Arithmetic Fuchsian Groups arising from Quaternion Algebras

Contents

1 Motivation 2
2 Representation Theoretical construction of Fuchsian Groups 2
3 Quaternion Algebras 2
  3.1 Quadratic forms and Orders 6
  3.2 Ramified Quaternions 8
4 Groups from Orders 9
1 Motivation

Fuchsian groups are discrete subgroups of $PSL(2, \mathbb{R})$, i.e. subgroups of the isometry group of the hyperbolic plane $\mathbb{H}^2$. One of the important features of those groups lies by the concept of uniformization of surfaces. Namely one can endow a compact Riemann surface of genus $g \geq 2$ with the structure of a quotient of the form:

$$X = \mathbb{H}^2 / \Gamma$$

where $\Gamma$ is Fuchsian group. This was the spark of an even greater and up to date still incomplete program, namely that of Thurston on geometrization of higher dimensional surfaces.

We will construct here a class of Fuchsian groups, the arithmetic Fuchsian groups, which have the property of coding all of their structure in terms of number-theoretic data. We use the notion of orders of quaternion algebras from which arithmetic Fuchsian groups will arise.

2 Representation Theoretical construction of Fuchsian Groups

Before we go into the number-theoretic construction of Let us consider a finite dimensional linear representation of $PSL(2, \mathbb{R})$:

$$T : PSL(2, \mathbb{R}) \rightarrow GL(n, \mathbb{R})$$

Then the subgroup $T(PSL(2, \mathbb{R})) \cap GL(n, \mathbb{Z})$ lifts to a discrete subgroup $\Gamma < PSL(2, \mathbb{R})$ given by:

$$\Gamma := T^{-1}(T(PSL(2, \mathbb{R})) \cap GL(n, \mathbb{Z}))$$

**Definition**: All subgroups of $PSL(2, \mathbb{R})$ obtained in that manner and all their subgroups of finite index are called **Arithmetic Fuchsian Groups**.

By the classification of all classical groups, due to A. Weil, we know that all arithmetic subgroups of $SL(2, \mathbb{R})$, up to a relation called commensurability, are given by Fuchsian Groups derived from quaternion algebras over totally real number fields. In this lecture we will construct the Arithmetic Fuchsian groups in terms of quaternion algebras.

3 Quaternion Algebras

**Definition**: Let $F$ be a field of $\text{char}(F) \neq 2$. A **Quaternion Algebra** $A$ over $F$ is a 4-dimensional $F$-Algebra with basis vectors $\{1, i, j, k\}$, where the algebra structure is given by $1$ being the multiplicative identity, the relations:

$$i^2 = a \cdot 1, \quad j^2 = b \cdot 1, \quad k = i \cdot j = -j \cdot i,$$
for some \( a, b \in \mathbb{F}^* \) and by linear extension of this multiplication over \( F \), so that \( \mathcal{A} \) is an associative \( F \)-Algebra. For an object with that structure, we write:

\[
\mathcal{A} = \left( \frac{a,b}{F} \right).
\]

For a field extension \( K/F \), we can extend the scalars of the algebra in the obvious manner:

\[
\mathcal{A} = \left( \frac{a,b}{F} \right) \otimes_F K \cong \left( \frac{a,b}{K} \right).
\]

**Examples:**

1. The first example of a quaternion algebra over \( F \), is the matrix algebra:

\[
M(2,F) \cong \left( \frac{1,1}{F} \right)
\]

with generators being given by:

\[
i = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \quad j = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}
\]

2. The first non-trivial one are the Hamiltonian Quaternions:

\[
\mathcal{H} = \left( \frac{-1,-1}{\mathbb{R}} \right)
\]

In general, a quaternion algebra \( \mathcal{A} \) is isomorphic either a division algebra, i.e. \( \mathcal{A}^* = \mathcal{A} - \{0\} \), or it is isomorphic to the matrix algebra \( M(2,F) \). In the following discussion we will try to find out when each case shows up. To do so, we construct a representation of the quaternion algebra that will allow us to correspond to this abstract construction matrix algebras:

Let \( \mathcal{A} = \left( \frac{a,b}{F} \right) \) be a quaternion algebra and \( F(\sqrt{a})/F \) a quadratic extension. Then \( \phi : \mathcal{A} \to M(2,F(\sqrt{a})) \) is a representation given by:

\[
1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \quad i \mapsto \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}; \quad j \mapsto \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}; \quad k \mapsto \begin{bmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{bmatrix},
\]

which are linearly independent matrices which build a basis of a subalgebra of \( M(2,F(\sqrt{a})) \)

So for an element \( x \in A \), \( x = x_0 + ix_1 + jx_2 + kx_3 \) we have:

\[
g_x := \phi(x) = \begin{bmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{bmatrix}
\]

In particular one can perform a straight-forward check that \( \phi \) defines a faithful algebra morphism, i.e.:

- \( g_x + g_y = g_{x+y} \)
• $g_{xy} = g_x \cdot g_y$

• $[x = y \iff g_x = g_y]$

Remark: By the representation we just defined, we see that if $a$ is a square $a \in (F^*)^2$ then obviously the morphism becomes an isomorphism onto $M(2, F)$.

