



Mathematics Research Reports


Christopher-Lloyd Simon

Conjugacy classes in $PSL_2(\mathbb{K})$

Volume 4 (2023), p. 23-45.

<https://doi.org/10.5802/mrr.16>

© The authors, 2023.

 This article is licensed under the
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.
<http://creativecommons.org/licenses/by/4.0/>



Mathematics Research Reports is member of the
Centre Mersenne for Open Scientific Publishing

www.centre-mersenne.org

e-ISSN: 2772-9559

Conjugacy classes in $\mathrm{PSL}_2(\mathbb{K})$

Christopher-Lloyd SIMON

(Recommended by Linus Kramer)

ABSTRACT. We first describe, over a field \mathbb{K} of characteristic different from 2, the orbits for the adjoint actions of the Lie groups $\mathrm{PSL}_2(\mathbb{K})$ and $\mathrm{PSL}_2(\mathbb{K})$ on their Lie algebra $\mathfrak{sl}_2(\mathbb{K})$. While the former are well known, the latter lead to the resolution of generalised Pell–Fermat equations which characterise the corresponding orbit. The synthetic approach enables to change the base field, and we illustrate this picture over the fields with three and five elements, in relation with the geometry of the tetrahedral and icosahedral groups. While the results may appear familiar, they do not seem to be covered in such generality or detail by the existing literature.

We apply this discussion to partition the set of $\mathrm{PSL}_2(\mathbb{Z})$ -classes of integral binary quadratic forms into groups of $\mathrm{PSL}_2(\mathbb{K})$ -classes. When $\mathbb{K} = \mathbb{C}$ we obtain the class groups of a given discriminant. Then we provide a complete description of their partition into $\mathrm{PSL}_2(\mathbb{Q})$ -classes in terms of Hilbert symbols, and relate this to the partition into genera. The results are classical, but our geometrical approach is of independent interest as it may yield new insights into the geometry of Gauss composition, and unify the picture over function fields.

Finally, we provide a geometric interpretation in the modular orbifold $\mathrm{PSL}_2(\mathbb{Z}) \backslash \mathbb{H}$ for when two points or two closed geodesics correspond to $\mathrm{PSL}_2(\mathbb{K})$ -equivalent quadratic forms, in terms of hyperbolic distances and angles between those modular cycles. These geometric quantities are related to linking numbers of modular knots. Their distribution properties could be studied using the geometry of the quadratic lattice $(\mathfrak{sl}_2(\mathbb{Z}), \det)$ but such investigations are not pursued here.

Acknowledgments. This article contains the main results obtained in Chapter 1 of my thesis. I would thus like to thank my thesis advisors Etienne Ghys and Patrick Popescu-Pampu for their guidance and encouragement; as well as Francis Bonahon, Louis Funar, Jean-Pierre Otal, and Anne Pichon, who carefully refereed my work. I am also grateful to Nicolas Bergeron for sharing stimulating discussions and to the members of the arithmetics & dynamics teams at Penn State for inviting me to present my works in their seminars. I owe Marie Dossin for helping me with the figures in TikZ. Finally, I thank the editors and referees of the MRR for their instructive comments.

Received September 18, 2022; revised May 20, 2023.

2020 *Mathematics Subject Classification.* 11E04, 22E20, 22E04.

Keywords. Lie algebra, adjoint action, killing form, binary quadratic forms, genus class group, Hilbert symbol, modular group, modular cycles.

1. Introduction

Adjoint action of $\mathrm{PSL}_2(\mathbb{K})$ on $\mathfrak{sl}_2(\mathbb{K})$. Let us work over a field \mathbb{K} of characteristic different from 2. The automorphism group $\mathrm{PGL}_2(\mathbb{K})$ of the projective line and its largest simple subgroup $\mathrm{PSL}_2(\mathbb{K})$ play a fundamental role in various areas of mathematics. They appear, for instance, in algebraic geometry when $\mathbb{K} = \mathbb{C}$ and in hyperbolic geometry when $\mathbb{K} = \mathbb{R}$; in arithmetics when $\mathbb{K} = \mathbb{Q}$ and in Galois theory when $\mathbb{K} = \mathbb{Z}/p$.

The first step to understand (the representation theory of) those linear algebraic groups is to describe their conjugacy classes, and more precisely the adjoint actions on their Lie algebra $\mathfrak{sl}_2(\mathbb{K})$. These actions preserve the Killing form, which is a multiple of the non-degenerate quadratic form $\det: \mathfrak{sl}_2(\mathbb{K}) \rightarrow \mathbb{K}$. It is well known that $\mathrm{PGL}_2(\mathbb{K})$ acts transitively on every level set of \det . After introducing the cross-ratio $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \in \mathbb{K}$ of two elements $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}_2(\mathbb{K})$ with non-zero determinant, we will precise this statement.

Proposition 1.1. *Let $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V})$ have determinant $-\delta \neq 0$ and $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \notin \{1, \infty\}$.*

The matrices $M \in \mathrm{PGL}_2(\mathbb{K})$ conjugating \mathfrak{a} to \mathfrak{b} have a well defined determinant in the quotient $\mathbb{K}^\times / \mathrm{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\delta}]^\times)$, and its is equal to the class of $\mathrm{bir}(\mathfrak{a}, \mathfrak{b})$.

In contrast, we will index the $\mathrm{PSL}_2(\mathbb{K})$ -orbits inside $\{\det = -\delta\}$ by the classes $[\chi]$ in the quotient group $\mathbb{K}^\times / \mathrm{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\delta}])$, and parametrize each orbit (δ, χ) by the solutions in $\mathbb{K} \times \mathbb{K}$ to the generalised Pell–Fermat equation $x^2 - \delta y^2 = \chi$. In homological terms, the conjugacy problem in $\mathrm{PSL}_2(\mathbb{K})$ has obstructions measured by the group $\mathbb{K}^\times / \mathrm{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\delta}]^\times)$, and when they vanish the conjugacies form a torsor under the group of units $\{\gamma \in \mathbb{K}[\sqrt{\delta}] \mid \mathrm{Nr}(\gamma) = 1\}$.

Theorem 1.2. *Let $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}_2(\mathbb{K})$ have determinant $-\delta \neq 0$ and $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) = 4\chi \notin \{1, \infty\}$. The elements $C \in \mathrm{SL}_2(\mathbb{K})$ such that $CaC^{-1} = \mathfrak{b}$ are parametrized by the Pell–Fermat conic:*

$$(x, y) \in \mathbb{K} \times \mathbb{K} : \quad x^2 - \delta y^2 = \chi, \quad C(x, y) = x(1 + \mathfrak{b}\mathfrak{a}^{-1}) + y(\mathfrak{a} + \mathfrak{b}).$$

In particular, \mathfrak{a} and \mathfrak{b} are conjugate by an element $C(x, y) \in \mathrm{SL}_2(\mathbb{K})$ if and only if $\mathrm{bir}(\mathfrak{a}, \mathfrak{b})$ belongs to the subgroup of norms $\mathrm{Nr}_{\mathbb{K}} \mathbb{K}[\sqrt{\delta}] \subset \mathbb{K}^\times$ of the quadratic extension, and by an element $C(x, 0) \in \mathrm{SL}_2(\mathbb{K}) \cap \mathbb{K}[\{\mathfrak{a}, \mathfrak{b}\}]$ if and only if $\mathrm{bir}(\mathfrak{a}, \mathfrak{b})$ belongs to the subgroup of squares $(\mathbb{K}^\times)^2 \subset \mathbb{K}^\times$.

The proofs of these statements can be reduced to elementary linear algebra once we thoroughly understand the geometry of the Lie algebra $\mathfrak{sl}_2(\mathbb{K})$ inside the quaternion algebra $\mathfrak{gl}_2(\mathbb{K})$. In short, commutativity rhymes with colinearity whereas anti-commutativity rhymes with orthogonality.

We recall this background material in the first two sections and provide an amusing application in the third to prove an analogue of Ptolemy’s identity for quadrilaterals inscribed in the isotropic cone \mathbb{X} of $(\mathfrak{sl}_2(\mathbb{K}), \det)$, relying on a natural quadratic desingularisation $\psi: \mathbb{K}^2 \rightarrow \mathbb{X}$.

Classes of binary quadratic forms. By polarizing a binary quadratic form on \mathbb{K}^2 with respect to the canonical symplectic form \det , we obtain an isomorphism:

$$Q = lx^2 + mxy + ry^2 \in \mathcal{Q}(\mathbb{K}^2) \quad \xleftrightarrow{Q(v)=\det(v, qv)} \quad \mathfrak{q} = \frac{1}{2} \begin{pmatrix} -m & -2r \\ 2l & m \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{K})$$

between the Poisson algebra $(\mathcal{Q}(\mathbb{K}^2), \mathrm{disc})$ and the Lie algebra $(\mathfrak{sl}_2(\mathbb{K}), -4\det)$, conjugating the actions of $\mathrm{PSL}_2(\mathbb{K})$ by change of variables and by conjugacy. After interpreting the values of quadratic forms as the scalar products with elements in the isotropic cone $Q(v) = \langle \mathfrak{q}, \psi(v) \rangle$, and computing that the products $Q_a(u)Q_b(v) = \langle \mathfrak{a}, \psi(u) \rangle \langle \mathfrak{b}, \psi(v) \rangle$ for primitive vectors $u, v \in \mathbb{K}^2$ are equivalent to the cross-ratio $\mathrm{bir}(Q_a, Q_b) = \mathrm{bir}(\mathfrak{a}, \mathfrak{b})$ in $\mathbb{K}^\times / \mathrm{Nr}(\mathbb{K}[\sqrt{\Delta}]^\times)$, we will deduce the following.

Proposition 1.3. *The set $\mathrm{Cl}_{\mathbb{K}}(\Delta)$ of $\mathrm{PSL}_2(\mathbb{K})$ -orbits in $\mathcal{Q}(\mathbb{K}^2)$ with non-square discriminant Δ embeds into the group $\mathbb{K}^\times / \mathrm{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\Delta}]^\times)$ of exponent two, by sending the class of the norm $x^2 - \frac{\Delta}{4}y^2$ of the \mathbb{K} -extension $\mathbb{K}[\sqrt{\Delta}]$ to the identity, and using the multiplication of values for composition.*

The motivation was to understand the space $\mathcal{Q}(\mathbb{Z}^2)$ of integral binary quadratic forms $Q(x, y) = lx^2 + mxy + ry^2$ up to change of variables by $\mathrm{PSL}_2(\mathbb{Z})$, and the class groups $\mathrm{Cl}(\Delta)$ of primitive classes with non-square discriminant $\Delta = m^2 - 4lr \in \mathbb{Z}$ introduced by Gauss in [7]. We refer to [3, 5] and [15] for the relevant background and history.

For a field \mathbb{K} of characteristic $\neq 2$, the extension of scalars $\mathbb{Z} \rightarrow \mathbb{K}$ induces a map $\mathcal{Q}(\mathbb{Z}^2) \rightarrow \mathcal{Q}(\mathbb{K}^2)$, yielding a group morphism $\mathrm{Cl}(\Delta) \rightarrow \mathrm{Cl}_{\mathbb{K}}(\Delta)$. We say that $Q_a, Q_b \in \mathcal{Q}(\mathbb{Z}^2)$ are \mathbb{K} -equivalent when they are conjugate by $C \in \mathrm{PSL}_2(\mathbb{K})$. When $\mathbb{K} \supset \mathbb{Q}$ this implies that they have the same discriminant (not just modulo $(\mathbb{K}^\times)^2$), and Theorem 1.2 and Proposition 1.3 show that their \mathbb{K} -equivalence is measured by $\mathrm{bir}(Q_a, Q_b) \equiv Q_a(1, 0)Q_b(1, 0) = l_a l_b \in \mathbb{K}^\times / \mathrm{Nr}(\mathbb{K}[\sqrt{\Delta}]^\times)$.

Thus, when $\mathbb{K} = \mathbb{C}$ this groups the $\mathrm{PSL}_2(\mathbb{Z})$ -classes of $\mathcal{Q}(\mathbb{Z}^2)$ according to their discriminant Δ , and as \mathbb{K} decreases we obtain finer partitions of the class groups $\mathrm{Cl}(\Delta)$ into \mathbb{K} -classes. In section 6 we provide a computable characterisation of \mathbb{Q} -equivalence in terms of the Hilbert symbols $(\delta, \chi)_p$ at all primes $p \in \mathbb{Z}$, which measures the obstruction to solving the equation $x^2 - \delta y^2 = \chi$ in \mathbb{Q}_p .

We also deduce from Theorem 1.2 a relation between the partition of $\mathrm{Cl}(\Delta)$ into \mathbb{Q} -classes and its partition into genera, which are given by the cosets $\mathrm{Cl}(\Delta) / \mathrm{Cl}(\Delta)^2$ modulo the subgroup of squares.

Theorem 1.4. *For non-square discriminants, genus equivalence implies \mathbb{Q} -equivalence. If the discriminant is fundamental then genus equivalence is implied by \mathbb{Q} -equivalence.*

Arithmetic equivalence of singular moduli & modular geodesics. We conclude with a geometric interpretation of \mathbb{K} -equivalence, which one may compare with [11]. The modular group $\mathrm{PSL}_2(\mathbb{Z})$ acts on the upper-half plane $\mathbb{H}\mathbb{P} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by linear fractional transformations, and the quotient is the modular orbifold $\mathbb{M} = \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathbb{H}\mathbb{P}$.

Consider primitive $Q_a, Q_b \in \mathcal{Q}(\mathbb{Z}^2)$ with non-square discriminant Δ , and denote $(\alpha', \alpha), (\beta', \beta)$ their roots (which one may order up to simultaneous inversion).

If $\Delta > 0$, then Q_a and Q_b are uniquely determined by $\alpha, \beta \in \mathbb{H}\mathbb{P}$, and their $\mathrm{PSL}_2(\mathbb{Z})$ -classes correspond to points $[\alpha], [\beta] \in \mathbb{M}$, called singular moduli.

Corollary 1.5. *Complex irrationals $\alpha, \beta \in \mathbb{Q}(\sqrt{\Delta})$ are \mathbb{K} -equivalent if and only if there exists a geodesic arc in \mathbb{M} from $[\alpha]$ to $[\beta]$ whose length λ is of the form $(\cosh \frac{\lambda}{2})^2 = \frac{1}{(2x)^2 - \Delta y^2}$ for $x, y \in \mathbb{K}$, in which case all geodesic arcs from $[\alpha]$ to $[\beta]$ have this property.*

If $\Delta < 0$ then Q_a and Q_b correspond to the oriented geodesics $(\alpha', \alpha), (\beta', \beta)$ in $\mathbb{H}\mathbb{P}$ and their $\mathrm{PSL}_2(\mathbb{Z})$ -classes correspond to primitive closed oriented geodesics in \mathbb{M} , called modular geodesics.

Corollary 1.6. *Two modular geodesics of the same length $2 \sinh^{-1}(\sqrt{\Delta}/2)$ are \mathbb{K} -equivalent if and only if one of the following equivalent conditions hold:*

- θ *There exists one intersection point with angle $\theta \in]0, \pi[$ such that $(\cos \frac{\theta}{2})^2 = \frac{1}{(2x)^2 - \Delta y^2}$ for $x, y \in \mathbb{K}$, in which case all intersections have this property.*
- λ *There exists one co-oriented ortho-geodesic of length λ such that $(\cosh \frac{\lambda}{2})^2 = \frac{1}{(2x)^2 - \Delta y^2}$ for $x, y \in \mathbb{K}$, in which case all such ortho-geodesics have this property.*

In conclusion, the \mathbb{Q} -equivalence is measured by the geometric quantities $(\cos \frac{\theta}{2})^2$ or $(\cosh \frac{\lambda}{2})^2$ as elements in $\mathbb{Q}^\times \bmod \mathrm{Nr}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{\Delta}))$, and their multiplication implies a geometric interpretation for the multiplication of genera.

2. Geometric algebra of $\mathfrak{gl}_2(\mathbb{K})$

Fix a field \mathbb{K} of characteristic different from 2 and a \mathbb{K} -vector space \mathbb{V} of dimension 2.

