LECTURES ON SHIMURA CURVES 3: MORE FUCHSIAN GROUPS

PETE L. CLARK

1. Automorphisms of uniformized algebraic curves

Just as the complex uniformization of elliptic curves was a powerful tool in understanding their structure, the same holds for algebraic curves of higher genus uniformized by Fuchsian groups.

Let Γ be a Fuchsian group of the first kind, and let

$$N(\Gamma) = \{m \in PSL_2(\mathbb{R}) \mid m^{-1}\Gamma m = \Gamma\}$$

be its normalizer in $PSL_2(\mathbb{R})$.

Proposition 1. *$N(\Gamma)$ is itself a Fuchsian group, and Γ has finite index in $N(\Gamma)$.*

Proof: Since Γ is necessarily nonabelian, that $N(\Gamma)$ is Fuchsian was shown in the last set of notes. Moreover, we have $\mu(\Gamma\backslash\mathcal{H}) = \mu(N(\Gamma)\backslash\mathcal{H}) \cdot [N(\Gamma) : \Gamma]$. Since the left hand side is finite and the volume of every fundamental region is positive, we conclude that the index must be finite.

Proposition 2. *Let $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ be the affine algebraic curve associated to Γ. We have a canonical injection $\iota : N(\Gamma)/\Gamma \hookrightarrow \mathrm{Aut}(Y(\Gamma))$. If Γ is of hyperbolic type, ι is an isomorphism.*

Proof: Writing $Y(\Gamma) = \Gamma\backslash\mathcal{H}$, it is natural to ask (as we did in the "parabolic" case $\mathbb{C}/\Lambda$) which elements $\sigma \in PSL_2(\mathbb{R}) = \mathrm{Aut}(\mathcal{H})$ descend to give automorphisms of $Y(\Gamma)$. The condition we need is clearly that for all $z \in \mathcal{H}$ and $\gamma \in \Gamma$, there exists $\gamma' \in \Gamma$ such that

$$\sigma(\gamma z) = \gamma'(\sigma z).$$

Of course this holds for all $z \iff \sigma\gamma = \gamma'\sigma$; in other words the condition is that $\sigma\Gamma\sigma^{-1} = \Gamma$, i.e., that $\sigma \in N(\Gamma)$. This defines a natural action of $N(\Gamma)$ on $Y(\Gamma)$ by automorphisms, and it is easy to see that its kernel is Γ itself.

Now, if Γ is of hyperbolic type, then $\mathcal{H} \to \Gamma\backslash\mathcal{H}$ is the universal covering map, and by covering space theory, all automorphisms of $Y(\Gamma)$ lift to the universal cover.

Exercise 3.X: Suppose that Γ is a Fuchsian group (of the first kind) without elliptic points, but with cusps. Does the conclusion of the previous proposition hold? Discuss. (Hint: the proof *does* go through, but is of less use. Why?)

Corollary 3. *The automorphism group of a complex algebraic curve of genus at least 2 is finite.*

Proof: By the uniformization theorem, all such curves are of the form $\Gamma\backslash\mathcal{H}$, where Γ is a group of hyperbolic type.

In fact we can do much better.

Theorem 4. *(Hurwitz) The automorphism group of a complex algebraic curve of genus $g \geq 2$ is at most $84(g-1)$.*

Proof: Write $X = \Gamma\backslash\mathcal{H}$ for a Fuchsian group Γ of hyperbolic type. By Equation XX we have $\mathrm{vol}(\Gamma) = 4\pi(g-1)$. Then

$$\#\operatorname{Aut}(X) = [N(\Gamma) : \Gamma] = \frac{\mathrm{vol}(\Gamma)}{\mathrm{vol}(N(\Gamma))} \leq \frac{4\pi(g-1)}{\pi/21},$$

where the last inequality is by Exercise XX. The result follows.

Remark: By an application of the "Lefschetz principle" one gets the same result for a curve defined over any field of characteristic zero. It is possible to prove purely algebraically that a curve of genus ≥ 2 over any field has a finite automorphism group. (In fact one can show this for all varieties of general type, i.e., for which some positive multiple of the canonical bundle gives a birational embedding; for algebraic curves, this is equivalent to $g \geq 2$.) However, the bound of $84(g-1)$ *does not hold* in characteristic p (at least, not for all p). This is another example of the apparent indispensability of analytic methods in algebraic geometry.

Remark: Assuming the finiteness of the automorphism group, it is possible to prove the bound $84(g-1)$ using the Riemann-Hurwitz formula.[1]

Problem: Fix any genus $g \geq 2$. Then, there exists a number $P = P(g)$ such that if k is an algebraically closed field of characteristic zero or of characteristic greater than $P(g)$, then for any smooth projective curve C/k, $\operatorname{Aut}(C) \leq 84(g-1)$. Can this be proved by model-theoretic means?

