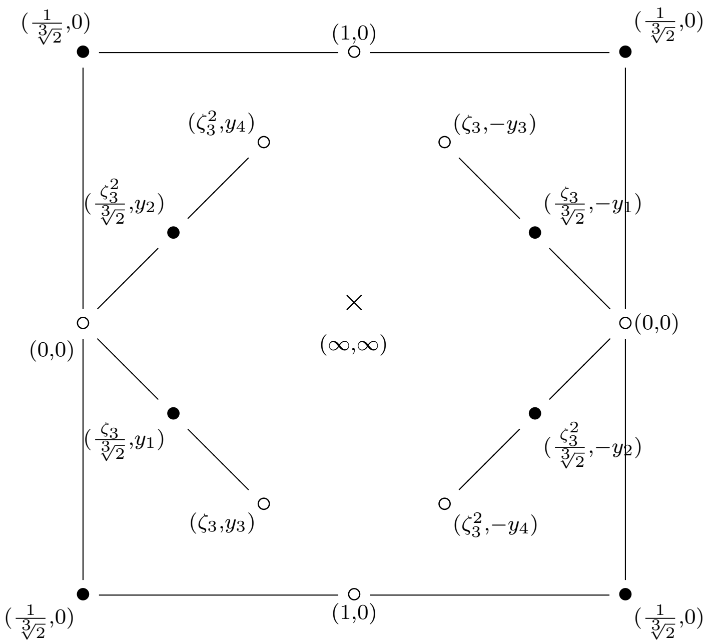
DESSINS D'ENFANTS:

Function Theory and Algebra of Belyi Functions on Riemann Surfaces

With

Combinatorics and Group Theory of Belyi Functions on Riemann Surfaces



by Prof. Jürgen Wolfart and Prof. Gareth Jones

in the 16^{th} Jyväskylä Summer School
24th July - 4th August 2006

Lecture Notes Taken by Tuomas Puurtinen

Contents

Lecture 1

by Prof. Jürgen Wolfart

1 Riemann Surfaces and Algebraic Curves

Riemann surfaces are Haudorff spaces with a countable base topology, where chart maps to $\mathbb{C}$ are defined with biholomorphic transition functions where they coincide. We are discussing here only connected Riemann surfaces.

1.1 Examples

1. Riemann sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C})$: Take two charts U_1 and U_2, for example $U_1 \cong \mathbb{C}$ and $U_2 \cong (\mathbb{C} - \{0\}) \cup \{\infty\}$. Then $z \mapsto \frac{1}{z}$ is a holomorphic mapping between the charts.

2. $F_n^{\text{aff}} = \{\, (x, y) \in \mathbb{C}^2 \,|\, x^n + y^n = 1 \,\}$, $n > 1$ is a "Fermat curve". Take as charts for example $(x, y) \mapsto y$, which is homeomorphic in suitable neighboughoods of all points except $x = 0$, $y^n = 1$, and $(x, y) \mapsto x$ which is homeomorphic in suitable neighbourhoods of all points except $y = 0$, $x^n = 1$, with transition functions $x = \sqrt[n]{1 - y^n}$ and $y = \sqrt[n]{1 - x^n}$.

3. More general: all "smooth" affine algebraic curves
$$X^{\text{aff}} := \{\, (x, y) \in \mathbb{C}^2 \,|\, f(x, y) = 0 \,\}$$
for some polynomial f with the property that in all $p \in X^{\text{aff}}$
$$\frac{\partial f}{\partial x}(p) \neq 0 \quad \text{or} \quad \frac{\partial f}{\partial y}(p) \neq 0.$$
The implicit function theorem says that locally around p all solutions of $f(x, y) = 0$ are of the shape $(h(y), y)$ or $(x, g(x))$ where h and g are holomorphic. Then the projections serve as charts.

4. Affine hyperelliptic curves: $y^2 = (x - a_1) \cdot \ldots \cdot (x - a_n)$ with pairwise distinct $a_1, \ldots, a_n$. For example $f = y^2 - \Pi(x - a_i)$ and we have
$$\frac{\partial f}{\partial y}(p) = 2y = 0$$
in all $(a_i, 0)$, but
$$\frac{\partial f}{\partial x}(p) \neq 0$$
in these $(a_i, 0)$.

Theorem 1.1 *Let X, Y be connected Riemann surfaces, $f : X \to Y$ non-constant holomorphic mapping, $p \in X$, $f(p) = p' \in Y$. Then there exist charts $z : U(p) \to V \subset \mathbb{C}$ and $w : U'(p') \to V' \subset \mathbb{C}$ with $z(p) = 0$, $w(p') = 0$ such that*

$$\begin{array}{ccc} U & \xrightarrow{f} & U' \\ {\scriptstyle z}\downarrow & & \downarrow{\scriptstyle w} \\ \mathbb{C} : z & \longmapsto & w = z^n : \mathbb{C} \end{array}$$

is commutative for some choice $n \in \mathbb{N}$ independent of the choice of the charts. The constant $n = \operatorname{mult}_p f$ is the multiplicity of f in p.

If $n = 1$ then f is locally biholomorphic (”unramified at p”) otherwise ”ramified” of order n.

1.2 Important Consequences

1. If $f : X \to \hat{\mathbb{C}}$ is meromorphic, then if it's non-constant, then the zeros and poles are discrete in X.

2. Ramification points of f are discrete in X.

3. Identity theorem, maximum principle, open mapping theorem are valid.

4. On compact Riemann surfaces we have for $f : X \to \hat{\mathbb{C}}$ (meromorphic, non-constant function) only a finite number of zeros or poles, and also a finite number of ramification points. Holomorphic functions $f : X \to \mathbb{C}$ have to be constant.

5. If $f : X \to Y$ is holomorphic and non-constant, X compact, then f is surjective and Y is compact as well.

6. Under the same hypothesis $\deg f := \sum_{p \in f^{-1}(y)} \operatorname{mult}_p f$ is independent of $y \in Y$.

1.3 More Examples

1. Fermat curve:

   $$F_n := \{\, [x, y, z] \in \mathbb{P}^2(\mathbb{C}) \mid x^n + y^n = z^n \,\}$$

   better (symmetric) $x^n + y^n + z^n = 0$, covered by affine curves with $z = 1$, $y = 1$, $x = 1$. We'll get different affine Fermat curves, when we take charts of the form $\frac{x}{y}, \frac{y}{z}, \frac{z}{x}$. This's a typical example of a ”smooth projective algebraic curve". Of course, because $\mathbb{P}^2(\mathbb{C})$ is compact, then F_n is compact.

2. Try to compactify also hyperellictic curves

$$y^2 = \Pi_{i=1}^n (x - a_i) \Rightarrow y^2 z^{n-2} = \Pi_i (x - a_i z).$$

Now if $z = 1$ then we'll have an affine curve, or if $z = 0$ then $x^n = 0$ and so on $x = 0$, normalizing by $y = 1$ we get affine equation

$$z^{n-2} = \Pi(x - a_i).$$

Implicit function theorem isn't applicable in situations $n > 3$. Here, write $y^2 = q(x)$ with

$$\deg q = \begin{cases} 2g + 1, \\ 2g + 2 \end{cases}$$

and with

$$z := \frac{1}{x} \quad \text{and} \quad w := \frac{y}{x^{g+1}}.$$

$$k(z) := z^{2g+2} q\left(\frac{1}{z}\right) \in \mathbb{C}[z]$$

with $\deg k = 2g + 2$. So then $y^2 = q(x) \Leftrightarrow w^2 = k(z)$ in all points $x \neq 0, \neq z \ldots$.

$$x = y = \infty \Leftrightarrow z = 0 \Leftrightarrow \begin{cases} w = 0, & \text{for } \deg q = 2q + 1 \\ w = \pm\sqrt{k(0)} & \text{for } \deg q = 2q + 2 \end{cases}$$

1.4 Fact

Riemann surfaces are orientable! That is an implication from that the transition functions are biholomorphic respecting the orientation. Surfaces can also be triangulated: Suppose you have X triangulated. Then we have the Euler characteristic

$$\chi(X) := f - e + v,$$

with f, e and v counting "faces", "edges" and "vertices", which does not depend on the triangulation. For example $\chi(\hat{\mathbb{C}}) = 2$ and $\chi(\text{Torus}) = 0$.

Theorem 1.2 (Riemann-Hurwitz) *If $f : X \to Y$ is non-constant holomorphic mapping of compact Riemann surfaces, then*

$$2g(X) - 2 = \deg f(2g(Y) - 2) + \sum_{p \in X} (\text{mult}_p f - 1).$$

Several applications, e.q: $g(Y) \leq g(X)$ with "=" only if f is isomorphism (unramified) or $g = 1$ and f is unramified. If $g(X) > g(Y) = 0$ or 1, then f is ramified.

Now F_n (n>2) has genus $\frac{(n-1)(n-2)}{2}$, and we consider $f : F_n \to \hat{\mathbb{C}} : [x, y, z] \mapsto \frac{x}{z}$: For example $z = 1$, $x^n + y^n = 1$, $f : (x, y) \mapsto x$ and $\deg f = n$. Exceptionally, f has only one preimage in points with $x^n = 1$: n points with $\mathrm{mult}_p\, f = n$. If then $z = 0$, $x^n + y^n = 0$, $y = 1$, n points on F_n, f has n poles and it's unramified. Now Riemann-Hurwitz implies that

$$2g(F_n) - 2 = n(-2) + n(n-1) = n^2 - 3n.$$

Exercise 1.1 *Find as many automorphisms of F_n as possible! (if possible, find $6n^2$ automorphisms.) Determine the structure of* $\mathrm{Aut}\, F_n$.

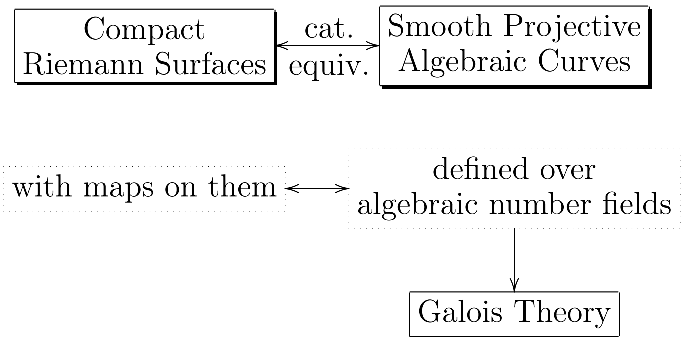
Exercise 1.2 *Apply Riemann-Hurwitz to determine the genus of the (compact) hyperelliptic curves.*

Theorem 1.3 *There is an equivalence between the categories "compact Riemann surfaces" and "smooth projective algebraic curves".*

Lecture 2

by Prof. Gareth Jones

2 Introduction to Riemann Surfaces and Algebraic Curves



Special case: Riemann surfaces of genus 1.

Elliptic curve: algebraic curve $y^2 = p(x)$, where p is a cubic polynomial on $\mathbb{C}[x]$ with distinct roots e_1, e_2, e_3. Discriminant $\Delta = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$. Here p has distinct roots if and only if $\Delta \neq 0$. Applying an affine substitution of $ax + b$ for x we can put the equation in Weierstrass normal form

$$y^2 = 4x^3 - c_2 x - c_3, \quad (c_2, c_3 \in \mathbb{C}).$$

Then $\Delta = c_2^3 - 27c_3^2$ (easy exercise).

Alternatively, applying affine substitutions to x and x, we get Legendre normal form

$$y^2 = x(x-1)(x-\lambda) \quad (\lambda \in \mathbb{C}\backslash\{0,1\}).$$

Exercise 2.1 *Find Δ and these normal forms for the elliptic curve*

$$y^2 = x^3 - 9x^2 + 23x - 15.$$

Now write the elliptic curve E as $y = \sqrt{p(x)}$, a 2-valued function of x. The projection $(x, y) \mapsto x$ is in general 2-to-1, showing that E is a 2-sheeted covering of the Riemann sphere $\hat{\mathbb{C}} = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Special cases: if $x = e_j$, $j = 1, 2, 3$, then only $y = 0$ is possible, and if $x = \infty$ then only $y = \infty$ is possible. E is a branched covering of $\hat{\mathbb{C}}$, with branch-points at e_1, e_2, e_3 and ∞.

If $z = e_j + re^{i\vartheta}$, let z rotate once around e_j (but not the other roots) in the positive directions (anti-clockwise). Then $\sqrt{(z - e_j)}$ is multiplied by $e^{i\pi} = -1$. This means that a point (x, y) on E above x moves to $(x, -y)$, i.e. we pass from one sheet of E to the other. The same happens if we follow a circle around ∞, where $x = re^{i\vartheta}$, with large constant r: each of the three factors $\sqrt{(x - e_j)}$ is multiplied by -1, and hence so is y. Construct the Riemann surface of E by taking two copies of $\hat{\mathbb{C}}$ (one for each branch of $\sqrt{p(x)}$), and joining them across two disjoint cuts between e_1 and e_2, and e_3 and ∞. The result is a torus, of genus 1.

2.1 Alternative Approach to Riemann Surfaces of genus 1

Let ω_1 and ω_2 be elements of $\mathbb{C}$ which are linearly independent over $\mathbb{R}$. They generate a lattice

$$\Lambda = \Lambda(\omega_1, \omega_2) = \{\, m\omega_1 + n\omega_2 \,|\, m, n \in \mathbb{Z} \,\}.$$

We call ω_1 and ω_2 a basis for Λ. Λ is a subgroup of $\mathbb{C}$, and Λ is discrete (every $\omega \in \Lambda$ has an open neighbourhood containing no other element of Λ).

Define $z_1 \equiv z_2 \mod \Lambda$ if $z_1 - z_2 \in \Lambda$. Equivalence classes = cosets $z + \Lambda$ of Λ in $\mathbb{C}$. Quotient space is then $\mathbb{C}/\Lambda$.

The parallellogram $P = \{\, x\omega_1 + y\omega_2 \,|\, x, y \in [0, 1] \,\}$ is a fundamental region for Λ, i.e. each $z \in \mathbb{C}$ is equivalent to an element of P, and if two elements of P are equivalent, then they lie on the boundary ∂P. Form $\mathbb{C}/\Lambda$ by identifying equivalent points $z_1, z_2 \in \partial P$. The holomorphic structure on $\mathbb{C}$ yields a holomorphic structure on $\mathbb{C}/\Lambda$. Also $\mathbb{C}/\Lambda$ is a group, structure inherited from $\mathbb{C}$.

To show the link between these two approaches, we need elliptic functions. These are doubly periodic meromorphic functions. Doubly periodic means

$$f(z + \omega) = f(z) \quad \text{for all } z \in \mathbb{C} \text{ and all } \omega \in \Lambda.$$

Meromorphic: holomorphic or a pole of finite order at each point in $\mathbb{C}$. Equivalently, $f(x) = \sum_{n=k}^{\infty} a_n (z - a)^n$ near each a (Laurent series).

For a given Λ, such functions form a field $F(\Lambda)$. Think of these as the meromorphic functions on $\mathbb{C}/\Lambda$ by defining $f(z + \Lambda) = f(z)$ (well-defined). $\mathbb{C}/\Lambda$ is compact, so the theory of such functions works nicely.

We need some non-constant examples: Weierstrass function

$$\wp(z) = \frac{1}{z^2} + \sum\nolimits_{\omega}' \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)$$

where $\sum'$ means the sum over $\omega \neq 0$ in Λ. This is uniformly convergent on compact subsets of $\mathbb{C}\backslash\Lambda$ so $\wp$ is meromorphic, with poles of order 2 at the lattice-points. To show $\wp$ is double periodic, first consider

$$\wp'(z) = -2\sum_{\omega} \frac{1}{(z-\omega)^3}.$$

This is meromorphic, with poles of order 3 at the lattice-points.

Exercise 2.2 *Show that $\wp'$ is doubly periodic with respect to Λ. Deduce that $\wp$ is also doubly periodic (Hint: $\wp$ is an even function).*

Thus $\wp, \wp' \in F(\Lambda)$ so the field $\mathbb{C}(\wp, \wp')$ of rational functions of $\wp$ and $\wp'$ is contained in $F(\Lambda)$. In fact, $F(\Lambda) = \mathbb{C}(\wp, \wp')$. $\wp$ and $\wp'$ are not algebraically independent: they satisfy

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3,$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$, and where $G_k = \sum'_\omega \omega^{-k}$ is the Eisenstein series. Comparing this equation with the Weierstrass normal form $y^2 = 4x^3 - c_2x - c_3$ for E, we can write $x = \wp(z)$, $y = \wp'(z)$ for an appropriate lattice Λ. (Given any c_2, c_3 with $\Delta \neq 0$, one can find a lattice Λ such that g_2 and g_3 for Λ are equal to c_2 and c_3.) Identify each point $(x, y) \in E$ with the corresponding point $z + \Lambda \in \mathbb{C}/\Lambda$. Thus we identify E with $\mathbb{C}/\Lambda$. (Compare with parametrising $x^2+y^2 = 1$ by $x = \sin z$ and $y = \cos z$, where $z \in \mathbb{R}/2\pi\mathbb{Z}$.

Suppose that Λ and Λ' are lattices in $\mathbb{C}$. The Riemann surfaces $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic (as Riemann surfaces) if and only if Λ and Λ' are similar lattices, in the sense that $\Lambda' = \mu\Lambda$ for some $\mu \in \mathbb{C}\backslash\{0\}$.

If Λ has basis ω_1, ω_2, then elements ω_1', ω_2' of Λ form a basis for Λ if and only if $\omega_2' = a\omega_2 + b\omega_1$ and $\omega_1' = c\omega_2 + d\omega_1$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$. The 2×2 integer matrices with $ad - bc = \pm 1$ form a group $\mathrm{GL}_2(\mathbb{Z})$ under multiplication and those with $ad - bc = 1$ form $\mathrm{SL}_2(\mathbb{Z})$, a normal subgroup (of index 2).

The modulus $\tau = \frac{\omega_2}{\omega_1}$ of a basis is invariant under the similarity transformation of multiplying Λ by μ. Changing basis by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ transforms $\tau = \frac{\omega_2}{\omega_1}$ to

$$\tau' = \frac{\omega_2'}{\omega_1'} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1} = \frac{a\tau + b}{c\tau + d}.$$

These transformations form a group $\mathrm{PGL}_2(\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z})/\{\pm 1\}$. Transposing ω_1 and ω_2 necessary, we can assume that $\operatorname{Im}\tau > 0$, i.e. τ is the upper half place $\mathbb{H} = \{\, \tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0 \,\}$.