Involutive algebra. The \mathbb{K} -algebra $\mathfrak{gl}(\mathbb{V})$ of linear endomorphisms of \mathbb{V} is isomorphic to $\mathbb{V} \otimes \mathbb{V}^*$ with product defined by $(u \otimes \mu) \cdot (v \otimes \nu) = u \otimes \mu(v)\nu$. It is endowed with the canonical linear form $\text{Tr}: \mathfrak{gl}(\mathbb{V}) \rightarrow \mathbb{K}$ defined by $\text{Tr}(u \otimes \mu) = \mu(u)$. Let us find a canonical *involution* $M \mapsto M^\#$ on $\mathfrak{gl}(\mathbb{V})$, that is an anti-commutative linear endomorphism of order two, to deduce a canonical non-degenerate bilinear form $(M, N) \mapsto \text{Tr}(MN^\#)$ isomorphic to the pairing $\mathfrak{gl}(\mathbb{V}) \times \mathfrak{gl}(\mathbb{V})^* \rightarrow \mathbb{K}$.

A non-degenerate bilinear form $\omega: \mathbb{V} \times \mathbb{V} \rightarrow \mathbb{K}$ is equivalent to an isomorphism $\omega^*: \mathbb{V} \rightarrow \mathbb{V}^*$. Its associated adjoint involution $\#: \mathfrak{gl}(\mathbb{V}) \rightarrow \mathfrak{gl}(\mathbb{V})$ is the composition of $(\omega^*) \otimes (\omega^*)^{-1}: \mathbb{V} \otimes \mathbb{V}^* \rightarrow \mathbb{V}^* \otimes \mathbb{V}$ with the canonical map switching factors, thus $\#: u \otimes \mu \mapsto (\omega^*)^{-1}(\mu) \otimes \omega^*(u)$. Observe that $\#$ only depends on ω up to scaling. The plane \mathbb{V} admits a unique non-degenerate anti-symmetric bilinear form ω up to scaling as $\Lambda^2 \mathbb{V}^* \simeq \mathbb{K}$, and this defines our canonical involution $\#$.

Only after choosing a basis of \mathbb{V} do we have the identifications $\mathbb{V} = \mathbb{K}^2$ and $\mathfrak{gl}(\mathbb{V}) = \mathfrak{gl}_2(\mathbb{K})$. Then $\omega(u, v) = \det(u, v)$ and the associated adjoint involution on $\mathfrak{gl}_2(\mathbb{K})$ is the transpose-comatrix:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto M^\# = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

The fixed subalgebra of $M \mapsto M^\#$ is reduced to the center $\mathbb{K}\mathbf{1}$ of $\mathfrak{gl}(\mathbb{V})$. Composing $(M, M^\#)$ with addition or multiplication yields the central elements:

$$\text{Tr}(M)\mathbf{1} := M + M^\# \quad \text{and} \quad \det(M)\mathbf{1} := M \times M^\#$$

which recovers the linear *trace* map $\text{Tr}: \mathfrak{gl}(\mathbb{V}) \rightarrow \mathbb{K}$, and defines the multiplicative *determinant* map $\det: \mathfrak{gl}(\mathbb{V}) \rightarrow \mathbb{K}$. The involution $\#$ preserves the group $\text{GL}(\mathbb{V})$ of invertible elements, which consists in those $A \in \mathfrak{gl}(\mathbb{V})$ such that $\det(A) \in \mathbb{K}^\times$, in which case $A^{-1} = \det(A)^{-1} A^\#$.

For $A \in \text{GL}(\mathbb{V})$ and $M \in \mathfrak{gl}(\mathbb{V})$ we have $(AMA^{-1})^\# = AM^\#A^{-1}$, so the left adjoint linear action of $\text{GL}(\mathbb{V})$ on $\mathfrak{gl}(\mathbb{V})$ preserves the involution, whence all the structures which will follow.

The kernel $\text{SL}(\mathbb{V})$ of the determinant morphism $\det: \text{GL}(\mathbb{V}) \rightarrow \mathbb{K}^\times$ is called the subgroup of units, thus $A \in \text{SL}(\mathbb{V}) \iff \det(A) = 1 \iff A^\# = A^{-1}$. The kernel $\mathfrak{sl}(\mathbb{V})$ of the trace form is the anti-symmetric part for the involution, thus $a \in \mathfrak{sl}(\mathbb{V}) \iff \text{Tr}(a) = 0 \iff a^\# = -a$.

Quadratic space. On the vector space $\mathfrak{gl}(\mathbb{V})$, the determinant defines a non-degenerate quadratic form, and as $\det(M+N)\mathbf{1} = (M+N)(M+N)^\# = (\det(M) + \text{Tr}(MN^\#) + \det(N))\mathbf{1}$, its polar symmetric bilinear form is

$$\langle M, N \rangle = \text{tr}(MN^\#) \quad \text{where} \quad \text{tr}(P) := \frac{1}{2} \text{Tr}(P).$$

The involution $\#$ has eigenvalues ± 1 and its eigenspaces provide a decomposition

$$\mathfrak{gl}(\mathbb{V}) = \mathbb{K}\mathbf{1} \oplus \mathfrak{sl}(\mathbb{V})$$

which is orthogonal with respect to the determinant form. Thus every $M \in \mathfrak{gl}(\mathbb{V})$ splits as the sum of its symmetric and anti-symmetric parts with respect to the involution:

$$M = \text{tr}(M)\mathbf{1} + \text{pr}(M), \quad \text{where} \quad \text{tr}(M)\mathbf{1} = \frac{M+M^\#}{2} \quad \text{and} \quad \text{pr}(M) := \frac{M-M^\#}{2}.$$

In particular $\det(M)\mathbf{1} = \text{tr}(M)^2\mathbf{1} - \text{pr}(M)^2$ which we may write $\det = \text{tr}^2 - \text{pr}^2$.

The 4-dimensional space $\mathfrak{gl}(\mathbb{V})$, which contains the isotropic cone $\mathfrak{gl}(\mathbb{V}) \setminus \text{GL}(\mathbb{V})$ defined by $\det(M) = \langle M, M \rangle = 0$, decomposes as the direct sum of the anisotropic line $\mathbb{K}\mathbf{1}$

and its orthogonal hyperplane $\mathfrak{sl}(\mathbb{V})$ defined by $\mathrm{tr}(M) = \langle \mathbf{1}, M \rangle = 0$. Denote by \mathbb{X} the isotropic cone for the determinant restricted to the kernel $\mathfrak{sl}(\mathbb{V})$ of the trace:

$$\mathbb{X} = \{M \in \mathfrak{gl}(\mathbb{V}) \mid \langle \mathbf{1}, M \rangle = 0 = \langle M, M \rangle\} = \{\mathfrak{a} \in \mathfrak{sl}(\mathbb{V}) \mid \det(\mathfrak{a}) = 0\}.$$

Discriminant. The relation $M^2 - (M + M^\#)M + (MM^\#) = 0$ yields the Cayley–Hamilton identity $\chi_M(M) = 0$ for $X^2 - \mathrm{Tr}(M)X + \det(M) \in \mathbb{K}[X]$ the *characteristic polynomial* of M . Hence a non-central element $M \in \mathfrak{gl}_2(\mathbb{K}) \setminus \mathbb{K}\mathbf{1}$ generates a commutative subalgebra $\mathbb{K}[M] = \mathrm{Span}(\mathbf{1}, M)$ of dimension 2, which is isomorphic to the quadratic extension $\mathbb{K}[X]/(\chi_M)$ of \mathbb{K} with Galois involution given by the restriction of the involution $\#$.

The discriminant of $M \in \mathfrak{gl}(\mathbb{V})$ is defined as that of its characteristic polynomial, equal to

$$\mathrm{disc}(M) = \mathrm{Tr}(M)^2 - 4\det(M).$$

In particular $\mathrm{disc}(A) = \mathrm{Tr}(A)^2 - 4$ for $A \in \mathrm{SL}(\mathbb{V})$ and $\mathrm{disc}(\mathfrak{a}) = -4\det(\mathfrak{a})$ for $\mathfrak{a} \in \mathfrak{sl}(\mathbb{V})$.

We call $M \in \mathfrak{gl}(\mathbb{V})$ *semi-simple* when $\mathrm{disc}(M) \neq 0$, that is when χ_M has simple roots in its splitting field. If these roots belong to \mathbb{K} then $\mathbb{K}[M]$ is isomorphic to the direct product $\mathbb{K} \times \mathbb{K}$, otherwise $\mathbb{K}[M]$ is a simple \mathbb{K} -algebra (no proper ideals). In both cases $\mathbb{K}[M]$ is a semi-simple \mathbb{K} -algebra (a product of simple algebras). When $\mathrm{disc}(M) = 0$ we have $\chi_M(X) = (X - \lambda)^2$ for $\lambda \in \mathbb{K}$ so the algebra $\mathbb{K}[M]$ is not integral (it has zero divisors) as $M - \lambda\mathbf{1}$ is nilpotent.

The discriminant is preserved under the projection $\mathrm{disc}(M) = \mathrm{disc}(\mathrm{pr} M)$, so an element is semi-simple if and only if its projection in $\mathfrak{sl}(\mathbb{V})$ lies outside the cone \mathbb{X} .

Projectivisation. In the projective 3-space $\mathbb{P}(\mathfrak{gl}(\mathbb{V}))$, the point $\mathbb{P}(\mathbb{K}\mathbf{1})$ and the plane $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$ are mutually polar with respect the non-degenerate quadric $\mathbb{P}(\mathfrak{gl}(\mathbb{V})) \setminus \mathrm{PGL}(\mathbb{V})$. The point lies off the quadric and its polar plane intersects the quadric transversely along the non-degenerate conic $\mathbb{P}(\mathbb{X})$. Geometrically, the conic $\mathbb{P}(\mathbb{X})$ consists in the set of tangency points between the quadric $\mathbb{P}(\{\det = 0\})$ and the pencil of lines through $\mathbb{P}(\mathbf{1})$.

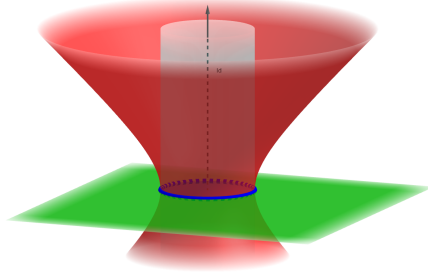


FIGURE 1. The quadric $\mathbb{P}(\{\det = 0\})$ in $\mathbb{P}(\mathrm{GL}(\mathbb{V}))$. The point $\mathbb{P}(\mathbf{1})$ lies off the quadric and its polar plane $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$ intersects the quadric in the conic $\mathbb{P}(\mathbb{X})$.

Over \mathbb{K} , the isomorphism types of the quadric $\mathbb{P}(\{\det = 0\})$ and of the conic $\mathbb{P}(\mathbb{X})$ are given, in terms of the classes in $\mathbb{K}^\times/(\mathbb{K}^\times)^2$ of the diagonal elements appearing in the diagonalisation of the quadratic form \det , by $\{1, -1, 1, -1\}$ and $\{-1, 1, -1\}$.

Lemma 2.1 (Equivariant ruling of the quadric). *The map $\Psi: M \mapsto (\ker M, \mathrm{im} M)$ defines a bijective algebraic correspondence between the projective quadric $\mathbb{P}(\{\det = 0\})$ and $\mathbb{P}(\mathbb{V}) \times \mathbb{P}(\mathbb{V})$ sending the projective conic $\mathbb{P}(\mathbb{X})$ to the diagonal $\mathbb{P}(\mathbb{V})$. The map Ψ conjugates the adjoint action of $\mathrm{PGL}(\mathbb{V})$ restricted to $\mathbb{P}(\{\det = 0\})$ with its tautological diagonal action on $\mathbb{P}(\mathbb{V}) \times \mathbb{P}(\mathbb{V})$.*

Recall that the action of $\mathrm{PGL}(\mathbb{V})$ on $\mathbb{P}(\mathbb{V})$ is simply-transitive on triples of distinct lines. For a symplectic form ω on \mathbb{V} , we define the Maslov index of such a triple $x_1, x_2, x_3 \in \mathbb{P}(\mathbb{V})$ as the element $\omega(\vec{x}_1, \vec{x}_2) \in \mathbb{K}^\times / (\mathbb{K}^\times)^2$ where the three vectors $\vec{x}_i \in x_i \subset \mathbb{V}$ sum up to zero. The level sets of the Maslov index do not depend on the choice of ω . One may show [13, Proposition 1.39] that the action of $\mathrm{PSL}(\mathbb{V})$ on $\mathbb{P}(\mathbb{V})$ is simply-transitive on triples of distinct lines with a given Maslov index.

3. The Lie algebra $\mathfrak{sl}_2(\mathbb{K})$

Orthogonality & colinearity. The associative algebra $\mathfrak{gl}(\mathbb{V})$ inherits the structure of a Lie algebra by taking (half of) the commutator:

$$\{M, N\} = \frac{1}{2}(MN - NM)$$

and as $\{M, N\} = \{\mathrm{pr} M, \mathrm{pr} N\}$ we may quotient by its center $\mathbb{K}\mathbf{1}$ to find a Lie bracket on $\mathfrak{sl}(\mathbb{V})$. From a geometric perspective, the kernel $\mathfrak{sl}(\mathbb{V})$ of the trace form is a 3-dimensional Lie algebra, that of the Lie group $\mathrm{SL}(\mathbb{V})$, kernel of the determinant morphism.

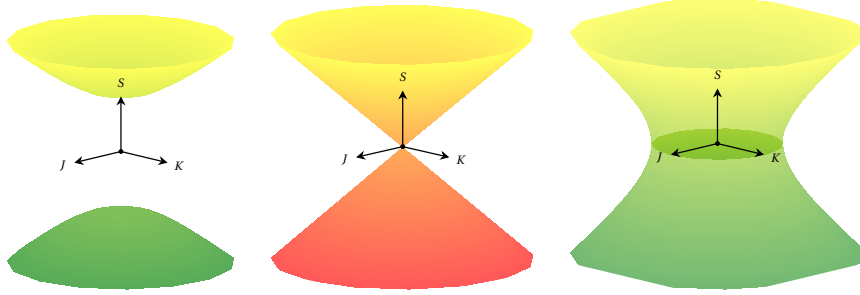


FIGURE 2. The level surfaces 1, 0, -1 of \det in $\mathfrak{sl}_2(\mathbb{Q})$.

From now on we will focus on the geometry of $\mathfrak{sl}(\mathbb{V})$ with the restricted scalar product $\langle a, b \rangle$ and Lie bracket $\{a, b\}$. For $a, b \in \mathfrak{sl}(\mathbb{V})$, the decomposition $ab = \mathrm{tr}(ab)\mathbf{1} + \mathrm{pr}(ab)$ rewrites as

$$ab = -\langle a, b \rangle \mathbf{1} + \{a, b\}$$

thus a, b are orthogonal if and only if they anti-commute, in which case $\{a, b\} = ab$. The Jacobi relation implies that $\{a, b\} \perp \mathrm{Span}(a, b)$ for all $a, b \in \mathfrak{sl}(\mathbb{V})$. (Following [1, 9], this yields a geometric interpretation of the Jacobi relation as the orthocenter theorem for triangles in $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$.)

The Killing form associated to the bracket is proportional to the scalar product:

$$-\frac{1}{8} \mathrm{Tr}(c \mapsto 2\{a, 2\{b, c\}\}) = -\mathrm{tr}(c \mapsto \{a, \{b, c\}\}) = -\mathrm{tr}(ab) = \mathrm{tr}(ab^\#) = \langle a, b \rangle.$$

The non-degeneracy of the Killing form implies that of the Lie bracket. It also implies that a, b are colinear if and only if $\{a, b\} = 0$. Hence the quantity $[a, b, c] := \langle \{a, b\}, c \rangle = \frac{1}{2}(\mathrm{tr}(bac) - \mathrm{tr}(abc))$ defines a volume form on $\mathfrak{sl}(\mathbb{V})$, that is an alternate non-degenerate trilinear form over \mathbb{K} .

