FINITE GROUP ACTIONS ON CURVES OF GENUS ZERO

MARIO GARCIA-ARMAS

Abstract. We classify, up to conjugacy, the finite (constant) subgroups $G$ of adjoint absolutely simple algebraic groups of type $A_1$ over an arbitrary field $k$ of characteristic not 2.

1. Introduction

The finite subgroups of $\text{PGL}_2(\mathbb{C})$ have been known for over a century: these are cyclic, dihedral and the so-called polyhedral groups $A_4$, $S_4$ and $A_5$ (see, e.g., [Kl56]). Any two isomorphic finite subgroups of $\text{PGL}_2(\mathbb{C})$ are conjugate. All of the above remains true if one replaces $\mathbb{C}$ by any algebraically closed field $k$ and asks about finite subgroups of order prime to $\text{char}(k)$ (see [Se72, §2.5]). Using this result as a starting point, A. Beauville [Beau10] classified, up to conjugacy, the finite subgroups $G$ of $\text{PGL}_2(k)$ over an arbitrary field $k$, under the assumption that $|G|$ is prime to $\text{char}(k)$. X. Faber [Fa11] completed this picture by classifying the $p$-irregular subgroups of $\text{PGL}_2(k)$, i.e., subgroups whose order is divisible by $p = \text{char}(k)$, and describing their conjugacy classes.

In this paper, we are interested in studying the finite (constant) subgroups of (possibly non-split) adjoint absolutely simple algebraic groups of type $A_1$ over a field $k$, as well as their conjugacy classes. In doing so, we restrict our attention to fields $k$ of characteristic different from 2.

2010 Mathematics Subject Classification. 20G15, 20G10, 11E20.

Key words and phrases. finite group actions, special orthogonal groups, quadratic forms.

The author is partially supported by a Four Year Fellowship, University of British Columbia.
Theorem 1.1. Let $k$ be a field of characteristic $p > 2$ and suppose that $\text{SO}(q)$ contains a $p$-irregular subgroup. Then the quadratic form $q$ is isotropic, i.e., there exists an isomorphism $\text{SO}(q) \cong \text{PGL}_2$.

It remains to classify the $p$-regular subgroups $G$ of $\text{SO}(q)$, so we may assume henceforth that $\text{char}(k)$ is prime to $|G|$. Over an algebraic closure $\overline{k}$ of $k$, we have that $\text{SO}(q)(\overline{k}) \cong \text{PGL}_2(\overline{k})$. Thus any finite subgroup $G$ of $\text{SO}(q)$ embeds into $\text{PGL}_2(\overline{k})$, so it must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$, $D_{2n}$ (the dihedral group of $2n$ elements), $A_4$, $S_4$ or $A_5$. Theorem 1.2 below classifies these subgroups up to isomorphism and Theorem 1.3 up to conjugacy. Taking $q = (-1, -1, 1)$ in these theorems, we recover the results in [Beau10].

We will prove Theorem 1.2 in Section 2. Note that the classification of polyhedral groups in parts (b) and (c) is hinted at in [Se78]; here we make it explicit for completeness. Throughout the paper, we denote a primitive $n$-th root of 1 by $\omega_n$, and we set $\alpha_n = (\omega_n + \omega_n^{-1})/2$ and $\beta_n = \alpha_n^2 - 1$.

Theorem 1.2. Let $q$ be a nondegenerate quadratic form of discriminant 1 and let $q_0 = (1, 1, 1)$.

(a) The group $D_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$ is always contained in $\text{SO}(q)$. For $n \geq 3$, the group $\text{SO}(q)$ contains $\mathbb{Z}/n\mathbb{Z}$ and $D_{2n}$ if and only if $\alpha_n \in k$ and $q$ represents $-\beta_n$.

(b) The group $\text{SO}(q)$ contains $A_4$ and $S_4$ if and only if $q \simeq q_0$.

(c) The group $\text{SO}(q)$ contains $A_5$ if and only if $\sqrt{5} \in k$ and $q \simeq q_0$.

We will prove Theorem 1.3 in Section 3. Our argument relies on Galois cohomology techniques, building on the approach taken in [Beau10].

Theorem 1.3. Let $q = (-a, -b, ab)$ be a nondegenerate quadratic form.

(a) The conjugacy classes of $\mathbb{Z}/2\mathbb{Z}$ inside $\text{SO}(q)$ are in natural bijective correspondence with the set $D(q) \subset k^2/k^{\times 2}$ consisting of nonzero square classes represented by $q$.

(b) Let $Q_{a,b} = \{(x, y) \in (k^\times/k^{\times 2})^2 | (ax, by)^2 \equiv (a, b)^2\}$. The symmetric group $S_3 = \{s, t | s^2 = t^2 = (st)^2 = 1\}$ acts on $Q_{a,b}$ by setting $s \cdot (x, y) = (-bxy, abx)$ and $t \cdot (x, y) = (x, -axy)$ for all $(x, y) \in Q_{a,b}$. Then the conjugacy classes of $(\mathbb{Z}/2\mathbb{Z})^2$ inside $\text{SO}(q)$ are in natural bijective correspondence with $Q_{a,b}/S_3$.

