Products of conjugacy classes of the special linear group over a Euclidean field

van Yperen, Kevin

K. van Yperen

Products of conjugacy classes of the special linear group over a Euclidean field

Bachelor thesis

September 6, 2024

Thesis supervisor: H.W. Lenstra

Leiden University
Mathematical Institute

Contents

1 Introduction

Let G be a group and let $B, C, D \subseteq G$ be conjugacy classes. We wish to know if there exist $b \in B, c \in C$ and $d \in D$ such that $bcd = 1$. It will be shown that the permutation of the conjugacy classes is not relevant to the existence of a solution. We will answer this question for $G = \mathrm{SL}_2(K)$ where K is a Euclidean field, see definition 3.4. Note that $\mathbb{R}$ is a Euclidean field. A matrix $A \in \mathrm{SL}_2(K)$ is said to be **hyperbolic** if its minimum polynomial is quadratic and splits into two different linear factors. We call A **parabolic** if its minimum polynomial is quadratic and splits into two equal linear factors. If the minimum polynomial of A is quadratic and irreducible then we say that A is **elliptic**. Lastly, if the minimum polynomial is linear then we say that A is **trivial**. We know from linear algebra that two matrices in the same conjugacy class have the same minimum polynomial so we may also call conjugacy classes hyperbolic, parabolic, elliptic and trivial.

It is known that two non-trivial matrices of determinant 1 are conjugate under $\mathrm{GL}_2(K)$ if and only if they have equal trace. Thus if two matrices of determinant 1 are conjugate under $\mathrm{SL}_2(K)$ then they have equal trace. However, the converse does not always hold. When working over a Euclidean field we do however have the following. If the matrices are hyperbolic or trivial then the converse does hold. For elliptic and parabolic matrices the converse almost holds. Because we only allow conjugation under $\mathrm{SL}_2(K)$ we see that the orientation of the basis vectors is preserved. Thus for example two rotations of equal but opposite angles have the same trace but a different orientation. We shall show that this is in fact the only obstruction to determining whether two matrices of equal trace are conjugate under $\mathrm{SL}_2(K)$. In order to classify the conjugacy classes we shall introduce the sign, which keeps track of the orientation. Formally, if we denote the set of non-hyperbolic matrices by X, then the sign is a map $\mathrm{sign} : X \to \{-1, 0, 1\}$ such that $\mathrm{sign}(A) = 0$ if and only if A is trivial, see definition 4.9. Intuitively, a matrix has sign 1 if it rotates counter clockwise and -1 if it rotates clockwise. We shall show that two matrices in the same conjugacy class have the same sign thus we can extend the sign to conjugacy classes.

We will also need to define the angle of non-hyperbolic matrices. Because we are working over Euclidean fields instead of $\mathbb{R}$ we will need to generalize the notion of an angle, which will be done in section 3.2. Just as with $\mathbb{R}$ we will obtain two maps, cos and sin, from a totally ordered abelian group L to the field K. We call the group L the winding group. We will also have a positive element π in L. We know in the case $K = \mathbb{R}$ that every elliptic matrix is conjugate under $\mathrm{SL}_2(\mathbb{R})$ to a rotation matrix. This in fact generalizes to Euclidean fields. The angle also holds information on the sign of the matrix because if it is greater than π then the sign is negative. We thus define the angle of an elliptic matrix as the angle of this rotation matrix if the sign is positive and we define it to be the angle minus π if the sign is negative. As it turns out we will have to assign a infinitesimal angle to the parabolic matrices. Thus we have to consider the extended winding group $L \oplus \mathbb{Z}\epsilon$. The angle of a matrix is a map $\theta : X \to L \oplus \mathbb{Z}\epsilon$ such that $\theta(A) = 0$ if and only if A is trivial and $0 \leq \theta(A) < \pi$ for all $A \in X$, see definition 5.11.

Write $\mathrm{sign}(B, C, D) = \mathrm{sign}(B)\mathrm{sign}(C)\mathrm{sign}(D)$ and similarly $\theta(B, C, D) = \theta(B)+\theta(C)+\theta(D)$. In this thesis we prove the following theorem.

Theorem 1.1. *Let B, C, D be non-trivial conjugacy classes of $\mathrm{SL}_2(K)$, where K is a Euclidean field. There are three cases:*

1. *If at least two of the three classes are hyperbolic then there exist $b \in B$, $c \in C$ and $d \in D$ such that $bcd = 1$.*
2. *If exactly one of the three classes, say B, is hyperbolic then there exist $b \in B$, $c \in C$ and $d \in D$ such that $bcd = 1$ if and only if $\mathrm{sign}(\mathrm{Tr}(B))\mathrm{sign}(C)\mathrm{sign}(D) = -1$.*
3. *If none are hyperbolic then there exist $b \in B$, $c \in C$ and $d \in D$ such that $bcd = 1$ if and only if one of the following holds:*
   - $\mathrm{sign}(B, C, D) = -1$ *and* $\theta(B, C, D) \leq \pi$
   - $\mathrm{sign}(B, C, D) = 1$ *and* $\theta(B, C, D) \geq 2\pi$.

For trivial classes the question turns out to be trivial. This will be seen in section 2.1, see proposition 2.3.

The question is equivalent to calculating the products of conjugacy classes. This has already been done for $K = \mathbb{R}$ by S. Orevkov in [1]. This thesis differs from [1] in three main ways.

We generalize the result to any Euclidean field. To do this we will have to introduce cyclically ordered groups in section 2.3 and generalized circle groups in section 3.2. We will also have to calculate the conjugacy classes of $\mathrm{SL}_2(K)$ in section 4.

Another difference is that by considering triples of conjugacy classes instead of products of conjugacy classes we have more symmetries we can leverage. Fundamentally we use the same method. However, using the symmetries we have to do less calculations. We also study these symmetries for a general group G in section 2.2.

Lastly, our result is more theoretical. One interesting result is that elliptic and parabolic classes behave similarly enough that they can be treated together. We also see that the sign is of great importance. Also, due to the sign and the angle of a matrix we are capable of formulating the theorem more compactly.

This thesis consists of 4 main sections. In section 2 we shall first treat some preliminary results on conjugacy classes. These results will help us determine the conjugacy classes of $\mathrm{SL}_2(K)$ where K is a Euclidean field. We shall also study the symmetries of the triples that will reduce the number of computations required. Lastly, we give a short introduction to cyclically ordered groups.

In section 3 we introduce ordered fields and Euclidean fields. We generalize many notions that will be needed in the proof from $\mathbb{R}$ to a Euclidean field. In particular, we will need the totally ordered group L. This group can be obtained by unrolling the circle group of K, which is a cyclically ordered group. The totally ordered group L was first constructed by L. Rieger. We give a new characterisation of this L in terms of windings of a cyclically ordered group. We shall see that the totally ordered group L is in fact a terminal object in the category of windings, see definition 2.20.

In section 4 we compute the conjugacy classes of $\mathrm{SL}_2(K)$. We will also prove some properties of these conjugacy classes that will be needed later.

Finally in section 5 we prove the main theorem.

The main motivation behind this thesis was a previous thesis by Daan Heus, see [2]. To prove the main theorem of his thesis Daan used hyperbolic geometry to give a condition on the angles of triples of elliptic matrices which multiply to the identity. The aim of this thesis was to provide an algebraic proof of the same condition and to generalise this result.

Very little is assumed of the reader. We only assume that the reader is familiar with group theory including ordered groups, linear algebra, a little bit of field extensions and exterior powers. Exterior powers only play a small role so if the reader is not familiar with exterior powers and is fine with giving up abstraction then the reader can replace all instances of V with k^2, $\mathrm{Aut}_k(V)$ with $\mathrm{GL}_2(k)$, $\mathrm{Aut}_k(V,\delta)$ with $\mathrm{SL}_2(k)$, $\mathrm{Aut}_k(V,\pm\delta)$ with $\mathrm{SL}_2^{\pm}(k)$ (the matrices with determinant equal to ± 1) and lastly $\delta(v \wedge w)$ with $\det([v,w])$ in section 4. The book [3] contains all of the relevant information on these topics except for ordered groups. For ordered groups we refer the reader to [4].

2 Group Theory

2.1 Conjugacy classes

Let G be a group. An automorphism $\sigma \in \mathrm{Aut}(G)$ is called an inner automorphism if there exists $g \in G$ such that $\sigma = \sigma_g := (x \mapsto gxg^{-1})$. The set of inner automorphisms, $\mathrm{Inn}(G)$, is a normal subgroup of $\mathrm{Aut}(G)$ and $g \mapsto \sigma_g$ defines a surjective homomorphism from G to the group of inner automorphisms of G with kernel $\mathrm{Z}(G)$, the centre of G.

Thus for any subgroup $H \subseteq G$ we can define an action of H on G via the inner automorphisms, namely for $h \in H$, $g \in G$ we define ${}^h g = hgh^{-1}$. The conjugacy classes of G under H are the orbits of this action. Because the orbits form a partition of the set G, we will denote the set of conjugacy classes as $G/{\sim_H}$ and if $H = G$ we will simply write $G/{\sim}$. We will also write $x \sim_H y$ if $x, y \in G$ are in the same orbit under H; in this case we say that x and y are conjugate under H.

Given three conjugacy classes $B, C, D \in \mathrm{SL}_2(\mathbb{R})/{\sim}$ we want to know if there are $b \in B, c \in C$ and $d \in D$ such that $bcd = 1$. If we define for two subsets $C, D \subseteq G$ the product to be $CD = \{cd | c \in C, d \in D\}$ then we can reformulate the question to the following: given three conjugacy classes $B, C, D \in \mathrm{SL}_2(\mathbb{R})/{\sim}$ when do we have $1 \in BCD$?

Lemma 2.1. *Say $B, C, D \in G/{\sim}$. Then we have that $1 \in BCD$ if and only if $BC \supseteq D^{-1}$, where $D^{-1} = \{d^{-1} | d \in D\}$.*

Proof. Say $1 \in BCD$, then there exist $b \in B, c \in C$ and $d \in D$ such that $bcd = 1$. We then see that $d^{-1} = bc \in BC$. Now let $g \in G$, then we see that

$$({}^g d)^{-1} = {}^g(d^{-1}) = {}^g(bc) = ({}^g b)({}^g c) \in BC.$$

Hence, we find that $BC \supseteq D^{-1}$.

Say $BC \supseteq D^{-1}$. Then there exist $b \in B$, $c \in C$ and $d \in D$ such that $bc = d^{-1}$. Hence, we find that $bcd = 1$. Thus $1 \in BCD$. □

The conjugacy class of an element in the center is just that single element. Note that if a conjugacy class has one element then it must be contained in the center.

Definition 2.2. *Let G be a group. A conjugacy class which contains only one element is called trivial.*

Proposition 2.3. *Let $B, C, D \in G/\sim$ such that $D = \{z\}$ is trivial, where $z \in \mathrm{Z}(G)$. Then we see that $1 \in BCD$ if and only if $B = z^{-1}C^{-1}$.*

Proof. Say we have a solution $1 = bcd$ with $b \in B$, $c \in C$ and $d \in D$. Then we see that $d = z$ and $z^{-1}c^{-1} = b$. Now let $g \in G$. Then we see that ${}^{g}b = z^{-1}({}^{g}c)^{-1}$. Hence, we find that $B = z^{-1}C^{-1}$.

