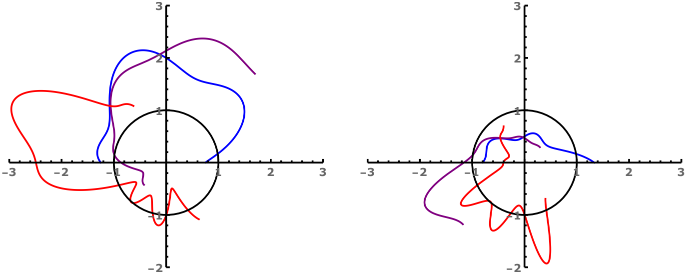
The Euclidean Algorithm in Circle/Sphere Packings

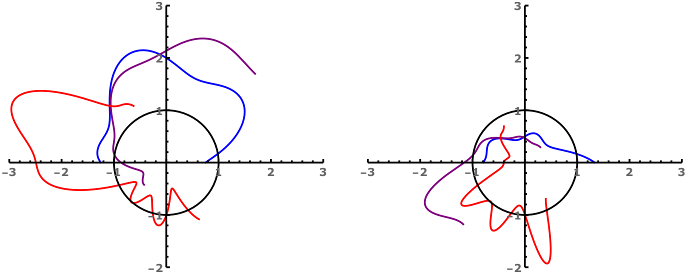
Arseniy (Senia) Sheydvasser

October 25, 2019

Circle/Sphere Inversions

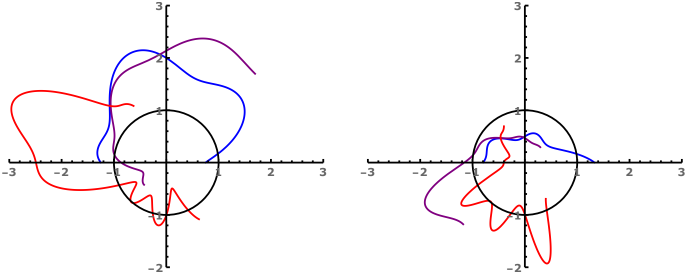


Circle/Sphere Inversions



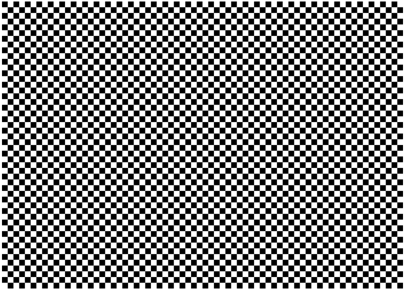
- Choose a circle C with center (x_0, y_0) and radius R.

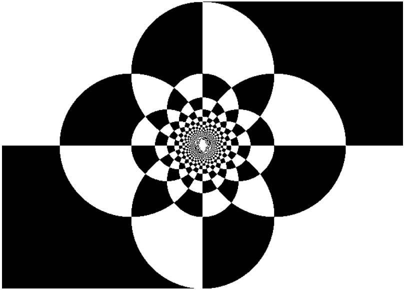
Circle/Sphere Inversions



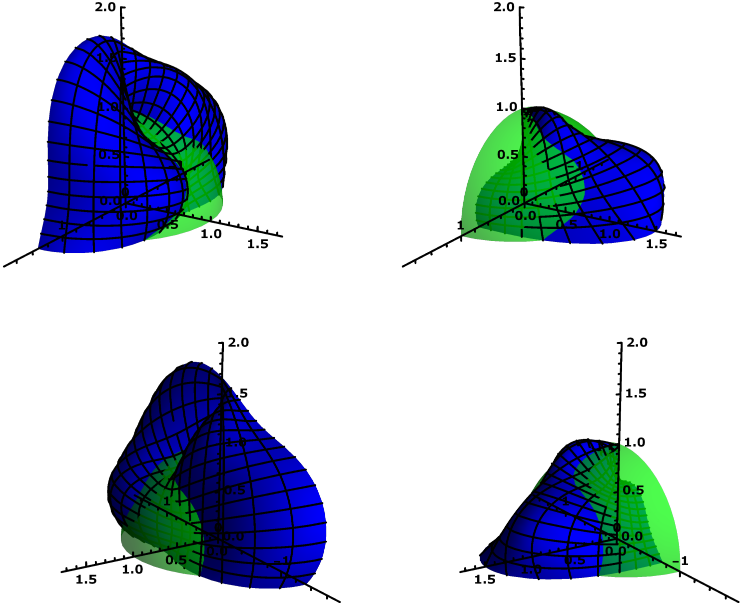
- Choose a circle C with center (x_0, y_0) and radius R.
- To invert a point (x, y) through, measure the distance r between (x_0, y_0) and (x, y), and move (x, y) to distance R/r from (x_0, y_0) (along the same ray).

Circle/Sphere Inversions





Circle/Sphere Inversions



Circle/Sphere Inversions

Definition

$\text{Möb}(\mathbb{R}^n)$ is the group generated by n-sphere reflections in $\mathbb{R}^n \cup \{\infty\}$.

Circle/Sphere Inversions

Definition

Möb($\mathbb{R}^n$) is the group generated by n-sphere reflections in $\mathbb{R}^n \cup \{\infty\}$.

