Chapter 1

Dessins d'Enfants

These are notes for BUNTES Spring 2018, the topic is Dessins d'Enfants, they were last updated April 15, 2018. For more details see the webpage. These notes are by Alex, feel free to email me at alex.j.best@gmail.com to report typos/suggest improvements, I'll be forever grateful.

1.1 Overview (Angus)

1.1.1 Belyi morphisms

Let X be an algebraic curve over $\mathbf{C}$ (i.e. a compact Riemann surface) when is X defined over $\overline{\mathbf{Q}}$?

Theorem 1.1.1 (Belyi)**.** *An algebraic curve $X/\mathbf{C}$ is defined over $\overline{\mathbf{Q}}$ $\iff$ there exists a morphism $\beta\colon X \to \mathbf{P}^1$ $\mathbf{C}$ ramified only over $\{0, 1, \infty\}$.*

Definition 1.1.2 (Ramified)**.** (AG) A morphism $f\colon X \to Y$ is **ramified** at $x \in X$ if on local rings the induced map $f^{\#}\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ descended to

$$\mathcal{O}_{Y,f(x)}/\mathfrak{m} \to \mathcal{O}_{X,x}/f^{\#}(\mathfrak{m})$$

is not a finite inseparable field extension.

(RS) A morphism $f\colon X \to Y$ is ramified at $x \in X$ if there are charts around x and $f(x)$ such that $f(x) = x^n$. This n is the **ramification index**.

Definition 1.1.3 (Belyi morphisms)**.** A **Belyi morphism** is one ramified only over $\{0, 1, \infty\}$

A **clean Belyi morphism** or **pure Belyi morphism** is a Belyi morphism where the ramification indices over 1 are all exactly 2.

Lemma 1.1.4. *A curve X admits a Belyi morphism iff it admits a clean Belyi morphism.*

Proof. If $\alpha\colon X \to \mathbf{P}^1$ $\mathbf{C}$ is Belyi, then $\beta = 4\alpha(1-\alpha)$ is a clean Belyi morphism. □

1.1.2 Dessin d'Enfants

Definition 1.1.5. A **dessin d'Enfant** (or Grothendieck Dessin or just **Dessin**) is a triple (X_0, X_1, X_2) where X_2 is a compact Riemann surface, X_1 is a graph, $X_0 \subset X_1$ is a finite set of points, where $X_2 \setminus X_1$ is a collection of open cells. $X_1 \setminus X_0$ is a disjoint union of line segments

Lemma 1.1.6. *The data of a dessin is equivalent to a graph with an ordering on the edges coming out of each vertex.*

Definition 1.1.7 (Clean dessins)**.** A **clean dessin** is a dessin with a colouring (white and black) on the vertices such that adjacent vertices do not share a colour.

1.1.3 The Grothendieck correspondence

Given a Belyi morphism $\beta\colon X \to \mathbf{P}^1\,\mathbf{C}$ the graph $\beta^{-1}([0,1])$ defines a dessin.

Theorem 1.1.8. *The map*

$$\{\textit{(Clean) Belyi morphisms}\} \to \{\textit{(clean) dessins}\}$$

$$\beta \mapsto \beta^{-1}([0,1])$$

is a bijection up to isomorphisms.

Example 1.1.9.

$$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C}$$
$$x \mapsto x^3$$

$$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C}$$
$$x \mapsto x^3 + 1$$

1.1.4 Covering spaces and Galois groups

A Belyi morphism defines a covering map.

$$\tilde{\beta}\colon \tilde{X} \to \mathbf{P}^1\,\mathbf{C} \setminus \{0,1,\infty\}$$

the coverings are controlled by the profinite completion of

$$\pi_1(\mathbf{P}^1\,\mathbf{C} \setminus \{0,1,\infty\}) = \mathbf{Z} * \mathbf{Z} = F_2.$$

Theorem 1.1.10. *There is a faithful action*

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \circlearrowright \hat{\pi}_1(\mathbf{P}^1\,\mathbf{C} \setminus \{0,1,\infty\})$$

Proof. By Belyi's theorem every elliptic curve $E/\overline{\mathbf{Q}}$ admits a Belyi morphism. For each $j \in \overline{\mathbf{Q}}$ there exists an elliptic curve $E_j/\overline{\mathbf{Q}}$ with j-invariant j.

Given $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$,

$$\sigma(E_j) = E(\sigma(j))$$

assume $\sigma \mapsto 1$,

$$E_j \cong E_{\sigma(j)}\ \forall j$$
$$j = \sigma(j)\ \forall j$$

a contradiction. □

Corollary 1.1.11. *We have a faithful action of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on dessins.*

Theorem 1.1.12. *We have a faithful action of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *on the set of dessins of any fixed genus.*

1.1.5 Exercises

Exercise 1.1.13. Compute the Dessins for the following Belyi morphisms

1. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ \mapsto x^4$$
2. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ \mapsto x^2(3-2x)$$
3. $$\mathbf{P}^1\,\mathbf{C} \to \mathbf{P}^1\,\mathbf{C},\ \mapsto \frac{1}{x(2-x)}$$

Exercise 1.1.14. Give an alternate proof of the fact that X admits a Belyi morphism is and only if it admits a clean Belyi morphism using dessins and the Grothendieck correspondence.

Exercise 1.1.15. Prove that a Belyi morphism corresponding to a tree, that sends ∞ to ∞ is a polynomial.

1.2 Riemann Surfaces I (Ricky)

1.2.1 Definitions

Definition 1.2.1. A **topological surface** is a Hausdorff space X wich has a collection of charts

$$\{\phi_i \colon U_i \xrightarrow{\sim} \phi_i(U_i) \subseteq \mathbf{C},\ \text{open}\}_{i\in I}$$

such that

$$X = \bigcup_{i\in I} U_i.$$

We call X a **Riemann surface** if the transition functions $\phi_i \circ \phi_j^{-1}$ are holomorphic.

1.2.2 Examples

Example 1.2.2. Open subsets of $\mathbf{C}$, e.g.

$$\mathbf{C}$$
$$\mathbf{D} = \{z \in \mathbf{C} : |z| < 1\}$$
$$\mathbf{H} = \{z \in \mathbf{C} : \operatorname{im} z > 0\}.$$

Example 1.2.3. $\hat{\mathbf{C}}$ = Riemann sphere = $\mathbf{C} \cup \{\infty\}$. A basis of neighborhoods of ∞ is given by

$$\{z \in \mathbf{C} : |z| > R\} \cup \{\infty\}.$$

Example 1.2.4.

$$\mathbf{P}^1(\mathbf{C}) = \{[z_0 : z_1] : (z_0, z_1) \neq (0,0)\}$$
$$U_0 = \{[z_0, z_1] : z_0 \neq 0\} \to \mathbf{C}$$
$$[z_0 : z_1] \mapsto \frac{z_1}{z_0}$$
$$U_1 = \{[z_0, z_1] : z_1 \neq 0\} \to \mathbf{C}$$
$$[z_0 : z_1] \mapsto \frac{z_0}{z_1}.$$

Example 1.2.5. Let $\Lambda = \mathbf{Z} \oplus \mathbf{Z}i \subseteq \mathbf{C}$ then $X = \mathbf{C}/\Lambda$ is a Riemann surface.

1.2.3 Morphisms

Definition 1.2.6 ((Holo/Mero)-morphisms of Riemann surfaces)**.** A **morphism of Riemann surfaces** is a continuous map

$$f : S \to S'$$

such that for all charts ϕ, ψ on S, S' respectively we have $\psi \circ f \circ \phi^{-1}$ is holomorphic.

We call a morphism $f : S \to \mathbf{C}$ a **holomorphic function** on S.

We say $f : S \to \mathbf{C}$ is a **meromorphic function** is $f \circ \phi^{-1}$ is meromorphic.

Exercise 1.2.7. The set of meromorphic functions on a Riemann surface form a field.

We denote the field of meromorphic functions by $\mathcal{M}(S)$.

Proposition 1.2.8 (1.26)**.**

$$\mathcal{M}(\hat{\mathbf{C}}) = \mathbf{C}(z).$$

Proof. Let $f : \hat{\mathbf{C}} \to \mathbf{C}$ be meromorphic. Then the number of poles of f is finite say at $a_1, \ldots, a_n$. So, locally at a_i we can write

$$f(z) = \sum_{j=1}^{j_i} \frac{\lambda_{j,i}}{(z - a_i)^j} + h_i(z)$$

with h_i holomorphic. Then

$$f(z) - \sum_{i=1}^{n} \sum_{j=1}^{j_i} \frac{\lambda_{j,i}}{(z - a_i)^j}$$

is holomorphic everywhere. By Liouville's theorem this is constant. □

We say S, S' are isomorphic if $\exists f : S \to S', g : S' \to S$ morphisms such that $f \circ g = \mathrm{id}_{S'}$, $g \circ f = \mathrm{id}_S$.

Exercise 1.2.9. Show that

$$\hat{\mathbf{C}} \simeq \mathbf{P}^1(\mathbf{C}).$$

Remark 1.2.10. $\mathbf{C} \not\simeq \mathbf{D}$ by Liouville.

If S, S' are connected compact Riemann surfaces, then any nonconstant morphism $f : S \to S'$ is surjective. (Nonconstant holomorphic maps are open)

1.2.4 Ramification

Definition 1.2.11 (Orders of vanishing)**.** The **order of vanishing** at $P \in S$ of a holomorphic function on S is defined as follows: For ϕ a chart centered at P write

$$f \circ \phi^{-1}(z) = a_n z^n + a_{n+1} z^{n+1} + \cdots, \ a_n \neq 0$$

then $\mathrm{ord}_P(f) = n$.

More generally, for $f : S \to S'$ we can define $m_P(f)$ (**multiplicity** of f at P) by using a chart ψ on S' and setting

$$m_P(f) = \mathrm{ord}_P(\psi \circ f).$$

If $m_P(f) \geq 2$ then we call P a **branch point** of f and call f ramified at P.

