and EC^8 of rank 8. Here we are following the notational conventions of [Ad, Section 2]; in particular, $D(T)$ means "double 2-torus" and EC^8 means "exotic candidate of rank 8". By construction $D(T)$ has depth 1.

Proposition 5.3. *The subgroup $EC^8 \simeq (\mathbb{Z}/2\mathbb{Z})^8$ of E_8 has depth* 2.

Our proof of this proposition uses the theory of quadratic forms over $\mathbb{Z}/2\mathbb{Z}$. Recall that if q is a quadratic form on $V = (\mathbb{Z}/2\mathbb{Z})^m$, the associated symmetric (or, equivalently, skew-symmetric) bilinear form $b_q \colon V \times V \longrightarrow V$ is defined by $b_q(v, w) = q(v+w) - q(v) - q(w)$. Note that the "usual" relationship between q and b_q breaks down in characteristic 2: in particular, $b_q(v, v) = 0$ for any $v \in V$. The kernel of b_q is called *the radical* of q.

We shall say that $v \in V$ is an *anisotropic* vector for q if $q(v) = 1$ and an *isotropic* vector if $q(v) = 0$. In the sequel we shall be interested in counting the number of anisotropic vectors for a given form q. This is not a difficult task (at least in principle) because q can always be written as a direct sum of quadratic forms of dimension 1 and 2 (see, e.g., [Pf, Theorem 1.4.3]), and if $q = r \oplus s$ then a simple counting argument shows that

$$\begin{aligned} |q^{-1}(0)| &= |r^{-1}(0)| \cdot |s^{-1}(0)| + |r^{-1}(1)| \cdot |s^{-1}(1)| \\ |q^{-1}(1)| &= |r^{-1}(1)| \cdot |s^{-1}(0)| + |r^{-1}(0)| \cdot |s^{-1}(1)| \,. \end{aligned} \tag{5.1}$$

Lemma 5.4. *Let q be a quadratic form on $V = (\mathbb{Z}/2\mathbb{Z})^7$. Suppose the radical of q has dimension 1. Then q has* 56, 64 *or* 72 *anisotropic vectors in V.*

Proof. Write $q \simeq q_1 \oplus q_2 \oplus q_3 \oplus <e>$, where q_1, q_2 and q_3 are regular 2-dimensional quadratic forms and $e = 0$ or 1; see, e.g., [Pf, Theorem 1.4.3]. (Here, the 1-dimensional form $<e>$ is the radical of q.) Note that over $\mathbb{Z}/2\mathbb{Z}$ there are only two classes of regular 2-dimensional quadratic forms: the hyperbolic form h given by $h(x_1, x_2) = x_1 x_2$ and the anisotropic form $a(x_1, x_2) = x_1^2 + x_2^2 + x_1 x_2$. Since $a \oplus a \simeq h \oplus h$ (see [Pf, Example 2.4.5]), we may assume without loss of generality that $q_2 = q_3 = h$.

Case 1: $e = 1$. Using (5.1) it is easy to see that if q_0 is any quadratic form on $(\mathbb{Z}/2\mathbb{Z})^m$ then $q = q_0 \oplus <1>$ has exactly 2^m anisotropic vectors in $(\mathbb{Z}/2\mathbb{Z})^{m+1}$. In our situation $q_0 = q_1 \oplus q_2 \oplus q_3$ and $m = 6$; thus we conclude that $|q^{-1}(1)| = 64$. From now on we shall assume that $e = 0$.

Case 2. $q = h \oplus h \oplus h \oplus <0>$. We apply (5.1) to this form recursively. Since $|h^{-1}(0)| = 3$ and $|h^{-1}(1)| = 1$, we obtain $|q^{-1}(1)| = 56$.

Case 3. $q = a \oplus h \oplus h \oplus <0>$. We note that $|a^{-1}(0)| = 1$ and $|a^{-1}(1)| = 3$, and apply (5.1) recursively, to conclude that $|q^{-1}(1)| = 72$.

This completes the proof of the lemma. $\square$

Proof of Proposition 5.3. Recall that $EC^8 = A_1 \times A_2 \subset G_2 \times F_4 \subset E_8$, where $A_1 = (\mathbb{Z}/2\mathbb{Z})^3$ is the unique (up to conjugacy) nontoral abelian 2-subgroup of G_2 and A_2 is the unique (again, up to conjugacy) nontoral abelian 2-subgroup of F_4; see [Gri, Theorem 2.17]. Thus, A_1 has a subgroup of index 2 which is toral in G_2, and A_2 has a subgroup of index 2 which is toral in F_4. Taking a direct product of these toral subgroups, we construct a subgroup of EC^8 of index 4 which is toral in $G_2 \times F_4$ and, hence, in E_8. This proves that the depth of EC^8 is ≤ 2.

It remains to show that the depth of EC^8 is ≥ 2. Recall that elements of E_8 of order 2 fall into two conjugacy classes: class A and class B; cf. [Ad, Section 5] or [Gri, (2.14)]. If T is a maximal torus in E_8 and $T_{(2)} = \{t \in T \, : \, t^2 = 1\}$ then we have a naturally defined W_{E_8}-invariant quadratic form q on $T_{(2)} \simeq (\mathbb{Z}/2\mathbb{Z})^8$; see [Gri, Definition 2.15]. By [Gri, Lemma 2.16] this form is non-singular and has maximal Witt index; moreover, an element x of $T_{(2)}$ is of type A in E_8 if $q(x) = 1$ and of type B if $q(x) = 0$.

In particular, of the 255 nonidentity elements of $T_{(2)}$, 120 are of type A and 135 are of type B. On the other hand, of the 255 nonidentity elements of EC^8, 56 are of type A and 199 are of type B; see [Ad, Section 5].

We now proceed to prove that the depth of EC^8 is ≥ 2. Assume, to the contrary, that EC^8 has a toral subgroup U of rank 7. Since q is non-singular (i.e., the associated symplectic form b_q is non-degenerate) on $T_{(2)}$, the radical of $q_{|U}$ is of dimension ≤ 1. On the other hand, since $\dim(U)$ is odd, the radical of $q_{|U}$ cannot be trivial; thus it has dimension exactly 1. By Lemma 5.4, q has at least 56 anisotropic vectors in U, i.e., U has at least 56 elements of type A. On the other hand, EC^8 has exactly 56 elements of type A. We therefore conclude that every element of type A lies in U. We claim that this is impossible because the elements of type A generate EC^8. This contradiction will complete the proof of the proposition.

To prove the claim, recall that $EC^8 = A_1 \times A_2$, where $A_1 \simeq (\mathbb{Z}/2\mathbb{Z})^3$ lies in G_2 and $A_2 = (\mathbb{Z}/2\mathbb{Z})^5$ lies in F_4, as above. Moreover, A_2 has a subgroup R of order 4 (called the radical of EC^8) such that

$$S = (A_2 - R) \cup (A_1 R - R)$$

is precisely the set of elements of EC^8 of type A; see [Gri, Theorem 2.17]. We want to show that $<S> = EC^8$. Indeed, $A_2 - R$ contains 28 of the 32 elements of A_2; these elements clearly generate all of A_2. Thus $A_2 \subset <S>$. In particular, $R \subset <S>$. Now R, together with $A_1 R$ generate A_1. We thus conclude that both A_1 and A_2 lie in $<S>$. This proves that $EC^8 = A_1 \times A_2 = <S>$, as claimed. $\square$

We are now ready to give an alternative proof of a theorem of Serre.

Corollary 5.5. *(Serre, see* [T_1, Proposition 9, p. 30] *or* [T_2, p. 1132]*) Suppose $E_8 \hookrightarrow S$, where $S = \mathrm{GL}_n$, SL_n or Sp_{2n} for some n. We shall view S as an E_8-variety via the left multiplication action. Suppose $K = k(S)^{E_8}$ and L/K is a splitting field of S. Then $[L : K]$ is divisible by 60.*

Proof. Recall 2 and 3 are torsion primes of E_8, i.e., E_8 has an abelian 3-subgroup and an abelian 5-subgroup, both of depth ≥ 1. Moreover, by Proposition 5.3, E_8 contains an abelian 2-subgroup of depth 2. Thus Corollary 4.8 tells us that $[L : K]$ is divisible by $2^2 \cdot 3 \cdot 5 = 60$. □

Exceptional group E_7 (adjoint). We will now show that the (adjoint) group E_7 has an elementary abelian 2-subgroup of depth ≥ 2. We begin with the following lemma.

Lemma 5.6. *Let $f \colon G \longrightarrow G'$ be a surjective homomorphism of algebraic groups, such that $\mathrm{Ker}(f)$ is special. Suppose H is a finite abelian subgroup of G and $f(H)$ is toral in G'. Then H is toral in G.*

Proof. Suppose $f(H) \subset T' \subset G'$, where T' be a torus in G'. Denote $f^{-1}(T')$ by S. Then $H \subset S \subset G$. Moreover, since both $\mathrm{Ker}(f)$ and $S/\mathrm{Ker}(f) \simeq T'$ are special, we conclude that S is special as well; see Remark 4.2. This means that H is toral in S (see e.g., [Se_5, 1.5.1] or Example 6.6); hence, H is toral in G. □

Proposition 5.7. *The (adjoint) group E_7 has an elementary abelian 2-subgroup of depth ≥ 2.*

Our proof uses the idea of Adams (see [Ad, Introduction]) to study nontoral 2-subgroups in groups of type E_7 by embedding $2E_7$ into E_8.

Proof. Let EC^8 be a maximal elementary abelian subgroup of E_8 of rank 8, as in Proposition 5.3. As we mentioned in the proof of that proposition, EC^8 has 56 elements of type A (in E_8). Let x be one of these 56 elements. Denote the centralizer $C_{E_8}(x)$ by C. Note that $EC^8 \subset C$. Moreover, $C \simeq 2A_1E_7$; see [Gri, p. 280]. Thus there is an exact sequence

$$\{1\} \longrightarrow \mathrm{SL}_2 \longrightarrow C \xrightarrow{f} E_7 \longrightarrow \{1\}\,.$$

We claim that $f(EC^8)$ has depth ≥ 2 in E_7. Indeed, assume the contrary. Then $f(EC^8)$ contains a subgroup H' of index 2 which is toral in E_7. By Lemma 5.6, $H = f^{-1}(H') \cap EC^8$ is toral in C and thus in E_8. Since H is a toral subgroup of index 2 in EC^8, this implies that EC^8 has depth ≤ 1, contradicting Proposition 5.3. □

We can now prove an analogue of Corollary 5.5 for E_7.

Corollary 5.8. *Suppose $E_7 \hookrightarrow S$, where $S = \mathrm{GL}_n$, SL_n or Sp_{2n} for some n. We shall view S as an E_7-variety via the left multiplication action. Suppose $K = k(S)^{E_7}$ and L/K is a splitting field of S. Then $[L : K]$ is divisible by 12.*

Proof. Recall E_7 has a nontoral abelian 3-subgroup, i.e., a 3-subgroup of depth ≥ 1; see, e.g., [Gri]. Moreover, by Proposition 5.7, E_7 contains an abelian 2-subgroup of depth ≥ 2. Thus Corollary 4.8 tells us that $[L : K]$ is divisible by $2^2 \cdot 3 = 12$. □

6. Splitting groups

Definition and first examples.