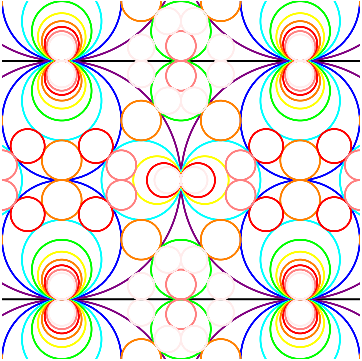
Question

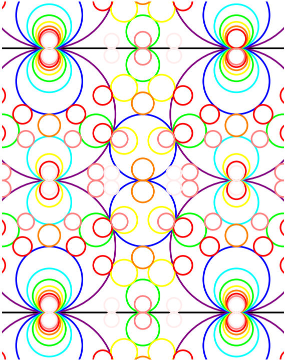
Let Γ be a subgroup of Möb($\mathbb{R}^n$), and S an n-sphere. What does the orbit $\Gamma.S$ look like? Can we compute it effectively?

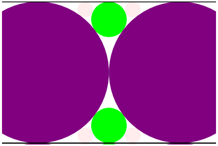
Motivation

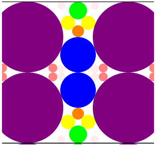
Question

What analogs of the Apollonian circle packing are there?





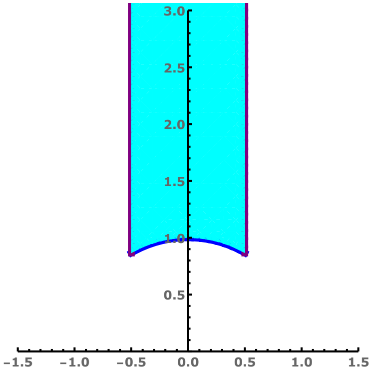




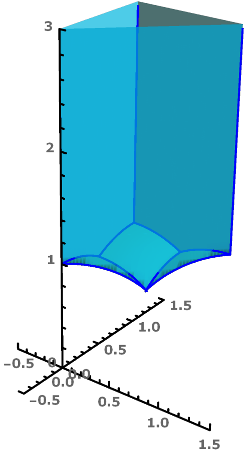
Motivation

Question

What do hyperbolic quotient manifolds $\mathbb{H}^n/\Gamma$ look like?

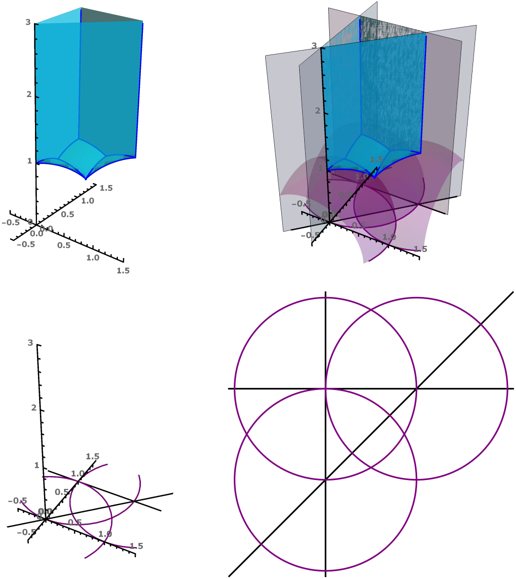


$SL(2, \mathbb{Z})$



$SL(2, \mathbb{Z}[i])$

Motivation



Accidental Isomorphisms

Question

How do you even represent elements in $\text{M\"ob}(\mathbb{R}^n)$*?*

Accidental Isomorphisms

Question

How do you even represent elements in Möb$(\mathbb{R}^n)$?

Möb$^0(\mathbb{R})$	$SL(2,\mathbb{R})/\{\pm 1\}$
Möb$^0(\mathbb{R}^2)$	$SL(2,\mathbb{C})/\{\pm 1\}$
Möb$^0(\mathbb{R}^3)$	
Möb$^0(\mathbb{R}^4)$	$SL(2,H)/\{\pm 1\}$
$\vdots$	

- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $SL(2,\mathbb{R})$ or $SL(2,\mathbb{C})$.
- $z \mapsto (az+b)(cz+d)^{-1}$ is an orientation-preserving Möbius transformation.
- $z \mapsto (a\overline{z}+b)(c\overline{z}+d)^{-1}$ is an orientation-reversing Möbius transformation.

Accidental Isomorphisms

Question

How do you even represent elements in Möb$(\mathbb{R}^n)$?

$\text{Möb}^0(\mathbb{R})$	$SL(2,\mathbb{R})/\{\pm 1\}$
$\text{Möb}^0(\mathbb{R}^2)$	$SL(2,\mathbb{C})/\{\pm 1\}$
$\text{Möb}^0(\mathbb{R}^3)$	???
$\text{Möb}^0(\mathbb{R}^4)$	$SL(2,H)/\{\pm 1\}$
$\vdots$	???

- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $SL(2,\mathbb{R})$ or $SL(2,\mathbb{C})$.
- $z \mapsto (az+b)(cz+d)^{-1}$ is an orientation-preserving Möbius transformation.
- $z \mapsto (a\bar{z}+b)(c\bar{z}+d)^{-1}$ is an orientation-reversing Möbius transformation.

Vahlen's Matrices

- Vahlen, 1901: For any n, there is an isomorphism between Möb($\mathbb{R}^n$) and a group of 2×2 matrices with entries in a (subset of a) Clifford algebra, quotiented by $\{\pm 1\}$.