(c) There is at most one conjugacy class of subgroups isomorphic to $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 3$) inside $\text{SO}(q)$.

(d) Suppose that $D_{2n}$ is contained in $\text{SO}(q)$ ($n \geq 3$). The set $D(\{1, -\beta_n\})$ consisting of nonzero square classes represented by $\langle 1, -\beta_n \rangle$ forms a subgroup of $k^\times/k^{\times 2}$. The class $\frac{a + b + 1}{2} k^{\times 2}$ is contained in $D(\{1, -\beta_n\})$: let $C$ be the subgroup generated by this class. Then the conjugacy classes of $D_{2n}$ inside $\text{SO}(q)$ are in natural bijective correspondence with $D(\{1, -\beta_n\})/C$.

(e) There is at most one conjugacy class of subgroups isomorphic to $A_4$, $S_4$ or $A_5$ inside $\text{SO}(q)$.

Acknowledgements. I thank Z. Reichstein for reading early versions of this paper and making several useful suggestions. I am also grateful to an anonymous referee for many helpful remarks.

2. Finite subgroups of $\text{SO}(q)$

Lemma 2.1. Let $q$ be a nondegenerate ternary quadratic form over $k$ and let $M$ be an element of $\text{SO}(q)(k)$. Then the following results hold.
(a) Suppose that $M$ is diagonalizable over $\overline{k}$. Then its eigenvalues are $1$, $\lambda$, and $\lambda^{-1}$ for some $\lambda \in \overline{k}^\times$. If $\lambda \neq \pm 1$, then $q$ becomes isotropic over $k(\lambda)$, which is an extension of $k$ of order dividing $2$.

(b) Suppose that $M$ is a nontrivial unipotent matrix. Then $q$ must be isotropic.

Proof. Let $Q$ be the matrix associated to $q$. Note that $M^{-1} = Q^{-1}TMQ$, whence the characteristic polynomial $P$ of $M$ satisfies $P(x) = -x^3P(1/x)$. It follows easily that the eigenvalues of $M$ must be $1, \lambda, \lambda^{-1}$ for some $\lambda \in \overline{k}$.

Suppose first that $M$ is diagonalizable. Taking the trace of $M$, we obtain that $\lambda + \lambda^{-1} \in k$, whence $[k(\lambda) : k]$ is $1$ or $2$. We show that $q$ becomes isotropic over $k(\lambda)$, provided that $\lambda \neq \pm 1$. Indeed, over this field we can select an eigenvector $v$ of $M$ associated to the eigenvalue $\lambda$. Then, we compute $q(v) = q(Mv) = \lambda^2 q(v)$, whence $q(v) = 0$. This completes the proof of part (a).

Suppose now that $M$ is a nontrivial unipotent matrix. Then we can find nonzero vectors $v_1, v_2$ such that $Mv_1 = v_1$ and $Mv_2 = v_1 + v_2$ (this follows easily after conjugating $M$ into Jordan canonical form). Let $b_q$ be the symmetric bilinear form associated to $q$. Note that $b_q(v_1, v_2) = b_q(Mv_1, Mv_2) = q(v_1) + b_q(v_1, v_2)$, whence $q(v_1) = 0$. This finishes the proof. \hfill $\Box$

Proof of Theorem 1.1 Let $G$ be a $p$-irregular subgroup inside $SO(q)$ and let $M \in G$ be any element of order $p$. Note that $0 = M^p - I = (M - I)^p$, whence $M$ is a unipotent matrix. By Lemma 2.1(b), it follows that $q$ is isotropic, so we obtain that $SO(q) \cong PGL_2$.

Proof of Theorem 1.2 (a) The first statement is trivial: the diagonal subgroup $D_0 \subset SO(q)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. Assume henceforth that $n \geq 3$. It suffices to prove that $\mathbb{Z}/n\mathbb{Z} \subset SO(q) \Rightarrow \alpha_n \in k$ and $q$ represents $-\beta_n \Rightarrow D_2n \subset SO(q)$.

