Determining large groups and varieties from small subgroups and subvarieties

This course will consist of two parts with the common theme of analyzing a geometric object via geometric sub-objects which are 'small' in an appropriate sense. This is an expanded course outline which includes some background references as well as some exercises relevant to this background. For an explanation of terminology used in the next three paragraphs, see the following sections.

In the first half of the course, we will begin by describing the work of H. W. Lenstra, Jr., on finding generators for the unit groups of subrings of number fields. Lenstra discovered that from the point of view of computational complexity, it is advantageous to first consider the units of the ring of S-integers of L for some moderately large finite set of places S. This amounts to allowing denominators which only involve a prescribed finite set of primes. We will develop a generalization of Lenstra's method which applies to find generators of small height for the S-integral points of certain algebraic groups G defined over number fields. We will focus on G which are compact forms of GL_d for $d \geq 1$.

In the second half of the course, we will turn to smooth projective surfaces defined by arithmetic lattices. These are Shimura varieties of complex dimension 2. We will try to generate subgroups of finite index in the fundamental groups of these surfaces by the fundamental groups of finite unions of totally geodesic projective curves on them, that is, via immersed Shimura curves.

In both settings, the groups we will study are S-arithmetic lattices in a product of Lie groups over local fields. We will use the structure of our generating sets to consider several open problems about the geometry, group theory, and arithmetic of these lattices. In particular, we will consider the structure of the cohomology of S-arithmetic groups and characteristic p analogues. We will also discuss connections with the congruence subgroup problem, which is open in many of the cases under consideration in this project.

1 Small generators for S-units of division algebras

The first goal of this course will be to generalize ideas of H. W. Lenstra Jr. for generating S-units of algebraic number fields to the noncommutative setting. This portion of the course should be readily accessible to graduate students of all backgrounds.

1.1 Algebraic numbers, units and heights

Let k be an algebraic number field, i.e., a finite extension of the rational numbers $\mathbb{Q}$. We will assume some familiarity with the basic theory of local and global fields. Good resources are the volume edited by Cassels and Fröhlich [1] and Weil's book Basic Number Theory [16]. Let V_∞ and V_f denote the archimedean and nonarchimedean places of k, respectively and k_v denote the completion of k at the place v.

Then k has a unique maximal order $\mathcal{O}_k$, the *ring of integers*. Then $\mathcal{O}_k$ is a free $\mathbb{Z}$-module generated by n elements, where $n = [k : \mathbb{Q}]$. Let k^* be the multiplicative group of nonzero elements of k and let $\mathcal{O}_k^*$ denote the group of units of $\mathcal{O}_k$, i.e., the group of invertible integers.

It is a classical fact, known as Dirichlet's Unit Theorem, that $\mathcal{O}_k^*$ is a free abelian group isomorphic to $\mu(k) \times \mathbb{Z}^{r_1+r_2-1}$, where r_1 and r_2 denotes the number of real and complex places of k, respectively, and $\mu(k)$ is the group of roots of unity in k. Recall that $n = r_1 + 2r_2$. It will be useful in what follows to think of k^* as being $\mathrm{GL}_1(k)$, the invertible 1×1 matrices over k, and $\mathcal{O}_k^*$ as the subgroup of 1×1 invertible integral matrices.

Exercise 1. *For which finite extensions ℓ/k of number fields is it the case that the rank of the unit group $\mathcal{O}_\ell^*$ is the same as the rank of the unit group $\mathcal{O}_k^*$?*

Definition 2. *Let $\{R_j\}_{j\in J}$ be an indexed family of locally compact topological rings. Assume that for all but finitely many $j \in J$ there exists a distinguished open compact subring $S_j \subset R_j$. The* restricted direct product

$$\prod_{j\in J}{}' R_j$$

of the rings R_j is the subring of the direct product $\prod R_j$ consisting of those elements $(x_j)_{j\in J}$ such that $x_j \in S_j$ for all but finitely many $j \in J$.

The most important restricted direct products are the adele and idele rings of a number field, though we will later consider such products for division algebras as well. Ideles were first considered by Chevalley in studying class field theory and the adeles were later considered by Weil (adele being an additive idele). We now recall their definitions.

Definition 3. *The* adele ring *of a number field k is the restricted direct product of the fields k_v with respect to the subring $\mathcal{O}_v$ for each nonarchimedean place, where $\mathcal{O}_v$ is the ring of integers of k_v. That is*

$$\mathbb{A}_k = \left\{ (x_v) \in \prod_{v\in V_\infty \cup V_f} k_v \ : \ x_v \in \mathcal{O}_v \text{ for all but finitely many } v \in V_f \right\}.$$

The idele ring $\mathbb{I}_k$ *of k is the restricted direct product of the k_v^* with respect to the subring $\mathcal{O}_v^*$ for v nonarchimedean.*

Consider the *diagonal embedding* of k into $\prod_v k_v$, i.e., the map sending x to the constant vector $(x)_v$. For any $x \in k$, $x \in \mathcal{O}_v$ for all but finitely many nonarchimedean v, so the diagonal embedding has image in $\mathbb{A}_k$. The same holds for the ideles.

Now, let S be a set of places of k. We assume that S is finite and that it contains all archimedean places. Set $S_f = S \cap V_f$. Let

$$k_S = \prod_{v \in S} k_v.$$

There is a natural embedding of k_S into $\mathbb{A}_k$ where $x = (x_v) \in k_S$ is sent to the adele with v-adic component x_v for $v \in S$ and 1 for all $v \notin S$. (Note that the image is not in $\mathbb{A}_k$ when $|S| = \infty$.) From here forward, k and k_S will always be considered as subsets of $\mathbb{A}_k$. We also have the obvious analogues for k^* and k_S^* in $\mathbb{I}_k$.

