STABLY CAYLEY GROUPS IN CHARACTERISTIC 0

M. BOROVOI, B. KUNYAVSKIĬ, N. LEMIRE, AND Z. REICHSTEIN

Abstract. A linear algebraic group G over a field k is called a Cayley group if it admits a Cayley map, i.e., a G-equivariant birational isomorphism over k between the group variety G and its Lie algebra. A Cayley map can be thought of as a partial algebraic analogue of the exponential map. A prototypical example is the classical "Cayley transform" for the special orthogonal group $\mathbf{SO}_n$ defined by Arthur Cayley in 1846. A linear algebraic group G is called *stably Cayley* if $G \times \mathbb{G}_m^r$ is Cayley for some $r \geq 0$. Here $\mathbb{G}_m^r$ denotes the split r-dimensional k-torus. These notions were introduced in 2006 by Lemire, Popov and Reichstein, who classified Cayley and stably Cayley simple groups over an algebraically closed field of characteristic zero.

In this paper we study reductive Cayley groups over an arbitrary field k of characteristic zero. The condition of being Cayley is considerably more delicate in this setting. Our main results are a criterion for a reductive group G to be stably Cayley, formulated in terms of its character lattice, and a classification of stably Cayley simple (but not necessarily absolutely simple) groups.

Contents

2010 *Mathematics Subject Classification.* Primary 20G15, 20C10.

Key words and phrases. Linear algebraic group, Cayley group, Cayley map, algebraic torus, integral representation, quasi-permutation lattice.

Borovoi was supported in part by the Hermann Minkowski Center for Geometry.

Kunyavskiĭ was supported in part by the Minerva Foundation through the Emmy Noether Institute for Mathematics.

Lemire was supported in part by an NSERC Discovery Grant.

Reichstein was supported in part by an NSERC Discovery Grant.

1. Introduction

Let k be a field of characteristic 0 and G be a connected linear algebraic k-group. A birational isomorphism $\phi\colon \operatorname{Lie}(G) \overset{\simeq}{\dashrightarrow} G$ is called a *Cayley map* if it is equivariant with respect to the conjugation action of G on itself and the adjoint action of G on its Lie algebra $\operatorname{Lie}(G)$, respectively. A Cayley map can be thought of as a partial algebraic analogue of the exponential map. A prototypical example is the classical "Cayley transform" for the special orthogonal group $\mathbf{SO}_n$ defined by Arthur Cayley [8] in 1846. A linear algebraic group G is called *Cayley* if it admits a Cayley map and *stably Cayley* if $G \times_k \mathbb{G}_m^r$ is Cayley for some $r \geq 0$. Here $\mathbb{G}_m$ denotes the split 1-dimensional torus. These notions were introduced by Lemire, Popov and Reichstein [20]; for a more detailed discussion and numerous classical examples, we refer the reader to [20, Introduction]. The main results of [20] are the classifications of simple Cayley and stably Cayley groups in the case where the base field k is algebraically closed and of characteristic 0. The goal of this paper is to extend some of these results to the case where k is an arbitrary field of characteristic 0.

Example 1.1. If k is algebraically closed and G is a reductive k-group, then by [20, Theorem 1.27] G is stably Cayley if and only if its character lattice is quasi-permutation; see Definition 2.1.

Example 1.2. Let T be a k-torus of dimension d. By definition, T is Cayley (respectively, stably Cayley) over k if and only if T is k-rational (respectively, stably k-rational). If k is algebraically closed, then $T \simeq \mathbb{G}_m^d$, hence T is always rational, and thus always Cayley. More generally, Voskresenskiĭ's criterion for stable rationality [29, Theorem 4.7.2] asserts that T is stably rational if and only if the character lattice $\mathsf{X}(T)$ is quasi-permutation (see Definition 2.1).

It has been conjectured that every stably rational torus is rational. To the best of our knowledge, this conjecture is still open. Moreover, we are not aware of any simple lattice-theoretic criterion for the rationality of T.

Note that the term "character lattice" is used in different ways in Examples 1.1 and 1.2. In both cases the underlying $\mathbb{Z}$-module is $\mathsf{X}(\overline{T})$ (where $\overline{T} = T \times_k \bar{k}$, $\bar{k}$ is an algebraic closure of k, and T is a maximal torus of G in Example 1.1) but the group acting on $\mathsf{X}(\overline{T})$ is the Weyl group $W = W(G,T)$ in Example 1.1 and the Galois group $\mathrm{Gal}(k)$ in Example 1.2. A key role in this paper will be played by the *character lattice* $\mathsf{X}(G)$ of a reductive k-group G, a notion that bridges the special cases considered in these two examples. The underlying $\mathbb{Z}$-module in this general setting is still $\mathsf{X}(\overline{T})$, but the group acting on it is the *extended Weyl group* $\mathrm{W}^{\mathrm{ext}} = W \rtimes A$, where W is the usual Weyl group of $\overline{G}$ and A is the image of $\mathrm{Gal}(\bar{k}/k)$ under the so-called "$*$-action" (see Tits [27, § 2.3] for a construction of the $*$-action). For the definition of $\mathrm{W}^{\mathrm{ext}}$, see Section 4. Equivalently, $\mathsf{X}(G)$ is the character lattice of the generic torus T_{gen} of G. This torus is defined over a certain transcendental field extension K_{gen} of k; see [29, §4.2]. Informally speaking, we think of the Weyl group W as "the geometric part" of $\mathrm{W}^{\mathrm{ext}}$, and of the image A of the $*$-action as "the arithmetic part". Examples 1.1 and 1.2 represent two opposite extremes, where the group $\mathrm{W}^{\mathrm{ext}}$ is "purely geometric" and "purely arithmetic", respectively. As we pass from a reductive group G to its generic torus T_{gen}, the geometric part migrates to the arithmetic part, while the overall group $\mathrm{W}^{\mathrm{ext}}$ remains the same.

We are now ready to state our first main theorem.

Theorem 1.3. *Let G be a reductive k-group. The following are equivalent:*

(a) *G is stably Cayley;*
(b) *for every field extension K/k, every maximal K-torus $T \subset G_K$ is stably rational over K;*
(c) *the generic K_{gen}-torus T_{gen} of G is stably rational;*
(d) *the character lattice $\mathsf{X}(G)$ of G is quasi-permutation.*

Next we turn our attention to classifying stably Cayley simple groups over an arbitrary field k of characteristic zero. The following results extend [20, Theorem 1.28], where k is assumed to be algebraically closed.

Theorem 1.4. *Let k be a field of characteristic* 0 *and G be an absolutely simple k-group. Then the following conditions are equivalent:*

(a) *G is stably Cayley over k;*

(b) *G is a k-form of one of the following groups:*

$$\mathbf{SL}_3,\ \mathbf{PGL}_n\ (n = 2 \text{ or } n \geq 3 \text{ odd}),\ \mathbf{SO}_n\ (n \geq 5),\ \mathbf{Sp}_{2n}\ (n \geq 1),\ \mathbf{G}_2,$$

or an inner *k-form of $\mathbf{PGL}_n$ ($n \geq 4$ even).*

Theorem 1.5. *Let G be a simple* (*but not necessarily absolutely simple*) *k-group over a field k of characteristic 0. Then the following conditions are equivalent:*

(a) *G is stably Cayley over k;*

(b) *G is isomorphic to $R_{l/k}(G_1)$, where l/k is a finite field extension and G_1 is either a stably Cayley absolutely simple group over l* (*i.e., one of the groups listed in Theorem* 1.4(*b*)) *or an outer l-form of $\mathbf{SO}_4$.*

Here $R_{l/k}$ denotes the Weil functor of restriction of scalars.

A key consequence of Theorem 1.3 is that, for a reductive k-group G, being stably Cayley is a property of its character lattice. If "stably Cayley" is replaced by "Cayley", this is no longer the case, even for simple groups. Indeed, the simple groups: $\mathbf{SU}_3$ and split $\mathbf{G}_2$, both defined over the field $\mathbb{R}$ of real numbers, have the same character lattice; both are stably Cayley. By a theorem of Iskovskikh [16], $\mathbf{G}_2$ is not Cayley over $\mathbb{R}$ (not even over $\mathbb{C}$); cf. [20, Proposition 9.10]. On the other hand, $\mathbf{SU}_3$ is Cayley, see Borovoi–Dolgachev [4, Thm. 1.2].

For reasons illustrated by the above example the problem of classifying simple Cayley groups, in a manner analogous to Theorems 1.4 and 1.5, appears to be out of reach at the moment. In particular, we do not know which outer forms of $\mathbf{PGL}_n$ (if any) are Cayley, for any odd integer $n \geq 5$. Note that all the inner forms of $\mathbf{PGL}_n$ over a field k of characteristic 0 are Cayley, see [20, Example 1.11]. The outer forms of $\mathbf{PGL}_n$ for even $n \geq 4$ are not stably Cayley (and hence, not Cayley) by Theorem 1.4.

The rest of this paper is structured as follows. Sections 2–6 are devoted to preliminary material on quasi-permutation lattices, automorphisms and semi-automorphisms of algebraic groups over non-algebraically closed fields, and (G, S)-fibrations. While some of this material is known, we have not been able to find references, where the definitions and results we need are proved in full generality. We have thus opted for a largely self-contained exposition.

Theorem 1.3 is proved in Section 7. Theorem 1.4 is an easy consequence of Theorem 1.3 and previously known results on character lattices of absolutely simple groups from [20] and Cortella and Kunyavskiĭ's paper [13]; the details of this argument are presented in Section 8. The proof of Theorem 1.5 relies on new results of character lattices and thus requires considerably more work. After passing to the algebraic closure $\bar{k}$, we are faced with the problem of classifying semisimple stably Cayley groups of the form $G = H^m/C$, where H is a simply connected simple group over $\bar{k}$ and $C \subset H^m$ is a central subgroup. Our classification theorem for such groups is stated in Section 9; see Theorem 9.1. The proof of Theorem 9.1, based on case-by-case analysis, occupies Section 10–18. In Section 19 we deduce Theorem 1.5 from Theorem 9.1 by passing back from $\bar{k}$ to k.

2. Preliminaries on quasi-permutation lattices

Let Γ be a finite group. By a Γ-lattice we mean a finitely generated free abelian group M viewed together with an integral representation $\Gamma \to \mathrm{Aut}(M)$. We also think of M as a $\mathbb{Z}[\Gamma]$-module; by a morphism (or exact sequence) of lattices we mean a morphism (or exact sequence) of $\mathbb{Z}[\Gamma]$-modules. When we write "lattice", rather than "Γ-lattice", we mean a Γ-lattice for some finite group Γ. We say that a lattice is faithful if the underlying integral representation is faithful. In those cases where we want to emphasize the dependence on Γ, we will sometimes write a lattice as a pair (Γ, M). (The integral representation $\Gamma \to \mathrm{Aut}(M)$ is assumed to be clear from the context.) This notation will be particularly useful if we view M as a Γ_0-lattice with respect to the different subgroups Γ_0 of Γ.

If $\varphi\colon \Gamma \xrightarrow{\sim} \Gamma'$ is an isomorphism of finite groups, then by a φ-isomorphism of lattices (Γ, L), (Γ', L') we will mean an isomorphism $\psi\colon L \xrightarrow{\sim} L'$ such that

$$\psi(\gamma x) = \varphi(\gamma)\psi(x) \text{ for all } \gamma \in \Gamma, x \in L.$$

By abuse of notation we will sometimes say that the lattices (Γ, M) and (Γ', M') are *isomorphic* instead of "φ-isomorphic" in two special cases: if $\Gamma = \Gamma'$ and $\varphi = \mathrm{id}$, or (ii) (Γ, M) and (Γ', M') are φ-isomorphic for some $\varphi\colon \Gamma \xrightarrow{\sim} \Gamma'$.

Now let k be a field, $T_{\mathrm{spl}} = \mathbb{G}_{\mathrm{m}}^d$ be the split d-dimensional k-torus, Γ be a finite group. By a multiplicative action of Γ on T_{spl} we mean an action by automorphisms of T_{spl} as an algebraic group over k. Recall that the following objects are in a natural bijective correspondence:

(i) Γ-lattices of rank d (up to isomorphism);
(ii) integral representations $\phi\colon \Gamma \to \mathbf{GL}_d(\mathbb{Z})$ (up to conjugacy in $\mathbf{GL}_d(\mathbb{Z})$);
(iii) multiplicative actions $\Gamma \to \mathrm{Aut}_{k\text{-grp}}(T_{\mathrm{spl}})$ (up to an automorphism of T_{spl} as an algebraic k-group).

A Γ-lattice L is called *permutation* if it has a $\mathbb{Z}$-basis permuted by Γ. We say that two Γ-lattices L and L' are *equivalent*, and write $L \sim L'$, if there exist short exact sequences

$$0 \to L \to E \to P \to 0 \qquad \text{and} \qquad 0 \to L' \to E \to P' \to 0$$

with the same Γ-lattice E, where P and P' are permutation Γ-lattices. For a proof that this is indeed an equivalence relation, see [10, Lemma 8]. Note that if there exists a short exact sequence

$$0 \to L \to L' \to Q \to 0,$$

where Q is a permutation Γ-lattice, then the trivial short exact sequence

$$0 \to L' \to L' \to 0 \to 0$$

shows that $L \sim L'$. In particular, if P is a permutation Γ-lattice, then the short exact sequence

$$0 \to 0 \to P \to P \to 0$$

shows that $P \sim 0$. If Γ-lattices L, L', M, M' satisfy $L \sim L'$ and $M \sim M'$ then $L \oplus M \sim L' \oplus M'$.

Definition 2.1. A Γ-lattice L is called *quasi-permutation* if it is equivalent to a permutation lattice, i.e., if there exists a short exact sequence

$$0 \to L \to P \to P' \to 0, \tag{2.1}$$

where both P and P' are permutation Γ-lattices.

Lemma 2.2. *Let $\Gamma_1 \twoheadrightarrow \Gamma$ be a surjective homomorphism of finite groups, and let L be a Γ-lattice. Then L is quasi-permutation as a Γ_1-lattice if and only if it is quasi-permutation as a Γ-lattice.*

Proof. It suffices to prove "only if". Assume that L is quasi-permutation as a Γ_1-lattice and let Γ_0 denote the kernel $\ker[\Gamma_1 \to \Gamma]$. From the short exact sequence (2.1) of Γ_1-lattices, where P and P' are some permutation Γ_1-lattices, we obtain the Γ_0-cohomology exact sequence

$$0 \to L \to P^{\Gamma_0} \to (P')^{\Gamma_0} \to 0$$

(because $L^{\Gamma_0} = L$ and $H^1(\Gamma_0, L) = 0$), which is a short exact sequence of Γ-lattices. It is easy to see that P^{Γ_0} and $(P')^{\Gamma_0}$ are permutation Γ-lattices, thus L is a quasi-permutation Γ-lattice. □

We say that a Γ-action on an algebraic variety X, defined over k, is *linearizable* (respectively, *stably linearizable*) if X is Γ-equivariantly birationally isomorphic (respectively, Γ-equivariantly stably birationally isomorphic) to a finite-dimensional k-vector space V with a linear Γ-action.

Remark 2.3. By the no-name lemma any two faithful linear actions of a finite group Γ on k-vector spaces V_1 and V_2 are stably Γ-equivariantly birationally equivalent; see, e.g., [20, Lemma 2.12(c)]. This makes stable linearizability a particularly natural notion.

Lemma 2.4. *Let L be a Γ-lattice, and let T_L be the associated split k-torus with multiplicative Γ-action (i.e., $\mathsf{X}(T_L) = L$).*

(a) *If L is a permutation lattice then the Γ-action on T_L is linearizable.*
(b) *L is quasi-permutation if and only if the Γ-action on T_L is stably linearizable.*

Proof. (a) Suppose $L \simeq \mathbb{Z}[S]$ for some finite Γ-set S. Let V be the k-vector space with basis $(e_s)_{s \in S}$. Then V carries a natural (permutation) Γ-action.

The morphism $T_L \to V$ given by

$$t \to \sum_{s \in S} s(t) e_s$$

is easily seen to be a Γ-equivariant birational isomorphism.

(b) By Lemma 2.2 we may assume that Γ acts faithfully on L. Let P be a faithful permutation Γ-lattice (e.g., $P = \mathbb{Z}[\Gamma]$). Let V be the linear representation of G constructed in part (a). It now suffices to show that the following conditions are equivalent:

(i) L is quasi-permutation,

(ii) $L \sim P$,

(iii) T_L and T_P are Γ-equivariantly stably birationally isomorphic,

(iv) T_L and V are Γ-equivariantly stably birationally isomorphic,

(v) T_L is stably linearizable.

Indeed, (i) and (ii) are equivalent by Definition 2.1. (ii) and (iii) are equivalent by [19, Proposition 1.4]; note that, in the terminology of [19, §1.4] $k(L)$ is precisely the field of rational functions of T_L.

In the proof of part (a) we showed that T_P and V are Γ-equivariantly birationally isomorphic. Consequently, (iii) is equivalent to (iv). Finally, (iv) $\Longrightarrow$ (v) by definition, and (v) $\Longrightarrow$ (iv) by the no-name lemma; see Remark 2.3. $\square$

Lemma 2.5 (cf. [20], Proposition 4.8)**.** *Let $W_1, \dots, W_m$ be finite groups. For each $i = 1, \dots, m$, let V_i be a finite-dimensional $\mathbb{Q}$-representation of W_i. Set $V := V_1 \oplus \dots \oplus V_m$. Suppose $L \subset V$ is a free abelian subgroup, invariant under $W := W_1 \times \dots \times W_m$.*

If L is a quasi-permutation W-lattice, then $L_i := L \cap V_i$ is a quasi-permutation W_i-lattice, for each $i = 1, \dots, m$.

Proof. It suffices to prove the lemma for $i = 1$. Set $V' := V/V_1 = V_2 \oplus \dots \oplus V_m$ and $L' = L/L_1 \subset V'$. Then W_1 acts trivially on V' and on L', in particular, L' is a permutation W_1-lattice. It follows from the short exact sequence of W_1-lattices

$$0 \to L_1 \to L \to L' \to 0$$

that the W_1-lattices L_1 and L are equivalent.

Now assume that L is a quasi-permutation W-lattice. Then it is a quasi-permutation W_1-lattice, and hence so is L_1. $\square$

Lemma 2.6 (cf. [20], Lemma 4.7)**.** *Let $W_1, \dots, W_m$ be finite groups. For each $i = 1, \dots, m$, let L_i be a W_i-lattice. Set $W := W_1 \times \dots \times W_m$ and construct a W-lattice $L := L_1 \oplus \dots \oplus L_m$.*

Then L is a quasi-permutation W-lattice if and only if L_i is a quasi-permutation W_i-lattice for each $i = 1, \dots, m$.

Proof. The "if" assertion is obvious from the definition. The "only if" assertion follows from Lemma 2.5. $\square$

Lemma 2.7. *Let Γ be a finite group and L a Γ-lattice of rank 1 or 2. Then L is quasi-permutation.*

Proof. This is easily deduced from [29, §4.9, Examples 6, 7]. □

3. Automorphisms and semi-automorphisms of split reductive groups

3.1. **Notational conventions.** Let G be a split reductive group over a field k. We will write T for a maximal k-torus of G, B for a Borel subgroup, $Z = Z(G)$ for the center of G, G^{ad} for G/Z, and T^{ad} for T/Z. We identify G^{ad} with the algebraic group $\mathrm{Inn}(G)$ of inner automorphisms of G. If $g \in G^{\mathrm{ad}}(k)$ (or $g \in T^{\mathrm{ad}}(k)$), we write $\mathrm{inn}(g)$ for the corresponding inner automorphism of G.

We will sometimes refer to a pair (T, B), where T is a split maximal k-torus and $T \subset B \subset G$ is a Borel subgroup defined over k, as a *Borel pair.* It is well known that the natural action of $G^{\mathrm{ad}}(k)$ on the set of Borel pairs is transitive and that the stabilizer in $G^{\mathrm{ad}}(k)$ of a Borel pair (T, B) is $T^{\mathrm{ad}}(k)$.

Given a split maximal torus $T \subset G$, let $\mathrm{RD}(G, T) := (X, X^\vee, R, R^\vee)$ be the *root datum* of (G, T). Here $X = \mathsf{X}(T)$ is the character group of T, $X^\vee = \mathrm{Hom}(X, \mathbb{Z})$ is the cocharacter group of T, $R = R(G, T) \subset X$ is the root system of G with respect to T, and $R^\vee \subset X^\vee$ is the coroot system of G with respect to T. The bijection $R \to R^\vee$ sending a root to the corresponding coroot is a part of the root datum structure. For details, see [25, §1.1] or [26, §7.4].

Given a Borel pair (T, B), let $\mathrm{BRD}(G, T, B) := (X, X^\vee, R, R^\vee, \Delta, \Delta^\vee)$ be the *based root datum of* (G, T, B). Here $\Delta \subset R$ is the basis of R defined by B, and $\Delta^\vee \subset R^\vee$ is the corresponding basis of $R^\vee$. For details, see [25, §1.9].

The automorphism group $\mathrm{Aut}(G)$ is known to carry the structure of a k-group scheme; note however, that this k-group scheme may not be of finite type. The automorphism groups $\mathrm{Aut}\,\mathrm{RD}(G, T)$ and $\mathrm{Aut}\,\mathrm{BRD}(G, T, B)$ are closed group subschemes of $\mathrm{Aut}(G)$ defined over k. These k-group schemes are discrete, in the sense that their identity components are trivial.