Reading Project: What new possibilities arise for $\operatorname{Aut}(C)$ when C is a genus g algebraic curve defined over a field of characteristic p, when $g \gg p$? Note that every curve in positive characteristic is the "good reduction" of some algebraic curve of characteristic 0 (this follows, e.g., from the smoothness of the moduli space of curves of genus g). How much of the automorphism group can be lifted?

2. Some modular curves

It would be perverse if we did not illustrate the preceding theory by discussing certain classical modular curves, i.e., Riemann surfaces of the form $\Gamma\backslash\mathcal{H}$, where $\Gamma \subset PSL_2(\mathbb{Z})$ is a congruence subgroup. In one's daily (mathematical) life, it is very convenient to have formulas for the genera, number of elliptic cycles, and number of cusps for $X_0(N)$, $X_1(N)$, $X(N)$. Such formulas have of course long since been worked out, and the complete story is rather complicated (especially if N is divisible by 4 or 9). Here we will work out some representative special cases:

First, the signature of $X(1)$ is $(2, 3; 1)$, meaning that there exists a unique conjugacy class of elliptic points of order 2, (given by the matrix S of the previous

[1] In fact, if I am not mistaken, this formula appears for the first time in the same paper in which Hurwitz proves the $84(g-1)$ bound.

notes), and a unique conjuacy class of elliptic points of order 3 (given by the matrix T). This follows from our geometric discussion of fundamental regions. We invite the reader to find a more arithmetic proof.

Proposition 5. *Let $\Gamma' \subset \Gamma$ be a subgroup of a Fuchsian group of finite index n. Let C_N a conjugacy class of order N elements of Γ, with representative elliptic point z.*
a) There are at most n Γ'-inequivalent elliptic points in the Γ equivalence class of z.
b) If Γ' is normal *in Γ, there is at most one.*

Exercise 3.X: Prove it.

As an application of this result, we will determine the elliptic points of $X(N) = \Gamma(N)\backslash\mathcal{H}$. In fact there are none, because neither S nor T is congruent to the identity matrix modulo any $N \geq 2$.

Note also that the ramification index over every preimage of the elliptic point $\sqrt{-1}$ is 2 (since 2 is the ramification degree of the entire uniformization map, and it is "used up" since the preimages of the elliptic points are not elliptic); similarly the ramification index at each preimage of $\sqrt{-3}$ is 3. (Note that because the covering is Galois, the ramification index does not depend upon the choice of preimage.)

As for the cusps, clearly there must be at least one Γ'-equivalence class of cusps lying above each cusp of Γ. For $PSL_2(\mathbb{Z})$ there is of course one cusp. What we are seeking then, is the number of $\Gamma(N)$ orbits on $\mathbb{P}^1(\mathbb{Q})$.

Lemma 6. *Let $a,\ b,\ c,\ d$ be integers such that $(a, b) = (c, d) = 1$, and $[a\ b]^t \equiv [c\ d]^t \pmod N$. Then there exists $\sigma \in \Gamma(N)$ such that $\sigma[a\ b]^t = [c\ d]^t$.*

Proof: ...

Lemma 7. *Let $s = \frac{a}{b}$ and $s' = \frac{c}{d}$ be cusps of $\Gamma(N)$, written in lowest terms as above. Then s and s' are equivalent under $\Gamma(N)$ iff $[a\ b]^t = \pm[c\ d]^t$.*

Proof: ...

Example: When $N = p$ is an odd prime, there are $\frac{p^2-1}{2}$ inequivalent cusps, so the ramification index at ∞ is p. Note that this shows that $PSL_2(\mathbb{F}_p)$ is generated by elements $x,\ y,\ z$ satisfying $x^2 = y^3 = z^p = xyz = 1$. We can compute the genus of $X(p)$ using the Riemann-Hurwitz formula:

$$2g(X(p))-2 = \frac{(p^2-1)(p^2-p)}{2(p-1)}(2g(X(1))-2)+\frac{(p^2-1)(p^2-p)}{2(p-1)}\cdot\left(\frac{1}{2}+\frac{2}{3}+\frac{p-1}{p}\right),$$

or

$$g(X(p)) = 1 + \frac{(p^2-1)(p-6)}{24}.$$

For example, one gets that $X(7)$ has genus 3 and admits $PSL_2(\mathbb{F}_7)$ as a group of automorphisms. Since this group has order $168 = 84(3-1)$, by Hurwitz's bound it must be the full automorphism group of $X(7)$. (Using the theory of triangle groups, it can be shown that whenever $p \geq 7$, $\mathrm{Aut}(X(p)) = PSL_2(\mathbb{F}_p)$.) This shows also that $N(\Gamma(7)) = \Gamma(1)$ (since it could not be any larger).