Remark. We can do everything using the adeles, by considering $\mathbb{I}_k$ as the $\mathbb{A}_k$-points of the k-algebraic group GL_1. That is, $\mathbb{I}_k \cong \mathrm{GL}_1(\mathbb{A}_k)$. Many people use $\mathbb{G}_m$ (m being for 'multiplicative') for GL_1, so $\mathbb{I}_k = \mathbb{G}_m(\mathbb{A}_k)$[1]. Then $k_S^* = \mathrm{GL}_1(k_S)$ and so forth.

Exercise 4. *Prove that k is discrete in $\mathbb{A}_k$ using the fact that $\mathcal{O}_k$ embeds discretely into the product of the completions k_v of k at the archimedean places v of k.*

Finally, we introduce heights on algebraic number fields. Let k be an algebraic number field, V_∞ its archimedean places, V_f its nonarchimedean places, and $V = V_\infty \cup V_f$. For any place $v \in V$, let $|\ |_v$ be the associated absolute value.

Definition 5. *The* height *on k is the function $\mathrm{H}_k : k^* \to \mathbb{R}$ given by*

$$\mathrm{H}_k(x) = \prod_{v \in V} \max\{1, |x|_v\}.$$

Exercise 6. *Set $k = \mathbb{Q}$, and let $x = r/s$, where $r, s \in \mathbb{Z}$, $s > 0$, and $\gcd(r, s) = 1$. Decompose $r = \pm p_1^{i_1} \cdots p_N^{i_N}$ and $s = q_1^{j_1} \cdots q_M^{j_M}$ as products of distinct prime numbers (taking ± 1 where appropriate). Show*

$$\mathrm{H}_{\mathbb{Q}}(x) = \max\{|r|, |s|\}$$

by showing that for the archimedean place ∞

$$\max\{1, |r/s|_\infty\} = \begin{cases} |r/s| & \text{if} \quad |r/s| \geq 1 \\ 1 & \text{if} \quad |r/s| \leq 1 \end{cases}$$

and for the nonarchimedean place associated with a prime q,

$$\max\{1, |r/s|_q\} = \begin{cases} 1 & q \notin \{q_1, \ldots, q_M\} \\ q_n^{j_n} & q = q_n \in \{q_1, \ldots, q_M\} \end{cases}.$$

[1] Using $\mathbb{G}_a$ for the additive group, we also have the ridiculous-looking isomorphism $\mathbb{A}_k \cong \mathbb{G}_a(\mathbb{A}_k)$.

Exercise 7. *Let $\mathcal{O}_{k,S}$ be the ring of S-units in the algebraic number field k, where $S \subset V$ is a finite set of places of k. Prove that the set*

$$\mathrm{BH}_{k,S}(y) = \{x \in \mathcal{O}_{k,S}^* \ : \ \mathrm{H}_k(x) \leq y\}$$

is finite.

One can think of the height as a measure of the number of bits necessary to store a given element of k^*.

1.2 Lenstra's algorithm and S-units

Let $V = V_\infty \cup V_f$ be the places of k, where V_∞ (resp. V_f) is the set of archimedean (resp. finite) places. If R is a k-algebra or $\mathcal{O}_k$-module and $v \in V$, let R_v denote the completion of R at v.

Suppose that S is a finite set of places of k with $V_\infty \subset S$ and let $S_f = S \smallsetminus V_\infty$. The *$S$-integers* of $\mathcal{O}_k$, denoted $\mathcal{O}_{k,S}$, is the ring of elements of k which lie in $\mathcal{O}_{k,v}$ for every $v \notin S$. The multiplicative group of units of $\mathcal{O}_{k,S}$ is the group $\mathcal{O}_{k,S}^*$ of S-units of k.

For example, suppose $k = \mathbb{Q}$ and that $S = \{\infty, p_1, \ldots, p_r\}$ where the p_j are prime numbers. Then $\mathcal{O}_{\mathbb{Q},S} = \mathbb{Z}_S$ is the subring $\mathbb{Z}[p_1^{-1}, \ldots, p_r^{-1}]$ of $\mathbb{Q}$, with unit group

$$\mathbb{Z}_S^* = \langle -1, p_1, \ldots, p_r \rangle \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^r,$$

generated by -1 and p_j for $1 \leq j \leq r$.

For general k, finding generators for $\mathcal{O}_{k,S}^*$ is much more difficult. We will be interested in whether there are generators of "small" height. Recall that $x \in k^*$ is the quantity

$$H_k(x) = \prod_{v \in V} \max\{1, |x|_v\},$$

where $|\ |_v$ is the normalized absolute value at v. One natural measure of the size of the field k is the absolute value of the discriminant Δ_k of k. Finally a measure of the size of S is simply the maximum m_S of the norm $N(v)$ of a finite place $v \in S$, where $N(v)$ is the order of the residue field of the completion of k at v. We will be interested in the following question:

Question 8. *What hypotheses on k and S are sufficient to insure that there is a polynomial $F(x, y)$ which is independent of k and S such that one can find generators for $\mathcal{O}_{k,S}^*$ which have height bounded by $F(|\Delta_k|, m_S)$?*

For example, suppose $k = \mathbb{Q}$. When $x = p$ is a prime number one has $|p|_v \leq 1$ for all places v except for the infinite place ∞, and $|p|_\infty = p$. Similarly, $|p^{-1}|_v \leq 1$ for all $v \neq p$, and $|p^{-1}|_p = p$. Thus $H_\mathbb{Q}(p^{\pm 1}) = p$, and $H_\mathbb{Q}(-1) = 1$. One sees from this that $\mathcal{O}_{\mathbb{Q},S}$ can be generated by elements of height bounded by m_S, where $\Delta_\mathbb{Q} = 1$.