3.2. **Semi-automorphisms.** Let $\overline{G}$ be a connected reductive group over an algebraic closure $\bar{k}$ of k. We denote by $\mathrm{SAut}(\overline{G})$ the group of $\bar{k}/k$-semi-automorphisms of $\overline{G}$. We view $\mathrm{SAut}(\overline{G})$ as an abstract group. For a definition of a semi-automorphism, see [3, §1.1] or [14, §1.2]. (Note that in these papers semi-automorphisms are called "semialgebraic" and "semilinear" automorphisms, respectively.) If G is a k-form of $\overline{G}$, then any element $\sigma \in \mathrm{Gal}(\bar{k}/k)$ defines a σ-semi-automorphism $\sigma_*\colon \overline{G} \to \overline{G}$, and any semi-automorphism of $\overline{G}$ is of the form $a = \alpha \circ \sigma_*$ where $\sigma \in \mathrm{Gal}(\bar{k}/k)$ and $\alpha\colon \overline{G} \to \overline{G}$ is a $\bar{k}$-automorphism of the $\bar{k}$-group $\overline{G}$.

Fix $(\overline{T}, \overline{B})$ as above. For any $a \in \mathrm{SAut}(\overline{G})$ there exists $g \in \overline{G}^{\mathrm{ad}}(\bar{k})$ such that $\mathrm{inn}(g)(a(\overline{T}), a(\overline{B})) = (\overline{T}, \overline{B})$. The semi-automorphism $\mathrm{inn}(g)a$

of $\overline{G}$ defines a semi-automorphism of $\overline{T}$ depending only on a (since the coset $\overline{T}^{\mathrm{ad}}g^{-1}$ is uniquely determined). The automorphism of $X = \mathsf{X}(\overline{T})$ induced by $\mathrm{inn}(g)a$ preserves $R = R(\overline{G}, \overline{T})$ and $\overline{B}$ and thus permutes the elements of the basis Δ of R defined by $\overline{B}$. In other words, it gives rise to an automorphism $\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B}) \to \mathrm{BRD}(\overline{G}, \overline{T}, \overline{B})$, depending only on a, which we denote by $\varphi_{\overline{T},\overline{B}}(a)$.

Proposition 3.1. (a) $\varphi_{\overline{T},\overline{B}}\colon \mathrm{SAut}(\overline{G}) \to \mathrm{Aut}\,\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B})$ *is a group homomorphism.*

(b) $\mathrm{Inn}(\overline{G}) \subset \mathrm{Ker}(\varphi_{\overline{T},\overline{B}})$.

(c) *Suppose* $(\overline{T}', \overline{B}')$ *is another Borel pair for* $\overline{G}$. *Choose* $u \in \overline{G}^{\mathrm{ad}}(\bar{k})$ *so that* $(\overline{T}, \overline{B}) = \mathrm{inn}(u)(\overline{T}', \overline{B}')$. *Then the following diagram commutes*

$$\begin{tikzcd}
 & \mathrm{Aut}\,\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B}) \arrow[dd, "\mathrm{inn}(u)^*"] \\
\mathrm{SAut}(\overline{G}) \arrow[ur, "\varphi_{\overline{T},\overline{B}}"] \arrow[dr, "\varphi_{\overline{T}',\overline{B}'}"'] & \\
 & \mathrm{Aut}\,\mathrm{BRD}(\overline{G}, \overline{T}', \overline{B}').
\end{tikzcd}$$

Moreover, the automorphism $\mathrm{inn}(u)^*$ *in this diagram is independent of the choice of* u.

Proof. (a) Given $a_1, a_2 \in \mathrm{SAut}(\overline{G})$, choose $g_1, g_2 \in \overline{G}^{\mathrm{ad}}$ so that $\mathrm{inn}(g_i)\, a_i(\overline{T}, \overline{B}) = (\overline{T}, \overline{B})$. Then $\mathrm{inn}(g_1)\,(a_1\,\mathrm{inn}(g_2)\,a_1^{-1}) \in \mathrm{Inn}(\overline{G})$; denote this inner automorphism by $\mathrm{inn}(g)$ for some $g \in \overline{G}^{\mathrm{ad}}$. Then $\mathrm{inn}(g)a_1a_2(\overline{T}, \overline{B}) = (\overline{T}, \overline{B})$ and thus

$$\varphi_{\overline{T},\overline{B}}(a_1a_2) = \mathrm{inn}(g)\,a_1a_2 = \mathrm{inn}(g_1)\,a_1\,\mathrm{inn}(g_2)\,a_2 = \varphi_{\overline{T},\overline{B}}(a_1)\,\varphi_{\overline{T},\overline{B}}(a_2)\,.$$

Therefore, $\varphi_{\overline{T},\overline{B}}$ is a homomorphism.

(b) is obvious from the definition.

(c) Let $a \in \mathrm{SAut}(\overline{G})$. By our choice of $u \in \overline{G}^{\mathrm{ad}}$, we have $(\overline{T}, \overline{B}) = \mathrm{inn}(u)(\overline{T}', \overline{B}')$. Choose $g \in \overline{G}^{\mathrm{ad}}$, as before, so that $\mathrm{inn}(g)\,a(\overline{T}, \overline{B}) = (\overline{T}, \overline{B})$. Then

$$\mathrm{inn}(u^{-1})\,\mathrm{inn}(g)\,(a\,\mathrm{inn}(u)\,a^{-1}) \in \mathrm{Inn}(\overline{G});$$

denote this automorphism by $\mathrm{inn}(g')$ for some $g' \in \overline{G}^{\mathrm{ad}}$. One readily checks that $\mathrm{inn}(g')a(\overline{T}', \overline{B}') = (\overline{T}', \overline{B}')$ and thus

$$\varphi_{\overline{T}',\overline{B}'}(a) = \mathrm{inn}(g')\,a = \mathrm{inn}(u^{-1})\,\mathrm{inn}(g)\,a\,\mathrm{inn}(u) = \mathrm{inn}(u^{-1})\,\varphi_{\overline{T},\overline{B}}(a)\,\mathrm{inn}(u),$$

as desired. To prove the last assertion of part (c), note that the coset uT is independent of the choice of u. Hence, so is the map $\mathrm{inn}(u)^*$ in the diagram. $\square$

3.3. **Automorphisms of split reductive groups.**

Proposition 3.2 (cf. [24, Exposé XXIV, Thm. 1.3])**.** *Let G be a split connected reductive group defined over k, $T \subset G$ be a split maximal torus, and $B \supset T$ be a Borel subgroup of G defined over k. Set $\overline{G} := G \times_k \bar{k}$.*

(a) *The composite homomorphism of abstract groups*

$$\phi_{T,B}\colon \operatorname{Aut}(\overline{G}) \hookrightarrow \operatorname{SAut}(\overline{G}) \xrightarrow{\varphi_{\overline{T},\overline{B}}} \operatorname{Aut}\operatorname{BRD}(G,T,B)$$

admits a $\operatorname{Gal}(\bar{k}/k)$*-equivariant splitting (homomorphic section) ψ of the form*

$$\psi\colon \operatorname{Aut}\operatorname{BRD}(G,T,B) \hookrightarrow \operatorname{Aut}(G,T,B) \hookrightarrow \operatorname{Aut}(\overline{G}).$$

Here $\operatorname{Aut}(G,T,B)$ *denotes the subgroup of* $\operatorname{Aut}(G)$ *consisting of automorphisms that preserve the Borel pair (T,B).*

(b) *The homomorphism $\phi_{T,B}$ of part (a) fits into a split short exact sequence of abstract groups*

$$1 \longrightarrow \operatorname{Inn}(\overline{G}) \longrightarrow \operatorname{Aut}(\overline{G}) \xrightarrow{\phi_{T,B}} \operatorname{Aut}\operatorname{BRD}(G,T,B) \longrightarrow 1,$$

which comes from a split short exact sequences of group schemes over k

$$1 \longrightarrow G^{\mathrm{ad}} \longrightarrow \operatorname{Aut}(G) \xrightarrow{\phi} \operatorname{Aut}\operatorname{BRD}(G,T,B) \longrightarrow 1. \tag{3.1}$$

Note that since T is split over k, the $\operatorname{Gal}(\bar{k}/k)$-action on $\operatorname{Aut}\operatorname{BRD}(G,T,B)$ is trivial.

Proof. (a) Recall that a *pinning* of (G,T,B) is a choice of a nonzero $X_\alpha \subset \mathfrak{g}_\alpha$ for each $\alpha \in \Delta$, where

$$\operatorname{Lie}(G) = \operatorname{Lie}(T) \oplus \bigoplus_{\alpha\in R} \mathfrak{g}_\alpha$$

is the root decomposition, and Δ is the basis of $R = R(G,T)$ associated with B. By the isomorphism theorem, see [24, Exposé XXIII, Thm. 4.1] or [12, Proposition 1.5.5], the canonical homomorphism

$$\operatorname{Aut}(G,T,B,(X_\alpha)_{\alpha\in\Delta}) \to \operatorname{Aut}\ \operatorname{BRD}(G,T,B)$$

is an isomorphism. Composing the inverse isomorphism with the natural embeddings

$$\operatorname{Aut}(G,T,B,(X_\alpha)_{\alpha\in\Delta}) \hookrightarrow \operatorname{Aut}(G,T,B) \hookrightarrow \operatorname{Aut}(G) \hookrightarrow \operatorname{Aut}(\overline{G}),$$

we obtain a section ψ of $\phi_{T,B}$ of the desired form.

(b) See [24, Exposé XXIV, Proof of Thm. 1.3]. □

Corollary 3.3. *Every abstract subgroup $\mathfrak{M} \subset \operatorname{Aut}(\overline{G})$, containing $\operatorname{Inn}(\overline{G})$ as a subgroup of finite index, is of the form $\mathfrak{M} = M(\bar{k})$ for some linear algebraic k-group $M = \operatorname{Inn}(G) \rtimes A \subset \operatorname{Aut}(G)$. Here $A \subset \operatorname{Aut}(G,T,B)$ is a finite k-group, all of whose $\bar{k}$-points are defined over k.*

Proof. Set $A' := \phi_{T,B}(\mathfrak{M}) \subset \operatorname{Aut}\operatorname{BRD}(G,T,B)$. Then A' is a finite algebraic k-group all of whose $\bar{k}$-points are defined over k. Set $M = \phi^{-1}(A') \subset \operatorname{Aut}(G)$, where $\phi\colon \operatorname{Aut}(G) \to \operatorname{Aut}\operatorname{BRD}(G,T,B)$ is a homomorphism of group k-schemes, as in (3.1). Then M is a group k-scheme and $M(\bar{k}) = \mathfrak{M}$. Set $A = \psi(A') \subset \operatorname{Aut}(G,T,B)$, where ψ is the splitting of Proposition 3.2, then $M = \operatorname{Inn}(G) \rtimes A$. Since M has finitely many connected components, and the identity component G^{ad} of M is an affine k-group, we conclude that M is affine as well. In other words, M is a linear algebraic k-group, as desired. □

4. The character lattice and the generic torus

Throughout this section G will denote a connected reductive k-group, not necessarily split, and $T \subset G$ will denote a maximal k-torus. We write $\overline{G} := G \times_k \bar{k}$, $\overline{T} = T \times_k \bar{k}$, and choose a Borel subgroup $\overline{B} \supset \overline{T}$ of $\overline{G}$.

4.1. **The character lattice of a reductive group.**

Definition 4.1. (a) We define $A_{T,\overline{B}}$ to be the image of the composite homomorphism

$$\operatorname{Gal}(\bar{k}/k) \hookrightarrow \operatorname{SAut}(\overline{G}) \xrightarrow{\varphi_{\overline{T},\overline{B}}} \operatorname{Aut}\ \operatorname{BRD}(\overline{G},\overline{T},\overline{B}) \hookrightarrow \operatorname{Aut}\ \mathsf{X}(\overline{T}).$$

(b) We define the *extended Weyl group* $\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B})$ by

$$\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B}) := W(\overline{G},\overline{T}) \cdot A_{T,\overline{B}} \subset \operatorname{Aut}\ \mathsf{X}(\overline{T}).$$

Note that $\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B})$ is a subgroup of $\operatorname{Aut}\ \operatorname{RD}(\overline{G},\overline{T})$ (and thus of $\operatorname{Aut}\ \mathsf{X}(\overline{T})$), because $W(\overline{G},\overline{T})$ is normal in $\operatorname{Aut}\ \operatorname{RD}(\overline{G},\overline{T})$. We call the pair $(\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B}),\mathsf{X}(\overline{T}))$ *the character lattice of* G.

Remark 4.2. Let $T' \subset G$ be another maximal k-torus, and $\overline{B}' \supset \overline{T}'$ be a Borel subgroup of $\overline{G}$. Then it is easy to see that for u as in Proposition 3.1(c), the isomorphism $\operatorname{inn}(u)^*\colon \mathsf{X}(\overline{T}) \to \mathsf{X}(\overline{T}')$ induces an isomorphism of groups

$$A_{\overline{T},\overline{B}} \xrightarrow{\sim} A_{\overline{T}',\overline{B}'}$$

and an isomorphism of lattices $(\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B}),\mathsf{X}(\overline{T})) \xrightarrow{\sim} (\mathrm{W}^{\mathrm{ext}}(G,T',\overline{B}')),\mathsf{X}(\overline{T}'))$. In other words, the character lattice $(\mathrm{W}^{\mathrm{ext}}(\overline{G},\overline{T},\overline{B}),\mathsf{X}(\overline{T}))$ is defined uniquely up to a canonical isomorphism.

Moreover, if $T = T'$ then $A_{T,\overline{B}'} = wA_{T,\overline{B}}w^{-1}$ for some $w \in W(\overline{G},\overline{T})$. Thus different choices of $\overline{B}$ give rise to the same (and not just isomorphic) subgroups $\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B})$ or $\operatorname{Aut}\ \mathsf{X}(\overline{T})$. For this reason we will write $\mathrm{W}^{\mathrm{ext}}(G,T)$ in place of $\mathrm{W}^{\mathrm{ext}}(G,T,\overline{B})$ from now on.

Lemma 4.3. $\mathrm{W}^{\mathrm{ext}}(G,T) = W(\overline{G},\overline{T}){\cdot}\operatorname{im}\lambda_T$, *where* $\lambda_T\colon \operatorname{Gal}(\bar{k}/k) \to \operatorname{Aut}\ \mathsf{X}(\overline{T})$ *is the usual action of the Galois group on the characters of* T.

Proof. By the definition of $\varphi_{\overline{T},\overline{B}}$, for any $\sigma \in \operatorname{Gal}(\bar{k}/k)$ there exists $w_\sigma \in W(\overline{G},\overline{T})$ such that $\varphi_{\overline{T},\overline{B}}(\sigma) = w_\sigma\, \lambda_T(\sigma)$. □

Corollary 4.4. *Suppose G is a connected reductive k-group, T is a maximal k-torus, and K/k is a field extension such that k is algebraically closed in K. Then* $\mathrm{W}^{\mathrm{ext}}(G,T) = \mathrm{W}^{\mathrm{ext}}(G_K,T_K)$ *as subgroups of* $\mathrm{Aut}\ \mathsf{X}(\overline{T}) = \mathrm{Aut}\ \mathsf{X}(T_{\overline{K}})$.

Proof. By Lemma 4.3, it suffices to show that $\mathrm{im}\,\lambda_T = \mathrm{im}\,\lambda_{T_K}$. Since T splits over $\bar{k}$, the action of the Galois group $\mathrm{Gal}(\overline{K}/K)$ on $\mathsf{X}(\overline{T})$ factors through the natural homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\bar{k}/k)$. By [18, Thm. VI.1.12], this homomorphism is surjective. Thus $\mathrm{im}\,\lambda_T = \mathrm{im}\,\lambda_{T_K}$, as desired. □

Lemma 4.5. *Let T be a maximal k-torus of G and $\overline{B} \supset \overline{T}$ be a Borel subgroup of $\overline{G}$. Then* $\mathrm{W}^{\mathrm{ext}}(G,T)$ *is a semi-direct product:* $\mathrm{W}^{\mathrm{ext}}(G,T) = W(\overline{G},\overline{T}) \rtimes A_{T,\overline{B}}$.

Proof. Since $A_{T,\overline{B}} \subset \mathrm{Aut}\ \mathrm{BRD}(\overline{G},\overline{T},\overline{B})$, every element of $A_{T,\overline{B}}$ preserves the basis Δ of $R(\overline{G},\overline{T})$ corresponding to $\overline{B}$, while in $W(\overline{G},\overline{T})$ only the identity element 1 preserves Δ. Thus $W(\overline{G},\overline{T}) \cap A_{T,\overline{B}} = \{1\}$. By definition $W(\overline{G},\overline{T}) \cdot A_{T,\overline{B}} = \mathrm{W}^{\mathrm{ext}}(G,T)$, and the lemma follows. □

4.2. **The generic torus.** Let T be a maximal k-torus of G and T_{gen} be the generic torus of G. Recall that T_{gen} is defined over the field $K_{\mathrm{gen}} := k(G/N_G(T))$, where $N_G(T)$ denotes the normalizer of T in G. For details of this construction, see [29, §4.2]. For notational simplicity we will write K in place of K_{gen} for the remainder of this section.

Proposition 4.6. *Let G be a connected reductive k-group and T be a maximal k-torus. Then*

(a) *the image $\mathfrak{A}$ of* $\mathrm{Gal}(\overline{K}/K)$ *in* $\mathrm{Aut}\ \mathsf{X}(\overline{T_{\mathrm{gen}}})$ *coincides with* $\mathrm{W}^{\mathrm{ext}}(G_K,T_{\mathrm{gen}})$.
(b) *The character lattice $(\mathfrak{A}, \mathsf{X}(\overline{T_{\mathrm{gen}}}))$ of the generic torus is isomorphic to the character lattice of G.*

If G is semisimple then the proposition is an immediate consequence of a theorem of Voskresenskiĭ's [29, Theorem 4.2.2]; cf. Lemma 4.5.

Proof. (a) We claim that the image of the Galois group $\mathrm{Gal}(\overline{K}/\bar{k}K)$ in $\mathrm{Aut}\ \mathsf{X}(\overline{T_{\mathrm{gen}}})$ coincides with the Weyl group $W(\overline{G_K},\overline{T_{\mathrm{gen}}})$. If G is semisimple this is Theorem 4.2.1 in [29]. In the general case, we consider the derived subgroup $G^{\mathrm{der}} = [G,G]$ of G which is a connected semisimple group. Consider the radical R of G (the identity component of the center). Since G is reductive, R is a k-torus. The generic torus T_{gen} of G and the generic torus $T'_{\mathrm{gen}} \subset G^{\mathrm{der}}_K$ of G^{der} are defined over the same field $K = k(G/N_G(T)) = k(G^{\mathrm{der}}/N_{G^{\mathrm{der}}}(T \cap G^{\mathrm{der}}))$. Note that $T_{\mathrm{gen}} = T'_{\mathrm{gen}} \cdot R_K$ and $T'_{\mathrm{gen}} \cap R_K$ is finite. Hence, there is a canonical isomorphism

$$\mathsf{X}(T_{\mathrm{gen}}) \otimes \mathbb{Q} = \mathsf{X}(T'_{\mathrm{gen}}) \otimes \mathbb{Q} \ \oplus\ \mathsf{X}(R_{\overline{K}}) \otimes \mathbb{Q}\,,$$

where $\mathsf{X}(T_{\mathrm{gen}})$ stands for $\mathsf{X}(\overline{T_{\mathrm{gen}}})$. Let

$$\rho\colon\ \mathrm{Gal}(\overline{K}/\bar{k}K) \to \mathrm{Aut}\ \mathsf{X}(T_{\mathrm{gen}}) \otimes \mathbb{Q},$$
$$\rho'\colon\ \mathrm{Gal}(\overline{K}/\bar{k}K) \to \mathrm{Aut}\ \mathsf{X}(T'_{\mathrm{gen}}) \otimes \mathbb{Q}$$

be the corresponding actions. Since R_K splits over $\bar{k}K$, the Galois group $\mathrm{Gal}(\overline{K}/\bar{k}K)$ acts trivially on $\mathsf{X}(R_{\overline{K}})$. Hence, for every $\sigma \in \mathrm{Gal}(\overline{K}/\bar{k}K)$ we have

$$\rho(\sigma) = (\rho'(\sigma), 1) \in \mathrm{Aut}\ \mathsf{X}(T'_{\mathrm{gen}}) \otimes \mathbb{Q}\ \times\ \mathrm{Aut}\ \mathsf{X}(R_{\overline{K}}) \otimes \mathbb{Q} \subset \mathrm{Aut}\ \mathsf{X}(T_{\mathrm{gen}}) \otimes \mathbb{Q}.$$

By Voskresenskiĭ's theorem [29, Theorem 4.2.1], we have $\mathrm{im}\,\rho' = W(G^{\mathrm{der}}_{\overline{K}}, T'_{\mathrm{gen}})$ and hence

$$\mathrm{im}\,\rho = W(G^{\mathrm{der}}_{\overline{K}}, T'_{\mathrm{gen}}) \times \{1\} = W(G_{\overline{K}}, T_{\mathrm{gen}}).$$

This proves the claim.

Now recall that by Lemma 4.3, $\mathrm{W}^{\mathrm{ext}}(G_K, T_{\mathrm{gen}})$ is generated by $\mathfrak{A}$ and $W(\overline{G_K}, T_{\mathrm{gen}})$. The claim tells us that, in fact, $W(\overline{G_K}, T_{\mathrm{gen}}) \subset \mathfrak{A}$. Hence, $\mathrm{W}^{\mathrm{ext}}(G_K, T_{\mathrm{gen}}) = \mathfrak{A}$.

