BELYI MAPS AND DESSINS D'ENFANTS
LECTURE 15

SAM SCHIAVONE

CONTENTS

I. REVIEW

Last time we:

(1) Given a Fuchsian group Γ and a fundamental domain D for Γ, showed how we can obtain a fundamental domain for any subgroup as a union of translates of D.
(2) Applied this in the particular case of $\Gamma = \Gamma(1) = \mathrm{PSL}_2(\mathbb{Z})$ and the subgroup $\Gamma(2)$.
(3) Specialized some results on covering spaces and monodromy to the particular case of the covering $\mathfrak{H} \to \Gamma\backslash\mathfrak{H}$ where Γ is a Fuchsian group.
(4) In particular, used Riemann-Hurwitz to give a formula for the genus of $\Gamma(N)\backslash\mathfrak{H}$.

II. EQUIVALENCE OF RIEMANN SURFACES AND ALGEBRAIC CURVES

Early on in the course, we saw that smooth projective plane curves were examples of compact Riemann surfaces. For a smooth projective plane curve C given by equation $F(X, Y, Z) = 0$ for some homogeneous polynomial F, we defined an atlas of compatible holomorphic charts which give C the structure of a Riemann surface.

In fact, much more is true. There is an equivalence of categories

$$\left\{ \begin{matrix} \text{compact, connected} \\ \text{Riemann surfaces} \end{matrix} \right\} \overset{\sim}{\longleftrightarrow} \left\{ \begin{matrix} \text{smooth, projective} \\ \text{algebraic curves over } \mathbb{C} \end{matrix} \right\} .$$

This is an instance of a more general family of results known as *GAGA*—Géométrie algébrique et géométrie analytique. These results, due mainly to Serre, show that there is an analytification functor that, given a scheme X of finite type over $\mathbb{C}$, produces a complex analytic space X^{an}, and that this defines an equivalence of categories.

Remark 1. Not all algebraic curves are plane curves! There are some curves that can't be smoothly embedded into $\mathbb{P}^2$. One is easy way to see this is using the degree-genus formula: a smooth projective plane curve given by a homogeneous degree d polynomial

Date: May 20, 2021.

$F(X,Y,Z) = 0$ has genus $\binom{d-1}{2}$. So the genus of any smooth projective plane curve is a triangular number: $0, 1, 3, 6, 10, \ldots$.

For an explicit example, write X, Y, Z, W be the homogeneous coordinates of $\mathbb{P}^3$, and consider the curve C given by the equations

$$X^2 + Y^2 + Z^2 - ZW + W^2 = 0$$
$$X^3 + 2XYZ + YZW = 0\,.$$

One can show that C is a smooth projective curve of genus 4, so it can't be embedded in $\mathbb{P}^2$ by the observation above.

The main take away is that we can pass freely between the category of smooth algebraic curves and the category of Riemann surfaces, phrasing our results in whichever terminology is more suitable.

[Mention example of elliptic curves and tori, p. 101 of GGD]

III. Belyi's Theorem

Belyi's Theorem tells us which complex algebraic curves can actually be defined over $\overline{\mathbb{Q}}$.

Definition 2. Let X be a projective curve over $\mathbb{C}$. Then X is defined over a field $K \subseteq \mathbb{C}$ if there exists a collection of polynomials with coefficients in K whose vanishing locus is isomorphic to X.

This is a bit more subtle than it may seem. Even if X is defined by polynomials whose coefficients are not in K, we may be able to find a different set of polynomials whose coefficients *are* in K that define an isomorphic curve. For instance, the curve

$$E_1 : y^2 = x^3 - \pi^3$$

is defined over $\mathbb{Q}(\pi)$, and from this equation, it doesn't look like it's defined over $\mathbb{Q}$. However, E_1 is in fact isomorphic to $E_2 : y^2 = x^3 - 1$ via the isomorphism

$$\begin{aligned} E_1 &\to E_2 \\ (x,y) &\mapsto \left(\frac{x}{\pi}, \frac{y}{\pi\sqrt{\pi}}\right)\,. \end{aligned}$$

E_2 is evidently defined over $\mathbb{Q}$, so E_1 is, too.