Vahlen's Matrices

- Vahlen, 1901: For any n, there is an isomorphism between Möb($\mathbb{R}^n$) and a group of 2×2 matrices with entries in a (subset of a) Clifford algebra, quotiented by $\{\pm 1\}$.
- We'll consider the case $n = 3$, Möb($\mathbb{R}^3$).

Vahlen's Matrices

- Vahlen, 1901: For any n, there is an isomorphism between $\text{Möb}(\mathbb{R}^n)$ and a group of 2×2 matrices with entries in a (subset of a) Clifford algebra, quotiented by $\{\pm 1\}$.
- We'll consider the case $n = 3$, $\text{Möb}(\mathbb{R}^3)$.
- Define

$$(w + xi + yj + zk)^{\ddagger} = w + xi + yj - zk$$

and H^{+} = quaternions fixed by $\ddagger$ (i.e. with no k-component).

Vahlen's Matrices

- Vahlen, 1901: For any n, there is an isomorphism between $\text{Möb}(\mathbb{R}^n)$ and a group of 2×2 matrices with entries in a (subset of a) Clifford algebra, quotiented by $\{\pm 1\}$.
- We'll consider the case $n = 3$, $\text{Möb}(\mathbb{R}^3)$.
- Define

$$(w + xi + yj + zk)^{\ddagger} = w + xi + yj - zk$$

and $H^+ =$ quaternions fixed by $\ddagger$ (i.e. with no k-component).

$$SL^{\ddagger}(2, H) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}(2, H) \middle| ab^{\ddagger}, cd^{\ddagger} \in H^+, ad^{\ddagger} - bc^{\ddagger} = 1 \right\}$$

What is $SL^{\ddagger}(2, H)$ as a Group?

$$SL^{\ddagger}(2, H) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ab^{\ddagger}, cd^{\ddagger} \in H^{+}, ad^{\ddagger} - bc^{\ddagger} = 1 \right\}$$

What is $SL^{\ddagger}(2, H)$ as a Group?

$$SL^{\ddagger}(2,H) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ab^{\ddagger}, cd^{\ddagger} \in H^{+}, ad^{\ddagger} - bc^{\ddagger} = 1 \right\}$$

Equivalently,

$$SL^{\ddagger}(2,H) = \left\{ \gamma \in SL(2,H) \middle| \gamma \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix} \overline{\gamma}^{T} = \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix} \right\}$$

What is $SL^{\ddagger}(2,H)$ as a Group?

$$SL^{\ddagger}(2,H) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ab^{\ddagger}, cd^{\ddagger} \in H^{+}, ad^{\ddagger} - bc^{\ddagger} = 1 \right\}$$

Equivalently,

$$SL^{\ddagger}(2,H) = \left\{ \gamma \in SL(2,H) \middle| \gamma \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix} \overline{\gamma}^{T} = \begin{pmatrix} 0 & k \\ -k & 0 \end{pmatrix} \right\}$$

Inverses are given as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d^{\ddagger} & -b^{\ddagger} \\ -c^{\ddagger} & a^{\ddagger} \end{pmatrix}$$

Möb($\mathbb{R}^3$) as $SL^\ddagger(2, H)$

- There is an action on $\mathbb{R}^3 \cup \{\infty\} = H^+ \cup \{\infty\}$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .z = (az + b)(cz + d)^{-1}$$

Möb($\mathbb{R}^3$) as $SL^{\ddagger}(2, H)$

- There is an action on $\mathbb{R}^3 \cup \{\infty\} = H^+ \cup \{\infty\}$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .z = (az + b)(cz + d)^{-1}$$

- Every orientation-preserving element of Möb($\mathbb{R}^3$) can be written as $z \mapsto (az + b)(cz + d)^{-1}$.
- Every orientation-reversing element of Möb($\mathbb{R}^3$) can be written as $z \mapsto (a\overline{z} + b)(c\overline{z} + d)^{-1}$.

Arithmetic Groups

Definition

What sort of subgroups Γ of $SL^{\ddagger}(2, H)$ should we consider?

- We will ask that Γ is discrete.
- We will ask that Γ carries some sort of algebraic structure.

Arithmetic Groups

Definition

What sort of subgroups Γ of $SL^{\ddagger}(2, H)$ should we consider?

- We will ask that Γ is discrete.
- We will ask that Γ carries some sort of algebraic structure.
- We will ask that Γ is *arithmetic*.

Arithmetic Groups

Definition

What sort of subgroups Γ of $SL^{\ddagger}(2, H)$ should we consider?

- We will ask that Γ is discrete.
- We will ask that Γ carries some sort of algebraic structure.
- We will ask that Γ is *arithmetic*.
- Note that $SL^{\ddagger}(2, H)$ can be seen as real solutions to a set of polynomial equations.
- Roughly, an arithmetic group is the set of integer solutions to that set of polynomial equations.

Arithmetic Groups

Definition

What sort of subgroups Γ of $SL^{\ddagger}(2, H)$ should we consider?

- We will ask that Γ is discrete.
- We will ask that Γ carries some sort of algebraic structure.
- We will ask that Γ is *arithmetic*.
- Note that $SL^{\ddagger}(2, H)$ can be seen as real solutions to a set of polynomial equations.
- Roughly, an arithmetic group is the set of integer solutions to that set of polynomial equations.
- Not quite true—can only define up to commensurability—but ignore that.