Example 1.2.12.

$$f : \mathbf{C} \to \mathbf{C},\ f(z) = z^2.$$

The chart $\phi_a(z) = z - a$ is centered at $a \in \mathbf{C}$. Then to compute $m_a(f)$ we compute

$$f \circ \phi_a^{-1}(z) = a^2 + 2az + z^2$$

hence

$$\operatorname{ord}_a(f) = \begin{cases} 0, & \text{if } a \neq 0 \\ 2, & \text{if } a = 0 \end{cases}.$$

1.2.5 Genus

Theorem 1.2.13 (Rado)**.** *Any orientable compact surface can be triangulated.*

Fact 1.2.14. *Riemann surfaces are orientable.*

Given such an oriented polygon coming from a Riemann surface, we can associate a word w to it from travelling around the perimeter.

Example 1.2.15. For the sphere $w = a^{-1}ab^{-1}bc^{-1}c$.

Fact 1.2.16. *Every such word can be normalised without changing the corresponding Riemann surface.*

$$w = \begin{cases} w_0 = aa^{-1}, \\ w_g = a_1b_1a_1^{-1}b_1^{-1}\cdots a_gb_ga_g^{-1}b_g^{-1} \end{cases}$$

*The (uniquely determined) g is the **genus** of the surface.*

Example 1.2.17. $w_1 = a_1b_1a_1^{-1}b_1^{-1}$.
$w_2 = a_1b_1a_1^{-1}b_1a_2b_2a_2^{-1}b_2^{-1}$.

Theorem 1.2.18.

$$\chi(S) = v - e + f = 2 - 2g(S).$$

1.3 Riemann Hurwitz Formula (Sachi)

Exercise 1.3.1 (Unimportant)**.** The genus is invariant under changing triangulation.

In particular there are at least two distinct ways of thinking about genus for Riemann surfaces R

1. $$\chi(R) = V - E + F = 2 - 2g$$
2. The dimension of the space of holomorphic differentials on R.

Goal: given R calculate genus

$$y^2 = (x+1)(x-1)(x+2)(x-2)$$

so in an ad hoc way

$$y = \sqrt{(x+1)(x-1)(x+2)(x-2)}$$

when x is not a root of the above we have two distinct values for y, we can imagine two copies of $\mathbf{C}$ sitting above each other and then square root will

land in both copies. We have to make branch cuts between the roots and glue along these to account for the fact that going around a small loop surrounding a root will change the sign of our square root. We end up with something looking like a torus here.

Here we examined the value where there were not enough preimages when we plugged in a value for x. The idea is to project to x, and understand the number of preimages.

$$P(x, y) = y^n + p_{n-1}(x)y^{n-1} + \cdots + p_0(x)$$

an irreducible polynomial.

$$R = \{(x, y) : P(x, y) = 0\}.$$

If we fix $x_0 \in \mathbf{P}^1\,\mathbf{C}$ we can analyse how many y values lie over this x. If we have fixed our coefficients we expect n solutions in y over $\mathbf{C}$, i.e. points $(x_0, y) \in R$.

For some values of x_0 this will not be true, there will be fewer y-values, this occurs when we have a multiple root. This happens precisely when the discriminant of this polynomial vanishes, the discriminant is a polynomial and so has finitely many roots.

Definition 1.3.2 (Branch points)**.** Let $\pi\colon R \to \mathbf{P}^1\,\mathbf{C}$. We say x_0 is a **branch point** if there are fewer than n distinct y-values above x. Then define the **total branching index**

$$b = \sum_{x \in \mathbf{P}^1\,\mathbf{C}} (\deg(\pi) - \#\pi^{-1}(x)).$$

Claim 1.3.3.

$$\chi(R) = \deg \pi \cdot \chi(\mathbf{P}^1\,\mathbf{C}) - b.$$

Lemma 1.3.4. *Locally given some choice of coordinates a non-constant morphism of Riemann surfaces*

$$f\colon R \to S$$

is given by $w \mapsto w^n$. More precisely given $r \in R$, $f(r) = s$ and $V_s \ni s$ a small neighbourhood choose an identification of

$$V_s \xrightarrow{\Psi} D$$

which sends $s \mapsto 0$ and we can find an analytic identification

$$r \in R_r \xrightarrow{\phi} D$$

such that

$$f(U_r) \subseteq V_s.$$

$$\begin{array}{ccc} U_r & \xrightarrow{f} & V_s \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ D & \xrightarrow[w \mapsto w^m]{} & D \end{array}$$

Proof. In Sachi's notes. □

Proof. Of Claim 1.3.3.

Triangulate R so that every face lies in some small coordinate neighborhood s.t.

$$\pi\colon R \to \mathbf{P}^1\,\mathbf{C}$$

is given by $w \mapsto w^m$, s.t. every edge, all branch points are vertices. This ensures that each face edge and vertex has $n = \deg(\pi)$ preimages (except branch points). Then accounting for branch points we have $\deg(\pi) - \#\pi^{-1}(x_0)$ preimages. □

Example 1.3.5. $P(x, y)$ plane curve, classically have

$$g = \frac{(d-1)(d-2)}{2}$$

$\mathbf{P}^2 = \{[x : y : z]\}$ and $(\mathbf{P}^2)^* = [a : b : c]$, lines in $\mathbf{P}^2$

$$ax + by + cz = 0$$

and we have lines $\leftrightarrow$ points. We have C^* the dual curve in $\mathbf{P}^2$ cut out by the tangent lines t_Q for $Q \in C$. Claim $\deg C^* = (d-1)d$.

Want

$$R : \{P(x, y) = 0\} \xrightarrow{\pi} \mathbf{P}^1 \mathbf{C}$$

compute b. In other words, if we fix an arbitrary point $Q \in C$ then there are $d(d-1)$ lines through Q which are tangent to C. Projecting to the x-coordinate $\iff$ family of lines through a point at ∞ $\iff$ $*$ line in $(\mathbf{P}^2)^*$. We have a new question: How many points does this line intersect (up to multiplicity). By bezout $\iff$ $\deg C^*$.

Proof (Matt emerton) Consider a point on C in $\mathbf{P}^2$ such that no tangent line to the curve at ∞ passes through it. Move this point to the origin. If we write

$$P(x, y) = f_d + f_{d-1} + \cdots + f_0$$

then

$$(f_d, f_{d-1}) = 1$$

suppose they share a linear factor:

$$0 = (f_d)_x x + (f_d)_y y + f_{d-1},$$

then this defines a line through the origin. (Because this gives an equation of an asymptote, this is a contradiction).

$$f_d + f_{d-1} + \cdots + f_0 = 0$$

$$df_d + (d-1)f_{d-1} + \cdots + f_1 = 0$$

$$\Longrightarrow$$

$$\begin{cases} f_d + f_{d-1} + \cdots + f_0 = 0 \\ f_{d-1} + 2f_{d-2} + \cdots + (d-1)f_1 = 0 \end{cases}.$$

Now these have $d(d-1)$ common solutions. C^* has degree $d(d-1)$ so $b = d(d-1)$. Riemann-Hurwitz implies

$$\chi(R) = 2\deg\pi - d(d-1)$$

$$\chi(R) = 2d - d(d-1)$$

so

$$g = \frac{(d-1)(d-2)}{2}.$$

A 3-fold equivalence of categories Amazing synthesis.

1. Analysis: Compact connected riemann surfaces.
2. Algebra: Field extensions $K/\mathbf{C}$ where K is finitely generated of transcendence degree 1 over $\mathbf{C}$.
3. Geometry: Complete nonsingular irreducible algebraic curves in $\mathbf{P}^n$.

3) curve $\to$ 2) field extension. Over C all rational functions $\frac{P(x)}{Q(x)}$ $\deg P = \deg Q$, $P, Q : C \to \mathbf{C} \cup \{\infty\}$.
3) $\to$ 1) take complex structure induced by $\mathbf{P}^n$.
1) $\to$ 2) associated field of meromorphic functions on X.
1) $\to$ 3) Any curve which is holomorphic has an embedding into $\mathbf{P}^n$ (Riemann-Roch).
2) $\to$ 1) $K/\mathbf{C}$ consider valuation rings R such that $K \supseteq R \supseteq \mathbf{C}$.

Example 1.3.6. $g = 0$, $\mathbf{P}^1\,\mathbf{C}$ $\mathbf{C}(t)$, $\mathbf{C} \cup \{\infty\}$.

Example 1.3.7. $g = 1$, elliptic curves, $f(x, y, z)$ smooth plane cubic, $f = 0$, $\mathbf{C}(\sqrt{f(x)}, x)$.

$$\mathbf{C}/\Lambda \to \mathbf{P}^2$$
$$z \mapsto (z, \wp(z), \wp'(z))$$
$$z \notin \Lambda$$

backwards

$$(x, y) \mapsto \int_{(x_0,y_0)}^{(x,y)} \frac{\mathrm{d}x}{y}$$

Riemann-Hurwitz (generally) There's nothing that doesn't generalise about the previous proof.

Claim 1.3.8. *For $\pi : R \to S$ a non-constant morphism of compact Riemann surfaces*

$$\chi(R) = \deg \pi \cdot \chi(S) - \sum_{x \in S} (\deg(\pi) - \#\pi^{-1}(x)).$$

Corollary 1.3.9. *There are no non-constant morphisms from a sphere to a surface of genus > 0.*

Proof.

$$f : \mathbf{P}^1\,\mathbf{C} \to S$$
$$\chi(\mathbf{P}^1\,\mathbf{C}) = \deg f\, \chi(S) - b$$
$$2 = (+) \cdot (-) - b.$$

□

Exercise 1.3.10.

$$x^n + y^n + z^n = 0$$

is not solvable in non-constant polynomials for $n > 2$.

Exercise 1.3.11.

$$E = \mathbf{C}/\mathbf{Z} + \mathbf{Z}i$$

multiplication by i rotates $x \mapsto xi$ let $x \sim xi$. If we mod out by $\sim$ to get $E/\sim$ this is still a Riemann surface and the quotient map

$$f : E \to E/\sim$$

is nice, compute the branch points of order 4 and order 2.

Exercise 1.3.12. X compact Riemann surface of $g \geq 2$ then there are at most $84(g-1)$ automorphisms of X.

Exercise 1.3.13. Klein quartic

$$x^3y + y^3z + z^3x = 0$$

has 168 automorphisms and is genus 3.

1.4 Riemann Surfaces and Discrete Groups (Rod)

Welcome to BUGLES (Boston university geometry learning expository seminar), the reason it is called bugles is because bugles are hyperbolic, and today we will see a lot of hyperbolic objects.