This allows us to restrict to transformations $\tau \mapsto \frac{a\tau+b}{c\tau+d}$ with $ad - bc = 1$. These form the modular group

$$\Gamma = \mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}.$$

Then

$$\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda' \quad \Leftrightarrow \quad \tau \text{ and } \tau' \text{ are equivalent under the action of } \Gamma \text{ on } \mathbb{H}$$

and

$$\boxed{\begin{array}{c}\text{Isomorphism classes}\\ \text{of elliptic curves } \mathbb{C}/\Lambda\end{array}} \longleftrightarrow \boxed{\text{Orbits of } \Gamma \text{ on } \mathbb{H}.}$$

How does Γ act on $\mathbb{H}$?

For example the region F defined by $|\tau| \geq 1$, $|\operatorname{Re}\tau| \leq \frac{1}{2}$ is a fundamental region for Γ. Every orbit of Γ contains a point in F. If two points in F are in the same orbit, they lie on the boundary. The element $X : \tau \mapsto \frac{-1}{\tau}$ fixes $\tau = i$, and this value of τ corresponds to the square lattice. The element $Z : \tau \mapsto \tau+1$ also pairs sides of F. The element $Y : \tau \mapsto \frac{-\tau-1}{\tau}$ fixes $\omega = e^{2\pi i/3}$ corresponding to the hexagonal lattice Λ.

One can show that Γ has a presentation $\Gamma = \langle X, Y \mid X^2 = Y^3 = 1 \rangle \cong C_2 * C_3$, the free product of C_2 and C_3.

Reduction mod $(n) : \mathbb{Z} \to \mathbb{Z}_n$ (ring-homomorphism) induces group homomorphisms $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}_n)$ and hence $\Gamma = \mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}_n) = \mathrm{SL}_2(\mathbb{Z}_n)/\{\pm I\}$.

$$\Gamma(n) := \ker \phi_n$$

is the principal conquence subgroup of level n.

E.g. $\Gamma(2)$ is a free group of rank 2, generated by $\tau \mapsto \frac{\tau}{-2\tau+1}$ (fixing 0) and $\tau \mapsto \frac{-\tau+2}{-2\tau+3}$ (fixing 1).

Exercise 2.3 *Show that Γ acts transitively on $\hat{\mathbb{Q}} = \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, and that $\Gamma(2)$ has three orbits on $\hat{\mathbb{Q}}$. Deduce that $\Gamma/\Gamma(2) \cong S_3$ (symmetric group of degree 3).*

Lecture 3

by Prof. Jürgen Wolfart

3 Continued from Lecture 1

3.1 Why Riemann Surfaces are Projective Algebraic Curves?

Sketch of ideas:

1. On a compact Riemann surface there are non-constant meromorphic functions $f : X \to \hat{\mathbb{C}}$. "$\Leftarrow$" by the theorem of Riemann-Roch.
2. All functions $g : X \to \hat{\mathbb{C}}$ constant on fibers of f are rational functions, in $\mathbb{C}(f)$. (Fiber means the points in $f^{-1}(q)$ for $q \in \hat{\mathbb{C}}$.)
3. Riemann-Roch: There are $h : X \to \hat{\mathbb{C}}$ separating points of the fibers of f for generic $q \in \hat{\mathbb{C}}$.
4. Consider elementary symmetric combinations

   $$\begin{aligned} S_1 &= h(p_1) + h(p_2) + \ldots + h(p_n), \text{ if } \{p_i\} = f^{-1}(q) \text{ outside ram. pts of } f, \\ S_2 &= h(p_1)h(p_2) + \ldots + h(p_{n-1})h(p_n) \\ &\vdots \\ S_n &= h(p_1) \cdot \ldots \cdot h(p_n). \end{aligned} \tag{1}$$

   These are meromorphic functions on X, constant on fibers of f.
5. There exists an algebraic equation between h and f, i.e.

   $$h^n - S_1 h^{n-1} + S_2 h^{n-2} - \ldots + (-1)^n S_n = 0, \tag{2}$$

   where the left side is in $\mathbb{C}(f)[h]$.
6. Algebra $\Rightarrow$ every meromorphic function on X lies in a field extension $\mathbb{C}(X)$ of $\mathbb{C}(f)$ of degree at most n.
7. Function fields determine equations $\Rightarrow$ use values of f and of h as coordinates for the curve equation 2 for the curve, resolve singularities pass to projective equation $\Rightarrow \square$.

4 Belyi functions

Theorem 4.1 *Let X be a compact Riemann surface, i.e. a smooth projective algebraic curve from $\mathbb{P}^N(\mathbb{C})$. X can be defined over $\bar{\mathbb{Q}}$ if and only if there exists meromorphic non-constant function $\beta : X \to \hat{\mathbb{C}}$ ramified above at most 3 points (critical values are without loss of generality 0,1 and ∞).*

There functions are called "Belyi functions" (Belyi 1980)

4.1 Existence of Belyi Functions: Simple Examples

1. $\hat{\mathbb{C}} = \mathbb{P}^1(\mathbb{C})$, $\beta : \hat{\mathbb{C}} \to \hat{\mathbb{C}} : z \mapsto z$ (unramified).

2. $\beta : \hat{\mathbb{C}} \to \hat{\mathbb{C}} : z \mapsto z^n$ is ramified in $z = 0$ and $z = \infty$.

3. Recall Tchebychev polynomials

$$\begin{aligned} T_0(z) &\equiv 1, \\ T_1(z) &= z, \\ T_2(z) &= 2z^2 - 1 \\ &\vdots \\ T_{n+1}(z) &= 2zT_n(z) - T_{n-1}(z) \end{aligned}$$

Now $\cos n\vartheta =: T_n(\cos\vartheta)$ with properties $T_n : [-1,1] \to [-1,1]$, $\deg T_n = n$, T_n has simple zeros in points $\cos \frac{2k-1}{2n}\pi$, where $k = 1, \ldots, n$ and double ± 1 in between. Also simple ± 1 values at points ± 1. Now the square T_n^2 has double zeros, double 1-values in between, simple 1-values at ± 1. Therefore T_n^2 (for $n > 0$) is a Belyi function.

$$\#\text{ramification points in } \mathbb{C} \quad = \quad \#\text{zeros of } (T_n^2)' \quad = \quad 2n - 1.$$

The picture of $\beta^{-1}([0,1])$ is $\cdots$ —— $\bullet$ —— $\circ$ —— $\cdots$ ending the both sides with $\bullet$ if the zeros of β are shown as $\circ$ and zeros of $\beta - 1$ as $\bullet$.

4. $X = F_n : x^n + y^n = z^n$. Then for example $\beta : F_n \to \hat{\mathbb{C}} : [x, y, z] \mapsto \frac{x^n}{z^n}$. On the affine part $z = 1$, $\beta : (x, y) \mapsto x^n$, $\deg\beta = n^2$. Less than n^2 points in $\beta^{-1}(x^n)$ occur in

   - points with $x^n = 0 \Rightarrow y = \zeta_n^2$ (n points with $\beta(x, y) = 0$, ramification order is n),
   - points with $x^n = 1 \Rightarrow y = 0$, $\beta : (x, y) = (\zeta_n^k, 0) \mapsto 1$, ram. order is n.

- $z = 0$, consider $\frac{1}{\beta} = \frac{z^n}{x^n}$: take $x = 1$, gives n zeros, all of $\text{mult}_p \beta = n$.

Therefore β is a Belyi function.

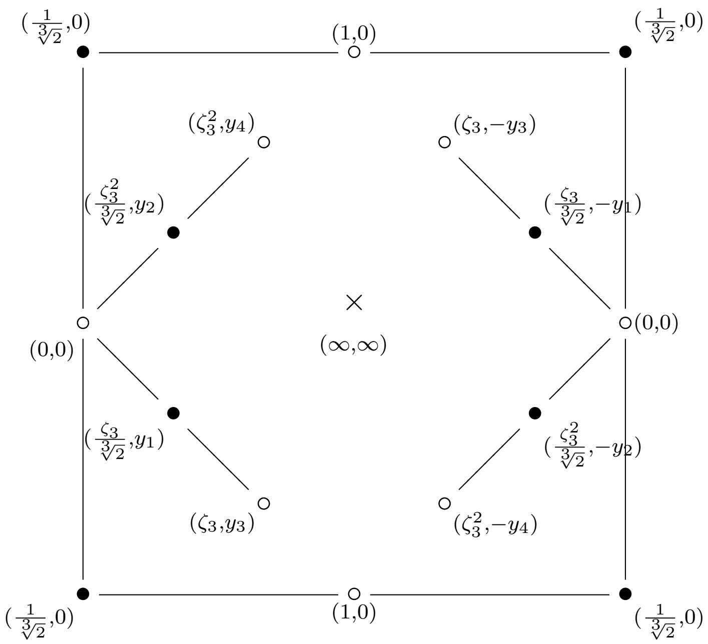
A surjective Belyi function of a compact Riemann surface $\beta : X \to \hat{\mathbb{C}}$ induces a natural triangulation by $\beta^{-1}(\hat{\mathbb{R}})$ where the preimage $\beta^{-1}(\underset{0}{\circ} \text{———} \overset{1}{\bullet})$ divides X in simply connected cells. It gives a bipartite graph embedded in X, which is called "dessin d'enfants" (by Grothendieck).

If β is a Belyi function, then also $\frac{1}{\beta}$, $1 - \beta$, $1 - \frac{1}{\beta}$, $\frac{1}{1-\beta}$, $\frac{\beta}{\beta-1}$ are Belyi functions. These permute the critical values $0, 1, \infty$.

If β is a Belyi function, then also is $4\beta(1-\beta)$: that's because $\infty \mapsto \infty$, $0 \mapsto 0$, $1 \mapsto 0$, $\frac{1}{2} \mapsto 1$. Also $\beta \mapsto 4\beta(1-\beta)$ from $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$ is a Belyi function. This last action induces a new bipartite graph, which can be reduced to simpler one-colour one. This corresponds to the theory of "maps".

4.2 Another Example

For the construction of Belyi functions $y^2 = x(x-1)(x-\frac{1}{\sqrt[3]{2}})$ elliptic function defined $/\bar{\mathbb{Q}}$. Start with $(x, y) \mapsto x$, study ramification points: this mapping is ramified in $(\infty, \infty), (0, 0), (1, 0), (\frac{1}{\sqrt[3]{2}}, 0)$. The preimage of the unit interval in β is of following shape:



Now

$$\begin{aligned}(x,y) \mapsto x \mapsto x^3 &\mapsto 4x^3(1-x^3)\\ \infty &\mapsto \infty\\ 0 &\mapsto 0\\ 1 &\mapsto 1\\ \frac{1}{\sqrt[3]{2}} &\mapsto \frac{1}{2}.\end{aligned}$$

This step (using polynomials sending algebraic critical values) may induce new ramifications, here $x \mapsto x^3$ ramified in $x = 0$ and $x = \infty$, so the composite $(x,y) \mapsto x^3$ is ramifield above $0, 1, \infty, \frac{1}{2}$. The composite map will be a Belyi function sending

$$\begin{aligned}(\infty,\infty) &\mapsto \infty \qquad \text{(pole of order 12)}\\ (0,0) &\mapsto 0 \qquad \text{(multiplicity 6)}\\ (1,0) &\mapsto 0 \qquad \text{(multiplicity 2)}\\ (\zeta_3^k, \pm y_k) &\mapsto 0\\ (\frac{1}{\sqrt[3]{2}}, 0) &\mapsto 1 \qquad \text{(multiplicity 4).}\end{aligned}$$

Belyi algorithm to construct β systematically: Take an equation defined $/\bar{\mathbb{Q}}$ some function $X \to \hat{\mathbb{C}}$, ramified above $\alpha_1, \ldots, \alpha_n \in \bar{\mathbb{Q}}$. Combine with a polynomial $p : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ sending $\alpha_1, \ldots, \alpha_n \to \mathbb{Q}$; if new ramifications arise, repeat the procedure... All critical points $\subset \mathbb{Q}$, suppose $0, 1, \infty \subset$ "crit. points". For example if $0 < \frac{m}{n+m} < 1$ is a critical point, apply $z \mapsto \frac{(m+n)^{m+n}}{m^n n^n} z^n(1-z)^n$. Then

$$\begin{aligned}0 &\mapsto 0\\ 1 &\mapsto 0\\ \infty &\mapsto \infty\\ \frac{m}{m+n} &\mapsto 1.\end{aligned}$$

Only ramification occurs in $0, 1, \frac{m}{n+m}, \infty$.

Exercise 4.2 (continued from 2.) *Find a Belyi function and a nice dessin picture for $y^2 = x^n - 1$, $n > 3$.*

Exercise 4.3 *Find a Belyi function and a dessin for the elliptic curve*

$$y^2 = x(x-1)(x - \frac{\zeta_3^{\pm 1}}{\sqrt[3]{2}}).$$

Lecture 4

by Prof. Gareth Jones

5 Continued from Lecture 2

5.1 More on Tori

Recall the correspondence between the isomorphism classes of elliptic curves and the orbits of Γ on $\mathbb{H}$.

We would like a "nice" function on $\mathbb{H}$, taking a single value on each orbit of Γ, and different values on different orbits. We can regard g_2, g_3 and $\Delta = g_2^3 - 27g_3^2$ as functions of $\tau \in \mathbb{H}$ by evaluating them for the lattice $\Lambda = \Lambda(1, \tau)$ with $\omega_2 = \tau$ and $\omega_1 = 1$, and with modulus τ. Difficulty: if replace Λ with a similar lattice $\Lambda' = \mu\Lambda$ then g_2, g_3 are multiplied by μ^{-4} and μ^{-6}, and Δ by μ^{-12}. But if we define

$$J(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)} = \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}$$

then the powers of μ cancel, so $J(\tau)$ depends only on the similarity class of Λ. Also, g_2, g_3 and hence J are independent of the basis of Λ. So J is invariant under the action of Γ on $\mathbb{H}$, i.e.

$$J(T(\tau)) = J(\tau)$$

for all $\tau \in \mathbb{H}$ and $T \in \Gamma$. J is the *elliptic modular function* (but not an elliptic function!). J is holomorphic on $\mathbb{H}$, and it induces a bijection between the orbits of Γ on $\mathbb{H}$ and complex numbers, i.e. $\Gamma\backslash\mathbb{H} \leftrightarrow \mathbb{C}$.

Exercise 5.1 *Evaluate $J(\tau)$ at $\tau = i$ and $\tau = \omega = e^{2\pi i/3}$ and find the corresponding elliptic curves.*

5.2 Alternative Approach to Finding a "Nice" Function

Put each elliptic curve E into Legendre form

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

where $\lambda \in \mathbb{C}\backslash\{0, 1\}$ and regard λ as a function of the modulus τ corresponding to E. The difficulty here is that the Legendre form for E is not quite unique. This is because there are 6 ways of sending two of the three roots of $p(x)$ to 0 and 1, with the third going to λ, by an affine transformation.

For instance, if we replace x with $1-x$ (transposing the roots 0 and 1) the right-hand side of the Legendre equation becomes

$$(1-x)(-x)(1-x-\lambda) = -x(x-1)(x-(1-\lambda)).$$

If we also replace y with iy the left-hand side becomes $-y^2$, so we have an isomorphic elliptic curve with Legendre form

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

Thus λ is replaced with $1-\lambda$. Another substitution (find it!) replaces λ with $\frac{1}{\lambda}$. These two substitutions generate a group isomorphic to S_3 (corresponding to permuting the three roots e_1, e_2 and e_3 of $p(x)$), and the six permutations give rise to six values

$$\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}.$$

One can define λ uniquely as a function of τ by noting that $\wp'(z) = 0$ at $z = \frac{\omega_1}{2}$ and $\frac{\omega_1+\omega_2}{2}$ (why?), so the differential equation

$$(\wp')^2 = p(\wp)$$

implies that the roots e_1, e_2 and e_3 of $p(x)$ are at $x = \wp(\frac{\omega_1}{2})$, $\wp(\frac{\omega_2}{2})$ and $\wp(\frac{\omega_1+\omega_2}{2})$.

An affine transformation $L : x \mapsto ax+b$ sending e_2 and e_3 to 0 and 1 respectively sends e_1 to

$$\lambda = \frac{e_1 - e_2}{e_3 - e_2}$$

and this depends only on τ. This function λ is holomorphic on $\mathbb{H}$, and is invariant under $\Gamma(2)$ (a normal subgroup of index 6 in Γ), but not under Γ. The 6 cosets of $\Gamma(2)$ in Γ give the 6 possible values for λ. These two functions are related by:

$$J(\tau) = \frac{4(1-\lambda(\tau)+\lambda(\tau)^2)^3}{27\lambda(\tau)^2(1-\lambda(\tau))^2}$$

Thus six values of λ correspond to each value of J. Then

$$\beta(x) = \frac{4(1-x+x^2)^3}{27x^2(1-x)^2}$$

is a Belyi function. It has triple zeros of β at $e^{\pm 2\pi i/6} (= \zeta_6^{\pm 1})$, double zeros of $\beta - 1$ at $-1, \frac{1}{2}, 2$, and double poles of β at $0, 1, \infty$.

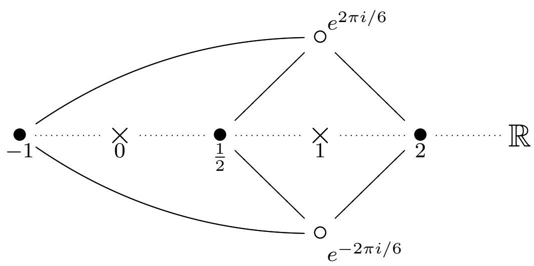
6 Embeddings of Graphs, Maps and Hypermaps

Graph $\mathcal{G} = (V, E)$ (vertices and edges), connected, finite (relax this later), allow loops $\bigcirc\!\bullet$ and multiple edges $\bullet\!\!\equiv\!\!\bullet$. Map $\mathcal{M} : \mathcal{G} \hookrightarrow X$, X is a surface, connected, compact, without boundary, and oriented (chosen orientation counter-clockwise). The faces (connected components of $X \backslash \mathcal{G}$) must be simply-connected, i.e. homeomorphic to an open disc. Examples: Platonic solids on $X = S^2$.

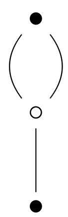
Assume that $\mathcal{G}$ is bipartite, i.e. we can colour the vertices black and white so that each edge joins a black vertex to a white vertex $\circ\!-\!\!\!-\!\!\!-\!\bullet$ (possible iff each circuit in $\mathcal{G}$ has even length). Call these *bipartite maps* (=dessins d'enfants) denoted by $\mathcal{B}$.