When $a, b \in \mathfrak{sl}(\mathbb{V})$ are not colinear, they span the plane $\mathrm{Span}(a, b) = \{a, b\}^\perp$. In the projective plane $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$ the line through the distinct points $\mathbb{P}(a), \mathbb{P}(b)$ is polar to the point $\mathbb{P}(\{a, b\})$ with respect to the conic $\mathbb{P}(\mathbb{X})$. Their relative position with respect to the conic is given by the discriminant $\mathrm{disc}\{a, b\} \in \mathbb{K} / (\mathbb{K}^\times)^2$ of the quadratic form \det restricted to the plane $\mathrm{Span}(a, b)$.

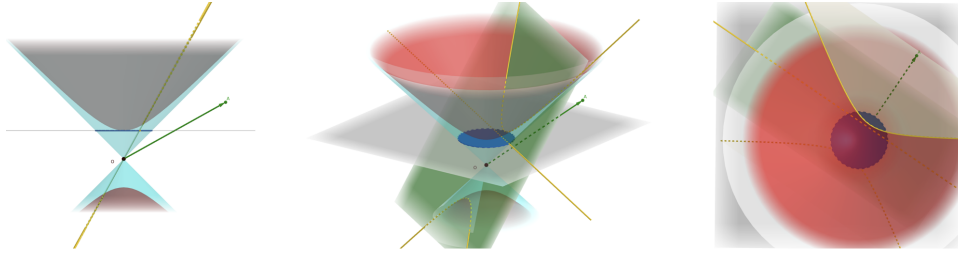


FIGURE 3. The projectivisation $\mathbb{P}: \mathfrak{sl}_2(\mathbb{Q}) \rightarrow \mathbb{Q}\mathbb{P}^2$ sends an orthogonal pair (a, a^\perp) to a polar pair (here $a \notin \mathbb{X}$ so a^\perp is not tangent to \mathbb{X}).

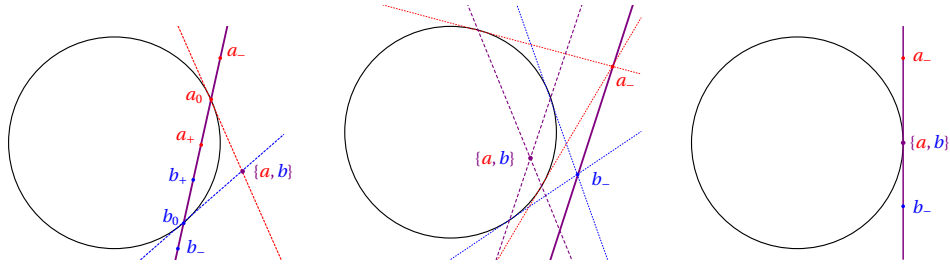


FIGURE 4. In the projective plane $\mathbb{P}(\mathfrak{sl}_2(\mathbb{Q}))$ with the conic $\mathbb{P}(\mathbb{X})$: various configurations of the line $(\mathbb{P}(a), \mathbb{P}(b))$ and its pole $\mathbb{P}(\{a, b\})$.

Subalgebras & commutants. Enlarges Figures 3 and 4. Elements $a, b \in \mathfrak{sl}(\mathbb{V})$ generate an associative subalgebra $(\mathbb{K}[a, b], \cdot)$ of $(\mathfrak{gl}(\mathbb{V}), \cdot)$ and generate a Lie subalgebra $(\mathcal{L}(a, b), \{\cdot, \cdot\})$ of $(\mathfrak{sl}(\mathbb{V}), \{\cdot, \cdot\})$. Since the Lie bracket equals half the commutator of the associative product, we clearly have $\mathbb{K}[a, b] \supset \mathbb{K}1 \oplus \mathcal{L}(a, b)$.

Proposition 3.1 (Subalgebras). *Let $a, b \in \mathfrak{sl}(\mathbb{V})$. In terms of the underlying vector spaces we have $\mathbb{K}[a, b] = \mathbb{K}1 \oplus \mathcal{L}(a, b)$ and $\mathcal{L}(a, b) = \mathrm{Span}(a, b, \{a, b\})$.*

There are four possibilities for the isomorphism type of $\mathcal{L}(a, b)$ given by the relative position of $a, b, \{a, b\}$ with respect to the isotropic cone $\mathbb{X} \subset \mathfrak{sl}(\mathbb{V})$, as follows.

0. If $a = 0 = b$, then $\mathcal{L}(a, b) = \{0\}$.
1. If $\{a, b\} = 0$ but $\det(a) \neq 0$ then $\mathcal{L}(a, b)$ is the abelian Lie algebra of $\dim = 1$.
2. If $\{a, b\} \neq 0$ but $\det\{a, b\} = 0$ then $\mathcal{L}(a, b)$ is the affine Lie algebra of $\dim = 2$.
3. If $\det\{a, b\} \neq 0$ then $\mathcal{L}(a, b) = \mathfrak{sl}(\mathbb{V})$.

Over every field \mathbb{K} of characteristic different from 2, each of these cases can be realised by choosing a, b appropriately.

The previous Proposition could have been formulated for $M, N \in \mathfrak{gl}(\mathbb{V})$, since they generate the same associative and Lie algebras as their projections $a, b \in \mathfrak{sl}(\mathbb{V})$.

Proposition 3.2 (Commutants). *Consider the adjoint actions of the groups $\mathrm{GL}(\mathbb{V})$ and $\mathrm{SL}(\mathbb{V})$ on the space $\mathfrak{sl}(\mathbb{V})$ and its projectivisation $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$. Let $p \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$.*

The stabilizer of p under $\mathrm{GL}(\mathbb{V})$ is $(\mathbb{K}[p])^\times$, that is the complement of the degenerate conic $x^2 + y^2 \det(p) = 0$ in the plane $\mathbb{K}[p] = \{x1 + yp\}$.

The stabilizer of p under $\mathrm{SL}(\mathbb{V})$ is $(\mathbb{K}[p])^\times \cap \mathrm{SL}(\mathbb{V})$, that is the conic $x^2 + y^2 \det(p) = 1$ in the plane $\mathbb{K}[p] = \{x1 + yp\}$, which is non-degenerate except when $p \in \mathbb{X}$.

The stabiliser of $\mathbb{P}(p)$ under $\mathrm{GL}(\mathbb{V})$ is the $\mathbb{Z}/2$ -graded subgroup $(\mathbb{K}[p])^\times \sqcup (\mathbb{K}[p]^\perp)^\times$ formed by the union of the complements of two degenerate conics.

The stabiliser of $\mathbb{P}(p)$ under $\mathrm{SL}(\mathbb{V})$ is the $\mathbb{Z}/2$ -graded subgroup $(\mathbb{K}[p] \cap \mathrm{SL}(\mathbb{V})) \sqcup (\mathbb{K}[p]^\perp \cap \mathrm{SL}(\mathbb{V}))$ formed by the union of two non-degenerate conics isomorphic to $x^2 + y^2 \det(p) = \pm 1$.

(The conic $\mathbb{K}[p]^\perp \cap \mathrm{SL}(\mathbb{V})$ is isomorphic to $x^2 + y^2 \det(p) = -1$ but does not have a privileged parameterisation and may have no \mathbb{K} -points.)

Proof. For $C \in \mathrm{GL}(\mathbb{V})$, if CpC^{-1} is proportional to p , then either it equals $+p$ in which case $\langle \mathrm{pr} C, p \rangle = 0$ and $C \in \mathbb{K}[p]$, or else it equals $-p$ in which case $\langle \mathrm{pr} C, p \rangle = 0$ and $\mathrm{pr} C \in \mathbb{K}[p]^\perp$. Recall that the quadratic space $(\mathfrak{gl}(\mathbb{V}), \det)$ is isomorphic to a sum of two hyperbolic planes. Hence the restrictions of \det to the summands of the decomposition $\mathfrak{gl}(\mathbb{V}) = \mathbb{K}[p] \oplus \mathbb{K}[p]^\perp$ must have opposite Witt classes, and the former is $(1, \det(p))$ so the latter is equivalent to $(-1, -\det(p))$. \square

We refer to [13, 1.28] for analogous descriptions of the stabilizers of $p \in \mathbb{X} \setminus \{0\}$.

Cosine and cross-ratio. For $\mathfrak{a} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$, choose a square root of $\delta := -\det(\mathfrak{a})$ and extend the scalars to the field $\mathbb{K}' = \mathbb{K}[\sqrt{\delta}]$. The tautological action of \mathfrak{a} on the plane \mathbb{K}'^2 has two eigendirections for the eigenvalues $\pm\sqrt{\delta}$. These lines are mapped by $\Psi \otimes \mathbb{K}'$ to the intersection of the cone $\mathbb{X} \otimes \mathbb{K}'$ with the orthogonal plane \mathfrak{a}^\perp . We deduce an ordered pair of points $\alpha', \alpha \in \mathbb{K}'\mathbb{P}^1$.

We may now define and relate the cosine $\cos(\mathfrak{a}, \mathfrak{b})$ and cross-ratio $\mathrm{bir}(\mathfrak{a}, \mathfrak{b})$ of $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$. These equivalent quantities, together with the discriminants $\mathrm{disc}(\mathfrak{a})$ and $\mathrm{disc}(\mathfrak{b})$, are the only $\mathrm{PGL}(\mathbb{V})$ -invariants for a pair of elements in $\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$.

Lemma 3.3. For $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$, if we choose a square root of $\det(\mathfrak{a}\mathfrak{b})$ then we may define their cosine $\cos(\mathfrak{a}, \mathfrak{b}) \in \mathbb{K}[\sqrt{\det(\mathfrak{a}\mathfrak{b})}]$ by

$$\cos(\mathfrak{a}, \mathfrak{b}) := \frac{\langle \mathfrak{a}, \mathfrak{b} \rangle}{\sqrt{\langle \mathfrak{a}, \mathfrak{a} \rangle \langle \mathfrak{b}, \mathfrak{b} \rangle}} = \frac{-\frac{1}{2} \mathrm{Tr}(\mathfrak{a}\mathfrak{b})}{\sqrt{\det(\mathfrak{a}\mathfrak{b})}}$$

and we may order their polar points $\mathbb{P}(\mathfrak{a}^\perp \cap \mathbb{X}) = \{\alpha', \alpha\}$ and $\mathbb{P}(\mathfrak{b}^\perp \cap \mathbb{X}) = \{\beta', \beta\}$ up to simultaneous inversion, so as to define their cross-ratio $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \in \mathbb{K}[\sqrt{\det(\mathfrak{a}\mathfrak{b})}]$:

$$\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) := \mathrm{bir}(\alpha', \alpha; \beta', \beta) = \frac{(\alpha - \alpha')(\beta - \beta')}{(\alpha - \beta')(\beta - \alpha')}$$

For a same choice of $\sqrt{\det(\mathfrak{a}\mathfrak{b})}$, these quantities are related by

$$\frac{1}{\mathrm{bir}(\mathfrak{a}, \mathfrak{b})} = \frac{1 + \cos(\mathfrak{a}, \mathfrak{b})}{2}.$$

Remark 3.4. When $\det(\mathfrak{a}) = \det(\mathfrak{b})$, this common value yields a canonical choice for $\sqrt{\det(\mathfrak{a}\mathfrak{b})}$.

Remark 3.5. For $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$: $\det\{\mathfrak{a}, \mathfrak{b}\} = 0 \iff \cos(\mathfrak{a}, \mathfrak{b})^2 = 1 \iff \mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \in \{1, \infty\}$.

4. Ptolemy's theorem for quadrilaterals inscribed in $\mathbb{P}(\mathbb{X})$

Parametrizing the cone. Choose a symplectic form ω on \mathbb{V} and consider the associated quadratic map $\psi: \mathbb{V} \rightarrow \mathfrak{gl}(\mathbb{V})$ given by $\psi(v) = -v \otimes \omega^*(v) = \omega(\cdot, v)v$. Thus $\psi(v)$ is nilpotent with image $\mathbb{K}v$. Consequently, $\psi(u)\psi(v) \in \mathfrak{gl}(\mathbb{V})$ equals $-\omega(u, v)^2$ times the projection on $\mathbb{K}u$ parallel to $\mathbb{K}v$, whence $\{\psi(u), \psi(v)\} \in \mathfrak{sl}(\mathbb{V})$ equals $-\omega(u, v)^2$ times the symmetry with respect $\mathbb{K}u$ parallel to $\mathbb{K}v$.

A symplectic basis of (\mathbb{V}, ω) is a pair $(u, v) \in \mathbb{V} \times \mathbb{V}$ such that $\omega(u, v) = 1$. Denote by $S_{u,v} \in \mathrm{GL}(\mathbb{V})$ the unique element of order 4 sending u to v , and by $\mathbb{H}_\omega \subset \mathrm{SL}(\mathbb{V}) \cap \mathfrak{sl}(\mathbb{V})$ the set of such $S_{u,v}$. Let \mathbb{X}_ω be the set of elements $p \in \mathbb{X}$ such that there exists $S_{u,v} \in \mathbb{H}_\omega$

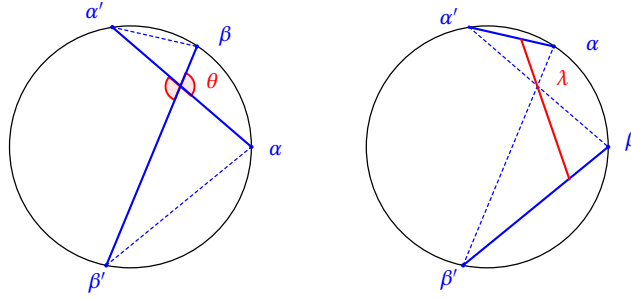


FIGURE 5. Angle at intersection $\frac{1}{\mathrm{bir}(\alpha', \alpha, \beta', \beta)} = \left(\cos \frac{\theta}{2}\right)^2$. Length of ortho-geodesic $\frac{1}{\mathrm{bir}(\alpha', \alpha, \beta', \beta)} = \left(\cosh \frac{\lambda}{2}\right)^2$.

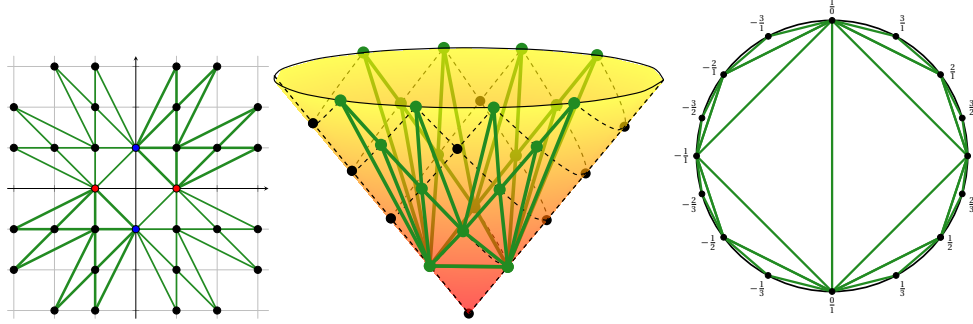


FIGURE 6. The quadratic map $\psi: \mathbb{Q}^2 \rightarrow \mathbb{X}$, and the isomorphism $\mathbb{P}(\psi): \mathbb{P}(\mathbb{Q}^2) \rightarrow \mathbb{P}(\mathbb{X})$ of projective lines. Consult [13, Chapter 2] for details about this construction.

for which the scalar product $\langle p, S_{u,v} \rangle$ is a sum of squares $x^2 + y^2$ of elements $x, y \in \mathbb{K}$ (in which case this is true for all $S_{u,v} \in \mathbb{H}_\omega$).