Proposition: There exists an isomorphism:

$$A = \left( \frac{a, b}{F} \right) \cong \left( \frac{ax^2, by^2}{F} \right); \; x, y \in F.$$  

Moreover quaternion algebras are simple central $F$-Algebras, i.e.:

1. $\text{Rad}(A) = 0$

2. $\mathcal{Z}(A) = \{ x \in A | [x, y] = 1 \; \forall y \in A \} = F \cdot 1$

Proof:

• Let $A = \left( \frac{a, b}{F} \right)$ and $A' = \left( \frac{ax^2, by^2}{F} \right)$ with bases $\{1, i, j, k\}$ and $\{1, i', j', k'\}$ respectively. Then the $F$-algebra homomorphism:

$$\phi: A \longrightarrow A'$$

$$1 \longmapsto 1$$

$$i' \longmapsto xi$$

$$j' \longmapsto yj$$

$$k' \longmapsto xyk$$

is indeed a $F$-algebra isomorphism: $(xi)^2 = ax^2; \; (yj)^2 = by^2; \; (xi)(yj) = (xy)ij = -(xy)ji = -(yj)(xi)$

• As $\bar{F}$ is algebraically closed, so $\forall x \in \left( \frac{a, b}{F} \right) \exists y \in \left( \frac{a, b}{\bar{F}} \right)$ such that $x = y^2$. So from the statement we just showed above follows:

$$\left( \frac{a, b}{F} \right) \cong \left( \frac{1, 1}{\bar{F}} \right) \cong M(2, \bar{F}).$$

Further we know that $\mathcal{Z}(M(2, \bar{F})) = \bar{F} \cdot 1$. But we also know that one obtains $\left( \frac{a, b}{\bar{F}} \right)$ just by a scalar extension $\left( \frac{a, b}{F} \right) \otimes \bar{F} \cong \left( \frac{a, b}{\bar{F}} \right)$ and therefore $\mathcal{Z}(\left( \frac{a, b}{\bar{F}} \right)) = \bar{F} \cdot 1$.

• Let $0 \neq a \triangleleft A$, then we have for the extension of scalars $0 \neq a \otimes_F \bar{F} \triangleleft M(2, \bar{F})$. Where $\bar{F}$ be the algebraic closure of $F$. But the matrix algebra over a field is obviously simple as:

$$0 \neq a = M(I); \; \text{for} \; I \triangleleft \bar{F} \iff I = \bar{F}.$$  

So $a$ is a 4-dimensional $F$-vector space, and already by the dimension follows $a = A$.  

4
**Definition:** Let \( x \in \mathcal{A} = \left( \frac{a,b}{F} \right) \)

**Standard involution:**
\[
i : A \longrightarrow A
\]
\[
x \mapsto \overline{x} = x_0 - x_1 i - x_2 j - x_3 k
\]

**Reduced trace:**
\[
tr : A \longrightarrow F
\]
\[
x \mapsto x + \overline{x} = 2x_0
\]
and \( tr(x) = Tr(g_x) \)

**Reduced Norm:**
\[
n : A \longrightarrow F
\]
\[
x \mapsto x \overline{x} = x_0^2 - x_1^2 a - x_2^2 b - x_3^2 ab
\]
and \( n(x) = \det(g_x) \)

**Theorem:** A quaternion algebra \( \mathcal{A} \) is a division algebra, if and only if the following equivalence holds:
\[
n(x) = 0 \iff x = 0
\]

**Proof:**
\[\bullet \iff \text{ Assume } [n(x) \neq 0 \iff x \neq 0] (\iff [-n(x) = 0 \iff -x = 0])\]
\[
x \neq 0 \implies n(x) \neq 0 \quad \text{and} \quad n(x) = x \cdot \overline{x}
\]
\[
\implies x = \frac{x}{n(x)} \implies \forall x \in \mathcal{A}, x \neq 0, \exists x^{-1} \in \mathcal{A} \text{ s.t. } x \cdot x^{-1} = 1
\]
\[
\Rightarrow \mathcal{A} \text{ is a division algebra.}
\]
\[\bullet \Rightarrow \text{ Let } \mathcal{A} \text{ be a division algebra and take } 0 \neq x \in \mathcal{A}. \text{ So we have:} \]
\[
1 = n(1) = n(x \cdot x^{-1}) = n(x)n(x^{-1}) \implies n(x) \neq 0
\]
and \( n(x) \neq 0 \implies x \neq 0 \) is obvious.