6.1 Examples of Bipartite Maps

1. The dessin $\mathcal{B}_1$ corresponding to β is

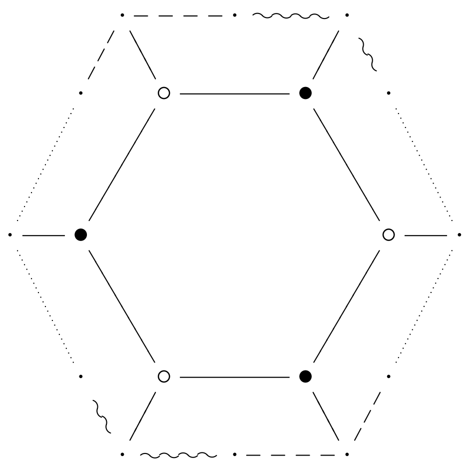


   Here $\times$ denotes a face-centre.

2. $\mathcal{B}_2 =$  Quotient of $\mathcal{B}_1$ by a half-turn about $\frac{1}{2}$.

3. Identify opposite edges of the hexagon to get a bipartite map $\mathcal{B}_3$ on a

torus.



Each black and white pair are joined by a single edge, so $\mathcal{G} = K_{3,3}$, the complete bipartite graph with 3 black and 3 white vertices.

Describe $\mathcal{B}$ algebraically: use the orientation of X to define two permutations x and y of the set E of edges. For each $e \in E$, ex and ey are the next edges around the incident black and white vertices, following the orientation of X. Warning: these are not generally automorphisms.

Black vertices $\longleftrightarrow$ cycles of x on E

White vertices $\longleftrightarrow$ cycles of y on E

Faces $\longleftrightarrow$ cycles of xy on E

The orders l, m, n of x, y, xy are the least common multiples of their cycle lengths. Call (l, m, n) *the type of* $\mathcal{B}$. E.g. $\mathcal{B}_1$ and $\mathcal{B}_2$ have type $(3, 2, 2)$, $\mathcal{B}_3$ has type $(3, 3, 3)$. The *monodromy group* of $\mathcal{B}$ is the subgroup $G = \langle x, y \rangle$ generated by x and y in the symmetric group $\mathrm{Sym}(E)$ of all permutations of E.

$\mathcal{G}$ is connected, so G acts transitively on E, so the action is equivalent to the action on the cosets Hg ($g \in G$) of a stabilizer $H = G_e$ ($e \in E$). Say G acts *regularly* if $G_e = 1$; this action is equivalent to G acting on itself by right multiplication.

In $\mathcal{B}_1$, $x^3 = y^2 = (xy)^2 = 1$, and these relations define the dihedral group D_3 of order 6, so G is a quotient of D_3. G is transitive on the 6 edges, so $|G : G_e| = 6$ (the index of the subgroup), so $G \cong D_3$ with $G_e = 1$. G acts regularly. In $\mathcal{B}_2$, $G \cong D_3$, but $|G_e| = 2$, so the action is not regular.

In $\mathcal{B}_3$, $G \cong C_3 \times C_3$ acting regularly. Here $x^3 = y^3 = 1$ and $xy = yx$.

6.2 More Definitions

Algebraic bipartite map: (G, x, y, E) where $G = \langle x, y \rangle$ is a permutation group acting transitively on a set E. Reconstruct a bipartite map $\mathcal{B}$ from (G, x, y, E):

$$\begin{aligned} \text{edges} &= \text{elements of } E \\ \text{black/white vertices} &= \text{cycles of } x \text{ and } y \\ \text{faces} &= \text{cycles of } xy \\ \text{Incidence} &= \text{containment in a cycle.} \end{aligned}$$

Exercise 6.1 *Take $x = (1, 2, \ldots, N)$ and $y = (1, 2)$ in S_N. Find $\mathcal{B}$ and G.*

An *automorphism* of $\mathcal{B}$ is a permutation of E commuting with x and y, or equivalently commuting with G. E.g. rotations for the example dessins $\mathcal{B}_1$ and $\mathcal{B}_3$, translations for $\mathcal{B}_3$, but only the identity for $\mathcal{B}_2$. The automorphisms form a group

$$\operatorname{Aut}\mathcal{B} = C(G) = C = \{\, c \in \operatorname{Sym}(E) \mid cg = gc \text{ for all } g \in G \,\},$$

the centraliser of G in $\operatorname{Sym}(E)$.

A permutation group is *semiregular* (acts freely) if each stabiliser is trivial.

$$\text{The group is} \left\{ \begin{array}{c} \text{semiregular} \\ \text{transitive} \\ \text{regular} \end{array} \right\} \text{ as } \left\{ \begin{array}{c} \text{at most} \\ \text{at least} \\ \text{exactly} \end{array} \right\} \begin{array}{c} \text{one group element} \\ \text{takes one point to another.} \end{array}$$

Thus regular $\Leftrightarrow$ transitive and semiregular.

Theorem 6.1 *Let G be any transitive group, and $C = C(G)$ its centraliser.*

(i) C acts semiregularly.

(ii) C acts regularly iff G does.

(iii) If C and G act regularly then $C \cong G$.

Proof.

(i) Let $c \in C$ fix e. Any e' has the form $e' = eg$ for some $g \in G$ by transitivity. Then $e'c = egc = ecg = eg = e'$, so $c = 1$.

(ii) Let C act regularly. Then C is transitive, so its centraliser is semiregular by (i) applied to C; but G commutes with C, so G is semiregular, and being transitive it must be regular.

Conversely, let G act regularly, so it is acting on itself by right-multiplication $\rho_g : e \mapsto eg$; then left-multiplication $\lambda_c : e \mapsto c^{-1}e$ commutes with right-multiplication ($c^{-1}(eg) = (c^{-1}e)g$), and acts transitively, so C is transitive, and C is semiregular by (i), so C is regular.

(iii) When C and G act regularly, then $\lambda_g \leftrightarrow \rho_g$ gives the isomorphism $C \cong G$.

□

A dessin $\mathcal{B}$ is *regular* if G (equivalently $\mathrm{Aut}\,\mathcal{B}$) is regular in E. From the last examples $\mathcal{B}_1$ and $\mathcal{B}_3$ are regular, $\mathcal{B}_2$ is not.

Exercise 6.2 *Show that $C \cong N_G(G_e)/G_e$ where $N_G(G_e)$ is the normaliser of G_e in G.*

Exercise 6.3 *If $\mathcal{B}$ is a regular dessin of type (l, m, n) with N edges, what is its genus? Are there finitely or infinitely many dessins of a given type and genus?*

Lecture 5

by Prof. Jürgen Wolfart

7 Uniformisation and Fuchsian Groups

Exercise 7.1 *How does the dessin change if the Belyi function β is replaced by $1-\beta$, $\frac{1}{\beta}$? How are the pole orders encoded in the dessin? Start by some dessin, how can you modify β such that every edge* $\bullet$ —— $\circ$ *is replaced by* $\bullet$ —— $\circ$ —— $\bullet$ —— $\circ$ *?*

7.1 Uniformisation

Theorem 7.1 *Let X be a connected manifold. There is always a "universal simply connected covering" $F : Y \to X$, where Y is a simply connected manifold with the following uniqueness property. Let F' be any other covering $Y' \to X$ and $p \in X, q \in Y$, $q' \in Y'$ s.t. $F(q) = p = F'(q')$ then there is a unique covering map $f : Y \to Y'$, such that $f(q) = q'$ making the diagram*

$$\begin{array}{ccc} Y & \overset{f}{\dashrightarrow} & Y' \\ & {\scriptstyle F}\searrow \quad \swarrow{\scriptstyle F'} & \\ & X & \end{array}$$

commute i.e. $F = F' \circ f$.

"Covering" means: $\forall p \in X \exists U = U(p)$ s.t. $F^{-1}U = \dot{\bigcup} V_n$ (disjoint union) where $F|_{V_n} : V_n \to U$ is a homeomorphism.

Proposition 7.2 *X is a Riemann surface $\Rightarrow$ Y is simply connected Riemann surface, F holomorphic and unramified.*

Contruction of Y and F is given by homotopy theory. As a set,

$$Y = \{ (p, [\gamma]) \,|\, p \in X, [\gamma] \in \pi_1(X, p) \}$$

(closed curves modulo homotopy, with starting point p). Define a topology, define F as projection, control properties, in particular simple connectedness.

Theorem 7.3 (Extended Riemann Mapping Theorem, Main Theorem of Uniformisation) *If Y is simply connected, Y is isomorphic to $\hat{\mathbb{C}}$, $\mathbb{C}$ or to $\mathbb{H} \cong \mathbb{D}$ (open unit disc).*

Theorem 7.4 *Every Riemann surface X is homeomorphic to some quotient space $G\backslash Y$ where Y is the universal covering space and G is the "covering group"* $\subset \operatorname{Aut} Y$ *consisting of all* $\gamma \in \operatorname{Aut} Y$ *with* $F \circ \gamma = F$ *permuting transitively the fibers of F.*

($\Leftarrow$ uniqueness part of theorem 7.1.) G acts without fixed points, it is torsion free, it acts discontinuously.

Here "discontinuously" (properly) means: $\forall q \in Y \exists V = V(q)$ s.t. $V \cap \gamma V = \emptyset$ except for finitely many $\gamma \in G$.

Proposition 7.5 *a)* $Y = \hat{\mathbb{C}}$, $\operatorname{Aut} \hat{\mathbb{C}} \cong \mathrm{PSL}_2(\mathbb{C})$

$$X = \hat{\mathbb{C}} \Leftarrow G = \{\mathrm{id}\} \Leftarrow \begin{cases} z \mapsto \frac{az+b}{cz+a} \\ \textit{have fixed points} \end{cases}$$

b) $Y = \hat{\mathbb{C}}$, $\operatorname{Aut} \mathbb{C} = \{\, z \mapsto az + b \,|\, a \in \mathbb{C}^*, b \in \mathbb{C} \,\}$

$$G \subset \{\, \textit{translations} \,\} \Leftarrow \textit{no fixed point iff } a = 1$$

It follows that G either $\cong \mathbb{Z}$ or a lattice Λ. Also $X = \mathbb{C}$ or $\mathbb{Z}\backslash\mathbb{C}$ or $\Lambda\backslash\mathbb{C}$, a torus (elliptic curve). For example in the case $X = \mathbb{Z}\backslash\mathbb{C}$

$$F(z) = \exp z, F : \mathbb{C} \to \mathbb{C}^* = \mathbb{C} - \{0\}$$

and $\exp(z + 2\pi i k) = \exp(z)$ *for all* $k \in \mathbb{Z}$.

c) $Y = \mathbb{H} \cong \mathbb{D}$ *in all other cases, in particular for all compact Riemann surfaces X with $g > 1$. Here* $G \subset \operatorname{Aut} \mathbb{H}$ *and it is called "Fuchsian group".*

In general, discontinuous groups may have fixed points, i.e. points $p \in Y$ with a finite

$$G_p := \{\, \gamma \in G \,|\, \gamma(p) = p \neq \{\mathrm{id}\} \,\}.$$

Theorem 7.6 *For a discontinuous group G acting on $Y = \hat{\mathbb{C}}, \mathbb{C}, \mathbb{H}$ the following holds:*

a) for $p \in G, \gamma(p) = p$ there exists a local chart such that diagram

$$\begin{array}{ccc} U(p) & \xrightarrow{\gamma} & U(p) \\ \downarrow z & & \downarrow z \\ \mathbb{D} & \xrightarrow[z \mapsto \zeta_n^k z]{} & \mathbb{D} \end{array}$$

commutes and $z \mapsto z^n : \mathbb{D} \to \mathbb{D}$ *induces the quotient map* $U \to G_p\backslash U$ *for* $G_p = \langle \gamma \rangle$.

b) all stabilizing subgroups are finite cyclic

c) fixed points of G form a discrete subset

d) $G\backslash Y$ has a holomorphic structure as a Riemann surface s.t. the quotient map $Y \to G\backslash Y : z \mapsto Gz$ is holomorphic, ramified of multiplicity n in fixed points of order n.

For now $Y = \mathbb{H}$ and G discontinuous $\subset \operatorname{Aut}\mathbb{H}$.

Theorem 7.7 $\operatorname{Aut}\mathbb{H} = \mathrm{PSL}_2(\mathbb{R})$*, the group of orientation preserving hyperbolic motions.*

It is clear that $\operatorname{Aut}\mathbb{H} \supseteq \mathrm{PSL}_2\mathbb{R}$, acting (simply) transitively on {points} and {lines}, by conjugation with a Cayley map pass to $\gamma \in \operatorname{Aut}\mathbb{H}$ by combination with some $\mu \in \mathrm{PSL}_2\mathbb{R}$, suppose $\gamma(i) = i$, suppose $\gamma \in \operatorname{Aut}\mathbb{D}$, and $\gamma(0) = 0$. Lemma (Schwarz): If holomorphic $\delta : \mathbb{D} \to \mathbb{D}$ has $\delta(0) = 0$, then

$$|\delta(z)| \leq |z| \ \forall z \in \mathbb{D} \text{ with "="} \text{ iff}$$

$$\delta(z) = \lambda z \text{ with } |\lambda| = 1.$$

Hence, δ and its inverse mapping satisfy both $|\delta^{\pm 1}(z)| \leq |z|$, therefore $\delta(z) = \lambda z$ is a hyperbolic motion $\Rightarrow \square$.

Theorem 7.8 $G \subset \mathrm{PSL}_2(\mathbb{R})$ *acts discontinuously on $\mathbb{H}$, iff G is a discrete subgroup of* $\mathrm{PSL}_2(\mathbb{R})$.

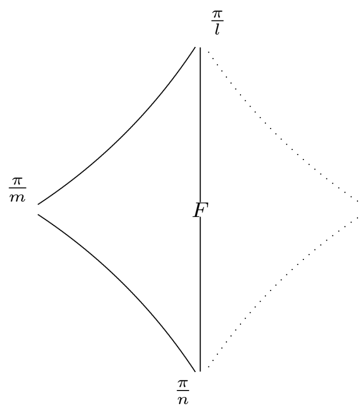
7.2 Fuchsian Groups

There are two methods for the contruction of Fuchsian groups:

- Arithmetic: Construct discrete groups of $\mathrm{PSL}_2\mathbb{R}$ by number theory, e.g. $\Gamma = \mathrm{PSL}_2\mathbb{Z}$ (modular group).
- Geometry (Poincaré): Start with a "suitable" hyperbolic polygon F (later serving as the fundamental domain for G), and generate G by side-pairing transformations.

Example: the "triangle groups" $\langle l, m, n\rangle$ (drawing in $\mathbb{D}$ instead of $\mathbb{H}$), $l, m, n \in \mathbb{N}\backslash\{0\}$ or ∞ with

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



For example $\langle 2, 3, \infty \rangle = \mathrm{PSL}_2\,\mathbb{Z}$ and

$$\langle \infty, \infty, \infty \rangle = \Gamma(2) = \{\, \gamma \in \Gamma = \mathrm{PSL}_2\,\mathbb{Z} \,|\, \gamma \equiv E \mod 2 \,\}$$

Also $\Gamma/\Gamma(2) = \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Fact: there are 85 triangle groups which are "arithmetically defined" (Takeuchi $\sim$ 1970).

$$\gamma_0^l = 1 = \gamma_1^m = \gamma_\infty^n = \gamma_\infty \gamma_1 \gamma_0.$$

Theorem 7.9 *a) These triangle groups $\langle l, m, n \rangle = \langle \gamma_0, \gamma_1, \gamma_\infty \rangle$ are discontinuous on $\mathbb{H}$ with F as "fundamental region" (i.e. F open and $F \cap \gamma F = \emptyset \forall \gamma \in G - \{1\}$ and $\bigcup_{\gamma \in G} \gamma \bar{F} = \mathbb{H}$) (hard work!)*

$\vdots$

d) There is a meromorphic G-invariant function $j : \mathbb{H} \to \hat{\mathbb{C}}$ ($j(\gamma(z)) = j(z) \forall z \in \mathbb{H}$ and $\gamma \in G$) mapping the two parts of F biholomorphicaly onto $\mathbb{H}$ and $-\mathbb{H}$, border edges onto $\hat{\mathbb{R}}$ and the vertices onto $0, 1, \infty$, with multiplicities l, m, n.

Exercise 7.2 *Let G be a (possibly ramified) covering group of X acting discontinuously on Y with $X \cong G\backslash Y$ and let $N \lhd G$ normal subgroup, $X' := N\backslash Y$. Show that G/N acts as group of automorphisms on X' s.t.*

$$(G/N)\backslash X' \cong X.$$

Give an example of a Riemann surface with an automorphism group $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$, $N \in \mathbb{N}\backslash\{0\}$.

Lecture 6

by Prof. Gareth Jones

8 Continued from Lecture 4

8.1 More on Dessins

Isomorphism of dessins: If $\mathcal{B} = (G, x, y, E)$ and $\mathcal{B}' = (G', x', y', E')$ are bipartite maps (=dessins), then an isomorphism $i : \mathcal{B} \to \mathcal{B}'$ consists of a group-isomorphism $\theta : G \to G'$ sending x to x', y to y', and a bijection $\phi : E \to E'$ compatible with θ, i.e. $\phi(eg) = \phi(e)\theta(g)$ for all $e \in E$ and for all $g \in G$:

$$\begin{array}{ccc} E \times G & \longrightarrow & E \\ \phi \downarrow \ \downarrow \theta & & \downarrow \phi \\ E' \times G' & \longrightarrow & E' \end{array}$$

Theorem 8.1 *Every dessin $\mathcal{B}$ is isomorphic to $A\backslash\tilde{\mathcal{B}}$ for some regular dessin $\tilde{\mathcal{B}}$ and subgroup $A \subseteq \operatorname{Aut}\tilde{\mathcal{B}}$.*

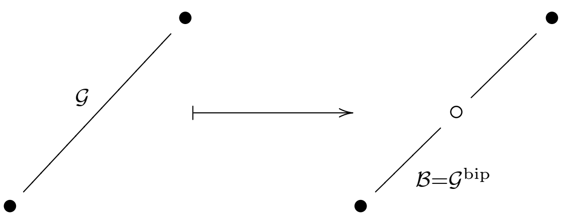
Proof. Take G to be the monodromy group of $\mathcal{B}$, and take $\tilde{\mathcal{B}}$ to be the dessin corresponding to the regular representation of G, so $\tilde{\mathcal{B}}$ is regular (Theorem 2.1). Take $A = \{\, \lambda_g \mid g \in G_e \,\}$ for some $e \in E$; then orbits of A on E are just cosets $G_e g$ ($g \in G$), so $A\backslash\tilde{\mathcal{B}} \cong \mathcal{B}$. □

Call $\tilde{\mathcal{B}}$ the canonical regular cover of $\mathcal{B}$.