Plan

1. Uniformization
2. Fuchsian groups
3. Automorphisms of Riemann surfaces

Proposition 1.4.1.

$$\mathrm{Aut}(\hat{\mathbf{C}}) = \{z \mapsto \frac{az+b}{cz+d}\}$$

$$\mathrm{Aut}(\mathbf{C}) = \{z \mapsto za + b\}$$

$$\mathrm{Aut}(\mathbf{H}) = \{z \mapsto \frac{az+b}{cz+d}, a, b, c, d \in \mathbf{R}\} = \mathrm{PSL}_2(\mathbf{R})$$

Theorem 1.4.2. *Σ has a universal cover $\widetilde{\Sigma}$ with $\pi_1(\Sigma) = 1$. $\widetilde{\Sigma} \to \Sigma$ holomorphic. $\Sigma = \widetilde{\Sigma}/G$ for $G = \pi_1(\Sigma)$. G acts freely and properly discontinuously.*

1.4.1 Uniformization

Theorem 1.4.3. *The only simply connected Riemann surfaces are $\hat{\mathbf{C}}$, $\mathbf{C}$, $\mathbf{H}$.*

Theorem 1.4.4. *Σ is a Riemann surface then*

$$g = 0 : \Sigma \cong \hat{\mathbf{C}}$$
$$g = 1 : \Sigma \cong \mathbf{C}/\Lambda$$
$$g \geq 2 : \Sigma \cong \mathbf{H}/K.$$

Proof. $g = 0$ Uniformization.

$g \geq 1$ $\hat{\mathbf{C}}$ can't be a cover by Riemann-Hurwitz. $g = 1$ $\pi_1(\Sigma) = \mathbf{Z} \oplus \mathbf{Z}$ abelian.

Claim: no subgroup of $\mathrm{Aut}(\mathbf{H})$ is isomorphic to $\mathbf{Z} \oplus \mathbf{Z}$ acting freely and properly discontinuously. So $\widetilde{\Sigma} = \hat{\mathbf{C}}$ $z \mapsto az + b$ free id $a = 1$ so $z \mapsto z + \lambda_1$ $z \mapsto z + \lambda_2$.

$g = 2$ $\pi_1(\Sigma)$ is not abelian but $z \mapsto z + \lambda_1$ is abelian!

$$\Sigma = \mathbf{H}/K,\ K \subseteq \mathrm{PSL}_2(\mathbf{R}).$$ □

Goal Understand Σ through $\widetilde{\Sigma}$ and G.

Fuchsian groups $g \geq 2$.

$$\mathrm{Aut}(\mathbf{H}) = \mathrm{PSL}_2(\mathbf{R}) = \mathrm{Isom}^+(\mathbf{H}, \frac{|\,\mathrm{d}z|^2}{\Im Z})$$

hyperbolic $\mathbf{H}$, $\mathbf{D}$ and $\mathrm{PSL}_2(\mathbf{R})$ acts transitively on geodesics.

Definition 1.4.5 (Fuchsian groups)**.** A **Fuchsian group** is a discrete subgroup of $\mathrm{PSL}_2(\mathbf{R})$.

Remark 1.4.6. (proof in book) Even if Γ doesn't act freely the quotient

$$\mathbf{H} \to \mathbf{H}/\Gamma$$

is still a covering map and $\mathbf{H}/\Gamma$ is a Riemann surface.

Reflections on H Say μ is a geodesic in $\mathbf{H}$, i.e. a horocycle.There is $M \in \mathrm{PSL}_2(\mathbf{R})$ with $M\mu$ the imaginary axis. Then $R = -\bar{z}$ is the reflection over the imaginary axis. Now $R_\mu = M^{-1} \circ R \circ M$ is a reflection over μ.

$$R_\mu = \frac{a\bar{z} + b}{c\bar{z} + d} \notin \mathrm{PSL}_2(\mathbf{R})$$

this is a a problem for us.

Triangle groups Given $n, m, l \in \mathbf{Z} \cup \{\infty\}$ then there is a hyperbolic triangle with angles $\pi/n, \pi/m, \pi/l$ if

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} < 1.$$

With area $\pi(1 - \frac{1}{n} - \frac{1}{m} - \frac{1}{l})$.

In the disk model we can start with a wedge of the disk and by adding a choice third geodesic with endpoints on the edge we can adjust the other angles to be what we like.So we can construct hyperbolic triangles with whatever angles we like. Then let R_1 be the reflection over 1 edge, R_2 , R_3 similarly. By reflecting our original triangle T with these reflections we can tessellate the disk, colouring alternately the triangles obtained using an odd or even number of reflections.

The only remaining problem is that R_i's are not in $\mathrm{PSL}_2(\mathbf{R})$. The solution is to define $x_1 = R_3 \circ R_1$, $x_2 = R_1 \circ R_2$, $x_3 = R_2 \circ R_3$ which are all in $\mathrm{PSL}_2(\mathbf{R})$ now. Now we need to take the union of two adjacent triangles before as a fundamental domain, some quadrilateral that still tessellates. So we have formed a Fuchsian group from our triangles.

A presentation for this group is

$$\langle x_1, x_2, x_3 | x_1^n = x_2^m = x_3^l = x_1x_2x_3 = 1 \rangle$$

note n, m, l can still be ∞.

Definition 1.4.7 (Triangle groups)**.** Let $\Gamma_{n,m,l}$ be the **triangle group** with signature $(1/n, 1/m, 1/l)$.

Remark 1.4.8.

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} = 1$$
$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} > 1$$

still work on $\mathbf{C}$ and $\hat{\mathbf{C}}$ respectively.

Example 1.4.9 ($\mathrm{PSL}_2(\mathbf{Z})$)**.** Consider $\Gamma_{2,3,\infty}$ angles $\pi/2, \pi/3, 0$. We can draw such a triangle in the upper half plane with vertices $i, e^{\pi i/3}, \infty$. So a fundamental domain will be the region obtained by reflecting through the imaginary axis, given by $-\frac{1}{2} \leq \Re z \leq \frac{1}{2}$, $|z| \geq 1$. We have $R_1 = \frac{1}{\bar{z}}, R_2 = -\bar{z} + 1, R_3 = -\bar{z}$ so $x_1 = \frac{-1}{z}, x_2 = \frac{1}{-z+1}, x_3 = z + 1$. Then $\Gamma_{2,3,\infty} \cong \mathrm{PSL}_2(\mathbf{Z})$. Sometimes denoted $\Gamma(1)$.

Observation 1.4.10. If $\Gamma_1 < \Gamma_2$ and T is a fundamental domain of Γ_2 then if $\gamma_1, \gamma_2, \ldots, \gamma_n \in \Gamma_2$ are representatives of $\Gamma_1 \backslash \Gamma_2$ then

$$\bigcup \gamma_i(T)$$

is a fundamental domain for Γ_1.

Example 1.4.11 ($\Gamma(1)$)**.**

$$\Gamma(2) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{id} \pmod 2\}$$

then

$$[\Gamma(1) : \Gamma(2)] = 6$$

representatives of $\Gamma(2)\backslash\Gamma(1)$ are

$$x_1 = \mathrm{id},\ x_2 = \frac{-1}{z-1}, x_3 = \frac{z-1}{z},\ x_4 = \frac{z-1}{z},\ x_5 = \frac{-z}{x-1},\ x_6 = \frac{-1}{z}.$$

Lets see what these do, for example if $z = e^{i\theta}$

$$\Re(x_2(z) = \frac{-1}{e^{i\theta} - 1} = \frac{-e^{i\theta} + 1}{2 - 2\cos\theta}) = \frac{1 - \cos\theta}{2 - 2\cos\theta}\frac{1}{2}$$

if we plot this we see we get two copies of a 0,0,0 triangle so this corresponds to $\Gamma_{\infty,\infty,\infty}$.

$$\langle x_1, x_2, x_3 | x_1 x_2 x_3 = 1\rangle = \langle x_1, x_2\rangle = \pi_1(\mathbf{P}^1 \setminus \{0, 1, \infty\}).$$

Proposition 1.4.12. *$S_1 = \mathbf{H}/\Gamma_1$, $S_2 = \mathbf{H}/\Gamma_2$ then*

$$S_1 \cong S_2 \iff \Gamma_1 = T \circ \Gamma_2 \circ T^{-1},\ T \in \mathrm{PSL}_2(\mathbf{R}).$$

Proof. $\Leftarrow$ Define an $\phi\colon S_1 \to S_2$ via $\phi([z]_1) = [T(z)]_2$.

$\Rightarrow$ Take a lift

$$\begin{array}{ccc} \mathbf{H} & \xrightarrow{\tilde{\phi}} & \mathbf{H} \\ \downarrow & & \downarrow \\ \mathbf{H}/\Gamma_1 & \xrightarrow[\phi]{} & \mathbf{H}/\Gamma_2 \end{array}$$

then $T = \tilde{\phi}$. □

Proposition 1.4.13. *Γ a Fuchsian group acts freely*

$$\mathrm{Aut}(\mathbf{H}/\Gamma) = N(\Gamma)/\Gamma.$$

Proof. Previous proposition, set $\Gamma_1 = \Gamma_2$

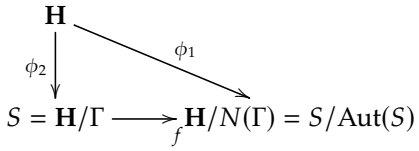
$$N(\Gamma) \to \mathrm{Aut}(\mathbf{H}/\Gamma)$$

kernel is Γ. □

Corollary 1.4.14. *Let Σ be a Riemann surface with $g \geq 2$ then*

$$|\operatorname{Aut}(\Sigma)| < \infty.$$

Proof.



since ϕ_1, ϕ_2 are holomorphic then so is f. So $\deg f = |N(\Gamma)/\Gamma|$ and $\deg f < \infty$. □

Say Σ, $g \geq 2$, $G \subseteq \operatorname{Aut}(\Sigma)$. Let $\bar{g}$ be the genus of Σ/G

$$2g - 2 = |G|(2\bar{g} - 2) + \sum_p (I(p) - 1) = |G|(2\bar{g} - 2 + \sum_{i=1}^{n}(1 - \frac{1}{|I(p_i)|}))$$

where $I(p)$ is the stabiliser of p in G and $\{p_i\}$ area maximal set of fixed points of G inequivalent under the action of G.

Exercise 1.4.15. Σ, $g \geq 2$ then $|\operatorname{Aut}(\Sigma)| \leq 84(g-1)$. Hint: cases.