(b) Consider two maximal tori in G_K, T_{gen} and $T_K = T \times_k K$. By Remark 4.2 the lattices

$$(\mathrm{W}^{\mathrm{ext}}(G_K, T_{\mathrm{gen}}), \mathsf{X}(\overline{T_{\mathrm{gen}}})) \text{ and } (\mathrm{W}^{\mathrm{ext}}(G_K, T_K), \mathsf{X}(\overline{T_K}))$$

are isomorphic. By part (a), the character lattice $(\mathfrak{A}, \mathsf{X}(\overline{T_{\mathrm{gen}}}))$ of the generic torus coincides with $(\mathrm{W}^{\mathrm{ext}}(G_K, T_{\mathrm{gen}}), \mathsf{X}(\overline{T_{\mathrm{gen}}}))$. On the other hand, since the k-variety $G/N_G(T)$ is absolutely irreducible, k is algebraically closed in $K = k(G/N_G(T))$. Thus by Corollary 4.4, $(\mathrm{W}^{\mathrm{ext}}(G_K, T_K), \mathsf{X}(\overline{T_K}))$ coincides with $(\mathrm{W}^{\mathrm{ext}}(G, T), \mathsf{X}(\overline{T}))$, which is the character lattice of G. □

5. Forms of reductive groups

Let G_{spl} be a split connected reductive k-group. Recall that any k-form G of G_{spl} is k-isomorphic to a twisted group ${}_zG_{\mathrm{spl}}$ for some cocycle $z \in Z^1(k, \mathrm{Aut}(\overline{G_{\mathrm{spl}}}))$. Sending z to ${}_zG_{\mathrm{spl}}$ gives rise to a natural bijective correspondence between the non-abelian Galois cohomology set $H^1(k, \mathrm{Aut}(\overline{G_{\mathrm{spl}}}))$ and the isomorphism classes of k-forms of G_{spl}. For details on this, see e.g. [26, §§11.3 and 12.3].

5.1. **Choosing a "small" cocycle.** Let G be a connected reductive k-group, not necessarily split. Let $T \subset G$ be a maximal torus, and let $\overline{B} \supset \overline{T}$ be a Borel subgroup. Let G_{spl} be a split k-form of G. We choose and fix a $\bar{k}$-isomorphism $\theta\colon \overline{G_{\mathrm{spl}}} \to \overline{G}$. Choose a Borel pair $(T_{\mathrm{spl}}, B_{\mathrm{spl}})$ in G_{spl}. After composing θ with an inner automorphism of $\overline{G}$, we may (and shall) assume that θ takes $(\overline{T_{\mathrm{spl}}}, \overline{B_{\mathrm{spl}}})$ to $(\overline{T}, \overline{B})$. Then θ induces isomorphisms $\mathrm{Aut}(\overline{G}) \to \mathrm{Aut}(\overline{G_{\mathrm{spl}}})$, $\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B}) \to \mathrm{BRD}(\overline{G_{\mathrm{spl}}}, \overline{T_{\mathrm{spl}}}, \overline{B_{\mathrm{spl}}}) = \mathrm{BRD}(G_{\mathrm{spl}}, T_{\mathrm{spl}}, B_{\mathrm{spl}})$, etc.

Definition 5.1. Let G, G_{spl} and θ be as above. Let $A_{T,\overline{B}}$ denote the image of $\mathrm{Gal}(\bar{k}/k)$ in $\mathrm{Aut}\,\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B})$, as in Definition 4.1, it is a finite group. Note that θ induces an isomorphism

$$\theta_*\colon\ \mathrm{Aut}\,\mathrm{BRD}(\overline{G}, \overline{T}, \overline{B}) \xrightarrow{\sim} \mathrm{Aut}\,\mathrm{BRD}(G_{\mathrm{spl}}, T_{\mathrm{spl}}, B_{\mathrm{spl}}).$$

Set ${}^\theta A := \theta_*(A_{T,\overline{B}}) \subset \operatorname{Aut}\operatorname{BRD}(G_{\rm spl}, T_{\rm spl}, B_{\rm spl})$. We define $M_G \subset \operatorname{Aut}(G_{\rm spl})$ to be the preimage of the finite group ${}^\theta A$ in $\operatorname{Aut}(G_{\rm spl})$ under

$$\phi\colon\ \operatorname{Aut}(G_{\rm spl}) \to \operatorname{Aut}\operatorname{BRD}(G_{\rm spl}, T_{\rm spl}, B_{\rm spl})\,;$$

see exact sequence (3.1) of Proposition 3.2(b) (for $G_{\rm spl}$). Then M_G is an algebraic group defined over k; see Corollary 3.3. Set

$${}^\theta \mathrm{W}^{\rm ext} := \theta_*(\mathrm{W}^{\rm ext}(G,T)) \subset \operatorname{Aut}\,\mathsf{X}(T_{\rm spl})\,,$$

so that ${}^\theta \mathrm{W}^{\rm ext} = W(G_{\rm spl}, T_{\rm spl}) \cdot {}^\theta A$. Note that the group ${}^\theta \mathrm{W}^{\rm ext}$ acts multiplicatively (i.e., by group automorphisms) on the split k-torus $T_{\rm spl}$.

Proposition 5.2. *With the notation of Definition 5.1, G is isomorphic to ${}_zG_{\rm spl}$ for some cocycle $z \in Z^1(k, M_G)$.*

Proof. For $\sigma \in \operatorname{Gal}(\bar k/k)$ denote by $\beta(\sigma)$ the semi-automorphism of $\overline{G}$ and by $\beta_{\rm spl}(\sigma)$ the semi-automorphism of $\overline{G_{\rm spl}}$ induced by σ. Under the usual correspondence between k-forms of $G_{\rm spl}$ and $H^1(k, \operatorname{Aut}(\overline{G_{\rm spl}}))$, G is k-isomorphic to ${}_zG$, for the cocycle $z(\sigma) := {}^\theta\beta(\sigma) \circ \beta_{\rm spl}(\sigma)^{-1}\colon \overline{G_{\rm spl}} \to \overline{G_{\rm spl}}$, where ${}^\theta\beta(\sigma)$ is the image of $\beta(\sigma)$ under the isomorphism $\operatorname{Aut}(\overline{G}) \xrightarrow{\simeq} \operatorname{Aut}(\overline{G_{\rm spl}})$ induced by θ.

It remains to show that $z(\sigma) \in M_G(\bar k)$, or equivalently, $z_{\rm BRD}(\sigma) := \varphi_{\overline{T_{\rm spl}},\overline{B_{\rm spl}}} \circ z(\sigma)$ lies in ${}^\theta A$, for every $\sigma \in \operatorname{Gal}(\bar k/k)$. Consider the diagram

$$\begin{tikzcd}
 & \operatorname{SAut}(\overline{G}) \arrow[r, "\varphi_{\overline{T},\overline{B}}"] \arrow[d, "\simeq"'] & \operatorname{Aut}\operatorname{BRD}(\overline{G},\overline{T},\overline{B}) \arrow[d, "\simeq"', "\theta_*"] \\
\operatorname{Gal}(\bar k/k) \arrow[ur, hook, "\beta"] \arrow[dr, hook, "\beta_{\rm spl}"'] & & \\
 & \operatorname{SAut}(\overline{G_{\rm spl}}) \arrow[r, "\varphi_{\overline{T_{\rm spl}},\overline{B_{\rm spl}}}"] & \operatorname{Aut}\operatorname{BRD}(\overline{G_{\rm spl}},\overline{T_{\rm spl}},\overline{B_{\rm spl}}),
\end{tikzcd}$$

where the vertical isomorphisms are induced by θ. The commutativity of this diagram tells us that

$$z_{\rm BRD}(\sigma) = \theta_*(\gamma(\sigma)) \circ \gamma_{\rm spl}(\sigma)^{-1},$$

where $\gamma := \varphi_{\overline{T},\overline{B}} \circ \beta$ and $\gamma_{\rm spl} := \varphi_{\overline{T_{\rm spl}},\overline{B_{\rm spl}}} \circ \beta_{\rm spl}$ denote the actions of $\operatorname{Gal}(\bar k/k)$ on $\operatorname{BRD}(\overline{G},\overline{T},\overline{B})$ and on $\operatorname{BRD}(\overline{G_{\rm spl}},\overline{T_{\rm spl}},\overline{B_{\rm spl}}) = \operatorname{BRD}(G_{\rm spl}, T_{\rm spl}, B_{\rm spl})$, respectively. Since the Galois group $\operatorname{Gal}(\bar k/k)$ acts trivially on $\operatorname{BRD}(G_{\rm spl}, T_{\rm spl}, B_{\rm spl})$, we see that $\gamma_{\rm spl}(\sigma) = \mathrm{id}$ and $z_{\rm BRD}(\sigma) = \theta_*(\gamma(\sigma))$. By definition, $\gamma(\sigma) \in A_{T,\overline{B}}$. Thus $z_{\rm BRD}(\sigma) \in\ \theta_*(A_{T,\overline{B}}) = {}^\theta A$, as desired. $\square$

5.2. **Forms of Cayley groups.**

Lemma 5.3. *Let G be a split reductive k-group, M be a closed k-subgroup of* $\operatorname{Aut}(G)$ *containing* $\operatorname{Inn}(G)$*, and $z \in Z^1(k, M)$.*

(a) *If there exists an M-equivariant birational isomorphism $f\colon G \dashrightarrow \mathrm{Lie}(G)$, then ${}_zG$ is a Cayley group.*
(b) *If there exists an M-equivariant birational isomorphism $f\colon G \times_k \mathbb{A}^r \dashrightarrow \mathrm{Lie}(G) \times_k \mathbb{A}^r$ for some $r \geq 0$, where M acts trivially on the affine space $\mathbb{A}^r$, then ${}_zG$ is a stably Cayley group.*
(c) *If G is Cayley, then any inner form of G is also Cayley.*
(d) *If G is stably Cayley, then any inner form of G is also stably Cayley.*

Proof. (a) Since f is M-equivariant, we can twist f by z and obtain an ${}_zM$-equivariant birational isomorphism

$$ {}_zf\colon {}_zG \dashrightarrow {}_z\mathrm{Lie}(G)\,. $$

By functoriality of the twisting operation, ${}_z\mathrm{Inn}(G) = \mathrm{Inn}({}_zG) \subset {}_zM$ ([26, Lemma 16.4.6]) and ${}_z\mathrm{Lie}(G) = \mathrm{Lie}({}_zG)$. Thus ${}_zf$ is an ${}_zM$-equivariant (and, in particular, $\mathrm{Inn}({}_zG)$-equivariant) rational map ${}_zG \dashrightarrow \mathrm{Lie}({}_zG)$. Twisting f^{-1} by z in a similar manner, we see that ${}_zf$ is, in fact, a birational isomorphism, i.e., a Cayley map for ${}_zG$.

(b) Replace G by $G \times \mathbb{G}_m^r$ and apply part (a).

(c) An inner form of G is, by definition, a twisted form ${}_zG$, where $z \in Z^1(k, \mathrm{Inn}(G))$. If G is a Cayley group, then there exists an $\mathrm{Inn}(G)$-equivariant birational isomorphism $f\colon G \dashrightarrow \mathrm{Lie}(G)$, hence by (a), ${}_zG$ is a Cayley group.

(d) If G is a stably Cayley group, then $G \times_k \mathbb{G}_m^r$ is Cayley for some r, and we may identify $\mathrm{Inn}(G)$ with $\mathrm{Inn}(G \times_k \mathbb{G}_m^r)$. If $z \in Z^1(k, \mathrm{Inn}(G)) = Z^1(k, \mathrm{Inn}(G \times_k \mathbb{G}_m^r))$, then by (b), the twisted group ${}_z(G \times_k \mathbb{G}_m^r) = {}_zG \times_k \mathbb{G}_m^r$ is Cayley, hence ${}_zG$ is stably Cayley. $\square$

6. (G, S)-fibrations and (G, S)-varieties

The proof of Theorem 1.3 in the next section relies on the notions of (G, S)-fibration and (G, S)-variety. This section will be devoted to preliminary material on these notions.

6.1. (G, S)**-fibrations.** Let G be a linear algebraic k-group and S be a k-subgroup. Recall that a (G, S)-fibration is a morphism of k-varieties $\pi\colon X \to Y$, where G acts on X on the left, π is constant on G-orbits, and after a surjective étale base change $Y' \to Y$ there is a G-equivariant isomorphism between $G/S \times_k Y'$ and $X \times_Y Y'$ over Y', cf. [9, §2.2]. If $S = \{1\}$, then a (G, S)-fibration is the same thing as a left G-torsor. Note that in general, $X \to Y$ can be both a (G, S_1)-fibration and a (G, S_2)-fibration for non-isomorphic k-subgroups $S_1, S_2 \subset G$. However over an algebraic closure of k, S_1 and S_2 become conjugate.

The following lemma generalizes well-known properties of torsors to the category of (G, S)-fibrations.

Lemma 6.1. *Let $\pi\colon X \to Y$, $\pi_1\colon X_1 \to Y_1$ and $\pi_2\colon X_2 \to Y_2$ be (G, S)-fibrations.*

(a) *Every G-equivariant morphism $f\colon X_1 \to X_2$ is a morphism of (G,S)-fibrations, i.e., gives rise to a Cartesian diagram*

$$\begin{tikzcd} X_1 \arrow[r, "f"] \arrow[d, "\pi_1"'] & X_2 \arrow[d, "\pi_2"] \\ Y_1 \arrow[r, "\overline{f}"] & Y_2 . \end{tikzcd}$$

In other words, $X_1 = X_2 \times_{Y_2} Y_1$, where the G-action on $X_2 \times_{Y_2} Y_1$ is induced by the G-action on X_2.

(b) *Every G-invariant closed (respectively, open) subvariety $X_0 \subset X$ is of the form $\pi^{-1}(Y_0)$ for some closed (respectively, open) subvariety Y_0 of Y. In particular, X_0 is itself the total space of a (G,S)-fibration $\pi_{|X_0}\colon X_0 \to Y_0$.*

(c) *The map f in part (a) is dominant if and only if $\overline{f}$ is dominant.*

Proof. (a) We first define the map $\overline{f}\colon Y_1 \to Y_2$ locally in the étale topology on Y_1. Let $\{U_\alpha\}$ be an étale open cover of Y_1 such that X_1 is G-equivariantly isomorphic to $G/S \times_k U_\alpha$, over each U_α. Then over each U_α, the map π_1 has a section $s_\alpha\colon U_\alpha \to \pi_1^{-1}(U_\alpha)$, and we can define $\overline{f}$ by composing s, f and π_2. The resulting local map is independent of the choice of s; these maps patch up to a k-morphism $\overline{f}\colon Y_1 \to Y_2$ by étale descent.

By the universal property of fibered products there exists a morphism $\phi\colon X_1 \to X_2 \times_{Y_2} Y_1$ over Y_1. This morphism is unique and hence, G-equivariant. Thus it suffices to show that ϕ is an isomorphism. Note that ϕ is a G-equivariant morphism between (G,S)-fibrations over Y_1. We want to show that if $Y_1 = Y_2$ and $\overline{f} = \mathrm{id}$ in the above diagram then f is an isomorphism. We do this by constructing f^{-1}. Let $\{U_\alpha\}$ be an étale local cover of Y_1, trivializing both X_1 and X_2. That is, over each U_α, X_1 and X_2 are both G-equivariantly isomorphic to $G/S \times_k U_\alpha$. Hence, f^{-1} is (uniquely) defined and is G-equivariant over each U_α. Once again, using étale descent, we see that these local inverses patch together to a well-defined G-equivariant k-morphism $f^{-1}\colon X_2 \to X_1$.

(b) Since open subsets are complements of closed subsets, it suffices to consider the case where X_0 is closed. We claim that $\pi(X_0)$ is closed in Y. It is enough to check this claim locally in the étale topology, so we may assume that $X = G/S \times_k Y$ and π is the projection onto the second factor. Since X_0 is G-equivariant, X_0 contains $\{1\} \times_k \pi(X_0)$. Moreover, since X_0 is closed, X_0 contains $\{1\} \times \overline{\pi(X_0)}$. We conclude that $\overline{\pi(X_0)}$ is contained in $\pi(X_0)$, i.e., $\pi(X_0)$ is closed, as claimed.

After replacing Y by $\pi(X_0)$ and X by $\pi^{-1}(\pi(X_0))$, it now suffices to show that if $X_0 \subset X$ is closed and G-invariant and $\pi(X_0) = Y$ then $X_0 = X$. To do this, we construct the inverse to the inclusion map $X_0 \hookrightarrow X$. We first do this étale-locally, where we may assume $X = G/S \times_k Y$ and hence, $X_0 = X$, then use étale descent to patch together local inverses into a morphism $X \to X_0$ defined over Y.

(c) By part (b), the closure of $f(X_1)$ in X_2 is of the form $\pi_2^{-1}(C)$ for some closed subset $C \subset Y_2$. Thus f is dominant if and only if $C = Y_2$, that is, if and only if $\overline{f}$ is dominant. □

Let $N := N_G(S)$ be the normalizer of S in G, $W := N/S$, and $X \to Y$ be a (G,S)-fibration. Note that W is again a linear algebraic group over k. Denote the S-fixed point locus in X by X^S. The G-action on X induces an N-action on X^S. Since S acts trivially on X^S, this N-action descends to a W-action on X^S. By trivializing the (G,S)-fibration $X \to Y$ over an étale cover $Y' \to Y$, we see that $X^S \to Y$ is in fact a W-torsor; see [9, Proposition 2.9]. Conversely, starting with a W-torsor $Z \to Y$, we can build a (G,S)-fibration $X \to Y$ by setting X to be the "homogeneous fiber space" $G \times^N Z$, i.e., the quotient of $G \times_k Z$ by the left N-action given by $n \cdot (g,x) \to (gn^{-1}, nx)$. This quotient can either be constructed locally, in the étale topology on Y, by descent, or globally as a geometric quotient in the sense of geometric invariant theory. For details on these constructions, we refer the reader to [9, §2.2].

Proposition 6.2. *Let Var_k be the category of quasi-projective varieties, and $Fib_{(G,S)}$ be the functor from Var_k to the category of sets which associates to a quasi-projective variety Y the set of isomorphism classes of (G,S)-fibrations over Y, and to a k-morphism of varieties $\tilde{Y} \to Y$ the pull-back morphism which base-changes (G,S)-fibrations over Y to $\tilde{Y}$. If $S = \{1\}$, we will write Tor_G in place of $Fib_{(G,S)}$.*

Then the two constructions described above give rise to an isomorphism between the functors $Fib_{(G,S)}$ and Tor_W.

Proof. See [9, Proposition 2.10]. □

6.2. **(G,S)-varieties.** A k-variety X with a left action of G is called a (G,S)-*variety* if it contains a dense open subset $X' \subset X$ which is the total space of a (G,S)-fibration $X' \to Y$.

Lemma 6.3. *Let G be a reductive k-group, $T \subset G$ a maximal k-torus, and M be an algebraic subgroup of the group k-scheme* $\mathrm{Aut}(G)$ *containing* $\mathrm{Inn}(G)$. *Then G and its Lie algebra* $\mathrm{Lie}(G)$ *are both (M, T^{ad})-varieties.*

In the case where $M = \mathrm{Inn}(G)$, the lemma was proved in [9, Proposition 4.3].

Proof. Being a (G,S)-variety is a geometric notion. That is, suppose k'/k is a field extension. Then X is a (G,S)-variety over k if and only if $X_{k'}$ is a $(G_{k'}, S_{k'})$-variety over k'. Thus, after replacing k by a suitable k', we may assume that G and T are split.

We will only consider the M-action on G; the case of the M-action on $\mathrm{Lie}(G)$ is similar. By Corollary 3.3, $M = \mathrm{Inn}(G) \rtimes A$, where A is a finite group of automorphisms of G and every element of A preserves T.

Our proof will rely on [9, Proposition 2.16]. To apply this proposition we need to check that the M-action on G is stable, i.e., the M-orbit of

$x \in G(\bar{k})$ is closed for x in general position. By [9, Corollary 4.2], the conjugation action of G on itself is stable. Since A is a finite group, the group M contains G^{ad} as a subgroup of finite index, and therefore the M-action on G is also stable.

By [9, Proposition 2.15(i)], we can now conclude that G is an (M, S)-variety for some subgroup $S \subset M$. Moreover, by [9, Proposition 2.16], in order to show that we may take $S = T^{\mathrm{ad}}$, it suffices to exhibit a dense subset $D \subset G(k)$ defined over k such that the stabilizer of every $p \in D$ in M is conjugate to T^{ad}.

In fact, it suffices to construct a dense open subset $U \subset T$ defined over k such that the stabilizer of every $p \in U(k)$ is conjugate to T^{ad}; we can then take D to be the union of $\mathrm{Inn}(G)$-translates of $U(k)$.