Now if $B = z^{-1}C^{-1}$ then there must exist $b \in B$ and $c \in C$ such that $b = z^{-1}c^{-1}$. This gives us that $bcz = 1$. Therefore, $1 \in BCD$. □

The following lemma will help us determine the conjugacy classes.

Lemma 2.4. *Let $H \subseteq G$ be a subgroup. Say $I \subseteq G$ is a subset such that $HI = G$. Then for all $x, y \in G$ we have: $x \sim_G y$ if and only if $\exists \sigma \in I$ such that ${}^{\sigma}x \sim_H y$.*

Proof. Clearly, if ${}^{\sigma}x \sim_H y$ then $x \sim_G y$ because ${}^{\sigma}x \sim_G x$. Now say $x \sim_G y$. Then we let $g \in G$ be such that ${}^{g}x = y$. Now we write $g = h\sigma$ with $\sigma \in I$ and $h \in H$. Then we see that $y = {}^{h\sigma}x = {}^{h}({}^{\sigma}x)$. So ${}^{\sigma}x \sim_H y$. □

For any $\sigma \in \mathrm{Z}(G)$ and $x \in G$ we have that ${}^{\sigma}x = x$. This gives us the following corollary.

Corollary 2.5. *Let $H \subseteq G$ be a subgroup such that $G = H\mathrm{Z}(G) = \{hz | h \in H, z \in \mathrm{Z}(G)\}$. Then $x \sim_G y$ if and only if $x \sim_H y$.*

Noting that $[G : H]$ is the minimal cardinality of a subset I of G such that $HI = G$, we get the following corollary.

Corollary 2.6. *Let $H \subseteq G$ be a subgroup. Then any conjugacy class of G under G splits into at most $[G : H]$ conjugacy classes of G under H.*

The following lemma will give us a condition for when a conjugacy class doesn't split under a subgroup.

Lemma 2.7. *Let $N \subseteq G$ be a normal subgroup, $I \subseteq G$ be a subset such that $NI = G$ and $x \in G$. If for all $\sigma \in I$ there exists $y_\sigma \in G$ such that ${}^{\sigma}y_\sigma = y_\sigma$ and $x \sim_N y_\sigma$, then for all $y \in G$ we have $x \sim_G y$ if and only if $x \sim_N y$.*

Proof. Say $x \sim_G y$. Then by lemma 2.4 we see that there exists $\sigma \in I$ such that ${}^{\sigma}x \sim_N y$. Let $n, n', n'' \in N$ be such that ${}^{n\sigma}x = y$, ${}^{n'}y_\sigma = x$ and $n'' = {}^{\sigma}n' \in N$. Now we see that $y = {}^{n\sigma}x = {}^{n\sigma n'}y_\sigma = {}^{nn''\sigma}y_\sigma = {}^{nn''}y_\sigma = {}^{nn''(n')^{-1}}x$. So $x \sim_N y$. □

Lastly, the following lemma will allow us to compute the product of two conjugacy classes.

Lemma 2.8. *Let $B, C \subseteq G$ be conjugacy classes and let $b \in B$. Define $S = \{bc | c \in C\}$. Then for any conjugacy class $D \subseteq G$ we have $D \subseteq BC$ if and only if $D \cap S \neq \emptyset$.*

Proof. If $D \subseteq BC$ then we see that there must exist $b' \in B, c' \in C$ and $d' \in D$ such that $d' = b'c'$. We know that there is a $g \in G$ such that ${}^g b' = b$. Thus we see that $b\, {}^g c' = {}^g d' \in D$. Thus $D \cap S \neq \emptyset$.

Say $D \cap S \neq \emptyset$. Then there exist $b \in B$, $c \in C$ and $d \in D$ such that $d = bc$. We see that for any $g \in G$ we have that ${}^g d = {}^g b\, {}^g c \in BC$. Thus $D \subseteq BC$. □

2.2 Symmetries of W_G

Let G be a group. In this section we construct a group of symmetries of $W_G = \{(B, C, D) \in (G/\sim)^3 | 1 \in BCD\}$ that will reduce the number of calculations required. If $G = \mathrm{SL}_2(K)$ we shall simply write W for W_G.

We first look at the action of S_3, the permutation group of three elements, on $(G/\sim)^3$ by permuting the coordinates. The following lemma shows that W_G is stable under this action.

Lemma 2.9. *Let $(B, C, D) \in W_G$ then $(D, B, C) \in W_G$ and $(C, B, D) \in W_G$.*

Proof. Say we have a solution $bcd = 1$. Thus we see that $dbc = dbcdd^{-1} = dd^{-1} = 1$ and also $bcb^{-1}bd = bcd = 1$. Note that $bcb^{-1} \in C$. Hence, we have found that $(D, B, C) \in W_G$ and $(C, B, D) \in W_G$. □

Because (anti-)automorphisms of G send conjugacy classes to conjugacy classes we also have an action of the group of automorphisms and anti-automorphisms on the set $(G/\sim)^3$ given by $\phi * (B, C, D) = (\phi(B), \phi(C), \phi(D))$ where ϕ is an (anti-)automorphism. Note that if G is not abelian then the group of automorphisms and anti-automorphisms is isomorphic to the group $\langle \mathrm{h} \rangle \times \mathrm{Aut}(G)$, where h is inversion and the isomorphism is given by $(f, g) \mapsto f \circ g$. We clearly see that W_G is stable under this action. Note that for anti-automorphisms the order of the elements in the equation $bcd = 1$ is reversed. However, lemma 2.9 shows that the order is not relevant to the existence of a solution for $bcd = 1$.

Because the inner automorphisms act trivially on $(G/\sim)$ we can factor the action on $(G/\sim)$ and W_G through $\langle \mathrm{h} \rangle \times (\mathrm{Aut}(G)/\mathrm{Inn}(G))$. Note that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$. We thus have shown the following lemma.

Lemma 2.10. *The action of $\langle \mathrm{h} \rangle \times \mathrm{Aut}(G)$ on $(G/\sim)^3$ can be restricted to W_G and can be factored through $\langle \mathrm{h} \rangle \times (\mathrm{Aut}(G)/\mathrm{Inn}(G)) = \langle \mathrm{h} \rangle \times \mathrm{Out}(G)$.*

□

Let $\lambda_x : G \to G$ denote left multiplication by x. We can also define an action of $\mathrm{Z}(G)$ on G given by restricting the left Cayley action of G to $\mathrm{Z}(G)$. Because $\lambda_z \circ \sigma_g = \sigma_g \circ \lambda_z$ for $z \in \mathrm{Z}(G)$ and $g \in G$ we see that we have an action of $\mathrm{Z}(G)$ on $G/\sim$. To get an action on W_G we first have to define $G_* = \{(x, y, z) \in (\mathrm{Z}(G))^3 | xyz = 1\}$. It is easy to show that G_* is a group with coordinate-wise multiplication. We can now define an action of G_* on $(G/\sim)^3$ given by $(x, y, z) * (B, C, D) = (\lambda_x(B), \lambda_y(C), \lambda_z(D))$. The following lemma shows that this action can be restricted to an action on W_G.

Lemma 2.11. *Let $(x, y, z) \in G_*$ and $(B, C, D) \in W_G$. Then $(\lambda_x(B), \lambda_y(C), \lambda_z(D)) \in W_G$.*

Proof. We note that for $x, y \in \mathrm{Z}(G)$ and $b, c \in G$ we have that $\lambda_x(b)\lambda_y(c) = \lambda_{xy}(bc)$. Let $b \in B$, $c \in C$ and $d \in D$ be a solution $bcd = 1$. Because $xyz = 1$ we see that $1 = bcd = \lambda_{xyz}(bcd) = \lambda_x(b)\lambda_y(c)\lambda_z(d)$. Thus we have that $(\lambda_x(B), \lambda_y(C), \lambda_z(D)) \in W_G$. □

We now wish to see how these actions commute. First note that because all conjugacy classes in an abelian group consist of only 1 element, we see that G_* and $W_{\mathrm{Z}(G)}$ are essentially the same. We thus have an action of S_3 and $\langle \mathrm{h} \rangle \times \mathrm{Out}(G)$ on G_*. In order the differentiate the actions of these two groups on W_G and G_* we shall write the action on G_* using the symbol $\star$.

Lemma 2.12. *Let* $(B,C,D) \in (G/\sim)^3$*,* $\sigma \in \mathrm{S}_3$*,* $\phi \in \langle \mathrm{h} \rangle \times \mathrm{Out}(G)$ *and* $z \in G_*$*. Then we have the following:*

- $\sigma(\phi(\sigma^{-1}(B,C,D))) = \phi(B,C,D)$.
- $\sigma(z(\sigma^{-1}(B,C,D))) = (\sigma \star z)(B,C,D)$.
- $\phi(z(\phi^{-1}(B,C,D))) = (\phi \star z)(B,C,D)$.

□

We have in fact now found an action of $G_* \rtimes (\mathrm{S}_3 \times \mathrm{Out}(G) \times \langle \mathrm{h} \rangle)$ on W_G.

Definition 2.13. *Let* G *be a group. We define* $\mathrm{WSym}(G) = G_* \rtimes (\mathrm{S}_3 \times \mathrm{Out}(G) \times \langle \mathrm{h} \rangle)$.

2.3 Cyclically ordered groups

Definition 2.14. *Let* X *be a set. A cyclic order on* X *is a ternary relation, written as* $[a,b,c]$ *for* $a,b,c \in X$*, of pairwise distinct elements such that for all pairwise distinct elements* $a,b,c \in X$ *we have that:*

1. *if* $[a,b,c]$ *then* $[c,a,b]$
2. $[a,b,c]$ *or* $[a,c,b]$
3. *if* $[a,b,c]$ *then not* $[a,c,b]$
4. *for all* $d \in X \backslash \{a,b,c\}$*: if* $[a,b,c]$ *and* $[a,c,d]$ *then* $[a,b,d]$

We say that X *is cyclically ordered as a set.*

Example 2.15. If X is a totally ordered set then X can be cyclically ordered by $[x,y,z]$ if and only if $x < y < z$ or $z < x < y$ or $y < z < x$.

Definition 2.16. *Let* C *be a group and say* C *is cyclically ordered as a set. Then we say that* C *is cyclically ordered as a group if for all* $a,b,c,x,y \in C$ *we have that* $[a,b,c]$ *implies* $[xay, xby, xcy]$.

Definition 2.17. *Let* L *be a totally ordered group. Then* $z \in L$ *will be called cofinal if* z *is positive and for every* $x \in L$ *there exists* $n \in \mathbb{Z}$ *such that* $x < z^n$.

Example 2.18. Let L be a totally ordered group and z a cofinal element in the center of L. Now we can cyclically order $L/\langle z \rangle$ by defining for $a,b,c \in L/\langle z \rangle$: $[a,b,c]$ if and only if $[r_a, r_b, r_c]_L$ where $r_a \in L$ is the unique representative of a such that $1 \leq r_a < z$ and $[r_a, r_b, r_c]_L$ is defined as in example 2.15.