Exercise 8.1 *Let $\mathcal{B}$ consist of a path of N edges, alternately white, black, white, etc.* $\bullet$ —— $\circ$ —— $\bullet$ —— $\circ$ —— $\cdots$ *Find G, C, $\tilde{\mathcal{B}}$ and A for this dessin.*

What about embeddings of graphs $\mathcal{G}$ which are not necessarily bipartite, e.g. the tetrahedron or octahedron?

Convert $\mathcal{G}$ into a bipartite graph by regarding the vertices of $\mathcal{G}$ as black vertices, and placing a white vertex in each edge of $\mathcal{G}$.



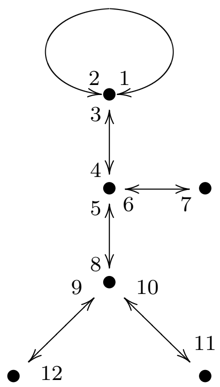
This gives a bipartite graph $\mathcal{G}^{\text{bip}}$. Any embedding of $\mathcal{G}$ in a surface gives a bipartite map $\mathcal{B}$. The edges of $\mathcal{B}$ correspond to the directed edges (=darts) of $\mathcal{G}$. The rotations x and y of the set E of edges of $\mathcal{B}$ correspond to rotations x and y of the set Ω of darts of $\mathcal{G}$. So x rotates darts α around their incident vertices following the orientation of the surface amd y reverses the direction of each dart, so $y^2 = 1$.

We can define an algebraic map (not necessarily bipartite) to be a 4-tuple (G, x, y, Ω) where $G = \langle x, y\rangle$ is a transitive permutation group acting on Ω, with $y^2 = 1$. As before, we can identify the vertices, edges and faces with cycles of x, y and xy on Ω, incidence given by non-empty intersection.

The algebraic theory is similar to that for bipartite maps.

8.2 Example

$\mathcal{M}$, Monsieur Mathieu:



Here $|\Omega| = 12$. So

$$x = (1\,2\,3)(4\,5\,6)(7)(8\,9\,10)(11)(12)$$

and

$$y = (1\,2)(3\,4)(5\,8)(6\,7)(9\,12)(10\,11).$$

Now $G = \langle x, y\rangle$. GAP $\Rightarrow |G| = 95040, G \cong M_{12}$.

Finite simple groups (classified $\sim$ 1980): C_p, A_n, where $(n \geq 5)$, groups of Lie type, e.g. $\mathrm{PSL}_2(\mathbb{F}_q)$, 26 sporadic groups, e.g. Mathieu group M_n where $n = 11, 12, 22, 23, 24$. In this example, $G_\alpha \cong M_{11}$ for $\alpha \in \Omega$. $\mathcal{M}$ has genus 0, and type $(3, 2, 11)$. The corresponding bipartite map $\mathcal{B}$ has canonical regular cover $\tilde{\mathcal{B}}$ of type $(3, 2, 11)$ and genus $g = 3601$ (see Exercise 2.3), $\mathrm{Aut}\,\tilde{\mathcal{B}} \cong M_{12}$.

By Belyi's theorem $\tilde{\mathcal{B}}$ corresponds to an algebraic curve defined over an algebraic number field. The field of definition is $\mathbb{Q}(\sqrt{-11})$. This has Galois group isomorphic to C_2, generated by complex conjugation. Applying this to the coefficients of the algebraic curve and the Belyi function, we get the mirror image of $\mathcal{M}$, $\bar{\mathcal{M}}$. Later we will see more interesting and less obvious actions of Galois groups of maps.

9 Galois Theory

9.1 Basic Galois Theory

Every field F has an algebraic closure $\bar{F}$, a minimal extension field of F over which every $f \in F[x]$ splits into linear factors. This field $\bar{F}$ is:

- unique up to isomorphisms fixing F,
- an algebraic extension of F, i.e. every $\alpha \in \bar{F}$ is a root of some non-zero $f \in F[x]$, or equivalently $|F(\alpha) : F| < \infty$.

Important case:

$$\bar{\mathbb{Q}} := \{\, \alpha \in \mathbb{C} \mid f(\alpha) = 0 \text{ for some non-zero } f \in \mathbb{Q}[x] \,\}$$

the field of algebraic numbers. Motivation: Belyi's Theorem.

A field extension $K \supseteq F$ is *normal* (or *Galois*) if every embedding $e : K \hookrightarrow \bar{F}$ (fixing F) satisfies $e(K) = K$.

(Strictly speaking, "Galois = normal and separable", where "separable" means that irreducible polynomials don't have repeated roots; all fields of characteristic 0 are separable, so we'll ignore this point by assuming that $\mathrm{char}\, F = 0$ for all fields F mentioned.)

Example 9.1 $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_n)$ *the n^{th} cyclotomic field,* $\zeta_n = \exp(\frac{2\pi i}{n})$. *Any embedding* $e : \mathcal{K} \hookrightarrow \bar{\mathbb{Q}}$ *sends* ζ_n *to some* $\zeta_n^j \in K$, *so* $e(K) = K$. *This is a Galois extension.*

Example 9.2 $F = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, $\alpha = 2^{1/3} \in \mathbb{R}$. *There is an embedding* $e : K \hookrightarrow \bar{\mathbb{Q}}$ *sending* α *to* $\alpha\zeta_3 \notin K$. *This extension is not Galois.*

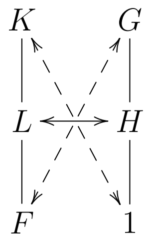
Theorem 9.1 $K \supseteq F$ *is a finite Galois extension if and only if* K *is the splitting field of some* $f \in F[x]$.

The Galois group $\mathrm{Gal}\, K$ of a field K is the group of all field automorphisms of K. If $H \leq \mathrm{Gal}\, K$, then $\mathrm{fix}\, H$ is the subfield fixed pointwise by H. If $F \subseteq K$ then $\mathrm{Gal}\, K/F$ is the subgroup of $\mathrm{Gal}\, K$ fixing F pointwise.

In Theorem 9.1 $G = \mathrm{Gal}\, K/F$ permutes the roots of f faithfully so we can embed G in S_n, $n = \deg(f) =$"no. of roots of f", and $|G| = |K : F|$.

Example 9.3 *$K = \mathbb{Q}(\alpha, \zeta_3)$, $\alpha = 2^{1/3} \in \mathbb{R}$ as before, $F = \mathbb{Q}$. K is the splitting field of $f(x) = x^3 - 2$. Degree is $|K : F| = 6$, basis $1, \alpha, \alpha^2, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3$. f has three roots $\alpha_j = \alpha\zeta_3^j$ $(j = 0, 1, 2)$ permuted faithfully by $G = \operatorname{Gal} K/F$, so $G \hookrightarrow S_3$. Since $|G| = |K : F| = 6$ and $|S_3| = 6$, $G \cong S_3$.*

Theorem 9.2 (Fundamental Theorem of Galois Theory) *Let $K \supseteq F$ be a finite Galois extension, $G = \operatorname{Gal} K/F$. There is an order-reversing bijection $L \mapsto H = \operatorname{Gal} K/L$ between fields L such that $K \supseteq L \supseteq F$, and subgroups $H \leq G$. The inverse sends each H to $L = \operatorname{fix} H$. We have $|K : L| = |H|$ and $|L : F| = |G : H|$. $L \supseteq F$ is Galois iff $H \trianglelefteq G$, in which case $\operatorname{Gal} L/F \cong G/H$.*



In example 1,

$$\operatorname{Gal} \mathbb{Q}(\zeta_n)/\mathbb{Q} = \{\, \theta_j : \zeta_n \mapsto \zeta_n^j \mid (j, n) = 1 \,\} \cong U_n = \mathbb{Z}_n^*,$$

the group of units $\mod n$. This is abelian, so all subfields of $\mathbb{Q}(\zeta_n)$ are Galois over $\mathbb{Q}$.

In example 3, $S_3 \rhd A_3 \cong C_3$, and the field L corresponding to $H = A_3$ is the Galois extension $\mathbb{Q}(\zeta_3)$ of $\mathbb{Q}$. The subfield $L = \mathbb{Q}(\alpha)$ corresponds to a non-normal subgroup of G

Exercise 9.1 *Find the splitting field K of $x^n - 2$, describe the Galois group of K, and find the subgroups fixing $2^{1/n} \in \mathbb{R}$ and ζ_n.*

9.2 The Absolute Galois Group

The *absolute Galois group* of a field F is $\operatorname{Gal} \bar{F}/F$. The *absolute Galois group* is $\operatorname{Gal} \bar{\mathbb{Q}}/\mathbb{Q}$, denoted by $\underline{\underline{G}}$. Let $\mathcal{K}$ denote the set of all finite Galois extensions K of $\mathbb{Q}$, and let $G_K = \operatorname{Gal} K/\mathbb{Q}$, a finite group of order $|K : \mathbb{Q}|$.

Theorem 9.3 *(i) $\bar{\mathbb{Q}}$ is the union of all the fields $K \in \mathcal{K}$*

(ii) Each $K \in \mathcal{K}$ is invariant under $\underline{\underline{G}}$.

Proof.

(i) Each $K \in \mathcal{K}$ is a finite extension of $\mathbb{Q}$, so if $\alpha \in K$ then $|\mathbb{Q}(\alpha) : \mathbb{Q}| \leq |K : Q| < \infty$, so $\alpha \in \bar{\mathbb{Q}}$. Conversely, if $\alpha \in \bar{\mathbb{Q}}$ then $f(\alpha) = 0$ for some non-zero $f \in \mathbb{Q}[x]$, and $\alpha \in K =$"splitting field of f".

(ii) Follows by definition of "Galois".

□

Thus each $g \in \underline{\underline{G}}$ is uniquely determined by its restrictions $g_K \in G_K$ to the fields $K \in \mathcal{K}$. If $K \supseteq L$ where $K, L \in \mathcal{K}$ then L is invariant under G_K so there is a restriction homomorphism $\rho_{K,L} : G_K \to G_L$ sending g_K to g_L, i.e.

$$\rho_{K,L}(g_K) = g_L$$

whenever $K \supseteq L$. Conversely if we have elements $g_K \in G_K$ for each $K \in \mathcal{K}$, with $\rho_{K,L}(g_K) = g_L$ whenever $K \supseteq L$, we can define $g \in \underline{\underline{G}}$ by $g(\alpha) = g_K(\alpha)$ where $\alpha \in K \in \mathcal{K}$. (Check independence of K.) We can therefore identify $\underline{\underline{G}} = \operatorname{Gal} \bar{\mathbb{Q}}$ with the group

$$\{\, (g_K) \in \Pi := \Pi_{K \in \mathcal{K}} G_K \mid \rho_{K,L}(g_K) = g_L \text{ whenever } K \supseteq L \text{ in } \mathcal{K} \,\},$$

the subgroup of the cartesian product Π consisting of elements whose coordinates are compatible with the $\rho_{K,L}$'s.

This is the projective limit $\varprojlim G_K$ of the finite groups G_K and homomorphisms $\rho_{K,L}$, a profinite group.

Exercise 9.2 *Show that* $\bigcup_{n \geq 1} \mathbb{Q}(\zeta_n)$ *is a subfield of* $\bar{\mathbb{Q}}$*, and describe its Galois group.*

Exercise 9.3 *What are the cardinalities of* $\bar{\mathbb{Q}}$ *and* $\underline{\underline{G}}$*?*

To get a bijection between fields and groups, we need some topology:

Put the discrete topology on each G_K ($K \in \mathcal{K}$), so all subsets are open and closed. This induces a product topology on Π, the weakest such that the projections $\Pi \to G_K$ are continuous. $\underline{\underline{G}} \hookrightarrow \Pi$, so $\underline{\underline{G}}$ inherits a topology from Π, the *Krull topology.* (Intuitively, elements of $\underline{\underline{G}}$ are "close together" if they agree on a large subfield of $\bar{\mathbb{Q}}$.) Multiplication and inversion are continuous in each G_K, and hence also in Π and $\underline{\underline{G}}$, so these are topological groups.

Exercise 9.4 *Show that* $\underline{\underline{G}}$ *is a closed subgroup of* Π*, and both* Π *and* $\underline{\underline{G}}$ *are compact Hausdorff spaces.*

Warning: $\underline{\underline{G}}$ is topologically unpleasant: homeomorphic to a Cantor set.

The Fundamental Theorem (9.1) extends to the extension $\bar{\mathbb{Q}} \supseteq \mathbb{Q}$ provided we restrict the bijection to the closed subgroups of $\underline{\underline{G}}$, *not* all subgroups.

Exercise 9.5 *In any topological group, every open subgroup is closed, and every closed subgroup of finite index is open.*

Lecture 7

by Prof. Jürgen Wolfart

10 Continued from Lecture 5

Theorem 10.1 *a) Fuchsian triangle groups $\mathcal{G}$ are discontinuous on $\mathbb{H}$ with F as "fundamental domain".*

b) $\mathcal{G}$ is generated by γ_0, γ_1, γ_∞ (by any two of them)

c) $\mathcal{G}$ is presented by $\langle \gamma_0, \gamma_1, \gamma_\infty \,|\, \gamma_0^l = \gamma_1^m = \gamma_\infty^n = 1 = \gamma_\infty\gamma_1\gamma_0 \rangle$

d) There is a meromorphic $\mathcal{G}$-invariant ($\mathcal{G}$-"automorphic") function $j : \mathbb{H} \to \hat{\mathbb{C}}$ mapping the two (open) parts of F onto $\mathbb{H}$ and $-\mathbb{H}$, border edges on $\hat{\mathbb{R}}$, vertices to $0, 1, \infty$ with ramification multiplicities l, m, n.

e) j provides an identification of $\mathcal{G}\backslash\mathbb{H}$ with $\hat{\mathbb{C}}$ (in case that l, m, n finite)

Remark: In case of cusps, omit these points! I.e. for $\mathcal{G} = \langle \infty, \infty, \infty \rangle \cong \Gamma(2)$, $j : \mathbb{H} \to \hat{\mathbb{C}} - \{ 0, 1, \infty \}$ universal covering map!

Exercise 10.1 *Show that $\langle 2, 2, n \rangle = \mathcal{G}$ is a "spherical" trianglegroup and*

$$j(z) = \frac{1}{4}\left(2 + z^n + \frac{1}{z^n}\right).$$

10.1 Remarks

Triangle groups are (the only) "rigid" Fuchsian groups, i.e. uniquely determined by their presentation up to conjugation in $\mathrm{PSL}_2(\mathbb{R})$.

There is a bijection between $\{ \mathcal{G} -$ automorphic functions on $\mathbb{H} \}$ and $\{$ meromorphic functions on $\mathcal{G}\backslash\mathbb{H} \}$.

10.2 More General Facts about Fuchsian Groups

Theorem 10.2 *a) Let $p \in \mathbb{H}$ be a non-fixed point for $\mathcal{G}$ and let d be the hyperbolic distance on $\mathbb{H}$. Then (Dirichlet)*

$$F := \{ z \in \mathbb{H} \,|\, d(p, z) < d(\gamma(p), z) \ \forall \gamma \in \mathcal{G} - \{\mathrm{id}\} \} \neq \emptyset$$

is a fundamental domain for $\mathcal{G}$ bounded by side-edges

$$\begin{aligned} l_\sigma := \{ z \in \mathbb{H} \,|\, & d(p, z) = d(\sigma(p), z), \ \sigma \in \mathcal{G} - \{\mathrm{id}\} \\ & d(p, z) \leq d(z, \gamma(z)) \ \forall \gamma \in \mathcal{G} - \{\mathrm{id}, \sigma\} \}. \end{aligned}$$

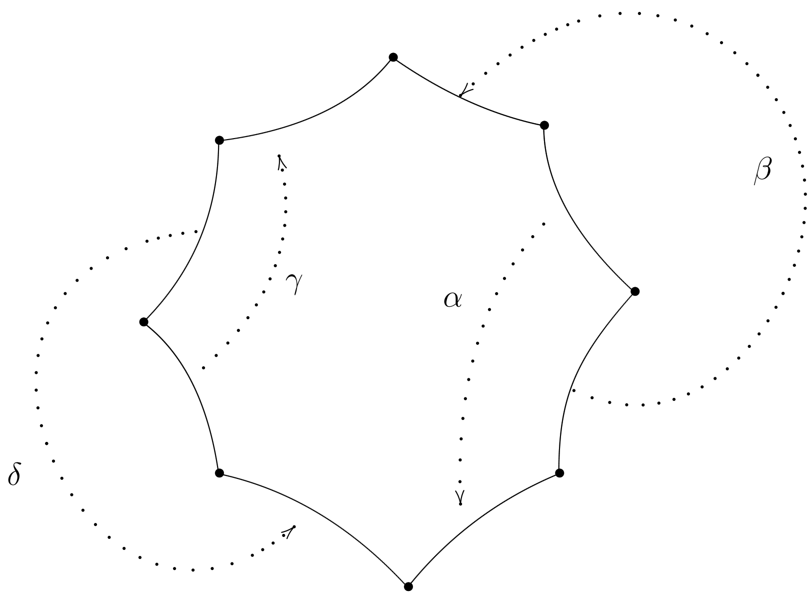
b) For all compact $C \subset \mathbb{H}$, $l_\sigma \cap C \neq \emptyset$ for finitely many $\sigma \in \mathcal{G}$ only. $\bar{F}$ compact $\Rightarrow F$ is a finite convex polygon bounded by finitely many side edges, $\bar{F}$ compact $\subset \mathbb{H} \Leftrightarrow X = \mathcal{G}\backslash\mathbb{H}$ is a compact Riemann surface.

c) $\mathcal{G}$ is generated (finitely in the "cocompact" case) by "side-pairing" transformations $\sigma \in \mathcal{G}$ sending $l_{\sigma^{-1}}$ to l_σ, sending F to a neighbour σF with common side l_σ.

d) Loops around vertices of $F \rightsquigarrow$ relations between these generators $\rightsquigarrow$ presentation of $\mathcal{G}$.

e) (Poincaré) If F is an $\mathbb{H}$-polygon with side-pairings and some condition on the angles guaranteeing that locally around F, the images γF have no overlapping $\Rightarrow$ the plane is covered by $\mathcal{G}F$ without overlappings and with $\mathbb{H} = \mathcal{G}\bar{F}$, $\mathcal{G} = \langle$ side-pairings $\rangle$.