Consider the set T^{reg} of regular points of T. By [2, §12.2], T^{reg} is a dense open subset of T defined over k. We claim that for $t \in T^{\mathrm{reg}}$ in general position, $\mathrm{Stab}_M(t) = T^{\mathrm{ad}}$. Indeed, suppose $g \in M$ stabilizes t. Since t lies in a unique maximal torus of G (see [2, Proposition 12.2(4)]), $g(T) = T$. Equivalently, g lies in $N_{G^{\mathrm{ad}}}(T^{\mathrm{ad}}) \rtimes A \subset M$. The latter group acts on T via its finite quotient $W \rtimes A$, and the $W \rtimes A$-action on T is faithful (see the proof of Lemma 4.5). The fixed points of each element of $W \rtimes A$ form a proper closed subvariety of T^{reg}. Removing these closed subvarieties from T^{reg}, we obtain a dense open subset $U \subset T$ such that $\mathrm{Stab}_{W \rtimes A}(t) = \{1\}$ or equivalently, $\mathrm{Stab}_M(t) = T^{\mathrm{ad}}$ for every $t \in U$, as desired. □

Proposition 6.4. *Suppose X_1 and X_2 are (G, S)-varieties such that the fixed point loci X_1^S and X_2^S are irreducible. Set $N := N_G(S)$, $W := N/S$. Then*

(a) *every G-equivariant dominant rational map $\alpha\colon X_1 \dashrightarrow X_2$ restricts to a W-equivariant dominant rational map $\beta\colon X_1^S \dashrightarrow X_2^S$.*

(b) *Every W-equivariant dominant rational map $\beta\colon X_1^S \dashrightarrow X_2^S$ lifts to a unique G-equivariant dominant rational map $\alpha\colon X_1 \dashrightarrow X_2$.*

(c) *Moreover, β is a birational isomorphism if and only if so is α.*

Proof. For $i = 1, 2$ let X_i' be a G-invariant dense open subset of X_i which is the total space of a (G, S)-fibration, $X_i' \to Y_i$. Since each X_i^S is irreducible, the non-empty open subset $(X_i')^S$ is dense in X_i^S. Hence, the dominant rational map $X_1^S \dashrightarrow X_2^S$ restricts to a dominant rational map $(X_1')^S \dashrightarrow (X_2')^S$, and we may, without loss of generality, replace X_i by X_i' and thus assume that X_i is the total space of a (G, S)-fibration $X_i \to Y_i$. Lemma 6.1(b) now tells us that after removing a proper closed subset from Y_1 (and its preimages from X_1 and X_1^S), we may assume that f is regular. By Proposition 6.2, $X_i^S \to Y$ is a W-torsor for $i = 1, 2$. By Lemma 6.1(a), α is a morphism of (G, S)-fibrations, and $\beta = \alpha_{|X_1^S} : X_1^S \to X_2^S$ is a morphism of W-torsors. By Proposition 6.2, $X_i^S \to Y$ is a W-torsor for $i = 1, 2$. We thus obtain the following diagram

$$\begin{tikzcd}
X_1 \arrow[rrr, "\alpha"] \arrow[ddd] & & & X_2 \arrow[ddd] \\
& X_1^S \arrow[r, "\beta"] \arrow[ul, hook] \arrow[ddl] & X_2^S \arrow[ur, hook] \arrow[ddr] & \\
& & & \\
Y_1 \arrow[rrr, "\overline{\alpha}=\overline{\beta}"] & & & Y_2\,.
\end{tikzcd}$$

By Proposition 6.2, α restricts to β and β lifts to α in a unique way. Moreover, α and β induce the same morphism $\overline{\alpha} = \overline{\beta} \colon Y_1 \to Y_2$.

By Lemma 6.1(c), α is dominant if and only if $\overline{\alpha} = \overline{\beta}$ is dominant if and only if β is dominant. This proves (a) and (b).

(c) If α is a birational isomorphism, then restricting α^{-1} to X_1^S, we obtain an inverse for β. Similarly, if β is a birational isomorphism, then extending β^{-1} to $X_2 \dashrightarrow X_1$, we obtain an inverse for α. $\square$

Corollary 6.5. *Let G be a connected reductive k-group and $T \subset G$ be a maximal k-torus. Then G is Cayley if and only if there exists a $W(G,T)$-equivariant birational isomorphism $T \overset{\simeq}{\dashrightarrow} \mathrm{Lie}(T)$ defined over k.*

Note that here, as before, we view the Weyl group $W(G,T)$ as an algebraic group over k.

Proof. By Lemma 6.3, with $M = \mathrm{Inn}(G)$, $X_1 = G$ and $X_2 = \mathrm{Lie}(G)$ are both $(\mathrm{Inn}(G), T^{\mathrm{ad}})$-varieties. The fixed point loci, $X_1^{T^{\mathrm{ad}}} = T$ and $X_2^{T^{\mathrm{ad}}} = \mathrm{Lie}(T)$, are irreducible. The desired conclusion is now a direct consequence of Proposition 6.4: there exists a G-equivariant birational isomorphism

$$\alpha \colon G = X_1 \overset{\simeq}{\dashrightarrow} X_2 = \mathrm{Lie}(G)$$

(i.e., a Cayley map for G) if and only if there exists a $W(T)$-equivariant birational isomorphism $\beta \colon T = X_1^{T^{\mathrm{ad}}} \overset{\simeq}{\dashrightarrow} X_2^{T^{\mathrm{ad}}} = \mathrm{Lie}(T)$. $\square$

7. Proof of Theorem 1.3

(a) $\Longrightarrow$ (b). First suppose G is Cayley over k. Then G_K is Cayley over K for every field extension K/k. Then by Corollary 6.5, every maximal K-torus T of G_K is K-rational.

Now suppose G is stably Cayley over k, i.e., $G \times \mathbb{G}_m^r$ is Cayley for some $r \geq 0$. Then the above argument shows that for every K-torus T of G, $T \times \mathbb{G}_m^r$ is K-rational. Hence, T is stably K-rational, as claimed.

(b) $\Longrightarrow$ (c) is obvious.

(c) $\Longleftrightarrow$ (d). By Proposition 4.6, the character lattice $\mathsf{X}(G)$ of G is isomorphic to the character lattice of the generic torus T_{gen} of G. Since a torus T is stably rational if and only if its character lattice $\mathsf{X}(T)$ is quasi-permutation (see [29, Theorem 4.7.2]), (c) and (d) are equivalent.

(d) $\Longrightarrow$ (a). Let $G_{\rm spl}$ be a split k-form of G. Let $(T_{\rm spl}, B_{\rm spl})$ be a Borel pair in $G_{\rm spl}$ defined over k, T be a maximal k-torus of G, and $\overline{B}$ be a Borel subgroup defined over the algebraic closure $\bar{k}$ and containing $\overline{T}$. We choose and fix an isomorphism $\theta\colon \overline{G_{\rm spl}} \to \overline{G}$ taking $(\overline{T_{\rm spl}}, \overline{B_{\rm spl}})$ to $(\overline{T}, \overline{B})$, and we construct the subgroup $M_G \subset \mathrm{Aut}(G_{\rm spl})$ using θ, as in Subsection 5.1. By Proposition 5.2, G is isomorphic to ${}_zG_{\rm spl}$ for some cocycle $z \in Z^1(k, M_G)$. By Lemma 5.3(b), in order to show that G is stably Cayley, it suffices to construct an M_G-equivariant birational isomorphism

$$G_{\rm spl} \times \mathbb{G}_m^r \overset{\simeq}{\dashrightarrow} \mathrm{Lie}(G_{\rm spl}) \times \mathbb{A}^r \tag{7.1}$$

for some $r \geq 0$, where M_G acts trivially on the split torus $\mathbb{G}_m^r$ and the affine space $\mathbb{A}^r$. By Lemma 6.3, $X_1 := G_{\rm spl} \times \mathbb{G}_m^r$ and $X_2 := \mathrm{Lie}(G_{\rm spl}) \times \mathbb{A}^r$ are both (M_G, S)-varieties, where $S := (T_{\rm spl})^{\rm ad}$. By Proposition 6.4, in order to construct an M_G-equivariant birational isomorphism (7.1), it suffices to construct an $N_{M_G}(S)/S$-equivariant birational isomorphism $X_1^S \dashrightarrow X_2^S$, where $X_1^S = T_{\rm spl} \times \mathbb{G}_m^r$, $X_2^S = \mathrm{Lie}(T_{\rm spl}) \times \mathbb{A}^r$. Note that $N_{M_G}(S)/S$ is isomorphic to the group ${}^\theta\mathrm{W}^{\rm ext} \subset \mathrm{Aut}\,\mathsf{X}(T_{\rm spl})$ (see Subsection 5.1).

It thus remains to show that there exists a ${}^\theta\mathrm{W}^{\rm ext}$-equivariant birational isomorphism

$$T_{\rm spl} \times \mathbb{G}_m^r \overset{\simeq}{\dashrightarrow} \mathrm{Lie}(T_{\rm spl}) \times \mathbb{A}^r \tag{7.2}$$

for some $r \geq 0$. By the definition of ${}^\theta\mathrm{W}^{\rm ext}$, the lattice $({}^\theta\mathrm{W}^{\rm ext}, \mathsf{X}(T_{\rm spl}))$ is isomorphic to the character lattice $(V(G,T), \mathsf{X}(\overline{T}))$ of G. By condition (d) of the theorem, the character lattice of G is quasi-permutation, hence so is the lattice $({}^\theta\mathrm{W}^{\rm ext}, \mathsf{X}(T_{\rm spl}))$. By Lemma 2.4(b), this implies that the ${}^\theta\mathrm{W}^{\rm ext}$-action on the split torus $T_{\rm spl}$ is stably linearizable. In other words, $T_{\rm spl}$ is ${}^\theta\mathrm{W}^{\rm ext}$-equivariantly stably birationally isomorphic to a faithful linear representation V of the finite group ${}^\theta\mathrm{W}^{\rm ext}$. On the other hand, by Remark 2.3, the vector space V is ${}^\theta\mathrm{W}^{\rm ext}$-equivariantly stably birationally isomorphic to $\mathrm{Lie}(T_{\rm spl})$. Composing these two ${}^\theta\mathrm{W}^{\rm ext}$-equivariant birational isomorphisms, we see that $T_{\rm spl}$ and $\mathrm{Lie}(T_{\rm spl})$ are ${}^\theta\mathrm{W}^{\rm ext}$-equivariantly stably birationally isomorphic. In other words, (7.2) holds for a suitable $r \geq 0$, as claimed. This completes the proof of Theorem 1.3. □

Corollary 7.1. *Let k be a field of characteristic* 0. *Then every reductive k-group G of rank ≤ 2 is stably Cayley.*

Proof. By Lemma 2.7 the character lattice of G is quasi-permutation. Thus G is stably Cayley by Theorem 1.3.

Alternatively, the generic torus of G is of dimension ≤ 2 and hence, is rational; see [29, §4.9, Examples 6, 7]. Once again, we conclude that G is stably Cayley by Theorem 1.3. □

8. Proof of Theorem 1.4

To show that (a) $\Longrightarrow$ (b), suppose G is stably Cayley over k. Then $G_{\bar{k}}$ is stably Cayley over $\bar{k}$, where $\bar{k}$ denotes an algebraic closure of k. By [20, Theorem 1.28], $G_{\bar{k}}$ is one of the following groups:

$$\mathbf{SL}_3,\ \mathbf{SO}_n\ (n \neq 2,4),\ \mathbf{Sp}_{2n}\ (n \geq 1),\ \mathbf{PGL}_n\ (n \geq 2),\ \mathbf{G}_2. \tag{8.1}$$

In other words, G is a k-form of one of these groups. (Note that the group $\mathbf{SL}_2$, which appears in the statement of [20, Theorem 1.28], is isomorphic to $\mathbf{Sp}_2$.) If G is an outer form of $\mathbf{PGL}_n$ where $n \geq 4$ is even, then by [13, Theorem 0.1] the generic torus of G is not stably rational, and by Theorem 1.3, G is not stably Cayley. Thus if G is stably Cayley, then G is one of the groups listed in part (b).

It remains to prove that (b) $\Longrightarrow$ (a), i.e., that all groups listed in part (b) are stably Cayley.

The classical Cayley transform shows that all forms of $\mathbf{SO}_n$ and $\mathbf{Sp}_{2n}$ are Cayley; see [20, Example 1.16]. All forms of the groups $\mathbf{SL}_3$ and $\mathbf{G}_2$ are of rank 2, hence their generic tori are rational by [29, Example 4.9.7], and by Theorem 1.3, these groups are stably Cayley. Every inner form of $\mathbf{PGL}_n$ is Cayley by [20, Example 1.11]; cf. also Lemma 5.3(c). Finally, the generic torus of any form of $\mathbf{PGL}_n$ for n odd is rational, hence stably rational by [30, Corollary of Theorem 8]. By Theorem 1.3, we conclude that outer forms of $\mathbf{PGL}_n$ for n odd are stably Cayley. This completes the proof of Theorem 1.4. $\square$

9. Statement of Theorem 9.1 and first reductions

In view of Theorem 1.4 it is natural to ask for a classification of stably Cayley semisimple groups, initially over an algebraically closed field of characteristic zero. This problem turns out to be significantly more complicated; a complete solution is out of reach at the moment; cf. Remark 9.3. Fortunately, for the purpose of proving Theorem 1.5, we can limit our attention to semisimple groups all of whose simple components are of the same type. Theorem 9.1 stated below gives a classification of stably Cayley groups of this form; this theorem will be a key ingredient in our proof of Theorem 1.5 in Section 19. The proof of Theorem 9.1 will occupy much of the remainder of this paper.

Theorem 9.1. *Let k be an algebraically closed field of characteristic* 0 *and G be a semisimple k-group of the form H^m/C, where H is a simple and simply connected k-group and C is a central k-subgroup of H^m. (In other words, the universal cover of G is of the form H^m.) Then G is stably Cayley if and only if G is isomorphic to a direct product $G_1 \times_k \cdots \times_k G_s$, where each G_i is either a stably Cayley simple k-group* (*i.e., is one of the groups listed in* (8.1)) *or* $\mathbf{SO}_4$.

Note that $\mathbf{SO}_4$ is semisimple but not simple. The "if" direction of Theorem 9.1 is obvious, since the direct product of stably Cayley groups is stably

Cayley. (As we mentioned in the previous section, $\mathbf{SO}_4$ is Cayley via the classical Cayley transform.) Thus we only need to prove the "only if" direction. The proof will proceed by case-by-case analysis, depending on the type of H. We begin with the following easy reduction.

Lemma 9.2. *Let H be a simply connected simple group over an algebraically closed field k and C be a central subgroup of H^m for some $m \geq 1$. Let H_i denote the i^{th} factor of H^m, π_i denote the natural projection $H^m \to H_i$, and $C_i := \pi_i(C) \subset Z(H_i)$, where $Z(H_i)$ denotes the center of H_i. Assume H^m/C is stably Cayley. Then*

(a) *H_i/C_i is stably Cayley;*
(b) *H is of type $\mathbf{A}_n$ $(n \geq 1)$, $\mathbf{B}_n$ $(n \geq 2)$, $\mathbf{C}_n$ $(n \geq 3)$, $\mathbf{D}_n$ $(n \geq 4)$, or $\mathbf{G}_2$.*

Proof. Part (a) is a direct consequence of [20, Prop. 4.8]. To prove part (b), note that by [20, Thm. 1.28], H_1/C_1 is of one of the types listed in the statement of the lemma. □

We will now settle two easy cases of Theorem 9.1, where H is of type $\mathbf{C}_n$ $(n \geq 3)$ and $\mathbf{G}_2$.

Proof of Theorem 9.1 *for $H = \mathbf{G}_2$.* Here $Z(H) = \{1\}$, so $C \subset Z(H)^m$ is trivial, and

$$H^m/C = H^m = \mathbf{G}_2 \times_k \cdots \times_k \mathbf{G}_2 \text{ (m times)}$$

is a product of stably Cayley simple groups. □

Proof of Theorem 9.1 *for H of type $\mathbf{C}_n$ $(n \geq 3)$.* Let $H = \mathbf{Sp}_{2n}$ and C be a subgroup of $Z(H)^m = \mu_2^m$. We will show that if H^m/C is stably Cayley, then $C = \{1\}$.

Indeed, if H^m/C is stably Cayley, then, by Lemma 9.2, so is H_i/C_i. Here $H_i = \mathbf{Sp}_{2n}$, and C_i is a central subgroup (either μ_2 or $\{1\}$). On the other hand, by [20, Theorem 1.28], if the group $\mathbf{Sp}_{2n}/C_i$ is stably Cayley for some $n \geq 3$ then $C_i = \{1\}$. Thus C projects trivially to every H_i, which is only possible if $C = \{1\}$. We conclude that

$$H^m/C = H^m = \mathbf{Sp}_{2n} \times_k \cdots \times_k \mathbf{Sp}_{2n} \text{ (m times)}$$

is a product of Cayley simple groups, as desired. □

Remark 9.3. We conjecture that Theorem 9.1 remains true for every semisimple k-group G over an algebraically closed field k of characteristic 0, without any additional assumption on the universal cover of G. That is, a semisimple k-group is stably Cayley, if and only if it is isomorphic to a direct product $G_1 \times_k \cdots \times_k G_s$, where each G_i is either a stably Cayley simple group or $\mathbf{SO}_4$.

10. Quasi-invertible lattices

The proof of the "only if" direction of Theorem 9.1 in the remaining cases, where H is of type $\mathbf{A}_n$, $\mathbf{B}_n$ or $\mathbf{D}_n$, is more involved. In this section, in preparation for this proof, we will describe a general method for showing that certain lattices are not quasi-permutation (and more generally, cannot even be direct summands of quasi-permutation lattices). Our approach is originally due to Voskresenskiĭ. Proposition 10.6 is essentially [28, Theorem 7 and its corollary]; see also [10, Proposition 1(ii)] and [11, Proposition 9.5(ii)]. For the sake of completeness we supply short proofs for Lemmas 10.4 and 10.5 below.

Definition 10.1. A Γ-lattice L is called *quasi-invertible* if it is a direct summand of a quasi-permutation Γ-lattice.

Lemma 10.2 (J.-L. Colliot-Thélène)**.** *A Γ-lattice L is* quasi-invertible *if and only if it fits into a short exact sequence*

$$0 \to L \to P \to I \to 0, \tag{10.1}$$

where P is a permutation Γ-lattice and I is an invertible Γ-lattice, i.e. a direct summand of a permutation Γ-lattice.

Proof. For a Γ-lattice L we have a flasque resolution

$$0 \to L \to P \to F \to 0,$$

where P is a permutation Γ-lattice and F is a flasque Γ-lattice, see [10, § 1] or [21, Ch. 2] for the theory of flasque resolutions. We write $[L]^{\mathrm{fl}}$ for the class of F up to addition of a permutation lattice (note that F is defined up to addition of a permutation lattice). We have $[L \oplus L']^{\mathrm{fl}} = [L]^{\mathrm{fl}} \oplus [L']^{\mathrm{fl}}$. If L is quasi-invertible, then $L \oplus L'$ is quasi-permutation for some L', hence $[L]^{\mathrm{fl}} \oplus [L']^{\mathrm{fl}} = [L \oplus L']^{\mathrm{fl}} = 0$. We see that $[L]^{\mathrm{fl}}$ is invertible, hence L fits into an exact sequence (10.1) with I invertible.

Conversely, if L fits into an exact sequence (10.1) with I invertible, say $I \oplus J = P'$ is permutation, then adding I to (10.1) twice on the left, and then adding J twice on the right, we obtain an exact sequence

$$0 \to L \oplus I \to P \oplus I \oplus J \to I \oplus J \to 0,$$

which shows that L is quasi-invertible. □

Lemma 10.3 (J.-L. Colliot-Thélène)**.** *Let $\Gamma_1 \twoheadrightarrow \Gamma$ be a surjective homomorphism of finite groups, and let L be a Γ-lattice. Then L is quasi-invertible as a Γ_1-lattice if and only if it is quasi-invertible as a Γ-lattice.*

Proof. We argue as in the proof of Lemma 2.2. It suffices to prove "only if". Assume that L is quasi-invertible as a Γ_1-lattice, then by Lemma 10.2, L fits into a short exact sequence (10.1) of Γ_1-lattices, where P is a permutation Γ_1-lattice and I is an invertible Γ_1-lattice. Set $\Gamma_0 = \ker[\Gamma_1 \to \Gamma]$. From (10.1) we obtain the Γ_0-cohomology exact sequence

$$0 \to L \to P^{\Gamma_0} \to I^{\Gamma_0} \to 0$$

(because $L^{\Gamma_0} = L$ and $H^1(\Gamma_0, L) = 0$), which is a short exact sequence of Γ-lattices. It is easy to see that P^{Γ_0} is a permutation Γ-lattice and I^{Γ_0} is an invertible Γ-lattice, hence by Lemma 10.2, L is a quasi-permutation Γ-lattice. □

Suppose (Γ, L) and (Γ', L') are φ-isomorphic for some isomorphism $\varphi\colon \Gamma \to \Gamma'$; for a definition of φ-isomorphism, see the beginning of Section 2. Then clearly L is permutation (respectively, quasi-permutation, respectively, quasi-invertible) if and only if so is L'.

The Tate–Shafarevich group of a Γ-lattice L is defined as

$$Ш^2(\Gamma, L) = \ker\left[H^2(\Gamma, L) \to \prod_{\Gamma_{\rm c}\subset\Gamma} H^2(\Gamma_{\rm c}, L)\right],$$

where $\Gamma_{\rm c}$ runs over the set of all *cyclic* subgroups of Γ. If L is a quasi-invertible Γ-lattice, then for any subgroup $\Gamma' \subset \Gamma$ we have $Ш^2(\Gamma', L) = 0$, cf. [21, Prop. 2.9.2(a)]. Note however, that there exist Γ-lattices L such that $Ш^2(\Gamma', L) = 0$ for every subgroup Γ' of Γ but L is not quasi-invertible; see the end of the proof of Prop. 12.4.

The following lemmas can be used to show that a given lattice is not quasi-invertible. Let Γ be a finite group. Consider the norm homomorphism

$$N_\Gamma\colon \mathbb{Z} \to \mathbb{Z}[\Gamma], \quad N_\Gamma(a) = a\sum_{s\in\Gamma} s \text{ for } a \in \mathbb{Z},$$

and the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[\Gamma] \to J_\Gamma \to 0, \tag{10.2}$$

where $J_\Gamma = \operatorname{coker} N_\Gamma$.

Lemma 10.4. *Let Γ be a finite group, and $\Gamma' \subset \Gamma$ any subgroup. Then $Ш^2(\Gamma', J_\Gamma) \cong H^3(\Gamma', \mathbb{Z})$.*

Proof. From (10.2) we obtain a cohomology exact sequence

$$H^2(\Gamma', \mathbb{Z}[\Gamma]) \to H^2(\Gamma', J_\Gamma) \to H^3(\Gamma', \mathbb{Z}) \to H^3(\Gamma', \mathbb{Z}[\Gamma]). \tag{10.3}$$

We have $H^i(\Gamma', \mathbb{Z}[\Gamma']) = 0$ for $i \geq 1$, hence $H^i(\Gamma', \mathbb{Z}[\Gamma]) = 0$ for $i \geq 1$, and we see from (10.3) that $H^2(\Gamma', J_\Gamma) \cong H^3(\Gamma', \mathbb{Z})$.

