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.

In the first half of the course, we will begin by describing the work on 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 easily accessible to graduate students of all backgrounds. We will assume familiarity with basic algebraic number theory, and some exposure to the theory of division algebras over local and global fields will be useful. A good way to prepare for this part of the course is to read Chapters I–V and VIII–XI in André Weil's *Basic Number Theory* [13] and Lenstra's survey [5].

1.1 Number fields and Lenstra's algorithm

The Dirichlet unit theorem says that the unit group $\mathcal{O}_k^*$ of the ring of integers O_k of a number field k is a finitely generated abelian group. The explicit computation of generators for $\mathcal{O}_k^*$ is a basic problem in computational number theory. This problem arises in many contexts, e.g. in class field theory.

Dirichlet's theorem specifies exactly how many generators one needs for $\mathcal{O}_k^*$. One measure of the difficulty of finding a set of generators is simply the number of bits of data necessary to specify each element of the set. This leads to the notion of the height of elements of k. One cannot expect to generate O_k^* by elements whose height is bounded by a constant times a fixed power of the absolute value $|\Delta_k|$ of the discriminant of k. A surprising discovery of H. W. Lenstra was that one can find such "small" generators for the unit group $\mathcal{O}_{k,S}^*$ of the S-integers $\mathcal{O}_{k,S}$ of k for some moderately large set of places S. To describe this result we need some additional notation.

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. Our notion of complexity of a generator comes from the height of an algebraic number. The height of $x \in k^*$ 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.

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 $|\epsilon_k|_v \le 1$ 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 [5] is somewhat surprising:

Theorem 1. (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.

1.2 Algebraic groups and division algebras

The first goal of this course will be to generalize the above results to the noncommutative 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.

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. In particular, we exploit an embedding of our algebra into matrices over a finite extension ℓ of k and use the extension of the usual height H_ℓ to $n \times n$ matrices over ℓ. This has the added feature of being very concrete when one wants to actually compute a generating set for the S-units.

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 [2] 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.

1.3 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 [5].

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 [11]). 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 [10]. 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 [1] or of Hartshorne [3] would be helpful. It would also be very useful preparation to read Chapters 1 and 9 of [12] and relevant parts of [4] to understand the arithmetic theory of Fuchsian groups, since the groups we will consider are the natural generalization to one dimension higher.

2.1 Positive Fuchsian curves on arithmetic surfaces

We will begin with a crash-course on Nori's Weak Lefschetz Theorem [9]. We will sketch the alternate proof of Napier and Ramachandran [8].

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 $\mathbf{H}^2_{\mathbb{C}}$. We will describe the constructions of these spaces and describe the cocompact arithmetic lattices acting on them. This will require quaternion algebras over number fields and some basic hermitian linear algebra over number fields.

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.

2.2 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 [6]). 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 [7] on the structure of Albanese varieties of complex hyperbolic surfaces 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] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley Classics Library, John Wiley and Sons (1994).

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

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

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

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

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

[7] 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).

[8] 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.

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

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

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

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

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