To prove the first implication, let $M$ be an element of order $n$ in $SO(q)(k)$. By Lemma 2.1(a), we may assume that the eigenvalues of $M$ are $1, \omega_n$ and $\omega_n^{-1}$, after replacing $M$ by a power of itself if necessary. Using Lemma 2.1(a) again, we see that $\alpha_n \in k$ and $q$ becomes isotropic over $k(\omega_n) = k(\sqrt[n]{\beta_n})$. It suffices to prove that $q$ is isotropic over $k(\sqrt[n]{\beta_n})$ if and only if $q$ represents $-\beta_n$. If $q$ is isotropic over $k$, then $q$ is universal, so there is nothing to prove. Suppose that $q$ is anisotropic over $k$. It follows from [EKM08, Prop. 34.8] that $q \simeq q_0 \otimes N_{k(\sqrt[n]{\beta_n})/k}(1) q_1$ for some nondegenerate quadratic forms $q_0, q_1$, where $q_1$ is anisotropic over $k(\sqrt[n]{\beta_n})$. If $q$ is isotropic over $k(\sqrt[n]{\beta_n})$, we conclude that $q \neq q_1$ and thus $\dim(q_0) = \dim(q_1) = 1$ (recall that $N_{k(\sqrt[n]{\beta_n})/k}(1, -\beta_n)$). It follows that $q_1 \cong (\beta_n, \gamma)$ by taking discriminants, whence $q$ represents $-\beta_n$. Conversely, suppose that the latter holds. Then we must have that $q \simeq (-\beta_n, -\gamma, \beta_n \gamma)$ for some $\gamma \in k^\times$, so it follows that $q$ is isotropic over $k(\sqrt[n]{\beta_n})$.

Suppose next that $\alpha_n \in k$ and $q$ represents $-\beta_n$. As we saw above, we may assume that $q = (-\beta_n, -\gamma, \beta_n \gamma)$ for some $\gamma \in k^\times$. The matrices

\[
s = \begin{pmatrix}
1 & 0 & 0 \\
0 & \alpha_n & \beta_n \\
0 & 1 & \alpha_n
\end{pmatrix},
\quad
t = \begin{pmatrix}
-1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & -1
\end{pmatrix},
\]

are contained in $SO(q)(k)$ and satisfy $s^n = t^2 = (st)^2 = 1$, whence they generate a subgroup isomorphic to $D_{2n}$. The proof of this part is complete.

(b) It clearly suffices to prove that $A_4 \subset SO(q) \Rightarrow q \simeq q_0 \Rightarrow S_4 \subset SO(q)$. Recall that $A_4$ acts linearly on $k^3$ by rotations on the tetrahedron with vertices
(ε₁, ε₂, ε₁ε₂), where ε₁ = ±1. This representation is absolutely irreducible and leaves q₀ invariant, i.e., we have a linear representation ρ: A₄ ↪ SO(q₀)(k). Recall that any absolutely irreducible representation of a finite group admits at most one invariant quadratic form, up to a scalar. Indeed, after passing to the algebraic closure, this is an immediate consequence of Schur’s lemma. It follows that q ∼ c·q₀ for some c ∈ k⁺; taking discriminants, we conclude that c = 1.

On the other hand, S₄ acts linearly on k³ by rotations on the cube with vertices (±1, ±1, ±1) and the corresponding representation has trivial determinant. The form q₀ is invariant under this action and therefore S₄ embeds into SO(q₀)(k). If q ∼ q₀, then SO(q) ∼= SO(q₀) and the result follows.

(c) Note that A₅ ⊂ SO(q) ⇒ A₄ ⊂ SO(q) ⇒ q ∼ q₀ by part (b). Since A₅ contains elements of order 5, it is necessary that ω₅ + ω⁻¹₅ ∈ k, which happens if and only if √5 ∈ k.

Conversely, if √5 ∈ k, the group A₅ acts linearly on k³ by rotations on the icosahedron with vertices (±φ, ±1, 0), (0, ±φ, ±1), (±1, 0, ±φ), where φ = (1 + √5)/2, and this action preserves q₀. The result readily follows. □

**Remark 2.2.** The conclusion in part (a) of the above theorem is independent of the choice of ω₅. Indeed, an easy exercise on Chebyshev polynomials shows that (ω₅ + ω⁻¹₅)/2 ∈ k and q represents 1 − (ω₅ + ω⁻¹₅)²/4 = −(ω₅ − ω⁻¹₅)²/4 if and only if the same holds for every n-th root of 1.

**Example 2.3.** Let k = Q. A primitive n-th root of 1 is given by ωₙ = exp(2πi/n). Recall that ω₅ + ω⁻¹₅ ∈ Q if and only if n = 1, 2, 3, 4 or 6. The group SO(q) contains Z/4Z and D₈ if and only if q represents 1. Moreover, SO(q) contains Z/3Z and D₆ if and only if it contains Z/6Z and D₁₂ if and only if q represents 3.

### 3. Conjugacy classes of subgroups

The purpose of this section is to prove Theorem 1.3. We recall the following construction for convenience.

**Construction 3.1.** ([Beau10, §2]) Let G be an algebraic group defined over k and let H ⊂ G(k) be a subgroup. Fix a separable closure kₛ of k and set Γ = Gal(kₛ/k). Define the pointed set Emb₁(H, G(k)) as the set of embeddings H ↪ G(k) which are conjugate by an element of G(kₛ) to the natural inclusion i: H ↪ G(k), modulo conjugacy by an element of G(k). Also, define the pointed set Conj(H, G(k)) consisting of subgroups of G(k) which are conjugate to H over G(kₛ), modulo conjugacy by an element of G(k).