Lemma 4.1. *The quadratic map $\psi: \mathbb{V} \rightarrow \mathbb{X}$ has image \mathbb{X}_ω and is two-to-one outside the origin. It intertwines the tautological action of $\mathrm{SL}(\mathbb{V})$ on \mathbb{V} with the restriction of its adjoint action on \mathbb{X}_ω . For all $u, v \in \mathbb{V}$ we have $2\langle \psi(u), \psi(v) \rangle = \omega(u, v)^2$.*

We have $\mathbb{P}(\mathbb{X}_\omega) = \mathbb{P}(\mathbb{X})$ and the map $\mathbb{P}(\psi): \mathbb{P}(\mathbb{V}) = \mathbb{P}(\mathbb{X}_\omega)$ is an isomorphism of projective lines, inverse to the restriction of Ψ to $\mathbb{P}(\mathbb{X})$. For distinct $u, v, x, y \in \mathbb{X}_\omega$ we have:

$$\text{(CRS)} \quad \mathrm{bir}(u, v, x, y)^2 = \frac{\langle u, v \rangle \cdot \langle x, y \rangle}{\langle u, y \rangle \cdot \langle x, v \rangle}.$$

Proof. One may show that $\psi(\mathbb{V}) = \mathbb{X}_\omega$ and $\mathbb{P}(\mathbb{X}_\omega) = \mathbb{P}(\mathbb{X})$ by computing in a symplectic basis of \mathbb{V} . The last equality equals the cross-ratio of the four lines in \mathbb{V} generated by preimages of u, v, x, y , computed in terms of the area form, as in the image below. \square

$$\frac{XY}{XV} = \frac{\omega(\vec{x}, \vec{y})}{\omega(\vec{x}, \vec{v})} \quad \frac{UV}{UY} = \frac{\omega(\vec{u}, \vec{v})}{\omega(\vec{u}, \vec{y})}$$

Ptolemy's theorem for ideal quadrilaterals. We now apply the previous lemma to show the following analogue of Ptolemy's theorem for quadrilaterals inscribed in the projective conic $\mathbb{P}(\mathbb{X})$, which appeared in [10, Proposition 2.6]. It is better formulated if we fix a symplectic form ω on \mathbb{V} and consider vectors in the subset \mathbb{X}_ω of the isotropic cone \mathbb{X} . Since $\mathbb{P}(\mathbb{X}_\omega) = \mathbb{P}(\mathbb{X})$ we may always lift a quadrilateral to such a quadruple, and any lift will satisfy the identity.

Proposition 4.2. *For distinct $u, v, x, y \in \mathbb{X}_\omega$, the following identity holds in a quadratic extension of \mathbb{K} :*

$$(IPS) \quad \sqrt{\langle u, v \rangle \cdot \langle x, y \rangle} = \sqrt{\langle u, y \rangle \cdot \langle x, v \rangle} + \sqrt{\langle u, x \rangle \cdot \langle v, y \rangle}.$$

This formula is invariant under the action of $(\mathbb{K}^\times)^2$ by individual dilatation of u, v, x, y , so we may suppose they lie on a conic section $\{p \in \mathbb{X}_\omega \mid \langle S_{u,v}, p \rangle = 1\}$.

Proof. This identity is equivalent, after dividing by the left-hand side, to:

$$\sqrt{\frac{\langle u, v \rangle \cdot \langle x, y \rangle}{\langle u, y \rangle \cdot \langle x, v \rangle}} + \sqrt{\frac{\langle u, v \rangle \cdot \langle x, y \rangle}{\langle u, x \rangle \cdot \langle v, y \rangle}} = 1.$$

But this follows from the identity in the previous Lemma 4.1 and the addition rule of cross-ratios $\text{bir}(u, v, x, y)^{-1} + \text{bir}(u, v, y, x)^{-1} = 1$. \square

5. The adjoint actions of $\text{PGL}_2(\mathbb{K})$ and $\text{PSL}_2(\mathbb{K})$ on $\mathbb{P}(\mathfrak{sl}_2(\mathbb{K}))$

The isomorphism $\text{PGL}(\mathbb{V}) \rightarrow \text{SO}(\mathfrak{sl}(\mathbb{V}), \det)$. The left adjoint linear action of $\text{GL}(\mathbb{V})$ on $\mathfrak{gl}(\mathbb{V})$ preserves the involution whence every structure which derives from it, such as the determinant form and the orthogonal decomposition $\mathbb{K}\mathbf{1} \oplus \mathfrak{sl}(\mathbb{V})$. It also preserves the orientations of $\mathfrak{sl}(\mathbb{V})$ defined for a basis as the class of its determinant in $\mathbb{K}^\times / (\mathbb{K}^\times)^2$. Only the scalar matrices act trivially, and the maximal subspace on which the action is trivial equals $\mathbb{K}\mathbf{1}$. Therefore no information is lost after quotienting by these centers, and this yields a faithful representation $\text{PGL}(\mathbb{V}) \rightarrow \text{SO}(\mathfrak{sl}(\mathbb{V}), \det)$ into the group of orientation preserving isometries of $(\mathfrak{sl}(\mathbb{V}), \det)$.

Proposition 5.1. *The adjoint action yields an isomorphism $\text{PGL}(\mathbb{V}) \simeq \text{SO}(\mathfrak{sl}(\mathbb{V}), \det)$.*

Proof. To prove surjectivity, we use a theorem of Cartan–Dieudonné [6] stating that every isometry of a symmetric non-degenerate bilinear form over a d -dimensional \mathbb{K} -vector space is a product of at most d reflections. In particular, an element of $\text{SO}(\mathfrak{sl}_2(\mathbb{K}), \det)$ is a product of at most 3 reflections, but since it has determinant 1 it is in fact a product of exactly two reflections. Thus we must express all products of two reflections as the conjugacy by some element.

If $q \in \mathfrak{gl}(\mathbb{V})$ is not isotropic, that is $\det(q) \neq 0$, then the orthogonal reflection $\sigma_q \in \text{End}(\mathfrak{gl}(\mathbb{V}))$ of vector q across q^\perp is given by

$$\sigma_q(m) = m - 2 \frac{\langle q, m \rangle}{\langle q, q \rangle} \cdot q.$$

Notice that the orthogonal reflection of vector $\mathbf{1}$ across $\mathfrak{sl}(\mathbb{V})$ equals $\sigma_{\mathbf{1}} : m \mapsto -m^\#$. The endomorphism $\mu_q \in \text{End}(\mathfrak{gl}(\mathbb{V}))$ corresponding to left multiplication by q , left conjugates $\sigma_{\mathbf{1}}$ to σ_q . In formulae, we have $\mu_q : m \mapsto qm$ and $\sigma_q = \mu_q \circ \sigma_{\mathbf{1}} \circ \mu_q^{-1}$. Thus

$$\sigma_q(m) = -q(q^{-1}m)^\# = -\frac{qm^\#q}{\det(q)}.$$

Now restricting the attention to $\text{End}(\mathfrak{sl}(\mathbb{V}))$, we notice that for $q, m \in \mathfrak{sl}(\mathbb{V})$ this formula becomes $\sigma_q(m) = -qm q^{-1}$. Hence for $p, q \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$ the reflection $\sigma_p \circ \sigma_q \in \text{SO}(\mathfrak{sl}(\mathbb{V}), \det)$ coincides with the left adjoint action of $pq \in \text{GL}(\mathbb{V})$. \square

The adjoint action commutes with the projectivisation map $\mathfrak{sl}(\mathbb{V}) \rightarrow \mathbb{P}(\mathfrak{sl}(\mathbb{V}))$. This realizes $\mathrm{PGL}(\mathbb{V})$ as a subgroup inside the automorphism group $\mathrm{PGL}(\mathfrak{sl}(\mathbb{V}))$ of the projective plane $\mathbb{P}(\mathfrak{sl}(\mathbb{V}))$, namely the stabiliser of the non-degenerate conic $\mathbb{P}(\mathbb{X})$.

The description of the actions of $\mathrm{PGL}(\mathbb{V})$ and $\mathrm{PSL}(\mathbb{V})$ on $\mathbb{P}(\mathbb{X})$ follow from Lemma 2.1.

Symmetric space of $\mathrm{PGL}(\mathbb{V})$. We call *symmetry* of $\mathrm{PGL}(\mathbb{V})$ an element of order two (since it maps to an orthogonal symmetry in $\mathrm{SO}(\mathfrak{sl}(\mathbb{V}), \det)$). Those are represented by the elements in $\mathrm{GL}(\mathbb{V}) \cap \mathfrak{sl}(\mathbb{V}) = \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$, so the symmetries of $\mathrm{PGL}(\mathbb{V})$ correspond by the projectivisation map to the complement $\mathbb{P}(\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X})$ of the projective conic. This is an open projective variety whose irreducible components over \mathbb{K} are indexed by the values of $\det: \mathrm{GL}(\mathbb{V}) \cap \mathfrak{sl}(\mathbb{V}) \rightarrow \mathbb{K}^\times / (\mathbb{K}^\times)^2$. We call this variety $\mathbb{P}(\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X})$ the *symmetric space* of $\mathrm{PGL}(\mathbb{V})$, in the spirit of [2].

Hence the group $\mathrm{PGL}(\mathbb{V})$ acts on its symmetric space $\mathbb{P}(\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X})$ by the projectivised adjoint representation, and the elements of order two are the symmetries. Since $s \in \mathrm{GL}(\mathbb{V}) \cap \mathfrak{sl}(\mathbb{V})$ maps to an element of order two in $\mathrm{SO}(\mathfrak{sl}(\mathbb{V}), \det)$ which fixes the line $\mathbb{K}s$, it acts like minus the identity on the orthogonal plane s^\perp , thus corresponding to the orthogonal symmetry across the line $\mathbb{K}s$:

$$\forall x \in \mathfrak{sl}(\mathbb{V}) : \quad sx s^{-1} + x = 2 \frac{\langle s, x \rangle}{\langle s, s \rangle} \cdot s$$

and we recognise from the proof of Proposition 5.1 the expression for the composition of reflections $\sigma_s \circ \sigma_{\mathbf{1}} \in \mathrm{SO}(\mathfrak{gl}(\mathbb{V}), \det)$ restricted to $\mathfrak{sl}(\mathbb{V})$.

Action of $\mathrm{PGL}(\mathbb{V})$ on $\mathbb{P}(\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X})$. Let us begin with another corollary to Lemma 4.1, which describes the adjoint action of an element $C \in \mathrm{PSL}(\mathbb{V})$ on $\mathfrak{sl}(\mathbb{V})$.

Corollary 5.2. *For $C \in \mathrm{SL}(\mathbb{V})$, the adjoint action of C on $\mathfrak{sl}(\mathbb{V})$ restricted to the plane $(\mathrm{pr} C)^\perp$ is equivalent over \mathbb{K} to the tautological action of C^2 on \mathbb{V} .*

Proposition 5.3. *Consider distinct $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V})$ with determinant $d \neq 0$ and $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \neq \infty$. The quadratic subalgebra $\mathbb{K}\{\mathfrak{a}, \mathfrak{b}\}$ of $\mathfrak{gl}(\mathbb{V})$ contains a unique $M \in \mathrm{GL}(\mathbb{V})$ with $\mathrm{Tr}(M) = 2$ which conjugates \mathfrak{a} to \mathfrak{b} . It is given by*

$$M = \mathbf{1} + \frac{\mathrm{bir}(\mathfrak{a}, \mathfrak{b})}{2d} \cdot \{\mathfrak{a}, \mathfrak{b}\} = \frac{(d + \langle \mathfrak{a}, \mathfrak{b} \rangle) \mathbf{1} + \{\mathfrak{a}, \mathfrak{b}\}}{d + \langle \mathfrak{a}, \mathfrak{b} \rangle} \quad \text{and} \quad \det(M) = \mathrm{bir}(\mathfrak{a}, \mathfrak{b}).$$

Proof. First suppose $d = 1$, so $\mathfrak{a}, \mathfrak{b} \in \mathbb{H}$. For $x \in \mathbb{K}$, set $M = \mathbf{1} + x\{\mathfrak{a}, \mathfrak{b}\}$. Then we have $M\mathfrak{a} = \mathfrak{b}M \iff \mathfrak{a} + x\{\mathfrak{a}, \mathfrak{b}\}\mathfrak{a} = \mathfrak{b} + x\mathfrak{b}\{\mathfrak{a}, \mathfrak{b}\}$. But $\{\mathfrak{a}, \mathfrak{b}\}\mathfrak{a} = \frac{1}{2}(\mathfrak{a}\mathfrak{b}\mathfrak{a} + \mathfrak{b})$, and since $\mathfrak{a} \in \mathbb{H}$ acts like a symmetry across $\mathbb{K}\mathfrak{a}$, we have $\mathfrak{a}\mathfrak{b}\mathfrak{a} = -\mathfrak{a}\mathfrak{b}\mathfrak{a}^{-1} = \mathfrak{b} - 2\langle \mathfrak{a}, \mathfrak{b} \rangle \mathfrak{a}$ so $\{\mathfrak{a}, \mathfrak{b}\}\mathfrak{a} = \mathfrak{b} - \langle \mathfrak{a}, \mathfrak{b} \rangle \mathfrak{a}$. Similarly $\mathfrak{b}\{\mathfrak{a}, \mathfrak{b}\} = \mathfrak{a} - \langle \mathfrak{a}, \mathfrak{b} \rangle \mathfrak{b}$. Thus $M\mathfrak{a} = \mathfrak{b}M \iff (\mathfrak{a} - \mathfrak{b})(1 - x(1 + \langle \mathfrak{a}, \mathfrak{b} \rangle)) = 0 \iff 1 = x(1 + \langle \mathfrak{a}, \mathfrak{b} \rangle)$ since $\mathfrak{a} - \mathfrak{b} \neq 0$.

Now suppose $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}(\mathbb{V})$ have the same determinant $d \neq 0$. Divide them by \sqrt{d} , which may live in a quadratic extension \mathbb{K}' of \mathbb{K} , to get $\mathfrak{a}', \mathfrak{b}' \in \mathbb{H}$ as before with $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) = \mathrm{bir}(\mathfrak{a}', \mathfrak{b}')$. Since $\{\mathfrak{a}, \mathfrak{b}\}/d = \{\mathfrak{a}', \mathfrak{b}'\}$ we have $\mathbb{K}'\{\mathfrak{a}, \mathfrak{b}\} = \mathbb{K}'\{\mathfrak{a}', \mathfrak{b}'\}$, and for $M \in \mathbb{K}'\{\mathfrak{a}, \mathfrak{b}\}^\times$ an invertible element of this quadratic algebra, we have $M\mathfrak{a} = \mathfrak{b}M \iff M\mathfrak{a}' = \mathfrak{b}'M$ which completes the proof. \square

Corollary 5.4. *The group $\mathrm{PGL}(\mathbb{V})$ acts transitively on each level set of the determinant in $\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$, and therefore on each irreducible component of its symmetric space $\mathbb{P}(\mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X})$. The semi-simple conjugacy classes in $\mathrm{PGL}(\mathbb{V})$ are classified by the value of $(\mathrm{Tr} A)^2 / \mathrm{disc}(A) \in \mathbb{K}$, which is 0 for the class of involutions.*

Recall that if $\det(\mathfrak{a}) \neq 0$ then the stabiliser of $\mathfrak{a} \in \mathfrak{sl}_2(\mathbb{K}) \setminus \mathbb{X}$ in $\mathfrak{gl}_2(\mathbb{K})$ is reduced to the quadratic subalgebra $\mathbb{K}[\mathfrak{a}]$. This implies the following Corollary, which will have arithmetic applications bearing to the genus of quadratic forms.

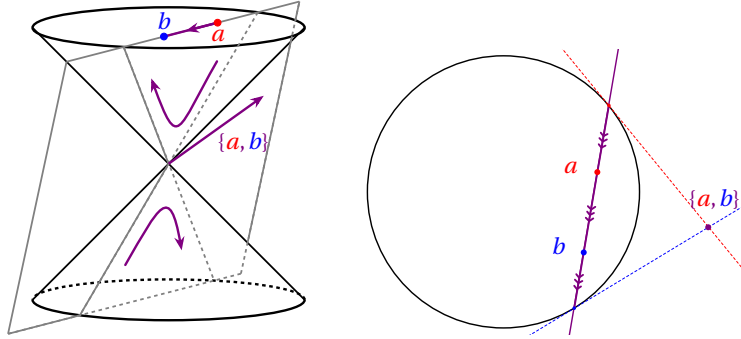


FIGURE 7. The one parameter group generated by $\{a, b\}$, which is contained in $\text{Span}(\mathbf{1}, \{a, b\})$, acts by translation along the line (a, b) .