One can ask if every cyclically ordered group can be constructed as in example 2.18. This question was answered by L. Rieger in [5]. To do this we need to keep track of the winding number which will be done as follows. We will in fact also show that this construction is unique up to a unique isomorphism, see definition 2.20 and theorem 2.21.

Let C be a cyclically ordered group. For $x,y \in C$ define $f_{xy} = 1$ if $[1, x^{-1}, y]$ and otherwise $f_{xy} = 0$. Define $\tilde{L} = \mathbb{Z} \times C$ as a set and endow $\tilde{L}$ with the following binary operation:

$$(n,x) * (m,y) = (n + m + f_{xy}, xy).$$

Let $P = \{(n,x) \in \tilde{L} | n > 0 \text{ or } (n = 0 \text{ and } x \neq 1)\}$. Note that the first coordinate of $(1,1) \in \tilde{L}$ is the generator of $\mathbb{Z}$ whereas the second coordinate is the neutral element of C.

Theorem 2.19. *Let C be a cyclically ordered group and define $\tilde{L}$, the binary operation $*$ on $\tilde{L}$ and P as above. Then $(\tilde{L}, *)$ is a group and is totally ordered by P. The element $\tilde{z} = (1,1) \in \tilde{L}$ is a cofinal element in the center. Lastly, the projection map $\tilde{\pi} : \tilde{L} \to C$ is a homomorphism such that for all $a, b \in \tilde{L}$ with $1 < a < b < \tilde{z}$ we have $[1, \tilde{\pi}(a), \tilde{\pi}(b)]$.*

Proof. The proof can be found in [6]. □

This result can be restated in the following way.

Definition 2.20. *Let C be a cyclically ordered group. A triple (L, z, f) is called a winding of C if L is a totally ordered group, z is a cofinal element in the center of L and $f : L \to C$ is a group homomorphism such that $z \in \ker(f)$ and for all $a, b \in L$ with $1 < a < b < z : [1, f(a), f(b)]$. A morphism of windings (L, z, f) to (L', z', f') is a morphism of totally ordered groups $g : L \to L'$ such that $g(z) = z'$ and $f = f' \circ g$. The category of windings over a fixed cyclically ordered group C shall be denoted* $\mathrm{Wind}(C)$.

Letting $\tilde{L}$, $\tilde{z}$ and $\tilde{\pi}$ be as in theorem 2.19 we see that $(\tilde{L}, \tilde{z}, \tilde{\pi})$ is a winding of C.

Theorem 2.21. *Let C be a cyclically ordered group. The object $(\tilde{L}, \tilde{z}, \tilde{\pi})$ is a terminal object in* $\mathrm{Wind}(C)$. *In particular, it is unique up to a unique isomorphism.*

Proof. Let (L, z, f) be a winding of C. First note that for every element $x \in L$ there exist unique $n \in \mathbb{Z}$ and $x' \in L$ such that $1 \leq x' < z$ and $x = x'z^n$. Now we have to define $g : L \to \tilde{L}$ as $g(x) = (n, f(x'))$. This is in fact the only way we could define g because $z \mapsto (1,1)$ and $x' \mapsto (0, f(x'))$, because g must be a morphism of totally ordered groups.

We shall now show that g is order preserving. Let $x, y \in L$, $x = x'z^n$ and $y = y'z^m$. Note that $x < y$ if and only if $n < m$ or $n = m$ and $x' < y'$. Say $n < m$ then clearly $g(x) < g(y)$. Say $n = m$ and $1 = x' < y'$, then $g(x) = (n, 1)$ and $g(y) = (m, f(y'))$. We see that $g(x) < g(y)$ because $g(y)g(x)^{-1} = (0, f(y'))$ is positive. Say $x' \neq 1$, then by definition of a winding we have that $[1, f(x'), f(y')]$. Hence, $(m, f(y'))(n, f(x'))^{-1} = (m, f(y'))(-n-1, f(x')^{-1}) = (0, f(y'(x')^{-1})$ which is positive because $1 < y'(x')^{-1} < z$ so $f(y'(x')^{-1}) \neq 1$. We have thus shown that g is an order preserving map. We leave the rest of the details to the reader. □

Say C is a cyclically ordered group. Then we see that the rule $a < b$ if and only if $[1, a, b]$ for $a, b \in C^\circ = C \backslash \{1\}$ totally orders the set C°. It is useful to answer the converse question: when does a total order on C° give rise to a cyclic order on C? The following proposition gives an answer.

Proposition 2.22. *Let C be a group and let $<$ be a total order on C° such that for all $a, b \in C^\circ$ with $a < b$ we have that $b^{-1} < ab^{-1}$. Then the rule $[a, b, c]$ if and only if $ba^{-1} < ca^{-1}$ defines a cyclic order on the set C. If it is assumed that for all $g \in C$ and $a, b \in C^\circ$ with $a < b$ we have that ${}^g a < {}^g b$ then the rule defines a cyclic order on the group C. Moreover, given a cyclically ordered group C we can define for $a, b \in C^\circ : a < b$ if and only if $[1, a, b]$. This defines a total order on C°. These constructions are each other's inverses.*

Proof. Let $a, b, c \in C$ be pairwise distinct. We first show that if $[a, b, c]$ then $[c, a, b]$. Because we know that $[a, b, c]$ we have that $ba^{-1} < ca^{-1}$. Thus we have that:

$$ac^{-1} = (ca^{-1})^{-1} < ba^{-1}(ca^{-1})^{-1} = bc^{-1}.$$

Here the $<$ follows from the condition that if $a < b$ then $b^{-1} < ab^{-1}$. We have thus shown that $[c, a, b]$.

Because $<$ is a total order we see that $ba^{-1} < ca^{-1}$ or $ca^{-1} < ba^{-1}$. Thus we see that $[a, b, c]$ or $[a, c, b]$.

By anti-symmetry we see that if $ba^{-1} < ca^{-1}$ then not $ca^{-1} < ba^{-1}$. Hence, we have that if $[a, b, c]$ then not $[a, c, b]$.

Now let $d \in C \backslash \{a, b, c\}$. By the transitivity of $<$ we see that if $[a, b, c]$ and $[a, c, d]$ then we have that $ba^{-1} < ca^{-1}$ and $ca^{-1} < da^{-1}$. Thus we have that $ba^{-1} < da^{-1}$. Therefore, $[a, b, d]$.

We have now shown that C is cyclically ordered as a set. We now show that if the additional assumption is made then C is cyclically ordered as a group. Let $a, b, c, x, y \in C$ and say $[a, b, c]$. We now see that $ba^{-1} < ca^{-1}$. Thus we find that

$$(xby)(xay)^{-1} = xba^{-1}x^{-1} < xca^{-1}x^{-1} = (xcy)(xay)^{-1}.$$

Here the inequality follows from the extra assumption. Hence, we see that $[xay, xby, xcy]$. We have thus shown that C is cyclically ordered as a group.

The rest of the proof of the proposition will be left to the reader as we shall not need the rest. □

3 Ordered fields

3.1 Ordered fields

In this section we give a short introduction to ordered fields and specifically Euclidean fields. The reader can find more details regarding ordered fields in [3].

Definition 3.1. *Let K be a field and let $P \subseteq K^*$ be a subset. Then we say that K is ordered by P if:*

- $\forall x \in K^* : x \in P$ *or* $-x \in P$.
- $\forall x, y \in P : x + y \in P$ *and* $xy \in P$.

The set P can be thought of as the set of positive elements. An obvious example is $\mathbb{R}$ with $P = \{x \in \mathbb{R} | x > 0\}$. As the name suggests P induces a strict total ordering on the field K. One may check that the relation $x < y$ if $y - x \in P$ is irreflexive, antisymmetric and transitive.

Definition 3.2. *Let K be an ordered field ordered by P. Then we shall define for $x, y \in K$ $x < y$ if $y - x \in P$.*

The following proposition summarises some basic facts of ordered fields.

Proposition 3.3. *Let K be a field ordered by P.*

1. *The set P is a subgroup of K^* of index 2. In particular, 1 is positive and the multiplicative inverse of a positive element is positive.*
2. $-1 \notin P$.
3. *Every non-zero square is positive.*

□

As an immediate consequence we see that if a field K can be ordered then $\mathrm{char(K)} = 0$ because otherwise $0 = 1 + 1 + ... + 1 \in P$. We also see that $\mathbb{C}$ cannot be ordered because $\mathrm{i}^2 = -1$.

Definition 3.4. *Let K be an ordered field. We call K a Euclidean field if $(K^*)^2$ has index 2 in K^*.*

Lemma 3.5. *Let K be a Euclidean field. Then any positive element has a square root in K.*

Proof. This follows trivially because $(K^*)^2 \subseteq P \subseteq K^*$ and both $(K^*)^2$ and P have index 2 in K^*. $\square$

Lemma 3.6. *Let K be a Euclidean field. Let E, F be two field extensions of K of degree 2. Then $E \cong F$ as field extensions of K.*

Proof. We will show that $F \cong K(\mathrm{i})$ as field extensions of K. Because F is a degree 2 field extension of K there must be $a \in K$ such that $F \cong K(\sqrt{a})$ as field extensions of K. We note that $-a$ must be positive otherwise $K(\sqrt{a})$ is not of degree 2 over K. So letting $\sqrt{-a}$ be the positive square root of $-a$, which exists due to lemma 3.5, we see that $\sqrt{a} = \sqrt{-a}\mathrm{i}$ with $\sqrt{-a} \in K$. Therefore $K(\mathrm{i}) = K(a)$. $\square$

Definition 3.7. *Let K be a field ordered by P. Then* $\mathrm{sign} : K \to \{-1, 0, 1\}$ *is the map defined by*

$$\mathrm{sign}(x) = \begin{cases} -1 & \text{if } x \in -P \\ 0 & \text{if } x = 0 \\ 1 & \text{if } x \in P. \end{cases}$$

3.2 Circle groups

Definition 3.8. *Let K be a field. We define the unit circle as $C_K = \{(x, y) \in K^2 | x^2 + y^2 = 1\}$.*

The unit circle can naturally be given an abelian group structure.

Definition 3.9. *Let K be a field and let C_K be the corresponding unit circle. We define $(x, y) + (x', y') = (xx' - yy', xy' + x'y)$, which turns C_K into an abelian group.*

For $K = \mathbb{R}$ we see that $C_{\mathbb{R}} \cong \mathbb{R}/2\pi\mathbb{Z}$. We see that using the construction of example 2.18 the group $C_{\mathbb{R}}$ is a cyclically ordered group. In fact we can show the following lemma.

