Jyväskylä Summer School 2006: Course MA2

Lectures by Gareth Jones

1. Elliptic curves and the modular group

In this lecture we will consider a special class of algebraic curves called elliptic curves. We shall construct their associated Riemann surfaces in two different ways: firstly as branched coverings of the sphere obtained from many-valued algebraic functions, and secondly as quotients of the complex plane by lattices. By using elliptic functions, we will see that these two approaches are equivalent. The second approach leads us to consider the modular group and its action on the hyperbolic plane, which will be important when we consider maps on surfaces.

1.1 Elliptic curves.

An *elliptic curve* is an algebraic curve E given by an equation

$$y^2 = p(x)$$

where p is a cubic polynomial in $\mathbf{C}[x]$ with three distinct roots, which we will denote by e_1, e_2 and e_3. (Despite the name, these curves are *not* ellipses, and there is little connection between them; the name arises because efforts in the 18th century to calculate the perimeter of an ellipse gave rise to integrals of the form $\int p(x)^{-1/2}\,dx$, where p is a cubic polynomial, and hence to the study of algebraic curves of the above form.)

The *discriminant* of $p(x)$ is defined to be

$$\Delta = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2.$$

The statement that $p(z)$ has distinct roots is equivalent to the statement that $\Delta \neq 0$.

By applying an affine transformation to replace x with $ax + b$ for suitable constants a and b, one can convert any elliptic curve E into *Weierstrass normal form*

$$y^2 = 4x^3 - c_2x - c_3$$

where $c_2, c_3 \in \mathbf{C}$. It is then simple to show that $\Delta = c_2^3 - 27c_3^2$. Alternatively, by applying such transformations to both x and y one can put E into *Legendre normal form*

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

where $\lambda \in \mathbf{C} \setminus \{0, 1\}$.

Exercise 1.1. Find the discriminant for the elliptic curve $y^2 = x^3 - 9x^2 + 23x - 15$. Put the curve into Weierstrass and Legendre normal forms.

By writing the equation for E as $y = \sqrt{p(x)}$ we can regard y as a two-valued function of x, so that the projection $(x, y) \mapsto z$ gives E as a two-sheeted covering of the Riemann

sphere $\hat{\mathbf{C}} = \mathrm{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$. Each $x \in \hat{\mathbf{C}}$ is covered by two points $(x, y) \in E$, differing by multiplying y by -1, with the exception of the four points e_1, e_2, e_3 and ∞, which are covered by only one point $(0, e_j)$ or (∞, ∞) in E. (Strictly speaking, we should represent E as a *projective* curve in $\mathrm{P}^2(\mathbf{C})$ in order to allow (∞, ∞) to be a point on E covering $\infty \in \hat{\mathbf{C}}$.)

If we let x rotate once around e_j in the positive direction, by putting $x = e_j + re^{i\theta}$ for some small fixed r and letting θ increase from 0 to 2π, then $\sqrt{x - e_j}$ and hence y are multiplied by $e^{i\pi} = -1$, so the point (x, y) in E moves from one sheet of the surface to the other. The same applies if we rotate around ∞ by using a circle $x = re^{i\theta}, 0 \leq \theta \leq 2\pi$, for large fixed r, so the covering is branched over the three roots e_j and ∞. We can therefore form the Riemann surface of $y = \sqrt{p(x)}$ by taking two copies of $\hat{\mathbf{C}}$ (one for each branch of the function) and joining them across two disjoint cuts between e_1 and e_2 and between e_3 and ∞. These cuts make each copy of $\hat{\mathbf{C}}$ into an annulus, and joining these two annuli across the cuts creates a torus. This is the Riemann surface associated with the elliptic curve $y^2 = p(x)$, a compact surface of genus $g = 1$.

(As a generalisation, we can similarly construct the Riemann surface of a *hyperelliptic curve* $y^2 = p(x)$, where p is a polynomial of degree n with distinct roots. It has genus $\lfloor (n-1)/2 \rfloor$.)

1.2 Lattices and tori.

We now consider an alternative construction of Riemann surfaces of genus 1. We will see the connection between these two approaches later in the lecture. Let ω_1 and ω_2 be two elements of $\mathbf{C}$ which are linearly independent over $\mathbf{R}$. The *lattice* they span is the set

$$\Lambda = \Lambda(\omega_1, \omega_2) = \omega_1 \mathbf{Z} + \omega_2 \mathbf{Z} = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbf{Z}\} \subset \mathbf{C}.$$

We call ω_1, ω_2 a *basis* for Λ. It is easy to check that Λ is a subgroup of $\mathbf{C}$ under addition. It is *discrete* in the sense that each element of Λ has an open neighbourhood containing no other elements of Λ, so that Λ inherits the discrete topology from $\mathbf{C}$.