Definition 6.1. Let X be a generically free primitive G-variety and let $K = k(X)^G$. We shall say that a finite group A is a *splitting group* for X if there exists a splitting field L for X such that L/K is (finite) Galois and $\mathrm{Gal}(L/K) = A$.

Example 6.2. *Let G be a finite group and let X be a generically free irreducible G-variety. Then G is a splitting group for X.*

Proof. Suppose $L = k(X)$ and $K = k(X)^G$. Then $k(X_L) = L \otimes_K L = L \oplus \cdots \oplus L$ ($|G| = [L : K]$ times). In other words, up to birational equivalence, X_L is the disjoint union of $|G|$ copies of Y and G acts on X_L by permuting these copies. Consequently, X_L is split as a G-variety and $G = \mathrm{Gal}(L/K)$ is a splitting group. $\square$

Example 6.3. *Let G be a (connected) semisimple group, and let W be the Weyl group of G. Then every irreducible generically free G-variety X has a splitting group which is isomorphic to a subgroup of W.*

Proof. Let X be a generically free irreducible G-variety and let $\pi\colon X \dashrightarrow X/G$ be the rational quotient map. An irreducible subvariety S of X is called a *Galois section* if GS is dense in X, i.e., $\pi_{|S}$ is dominant, and the field extension $k(S)/k(X)^G$ induced by π, is a finite Galois extension. We shall denote the group $\mathrm{Gal}(k(S)/k(X)^G)$ by $\mathrm{Gal}(S)$.

A theorem of Galitskii asserts that every G-variety X has a Galois section S; see [Ga]. Moreover, by [Po, Remark 1.6.3] S can be chosen so that $\mathrm{Gal}(S)$ is isomorphic to a subgroup H of W. It is easy to see that in order to split X as a G-variety it is sufficient to split S as a $\mathrm{Gal}(S)$-variety. Now Example 6.2 tells us that H is a splitting group for X. $\square$

If G is a connected but not necessarily semisimple then the assertion of Example 6.3 remains true if we define W as the Weyl group of $G_{ss} = G/R(G)$, where $R(G)$ is the radical of G.

Two elementary lemmas from group theory. Our next goal is to prove Theorem 1.2. We begin with two elementary lemmas.

Lemma 6.4. *Let P be a finite abelian group.*

(a) Every quotient group of P is isomorphic to a subgroup of P.

(b) Every subgroup of P is isomorphic to a quotient group of P.

Proof. Suppose Q is a quotient group of P. Then every character of Q lifts to a character of P. This gives an inclusion $Q^* \hookrightarrow P^*$ of dual groups. Since $Q^* \simeq Q$ and $P^* \simeq P$, part (a) follows. Part (b) is proved in a similar manner. $\square$

Lemma 6.5. *Let A and B be (abstract) groups and $A \times B$ acts on a set Z. Let W be the set of A-orbits in Z and let $f\colon Z \longrightarrow W$ be the natural projection. Assume $z \in Z$ and $w = f(z)$. Then*

(a) $\mathrm{Stab}_B(z)$ is a normal subgroup of $\mathrm{Stab}_B(w)$.

(b) Let $S = \mathrm{Stab}_{A\times B}(z)$. Then $\mathrm{Stab}_B(z)$ is normal in S and $S/\mathrm{Stab}_B(z)$ is isomorphic to a subgroup of A; we shall denote this subgroup by A_0.

(c) $\mathrm{Stab}_B(w)/\mathrm{Stab}_B(z)$ is isomorphic to a quotient of A_0.

Proof. (a) Suppose $b \in \mathrm{Stab}_B(w)$. Since the actions of A and B on Z commute, $f(bz) = bf(z) = bw = w$. Consequently, $bz = az$ for some $a \in A$ and thus

$$b\,\mathrm{Stab}_B(z)b^{-1} = \mathrm{Stab}_B(bz) = \mathrm{Stab}_B(az) = \mathrm{Stab}_B(z)\,.$$

This proves part (a).

Let π_A and π_B be, respectively, the natural projections $A \times B \longrightarrow A$ and $A \times B \longrightarrow B$.

(b) The kernel of the map $\pi_A \colon S \longrightarrow A$ is $S \cap B = \mathrm{Stab}_B(z)$, and part (b) follows.

(c) Note that $b \in \mathrm{Stab}_B(w)$ if and only if $bz = az$ for some $a \in A$ or, equivalently, if $(a^{-1}, b) \in S$ for some $a \in A$. In other words, $\mathrm{Stab}_B(w) = \pi_B(S)$. Consequently, we have a surjective homomorphism

$$\pi_B \colon A_0 = S/\,\mathrm{Stab}_B(z) \longrightarrow \mathrm{Stab}_B(w)/\,\mathrm{Stab}_B(z)\,.$$

This completes the proof of part (c). □

Proof of Theorem 1.2. Let $K = k(X)^G$ and let L/K be a Galois extension such that $\mathrm{Gal}(L/K) = A$ and X_L is split. Note that $A \times G$ acts rationally on X_L. By a theorem of Rosenlicht (see [Ro$_1$, Theorem 1]), we can choose a birational model for X_L so that this action becomes regular. Moreover, after applying Proposition 2.2 and Theorem 2.5 to X_L, we may assume that

(i) X_L is smooth and projective, and

(ii) for every $z \in X_L$, $\mathrm{Stab}_{A \times G}(z)$ is Levi-commutative (see Definition 2.3).

Note that by our construction the map $h \colon X_L \dashrightarrow X$ is a rational quotient map for the A-action on X_L. Since A is a finite group and X_L is projective, there exists a geometric quotient map $f \colon X_L \longrightarrow W = X_L//A$ for the A-action on X_L with W projective; see Lemma 2.1. Note that by the universal property of categorical (and, hence, geometric) quotients, the G-action on X_L descends to W; by our construction, W and X are birationally isomorphic as G-varieties. Applying the Going Down Theorem 2.6 to the birational isomorphism $X \overset{\simeq}{\dashrightarrow} W$, we conclude that W has a H-fixed point. Denote this point by w.

Now choose $z \in f^{-1}(w) \in X_L$ and apply Lemma 6.5 with $Z = X_L$ where we view Z as an $A \times H$-variety via the obvious inclusion of $A \times H$ in $A \times G$. By Lemma 6.5(b), A has a subgroup $A_0 \simeq S/\,\mathrm{Stab}_H(w)$, where $S = \mathrm{Stab}_{A \times H}(z)$. Note that S is a finite subgroup of $\mathrm{Stab}_{A \times G}(z)$, and $\mathrm{Stab}_{A \times G}(z)$ is Levi-commutative by our construction (see condition (ii) above). We conclude that S is abelian; see Lemma 2.4. Thus A_0 is also abelian.

By Lemma 6.5(c), A_0 has a quotient of the form $\mathrm{Stab}_H(w)/\,\mathrm{Stab}_H(z) = H/\,\mathrm{Stab}_H(z)$. Denote $\mathrm{Stab}_H(z)$ by H'. Since $Z = X_L$ is split, Lemma 4.3(b) says that H' is toral in G. Thus H/H' is a quotient of A_0, with H' toral. By Lemma 6.4, A_0 (and, hence, A) has a subgroup isomorphic to H/H', as claimed. □

Examples.

Example 6.6. (cf. [Se$_5$, 1.5.1]) *Let G be a special group (see Remark 4.2). Then every finite abelian subgroup of G is toral.*

Indeed, let V be a generically free linear representation of G and let H be a finite abelian subgroup of G. Since G is special, V is split, i.e., $A = \{1\}$ is a splitting group for V. On the other hand, since the origin of V is a smooth H-fixed point, there exists a toral subgroup H_T of H such that H/H_T is isomorphic to a subgroup of $A = \{1\}$. In other words, $H = H_T$ is toral, as claimed. $\square$

Example 6.7. *Let $a_1, \ldots, a_n$ be independent variables over k and let $q = <a_1, \ldots, a_n>$ be the generic quadratic form of dimension n. Then any splitting group of q contains a copy of $(\mathbb{Z}/2\mathbb{Z})^{[\frac{n+1}{2}]}$.*

The proof is the same as in Proposition 5.1(b), with Theorem 1.2 used in place of Theorem 1.1. $\square$

Example 6.8. *Let $G = E_7$ (adjoint) or E_8. Suppose $G \hookrightarrow S$, where $S = \mathrm{GL}_n$, SL_n or Sp_{2n} for some n. Then any splitting group of S (viewed as a G-variety with respect to the left multiplication action) contains a copy of $(\mathbb{Z}/2\mathbb{Z})^2$.*

Indeed, G has an elementary abelian 2-subgroup H of depth ≥ 2; see Propositions 5.3 and 5.7. If $X = \overline{S}$ is a smooth projective model for S (as an S-variety) then the argument of Corollary 4.8 shows that H has a fixed point in X. Thus we can apply Theorem 1.2 to X. $\square$

7. Abelian subgroups of PGL_n

The rest of this paper will be devoted to applications of Theorem 1.2 (with $G = \mathrm{PGL}_n$) to the theory of central simple algebras. In this section we lay the foundation for these applications by studying finite abelian subgroups of PGL_n.

Symplectic modules. We begin by recalling the notion of a symplectic module from [TA_2]. Let H be an abelian group; in the sequel we shall refer to such groups as $\mathbb{Z}$-modules or just modules. We will always assume H is finite. A skew-symmetric form on H is a skew-symmetric $\mathbb{Z}$-bilinear map $\omega\colon H \times H \longrightarrow \mathbb{Q}/\mathbb{Z}$. If H is written multiplicatively, we will usually identify $\mathbb{Q}/\mathbb{Z}$ with the multiplicative group of roots of unity in k^*. A subgroup (or, equivalently, a $\mathbb{Z}$-submodule) H' of H is called *isotropic* if $\omega(h, h') = 0$ for every $h, h' \in H'$.

We will say that ω is *symplectic* if it is non-degenerate, i.e., the homomorphism $H \longrightarrow H^*$ it defines, is an isomorphism. If ω is symplectic then a subgroup $H' \subset H$ is called *Lagrangian* if it is a maximal isotropic subgroup, i.e., if H' is not contained in any other isotropic subgroup. It is easy to see that H' is Lagrangian if and only if it is isotropic and $|H'|^2 = |H|$; cf. [TA_2, Corollary 3.1].

Lemma 7.1. *Let (H, ω) be a symplectic module of order n^2.*

(a) If Λ is a Lagrangian submodule then $H/\Lambda \simeq \Lambda$ (as abelian groups).

(b) Let H_1 be a subgroup of H, and let I be an isotropic subgroup of H_1. Then H_1/I contains an isomorphic copy of I_1, where I_1 is an isotropic subgroup of H and $|H_1|$ divides $n|I_1|$.

Proof. (a) For $h \in H$, let $\chi_h\colon \Lambda \longrightarrow k^*$ be the character given by $\chi_h(l) = \omega(h, l)$. Then $h \mapsto \chi_h$ is a group homomorphism $\phi\colon H \longrightarrow \Lambda^*$. Since ω is non-degenerate, ϕ is onto. Since Λ is Lagrangian, $\mathrm{Ker}(\phi) = \Lambda$. Thus $H/\Lambda \simeq \Lambda^*$. Since $\Lambda^* \simeq \Lambda$, the lemma follows.