Lemma 3.10. *Let K be an ordered field. The relation $(x_1, y_1) < (x_2, y_2)$ if and only if $\frac{y_1}{x_1 - 1} < \frac{y_2}{x_2 - 1}$ on $C_K^\circ = C_K \backslash \{(1, 0)\}$ satisfies the conditions of proposition 2.22.*

Proof. We first note that the map $\phi : C_K^\circ \to K$ given by $(x, y) \mapsto \frac{y}{x-1}$ is a bijection. It is in fact the stereographic projection. Now we can carry the total order on K over to a total order on C_K°. Because C_K is abelian we only have to show that for all $a, b \in C_K^\circ$ such that $a < b$ we have that $b^{-1} < b^{-1}a$.

We wish to show that if $(x_1, y_1) < (x_2, y_2)$ then $(x_2, -y_2) < (x_2, -y_2) + (x_1, y_1)$. So we know that $\frac{y_1}{x_1-1} < \frac{y_2}{x_2-1}$. Because $|x_1| \leq 1$ for all $(x_1, y_1) \in C_K$ we see that $x_1 - 1 < 0$ for all $(x_1, y_1) \in C_K^\circ$. Thus we have $y_1(x_2 - 1) < y_2(x_1 - 1)$. Therefore we see that:

$$\begin{aligned} -y_2(x_1x_2 + y_1y_2 - 1) &= -x_1x_2y_2 - y_1y_2^2 + y_2 \\ &= -x_1x_2y_2 - y_1(1 - x_2^2) + y_2 \\ &= -x_1x_2y_2 - y_1 + x_2^2y_1 + y_2 + y_1(x_2 - 1) - y_1(x_2 - 1) \\ &< -x_1x_2y_2 - y_1 + x_2^2y_1 + y_2 + y_2(x_1 - 1) - y_1(x_2 - 1) \\ &= -x_1x_2y_2 + x_2^2y_1 + x_1y_2 - x_2y_1 \\ &= (x_2 - 1)(x_2y_1 - x_1y_2) \end{aligned}$$

We conclude that $\frac{-y_2}{x_2-1} < \frac{x_2y_1 - x_1y_2}{x_1x_2 + y_1y_2 - 1}$. Therefore $(x_2, -y_2) < (x_2, -y_2) + (x_1, y_1)$. $\square$

Corollary 3.11. *Let K be an ordered field. Then the circle group C_K can be cyclically ordered using lemma 3.10 and proposition 2.22.*

Because C_K is a cyclically ordered group we can use theorem 2.19 to find a totally ordered abelian group L and a cofinal element $z \in \mathrm{Z}(L)$ such that $L/\langle z \rangle \cong C_K$ as cyclically ordered groups.

Definition 3.12. *Let K be an ordered field. The pair (L, z, ω) will always denote the terminal object in* $\mathrm{Wind}(C_K)$. *The group L will be called the winding group of K.*

We see that for $K = \mathbb{R}$ we have that $L \cong \mathbb{R}$ as ordered groups, however it need not be the case in general that $L \cong K$.

Definition 3.13. *Let K be an ordered field. We define* $\cos : L \to K$ *as follows:* $\cos = p_1 \circ q$, *where $q : L \to C_K$ is the quotient map and $p_1 : C_K \to K$ is projection onto the first coordinate. Similarly, we have* $\sin : L \to K$ *given by* $\sin = p_2 \circ q$.

One can check that for $K = \mathbb{R}$ with the isomorphism $L \to \mathbb{R}$ uniquely determined by $z \mapsto 2\pi$ one retrieves the usual definitions of sine and cosine. Lastly, we also have the following.

Lemma 3.14. *Let K be a Euclidean field. The maps* $\cos$ *and* $\sin$ *surject onto* $[-1, 1] \subseteq K$.

Proof. Say $x \in [-1, 1]$. Then $1 - x^2 \geq 0$. Let y be a square root of $1 - x^2$ which exists due to lemma 3.5 we see that $(x, y) \in C_K$. And because the map $L \to C_K$ is a surjection we see that there is an element $l \in L$ such that $\cos(l) = x$. The proof for sin is analogous. $\square$

Definition 3.15. *The unique representative x of $(0, 1) \in C_K$ in L such that $1 < x < z$ will be denoted $\pi/2$. We also define $\pi = \pi/2 + \pi/2$.*

One may now easily verify the usual identities involving π, cos and sin. For example we have for all $x \in L : \cos(x + \pi) = -\cos(x)$ and $\sin(2\pi) = 0$.

Lastly, in order to accommodate for the parabolic elements we will need to extend the group L.

Definition 3.16. *Let K be an ordered field. Then the group $L \oplus \mathbb{Z}\epsilon$ will denote the extended winding group. It is totally ordered by the relation $a + n\epsilon < b + m\epsilon$ if and only if $a < b$ in L or $a = b$ and $n < m$.*

We can now extend the sine and cosine to the extended unrolled group simply by defining $\sin(a + n\epsilon) = \sin(a)$ and $\cos(a + n\epsilon) = \cos(a)$.

4 Conjugacy classes of $\mathrm{SL}_2(K)$

In this section K will always be a Euclidean ordered field and $P \subseteq K$ will always denote the set of positive elements. We will denote an arbitrary field by k. In this section we determine the conjugacy classes of $\mathrm{SL}_2(K)$. Let V be a fixed two-dimensional k-vector space and let $\det : \mathrm{End}(V) \to k$ denote the canonical determinant map.

Because V is two-dimensional, $\bigwedge^2 V$ is a one-dimensional k-vector space. We choose an isomorphism $\delta : \bigwedge^2 V \to k$. We will write $\mathrm{Aut}_k(V, \delta)$ for the group of linear automorphisms of V that act as the identity on $\bigwedge^2 V$. Technically, the group $\mathrm{Aut}_k(V, \delta)$ is independent of choice of δ. However, it will be useful to include δ in the notation. Note that in the case $V = k^2$ we have that $\mathrm{Aut}_k(V, \delta) = \mathrm{SL}_2(k)$. In general we can always find an isomorphism $V \cong k^2$. This gives an isomorphism $\mathrm{Aut}_k(V, \delta) \cong \mathrm{SL}_2(k)$.

If we now take a k-linear endomorphism $f : V \to V$ then we can give V a $k[X]$-module structure by defining $p(X)(v) = p(f)(v)$; we denote this module by V_f. The Cayley-Hamilton theorem tells us that $\chi_f(f) = 0$, where χ_f is the characteristic polynomial of f. Therefore, the $k[X]$-module V_f is a torsion module. Using the structure theorem for finitely generated modules over a principal ideal domain we find that $V \cong_{k[X]} k[X]/(p_1) \oplus k[X]/(p_2)$ with $\deg(p_1) + \deg(p_2) = 2$, because $\chi_f = p_1 p_2$.

There are two situations. Namely, $V_f \cong_{k[X]} k[X]/(X^2 - \mathrm{Tr}(f)X + \det(f))$ or $V_f \cong_{k[X]} (k[X]/(X-a))^{\oplus 2}$ with $a \in k$. If $V_f \cong_{k[X]} (k[X]/(X-a))^{\oplus 2}$ then we have that $f = a$. If we now demand that $\det(f) = 1$, then we find that $V_f \cong_{k[X]} k[X]/(X^2 - \mathrm{Tr}(f)X + 1)$ or $V_f \cong_{k[X]} (k[X]/(X-a))^{\oplus 2}$ with $a = \pm 1$. Because the maps ± 1 are contained in the center they form their own conjugacy classes.

We thus have to focus on the other situation. These linear maps come in 3 types, depending on the $k[X]$-module V_f. If $\chi_f = X^2 - \mathrm{Tr}(f)X + 1$ splits into two distinct monic linear factors then we shall call f **hyperbolic**. If χ_f splits into two equal linear factors then we call f **parabolic**. Lastly, if χ_f is irreducible then we call f **elliptic**. The maps ± 1 are called **trivial** because they are in the center. Note that for a Euclidean field this is equivalent to the definition given in the introduction.

Because the minimum polynomial of f is only dependent on the trace of f we have the following lemma:

Lemma 4.1. *Let $f \in \mathrm{Aut}_K(V, \delta)$.*

- *f is hyperbolic if and only if $|\mathrm{Tr}(f)| > 2$*
- *f is parabolic if and only if $|\mathrm{Tr}(f)| = 2$ and $f \neq \pm 1$*
- *f is elliptic if and only if $|\mathrm{Tr}(f)| < 2$.*

□

The reason for considering V_f is the following lemma.

Lemma 4.2. *Let V be a k-vector space. Let $f, g \in \mathrm{Aut}_k(V)$ be k-linear automorphisms. Then f, g are conjugate under $\mathrm{Aut}_k(V)$ if and only if $V_f \cong_{k[X]} V_g$.*

Proof. If $f, g \in \mathrm{Aut}_k(V)$ are conjugate then we see that $\varphi : (V, f) \to (V, g)$ given by $\varphi(v) = \rho v$ defines a $k[X]$-linear isomorphism, where $\rho \in \mathrm{Aut}_k(V)$ is such that $\rho f \rho^{-1} = g$. Similarly, if we are given a $k[X]$-linear isomorphism $\varphi : (V, f) \to (V, g)$, then we see that $\varphi \in \mathrm{Aut}_k(V)$ and that $\varphi f \varphi^{-1} = g$. Thus, f and g are conjugate under $\mathrm{Aut}_k(V)$. □

Because the module V_f is fully determined by $\mathrm{Tr}(f)$ for a non-trivial $f \in \mathrm{Aut}_k(V, \delta)$, we see that two non-trivial k-linear maps $f, g \in \mathrm{Aut}_k(V, \delta)$ are conjugate under $\mathrm{Aut}_k(V)$ if and only if $\mathrm{Tr}(f) = \mathrm{Tr}(g)$.

Lemma 4.3. *Let $\epsilon, \eta \in \mathrm{Aut}_k(V, \delta)$ be non-trivial. Then ϵ and η are conjugate under $\mathrm{Aut}_k(V)$ if and only if $\mathrm{Tr}(\epsilon) = \mathrm{Tr}(\eta)$.*

□

We have thus described the conjugacy classes of $\mathrm{SL}_2(k)$ under $\mathrm{GL}_2(k)$.

4.1 Signature of a linear map

We will start by considering $\mathbb{P}(V) = (V \backslash \{0\})/k^*$, the projective line. We note that by linearity the group of automorphisms of V acts on $\mathbb{P}(V)$ simply by choosing a representative. We would now like to study the action of the subgroup $\mathrm{Aut}_k(V, \delta)$ of $\mathrm{Aut}_k(V)$ on $\mathbb{P}(V)$.

Proposition 4.4. *Let $f \in \mathrm{Aut}_k(V, \delta)$.*

- *f is hyperbolic if and only if f has exactly two fixed points in $\mathbb{P}(V)$.*
- *f is parabolic if and only if f has exactly one fixed point in $\mathbb{P}(V)$.*

- *f is elliptic if and only if f has no fixed points in $\mathbb{P}(V)$.*
- *f is trivial if and only if f fixes all points of $\mathbb{P}(V)$.*

Proof. We first prove $\implies$. We first note that if $f \in \mathrm{Aut}_k(V, \delta)$ is hyperbolic, then χ_f splits into two distinct linear factors. This means that f has exactly two linearly independent eigenvectors. These eigenvectors appear as fixed points when considering the action of f on $\mathbb{P}(V)$.

