QUATERNION ALGEBRA AND SHIMURA CURVES

YONG-QI LIANG

Abstract. The aim of this work is to give an introduction to quaternion algebra and Shimura curves. We start by giving some basic notions of quaternion algebra. Then a definition of Shimura curve is shown. At last the theorem of Kazhdan-Margulis is given without proof.

1. Quaternion Algebra

Definition 1.1. Let F be a field $(char(F) = 0)$, a *quaternion algebra* over F is a 4-dimensional F-algebra $B_{a,b} = F \oplus Fi \oplus Fj \oplus Fk$ with the multiplication defined by the relations : $i^2 = a, j^2 = b, ij = k = -ji$ where $a, b \in F^*$.

Definition 1.2. $B_{a,b}$ is a quaternion F-algebra , the *reduced norm* is a map $n : B_{a,b} \to F, x+yi+zj+wk \mapsto x^2-ay^2-bz^2+abw^2$,Then $n(\alpha\beta) = n(\alpha)n(\beta)$ for every $\alpha, \beta \in B$, and $B^{\times,1}_{a,b} = \{u \in B^{\times}_{a,b} | n(u) = 1\}$ is a subgroup of $B^{\times}_{a,b}$. The *reduced trace* is a map $tr : B_{a,b} \to F, x + yi + zj + wk \mapsto 2x$.

Remark 1.3. If $\alpha \in B$, then α is a unit if and only if $n(\alpha) \neq 0$, and $\alpha^{-1} = \bar{\alpha}/n(\alpha)$, where the conjugate $\bar{\alpha} = x - yi - zj - wk$ if $\alpha = x + yi + zj + wk$.

Remark 1.4.

(1)$B_{a,b}$ is central simple F-algebra(i.e. B is a simple algebra and its center is F).

(2)$B_{a,b} \simeq B_{a\lambda^2,b\mu^2}$ for every $\lambda, \mu \in F^*$. Let $B_{a,b} = F \oplus Fi \oplus Fj \oplus Fk$ and $B_{a\lambda^2,b\mu^2} = F \oplus Fi' \oplus Fj' \oplus Fk'$, if we set $\varphi(i) = \frac{1}{\lambda}i'$ and $\varphi(j) = \frac{1}{\mu}j'$, then φ can be extend to an isomorphism from $B_{a,b}$ to $B_{a\lambda^2,b\mu^2}$.

(3)By Wedderburn's Theorem (i.e. Every central simple algebra is of the form $M_n(D)$ for some $n \in \mathbb{N}$ with D a division algebra) $B = B_{a,b}$ is isomorphic to a 4-dimensional division algebra (said to be ramified) or $M_2(F)$ (said to be split) .

(4)If $F = \mathbb{C}$, every element in $\mathbb{C}^*$ is a square, hence $B_{a,b} \simeq B_{1,1}$ by (2). One can verify that $\varphi(i) = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \varphi(j) = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ extends to an isomorphism from $B_{1,1}$ to $M_2(\mathbb{C})$.

(5)If $F = \mathbb{R}$ then every quaternion algebra is isomorphic to $M_2(\mathbb{R})$ or the Hamiltonnian quaternion $\mathbb{H} = B_{-1,-1}$. By (2), there are only four types

Key words and phrases. quaternion algebra , Shimura curve.
This work was completed with the help of Prof. Ullmo and Prof. Ouyang .

$B_{1,1}, B_{1,-1}, B_{-1,1}, \mathbb{H} = B_{-1,-1}$ for B. Note that $k^2 = ijij = -iijj = -ab$, by the symmetry of i, j, k one obtains $B_{1,1} \simeq B_{1,-1} \simeq B_{-1,1}$. One can verify that φ given in (4) is an isomorphism from $B_{1,1}$ to $M_2(\mathbb{R})$ with $F = \mathbb{R}$.