(b) We may assume without loss of generality that I is a maximal isotropic subgroup of H_1. Indeed, let I_{max} be a maximal isotropic subgroup of H_1 containing I. Suppose we can find an isotropic subgroup I_1 such that $|H_1|$ divides $n|I_1|$ and H/I_{max} has a subgroup isomorphic to I_1. Since H/I_{max} is isomorphic to a quotient, and hence a subgroup of H/I (see Lemma 6.4), the same I_1 will work for I.

Thus we may (and will) assume that I is a maximal isotropic subgroup of H_1. Let Λ be a Lagrangian subgroup of H containing I. Then $\Lambda \cap H_1 = I$ and thus $H_1/I \hookrightarrow H/\Lambda \simeq \Lambda$; the last isomorphism is given by part (a). Denote the image of H_1/I in Λ by I_1. Then

$$|H_1| = |I| \cdot |H_1/I| = |I| \cdot |I_1|$$

divides $|\Lambda| \cdot |I_1| = n|I_1|$, as claimed. □

Definition 7.2. (cf. [TA$_2$, Section 4]) Let A be an abelian group. We define a skew-symmetric form ω_A on $A \times A^*$ by

$$\omega_1(a_1 \oplus \chi_1, a_2 \oplus \chi_2) = \chi_1(a_2) - \chi_2(a_1) .$$

Lemma 7.3. *(a) $(A \times A^*, \omega_A)$ is a symplectic module, and $A \times \{1\}$ is a Lagrangian submodule.*

(b) Moreover, every symplectic module H is of the form $(A \times A^*, \omega_A)$ for a suitable Lagrangian submodule A of H.

(c) Let (H, ω) be a symplectic module, $H \simeq (\mathbb{Z}/p\mathbb{Z})^{2r}$. If $s \leq r$ then (H, ω) has a symplectic submodule $(H_1, \omega_{|H_1})$ of rank $2s$.

Proof. Parts (a) and (b) are proved in [TA$_2$, Section 4]. Proof of (c): By part (b), we can write (H, ω) as $(A \times A^*, \omega_A)$, where $A = (\mathbb{Z}/p\mathbb{Z})^r$. Let $e_1, \dots, e_r$ be an $\mathbb{Z}/p\mathbb{Z}$-basis of A, viewed as an r-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Then the module H_1 spanned by $(e_i, 1)$ and $(1, e_j^*)$ as i, j range from 1 to s, has the desired properties. □

The form α_H. Abelian subgroups of PGL_n are naturally endowed with a skew-symmetric bilinear form.

Definition 7.4. Let H be a finite abelian subgroup of PGL_n. For $a, b \in H$ define $\alpha_H(a, b) = ABA^{-1}B^{-1}$, where A and B are elements of GL_n representing a and b respectively. It is easy to see that $\alpha_H(a, b)$ does not depend of the choice of A and B and $\alpha_H \colon H \times H \longrightarrow k^*$ defined this way, is a skew-symmetric form on H.

Lemma 7.5. *Let H be a finite abelian subgroup of PGL_n. Then the following conditions are equivalent.*

(a) H lifts to an abelian subgroup of SL_n.

(b) H is toral.

(c) The skew-symmetric form $\alpha_H \colon H \times H \longrightarrow k^*$ given in Definition 7.4 is trivial, i.e., $\alpha_H(a, b) = 1$ for every $a, b \in H$.

Proof. (a) $\Longrightarrow$ (b). Recall that every finite abelian subgroup of SL_n can be simultaneously diagonalized and hence, is toral. (Alternatively, since SL_n is a special group, this follows from Example 6.6.) The tori of PGL_n are precisely the images of the tori in SL_n under the natural projection $\mathrm{SL}_n \longrightarrow \mathrm{PGL}_n$, and part (b) follows.

(b) $\Longrightarrow$ (c). Suppose H is contained in a maximal torus $T \subset \mathrm{PGL}_n$ and let S be the preimage of T in SL_n. Then S is a maximal torus of SL_n. Thus any $a, b \in H$ can be lifted to, respectively, $A, B \in S$. Since A and B commute, we conclude that $\alpha_H(a, b) = ABA^{-1}B^{-1} = 1$, as claimed.

(c) $\Longrightarrow$ (a). Since α_H is trivial, the preimage of H in SL_n is a finite abelian group. □

The embedding ϕ. We will now show that any symplectic module H can be obtained from an abelian subgroup of PGL_n, as above, with $n = \sqrt{|H|}$. Note that by Lemma 7.3(b) we may assume $H = (A \times A^*, \omega_A)$ for some abelian group A.

Definition 7.6. (cf. [RY, Definitions 8.7 and 8.10]) Let A is an abelian group of order n. We define the embedding

$$\phi\colon A \times A^* \hookrightarrow \mathrm{PGL}_n$$

as follows. Identify PGL_n with $\mathrm{PGL}(V)$, where $V = k[A] =$ the group algebra of A. The group A acts on V by the regular representation $a \mapsto P_a \in \mathrm{GL}(V)$, where

$$P_a\Big(\sum_{b \in A} c_b b\Big) = \sum_{b \in A} c_b ab$$

for any $a \in A^*$ and $c_b \in k$. The dual group A^* acts on V by the representation $\chi \mapsto D_\chi \in \mathrm{GL}(V)$, where

$$D_\chi\Big(\sum_{a \in A} c_a a\Big) = \sum_{a \in A} c_a \chi(a) a$$

for any $\chi \in A^*$ and $c_a \in k$. We define ϕ by

$$\phi(a, \chi) = \text{ the image of } P_a D_\chi \text{ in } \mathrm{PGL}(V)\ .$$

Lemma 7.7. *Let A be a finite abelian group, $a, b \in A$ and $\chi, \mu \in A^*$. Then*

(a) $D_\chi P_a = \chi(a) P_a D_\chi$.

(b) $(P_a D_\chi)(P_b D_\mu)(P_a D_\chi)^{-1} = \chi(b)\mu^{-1}(a)(P_b D_\mu)$

(c) The embedding ϕ of Definition 7.6 is a monomorphism of groups, and $\phi(A \times A^*)$ is subgroup of PGL_n isomorphic to $A \times A^*$.

Proof. See [RY, Lemmas 8.8 and 8.11(i)]. ☐

Lemma 7.8. *Let A be an abelian group of order n and let $\phi\colon A \times A^* \hookrightarrow \mathrm{PGL}_n$ be the embedding of Definition 7.6. Then ϕ induces an isomorphism of $(A \times A^*, \omega_A)$ and $(\phi(A \times A^*), \alpha)$ as modules with skew-symmetric forms, where ω_A is as in Definition 7.2 and $\alpha = \alpha_{\phi(A \times A^*)}$ is as in Definition 7.4. In particular, $(\phi(A \times A^*), \alpha)$ is a symplectic module.*

Proof. Let $h_1 = (a_1, \chi_1)$ and $h_2 = (a_2, \chi_2) \in A \times A^*$. Then we want to show that

$$\alpha(\phi(h_1), \phi(h_2)) = \omega_A(h_1, h_2) = \chi_1(a_2)\chi_2(a_1)^{-1}\ .$$

On the other hand, by definition of α, we have

$$\alpha(\phi(h_1), \phi(h_2)) = (P_{a_1} D_{\chi_1})(P_{a_2} D_{\chi_2})(P_{a_1} D_{\chi_1})^{-1}(P_{a_2} D_{\chi_2})^{-1}\ .$$

The desired equality now follows from Lemma 7.7(b). ☐

Corollary 7.9. *Let A be an abelian group of order $n = p^r$. Then the subgroup $H = \phi(A \times A^*) \subset \mathrm{PGL}_n$ is of depth r.*

Proof. Let H_T be any maximal (with respect to inclusion) toral subgroup of H. By Lemma 7.5, H_T is isotropic; as it is maximal, it is Lagrangian. The index $[H : H_T] = n^2/n = n = p^r$, and hence, the depth of H is r. ☐

If $n = p^r$ then the depth of any p-subgroup of PGL_n is $\leq r$. This can be shown directly or, alternatively, derived from Theorem 1.1, since any central simple algebra of degree n is split by a degree n extension of its center.

8. Symplectic modules and division algebras

We now know enough about the nontoral subgroups of PGL_n to proceed with our results on division algebras.

When is $RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$ a division algebra? We begin with an application of Theorem 1.1.

Let X be a generically free irreducible PGL_n-variety. Recall that $A = RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$ is a central simple algebra with the center $Z(A) = k(X)^{\mathrm{PGL}_n}$; A is of the form $\mathrm{M}_s(D)$, where D is a division algebra. The degree d of D is called the index of A, and $sd = n$. The following lemma relates smooth points in X fixed by finite abelian subgroups of PGL_n, to the index of A.

Let H be a finite abelian subgroup of PGL_n. The skew-symmetric form α_H on H may be singular; the quotient $H/\operatorname{Ker}(\alpha_H)$ is a symplectic module, and hence, $|H/\operatorname{Ker}(\alpha_H)| = m^2$ for some integer m.

Lemma 8.1. *With the notations as above, suppose that H has a smooth fixed point $x \in X$.*

Then the index of A is divisible by m. In particular, $m \mid n$, and if $H = \phi_P(P \times P^*)$ where P is an abelian group of order n (so that $m = n$), then A is a division algebra.

Proof. Let F be the center of D (and of $A = \mathrm{M}_s(D)$), and let K be a maximal subfield of D. Recall that $[K : F] = d = \deg(D) = \operatorname{index}(A)$ and that K is a splitting field of A. By Theorem 1.1, d is divisible by $|H/H_T|$ where H_T is some toral subgroup of H. By Lemma 7.5, H_T is isotropic in H; we may assume that H_T is a maximal isotropic subgroup of H. Then $H_T \supset \operatorname{Ker}(\alpha_H)$, and the image of H_T in $H/\operatorname{Ker}(\alpha_H)$ is Lagrangian; it follows that $|H/H_T| = m$, i.e., d is divisible by m.

The equality $sd = n$ implies then that $m \mid n$, and if $m = n$ then $s = 1$, i.e., A is a division algebra. □

Proof of Theorem 1.3. The following proposition is an application of Theorem 1.2.

Proposition 8.2. *Let H be a finite abelian subgroup of PGL_n of order $n^2 = p^{2r}$, such that (H, α_H) is a symplectic module (i.e., α_H is non-degenerate on H; see Definition 7.4). Suppose $X' \dashrightarrow X$ is a rational cover of irreducible generically free PGL_n-varieties, p^e is the largest power of p dividing $\deg(X'/X)$, and X has a smooth point fixed by H. Then any splitting group A' for X' contains an isomorphic copy of some isotropic subgroup $I_1 \subset H$, where $|I_1| \geq p^{r-e}$.*

In particular, if $e = 0$, A' contains an isomorphic copy of a Lagrangian subgroup of H.