**Theorem:** If \( \mathcal{A} = \left( \frac{a,b}{F} \right) \not\cong M(2, F) \), then \( \mathcal{A} \) is a division algebra.

**Proof:**
\[\bullet \text{ First take } a \notin F^{*2}, \text{ i.e. not a square.} \]
\[\bullet \text{ Let } \mathcal{L} = F(i) \text{ so we have } \mathcal{A} = \mathcal{L} + \mathcal{L}j\]
Assumption: $A$ is not a division algebra. Then by the last theorem we have that:

$$\exists x \in A, \ x = x_0 + x_1 i + x_2 j + x_3 k \not= 0 \text{ s.t. } n(x) = 0$$

$$\implies n_L(x_0 + ix_1) - b \cdot n_L(x_2 - ix_3) = 0$$

If $x_2 - ix_3 = 0$, then $n_L(x_0 + ix_1) = 0$

$$\implies x_0 + ix_1 = 0 \implies x = 0;$$

Which leads to a contradiction. So $x_2 + ix_3 \not= 0$ and we can write:

$$b = \frac{n_L(x_0 + ix_1)}{n_L(x_2 + ix_3)} = n_L(q_0 - iq_1) = q_0^2 - aq_1^2,$$

with $q_0, q_1 \in F$. From here we can construct a map $\psi : A \to M(2, F)$ by sending the basis to:

$$1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \ i \mapsto \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}; \ j \mapsto \begin{bmatrix} q_0 & -q_1 \\ aq_1 & -q_0 \end{bmatrix}; \ k \mapsto \begin{bmatrix} aq_1 & -q_0 \\ aq_0 & aq_1 \end{bmatrix}$$

So under this map one has: $\psi(i)^2 = a; \psi(j)^2 = b$ and all matrices are linearly independent, which gives an isomorphism $\psi : A \xrightarrow{\sim} M(2, F)$.

3.1 Quadratic forms and Orders

**Theorem:** As always let $A = \left( \frac{a,b}{F} \right)$. Then $A$ is not a division algebra, i.e. $A \cong M(2, F)$ if and only if $\exists (x,y) \in F \times F$ that solves the quadratic form/ conic equation: $ax^2 + by^2 = 1$.

**Proof:** $\implies$

- First we show that $y \not= 0$ exists in the subspace of $A$ spanned by $\{i,j,k\} = A_0$ such that the induced norm $n_0(y) = 0$: Assume that there is no such $y$. [@] Since $A$ is not a division algebra we know that an $x = a_0 + ia_1 + ja_2 + ka_3$ exists with $n(x) = 0$. If $a_0 = 0$ then we are done, so lets assume that $a_0 \not= 0$, that means that one of $a_1, a_2, a_3$ is non-zero. Without loss of generality take $a_1 \not= 0$. Moreover

$$n(x) = 0 \implies a_0^2 - ba_2^2 = a(a_1^2 - ba_3^2)$$

Under this relation we see that $n_0(y) = 0$ for

$$y := b(a_0a_3 + a_1a_2)i + a(a_1^2 - ba_3^2)j + (a_0a_1 + ba_2a_3)ij$$

Because of [@] we have $y = 0$:

$$y = 0 \implies -a_1^2 + aba_3^2 = 0 \implies n(a_1i + a_3ij) = 0 \implies a_1 = 0$$

which leads to a contradiction.
Now we know that \( a_1, a_2, a_3 \) exist with 
\[-a_1^2 - b a_2^2 + a b a_3^2 = 0,\]
from which at least two are non-zero. If \( a_3 \neq 0 \) then the pair \((x, y) = (a_2 a_1^{-1}, a_1^{-1})\) satisfies the relation 
\[a x^2 + b y^2 = 1\] 
If \( a_3 = 0 \) then the pair \((x, y) = (1 + a_2 a_1^{-1}, a_2)\) satisfies the relation 
\[a x^2 + b y^2 = 1\]
That completes the first implication.

\[\Leftarrow: \text{Now we want to find non-zero element in } \mathcal{A} \text{ with norm 0, i.e. non-invertible.}\]