Examples of Arithmetic Groups

- $\Gamma = SL(2, \mathbb{Z})$
- $\Gamma(N)$

Examples of Arithmetic Groups

- $\Gamma = SL(2, \mathbb{Z})$
- $\Gamma(N)$
- $SL(2, \mathbb{Z}[i])$
- $SL(2, \mathbb{Z}[\sqrt{-2}])$
- $SL\left(2, \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)$

Examples of Arithmetic Groups

- $\Gamma = SL(2, \mathbb{Z})$
- $\Gamma(N)$
- $SL(2, \mathbb{Z}[i])$
- $SL(2, \mathbb{Z}[\sqrt{-2}])$
- $SL\left(2, \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)$
- What about $SL^{\ddagger}(2, H)$?

Examples of Arithmetic Groups inside $SL^{\ddagger}(2, H)$

- Classical answer: choose a quadratic form q of signature $(4,1)$, and take $SO^{+}(q,\mathbb{Z})$ (use the classical isomorphism $SO^{+}(4,1) \cong \text{Möb}(\mathbb{R}^3)$ to make sense of this)

Examples of Arithmetic Groups inside $SL^{\ddagger}(2, H)$

- Classical answer: choose a quadratic form q of signature $(4, 1)$, and take $SO^{+}(q, \mathbb{Z})$ (use the classical isomorphism $SO^{+}(4, 1) \cong \text{Möb}(\mathbb{R}^3)$ to make sense of this)
- Very hard to find any non-trivial elements of this group.
- $-4X_1^2 + 2X_2X_1 + X_3X_1 - 3X_4X_1 + 5X_2^2 + 6X_3^2 + 7X_4^2 + 22X_5^2 - 5X_2X_3 + X_2X_4 + X_3X_4 - X_2X_5 + 2X_3X_5 + 4X_4X_5$

Examples of Arithmetic Groups inside $SL^{\ddagger}(2, H)$

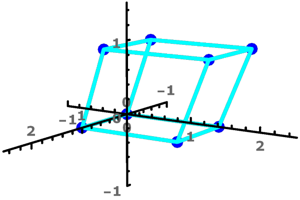
- Classical answer: choose a quadratic form q of signature $(4, 1)$, and take $SO^{+}(q, \mathbb{Z})$ (use the classical isomorphism $SO^{+}(4, 1) \cong \text{Möb}(\mathbb{R}^{3})$ to make sense of this)
- Very hard to find any non-trivial elements of this group.
- $-4X_1^2 + 2X_2X_1 + X_3X_1 - 3X_4X_1 + 5X_2^2 + 6X_3^2 + 7X_4^2 + 22X_5^2 - 5X_2X_3 + X_2X_4 + X_3X_4 - X_2X_5 + 2X_3X_5 + 4X_4X_5$
- There is a better way!

Examples of Arithmetic Groups inside $SL^{\ddagger}(2, H)$

- Let $\mathcal{O}$ be an order of H that is closed under $\ddagger$ (i.e. $\mathcal{O} = \mathcal{O}^{\ddagger}$).
- Then $SL^{\ddagger}(2, \mathcal{O}) = SL^{\ddagger}(2, H) \cap \mathrm{Mat}(2, \mathcal{O})$ is an arithmetic group.

Examples of Arithmetic Groups inside $SL^{\ddagger}(2, H)$

- Let $\mathcal{O}$ be an order of H that is closed under $\ddagger$ (i.e. $\mathcal{O} = \mathcal{O}^{\ddagger}$).
- Then $SL^{\ddagger}(2, \mathcal{O}) = SL^{\ddagger}(2, H) \cap \mathrm{Mat}(2, \mathcal{O})$ is an arithmetic group.
- Here, an order means a sub-ring that is also a lattice.
- Example: $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\dfrac{1+\sqrt{2}i+\sqrt{5}j}{2} \oplus \mathbb{Z}\dfrac{\sqrt{2}i+\sqrt{10}k}{2}$



Maximal ‡-Orders

- Why ask that $\mathcal{O} = \mathcal{O}^{\ddagger}$?
- Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d^{\ddagger} & -b^{\ddagger} \\ -c^{\ddagger} & a^{\ddagger} \end{pmatrix}$

Maximal ‡-Orders

- Why ask that $\mathcal{O} = \mathcal{O}^\ddagger$?
- Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d^\ddagger & -b^\ddagger \\ -c^\ddagger & a^\ddagger \end{pmatrix}$

Definition

If $\mathcal{O}$ is an order of H closed under ‡, we say that $\mathcal{O}$ is a *‡-order*. If $\mathcal{O}$ is not contained inside any larger ‡-order, we say that it is a *maximal ‡-order*.

Maximal ‡-Orders

- Why ask that $\mathcal{O} = \mathcal{O}^{\ddagger}$?
- Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d^{\ddagger} & -b^{\ddagger} \\ -c^{\ddagger} & a^{\ddagger} \end{pmatrix}$

Definition

If $\mathcal{O}$ is an order of H closed under ‡, we say that $\mathcal{O}$ is a *‡-order*. If $\mathcal{O}$ is not contained inside any larger ‡-order, we say that it is a *maximal ‡-order*.

- Originally studied by Scharlau (1970s) in the context of central simple algebras, and then Azumaya algebras.