If f is parabolic then it has exactly one eigenvalue. Now the dimension of the eigenspace must be either 1 or 2. If the dimension is 2 then f must be trivial. So the dimension of the eigenspace must be 1. This means that when looking at the action of f on $\mathbb{P}(V)$, we get exactly one fixed point.

Lastly, if f is elliptic then χ_f doesn't split and so f doesn't have eigenvectors. We conclude that f doesn't fix any point of $\mathbb{P}(V)$.

Clearly, if $f = \pm 1$ then f acts as the identity on $\mathbb{P}(V)$. This proves $\implies$.

To prove $\impliedby$, we simply note that the set of hyperbolic maps, the set of parabolic maps, the set of elliptic maps and the set of trivial maps partition $\mathrm{Aut}_k(V, \delta)$. □

Definition 4.5. *Let k be an ordered field and $f \in \mathrm{Aut}_k(V, \delta)$. We define $\phi_f : \mathbb{P}(V) \to \{-1, 0, 1\}$ given by $\phi_f(p) = \mathrm{sign}(\delta(v \wedge f(v)))$, where $p \in \mathbb{P}(V)$ and $v \in V \backslash \{0\}$ is a representative of p.*

Note that this is independent of the representative, because if $v, w \in V$ are both representatives of p then there exists $\lambda \in k^*$ such that $w = \lambda v$. Now we see that by proposition 3.3:

$$\mathrm{sign}(\delta(w \wedge f(w))) = \mathrm{sign}(\delta(\lambda v \wedge \lambda f(v))) = \mathrm{sign}(\lambda^2 \delta(v \wedge f(v))) = \mathrm{sign}(\delta(v \wedge f(v))).$$

It is easy to verify that $\phi_f(p) = 0$ if and only if p is a fixed point of f. We may sometimes abuse notation and write $\phi_f(v)$ for $v \in V \backslash \{0\}$.

Lemma 4.6. *Let k be an ordered field and let V, W be two-dimensional vector spaces over k. Let $\sigma : V \to W$ be an isomorphism and let $\delta : \bigwedge^2 V \to k$ and $\epsilon : \bigwedge^2 W \to k$ be isomorphisms. Let $t \in k$ be such that the k-linear morphism $\epsilon(\bigwedge^2 \sigma)\delta^{-1} : k \to k$ is given by multiplication by t. Then for all $p \in \mathbb{P}(V)$: $\phi_{\sigma f \sigma^{-1}}(\sigma(p)) = \mathrm{sign}(t)\phi_f(p)$.*

□

Lemma 4.7. *Let k be an ordered field and $f \in \mathrm{Aut}_k(V, \delta)$ be parabolic. Then either for all $p \in \mathbb{P}(V) : \phi_f(p) \geq 0$ or for all $p \in \mathbb{P}(V) : \phi_f(p) \leq 0$.*

Proof. We first consider the following case. Let $W = k^2$, $\epsilon : \bigwedge^2 W \to k$ given by $\epsilon((1, 0) \wedge (0, 1)) = 1$ and $g = \begin{pmatrix} \mp 1 & 0 \\ 1 & \mp 1 \end{pmatrix} \in \mathrm{Aut}_k(W)$. We can compute $\phi_g(p) \geq 0$ for all $p \in \mathbb{P}(W)$. Now let V, f and δ be as in the lemma. Depending on the trace we see that $(f \pm 1)^2 = 0$. We see that f and g have the same minimum polynomials hence we have a $k[X]$-linear isomorphism $\sigma : W_g \to V_f$ with $\sigma g \sigma^{-1} = f$. Hence, using lemma 4.6 we see that either for all $p \in \mathbb{P}(V) : \phi_f(p) \geq 0$ or for all $p \in \mathbb{P}(V) : \phi_f(p) \leq 0$. □

We will need a similar lemma for elliptic elements. However, we will now require that the field be Euclidean.

Lemma 4.8. *Let $f \in \mathrm{Aut}_K(V, \delta)$ be elliptic. Then either for all $p \in \mathbb{P}(V) : \phi_f(p) > 0$ or for all $p \in \mathbb{P}(V) : \phi_f(p) < 0$.*

Proof. Because the minimum polynomial of f is irreducible we have a field $K(f)$ that as a vector space over K has dimension 2. Using lemma 3.6 we can construct an isomorphism $K(f) \cong K(\mathrm{i})$ of field extensions of K. Let $c, s \in K$ be such that $f \mapsto c+s\mathrm{i}$. Lastly, note that V is a one-dimensional vector space over $K(f)$ so we can find a $K(f)$-linear isomorphism $V \cong_{K(f)} K(f)$.

We now have a K-linear isomorphism $\sigma : V \to K(\mathrm{i})$. Define $\epsilon : \bigwedge^2 K(\mathrm{i}) \to K$ as $\epsilon(1 \wedge \mathrm{i}) = 1$. Let t be as in lemma 4.6. By construction $\sigma f \sigma^{-1}$ is multiplication by $c + s\mathrm{i}$. We can compute $\phi_{c+s\mathrm{i}}(a + b\mathrm{i}) = \mathrm{sign}(a^2 + b^2)\mathrm{sign}(s)$ where $a + \mathrm{i}b \neq 0$. By proposition 3.3 we see that $\mathrm{sign}(a^2 + b^2) = 1$. Using lemma 4.6 we see that $\phi_f(p) = \mathrm{sign}(t)\mathrm{sign}(s)$, which is independent of p. Also note that t and s are non-zero hence $\phi_f(p)$ is non-zero. □

Now using lemma 4.7 and lemma 4.8 we can make the following definition.

Definition 4.9. *Let $X \subseteq \mathrm{Aut}_K(V, \delta)$ be the set of non-hyperbolic maps. Then we define* $\mathrm{sign} : X \to \{-1, 0, 1\}$ *given by*

$$\mathrm{sign}(f) = \begin{cases} 1 \text{ if } \exists p \in \mathbb{P}(V) : \phi_f(p) = 1 \\ -1 \text{ if } \exists p \in \mathbb{P}(V) : \phi_f(p) = -1 \\ 0 \text{ else.} \end{cases}$$

Lemma 4.10. *Let $f \in \mathrm{Aut}_K(V, \delta)$ be non-hyperbolic. Then f is trivial if and only if* $\mathrm{sign}(f) = 0$.

Proof. If f is trivial then clearly $\mathrm{sign}(f) = 0$. If f is non-trivial then f cannot fix all points of $\mathbb{P}(V)$ by proposition 4.4. Hence, we see that ϕ_f is nonzero somewhere which means that $\mathrm{sign}(f) \neq 0$. □

Lemma 4.11. *Let $f, g \in \mathrm{Aut}_K(V, \delta)$ be non-hyperbolic. If $f \sim g$ then* $\mathrm{sign}(f) = \mathrm{sign}(g)$.

Proof. Say $h \in \mathrm{Aut}_K(V, \delta)$ such that $f = {}^h g$. Then we see that

$$\begin{aligned} \phi_f(v) &= \mathrm{sign}(\delta(v \wedge f(v))) \\ &= \mathrm{sign}(\delta(v \wedge hgh^{-1}(v))) \\ &= \mathrm{sign}(\det(h)\delta(h^{-1}(v) \wedge g(h^{-1}(v)))) \\ &= \phi_g(h^{-1}(v)). \end{aligned}$$

Because $h^{-1} : \mathbb{P}(V) \to \mathbb{P}(V)$ is a bijection we conclude that $\mathrm{sign}(f) = \mathrm{sign}(g)$. □

We conclude with an explicit method of calculating the sign.

Lemma 4.12. *Let $f \in \mathrm{Aut}_K(V, \delta)$ be non-hyperbolic, choose a basis, say e_1, e_2, such that $\delta(e_1 \wedge e_2) = 1$ for V and write $A_f = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ for the matrix of f on this basis. Then* $\mathrm{sign}(f) = \mathrm{sign}(a_{21} - a_{12})$.

Proof. Explicit calculations show that $\phi_f(e_1) = \mathrm{sign}(a_{21})$ and $\phi_f(e_2) = \mathrm{sign}(-a_{12})$. If f is trivial then we see that $a_{21} = a_{12} = 0$ and so indeed $\mathrm{sign}(f) = \mathrm{sign}(a_{21} - a_{12})$. If f is nontrivial then by proposition 4.4 we see that f has at most 1 fixed point of $\mathbb{P}(V)$ so we must have that $\mathrm{sign}(f) = \mathrm{sign}(a_{21})$ or $\mathrm{sign}(f) = \mathrm{sign}(-a_{12})$; note that e_1 and e_2 are representatives of different points in $\mathbb{P}(V)$. By lemma 4.7 and lemma 4.8 we see that if $\mathrm{sign}(f) \neq \mathrm{sign}(a_{12})$ then $\mathrm{sign}(a_{12}) = 0$ and similarly if $\mathrm{sign}(f) \neq \mathrm{sign}(-a_{21})$ then $\mathrm{sign}(-a_{21}) = 0$. Thus we see that $\mathrm{sign}(f) = \mathrm{sign}(\mathrm{sign}(a_{21}) + \mathrm{sign}(-a_{12})) = \mathrm{sign}(a_{21} - a_{12})$. □

4.2 Proof of the classification

Now we prove the classification of the conjugacy classes of $\mathrm{Aut}_K(V, \delta)$.

Theorem 4.13. *Let $\epsilon, \eta \in \mathrm{Aut}_K(V, \delta)$.*

1. *If $|\mathrm{Tr}(\epsilon)| > 2$ then $\epsilon \sim \eta \iff \mathrm{Tr}(\epsilon) = \mathrm{Tr}(\eta)$.*
2. *If $|\mathrm{Tr}(\epsilon)| \leq 2$ then $\epsilon \sim \eta \iff \mathrm{Tr}(\epsilon) = \mathrm{Tr}(\eta)$ and $\mathrm{sign}(\epsilon) = \mathrm{sign}(\eta)$.*

Proof. Write $\mathrm{Aut}_K(V, \pm\delta)$ for the group of linear automorphisms of V that act as $\pm\mathrm{id}$ on $\bigwedge^2 V$. Now we note that $\mathrm{Z}(\mathrm{Aut}_K(V)) \cong K^*$ and that $\mathrm{Aut}_K(V) = \mathrm{Aut}_K(V, \pm\delta)\mathrm{Z}(\mathrm{Aut}_K(V))$ because the index $(K^* : (K^*)^2) = 2$. Thus we see using lemma 2.5 and lemma 4.3 that two linear maps of determinant 1 are conjugate in $\mathrm{Aut}_K(V, \pm\delta)$ if and only if they have the same trace. Lastly, we note that the index $(\mathrm{Aut}_K(V, \pm\delta) : \mathrm{Aut}_K(V, \delta)) = 2$.

Now choose a basis $v_1, v_2 \in V$ such that $\delta(v_1 \wedge v_2) = 1$.