Now let $\Gamma_{\rm c} \subset \Gamma'$ be a *cyclic* subgroup. We have $H^2(\Gamma_{\rm c}, J_\Gamma) \cong H^3(\Gamma_{\rm c}, \mathbb{Z})$. By periodicity for cyclic groups, cf. [1, IV.8, Thm. 5], we have

$$H^3(\Gamma_{\rm c}, \mathbb{Z}) \cong H^1(\Gamma_{\rm c}, \mathbb{Z}) = \operatorname{Hom}(\Gamma_{\rm c}, \mathbb{Z}) = 0.$$

Thus $H^2(\Gamma_{\rm c}, J_\Gamma) = 0$ and consequently, $Ш^2(\Gamma', J_\Gamma) = H^2(\Gamma', J_\Gamma) \cong H^3(\Gamma', \mathbb{Z})$. □

Lemma 10.5. *Let $\Gamma = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, where p is a prime. Then $H^3(\Gamma, \mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. For any group Γ, the group $H^3(\Gamma,\mathbb{Z})$ is canonically isomorphic to $H^2(\Gamma,\mathbb{C}^\times)$. The latter group is called the *Schur multiplier* of Γ. For finite abelian groups, the Schur multipliers were computed by Schur in [23, §4, VIII]. In particular, by [23, §4, VIII], the Schur multiplier of $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order p, which proves the lemma.

An alternative proof based on modern references proceeds as follows. For any finite group Γ, the group $H^3(\Gamma,\mathbb{Z})$ is dual to $H^{-3}(\Gamma,\mathbb{Z})$, cf. [7, Thm. XII.6.6] or [6, Thm. VI.7.4]. By definition $H^{-3}(\Gamma,\mathbb{Z}) = H_2(\Gamma,\mathbb{Z})$. For an *abelian* group Γ we have $H_2(\Gamma,\mathbb{Z}) = \Lambda^2(\Gamma)$ (the second exterior power of the $\mathbb{Z}$-module Γ), see [22, Thm. 3] or [6, Thm. V.6.4(c)]. Clearly $\Lambda^2(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})\cong\mathbb{Z}/p\mathbb{Z}$, hence $H_2(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z},\mathbb{Z})\cong\mathbb{Z}/p\mathbb{Z}$ and $H^3(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z},\mathbb{Z})\cong\mathbb{Z}/p\mathbb{Z}$. □

As an immediate consequence, we obtain the following

Proposition 10.6. *Let $\Gamma = \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$, where p is a prime. Then $Ш^2(\Gamma, J_\Gamma)\cong\mathbb{Z}/p\mathbb{Z}$, and therefore the Γ-lattice J_Γ is not quasi-invertible.* □

The following example and subsequent proposition will be used in the proof of Theorem 1.5 in Section 19.

Example 10.7. Let H be an outer k-form of $\mathbf{PGL}_n$ for some even integer $n\geq 4$. Recall (see Section 8) that by [13, Theorem 0.1] the character lattice of H is not quasi-permutation. In fact, it is shown in [13, §5.1] that the character lattice of H is not quasi-invertible. Indeed, let T be a maximal k-torus of H. Note that $\mathrm{W}^{\mathrm{ext}}(H,T) = \mathrm{S}_n\times\mathbb{Z}/2\mathbb{Z}$ and $X(\overline{T}) = \mathbb{Z}\mathbf{A}_{2n-1}$ on which $\mathrm{W}^{\mathrm{ext}}(H,T)$ acts by permutations and sign changes. It is shown in [13, §5.1] that there exists a subgroup Γ of $\mathrm{W}^{\mathrm{ext}}(H,T)$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, and a direct summand M of the Γ-lattice $\mathsf{X}(\overline{T})$ isomorphic to J_Γ. Then $Ш^2(\Gamma, M)\neq 0$ and so $Ш^2(\Gamma, X(\overline{T}))\neq 0$. This implies that the $\mathrm{W}^{\mathrm{ext}}(H,T)$-lattice $X(\overline{T})$ is not quasi-invertible.

Proposition 10.8. *Let k be a field of characteristic zero and H be a reductive algebraic k-group with maximal k-torus T such that the character lattice $\mathsf{X}(H) = (\mathrm{W}^{\mathrm{ext}}(H,T),\mathsf{X}(\overline{T}))$ is not quasi-invertible. Then $G := H\times H'$ is not stably Cayley for any reductive algebraic k-group H'.*

Proof. Let T, T' and $S = T\times T'$ be maximal k-tori in H, H' and G, respectively. By Theorem 1.3, it suffices to show that the character lattice $\mathsf{X}(G) = (\mathrm{W}^{\mathrm{ext}}(G,S),\mathsf{X}(\overline{S}))$ is not quasi-invertible (and hence, not quasi-permutation). By Lemma 4.3, the extended Weyl group $\mathrm{W}^{\mathrm{ext}}(G,S)$ is generated by the Weyl group $W(G,S) = W(H,T)\times W(H',T')$ and the image of the natural action $\lambda_S\colon \mathrm{Gal}(\bar{k}/k)\to\mathrm{Aut}(\mathsf{X}(\overline{S}))$. Since both T and T' are defined over k, the image of λ_S preserves the direct sum decomposition

$$\mathsf{X}(\overline{S}) = \mathsf{X}(\overline{T})\oplus\mathsf{X}(\overline{T}')$$

and hence, so does $\mathrm{W}^{\mathrm{ext}}(G,S)$. Moreover, $\mathrm{W}^{\mathrm{ext}}(G,S)$ acts on $\mathsf{X}(\overline{T})$ via a surjection $\pi\colon \mathrm{W}^{\mathrm{ext}}(G,S)\to \mathrm{W}^{\mathrm{ext}}(H,T)$. By Lemma 10.3, $\mathsf{X}(\overline{T})$ is not quasi-invertible as a $\mathrm{W}^{\mathrm{ext}}(G,S)$ lattice and, since $\mathsf{X}(\overline{T})$ is a direct summand of $\mathsf{X}(\overline{S})$, we conclude that that $\mathsf{X}(\overline{S})$ is not quasi-invertible as a $\mathrm{W}^{\mathrm{ext}}(G,S)$-lattice. In other words, the character lattice $\mathsf{X}(G) = (\mathrm{W}^{\mathrm{ext}}(G,S), \mathsf{X}(\overline{S}))$ is not quasi-invertible, and therefore G is not stably Cayley, as desired. $\square$

11. A family of non-quasi-invertible lattices

We will now use the results of Section 10 to exhibit a large family of non-quasi-invertible lattices (i.e., lattices that are not direct summands of quasi-permutation lattices). These lattices will be used to complete the proof of Theorem 9.1.

Let Δ be a Dynkin diagram, $\Delta = \bigcup_{i=1}^m \Delta_i$, where Δ_i are the connected components of Δ. We assume that each Δ_i is of type $\mathbf{B}_{l_i}$ ($l_i \geq 1$) or of type $\mathbf{D}_{l_i}$ ($l_i \geq 3$). Note that $\mathbf{B}_1 = \mathbf{A}_1$ and $\mathbf{D}_3 = \mathbf{A}_3$ are allowed. The root system $R(\Delta_i)$ can be realized in a standard way in the space $V_i := \mathbb{Q}^{l_i}$ with standard basis $(\varepsilon_s)_{s\in S_i}$, where S_i is an index set consisting of l_i elements, see [5, Planches II, IV].

Let $S = \dot{\bigcup} S_i$ (disjoint union). Consider the vector space $V := \bigoplus_i V_i$ over $\mathbb{Q}$ with standard basis $(\varepsilon_s)_{s\in S}$. Set

$$\beta = \frac{1}{2}\sum_{s\in S} \varepsilon_s\,. \tag{11.1}$$

We denote by M the additive subgroup in V generated by β and by the basis elements ε_s for all $s\in S$. In other words, M is generated by the vectors of the form $\frac{1}{2}\sum_{s\in S} \pm\varepsilon_s$.

Denote the Weyl group $W(\Delta_i)$ by W_i and the Weyl group $W(\Delta) = \prod_{i=1}^m W_i$ by W. Consider the natural action of W on M. For $s\in S_i$ let c_s denote the automorphism of V_i acting as -1 on ε_s and as 1 on all the other ε_t ($t\in S_i,\ t\neq s$). The Weyl group $W_i = W(\Delta_i)$ is the semidirect product of the symmetric group S_{l_i}, acting by permutations of the basis vectors ε_s, and an abelian group Θ_i. If $\Delta_i \cong \mathbf{B}_{l_i}$, then $\Theta_i = \langle c_s\rangle_{s\in S_i}$, in particular $c_s\in W_i$. If $\Delta_i\cong \mathbf{D}_{l_i}$, then $\Theta_i = \langle c_s c_{s'}\rangle_{s,s'\in S_i}$. In this case $c_s\notin W_i$, but $c_sc_{s'}\in W_i$.

Proposition 11.1. *Let Δ, S, M, and W be as above. Assume that $|\Delta|\geq 3$. Then the W-lattice M is not quasi-invertible.*

Remark 11.2. Note that $\operatorname{rank}(M) = \dim(V) = |\Delta|$. If $|\Delta| = 1$ or 2 then M is quasi-permutation by Lemma 2.7.

Proof. First we consider the case $\Delta\cong \mathbf{D}_4$. Then M is not quasi-permutation, see [13, §7.1]. We will show that M is not quasi-invertible. Indeed, in [13, §7.1] the authors construct a subgroup $U\subset W$ of order 8[1], such that M restricted to U is a direct sum of U-sublattices $M = M_1\oplus M_3$ of ranks 1 and

[1]This group of order 8 is actually denoted by W_2 in [13]. We use the symbol U here to avoid a notational clash with the Weyl group $W_2 := W(\Delta_2)$.

3, respectively. Now in [17, Theorem 1] it is *stated* that the U-lattice M_3 is not quasi-permutation, but it is actually *proved* that $[M_3]^{\mathrm{fl}}$ is not invertible. Hence M_3 is not a quasi-invertible U-lattice, and M is not a quasi-invertible W-lattice.

From now on we will assume that $\Delta \ncong \mathbf{D}_4$. Let $\Gamma = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{e, \gamma_1, \gamma_2, \gamma_3\}$. Then by Proposition 10.6, $Ш^2(\Gamma, J_\Gamma) \cong \mathbb{Z}/2\mathbb{Z}$. The idea of our proof is to construct an embedding

$$\iota \colon \Gamma \to W \tag{11.2}$$

in such a way that M, restricted to $\iota(\Gamma)$, is isomorphic to a direct sum of a submodule $M_0 \simeq J_\Gamma$ and $|S| - 3$ Γ-lattices of rank 1. This will imply that

$$Ш^2(\Gamma, M) = Ш^2(\Gamma, M_0) = Ш^2(\Gamma, J_\Gamma) = \mathbb{Z}/2\mathbb{Z} \neq 0,$$

and hence M is not quasi-invertible. We will now fill in the details of this argument in two steps.

Step 1. Construction of the embedding (11.2)**.** We begin by partitioning each S_i for $i = 1, \ldots, m$ into three (non-overlapping) subsets $S_{i,1}$, $S_{i,2}$ and $S_{i,3}$, subject to the requirement that

$$|S_{i,1}| \equiv |S_{i,2}| \equiv |S_{i,3}| \equiv l_i \pmod 2, \text{ if } \Delta_i \text{ is of type } \mathbf{D}_{l_i}. \tag{11.3}$$

We then set U_1 to be the union of the $S_{i,1}$, U_2 to be the union of the $S_{i,2}$, and U_3 to be the union of the $S_{i,3}$, as i ranges from 1 to m.

Lemma 11.3. *If $|S| \geq 3$ and $\Delta \ncong \mathbf{D}_4$ then the subsets $S_{i,1}$, $S_{i,2}$ and $S_{i,3}$ of S_i can be chosen, subject to* (11.3)*, so that $U_1, U_2, U_3 \neq \emptyset$.*

To prove the lemma, note that if one of the Δ_i, say Δ_1, is of type $\mathbf{D}_l$, where $l \geq 3$ is odd, then we partition S_1 into three non-empty sets of odd order. If $m \geq 2$ then we partition S_i with $i \geq 2$ as follows:

$$S_{i,1} = S_{i,2} = \emptyset \text{ and } S_{i,3} = S_i. \tag{11.4}$$

Clearly $U_1, U_2, U_3 \neq \emptyset$, as desired.

Similarly, if one of the Δ_i, say Δ_1, is $\mathbf{D}_l$, where $l \geq 6$ is even, then we partition S_1 into three non-empty sets of even order, and partition the other S_i (if any) as in (11.4) for $i \geq 2$. Once again, $U_1, U_2, U_3 \neq \emptyset$.

If one of the Δ_i, say Δ_1, is of type $\mathbf{D}_4$, then by our assumption $m \geq 2$. We can now partition S_1 so that each of $S_{1,1}$ and $S_{1,2}$ has 2 elements and $S_{1,3} = \emptyset$, and partition S_i as in (11.4) for every $i \geq 2$. Once again, $U_1, U_2, U_3 \neq \emptyset$.

Thus we may assume without loss of generality that every Δ_i is of type $\mathbf{B}_{l_i}$. In this case condition (11.3) doesn't come into play and the lemma is obvious. This completes the proof of Lemma 11.3. □

We now define the embedding ι of (11.2) by

$$\iota(\gamma_\varkappa) = \prod_{s \in S \smallsetminus U_\varkappa} c_s \in \mathrm{Aut}(M) \text{ for } \varkappa = 1, 2, 3.$$

Recall that $\Gamma = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{e, \gamma_1, \gamma_2, \gamma_3\}$. One easily checks that the map $\iota\colon \Gamma \to \mathrm{Aut}(M)$ defined this way is a group homomorphism. By (11.3), its image is, in fact, in W. Moreover, since $U_\varkappa \neq \emptyset$ for all $\varkappa = 1, 2, 3$, we have $S \smallsetminus U_\varkappa \neq \emptyset$, hence $\iota(\gamma_\varkappa) \neq \mathrm{id}$, i.e., $\iota\colon \Gamma \to W$ is injective. We identify Γ with $\iota(\Gamma) \subset W$.

Step 2. Construction of the submodule M_0. Now let

$$\beta_\varkappa := \gamma_\varkappa(\beta) = \frac{1}{2}\left(\sum_{s\in U_\varkappa} \varepsilon_s - \sum_{s\in S\smallsetminus U_\varkappa} \varepsilon_s\right)$$

for $\varkappa = 1, 2, 3$, where β is as in (11.1). Since the set $\beta, \beta_1, \beta_2, \beta_3$ is the orbit of β under Γ, the sublattice $M_0 := \mathrm{Span}_{\mathbb{Z}}(\beta, \beta_1, \beta_2, \beta_3) \subset M$ is Γ-invariant. Note that

$$\beta + \beta_\varkappa = \sum_{s\in U_\varkappa} \varepsilon_s \,. \tag{11.5}$$

Since U_1, U_2 and U_3 are non-empty and disjoint, $\beta + \beta_1$, $\beta + \beta_2$, and $\beta + \beta_3$ are linearly independent. On the other hand,

$$\beta + \beta_1 + \beta_2 + \beta_3 = 0.$$

Therefore, the Γ-invariant sublattice $M_0 \subset M$ is of rank 3 and is isomorphic (as a Γ-lattice) to $J_\Gamma := \mathbb{Z}[\Gamma]/\mathbb{Z}$.

It remains to show that M can be written as a direct sum of M_0 and Γ-lattices of rank 1. Indeed, for each $\varkappa = 1, 2, 3$ choose an element $u_\varkappa \in U_\varkappa$ and set $U'_\varkappa = U_\varkappa \smallsetminus \{u_\varkappa\}$. (Note that $U'_\varkappa$ may be empty for some $\varkappa$). We set $S' = U'_1 \cup U'_2 \cup U'_3$. It follows from (11.5) that the abelian group generated by the ε_s, as s ranges over S', together with $\beta, \beta_1, \beta_2, \beta_3$, contains both β and ε_s for every $s \in S$ and hence, coincides with M. Since $\mathrm{rank}(M) = |S|$, we conclude that the set $\{\beta, \beta_1, \beta_2\} \cup \{\varepsilon_s \mid s \in S'\}$ is a basis of M. The group Γ acts on ε_s by ± 1. We see that the Γ-lattice M is a direct sum of $M_0 = \mathrm{Span}_{\mathbb{Z}}(\beta, \beta_1, \beta_2)$ and the Γ-lattices $\mathbb{Z}e_s$ of rank 1, as s ranges over S'. Thus

$$Ш^2(\Gamma, M) = Ш^2(\Gamma, M_0) = Ш^2(\Gamma, J_\Gamma) = \mathbb{Z}/2\mathbb{Z},$$

and therefore M is not a quasi-invertible W-lattice, as desired. □

12. More non-quasi-invertible lattices

In this section we continue to create a stock of non-quasi-invertible lattices which will be used in the proof of Theorem 9.1.

Proposition 12.1. *Let $M = \{(a_1, a_2, a_3) \in \mathbb{Z}^3 \mid a_1 + a_2 + a_3 \equiv 0 \pmod 2\}$ be the $W := (\mathbb{Z}/2\mathbb{Z})^3$-lattice with the action of $(\mathbb{Z}/2\mathbb{Z})^3$ on $M \subset \mathbb{Z}^3$ coming from the non-trivial action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}$. Then M is not quasi-invertible.*

Proof. Let $\varepsilon_1, \varepsilon_2, \varepsilon_3$ be the standard basis of $\mathbb{Z}^3$. For $i = 1, 2, 3$ let $c_i \in W$ denote the automorphism of M taking ε_i to $-\varepsilon_i$ and taking each of the other two ε_j to itself. Set $\sigma = c_2c_3$, $\tau = c_1c_2$, $\rho = c_1c_2c_3$. We consider the following basis of M:

$$e_1 = \varepsilon_2 - \varepsilon_1,\ e_2 = \varepsilon_2 - \varepsilon_3,\ e_3 = -\varepsilon_1 - \varepsilon_3.$$

A direct calculation shows that in this new basis $\{e_1, e_2, e_3\}$, the generators σ, τ, ρ of W are given by the following matrices:

$$\sigma = \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{pmatrix},\ \tau = \begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},\ \rho = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

By [17, Theorem 1, case W_2], our W-lattice M is not quasi-permutation. Moreover, the pair (W, M) is isomorphic to (U, M_3), where M_3 is the non-quasi-invertible U-lattice we mentioned at the beginning of the proof of Proposition 11.1. Therefore, M is not quasi-invertible. □

Let $\mathbb{Z}\mathbf{D}_3$ denote the root lattice of $\mathbf{D}_3$. Recall that

$$\mathbb{Z}\mathbf{D}_3 = \{a_1\varepsilon_1 + a_2\varepsilon_2 + a_3\varepsilon_3 \mid a_i \in \mathbb{Z},\ a_1 + a_2 + a_3 \in 2\mathbb{Z}\} \subset \mathbb{Q}^3,$$

where $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ is the standard basis of $\mathbb{Q}^3 = \mathbb{Q}\mathbf{D}_3$. The set

$$\{\varepsilon_1 + \varepsilon_2, \quad \varepsilon_1 - \varepsilon_2, \quad \varepsilon_2 - \varepsilon_3\}$$

is a basis of $\mathbb{Z}\mathbf{D}_3$.

Let $m \geq 2$. We consider $(\mathbb{Z}\mathbf{D}_3)^m \subset (\mathbb{Q}\mathbf{D}_3)^m$. Let $L \subset (\mathbb{Q}\mathbf{D}_3)^m$ be the lattice generated by $(\mathbb{Z}\mathbf{D}_3)^m$ and the vector

$$v_e := \varepsilon_1 + \varepsilon_4 + \varepsilon_7 + \dots + \varepsilon_{3m-2}.$$

The group $W(\mathbf{D}_3)^m$ acts on L.

Proposition 12.2. *For $m \geq 2$, the $W(\mathbf{D}_3)^m$-lattice L constructed above is not quasi-invertible.*

Proof. We consider the subgroup $\Gamma \subset W(\mathbf{D}_3)^m$ of order 4 generated by the following two commuting elements of order 2:

$$\begin{aligned} a =& (12)\ c_4c_5\ c_7c_8\ \dots\ c_{3m-2}c_{3m-1}, \\ b =& c_1c_2\ (45). \end{aligned}$$

Here c_i takes ε_i to $-\varepsilon_i$. Thus $\Gamma = \{e, a, b, ab\} \subset W(\mathbf{D}_3)^m$. We show that $Ш^2(\Gamma, L) = \mathbb{Z}/2\mathbb{Z}$.

Indeed, let $V = (\mathbb{Q}\mathbf{D}_3)^m$ with the basis $\varepsilon_1, \dots, \varepsilon_{3m}$. Let V_0 be the subspace of V spanned by

$$\varepsilon_1, \varepsilon_2,\ \varepsilon_4, \varepsilon_5,\ \dots, \varepsilon_{3m-2}, \varepsilon_{3m-1}.$$

It is Γ-invariant. Set $L_0 = L \cap V_0$. Clearly L/L_0 injects into V/V_0. Since Γ acts trivially on V/V_0, we see that $L/L_0 \cong \mathbb{Z}^m$ with trivial Γ-action. Thus we have a short exact sequence of Γ-lattices

$$0 \to L_0 \to L \to \mathbb{Z}^m \to 0.$$

Since $\mathbb{Z}^m$ is a permutation Γ-lattice, we see that

$$Ш^2(\Gamma, L) \cong Ш^2(\Gamma, L_0).$$

We prove that $Ш^2(\Gamma, L_0) = \mathbb{Z}/2\mathbb{Z}$.