Proof. By the Going Up Theorem 2.7(a), X' has an H_1-fixed point for some subgroup H_1 of H of order p^{2r-e}. By Theorem 1.2, A' contains a copy of H_1/I, where I is a toral subgroup of H_1. Lemma 7.5 says that α_H restricted to I is trivial, i.e., I is an isotropic subgroup. Thus by Lemma 7.1(b), H_1/I contains a copy of I_1, where I_1 is an isotropic subgroup of H_1 and $|H_1|$ divides $p^r \cdot |I_1|$. Since $|H_1| \geq p^{2r-e}$, this translates into $|I_1| \geq p^{r-e}$, as claimed. □

We now continue with the proof of Theorem 1.3. Recall that $\mathrm{UD}(n) = RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$, where $X = \mathrm{M}_n \times \mathrm{M}_n$, with PGL_n acting by simultaneous conjugation; see Example 3.1. Let $D = \mathrm{UD}(n) \otimes_{Z(n)} K$, as in the statement of Theorem 1.3. Then $D = RMaps_{\mathrm{PGL}_n}(X_K, \mathrm{M}_n)$. Recall that we are assuming $n = p^r$, and p^e is the highest power of p dividing $[K : Z(n)] = \deg(X_K/X)$. Also recall that A is a splitting group for D if and only if A is a splitting group for X_K (as a PGL_n-variety); see Definition 6.1.

Note that $X = \mathrm{M}_n \times \mathrm{M}_n$ has a smooth point (namely, the origin) fixed by all of G. Let P be an abelian p-group of order $n = p^r$; then $H = \phi_P(P \times P^*)$ is an abelian p-subgroup of PGL_n. By Lemma 7.8, (H, α_H) is a symplectic module. Applying Proposition 8.2 to H and remembering that every symplectic module of order p^{2r} is isomorphic to one of the form $\phi_P(P \times P^*)$ for some P (see Lemmas 7.3(b) and 7.8), we obtain the following generalization of [TA_1, Corollary 7.2] (in characteristic 0):

Proposition 8.3. *Let $Z(p^r)$ be the center of the generic division algebra* $\mathrm{UD}(p^r)$*, let K be a field extension of $Z(p^r)$ and let $D = \mathrm{UD}(p^r) \otimes_{Z(p^r)} K$. Suppose p^e is the highest power of p dividing $[K : Z(p^r)]$, where e is a non-negative integer and $e \leq r - 1$.*

If A is a splitting group of D then for every symplectic module H of order p^{2r}, there exists an isotropic submodule I_1 of order p^{r-e} such that A contains an isomorphic copy of I_1. $\square$

In order to finish the proof of Theorem 1.3 we use a comparison argument, as in the proof of [TA_1, Proof of Theorem 7.3]. Let

$$H_1 = \phi_{P_1}(P_1 \times P_1^*) \text{ and } H_2 = \phi_{P_2}(P_2 \times P_2^*) \ , \tag{8.1}$$

where

$$P_1 = (\mathbb{Z}/p\mathbb{Z})^r \text{ and } P_2 = \mathbb{Z}/p^r\mathbb{Z} \ . \tag{8.2}$$

By Proposition 8.3, A contains an isomorphic copy I_1 of an isotropic subgroup of H_1, and an isomorphic copy I_2 of an isotropic subgroup of H_2, such that $|I_1| = |I_2| = p^{r-e}$. Since $H_1 \simeq (\mathbb{Z}/p\mathbb{Z})^{2r}$ and $H_2 \simeq (\mathbb{Z}/p^r\mathbb{Z})^2$, $I_1 \simeq (\mathbb{Z}/p\mathbb{Z})^{r-e}$ and I_2 has rank ≤ 2. We may assume without loss of generality that both I_1 and I_2 are contained in the same Sylow p-subgroup A_p of A. Since the intersection of I_1 and I_2 has exponent p and rank ≤ 2, we see that

$$|A_p| \geq |I_1 I_2| = \frac{|I_1|\,|I_2|}{|I_1 \cap I_2|} \geq \frac{p^{2r-2e}}{p^2} = p^{2r-2e-2} \ ,$$

where $I_1 I_2 = \{\gamma_1\gamma_2 \mid \gamma_1 \in I_1, \ \gamma_2 \in I_2\}$.

This shows that $|A_p|$ is divisible by $p^{2r-2e-2}$ and, hence, so is $|A|$, as claimed. $\square$

Remark 8.4. The only property of $X = \mathrm{M}_n \times \mathrm{M}_n$ used in the above proof is that each of the finite abelian subgroups $H_1 \simeq (\mathbb{Z}/p^r\mathbb{Z})^2$ and $H_2 \simeq (\mathbb{Z}/p\mathbb{Z})^r$ of PGL_n has a smooth fixed point in X. Thus our argument shows that Theorem 1.3 remains valid if the universal division algebra $\mathrm{UD}(n)$ is replaced by the algebra $U' = RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$, where X is an irreducible generically free PGL_n-variety X such that H_i has a smooth fixed point in X for $i = 1, 2$. There are many choices for such X; in particular, Proposition 8.6 shows that X can be chosen so that $\dim(X/\mathrm{PGL}_n) = 2r$ or, equivalently, $\mathrm{trdeg}_k(Z(U')) = 2r$, where $Z(U')$ is the center of U'.

Remark 8.5. Tignol and Amitsur showed that if A is an *abelian* splitting group of $\mathrm{UD}(p^r)$ and

$$A_p \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_l}\mathbb{Z} \tag{8.3}$$

is its Sylow p-subgroup then $n_\nu + n_{\nu+1} \geq [r/\nu]$ for every $\nu = 1, 2, \ldots$; see [TA$_1$, Theorem 7.4]. Consequently, the order of A_p (and, hence, of A) is divisible by $p^{f(r)}$, where

$$f(r) = r + \sum_{\nu \geq 3} \left\{ \frac{[r/\nu]}{2} \right\} ;$$

see [TA$_1$, Theorem 7.5]. Here $[x]$ is the greatest integer $\leq x$ and $\{x\}$ is the smallest *nonnegative* integer $\geq x$. Note that $f(r) = \frac{1}{2} r \ln(r) + O(r)$, as $r \to \infty$; see [TA$_1$, Remark 7.5] (a more precise asymptotic estimate is given in [TA$_2$, Corollary 6.2]).

The same assertions hold if A is an abelian splitting group for any prime-to-p extension of $\mathrm{UD}(p^r)$: the proof given in [TA$_1$, Theorem 7.5] goes through unchanged, except that we use Proposition 8.3 (with $e = 0$) in place of [TA$_1$, Corollary 7.2],

Moreover, let $D = \mathrm{UD}(p^r) \otimes_{Z(p^r)} K$, where p^e is the highest power of p which divides $[K : Z(p^r)]$, as in the statement of Theorem 1.3. Suppose A is a splitting group of D and A_p is the Sylow p-subgroup of A. If A_p is as in (8.3) then a slight modification of the proof of [TA$_2$, Lemma 6.1] (again, based on Proposition 8.3) shows that $n_\nu + n_{\nu+1} \geq [r/\nu] - e$ for every $\nu = 1, 2, \ldots$ and consequently, the order of A_p (and, hence, of A) is divisible by $p^{f_e(r)}$, where

$$f_e(r) = r - e + \sum_{\nu \geq 3} \left\{ \frac{[r/\nu] - e}{2} \right\} .$$

It is easy to see that for a fixed e and large r, $f_e(r)$ also grows as $\frac{1}{2} r \ln(r) + O(r)$.

Reduction of Theorem 1.4 to a geometric problem. Our proof of Theorem 1.4 will be based on Proposition 8.2. The idea is to construct a generically free PGL_{p^r}-variety X with two smooth points x_1 and x_2 whose stabilizers contain "incompatible" symplectic modules H_1 and H_2. Let P_1 and P_2 be as in (8.2); this time we take

$$H_2 = \phi_{P_2}(P_2 \times P_2^*) \simeq (\mathbb{Z}/p^r\mathbb{Z})^2 ,$$

as in (8.1), but allow H_1 to be smaller:

$$H_1 \ = \text{rank 6 symplectic subgroup of } \phi_{P_1}(P_1 \times P_1^*) .$$

Note that $H_1 \simeq (\mathbb{Z}/p\mathbb{Z})^6$ with desired properties exists by Lemma 7.3(c).

Suppose X is an irreducible generically free PGL_n-variety, and x_1, x_2 are smooth points of X such that x_i is fixed by H_i. Let D be the algebra $RMaps_{\mathrm{PGL}_n}(X, \mathrm{M}_n)$. Since X has a smooth point fixed by H_2, Lemma 8.1 tells us that D is a division algebra. Moreover, in view of Proposition 8.2 (with $X = X'$) any splitting group A of X (or equivalently, of D) will contain subgroups L_1 and L_2 which are isomorphic to Lagrangian submodules of H_1 and H_2, respectively. Note that $L_1 \simeq (\mathbb{Z}/p\mathbb{Z})^3$ and $L_2 \simeq (\mathbb{Z}/p^i\mathbb{Z}) \times (\mathbb{Z}/p^{r-i}\mathbb{Z})$, for some $0 \leq i \leq r$. Then $L_1 \cap L_2$ is an abelian group of exponent p and rank ≤ 2. Thus

$$|A| \geq |L_1 L_2| = \frac{|L_1|\,|L_2|}{|L_1 \cap L_2|} \geq \frac{p^3 p^r}{p^2} = p^{r+1} ;$$

this shows that D is not a a crossed product. The same argument shows that any prime-to-p extension of D is not a crossed product.

Thus, in order to prove Theorem 1.4 it is sufficient to construct an irreducible generically free PGL_n-variety X such that $\mathrm{trdeg}_k\, k(X)^{\mathrm{PGL}_n} = \dim(X/\mathrm{PGL}_n) = 6$ and X has smooth points x_1 and x_2 such that x_i is fixed by H_i.

Note that both H_1 and H_2 are contained in the finite subgroup G of PGL_n generated by the permutation matrices and by the diagonal matrices all of whose entries are p^rth roots of unity. We will construct X as $\mathrm{PGL}_n *_G Y$, where Y is a 6-dimensional primitive G-variety with two points, y_1 and y_2 such that H_i fixes y_i. Indeed, if Y is as above then the points $x_1 = (1_{\mathrm{PGL}_n}, y_1)$ and $x_2 = (1_{\mathrm{PGL}_n}, y_2)$ of X have the desired properties. (Recall that $\mathrm{PGL}_n *_G Y$ is defined as the geometric quotient of $\mathrm{PGL}_n \times Y$ by the G-action given by $g \cdot (h, y) = (hg^{-1}, gy)$; see [PV, Section 4.8].)

Therefore, in order to prove Theorem 1.4 it is enough to establish the following result.