The next relevant example is when $k = \mathbb{Q}(\sqrt{d})$ is the real quadratic field associated to a square free integer $d > 1$ and S consists of the two archimedean

places and no finite places. Then

$$\mathcal{O}_{k,S}^* = \mathcal{O}_k^* = \{\pm\epsilon_k^j\}_{j=-\infty}^{\infty}$$

is generated by -1 and a fundamental unit ϵ_k of k whose embedding $\epsilon_{k,1}$ at one infinite place ∞_1 of k satisfies $\epsilon_{k,1} > 1$. One then has

$$|\epsilon_k|_{\infty_2} = |\epsilon_k|_{\infty_1}^{-1} = \epsilon_{k,1}^{-1} < 1$$

at the other infinite place ∞_2, while $|\epsilon_k|_v \leq 1$ at all finite places v. So

$$H_k(\epsilon_k) = \epsilon_{k,1}.$$

The Brauer–Siegel Theorem implies that for any $\delta > 0$, there is a constant $c_\delta > 0$ independent of the real quadratic field k such that

$$H_k(\epsilon_k) = \epsilon_{k,1} > c_\delta \cdot \frac{\exp(|\Delta_k|^{\frac{1}{2}-\delta})}{h_k}.$$

where h_k is the class number of k. It is a major open problem determine whether or not there are infinitely many real quadratic fields of class number 1, and it is widely believed that there are. If there are infinitely many such k, we see that their unit groups $\mathcal{O}_k^*$ cannot be generated by elements whose heights are bounded by a polynomial in $|\Delta_k|$.

In view of this, the following result shown by Lenstra in [7] is somewhat surprising:

Theorem 9. (Lenstra) *Suppose S contains V_∞ and all places v of norm bounded by $(2/\pi)^s|\Delta_k|^{1/2}$, where s is the number of complex places of k. Then $\mathcal{O}_{k,S}^*$ is generated by those elements with height bounded above by $(2/\pi)^s|\Delta_k|^{1/2}m_S$, where m_S is the maximum norm of a nonarchimedean place in S.*

Lenstra's proof is geometric. Indeed, he builds an explicit fundamental set for the action of $\mathcal{O}_{k,S}^*$ on the space

$$X_S = \prod_{v \in S} k_v^*,$$

which is a locally compact space on which $\mathcal{O}_{k,S}^*$ acts discretely and cocompactly. He then uses a lemma from geometric group theory to recover a set of generators, and proves that these generators have height bounded as above. The sections of [7] which are most relevant to the above Theorem are §1 and §6.

1.3 Algebraic groups and division algebras

The first goal of this course will be to generalize the above results to the non-commutative setting. From the point of view of algebraic groups, the group of S-units of a number field k is the group of S-integral points of the algebraic group GL_1/k. We will be generalize this by considering the S-integral

points of algebraic groups which are compact forms of the group GL_d for $d \geq 1$ constructed in the following way.

Let D be finite dimensional division algebra with center k. The dimension of D over k then equals d^2 for some integer d. By letting D act on itself by left multiplication, we have an algebra embedding of D into $\mathrm{Mat}_{d^2}(k)$. This realizes the multiplicative group $G = D^* = D \smallsetminus \{0\}$ as an algebraic group. The group G becomes isomorphic to GL_d over an algebraic closure of k.

We will begin the course recalling the basic structure of division algebras over local and global fields, their adelic points, S-orders $\mathcal{O}_{D,S}$ of division algebras D when S is a finite set of places of k, and the S-units groups $\mathcal{O}^*_{D,S}$ of such orders. As in the case of number fields, $\mathcal{O}^*_{D,S}$ is a finitely generated group. For background (when $d = 2$) we recommend chapters 6 and 7 of [9]. This reference also describes the connection of the groups $\mathcal{O}^*_{D,S}$ to geometry.

The groups $\mathcal{O}^*_{D,S}$ act on products of symmetric spaces and Bruhat–Tits buildings, and include a large number of classically studied groups. For example, when $S = V_\infty$ and D is a quaternion algebra over k with certain ramification properties, we obtain cocompact lattices acting on products of hyperbolic planes and hyperbolic 3-spaces. Finding generators and relators for these groups has been of significant interest since the late 19^{th} century.

We also must introduce a notion of height on a division algebra D over a number field k. Rather than utilizing a projective embedding of D, we will construct a height that is more closely related to the group law on the algebra.

We consider the S-units $\mathcal{O}^*_{D,S}$ as a discrete subgroup acting cocompactly on the product $\prod_{v \in S} D^*_v$. Using Minkowski's lattice point theorem, we generalize Lenstra's fundamental set in the number field case to get an effectively computable fundamental set for the action of $\mathcal{O}^*_{D,S}$.

This leads to a primitive recursive algorithm for computing generators for $\mathcal{O}^*_{D,S}$, strengthening the results of Grunewald and Segal [3] for these S-arithmetic lattices. Indeed, we will use our fundamental domain and some combinatorial group theory to construct generators of height bounded explicitly in the basic arithmetic invariants of D, S and k. Considering k as an algebra of degree 1 recovers Lenstra's results as a special case.