For $\gamma \in \Gamma$ we set $v_\gamma = \gamma \cdot v_e$. If $m > 2$ we set

$$\delta = \varepsilon_7 + \varepsilon_{10} + \cdots + \varepsilon_{3m-2}.$$

If $m = 2$ we set $\delta = 0$. We obtain

$$\begin{aligned} v_e &= \varepsilon_1 + \varepsilon_4 + \delta,\\ v_a &= \varepsilon_2 - \varepsilon_4 - \delta,\\ v_b &= -\varepsilon_1 + \varepsilon_5 + \delta,\\ v_{ab} &= -\varepsilon_2 - \varepsilon_5 - \delta. \end{aligned}$$

Clearly

$$v_e + v_a + v_b + v_{ab} = 0.$$

Set $M_0 = \langle v_e, v_a, v_b, v_{ab}\rangle$, then $M_0 \cong J_\Gamma := \mathbb{Z}[\Gamma]/\mathbb{Z}$, and by Proposition 10.6 we have $Ш^2(\Gamma, M_0) = \mathbb{Z}/2\mathbb{Z}$.

Set $\beta_1 = v_e,\ \beta_2 = v_a,\ \beta_3 = v_b$. We set

$$\begin{aligned} \beta_4 &= \varepsilon_4 - \varepsilon_5,\\ \beta_5 &= \varepsilon_7 + \varepsilon_8,\\ \beta_6 &= \varepsilon_7 - \varepsilon_8,\\ &\cdots\cdots\cdots\cdots\\ \beta_{2m-1} &= \varepsilon_{3m-2} + \varepsilon_{3m-1},\\ \beta_{2m} &= \varepsilon_{3m-2} - \varepsilon_{3m-1}. \end{aligned}$$

By Lemma 12.3 below, the set $\boldsymbol{\beta} := \{\beta_1, \ldots, \beta_{2m}\}$ is a basis of L_0. We have $M_0 = \langle \beta_1, \beta_2, \beta_3\rangle$. Our Γ-lattice L_0 decomposes into a direct sum of Γ-sublattices

$$L_0 = M_0 \oplus \langle\beta_4\rangle \oplus \cdots \oplus \langle\beta_{2m}\rangle.$$

For $4 \le i \le 2m$ the Γ-lattice $\langle\beta_i\rangle$ is of rank 1, hence quasi-permutation, and therefore $Ш^2(\Gamma, \langle\beta_i\rangle) = 0$. It follows that $Ш^2(\Gamma, L_0) = Ш^2(\Gamma, M_0) = \mathbb{Z}/2\mathbb{Z}$, hence $Ш^2(\Gamma, L) = \mathbb{Z}/2\mathbb{Z}$. Thus L is not a quasi-invertible $W(\mathbf{D}_3)^m$-lattice. □

Lemma 12.3. *The set $\boldsymbol{\beta} := \{\beta_1, \ldots, \beta_{2m}\}$ is a basis of L_0.*

Proof. First note that $\boldsymbol{\beta} \subset L_0$. Since the set $\boldsymbol{\beta}$ has $2m$ elements and the lattice L_0 is of rank $2m$, it suffices to show that $\boldsymbol{\beta}$ generates L_0.

Recall that $L_0 = L \cap V_0$ and that L is generated by $(\mathbb{Z}\mathbf{D}_3)^m$ and v_e. Since $v_e \in V_0$, we see that L_0 is generated by v_e and $(\mathbb{Z}\mathbf{D}_3)^m \cap V_0$. Since $v_e = \beta_1 \in \boldsymbol{\beta}$, it suffices to prove that $(\mathbb{Z}\mathbf{D}_3)^m \cap V_0 \subset \langle\boldsymbol{\beta}\rangle$. Clearly $(\mathbb{Z}\mathbf{D}_3)^m \cap V_0$ is generated by the vectors

$$\varepsilon_1 + \varepsilon_2\ , \varepsilon_1 - \varepsilon_2,\ \varepsilon_4 + \varepsilon_5,\ \varepsilon_4 - \varepsilon_5,\ \ldots,\ \varepsilon_{3m-2} + \varepsilon_{3m-1},\ \varepsilon_{3m-2} - \varepsilon_{3m-1}.$$

Note that all the vectors in this list starting with $\varepsilon_4-\varepsilon_5$ are clearly contained in $\boldsymbol{\beta}$. It remains to show that the vectors $\varepsilon_1+\varepsilon_2$, $\varepsilon_1-\varepsilon_2$, $\varepsilon_4+\varepsilon_5$ are contained in $\langle\boldsymbol{\beta}\rangle$.

Note that $2\delta \in \langle\boldsymbol{\beta}\rangle$ (because $2\varepsilon_7 \in \langle\boldsymbol{\beta}\rangle, \dots, 2\varepsilon_{3m-2} \in \langle\boldsymbol{\beta}\rangle$). We have

$$\beta_1 + \beta_2 = v_e + v_a = \varepsilon_1 + \varepsilon_2,$$

hence $\varepsilon_1 + \varepsilon_2 \in \langle\boldsymbol{\beta}\rangle$. We have

$$\beta_1 + \beta_3 = v_e + v_b = \varepsilon_4 + \varepsilon_5 + 2\delta,$$

hence $\varepsilon_4 + \varepsilon_5 \in \langle\boldsymbol{\beta}\rangle$. Since also $\varepsilon_4 - \varepsilon_5 \in \boldsymbol{\beta} \subset \langle\boldsymbol{\beta}\rangle$, we see that $2\varepsilon_4 \in \langle\boldsymbol{\beta}\rangle$. We have

$$\beta_1 - \beta_2 = v_e - v_a = \varepsilon_1 - \varepsilon_2 + 2\varepsilon_4 + 2\delta,$$

hence $\varepsilon_1-\varepsilon_2 \in \langle\boldsymbol{\beta}\rangle$. We conclude that $(\mathbb{Z}\mathbf{D}_3)^m \cap V_0 \subset \langle\boldsymbol{\beta}\rangle$, hence $\boldsymbol{\beta}$ generates L_0 and is a basis of L_0. This completes the proofs of Lemma 12.3 and of Proposition 12.2. □

We will now consider the root system $\mathbf{A}_{n-1}$, which is embedded in $\mathbb{Z}^n$, see [5, Planche I]. Let $\mathbb{Z}\mathbf{A}_{n-1}$ denote the root lattice of $\mathbf{A}_{n-1}$, and let $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ denote the standard basis of the root system $\mathbf{A}_{n-1}$ and of $\mathbb{Z}\mathbf{A}_{n-1}$ (*loc. cit*). Let Λ_n denote the weight lattice of $\mathbf{A}_{n-1}$, and let $\omega_1, \omega_2, \dots, \omega_{n-1}$ denote the standard basis of Λ_n consisting of fundamental weights (*loc. cit*).

Consider $\mathbb{Z}\mathbf{A}_2 \subset \Lambda_3$. The nontrivial automorphism σ of the basis $\Delta = \{\alpha_1, \alpha_2\} = \{\varepsilon_1-\varepsilon_2, \varepsilon_2-\varepsilon_3\}$ (*loc. cit*) induces the automorphism $(-1)\circ(1,3)$ of $\mathbb{Z}\mathbf{A}_2$ (where $-1 \in \operatorname{Aut}\mathbb{Z} \subset \operatorname{Aut}\mathbb{Z}^3$, $(1,3) \in \mathrm{S}_3 \subset \operatorname{Aut}\mathbb{Z}^3$), and an automorphism σ_* of $\mathrm{S}_3 = W(\mathbf{A}_2)$ (namely, the conjugation by the transposition $(1,3)$).

Let $m \geq 2$. We consider $(\mathbb{Z}\mathbf{A}_2)^m \subset (\Lambda_3)^m$. Let $(\mathbb{Z}\mathbf{A}_2)^{(i)} \subset \Lambda_3^{(i)}$ be the i^{th} factor. Let $\omega_1^{(i)}, \omega_2^{(i)}$ be the basis of $\Lambda_3^{(i)}$ consisting of fundamental weights.

Let $\mathbf{a} = (a_1, \dots, a_m)$ (a row vector), where each a_i equals 1 or 2. In particular, let $\mathbf{1}_m = (1, \dots, 1)$. Let $L_{\mathbf{a}}$ denote the $(\mathrm{S}_3)^m$-lattice generated by $(\mathbb{Z}\mathbf{A}_2)^m$ and the vector

$$x_{\mathbf{a}} := \sum_{i=1}^{m} a_i \omega_1^{(i)}.$$

Proposition 12.4. *For $m \geq 2$ and for any* $\mathbf{a}$ *as above* (*i.e., each a_i equals* 1 *or* 2), *the* $(\mathrm{S}_3)^m$*-lattice $L_{\mathbf{a}}$ is not quasi-invertible.*

Proof. First we note that $L_{\mathbf{a}}$ is ϕ-isomorphic to $L_{\mathbf{1}_m}$ with respect to some automorphism φ of $(\mathrm{S}_3)^m$ (for a definition of φ-isomorphism, see the beginning of Section 2).

Indeed, let α_1, α_2 be the standard basis of the root system $\mathbf{A}_2$ (and of $\mathbb{Z}\mathbf{A}_2$). Let

$$\omega_1 = \frac{1}{3}(2\alpha_1 + \alpha_2),\ \omega_2 = \frac{1}{3}(\alpha_1 + 2\alpha_2)$$

be the fundamental weights, this is the standard basis of Λ_3 (*loc. cit.*). Let $\overline{\omega}_1, \overline{\omega}_2$ be their images in $\Lambda_3/\mathbb{Z}\mathbf{A}_2 \cong \mathbb{Z}/3\mathbb{Z}$. Since

$$\omega_1 + \omega_2 = \alpha_1 + \alpha_2 \in \mathbb{Z}\mathbf{A}_2,$$

we have $\overline{\omega}_1 + \overline{\omega}_2 = 0$, hence $\overline{\omega}_2 = 2\overline{\omega}_1$. Thus the nontrivial automorphism σ of the Dynkin diagram $\mathbf{A}_2$ takes $\overline{\omega}_1$ to $\overline{\omega}_2 = 2\overline{\omega}_1$ when acting on $\Lambda_3/\mathbb{Z}\mathbf{A}_2$.

Now let $\mathbf{a}$ be as above. Write $\Delta = (\mathbf{A}_2)^m$, $\Delta = \Delta_1 \cup \dots \cup \Delta_m$. For each $i = 1, \dots, m$ we define an automorphism τ_i of $\Delta_i = \mathbf{A}_2$. If $a_i = 1$, we set $\tau_i = \mathrm{id}$, while if $a_i = 2$, we set $\tau_i = \sigma_i$, where σ_i is the nontrivial automorphism of Δ_i. Then the automorphism $\tau = \prod_i \tau_i$ of $\Delta = (\mathbf{A}_2)^m$ acts on $(\Lambda_3)^m$ and takes $L_{\mathbf{1}_m}$ to $L_{\mathbf{a}}$. We see that the $(\mathrm{S}_3)^m$-lattices $L_{\mathbf{1}_m}$ and $L_{\mathbf{a}}$ are τ_*-isomorphic, where τ_* is the induced automorphism of $(\mathrm{S}_3)^m$. Thus, in order to prove that the $(\mathrm{S}_3)^m$-lattice $L_{\mathbf{a}}$ is not quasi-invertible, it suffices to show that $L_{\mathbf{1}_m}$ is not quasi-invertible.

Let $\alpha_1^{(i)}, \alpha_2^{(i)}$ be the standard basis of $(\mathbb{Z}\mathbf{A}_2)^{(i)}$. Let $\omega_1^{(i)}, \omega_2^{(i)}$ be the standard basis of $\Lambda_3^{(i)}$, then

$$\omega_1^{(i)} = \frac{1}{3}(2\alpha_1^{(i)} + \alpha_2^{(i)}).$$

Let $\alpha_1, \dots, \alpha_{3m-1}$ be the standard basis of $\mathbb{Z}\mathbf{A}_{3m-1}$. We denote by $\lambda_1, \dots, \lambda_{3m-1}$ (rather than $\omega_1, \dots, \omega_{3m-1}$) the standard basis of Λ_{3m} consisting of fundamental weights. Then we have (*loc. cit.*)

$$\lambda_1 = \frac{1}{3m}((3m-1)\alpha_1 + (3m-2)\alpha_2 + \dots + 2\alpha_{3m-2} + \alpha_{3m-1}). \tag{12.1}$$

We embed $(\mathbb{Z}\mathbf{A}_2)^m$ into $\mathbb{Z}\mathbf{A}_{3m-1}$ as follows:

$$\alpha_1^{(i)} \mapsto \alpha_{3(i-1)+1}, \quad \alpha_2^{(i)} \mapsto \alpha_{3(i-1)+2}$$

(i.e., $\alpha_1^{(1)} \mapsto \alpha_1$, $\alpha_2^{(1)} \mapsto \alpha_2$, $\alpha_1^{(2)} \mapsto \alpha_4$, $\alpha_2^{(2)} \mapsto \alpha_5$, etc.). This embedding induces an embedding

$$\psi\colon (\mathbb{Q}\mathbf{A}_2)^m \hookrightarrow \mathbb{Q}\mathbf{A}_{3m-1}.$$

Set

$$M = \Lambda_{3m} \cap \psi((\mathbb{Q}\mathbf{A}_2)^m).$$

We show that $M = \psi(L_{\mathbf{1}_m})$. Since by (12.1) the image of λ_1 in $\Lambda_{3m}/\mathbb{Z}\mathbf{A}_{3m-1}$ is of order $3m$, we see that Λ_{3m} is generated by $\mathbb{Z}\mathbf{A}_{3m-1}$ and λ_1, hence the set $\{\alpha_1, \dots, \alpha_{3m-1}, \lambda_1\}$ is a generating set for Λ_{3m}. From (12.1) we see that

$$\alpha_{3m-1} = 3m\lambda_1 - (3m-1)\alpha_1 - (3m-2)\alpha_2 - \dots - 2\alpha_{3m-2},$$

hence the set $\Xi := \{\alpha_1, \dots, \alpha_{3m-2}, \lambda_1\}$ is a basis for Λ_{3m}. The subset

$$\Xi' := \{\alpha_1, \alpha_2,\ \alpha_4, \alpha_5,\ \dots,\ \alpha_{3m-5}, \alpha_{3m-4},\ \alpha_{3m-2}\}$$

of Ξ is contained in M. Set $N := \mathbb{Z}[\Xi \smallsetminus \Xi'] \cap M \subset \mathbb{Q}\mathbf{A}_{3m-1}$, then clearly $M = \mathbb{Z}\Xi' \oplus N$. Since $\operatorname{rank} M = 2m = |\Xi'| + 1$, we see that $\operatorname{rank} N = 1$. The element

$$\mu := m\lambda_1 - (m-1)\alpha_3 - (m-2)\alpha_6 - \cdots - \alpha_{3m-3} = \frac{1}{3}((3m-1)\alpha_1 \\ +(3m-2)\alpha_2 + (3m-4)\alpha_4 + (3m-5)\alpha_5 + \cdots + 2\alpha_{3m-2} + \alpha_{3m-1})$$

is contained in N and indivisible in M, hence the one-element set $\{\mu\}$ is a basis of N, and $\Xi' \cup \{\mu\}$ is a basis of M. Now

$$\mu - (m-1)(\alpha_1+\alpha_2) - (m-2)(\alpha_4+\alpha_5) - \cdots - 1(\alpha_{3(m-2)+1} + \alpha_{3(m-2)+2})$$
$$= \frac{1}{3}((2\alpha_1+\alpha_2) + (2\alpha_4+\alpha_5) + \cdots + (2\alpha_{3m-2} + \alpha_{3m-1}))$$
$$= \psi(\omega_1^{(1)} + \omega_1^{(2)} + \cdots + \omega_1^{(m)}).$$

We see that M is generated by $\psi((\mathbb{Z}\mathbf{A}_2)^m)$ and $\psi(\omega_1^{(1)} + \omega_1^{(2)} + \cdots + \omega_1^{(m)})$, hence $M = \psi(L_{\mathbf{1}_m})$, thus M is isomorphic to $L_{\mathbf{1}_m}$. Therefore, it suffices to prove that M is not quasi-invertible.

The quotient lattice Λ_{3m}/M injects into the $\mathbb{Q}$-vector space $\mathbb{Q}\mathbf{A}_{3m-1}/\psi((\mathbb{Q}\mathbf{A}_2)^m)$ with basis $\overline{\alpha_3}, \overline{\alpha_6}, \dots, \overline{\alpha_{3(m-1)}}$ on which $(\mathrm{S}_3)^m$ acts trivially. Thus we obtain a short exact sequence

$$0 \to M \to \Lambda_{3m} \to \mathbb{Z}^{m-1} \to 0,$$

where $\mathbb{Z}^{m-1}$ is a trivial, hence permutation, $(\mathrm{S}_3)^m$-lattice. It follows that the $(\mathrm{S}_3)^m$-lattices M and Λ_{3m} are equivalent, and therefore it suffices to show that Λ_{3m} is not a quasi-invertible $(\mathrm{S}_3)^m$-lattice.

Now we embed $\mathrm{S}_3 \times \mathrm{S}_3$ into $(\mathrm{S}_3)^m$ as follows: $(s,t) \in \mathrm{S}_3 \times \mathrm{S}_3$ maps to $(s,t,\dots,t) \in (\mathrm{S}_3)^m$. With the notation of [20, (6.4)] we have $\Lambda_{3m} = Q_{3m}(1)$. By [20, Proposition 7.1(b)], with respect to the above embedding $\mathrm{S}_3 \times \mathrm{S}_3 \hookrightarrow (\mathrm{S}_3)^m$, we have

$$Q_{3m}(1)|_{\mathrm{S}_3 \times \mathrm{S}_3} \sim \Lambda_6|_{\mathrm{S}_3 \times \mathrm{S}_3}.$$

By [20, Proposition 7.4(b)], Λ_6 is not a quasi-permutation $\mathrm{S}_3 \times \mathrm{S}_3$-lattice, and it is actually proved there that $[\Lambda_6]^{\mathrm{fl}}$ (see [21, § 2.7] for the notation) is not an invertible $\mathrm{S}_3 \times \mathrm{S}_3$-lattice. It follows that Λ_6 is not a quasi-invertible $\mathrm{S}_3 \times \mathrm{S}_3$-lattice (although $Ш^2(\Gamma', \Lambda_6) = 0$ for every subgroup Γ' of $\mathrm{S}_3 \times \mathrm{S}_3$). Thus Λ_{3m} is not a quasi-invertible $\mathrm{S}_3 \times \mathrm{S}_3$-lattice, hence it is not a quasi-invertible $(\mathrm{S}_3)^m$-lattice. Thus $L_{\mathbf{1}_m}$ is not a quasi-invertible $(\mathrm{S}_3)^m$-lattice, and therefore $L_{\mathbf{a}}$ is not a quasi-invertible $(\mathrm{S}_3)^m$-lattice for any $\mathbf{a}$ as above. This completes the proof of Proposition 12.4. □

13. Standard subgroups

In this and the next sections we will collect several elementary results from combinatorial linear algebra, which will be needed to complete the proof of Theorem 9.1.

Let $e_1, \dots, e_m$ be the standard $\mathbb{Z}/n\mathbb{Z}$-basis of $(\mathbb{Z}/n\mathbb{Z})^m$. We say that a subgroup $S \subset (\mathbb{Z}/n\mathbb{Z})^m$ is *standard* if S is generated by $n_1e_1, \dots, n_re_r$ for some $1 \le r \le m$ and some integers $n_1, \dots, n_r$, where n_i divides n_{i+1} for $i = 1, \dots, r-1$.

Let W be a finite group, P be a W-lattice, and $\lambda\colon P \to \mathbb{Z}/n\mathbb{Z}$ be a surjective morphism of W-modules, where W acts trivially on $\mathbb{Z}/n\mathbb{Z}$. Given a subgroup S of $(\mathbb{Z}/n\mathbb{Z})^m$, let P^m_S denote the preimage of S in P^m with respect to the homomorphism $\lambda^m\colon P^m \to (\mathbb{Z}/n\mathbb{Z})^m$. We regard P^m_S as a W-submodule of P^m, where W acts diagonally on P^m.

Lemma 13.1. *Let W, P, n and λ be as above. For every subgroup $S \subset (\mathbb{Z}/n\mathbb{Z})^m$ there exists a standard subgroup $S_{\mathrm{st}} \subset (\mathbb{Z}/n\mathbb{Z})^m$ with the following property: there exist an isomorphism $g_P\colon P^m_S \xrightarrow{\sim} P^m_{S_{\mathrm{st}}}$ of W-modules and an automorphism g of $(\mathbb{Z}/n\mathbb{Z})^m$ taking S to S_{st} such that the following diagram commutes:*

$$\begin{tikzcd} P^m_S \arrow[r, "\lambda^m"] \arrow[d, "g_P"] & S \arrow[r, hook] \arrow[d] & (\mathbb{Z}/n\mathbb{Z})^m \arrow[d, "g"] \\ P^m_{S_{\mathrm{st}}} \arrow[r, "\lambda^m"] & S_{\mathrm{st}} \arrow[r, hook] & (\mathbb{Z}/n\mathbb{Z})^m. \end{tikzcd}$$

Proof. The homomorphism $\lambda^m\colon P^m \to (\mathbb{Z}/n\mathbb{Z})^m$ can be written as

$$\lambda^m = \lambda \otimes_{\mathbb{Z}} \mathrm{id}\colon P \otimes_{\mathbb{Z}} \mathbb{Z}^m \longrightarrow \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}^m.$$

Since for any $g \in \mathbf{GL}_m(\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}^m)$ the diagram

$$\begin{tikzcd} P \otimes_{\mathbb{Z}} \mathbb{Z}^m \arrow[r, "\lambda\otimes\mathrm{id}_{\mathbb{Z}^m}"] \arrow[d, "\mathrm{id}_P\otimes g"] & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}^m \arrow[d, "\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}\otimes g"] \\ P \otimes_{\mathbb{Z}} \mathbb{Z}^m \arrow[r, "\lambda\otimes\mathrm{id}_{\mathbb{Z}^m}"] & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}^m \end{tikzcd}$$

commutes, it suffices to show that for every subgroup $S \subset (\mathbb{Z}/n\mathbb{Z})^m$ there exists $g \in \mathbf{GL}_m(\mathbb{Z})$ such that $g(S)$ is standard.