Recall the definition of a Belyi map:

Definition 3. A Belyi map is a morphism $\varphi : X \to \mathbb{P}^1$ of (smooth, projective) algebraic curves that is unramified outside of $\{0, 1, \infty\}$.

Theorem 4 (Belyi's Theorem)**.** *Let X be a smooth, projective curve over $\mathbb{C}$. Then X is defined over $\overline{\mathbb{Q}}$ iff there exists a Belyi map $\varphi : X \to \mathbb{P}^1$.*

Remark 5.

- A curve X can be defined as the vanishing set of finitely many polynomials, each of which has only finitely many nonzero coefficients. So if X is defined over $\overline{\mathbb{Q}}$, we can find polynomials all of whose coefficients lie in $\overline{\mathbb{Q}}$. But since there are only finitely many of them, they must in fact lie inside some finite extension K of $\mathbb{Q}$.
- In Belyi's (and the textbook's) statement, they only assume that φ is ramified over at most 3 points, rather than explicitly using $0, 1, \infty$. However, these two conditions are actually equivalent since $\operatorname{Aut}(\mathbb{P}^1) \cong \mathrm{PSL}_2(\mathbb{C})$ acts triply transitively on $\mathbb{P}^1$. That is, given any 3 distinct points $w_1, w_2, w_3 \in \mathbb{P}^1$, there exists an automorphism $\psi : \mathbb{P}^1 \to \mathbb{P}^1$ mapping w_1, w_2, w_3 to $0, 1, \infty$. If none of w_1, w_2, w_3 is ∞, then we can simply take
$$\psi(z) = \frac{(w_2 - w_3)(z - w_1)}{(w_2 - w_1)(z - w_3)},$$
and there is a similar formula if one of the points is ∞.

Thus, given any map $\varphi : X \to \mathbb{P}^1$ ramified only above 3 points w_1, w_2, w_3, we can post-compose with ψ to obtain the map $\psi \circ \varphi$ that is ramified only above $0, 1, \infty$.

The reverse direction was known before Belyi's paper, but requires some more theory about the Galois action. We will prove the forward implication, which is the direction due to Belyi. Assume that X is defined over $\overline{\mathbb{Q}}$ and choose defining equations for X with coefficients in $\overline{\mathbb{Q}}$. The outline of the proof is the following.

(1) Choose any morphism $f : X \to \mathbb{P}^1$. Then f will be ramified over some finite set of points B defined over $\overline{\mathbb{Q}}$.
(2) Use the minimal polynomials of the elements of B to construct a polynomial h such that $h \circ f$ is ramified only over points defined over $\mathbb{Q}$.
(3) By the previous step, we may assume that $B \subseteq \mathbb{Q} \cup \{\infty\}$. We find a polynomial that "squishes" two of the ramification values together without introducing any further ramification. More precisely, if
$$B = \{0, 1, \infty, \lambda_1, \ldots, \lambda_k\},$$
we find a polynomial $g_{\lambda_1} \in \mathbb{Q}[x]$ such that $g_{\lambda_1} \circ f$ has strictly fewer ramification values, namely
$$\{0, 1, \infty, g_{\lambda_1}(\lambda_2), \ldots, g_{\lambda_1}(\lambda_k)\}.$$
We then apply the same process for $\lambda_2, \ldots, \lambda_k$ until the resulting map is ramified only above $\{0, 1, \infty\}$.

Before we dive into the proof, let's consider an example illustrating step (3). Let
$$E : y^2 = x(x-1)(x-\lambda)$$
where $\lambda \in \mathbb{Q}$ and $0 < \lambda < 1$. Then we can write $\lambda = \dfrac{m}{m+n}$ for some $m, n \in \mathbb{Z}_{\geq 1}$. Now E is certainly defined over $\overline{\mathbb{Q}}$ (over $\mathbb{Q}$, even), so by Belyi's Theorem, we should be able to find a Belyi map $\varphi : E \to \mathbb{P}^1$. Take as our starting morphism in step (1) the function x, i.e., $(x, y) \mapsto x$. Note that x is ramified exactly over the values $0, 1, \lambda, \infty$. We now want to