1.4 Applications, questions, and problems

We now list several projects related to the first half of the course.

Run time analysis. We begin with a problem in the number field setting. Lenstra shows that one can determine generators for $\mathcal{O}^*_k$ in time at most

$$(2 \log |\Delta_k|)^{\mathrm{O}(n)} |\Delta|^{\frac{3}{4}}.$$

He raises the question of whether the $\frac{3}{4}$ can be reduced unconditionally, possibly to $\frac{1}{2}$. See §5 of [7].

Behavior of heights. Our notion of height on an algebra requires a choice of subfield ℓ of D. Analyze the generating sets coming from different subfields ℓ. Is there a canonical ℓ that gives the 'smallest' generators for $\mathcal{O}^*_{D,S}$?

Small topological generators. Let D be a division algebra over the number field k and S a finite set of places of k containing all archimedean places. Our results exploit a set of *topological generators* for the group

$$D_S^* = \prod_{v \in S} D_S^*.$$

This is a finite subset $R \subset D_S^*$ such that R and U generate D_S^* for any open subgroup U of D_S^*. What is the minimum height of a set of topological generators of D_S^*?

Shrinking S. In the number field case, Lenstra is able to use the fact that $\mathcal{O}_S^*$ is a finitely generated abelian group to study generators for $\mathcal{O}_{S'}^*$ where $S' \subset S$. This is not possible in the noncommutative setting. Use the geometry of Bruhat–Tits buildings to find an effectively computable generating set for $\mathcal{O}_{D,S'}^*$ for $S' \subset S$.

Groups acting on products of trees. Let $k = \mathbb{Q}$ and let D be a quaternion division algebra over $\mathbb{Q}$ ramified at the infinite place. Let S contain exactly two places over which D is not a division algebra. Then $\mathcal{O}_{D,S}^*$ is a lattice acting irreducibly on a product of two Bruhat–Tits trees (see [14]). Find a presentation for the group $\mathcal{O}_{D,S}^*$. No such explicit presentations are known in the literature.

Cohomology of S-arithmetic groups. Groups of S-units of division algebras are fundamental examples of S-arithmetic lattices, and the cohomology of arithmetic and S-arithmetic groups are of very significant interest. Present some S-unit groups and use a computer algebra program to study the behavior of their cohomology groups on subgroups of finite index. Of particular interest lately has been the growth of torsion in cohomology of arithmetic groups, and it would be interesting to get an idea what might happen in the S-arithmetic setting.

The congruence subgroup problem. Again, using a presentation for an S-unit group, analyze the possible finite quotients of $\mathcal{O}_{D,S}^*$. There is a natural system of finite quotients arising from reductions of $\mathcal{O}_k$ modulo ideals. In its most basic form, the congruence subgroup problem asks whether or not these are the only finite quotients. For example, it is known that $\mathrm{SL}_2(\mathcal{O}_k)$ has the congruence subgroup property if and only if k is not $\mathbb{Q}$ or an imaginary quadratic field [13]. This question is open for all but some small cases relevant to this project (e.g., it is open for lattices acting irreducibly on a product of Bruhat–Tits trees).

Other fields. Study analogous questions for algebras in characteristic p or algebras over higher dimensional fields.

Other algebraic groups. The obstruction to generalizing our results to arbitrary S-arithmetic lattices in a reductive algebraic group over a number

field lies in our use of Minkowski's lattice point theorem. Find a way to obtain generators for other classes of S-arithmetic lattices, e.g., lattices in products of orthogonal groups of quadratic forms over number fields.

Cayley algebras. Generalize our methods to nonassociative algebras, particularly Cayley algebras over number fields.

2 Generating arithmetic varieties by arithmetic subvarieties

The second half of this course will concentrate on generating fundamental groups of certain smooth projective arithmetically defined surfaces by the fundamental groups of a nice collection of small subvarieties. The main tools are so-called Lefschetz Theorems. These give sufficiently conditions for the fundamental group of a Zariski closed subset Y of a variety X to generate a subgroup of finite index in the fundamental group of X .

We will consider X which are complex surfaces given by the quotient of a hermitian symmetric domain W by a cocompact arithmetic lattice. The Y we will consider are the connected union of Shimura curves on X. We will not assume that students have a background in the theory of arithmetic groups, hermitian symmetric domains, or Shimura varieties. Some familiarity with the basic complex algebraic geometry found in the first chapters of Griffiths and Harris [2] or of Hartshorne [4] would be helpful. It would also be very useful preparation to read Chapters 1 and 9 of [15] and relevant parts of [6] to understand the arithmetic theory of Fuchsian groups, since the groups we will consider are the natural generalization to one dimension higher.

2.1 The upper half plane and Fuchsian groups

Let $\mathbf{H}$ denote the upper half plane

$$\{z \in \mathbb{C} \ : \ \mathrm{Im}(z) > 0\}$$

equipped with the usual hyperbolic metric $|dz|/\mathrm{Im}(z)$. It is a classical fact that the group of holomorphic (equivalently, orientation preserving) isometries of $\mathbf{H}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm \mathrm{I}\}$ acting by Möbius transformations.