(6)If $F = \mathbb{Q}_p$ then the Hilbert symbol (to be discussed later, see definition1.5 and proposition1.7)

$$(a, b)_p = \begin{cases} 1 & , \text{ if } B_{a,b} \simeq M_2(\mathbb{Q}_p), \\ -1 & , \text{ if } B_{a,b} \text{ is a division algebra.} \end{cases}$$

(7)Let F be a number field , and B be a quaternion algebra over F , let

$$d(B) = \{v | v \text{ is a prime } (include\ \infty) \text{ of } F \text{ such that } F_v \otimes_F B \text{ is ramified}\}$$

where F_v is the v-adic completion of F, we have the following properties:

(a)$d(B)$ is a finite set with an even number of elements;(see theorem1.8 below for $F = \mathbb{Q}$)

(b)$B \simeq B'$ if and only if $d(B) = d(B')$;

(c)If S is a set containing a finite even number of primes of F , then there exists a quaternion algebra B over F such that $S = d(B)$.

Definition 1.5. Let k be a field, define the *Hilbert symbol* $(a, b) = 1$ if $0 = Z^2 - aX^2 - bY^2$ has a nonzero solution over k, otherwise $(a, b) = -1$. In particular, if $k = \mathbb{Q}_p$ the Hilbert symbol will denoted by $(a, b)_p$.

Lemma 1.6. *If* $(a, b)_p = -1$*, then* $n(x+yi+zj+wk) = x^2-ay^2-bz^2+abw^2 = 0$ *has no nonzero solution.*

Proof. A proof using the theory of quadratic forms is given in [3, p.39] □

Proposition 1.7. *The quaternion algebra* B *is a division algebra if and only if* $(a, b) = -1$*.*

Proof. First, B is a division algebra if and only if all the nonzeros are unit, if and only if $n(\alpha) \neq 0$ for all $\alpha \neq 0$ by remark 1.3, in other words $0 = x^2 - ay^2 - bz^2 + abw^2$ has no nonzero solution. In this case, one can deduce that $0 = x^2 - ay^2 - bz^2$ has no nonzero solution, hence $(a, b) = -1$. Conversely if $(a, b) = -1$, then $n(x + yi + zj + wk) = x^2 - ay^2 - bz^2 + abw^2 = 0$ has no nonzero solution by the lemma above, so B is a division algebra. □

Theorem 1.8 (Hilbert)**.** $\Pi_{p \leq \infty}(a, b)_p = 1$.

Proof. A proof is given in [3, p.23]. □

Definition 1.9. Let F be the fraction field of an integral domain R and B be a quaternion algebra over F, a *R-lattice* is a R-submodule L of B satisfying

(1)L is finitely generated as a R-module,

(2)L contains a F-basis of B.

A *R-order* of B is a R-lattice in B which is a subring of B with the same identity.

Definition 1.10. Let B be a quaternion algebra over F, R be the ring of integers of F. An *Eichler order* $\mathcal{O}$ in B is the intersection of two maximal R-orders in B. The *level* m of $\mathcal{O}$ is the index of $\mathcal{O}$ in any maximal order containing it.

Definition 1.11. Let B be a quaternion algebra over F, we define the *discriminant* of B $disc(B) = \Pi_{p \in d(B)-\{\infty\}} p$.

2. Shimura Curves

Definition 2.1. Let B be a quaternion algebra over $\mathbb{Q}$ of discriminant D such that $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$, and let $\mathcal{O}$ be an Eichler order of level m in B, and set $\Gamma_0^D(m) = \mathcal{O}^{\times,1}$, then there exists a well-define action of $B^\times$ on the upper half plane $\mathcal{H}$. We define the *Shimura curve* $X_0^D(m) = \Gamma_0^D(m) \backslash \mathcal{H}$.

Indeed, $X_0^D(m)$ is a moduli space for Abelian varieties A of dimension 2 over $\mathbb{C}$ with an embedding $i : B \to End(A) \otimes \mathbb{Q}$ and some level structure depending on m, one can find a description in [4, p.35].

Proposition 2.2. *If B is a division algebra, then X_0^D is a compact Riemann surface.*

More generally, if $G_{\mathbb{Q}}$ is a semi-simple algebraic group over $\mathbb{Q}$ and $\Gamma \subset G(\mathbb{Q})$ is an arithmetic lattice(to be defined in the next lecture), then $\Gamma \backslash G(\mathbb{R})$ is compact if and only if $G_{\mathbb{Q}}$ is $\mathbb{Q}$-anisotropic (i.e. $G(\mathbb{Q})$ has no nontrivial unipotent element— all its eigenvalue are 1).