The centralizer of H in G, which we denote by Z, will be a closed subgroup of G defined over k (cf. [Bo91, Ch. 1, §1.7]). The kernel H¹(k, Z)₀ of the natural map H¹(k, Z) → H¹(k, G) is isomorphic to Emb₁(H, G(k)) as pointed sets. The normalizer N of H in G(kₛ) acts on 1-cocycles Γ → Z(kₛ) in the following way: an element n ∈ N sends σ → aₙσ to σ → n⁻¹aₙσ(n). This (right) action descends to H¹(k, Z) and preserves H¹(k, Z)₀. Then there is an isomorphism of pointed sets between H¹(k, Z)₀/N and Conj(H, G(k)).

Now recall that any two isomorphic finite subgroups (of order prime to char(k)) of SO(q)(kₛ) ∼= PGL₂(kₛ) are conjugate. Therefore, the conjugacy classes of finite subgroups of SO(q) of the same isomorphism type as some particular subgroup
$H \subset \text{SO}(q)$ are in natural bijective correspondence with $\text{Conj}(H, \text{SO}(q)(k))$, independently of the choice of $H$.

We now state some basic facts about the structure of $\text{SO}(q)$. The proofs are easy and are left to the reader. In the sequel, we write $\text{diag}(a_1, \ldots, a_n)$ for the diagonal matrix with entries $a_1, \ldots, a_n$ along the diagonal.

Lemma 3.2. Let $q = (-a, -b, ab)$ be a nondegenerate quadratic form. If $H$ is a finite subgroup of $\text{SO}(q)$, let $Z$ be the centralizer of $H$ in $\text{SO}(q)$ and let $N$ be the normalizer of $H$ in $\text{SO}(q)(k_s)$.

(a) Let $H \cong \mathbb{Z}/2\mathbb{Z}$ be generated by the diagonal matrix $\text{diag}(1, -1, -1)$. Then we have that

$$Z = \left\{ \begin{pmatrix} \det M & 0 \\ 0 & M \end{pmatrix} : M \in \text{O}((-b, ab)) \right\} \cong \text{O}((-b, ab))$$

and $N = Z(k_s)$.

(b) Let $H \cong (\mathbb{Z}/2\mathbb{Z})^2$ be the diagonal subgroup inside $\text{SO}(q)$. Then we have that $Z = H$ and $N$ is isomorphic to $S_4$. Explicitly, if we set $u = \sqrt{-a}$ and $v = \sqrt{-b}$, the matrices

$$\begin{pmatrix} 0 & vu^{-1} & 0 \\ 0 & 0 & u \\ -v^{-1} & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -u \\ 0 & -u^{-1} & 0 \end{pmatrix},$$

generate a subgroup $N' \subset \text{SO}(q)(k_s)$ isomorphic to $S_3$ and $N = H \rtimes N'$.

(c) Let $n \geq 3$ and suppose that $H \cong \mathbb{Z}/n\mathbb{Z}$ is contained in $\text{SO}(q)$. Using the same notation from Theorem 1.2, we may assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ and $H$ is generated by the matrix

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & \beta_n \\ 0 & 1 & \alpha_n \end{pmatrix}.$$ 

Then we have that

$$Z = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & M \end{pmatrix} : M \in \text{SO}((-\gamma, \beta_n\gamma)) \right\} \cong \text{SO}((-\gamma, \beta_n\gamma)).$$

(d) Let $n \geq 3$ and suppose that $H \cong D_{2n}$ is contained in $\text{SO}(q)$. As before, assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ and $H$ is generated by the matrices

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & \beta_n \\ 0 & 1 & \alpha_n \end{pmatrix}, \quad t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$ 

Then we have that $Z \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $s$ and $t$. Assume without loss of generality that $\omega_{2n} \in k_s$ satisfies $\omega_{2n}^2 = \omega_n$. Then the matrices

$$\bar{s} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_{2n} & 2\alpha_n\beta_n \\ 0 & (2\alpha_n)^{-1} & \alpha_{2n} \end{pmatrix}, \quad \bar{t} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

generate $N \cong D_{4n}$ inside $\text{SO}(q)(k_s)$.

(e) Let $H = A_4$, $S_4$ or $A_5$ and suppose that $H$ is contained in $\text{SO}(q)$. Then the centralizer $Z$ is trivial.

□
Remark 3.3. Since any two finite isomorphic subgroups $H_1$ and $H_2$ of $\text{SO}(q)$ are conjugate over $k$, their centralizers will also be conjugate over $k$ (in particular, they must be isomorphic). However, they are not necessarily isomorphic over $k$. For a concrete example, take $k = \mathbb{R}$, $q = (-1, -1, 1)$, $H_1$ generated by $\text{diag}(1, -1, -1)$ and $H_2$ generated by $\text{diag}(-1, -1, 1)$. A simple computation shows that $Z(H_1) \cong \text{O}((-1, 1))$ and $Z(H_2) \cong \text{O}((-1, -1))$. These groups are not isomorphic; the identity component $Z(H_1)^\circ$ is isomorphic to $\mathbb{G}_m$ while $Z(H_2)^\circ \cong \text{SO}_2$, which is a non-split torus over $\mathbb{R}$.