Exercise 10. *Let $\Gamma < \mathrm{PSL}_2(\mathbb{R})$ be a subgroup. Then $\Gamma\backslash\mathbf{H}$ is Hausdorff if and only if Γ is discrete in $\mathrm{PSL}_2(\mathbb{R})$ in the quotient topology descended from the natural topology on $\mathrm{SL}_2(\mathbb{R})$ considered as a subspace of $\mathrm{M}_2(\mathbb{R}) \cong \mathbb{R}^4$. (Hint: Show that a subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is discrete if and only if the identity is an isolated point, i.e., no sequence in Γ converges to the identity unless it is eventually constant.)*

If Γ is torsion-free, then $\Gamma\backslash\mathbf{H}$ is a manifold. Since Γ acts on $\mathbf{H}$ by isometries, the complex structure on $\mathbf{H}$ descends to a complex structure on $C_\Gamma = \Gamma\backslash\mathbf{H}$,

so C_Γ is a Riemann surface. Therefore, when C_Γ is compact, it is a projective curve over $\mathbb{C}$. See Shimura's book [15] for more details.

Definition 11. *A* Fuchsian group *is a discrete subgroup* Γ *of* $\mathrm{PSL}_2(\mathbb{R})$. *If* $C_\Gamma = \Gamma\backslash\mathbf{H}$ *has finite volume with respect to the metric induced from* $\mathbf{H}$, *then* Γ *is called a* lattice, *or a Fuchsian group of* cofinite volume. *If* C_Γ *is compact, then* Γ *is called* cocompact.

If Γ is a cocompact and torsion-free Fuchsian group, the C_Γ is a smooth projective curve of genus $g_\Gamma \geq 2$. If Γ is not cocompact, then C_Γ is quasi-projective. Every finitely generated Fuchsian group has a torsion-free subgroup of finite index, so if Γ is a cocompact (resp. non-cocompact) lattice in $\mathrm{PSL}_2(\mathbb{R})$, then C_Γ is finitely covered by a smooth projective (resp. quasi-projective) curve.

Exercise 12. *Prove that every cocompact Fuchian group contains a torsion-free subgroup of finite index. (Hint: First use the fact that* C_Γ *is a smooth projective curve to prove that* Γ *has finitely many conjugacy classes of finite subgroups. Then lift* Γ *to* $\mathrm{SL}_2(\mathbb{R})$ *and consider the ring* R *generated by the coefficients of elements of this lift. Now consider the natural homomorphisms of* Γ *to* $\mathrm{PSL}_2(R/\mathfrak{p})$, *where* $\mathfrak{p}$ *is a maximal ideal of* R.*)*

We now describe how number theory, particularly quaternion algebras, determine a special class of Fuchsian groups called *arithmetic Fuchsian groups*. These will be fundamental objects of study for the remainder of the course.

2.2 Arithmetic Fuchsian groups and quaternion algebras

The most important Fuchsian groups are undoubtedly the arithmetic Fuchsian groups, which we now describe. The canonical example is the *modular group* $\mathrm{PSL}_2(\mathbb{Z})$. The quotient of the hyperbolic plane by the modular group is the famed modular curve, which is a noncompact finite volume hyperbolic orbifold[2]. Note that the modular group has elements of finite order, so the quotient does not inherit a manifold structure from $\mathbf{H}$. Our interest is in cocompact arithmetic Fuchsian groups, but we begin by explaining how the modular group fits the definition of an arithmetic lattice, as it will make the general definition less painful.

Let $k = \mathbb{Q}$, and consider the central simple k-quaternion algebra $A = \mathrm{M}_2(k)$. Let V_∞ be the archimedean places of k and V_f the nonarchimedean places (i.e., the rational primes). Then A is unramified at every place of k, i.e., $A \otimes_k k_v \cong \mathrm{M}_2(k_v)$ for every place v.

Set

$$A_{\mathbb{R}} = \prod_{v \in V_\infty} A \otimes_k k_v \cong \mathrm{M}_2(\mathbb{R}).$$

Let A^* be the invertible elements of A and A^1 be the elements of reduced norm 1. Then $A^*_{\mathbb{R}}/k^* \cong \mathrm{PGL}_2(\mathbb{R})$ and $A^1_{\mathbb{R}} \cong \mathrm{SL}_2(\mathbb{R})$.

[2] An orbifold is the quotient of $\mathbf{H}$ by a discrete group of isometries. Elements of finite order have fixed points, in which case the covering $\mathbf{H} \to C_\Gamma$ ramifies.

Consider the maximal order $\mathcal{O} = \mathrm{M}_2(\mathbb{Z})$ of A. Then $\mathrm{SL}_2(\mathbb{Z})$ is the group $\mathcal{O}^1$ of elements in $\mathcal{O}$ with reduced norm one. The modular group is the subgroup $\mathbb{P}\mathcal{O}^1$ of A^*/k^*.

Now, we consider a natural generalization of the above interpretation of $\mathrm{PSL}_2(\mathbb{Z})$. Let k be a number field and A a central simple k-quaternion algebra. As above, let V_∞ and V_f be the archimedean and nonarchimedean places of k, respectively. Then we have

$$A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})^{r_1} \oplus \mathbb{H}^{r_2} \oplus \mathrm{M}_2(\mathbb{C})^s,$$

where $r_1 + r_2$ is the number of real places of k and s the number of complex places. Let $\mathcal{O} \subset A$ be a maximal order.