Exercise 3.X:[2] Let $\Gamma \subset PSL_2(\mathbb{Z})$ be a subgroup of index M, and let e_2 (resp. e_3) denote the number of elliptic cycles of order 2 (resp. 3) for Γ. Let e_∞ denote the number of cusps of Γ. Let $X(\Gamma)$ be the compactification of $\Gamma\backslash\mathcal{H}$ (i.e., with cusps added). Show that

$$g(X(\Gamma)) = 1 + \frac{M}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{e_\infty}{2}.$$

Next we want to carry out a similar analysis of $X_0(N)$ for *squarefree* N[3]

Exercise 3.X: a) Suppose $N = p$. Show that $\Gamma_0(p)$ has two orbits on $\mathbb{P}^1(\mathbb{Q})$, with representatives given by 0 and ∞. (Hint: think p-adically.)
b) Show that, if $N = p_1 \cdots p_r$ is a product of distinct primes, $\Gamma_0(N)$ has 2^r inequivalent cusps.

Proposition 8. *For $\Gamma = \Gamma_0(N)$ with squarefree N, we have*

$$e_2(N) = \prod_{p \mid N} (1 + (\frac{-4}{p})),$$

$$e_3(N) = \prod_{p \mid N} (1 + (\frac{-3}{p})).$$

Proof: ....

Exercise 3.X: Give a more "natural" proof based upon the moduli interpretation of $X_0(N)$ (and in particular on cyclic subgroups of elliptic curves with $j = 0$ or 1728).

Thus for squarefree $N = p_1 \cdots p_r$ we have

$$g(X_0(N)) = 1 + \frac{\prod_{i=1}^r (p_i + 1)}{12} - \frac{\prod_{p \mid N} (1 + (\frac{-4}{p}))}{4} - \frac{\prod_{p \mid N} (1 + (\frac{-3}{p}))}{3} - 2^{r-1}.$$

In other words, the genus is roughly $\frac{N}{12}$.

Let us now turn to the question of the automorphism group of $X_0(N)$; for simplicity, we will consider the case $N = p$ is prime.[4] In this case, we can explicitly write down a nontrivial element of $N(\Gamma_0(p)/\Gamma_0(p)$; namely, the matrix $w_p = \frac{1}{\sqrt{p}} \begin{bmatrix} 0 & -1 \\ p & 0 \end{bmatrix}$.
Let us check it:

$$\frac{1}{p} \begin{bmatrix} 0 & 1 \\ -p & 0 \end{bmatrix} \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ p & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -pb & a \end{bmatrix}.$$

The induced automorphism on $X_0(p)$ clearly has order 2, and indeed, $w_p^2 = p \cdot I_2$.

Exercise 3.X: Show that w_p has the following modular interpretation: given a pair E_1 and a degree p subgroup H, $w_p(E_1, H) = (E_1/H, H')$, where H' is the image in E_1/H of any other cyclic order p subgroup. Another way of saying this is: $X_0(p)$

[2]Prop. 1.40 in Shimura'a book.

[3]This restriction is just for simplicity, although later in the course we will see that the behavior of $X_0(N)$ as an *arithmetic surface* is much nicer in the case of squarefree level.

[4]In general, passing from the case of prime level to squarefree level will not result in qualitative change. The adelic perspective makes this claim especially clear.

parameterizes order p isogenies $\varphi : E_1 \to E_2$. Then $w_p(\varphi) = \varphi^\vee : E_2 \to E_1$, the dual isogeny.

Exercise 3.X: Use the modular interpretation of w_p to show: for $p > 3$, the w_p fixed points are in bijection with elliptic curves with CM by the maximal order of $\mathbb{Q}(\sqrt{-p})$ together with – when $-p \equiv 1 \pmod 4$ – the curves with $\mathbb{Z}[\sqrt{-p}]$-CM (i.e., the order of conductor 2).

Now a natural first reaction to this exciting development would be to look for further elements of $N(\Gamma_0(p)/\Gamma_0(p)$. In fact it can be shown[5] that there are none: this group has order 2. (More generally, if N is squarefree with r prime factors, then $N(\Gamma_0(N))/\Gamma_0(N) \cong (\mathbb{Z}/2\mathbb{Z})^r$. Can you find r independent involutions via a modular intepretation as above?) Later in the course we will pursue the quaternionic analogue of this in more detail (and using adelic methods). Let us write (as is traditional) $\Gamma_0^*(p)$ for $\langle \Gamma_0(p),\ w_p \rangle$.