Exercise 1.4.16. Consider

$$1 \to \Gamma(n) \to \Gamma(1) \to \mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) \to 1$$

compute genus of $\mathbf{H}/\Gamma(n)$.

1.5 Riemann Surfaces and Discrete Groups II (Jim)

1.5.1 Moduli space of compact Riemann surfaces with genus g

$g = 0$. Uniformization tells us that up to isomorphisms all Riemann surfaces of genus 0 are $\mathbf{P}^1$ hence the moduli space $\mathcal{M}_0 = \{\mathrm{pt}\}$.

$g = 1$. Uniformization tells us that each Riemann surface of genus 1 is a torus and can be written as $\mathbf{C}/\omega_1\mathbf{Z} + \omega_2\mathbf{Z} \to \mathbf{C}/(\mathbf{Z} \oplus \tau\mathbf{Z})$, with $\tau = \pm\omega_1/\omega_2$.

Proposition 1.5.1 (2.54)**.**

$$\mathcal{M}_1 \simeq \mathbf{H}/\mathrm{PSL}_2(\mathbf{Z}) \simeq \mathbf{C}.$$

Proof. Idea: Existence of

$$\mathbf{C}/\Lambda_{\tau_1} \xrightarrow{\sim} \mathbf{C}/\Lambda_{\tau_2}$$

with $\bar{T}([0]) = [0]$ is equivalent to the existence of $T \in \operatorname{Aut}(\mathbf{C})$ (choose $T(z) = wz$) such that $w(\mathbf{Z} \oplus \tau_1\mathbf{Z}) = \mathbf{Z} \oplus \tau_2\mathbf{Z}$. This in turn is equivalent to the existence of

$$A, A' \in \mathrm{GL}_2(\mathbf{Z})$$

s.t. $\det(A) = \det(A') = \pm 1$ so that

$$\begin{pmatrix} w \\ w\tau_1 \end{pmatrix} A \begin{pmatrix} 1 \\ \tau_2 \end{pmatrix} = A' \begin{pmatrix} w \\ w\tau_1 \end{pmatrix}$$

$$\implies \tau_q = A\psi_2 = \frac{a\tau_2 + b}{c\tau_2 + d}$$

and $A \in \mathrm{PSL}_2(\mathbf{R})$. Implies $A \in \mathrm{PSL}_2(\mathbf{Z})$ as both $\tau_1, \tau_2 \in \mathbf{H}$. Conversely if

$$\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + b}$$

isomorphism is induced by $T(z) = (c\tau_2 + d)z$. □

$g > 1$ $\mathcal{M}_g$ is a complex variety of dimension $3g-3$. Uniformization tells us that describing a Riemann surface amounts to specifying $2g$ real 2×2 matrices $\{\gamma_i\}_{i=1}^{2g}$ such that

1. $\det(\gamma_i) = 1$ which implies that γ_i depends on 3 real parameters so we have a total of $6g$.
2. $\prod_{i=1}^{g}[\gamma_i, \gamma_{g+i}] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 3 relations, so $6g-3$. Since for any $\gamma \in \mathrm{PSL}_2(\mathbf{R})$ $\Gamma = \langle \gamma_i \rangle$ and $\gamma\Gamma\gamma^{-1}$ uniformize isomorphic Riemann surfaces implies $6g-6$ real parameters, so $3g-3$ complex parameters.

1.5.2 Monodromy

Let $f\colon S_1 \to S$ be a morphism of degree d ramified over $y_1, \ldots, y_n \in S$. For $y \in S \setminus \{y_1, \ldots, y_n\}$ we have a group homomorphism

$$M_f\colon \pi_1(S \setminus \{y_1, \ldots, y_n\}) \to \mathrm{Bij}(f^{-1}(y))$$

$$\gamma \mapsto M_f(\gamma) = \sigma_\gamma^{-1}.$$

σ_γ is defined as follows:

$$\gamma \in \pi_1(S \setminus \{y_1, \ldots, y_n\})$$

lifts to a path $\widetilde{\gamma}$ from $x \in f^{-1}(y)$ to another $x' \in f^{-1}(y)$ set $\sigma_\gamma(x) = x'$. If we number the points in $f^{-1}(y)$ we may think of $M_f(\pi_1) \subseteq \Sigma_d$, via some $\phi\colon \{1, \ldots, d\} \to f^{-1}(y)$. $\mathrm{Mon}(f)$ is the image of $M_f(\pi_1)$ in Σ_d.

Monodromy and Fuchsian groups Let

$$\pi\colon \mathbf{H}/\Gamma_1 \to \mathbf{H}/\Gamma$$

be the Fuchsian group representation of the map

$$f\colon S_1 \to S \ni y.$$

Identifications $y = [z_0]_\Gamma$ for some $z_0 \in \mathbf{H}$.

$$\pi_1(S \setminus \{y_1, \ldots, y_n\}) \simeq \Gamma$$

$$f^{-1}(y) = \{[\beta z_0]_{\Gamma_1}\}$$

where β runs along a set of representatives of $\Gamma_1\backslash\Gamma$.

$$M_f\colon \Gamma \to \mathrm{Bij}(\Gamma_1\backslash\Gamma)$$
$$\gamma \mapsto M_f(\gamma)$$
$$\implies \gamma \sim \pi_1([z_0, \gamma(z_0)])$$

where $[z_0, \gamma(z_0)]$ is a path in $\mathbf{H}$. Lift this loop to $\mathbf{H}/\Gamma_1$ is the path $\pi_{\Gamma_1}(\beta[z_0, \gamma_0(z_0)])$. which corresponds to $\Gamma_1\beta\gamma$, this implies $\sigma_\gamma(\Gamma_1\beta) = \Gamma_1\beta\gamma$.

Corollary 1.5.2 (2.59)**.**

$$M_\pi : \Gamma \to \mathrm{Bij}(\Gamma_1 \backslash \Gamma)$$

induces an isomorphism

$$\frac{\Gamma}{\bigcap_{\beta \in \Gamma_1} \beta^{-1} \Gamma_1 \beta} \simeq \mathrm{Mon}(\pi)$$

characterize morphisms by monodromy. Let f_i have degree 2, non conjugate.

Proposition 1.5.3 (2.63)**.** *For S a compact Riemann surface and $\beta = \{a_1, \ldots, a_n\} \subset S$ for some $d \geq 1$ there are only finitely many pairs $(\tilde{S}, f)$ where $\tilde{S}$ is a compact Riemann surface and*

$$f : \tilde{S} \to S$$

is a degree d morphism with branching value set β.

Proof. Special case: Assume $S = \mathbf{P}^1$ and $n = 3$.

$$\Gamma = \Gamma(2) = \{A \in \mathrm{PSL}_2(\mathbf{Z}) : A = \mathrm{id} \pmod 2\}$$

$$= \pi_1(S' \setminus \{0, 1, \infty\})$$

is generated by γ_1, γ_2 so any map $M_f : \Gamma(2) \to \Sigma_d$ is determined by images of γ_1, γ_2. □

1.5.3 Galois coverings

Definition 1.5.4. A covering $f : S_1, \to S_2$ is Galois (or regular, or normal) if the covering group

$$\mathrm{Aut}(S, f) = \{h \in \mathrm{Aut}(S_1) : f \circ h = f\} = G$$

acts transitively on each fibre. With this notion we can think of $S_1 \to S_1/G$.

Proposition 1.5.5 (2.65)**.**

$$f : S_1 \to S_2$$

is Galois if and only if

$$f^* : M(S_2) \to M(S_1)$$

is a Galois extension. In this case $\mathrm{Aut}(S_1, f) \simeq \mathrm{Gal}(M(S_1)/M(S_2))$.

Example 1.5.6. Hyperelliptic covers of $\mathbf{P}^1$ given by

$$S = \{y^2 = \prod_{i=1}^{N} (x - a_i)\} \to \mathbf{P}^1$$

$$(x, y) \to x$$

covering group G is order 2 generated by the involution $J(x, y) = (x, -y)$.

Proposition 1.5.7 (2.66)**.** *A covering*

$$f : S_1 \to S_2$$

is normal/Galois iff

$$\deg(f) = |\mathrm{Mon}(f)|.$$

1.5.4 Normalization of coverings of $\mathbf{P}^1$

Let $f: S \to \mathbf{P}^1$ be a cover of $\deg d > 0$ with $\mathrm{Mon}(f) \leq \Sigma_d$.

The normalisation

$$\tilde{f}: \tilde{S} \to \mathbf{P}^1$$

associated to f has $\mathrm{Mon}(f) \cong \mathrm{Aut}(\tilde{S}, \tilde{g}$ and $\tilde{f}^*: M(\mathbf{P}^1) \to M(\mathbf{P}^1)$ is the normalisation of the extension

$$f^*: M(\mathbf{P}^1) \hookrightarrow M(S)$$

Normalization of extensions $K \hookrightarrow L$ is a Galois extension of K of lowest possible degree containing L.

Definition 1.5.8. Normalization of $f: S \to \mathbf{P}^1$ $\deg d > 0$ is a Galois covering $\tilde{f}: \tilde{S} \to \mathbf{P}^1$ of lowest possible degree s.t. $\exists \pi: \tilde{S} \to S$ with the diagram commuting.

Corollary 1.5.9 (2.73)**.**

$$\mathrm{Mon}(f) \simeq \mathrm{Aut}(\tilde{S}, \tilde{f})$$

Interpretation in terms of Fuchsian groups:

Proposition 1.5.10. *Let $f: S_1 \to S$ be a covering of Riemann surfaces $S_1 \setminus f^{-1}\{y_1, \ldots, y_n\} \to S \setminus \{y_1, \ldots, y_n\}$. The unramified cover and $\pi: \mathbf{H}/\Gamma_1 \to \mathbf{H}/\Gamma$ the Fuchsian group representatives. The normalisation of f can be represented as the compactification of*

$$\mathbf{H}/\bigcap_{\gamma \in \Gamma} \gamma^{-1}\Gamma_1\gamma \to \mathbf{H}/\Gamma_1 \to \mathbf{H}/\Gamma$$

so the covering group is isomorphic to $\Gamma/\bigcap \gamma^{-1}\Gamma_1\gamma \simeq \mathrm{Mon}(f)$.