Exercise 13. *Show that the group $\mathcal{O}^1$ of elements in $\mathcal{O}$ with reduced norm 1 is a discrete subgroup of*

$$A^1 \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{SL}_2(\mathbb{R})^{r_1} \oplus \left(\mathbb{H}^1\right)^{r_2} \oplus \mathrm{SL}_2(\mathbb{C})^s$$

and that the projection onto

$$\mathrm{SL}_2(\mathbb{R})^{j_1} \oplus \mathrm{SL}_2(\mathbb{C})^{j_2}$$

for any $j_1 \leq r_1$ and $j_2 \leq s$ is discrete if and only if $j_1 = r_1$ and $j_2 = s$.

Therefore, to produce arithmetic Fuchsian groups, we must assume that k is totally real and that A ramifies at exactly one real place of k, i.e., that

$$A \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R}) \oplus \mathbb{H}^{[k:\mathbb{Q}]-1}.$$

If $\mathcal{O}$ is a maximal order in A, let $\Gamma^1_{\mathcal{O}}$ be the image of $\mathcal{O}^1$ in $\mathrm{PSL}_2(\mathbb{R})$ under the natural projection.

Definition 14. *Let Γ_1 and Γ_2 be two subgroups of a group G. They are* commensurable *if $\Gamma_1 \cap \Gamma_2$ has finite index in both Γ_1 and Γ_2. They are* commensurable in the wide sense *if there exists $g \in G$ such that Γ_1 and $g\Gamma_2 g^{-1}$ are commensurable.*

Definition 15. *A lattice Γ in* $\mathrm{PSL}_2(\mathbb{R})$ *is an* arithmetic Fuchsian group *if there exists a totally real field k and a central simple k-quaternion algebra A such that*

- *A is unramified at exactly one archimedean place of k and*
- *there exists a maximal order $\mathcal{O}$ in A such that Γ is commensurable in the wide sense with the subgroup $\Gamma^1_{\mathcal{O}}$ of $\mathrm{PSL}_2(\mathbb{R})$ defined above.*

It is a nontrivial fact that $\Gamma^1_{\mathcal{O}}$ is indeed a lattice. Let Γ be an arithmetic Fuchsian group, k be the associated totally real field, and A the associated k-quaternion algebra. The space $C_\Gamma = \Gamma\backslash\mathbf{H}$ is noncompact if and only if $k = \mathbb{Q}$ and $A = \mathrm{M}_2(\mathbb{Q})$. That is, $\mathrm{PSL}_2(\mathbb{Z})$ determines the unique commensurability class of non-cocompact arithmetic Fuchsian groups. We refer to [15], [6], or [9] for details. We also refer to [9] for the following important result.

Theorem 16 (The Identification Theorem)**.** *Let $\Gamma < \mathrm{PSL}_2(\mathbb{R})$ be a lattice and consider the subgroup $\Gamma^{(2)}$ generated by the set of all squares in Γ. Then define*

$$k_0(\Gamma) = \mathbb{Q}\left(\{\mathrm{Tr}(\gamma) \ : \ \gamma \in \Gamma^{(2)}\}\right)$$

and the quaternion subalgebra $A_0(\Gamma)$ of $\mathrm{M}_2(\mathbb{R})$ generated by the natural lift of $\Gamma^{(2)}$ to $\mathrm{SL}_2(\mathbb{R})$. Then Γ is an arithmetic Fuchsian group if and only if $k_0(\Gamma)$ is totally real and $A_0(\Gamma)$, considered as a k_0-quaternion algebra, is unramified at exactly one place of k_0. Furthermore, two arithmetic Fuchsian groups Γ_1 and Γ_2 are commensurable if and only if $k_0(\Gamma_1) \cong k_0(\Gamma_2)$ and $A_0(\Gamma_1)$ and $A_0(\Gamma_2)$ are isomorphic as $k_0(\Gamma_j)$-quaternion algebras.

2.3 The unit disk and hermitian forms

We now study the unit disk model

$$\mathbf{D} = \{z \in \mathbb{C} \ : \ |z|^2 < 1\}$$

of the hyperbolic plane. The metric is the pullback metric from $\mathbf{H}$ under the Möbius transformation

$$f(z) = \frac{iz+1}{z+i},$$

which takes $\mathbf{H}$ to $\mathbf{D}$. Our goal in this section is to explain the dictionary between arithmetic Fuchsian groups coming from quaternion algebras over totally real fields and the natural description of arithmetic lattices acting on D using hermitian forms on CM fields.

Exercise 17. *Write the metric on $\mathbf{D}$ in terms of dz.*

Exercise 18. *Show that the isometry group of $\mathbf{D}$ is the projective unitary group*

$$\mathrm{PU}(1,1) = \{A \in \mathrm{PSL}_2(\mathbb{C}) \ : \ {}^t\overline{A}hA = h\},$$

where h is the hermitian form of signature $(1,1)$ on $\mathbb{C}^2$ with matrix

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

We now describe the arithmetic lattices in $\mathrm{PU}(1,1)$ and then prove that they are the arithmetic Fuchsian groups of §2.2 in disguise. We first need a definition.

Definition 19. *A* CM-pair *ℓ/k is a totally imaginary quadratic extension of a totally real number field.*

Note that if ℓ/k is a CM-pair, then there is a unique place of ℓ over each place of k, so saying 'place of k' and 'place of ℓ' really mean one in the same thing. We will abuse this relationship at will in what follows.

Let ℓ/k be a CM-pair and σ the nontrivial Galois involution fixing k. Then σ extends to complex conjugation at each place of ℓ. If V is a finite-dimensional

ℓ-vector space, then a hermtian form h on V is a bilinear map $V \times V \to \ell$ that satisfies the usual rules with complex conjugation replaced by the involution σ. It follows that for each archimedean place v of ℓ, h extends to a hermitian form on the complex vector space $V \otimes_\ell \ell_v$ in the usual sense.