Corollary 5.5. *Slightly reduced Figure 7. Consider distinct $a, b \in \mathfrak{sl}(\mathbb{V})$ with determinant $-\delta \neq 0$ and $\text{bir}(a, b) \neq \infty$.*

The matrices $M \in \text{PGL}_2(\mathbb{V})$ conjugating a to b have a well defined determinant in the quotient $\mathbb{K}^\times / \text{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\delta}]^\times)$, and it is equal to the class of $\text{bir}(a, b)$.

Let us now describe the structure of the orbits for the adjoint action of $\text{PSL}(\mathbb{V})$ on the non-zero level sets $\{\det = -\delta\} \subset \mathfrak{sl}(\mathbb{V})$, which is the main theorem in [13, Chapter 1].

Theorem 5.6. *Let $a, b \in \mathfrak{sl}(\mathbb{V})$ have $\det = -\delta \neq 0$ and $\text{bir}(a, b) = 4\chi \notin \{1, \infty\}$. The elements $C \in \text{SL}(\mathbb{V})$ such that $CaC^{-1} = b$ are parametrized by the Pell–Fermat conic:*

$$(x, y) \in \mathbb{K} \times \mathbb{K} : \quad x^2 - \delta y^2 = \chi$$

$$C(x, y) = x(\mathbf{1} + b a^{-1}) + y(a + b).$$

In particular, a and b are conjugate by some $C(x, y) \in \text{SL}(\mathbb{V})$ if and only if $\text{bir}(a, b)$ belongs to the subgroup of norms $\text{Nr}_{\mathbb{K}} \mathbb{K}[\sqrt{\delta}] \subset \mathbb{K}^\times$ of the quadratic extension, and by some $C(x, 0) \in \text{SL}(\mathbb{V}) \cap \mathbb{K}[\{a, b\}]$ if and only if $\text{bir}(a, b)$ belongs to the subgroup of squares $(\mathbb{K}^\times)^2 \subset \mathbb{K}^\times$.

Proof. Suppose first that $a, b \in \mathbb{H}$. Since $\det\{a, b\} \neq 0$ the elements $\mathbf{1}, a, b, \{a, b\}$ form a basis of $\mathfrak{gl}(\mathbb{V})$. Let $C \in \mathfrak{gl}(\mathbb{V})$ be decomposed as $C = t\mathbf{1} + x\{a, b\} + ya + zb$ for $t, x, y, z \in \mathbb{K}$. The condition $Ca = bC$ can be rewritten using $a^2 = -\mathbf{1} = b^2$ as well as $\{a, b\}a = b - \langle a, b \rangle a$ and $b\{a, b\} = a - \langle a, b \rangle b$. After grouping terms we find $Ca = bC \iff (t - x(1 + \langle a, b \rangle)) \cdot (a - b) + (z - y) \cdot (\mathbf{1} + ba) = 0$. But $a - b \in \text{Span}(a, b) \setminus \{0\}$ and $\mathbf{1} + ba = (1 - \langle a, b \rangle)\mathbf{1} - \{a, b\} \in \mathbb{K}[\{a, b\}] \setminus \{0\}$ so by orthogonality of the planes $\mathbb{K}[\{a, b\}]$ and $\text{Span}(a, b)$ we have $Ca = bC \iff t = x(1 + \langle a, b \rangle)$ & $y = z$.

Now for $x, y \in \mathbb{K}$ the determinant of $C = x(\mathbf{1} - ba) + y(a + b)$ can be computed using the orthogonality of $\text{Span}(\mathbf{1}, ab)$ and $\text{Span}(a, b)$ and the hypothesis $a, b \in \mathbb{H}$:

$$\det(C) = (x^2 + y^2) \cdot (2 + 2\langle a, b \rangle) = \frac{4(x^2 + y^2)}{\text{bir}(a, b)}$$

so $C \in \text{SL}(\mathbb{V}) \iff \text{bir}(a, b) = (2x)^2 + (2y)^2$. This proves the lemma for $\delta = -1$.

Finally, let us reduce the general case $\delta \neq 0$ to the previous one. The points $a' = a/\sqrt{d}$ and $b' = b/\sqrt{d}$ satisfy $\text{bir}(a, b) = \text{bir}(a', b')$ and the endomorphisms $C \in \text{SL}(\mathbb{V} \otimes \mathbb{K}')$ with $\mathbb{K}' = \mathbb{K}[\sqrt{d}]$ conjugating a to b are the same as those conjugating a' to b' . We just showed that those elements C correspond to the pairs $(x, y) \in \mathbb{K}' \times \mathbb{K}'$ such that $\text{bir}(a, b) = 4(x'^2 + y'^2)$ by the formula $C = x'(\mathbf{1} + b'a'^{-1}) + y'(a' + b')$. Setting $x = x'$ and $y = y'/\sqrt{d}$ which satisfy $4(x^2 + dy^2) = \text{bir}(a, b)$, we may rewrite $C = x(\mathbf{1} + ba^{-1}) + y(a + b)$. But recall that a

and b have coefficients in \mathbb{K} and that $\mathbf{a} + \mathbf{b} \neq 0$ is orthogonal to $\mathbf{1} + \mathbf{b}\mathbf{a}^{-1} \neq 0$. Hence C is has coefficients in \mathbb{K} if and only if $x, y \in \mathbb{K}$. \square

Remark 5.7. *Theorem 5.6 holds with coefficients restricted to any subring of \mathbb{K} containing $1/2$. For instance $\mathbb{Z}[1/2] \subset \mathbb{Q}$, or $\mathbb{Z}_p \subset \mathbb{Q}_p$ for odd prime p .*

Remark 5.8. *The problem of conjugating $\mathbf{a}, \mathbf{b} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$ by $C \in \mathrm{SL}(\mathbb{V})$ can be formulated as the search for fixed points under the transformation $C \mapsto \mathbf{a}C\mathbf{b}^{-1}$. Let us be more precise.*

The group $\mathfrak{gl}(\mathbb{V})^\times \times \mathfrak{gl}(\mathbb{V})^\times$ acts linearly on $\mathfrak{gl}(\mathbb{V})$ by $(A, B) \cdot C = ACB^{-1}$, preserving the isotropic cone $\{\det = 0\}$ and its complement $\mathfrak{gl}(\mathbb{V})^\times$. The $C \in \mathfrak{gl}(\mathbb{V})^\times$ conjugating $A, B \in \mathfrak{gl}(\mathbb{V})^\times$ correspond to the fixed points of (A, B) under this action. If they exist, then (A, B) must belong to the subgroup of pairs with $\det(A) = \det(B)$, preserving the level sets of \det , namely the stabiliser of $\mathrm{SL}(\mathbb{V})$.

The proof of Theorem 5.6 can be recast as the description of the linear action of (\mathbf{a}, \mathbf{b}) on $\mathfrak{gl}(\mathbb{V})$, which under the assumptions $\det(\mathbf{a}) = -\delta = \det(\mathbf{b})$ and $\langle \mathbf{a}, \mathbf{b} \rangle = \kappa \neq \pm\delta$ ensuring that $(\mathbf{1}, \{\mathbf{a}, \mathbf{b}\}, \mathbf{a}, \mathbf{b})$ forms a basis, is given by the following matrix, where $c = -\kappa/\delta$ is the cosine:

$$L_{\mathbf{a}} = \begin{pmatrix} 0 & 0 & \delta & -\kappa \\ 0 & 0 & 0 & 1 \\ 1 & \kappa & 0 & 0 \\ 0 & \delta & 0 & 0 \end{pmatrix}, \quad R_{\mathbf{b}^{-1}} = \frac{1}{\delta} \begin{pmatrix} 0 & 0 & -\kappa & \delta \\ 0 & 0 & 1 & 0 \\ 0 & \delta & 0 & 0 \\ 1 & \kappa & 0 & 0 \end{pmatrix}, \quad L_{\mathbf{a}}R_{\mathbf{b}^{-1}} = \frac{1}{\delta} \begin{pmatrix} -\kappa & \delta^2 - \kappa^2 & 0 & 0 \\ 1 & \kappa & 0 & 0 \\ 0 & 0 & 0 & \delta \\ 0 & 0 & \delta & 0 \end{pmatrix} = \begin{pmatrix} c & (1-c^2)\delta & 0 & 0 \\ 1/\delta & -c & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Its characteristic polynomial is $(X^2 + 1)^2 = (X - 1)^2(X + 1)^2$ and some eigenvectors for the eigenvalues $+1$ and -1 are $C(x, y)^\# = (x(1 + c), x/\delta, -y, -y)$ and $(x(1 + c), -x/\delta, y, -y)$.

Remark 5.9. *We have $\mathrm{Tr} C(x, y) = 2x(1 - \langle \mathbf{b}, \mathbf{a} \rangle / \delta) = 2x(1 + \cos(\mathbf{a}, \mathbf{b})) = 4x / \mathrm{bir}(\mathbf{a}, \mathbf{b}) = x/\chi$.*

Remark 5.10 (Square roots of $\mathbf{b}\mathbf{a}^{-1}$). *For $y = 0$ we recover the unique multiples of M satisfying the conditions in Proposition 5.3 which belong to $\mathrm{SL}(\mathbb{V} \otimes \mathbb{K}')$ where $\mathbb{K}' = \mathbb{K}[\sqrt{\mathrm{bir}(\mathbf{a}, \mathbf{b})}]$, namely:*

$$\pm C = \frac{1}{2} \sqrt{\mathrm{bir}(\mathbf{a}, \mathbf{b})} (\mathbf{1} + \mathbf{b}\mathbf{a}^{-1}).$$

These are the unique square roots of the product of symmetries $\mathbf{b}\mathbf{a}^{-1}$ in the extended quadratic algebra $\mathbb{K}'[\{\mathbf{a}, \mathbf{b}\}]$ since one may compute that $-\delta C^2 = \langle \mathbf{a}, \mathbf{b} \rangle + \{\mathbf{a}, \mathbf{b}\} = -\mathbf{b}\mathbf{a}$, thus

$$C^2 = \mathbf{b}\mathbf{a}^{-1}.$$

Our last proposition completes the description for the $\mathrm{PSL}(\mathbb{V})$ -orbits of pairs $\mathbf{a}, \mathbf{b} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$. Two such pairs are conjugate if and only if the obvious conditions on the scalar products hold, together with the Pell–Fermat conditions on the cross ratios given by Theorem 5.6.

Proposition 5.11. *The stabiliser $\mathrm{SL}(\mathbb{V}) \cap \mathbb{K}[\mathbf{a}]$ of $\mathbf{a} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$ acts transitively on the set of elements in $\mathfrak{sl}(\mathbb{V})$ with a given determinant and scalar product with \mathbf{a} .*

Proof. For $C = t\mathbf{1} + u\mathbf{a} \in \mathrm{SL}(\mathbb{V})$ and $\mathbf{b}, \mathbf{b}' \in \mathfrak{sl}(\mathbb{V})$, we have $C\mathbf{b} = \mathbf{b}'C$ if and only if $\langle \mathbf{a}, \mathbf{b} \rangle = \langle \mathbf{a}, \mathbf{b}' \rangle$ & $t(\mathbf{b} - \mathbf{b}') + u\{\mathbf{a}, \mathbf{b} + \mathbf{b}'\} = 0$. This last condition amounts to the colinearity of $(\mathbf{b} - \mathbf{b}')$ with $\{\mathbf{a}, \mathbf{b} + \mathbf{b}'\}$, that is $(\mathbf{b} - \mathbf{b}') \perp \mathbf{a}$ & $(\mathbf{b} - \mathbf{b}') \perp (\mathbf{b} + \mathbf{b}')$, so the claim follows. (If $\mathbf{b} \neq \mathbf{a}$ then $\pm C$ is unique.) \square

Consider the action of $\mathrm{PSL}(\mathbb{V})$ by conjugacy on itself. Let us say that $A, B \in \mathrm{PSL}(\mathbb{V})$ are of the same type if $\mathrm{disc}(A) \equiv \mathrm{disc}(B) \pmod{(\mathbb{K}^\times)^2}$, in which case we may define $\mathrm{bir}(A, B)$.

Corollary 5.12. *A pair of semi-simple elements A_1, A_2 of the same type is conjugate to another pair of semi-simple elements B_1, B_2 of the same type if and only if we have $\mathrm{bir}(A_1, A_2) = \mathrm{bir}(B_1, B_2)$ as well as $\mathrm{disc}(A_i) = \Delta_i = \mathrm{disc}(B_i)$ and*

$$\mathrm{bir}(A_i, B_i) \equiv 1 \pmod{\mathrm{Nr}_{\mathbb{K}}(\sqrt{\Delta_i})^\times}.$$

Examples over finite Fields. Let us fix a basis of \mathbb{V} to identify it with \mathbb{K}^2 , and first deduce a canonical basis for $\mathfrak{gl}(\mathbb{V}) = \mathfrak{gl}_2(\mathbb{K})$. Its elements together with their opposites forms the dihedral group of order 8 which acts faithfully on the square whose vertices have coordinates ± 1 :

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad K = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This orthogonal basis presents $\mathfrak{gl}_2(\mathbb{K})$ as a quaternion algebra, with product given by $J^2 = K^2 = \mathbf{1}$ and $KJ = -JK = S$. Its elements are defined over all \mathbb{K} since their coordinates belong to $\{-1, 0, 1\}$, in particular their properties are invariant under extension of scalars.

Example 5.13 (Conjugating elements with their opposites). *The pairs (K, J) and $(-K, -J)$ are conjugate by $S \in \mathrm{SL}_2(\mathbb{K})$. The elements S and $-S$ are conjugate by $K, J \in \mathrm{GL}_2(\mathbb{K})$ but according to Proposition 3.2, they are conjugate in $\mathrm{SL}_2(\mathbb{K})$ if and only if -1 is a sum of squares in \mathbb{K} .*

Example 5.14 (Conjugating J and K). *Let us show that J and K are conjugate by $\mathrm{SL}_2(\mathbb{K})$ but are conjugate by $\mathbb{K}\{J, K\}$ only when $2 \in (\mathbb{K}^\times)^2$.*

The $M \in \mathfrak{gl}_2(\mathbb{K})$ satisfying $MJ = KM$ are $M(p, q) = \begin{pmatrix} p & -p \\ q & q \end{pmatrix}$ for $p, q \in \mathbb{K}$, and $\det(M) = 2pq$. The only ones in $\mathbb{K}\{J, K\} = \mathbb{K}\{S\}$ are those for which $p = q$.

Applying Theorem 5.3 to J, K of determinant -1 with $\langle J, K \rangle = 0$ and $\{J, K\} = -S$ yields

$$C(x, y) = \frac{1}{\sqrt{2pq}} M(p, q) = \frac{1}{\sqrt{2pq}} \left[\frac{p+q}{2} (\mathbf{1} + S) + \frac{q-p}{2} (J + K) \right] \in \mathrm{SL}_2(\mathbb{K}[\sqrt{2pq}]).$$

Therefore J and K are always conjugate by $\mathrm{SL}_2(\mathbb{K})$ by choosing for instance $p = 2q$, but they are conjugate in $\mathbb{K}\{J, K\}$ only when $2 \in (\mathbb{K}^\times)^2$.

Example 5.15. *Let us describe the orbits for the adjoint action of $\mathrm{PSL}_2(\mathbb{F}_3)$ on the non-zero level sets of $(\mathfrak{sl}_2(\mathbb{F}_3), \det)$, given by $1: \{\pm S, \pm(J \pm K)\}$ and $-1: \{\pm J, \pm K, \pm S \pm J \pm K\}$.*

For $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}_2(\mathbb{F}_3)$ with $\det = -\delta \neq 0$, the hypothesis $\mathrm{bir}(\mathfrak{a}, \mathfrak{b}) \notin \{1, \infty\} \iff \cos(\mathfrak{a}, \mathfrak{b})^2 \neq 1$ becomes $\langle \mathfrak{a}, \mathfrak{b} \rangle = 0$, and leads to the equation $x^2 - \delta y^2 = -1$ which always has a solution. Hence Theorem 5.6 says that any two orthogonal elements of the same non-zero determinant are conjugate.