Example 1.5.11. Let $F(x, y) = y^2x - (y-1)^3$ consider

$$S_F \to \mathbf{P}^1$$

$$(x, y) \to x$$

S_F has genus 0. $S_F \to \mathbf{P}^1$ is of degree 3 and ramified at most over $0, \frac{-27}{4}, \infty$. $\mathrm{Mon}(x) \simeq \Sigma_3$ so not a normal covering. Normalization of (S_F, x) is $S_{\tilde{F}}, \tilde{x})$ where

$$\tilde{F}(x, y) = y^2(1-y)^2x + (1 - y + y^2)$$

1.6 Belyi's theorem (Maria)

Theorem 1.6.1. *Let S be a compact riemann surface, then the following are equivalent.*

1. *S is defined over $\overline{\mathbf{Q}}$ (iff over a number field)*
2. *S admits a morphism $f: S \to \mathbf{P}^1$ with at most 3 branching values.*

Definition 1.6.2 (Belyi functions)**.** A meromorphic function with less than 4 branching values is a **Belyi function**.

Remark 1.6.3.

1. Branching values can be taken to be in $\{0, 1, \infty\}$.
2. If $S \neq \mathbf{P}^1$, then $f: S \to \mathbf{P}^1$ has at least 3 branching values

Definition 1.6.4 (Belyi polynomials)**.** Let $m, n \in \mathbf{N}$, $\lambda = m/(m+n)$, define

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

Belyi polynomials.

Proposition 1.6.5. *P_λ satisfies*

1. *P_λ ramifies at exactly $0, 1, \lambda, \infty$.*
2. *$P_\lambda(0) = P_\lambda(1) = 0, P_\lambda(\lambda) = 1, P_\lambda(\infty) = \infty$.*

Example 1.6.6.

$$S_\lambda : y^2 = x(x-1)(x-\lambda)$$

with $\lambda = m/(m+n)$. From ex. 1.32

$$x \colon S_\lambda \to \mathbf{P}^1$$

$$(x, y) \mapsto x$$

$$\infty \mapsto \infty$$

ramifies over $0, 1, \lambda, \infty$. Then $f = P_\lambda \circ x \colon S_\lambda \to \mathbf{P}^1$ ramifies exactly at $(0,0), (1,0), (\lambda, 0), \infty$. With branching values $0, 0, 1, \infty$ so that f is a Belyi function.

1.6.1 Proof of a) implies b)

Note 1.6.7. Its enough to show $\exists f \colon S \to \mathbf{P}^1$ ramified over $\{0, 1, \infty, \lambda_1, \ldots, \lambda_n\} \subseteq \mathbf{Q} \cup \{\infty\}$. Given this we can repeatedly use Belyi polynomials to obtain $g \colon S \to \mathbf{P}^1$ ramified over $\{0, 1, \infty\}$.

Write $S = S_F$

$$F(x, y) = p_0(x) y^n + \cdots + p_n(x)$$

defined over $\overline{\mathbf{Q}}[x, y]$. Let $B_0 = \{\mu_1, \ldots, \mu_s\}$ be the branching values of $x \colon S_F \to \mathbf{P}^1$.

Theorem 1.86 says that the each μ_i is ∞, a root of $p_0(x)$ or a common root of F, F_y which implies by lemma 1.84 that $B_0 \subseteq \overline{\mathbf{Q}} \cup \{\infty\}$. If $B_0 \subseteq \mathbf{Q} \cup \{\infty\}$ we are done otherwise let $m_1(T) \in \mathbf{Q}[T]$ be the minimal polynomial of $\{\mu_1, \ldots, \mu_s\}$. Let $\{\beta_1, \ldots, \beta_d\}$ be the roots of $m_1'(T)$ and $p'(T)$ their min. poly. Note : $\deg P(t) < \deg m_1'(T)$

Note: $\text{Branch}(g \circ f) = \text{Branch}(g) \cup g(\text{Branch}(f))$ branching values.

So B_1 $\text{Branch}(m_1 \circ x) = m_1(\{\text{roots of } m_1'\}) \cup \{0, \infty\}$.

$$S \xrightarrow{x} \mathbf{P}^1 \xrightarrow{m_1} \mathbf{P}^1$$

If $B_1 \subseteq \mathbf{Q} \cup \{\infty\}$ done. Otherwise let $m_2(T)$ be the minimal polynomial $/\mathbf{Q}$ of $\{m_1(\beta_1), \ldots, m_1(\beta_d)\}$, $B_2 = \text{Branch}(m_2 \circ m_2 \circ x)$. Fact: $\deg(m(t)) < \deg(m_1(T))$.

Repeat inductively until $B_k \subseteq \mathbf{Q} \cup \{\infty\}$ which is guaranteed by the decreasing degrees.

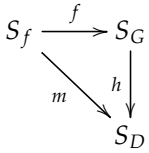
1.6.2 Algebraic characterization of morphisms

Proposition 1.6.8. *Defining a morphism $f: S_F \to S_G$ is equivalent to giving a pair of rational functions*

$$f = (R_1, R_2),\ R_i = \frac{P_i}{Q_i},\ P_i, Q_i \in \mathbf{C}[x, y],\ Q_i \notin (F)$$

such that $Q_1^{\deg_x(G)} Q_2^{\deg_y(G)} G(R_1, R_2) = HF$ for some $H \in \mathbf{C}[x, y]$. $f(R_1, R_2)$ is an isomorphism if there exists an inverse morphism $h: S_G \to S_F$.

Remark 1.6.9.



The fact that this diagram commutes can be expressed by polynomial identities.

1.6.3 Galois action

Let $\mathrm{Gal}(\mathbf{C}) = \mathrm{Gal}(\mathbf{C}/\mathbf{Q})$.

Definition 1.6.10. For $\sigma \in \mathrm{Gal}(\mathbf{C})$, $a \in \mathbf{C}$ denote $a^\sigma = \sigma(a)$,

1. If $P = \sum a_{ij} x^i y^j \in \mathbf{C}[x, y]$ set

   $$P^\sigma = \sum a_{ij}^\sigma x^i y^j \in \mathbf{C}[x, y]$$

   if $R = P/Q$ set $R^\sigma = P^\sigma / Q^\sigma$.

2. If $S \simeq S_F$, $S^\sigma = S_{F^\sigma}$.

3. If $\Psi = (R_1, R_2)\ S_F \to S_G$ is a morphism, set $\Psi^\sigma = (R_1^\sigma, R_2^\sigma): S_{F^\sigma} \to S_{G^\sigma}$.

4. For an equivalence class $(S, f) = (S_F, R(x, y))$ of ramified cvers of $\mathbf{P}^1$ set $(S, f)^\sigma = (S^\sigma, f^\sigma) = (S_{F^\sigma}, R^\sigma(x, y))$.

Exercise 1.6.11. Verify this Galois action is well-defined (lemma 3.12).

Recall: S_F is constructed from a noncompact Riemann surface $S_F^\times \subseteq \mathbf{C}^2$ by adding finitely many points, (theorem 1.86). If $P = (a, b) \in S_F^\times$ then $P^\sigma = (a^\sigma, b^\sigma)$. What about the other points?

1.6.4 Points and valuations

Definition 1.6.12. Let $\mathcal{M}$ be a function field. A (discrete) valuation of $\mathcal{M}$ is $v: \mathcal{M}^* \to \mathbf{Z}$ s.t.

1. $v(\phi\psi) = v(\phi) + v(\psi)$
2. $v(\phi \pm \psi) \geq \min\{v(\phi), v(\psi)\}$
3. $v(\phi) = 0$ if $\phi \in \mathbf{C}^*$
4. v is nontrivial $\exists \phi : v(\phi) \neq 0$

set $v(0) = \infty$.

Facts:

$$A_v = \{\phi \in \mathcal{M} : v(\phi) \geq 0\} \subseteq \mathcal{M}$$

is a subring that is a local ring with a maximal ideal

$$M_v = \{\phi \in \mathcal{M} : v(\phi) > 0\} = (\phi)$$

for some ϕ a uniformizer.

If $v(\phi) = 1$ v is normalised.

Proposition 1.6.13 (3.15)**.** *Every point $P \in S$ a compact Riemann surface defines a valuation on $\mathcal{M}(S)$ by $v_P(\phi) = \mathrm{ord}_P(\phi)$.*

Proof. Easy exercise. □

Theorem 1.6.14 (3.23)**.** *For any compact Riemann surface S*

$$P \in S \mapsto v_P = \mathrm{ord}_P$$

gives a 1-1 correspondence between points of S and normalised valuations on $\mathcal{M}(S)$.

Proof. Sketch: First prove it for $S = \mathbf{P}^1$.

Inductively meromorphic functions separate points.

Surjectivity study behaviour of valuations in finite extensions of fields and use a nonconstant morphism $f : S \to \mathbf{P}^1$ to reduce to the case of $\mathbf{P}^1$. □

Galois action on points

Definition 1.6.15.

1. Given a valuation v on $\mathcal{M}(S)$ define a valuation v^σ on $\mathcal{M}(S^\sigma)$ by $v^\sigma = v \circ \sigma^{-1}$ i.e. $v^\sigma(\psi^\sigma) = v(\psi)$ for all $\psi \in \mathcal{M}(S)$.

2. For $P \in S$ define $P^\sigma \in S^\sigma$ as the unique point in S^σ s.t. $v_{P^\sigma} = (v_P)^\sigma$.

Proposition 1.6.16 (3.25)**.**

1. *For $\sigma \in \mathrm{Gal}(\mathbf{C})$, $P \mapsto P^\sigma$ is a bijection $S \to S^\sigma$.*

2. *On $P \in S_F^\times$ this agrees with the previous definition of P^σ.*

3. *$a^\sigma = a$ for all $a \in \mathbf{Q} \cup \{\infty\}$ for all $\sigma \in \mathrm{Gal}(\mathbf{C})$.*

Proof. Sketch

1. $a \mapsto a^{\sigma^{-1}}$.

2. Follows as in proof of 3.22

3. Obvious for $a \in \mathbf{Q}$, for ∞:

$$(v_\infty)^\sigma(x - 1) = v_\infty(x - a^{\sigma^{-1}}) = 1 = v_\infty(x - 1)$$

for all $a \in \mathbf{C}$ implies $(v_\infty)^{\sigma^{-1}} = v_\infty$ implies $\infty^\sigma = \infty$.