Now, let V be a two-dimensional ℓ vector space. Let $\mathbf{G}$ be the subgroup of $\mathrm{GL}(V)$ preserving h. Choose a lattice $\mathcal{L} \subset V$, i.e., a $\mathcal{O}_\ell$-integral structure on V, where $\mathcal{O}_\ell$ is the ring of integers of ℓ. Then let $\Lambda = \Lambda_{\mathcal{L}}$ be the subgroup of $\mathbf{G}$ preserving $\mathcal{L}$.

For each archimedean place v of ℓ, let h^v be the associated hermitian form on $\mathbb{C}^2$. This defines an embedding of $\mathbf{G}$ into the real unitary group $\mathrm{U}(h^v)$.[3] It follows that Λ embeds as a discrete subgroup of

$$\mathbf{G}(\mathbb{R}) = \prod_v \mathrm{U}(h^v) \cong \mathrm{U}(1,1)^{r_1} \times \mathrm{U}(2)^{r_2}.$$

Our interest is in producing discrete subgroups of $\mathrm{U}(1,1)$, so we assume that $r_1 = 1$ and $r_2 = [k : \mathbb{Q}] - 1$. Therefore, h^v has signature $(1,1)$ at exactly one place v of ℓ and signature $(2,0)$ or $(0,2)$ at the other places. In other words, h is an indefinite hermitian form on ℓ_v for one and *exactly* one v.

Let h be as above and let Γ be the image of Λ in $\mathrm{PU}(1,1)$ under the natural projection map. It is again a nontrivial fact that Γ is a lattice acting on $\mathbf{D}$. Perhaps surprisingly, these determine exactly the same commensurability classes of groups defined in the previous section. We now describe in detail the dictionary between unitary groups of hermitian forms and arithmetic Fuchsian groups coming from quaternion algebras.

Exercise 20. *Let A be a quaternion algebra with center k and $\ell = k(\alpha)$ be a quadratic extension of k that embeds in A. Assume that $\mathrm{Tr}_{\ell/k}(\alpha) = 0$, so $\alpha^2 \in k$. Then, there exists an element $\beta \in A$ with the following properties.*

1. *$\{1, \alpha, \beta, \alpha\beta\}$ is a k-basis for A,*
2. *$\beta^2 \in k$,*
3. *$\alpha\beta = -\beta\alpha$,*
4. *the map $x \mapsto (\beta x \beta)/\beta^2$ restricts to the nontrivial Galois involution of the extesion ℓ/k.*

Now, assume that k is totally real and ℓ is totally imaginary. Prove that A ramifies at the embedding $\tau : k \to \mathbb{R}$ if and only if $\tau(\beta^2) < 0$.

We now describe how to use the previous exercise to give A the structure of a two-dimensional hermitian vector space over the quadratic subfield $\ell \subset A$. Let k be a totally real number field and $\ell = k(\alpha)$ a totally imaginary quadratic extension, and suppose that ℓ embeds in the central simple k-quaternion algebra

[3]Note that unitary groups are real Lie groups, not complex Lie groups; in essence this is because unitary groups are defined via complex conjugation, which is not a complex analytic function. Similarly, $\mathbf{G}$ should be considered an k-algebraic group rather than ℓ-algebraic.

A. Choose β as in the previous exercise. If Tr is the reduced trace from A to k, writing $z \in A$ as $x + y\beta$ for $x, y \in \ell$, set

$$h(x,y) = \frac{1}{2\alpha^2}\left(\alpha^2\left(x(y - \mathrm{Tr}(y))\right) + \beta\left(x(y - \mathrm{Tr}(y))\right)\beta\right).$$

Exercise 21. *Prove that h is a hermitian form on A, considered as a two-dimensional ℓ-vector space, and that h is indefinite at a place v of ℓ if and only if A is unramified at the unique place of k under v. In fact, show that (A, h) is isometric to ℓ^2 equipped with the hermitian form with matrix*

$$\begin{pmatrix} 1 & 0 \\ 0 & -\beta \end{pmatrix}.$$

The following completes our dictionary between arithmetic Fuchsian groups defined via quaternion algebras and arithmetic subgroups of $\mathrm{PU}(1,1)$ defined using hermitian forms.

Theorem 22. *Let k be a totally real number field and A a central simple k-quaternion algebra which is unramified at exactly one real place of k. Then there exists a quadratic subfield $\ell \subset A$ with the following properties.*

1. *The field ℓ is totally imaginary.*
2. *Let V denote A as a two-dimensional ℓ-vector space. Then the map $h(x,y)$ defined as above is a hermitian form on V with respect to the natural extension of the Galois involution of E/F.*
3. *The unitary group of h is isomorphic (as an algebraic group) to the group of invertible elements of A.*

Conversely, let ℓ/k be a CM-pair, and let h be a hermitian form on ℓ^2 which is indefinite at exactly one place of ℓ. Prove that there exists a central simple k-quaternion algebra A such that ℓ embeds in A and the hermitian form h comes from the above construction.

Exercise 23. *Prove the theorem.*

Exercise 24. *Is the dictionary between central simple k-quaternion algebras unramified at exactly one place of k and hermitian forms on ℓ^2 that are indefinite at exactly one place of ℓ, where ℓ/k is a CM-pair, a bijection? In other words, does each commensurability class of arithmetic Fuchsian groups defined via quaternion algebras determine a unique class defined via hermitian forms and vice versa? Relate you answer to the Identification Theorem.*

2.4 Positive Fuchsian curves on arithmetic surfaces

During the winter school we plan to give a crash-course on Nori's Weak Lefschetz Theorem [12]. We will sketch the alternate proof of Napier and Ramachandran [11].