Remark 3.4. Suppose we are in the situation of Lemma 3.2(c) with $\gamma = 1$. Then, $q = (-\beta_n, -1, \beta_n) \simeq (-1, -1, 1)$ and $\text{SO}(q) \cong \text{PGL}_2$, so we are dealing with the case studied in Beauville 2010. Any two cyclic subgroups of order $n$ inside $\text{SO}(q)$ are conjugate over $k$ (see Theorem 1.3), so the centralizer of such a subgroup is unique up to conjugacy. By Lemma 3.2(c), it must be isomorphic to $\text{SO}((-1, \beta_n))$, which is a split torus if and only if $\beta_n = \frac{1}{2}(\omega_n - \omega_n^{-1}) \in k$ if and only if $\omega_n \in k$ (since $\omega_n + \omega_n^{-1} \in k$). So in general the centralizer is not isomorphic to the split torus $\mathbb{G}_m$, contrary to an assertion made in the proof of Beauville 2010, Thm. 4.2 and it might have nontrivial cohomology. However, the final result in Beauville 2010 is unaffected since the map $H^1(k, \mathbb{Z}) \to H^1(k, G)$ still has trivial kernel (see Theorem 1.3).

We now recall some facts about the Galois cohomology of orthogonal groups of quadratic spaces (see Kac-Moody-Rigidity Theory §29.E for details). Let $q$ be any nondegenerate quadratic form of dimension $n$ defined over $k$. The cohomology set $H^1(k, \text{O}(q))$ classifies isometry classes of $n$-dimensional nondegenerate quadratic forms over $k$, while $H^1(k, \text{SO}(q))$ classifies isometry classes of $n$-dimensional quadratic forms $q'$ over $k$ such that $\text{disc}(q') = \text{disc}(q)$. The natural map $H^1(k, \text{SO}(q)) \to H^1(k, \text{O}(q))$ is injective. Let $D_0 \cong (\mathbb{Z}/2\mathbb{Z})^{n-1}$ and $D \cong (\mathbb{Z}/2\mathbb{Z})^n$ be the subgroups of diagonal matrices inside $\text{SO}(q)$ and $\text{O}(q)$, respectively. We have a commutative diagram

\[
\begin{array}{ccccccccc}
1 & \to & D_0 & \subset & D & \xrightarrow{\text{det}} & \mathbb{Z}/2\mathbb{Z} & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\text{SO}(q) & \subset & \text{O}(q) & & & & & & \\
\end{array}
\]

where the top row is exact. This induces a diagram on cohomology

\[
\begin{array}{cccccc}
1 & \to & H^1(k, D_0) & \xrightarrow{i} & (k^\times/k^\times 2)^n & \xrightarrow{p} & k^\times/k^\times 2 & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
H^1(k, \text{SO}(q)) & \xrightarrow{j_*} & H^1(k, \text{O}(q)) & & & & & & \\
\end{array}
\]

where $p: (c_1, \ldots, c_n) \mapsto c_1 \ldots c_n$ is the product map. This identifies $H^1(k, D_0)$ with the elements $(c_1, \ldots, c_n) \in (k^\times/k^\times 2)^n$ such that $c_1 \ldots c_n = 1 \mod k^\times 2$.

In what follows, we will abuse notation and refer to quadratic forms as elements of the cohomology sets $H^1(k, \text{SO}(q))$ and $H^1(k, \text{O}(q))$. The reader should bear in mind that we are tacitly referring to their isometry classes.

Lemma 3.5. Suppose that $q \simeq \langle b_1, \ldots, b_n \rangle$ is a nondegenerate quadratic form.

(a) The map $j_*$ takes $(c_1, \ldots, c_n)$ to $\langle c_1b_1, \ldots, c_nb_n \rangle$ and consequently, $i_*$ takes $(c_1, \ldots, c_n)$, with $c_1 \ldots c_n = 1 \mod k^\times 2$, to $\langle c_1b_1, \ldots, c_nb_n \rangle$. 

Thus $j^*K$

**Proof.** (a) This is certainly well known; for the lack of a direct reference, we supply a proof using Galois descent. Let $V$ be the $k$-vector space where $q$ is defined and write $q = \sum_i b_i v_i^* \otimes v_i^*$, where $v_1, \ldots, v_n$ is a basis of $V$.