Example (in $\mathbb{D}$): Let F be an 8-sided polygon with side-pairings as indicated below,



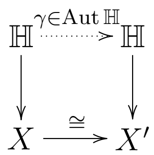
$\sum$ all angles $= 2\pi \Rightarrow$

$$\mathcal{G} = \langle\, \alpha, \beta, \gamma, \delta \,|\, \alpha\beta\alpha^{-1}\beta^{-1}\gamma\delta\gamma^{-1}\delta^{-1} = 1 \,\rangle$$

is a Fuchsian group with $\mathcal{G}\backslash\mathbb{H} = X$ compact of $g = 2$. This $\mathcal{G}$ is not rigid! $\mathcal{G}\backslash\mathbb{H}$ has six real free parametres $\Rightarrow$ "Teichmüller space".

Theorem 10.3 *a) Suppose $\mathcal{G} \subset \Delta$ are Fuchsian, $(\Delta : \mathcal{G}) < \infty$ with $\Delta = \dot{\bigcup}_k \mathcal{G}\gamma_k$, Δ has F_Δ as a fundamental domain. Then $F_\mathcal{G} := \bigcup_k \gamma_k F_\Delta$ is a fundamental domain for $\mathcal{G}$ ($\Rightarrow$ inducing a triangulation of $X = \mathcal{G}\backslash\mathbb{H}$ if Δ is a triangle group).*

b) Let X, X' be Riemann surfaces with surface (universal covering) groups $\mathcal{G}, \mathcal{G}' \subset \mathrm{Aut}\,\mathbb{H} = \mathrm{PSL}_2\,\mathbb{R}$. Then $X \cong X'$ iff $\mathcal{G}$ and $\mathcal{G}'$ are conjugate in $\mathrm{PSL}_2\,\mathbb{R}$.



(γ well defined $\Leftrightarrow$ induces a conjugation $\mathcal{G} \to \mathcal{G}'$)

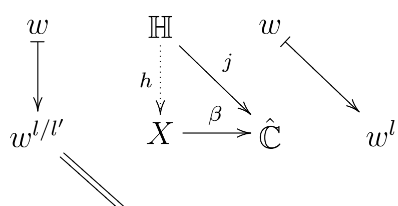
Recall that X compact Riemann surface is a smooth projective algebraic curve given by some equations. In case $g > 1$, $X = \mathcal{G}\backslash\mathbb{H}$ with some Fuchsian group $\mathcal{G}$. How are the equations determined by $\mathcal{G}$ and conversely?

Theorem 10.4 *Suppose X is a (compact) projective smooth algebraic curve. It has a Belyi function $\beta : X \to \hat{\mathbb{C}}$ (i.e. can be defined over $\bar{\mathbb{Q}}$) $\Leftrightarrow$ there is a triangle group $\Delta = \langle\, l, m, n \,\rangle$ (cocompact) and a finite index subgroup $\mathcal{G} \subseteq \Delta$ s.t. $X \cong \mathcal{G}\backslash\mathbb{H}$*

Proof.

"$\Leftarrow$": If $X \cong \mathcal{G}\backslash\mathbb{H}$, $\mathcal{G} \subseteq \Delta$, then $j : \mathbb{H} \to \hat{\mathbb{C}}$ with the j-function for $\Delta = \langle\, l, m, n \,\rangle$ induces a well-defined meromorphic mapping $\beta : \mathcal{G}z \mapsto j(z)$ ramified only in points $\mathcal{G}\Delta p_0, \mathcal{G}\Delta p_1, \mathcal{G}\Delta p_\infty \in X = \mathcal{G}\backslash\mathbb{H}$ (p_i fixed under γ_i), therefore a Belyi function; the dessin given by the Δ-tesselation on the upper half-plane $\mathbb{H}$, take the quotient by $\mathcal{G}$.

"$\Rightarrow$": Start with a Belyi function $\beta : X \to \hat{\mathbb{C}}$ s.t. least common multiple (lcm) of all multiplicities above 0, (1,∞) is l, (m,n). (Any common multiple does as well!) $\Delta = \langle\, l, m, n \,\rangle \subset \mathrm{PSL}_2\,\mathbb{R}$ and its j-function $\Rightarrow \beta^{-1}$ is only locally biholomorphic outside $0, 1, \infty$, but $\beta^{-1} \circ j$ is everywhere locally well-defined, holomorphically, so



commutes. $\mathbb{H}$ simply connected, so (by the monodromy theorem) $\beta^{-1} \circ j$ can be defined globally as holomorphic map h

$$h(z) = h(z') \Rightarrow z \in \Delta z'$$

So $X \cong \mathcal{G} \backslash \mathbb{H}$, where $\mathcal{G}$ is defined as $\{\, \gamma \in \Delta \,|\, h(z) = h(\gamma z)$ for all $z \in \mathbb{H}\,\}$.

□

10.3 Remarks

- In general, $\mathcal{G}$ is not the (unique) surface group for X, because it can have torsion. But if $l' = l$ etc., i.e. if β has the same multiplicity l (m, n) in all zeros (1-points, poles), then h is the universal covering map, $\mathcal{G}$ is the surface group of X. This occurs precisely, if the dessin for β is "uniform" ($\Leftarrow$ regular dessins).
- $\deg \beta = (\Delta : \mathcal{G})$.

Lecture 8

by Prof. Gareth Jones

11 From Dessins to Holomorphic Structures

11.1 Coverings

Let $\mathcal{B} = (G, x, y, E)$ and $\mathcal{B}' = (G', x', y', E')$ be algebraic bipartite maps. A *morphism* $\gamma : \mathcal{B} \to \mathcal{B}'$ or *covering* consists of a group-homomorphism $\theta : G \to G'$ and a function $\phi : E \to E'$ such that $x \mapsto x'$ and $y \mapsto y'$ under θ, and $\phi(eg) = \phi(e)\theta(g)$ for all $e \in E$, and for $g = x, y$ (equivalently for all $g \in G$).

Example: $\mathcal{B}_1 \to \mathcal{B}_2 = C_2 \backslash \mathcal{B}_1$ in section 6, lecture 4.

More generally, $\mathcal{B} \to A \backslash \mathcal{B} = \mathcal{B}'$, where $A \leq \operatorname{Aut} \mathcal{B}$ with G', x', y' the actions of G, x and y on the orbits of A. Coverings induced by automorphisms in this way are *regular*, or *normal*.

Exercise 11.1 *Show that θ and ϕ must be epimorphisms.*

γ is an isomorphism iff θ and ϕ are bijections, and then an automorphism if $\mathcal{B} = \mathcal{B}'$.

Exercise 11.1

$$\operatorname{Aut} \mathcal{B} = C(G) \cong N_G(G_e)/G_e.$$

Algebraic bipartite maps form a category.

The topological analogue of a morphism γ is a branched covering $X \to X'$ of surfaces, preserving orientation, with black vertices, white vertices, edges and faces on X' lifting to the same on X, and branching only at vertices or face-centers. We have a category of topological bipartite maps, and lecture 4 described a functor from these to algebraic bipartite maps. We can easily reverse this process, but with more work we can obtain holomorphic, rather than topological structures from algebraic bipartite maps.

11.2 Triangle Groups and Bipartite Maps

Consider algebraic bipartite maps of a given type (l, m, n), so in G we have $x^l = y^m = z^n = xyz = 1$. Consider the (abstract) group

$$\Delta = \Delta(l, m, n) = \langle\, X, Y, Z \mid X^l = Y^m = Z^n = XYZ = 1 \,\rangle$$

G is a quotient of Δ by $X \mapsto x$, etc. Then $\Delta \to G \to \mathrm{Sym}(E)$ gives a transitive action of Δ on the edge set E of $\mathcal{B}$. Bipartite maps of type $(l, m, n) \leftrightarrow$ "transitive actions of Δ". (Warning: actions of Δ can give maps of type (l', m', n') where $l'|l$, etc.) These actions correspond to conjugacy classes of subgroups $\Delta_e \leq \Delta$ $(e \in E)$. $\mathcal{B}$ is finite (compact) $\Leftrightarrow |\Delta : \Delta_e| < \infty$. Coverings $\mathcal{B} \to \mathcal{B}'$ correspond to inclusions $\Delta_e \leq \Delta_{e'}$ (easy exercise). Regular coverings correspond to normal inclusions. $\mathrm{Aut}\,\mathcal{B} \cong N_\Delta(\Delta_e)/\Delta_e$ (exercise 2.2) Theorem 2.1 and exercise 2.2 give

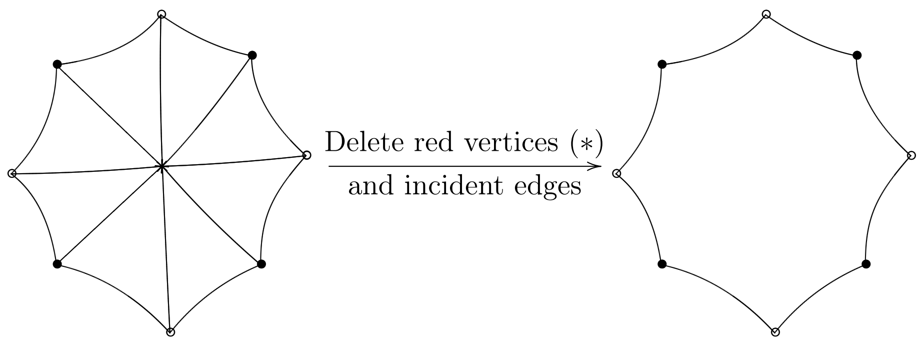
Theorem 11.1 *$\mathcal{B}$ is regular if and only if $\Delta_e \trianglelefteq \Delta$, in which case*

$$G \cong \mathrm{Aut}\,\mathcal{B} \cong \Delta/\Delta_e.$$

Example 11.1 *Let $\mathcal{B}$ correspond to the regular representation of $G = C_n \times C_n = \langle\, x, y \,|\, x^n = y^n = 1, xy = yx \,\rangle$. Then xy has order n, so the type is (n, n, n). Take $\Delta = \Delta(n, n, n)$, $\Delta_e = \mathrm{Ker}(\Delta \to G) \trianglelefteq \Delta$. G is abelian, so $\Delta_e \geq \Delta' =$ "commutator subgroup of Δ". Both have index n^2 in Δ, so $\Delta_e = \Delta'$. Here $G \cong \mathrm{Aut}\,\mathcal{B} \cong \Delta/\Delta_e = \Delta^{ab}$.*

The triangle group of type (l, m, n) has the same presentation as Δ (generators γ_0, γ_1, γ_∞ in Jürgen's lectures), so identify Δ with this group, $X, Y, Z =$ "rotations through $\frac{2\pi}{l}, \frac{2\pi}{m}, \frac{2\pi}{n}$ about the vertices of a triangle T with internal angles $\frac{\pi}{l}, \frac{\pi}{m}, \frac{\pi}{n}$". Assume that $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} < 1$ (typical case); if not, replace $\mathbb{H}$ with $\mathbb{C}$ or $\hat{\mathbb{C}}$. $\mathbb{H}$ is tesselated by the images of T under the extended triangle group $\Delta[l, m, n]$ generated by reflections in the sides of T, and $\Delta = \Delta(l, m, n)$ is the even subgroup of index 2, preserving orientation.

We can colour the vertices black, white or red as they are images of the vertices of T fixed by X, Y or Z. Every triangle has one vertex of each colour. Their valencies are $2l, 2m, 2n$ respectively.



This gives a bipartite map of type (l, m, n) on $\mathbb{H}$. This is the universal bipartite map $\mathcal{B}_\infty(l, m, n)$ of type (l, m, n). It is a regular map, with $\mathrm{Aut}\,\mathcal{B}_\infty(l, m, n) = \Delta(l, m, n)$, edge-stabiliser $\Delta_e = 1$.

Theorem 11.2 *Every bipartite map $\mathcal{B}$ of type (l, m, n) is isomorphic to a quotient $A\backslash\mathcal{B}_\infty(l, m, n)$ of $\mathcal{B}_\infty(l, m, n)$ by a subgroup $A \leq \operatorname{Aut}\mathcal{B}_\infty(l, m, n)$.*

Proof. Take A to consist of the automorphisms of $\mathcal{B}_\infty(l, m, n)$ induced by the subgroup Δ_e of Δ, and check that $\mathcal{B} \cong A\backslash\mathcal{B}_\infty(l, m, n)$. □

11.3 Holomorphic Structures

$A\backslash\mathcal{B}_\infty(l, m, n)$ has extra holomorphic structure, so denote it by $\mathcal{B}^{\mathrm{hol}}$. $\mathbb{H}$ is a Riemann surface, and Δ_e acts as a discontinuous group of automorphisms of $\mathbb{H}$ (since Δ does), so $\mathcal{B}^{\mathrm{hol}}$ is on a Riemann surface $X = A\backslash\mathbb{H}$. Coverings $\mathcal{B} \to \mathcal{B}'$ of bipartite maps correspond to inclusions $\Delta_e \leq \Delta_{e'}$ in Δ, so these induce branched coverings $X \to X'$ of Riemann surfaces. In particular, if we take $\Delta_{e'} = \Delta$, so $|E'| = 1$ corresponding to the trivial bipartite map with one edge, we get a covering $X \to X' = \hat{\mathbb{C}}$ branched only over the vertices 0 and 1, and the face-centre at ∞. This is a Belyi function (provided X is compact, i.e. $\mathcal{B}$ is finite). Then Belyi's Theorem gives:

Theorem 11.3 *If $\mathcal{B}$ is a finite algebraic map, then the Riemann surface X underlying $\mathcal{B}^{hol}$ is defined, as a smooth projective algebraic curve, over the field $\bar{\mathbb{Q}}$ of algebraic numbers.*

Example 11.2 (Example 4.1 revisited) *If $\mathcal{B}$ is as in example 11.1, the Riemann surface X uniformised by Δ' (="commutator subgroup of $\Delta = \Delta(n, n, n)$") is the n^{th} degree Fermat curve $F = F_n$ with affine equation $x^n + y^n = 1$, with Belyi function $\beta : (x, y) \mapsto x^n$. The black vertices are at $(0, \zeta_n^j)$ $j = 0, 1, \ldots, n-1$, and the white vertices are at $(\zeta_n^k, 0)$ $k = 0, 1, \ldots, n-1$. The edges (given by $\beta^{-1}([0, 1])$) between $v_j = (0, \zeta_n^j)$ and $w_k = (\zeta_n^k, 0)$ are given by $(r\zeta_n^k, s\zeta_n^j)$ where $r, s \in [0, 1]$ and $r^n + s^n = 1$.*

In general,

$$\begin{aligned} \operatorname{Aut}\mathcal{B} \cong \operatorname{Aut}\mathcal{B}^{\mathrm{hol}} &\cong N_\Delta(\Delta_e)/\Delta_e \\ &\leq N_{\mathrm{PSL}_2\mathbb{R}}(\Delta_e)/\Delta_e \qquad (\text{since } \Delta \leq \mathrm{PSL}_2\mathbb{R}) \\ &\cong \operatorname{Aut} X. \end{aligned}$$

Thus automorphisms of $\mathcal{B}$ act as automorphisms of the Riemann surface X (equivalently, of the algebraic curve).

Example 11.3 (=Examples 1 and 2 revisited) *If $\mathcal{B}$ is as in Example 11.1 and 11.2, then $\operatorname{Aut}\mathcal{B} \cong C_n \times C_n$, and this acts on X by multiplying x*

and y independently by n^{th} roots of 1. In this case, $\operatorname{Aut}\mathcal{B} \neq \operatorname{Aut} X$*, since* $\operatorname{Aut} X$ *is a semidirect product* $(C_n \times C_n) \rtimes S_3$ *of* $\operatorname{Aut}\mathcal{B}$ *by a complement* S_3*. The extra* S_3 *comes from permuting the 3 vertex-colours, or alternatively write* X *in projective form as* $x^n + y^n + z^n = 0$*, and let* S_3 *permute the coordinates.*

Exercise 11.2 *Explain example 11.3 by describing* $N_{\mathrm{PSL}_2\mathbb{R}}(\Delta_e)$*.*

11.4 Non-cocompact Triangle Groups

Suppose we want to consider all bipartite maps $\mathcal{B}$ of type $(3, 2, n)$ without restricting n. We take

$$\begin{aligned} \Delta = \Delta(3,2,\infty) &= \langle\, X, Y, Z \mid X^3 = Y^2 = Z^\infty = XYZ = 1 \,\rangle \\ &= \langle\, X, Y \mid X^3 = Y^2 = 1 \,\rangle \qquad \text{eliminating } Z = (XY)^{-1} \\ &\cong C_3 * C_2. \end{aligned}$$

The algebraic theory works as before. Geometrically, we take T to have a black vertex at i (angle $\frac{\pi}{2}$) and white vertex at ζ_3 (angle $\frac{\pi}{3}$), and a red vertex at ∞ on $\partial\mathbb{H}$ (angle $\frac{\pi}{\infty} = 0$). Reflections in the sides of T generate $\Delta[3, 2, \infty]$, the images of T tesselate $\mathbb{H}$, with vertices at the images of ∞.

Exercise 11.3 *Show that* $\Delta[3, 2, \infty] = \mathrm{PGL}_2(\mathbb{Z})$*, consisting of the transformations*

$$\tau \mapsto \frac{a\tau + b}{c\tau + d} \qquad a, \ldots, d \in \mathbb{Z},\ ad - bc = 1$$

or

$$\tau \mapsto \frac{a\bar{\tau} + b}{c\bar{\tau} + d} \qquad a, \ldots, d \in \mathbb{Z},\ ad - bc = -1.$$

The first type form the even subgroup $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$*.*

The orbit of ∞ under Γ is $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, so this is the set of red vertices. Deleting the red vertices and their incident edges, we get a bipartite map $\mathcal{B}_\infty(3, 2, \infty)$ of type $(3, 2, \infty)$. If Δ_e is a subgroup of finite index in $\Delta = \Gamma$, then $\Delta_e \backslash \mathbb{H}$ is a compact Riemann surface minus finitely many points, one for each orbit of Δ_e on $\mathbb{P}^1(\mathbb{Q})$

To deal with bipartite maps $\mathcal{B}$ of all possible types, use $\Delta(\infty, \infty, \infty) = \Gamma(2)$, congruence subgroup of level 2 in Γ. Here T has 3 vertices on $\partial\mathbb{H}$, at $0, 1$ and ∞. $\Gamma(2)$ is the even subgroup of $\Delta[\infty, \infty, \infty] =$ "group generated by reflections in the sides of T". Images of T tesselate $\mathbb{H}$, vertices are elements $\frac{p}{q} \in \mathbb{P}^1(\mathbb{Q})$, coloured black, white, red, as p is even and q is odd, or p and q are both odd, or p is odd and q is even (orbits of $\Gamma(2)$, see Exercise 2.3). Deleting red vertices and incident edges gives $\mathcal{B}_\infty(\infty, \infty, \infty) = \mathcal{B}_\infty$, the universal bipartite map. Every $\mathcal{B}$ is a quotient of $\mathcal{B}_\infty$.