Maximal $\ddagger$-Orders

- Why ask that $\mathcal{O} = \mathcal{O}^\ddagger$?
- Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d^\ddagger & -b^\ddagger \\ -c^\ddagger & a^\ddagger \end{pmatrix}$

Definition

If $\mathcal{O}$ is an order of H closed under $\ddagger$, we say that $\mathcal{O}$ is a $\ddagger$-*order*. If $\mathcal{O}$ is not contained inside any larger $\ddagger$-order, we say that it is a *maximal* $\ddagger$-*order*.

- Originally studied by Scharlau (1970s) in the context of central simple algebras, and then Azumaya algebras.

Theorem (S. 2017)

There is a polynomial time algorithm to determine whether a lattice $\mathcal{O}$ is a maximal $\ddagger$-order. (Easy computation of the discriminant, which is always square-free.)

Other Nice Properties of $SL^{\ddagger}(2, \mathcal{O})$ (S.2019)

- $\mathrm{Mat}(2, \mathcal{O})$ is a homotopy invariant of the hyperbolic manifold $\mathbb{H}^4 / SL^{\ddagger}(2, \mathcal{O})$

Other Nice Properties of $SL^{\ddagger}(2,\mathcal{O})$ (S.2019)

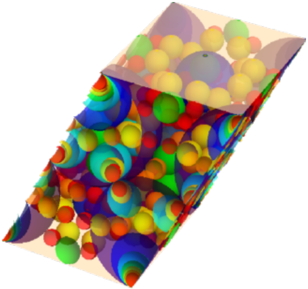
- $\mathrm{Mat}(2,\mathcal{O})$ is a homotopy invariant of the hyperbolic manifold $\mathbb{H}^4/SL^{\ddagger}(2,\mathcal{O})$
- For every arithmetic group $SO(q;\mathbb{Z})$, there is a group $SL^{\ddagger}(2,\mathcal{O})$ commensurable to it.

Other Nice Properties of $SL^{\ddagger}(2,\mathcal{O})$ (S.2019)

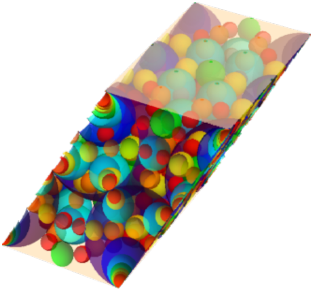
- $\mathrm{Mat}(2,\mathcal{O})$ is a homotopy invariant of the hyperbolic manifold $\mathbb{H}^4/SL^{\ddagger}(2,\mathcal{O})$
- For every arithmetic group $SO(q;\mathbb{Z})$, there is a group $SL^{\ddagger}(2,\mathcal{O})$ commensurable to it.
- Within its commensurability class, $SL^{\ddagger}(2,\mathcal{O})$ is maximal—i.e. it is not contained inside of any larger arithmetic group commensurable to it.

Sphere Packings

Choose some fix plane in $\mathbb{R}^3$ and act on it by $SL^{\ddagger}(2,\mathcal{O})$. What will this look like?



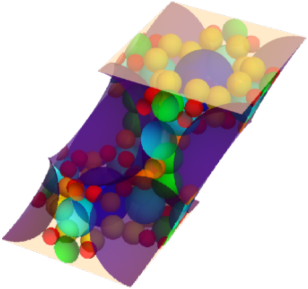
$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+j\sqrt{6}}{2}$



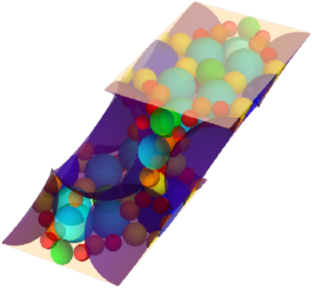
$\mathbb{Z} \oplus \mathbb{Z}i\sqrt{2} \oplus \mathbb{Z}\frac{1+i\sqrt{2}+j\sqrt{5}}{2}$

Sphere Packings

Choose some fix plane in $\mathbb{R}^3$ and act on it by $SL^{\ddagger}(2, \mathcal{O})$. What will this look like?



$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+j\sqrt{6}}{2}$



$\mathbb{Z} \oplus \mathbb{Z}i\sqrt{2} \oplus \mathbb{Z}\frac{1+i\sqrt{2}+j\sqrt{5}}{2}$

Practical Generation of Sphere Packings

Problem

How do you actually plot a sphere packing like this? How do you find elements in $SL^{\ddagger}(2, \mathcal{O})$*? How do you know when to stop?*

Practical Generation of Sphere Packings

Problem

How do you actually plot a sphere packing like this? How do you find elements in $SL^{\ddagger}(2, \mathcal{O})$*? How do you know when to stop?*

Problem

Given $a, b \in \mathcal{O}$ *such that* $ab^{\ddagger} \in H^{+}$*, can you give an algorithm to determine whether there are* $c, d \in \mathcal{O}$ *such that*
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL^{\ddagger}(2, \mathcal{O})$*?*

Practical Generation of Sphere Packings

Problem

How do you actually plot a sphere packing like this? How do you find elements in $SL^{\ddagger}(2, \mathcal{O})$? How do you know when to stop?

Problem

Given $a, b \in \mathcal{O}$ such that $ab^{\ddagger} \in H^{+}$, can you give an algorithm to determine whether there are $c, d \in \mathcal{O}$ such that
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL^{\ddagger}(2, \mathcal{O})$*?*

- Easy to check that this is equivalent to an algorithm to check whether $a\mathcal{O} + b\mathcal{O} = \mathcal{O}$.