□

1.6.5 Elementary invariants of the action of Gal(**C**).

Remark 1.6.17. The bijection $S \leftrightarrow S^\sigma$ is not holomorphic. In general S and S^σ are not isomorphic.

Theorem 1.6.18. *The action of* Gal(**C**) *on pairs* (S, f) *satisfies*

1. $$\deg(f^\sigma) = \deg(f)$$
2. $$(f(P))^\sigma = f^\sigma(P^\sigma)$$
3. $$\mathrm{ord}_{P^\sigma}(f^\sigma) = \mathrm{ord}_P(f)$$
4. $a \in \hat{\mathbf{C}}$ *is a branching value of* f *iff* a^σ *is a branching value of* f^σ.
5. $\mathrm{genus}(S) = \mathrm{genus}(S^\sigma)$ *i.e. they are homeomorphic.*
6. $\mathrm{Aut}(S, f) \to \mathrm{Aut}(S^\sigma, f^\sigma)$ *via* $h \mapsto h^\sigma$ *is a group homomorphism.*
7. *The monodromy group* $\mathrm{Mon}(f)$ *of* (S, f) *is isomorphic to* $\mathrm{Mon}(f^\sigma)$ *of* (S^σ, f^σ).

We will use properties 1 and 4 at least.

Proposition 1.6.19 (Criterion 3.29)**.** *For a compact Riemann surface S the following are equivalent*

1. S *is defined over* $\overline{\mathbf{Q}}$.
2. $\{S^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbf{C})}$ *contains only finitely many isomorphism classes of Riemann surfaces.*

Proof. 1 implies 2: $S = S_F$, $F = K[x, y]$ for K a number field then

$$|\{F^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbf{C})}| \leq [K : \mathbf{Q}]$$

2 implies 1 is section 3.7. □

Proof of b implies a in Belyi's theorem (3.61) Suppose $f : S \to \mathbf{P}^1$ is a morphism of degree d with branching values $\{0, 1, \infty\}$. By theorem 3.28 $\forall \sigma \in \mathrm{Gal}(\mathbf{C})$

$$f^\sigma : S^\sigma \to \mathbf{P}^1$$

is a morphism of degree d and branching values are

$$\{\sigma(0), \sigma(1), \sigma(\infty)\} = \{0, 1, \infty\}.$$

So $\{f^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbf{C})}$ gives rise to only finitely many monodromy homomorphisms.

$$F_{f^\sigma} : \pi_1(\mathbf{P}^1 \setminus \{0, 1, \infty\}) \to \Sigma_d$$

the fundamental group is free on two generators so there are only finitely many such maps. Theorem 2.61 implies $\{S^\sigma\}_{\sigma \in \mathrm{Gal}(\mathbf{C})}$ contains only finitely many equivalence classes so by the criterion S is defined over $\overline{\mathbf{Q}}$.

1.6.6 The field of definition of Belyi functions (3.8)

Proposition 1.6.20. *Belyi functions are defined over* $\overline{\mathbf{Q}}$.

Proof. Use the same methods as in 3.7. □

1.7 Dessins (Berke)

$$G_{\mathbf{Q}} \circlearrowright (X, D) \leftrightarrow (S, f) \circlearrowright G_{\mathbf{Q}}$$

where (X, D) is a dessin, (S, f) is a Belyi pair.

1.7.1 Dessins

Definition 1.7.1. A dessin is a pair (X, D) where X is an oriented compact topological surface and $D \subset X$ is a finite graph:

1. D is connected
2. D is bicoloured
3. $X \setminus D$ is a disjoint union of topological disks.

Not all of these are so important (for example 3 implies 1 (but the converse does not hold)). We can also obtain a bicoloured graph from an uncoloured graph by subdividing all edges and colouring the new vertices black and the others white.

A single edge in a sphere is, a single edge in a torus is not.

Permutation representation of a Dessin Label the edges of a dessin $\{1, \dots, N\}$ then

$$\sigma_0(i) = \text{subsequent edge in the cycle around the white vertex of } i$$

as we have a positive orientation on the edges

$$\sigma_1(i) = \text{subsequent edge in the cycle around the black vertex of } i.$$

Then we define

Definition 1.7.2. (σ_0, σ_1) is the permutation representation pair of (X, D).

Say

$$\sigma_0 = (1, \dots, N_1)(N_1 + 1, \dots, N_2) \cdots$$

a product of disjoint cycles. Then each of these cycles corresponds to a white vertex, where the length of the cycle is the degree of the corresponding vertex. Same for σ_1 and black vertices.

$$\{\text{cycles appearing in the decomposition of } \sigma_0\sigma_1\}$$
$$\updownarrow$$
$$\{\text{faces of } D\}$$

Exercise 1.7.3. Prove this.

Remark 1.7.4. D connected implies that $\langle \sigma_0, \sigma_1 \rangle$ is transitive on Σ_N. As D is bicoloured the cycles on D contain an even number of edges.

A dessin is not a triangulation of X but

$$\chi(X) = \#V - \#E + \#F$$

proof later.

Proposition 1.7.5.

$$\chi(X) = (\#\textit{cycles of } \sigma_0 + \#\textit{cycles of } \sigma_1) - N + \#\{\textit{cycles of } \sigma_0\sigma_1\}.$$

$$(\sigma_0, \sigma_1) \rightsquigarrow (X', D)$$
$$\langle \sigma_0, \sigma_1 \rangle \subseteq \Sigma_N$$

is transitive.

Proposition 1.7.6. *There exists* (X, D) *with permutation representation* (σ_0, σ_1).

Proof. Write $\sigma_0\sigma_1 = \tau_1 \cdots \tau_k$, τ_i disjoint cycles each of length n_i with $\sum n_i = N$. Create k faces bounded by $2n_1, \ldots, 2n_k$ vertices, and assign the vertices white and black colours so that the graph is bicoloured. As $\sigma_0\sigma_1$ should jump two each time we get an identification of all edges which we then glue using σ_0. □

Definition 1.7.7. We say that

$$(X_1, D_1) \sim (X_2, D_2)$$

if there exists an orientation preserving homeomorphism $\phi\colon X_1 \to X_2$, $\phi|_{D_1}\colon D_1 \xrightarrow{\sim} D_2$.

Theorem 1.7.8.

$$\{\textit{Dessins}\}/\sim \leftrightarrow \{(\sigma_0, \sigma_1),\ \langle \sigma_0, \sigma_1 \rangle \subseteq \Sigma_N \textit{ transitive}\}/\sim$$

1.7.1.1 Dessins 2 Belyi pairs

Triangle decomposition of $(X, D) \rightsquigarrow T(D)$ a set of triangles that cover D and intersect along edges or at vertices.

Example 1.7.9. Edge in the sphere, add an extra vertex $\times$ not on the edge and get a decomposition into two triangles.

We will label triangles by $T_j^{\pm}$ as there are two for each edge, by orientation some are the same.

$$T(D) \rightsquigarrow f_D\colon X \to \hat{\mathbf{C}}$$

Glue

$$f_j^?\colon T_j^? \to \overline{\mathbf{H}}^?$$

for $? \in \{+, -\}$, where $f_j^+ = f_j^-$ on the intersection. Where $\partial T_j \xrightarrow{\sim} \mathbf{R} \cup \{\infty\}$

$$\text{black} \mapsto 0$$

$$\text{white} \mapsto 1$$

$$\times \mapsto \infty$$

and we have $\text{Branch}(f_D) \subseteq \{0, 1, \infty\}$. Now $\deg f_D = \#\text{edges of } D$, $m_v(f_D) = \deg v$, $f_D^{-1}([0,1]) = D$. Modify X a little bit and use some lemma to get $S_D \simeq_{\text{top}} X$ for some Riemann surface with $f_D\colon S_D \to \mathbf{P}^1$.

Definition 1.7.10. (S, f) is a Belyi pair with S compact Riemann surface and f a Belyi function on S.

$$(S_1, f_1) \sim (S_2, f_2)$$

if it is an isomorphism of ramified coverings.

So we can now go in both directions.

$$\{\text{Dessins}\}/\sim$$

$$\updownarrow$$

$$\{\text{Belyi pairs}\}/\sim$$

$$(X, D) \mapsto (S_D, f_D)$$

$$(S, D_f) \mapsto (S, f)$$

Now to define the Galois action

$$G_{\mathbf{Q}} \circlearrowright \{\text{Dessins}\} \leftrightarrow \{\text{Belyi pairs}\}$$

$$\begin{array}{ccc} (X, D) & \dashrightarrow & (X, D)^\sigma \\ \downarrow & & \uparrow \\ (S_D, f_D) & \longrightarrow & (S_D^\sigma, f_D^\sigma)^\sigma \end{array}$$

The $G_{\mathbf{Q}}$ action is faithful on dessins of genus g.

Example 1.7.11. Same example $\mathbf{P}^1$ with a single edge, $f_D = z$, $\deg f_D = \#$ edges, $m_v(f) = \deg v$.

Exercise 1.7.12. String.

Exercise 1.7.13. n star.

1.8 A Sandwich Table of Dessins d'Enfants

Alex: So I haven't typed this section as it was a lot of pictures and I haven't got nice scans of them, will try at some point.

1.9 Belyi's theorem, effective Mordell and ABC (Angus)

We begin with one of the most famous results in arithmetic geometry.

Theorem 1.9.1 (Mordell conjugate/Falting's theorem)**.** *Let C be an algebraic curve of genus ≥ 2 over a number field K. Then $C(K)$ is finite.*

There are many proofs of this, Falting's being the original and most famous.

Remark 1.9.2. Falting's proof is not effective. That is, it cannot predict the number of points or give any bounds.

Today we'll show how this theorem follows from a (much harder conjecture), but how this nonetheless gives new insight into the question of effectiveness. Specifically we'll show ABC implies Mordell.

"Mordell is as easy as ABC"- Zagier

Conjecture 1.9.3 (ABC)**.** *Let $A, B, C \in \mathbf{Z}$ s.t.* $\gcd(A, B, C) = 1$ *and* $A + B + C = 0$*, then for all $\epsilon gt 0$ there exists a constant k_ϵ s.t.*

$$N(A, B, C) > k_\epsilon H(A, B, C)^{1-\epsilon}$$

where

$$N(A, B, C) = \prod_{p|ABC} p$$

$$H(A, B, C) = \max(|A|, |B|, |C|).$$

This is a remarkably deep statement about the integers. Something surprising about how one compares the additive and multiplicative structures of the integers.