Proof of 1. We note that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{Aut}_K(V, \pm\delta) \backslash \mathrm{Aut}_K(V, \delta)$ and that for all $\lambda \in K^*$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}.$$

Now using lemma 2.7 and using the fact that for every $t \in K$ with $|t| > 2$ there exists $\lambda \in K$ such that $t = \lambda + 1/\lambda$ we conclude that two hyperbolic linear maps of $\mathrm{Aut}_K(V, \delta)$ are conjugate if and only if they have equal trace.

Proof of 2. $\Longrightarrow$ follows from lemma 4.11 and lemma 4.3. For $\Longleftarrow$ we know that, by corollary 2.6, conjugacy classes split in at most two and we see that for all $\theta \in L$

$$\mathrm{sign}(\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}) \neq \mathrm{sign}(\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix})$$
$$\mathrm{sign}(\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}) = 1 \neq -1 = \mathrm{sign}(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})$$
$$\mathrm{sign}(\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}) = 1 \neq -1 = \mathrm{sign}(\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}).$$

Note that by lemma 3.14 every elliptic matrix is conjugate under $\mathrm{Aut}_K(V, \pm\delta)$ to a matrix of the form $\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$.

Lastly, we note that $\mathrm{sign}(\epsilon) = 0$ if and only if $\epsilon = \pm 1$. This proves $\Longleftarrow$. ☐

We categorise the conjugacy classes of $\mathrm{SL}_2(K)$ as follows.

Definition 4.14. *Let $\lambda \in K_{|\lambda|>1}, x, y \in \{\pm 1\}$ and $\alpha \in (0, 2\pi) \subseteq L$ but $\alpha \neq \pi$. Then we define the following:*

1. *$\mathfrak{c}_{\mathrm{p}}^{xy}$ is the conjugacy class of the matrix $\left(\begin{smallmatrix} x & 0 \\ y & x \end{smallmatrix}\right)$*
2. *$\mathfrak{c}_{\mathrm{e}}^{\alpha}$ is the conjugacy class of the matrix $\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$*
3. *$\mathfrak{c}_{\mathrm{h}}^{\lambda}$ is the conjugacy class of the matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$.*

The conjugacy classes of 1 and -1 will be labeled just 1 respectively -1 and are called the trivial conjugacy classes.

Note that theorem 4.13 proves that we have now named each conjugacy class of $\mathrm{SL}_2(K)$ exactly once.

4.3 Properties of the conjugacy classes

Because the following sections will involve a lot of computations involving matrices we will choose a basis $v_1, v_2 \in V$ such that $\delta(v_1 \wedge v_2) = 1$. This then gives an isomorphism $\mathrm{SL}_2(K) \cong \mathrm{Aut}_K(V, \delta)$. In this section we prove various properties of the conjugacy classes that will be needed later.

Lemma 4.15. *Let* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$*. Then we have* $a_{11}^2 + a_{12}^2 + a_{21}^2 + a_{22}^2 \geq 2$.

Proof. We first note that $(a_{11}^2 + a_{21}^2)(a_{12}^2 + a_{22}^2) = (a_{11}a_{12} + a_{21}a_{22})^2 + (a_{11}a_{22} - a_{21}a_{12})^2 = (a_{11}a_{12} + a_{21}a_{22})^2 + 1$. By proposition 3.3 we conclude that $(a_{11}^2 + a_{21}^2)(a_{12}^2 + a_{22}^2) \geq 1$.

Let $x \in K$ be such that $x > 0$ and $x^2 = a_{11}^2 + a_{21}^2$ and similarly let $y \in K$ be such that $y > 0$ and $y^2 = a_{12}^2 + a_{22}^2$. Note that because $a_{11}^2 + a_{21}^2$ and $a_{12}^2 + a_{22}^2$ are positive they must have a square root by lemma 3.5, and they have a positive square root because z and $-z$ for $z \in K$ square to the same element. Therefore, x and y exist. Now we must have that $xy \geq 1$ because if $xy < 1$ then we have $0 < xy < 1$ and so $0 < x^2y^2 < 1$ which contradicts $x^2y^2 \geq 1$.

Lastly, we note that $2xy \leq x^2 + y^2$ because $(x - y)^2 \geq 0$ by proposition 3.3. Thus we conclude that $2 \leq 2xy \leq x^2 + y^2 = a_{11}^2 + a_{12}^2 + a_{21}^2 + a_{22}^2$. □

We note that $(a_{11} + a_{22})^2 + (a_{21} - a_{12})^2 = a_{11}^2 + a_{12}^2 + a_{21}^2 + a_{22}^2 + 2 \geq 4$. Thus we get the following corollary.

Corollary 4.16. *Let* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$*. Then we have that* $(a_{11}+a_{22})^2+(a_{21}-a_{12})^2 \geq 4$.

Lemma 4.17. *Let* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{e}}^{\alpha}$ *with* $\alpha \in (0, \pi) \subseteq L$*. Then we have that* $a_{21} - a_{12} \geq 2\sin(\alpha)$*.*

Proof. We see by lemma 4.3 that $a_{11} + a_{22} = 2\cos(\alpha)$. Hence, using corollary 4.16 we find that $(a_{21} - a_{12})^2 \geq 4 - (2\cos(\alpha))^2 = 4\sin(\alpha)^2$. Now we note that $\alpha \in (0, \pi)$, thus $\sin(\alpha) > 0$. Also because the sign of $\mathfrak{c}_{\mathrm{e}}^{\alpha}$ is 1 we see that by lemma 4.12 that $a_{21} - a_{12} > 0$. Therefore we have that $a_{21} - a_{12} \geq 2\sin(\alpha)$. □

Lemma 4.18. *Let* $f = \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{e}}^{\alpha}$ *with* $\alpha \in (0, \pi) \subseteq L$*. Then* $a_{12} < 0, a_{21} > 0$*. Moreover, if* $x \in K_{\geq 2\sin(\alpha)}$ *respectively* $y \in K_{\leq -2\sin(\alpha)}$ *then there exists* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{e}}^{\alpha}$ *such that* $a_{21} = x$ *respectively* $a_{12} = y$*. Similarly, for every* $x \in K_{\geq 2\sin(\alpha)}$ *there exists* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{e}}^{\alpha}$ *such that* $a_{21} - a_{12} = x$*.*

Proof. We see that $\phi_f((1, 0)) = a_{21}$. Because $\mathrm{sign}(f) = 1$ and by lemma 4.8 we see that $a_{21} > 0$. Similarly, we see that $\phi_f((0, 1)) = -a_{12} > 0$. Hence, $a_{12} < 0$.

Now let $x \in K_{\geq 2\sin(\alpha)}$ and let $\gamma \in K_{>0}$ be such that $\gamma\sin(\alpha) = x$. Then we see that

$$\begin{pmatrix} \cos(\alpha) & (-1/\gamma)\sin(\alpha) \\ \gamma\sin(\alpha) & \cos(\alpha) \end{pmatrix} \in \mathfrak{c}_{\mathrm{e}}^{\alpha}.$$

Similarly, one can prove the analogous statement for $y \in K_{\leq -2\sin(\alpha)}$.

Lastly, let $x \in K_{\geq 2\sin(\alpha)}$. Note that $\gamma \mapsto \gamma + 1/\gamma$ is a function from $K_{>0}$ that surjects onto $[2, \infty)$. Thus let $\gamma \in K_{>0}$ be such that $(\gamma + 1/\gamma)\sin(\alpha) = x$. Note that $x/\sin(\alpha) \geq 2$. Again we see that

$$\begin{pmatrix} \cos(\alpha) & (-1/\gamma)\sin(\alpha) \\ \gamma\sin(\alpha) & \cos(\alpha) \end{pmatrix} \in \mathfrak{c}_{\mathrm{e}}^{\alpha}.$$

□

Lemma 4.19. *Let* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$. *Then* $a_{12} \leq 0, a_{21} \geq 0$ *and not both equal to zero. Moreover, if* $x \in K_{\geq 0}$ *respectively* $y \in K_{\leq 0}$ *then there exists* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$ *such that* $a_{21} = x$ *respectively* $a_{12} = y$. *Similarly, for every* $x \in K_{>0}$ *there exists* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$ *such that* $a_{21} - a_{12} = x$.

Proof. The proof of the first part is analogous to the proof of 4.18 except now we use lemma 4.7.

For the second and third part we just consider the matrices $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$ and $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$. □

Lemma 4.20. *Let* $\mathfrak{c}$ *be a non-trivial conjugacy class of* $\mathrm{SL}_2(K)$. *Then for every* $a_{11} \in K$ *there exist* $a_{12}, a_{21}, a_{22} \in K$ *such that* $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right) \in \mathfrak{c}$.

Proof. Let $t = \mathrm{Tr}(\mathfrak{c})$. The matrix $\left(\begin{smallmatrix} a & 1 \\ a(t-a)-1 & t-a \end{smallmatrix}\right)$ also has trace t. If the sign of A does not equal the sign of $\mathfrak{c}$, all we have to do is flip the off diagonal. Therefore we have found a matrix in $\mathfrak{c}$ of the form $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$. □

5 Proof of main theorem

5.1 Symmetries

In this section we prove the main result of the thesis. We first apply the theory of section 2.2 to the case $\mathrm{SL}_2(K)$. There are only two automorphisms that we have for every Euclidean field K, namely the identity and the inverse transpose. We also don't always have non-trivial automorphisms of the field K hence this is every automorphism we are guaranteed to have. The transpose has no effect on the trace of a conjugacy class and if the conjugacy class has a sign then it switches the sign. So we see that on the set of conjugacy classes the inverse transpose acts as the identity.

Another well known fact is that $\mathrm{Z}(\mathrm{SL}_2(K)) = \{\pm 1\}$. So we see that

$$(\mathrm{SL}_2(K))_* = \{(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)\} \cong \mathrm{V}_4.$$

Because $(-A)^{-1} = -(A)^{-1}$ for $A \in \mathrm{SL}_2(K)$, we find that h commutes with the symmetries from $(\mathrm{SL}_2(K))_*$. We give the following names to these elements: $\mathrm{v}_1 = (1,-1,-1), \mathrm{v}_2 = (-1,1,-1)$ and $\mathrm{v}_3 = (-1,-1,1)$.

All this gives us 8 unique symmetries of W which do not permute the conjugacy classes and a total of 48 symmetries on W. Thus, we are guaranteed to have a subgroup $\mathrm{V}_4 \rtimes (\mathrm{S}_3 \times \langle \mathrm{h} \rangle) \subseteq \mathrm{WSym}(\mathrm{SL}_2(K))$. The following lemma will be useful when working with these symmetries.

Lemma 5.1. *Let* $C \in \mathrm{SL}_2(K)/\sim$. *Then* $\mathrm{Tr}(-C) = -\mathrm{Tr}(C)$ *and* $\mathrm{Tr}(C^{-1}) = \mathrm{Tr}(C)$. *Moreover, if we assume* C *has a sign then* $-C$ *and* C^{-1} *have a sign and* $\mathrm{sign}(-C) = -\mathrm{sign}(C)$ *and* $\mathrm{sign}(C^{-1}) = -\mathrm{sign}(C)$.