Let $c = (c_1, \ldots, c_n) \in (k^\times/k^\times)^n$ and define $s_i \in k^\times$ satisfying $s_i^2 = c_i \mod k^\times$. Fix a finite Galois extension $K/k$ containing the $s_i$ and set $\Gamma_K = \text{Gal}(K/k)$. Recall that a 1-cocycle $\Gamma_K \to (\mathbb{Z}/2\mathbb{Z})^n$ representing $c$ is given by

$$\sigma \mapsto (s_1^{-1}\sigma(s_1), \ldots, s_n^{-1}\sigma(s_n)).$$

Thus $j_*(c)$ is represented by the 1-cocycle $a: \sigma \mapsto \text{diag}(s_1^{-1}\sigma(s_1), \ldots, s_n^{-1}\sigma(s_n))$. The quadratic space associated to $a$ can be obtained by twisting the Galois action on the pair $(V_K, q_K)$ and taking the $\Gamma_K$-invariant elements. Note that the twisted action is defined on $v = \sum_i \lambda_i v_i \in V_K$ ($\lambda_i \in K$) as

$$\sigma * v = \sum_i s_i^{-1}\sigma(\lambda_i) v_i, \quad \sigma \in \Gamma_K,$$

and $v \in aV_K$ is $\Gamma_K$-invariant if and only if $\lambda_i = s_if_i$ for some $f_i \in k$ and all $i$. A $k$-basis of $W = (aV_K)^{\Gamma_K}$ is given by $w_1 = s_1v_1, \ldots, w_n = s_nv_n$. The corresponding quadratic form is

$$q' = \sum_i b_i v_i^* \otimes v_i^* = \sum_i s_i^2 b_i (s_i^{-1}v_i^*) \otimes (s_i^{-1}v_i^*) \simeq \sum_i c_i b_i w_i^* \otimes w_i^*.$$ 

This finishes the proof.

(b) Let $i_q: D_{0,q} \hookrightarrow \text{SO}(q)$ and $i_{q'}: D_{0,q'} \hookrightarrow \text{SO}(q')$ be the embeddings corresponding to the subgroups of diagonal matrices. It is easy to see that the restriction $f|_{D_{0,q}}: D_{0,q} \to D_{0,q'}$ induces a map $F: H^1(k, D_{0,q}) \to H^1(k, D_{0,q'})$ sending $(c_1, \ldots, c_n)$ to $(1, c_1, \ldots, c_n)$. Hence, if $q'' = \langle x_1, \ldots, x_n \rangle$ is any quadratic form such that $\text{disc}(q'') = \text{disc}(q)$, it follows that

$$f_*(q'') = f_*(i_q(F(x_1/b_1, \ldots, x_n/b_n))) = i_{q''}(F(x_1/b_1, \ldots, x_n/b_n)) = \langle d \rangle \perp q''.$$

(c) Let $j_q: D_q \hookrightarrow \text{O}(q)$ and $j_{q'}: D_{0,q'} \hookrightarrow \text{SO}(q')$ be as before. Note that the restriction $f|_{D_q}: D_q \to D_{0,q'}$ induces a map $F: H^1(k, D_q) \to H^1(k, D_{0,q'})$ sending $(c_1, \ldots, c_n)$ to $(c_1 \ldots c_n, c_1, \ldots, c_n)$. The result follows using a similar argument to the one in part (b). \qed

We are ready to prove the main result of this section.
Proof of Theorem 1.3 (a) Let $H \cong \mathbb{Z}/2\mathbb{Z}$ be generated by diag$(1, -1, -1)$ inside $\text{SO}(q)$. By Lemma 3.2(a), its centralizer $Z$ is isomorphic to $O((-b, ab))$. By Lemma 3.2(c), the natural inclusion $Z \rightarrow SO(q)$ induces a map on cohomology $H^1(k, Z) \rightarrow H^1(k, SO(q))$ sending a binary quadratic form $q'$ to $\langle \text{disc}(q') \rangle \perp q'$. Hence, the kernel $H^1(k, Z)_0$ consists of the binary quadratic forms $q'$ such that $\langle \text{disc}(q') \rangle \perp q' \cong q$ (in particular, $\text{disc}(q') \in D(q)$). Define a map $\Psi: H^1(k, Z)_0 \rightarrow D(q)$ sending $q' \mapsto \text{disc}(q')$. If $q', q'' \in H^1(k, Z)_0$ satisfy $\Psi(q') = \Psi(q'')$, then $\langle \text{disc}(q') \rangle \perp q' \cong \langle \text{disc}(q'') \rangle \perp q'' \cong q$ implies $q' \cong q''$ by Witt’s Cancellation Theorem, so $\Psi$ is injective. To prove that $\Psi$ is surjective, let $d \in D(q)$ be arbitrary. Then $q = \langle d \rangle \perp q'$ for some quadratic form $q'$. Taking discriminants yields $\text{disc}(q') = d$. This implies that $q' \in H^1(k, Z)_0$ and $\Psi(q') = d$. This proves that $H^1(k, Z)_0$ is in natural bijection with $D(q)$. Moreover, since the normalizer $N$ coincides with $Z(k_s)$, the action of $N$ on $H^1(k, Z)$ is trivial. This finishes the proof.