Here $G(\mathbb{Q}) = B^{\times,1}$. If $\alpha = x + yi + zj + wk \in B^{\times,1}$ is a unipotent element, then $n(\alpha) = x^2 - ay^2 - bz^2 + abw^2 = 1$ and $tr(\alpha) = 2x = 2$, we obtain $x = 1$, $w^2 - a(\frac{y}{a})^2 - b(\frac{z}{b})^2 = 0$ in $\mathbb{Q}$, hence $(a, b)_p = 1$ for all prime p, then $d(B) = \phi = d(M_2(\mathbb{Q}))$, $B^{\times,1} \simeq SL_2(\mathbb{Q})$ by remark1.4, which contradicts to the fact that B is a division algebra. Similarly, one can prove that this proposition holds for the quaternion algebra over a totally real field (to be defined later).

Let

$$\begin{aligned}
\mathbb{A} &= \mathbb{R} \times \widehat{\Pi}_p \mathbb{Q}_p \\
&= \{(x, \ldots, x_p, \ldots) \in \mathbb{R} \times \Pi_p \mathbb{Q}_p |\ x_p \in \mathbb{Z}_p \text{for all but finitely many p}\} \\
B_{\mathbb{A}} &= B \otimes_{\mathbb{Q}} \mathbb{A} \simeq M_2(\mathbb{R}) \times \widehat{\Pi}_p (B \otimes_{\mathbb{Q}} \mathbb{Q}_p)
\end{aligned}$$

$$\begin{aligned}
\varphi_\infty &: B \to B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R}) \\
\varphi_p &: B \to B \otimes_{\mathbb{Q}} \mathbb{Q}_p \\
\varphi = \varphi_\infty \times \Pi_p \varphi_p &: B \to B_{\mathbb{A}} = B \otimes_{\mathbb{Q}} \mathbb{A} \simeq M_2(\mathbb{R}) \times \widehat{\Pi}_p (B \otimes_{\mathbb{Q}} \mathbb{Q}_p); \\
& \quad x \mapsto (x, \ldots, x, \ldots)
\end{aligned}$$

Let $\mathcal{O}$ be a $\mathbb{Z}$-order of B, $\varphi : \mathcal{O}^{\times,1} \to B^{\times,1}$ is injective, so one can view $\mathcal{O}^{\times,1}$ as a subgroup of $B_{\mathbb{A}}^{\times,1}$.

Proposition 2.3. *(1)$B^{\times}$ is a discrete subgroup of $B_{\mathbb{A}}^{\times}$.*

(2)$B^{\times,1}\backslash B_{\mathbb{A}}^{\times,1}$ is compact, if B is a division algebra.

Proposition 2.2 can also be proof by using adelic language, see [5, p.104].

Let F be a totally real field with $[F:\mathbb{Q}] = d$, and B be a quarternion algebra over F satisfying : $B \otimes_{F,\rho_1} \mathbb{R} \simeq M_2(\mathbb{R})$ for the embedding $\rho_1 : F \to \mathbb{R}$, and $B \otimes_{F,\rho_i} \mathbb{R} \simeq \mathbb{H}$ for all other embeddings $\rho_i : F \to \mathbb{R}$ $(2 \leq i \leq d)$, where $\mathbb{H}$ is the Hammiltonnian quaternion over $\mathbb{R}$. Then $B \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R}) \times \mathbb{H}^{d-1}$, therefore $B^{\times} \otimes_{\mathbb{Q}} \mathbb{R} \simeq GL_2(R) \times (\mathbb{H}^{\times})^{d-1}$, $B^{\times,1} \otimes_{\mathbb{Q}} \mathbb{R} \simeq SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$. Let $\mathcal{O}$ be an order of B, then $\mathcal{O}^{\times,1}$ can be viewed as a subgroup of $SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$. Let $\pi : SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1} \to SL_2(\mathbb{R})$ be the canonical projection, then $\pi(\mathcal{O}^{\times,1})$ is a discrete subgroup of $SL_2(\mathbb{R})$(see the proposition below), so $\mathcal{O}^{\times,1}$ acts naturally on the upper half plane $\mathcal{H}$, induced by the action of $SL_2(\mathbb{R})$ on $\mathcal{H}$ (i.e. $\gamma.z := \pi(\gamma).z$, with $\gamma \in \mathcal{O}^{\times,1}, z \in \mathcal{H}$). We can also define a curve $X = \mathcal{O}^{\times,1}\backslash\mathcal{H}$, which is a compact Riemann surface(see proposition2.10 below).