For our purposes (to connect it to the curves and Mordell) we'd like to remove the dependence on integrality and coprimality, by making it scaling invariant.

We now define

$$H(A, B, C) = \prod_v \max(|A|_v, |B|_v, |C|_v)$$

$$N(A, B, C) = \prod_{p \in I} p$$

for

$$I = \{p \text{ prime} : \max(|A|_p, |B|_p, |C|_p) > \min(|A|_p, |B|_p, |C|_p)\}.$$

Exercise 1.9.4 (For sanity)**.**

$$H(\lambda A, \lambda B, \lambda C) = H(A, B, C)$$

$$N(\lambda A, \lambda B, \lambda C) = N(A, B, C)$$

for $\lambda, A, B, C \in \mathbf{Q}^\times$. Moreover if $A, B, C \in \mathbf{Z}$ and gcd = 1 then we recover the original definition.

Since we have $A + B + C = 0$ and our functions are scaling invariant, they only depend on $r = -A/B$. We'll also reformulate it over an arbitrary number field K.

Note that to satisfy the hypotheses of the conjecture we require

$$r \in \mathbf{P}^1_K \setminus \{0, 1, \infty\}.$$

We now define

$$H(r) = \prod_v \max(1, |r|_v)$$

$$N(r) = \prod_{p \in I} p$$

for

$$I = \{p \text{ prime} : \max(v_p(r), v_p(1/r), v_p(r-1)) > 0\}.$$

Remark 1.9.5. In fact this new height is off from the old one by a constant factor, but since ABC allows for a constant factor this won't trouble us.

Motivation: ABC implies Fermat bound One can see this simply by assuming a solution

$$x^n + y^n = z^n,\ n \geq 3$$

and setting

$$(A, B, C) = (x^n, y^n, z^n)$$

then

$$N(A, B, C) = \prod_{p|ABC} p \leq |xyz| < \max(|x|^3, |y|^3, |z|^3) = H(A, B, C)^{3/n}.$$

So setting

$$\epsilon = 1 - 3/n$$

for (A, B, C) s.t. $H(A, B, C)$ is sufficiently large we get a contradiction to ABC. Thus ABC gives us a bound on the possible solutions to the Fermat equation, reducing the remainder of the conjecture to a finite computation.

Let us phrase this in the following alternate way: Let

$$F_n : x^n + y^n + z^n = 0$$

be the Fermat curve and consider the function

$$f : F_n \to \mathbf{P}^1$$

$$(x : y : z) \mapsto -\left(\frac{x}{y}\right)^n$$

ramified over $0, 1, \infty$.

Note 1.9.6. $\deg(f) = n^2$

Each of $0, 1, \infty$ has n preimages in $F_n(\overline{\mathbf{Q}})$.

The idea now is that $N(A, B, C)$ is measuring ramification, while $H(A, B, C)$ is a height function. The note above tells us that each of $0, 1, \infty$ contributes a factor of $O(H(A, B, C)^{n/n^2})$ to $N(A, B, C)$. So in this formulation, what we used was the existence of a rational function f such that

$$\#\{p \in C(\overline{\mathbf{Q}}) : f(p) \in \{0, 1, \infty\}\} < \deg(f).$$

Exercise 1.9.7. If C has genus 0 or 1, no such f can exist (hint: Riemann-Hurwitz).

ABC implies a bound on Mordell We begin with a technical proposition:

Proposition 1.9.8. *Let K be a number field an d C/K a curve. Let $f \in K(C)$ be a rational function of degree d. Then for $p \in C(K) \setminus f^{-1}(0)$ we have*

$$\log N_0(f(p)) < (1 - b_f(0)/d) \log H(f(p)) + O(\sqrt{\log H(f(p))} + 1)$$

with the following notation

$$N(r) = N_0(r)N_1(r)N_\infty(r)$$

$$N_0(r) = \prod_{\mathfrak{p} \supseteq (r)} \mathrm{Norm}(\mathfrak{p})$$

$$N_1(r) = \prod_{\mathfrak{p} \supseteq (1-r)} \mathrm{Norm}(\mathfrak{p})$$

$$N_\infty(r) = \prod_{\mathfrak{p} \supseteq (1/r)} \mathrm{Norm}(\mathfrak{p})$$

$$b_f(0) = \sum_{f(p)=0} (e_p - 1).$$

Proof. The genus 0 case follows from the fact that the f is a rational function (and in fact the error term is $O(1)$) (exercise). For the general case we need the theory of log heights on curves. From this we require the following

- For D a divisor on C we have a height function
$$h_D(\cdot)$$
which is well defined up to $O(1)$.
- If
$$D = \sum m_k D_k$$
is a decomposition into irreducible divisors, then
$$h_D(P) = \sum m_k h_{D_k}(P).$$
- For Δ a degree 0 divisor
$$h_\Delta(P) = O(\sqrt{\log H(f(P))} + 1).$$

Let $D = \mathrm{div}_0(f) = \sum m_k D_k$, $D' = \sum_{f(P)=0}(P)$ then $b_f(0) = \deg D'$. Then

$$\log H(f(P)) = h_D(P) + O(1) = \sum m_k h_{D_k}(P) + O(1)$$

since $\log H(f(P))$ is also a height function relative to D. We now turn to $N_0(f(P))$. Any prime occurring in this must also occur in $h_{D_k}(P)$ for some k (except for a finite set $\{p : p|f$ or p bad red. for $C\}$). Then

$$N_0(f(P)) < \sum h_{D_k}(P) + O(1) = h_{D'}(P) + O(1).$$

Letting

$$\Delta = (\deg D)D' - (\deg D')D$$

we have

$$h_\Delta(P) = O(\sqrt{\log H(f(P))} + 1)$$

thus

$$\begin{aligned}
\log N_0(f(P)) &< h_{D'}(P) + O(1) \\
&= \frac{1}{\deg D}(\deg D')h_{D'}(P) + O(1) \\
&= \frac{1}{\deg D}(\deg D')h_D(P) + O(\sqrt{\log H(f(P))} + 1) \\
&= \frac{1 - b_f(0)}{d} \log H(f(P)) + O(\sqrt{\log H(f(P))} + 1)
\end{aligned}$$

□

Remark 1.9.9. One can show the above for N_1, N_∞ instead making the appropriate replacements for f.

Adding the three terms together we get

$$\log N_0(f(P))N_1(f(P))N_\infty(f(P)) < \left(\left(1-\frac{b_f(0)}{d}\right)+\left(1-\frac{b_f(1)}{d}\right)+\left(1-\frac{b_f(\infty)}{d}\right)\right)\log H(f(P))+O(\cdots)$$

$$\log N(f(P)) < \frac{1}{d}\left(\#f^{-1}(0)+\#f^{-1}(1)+\#f^{-1}(\infty)\right)\log H(f(P))+O(\cdots)$$

$$< \frac{m}{d}\log H(f(P))+O(\cdots)$$

where

$$m = \#\{P \in C(\overline{\mathbf{Q}}) : f(P) \in \{0,1,\infty\}\}$$

exponentiating we get

$$N(f(P)) < H(f(P))^{m/d}K.$$

Theorem 1.9.10 (ABC implies Mordell)**.** *ABC implies Mordell.*

Proof. Let C be a given curve of genus $g \geq 2$ Belyi's theorem gives a function

$$f : C \to \mathbf{P}^1$$

ramified over $\{0,1,\infty\}$. By Riemann-Hurwitz $m = d+2-2g$, $d = \deg(f)$ m as above. Thus $m < d$, thus we can pick $0 < \epsilon < 1-\frac{m}{d}$ and so for sufficiently large $H(f(P))$ (i.e. all but finitely many) we have a counterexample to ABC. □

Remark 1.9.11 (Closing remarks)**.** Belyi's theorem gives an algorithm for determining $f : C \to \mathbf{P}^1$ i.e. it is effective.

One can also show ABC implies Siegel's theorem.

In fact it can be shown that a particular effective form of Mordell (applied to $y^2+y=x^5$) for all number fields implies ABC. This is related to Szpiro's conjecture.

References:

1. Elkies - ABC implies Mordell
2. Serre - Lectures on Mordell-Weil

1.10 Dessins, integer points on elliptic curves and a proof of the ABC conjecture (Alex)

1.10.1 A proof of the ABC theorem (for polynomials)

Last week Angus told us about the incredibly powerful ABC conjecture and its arithmetic consequences (apparently). This week we will prove this conjecture (for polynomials). The proof is very similar to some of the things Angus mentioned, but seeing as I wasn't there its new to me... Following Goldring / Stothers / Parab.

Let K be algebraically closed of characteristic 0, with $f \in K[x]$, we can define the radical as before

$$\mathrm{rad}(f) = \prod_{p|f} p$$

over the primes/irreducibles dividing f, this is the maximal squarefree polynomial dividing f. How do we measure size of a polynomial? Let $r(f) = \deg \mathrm{rad}(f)$, and $h(f_1, \ldots, f_n) = \max\{\deg f_i\}$. This is a complicated way of saying

$$\#\{x \in K : f(x) = 0\},$$

but we do so to emphasise the link with ABC.