Let $\pi\colon \mathbb{Z}^m \to (\mathbb{Z}/n\mathbb{Z})^m$ be the natural projection. Then $\pi^{-1}(S)$ is a finite index subgroup of $\mathbb{Z}^m$. There exist a basis $b_1, \dots, b_m$ of $\mathbb{Z}^m$ and integers $n_1 \,|\, n_2 \,|\, \dots \,|\, n_m$, such that $n_1 b_1, \dots, n_m b_m$ form a basis of $\pi^{-1}(S)$; cf. [18, Theorem III.7.8]. Now let $g \in \mathbf{GL}_m(\mathbb{Z})$ be the element that takes the basis $b_1, \dots, b_m$ to the standard basis of $\mathbb{Z}^m$. Then $g(\pi^{-1}(S))$ is the subgroup $n_1\mathbb{Z} \times \dots \times n_m\mathbb{Z}$ of $\mathbb{Z}^m$ and thus $S_{\mathrm{st}} := g(S) = \langle n_1 e_1, \dots n_m e_m \rangle = \langle n_1 e_1, \dots, n_r e_r \rangle$ is standard, where $r \le m$ is the largest integer such that n does not divide n_r. $\square$

Set $Q = \ker \lambda \subset P$. For a subgroup $S_1 \subset \mathbb{Z}/n\mathbb{Z}$ we set $P^1_{S_1} = \lambda^{-1}(S_1)$, so that $Q \subset P^1_{S_1} \subset P$.

Corollary 13.2. *Assume that S in Lemma 13.1 is cyclic. Then*

$$P^m_S \cong P^1_{S_1} \oplus Q^{m-1}$$

for some subgroup $S_1 \subset \mathbb{Z}/n\mathbb{Z}$ isomorphic to S.

Proof. By Lemma 13.1, we have $P^m_S \cong P^m_{S_{\rm st}}$. Since S is cyclic, say of order s, the group $S_{\rm st}$ is generated by $(n/s)e_1$. Set $S_1 = \langle (n/s)e_1 \rangle \subset \mathbb{Z}/n\mathbb{Z}$, then clearly

$$P^m_{S_{\rm st}} = P^1_{S_1} \oplus Q^{m-1},$$

and the corollary follows. □

Corollary 13.3. *Assume that S in Lemma 13.1 contains an element of order n. Then P^m_S has a direct summand isomorphic to P.*

Proof. By Lemma 13.1, P^m_S is isomorphic to $P^m_{S_{\rm st}}$ for some standard subgroup $S_{\rm st} \subset (\mathbb{Z}/n\mathbb{Z})^m$. From the definition of a standard subgroup we see that

$$P^m_{S_{\rm st}} = P^1_{S_1} \oplus \cdots \oplus P^1_{S_m} \ ,$$

where $S_i \subset \mathbb{Z}/n\mathbb{Z}$ is generated by $n_i e_i$ (for $i > r$ we take $n_i = 0$). Since $S_{\rm st}$ contains an element of order n, we see that $n_1 = 1$, hence S_1 is generated by e_1, i.e., $S_1 = \mathbb{Z}/n\mathbb{Z}$ and $P^1_{S_1} = P$. Thus P^m_S has a direct summand isomorphic to P. □

14. Coordinate and almost coordinate subspaces

Let F be a field, F^m be an m-dimensional F-vector space equipped with the standard basis $e_1 = (1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1)$.

Recall that the *Hamming weight* of a vector $v = (a_1, \ldots, a_m) \in F^m$ is defined as the number of non-zero elements among $a_1, \ldots, a_m$. We will say $v \in F^m$ is *defective* if its Hamming weight is $< m$ or, equivalently, if at least one of its coordinates is 0. The following lemma is well known; a variant of it is used to construct the standard open cover of the Grassmannian $\mathrm{Gr}(m, d)$ by $d(m-d)$-dimensional affine spaces, see, e.g., [15, §1.5]. For the sake of completeness, we supply a short proof.

Lemma 14.1. *Let V be a vector subspace of F^m of dimension $d \geq 2$. Then V has a basis consisting of defective vectors.*

Proof. Let A be a $d \times m$ matrix whose rows form a basis of V. Then

$$V = \{wA \mid w \in F^d\} .$$

Note that for any invertible $d \times d$ matrix B, the rows of BA will also form a basis of V. Since the rows of A are linearly independent, A has a nondegenerate $d \times d$ submatrix M. Let $B = M^{-1}$. Then the $d \times m$ matrix BA has a $d \times d$ identity submatrix. Since $d \geq 2$, this implies that every row of BA is defective. The rows of BA thus give us a desired basis of defective vectors for V. □

Definition 14.2. We will say that a subspace $V \subset F^m$ is a *coordinate subspace* if V has a basis of coordinate vectors $e_{i_1}, \ldots, e_{i_d}$, for some $I = \{i_1, \ldots, i_d\} \subset \{1, \ldots, m\}$. We will denote such a subspace by F_I.

In subsequent sections we will occasionally use this notation in the more general setting, where F is a commutative ring but not necessarily a field.

In this setting F_I will denote the free F-submodule of F^n generated by $e_{i_1}, \dots, e_{i_d}$.

Lemma 14.3. *Let $V \subset F^m$ be an F-subspace. Suppose $V \cap F_I$ is coordinate for every $I \subsetneq \{1, \dots, m\}$, then either*

- *V is the 1-dimensional subspace spanned by a vector $\mathbf{a} = (a_1, \dots, a_m)$, where $a_1 \neq 0, \ \dots, \ a_m \neq 0$, or*
- *V is coordinate.*

Proof. Assume that V is not of the form $\mathrm{Span}_F(\mathbf{a})$, where $\mathbf{a} = (a_1, \dots, a_m)$ and $a_1 \neq 0, \dots, a_m \neq 0$. Then V has a basis of defective vectors. Indeed, if $\dim(V) = 1$ this is obvious, since every vector in V is defective. The case where $\dim(V) \geq 2$ is covered by Lemma 14.1.

Clearly $v \in F^m$ is defective if and only if $v \in F_I$ for some $I \subsetneq \{1, \dots, m\}$. Thus V is spanned by $V \cap F_I$, as I ranges over the proper subsets of $\{1, \dots, m\}$. By our assumption, each $V \cap F_I$ is coordinate and therefore is spanned by coordinate vectors. We conclude that V itself is spanned by coordinate vectors, i.e., is coordinate, as desired. □

Definition 14.4. We will say that $V \subset F^m$ is *almost coordinate* if V has a basis of the form

$$e_{i_1}, \dots, e_{i_r}, e_{j_1} + e_{h_1}, \dots, e_{j_s} + e_{h_s}, \tag{14.1}$$

where $i_1, \dots, i_r, j_1, \dots, j_s, h_1, \dots, h_s$ are distinct integers between 1 and m. We will refer to a basis of this form as an *almost coordinate basis* of V.

Remark 14.5. An almost coordinate subspace $V \subset F^m$ has a unique almost coordinate basis. In other words, the set of integers $\{i_1, \dots, i_r\}$ and the set of unordered pairs $\{\{j_1, h_1\}, \dots, \{j_s, h_s\}\}$ in (14.1) are uniquely determined by V. Indeed, $\{i_1, \dots, i_r\}$ is the set of subscripts $i \in \{1, \dots, m\}$ such that the coordinate vector e_i lies in V. The set $\{\{j_1, h_1\}, \{j_2, h_2\}, \dots, \{j_s, h_s\}\}$ is then the set of unordered pairs $\{j, h\}$ such that $j, h \notin \{i_1, \dots, i_r\}$ and $e_j + e_h \in V$.

Proposition 14.6. *Let $F = \mathbb{Z}/2\mathbb{Z}$, and let $V \subset F^m$ be an F-subspace for some $m \geq 4$. Assume $V \cap F_I$ is almost coordinate in $F_I \cong (\mathbb{Z}/2\mathbb{Z})^r$ for every $I = \{i_1, \dots, i_r\} \subsetneq \{1, \dots, m\}$. Then either*

- *V is the 1-dimensional subspace spanned by $(1, \dots, 1)$, or*
- *V is almost coordinate.*

Proof. Assume that V is not of the form $\mathrm{Span}_F \{(1, \dots, 1)\}$. Then, once again, Lemma 14.1 tells us that V has a basis of defective vectors, i.e., V is spanned by $V \cap F_I$, as I ranges over the proper subsets of $\{1, \dots, m\}$. By our assumption, each $V \cap F_I$ is almost coordinate and therefore is spanned by vectors of Hamming weight 1 or 2. We conclude that V itself is spanned by vectors of weight 1 or 2. Choose a spanning set of the form

$$e_{i_1}, \dots, e_{i_r}, e_{j_1} + e_{h_1}, \dots, e_{j_s} + e_{h_s} \tag{14.2}$$

of minimal total Hamming weight, i.e., with minimal value of $r + 2s$. Here

$$i_1, \ldots, i_r, j_1, h_1, \ldots, j_s, h_s \in \{1, \ldots, m\}$$

and $j_1 \neq h_1, \ldots, j_s \neq h_s$. We claim that (14.2) is an almost coordinate basis of V, i.e., that the subscripts

$$i_1, \ldots, i_r, j_1, \ldots, j_s, h_1, \ldots, h_s \tag{14.3}$$

are all distinct. Clearly, Proposition 14.6 follows from this claim.

It thus remains to prove the claim. The minimality of the total Hamming weight of our spanning set (14.2) implies that we cannot remove any vectors, i.e., that it is a basis of V. In particular, the subscripts $i_1, \ldots, i_r$ and the pairs $(j_1, h_1), \ldots, (j_s, h_s)$ are distinct. If there is an overlap among subscripts (14.3), then, after permuting coordinates, we have either $i_1 = j_1$ or $j_1 = j_2$. We will now show that neither of these equalities can occur.

If $i_1 = j_1$ then we may replace $e_{j_1} + e_{h_1}$ by

$$e_{h_1} = (e_{j_1} + e_{h_1}) - e_{i_1} \in V\,.$$

We will obtain a new spanning set consisting of vectors of weight 1 or 2 with smaller total weight, a contradiction.

Now suppose $j_1 = j_2$. Denote this number by j. Then $V \cap F_{\{j,h_1,h_2\}}$ contains the vectors

$$e_j + e_{h_1} \text{ and } e_j + e_{h_2} \in V. \tag{14.4}$$

Since we are assuming that $m \geq 4$, $\{j, h_1, h_2\} \subsetneq \{1, \ldots, m\}$ and hence, $V \cap F_{\{j,h_1,h_2\}}$ is almost coordinate. The subspace in $F_{\{j,h_1,h_2\}}$ generated by the two vectors (14.4) is cut by the linear equation

$$x_j + x_{h_1} + x_{h_2} = 0$$

and clearly is not almost coordinate. It follows that $V \cap F_{\{j,h_1,h_2\}} = F_{\{j,h_1,h_2\}}$, hence V contains all three of the coordinate vectors e_j, e_{h_1} and e_{h_2}. Replacing $e_j + e_{h_1}$ and $e_j + e_{h_2}$ by e_j, e_{h_1} and e_{h_2} in our spanning set, we reduce the total weight by one, a contradiction. This completes the proof of the claim and thus of Proposition 14.6. □

15. Coordinate subspaces and quasi-permutation lattices

Proposition 15.1. *Let W be a finite group, M be a W-lattice and let $\lambda\colon M \to F := \mathbb{Z}/p\mathbb{Z}$ be a surjective morphism of W-modules, where p is a prime and W acts trivially on F. For any $m \geq 1$, and an F-subspace $S \subset V := F^m$, let M^m_S be the preimage of $S \subset F^m$ under the projection $\lambda^m\colon M^m \to F^m$.*

Assume that

(a) *M is a quasi-permutation W-lattice;*
(b) *the W^m-lattice $M^m_{S_1}$ is* not *quasi-permutation for any 1-dimensional subspace S_1 of F^m of the form $S_1 = \mathrm{Span}_F\{(a_1, \ldots, a_n)\}$, where $a_1 \neq 0, \ \ldots, a_m \neq 0$.*

Then, given a subspace $S \subset F^m$, M_S^m is a quasi-permutation W^m-lattice if and only if S is coordinate.

The following notation will be helpful in the proof of Proposition 15.1 and in the subsequent sections.

Definition 15.2. Let W be a finite group, M be a W-module and m be a positive integer. Given a subset $I \subset \{1, \dots, m\}$, we define the "coordinate subgroup" $W_I \subset W^m$ as

$$W_I := \{(w_1, \dots, w_m) \in W^m \mid \; w_i = \mathrm{id} \text{ if } i \notin I\}.$$

We will also define the W_I-submodule M_I of M^m as

$$M_I := \{(a_1, \dots, a_m) \in M^m \mid a_i = 0 \text{ if } i \notin I\}.$$

We shorten $W_{\{i\}}$, $M_{\{i\}}$ to W_i, M_i.

Proof of Proposition 15.1. The "if" assertion is clear. We will prove "only if" by induction on m. In the base case, $m = 1$, every subspace of V is coordinate, so there is nothing to prove.

For the induction step, assume that $m \geq 2$ and that our assertion has been established for all $m' < m$. Suppose that for some subspace $S \subset F^m$ the lattice M_S^m is quasi-permutation. We want to show that S is coordinate.

Since M_S^m is quasi-permutation, Lemma 2.5 tells us that $M_S^m \cap M_I$ is a quasi-permutation W_I-lattice for every $I \subsetneq \{1, \dots, m\}$ (cf. Definition 15.2 above). But $M_S^m \cap M_I = M_{S \cap F_I}^m$, and so by the induction hypothesis $S \cap F_I$ is a coordinate subspace in F_I (and hence, in F^m).

Now Lemma 14.3 tells us that either S is a 1-dimensional subspace of F^m which does not lie in any coordinate hyperplane or S is a coordinate subspace in F^m. Our assumption (b) rules out the first possibility. Hence, S is a coordinate subspace of F^m, as claimed. □

16. Proof of Theorem 9.1 for H of types $\mathbf{A}_{n-1}$ ($n \geq 5$), $\mathbf{B}_n$ ($n \geq 3$) and $\mathbf{D}_n$ ($n \geq 4$)

Starting from this section, we will prove Theorem 9.1 case by case.

Notation 16.1. Let R be an irreducible reduced root system. We denote by $Q = Q(R)$ the root lattice of R and by $P = P(R)$ the weight lattice of R, both lattices regarded as $W := W(R)$-lattices. Given a positive integer m and a subset $I \subset \{1, \dots, m\}$, we define $W_I \subset W^m$, and the W_I-modules Q_I, P_I, etc., as in Definition 15.2. The base field k is assumed to be algebraically closed of characteristic zero.

16.1. Case $\mathbf{A}_{n-1}$ ($n \geq 5$).

Theorem 16.2. *Let $G = (\mathbf{SL}_n)^m/C$, where $n \geq 5$ and C is a subgroup of $(\mu_n)^m = Z(\mathbf{SL}_n^m)$. Then the following conditions are equivalent:*

(a) *G is Cayley,*

(b) *G is stably Cayley,*

(c) *the character lattice* $\mathsf{X}(G)$ *is quasi-permutation,*
(d) $\mathsf{X}(G) = Q^m$*,*
(e) G *is isomorphic to* $(\mathbf{PGL}_n)^m$*.*

Proof. (a) $\Longrightarrow$ (b) is obvious.
(b) $\Longrightarrow$ (c) follows from [20, Thm. 1.27].
(d) $\Longrightarrow$ (e): clear.
(e) $\Longrightarrow$ (a): clear, because the group $\mathbf{PGL}_n$ is Cayley, see [20, Thm. 1.31], and a product of Cayley groups is obviously Cayley.
The implication (c) $\Longrightarrow$ (d) follows from the next proposition. $\square$

Proposition 16.3. *Let* $R = \mathbf{A}_{n-1}$*, where* $n \geq 5$*. Suppose an intermediate* W^m*-lattice* L *between* Q^m *and* P^m*. is quasi-permutation. Then* $L = Q^m$*.*

Proof. We proceed by induction on m. The base case, $m = 1$, follows from [20, Prop. 5.1]. For the induction step, assume that $m \geq 2$ and that the proposition holds for $m-1$. We will show that it also holds for m.

Set $I := \{2, \dots, m\} \subset \{1, 2, \dots, m\}$ and $F = P/Q = \mathbb{Z}/n\mathbb{Z}$. By Lemma 2.5, $L \cap P_I$ is a quasi-permutation W_I-lattice. By the induction hypothesis, $L \cap P_I = Q_I$. Set $S = L/Q^m \subset F^m$, then $S \cap F_I = 0$. It follows that the canonical projection $S \to F_1$ is injective. As $F = \mathbb{Z}/n\mathbb{Z}$, we have $S \cong \mathbb{Z}/d\mathbb{Z}$ for some divisor d of n.

In the notation of the beginning of Section 13, $L = P_S^m$ as a W-lattice (where W acts on P^m diagonally). By Corollary 13.2,

$$L \cong L_1 \oplus Q^{m-1}, \tag{16.1}$$

where $Q_1 \subset L_1 \subset P_1$. Clearly Q^{m-1} is quasi-permutation as a W-lattice because so is $Q = \ker[\mathbb{Z}[\mathrm{S}_n / \mathrm{S}_{n-1}] \to \mathbb{Z}]$. By assumption, L is a quasi-permutation W^m-lattice, hence it is quasi-permutation as a W-lattice. Since L and Q^{m-1} are quasi-permutation W-lattices, we see from (16.1) that $L_1 \sim L_1 \oplus Q^{m-1} \cong L \sim 0$, so that L_1 is a quasi-permutation W-lattice. By [20, Prop. 5.1] it follows that $L_1 = Q_1$, hence $S = 0$, and $P_S^m = Q^m$. Thus $L = Q^m$, which proves (d) for m and completes the proofs of Proposition 16.3 and Theorem 16.2. $\square$

16.2. **Case $\mathbf{B}_n$ ($n \geq 3$) and $\mathbf{D}_n$ ($n \geq 4$).** Let $n \geq 7$, R be the root system of $\mathbf{Spin}_n$ (of type $\mathbf{B}_{(n-1)/2}$ for n odd or of type $\mathbf{D}_{n/2}$ for n even) and M be the character lattice of $\mathbf{SO}_n$. If n is odd, then $M = Q$; if n is even, then $Q \subsetneq M \subsetneq P$. Set $F := P/M \cong \mathbb{Z}/2\mathbb{Z}$.

Theorem 16.4. *Let* $G = (\mathbf{Spin}_n)^m/C$*, where* $n \geq 7$*, and* C *is a central subgroup of* $(\mathbf{Spin}_n)^m$*. Then the following conditions are equivalent:*
(a) G *is Cayley,*
(b) G *is stably Cayley,*
(c) *the character lattice* $\mathsf{X}(G)$ *of* G *is quasi-permutation,*
(d) $\mathsf{X}(G) = M^m$*, where* $M = \mathsf{X}(\mathbf{SO}_n)$*,*
(e) G *is isomorphic to* $(\mathbf{SO}_n)^m$*.*

Proof. Only (c) $\Longrightarrow$ (d) needs to be proved; the other implications are easy.

Assume (c), i.e., $\mathsf{X}(G)$ is a quasi-permutation W^m-lattice. Clearly $Q^m \subset \mathsf{X}(G) \subset P^m$. We claim that $\mathsf{X}(G) \supset M^m$. If n is odd this is obvious, because $M^m = Q^m$. If n is even then by Lemma 2.5, $\mathsf{X}(G) \cap P_i$ is a quasi-permutation W_i-lattice. Now by [20, Thm. 1.28], we have $\mathsf{X}(G) \cap P_i = M_i$. Thus $\mathsf{X}(G) \supset M_1 \oplus \cdots \oplus M_m = M^m$, as claimed.

We will now show that $\mathsf{X}(G) = M^m$. Assume the contrary. Consider the surjection $\lambda\colon P \to P/M \cong \mathbb{Z}/2\mathbb{Z}$. Set $S = \mathsf{X}(G)/M^m \subset (\mathbb{Z}/2\mathbb{Z})^m$, then $S \neq 0$. In the notation of Lemma 13.1, we have $\mathsf{X}(G) = P^m_S$. Since $S \neq 0$, by Corollary 13.3 $\mathsf{X}(G)$ has a direct W-summand isomorphic to P. By Proposition 11.1, P is not quasi-invertible, hence $\mathsf{X}(G)$ is not quasi-invertible as a W-lattice. It follows that $\mathsf{X}(G)$ is not a quasi-invertible W^m-lattice, which contradicts (c). Thus (d) holds, as desired. □

Remark 16.5. Alternatively, we can prove Theorem 16.4 similar to the proof of Proposition 16.3. Namely, we prove by induction that $\mathsf{X}(G) = M^m$ using Corollary 13.2. Here we make use of the fact that by Proposition 11.1, P is not quasi-permutation.

Remark 16.6. Proposition 16.3 cannot be proved by an argument analogous to the proof of Theorem 16.4. Indeed, the proof of Theorem 16.4 relies on the fact that $\mathsf{X}(\mathbf{Spin}_n)$ *is not* quasi-invertible for $n \geq 7$ (see Proposition 11.1). On the other hand, $\mathsf{X}(\mathbf{SL}_n)$ *is* quasi-invertible (though it is not quasi-permutation) whenever n is a prime; see [11, Prop. 9.1 and Rem. 9.3].