We find for instance that S is conjugated to $J + K$ by the element $\mathbf{1} + S - K$. Moreover as -1 is a sum of squares in \mathbb{F}_3 we know that S and $-S$ are conjugate, for instance by $J + K \in \mathrm{SL}(\mathbb{V})$. From this we deduce that the level set 1 consists of a single orbit with 6 elements.

The quaternionic group $\pm\{1, S, J, K\}$ assembles the elements $\pm S \pm J \pm K$ in two orbits given by the product of their coefficients mod 3. Moreover we saw that $J, -J, K, -K$ are all conjugate. An exhaustive search confirms that the 12 element level set $\{\det = -1\}$ is partitioned into those 3 orbits with 4 elements, of which two form the vertices of tetrahedra whose edges intersect along the third forming the vertices of a square. Using Proposition 5.11, we find that the action of $\mathrm{PSL}_2(\mathbb{F}_3)$ on this picture recovers the isomorphism with the tetrahedral group $\Delta(2, 3, 3) \simeq \mathfrak{A}_4$.

One may also partition $\mathbb{K} \setminus \{0\}$ in two orbits forming the vertices of tetrahedra, whose edges correspond to level sets of the scalar product.

Example 5.16. *In $\mathfrak{sl}_2(\mathbb{F}_5)$ the level sets of \det for the values 1, 2 are given in the following table. Multiplication by 2 yields a bijection between level sets with opposite signs, and the 25 remaining elements belong to \mathbb{K} . Both forms $x^2 + y^2$ and $x^2 + 2y^2$ represent all elements in \mathbb{F}_5 , and one may use Theorem 5.6 to show that the action of $\mathrm{PSL}_2(\mathbb{F}_5)$ is transitive on each non-zero level set of \det .*

The orbits $\{\det = \pm 2\}$ form the vertices of two octahedra whose edges correspond to the orbits $\{\det = \pm 1\}$, and Proposition 5.11 shows that the action of $\mathrm{PSL}_2(\mathbb{F}_5)$ on this picture

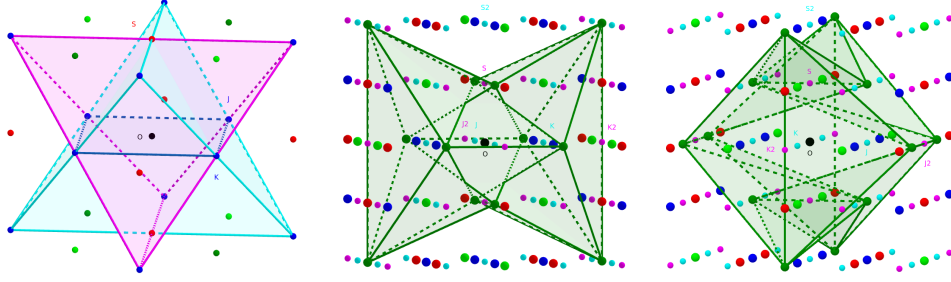


FIGURE 8. Inside $\mathfrak{sl}_2(\mathbb{F}_3)$: the isotropic cone \mathbb{X} , the orbit $\{\det = +1\}$ and the partition of $\{\det = -1\}$ into 3 orbits: the vertices of each tetrahedron and the intersections of their edges. Inside $\mathfrak{sl}_2(\mathbb{F}_5)$: the orbits $\det = -2, -1, 1, 2$ and an icosahedral orbit in $\mathbb{X} \setminus \{0\}$.

det	$\{kK + sS + jJ \mid k, s, j \in [-2, 2]\} \subset \mathfrak{sl}_2(\mathbb{F}_5)$	Cardinal
0	$2(\pm K \pm S), \pm K \pm 2J, \pm S \pm J, 0, 2(\pm K \pm S, \pm 2K \pm J, 2(\pm S \pm J))$	$12 + 1 + 12$
1	$\pm S, \pm 2K, \pm 2J, \pm K \pm S \pm 2J, \pm 2K \pm S \pm J, \pm 2K \pm 2S \pm 2J$	30
2	$\pm 2K \pm S, \pm S \pm 2J, \pm 2J \pm 2K, \pm J \pm 2S \pm K$	20

recovers the isomorphism with the icosahedral group $\Delta(2, 3, 5) \simeq \mathfrak{A}_5$. The set $\mathbb{X} \setminus \{0\}$ partitions in two orbits forming the vertices of icosahedra, whose edges can be defined using level sets of the scalar product.

6. Applications to binary quadratic forms

Let $\mathcal{Q}(\mathbb{V})$ be the space of quadratic forms $Q: \mathbb{V} \rightarrow \mathbb{K}$. After choosing a basis of \mathbb{V} , those amount to homogeneous polynomials in two ordered variables with coefficients in \mathbb{K} .

Isomorphism $\mathcal{Q}(\mathbb{V}) \simeq \mathfrak{sl}(\mathbb{V})$. One may polarise $Q \in \mathcal{Q}(\mathbb{V})$ with respect to any non-degenerate bilinear form on the plane \mathbb{V} , and one usually learns this for some euclidean scalar product, but we may also use a symplectic form: there exists a unique $\mathfrak{q} \in \mathfrak{sl}(\mathbb{V})$ such that $Q(v) = \omega(v, \mathfrak{q}v)$. If we fix a basis $\mathbb{V} = \mathbb{K}^2$ and $\omega = \det$ we have the formula

$$Q = lx^2 + mxy + ry^2 \in \mathcal{Q}(\mathbb{K}^2) \quad \longleftrightarrow \quad \mathfrak{q} = \frac{1}{2} \begin{pmatrix} -m & -2r \\ 2l & m \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{K}).$$

This defines a bijective correspondence between $\mathfrak{sl}_2(\mathbb{K})$ and $\mathcal{Q}(\mathbb{K}^2)$ through which the adjoint action of $\mathrm{PGL}_2(\mathbb{K})$ corresponds to the action by change of variables. It matches the discriminants $m^2 - 4lr$ and sends the Lie bracket $\{\mathfrak{a}, \mathfrak{b}\} = \frac{1}{2}(\mathfrak{a}\mathfrak{b} - \mathfrak{b}\mathfrak{a})$ of $\mathfrak{sl}_2(\mathbb{K})$ to the Poisson bracket of functions on \mathbb{K}^2 , under which quadratic forms are closed $\{Q_a, Q_b\} = \frac{1}{4}[(\partial_x Q_a)(\partial_y Q_b) - (\partial_x Q_b)(\partial_y Q_a)] = \{\mathfrak{a}, \mathfrak{b}\}$.

Consequently, all the notions defined for an element $\mathfrak{q} \in \mathfrak{sl}_2(\mathbb{K})$ or a pair of elements $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}_2(\mathbb{K})$, can be translated in terms of the corresponding binary quadratic forms $Q, Q_a, Q_b \in \mathcal{Q}(\mathbb{K}^2)$. For instance, after choosing a root $\sqrt{\mathrm{disc}(Q_a) \mathrm{disc}(Q_b)} = -4\sqrt{\det(\mathfrak{a}\mathfrak{b})}$, we may define the cosine:

$$\cos(Q_a, Q_b) = \frac{\mathrm{disc}(Q_a + Q_b) - (\mathrm{disc}(Q_a) + \mathrm{disc}(Q_b))}{2\sqrt{\mathrm{disc}(Q_a) \mathrm{disc}(Q_b)}} = \cos(\mathfrak{a}, \mathfrak{b})$$

and the cross-ratio of their roots $\{\alpha', \alpha\} \& \{\beta', \beta\}$, which are ordered up to simultaneous inversion:

$$\mathrm{bir}(Q_a, Q_b) = \mathrm{bir}(\alpha', \alpha; \beta', \beta) = \frac{(\alpha' - \alpha)(\beta' - \beta)}{(\alpha - \beta')(\beta - \alpha')} = \mathrm{bir}(\mathfrak{a}, \mathfrak{b}).$$

For a common choice of root these are related by

$$\text{bir}(Q_a, Q_b)^{-1} = \frac{1}{2}(1 + \cos(Q_a, Q_b)).$$

In particular, if Q_a, Q_b have the same discriminant Δ , which is to be chosen as the root $\sqrt{\text{disc}(Q_a)\text{disc}(Q_b)}$, then $\text{bir}(Q_a, Q_b)^{-1} = \text{disc}(Q_a + Q_b)/(4\Delta)$, and we may compute $\text{bir}(Q_a, Q_b) \equiv l_a l_b \pmod{\text{Nr}_{\mathbb{K}} \mathbb{K}[\sqrt{\Delta}]}$.

The actions by change of variable of $\text{PGL}_2(\mathbb{K})$ and $\text{PSL}_2(\mathbb{K})$ on $\mathcal{Q}(\mathbb{V})$ preserve the discriminant as an element of $\mathbb{K}/(\mathbb{K}^*)^2$ and \mathbb{K} respectively, as well as the cross ratio. Note that the condition $\text{bir}(Q_a, Q_b) \notin \{1, \infty\} \iff Q_a \neq \pm Q_b$ can always be achieved after conjugating Q_b by $\text{PSL}_2(\mathbb{K})$. Consequently, Proposition 5.3 and Theorem 5.6 describe the orbits of $\mathcal{Q}(\mathbb{V})$ under the action of $\text{PGL}_2(\mathbb{K})$ and $\text{PSL}_2(\mathbb{K})$ in terms of disc and bir, the latter being empty or $\mathbb{K}[\sqrt{\Delta}]^\times$ -torsors.

The variables live in the cone. Conversely one may try to recover some notions defined for binary quadratic form in terms of the corresponding matrices. This was the motivation leading to Lemma 4.1, namely to recover the values that a form $Q \in \mathcal{Q}(\mathbb{V})$ takes on \mathbb{V} in terms of the geometry of $\mathfrak{q} \in \mathfrak{sl}(\mathbb{V})$ with respect to \mathbb{X} . Indeed, Lemma 4.1 implies that if $\psi: v \in \mathbb{V} \mapsto p \in \mathbb{X}$ then

$$Q(v) = \det(v, \mathfrak{q}v) = \langle \mathfrak{q}, p \rangle.$$

So the elements $p \in \mathbb{X}$ in the cone play the role of the vector of variables $v \in \mathbb{V}$, whereas the other elements $\mathfrak{q} \in \mathfrak{sl}(\mathbb{V}) \setminus \mathbb{X}$ are the non-degenerate binary quadratic forms $Q \in \mathcal{Q}(\mathbb{V})$.

The values of Q on \mathbb{V} may xthus be interpreted in terms of the distances between \mathfrak{q}^\perp and \mathbb{X} . In particular, if $\text{disc } Q_a = \Delta = \text{disc } Q_b$ then for any $v_a, v_b \in \mathbb{V}$ which belong to \mathbb{K} -bases, we have:

$$\text{bir}(Q_a, Q_b) \equiv Q_a(v_a)Q_b(v_b) \pmod{\text{Nr}_{\mathbb{K}} \mathbb{K}[\sqrt{\Delta}]^\times}$$

whence $\text{bir}(a, b) \equiv \langle a, p_a \rangle \langle b, p_b \rangle \pmod{\text{Nr}_{\mathbb{K}} \mathbb{K}[\sqrt{\Delta}]^\times}$.

Proposition 6.1. *The set $\text{Cl}_{\mathbb{K}}(\Delta)$ of $\text{PSL}_2(\mathbb{K})$ -orbits in $\mathcal{Q}(\mathbb{V})$ with non-square discriminant Δ embeds into the group $\mathbb{K}^\times / \text{Nr}_{\mathbb{K}}(\mathbb{K}[\sqrt{\Delta}]^\times)$ of exponent two, by sending the class of the norm $x^2 - \frac{\Delta}{4}y^2$ of the \mathbb{K} -extension $\mathbb{K}[\sqrt{\Delta}]$ to the identity, and using the multiplication of values for composition.*

Describing \mathbb{Q} -equivalence with Hilbert symbols. In this paragraph we fix $\mathbb{V} = \mathbb{Q}^2$ and a non-square discriminant Δ . Consider two forms Q_a, Q_b representing variable \mathbb{Q} -classes in $\text{Cl}_{\mathbb{Q}}(\Delta)$, and let us provide a method for computing $\text{bir}(Q_a, Q_b) \pmod{\text{Nr}_{\mathbb{Q}} \mathbb{Q}[\sqrt{\Delta}]^\times}$.

$\mathcal{P} = \{-1, 2\} \cup \{3, 5, 7, \dots\}$ denotes the set of rational primes and \mathbb{Q}_p the p -adic completion of \mathbb{Q} . The prime -1 refers (following Conway [4]) to the place at which the completion of \mathbb{Q} is the Archimedean field $\mathbb{Q}_{-1} = \mathbb{R}$. For $\delta, \chi \in \mathbb{Q}_p^\times$ the *Hilbert symbol* $(\delta, \chi)_p$ equals 1 or -1 according to whether the homogenised Pell–Fermat equation $x^2 - \delta y^2 = \chi z^2$ admits a solution in $\mathbb{Q}_p \mathbb{P}^2$ or not. Thus we have $(\delta, \chi)_p = 1$ if and only if χ is the norm of an element in $\mathbb{Q}_p(\sqrt{\delta})$.

We define the set of prime obstructions to solving $(2x)^2 - \Delta y^2 = \text{bir}(Q_a, Q_b)$ by

$$\mathcal{P}(Q_a, Q_b) = \{p \in \mathcal{P} \mid (\Delta, \text{bir}(Q_a, Q_b))_p = -1\},$$

which only depends on the \mathbb{Q} -classes of Q_a and Q_b .

Theorem 6.2. *The forms Q_a and Q_b are \mathbb{Q} -equivalent if and only if $\mathcal{P}(Q_a, Q_b) = \emptyset$.*

Proof. Apply the Hasse–Minkowski theorem [12, Chapitre IV, Théorème 8] to the ternary quadratic form $(2x)^2 - \Delta y^2 - \text{bir}(Q_a, Q_b)z^2$: it represents 0 over \mathbb{Q} if and only if it represents 0 over \mathbb{Q}_p for all $p \in \mathcal{P}$. \square

The following lemma and remark enable us to turn the previous theorem into a finite method for computing \mathbb{Q} -classes.

Lemma 6.3. *If $p \in \mathcal{P} \setminus \{2\}$ divides δ and χ to even powers, then $(\delta, \chi)_p = 1$.*

In other terms $\mathcal{P}(Q_a, Q_b) \setminus \{2\}$ is contained in the set of primes appearing with odd valuations in the factorisation of Δ or $\mathrm{bir}(Q_a, Q_b)$. In particular it is finite.

Proof. A pedestrian method is to reduce the equation mod p , argue that there exists a solution by a counting procedure, and lift it to \mathbb{Q}_p using Hensel's lemma.

Alternatively, one may use the explicit formulae [12, Theorem III.1] for the Hilbert symbol at $p \neq 2$ in terms of the Legendre symbols of $\delta, \chi \in \mathbb{Q}_p$ at -1 and p . \square

Remark 6.4. *Hilbert proved a global relation among the local symbols: $\prod_{p \in \mathcal{P}} (\delta, \chi)_p = 1$, which is a reformulation of the quadratic reciprocity law. Consequently $\mathcal{P}(Q_a, Q_b) \setminus \{2\}$ determines $\mathcal{P}(Q_a, Q_b)$.*

Our final Proposition implies that Q_a & Q_b are \mathbb{Q} -equivalent if and only if $\mathcal{P}(Q_0, Q_a) = \mathcal{P}(Q_0, Q_b)$. This simplifies the determination of all sets $\mathcal{P}(Q_a, Q_b)$ to those involving a fixed element Q_0 .