The Euclidean Algorithm

Definition

Let R be an integral domain. Suppose there exists a well-ordered set W and a function $\Phi : R \to W$ such that for all $a, b \in R$ such that $b \neq 0$, there exists $q \in R$ such that $\Phi(a - bq) < \Phi(b)$. Then we say that R is a *Euclidean domain*.

Theorem

If R is a Euclidean domain, then it is a principal ideal domain, and there exists an algorithm that, on an input of $a, b \in R$, outputs $c, d \in R$ such that $ad - bc = g$, where g is a GCD of a and b. Furthermore, $SL(2, R)$ is generated by matrices of the form

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix},$$

where $r \in R$ and $u \in R^\times$.

The $\ddagger$-Euclidean Algorithm

Definition

Let $\mathcal{O}$ be a maximal $\ddagger$-order. Suppose there exists a well-ordered set W and a function $\Phi : \mathcal{O} \to W$ such that for all $a, b \in \mathcal{O}$ such that $b \neq 0$ and $ab^\ddagger \in H^+$, there exists $q \in \mathcal{O} \cap H^+$ such that $\Phi(a - bq) < \Phi(b)$. Then we say that $\mathcal{O}$ is a $\ddagger$-*Euclidean ring*.

Theorem

If $\mathcal{O}$ is a $\ddagger$-Euclidean ring, then $\mathcal{O}$ is a principal ring, and there exists an algorithm that, on an input of $a, b \in \mathcal{O}$ such that $ab^\ddagger \in H^+$, outputs $c, d \in \mathcal{O}$ such that $ad^\ddagger - bc^\ddagger = g$, where g is a right GCD of a and b. Furthermore, $SL^\ddagger(2, \mathcal{O})$ is generated by matrices of the form

$$\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} u & 0 \\ 0 & \left(u^{-1}\right)^\ddagger \end{pmatrix},$$

where $z \in \mathcal{O} \cap H^+$ and $u \in \mathcal{O}^\times$.

Illustration of the ‡-Euclidean Algorithm

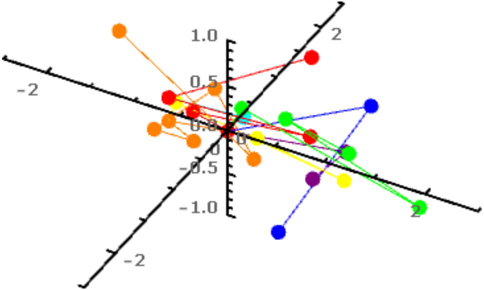
- Given a, b, consider $b^{-1}a$ and find the closest element of $\mathcal{O} \cap H^{+}$—call this q.

Illustration of the ‡-Euclidean Algorithm

- Given a, b, consider $b^{-1}a$ and find the closest element of $\mathcal{O} \cap H^+$—call this q.
- Define $(a_1, b_1) = (b, a - bq)$. Repeat until $b_i^{-1}a_i = 0$ or ∞.

Illustration of the ‡-Euclidean Algorithm

- Given a, b, consider $b^{-1}a$ and find the closest element of $\mathcal{O} \cap H^{+}$—call this q.
- Define $(a_1, b_1) = (b, a - bq)$. Repeat until $b_i^{-1}a_i = 0$ or ∞.



$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\frac{1 + i\sqrt{11}}{2} \oplus \mathbb{Z}\frac{3i\sqrt{11} + j\sqrt{143}}{11} \oplus \mathbb{Z}\frac{j\sqrt{143} + k\sqrt{13}}{2}$$

How Many ‡-Euclidean Rings Exist?

- Remember, any maximal ‡-order that is ‡-Euclidean is a principal ring. (Right class number $= 1$)

How Many ‡-Euclidean Rings Exist?

- Remember, any maximal ‡-order that is ‡-Euclidean is a principal ring. (Right class number = 1)

Journal de Théorie des Nombres de Bordeaux **7** *(1995), 93–96*

Definite Quaternion Orders of Class Number One

par Juliusz BRZEZINSKI

The purpose of the paper is to show how to determine all definite quaternion orders of class number one over the integers. First of all, let us recall that a quaternion order is a ring Λ containing the ring of integers $\mathbf{Z}$ as a subring, finitely generated as a $\mathbf{Z}$-module and such that $A = \Lambda \otimes \mathbf{Q}$ is a central simple four dimensional $\mathbf{Q}$-algebra. By the class number H_Λ of Λ, we mean the number of isomorphism classes of locally free left (or right-both numbers are equal) Λ-ideals in A. Recall that a left Λ-ideal I in A is locally free if for each prime number $p, I_p = I \otimes \mathbf{Z}_p$ is a principal left $\Lambda_p = \Lambda \otimes \mathbf{Z}_p$-ideal, where $\mathbf{Z}_p$ denotes the p-adic integers. Two locally free left Λ-ideals I and I' define the same isomorphism class if $I' = I\alpha$, where $\alpha \in A$.

A quaternion order is called definite if $\Lambda \otimes \mathbf{R}$ is the algebra of the Hamiltonian quaternions over the real numbers $\mathbf{R}$. We want to show that there are exactly 25 isomorphism classes of definite quaternion orders of class number one over the integers (an analoguous result, which is much more difficult to prove, says that there are 13 $\mathbf{Z}$-orders of class number one in imaginery quadratic fields over the rational numbers).