- We take first the existing solution of the quadratic equation: 
\[a x_0^2 + b y_0^2 = 1,\]
and show that \( a \in N_{F(\sqrt{b})/F(F(\sqrt{b}))} \). From \( x_0 = 0 \) the result would follow trivially, as 
\[F(\sqrt{b}) = F.\]
So assume \( x \neq 0 \), then we can write:
\[a = \frac{1}{x_0^2} + \frac{b y_0^2}{x_0} = N_{F(\sqrt{b})/F} \left( \frac{1}{x_0} + \sqrt{b} \frac{y_0}{x_0} \right) \implies a \in N_{F(\sqrt{b})/F(F(\sqrt{b}))}\]

- Now if \( b \) is a square in \( F \), i.e. \( \exists c \in F : \sqrt{b} = c \) then
\[c^2 = b = j^2 \implies (c + j)(c - j) = 0\]
and therefore \( \mathcal{A} \) has zero divisors, so it can’t be a division algebra. So assume \( \sqrt{b} \in F. \) From our last point we now that \( a \in N_{F(\sqrt{b})/F(F(\sqrt{b}))} \), hence \( \exists x_1, y_1 \in F, \) of which at least one is non-zero, with \( a = x_1^2 - b y_1^2 \) and follows that \( n(x_1 + i + y_1 j) = 0, \) so that \( \mathcal{A} \) has a non-zero, non-invertible element.

\[\square\]

The role of quaternion algebras in number theory, in particular in class field theory lies by the fact that they correspond to the constitutes of elements of order 2 in the Brauer group, a construction that aims to the classification of simple central algebras up to Morita-equivalence. In that context they are used for the construction of generalized reciprocity laws, which are the "fine structure" behind modular arithmetic. This is just a motivational appetizer, that may help to strengthen the nexus between algebraic number theory and differential geometry under the geometric constructions that appear from this abstract non-sense, a scent of which we describe here. But enough of this for now, let’s bring some "order":

**Definition:** Let \( F \) be a number-field, \( \mathcal{O}_F \) be the ring of integers of \( F \) and \( \mathcal{A} \) a quaternion-algebra over \( F \).

- Let \( V \) be a \( F \)-vector space and \( L \) a finitely generated \( \mathcal{O}_F \)-module contained in \( V \), then we call \( L \) an \( \mathcal{O}_F \)-Lattice in \( V \). Moreover, we call \( L \) a complete \( \mathcal{O}_F \)-Lattice in \( V \) if \( L \otimes_{\mathcal{O}_F} F \cong V \).

- An **Ideal** \( I \) of \( A \) is a complete \( \mathcal{O}_F \)-Lattice in \( A \).

- An **Order** \( \mathcal{O} \) in \( A \) is an ideal, which is endowed with a structure of a ring with 1.

- An order of \( A \) is **maximal** if it is maximal with respect to inclusion.

- The group of **units of reduced norm** 1 is \( \mathcal{O}^1 := \{ x \in \mathcal{O} | n(x) = 1 \} \).
3.2 Ramified Quaternions

Let $\mathcal{A} = \left( \frac{a,b}{F} \right)$, $F$ quadratic number field with $[K : \mathbb{Q}] = n$ and $K/F$ a finite extension. For each Galois field embedding $\sigma : F \to K$ we denote:

$$\mathcal{A}^\sigma = \left( \frac{\sigma(a), \sigma(b)}{\sigma(F)} \right)$$

$$\mathcal{A}^\sigma \otimes_F K = \left( \frac{\sigma(a), \sigma(b)}{K} \right)$$

Definition

- An element $\alpha \in F$ is called totally positive if $\sigma(\alpha) \geq 0$ for every real Galois field embedding $\sigma : F \to \mathbb{R}$
- $F$ is totally real, if every Galois embedding $\sigma_i : F \to \mathbb{C}$; $i \in \{1, \ldots, n\} \implies \sigma_i(F) \subset \mathbb{R}$, i.e. all Galois field embeddings have real image. We set $\sigma_1$ to be the one corresponding to the identity automorphism.
- For $\sigma : F \to \mathbb{R}$ of the number field $F$, then we call $\left( \frac{a,b}{F} \right)$ ramified at $\sigma$ if:
  $$\exists \rho : \left( \frac{\sigma(a), \sigma(b)}{\mathbb{R}} \right) \sim \mathcal{H}$$
  and unramified at $\sigma$ if:
  $$\exists \tilde{\rho} : \left( \frac{\sigma(a), \sigma(b)}{\mathbb{R}} \right) \sim M(2, \mathbb{R})$$

Proposition: Let $\mathcal{A}$ a quaternion algebra over a totally real number field $F$ such that the only unramified "place" is at $\sigma_1$. If $F \neq \mathbb{Q}$ then $\mathcal{A}$ is a division algebra.