□

Lemma 5.2. *Let* $(B, C, D) \in (\mathrm{SL}_2(K)/\sim)^3$ *such that all three are non-trivial. Assume that all three have a sign and that all three have non-zero trace. Then by applying symmetries in* $\mathrm{WSym}(\mathrm{SL}_2(K))$ *we can reduce this triple to a triple such that the signs and the signs of the traces of the first two are positive.*

Proof. It is clear from lemma 5.1 that we only need to keep track of the signs of the traces and the signs. Let $X = \{-1,1\}^6$ and let $Y \subseteq W$ be the set of triples such that all three classes have a non-zero sign and a non-zero trace. Then we define $\phi : Y \to X$ by $\phi((B,C,D)) = (\mathrm{sign}(\mathrm{Tr}(B)), \mathrm{sign}(B), \mathrm{sign}(\mathrm{Tr}(C)), \mathrm{sign}(C), \mathrm{sign}(\mathrm{Tr}(D)), \mathrm{sign}(D))$. Define an action of the group $\mathrm{WSym}(\mathrm{SL}_2(K))$ on X such that ϕ is compatible with both actions.

Now by applying symmetries we can write every element of X as $(+,+,+,\pm,\pm,\pm)$. The four cases where the second class doesn't have positive sign can be resolved using the following symmetries.

- for $(+,+,+,-,+,+)$ apply (23).
- for $(+,+,+,-,+,-)$ apply (13)h.
- for $(+,+,+,-,-,+)$ apply (13)hv$_2$.
- for $(+,+,+,-,-,-)$ apply (23)v$_1$.

□

Lemma 5.3. *Let $(B,C,D) \in (\mathrm{SL}_2(K))^3$ such that none are hyperbolic or trivial. Then we can apply a symmetry of W to this triple such that the first two classes of the resulting triple are $\mathfrak{c}_{\mathrm{p}}^{++}$ or $\mathfrak{c}_{\mathrm{e}}^{\alpha}$ with $0 < \alpha \leq \pi/2$.*

Proof. If there are no classes with zero trace then the lemma is just a reformulation of lemma 5.2. If there are classes with zero trace then we just choose a non-zero sign for the trace and use lemma 5.2 to find a symmetry which transforms the associated element in X into an element of which the first four coordinates are positive. After applying this symmetry to the triple (B,C,D) we might however find that a class has zero trace and positive sign. This class is $\mathfrak{c}_{\mathrm{e}}^{\pi/2}$. □

5.2 Products of classes with positive trace and sign

We now wish to compute the products of conjugacy classes. Lemma 2.8 suggests a method of computing the products. Namely, given two conjugacy classes $B, C \subseteq \mathrm{SL}_2(K)$ we first compute the set $\mathrm{Tr}(BC) \subseteq K$. Then for any $x \in \mathrm{Tr}(BC)$ with $|x| \leq 2$ we compute what classes with trace equal to x are contained in BC. The symmetries of W will allow us to only have to compute the products of a subset of the set of conjugacy classes of $\mathrm{SL}_2(K)$. We have chosen the set of conjugacy classes of non-negative trace and positive or no sign. Note that by the symmetries of W we see that $BC = CB$.

Lemma 5.4. *Let $B = C = \mathfrak{c}_{\mathrm{p}}^{++}$ and $D \in \mathrm{SL}_2(K)/\sim$ be such that $D \subseteq BC$. Then $\mathrm{Tr}(D) \in (-\infty, 2]$. Moreover, if $x \in (-\infty, 2]$ then there exists $D' \in \mathrm{SL}_2(K)/\sim$ such that $D' \subseteq BC$ and $\mathrm{Tr}(D') = x$.*

Proof. Let $b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in B$. By lemma 2.8 there are $c \in C$ and $d \in D$ such that $d = bc$. Write $c = \left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right) \in C$. We now note by lemma 4.3 that $\mathrm{Tr}(d) = \mathrm{Tr}(D)$. Hence, we see that $\mathrm{Tr}(D) = \mathrm{Tr}(bc) = c_{11} + c_{22} + c_{12}$. Now again by lemma 4.3 we see that $c_{11} + c_{22} = 2$ and by lemma 4.19 that $c_{12} \leq 0$. Hence, we find that $\mathrm{Tr}(D) \leq 2$.

Let $x \in (-\infty, 2]$. Now using lemma 4.19 we let $\left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right) \in \mathfrak{c}_{\mathrm{p}}^{++}$ such that $c_{12} = x - 2$. Then we see that $\mathrm{Tr}(\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right)) = c_{11} + c_{22} + c_{12} = 2 + x - 2 = x$. So choose D' as the class of the product of these two matrices. □

Lemma 5.5. *Let $0 < \alpha \leq \pi/2$, $B = \mathfrak{c}_{\mathrm{e}}^{\alpha}$, $C = \mathfrak{c}_{\mathrm{p}}^{++}$ and $D \in \mathrm{SL}_2(K)/\sim$ such that $D \subseteq BC$. Then $\mathrm{Tr}(D) \in (-\infty, 2\cos(\alpha))$. Moreover, if $x \in (-\infty, 2\cos(\alpha))$ then there exists $D' \in \mathrm{SL}_2(K)/\sim$ such that $D' \subseteq BC$ and $\mathrm{Tr}(D') = x$.*

Proof. The proof is analogous to the proof of lemma 5.4. For this proof choose $b = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$. □

Lemma 5.6. *Let* $0 < \alpha, \beta \leq \pi/2$ *but not both equal to* $\pi/2$*,* $B = \mathfrak{c}_{\mathrm{e}}^{\alpha}$*,* $C = \mathfrak{c}_{\mathrm{e}}^{\beta}$ *and* $D \in \mathrm{SL}_2(K)/\sim$ *such that* $D \subseteq BC$*. Then* $\mathrm{Tr}(D) \in (-\infty, 2\cos(\alpha+\beta)]$*. Moreover, if* $x \in (-\infty, 2\cos(\alpha+\beta)]$ *then there exists* $D' \in \mathrm{SL}_2(K)/\sim$ *such that* $D' \subseteq BC$ *and* $\mathrm{Tr}(D') = x$*.*

Proof. The proof is analogous to the proof of lemma 5.4. For this proof choose $b = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$. □

Lemma 5.7. *Let* $B = \mathfrak{c}_{\mathrm{e}}^{\pi/2}$*,* $C = \mathfrak{c}_{\mathrm{e}}^{\pi/2}$ *and* $D \in \mathrm{SL}_2(K)/\sim$ *such that* $D \subseteq BC$*. Then* $\mathrm{Tr}(D) \in (-\infty, -2]$*. Moreover, if* $x \in K_{\leq 2}$ *then there exists* $D' \in \mathrm{SL}_2(K)/\sim$ *with* $D' \subseteq BC$ *and* $\mathrm{Tr}(D') = x$*.*

Proof. The proof is analogous to the proof of lemma 5.4. For this proof choose $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. □

Lemma 5.8. *Let* $\lambda \in K$ *such that* $|\lambda| > 1$*. Then for all non-trivial conjugacy classes* $\mathfrak{c}$ *we have that* $\mathrm{Tr}(\mathfrak{c}\mathfrak{c}_{\mathrm{h}}^{\lambda}) = K$*.*

Proof. Let $r \in K$ and let $a_{11} = \frac{r - \mathrm{Tr}(\mathfrak{c})\lambda^{-1}}{\lambda - \lambda^{-1}}$. Then we let $a \in \mathfrak{c}$ such that the top left coordinate equals a_{11}, which exists due to lemma 4.20. Let $b = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. Now we see that $\mathrm{Tr}(ab) = a_{11}\lambda + a_{22}\lambda^{-1} = (a_{11} + a_{22})\lambda^{-1} + a_{11}(\lambda - \lambda^{-1}) = r$. □

We summarise the results in the following corollary.

Corollary 5.9. *Let* $B, C \subseteq \mathrm{SL}_2(K)$ *be conjugacy classes with non-negative trace and positive or no sign.*

- *If both* B, C *are parabolic then* $\mathrm{Tr}(BC) = (-\infty, 2]$*.*
- *If* $B = \mathfrak{c}_{\mathrm{e}}^{\alpha}, C = \mathfrak{c}_{\mathrm{p}}^{++}$ *then* $\mathrm{Tr}(BC) = (-\infty, 2\cos(\alpha))$*.*
- *If* $B = \mathfrak{c}_{\mathrm{e}}^{\alpha}, C = \mathfrak{c}_{\mathrm{e}}^{\beta}$ *but not both have zero trace then* $\mathrm{Tr}(BC) = (-\infty, 2\cos(\alpha+\beta))$*.*
- *If* B, C *are elliptic with zero trace then* $\mathrm{Tr}(BC) = (-\infty, -2]$*.*
- *If* B *or* C *is hyperbolic then* $\mathrm{Tr}(BC) = K$*.*

The following lemma computes the sign of every conjugacy class with sign in the product except for the case where B and C are both hyperbolic.

Lemma 5.10. *Let* $B, C \subseteq \mathrm{SL}_2(K)$ *be conjugacy classes with non-negative trace and positive or no sign and at least one has a sign. Let* $D \subseteq BC$ *be a conjugacy class with a sign. Then* $\mathrm{sign}(D) = 1$ *if* B *or* C *has non-zero trace, and* $\mathrm{sign}(D) = 0$ *if* B *and* C *have zero trace.*

Proof. Because $BC = CB$ we may assume that C has a sign. We use lemma 2.8 and lemma 4.13 to choose $b = \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix}$ where $t \geq 0$ is the trace. Let $c \in C$ be such that bc has a sign. Then we see that $\mathrm{sign}(bc) = \mathrm{sign}(\mathrm{Tr}(c) - c_{12}t)$. Now if both B and C have zero trace then we see that $\mathrm{sign}(bc) = 0$ by lemma 4.12. Hence, $\mathrm{sign}(D) = 0$. If at least one of the traces is non-zero then we see that $\mathrm{Tr}(c) > 0$ or $t > 0$. Note that if $\mathrm{Tr}(c) = 0$ then c is elliptic and so $c_{12} < 0$ by lemma 4.18 so $\mathrm{sign}(D) = \mathrm{sign}(bc) = 1$. Otherwise we see that $c_{12} \leq 0$ by lemma 4.19 and 4.18 because c must be elliptic or parabolic. So we see that $\mathrm{Tr}(C) - c_{12}t > 0$. Therefore $\mathrm{sign}(D) = \mathrm{sign}(bc) = 1$ by lemma 4.12. □

5.3 The main theorem

In this section we prove the main theorem of this thesis. First we make the following definition.