Definition 2.4. Two subgroups H_1 and H_2 of G are said to be *commensurable* if $H_1 \cap H_2$ is of finite index in both H_1 and H_2. Commensurability is an equivalent relation.

Let G be an algebraic group over $\mathbb{Q}$, then one can view G as a subgroup of GL_n for some $n \in \mathbb{N}$, set $G(\mathbb{Z}) = G(\mathbb{Q}) \cap GL_n(\mathbb{Z})$.

Definition 2.5. A subgroup Γ of $G(\mathbb{Q})$ is said to be *arithmetic* if Γ and $G(\mathbb{Z})$ are commensurable.

Remark 2.6.

(1)The notion of commensurability does not depend on the imbedding $i : G \hookrightarrow GL_n$, hence the definition makes sense.

(2)In particular, a subgroup $\Gamma \subseteq SL_2(\mathbb{Q})$ is arithmetic if Γ and $SL_2(\mathbb{Z})$ are commensurable.

Definition 2.7. A lattice Γ in a linear algebraic reductive group H over $\mathbb{R}$, is said to be *arithmetic* if there exists a reductive group G over $\mathbb{Q}$ such that $G \otimes_{\mathbb{Q}} \mathbb{R} \simeq H(\mathbb{R}) \times K(\mathbb{R})$ with a compact group $K_{\mathbb{R}}$, and a subgroup Γ' of $G(\mathbb{Q})$ commensurable with $G(\mathbb{Z})$ such that $\Gamma = \pi(\Gamma')$, where $\pi : H \times K \to H$ is the canonical projection.

Remark 2.8. Let B be a quaternion algebra over F as above, $B^{\times,1} \otimes_{\mathbb{Q}} \mathbb{R} \simeq SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$, $(\mathbb{H}^{\times,1})^{d-1}$ is compact, then $\Gamma = \pi(\mathcal{O}^{\times,1})$ with $\Gamma' = \mathcal{O}^{\times,1}$ is an arithmetic subgroup of $SL_2(\mathbb{R})$ for some order $\mathcal{O}$ in B. Non-isomorphic B's define different commensurability classes of arithmetic subgroups of $SL_2(\mathbb{R})$, and all such classes arise in this way, so there are countably many classes of arithmetic subgroups of $SL_2(\mathbb{R})$, and countably many such curves $X = \Gamma\backslash\mathcal{H}$.

Lemma 2.9. *Let all the notations be as above, if B is a division algebra over F, then Γ' is a discrete subgroup of $SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$ and $\Gamma'\backslash SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$ is compact.*

Proof. The proof makes use of adelic language, see [2]. ☐

Proposition 2.10. *If B is a division algebra, then $\Gamma = \pi(\Gamma')$ is a discrete subgroup of $SL_2(\mathbb{R})$ and $\Gamma\backslash\mathcal{H}$ is compact.*