Proof: Suppose $\mathcal{A}$ is not a division algebra. Then the last theorem implies, that $\mathcal{A} \cong M(2, \mathbb{F})$. Therefore we have:

$$\forall i \geq 2; \quad A^\sigma_i = M(2, \sigma_i(F)) \implies A^\sigma_i \otimes \mathbb{R} = M(2, \mathbb{R})$$

which contradicts the assumption for ramification.

In what follows we are interested in the situation of the last proposition to construct the arithmetic groups.
4 Groups from Orders

For an order $\mathcal{O}$ in $\mathcal{A}$ and the isomorphism $\rho^1 : \left( \frac{\sigma(a), \sigma(b)}{\mathbb{R}} \right) \cong M(2, \mathbb{R})$, it is $\rho^1(\mathcal{O}^1)$ subgroup of $SL(2, \mathbb{R})$ and $\Gamma = \rho^1(\mathcal{O}^1)/\{\pm 1\}$ a subgroup of $PSL(2, \mathbb{R})$.

**Theorem:** For an order $\mathcal{O}$ in $\mathcal{A}$ and the isomorphism $\rho^1 : \left( \frac{\sigma(a), \sigma(b)}{\mathbb{R}} \right) \cong M(2, \mathbb{R})$, it is $\rho^1(\mathcal{O}^1)$ subgroup of $SL(2, \mathbb{R})$ and $\Gamma = \rho^1(\mathcal{O}^1)/\{\pm 1\}$ a subgroup of $PSL(2, \mathbb{R})$. Then $\Gamma$, is a Fuchsian group.

**Proof:** Although the statement is true in general we will prove it here for simplicity without going into number theoretic details for:

$$\mathcal{A} = \left( \frac{a, b}{\mathbb{Q}} \right) \text{ and } \mathcal{O} = \{x \in \mathcal{A} | x_0, x_1, x_2, x_3 \in \mathbb{Z}\}.$$  

What is to be shown, is that $\Gamma$ is a discrete subgroup of $SL(2, \mathbb{R})$ under the constructed embedding $\phi$ of the algebra $\mathcal{A}$ into $SL(2, \mathbb{R})$, from paragraph 1. We do this by showing that there is a neighborhood $U$ of the identity in $SL(2, \mathbb{R})$ disjoint to $\rho^1(\mathcal{O}^1)$. For this purpose choose:

$$U := \{g = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} \in SL(2, \mathbb{R}) | |g_{11} - 1| \leq \frac{1}{2}; |g_{12}| \leq \frac{1}{2}; |g_{21}| \leq \frac{1}{2}; |g_{22} - 1| \leq \frac{1}{2} \};$$

take $g_x \in \rho^1(\mathcal{O}^1) \cap U$ and show that $g_x = id$:

$g_{11} = x_0 + \sqrt{a}x_1; g_{12} = x_2 + \sqrt{a}x_3; g_{21} = b(x_2 - \sqrt{a}x_3); g_{22} = x_0 - \sqrt{a}x_1; x_0, x_1, x_2, x_3 \in \mathbb{Z}$

The condition that $g$ lives in $U$ implies:

$$|g_{11} + g_{22} - 2| < 1 \implies |2x_0 - 2| < 1 \implies x_0 = 1.$$  

For $b > 1$:

$$|x_2 - \sqrt{a}x_3| < \frac{1}{2b} < \frac{1}{2} \implies |2x_2| < 1 \implies x_2 = 0$$

Further it is:

$$|x_1\sqrt{a}| < \frac{1}{2}; |x_3\sqrt{a}| < \frac{1}{2} \implies x_1 = x_3 = 0$$

That gives us: $g_x = id$, and therefore the quotient $\Gamma = \rho^1(\mathcal{O}^1)/\{\pm 1\}$ is a Fuchsian group, as it is a discrete subgroup of $PSL(2, \mathbb{R})$.

**Definition:** A subgroup $\Gamma < \Gamma$ is said to be a Fuchsian group derived from a quaternion algebra.

**Definition:** Two subgroups $\Gamma_1, \Gamma_2 < \Gamma$ of any group $\Gamma$ are said to be commensurable if: $[\Gamma_j : \Gamma_1 \cap \Gamma_2] < \infty; j = 1, 2$.

**Definition:** A group that is commensurable to a group of the form of $\Gamma$ constructed as above is said to be an Arithmetic Fuchsian group.

I general, for a totally real number field, we obtain an arithmetic group in that manner if and only if there is exactly one real Galois embedding such that the quaternion algebra is not a division algebra.