Proposition 6.5. *For $Q_a, Q_b, Q_c \in \mathrm{Cl}_{\mathbb{Q}}(\Delta)$ the set $\mathcal{P}(Q_a, Q_b)$ is equal to the symmetric difference of $\mathcal{P}(Q_c, Q_a)$ and $\mathcal{P}(Q_b, Q_c)$. In other terms for all $p \in \mathcal{P}$ we have:*

$$(\Delta, \mathrm{bir}(Q_c, Q_a) \mathrm{bir}(Q_a, Q_b) \mathrm{bir}(Q_b, Q_c))_p = 1.$$

Proof. According to [12, Theorem III.2], the Hilbert symbol of \mathbb{Q}_p defines a non-degenerate symmetric bilinear form on the \mathbb{F}_2 -vector space $(\mathbb{Q}_p^\times)/(\mathbb{Q}_p^\times)^2$. The lemma can thus be reformulated as $(\Delta, \chi_{a,b,c})_p = 1$ where $\chi_{a,b,c} = \mathrm{bir}(Q_c, Q_a) \mathrm{bir}(Q_a, Q_b) \mathrm{bir}(Q_b, Q_c)$.

We must therefore compare $\chi_{a,b,c} \in \mathbb{Q}^\times$ with the subgroup generated by the norms of elements in $\mathbb{Q}(\sqrt{\Delta})^\times$. Using the explicit formula for the cross-ratio we find that

$$\mathrm{bir}(Q_a, Q_b) = \frac{-\Delta/(l_a l_b)}{\mathrm{Nr}_{\Delta}(\alpha' - \beta)}, \quad \text{hence} \quad \chi_{a,b,c} = \frac{-\Delta^3/(l_a l_b l_c)^2}{\mathrm{Nr}_{\Delta}((\gamma' - \alpha)(\alpha' - \beta)(\beta' - \gamma))}.$$

Consequently $(\Delta, \chi_{a,b,c}) = (\Delta, -\Delta)_p = 1$ as desired. \square

Corollary 6.6. *Denoting Q_0 a representative for the norm of the \mathbb{Q} -extension $\mathbb{Q}(\sqrt{\Delta})$, the map $Q \mapsto \mathcal{P}(Q_0, Q)$ yields an isomorphism $\mathrm{Cl}_{\mathbb{Q}}(\Delta) = \prod_{p \in \mathcal{P}} \mathrm{Cl}_{\mathbb{Q}_p}(\Delta)$.*

Integral binary quadratic forms. Notice that under the 1:1 correspondence $\mathcal{Q}(\mathbb{Q}^2) \leftrightarrow \mathfrak{sl}_2(\mathbb{Q})$, the lattice $\mathcal{Q}(\mathbb{Z}^2)$ of integral binary quadratic forms gets mapped to the dual lattice $\mathfrak{sl}_2(\mathbb{Z})^\vee$ of $\mathfrak{sl}_2(\mathbb{Z})$ in $\mathfrak{sl}_2(\mathbb{Q})$ with respect to the quadratic form \det . We will concentrate on the primitive points of the lattices $\mathcal{Q}(\mathbb{V})$ or $\mathfrak{sl}(\mathbb{V})^\vee$, namely those which are visible from the origin, thus not multiples of another lattice point by a non-invertible integer.

Now for any field \mathbb{K} of characteristic different from 2, we may consider the extension of scalars $\mathfrak{sl}_2(\mathbb{Z}[1/2]) \rightarrow \mathfrak{sl}_2(\mathbb{K})$, and its restriction to $\mathfrak{sl}_2(\mathbb{Z})^\vee$. We say that $\mathfrak{a}, \mathfrak{b} \in \mathfrak{sl}_2(\mathbb{Z})^\vee$ are \mathbb{K} -equivalent when their images in $\mathfrak{sl}_2(\mathbb{K})$ belong to the same orbit under the adjoint action of $\mathrm{PSL}_2(\mathbb{K})$. We may thus group the conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ into \mathbb{K} -classes, and observe how this varies with \mathbb{K} .

When $\mathbb{K} \supset \mathbb{Q}$ has characteristic zero, the extension of scalars $\mathfrak{sl}_2(\mathbb{Q}) \rightarrow \mathfrak{sl}_2(\mathbb{K})$ is injective so the \mathbb{K} -equivalence implies the equality of discriminants. When $\mathbb{K} = \mathbb{C}$, this groups the integral binary quadratic forms according to their discriminant, and we find the finite class groups $\mathrm{Cl}(\Delta)$. When $\mathbb{K} = \mathbb{Q}$, this defines for each discriminant Δ a partition of the class group $\mathrm{Cl}(\Delta)$ into \mathbb{Q} -classes.

Class groups and genera. Fix a non-square discriminant Δ and consider the set $\text{Cl}(\Delta)$ of $\text{PSL}_2(\mathbb{Z})$ -equivalence classes of primitive integral binary quadratic forms with that discriminant. This is a finite set by the classical reduction theory of binary quadratic forms (see [5, 4]).

In [7], C. F. Gauss endowed $\text{Cl}(\Delta)$ with the structure of a finite abelian group which was later reformulated by Dirichlet as follows [15]. One may represent two classes in $\text{Cl}(\Delta)$ by forms Q_a and Q_b whose first coefficients l_a and l_b are coprime, and with the same middle coefficient m : their composition Q_c of the same discriminant is determined by its first coefficient $l_c = l_a l_b$ and middle coefficient m . (Beware that this corresponds to the *narrow* class group of ideals in \mathcal{O}_Δ .) The neutral element of $\text{Cl}(\Delta)$ is represented by any form which takes the value 1, for instance the principal form $x^2 + \epsilon xy + \frac{1}{4}(\epsilon - \Delta)y^2$ where $\epsilon \in \{0, 1\}$ satisfies $\Delta = \epsilon \pmod{4}$, obtained from the \mathbb{Q} -extension $\mathbb{Q}(\sqrt{\Delta})$ by restricting the norm to its unique order \mathcal{O}_Δ of discriminant Δ .

Two classes in $\text{Cl}(\Delta)$ *belong to the same genus* when for all $p \in \mathcal{P}$ they are conjugate by $\text{SL}_2(\mathbb{Z}_p)$, with $\mathbb{Z}_{-1} = \mathbb{R}$ (see [3, Chapter 14]). One may consult [5, Theorem 3.21] for several other characterisations, such as representing the same values in $(\mathbb{Z}/\Delta)^\times$. The equivalence classes for this relation form a group $\text{Gen}(\Delta)$ given by the multiplication of their sets of values in $(\mathbb{Z}/\Delta)^\times$. Gauss identified it with the quotient of his class group by the subgroup of squares. Moreover the kernel of the squaring map consists in the subgroup $\text{Sym}(\Delta)$ of classes invariant by the Galois involution. In other terms we have a short exact sequence of abelian groups:

$$1 \rightarrow \text{Sym}(\Delta) \rightarrow \text{Cl}(\Delta) \xrightarrow{\text{square}} \text{Cl}(\Delta) \rightarrow \text{Gen}(\Delta) \rightarrow 1.$$

For two classes in $\text{Cl}(\Delta)$ represented by Q_a, Q_b we saw that $\text{bir}(Q_a, Q_b) \equiv l_a l_b \pmod{\text{Nr}_{\mathbb{Q}} \mathbb{Q}[\sqrt{\Delta}]^\times}$. We used this multiplication of values to define the composition law on $\text{Cl}_{\mathbb{Q}}(\Delta)$ in Proposition 6.1. Hence the extension of scalars $\mathbb{Z} \rightarrow \mathbb{Q}$ yields a group morphism $\text{Cl}(\Delta) \rightarrow \text{Cl}_{\mathbb{Q}}(\Delta)$ whose kernel consists in the \mathbb{Z} -classes which are \mathbb{Q} -equivalent to the principal form. This kernel contains the subgroup of squares so we find a morphism of groups with exponent two $\text{Cl}(\Delta)/\text{Cl}(\Delta)^2 \rightarrow \text{Cl}_{\mathbb{Q}}(\Delta)$.

A fundamental discriminant Δ is that of (the ring of integers in) a quadratic extension of \mathbb{Q} , which means that $\Delta = 1 \pmod{4}$ is a square-free integer, or that $\Delta/4 \not\equiv 1 \pmod{4}$ is a square-free integer. For such Δ , the genus equivalence amounts to being conjugate by an element in $\text{PGL}_2(\mathbb{Q})$ ([5, Exercise 3.17]), which is implied by \mathbb{Q} -equivalence. This discussion implies the following.

Proposition 6.7. *In $\text{Cl}(\Delta)$, the principal genus $\text{Cl}(\Delta)^2$ is contained in the subgroup of classes which are \mathbb{Q} -equivalent to the principal form, thus genus equivalence implies \mathbb{Q} -equivalence. If Δ is fundamental then \mathbb{Q} -equivalence implies genus equivalence (but otherwise it may not).*

Example: \mathbb{Q} -equivalence and continued fractions. Let us observe the partition of $\text{Cl}(\Delta) = \mathbb{Z}/4 \times \mathbb{Z}/2$ into \mathbb{Q} -classes for the positive fundamental discriminants $1596 = 4 \times 3 \times 7 \times 19$ and $1768 = 8 \times 13 \times 17$, whose fundamental units have norm $+1$ and -1 .

The following tables exhibit the structure of $\text{Cl}(\Delta) \simeq \mathbb{Z}/4 \times \mathbb{Z}/2$. Each cell contains the coefficients (l, m, r) of a representative $\in \mathcal{Q}(\mathbb{Z}^2)$ together with the period of the continued fraction expansion of its first root $\frac{1}{2l}(-m + \sqrt{\Delta})$ and the set of prime obstructions $\mathcal{P}(Q_0, Q)$.

Remark 6.8. *Notice that \mathbb{Q} -equivalence does not control the period lengths of the continued fraction expansions: there exist \mathbb{Q} -equivalent forms whose roots have euclidean periods of different length.*

(1, -38, -38) [38, 1] \emptyset	(10, -34, -11) [3, 1, 2, 3] {7, 19}	(25, -14, -14) [1, 12, 1, 1] \emptyset	(10, -26, -23) [3, 3, 2, 1] {7, 19}
(2, -38, -19) [19, 2] {3, 19}	(5, -34, -22) [7, 2, 2, 1] {3, 7}	(29, -30, -6) [1, 4, 1, 5] {3, 19}	(5, -36, -15) [7, 1, 1, 2] {3, 7}

(1, 42, -1) [42, 42] \emptyset	(14, 40, -3) [2, 13, 1, 2, 13, 1] {2, 17}	(-9, 34, 17) [2, 4, 4, 2, 4, 4] \emptyset	(-3, 40, 14) [2, 1, 13, 2, 1, 13] {2, 17}
(21, 40, -2) [1, 1, 20, 1, 1, 20] {2, 13}	(7, 40, -6) [1, 5, 6, 1, 5, 6] {2, 17}	(-13, 26, 21) [2, 1 ⁶ , 2, 1 ⁶] {2, 13}	(-6, 40, 7) [6, 5, 1, 6, 5, 1] {2, 17}

Examples: \mathbb{Q} -classes modulo genera. We may apply the previous methods to partition $\mathrm{Cl}(\Delta)$ into \mathbb{Q} -classes (given by $\mathrm{SL}_2(\mathbb{Q}_p)$ -equivalence) using the Hilbert symbols, and into genera (given by $\mathrm{SL}_2(\mathbb{Z}_p)$ -equivalence) using the $\mathrm{Cl}(\Delta)^2$ -cosets.

Denoting by $S_{\mathbb{Q}}(\Delta)$ the kernel of the map $\mathrm{Cl}(\Delta) \rightarrow \mathrm{Cl}_{\mathbb{Q}}(\Delta)$, the discrepancy is measured by the dimension $c_{\mathbb{Q}}$ of the \mathbb{F}_2 -vector space $S_{\mathbb{Q}}(\Delta)/\mathrm{Cl}(\Delta)^2$. This depends on which odd primes divide Δ to an even power, and on the 2-adic valuation of Δ .

In each table, the discriminant of the first row are fundamental, and the others are not. In the second and third table, the units in the quadratic extensions have norm +1 and -1 respectively.

$\Delta < 0$	$\mathrm{Cl}(\Delta)$	$c_{\mathbb{Q}}$	$\Delta > 0$	$\mathrm{Cl}(\Delta)$	$c_{\mathbb{Q}}$	Δ	$\mathrm{Cl}(\Delta)$	$c_{\mathbb{Q}}$
$-2^2 \times 7$	$\mathbb{Z}/1$	1	$2^2 \times 3 \times 5$	$\mathbb{Z}/2$	1	5 & 13	$\mathbb{Z}/2$	1
$-2^3 \times 7$	$\mathbb{Z}/4$	1	$2^2 \times 3^2 \times 5$	$\mathbb{Z}/1$	1	5×13	$\mathbb{Z}/2$	1
$-2^4 \times 7$	$\mathbb{Z}/2$	2	$2^2 \times 3 \times 5^2$	$\mathbb{Z}/2$	2	$5^2 \times 13$	$\mathbb{Z}/2$	2
$-2^5 \times 7$	$\mathbb{Z}/4 \times \mathbb{Z}/2$	2	$2^2 \times 3^3 \times 5$	$\mathbb{Z}/2$	1	5×13^2	$\mathbb{Z}/2$	2
$-2^6 \times 7$	$\mathbb{Z}/2 \times \mathbb{Z}/2$	4	$2^2 \times 3 \times 5^3$	$\mathbb{Z}/1$	1	$5^3 \times 13$	$\mathbb{Z}/2$	1
$-2^7 \times 7$	$\mathbb{Z}/8 \times \mathbb{Z}/2$	4	$2^2 \times 3^3 \times 5^2$	$\mathbb{Z}/6$	2	5×13^3	$\mathbb{Z}/2$	1
$-2^3 \times 7^3$	$\mathbb{Z}/28$	1	$2^2 \times 3^2 \times 5^3$	$\mathbb{Z}/1$	1	$5^3 \times 13^3$	$\mathbb{Z}/2$	1

The last example fits in the family of $\Delta = p^u \times q^v$ for distinct primes $p, q \equiv 1 \pmod{4}$ and $u, v \in \mathbb{N}$. If $u = 1, v = 0$ then Δ is fundamental and the genera coincide with the \mathbb{Q} -classes. For $u, v \in \mathbb{N}^*$ we observe that $c_{\mathbb{Q}} = 1$ when both u, v are odd and $c_{\mathbb{Q}} = 2$ when either u or v is even.

7. Arithmetic equivalence of singular moduli and modular geodesics

The modular group $\mathrm{PSL}_2(\mathbb{Z})$ acts on the upper-half plane $\mathbb{H}\mathbb{P} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by linear fractional transformations, and the quotient is the modular orbifold $\mathbb{M} = \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathbb{H}\mathbb{P}$.

Consider primitive integral binary quadratic forms Q_a, Q_b with non-square discriminant Δ . Fix a root $\sqrt{\Delta}$ which is to be positive if $\Delta > 0$, and define the first roots of $Q_a(x, 1)$ and $Q_b(x, 1)$ by

$$\alpha = \frac{-m_a + \sqrt{\Delta}}{2l_a} \quad \text{and} \quad \beta = \frac{-m_b + \sqrt{\Delta}}{2l_b}.$$

Arithmetic equivalence of singular moduli. If $\Delta > 0$ then Q_a, Q_b are uniquely determined by their roots $\alpha, \beta \in \mathbb{H}\mathbb{P}$. Their $\mathrm{PSL}_2(\mathbb{Z})$ -classes correspond to points $[\alpha], [\beta] \in \mathbb{M}$,

often called singular moduli in the study of elliptic curves. The geodesic arc from α to β in $\mathbb{H}\mathbb{P}$ has length λ given in terms of the cross-ratio $\text{bir}(\alpha', \alpha; \beta', \beta)$ by the formula

$$\left(\cosh \frac{\lambda}{2}\right)^2 = \frac{1 + \cosh(\lambda)}{2} = \frac{1}{\text{bir}(Q_a, Q_b)}.$$

Corollary 7.1 (to Theorem 5.6). *Two singular moduli $[\alpha], [\beta] \in \mathbb{K}(\sqrt{\Delta})$ are \mathbb{K} -equivalent if and only if there exists a geodesic arc in \mathbb{M} from $[\alpha]$ to $[\beta]$ whose length λ is of the form*

$$\left(\cosh \frac{\lambda}{2}\right)^2 = \frac{1}{(2x)^2 - \Delta y^2} \quad \text{for } x, y \in \mathbb{K},$$

in which case all geodesic arcs from $[\alpha]$ to $[\beta]$ have this property.