Now the question is: is $\Gamma_0^*(p)/\Gamma_0(p) = \mathbb{Z}/2\mathbb{Z}$ equal to the full automorphism group of $X_0(p)$? The answer is clearly negative when the genus is zero – i.e., when $p \in \{2,\ 3,\ 7,\ 13\}$ – or one – when $p \in \{11,\ 17,\ 19\}$ – because the full automorphism groups of these Riemann surfaces are infinite. On the other hand, when the genus is at least two, perhaps this is the case. For small values of p, it is possible to write down explicit equations for $X_0(p)$ and thus to explicitly compute the automorphism group. For instance, one can check in this way that the genus 2 curve $X_0(23)$ has automorphism group of order 2.

However, consider now the case of $X_0(37)$, again of genus 2. Being a genus 2 curve, $X_0(37)$ must be hyperelliptic, meaning there exists an involution ι on $X_0(37)$ whose quotient is $\mathbb{P}^1$ (or equivalently, a degree 2 map $X_0(37) \to \mathbb{P}^1$). By the Riemann-Hurwitz formula, the number of branch points – which are precisely the ι-fixed points – must be 6. However, by Exercise 3.X, the number of fixed points of w_{37} is equal to the class number of $\mathbb{Q}(\sqrt{-37})$, or XX. We conclude that $w_{37} \neq \iota$. In fact the automorphism group here is $(\mathbb{Z}/2\mathbb{Z})^\times$.

What is amazing is that for any $p \neq 37$ such that $X_0(p)$ has genus at least 2, the automorphism group of $X_0(p)$ is generated by the Atkin-Lehner involution. This is a theorem of Ogg.

Before leaving this cast of characters, let us make a further remark. The group $\Gamma_0^*(p)$ is not contained in $PSL_2(\mathbb{Z})$ (in some sense it is our first explicit, nontrivial example of such a Fuchsian group), it is merely **commensurable** with it:

Definition: Two subgroup $H_1,\ H_2$ of a group G are commensurable if for $i = 1,\ 2$, $[H_i : H_1 \cap H_2] < \infty$.

Unlikely though it may sound, one defines the **commensurator** $\mathrm{Comm}(\Gamma)$ of a Fuchsian group Γ as the set of all $\sigma \in PSL_2(\mathbb{R})$ such that $\sigma^{-1}\Gamma\sigma$ is commensurable with Γ. In particular, the commensurator contains the normalizer, but note that w_p

[5] I think this result is due to Lehner and Newman.

does *not* normalize all of $PSL_2(\mathbb{Z})$. It is easy to see that the group $\langle PSL_2(\mathbb{Z}), w_p \rangle$ generated by $PSL_2(\mathbb{Z})$ and all the w_p's is an infinite extension of $PSL_2(\mathbb{Z})$. This infinitude is the key to a good theory of Hecke operators (which we shall, alas, not discuss) and in fact a characteristic property of the **arithmeticity** of $PSL_2(\mathbb{Z})$.

3. Triangle groups

Let $m_1,\ m_2,\ m_3$ be three positive integers such that $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$. As we mentioned earlier, there exists a hyperbolic triangle, unique up to isometry, with angles $\frac{\pi}{m_i}$ for $1 \leq i \leq 3$. Such a triangle, say $T = T(m_1, m_2, m_3)$ is easily seen to be a fundamental domain for the group generated by reflections R_i through the three sides of T. The R_i's are orientation-*reversing* isometries of $\mathcal{H}$ and are thus not conformal. But there exists an index 2 subgroup of conformal isometries, and no more than a moment's thought shows that it is generated by the three elements $r_i = R_j \circ R_k$ where we take (i, j, k) cycling around modulo 3. Note that r_i, being the composition of reflections through lines meeting at an angle of π/m_i, is a rotation through the ith vertex by an angle of $2pi/m_i$. Let

$$\Delta = \Delta(m_1, m_2, m_3) = \langle r_1,\ r_2,\ r_3 \rangle.$$

A fundamental domain for Δ is obtained by reflecting T through any one of its sides. In particular, Δ acts without limit points on $\mathcal{H}$ so is a Fuchsian group. The Riemann surface $\Delta\backslash\mathcal{H}$ is obtained by pairing two sets of adjacent sides on a quadrilateral lying entirely in $\mathcal{H}$, so that the quotient surface has no hyperbolic side-pairing elements and genus zero, so has signature $(0; m_1, m_2, m_3; 0)$. Conversely, it is not too hard to see that Δ is, up to conjugacy, the unique Fuchsian group with this signature.

List maximal triangle groups...