Definition 5.11. *Let $X \subseteq \mathrm{SL}_2(K)$ be the set of non-hyperbolic matrices. Let $L \oplus \mathbb{Z}\epsilon$ be the extended winding group of K, see definition 3.16. We define $\theta : X \to L \oplus \mathbb{Z}\epsilon$ as:*

- *For $\alpha \in (0, 2\pi)\backslash\{\pi\}$ we define $\theta(\mathfrak{c}_{\mathrm{e}}^{\alpha}) = \alpha$ if $\alpha \in (0, \pi)$ and $\theta(\mathfrak{c}_{\mathrm{e}}^{\alpha}) = \alpha - \pi$ if $\alpha \in (\pi, 2\pi)$.*
- *For $x, y, \in \{\pm 1\}$ we define $\theta(\mathfrak{c}_{\mathrm{p}}^{xy}) = \epsilon$ if $xy = 1$ and $\theta(\mathfrak{c}_{\mathrm{p}}^{xy}) = \pi - \epsilon$ if $xy = -1$.*
- *For $\mathfrak{c}$ a trivial conjugacy class we define $\theta(\mathfrak{c}) = 0$.*

Remark 5.12. For all non-hyperbolic $A \in \mathrm{SL}_2(K)$ we see that $\theta(A) = \theta(-A)$. This means that θ is also well defined on $X/\{\pm 1\} \subseteq \mathrm{PSL}_2(K)$. The group $\mathrm{PSL}_2(K)$ acts on the hyperbolic plane over K and if A is elliptic then A is a rotation of the hyperbolic plane around an angle of $2\theta(A)$. This gives a connection between this thesis and Daan Heus's thesis, see [2].

Theorem 5.13. *Let B, C, D be non-trivial conjugacy classes of $\mathrm{SL}_2(K)$, where K is a Euclidean field. There are three cases:*

1. *If at least two of B, C, D are hyperbolic then $1 \in BCD$.*
2. *If exactly one of the three classes, say B, is hyperbolic then $1 \in BCD$ if and only if $\mathrm{sign}(\mathrm{Tr}(B))\mathrm{sign}(C)\mathrm{sign}(D) = -1$.*
3. *If none are hyperbolic then $1 \in BCD$ if and only if one of the following holds:*
   (i) $\mathrm{sign}(B, C, D) = -1$ *and* $\theta(B, C, D) \leq \pi$
   (ii) $\mathrm{sign}(B, C, D) = 1$ *and* $\theta(B, C, D) \geq 2\pi$.

The proof of 5.13.1 and 5.13.2 are simple enough that we can do them right now.

Proof of 5.13.1 and 5.13.2. We start with 5.13.1. Say at least two classes are hyperbolic, say B and C. Using lemma 5.8 we see that there is a class E such that $\mathrm{Tr}(E) = \mathrm{Tr}(D)$ and $1 \in BCE$. Say D is hyperbolic then using theorem 4.13 we see that $E = D$ and so $1 \in BCD$. If D is not hyperbolic then it has a sign. Using theorem 4.13 and lemma 5.1 we see that $B^{-1} = B$ and $C = C^{-1}$. Hence, using lemma 2.10 we see that $1 \in BCD$ if and only if $1 \in BC(D^{-1})$. Because D is non-trivial and by lemma 5.1 we see that $\mathrm{sign}(D) \neq \mathrm{sign}(D^{-1})$ and $\mathrm{Tr}(D) = \mathrm{Tr}(D^{-1})$. Using theorem 4.13 we have $E = D$ or $E = D^{-1}$. Thus we have proved $1 \in BCD$. This proves 5.13.1.

Now we prove part 5.13.2. Say only B is hyperbolic. If B and C have negative trace then we apply v_3 to the triple (B, C, D). If B has negative trace and C has positive trace then we apply v_2. Next, if the resulting C has negative sign then we apply h to the triple. Using lemma 5.1 we see that this gives a triple (B', C', D') of classes such that $1 \in BCD$ if and only if $1 \in B'C'D'$ and B' is hyperbolic with positive trace and C' has positive sign. Using lemma 5.10 we see that $1 \in B'C'D'$ if and only if $\mathrm{sign}(\mathrm{Tr}(B'))\mathrm{sign}(C')\mathrm{sign}(D') = -1$. So we see that $1 \in BCD$ if and only if $\mathrm{sign}(\mathrm{Tr}(B'))\mathrm{sign}(C')\mathrm{sign}(D') = -1$. Noting that the symmetries h, v_2 and v_3 keep $\mathrm{sign}(\mathrm{Tr}(B'))\mathrm{sign}(C')\mathrm{sign}(D') = -1$ invariant shows that $1 \in BCD$ if and only if $\mathrm{sign}(\mathrm{Tr}(B))\mathrm{sign}(C)\mathrm{sign}(D) = -1$. This proves 5.13.2. □

The proof of 5.13.3 is similar to the proof of 5.13.2 however we want to use lemma 5.3 which does not specify what symmetries need to be performed.

Definition 5.14. *Let $W' \subseteq (\mathrm{SL}_2(K)/\sim)^3$ be the set of triples satisfying conditions (i) and (ii) of 5.13.3 where none of B, C, D are hyperbolic or trivial. Let $W^* \subseteq W$ be the set of elements such that none of three classes are trivial or hyperbolic.*

5.13.3 is proven if we show that $W^* = W'$. We will prove the theorem after proving the following lemmas.

Lemma 5.15. *Let $B, C, D \in \mathrm{SL}_2(K)/{\sim}$ be parabolic or elliptic. The symmetries of* S_3 *and* $\mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3$ *keep $\theta(B, C, D)$ and* $\mathrm{sign}(B, C, D)$ *invariant. Lastly, we also have that:* $\mathrm{sign}(\mathrm{h}(B, C, D)) = -\mathrm{sign}(B, C, D)$ *and* $\theta(\mathrm{h}(B, C, D)) = \pi - \theta(B, C, D)$.

□

Corollary 5.16. *The group* $\mathrm{WSym}(\mathrm{SL}_2(K))$ *also acts in the same way on W'.*

The following corollary is a simple consequence of lemma 5.1.

Corollary 5.17. *The group* $\mathrm{WSym}(\mathrm{SL}_2(K))$ *also acts in the same way on W^*.*

Lemma 5.18. *Let $(B, C, D) \in (\mathrm{SL}_2(K)/{\sim})^3$ such that all three are parabolic or elliptic. Furthermore, assume that the classes B and C have positive sign and have non-negative trace. Then $(B, C, D) \in W^*$ if and only if $(B, C, D) \in W'$.*

Proof. Say $(B, C, D) \in W^*$. Then by lemma 2.1 we see that $D^{-1} \subseteq BC$. Now there are three cases. Say $B = \mathfrak{c}_\mathrm{e}^\alpha$ and $C = \mathfrak{c}_\mathrm{e}^\beta$ with $\alpha, \beta \in (0, 2\pi)$. Now we see that $\alpha, \beta \in (0, \pi/2]$ because both have positive sign and non-negative trace. First assume that not both are $\pi/2$. Lemma 5.6 now tells us that $\mathrm{Tr}(D) = \mathrm{Tr}(D^{-1}) \leq 2\cos(\alpha + \beta)$ and $\mathrm{sign}(D) = -\mathrm{sign}(D^{-1}) = -1$. If $D = \mathfrak{c}_\mathrm{e}^\gamma$ is elliptic then we see that $\gamma \in (\pi, 2\pi)$ and $\cos(\gamma) \leq \cos(\alpha + \beta)$. The last inequality implies that $2\pi - \gamma \geq \alpha + \beta$. This gives $\pi \geq \alpha + \beta + \gamma - \pi$. Now we see that $(B, C, D) \in W'$ because $\mathrm{sign}(B, C, D) = -1$ and $\theta(B, C, D) \leq \pi$. If D is parabolic then we must have that $D = \mathfrak{c}_\mathrm{p}^{--}$ because $\mathrm{Tr}(D) \leq 2\cos(\alpha + \beta) < 2$ and $\mathrm{sign}(D) = -1$. Because $\alpha + \beta < \pi$ we find that $\alpha + \beta + \epsilon < \pi$. Therefore $(B, C, D) \in W'$ because $\mathrm{sign}(B, C, D) = -1$ and $\theta(B, C, D) \leq \pi$. If $\alpha = \beta = \pi/2$ then using lemma 5.7 we see that D can't be parabolic or elliptic. So this case doesn't occur.

The proof of the other two cases where B is elliptic and C is parabolic and where they both are parabolic is similar.

Now say $(B, C, D) \in W'$. There are again three cases. Say $B = \mathfrak{c}_\mathrm{e}^\alpha$ and $C = \mathfrak{c}_\mathrm{e}^\beta$ with $\alpha, \beta \in (0, \pi/2]$. Both B and C have positive sign. Note that $\theta(B, C, D) = \theta(B) + \theta(C) + \theta(D) \leq \pi + \theta(D)$ because B and C have positive sign and non-negative trace. By definition we know that $\theta(D) < \pi$. So we see that $\theta(B, C, D) < 2\pi$. This means that we must have that $\mathrm{sign}(D) = -1$. Say $D = \mathfrak{c}_\mathrm{e}^\gamma$ is elliptic with $\gamma \in (\pi, 2\pi)$. Then we see that $\alpha + \beta + \gamma - \pi \leq \pi$. This means that $\alpha + \beta \leq 2\pi - \gamma$ which tells us that $\cos(\gamma) \leq \cos(\alpha + \beta)$. So we have found that $\mathrm{Tr}(D^{-1}) = 2\cos(\gamma) \leq 2\cos(\alpha + \beta)$ and $\mathrm{sign}(D^{-1}) = 1$. Lemma 5.6 now tells us that $D^{-1} \subseteq BC$. So we have that $1 \in BCD$. If D is parabolic then we must have that $D = \mathfrak{c}_\mathrm{p}^{--}$ because $\mathrm{sign}(D) = -1$ and so $\theta(D) \leq \pi - \alpha - \beta < \pi - \epsilon$. This means that $\theta(D) = \epsilon$. So we must have that $D = \mathfrak{c}_\mathrm{p}^{--}$. By lemma 5.6 we see that $D^{-1} = \mathfrak{c}_\mathrm{p}^{-+} \subseteq BC$. Thus $(B, C, D) \in W^*$ by lemma 2.1.

The proof of the other two cases is again similar. □

Proof of 5.13.3. Let $(B, C, D) \in (\mathrm{SL}_2(K)/{\sim})^3$ such that all three are parabolic or elliptic. Let σ be a symmetry such that $\sigma(B, C, D)$ is a triple where the first two classes have positive sign and non-negative trace, which exists due to lemma 5.3. Then using corollaries 5.16 and 5.17 and lemma 5.18 we find that

$$(B, C, D) \in W^* \iff \sigma(B, C, D) \in W^* \iff \sigma(B, C, D) \in W' \iff (B, C, D) \in W'.$$

This proves 5.13.3. □

References

[1] S. Orevkov. "Products of conjugacy classes in $SL\_2(R)$". In: *Trudy Mosk. Mat. Obsch. (Russian), Trans. of Moscow Math. (English)* (2019).

[2] D. Heus. "Machten van Commutatoren". In: (2023).

[3] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854.

[4] Bourbaki. N. *Algebra II.* Springer Berlin, Heidelberg, 1981. ISBN: 978-3-540-00706-7.

[5] L.S. Rieger. "On the ordered and cyclically ordered groups". In: *Vestnik Král. Ceské Spol. Náuk* (1946).

[6] L. Fuchs. *Partially ordered algebraic systems.* Vol. 28. Pergamon Press, 1963, pp. 61–65.