“squish” these values together as in step (3). Define the polynomial

$$g_\lambda(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n \,.$$

Lemma 6. *Considered as a morphism $\mathbb{P}^1 \to \mathbb{P}^1$, g_λ satisfies the following properties.*

(1) g_λ is ramified only at the points $0, 1, \infty, \lambda$.
(2) $g_\lambda(0) = 0$, $g_\lambda(1) = 0$, $g_\lambda(\infty) = \infty$, and $g_\lambda(\lambda) = 1$.

Proof. The first 3 equalities of (2) are clear. Note that

$$1 - \lambda = 1 - \left(\frac{m}{m+n}\right) = \frac{m+n}{m+n} - \frac{m}{m+n} = \frac{n}{m+n}$$

so

$$g_\lambda(\lambda) = g_\lambda\left(\frac{m}{m+n}\right) = \frac{(m+n)^{m+n}}{m^m n^n} \left(\frac{m}{m+n}\right)^m \left(\frac{n}{m+n}\right)^n = 1\,.$$

Observe that

$$\begin{aligned} \frac{d}{dx} x^m (1-x)^n &= m x^{m-1} (1-x)^n - x^m \cdot n (1-x)^{n-1} \\ &= x^{m-1} (1-x)^{n-1} (m - (m+n)x)\,. \end{aligned}$$

So g_λ ramifies exactly at ∞ and the points x where $g_\lambda'(x) = 0$, which are the zeroes of the polynomial above, namely $0, 1$, and $\dfrac{m}{m+n} = \lambda$. □

Thus by post-composing with g_λ, we obtain the morphism

$$\varphi : E \xrightarrow{x} \mathbb{P}^1 \xrightarrow{g_\lambda} \mathbb{P}^1$$

which is ramified exactly at the points $(0,0), (1,0), (\lambda, 0), \infty \in E$, which map to $0, 0, 1, \infty \in \mathbb{P}^1$, respectively. Thus φ is only ramified above $0, 1, \infty$, so it is a Belyi map.

For step (2) in the outline above, we will need the following lemma.

Lemma 7. *Let $f : X \to Y$ and $g : Y \to Z$ be nonconstant morphisms of Riemann surfaces. Then*

$$\operatorname{Branch}(g \circ f) = \operatorname{Branch}(g) \cup g(\operatorname{Branch}(f))\,,$$

where Branch(f) *is the set of branch values of f.*

Proof. This basically follows from the chain rule. Suppose $P \in X$ and U is a chart containing P with local coordinate z. Let $z_0 = z(P)$ and let $\widehat{f}$ and $\widehat{g}$ be the local representations of f and g near P and $f(P)$, respectively. Then P is a ramification point of $g \circ f$ iff

$$0 = (\widehat{g} \circ \widehat{f})'(z_0) = \widehat{g}'(\widehat{f}(z_0))\widehat{f}'(z_0)\,.$$

If $\widehat{f}'(z_0) = 0$, then P is a ramification point of f, so $f(P) \in \operatorname{Branch}(f)$ and hence $g(f(P)) \in g(\operatorname{Branch}(f))$. If $\widehat{g}'(\widehat{f}(z_0))$, then $f(P)$ is a ramification point of g, so $g(f(P)) \in \operatorname{Branch}(g)$. □

Proof. Assume that X is defined over $\overline{\mathbb{Q}}$ and choose defining equations for X with coefficients in $\overline{\mathbb{Q}}$. Choose any morphism $f : X \to \mathbb{P}^1$. Then f is ramified over some finite set of values

$$B_0 = \{b_0, \dots, b_s\}$$

in $\overline{\mathbb{Q}} \cup \{\infty\}$. If $B_0 \subseteq \mathbb{Q} \cup \{\infty\}$, we are done; otherwise, let $m_1(T) \in \mathbb{Q}[T]$ be the minimal polynomial of $b_0, \dots, b_s$ (excluding ∞), i.e., m_1 is the monic polynomial of minimal degree such that $m_1(b_j) = 0$ for each j. By Lemma (7), the set of ramification values of $m_1 \circ f$ is

$$\begin{aligned} B_1 &:= \operatorname{Branch}(m_1 \circ f) = \operatorname{Branch}(m_1) \cup m_1(\operatorname{Branch}(f)) \\ &= \{m_1(\zeta) \in \mathbb{C} : m_1'(\zeta) = 0\} \cup \{0, \infty\}\,. \end{aligned}$$