First of all, we want to explicity describe all quaternion orders over the integers. This can be done by means of integral ternary quadratic forms

$$f = \sum_{1 \le i \le j \le 3} a_{i,j} X_i X_j,$$

where $a_{i,j} \in \mathbf{Z}$, which will be denoted by

$$f = \begin{pmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{13} & a_{12} \end{pmatrix}.$$

It is well known that each Λ can be given as $C_0(f)$, where f is a suitable integral ternary quadratic form and $C_0(f)$ is the even Clifford algebra of f.

Manuscrit reçu le 28 Février 1994.

THEOREM. *There are 25 isomorphism classes of $\mathbf{Z}$-orders with class number 1 in definite quaternion $\mathbf{Q}$-algebras. These classes are represented by the orders $C_0(f)$, where f is one of the following forms (the index of the matrix corresponding to a quadratic form f is the discriminant of the order $C_0(f)$):*

$$\begin{pmatrix} 1&1&1\\0&1&1\end{pmatrix}_2, \begin{pmatrix} 1&1&1\\0&0&1\end{pmatrix}_3, \begin{pmatrix} 1&1&1\\0&0&0\end{pmatrix}_4, \begin{pmatrix} 1&1&2\\0&1&1\end{pmatrix}_5, \begin{pmatrix} 1&1&2\\1&1&0\end{pmatrix}_6,$$

$$\begin{pmatrix} 1&1&2\\0&0&1\end{pmatrix}_6, \begin{pmatrix} 1&1&2\\0&1&0\end{pmatrix}_7, \begin{pmatrix} 1&1&3\\0&1&1\end{pmatrix}_8, \begin{pmatrix} 1&1&2\\0&0&0\end{pmatrix}_8, \begin{pmatrix} 1&1&3\\0&0&1\end{pmatrix}_9,$$

$$\begin{pmatrix} 1&1&3\\1&1&0\end{pmatrix}_{10}, \begin{pmatrix} 1&2&2\\2&0&1\end{pmatrix}_{10}, \begin{pmatrix} 1&1&4\\0&0&1\end{pmatrix}_{12}, \begin{pmatrix} 1&2&2\\0&1&1\end{pmatrix}_{12}, \begin{pmatrix} 1&1&3\\0&0&0\end{pmatrix}_{12},$$

$$\begin{pmatrix} 1&2&2\\2&0&0\end{pmatrix}_{12}, \begin{pmatrix} 1&2&2\\1&0&1\end{pmatrix}_{13}, \begin{pmatrix} 1&2&2\\0&0&0\end{pmatrix}_{16}, \begin{pmatrix} 1&1&5\\1&1&0\end{pmatrix}_{18}, \begin{pmatrix} 1&2&3\\2&1&0\end{pmatrix}_{18},$$

$$\begin{pmatrix} 1&2&3\\2&0&0\end{pmatrix}_{20}, \begin{pmatrix} 1&2&3\\0&1&0\end{pmatrix}_{22}, \begin{pmatrix} 1&3&3\\-1&1&1\end{pmatrix}_{28}, \begin{pmatrix} 2&2&2\\0&2&2\end{pmatrix}_{16}, \begin{pmatrix} 2&2&2\\0&0&2\end{pmatrix}_{24}.$$

Proof. Let Λ be a quaternion $\mathbf{Z}$-order with class number $H_\Lambda = 1$. Then

$$M_\Lambda = \frac{d(\Lambda)}{12} \prod_{p|d(\Lambda} \frac{1-p^{-2}}{1-e_p(\Lambda)p^{-2}} \le 1,$$

(see [K], Thm. 1 or [B2], (4.6)). Denoting by ϕ the Euler totient function, we have

$$(*) \quad \phi(d(\Lambda))(1+p_1)\cdots(1+p_r)(1+p'_1)\cdots(1+p'_s) \le 12(p_1-1)\cdots (p_r-1)p'_1\cdots p'_s,$$

where p_i and p'_s are all prime factors of $d(\Lambda$ such that $e_{p_i}(\Lambda) = 1$ and $e_{p'_i}(\Lambda) = 0$. This inequality implies that $\phi(d(\Lambda)) \le 12$ and if $\phi(d(\Lambda)) = 12$, then for each prime factor p of $d(\Lambda)$, $e_p(\Lambda) = -1$. The condition $\phi(d(\Lambda)) \le 12$ says that $2 \le d(\Lambda) \le 16$ or $d(\Lambda) = 18, 20, 21, 22, 24, 26, 28, 30, 36, 42$.

Assume now that Λ is a Gorenstein $\mathbf{Z}$-order. Then $\Lambda = C_0(f)$, where f is a primitive integral ternary quadratic form with only one class in its genus, since $T_\Lambda \le H_\Lambda$ (see [V], p. 88). Thus, using the tables [BI], we can first of all eliminate all classes with $\phi(d(\Lambda)) \le 12$ for which $T_\Lambda \ge 2$. The

Enumerating ‡-Euclidean Rings

Theorem (Brzezinski 1995)
Every order of H with square-free discriminant and class number 1 is isomorphic (as rings) to one of the following.