We say that two elements z, z' of $\mathbf{C}$ are *equivalent* mod Λ, written $z \equiv z' \bmod \Lambda$, if they lie in the same coset of Λ in $\mathbf{C}$, that is, if $z - z' \in \Lambda$. The parallelogram $P = \{x\omega_1 + y\omega_2 \mid x, y \in [0, 1]\}$ is a *fundamental region* for Λ in the sense that every element of $\mathbf{C}$ is equivalent to some element of P, and if two elements of P are equivalent then they both lie on the boundary ∂P of P. This means that we can form the quotient space $\mathbf{C}/\Lambda$ by identifying equivalent pairs of points in ∂P. The resulting space $\mathbf{C}/\Lambda = P/\Lambda$ is homeomorphic to a torus, but it has extra structure: because Λ is discrete it inherits the structure of a Riemann surface from $\mathbf{C}$, and because Λ is a normal subgroup of $\mathbf{C}$ it inherits the structure of an abelian group, isomorphic to $\mathbf{R}^2/\mathbf{Z}^2 \cong (S^1)^2$.

1.3 Elliptic functions.

Elliptic functions are doubly periodic meromorphic functions. We say that a function f defined on $\mathbf{C}$ is *doubly periodic* if it is invariant with respect to a lattice Λ, that is, $f(z + \omega) = f(z)$ for all $z \in \mathbf{C}$ and $\omega \in \Lambda$, so that we can regard f as a function on $\mathbf{C}/\Lambda$ by defining $f(z + \Lambda) = f(z)$. We say that f is meromorphic if, at each point $a \in \mathbf{C}$, f is

either holomorphic (i.e. analytic) or has a pole of finite order, so that f can be represented near a by a Laurent series

$$f(z) = \sum_{n=k}^{\infty} a_n (z-a)^n$$

for some finite k. Thus the elliptic functions are those which are meromorphic on a torus $\mathbf{C}/\Lambda$. For a given lattice Λ, the set $F(\Lambda)$ of all such functions is closed under addition, subtraction, multiplication and division (except by 0), so $F(\Lambda)$ is a field, which can be regarded as the field of meromorphic functions on $\mathbf{C}/\Lambda$.

The most important function in $F(\Lambda)$ is the *Weierstrass function*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega}{}' \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big),$$

where $\sum'_\omega$ denotes summation over all non-zero $\omega \in \Lambda$. One can show that this series is absolutely and uniformly convergent on all compact subsets of $\mathbf{C} \setminus \Lambda$, so $\wp$ is meromorphic on $\mathbf{C}$: it has poles of order 2 at the lattice-points $\omega \in \Lambda$ and it is analytic elsewhere. (It is tempting to write down the simpler series $\sum_\omega (z-\omega)^{-2}$, but unfortunately this does not converge; the extra terms $-1/\omega^2$ are included in the formula for $\wp$ to ensure convergence.) Note that $\wp$ is an even function (use $\Lambda = -\Lambda$): this will be useful later.

We need to show that $\wp$ is doubly periodic with respect to Λ, so that $\wp \in F(\Lambda)$. However the terms $-1/\omega^2$ in the formula make a direct proof difficult, so instead we take an indirect route, first proving that the derivative of $\wp$ is an elliptic function. Uniform convergence allows us to differentiate term by term, giving

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

where the summation is now over *all* $\omega \in \Lambda$. This is a meromorphic function, with poles of order 3 at the lattice points.

Exercise 1.2. Show that $\wp'$ is doubly periodic wth respect to Λ, so that $\wp' \in F(\Lambda)$. Deduce that $\wp$ is doubly periodic wth respect to Λ, so that $\wp \in F(\Lambda)$.

Since $F(\Lambda)$ is a field, containing $\wp, \wp'$ and the constant functions, it contains the field $\mathbf{C}(\wp, \wp')$ of all rational functions of $\wp$ and $\wp'$. Conversely, it can be shown that these are the only elliptic functions with respect to Λ, so that $F(\Lambda) = \mathbf{C}(\wp, \wp')$.

The functions $\wp$ and $\wp'$ are not algebraically independent: $\wp$ satisfies a differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$ are constants (depending on Λ) given by the *Eisenstein series* $G_k = \sum'_\omega \omega^{-k}$ for $k = 4, 6$. Apart from a change of notation, this differential equation is essentially the same as the Weierstrass normal form $y^2 = 4x^3 - c_2 x - c_3$ for an elliptic curve E. In fact, one can show that given any constants c_2 and c_3, provided $c_2^3 - 27c_3^2 \neq 0$ (as we are assuming), one can find a lattice $\Lambda \subset \mathbf{C}$ for which $g_2 = c_2$ and

$g_3 = c_3$. Then each $z \in \mathbf{C}$ determines a point $(x, y) = (\wp(z), \wp'(z)) \in E$, where $\wp$ is the Weierstrass function for Λ. One can show that every point on E arises in this way for some z, and that z and z' determine the same point if and only if they are equivalent mod Λ, so E is parametrised by the elements $z + \Lambda$ of $\mathbf{C}/\Lambda$.