If $B_1 \subseteq \mathbb{Q} \cup \{\infty\}$ we are done; otherwise, let m_2 be the minimal polynomial of

$$\operatorname{Branch}(m_1) = \{m_1(\zeta) \in \mathbb{C} : m_1'(\zeta) = 0\}\,.$$

Then

$$\deg(m_2) \leq \deg(m_1') \leq \deg(m_1) - 1\,.$$

Again by Lemma (7), the set of ramification values of $m_2 \circ m_1 \circ f$ is

$$\begin{aligned} B_2 &:= \operatorname{Branch}(m_2 \circ m_1 \circ f) = \operatorname{Branch}(m_2) \cup m_2(\operatorname{Branch}(m_1 \circ f)) \\ &= \{m_2(\zeta) \in \mathbb{C} : m_2'(\zeta) = 0\} \cup m_2(B_1)\,. \end{aligned}$$

Note that $m_2(B_1) \subseteq \mathbb{Q} \cup \{\infty\}$ by construction; indeed $m_2(B_1) = \{0, \infty, m_2(0)\}$. If $B_2 \subseteq \mathbb{Q} \cup \{\infty\}$ we are done; otherwise, let m_3 be the minimal polynomial of

$$\operatorname{Branch}(m_2) = \{m_2(\zeta) \in \mathbb{C} : m_2'(\zeta) = 0\}\,.$$

As before, we have

$$\deg(m_3) \leq \deg(m_2') \leq \deg(m_2) - 1\,.$$

Proceeding inductively, we construct a sequence of polynomials $m_1, m_2, m_3, \dots$ such that

$$\deg(m_1) > \deg(m_2) > \deg(m_3) > \cdots\,.$$

Thus after finitely many steps, we obtain a polynomial m_ℓ of degree 1, at which point we obtain

$$B_\ell = \operatorname{Branch}(m_\ell \circ \cdots \circ m_2 \circ m_1 \circ f) \subseteq \mathbb{Q} \cup \{\infty\}\,,$$

as desired.

Thus by the previous paragraph (step (2)), we may assume that $\operatorname{Branch}(f) \subseteq \mathbb{Q} \cup \{\infty\}$. We now proceed with step (3) as in the example. Applying a Möbius transformation, we may move three of the branch values of f to $0, 1, \infty$. Thus we may take

$$\operatorname{Branch}(f) = \{0, 1, \infty, \lambda_1, \cdots, \lambda_k\} \subseteq \mathbb{Q} \cup \{\infty\}\,.$$

Applying the Möbius transformations $x \mapsto 1 - x$ and $x \mapsto 1/x$, we may further assume that $0 < \lambda_1 < 1$. (Note that these two transformations preserve the set $\{0, 1, \infty\}$.) Postcomposing with g_{λ_1}, we obtain the morphism $g_{\lambda_1} \circ f$ with branch values

$$\operatorname{Branch}(g_{\lambda_1} \circ f) = \{0, 1, \infty, g_{\lambda_1}(\lambda_2), \dots, g_{\lambda_1}(\lambda_k)\} \subseteq \mathbb{Q} \cup \{\infty\}$$

which contains strictly fewer values than $\operatorname{Branch}(f)$. Proceeding inductively (next we would take $g_{g_{\lambda_1}(\lambda_2)} \circ g_{\lambda_1} \circ f$), we obtain a morphism $\varphi : X \to \mathbb{P}^1$ ramified only above $0, 1, \infty$. □

[Show Example 3.4, p. 173 of GGD. Then show Belyi's original proof in *On Galois extensions of a maximal cyclotomic field*.]