Exercise 11.4 *Draw* $\mathcal{B}_\infty$*!*

Lecture 9

by Prof. Gareth Jones

12 Quasiplatonic Surfaces, and Automorphisms

12.1 Definitions and Properties

Any compact Riemann surface X of genus $g > 1$ can be uniformised by an essentially unique (upto conjugation by isometries) torsion-free Fuchsian group K ($\cong \pi_1 X$). Isomorphisms $X \to X'$ are induced by conjugating isometries of $\mathbb{H}$ taking K to K'. Taking $X = X'$ we see that automorphisms of X are induced by isometries normalising K. Since K acts trivially on $K\backslash\mathbb{H}$, we get

$$\operatorname{Aut} X \cong N(K)/K$$

where N denotes the normalizer in $\mathrm{PSL}_2\,\mathbb{R}$. (If $g = 1$, replace $\mathbb{H}$ with $\mathbb{C}$, replace K with a lattice Λ unique up to similarity — see the Elliptic Curves lecture.) We say that X (compact, of genus $g > 1$), is *quasiplatonic* if X is uniformised by a subgroup K as above, with K normally contained in a triangle group.

Theorem 12.1 *If X is a compact Riemann surface of genus $g > 1$, the following are equivalent:*

a) X is quasiplatonic,

b) $N(K)$ is a triangle group (K as above)

c) X has a Belyi function $\beta : X \to \hat{\mathbb{C}}$ which is a regular covering,

d) X corresponds to a regular dessin.

Proof.

a) $\Rightarrow$ b): $N(K)$ is a Fuchsian group (since K is) and it contains a triangle group. Any Fuchsian group containing a triangle group must be a triangle group (by Teichmüller theory — triangle groups are the only rigid Fuchsian groups).

b) $\Rightarrow$ c): Inclusion $K \leq N(K)$ induces a Belyi function

$$X \cong K\backslash\mathbb{H} \to N(K)\backslash\mathbb{H} \cong \hat{\mathbb{C}}.$$

Since $K \trianglelefteq N(K)$, this is a regular covering.

c) ⇒ d): Use β to lift the trivial dessin ($\underset{0}{\circ}$——$\underset{1}{\bullet}$) on $\hat{\mathbb{C}}$ to X, and since β is regular we get a regular dessin on X.

d) ⇒ a): If X corresponds to a regular dessin $\mathcal{B}$, then K is normal in the corresponding triangle group.

□

Example 12.1 *The n^{th} degree Fermat curve ($n > 3$) corresponds to a regular dessin, and is uniformised by the commutator subgroup of $\Delta(n, n, n)$ which is normal.*

Exercise 12.1 *For genus $g = 1$, what are the analogues of the quasiplatonic surfaces?*

One can characterise the quasiplatonic surfaces as the local maxima for $|\operatorname{Aut} X|$, in the sense that, within the Teichmüller space of all compact Riemann surfaces of genus g, every other surface sufficiently close to X has fewer automorphisms.

12.2 Hurwitz Groups and Surfaces

Here we look for global maxima of $|\operatorname{Aut} X|$.

Problem: Given $g > 1$, what are the most symmetric Riemann surfaces of genus g?

We have $\operatorname{Aut} X \cong N(K)/K$, with $N(K)$ Fuchsian. The index $|N(K) : K|$ is finite, equal to the ratio of the areas of the fundamental regions of these two groups. For K this is $4\pi(g-1)$, so maximising $|\operatorname{Aut} X|$ is equivalent to minimising the area for $N(K)$. One can show that among all Fuchsian groups, this area is minimised by the triangle group $\Delta(3, 2, 7) = \Delta(2, 3, 7)$, given by

$$\Delta = \langle\, X, Y, Z \mid X^3 = Y^2 = Z^7 = XYZ = 1 \,\rangle.$$

Exercise 12.2 *Prove that Δ has a fundamental region of area $\frac{\pi}{21}$, and this is the minimum among all triangle groups. Use the Gauss-Bonnet formula: "area"$=\pi - \alpha - \beta - \gamma$ for a hyperbolic triangle with internal angles α, β, γ.*

This gives us the Hurwitz bound

$$|\operatorname{Aut} X| \leq \frac{4\pi(g-1)}{\pi/21} = 84(g-1),$$

attained iff $X \cong K\backslash\mathbb{H}$ where K is a normal subgroup of finite index in $\Delta = \Delta(3,2,7)$. (Every proper normal subgroup in Δ is torsion-free, easy exercise.) These surfaces X and finite groups $G = \operatorname{Aut} X$ are called *Hurwitz surfaces* and *Hurwitz groups*. These surfaces are all quasiplatonic.

Example 12.2 *The modular group* $\Gamma = \mathrm{PSL}_2(\mathbb{Z}) = \Delta(3,2,\infty)$ *maps onto* $G = \mathrm{PSL}_2(7) = \mathrm{PSL}_2(\mathbb{Z}_7)$ *by reducing coefficients* $\mod 7$*. The generator* $Z : \tau \mapsto \tau + 1$ *is mapped to an element* z *of order* 7 *in* G*, so* G *is a quotient* Δ/K *of* $\Delta = \Delta(3,2,7)$*.*

$$|G| = 168 \left(= \frac{7(7^2-1)}{2} \right),$$

so the surface $X = K\backslash\mathbb{H}$ *has genus* $g = 1 + \frac{168}{84} = 3$*. This is Klein's quartic curve, given in projective coordinates by*

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

with $\operatorname{Aut} X \cong \mathrm{PSL}_2(7)$*.*

Exercise 12.3 *Prove that there is no Hurwitz group of genus 2.*

12.3 Kernels and Epimorphisms

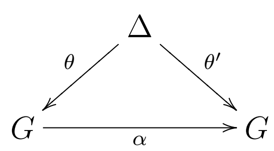
It's useful to count normal subgroups K of a triangle group Δ with a given quotient group $G \cong \Delta/K$.

Proposition 12.2 *If* Δ *is any finitely generated group, and* G *is any finite group, the number* $n_\Delta(G)$ *of* $K \trianglelefteq \Delta$ *with* $\Delta/K \cong G$ *is given by*

$$n_\Delta(G) = \frac{|\operatorname{Epi}(\Delta, G)}{|\operatorname{Aut} G|},$$

where $\operatorname{Epi}(\Delta, G)$ *is the set of all epimorphisms* $\theta : \Delta \to G$*.*

Proof. These normal subgroups K are the kernels of the epimorphisms $\theta : \Delta \to G$, and $\ker\theta = \ker\theta'$ iff $\theta' = \alpha \circ \theta$ for some $\alpha \in \operatorname{Aut} G$. Hence the kernels correspond to the orbits of $\operatorname{Aut} G$ acting by composition on $\operatorname{Epi}(\Delta, G)$.



Since $\operatorname{Aut} G$ acts semiregularly (i.e. $\alpha \circ \theta = \theta \Rightarrow \alpha = \mathrm{id}$), its orbits all have size $|\operatorname{Aut} G|$. By the hypotheses, $\operatorname{Epi}(\Delta, G)$ is finite, so the result follows. $\square$

For many G, $|\operatorname{Aut} G|$ is known or easily found, so concentrate on counting epimorphisms. If Δ is a triangle group

$$\Delta(l, m, n) = \langle X, Y, Z \mid X^l = Y^m = Z^n = XYZ = 1 \rangle,$$

finding epimorphisms $\Delta \to G$ is equivalent to finding triples $x, y, z \in G$ such that

a)
$$x^l = y^m = z^n = xyz = 1$$
(so there is a homomorphism $\Delta \to G : X \mapsto x$ etc.)

b) G is generated by x, y and z (or by any two of these), so we have an epimorphism.

If we want K to be torsion-free, we also require:

c) x, y and z must have orders exactly l, m and n.

12.4 Direct Counting

Example 12.3 *Let $\Delta = \Delta(5, 2, \infty)$ and $G = A_5$, so we count $K \trianglelefteq \Delta$ with $\Delta/K \cong A_5$. This is equivalent to counting regular maps $\mathcal{M}$ ($m = 2$) with valency 5 ($l = 5$) and $\operatorname{Aut} \mathcal{M} \cong A_5$. A_5 has 24 elements x of order 5 (the 5-cycles), and 15 elements of order 2 (the double transpositions $(ab)(cd)$) giving $24 \times 15 = 360$ pairs x, y satisfying the relations of Δ. The subgroup $H = \langle x, y \rangle$ has order divisible by 10, so $H \cong D_5$ or $H = A_5$. There are 6 subgroups $H \cong D_5$, each generated by $4 \times 5 = 20$ pairs x, y, so 120 pairs don't generate A_5. Hence $360 - 120 = 240$ do generate A_5. Thus $|\operatorname{Epi}(\Delta, G)| = 240$. Now $\operatorname{Aut} A_5 = S_5$ (acting by conjugation) of order 120, so $n_\Delta(G) = \frac{240}{120} = 2$. Thus Δ has two normal subgroups K with $\Delta/K \cong A_5$, i.e. there are two regular 5-valent maps $\mathcal{M}$ with $\operatorname{Aut} \mathcal{M} \cong A_5$. One is the icosahedron, represented by*

$$\theta : X \mapsto x = (1, 2, 3, 4, 5),\ Y \mapsto y = (1, 2)(3, 4),\ Z \mapsto z = (2, 5, 4).$$

The other one is the great dodecahedron, with 12 pentagonal faces, and the vertices and edges of an icosahedron. It's represented by

$$\theta : X \mapsto x = (1, 2, 3, 4, 5),\ Y \mapsto y = (1, 3)(2, 4),\ Z \mapsto z = (1, 2, 3, 5, 4).$$

This has genus $g = 1 + \frac{N}{2}(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}) = 4$ *(where in this case* $N = 60$ *and* $l = 5$*,* $m = 2$*,* $n = 3$*.) The underlying algebraic curve is Bring's curve, given in* $\mathbb{P}^4(\mathbb{C})$ *by*

$$x_1^k + x_2^k + x_3^k + x_4^k + x_5^k = 0 \qquad (k = 1, 2, 3).$$

$\mathrm{Aut}\, X \cong S_5$ *(permuting the coordinates), and the subgroup* A_5 *is the automorphism group of the map.*

12.5 Counting by Character Theory

A (complex) *representation* of a group G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, V a vector space over $\mathbb{C}$. $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$ are *equivalent* if some isomorphism $V \to V'$ commutes with G. The representation ρ is *irreducible* is V has no G-invariant subgroups other than 0 and V. A finite group G has c irreducible representations, up to isomorphism, where c is the number of conjugacy classes in G. The *character table* of G is a $c \times c$ array, "entries" = "trace of $\rho(g)$ on each conjugacy class" (constant on each class).

Proposition 12.3 *If* $\mathcal{X}, \mathcal{Y}$ *and* $\mathcal{Z}$ *are conjugacy classes in a finite group* G*, then the number of solutions of* $xyz = 1$ *in* G *with* $x \in \mathcal{X}$*,* $y \in \mathcal{Y}$*,* $z \in \mathcal{Z}$ *is equal to*

$$\frac{|\mathcal{X}| \cdot |\mathcal{Y}| \cdot |\mathcal{Z}|}{|G|} \cdot \sum_{\chi} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)},$$

where χ *ranges over the irreducible characters of* G*.*

In A_5 there are $c = 5$ conjugacy classes: the identity, 15 double transpositions, 20 3-cycles, and two classes of 12 5-cycles. Hence there are 5 irreducible characters and the character table looks like in table 1 where $\lambda, \mu = \frac{1 \pm \sqrt{5}}{2}$.

1	(..)(..)	(...)	$(.....)^+$	$(.....)^-$
1	1	1	1	1
3	1	0	λ	μ
3	1	0	μ	λ
4	0	1	-1	-1
5	1	-1	0	0

Table 1: The character table of A_5.

Example 12.4 *Take* $\Delta = \Delta(3,3,5)$, $G = A_5$ *and count* $K \trianglelefteq \Delta$ *with* $\Delta/K \cong A_5$. *There is only one choice for the classes* $\mathcal{X}$ *and* $\mathcal{Y}$ *of elements* x, y *of order 3, and there are two choices for the class* $\mathcal{Z}$ *containing* z *of order 5. In each case there are 60 triples* x, y, z *in these classes satisfying* $xyz = 1$, *giving 120 triples. Hence there is* $\frac{120}{120} = 1$ *normal subgroup* K. *This gives a single regular bipartite map of type* $(3,3,5)$ *with* $\mathrm{Aut}\,\mathcal{B} \cong A_5$. *Exercise* $\Rightarrow$ *genus* $g = 5$. *It's a double covering of the dodecahedron branched over the 12 face-centres, with vertices coloured alternately black and white.*

Lecture 10

by Prof. Jürgen Wolfart

13 Moduli Fields and Fields of Definition

"Existence of Belyi function $\beta \Rightarrow X$ is defined over $\bar{\mathbb{Q}}$."

K is a *field of definition* for the compact Riemann surface X iff X is isomorphic to a smooth projective algebraic curve $\subset \mathbb{P}^N(\mathbb{C})$ given by equations $p_i(x_0, \dots, x_N) = 0$, all $p_i \in K[x_0, \dots, x_N]$. If K is a field of definition, then $\mathbb{C} \supset L \supset K$ is a field of definition. Is there a minimal field of definition? Is it in $\bar{\mathbb{Q}}$?

Let

$$\underline{\underline{G}}_{\mathbb{C}} := \text{group of field automorphisms of } \mathbb{C}.$$

Suppose X to be defined over K by equations $p_i(x_0, \dots, x_N) = 0$, take $\sigma \in \underline{\underline{G}}_{\mathbb{C}}$, let X^σ be defined by the equations $p_i^\sigma(x_0, \dots, x_N) = 0$ (apply σ to all coefficients of all p_i) $\Leftrightarrow$

$$\{\, [\sigma(x_0), \dots, \sigma(x_N)] \mid [x_0, \dots, x_N] \in X \,\} =: X^\sigma.$$

This is again a smooth curve!

By the same reason

$$\begin{array}{ccc} X & \rightsquigarrow & X^\sigma \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta^\sigma} \\ \hat{\mathbb{C}} & \xrightarrow{\cong} & \mathbb{P}^1(\mathbb{C}) \end{array}$$

commutes. Here β^σ is defined by applying σ to the coefficients of β, and it remains a Belyi function on X^σ, because vanishing of derivatives is preserved under σ, and $\sigma(0) = 0$, $\sigma(1) = 1$, $\sigma(\infty) = \infty$. The list of all multiplicities of β is preserved under σ and degree of β equals to degree of β^σ. This implies that σ maps the dessin D for β a dessin D^σ of the same type for β^σ on X^σ. Now $\underline{\underline{G}}_{\mathbb{C}}$ acts on dessins of a given type and with a given no. of edges! Finite orbits $\Rightarrow$

Theorem 13.1 *a) The subgroup $\underline{\underline{G}}(D) := \{\, \sigma \in \underline{\underline{G}}_{\mathbb{C}} \mid D \cong D^\sigma \,\}$ is of finite index in $\underline{\underline{G}}_{\mathbb{C}}$.*

b) $\sigma \in \underline{\underline{G}}(D) \Leftrightarrow$ *there exist (biholomorphic!) isomorphisms* $f_\sigma : X \to X^\sigma$ *for which*

$$\begin{array}{ccc} X & \xrightarrow{f_\sigma} & X^\sigma \\ {\scriptstyle\beta}\downarrow & \swarrow {\scriptstyle\beta^\sigma} & \\ \hat{\mathbb{C}} & & \end{array}$$

commutes with the respective Belyi functions.

c) The "moduli field" $M(D) := \{\, \zeta \in \mathbb{C} \,|\, \sigma(\zeta) = \zeta \;\forall \sigma \in \underline{\underline{G}}(D) \,\}$ *has finite degree* $[M(D) : \mathbb{Q}] \Rightarrow$ *is a numberfield. (Reason: all* $\zeta \in M(D)$ *have a finite orbit under* $\underline{\underline{G}}_{\mathbb{C}}$*, length of orbit is bounded by* $(\underline{\underline{G}}_{\mathbb{C}} : \underline{\underline{G}}(D)) \Rightarrow [M(D) : \mathbb{Q}] \leq (\underline{\underline{G}}_{\mathbb{C}} : \underline{\underline{G}}(D))$*.)*

Consequence: Also $\underline{\underline{G}}(X) := \{\, \sigma \in \underline{\underline{G}}_{\mathbb{C}} \,|\, \exists$ isomorph. $f_\sigma : X \to X^\sigma \,\}$ and it follows that the corresponding fixed field $M(X)$ of $\underline{\underline{G}}(X)$ in $\subseteq M(D)$, and therefore we have again a number field.

Theorem 13.2 *$M(X)$ depends only on the isomorphism class of X and is contained in any field of definition for X (analoguous for $M(D) \subset$ field of definitions for X and β).*

Suppose $X \cong X'$, i.e. there is an isomorphism $h : X \to X'$ and suppose that $\sigma \in \underline{\underline{G}}(X)$, i.e. there is an isomorphism $f_\sigma : X \to X^\sigma$. We have an isomorphism $h^\sigma : X^\sigma \to X'^\sigma$ and we can contruct an isomorphism to make the diagram

$$\begin{array}{ccc} X & \xrightarrow{h} & X' \\ {\scriptstyle f_\sigma}\downarrow & & \vdots \\ X^\sigma & \xrightarrow{h^\sigma} & X'^\sigma \end{array}$$

commute. $h^\sigma \circ f_\sigma \circ h^{-1}$ gives the isomorphism we are looking for $\Rightarrow \sigma \in \underline{\underline{G}}(X')$ $\Rightarrow$

$$\underline{\underline{G}}(X) \cong \underline{\underline{G}}(X') \Rightarrow \text{ claim.}$$

Theorem 13.3 *$M(X)$ is a field of definition for X if $g(X) = 0$ or 1.*

Proof. $g = 0 \Leftrightarrow X \cong \hat{\mathbb{C}} \cong \mathbb{P}^1(\mathbb{C})$, defined $/\mathbb{Q}$.