Proposition 8.6. *Let G be a finite group and let $H_1, \dots, H_s$ be abelian subgroups of G, $r_i = \mathrm{rank}(H_i)$ and $r = \max\{r_i \mid i = 1, \dots, s\}$. Then there exists a generically free primitive r-dimensional projective G-variety Y with smooth points $y_1, \dots, y_s$ such that $H_i \subset \mathrm{Stab}(y_i)$.*

Remark 8.7. Note that $\dim(Y)$ cannot be less than r. More precisely, if H is a finite abelian group, Y is a quasiprojective H-variety, and y is a smooth point of Y fixed by H then

$$\mathrm{codim}_y(Y^H) \geq \mathrm{rank}(H) \ . \tag{8.4}$$

Indeed, assume the contrary: $\mathrm{codim}_y(Y^H) < \mathrm{rank}(H)$. By Lemma 2.1(a), y has an H-invariant affine neighborhood in Y. Replacing Y by this neighborhood, we may assume Y is affine. By the Luna Slice Theorem [PV, Corollary to Theorem 6.4], Y^H is smooth at y and

$$\dim(T_y(Y)) - \dim(T_y(Y)^H) = \mathrm{codim}_y(Y^H) < \mathrm{rank}(H) \ ;$$

hence, the action of H on $T_y(Y)$ cannot be faithful. In other words, there exists a subgroup $H' \subset H$, $H' \neq \{1\}$, which acts trivially on $T_y(Y)$. Applying [PV, Corollary to Theorem 6.4] to the action of H' on Y, we see that H' acts trivially on all of Y. This contradicts our assumption that the G-action on Y is generically free. □

9. Constructing a G-variety with prescribed stabilizers

As we have just seen, Theorem 1.4 follows from Proposition 8.6. This section will thus be devoted to proving Proposition 8.6. Our general approach is to first construct a higher-dimensional variety with desired properties (this is easy), then replace it by a "generic" G-invariant hypersurface passing through $y_1, \dots, y_s$, thus reducing the dimension by 1. To carry out this program, we first reduce to a situation where Y^{H_i} has the highest possible dimension at y_i (Theorem 9.3), then apply Theorem 9.7, which may be viewed as a weak form of Bertini's theorem in the equivariant setting.

A local system of parameters. The following lemma summarizes some known facts about the local geometry of a smooth G-variety near a point fixed by a finite abelian group.

Lemma 9.1. *Let H be a finite abelian group, let X be a smooth quasiprojective H-variety, and let $D_1, \dots, D_l$ be H-invariant hypersurfaces passing through a point $x \in X$ and intersecting transversely at x.*

(1) There exists a local coordinate system (a regular system of parameters) $u_1, \dots, u_n$ with the following properties:

(i) The group H acts on each u_i by a character ξ_i;

(ii) u_i is the local equation of D_i for $i = 1, \dots, l$;

(iii) The germ of the fixed-point set X^H at x is given by the local equations $u_{i_1} = \cdots = u_{i_t} = 0$ where $\{i_1, \dots, i_t\}$ is the set of all subscripts i for which the character ξ_i is nontrivial.

(2) Let $\pi\colon X' \longrightarrow X$ be the blowup with the center Z given by the local equations $u_{j_1} = \cdots = u_{j_s} = 0$ at x. (In particular, we can take $Z = X^H$.) Let $\widetilde{D}_i \subset X'$ be the strict transform of D_i. Then we have:

(i) $\widetilde{D}_1, \dots, \widetilde{D}_l$ and the exceptional divisor $\pi^{-1}(Z)$ are in normal crossing in a neighborhood of $\pi^{-1}(x)$;

(ii) the natural isomorphism $\pi^{-1}(x) \cong \mathbb{P}(T_xX/T_xZ)$ identifies $\widetilde{D}_i \cap \pi^{-1}(x)$ with $\mathbb{P}(L_i)$, where L_i is an H-invariant subspace of T_xX/T_xZ of codimension 0 or 1.

Note that if u_i is a local equation of D_i and H acts on u_i by a character ξ_i then H acts by the character ξ_i on the conormal space $(T_xX/T_xD_i)^*$.

Proof. By Lemma 2.1(a), we may assume without loss of generality that X is affine.

(1) Denote by $\mathcal{O}_x$ the local ring of X at x, by $\mathfrak{m}_x$ its maximal ideal, and by $\mathfrak{p}_{D_i}$ the ideal of D_i in $\mathcal{O}_x$.

To construct $u_1, \dots, u_l$, note that the group H acts on $\mathcal{O}_x$, the ideals $\mathfrak{m}_x$ and $\mathfrak{p}_{D_i}$ are H-invariant subspaces in $\mathcal{O}_x$, and the H-representation $(\mathfrak{p}_{D_i} + \mathfrak{m}_x^2)/\mathfrak{m}_x^2 \cong \mathfrak{p}_{D_i}/(\mathfrak{p}_{D_i} \cap \mathfrak{m}_x^2)$ is one-dimensional; let ξ_i be the corresponding character of H. The H-linear epimorphism $\mathfrak{p}_{D_i} \longrightarrow \mathfrak{p}_{D_i}/(\mathfrak{p}_{D_i} \cap \mathfrak{m}_x)$ splits; this yields a generator $u_i \in \mathfrak{p}_{D_i}$ — a local equation of D_i — on which H acts by the character ξ_i.

To construct $u_{l+1}, \dots, u_n$, consider the H-linear epimorphism

$$\mathfrak{m}_x \longrightarrow \mathfrak{m}_x/(\mathfrak{p}_{D_1} + \cdots + \mathfrak{p}_{D_l} + \mathfrak{m}_x^2) \cong \frac{\mathfrak{m}_x/\mathfrak{m}_x^2}{\sum_{i=1}^{l} (\mathfrak{p}_{D_i} + \mathfrak{m}_x^2)/\mathfrak{m}_x^2} \ ;$$

its splitting yields the elements $u_{l+1}, \dots, u_n \in \mathfrak{m}_x$ such that H acts on each of them by a character and the images of $u_1, \dots, u_n$ in $\mathfrak{m}_x/\mathfrak{m}_x^2$ form a basis there. It follows that $u_1, \dots, u_n$ form a regular system of parameters at x that satisfies properties (1)(i) and (1)(ii).

According to the Luna Slice Theorem [PV, Corollary to Theorem 6.4], X^H is given in a neighborhood of x by the local equations $u_{i_1} = \cdots = u_{i_t} = 0$, where $\{i_1, \dots, i_t\}$ is the set of all subscripts i for which the character ξ_i is nontrivial. This proves part (1)(iii).

(2) Let U be a small enough affine neighborhood of x in X so that $u_1, \dots, u_n$ form a local coordinate system (i.e., their differentials are linearly independent) everywhere on U. The blown-up variety X' in a neighborhood of $\pi^{-1}(x)$ is covered by the charts U_i, $1 \leq i \leq s$, where U_i is the complement in $\pi^{-1}(U)$ of the strict transform of the subvariety $u_{j_i} = 0$; the local coordinates in U_i are $v_{j_i} = \pi^* u_{j_i}$, $v_{j_{i'}} = \pi^* u_{j_{i'}}/\pi^* u_{j_i}$ for $i' \neq i$, and $v_j = \pi^* u_j$ for $j \notin \{j_1, \dots, j_s\}$. The exceptional divisor in U_i is given by the local equation $v_{j_i} = 0$, and $\widetilde{D}_j$ is given by the local equation $v_j = 0$ in case $j \neq j_i$, and is empty in case $j = j_i$. Since the local equations of $\widetilde{D}_1, \dots, \widetilde{D}_l$ and of the exceptional divisor are elements of the same local coordinate system, they are transverse; this proves (2)(i).

The local equations in U_i of the preimage $\pi^{-1}(x)$ are $v_j = 0$ for $j \notin \{j_1, \dots, j_s\}$, and $v_{j_i} = 0$; hence, $\pi^{-1}(x)$ is contained in $\widetilde{D}_j$ if $j \notin \{j_1, \dots, j_s\}$, so that in this case $\widetilde{D}_j \cap \pi^{-1}(x) = \pi^{-1}(x)$ as claimed in (2)(ii). If $j \in \{j_1, \dots, j_s\}$ then $D_i \supset Z$ and $\widetilde{D}_j \cap \pi^{-1}(x)$ can be identified with $\mathbb{P}(T_x D_i / T_x Z)$; here $L_i = T_x D_i / T_x Z$ is an H-invariant subspace of $T_x X / T_x Z$ of codimension 1 as claimed. This completes the proof of (2)(ii). □

Lemma 9.2. *Let G be a finite group, H be an abelian subgroup of G, X be a smooth quasiprojective G-variety and $x \in X^H$. Then there exists a sequence of blowups*

$$f \colon X_i \longrightarrow \dots \longrightarrow X_0 = X \tag{9.1}$$

with smooth G-invariant centers, a point $y \in X_i^H$ satisfying $f(y) = x$, and smooth G-invariant hypersurfaces $D_1, \dots, D_l$ meeting transversely, such that locally at y, the fixed point set X_i^H coincides with $D_1 \cap \dots \cap D_l$.

Proof. By Theorem 2.5, we may assume that $\mathrm{Stab}(x)$ is commutative.

The statement of the Lemma follows from the case $H = \mathrm{Stab}(x)$. Indeed, if $X_i^{\mathrm{Stab}(y)} = D_1 \cap \dots \cap D_l$ locally at y, then by Luna's slice theorem (see [PV, Theorem 6.4]), X_i^H is the intersection of those of D_j for which the action of H on the normal space $T_y(X_i)/T_y(D_j)$ is nontrivial; thus, X_i^H is the intersection of some of D_j, as claimed. (Note that the Luna Slice Theorem can be applied to the G-action on X_i because X_i is quasiprojective and, hence, every point of X_i has an open affine G-invariant neighborhood; see Lemma 2.1.)

From now on we assume that $\mathrm{Stab}(x) = H$. Let $X' = X - G \cdot \bigcup_{H' \underset{\neq}{\supset} H} X^{H'}$; this is a G-invariant open dense quasiprojective subvariety of X containing x and not containing any point whose stabilizer is strictly larger than H. If we can find a sequence of blowups (9.1) for X', then we can extend it to a similar sequence for X by extending each blowup center in X' to its closure in X and equivariantly resolving it before blowing it up, in case it is not smooth; for equivariant resolution of singularities, see either [V, Theorem 7.6.1] or [BM, Theorem 13.2].

Thus, we may assume that X does not contain points with stabilizers strictly containing H; this implies that the subvarieties $X^{gHg^{-1}}$ for different $g \in G$ are disjoint unless they coincide. Each of these subvarieties is smooth by Luna's slice theorem (see [PV, Corollary to Theorem 6.4]), and hence, their union $GX^H = \bigcup_{g \in G} X^{gHg^{-1}}$ is smooth.

Let $\dim X = n$, and let

$$X_n \xrightarrow{\pi_n} \dots \xrightarrow{\pi_{i+1}} X_i \xrightarrow{\pi_i} \dots \xrightarrow{\pi_1} X_0 = X$$

be the sequence of blowups with the centers $Z_i = GX_i^H \subset X_i$; they are G-invariant. Inductively, each X_i has no points whose stabilizers strictly contain H; together with the fact that X_i is smooth, this implies that Z_i is smooth, and hence, X_{i+1} is smooth, so that X_i and Z_i are smooth for every i.

Let $E_i = D_{i1} \cup \dots \cup D_{ii}$ be the exceptional divisor in X_i, where $D_{ij} \subset X_i$ is the strict transform (in X_i) of the exceptional divisor of $\pi_j \colon X_j \longrightarrow X_{j-1}$. We claim that E_i is a normal crossing divisor. The proof is by induction on i. The base case, $i = 0$, is obvious, since $E_0 =$ the empty divisor, is normal crossing. For the inductive step, we assume that E_i is a normal crossing divisor. Then E_{i+1} is also a normal crossing divisor by Lemma 9.1(2)(i). This completes the proof of the claim.

To obtain the required point $y \in X_m^H$, we start with $x_0 = x$ and inductively construct $x_i \in X_i$ satisfying $\pi_i(x_i) = x_{i-1}$ and $x_i \in X_i^H \cap D_{i1} \cap \cdots \cap D_{ii}$, until we get a point $y = x_m$ with the desired properties.