The two hermitian symmetric domains W which we will consider are the product $\mathbf{H}^2 \times \mathbf{H}^2$ of two hyperbolic planes and the complex hyperbolic plane $\mathbf{H}^2_{\mathbb{C}}$, as described in the previous sections. Let Γ be a co-compact arithmetic lattice acting on W. In $X = \Gamma\backslash W$ we will consider *Fuchsian curves*. These are totally geodesic π_1-injective immersions of a projective curve $C = \Sigma\backslash\mathbf{H}^2$ realized as an arithmetic quotient of the hyperbolic plane in $\Gamma\backslash X$. We will give a complete classification of the Fuchsian curves on any such X. Our goal will then be to determine a finite collection of Fuchsian curves on X with the property that the union Y of these curves is a connected closed subset of X whose fundamental group $\pi_1(Y)$ maps to a subgroup of finite index in $\pi_1(X)$. A more subtle question is whether the same is true when we replace $\pi_1(Y)$ by the group generated by the fundamental groups of the irreducible components of Y.

2.5 Applications, questions, and problems

Effectivity. Show in an effective way how to generate $\pi_1(X)$ from a finite set of fundamental groups of irreducible Fuchsian curves.

Higher dimensional analogues. Prove similar results for other Shimura varieties. The results of Napier and Ramachandran hold for ample subvarieties of higher codimension, and it is natural to consider generating fundamental groups other Shimura varieties by smaller Shimura varieties. Of particular interest are arithmetic lattices in $\mathrm{SU}(n,1)$ for large n, where one can potentially prove strong cohomological vanishing theorems previously inaccessible using the Trace Formula. This also may have applications to disproving a (believed to be false) conjecture of Hartshorne on the intersection properties of ample subvarieties of smooth projective varieties.

Cohomology of arithmetic groups and modular cycles on Shimura varieties. The extent to which the cohomology of a Shimura variety is determined by the cohomology of its Shimura subvarieties is an important question with applications (especially in the middle dimension) to the Langlands program. Study the extent to which the cohomology of a Shimura variety is determined by its Shimura subvarieties using weak Lefschetz techniques and analysis of normal bundles to totally geodesic subvarieties.

The congruence subgroup problem. For lattices acting irreducibly and cocompactly on a product of hyperbolic planes, we are again in a situation where the congruence subgroup problem is open. Fuchsian curves are known to have a wealth of noncongruence subgroups, and one can quantify the congruence subgroup property in terms of the number of étale coverings of the surface S (see [8]). Can one use a positive Fuchsian divisor on a Shimura variety S to count the number of finite étale coverings of S of degree d for large d?

Albanese varieties of complex hyperbolic surfaces There has been some work [10] on the structure of Albanese varieties of complex hyperbolic sur-

faces coming from congruence subgroups. In particular, they have complex multiplication. Consider a noncongruence subgroup. Does the Albanese have complex multiplication, or can a non-CM factor of the Jacobian of a Fuchsian curve contribute?

Characteristic p analogues A simplified version of the methods of Napier and Ramachandran show that the étale fundamental group of S is generated by those of connected unions of Fuchsian curves. Use this to consider similar problems for Shimura varieties in positive characteristic. Where appropriate, consider the effect on the structure of étale cohomology.

References

[1] Algebraic Number Theory, J. W. S. Cassels and A. Frólich eds., Academic Press (1967).

[2] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley Classics Library, John Wiley and Sons (1994).

[3] F. Grunewald and D. Segal, *Decision problems concerning S-arithmetic groups*, J. Symbolic Logic **50** no. 3 (1985), 743–772.

[4] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag (1977).

[5] S. Helgason, *Differential Geometry, Lie Groups, and Symmetric Spaces*, Pure and Applied Mathematics **80**, Academic Press (1978).

[6] S. Katok, *Fuchsian Groups*, Chicago Lectures in Mathematics, University of Chicago Press (1992).

[7] H. W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** no. 2 (1992), 211–244.

[8] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics **212**, Birkhäuser (2003).

[9] C. Maclachlan and A. W. Reid, *The Arithmetic of Hyperbolic* 3*-Manifolds*, Graduate Texts in Mathematics **219**, Springer (2003).

[10] V. K. Murty and D. Ramakrishnan, *The albanese of unitary Shimura varieties*, in The Zeta Functions of Picard Modular Surfaces, Centre de Recherches Mathematiques (1992).

[11] T. Napier and M. Ramachandran, *The L^2 $\overline{\partial}$-method, weak Lefschetz theorems, and the topology of Kähler manifolds*, J. Amer. Math. Soc. **11** no. 2 (1998), 375–396.

[12] M. Nori, *Zariski's conjecture and related problems*, Ann. Sci. École Norm. Sup. **16** no. 2 (1983), 305–344.

[13] J.-P. Serre, *Le problème des groupes de congruence pour* SL_2, Ann. of Math. **92** (1970), 489–527.

[14] J.-P. Serre, *Trees*, Springer Monographs in Mathematics, Springer (2003).

[15] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematics Society of Japan **11**, Princeton University Press (1994).

[16] A. Weil, *Basic Number Theory*, Classics in Mathematics, Springer (1995).