(b) Let $H \cong (\mathbb{Z}/2\mathbb{Z})^2$ be the subgroup $D_0$ of diagonal matrices inside $\text{SO}(q)$. By Lemma 3.2(b), we have that $Z = H$ and the map $H^1(k, Z) \rightarrow H^1(k, \text{SO}(q))$ induced by the natural inclusion sends $(x, y, z)$, with $xyz = 1$ mod $k^\times 2$, to $(-ax, -by, abz)$. Therefore, $(x, y, z) \in H^1(k, Z)_0$ if and only if $(-ax, -by, abz) \cong (a, -b, ab)$, which is clearly equivalent to $(ax, by)_2 \cong (a, b)$. It follows easily that $H^1(k, Z)_0 \cong Q_{a,b}$.

We should now determine the action of the normalizer $N$ on $Q_{a,b}$. By Lemma 3.2(b), we have $N = H \rtimes N'$, where $N' \cong S_3$. Since $H$ acts trivially on $H^1(k, Z)$, we only need to determine how $N'$ acts on $H^1(k, Z)_0$. Recall that $N'$ is generated by the matrices

$$s = \begin{pmatrix} 0 & vu^{-1} & 0 \\ 0 & 0 & u \\ v^{-1} & 0 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -u \\ 0 & -u^{-1} & 0 \end{pmatrix},$$

where $u = \sqrt{-a}$ and $v = \sqrt{-b}$. Note that a 1-cocycle $l: \text{Gal}(k_s/k) \rightarrow Z(k_s)$ representing $(x, y) \in Q_{a,b}$ is given by

$$\sigma \mapsto l_\sigma = \text{diag}(x_1^{-1}\sigma(x_1), y_1^{-1}\sigma(y_1), x_1^{-1}\sigma(x_1)y_1^{-1}\sigma(y_1)),$$

where $x_1^2 = x$ mod $k^\times 2$ and $y_1^2 = y$ mod $k^\times 2$. We compute

$$s^{-1}l_\sigma(s) = \text{diag}((ux_1y_1)^{-1}\sigma(ux_1y_1)(uvx_1)^{-1}\sigma(uvx_1)(uy_1)^{-1}\sigma(uy_1)),$$

and

$$t^{-1}l_\sigma(t) = \text{diag}((ux_1y_1)^{-1}\sigma(ux_1y_1)(uvx_1)^{-1}\sigma(uvx_1)(uy_1)^{-1}\sigma(uy_1)).$$

Thus, the 1-cocycles $\sigma \mapsto s^{-1}l_\sigma(s)$ and $\sigma \mapsto t^{-1}l_\sigma(t)$ correspond to the elements $(-bx, y, abx)$ and $(x, -axy)$ in $Q_{a,b}$, respectively. Hence $N' \cong S_3$ acts on $Q_{a,b}$ as claimed, and the result follows easily.

(c) We may assume that we are in the situation of Lemma 3.2(c), i.e., $q = \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ and the centralizer $Z$ of $Z/nZ$ is isomorphic to $\text{SO}((-\gamma, \beta_n\gamma))$. By Lemma 3.2(b), the natural map $H^1(k, Z) \rightarrow H^1(k, \text{SO}(q))$ sends a binary quadratic form $q'$ (with $\text{disc}(q') = -\beta_n$) to $(-\beta_n) \perp q'$. By Witt’s Cancellation Theorem, the kernel $H^1(k, Z)_0$ is trivial and the claim follows.

(d) We may assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ and $H \cong D_{2n}$ is as in Lemma 3.2(d). The centralizer $Z \cong \mathbb{Z}/2\mathbb{Z}$ is generated by diag$(1, -1, -1)$. Let $D_0 \subset \text{SO}(q)$ be the subgroup of diagonal matrices; the natural inclusion $Z \rightarrow D_0$ induces a map $H^1(k, Z) \cong k^\times /k^\times 2 \rightarrow H^1(k, D_0)$ sending $c \in k^\times /k^\times 2$ to $(1, c, c)$. Therefore the natural map $H^1(k, Z) \rightarrow H^1(k, \text{SO}(q))$ sends $c \in k^\times /k^\times 2$ to $(-\beta_n, -c\gamma, c\beta_n\gamma)$. By Witt’s Cancellation Theorem, the kernel $H^1(k, Z)_0$ is given by those square classes.
c such that \( \{ -c_\gamma, c_\beta \gamma \} \simeq \{ -\gamma, \beta_\gamma \} \). It follows easily that \( c \in H^1(k, Z)_0 \) if and only if \( \{ 1, -\beta_\gamma \} \) represents \( c \), i.e., \( H^1(k, Z)_0 \cong D(\{ 1, -\beta_\gamma \}) \).