17. Proof of Theorem 9.1 for H of type $\mathbf{A}_1 = \mathbf{B}_1 = \mathbf{C}_1$

We will continue using Notation 16.1. Let $R = \mathbf{A}_1$. Set $F = Q/P = \mathbb{Z}/2\mathbb{Z}$.

Let $G = (\mathbf{SL}_2)^m/C$, where C is a subgroup of $Z((\mathbf{SL}_2)^m) = (\mu_2)^m$. We have $Q^m \subset \mathsf{X}(G) \subset P^m$. Set $S := \mathsf{X}(G)/Q^m \subset F^m = (\mathbb{Z}/2\mathbb{Z})^m$.

Theorem 17.1. *Let $G = (\mathbf{SL}_2)^m/C$, where C is a subgroup of $Z((\mathbf{SL}_2)^m) = (\mu_2)^m$. Then the following conditions are equivalent:*

(a) *G is Cayley,*
(b) *G is stably Cayley,*
(c) *the character lattice $\mathsf{X}(G)$ is a quasi-permutation W^m-lattice,*
(d) *$S := \mathsf{X}(G)/Q^m$ is an almost coordinate subspace of $F^m = (\mathbb{Z}/2\mathbb{Z})^m$,*
(e) *G decomposes into a direct product of normal subgroups $G_1 \times_k \cdots \times_k G_s$, where each G_i is isomorphic to either $\mathbf{SL}_2$, $\mathbf{PGL}_2$ or $\mathbf{SO}_4$.*

Remark 17.2. The set of normal subgroups $G_1, \dots, G_s$ in part (e) is uniquely determined by G; see Remark 14.5.

Proof of Theorem 17.1. Only the implication (c) $\Longrightarrow$ (d) needs to be proved; all the other implications are easy. The implication (c) $\Longrightarrow$ (d) follows from the next proposition. □

Proposition 17.3. *Let $R = \mathbf{A}_1$ and L be an intermediate W-lattice between Q^m and P^m, i.e., $Q^m \subset L \subset P^m$. Write $S = L/Q^m \subset F^m = (\mathbb{Z}/2\mathbb{Z})^m$. Then L is quasi-permutation if and only if S is almost coordinate.*

Proof. The "if" assertion follows easily from Lemmas 2.6 and 2.7. To prove the "only if" assertion, we begin by considering three special cases which will be of particular interest to us.

Case 1: $m \le 2$. Here every subspace of $(\mathbb{Z}/2\mathbb{Z})^m$ is almost coordinate, and condition (d) holds automatically.

Case 2: S is the line $\langle \mathbf{1}_m \rangle = \{0, \mathbf{1}_m\} \subset (\mathbb{Z}/2\mathbb{Z})^m$, where $\mathbf{1}_m = (1, \dots, 1)$. This $S = \langle \mathbf{1}_m \rangle$ is not almost coordinate for any $m \ge 3$. Thus we need to show that (c) does not hold, i.e., the lattice $L = P^m_{\langle \mathbf{1}_m \rangle}$ is not quasi-permutation. This lattice is isomorphic to the lattice M described at the beginning of Section 11, in the case where Δ is the disjoint union of m copies of $\mathbf{B}_1$ (or, equivalently, of $\mathbf{A}_1$) for $m \ge 3$. By Proposition 11.1, for $m \ge 3$, the lattice $M \simeq L = P^m_{\langle \mathbf{1}_m \rangle}$, is not quasi-invertible, hence not quasi-permutation, as claimed.

Case 3: $m = 3$. There are two subspaces S of $(\mathbb{Z}/2\mathbb{Z})^3$ that are not almost coordinate: (i) the line $\langle \mathbf{1}_3 \rangle$ and (ii) the 2-dimensional subspace cut out by $x_1 + x_2 + x_3 = 0$. Once again we need to show that in both of these cases L is not quasi-permutation.

(i) is covered by Case 2 (with $m = 3$). If S is as in (ii), then L is isomorphic to the lattice M defined in the statement of Proposition 12.1. By this proposition, L is not quasi-invertible, hence not quasi-permutation, as claimed.

We now proceed with the proof of the proposition by induction on $m \ge 1$. The base case, where $m \le 3$, is covered by Cases 1 and 3 above. For the induction step assume that $m \ge 4$ and that the proposition has been established for all $m' \le m - 1$.

Suppose that for some subspace $S = L/Q^m \subset (\mathbb{Z}/2\mathbb{Z})^m$ we know that $L = P^m_S$ is quasi-permutation. Our goal is to show that S is almost coordinate.

Since L is quasi-permutation, by Lemma 2.5, we conclude that $L \cap P_I$ is a quasi-permutation W_I-lattice for every $I = \{i_1, \dots, i_r\} \subsetneq \{1, \dots, m\}$. By the induction hypothesis, $(L \cap P_I)/Q_I = S \cap F_I$ is an almost coordinate subspace in $F_I = (\mathbb{Z}/2\mathbb{Z})^r$.

Now Proposition 14.6 tells us that S is either the line $\langle \mathbf{1}_m \rangle$, or almost coordinate. If S is the line $\langle \mathbf{1}_m \rangle$, then L is not quasi-permutation by Case 2, contradicting our assumption. Thus S is almost coordinate, which completes the proofs of Proposition 17.3 and Theorem 17.1. $\square$

18. Proof of Theorem 9.1 for H of types $\mathbf{A}_2$, $\mathbf{B}_2 = \mathbf{C}_2$, and $\mathbf{A}_3 = \mathbf{D}_3$

18.1. **Case $\mathbf{A}_2$.** Once again, we will continue using Notation 16.1. Set $F := P/Q \simeq \mathbb{Z}/3\mathbb{Z}$.

Theorem 18.1. *Let $G = (\mathbf{SL}_3)^m/C$, where C is a subgroup of $(\mu_3)^m = Z((\mathbf{SL}_3)^m)$. Then the following conditions are equivalent:*

(a) *G is Cayley,*
(b) *G is stably Cayley,*
(c) *the character lattice $\mathsf{X}(G)$ is a quasi-permutation W^m-lattice,*
(d) *$S := \mathsf{X}(G)/Q^m$ is a coordinate subspace of $F^m \simeq (\mathbb{Z}/3\mathbb{Z})^m$,*
(e) *G decomposes into a direct product of normal subgroups $G_1 \times_k \cdots \times_k G_s$, where each G_i is isomorphic to either $\mathbf{SL}_3$ or $\mathbf{PGL}_3$.*

Proof. Once again, only the implication (c) $\Longrightarrow$ (d) needs to be proved; the other implications are easy.

Clearly $Q^m \subset \mathsf{X}(G) \subset P^m$; assume $\mathsf{X}(G)$ is quasi-permutation. The W-lattices P and Q are quasi-permutation, see [20, Thm. 1.28]. If $S \subset F^m$ is the 1-dimensional subspace $\langle \mathbf{a} \rangle$ spanned by a vector $\mathbf{a} = (a_1, \dots, a_m)$ such that $a_1 \neq 0, \ \dots, a_m \neq 0$, then from Proposition 12.4 it follows that $\mathsf{X}(G) = P^m_{\langle \mathbf{a} \rangle}$ is not a quasi-permutation W^m-lattice, a contradiction. Now by Proposition 15.1, $\mathsf{X}(G) = P^m_S$ is quasi-permutation if and only if S is coordinate. This shows that (c) $\Longrightarrow$ (d). □

18.2. **Case $\mathbf{B}_2 = \mathbf{C}_2$.** Set $F := P/Q = \mathbb{Z}/2\mathbb{Z}$.

Theorem 18.2. *Let $G = (\mathbf{Spin}_5)^m/C$, where C is a subgroup of the finite k-group $(\mu_2)^m = \ker[(\mathbf{Spin}_5)^m \to (\mathbf{SO}_5)^m]$. Then the following conditions are equivalent:*

(a) *G is Cayley,*
(b) *G is stably Cayley,*
(c) *the character lattice $\mathsf{X}(G)$ is quasi-permutation,*
(d) *$S := \mathsf{X}(G)/Q^m$ is a coordinate subspace of $F^m = (\mathbb{Z}/2\mathbb{Z})^m$,*
(e) *G decomposes into a direct product of normal subgroups $G_1 \times_k \cdots \times_k G_s$, where each G_i is isomorphic to either $\mathbf{Spin}_5 = \mathbf{Sp}_4$ or $\mathbf{SO}_5$.*

Proof. As in the proof of Theorem 18.1, we only need to establish the implication (c) $\Longrightarrow$ (d). We have $Q^m \subset \mathsf{X}(G) \subset P^m$. The W-lattices P and Q are quasi-permutation, see [20, Thm. 1.28]. If $S \subset F^m$ is the 1-dimensional subspace $\langle \mathbf{1}_m \rangle$ spanned by the vector $\mathbf{1}_m = (1, \dots, 1)$ then by Proposition 11.1, $P^m_{\langle \mathbf{1}_m \rangle}$ is not a quasi-invertible W^m-lattice. Now by Proposition 15.1, the W^m-lattice $\mathsf{X}(G) = P^m_S$ is quasi-permutation if and only if S is coordinate, which completes the proof of the theorem. □

18.3. **Case $\mathbf{A}_3 = \mathbf{D}_3$.** Here $P/Q \simeq \mathbb{Z}/4\mathbb{Z}$.

Theorem 18.3. *Let $G = (\mathbf{Spin}_6)^m/C$, where C is a subgroup of $Z(G) = (\mu_4)^m = \ker[(\mathbf{Spin}_6)^m \to (\mathbf{PSO}_6)^m]$. We have $Q^m \subset \mathsf{X}(G) \subset P^m$, where P, Q and $\mathsf{X}(G)$ are the character lattices of $\mathbf{PSO}_6$, $\mathbf{Spin}_6$ and G, respectively. Then the following conditions are equivalent:*

(a) *G is Cayley,*
(b) *G is stably Cayley,*

(c) $\mathsf{X}(G)$ *is quasi-permutation,*
(d) $\mathsf{X}(G) \subset (2P)^m$ *and* $\mathsf{X}(G)/Q^m$ *is a coordinate subspace of* $(2P/Q)^m = (\mathbb{Z}/2\mathbb{Z})^m$*,*
(e) G *decomposes into a direct product of normal subgroups* $G_1 \times_k \cdots \times_k G_s$*, where each* G_i *is isomorphic to either* $\mathbf{SO}_6$ *or* $\mathbf{PSO}_6 = \mathbf{PGL}_4$*.*

Proof. Both $\mathbf{SO}_6$ and $\mathbf{PSO}_6 = \mathbf{PGL}_4$ are Cayley; see [20, Introduction]. Consequently, (e) $\Longrightarrow$ (a). Thus we only need to show that (c) $\Longrightarrow$ (d); the other implications are immediate. Assume that $\mathsf{X}(G)$ is quasi-permutation.

First we claim that $\mathsf{X}(G) \subset (2P)^m$. Indeed, assume the contrary. Then $\mathsf{X}(G)/Q^m$ contains an element of order 4. By Corollary 13.3, the W^m-lattice $\mathsf{X}(G)$ restricted to the diagonal subgroup W has a direct summand isomorphic to the character lattice P of $\mathbf{Spin}_6$. By Proposition 11.1, the W-lattice P is not quasi-invertible. We conclude that $\mathsf{X}(G)$ is not quasi-invertible as a W-lattice and hence not a quasi-invertible W^m-lattice, contradicting our assumption that $\mathsf{X}(G)$ is quasi-permutation. This proves the claim.

As we mentioned above, $\mathbf{SO}_6$ and $\mathbf{PSO}_6$ are both Cayley. Hence, the W-lattices $2P$ and Q are quasi-permutation. Set $F = 2P/Q \simeq \mathbb{Z}/2\mathbb{Z}$. If $S := \mathsf{X}(G)/Q^m \subset F^m$ is the 1-dimensional subspace $\langle \mathbf{1}_m \rangle$ spanned by the vector $\mathbf{1}_m = (1, \dots, 1)$, then by Proposition 12.2, $\mathsf{X}(G)$ is not a quasi-invertible W^m-lattice, a contradiction. Now Proposition 15.1 tells us that the W^m-lattice $\mathsf{X}(G)/Q^m$ is coordinate in $(2P/Q)^m$, and (d) follows. □

This completes the proof of Theorem 9.1.

19. Proof of Theorem 1.5

In this section we deduce Theorem 1.5 from Theorem 9.1. Clearly (b) implies (a), so we only need to show that (a) implies (b).

Let G be a stably Cayley simple k-group (not necessarily absolutely simple) and $\bar{k}$ be a fixed algebraic closure of k. Then $\overline{G} := G \times_k \bar{k}$ is stably Cayley over $\bar{k}$ and is of the form H^m/C, where H is a simple and simply connected $\bar{k}$-group and C is a central k-subgroup of H^m. By Theorem 9.1, $\overline{G} = G_{1,\bar{k}} \times_{\bar{k}} \cdots \times_{\bar{k}} G_{s,\bar{k}}$, each $G_{i,\bar{k}}$ is either a stably Cayley simple group or is isomorphic to $\mathbf{SO}_{4,\bar{k}}$. (Recall that $\mathbf{SO}_{4,\bar{k}}$ is stably Cayley and semisimple, but is not simple.) Here we write $G_{i,\bar{k}}$ for the factors in order to emphasize that they are defined over $\bar{k}$.

If H is not of type $\mathbf{A}_1$, then the subgroups $G_{i,\bar{k}}$ are simple and hence, intrinsic in $\overline{G}$: they are the minimal closed connected normal subgroups of dimension ≥ 1. If H is of type $\mathbf{A}_1$, this is no longer obvious, since some of the groups $G_{i,\bar{k}}$ may not be simple (they may be isomorphic to $\mathbf{SO}_{4,\bar{k}}$). However, in this case the subgroups $G_{i,\bar{k}}$ are intrinsic in $\overline{G}$ as well by Remark 17.2. Hence, in all cases, the Galois group $\mathrm{Gal}(\bar{k}/k)$ permutes $G_{1,\bar{k}}, \dots, G_{s,\bar{k}}$. Since G is simple over k, this permutation action is transitive.

Let $l \subset \bar{k}$ be the subfield corresponding to the stabilizer of $G_{1,\bar{k}}$ in $\mathrm{Gal}(\bar{k}/k)$. Then $G_{1,\bar{k}}$ and $G_{\geq 2,\bar{k}} := G_{2,\bar{k}} \times_{\bar{k}} \cdots \times_{\bar{k}} G_{s,\bar{k}}$ are $\mathrm{Gal}(\bar{k}/l)$-invariant, and we obtain l-forms of these two $\bar{k}$-groups, which we will denote by $G_{1,l}$ and $G_{\geq 2,l}$. Then $G = R_{l/k}(G_{1,l})$, where $G_{1,l}$ is either absolutely simple or an l-form of $\mathbf{SO}_{4,l}$. In the latter case $G_{1,l}$ has to be an *outer* l-form of the split l-form of $\mathbf{SO}_4$; otherwise $G_{1,l}$ will not be l-simple and consequently, G will not be k-simple.

Now consider the case when $G_{1,l}$ is not an l-form of $\mathbf{SO}_{4,l}$. Then $G_{1,l}$ is absolutely simple. Since G is stably Cayley over k,

$$G \times_k l = G_{1,l} \times_l G_{\geq 2,l} \text{ is stably Cayley over } l. \tag{19.1}$$

It remains to show that $G_{1,l}$ is stably Cayley over l. Assume the contrary. Note that $G_{1,\bar{k}}$ is stably Cayley over $\bar{k}$. Comparing the classification of stably Cayley simple $\bar{k}$-groups over an algebraically closed field $\bar{k}$ of characteristic 0 in [20, Theorem 1.28] with the classification of stably Cayley absolutely simple l-groups over a field l of characteristic 0, not necessarily algebraically closed, in Theorem 1.4, we see that $G_{1,l}$ is an outer l-form of $\mathbf{PGL}_{n,l}$ for some even integer $n \geq 4$. Then by Example 10.7 the character lattice of $G_{1,l}$ is not quasi-invertible, and by Proposition 10.8 the product $G_{1,l} \times_l G_{\geq 2,l}$ cannot be stably Cayley over l, which contradicts (19.1). This contradiction completes the proof of Theorem 1.5. □

Acknowledgements. The authors are very grateful to Jean-Louis Colliot-Thélène for proving Lemma 10.3 and for stating and proving Lemma 10.2.

References

[1] *Algebraic Number Theory,* Proc. instructional conf. organized by the London Math. Soc. (J.W.S. Cassels, A. Fröhlich, eds.), Academic Press, London, 1967.

[2] A. Borel, *Linear Algebraic Groups,* 2nd ed., Graduate Texts in Math., vol. 126, Springer-Verlag, New York, 1991.

[3] M. Borovoi, *Abelianization of the second nonabelian Galois cohomology*, Duke Math. J. **72** (1993), 217–239.

[4] M. Borovoi, I. Dolgachev, *Real reductive Cayley groups of rank* ≤ 2, `arXiv:1212.1065v2[math.AG]`.

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

[6] K.S. Brown, *Cohomology of Groups,* Graduate Texts in Math., vol. 87, Springer-Verlag, New York–Berlin, 1982.

[7] H. Cartan, S. Eilenberg, *Homological Algebra,* Princeton Univ. Press, Princeton, NJ, 1956.

[8] A. Cayley, *Sur quelques propriétés des déterminants gauches*, J. reine angew. Math. **32** (1846), 119–123; reprinted in: *The Coll. Math. Papers of Arthur Cayley*, Vol. I, No. 52, Cambridge Univ. Press, 1889, 332–336.

[9] J.-L. Colliot-Thélene, B.È. Kunyavskiĭ, V.L. Popov, Z. Reichstein, *Is the function field of a reductive Lie algebra purely transcendental over the field of invariants for the adjoint action?*, Compos. Math. **147** (2011), 428–466.

[10] J.-L. Colliot-Thélène, J.-J. Sansuc, *La R-équivalence sur les tores,* Ann. Sci. École Norm. Sup. (4) **10** (1977), 175–229.

[11] J.-L. Colliot-Thélène, J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: applications,* J. Algebra **106** (1987), 148–205.

[12] B. Conrad, *Reductive group schemes (SGA3 Summer School, 2011),* `http://math.stanford.edu/~conrad/papers/luminysga3.pdf`.

[13] A. Cortella, B. Kunyavskiĭ, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000), 771–793.

[14] Y.Z. Flicker, C. Scheiderer, R. Sujatha, *Grothendieck's theorem on non-abelian H^2 and local-global principles*, J. Amer. Math. Soc. **11** (1998), 731–750.

[15] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Wiley-Interscience, 2011.

[16] V.A. Iskovskikh, *Two nonconjugate embeddings of the group $S_3 \times Z_2$ into the Cremona group,* (Russian) Tr. Mat. Inst. Steklova 241 (2003), Teor. Chisel, Algebra i Algebr. Geom., 105–109; translation in Proc. Steklov Inst. Math. **241**, no. 2 (2003), 93–97.

[17] B.È. Kunyavskiĭ, *Three-dimensional algebraic tori,* in: Investigations in Number Theory, Saratov. Gos. Univ., Saratov, 1987, pp. 90–111; English transl.: Selecta Math. Sov. **21**(1990), 1–21.

[18] S. Lang, *Algebra*, revised third edition, Graduate Texts in Math., vol. 211, Springer-Verlag, New York, 2002.

[19] N. Lemire, M. Lorenz, *On certain lattices associated with generic division algebras,* J. Group Theory **3** (2000), 385–405.

[20] N. Lemire, V.L. Popov, Z. Reichstein, *Cayley groups*, J. Amer. Math. Soc. **19** (2006), 921–967.

[21] M. Lorenz, *Multiplicative Invariant Theory,* Encycl. Math. Sci., vol. 135, Invariant Theory and Algebraic Transformation Groups, VI, Springer-Verlag, Berlin, 2005.

[22] C. Miller, *The second homology group of a group; relations among commutators,* Proc. Amer. Math. Soc. **3** (1952), 588–595.

[23] I. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen,* J. reine angew. Math. **132** (1907), 85–137, see also: Gesam. Abh., Bd. I, Springer-Verlag, Berlin-New York, 1973, 198–250.

[24] *Séminaire de géométrie algébrique du Bois Marie* 1962–64*, Schémas en groupes (SGA3)* (M. Demazure, A. Grothendieck, eds.), Lecture Notes Math., vol. 151, 152, 153, Springer-Verlag, Berlin–New York, 1970.

[25] T.A. Springer, *Reductive groups,* in: "Automorphic forms, representations and L-functions (Corvallis, Oregon, 1977)", Proc. Sympos. Pure Math., XXXIII, Part 1, Amer. Math. Soc., Providence, RI, 1979, pp. 3–27.

[26] T.A. Springer, *Linear Algebraic Groups,* 2nd ed., Progr. Math., vol. 9, Birkhäuser, Boston, MA, 1998.

[27] J. Tits, *Classification of algebraic semisimple groups,* in: Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 33–62.

[28] V.E. Voskresenskiĭ, *Birational properties of linear algebraic groups,* Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970), 3–19; English transl.: Math. USSR Isv. **4** (1970), 1–17.

[29] V.E. Voskresenskiĭ, *Algebraic Groups and Their Birational Invariants*, Transl. Math. Monographs, vol. 179, Amer. Math. Soc., Providence, RI, 1998.

[30] V.E. Voskresenskiĭ, A.A. Klyachko, *Toroidal Fano varieties and root systems*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 237–263; English transl.: Math. USSR Izv. **24** (1984), 221–244.

Borovoi: Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, 69978 Tel Aviv, Israel
E-mail address: borovoi@post.tau.ac.il

Kunyavskiĭ: Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel
E-mail address: kunyav@macs.biu.ac.il

Lemire: Department of Mathematics, University of Western Ontario, London, ON N6A 5B7, Canada
E-mail address: nlemire@uwo.ca

Reichstein: Department of Mathematics, Univ. of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mail address: reichst@math.ubc.ca