Suppose x_i has been constructed for some $i \geq 0$. Note that near x_i, the center $Z_i = GX_i^H$ coincides with X_i^H.

Case 1. The germ of X_i^H at x_i does not contain the germ of $S = \bigcap_{j=1}^i D_{ij}$. Let

$$W = \pi_{i+1}^{-1}(x_i) \cap \bigcap_{j=1}^{i+1} D_{i+1,j} \subset X_{i+1} \ .$$

We claim $W \neq \emptyset$. Indeed, since $x_i \in X_i^H$, we have $\pi_{i+1}^{-1}(x_i) \subset \pi_{i+1}^{-1}(Z_i) = D_{i+1,i+1}$, and thus

$$W = \pi_{i+1}^{-1}(x_i) \cap \bigcap_{j=1}^{i} D_{i+1,j} \ . \tag{9.2}$$

Since $D_{i+1,j}$ is the strict transform of D_{ij}, $\bigcap_{j=1}^i D_{i+1,j}$ contains the strict transform of $S = \bigcap_{j=1}^i D_{ij}$. Thus W contains the intersection of the strict transform of S with $\pi_{i+1}^{-1}(x_i)$. As the germ of S at x_i is not contained in the germ of the blowup center Z_i, i.e., of X_i^H, the strict transform of S is nonempty and intersects $\pi_{i+1}^{-1}(x_i)$. Consequently, W is nonempty, as claimed.

We now identify $\pi_{i+1}^{-1}(x_i)$ with $\mathbb{P}(T_{x_i}X_i/T_{x_i}Z_i)$ in the usual manner. Note that this identification is H-equivariant. Then by Lemma 9.1(2)(ii), $\pi_{i+1}^{-1}(x_i) \cap D_{i+1,j}$ is identified with $\mathbb{P}(L_j)$, where L_j is an H-invariant subspace of the normal space $T_{x_i}X_i/T_{x_i}Z_i$. Thus W is identified with $\mathbb{P}(L)$, where $L = L_1 \cap \cdots \cap L_i$; see (9.2). Note that $L \neq (0)$ because $W \neq \emptyset$; moreover, H acts linearly on L. Since H is diagonalizable, it has an eigenvector in L, i.e., a fixed point in $W \cong \mathbb{P}(L)$. This fixed point is our new point x_{i+1}. By our construction, $\pi_{i+1}(x_{i+1}) = x_i$ and $x_{i+1} \in X_{i+1}^H \cap \bigcap_{j=1}^{i+1} D_{i+1,j}$, as desired.

Case 2: X_i^H at x_i contains $\bigcap_{j=1}^i D_{ij}$ at x_i. Note that this is necessarily the case if $i = n$. By Lemma 9.1(1), X_i^H at x_i coincides with the intersection of those of D_{ij} for which the action of H on $T_{x_i}X_i/T_{x_i}D_{ij}$ is nontrivial; in particular, X_i^H at x_i is an intersection of smooth G-invariant hypersurfaces meeting transversely, as required.

Thus, we see that for some $i \leq n$, Case 2 occurs and we get a point $x_i \in X_i$ with the required properties. □

Resolving the action on the tangent space. In this subsection we prove the following result.

Theorem 9.3. *Let G be a finite group, let X be a smooth quasiprojective G-variety, let $H_1, \dots, H_s$ be abelian subgroups of G and $x_1, \dots, x_s$ be points of X such that x_i is fixed by H_i. Denote the rank of H_i by r_i. Then there is a sequence of blowups $\pi\colon X_m \longrightarrow \cdots \longrightarrow X_0 = X$ with smooth G-invariant centers, and points $y_1, \dots, y_s \in X_m$, such that $\pi(y_i) = x_i$, $y_i \in X_m^{H_i}$, and $X_m^{H_i}$ has codimension r_i at y_i.*

Our proof relies on the following two simple lemmas.

Lemma 9.4. *Let H be a finite abelian group, let X be an H-variety and $x \in X^H$ be a smooth point of X. If $\pi\colon \widetilde{X} \longrightarrow X$ is a blowup with a smooth H-invariant center $Z \subset X$ then there exists a point $\widetilde{x} \in \pi^{-1}(x)$ fixed by H such that $\dim_{\widetilde{x}}(\widetilde{X}^H) \geq \dim_x(X^H)$.*

Proof. Replacing X by the set of its smooth points (which is clearly H-invariant), we may assume that X is smooth. We claim that $\pi(\widetilde{X}^H) = X^H$. The inclusion $\pi(\widetilde{X}^H) \subset X^H$ is obvious. To prove the opposite inclusion, note that since π is an isomorphism over $X \setminus Z$, every $y \in X^H - Z$ lies in $\pi(\widetilde{X}^H)$. On the other hand, if $y \in Z^H$ then $\pi^{-1}(y)$ can be identified with $\mathbb{P}(T_yX/T_yZ)$ as H-varieties, and the (linear) action of H on $\mathbb{P}(T_yX/T_yZ)$ has a fixed point $\widetilde{y}$; then $y = \pi(\widetilde{y}) \in \pi(\widetilde{X}^H)$. This proves the claim, and the lemma follows. □

Remark 9.5. Lemma 9.4 remains true under the more general assumption that H is Levi-commutative rather than finite abelian; see Definition 2.3 and Lemma 2.4(iv). The version we stated is sufficient for our application.

Lemma 9.6. *Let A be a finite abelian group of rank r. An elementary operation on A^s is one of the form*

$$(\xi_1, \dots, \xi_i, \dots, \xi_s) \longrightarrow (\xi_1, \dots, \xi_i - \xi_j, \dots, \xi_s)$$

for some $1 \leq i, j \leq s$, where $i \neq j$.

Assume $s \geq r$. Then any $\xi = (\xi_1, \dots, \xi_s) \in A^s$ can be transformed, by a finite sequence of elementary operations, into an s-tuple with at least $s - r$ zeros. (Here by a zero, we mean the identity element of A.)

Proof. First we note that it does no harm to permute the components of ξ. In other words, we may as well consider an operation of the form $(\xi_1, \dots, \xi_s) \mapsto (\xi_{\sigma(1)}, \dots, \xi_{\sigma(s)})$ with $\sigma \in \mathrm{S}_n$, as another type of elementary operation. The assertion of the lemma is then equivalent to saying that any $\xi \in A^s$ can be transformed, by these two types of elementary operations, into an s-tuple $\lambda = (\lambda_1, \dots, \lambda_r, 0_A, \dots, 0_A)$, where 0_A is the identity element of A.

We will prove this assertion by induction on r. Suppose $r = 1$, i.e., $A = \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$. We can use elementary operations to perform the Euclidean algorithm on ξ_1 and ξ_2. After interchanging them if necessary, we may assume $\xi_2 = 0$. (The new value of ξ_1 is the greatest common divisor of the old values of ξ_1 and ξ_2). Applying the same procedure to ξ_1 and ξ_3, then ξ_1 and ξ_4, etc., we reduce the original s-tuple to $(\xi_1, 0, \dots, 0)$, as claimed.

For the induction step, write $A = B \times C$, where B has rank $r-1$ and C is cyclic. Set $\xi_i = (\beta_i, \gamma_i)$, where $\beta_i \in B$ and $\gamma_i \in C$. As we saw above, after performing a sequence of elementary operations, we may assume $\gamma_2 = \dots = \gamma_s = 0_C$. By the induction assumption, there exists a sequence of elementary operations in B^{s-1} which reduces $(\beta_2, \dots, \beta_s)$ to $(\lambda_2, \dots, \lambda_r, 0_B, \dots, 0_B)$. (Note that since $r \leq s$, $\mathrm{rank}(B) = r - 1 \leq s - 1$, so that we may, indeed, use the induction assumption.) Applying the same sequence to $(\xi_2, \dots, \xi_s)$, we reduce $(\xi_1, \dots, \xi_s)$ to

$$(\xi_1, (\lambda_2, 0_C), \dots, (\lambda_r, 0_C), 0_A, \dots, 0_A) \in A^s \ .$$

This completes the proof of the lemma. □

Proof of Theorem 9.3. By (8.4), we have

$$\mathrm{codim}_{x_i}(X^{H_i}) \geq r_i \tag{9.3}$$

for any i. We want to modify X by a sequence of blowups so as to decrease $\operatorname{codim}_{x_i} X^{H_i}$ to r_i for each i. (Of course, after each blowup $\widetilde{X} \longrightarrow X$ we replace X by $\widetilde{X}$ and x_i by $\widetilde{x}_i$, as in Lemma 9.4.) We claim that we may do this for one i at a time; in other words, we may assume $s = 1$. Indeed, suppose we have reduced to the case where $\operatorname{codim}_{x_1}(X^{H_1}) = r_1$. If we now perform a further blowup $\widetilde{X} \longrightarrow X$ and choose $\widetilde{x_1}$ above x_1 as in Lemma 9.4, then Lemma 9.4 and (9.3) tell us that $\operatorname{codim}_{\widetilde{x_1}}(\widetilde{X}^{H_1}) = r_1$. Thus we are free to perform another sequence of blowups that would give us the desired equality for $i = 2$, then $i = 3$, etc.

We will thus assume $s = 1$ and set $x = x_1$, $H = H_1$, $r = r_1$.

By performing a sequence of blowups given by Lemma 9.2, we may assume that there exist G-invariant divisors $D_1, \dots, D_c$ such that $X^H = D_1 \cap \dots \cap D_c$ in a neighborhood of x, $c = \operatorname{codim}_x X^H$ and $D_1, \dots, D_c$ intersect at x transversely.

Note that $T_x(X)/T_x(X_i^H) \cong \bigoplus_{j=1}^c T_x(X)/T_x(D_j)$. Here H acts on each one-dimensional space $T_x(X)/T_x(D_i)$ by a character $\xi_i \in H^*$ which is nontrivial by Lemma 9.1(1)(iii). In other words, the linear action of H on the tangent space $T_x(X)$ decomposes as a direct sum of c nontrivial characters $\xi_1, \dots, \xi_c$ and $n - c = \dim X^H$ trivial characters.

Recall that by (9.3), $c \geq r$. We would like to modify X by a sequence of blowups to arrive at the situation where $c = r$. In other words, if $c > r$, we want to perform a sequence of blowups that would lower the value of c.

With this goal in mind, we would like to know how the characters ξ_i change after one blowup. Specifically, we will consider the blowup $\pi\colon \widetilde{X} \longrightarrow X$ with center $Z = D_i \cap D_j$, where $1 \leq i, j \leq c$, $i \neq j$. Since Z is of codimension 2 in X, $\pi^{-1}(x)$ is isomorphic to $\mathbb{P}^1$. Let $\widetilde{x}$ be the (unique) point of $\pi^{-1}(x)$ that lies in the strict transform of D_i, take $\widetilde{D}_l$ to be the strict transform of D_l for $l = 1, \dots, \widehat{j}, \dots, c$, and let $\widetilde{D}_j = \pi^{-1}(Z)$ be the exceptional divisor of π. Then the action of H in $T_{\widetilde{x}}\widetilde{X}$ is given by the direct sum of the characters $\widetilde{\xi}_l = \xi_l$ if $l \neq i$, $\widetilde{\xi}_i = \xi_i \xi_j^{-1}$, and $(\dim X - c)$ trivial characters. In other words, the new characters $\widetilde{\xi}_1, \dots, \widetilde{\xi}_c \in H^*$ are obtained from the old characters $\xi_1, \dots, \xi_c \in H^*$ by an elementary operation, as in Lemma 9.6. (Note that our group H^* is written multiplicatively, whereas the group A in Lemma 9.6 is written additively.)