$g(X) = 1 \Leftrightarrow X \cong \Lambda \backslash \mathbb{C}, \Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ $(\tau \in \mathbb{H})$. X defined $/\mathbb{Q}(g_2(\tau), g_3(\tau)) \supseteq \mathbb{Q}(j(\tau))$, so we see that X can be defined even over $\mathbb{Q}(j(\tau))$. X^σ defined $/\mathbb{Q}(\sigma(g_2(\tau)), \sigma(g_3(\tau)))$, even over $\mathbb{Q}(\sigma(j(\tau)))$, where $\sigma \in \underline{\underline{G}}_{\mathbb{C}}$. So $X \cong X^\sigma \Leftrightarrow \sigma(j(\tau)) = j(\tau)$. $M(X)$ is generated by $j(\tau)$ and $\mathbb{Q}(j(\tau))$ is a field of definition. □

But: in high genera there are counter examples, where X cannot be defined over $M(X)$. (Earle 1969, Shimura, Dèbes/Emsalem, Fuertes/Gonzalez).

Example by Earle in $g = 2$, $\zeta = \zeta_3 = e^{\frac{2\pi i}{3}}$

$$X : y^2 = x(x-\zeta)(x+\zeta)(x-\zeta^2 t)(x+\frac{\zeta^2}{t})$$

defined over $\mathbb{Q}(\zeta)$, and where $t \in \mathbb{Q}, t \neq 0, 1, t > 0$.

1. X cannot by defined over $\mathbb{Q}$. Note that point pairs $(\infty,\infty), (0,0)$, $(\zeta, 0), (-\zeta, 0)$,$(\zeta^2 t, 0), (-\frac{\zeta^2}{t}, 0)$ are "intrinsic", also their image points in $\mathbb{P}^1(\mathbb{C})$ under $(x, y) \mapsto x$, upto $\mathrm{PSL}_2\,\mathbb{C}$-transformations. If X can be defined over $\mathbb{Q}$, then there is an anticonformal automorphism of X, permuting the critical points on $\mathbb{P}^1(\mathbb{C})$: doesn't exist (by calculation of cross-ratios)!

2. $M(X) = \mathbb{Q} = \mathbb{R} \cap \mathbb{Q}(\zeta)$, $X \cong \bar{X}$, i.e. there is a holomorphic isomorphism $X \to \bar{X}$. There is an anticonformal mapping $(x, y) \mapsto (-\frac{1}{\bar{x}}, \frac{i\bar{y}}{\bar{x}^3})$, which is in fact an anticonformal automorphism (of order 4).

Theorem 13.4 *If $M(X) \in \bar{\mathbb{Q}}$, then X can be defined over a number field. (Weil, J.W., B. Köck)*

Idea: Any field of definition K for X is finitely generated over $M(X)$ because for a model of X defined over K

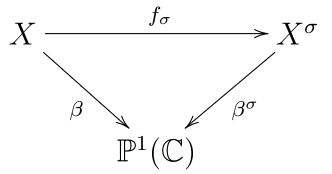
$$\sigma|_K = \mathrm{id} \Rightarrow X = X^\sigma.$$

Suppose for simplicity $K = M(X)(\xi)$ where ξ is transcendential, then there exists $\sigma \in \underline{\underline{G}}_{\mathbb{C}}$, $\sigma|_{M(X)} = \mathrm{id}_{M(X)}$, $\sigma(\xi) \mapsto \eta$ (η any other transcendential number). And because $\sigma \in \underline{\underline{G}}(X)$, there exists $f_\sigma : X \to X^\sigma$. Equations $p_i(x) = 0 \rightsquigarrow p_i^\sigma(x) = 0$ coefficients rational in $\xi \rightsquigarrow$ coefficients rational in η. Now try to insert in f_σ instead of η some algebraic $\alpha \in \bar{\mathbb{Q}}$, and it can be shown that f_σ is still an isomorphism for infinitely many $\alpha \in \bar{\mathbb{Q}}$. This gives the claim.

Theorem 13.5 (Weil) *Let X be defined over a finite extension L of $M := M(X)$. Then X can be defined over M itself if and only if $\forall \sigma \in \mathrm{Gal}\,\bar{M}/M$ there is an isomorphism $f_\sigma : X \to X^\sigma$ such that $\forall \sigma, \tau \in \mathrm{Gal}\,\bar{M}/M$ we have*

$$f_{\sigma\tau} = f_\sigma^\tau \circ f_\tau.$$

Analoguous statement holds for $M(D)$ and the field of definition for X and β, with diagram

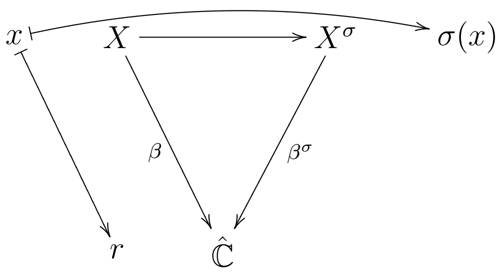


commuting.

Consequence: If $\operatorname{Aut} X = \{\text{id}\}$, then X is defined over $M(X)$. $\Leftarrow f_\sigma$ is unique (generic case for $g > 2$).

Theorem 13.6 (Coombes/Harbater, Dèbes/Emsalem, J.W., B. Köck) *Quasiplatonic curve X can be defined $/M(X)$.*

Idea: The canonical projection $X \to \operatorname{Aut} X \backslash X \cong \mathbb{P}^1(\mathbb{C})$ is a Belyi function, assume that the critical points are $0, 1, \infty$. Let D be the corresponding (regular) dessin on X, $M(D) \subset \bar{\mathbb{Q}}$. Prove first that X, β are defined $/M(D)$. Let $r \neq 0, 1$, $r \in M(D) \subset \mathbb{C} \subset \hat{\mathbb{C}}$, fix one $x \in \beta^{-1}(r), \sigma \in \operatorname{Gal} \bar{\mathbb{Q}}/M(D)$ to make the following diagram



commute. $\sigma(r) = r \Rightarrow \sigma(x) \in (\beta^\sigma)^{-1}(r)$, choose f_σ so that $f_\sigma(x) = \sigma(x)$ $\Rightarrow$ unique choice for f_σ and it has been shown that Weil's conditions are satisfied! The proof that X can be defined even over $M(X) \subseteq M(D)$ needs some additional arguments.

Exercise 13.1 *Show that the elliptic curve can be defined over $\mathbb{Q}(j(\tau)) \subseteq \mathbb{Q}(g_2(\tau), g_3(\tau))$.*

Exercise 13.2 *Suppose X defined $/\bar{\mathbb{Q}}$, $g(X) > 1$. ($\operatorname{Aut} X$ finite $\Rightarrow$) Show that all automorphisms $f : X \to X$ are also defined $/\bar{\mathbb{Q}}$.*

Lecture 11

by Prof. Gareth Jones

14 Regular Embeddings of Complete Bipartite Graphs

14.1 Regular Maps

Every bipartite map $\mathcal{B}$ is a quotient of a regular bipartite map $\widetilde{\mathcal{B}}$ by some $A \leq \operatorname{Aut}\widetilde{\mathcal{B}}$. Similarly for maps $\mathcal{M}$. Hence the importance of regular maps. One can try to classify these by type, group, genus or graph.

a) Classifying by type: Study finite quotients of the triangle group $\Delta = \Delta(l, m, n)$ of a given type (see previous lectures for some ideas). If $\frac{1}{l} + \frac{1}{m} + \frac{1}{n} \leq 1$ (so Δ is infinite) then a theorem by Mal'cev states that a finitely-generated linear group is residually finite ($\bigcap\{\, K \trianglelefteq \Delta \mid |\Delta : K| < \infty \,\} = 1$), so Δ has infinitely many $K \trianglelefteq \Delta$ of finite index, so we get infinitely many regular maps of type (l, m, n).

Example 14.1 *Taking* $\Delta = \Delta(3, 2, 7)$ *we get infinitely many Hurwitz groups and Hurwitz surfaces. E.g. Macbeath (1964):* $\mathrm{PSL}_2(\mathbb{F}_q)$ *is a Hurwitz group* $\Leftrightarrow q = 7$*, or* $q = p \equiv \pm 1 \mod 7$ *(p prime), or* $q = p^3$*, prime* $p \equiv \pm 2, \pm 3 \mod 7$*. Conder (∼ 1980):* A_n *is a Hurwitz group for all* $n \geq 168$ *(and some* $n < 168$*).*

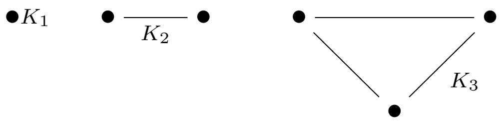
b) Classifying by group: Difficulty: G usually has many generating pairs x, y. J.D. Dixon (∼ 1964): If x, y are randomly-chosen elements of $G = S_n$, then they generate either S_n or A_n with probabilities $\to \frac{3}{4}$ (not both elements even) or $\frac{1}{4}$ (both elements even) as $n \to \infty$. There are similar results for other classes of groups.

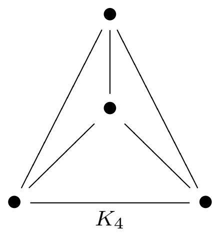
c) Classifying by genus: If $g = 0$ or 1 there are infinitely many regular maps, but they are well-known (e.g. see Chapter 8 of Coxeter and Moser for $g = 1$). If $g > 1$, Hurwitz's bound $|G| \leq 84(g-1)$ implies that there are only finitely many regular maps of genus g, and these can by classified by hand (for small g) or computer (for larger g).

d) Classifying by graph: *Problem*: Given a graph $\mathcal{G}$ (or class of graphs $\mathcal{G}$), find all regular maps with $\mathcal{G}$ as the embedded graph. Equivalently, look for $G \leq \operatorname{Aut}\mathcal{G}$, transitive on the vertex-set V, with vertex-stabiliser

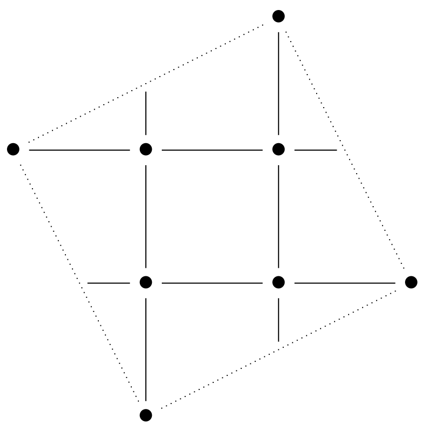
G_v ($v \in V$) cyclic and transitive on the neighbours of v (induced by rotating the surface around v). Such an embedding can exist only if $\mathcal{G}$ is arc-transitive, i.e. $\mathrm{Aut}\,\mathcal{G}$ acts transitively on the arcs (=directed edges) of $\mathcal{G}$.

Example 14.2 *Take $\mathcal{G} = K_n$ = "complete graph on n vertices". The graphs*





are regular embeddings, $g = 0$.



$K_5 \hookrightarrow$"torus", $g = 1$. For K_6 there's no embedding and for K_7 two examples on torus (see if you can find them, imitating K_5).

Theorem 14.1 (Biggs, 1971) *K_1 has a regular embedding $\Leftrightarrow n = p^e$ for some prime p.*

Theorem 14.2 (James & J. 1985) *Regular embeddings of K_n classified and enumerated.*

Biggs's examples are the onlny ones. His construction: Take $V = \mathbb{F}_n$, finite field of order $n = p^e$, unique up to isomorphism. Multiplicative group $\mathbb{F}_n^* = \mathbb{F}_n \backslash \{0\}$ is cyclic, so choose a generator α. The cyclic order of neighbours of each vertrex v is $v+1$, $v+\alpha$, $v+\alpha^2$, ..., $v+\alpha^{n-2}$. Check that this gives a regular embedding $\mathcal{M}(\alpha)$,

$$G = \mathrm{Aut}\,\mathcal{M}(\alpha) \cong \mathrm{AGL}_1(\mathbb{F}_n) = \{\, t \mapsto at+b \,|\, a,b \in \mathbb{F}_n, a \neq 0 \,\}.$$

$$\mathcal{M}(\alpha) \cong \mathcal{M}(\alpha') \Leftrightarrow \alpha, \alpha' \text{ are conjugate under } \mathrm{Gal}(\mathbb{F}_n) \cong C_e,$$

where C_e is generated by the Frobenius automorphism $t \mapsto t^p$. Therefore

$$\#\text{maps } \mathcal{M}(\alpha) = \frac{\phi(n-1)}{e},$$

where $\phi(n-1)$ is the number of choices of α generating $\mathbb{F}_n^* \cong C_{n-1}$ and e is the size of orbits of $\mathrm{Gal}(\mathbb{F}_n)$.

Hint for K_7: Dessin represents the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$. Black/white vertices = 7 points & 7 lines. Can you get a regular embedding of K_4 from this? Can you get two of them?

14.2 Complete Bipartite Graphs

Take $\mathcal{G} = K_{n,n}$ ="complete bipartite graph with n black vertices and n white vertices, every black and white pair joined by one edge", so $|V| = 2n$ and $|E| = n^2$.

We look for embeddings $\mathcal{M}$ of $K_{n,n}$ which are regular as *maps*, not just as bipartite maps, i.e. $\mathrm{Aut}\,\mathcal{M}$ (ignoring the vertx-colours) should act transitively on directed edges, not just on edges, so $\mathrm{Aut}\,\mathcal{M} = \mathrm{Aut}\,\mathcal{B} \rtimes C_2$ where $\mathrm{Aut}\,\mathcal{B} = G$ is the automorphism group of the dessin (preserving vertex-colours), and C_2 reverses them.

Example 14.3 *The Fermat curve $x^n + y^n = 1$, with Belyi function $\beta(x,y) = x^n$, gives a regular embedding of $K_{n,n}$ of genus $g = \frac{(n-1)(n-2)}{2}$, with $G = C_n \times C_n$ acting by sending (x,y) to $(x\zeta_n^j, y\zeta_n^k)$; here the automorphism $(x,y) \mapsto (y,x)$ transposes black and white vertices, giving* $\mathrm{Aut}\,\mathcal{M} = (C_n \times C_n) \rtimes C_2$ *(isomorphic to wreath product of C_n and C_2, $C_n \wr C_2$). This is the standard embedding S_n of $K_{n,n}$.*

Thus if $\nu(n) :=$ "number of regular embeddings of $K_{n,n}$ (up to isomorphism). Then $\nu(n) \geq 1$ for all n, since $\mathcal{S}_n$ exists for all n.

Theorem 14.3 (Nedelar, Škoviera & J. ~ 2001) $\nu(n) = 1$ *(i.e. $\mathcal{S}_n$ is the only regular embedding of $K_{n,n}$) $\Leftrightarrow$ $(n, \phi(n)) = 1 \Leftrightarrow n = p_1 \dots p_k$, p_i distinct primes, $p_i \nmid p_j - 1$ when $i \neq j$.*

(Compare with a result of Burnside, $\sim$ 1900: these are the n for which there is only one group of order n, namely C_n. The proofs are independent.)

The asymptotic density of these integers n is (by Erdős, 1948)

$$\frac{\text{number of such integers } n \leq N}{N} \sim \frac{e^{-\gamma}}{\log\log\log N} \text{ as } N \to \infty$$

where γ is Euler's constant.

Theorem 14.4 (Nedela, Škoviera & J.) *If $n = p^e$, prime $p > 2$, then $\nu(n) = p^{e-1}$.*

These maps all have genus $g = \frac{(n-1)(n-2)}{2}$. They have valency n, and the faces are all $2n$-gons. The groups $G = \operatorname{Aut}\mathcal{B}$ (preserving the vertex-colours) have the form

$$G = G_f = \langle\, g, h \,|\, g^n = h^n = 1, g^{-1}hg = h^{1+p^f} \,\rangle,$$

where $f = 1, 2, \ldots, e$. (If $f = e$ then $p^f = p^e = n$, so $h^{1+p^f} = h$, so $G = C_n \times C_n$ with $\mathcal{M} = \mathcal{S}_n$)

For a given $G = G_f$, the maps $\mathcal{M}$ correspond to orbits of $\operatorname{Aut} G$ on pairs of elements x, y such that

1. $G = XY$ with $X \cap Y = 1$, $X = \langle x\rangle$ and $Y = \langle y\rangle$, both of order n;
2. some $\alpha \in \operatorname{Aut} G$ transposes x and y.

(Here x and y represent rotations around a black and a white vertex, α is conjugation of G by an automorphism of $\mathcal{M}$ reversing the edge between them.) As representatives of the orbits of $\operatorname{Aut} G$ on such pairs, one can take $x = g^u$, $y = g^u h$ (or $(gh)^u$, more convinient for Galois theory) where $u = 1, 2, \ldots, p^{e-f}$ and $(u, p) = 1$.

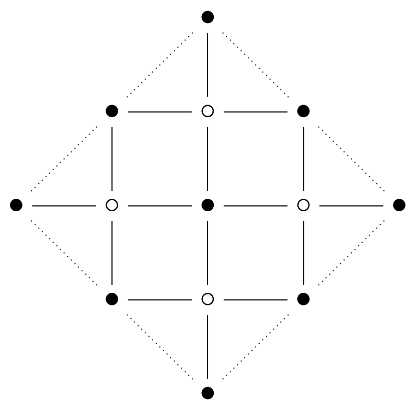
For each f we have $\phi(p^{e-f})$ possible choices of u, so summing over $f = 1, \ldots, e$ we get $\sum_{f=1}^{e} \phi(p^{e-f}) = p^{e-1}$ maps $\mathcal{M}$. These correspond to normal subgroups $K \trianglelefteq \Delta(n, n, n)$, which are also normal in $\Delta(n, 2, 2n)$ which contans $\Delta(n, n, n)$ with index 2.

$$K \trianglelefteq \Delta(n, n, n) \leq \Delta(n, 2, 2n)$$

The proof depends on:

Theorem 14.5 (Huppert, 1951) *If G is a p-group ($|G|$ is a power of p) for a prime $p > 2$, and $G = XY$ for cyclic subgroup X and Y, then G is metacyclic (i.e. there is a cyclic $N \trianglelefteq G$ with G/N cyclic).*

In our case $|G| = n^2 = p^{2e}$, and we can take $N = \langle h \rangle$. There are exceptions to Huppert's Theorem when $p = 2$, and there are also exceptional regular embeddings for $n = 2^e$. E.g. $n = q = 2^2$:



These is an embedding $\mathcal{N}_4$ of $K_{4,4}$ of genus $g = 1 \neq \frac{(n-1)(n-2)}{2}$.

Theorem 14.6 (Du, Kwak, Nedela, Škoviera & J. ∼ 2005) *The regular embeddings of $K_{n,n}$ for $n = 2^e$ are:*

- *these corresponding to G_f for $f = 2, 3, \dots, e$ (not $f = 1$).*
- *$\mathcal{N}_4$ if $e = 2$.*
- *four similar exceptions for each $e \geq 3$.*

Recent result (Apice 2006): complete classification for *all* n.