$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\tfrac{1+i+j+k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\tfrac{1+i+\sqrt{6}j}{2} \oplus \mathbb{Z}\tfrac{\sqrt{6}j+\sqrt{6}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\tfrac{1+i+\sqrt{10}j}{2} \oplus \mathbb{Z}\tfrac{\sqrt{10}j+\sqrt{10}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\tfrac{1+\sqrt{2}i+\sqrt{5}j}{2} \oplus \mathbb{Z}\tfrac{\sqrt{2}i+\sqrt{5}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\tfrac{2+\sqrt{2}i+\sqrt{26}j}{4} \oplus \mathbb{Z}\tfrac{\sqrt{2}i-\sqrt{26}j+2\sqrt{13}k}{4}$$
$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\tfrac{1+\sqrt{3}i}{2} \oplus \mathbb{Z}\tfrac{i+\sqrt{3}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\tfrac{1+\sqrt{7}j}{2} \oplus \mathbb{Z}\tfrac{i+\sqrt{7}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\tfrac{1+\sqrt{3}j}{2} \oplus \mathbb{Z}\tfrac{\sqrt{2}i+\sqrt{6}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\tfrac{1+\sqrt{11}j}{2} \oplus \mathbb{Z}\tfrac{\sqrt{2}i+\sqrt{11}k}{2}$$
$$\mathbb{Z} \oplus \mathbb{Z}\sqrt{5}i \oplus \mathbb{Z}\tfrac{1+\sqrt{5}i+\sqrt{10}j}{2} \oplus \mathbb{Z}\tfrac{1+\sqrt{5}i+\sqrt{2}k}{2}$$

Enumerating ‡-Euclidean Rings

Theorem

Every maximal ‡-order of H with class number 1 is isomorphic (as rings with involution) to one of the following.

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{2}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}j+\sqrt{2}k}{2}$
$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{6}j}{2} \oplus \mathbb{Z}\frac{1+\sqrt{3}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{1+\sqrt{3}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{6}k}{2}$
$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{10}j}{2} \oplus \mathbb{Z}\frac{\sqrt{10}j+\sqrt{10}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+\sqrt{3}j}{2} \oplus \mathbb{Z}\frac{i+\sqrt{3}k}{2}$
$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{6}}{2}j \oplus \mathbb{Z}\frac{\sqrt{6}j+\sqrt{6}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{2+\sqrt{2}i+\sqrt{10}j}{4} \oplus \mathbb{Z}\frac{\sqrt{2}i-\sqrt{10}j+2\sqrt{5}k}{4}$
$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{1+\sqrt{2}i+\sqrt{5}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{10}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+\sqrt{7}j}{2} \oplus \mathbb{Z}\frac{i+\sqrt{7}k}{2}$
$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+\sqrt{7}j}{2} \oplus \mathbb{Z}\frac{1+\sqrt{7}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{2+\sqrt{2}i+\sqrt{26}j}{4} \oplus \mathbb{Z}\frac{i\sqrt{2}-\sqrt{26}j+2\sqrt{13}k}{4}$
$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\sqrt{5}j \oplus \mathbb{Z}\frac{1+i+\sqrt{5}j+\sqrt{5}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{3}i}{2} \oplus \mathbb{Z}\sqrt{3}j \oplus \mathbb{Z}\frac{\sqrt{3}j+k}{2}$
$\mathbb{Z} \oplus \mathbb{Z}\sqrt{5}i \oplus \mathbb{Z}\frac{1+\sqrt{5}i+\sqrt{10}j}{2} \oplus \mathbb{Z}\frac{1+\sqrt{5}i+\sqrt{2}k}{2}$	$\mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{7}i}{2} \oplus \mathbb{Z}\sqrt{7}j \oplus \mathbb{Z}\frac{\sqrt{7}j+k}{2}$

Enumerating ‡-Euclidean Rings

Theorem

Every maximal ‡-order of H that is a ‡-Euclidean ring is isomorphic (as rings with involution) to one of the following. For each one, we can take $\Phi = nrm$.

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{6}j}{2} \oplus \mathbb{Z}\frac{1+\sqrt{3}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{10}j}{2} \oplus \mathbb{Z}\frac{\sqrt{10}j+\sqrt{10}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{6}}{2}j \oplus \mathbb{Z}\frac{\sqrt{6}j+\sqrt{6}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{1+\sqrt{2}i+\sqrt{5}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{10}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+\sqrt{7}j}{2} \oplus \mathbb{Z}\frac{1+\sqrt{7}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+i+\sqrt{2}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}j+\sqrt{2}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{1+\sqrt{3}j}{2} \oplus \mathbb{Z}\frac{\sqrt{2}i+\sqrt{6}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+\sqrt{3}j}{2} \oplus \mathbb{Z}\frac{i+\sqrt{3}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{2+\sqrt{2}i+\sqrt{10}j}{4} \oplus \mathbb{Z}\frac{\sqrt{2}i-\sqrt{10}j+2\sqrt{5}k}{4}$

$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{1+\sqrt{7}j}{2} \oplus \mathbb{Z}\frac{i+\sqrt{7}k}{2}$

$\mathbb{Z} \oplus \mathbb{Z}\sqrt{2}i \oplus \mathbb{Z}\frac{2+\sqrt{2}i+\sqrt{26}j}{4} \oplus \mathbb{Z}\frac{i\sqrt{2}-\sqrt{26}j+2\sqrt{13}k}{4}$

Enumerating ‡-Euclidean Rings