Now Lemma 9.6 tells us that there is a sequence of of elementary operations which transforms $(\xi_1, \dots, \xi_c)$ to $(\lambda_1, \dots, \lambda_r, 1_{H^*}, \dots, 1_{H^*})$ for some $\lambda_1, \dots, \lambda_r \in H^*$. Recall that initially our characters ξ_i are all nontrivial. We want to follow the above sequence of elementary operations until we create the first trivial character. Each one of these transformations is given by a blowup of a codimension 2 subvariety, as described above. When the first trivial character appears, $\dim(X^H)$ goes up by one. At that point, we reduce c by 1 and repeat the above procedure, until c becomes equal to r. □

A weak equivariant Bertini theorem.

Theorem 9.7. *Let G be a finite group, X a primitive smooth projective G-variety, $x_1, \dots, x_s$ points of X with stabilizers $H_i = \operatorname{Stab}(x_i)$ for $i = 1, \dots, s$. Suppose that each x_i is not an isolated point of X^{H_i} and $\dim(X) \geq 2$. Then*

(a) there exists a smooth closed G-invariant primitive hypersurface $W \subset X$ passing through $x_1, \dots, x_s$.

(b) Moreover, if X is a generically free G-variety then we can choose W so that it is also generically free.

We shall need the following variant of Bertini's theorem; for lack of a reference we will supply a proof.

Lemma 9.8. *Let $x_1, \dots, x_s$ be points in $\mathbb{P}^n$ and let V_d be the space of homogeneous polynomials of degree $d \geq s+1$ in $\mathbb{P}^n$ that vanish at $x_1, \dots, x_s$.*

(a) Suppose Y is a locally closed subvariety of $\mathbb{P}^n$, y is a smooth point of Y and $V_{d,y} = \left\{ P \in V_d \;\middle|\; P|_Y \text{ has zero of order } > 1 \text{ at } y \right\}$. Then the codimension of $V_{d,y}$ in V_d is given by

$$\operatorname{codim}(V_{d,y}) = \begin{cases} \dim_y(Y) + 1 & \text{if } y \notin \{x_1, \dots, x_s\} , \\ \dim_y(Y) & \text{if } y \in \{x_1, \dots, x_s\} . \end{cases}$$

(b) Suppose $Y_1, \dots, Y_l$ are smooth locally closed subvarieties of $\mathbb{P}^n$ such that

$$x_j \text{ is not an isolated point of } Y_i \text{ for all } i, j. \tag{9.4}$$

Then a generic hypersurface of degree $d \geq s+1$ in $\mathbb{P}^n$ that passes through $x_1, \dots, x_s$, is transverse to $Y_1, \dots, Y_l$.

Note that assumption (9.4) in part (b) is necessary, since otherwise no hypersurface passing through x_j can be transverse to Y_i. (By definition, a hypersurface W is transverse to a one-point set $\{x_j\}$ iff W does not pass through x_j.)

Proof. (a) Choose an affine subset $\mathbb{A}^n = \operatorname{Spec} k[z_1, \dots, z_n] \subset \mathbb{P}^n$ that contains $x_1, \dots, x_s$ and y; then V_d may be identified with the space of all polynomials in $z = (z_1, \dots, z_n)$ of degree $\leq d$ (not necessarily homogeneous) that vanish at the points $x_1, \dots, x_s$.

Consider the linear map $\phi_y \colon V_d \longrightarrow \mathcal{O}_y/\mathfrak{m}_y^2$, where $\mathcal{O}_y/\mathfrak{m}_y^2$ is the space of 1-jets of regular functions on $\mathbb{A}^n$ at y; ϕ_y sends each polynomial $P \in V_d$ into its 1-jet at y (cf. [Ha, Proof of Theorem 8.18]). Then $V_{d,y} = \phi_y^{-1}(N_y)$ where N_y is the subspace of $\mathcal{O}_y/\mathfrak{m}_y^2$ consisting of the jets of all functions that vanish on Y; N_y may be identified with the conormal space to Y at y, and hence, it is a linear subspace of $\mathcal{O}_y/\mathfrak{m}_y^2$ of dimension $\dim(N_y) = \operatorname{codim}_y(Y)$.

Assume $y \notin \{x_1, \dots, x_s\}$. Let $l(z)$ be a linear combination of $z_1, \dots, z_n$ whose value at y is different from its values at $x_1, \dots, x_s$. Then the degree s polynomial $P(z) = \Big(l(z) - l(x_1)\Big) \dots \Big(l(z) - l(x_s)\Big)$ vanishes at $x_1, \dots, x_s$ and does not vanish at y. This means that $\phi_y(P(z))$ and $\phi_y(z_j P(z))$ (where $j = 1, \dots, n$) span $\mathcal{O}_y/\mathfrak{m}_y^2$ as a k-vector space. Hence, ϕ_y is onto, and

$$\begin{aligned} \operatorname{codim}(V_{d,y}) = \operatorname{codim}(\phi_y^{-1}(N_y)) &= \dim(\mathcal{O}_y/\mathfrak{m}_y^2) - \dim(N_y) \\ &= n + 1 - \operatorname{codim}_y(Y) = \dim_y(Y) + 1 \end{aligned}$$

as claimed.

Now suppose $y \in \{x_1, \dots, x_s\}$, say, $y = x_1$. In this case $\phi_y(V_d)$ is clearly contained in $\mathfrak{m}_y/\mathfrak{m}_y^2$; we will show that, in fact, equality holds. Indeed, we may assume without loss of generality that $y = x_1 = (0, \dots, 0) \in \mathbb{A}^n$. Let $l(z)$ be a linear combination of $z_1, \dots, z_n$ such that $l(x_2), \dots, l(x_s) \neq l(x_1) = 0$ and let $Q(z) = \Big(l(z) - l(x_2)\Big) \dots \Big(l(z) - l(x_s)\Big)$. Given any linear function $a(z)$ in $z_1, \dots, z_n$, let $R(z) = a(z)Q(z)$. Note that $R(z)$ vanishes at $x_1, \dots, x_s$ and has degree s; hence,

$R(z) \in V_d$. On the other hand, $\phi_y(R)$ equals $R(z)$ modulo the terms of degree ≥ 2 in $z_1, \dots, z_n$, i.e., $\phi_y(R) = Q(0)a(z) \pmod{\mathfrak{m}_y^2}$, where $Q(0)$ is a nonzero element of k. This means that $\phi_y(V_d)$ contains $a(z)$, thus proving that $\phi_y(V_d) = \mathfrak{m}_y/\mathfrak{m}_y^2$, as desired. Now

$$\begin{aligned}\operatorname{codim}(V_{d,y}) = \operatorname{codim}(\phi_y^{-1}(N_y)) &= \dim(\mathfrak{m}_y/\mathfrak{m}_y^2) - \dim(N_y) \\ &= n - \operatorname{codim}_y(Y) = \dim_y(Y) \ .\end{aligned}$$

(b) After replacing each Y_i by the collection of its irreducible components, we may assume each Y_i is irreducible. Moreover, we may assume without loss of generality that $l = 1$; we shall denote Y_1 by Y.

Let X be the algebraic subvariety of $V_d \times Y$ given by

$$X = \left\{ (P, y) \ \Big| \ P|_Y \text{has a zero of order } > 1 \text{ at } y \right\} ;$$

Denote the natural projections of X to V_d and Y by π_1 and π_2. We want to show that $\dim(\pi_1(X)) < \dim(V_d)$. It is thus enough to prove that $\dim(X) < \dim(V_d)$. Write $X = X_1 \cup X_2$, where $X_1 = \pi_2^{-1}(Y - \{x_1, \dots, x_s\})$ and $X_2 = \pi_2^{-1}(Y \cap \{x_1, \dots, x_s\})$. It is enough to show that $\dim(X_i) < \dim(V_d)$ for $i = 1, 2$. The fibers of π_2 are precisely the sets $V_{d,y}$ we considered in part (a). Since $\dim(V_{d,y}) = \dim(V_d) - \dim(Y) - 1$ for every $y \in Y - \{x_1, \dots, x_s\}$, we conclude that $\dim(X_1) \leq \dim(V_d) - 1$.

It remains to show that $\dim(X_2) \leq \dim(V_d) - 1$. If $Y \cap \{x_1, \dots, x_s\} = \emptyset$ then $X_2 = \emptyset$, and there is nothing to prove. On the other hand, if $Y \cap \{x_1, \dots, x_s\} \neq \emptyset$ then assumption (9.4) says that $\dim(Y) \geq 1$. Thus by part (a),

$$\dim(X_2) \leq \dim(V_d) - \dim(Y) \leq \dim(V_d) - 1 \ ,$$

as claimed. □

Proof of Theorem 9.7. We begin with three simple observations. First of all, we may assume without loss of generality that the orbits Gx_i are disjoint. Indeed, if W passes through x_i then it will pass through every point of Gx_i. Thus if, say, x_j happens to lie in Gx_i then we can simply remove x_j from our finite collection of points and proceed to construct W for the smaller collection.

Secondly, part (b) is an immediate consequence of part (a). Indeed, since G is a finite group, generically free G-varieties are precisely faithful G-varieties, i.e., G-varieties, where every nonidentity element of G acts nontrivially. The set

$$X_0 = \{x \in X \mid \operatorname{Stab}(x) = \{1\}\}$$

is open and dense in X; in order to ensure that W is generically free, it is enough to construct W so that $W \cap X_0 \neq \emptyset$. This is accomplished by applying part (a) to the collection $\{x_0, x_1, \dots, x_s\}$, where $x_0 \in X_0$. Therefore, it is enough to prove part (a).

Thirdly, since G is a finite group and X is projective, there exists a (finite) geometric quotient morphism $\psi \colon X \longrightarrow X//G$ with $X//G$ projective; see Lemma 2.1. Since X is a primitive G-variety, $X//G$ is irreducible. (Recall that the geometric quotient $X//G$ is a birational model for the rational quotient X/G which is irreducible since X is primitive.) Note that X is partitioned into a union of non-intersecting smooth locally closed subsets $\widetilde{X^H} = \{x \in X \mid \operatorname{Stab}(x) = H\}$, where

H ranges over the set of subgroups of G. By the Luna Slice Theorem [PV, Theorem 6.1] the morphism

$$\psi|_{\widetilde{X^H}} : \widetilde{X^H} \longrightarrow \psi(\widetilde{X^H}) \tag{9.5}$$

is étale, and hence, the sets $\psi(\widetilde{X^H})$ are also smooth. (Note that Luna's theorem can be applied to the G-action in a neighborhood of any point of X by Lemma 2.1(a).) Two subvarieties $\psi(\widetilde{X^H})$ and $\psi(\widetilde{X^{H'}})$ coincide if the subgroups H and H' are conjugate, and are disjoint otherwise. In other words, $X//G$ is partitioned into a union of nonintersecting smooth locally closed subsets $\psi(\widetilde{X^H})$ for all conjugacy classes of subgroups $H \subset G$, so that every point $y \in X//G$ lies in $\psi(\widetilde{X^H})$ where H belongs to the conjugacy class of the stabilizers of points in $\psi^{-1}(y)$.