What about the associated algebraic curves, Galois orbits, fields of definition, etc. Jürgen, Manfred Streit, Antoine Coste.

Lecture 12

by Prof. Jürgen Wolfart

15 Generalised Fermat Curves

Theorem 15.1 *Let X be a quasiplatonic curve with a regular dessin D of type (l, m, n), and suppose that for any dessin D' of the same type* $\operatorname{Aut} D' \cong \operatorname{Aut} D$ *implies $D \cong D'$. Then X can be defined over $\mathbb{Q}$.*

Proof. l, m, n is invariant under the action of $\underline{\underline{G}}_{\mathbb{C}}$ or $\operatorname{Gal} \bar{\mathbb{Q}}/\mathbb{Q}$, and moreover

$$\operatorname{Aut} X^\sigma \cong \operatorname{Aut} X.$$

$\Rightarrow \operatorname{Aut} D^\sigma \cong \operatorname{Aut} D$. From the hypothesis therefore follows $D^\sigma \cong D$. $\Rightarrow$ $\underline{\underline{G}}(D) = \underline{\underline{G}}_{\mathbb{C}} \Rightarrow M(D) = \mathbb{Q} \Rightarrow X$ can be defined over $\mathbb{Q}$. □

Theorem 15.1 applies to all quasiplatonic curves up to $g = 5$.

Recall: Fermat curves F_n, $n > 3$, have a regular dessin of type (n, n, n), based on $K_{n,n}$. Suppose now that $n = p^e > 3$ (odd prime power) and suppose that all dessins are based on $K_{n,n}$, and they are regular as *maps* (i.e. there is edge-transitive automorphism group and moreover a colour-exchanging (orientable) involution $\circ \longleftrightarrow \bullet$. Recall that then [G.J., Nedela, Škoviera]

$$\operatorname{Aut} D \cong C_n \rtimes C_n := \langle\, g, h \,|\, g^n = h^n = 1,\ h^g := g^{-1}hg = h^{1+p^f} \,\rangle = G_f$$

(colour-preserving subgroup) for some $f = 1, \ldots, e$

- the G_f are pairwise non-isomorphic
- $\forall\ f = 1, \ldots, e$ there are quotients $\Delta/K_{f,u} \cong G_f$ for $\Delta = \langle n, n, n\rangle$ by the kernel $K_{f,u}$ of the homomorphism $\gamma_0 \mapsto g^u$, $\gamma_1 \mapsto (gh)^u$ for some u coprime to p
- these kernels $K_{f,u}$, $K_{f,v}$ are different $\Leftrightarrow u \not\equiv v \mod p^{n-f}$ (giving $p^{e-f} - p^{e-f-1}$ different surface groups if $f < e$)
- the case $f = e$ we have $G_e \cong C_n \times C_u \Rightarrow K_{e,1} = [\Delta, \Delta]$ and $K_{e,1}\backslash\mathbb{H} \cong F_n$.

Call $X_{f,u} := K_{f,u}\backslash\mathbb{H}$ for $f = 1, \ldots, e$ and $u \in (\mathbb{Z}/p^{e-f}\mathbb{Z})^*$ "generalised Fermat curves".

Theorem 15.2 (G.J.,Manfred Streit, J.W.) *For fixed $n = p^e$ odd and $f \in \{1, \dots e\}$, these $X_{f,u}$ form one Galois orbit. Their moduli field $M(X_{f,u})$ (= a minimal field of definition) is*

$$\mathbb{Q}(\eta), \ \eta = \exp\left(\frac{2\pi i}{p^{e-f}}\right).$$

Ideas for the proof:

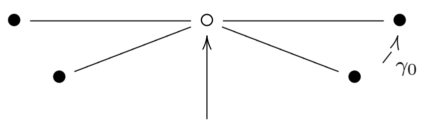
1. Show that $X_{f,u} \cong X_{g,v} \Leftrightarrow f = g$ and $u \equiv v \mod p^{e-f}$. $G_f \cong G_g \Leftrightarrow f = g$. Therefore the first implication is done. $X_{f,u} \cong X_{f,v} \Leftrightarrow K_{f,u}$ and $K_{f,v}$ conjugate in $\mathrm{PSL}_2 \mathbb{R}$ (even in $\langle 2, 3, 2n\rangle$). That possibility can be excluded.

2. For all $\sigma \in \mathrm{Gal}\,\bar{\mathbb{Q}}/\mathbb{Q}$ consider $X^{\sigma}_{f,u}$.

$$\left.\begin{array}{r}\text{Ramifications are preserved}\\ \text{Regularity is preserved}\\ \mathrm{Aut}\, X_{f,u} \text{ is preserved}\end{array}\right\} \Rightarrow X^{\sigma}_{f,u} \cong \text{ some } X_{f,v}, \ v \in (\mathbb{Z}/p^{e-f}\mathbb{Z})^*.$$

   $\Rightarrow$ Galois orbits are parts of $\{ X_{f,u} \mid u \in (\mathbb{Z}/p^{e-f}\mathbb{Z})^* \}$

3. Acting on $X_{f,u}$ (and the dessin), g has p^f (white) fixed points and gh has p^f (black) fixed points. G_f is considered as automorphism group $\cong \Delta/K_{f,u}$, for the



   fixed point of γ_0

$$\gamma_0 \mapsto g^u \Rightarrow g = (g^u)^{u'}$$

   (where $uu' \equiv 1 \mod n$) number of the fixed points calculate the index

$$(N_{G_f}(\langle g\rangle) : \langle g\rangle) = p^f = (N_{G_f}(\langle hg\rangle) : \langle hg\rangle)$$

4. Locally in the fixed points, γ_0 and γ_1 behave like $z \mapsto \zeta_n z+$ "higher z-powers". Fixed point $\leftrightarrow 0 = z$. $\Rightarrow g^u$ has also multiplier $\zeta = \zeta_n$ in the corresponding fixed point $\Rightarrow g$ has multiplier $\zeta^{u'}$ in the corresponding fixed point. All g-fixed points form an orbit under $\left\langle h^{p^{e-f}}\right\rangle$-orbit and g has the same multiplier $\zeta^{u'}$ in all its fixed points! Also gh has the multiplier $\zeta^{u'}$ ($u'u \equiv 1 \mod n$) in all its • fixed points. $\Rightarrow$ In its family, $X_{f,u}$ is characterised by the multipliers $\zeta^{u'}$ of g and gh in their fixed points. Fixed points of g: action locally by $z \mapsto \zeta^{u'} z+$ "higher terms".

5. Behaviour of the multipliers under $\sigma \in \operatorname{Gal} \bar{\mathbb{Q}}/\mathbb{Q}$. Suppose $g \in \operatorname{Aut} X$ with fixed points $P \in X$ and multiplier $\xi \Rightarrow$ on X^σ, g has fixed point P^σ with multiplier $\sigma(\xi)$. Choose for the local chart some $X \to \hat{\mathbb{C}}$ globally meromorphic, defined over $\bar{\mathbb{Q}}$, $P \mapsto 0$ simple zero in P, multipliers are always roots of unity ($\Leftarrow$ finite order), $\xi \mapsto \sigma(\xi)$ root of unity, same order.

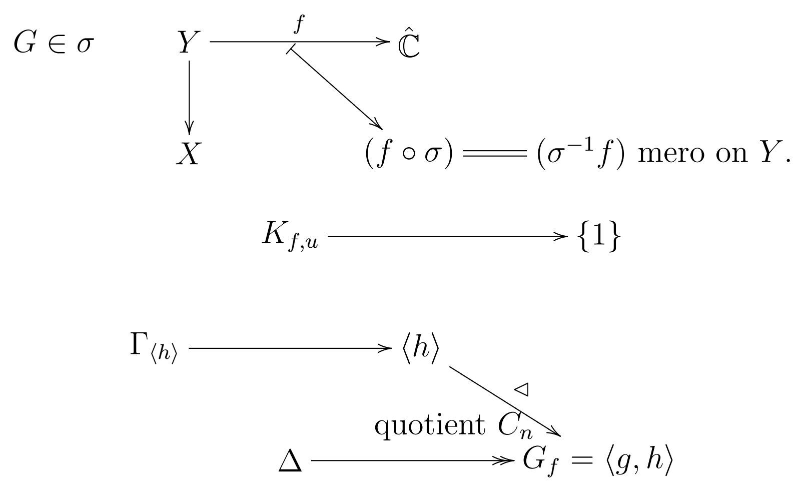
6. $\sigma \in \operatorname{Gal} \bar{\mathbb{Q}}/\mathbb{Q}$, $\sigma|_{\mathbb{Q}(\eta)} = \mathrm{id}_{\mathbb{Q}(\eta)}$, where $\eta = e^{\frac{2\pi i}{p^{e-f}}}$. $\sigma(\zeta^{u'}) = \zeta^{v'}$ (primitive n^{th}-root of unity) with $v' \equiv u' \mod p^{e-f} \Leftrightarrow v \equiv u \mod p^{e-f} \Leftrightarrow X_{f,u} \cong X_{f,v} \Rightarrow \sigma \in \underline{\underline{G}}(X_{f,u}) \Rightarrow \mathbb{Q}(\eta)$ is a field of definition. $\operatorname{Gal} \bar{\mathbb{Q}}/\mathbb{Q}$ acts transitively on the primitive n^{th} roots of unity $\Rightarrow$ acts transitively on $\{X_{f,u}\} \Rightarrow$ they form a Galois orbit. $M(X_{f,u}) = \mathbb{Q}(\eta)$ is a field of definition.

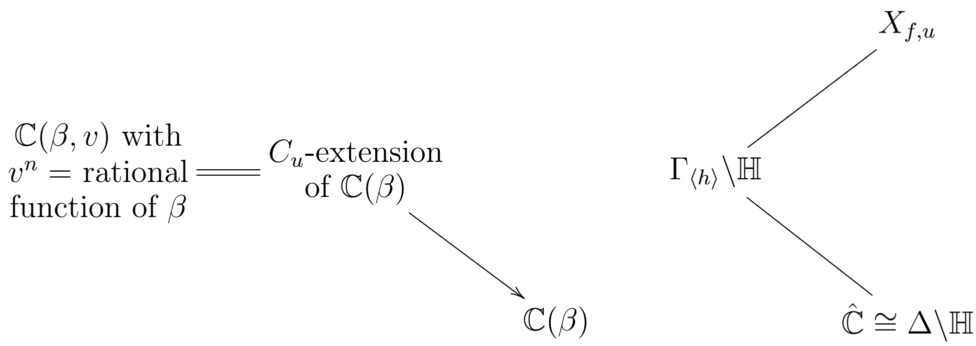
Theorem 15.3 *Let $n = p^e > 3$ be an odd prime power and $f \geq \frac{e}{2}$. Then we have a (singular, affine) model for $X_{f,1}$, given by the equations*

$$\begin{aligned} v^n &= \beta(\beta - 1) \\ w^{p^{e-f}} &= 1 - \beta \\ z^{p^f} &= w^{-r} \prod_{k=0}^{p^{e-f}-1} (w - \eta^k)^{ak} \end{aligned}$$

where $a := p^{2f-e}$, $r := \left((1 + p^f)^{p^{e-f}} - 1\right)/p^e$ ($\in \mathbb{N}$, coprime to p).

Idea: Covering groups $\leftrightarrow$ Galois groups of extensions of function fields.





Equations for $X_{f,u} = K_{f,u}\backslash\mathbb{H} \Leftarrow$ algebraic relations in the corresponding function field. This is the composite field of the function field for $\Gamma_{\langle h\rangle}\backslash\mathbb{H}$ and $\Gamma_{\langle g\rangle}\backslash\mathbb{H}$ where $\Gamma_{\langle h\rangle}$ and $\Gamma_{\langle g\rangle}$ are the preimages of $\langle h\rangle$ and $\langle g\rangle$ under the epimorphism $\Delta \to G_f$. Since

$$\Gamma_{\langle h\rangle}\backslash\mathbb{H} \to \Delta\backslash\mathbb{H} = \hat{\mathbb{C}}$$

is a cyclic covering ramified with multiplicity n above $0, 1, \infty$, with an additional symmetry between 0 and 1, we get $\mathbb{C}(\beta, v)$ as function field for the covering space with $v^n = \beta(\beta - 1)$. The corresponding construction for $\Gamma_{\langle g\rangle}\backslash\mathbb{H}$ is more complicated, since it needs a two-step tower of normal coverings.

Exercises

16 Some Hints Concerning Exercises

Exercise 1.1

F_n projective Fermat curve of exponent n, then $\operatorname{Aut} F_n \subseteq (C_n \times C_n) \rtimes S_3$ (semidirect product), see Gareth's Lecture 8. Moreover "=" holds if $n > 3$ because its surface group K is the commutator subgroup $[\Delta, \Delta]$ of the triangle group $\Delta = \langle n, n, n \rangle$, and $\operatorname{Aut} F_n = N(K)/K$, $N(K) = \langle 2, 3, 2n \rangle$ containing Δ as a normal subgroup with quotient S_3. In fact, the hyperbolic triangle for the construction of $\langle 2, 3, 2n \rangle$ results from that for $\langle n, n, n \rangle$ by barycentric subdivision, and it can be shown that $\langle 2, 3, 2n \rangle$ is maximal Fuchsian group, so $N(K)$ cannot be larger than $\langle 2, 3, 2n \rangle$ (the analogous statement for $n = 3$, i.e. for $\langle 2, 3, 6 \rangle$ would be definitely wrong!).

Exercise 1.2/4.2

The genus of the (compact) hyperelliptic curve with affine equation $y^2 = q(x)$, $\deg q = \begin{Bmatrix} 2g+1 \\ 2g+2 \end{Bmatrix}$ with $\begin{Bmatrix} 2 \\ 1 \end{Bmatrix}$ points above $x = \infty$ is g by application of Riemann-Hurwitz to the mapping $f : (x, y) \mapsto x$ of degree 2: It is ramified in $2g + 2$ points with multiplicity 2, hence we have in fact

$$2g - 2 = 2 \cdot (-2) + \sum (\operatorname{mult}_p f - 1) = -4 + (2g + 2) \cdot 1.$$

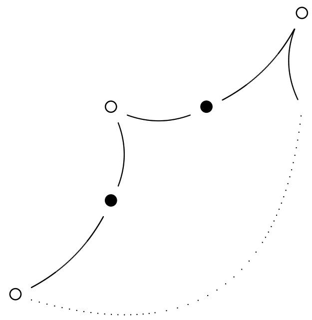
In the special case $q(x) = x^n - 1 = \prod_{k=1}^{n} (x - \zeta_n^k) \Rightarrow$

$$\left.\begin{matrix} X \to & \hat{\mathbb{C}} \to & \hat{\mathbb{C}} \\ (x,y) \mapsto & x \mapsto & x^n \end{matrix}\right\} \text{ ramified above } \begin{cases} 0 \text{ in 2 points, mult} = n \\ 1 \text{ in } n \text{ points, mult} = 2 \\ \infty \text{ in 1 point, mult} = 2n \text{ for } 2 \mid n \\ \infty \text{ in 2 points, mult} = n \text{ for } 2 \nmid n \end{cases}$$

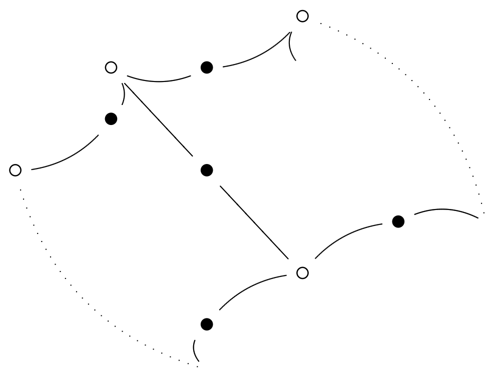
defines a Belyi function of $\deg 2n$ and the dessin for this Belyi function looks like two planes with this bipartite graph,

glued in the black points (and the point ∞ if n is even).

A picture in $\mathbb{H} \cong \mathbb{D}$ can be given and by a $2n$-sided polygon



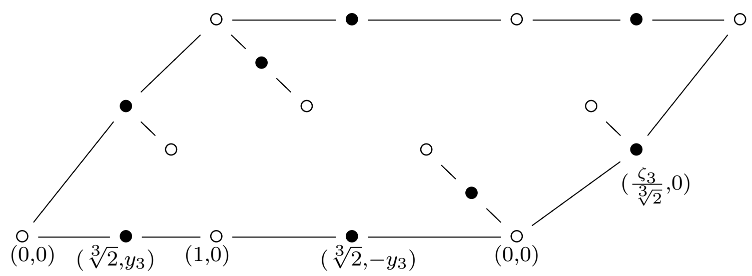
in the case $2|n$ and a $2(n-1)$-sided polygon, subdivided in two cells



if $2 \nmid n$.

<u>Exercise 4.3</u>

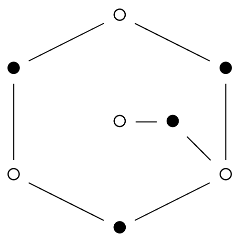
A Belyi function for $y^2 = x(x-1)(x - \frac{\zeta_3}{\sqrt[3]{2}}$ is formally the same $(x, y) \mapsto 4x^3(1-x^3)$ as if ζ_3 is replaced by 1, but with different ramifications, so the dessin now looks like



in a fundamental parallellogram for the elliptic curve. For $\zeta_3^2 = \bar{\zeta}_3$ instead of ζ_3 a mirror image of this dessin arises.

Exercise 7.1

$\beta \mapsto 1-\beta$ exchanges the colours of the bipartite graph, $\beta \mapsto \frac{1}{\beta}$ preserves $\beta = 1$ and exchanges zeros and poles, hence cell centers and 0-vertices $\Rightarrow$ the pole orders of β are the zero orders of that modified dessin $= \frac{1}{2}$ #"border edges of the cell", but the "inner edges" having the face on both sides have to be counted twice!



$$\beta \mapsto 16\beta(\beta - \frac{3}{4})^2$$

replaces $\underset{0}{\circ}$ —— $\underset{1}{\bullet}$ by $\underset{0}{\circ}$ —— $\underset{\frac{1}{4}}{\bullet}$ —— $\underset{\frac{3}{4}}{\circ}$ —— $\underset{1}{\bullet}$. (Idea: Take $\frac{1}{2}(1+T_n(2\beta-1))$, n odd, to insert more vertices with T_n the n^{th} Tshebychev polynomial)