We now consider the action of the normalizer \( N \cong D_{4n} \) generated by

\[
\bar{s} = \begin{pmatrix}
1 & 0 & 0 \\
0 & \alpha_{2n} & 0 \\
0 & (2\alpha_{2n})^{-1} & \alpha_{2n}
\end{pmatrix}, \quad t = \begin{pmatrix}
-1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & -1
\end{pmatrix}.
\]

Note that \( H \) is the subgroup of \( N \) generated by \( s = \bar{s}^2 \) and \( t \). Clearly the action of \( H \) on \( H^1(k, Z)_0 \) is trivial, so we only need to compute the action of \( \bar{s} \) on \( H^1(k, Z)_0 \). Unraveling the identification \( H^1(k, Z)_0 \cong D(\{ 1, -\beta_\gamma \}) \), we see that a 1-cocycle \( l : \text{Gal}(k_s/k) \rightarrow Z(k_s) \) representing \( c \in H^1(k, Z)_0 \) is given by \( \sigma \rightarrow l_\sigma = \text{diag}(1, c_1^{-1} \sigma(c_1), c_1^{-1} \sigma(c_1)) \), where \( c_1 \in k_s \) satisfies \( c_1^2 = c \mod k \times 2 \).

Then we compute the 1-cocycle

\[
\sigma \mapsto \bar{s}^{-1} \sigma(\bar{s}) = \text{diag}(1, (\alpha_{2n} c_1)^{-1} \sigma(\alpha_{2n} c_1), (\alpha_{2n} c_1)^{-1} \sigma(\alpha_{2n} c_1)).
\]

It corresponds to the square class of \( (\alpha_{2n} c_1)^2 \), which is precisely \( \frac{\alpha_2 + 1}{2} c \). This completes the proof.

(e) This is immediate from Lemma 3.2(e).

**Remark 3.6.** Suppose we are in the situation of Theorem 1.3(d) and \( n \) is odd.

Then a simple computation shows that \( \frac{\alpha_2 + 1}{2} = \frac{1}{4} \left( \omega_n^{\frac{1}{2}} + \omega_n^{-\frac{1}{2}} \right)^2 \in k \times 2 \). Therefore, the conjugacy classes of \( D_{2n} \) are in natural bijective correspondence with \( D(\{ 1, -\beta_\gamma \}) \) for odd \( n \). This is not necessarily true for even \( n \).

We now make the correspondences in parts (a), (b) and (d) of Theorem 1.3 more explicit, by exhibiting representatives for each conjugacy class.

- Let \( q = \langle -a, -b, ab \rangle \), let \( d \in D(q) \) and let \( q' = \langle d, x, y \rangle \) be a quadratic form isometric to \( q \). Select \( P \in \text{GL}_3(k) \) such that \( q = q' \circ P \). Then the element \( d \in D(q) \) corresponds to the conjugacy class of the subgroup \( P^{-1} H P \subset SO(q) \), where \( H \cong \mathbb{Z}/2\mathbb{Z} \) is generated by \( \text{diag}(1, -1, 1) \).
- Let \( q = \langle -a, -b, ab \rangle \), let \( (x, y) \in Q_{a,b} \) and let \( q' = \langle -ax, -by, abxy \rangle \). Select \( P \in \text{GL}_3(k) \) such that \( q = q' \circ P \). The element \( (x, y) \) corresponds to the conjugacy class of the subgroup \( P^{-1} D_0 P \subset SO(q) \), where \( D_0 \cong \mathbb{Z}/2\mathbb{Z} \) is the subgroup of diagonal matrices in \( SO(q) \). Elements of \( Q_{a,b} \) in the same \( S_3 \)-orbit yield subgroups which are conjugate over \( k \).
- Let \( q = \langle -\beta_\gamma, -\gamma, \beta_\gamma \gamma \rangle \) and let \( c \in D(\{ 1, -\beta_\gamma \}) \). Then the quadratic form \( q' = \langle -\beta_\gamma, -c_\gamma, c_\beta \gamma \rangle \) is isometric to \( q \), so we may select \( P \in \text{GL}_3(k) \) such that \( q = q' \circ P \). The element \( c \) corresponds to the conjugacy class of the subgroup \( P^{-1} H P \subset SO(q) \), where \( H \cong D_{2n} \) is as in Lemma 3.2(d). The elements \( c \) and \( \frac{\alpha_2 + 1}{2} c \) yield subgroups which are conjugate over \( k \).

**References**

[Beau10] A. Beauville, *Finite subgroups of PGL_2(K)*, Vector bundles and complex geometry, 23–29, Contemp. Math., 522, Amer. Math. Soc., Providence, RI, 2010.
[Bo91] A. Borel, *Linear Algebraic Groups*, 2nd ed., Springer-Verlag, 1991.
[EKM08] R. Elman, N. Karpenko and A. Merkurjev, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications, vol. 56, American Mathematical Society, Providence, RI, 2008.
[Fa11] X. Faber, *Finite p-irregular subgroups of PGL_2(k)*, arXiv:1112.1999v2 [math.NT], 2011.
[Kl56] F. Klein, Lectures on the icosahedron and the solution of equations of the fifth degree, 2nd. revised edition, Dover Publications, Inc., New York, 1956.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, The book of involutions, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998, with a preface by J. Tits.

[Se72] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, Invent. Math. 15 (1972), no. 4, 259–331

[Se78] J.-P. Serre, Extensions icosoédriques, Séminaire de Théorie des Nombres de Bordeaux 1979-1980, no. 19.

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