We are now ready to proceed with the proof of part (a). Since $X//G$ is projective, we can embed it in $\mathbb{P}^N$ for some N. Let U be a generically chosen hypersurface of degree $s+1$ in $\mathbb{P}^N$ which passes through $\psi(x_1), \dots, \psi(x_s)$, and let $\overline{W} = X//G \cap U$. We claim that

$$W = \pi^{-1}(\overline{W}) \subset X$$

satisfies the conditions of part (a). By our construction W is a closed G-invariant hypersurface in X passing through $x_1, \dots, x_s$; thus we only need to show that W is smooth and primitive.

Since each x_i lies in X^{H_i} and is not its isolated point, each $\psi(x_i)$ lies in $\psi(\widetilde{X^{H_i}})$ and is not its isolated point; it follows that $\psi(x_i)$ is not an isolated point of any $\psi(\widetilde{X^H})$. By Lemma 9.8(b), U intersects every subvariety $\psi(\widetilde{X^H})$ transversely.

Let $x \in W$ and $H = \mathrm{Stab}(x)$; then $x \in \widetilde{X^H}$ and $\psi(x) \in \psi(\widetilde{X^H})$. Let f be a local equation of U at $\psi(x)$; then $\psi^*(f)$ is a local equation of W in X at x. Since U is transverse to $\psi(\widetilde{X^H})$, the restriction $f|_{\psi(\widetilde{X^H})}$ is nondegenerate at $\psi(x)$. As the morphism (9.5) is étale, $\psi^*(f|_{\psi(\widetilde{X^H})}) = \psi^*(f)|_{\widetilde{X^H}}$ is a nondegenerate function on $\widetilde{X^H}$ at x. Hence, $\psi^*(f)$ is nondegenerate at x; in other words, W is smooth at x.

It remains to prove that W is primitive or, equivalently, $\overline{W}$ is irreducible. By [Ha, Corollary III.7.9], $\overline{W} = X//G \cap U$ is connected. On the other hand, since W is smooth, $\overline{W} = W//G$ is normal. We conclude that $\overline{W}$ is irreducible, as claimed. $\square$

Proof of Proposition 8.6. If $r = 0$ then $H_1 = \cdots = H_s = \{1\}$, and we can take Y to be a set of $|G|$ points with a transitive G-action and $y_1, \dots, y_s$ to be any s points in Y (not necessarily distinct). From now on we shall assume $r \geq 1$.

Let V be a generically free linear representation of G. By Proposition 2.2 and Theorem 2.5, there exists a smooth projective G-variety X such that $X \simeq V$ (as G-varieties) and $\mathrm{Stab}(x)$ is commutative for any $x \in X$. (Note that a Levi-commutative finite group is commutative.) Every H_i has a smooth fixed point in V, namely the origin. Applying the Going Down Theorem 2.6 to the birational isomorphism $V \overset{\simeq}{\dashrightarrow} X$, we conclude that $X^{H_i} \neq \emptyset$ for every i. The resulting smooth projective irreducible generically free G-variety X is the starting point for our construction.

After birationally modifying X by a sequence of blowups with smooth G-equivariant centers, we may assume that there are points $x_1, \dots, x_s \in X$ such that each x_i is fixed by H_i and the codimension of X^{H_i} at x_i is r_i; see Theorem 9.3.

If $\dim X > r = \max_i r_i$ then $\dim X > r_i = \operatorname{codim}_{x_i} X^{H_i}$ and hence, x_i is not an isolated fixed point of H_i for each i. In addition, $\dim X > r \geq 1$ implies $\dim X \geq 2$. Then Theorem 9.7(b) yields a smooth closed generically free G-invariant primitive hypersurface W in X passing through $x_1, \dots, x_s$. Replacing X by this hypersurface reduces $\dim X$ by one. Applying this procedure $\dim X - r$ times, we obtain a smooth G-invariant primitive subvariety Y of dimension r passing through $x_1, \dots, x_s$, and hence, having points fixed by $H_1, \dots, H_s$. This completes the proof of Proposition 8.6 and thus of Theorem 1.4. □

Remark 9.9. A closer examination of the proof of Proposition 8.6 shows that the G-variety Y can, in fact, be constructed over $\mathbb{Q}$. Thus the division algebra D is Theorem 1.4 can be assumed to be defined over $\mathbb{Q}$. This means that there exists a finitely generated field extension $F/\mathbb{Q}$ and a division algebra D_0 with center F such that $\operatorname{trdeg}_{\mathbb{Q}}(F) = 6$ and $D = D_0 \otimes_F K$.

Remark 9.10. Our argument can be modified to prove the following stronger form of Theorem 1.4: for any integer $e \geq 0$ there exists a division algebra D with center K such that

(a) K is a finitely generated extension of k of transcendence degree $6 + 2e$ and

(b) any extension of D of degree s is not a crossed product, provided that $p^{e+1} \nmid s$.

References

[Ad] J. F. Adams, *2-tori in E_8*, Math. Ann., 287 (1987), 29–39.

[BM] E. Bierstone, P. D. Milman, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Invent. math. **128** (1997), no. 2, 207–302.

[Bor$_1$] A. Borel, *Sous groupes commutatifs et torsion des groupes de Lie compacts connexes*, Tôhoku Math. J. (2) **13** (1961), 216–240.

[Bor$_2$] A. Borel, *Linear Algebraic Groups*, 2nd edition, Springer-Verlag, 1991.

[BS] A. Borel, J.-P. Serre, *Sur certains sous groupes des groupes de Lie compacts*, Comment. Math. Helv. **27** (1953), 128–139.

[Br] E. Brussel, *Noncrossed products and nonabelian crossed products over $\mathbb{Q}(t)$ and $\mathbb{Q}((t))$*, Amer. J. Math **117** (1995), no. 2, 377–393.

[BR] J. Buhler, Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), 159–179.

[DC] J. A. Dieudonne, J. B. Carrell, Invariant Theory, Old and New, Academic Press, New York—Longon, 1971.

[Ga] L. Yu. Galitskii, *On the existence of Galois sections*, in "Lie Groups, their Discrete Subgroups and Invariant Theory", Advances in Soviet Math. **8** (1992), Amer. Math. Soc., Providence, RI, 65–68.

[Gri] R. L. Griess, Jr., *Elementary abelian p-subgroups of algebraic groups*, Geom. Dedicata **39** (1991), 253–305.

[Gro] A. Grothendieck, *La torsion homologique et les sections rationnelles*, Exposé 5, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[Ha] R. Hartshorne. Algebraic geometry. Springer, 1977.

[I] A. V. Iltyakov, *On rational invariants of the group E_6*, Proc. Amer. Math. Soc. **124**, no. 12 (1996), 3637–3640.

[JW] B. Jacob, A. R. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1996), no. 2, 693–721.

[Ka] T. Kambayashi, *Projective representations of algebraic groups of transformations*, Amer. J. Math. **88** (1966), 199–205.

[Ko] V. E. Kordonsky, *On the essential dimension and Serre's Conjecture II for exceptional groups*, preprint (in Russian).

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The Book of Involutions, AMS Colloquium Publications, vol. 44.

[L] S. Lang, Algebra, Addison—Wesley, 1965.

[OV] A. L. Onishchik, E. B. Vinberg. Lie Groups and Algebraic Groups. Springer-Verlag, 1990.

[Pf] A. Pfister, Quadratic Forms with Applications to Algebraic Geometry and Topology, London Math. Soc. Lect. Notes Ser. **217**, Cambridge University Press, 1996.

[Po] V. L. Popov, *Sections in Invariant Theory*, Proceedings of the Sophus Lie Memorial Conference, Scandinavian University Press, 1994, 315–362.

[PV] V. L. Popov, E. B. Vinberg, *Invariant Theory*, in Encyclopedia of Math. Sciences **55**, Algebraic Geometry IV, edited by A. N. Parshin and I. R. Shafarevich, Springer-Verlag, 1994.

[Pr] C. Procesi, *The invariant theory of $n \times n$-matrices*, Advances in Math. **19** (1976), 306–381.

[Re] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation Groups, to appear. Preprint available at http://ucs.orst.edu/~reichstz/pub.html.

[RY] Z. Reichstein, B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, with an appendix by J. Kollár and E. Szabó, Canadian J. Math., to appear. Preprint available at http://ucs.orst.edu/~reichstz/pub.html.

[Ro_1] M. Rosenlicht, *Some basic theorems on algebraic groups*, American Journal of Math., **78** (1956), 401–443.

[Ro_2] M. Rosenlicht, *A remark on quotient spaces*, Anais da Academia Brasileira de Ciências **35** (1963), 487–489.

[R] L. H. Rowen, Polynomial Identities in Ring Theory, Academic Press, 1980.

[RS] L. H. Rowen, D. J. Saltman, *Prime to p extensions of division algebras*, Israel J. Math. **78** (1992), 197–207.

[Se_1] J.-P. Serre, *Espaces fibrés algébriques*, Exposé 1, Séminaire C. Chevalley, Anneaux de Chow et applications, 2nd année, IHP, 1958.

[Se_2] J.-P. Serre, Local fields, Springer-Verlag, 1979.

[Se_3] J.-P. Serre, *Cohomologie galoisienne: progrès et problèmes*, in "Séminaire Bourbaki, Volume 1993/94, Exposés 775–789", Astérisque **227** (1995), 229–257.

[Se_4] J.-P. Serre, Galois Cohomology, Springer, 1997.

[Se_5] J.-P. Serre, *Sous-groupes finis des groupes de Lie*, Séminaire Bourbaki, 1998–99, n° 864, Juin 1999.

[SS] T. A. Springer, R. Steinberg, *Conjugacy classes*, in " Seminar on algebraic groups and related Finite Groups", Lect. Notes in Math. **131** (1970), 281–312.

[St] R. Steinberg, *Torsion in reductive groups*, Advances in Math. **15** (1975), 63–92.

[TA_1] J.-P. Tignol, S. A. Amitsur, *Kummer subfields of Maltsev-Neumann division algebras*, Israel J. Math. **50**, nos. 1-2 (1985), 114–144.

[TA_2] J.-P. Tignol, S. A. Amitsur, *Symplectic modules*, Israel J. Math. **54**, no. 3 (1986), 266–290.

[T_1] J. Tits, Résumé de cours, Annuaire du College de France, 1991-92, 115–133.

[T_2] J. Tits, *Sur les degrés des extensions de corps déployant les groupes algébriques simples*, C. R. Acad. Sci. Paris, t. 315, Série I (1992), 1131–1138.

[V] O. E. Villamayor U., *Patching local uniformizations*, Ann. scient. Éc. Norm. Sup., 4e série, **25** (1992), 629–677.

Department of Mathematics, Oregon State University, Corvallis, OR 97331
E-mail address: `zinovy@math.orst.edu`

Department of Mathematics and Computer Science, University of the Negev, Be'er Sheva', Israel
Current mailing address: Hashofar 26/3, Ma'ale Adumim, Israel
E-mail address: `youssin@math.bgu.ac.il`