Arithmetic equivalence of modular geodesics. If $\Delta < 0$, then Q_a and Q_b correspond to oriented geodesics $(\alpha', \alpha), (\beta', \beta)$ in $\mathbb{H}\mathbb{P}$. Their $\text{PSL}_2(\mathbb{Z})$ -classes correspond to primitive closed oriented geodesics in \mathbb{M} called modular geodesics, with length $2 \sinh^{-1}(\sqrt{|\Delta|}/2)$.

Consider the oriented hyperbolic geodesics (α', α) and (β', β) in $\mathbb{H}\mathbb{P}$. If they intersect, then their angle θ is given in terms of the cross-ratio $\text{bir}(\alpha', \alpha; \beta', \beta)$ by the formula

$$\left(\cos \frac{\theta}{2}\right)^2 = \frac{1 + \cos(\theta)}{2} = \frac{1}{\text{bir}(Q_a, Q_b)}.$$

If they do not intersect, then they have a unique common perpendicular geodesic arc, which may receive compatible co-orientations from each axis or not. When it is the case, its length λ is given in terms of the cross-ratio $\text{bir}(\alpha', \alpha; \beta', \beta)$ by the formula

$$\left(\cosh \frac{\lambda}{2}\right)^2 = \frac{1 + \cosh(\lambda)}{2} = \frac{1}{\text{bir}(Q_a, Q_b)}$$

Corollary 7.2 (to Theorem 5.6). *Two modular geodesics of the same length $2 \sinh^{-1}(\sqrt{|\Delta|}/2)$ are \mathbb{K} -equivalent if and only if we have one of the following equivalent conditions:*

θ *There exists one intersection point with angle $\theta \in]0, \pi[$ such that*

$$\left(\cos \frac{\theta}{2}\right)^2 = \frac{1}{(2x)^2 - \Delta y^2} \quad \text{for } x, y \in \mathbb{K}$$

in which case all intersection points have this property.

λ *There exists one co-oriented ortho-geodesic of length λ such that*

$$\left(\cosh \frac{\lambda}{2}\right)^2 = \frac{1}{(2x)^2 - \Delta y^2} \quad \text{for } x, y \in \mathbb{K}$$

in which case all co-oriented ortho-geodesics have this property.

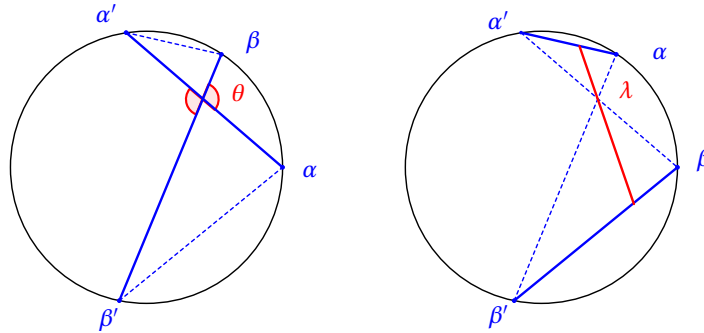


FIGURE 9. Cross-ratios and cosines in the real case.

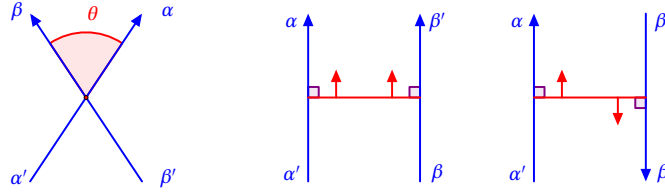


FIGURE 10. Angle well defined in $]0, \pi[$. Ortho-geodesics well and badly co-oriented.

Remark 7.3. *Theorem 5.6 holds over any integral ring in which 2 is invertible, so one may similarly characterise genus equivalence (for all discriminants Δ) replacing \mathbb{Q} by \mathbb{Z}_p for all $p \in \mathcal{P}$.*

Linking numbers of modular knots. Let us briefly relate the arithmetic-geometric intersections of modular geodesics to the topological linking numbers of modular knots, referring to [14] as well as [13, Chapter 0 and Chapter 5] for the details and much more about this.

The unit tangent bundle of the modular orbifold $\mathbb{M} = \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathbb{H}\mathbb{P}$ can be identified with the manifold $\mathbb{U} = \mathrm{PSL}_2(\mathbb{Z}) \backslash \mathrm{PSL}_2(\mathbb{R})$, homeomorphic to the complement of a trefoil knot in the sphere. The primitive closed geodesics of \mathbb{M} lift in \mathbb{U} to the primitive periodic orbits for the geodesic flow: one may ask about the linking numbers between these *modular knots*. They correspond to the $\mathrm{PSL}_2(\mathbb{Z})$ -classes of primitive $A \in \mathrm{PSL}_2(\mathbb{Z})$, or of primitive $\alpha \in \mathfrak{sl}_2(\mathbb{Z})^\vee$, with positive discriminant.

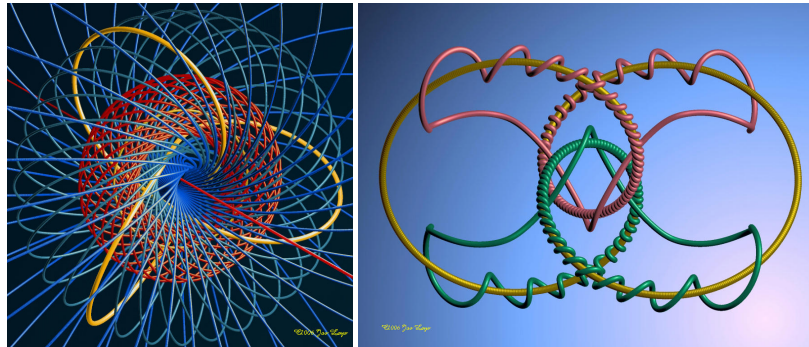


FIGURE 11. The Seifert fibration $\mathbb{U} \rightarrow \mathbb{M}$ and two modular knots from the online article [8], which proposes an animated introduction to the topology and dynamics of \mathbb{U} .

Let us introduce, for any pair of modular geodesics γ_A, γ_B , the following sums of the arithmetic-geometric quantities encountered in Corollary 7.2 over their oriented intersection angles $\theta \in]0, \pi[$:

$$L_q(A, B) = \frac{1}{2} \sum (\cos \frac{\theta}{2}) \quad \text{and} \quad \mathrm{Cos}_q(A, B) = \frac{1}{2} \sum (\cos \theta)$$

and study their variations as we deform the metric on \mathbb{M} by opening the cusp.

The complete hyperbolic metrics on the orbifold \mathbb{M} correspond to the faithful and discrete representations $\rho: \mathrm{PSL}_2(\mathbb{Z}) \rightarrow \mathrm{PSL}_2(\mathbb{R})$ up to conjugacy. Since $\mathrm{PSL}_2(\mathbb{Z})$ is the free amalgam of its cyclic subgroups of order 2 and 3 generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$,

they form a 1-dimensional real algebraic set parametrized by $q \in \mathbb{R}_+^*$, fixing S and conjugating T by $\exp(-\frac{1}{2} \log(q)K)$:

$$S_q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T_q = \begin{pmatrix} 1 & -q \\ q^{-1} & 0 \end{pmatrix} \quad L_q = \begin{pmatrix} q & 0 \\ 1 & q^{-1} \end{pmatrix} \quad R_q = \begin{pmatrix} q & 1 \\ 0 & q^{-1} \end{pmatrix}.$$

The geometric-algebra of $\mathrm{PSL}_2(\mathbb{K})$ applies in to the image of $\rho_q: \mathrm{PSL}_2(\mathbb{Z}) \rightarrow \mathrm{PSL}_2(\mathbb{R})$, so when the axes of $A_q, B_q \in \mathrm{SL}_2(\mathbb{R})$ intersect, their oriented angle has cosine:

$$\cos(A_q, B_q) = \mathrm{sign}(\mathrm{Tr}(A_q) \mathrm{Tr}(B_q)) \frac{\mathrm{Tr}(A_q B_q) - \mathrm{Tr}(A_q B_q^{-1})}{\sqrt{\mathrm{disc}(A_q) \mathrm{disc}(B_q)}}.$$

The hyperbolic conjugacy classes of $\mathrm{PSL}_2(\mathbb{Z})$ still index the closed geodesics in the quotient $\mathbb{M}_q = \rho_q(\mathrm{PSL}_2(\mathbb{Z})) \backslash \mathbb{H}\mathbb{P}$ which do not surround the cusp. We may thus define the analogous sums $L_q(A, B)$ and $\mathrm{Cos}_q(A, B)$ over the intersection angles $\theta_q \in]0, \pi[$ between the q -modular geodesics $\gamma_{A_q}, \gamma_{B_q} \subset \mathbb{M}_q$ of the $\frac{1}{2}(\cos \frac{1}{2} \theta_q)^2$ and $(\cos \theta_q)$.

As $q \rightarrow \infty$, the hyperbolic orbifold \mathbb{M}_q has a convex core which retracts onto a thin neighbourhood of the long geodesic arc connecting its conical singularities, whose pre-image in the universal cover $\mathbb{H}\mathbb{P}$ is a trivalent tree. In the limit we recover the action of $\mathrm{PSL}_2(\mathbb{Z})$ on its Bruhat–Tits building, the infinite planar trivalent tree \mathcal{T} , and by studying its combinatorics [14] proves the following.

Theorem 7.4 (Linking and intersection numbers from boundary evaluations). *For primitive hyperbolic $A, B \in \mathrm{PSL}_2(\mathbb{Z})$, the functions $L_q(A, B)$ and $\mathrm{Cos}_q(A, B)$ on the $\mathrm{PSL}_2(\mathbb{R})$ -character variety of $\mathrm{PSL}_2(\mathbb{Z})$ have limits*

$$\begin{aligned} L_q(A, B) &\xrightarrow{q \rightarrow \infty} \mathrm{lk}(A, B), \\ \mathrm{Cos}_q(A, B) &\xrightarrow{q \rightarrow \infty} \mathrm{lk}(A, B) - \mathrm{lk}(A^{-1}, B) = \mathrm{lk}(A, B) - \frac{1}{4} I(A, B). \end{aligned}$$

Hence the functions L_q & Cos_q interpolate between the geometry at $q = 1$ of the arithmetic group $\mathrm{PSL}_2(\mathbb{Z}) \subset \mathrm{PSL}_2(\mathbb{R})$ and the topology at $q = +\infty$ of the combinatorial action $\mathrm{PSL}_2(\mathbb{Z}) \rightarrow \mathrm{Aut}(\mathcal{T})$.

Remark 7.5. *This discussion naturally carries over to the field of functions $\mathbb{K} = \mathbb{Q}(q)$ on the character variety of $\mathrm{PSL}_2(\mathbb{Z})$, or its universal quadratic closure.*

The series $L_q(A, B)$ is thus reminiscent of the special value at $s = 2$ of a restricted zeta function: its terms $\frac{1}{2}(1 + \cos(A_q, B_q)) = 1/\mathrm{bir}(A_q, B_q)$ are the inverse norms of certain principal ideals for the quadratic extension of $\mathbb{Q}(q)$ generated by $\sqrt{\mathrm{disc}(A_q) \mathrm{disc}(B_q)}$.

Let us display the graphs of $q \mapsto 2L_q(A, B)$ and $q \mapsto 2L_q(A, B^{-1})$ along with their average $\frac{1}{2}I(A, B)$ for some pairs $A, B \in \mathrm{PSL}_2(\mathbb{N})$. The legend $A = [a_0, a_1, \dots]$ means $A = R^{a_0} L^{a_1} \dots$ has attractive fixed point $\alpha \in \mathbb{R}\mathbb{P}^1$ with continued fraction $\alpha = a_0 + \frac{1}{a_1 + \dots}$.

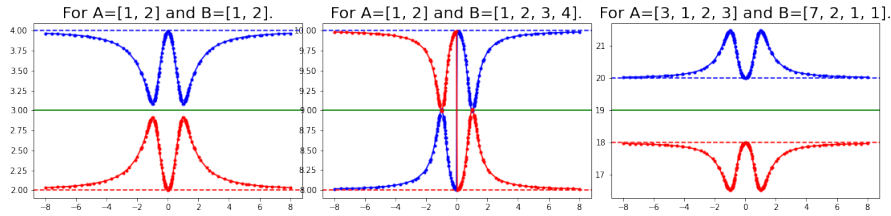


FIGURE 12. $L_q(A, B)$ interpolates between the arithmetic at 1 and the topology at $+\infty$.

Remark 7.6. Variation on Theorem 7.4 can be obtained by applying by any continuous function on the interval $[0, 1]$ to the terms of $L_q(A, B)$. A particularly interesting example is given by

$$L_q(A, B) = \frac{1}{2} \sum \mathcal{L}\left(\cos \frac{\theta}{2}\right) = \frac{1}{2} \sum \mathcal{L}(\mathrm{bir}(\alpha', \alpha; \beta', \beta)),$$

where $\mathcal{L}(z) = \sum_{n=1}^{\infty} \frac{z^n}{n^2} + \frac{1}{2} \log(|z|) \log(1-z)$ is Rogers' normalisation of the dilogarithm, yielding

$$\mathcal{L}_q(A, B) \xrightarrow{q \rightarrow \infty} \frac{\pi}{6} \mathrm{lk}(A, B).$$

References

- [1] V. Arnold. Lobachevsky triangle altitudes theorem as the Jacobi identity in the Lie algebra of quadratic forms on symplectic plane. *J. Geom. Phys.*, 53(4):421–427, 2005.
- [2] Élie Cartan. *Leçons sur la géométrie projective complexe. La théorie des groupes finis et continus et la géométrie différentielle traitées par la méthode du repère mobile. Leçons sur la théorie des espaces à connexion projective.* Les Grands Classiques Gauthier-Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1992. Reprint of the editions of 1931, 1937 and 1937.
- [3] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.
- [4] John Conway and Francis Fung. *The sensual (quadratic) form*. MAA, 1997.
- [5] David Cox. *Primes of the form $x^2 + ny^2$* . Wiley-Interscience, 1997.
- [6] Jean Dieudonné. *La géométrie des groupes classiques*. Springer-Verlag, 3 edition, 1971.
- [7] Carl Friedrich Gauss. *Recherches Arithmétiques*. Courcier, 1807.
- [8] Étienne Ghys and Jos Leys. Lorenz and modular flows: a visual introduction, 2016. <http://www.ams.org/publicoutreach/feature-column/fcarc-lorenz>.
- [9] Nikolai Ivanov. Arnol'd, the Jacobi identity, and orthocenters. *Amer. Math. Monthly*, 118(1):41–65, 2011.
- [10] Robert Penner. The decorated Teichmüller space of punctured surfaces. *Comm. Math. Phys.*, 113(2):299–339, 1987.
- [11] Robert Penner. The geometry of the Gauss product. *J. Math. Sci.*, 81(3):2700–2718, 1996.
- [12] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1970.
- [13] Christopher-Lloyd Simon. *Arithmetic and Topology of Modular knots*. Thèse, Université de Lille, June 2022. PDF on HAL.
- [14] Christopher-Lloyd Simon. Linking numbers of modular knots, 2022. Preprint <https://arxiv.org/abs/2211.05957>.
- [15] André Weil. *Number theory: An approach through history From Hammurapi to Legendre*. Birkhäuser, 1984.

Christopher-Lloyd SIMON: Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA

E-mail: cks6029@psu.edu