The result is then

Theorem 1.10.1 (Mason-Stothers)**.** *Let*

$$e, f, g \in K[x],\ e + f = g$$

be pairwise coprime and all of height > 0*. Then*

$$h(e, f, g) < r(efg) = r(e) + r(f) + r(g).$$

We have sharpness if and only if f/g *is a Belyi map for* $\mathbf{P}^1 \to \mathbf{P}^1$ *with* $(f/g)(\infty) \in \{0, 1, \infty\}$*. Another way of saying this is that if* $\deg f = \deg g$ *then their leading coefficients are equal, and hence* $\deg(e) < \deg(f)$*.*

Proof. First of all we note that the statement is symmetric in e, f, g, so we may arrange that $h(g) \leq h(e, f)$ which implies that $h(e) = h(f) = h(e, f, g)$. The second statement is less obviously invariant but note that ϕ is a Belyi function is equivalent to $1 - \phi$ and $1/\phi$ being Belyi also and this preserves $\phi(\infty) \in \{0, 1, \infty\}$, so rearranging does not change the truth of the second statement either. Let $\phi = f/g$ so $\deg(\phi) = \max\{\deg(f), \deg(g)\} = h(e, f, g)$, we will denote this by h now. Apply Riemann-Hurwitz (suprise-suprise)

$$-2 = -2h + \sum_{x \in \mathbf{P}^1} e_\phi(x) - 1.$$

Let

$$R_y = \sum_{x : f(x) = y} e_\phi(x) - 1$$

be the ramification above y, we will consider B_0, B_1, B_∞. These ramification numbers will simply be $h - \#(\phi^{-1}(y))$. Lets begin with R_1, we have $f(x)/g(x) = 1$ so $e(x) = 0$ and in fact

$$R_1 = h(e) - r(e) = h - r(e).$$

For R_0 we have either $f(x) = 0$ or $g(x) = \infty$. Having $g(x) = \infty$ means $x = \infty$ but this cannot really happen as $h(f) \geq h(g)$. So this is really just

$$\sum_{x : f(x) = 0} e_\phi(x) - 1 = h - r(f).$$

Finally $\phi(x) = \infty$ only when $g(x) = 0$ or $x = \infty$. If $h(f) = h(g)$ then $\phi(\infty) \neq \infty$ and we have simply

$$R_\infty = h - r(g).$$

If $h(g) < h(f)$ then we also have $\phi(\infty) = \infty$ so we pick up an extra preimage and we get instead

$$R_\infty = h - (r(g) + 1).$$

Back up in Riemann-Hurwitz this comes down (magically?) to

$$-2 = \cancelto{0}{-2h + h + h} + h - r(e) - r(f) - r(g) + R - \delta_{h(f) > h(g)}$$

so

$$R = h - r(efg) - 2 + \delta_{h(f)>h(g)}$$

but of course $R \geq 0$ so

$$h \geq r(efg) + 1$$

with equality exactly when

$$h = r(efg) + 1 \implies R = 0,\ h(f) > h(g).$$

$R = 0$ is equivalent to being Belyi. □

1.10.2 Back to number theory

That was all well and good, but this is a number theory seminar, not a function field analogues of number theory seminar, so let's take it back to why we are all here, solving Diophantine equations.

Let's try and find nontrivial integral points on Mordell curves!

$$E_k : y^2 = x^3 + k.$$

Example 1.10.2.

$$1001^2 = 5009^3 - (5009^3 - 1001^2)$$

so I found a large point on

$$y^2 = x^3 - (5009^3 - 1001^2) = x^3 - 125675213728$$

are you not impressed?

Although this point would look slightly non-trivial if I started with the curve 5009^3 is roughly 125675213728 anyway so you should only be impressed if I find points of height somewhat larger than the coefficients. We should probably ask that

$$|x|^3 > |k|$$

by some margin at least.

A nice question is then given k how big can an integer point (x, y) on E_k be? Bounds are known, e.g. Via work of Baker we get

$$\max(|x|, |y|) < e^{10^{10}|k|^{1000}}.$$

Ouch.

If we want to study more realistic bounds we can instead reverse the problem. Can we minimise $x^3 - y^2$ for integer x, y, how close can the square of a large integer and the cube of a large integer be? Euler showed that $x^3 - y^2 = 1$ has only 1 (interesting) solution, for example.

Marshall Hall was interested in this, did some nice computations and conjectured:

Conjecture 1.10.3 (Mashall Hall's conjecture, 1970)**.** *If*

$$x^3 - y^2 = k$$

for integers x, y then

$$|k| > \frac{\sqrt{|x|}}{5}$$

(or $k = 0$...).

This is false!

Example 1.10.4 (Elkies (who else?))**.** If

$$x = 5853886516781223,\ y = 447884928428402042307918$$

is a point on

$$y^2 = x^3 - 1641843$$

then

$$\frac{\sqrt{|x|}}{k} = 46.6004943471754.$$

This is far larger than the previous best known, but still remains the record as far as I can tell. It seems Hall's conjecture is unlikely to be true for any fixed constant, but the following of Stark-Trotter is more believable.

Conjecture 1.10.5 (Stark-Trotter/Weak Hall)**.** *For any $\epsilon > 0$ there is some $C(\epsilon)$ such that for any x, y integers*

$$|x^3 - y^2| > C(\epsilon)x^{\frac{1}{2}-\epsilon}$$

for any $x > C(\epsilon)$.

If Hall's/Stark-Trotter is true we get a *huge* improvement on Baker

$$\frac{\sqrt{|x|}}{|k|} < 100 \implies x < 10^4 k^2$$

and hence

$$y^2 = x^3 + k < 10^{12}k^6 + k$$

giving polynomial bounds on x, y in terms of k.

How might one find such triple (x, y, k) that is extremal? One approach is to try and come up with a parametrisation of nice triples. We can search for polynomials $X(t), Y(t), K(t)$ and then plug in various integer values for t and hope for the best. To give ourselves the best chance of succeeding we want $K(t)$ to be smaller than $X(t)^3$ and $Y(t)^2$ for some values of t. This leads us to ask for K to be of smallest degree possible. So how low can we go?

This is the point where we come full circle right, we are searching for

$$X(t)^3 - Y(t)^2 = K(t)$$

with degree of K minimised, so we apply Mason-Stothers to see that, if M is the degree of the left hand terms we have $\deg(X) = 2m$ and $\deg(Y) = 3m$, indeed h in Mason-Stothers is then $6m$ We also have $r(X^3) = r(X) \leq 2m$ and $r(X^2) = r(Y) \leq 3m$ so together Mason-Stothers gives

$$6m < 2m + 3m + r(K)$$

or $m < r(K)$. So we have lower-bounded the degree of K in terms of $\frac{1}{2}\deg(X)$ for example.

We just proved:

Conjecture 1.10.6 (Birch B. J., Chowla S., Hall M., Jr., Schinzel A. On the difference $x^3 - y^2$, 1965.)**.** *Let X, Y be two coprime polynomials with X^3, Y^2 of equal degree ($6m$) and equal leading coefficient, then*

$$K = X^3 - Y^2$$

is of degree $> m$.

(Now the speaker has just given a theorem with an inequality, so in order to appear smart one of you should ask is this bound sharp.)

The bound is sharp, this can mean several things in general, originally it was asked that for infinity many m *there is an example where* $\deg K = m + 1$.

The first part was proved initially by Davenport (in the same year, and journal). The second part had to wait until '81 for Stothers to prove it.

Someone else should probably also ask, how is any of this related to Dessins?

To prove sharpness we have to exhibit for each m triple of polynomials X, Y, K of degrees $2m, 3m, m+1$. Coming up with polynomial families is hard, drawing stupid pictures is easy, can Dessins aid us here?

Lets back-track, when we proved Mason-Stothers we also said that sharpness was equivalent to f/g being Belyi, so $X(t)^3/K(t) = (K(t) + Y(t)^2)/K(t) = Y(t)^2/K(t)+1$ should be a Belyi map of degree $6m$ from $\mathbf{P}^1 \to \mathbf{P}^1$. What does its ramification look like? We should have all preimages of 0 degree 3, preimages of 1 degree 2, and above infinity $m+1$ points of degree 1 and the remaining of degree $6m - (m+1) = 5m - 1$.

How can we draw a Dessin like this? Begin with a tree with all internal vertices degree 3, with $2m$ vertices, this will have $2m - 1$ edges, and as it is trivalent by the handshake lemma

$$3\#\{\text{internal}\} + \#\{\text{leaves}\} = 4m - 2$$

and

$$\#\{\text{internal}\} + \#\{\text{leaves}\} = 2m$$

giving

$$2\#\{\text{internal}\} = 2m - 2$$
$$\#\{\text{internal}\} = m - 1$$
$$\#\{\text{leaves}\} = m + 1$$

Add loops to the leaves, you now have a clean Dessin as above. It has $2m - 1 + m + 1 = 3m$ edges. We have a face for every loop of degree 1, and one on the outside of degree $m + 1 + 2(2m - 1) = 5m - 1$ as each internal edge is traversed twice if you walk around the outside. So this works!

Example 1.10.7. For $m = 1$

$$(x^2 + 2)^3 - (x^3 + 3x)^2 = 3x^2 + 8.$$

$m = 2$

$$(x^4 + 4x)^3 - (x^6 + 6x^3 + 6)^2.$$

Example 1.10.8. For $m = 5$

$$X(t) = \frac{1}{9}(t^{10} + 6t^7 + 15t^4 + 12t)$$

$$Y(t) = \frac{1}{54}(2t^{15} + 18t^{12} + 72t^9 + 144t^6 + 135t^3 + 27)$$

$$K(t) = -\frac{1}{108}(3t^6 + 14t^3 + 27)$$

and we can let $t = -3$ to get $X(-3) = 5234$, $Y(-3) = -378661$ and $K(-3) = -17$, so we have a point

$$(5234, 378661) \in E_{17} \colon y^2 = x^3 + 17$$

letting $t = \pm 9$ we get

$$|384242766^3 - 7531969451458^2| = 14668$$

$$|390620082^3 - 7720258643465^2| = 14857$$

both of which have

$$\frac{\sqrt{|x|}}{k} \approx 1.33,$$

these get lower as we increase t though.

We should expect this decrease from this method as if $\deg X = 2m$ and $\deg K = m + 1$ then $\sqrt{X(t)}/K(t)$ grows like $t^m/t^{m+1} = t^{-1}$.

Can we do the same for abc?

Take the Dessin with a deg 1 vertex at infinity, degree 3 at 0 with an edge surrounding 1, we get a Belyi function

$$f(x) = \frac{64x^3}{(x+9)^3(x+1)},\ f(x) - 1 = -\frac{(x^2 - 18x - 27)^2}{(x+9)^3(x+1)}$$

plugging in $x = a/b$ and cross multiplying gives

$$64a^3b + (a^2 - 18ab - 27b^2)^2 = (a + 9b)^3(a + b)$$

which could of course be verified independently, but how would you find this identity without Dessins? Now for $a = -32$, $b = 23$ we get

$$-2^{21} \cdot 23 + 11^2 = -1 \cdot 3^2 \cdot 5^6 \cdot 7^3$$

or

$$11^2 + \cdot 3^2 \cdot 5^6 \cdot 7^3 = 2^{21} \cdot 23$$

This is the second highest quality abc triple known with quality

$$\frac{\log c}{\log R} = 1.62599$$

(the current winner has quality 1.6299).

References

1. On Marshall Hall's Conjecture and Gaps Between Integer Points on Mordell Elliptic Curves - Ryan D'Mello