Proof. $\mathbb{H}^{\times,1} = \{x + yi + zj + wk \in \mathbb{H} | x^2 + y^2 + z^2 + w^2 = 1\} \simeq SO_3(\mathbb{R})$, which is a compact group, hence $(\mathbb{H}^{\times,1})^{d-1}$ is compact. Γ' is a discrete subgroup of $SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$ by the lemma above, so $\Gamma' \cap (\mathbb{H}^{\times,1})^{d-1}$ is discrete in $(\mathbb{H}^{\times,1})^{d-1}$, hence $\Gamma' \cap (\mathbb{H}^{\times,1})^{d-1}$ must be a finite set, thus $\Gamma = \pi(\Gamma')$ is also a discrete subgroup of $SL_2(\mathbb{R})$. $\Gamma'\backslash SL_2(\mathbb{R}) \times (\mathbb{H}^{\times,1})^{d-1}$ is compact by the lemma above, so $\pi(\Gamma')\backslash SL_2$ is also compact. We know that $\mathcal{H} \simeq SL_2(\mathbb{R})/SO_2$. Therefore, by definition, $\Gamma\backslash\mathcal{H} = \pi(\Gamma')\backslash\mathcal{H} \simeq \pi(\Gamma')\backslash SL_2(\mathbb{R})/SO_2$ is compact. ☐

Remark 2.11. In the proof above the compactness of $(\mathbb{H}^{\times,1})^{d-1}$ is essential. We consider this example: $F = \mathbb{Q}(\sqrt{2})$, $B = B_{3,3}$ a quaternion division algebra over F, but $B \otimes \mathbb{R} \simeq M_2(\mathbb{R}) \times M_2(\mathbb{R})$. $D = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$ is the ring of integers, and $\mathcal{O} = D[1, i, j, k]$ is an order of B, $\pi(\mathcal{O}^{\times,1}) = SL_2(D)$. However, $SL_2(D)$ is not a discrete subgroup of $GL_2(\mathbb{R})$.

$$\begin{pmatrix} (\sqrt{2}-1)^n & \\ & (\sqrt{2}+1)^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} (\sqrt{2}+1)^n & \\ & (\sqrt{2}-1)^n \end{pmatrix}$$
$$= \begin{pmatrix} 1 & (\sqrt{2}-1)^{2n} \\ & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \text{as } n \to \infty.$$

Let $G_{\mathbb{Q}}$ be a linear algebraic group over $\mathbb{Q}$, let K_∞ be a maximal compact subgroup of $G(\mathbb{R})$, then the symmetric space $G(\mathbb{R})/K_\infty \simeq \mathcal{H}$, let $\pi : G(\mathbb{R}) \to \mathcal{H}$ be the canonical projection.

Definition 2.12. A lattice Γ in $\mathcal{H}$ is said to be *arithmetic* if there is a arithmetic subgroup Γ' of $G(\mathbb{Q})$ such that $\Gamma = \pi(\Gamma')$.

Not every discrete subgroup of $SL_2(\mathbb{R})$ is arithmetic. It is a classical fact that every compact Riemann surface of genus > 1 is isomorphic to $\Gamma\backslash\mathcal{H}$ where Γ is a discrete subgroup of $Aut(\mathcal{H}) = SL_2(\mathbb{R})$. Since there are uncountably many such Riemann surfaces, so there are uncountably many discrete subgroups of $SL_2(\mathbb{R})$, but only countably many ones are arithmetic.

Theorem 2.13 (Kazhdan-Margulis)**.** *Let Γ be a lattice in $SL_2(\mathbb{R})$. Then Γ is arithmetic if and only if $[comm(\Gamma) : \Gamma] = \infty$, where*

$$comm(\Gamma) = \left\{x \in SL_2(\mathbb{R}) | \Gamma \text{ and } x\Gamma x^{-1} \text{are commensurable}\right\}.$$

Proof. This is a special case of a much more general result. A proof is given in [6] . ☐

Remark 2.14. The condition $[comm(\Gamma) : \Gamma] = \infty$ means that there exists a nontrivial Hecke operator on $X = \Gamma\backslash\mathcal{H}$.

References

[1] C.Maclachlan. Introduction to arithmetic Fuchsian groups.

[2] G.Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

[3] J.-P.Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer-Verlag, 1973.

[4] J.S.Milne. *Canonical Models of Shimura Curves*.

[5] M.-F.Vigneras. *Arithmétique des Algèbres de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[6] R.J.Zimmer. *Ergodic Theory and Semisimple Groups*. Birkh 1984.

[7] R.Kohel. Hecke module structure of quaternions.

Institute of Mathematics, Chinese Academy of Sciences

E-mail address: yongqi.liang@163.com