This completes the identification of elliptic curves E with tori $\mathbf{C}/\Lambda$. Using the Uniformization Theorem (see later in MA1), one can show every compact Riemann surface of genus 1 arises in these two equivalent ways.

1.4 The modular group.

Riemann surfaces X and X' are defined to be *isomorphic*, written $X \cong X'$, if there is a biholomorphic function $f : X \to X'$, that is, a bijection f such that f and f^{-1} are both holomorphic. One can show that if Λ and Λ' are lattices in $\mathbf{C}$ then $\mathbf{C}/\Lambda \cong \mathbf{C}/\Lambda'$ if and only if Λ and Λ' are similar, meaning that $\Lambda' = \mu\Lambda$ for some $\mu \in \mathbf{C} \setminus \{0\}$. This motivates the definition of the *modulus* $\tau = \omega_2/\omega_1$, since it is invariant under multiplying ω_1 and ω_2 (and hence Λ) by any $\mu \neq 0$. Transposing ω_1 and ω_2 replaces τ with $1/\tau$, so (renumbering if necessary) we can assume that τ is an element of the upper half plane

$$\mathbf{H} = \{\tau \in \mathbf{C} \mid \operatorname{Im} \tau > 0\}.$$

Unfortunately, τ depends not just on Λ but also on our choice of a basis for Λ, so we need to consider what happens when we change the basis. Any two elements of Λ have the form

$$\omega_2' = a\omega_2 + b\omega_1,$$
$$\omega_1' = c\omega_2 + d\omega_1,$$

with $a, b, c, d \in \mathbf{Z}$, and one can show that they form a basis for Λ if and only if $ad - bc = \pm 1$, so that the inverse of the change of basis matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has integer entries. These matrices form the *general linear group* $GL_2(\mathbf{Z})$, and they act on moduli τ by Möbius (or linear fractional) transformations

$$M : \tau \mapsto \tau' = T(\tau) = \frac{a\tau + b}{c\tau + d}.$$

The matrices M with $\det M = -1$ transpose the upper and lower half planes, while those with $\det M = 1$ preserve them, so we may assume that M is an element of the *special linear group* $SL_2(\mathbf{Z}) = \{M \in GL_2(\mathbf{Z}) \mid \det M = 1\}$, a normal subgroup of index 2 in $GL_2(\mathbf{Z})$. The matrices $M = \pm I$ form a normal subgroup of $SL_2(\mathbf{Z})$ which acts trivially on $\mathbf{H}$, so there is an induced action of the *modular group*, or *projective special linear group*

$$\Gamma = PSL_2(\mathbf{Z}) = SL_2(\mathbf{Z})/\{\pm I\} = \{\pm M \mid M \in SL_2(\mathbf{Z})\}$$

on $\mathbf{H}$. This group consists of the transformations

$$T : \tau \mapsto \frac{a\tau + b}{c\tau + d}$$

of $\mathbf{H}$, where $a, b, c, d \in \mathbf{Z}$ and $ad - bc = 1$. What we have shown is that lattices Λ and Λ', with moduli $\tau, \tau' \in \mathbf{H}$ with respect to some bases, are similar if and only if $\tau' = T(\tau)$ for some $T \in \Gamma$. Thus isomorphism classes of tori correspond to orbits of Γ on $\mathbf{H}$.

In order to understand the action of Γ on $\mathbf{H}$ it is useful to consider a fundamental region

$$F = \{\tau \in \mathbf{H} \mid |\tau| \geq 1,\ -1/2 \leq \mathrm{Re}(\tau) \leq 1/2\}$$

for Γ: as in the case of Λ and P, F contains an element from each orbit of Γ, and if two elements of F are in the same orbit then they both lie on the boundary ∂F of F. It follows that $\mathbf{H}$ is tessellated by the images of F under Γ, just as $\mathbf{C}$ is tessellated by the images of P under Λ. This is called the *modular tessellation* of $\mathbf{H}$.

The element $X : \tau \mapsto -1/\tau$ of Γ fixes $\tau = i$, which corresponds to the square lattice $\Lambda(1, i) = \{m + ni \mid m, n \in \mathbf{Z}\}$, and the element $Y : \tau \mapsto (-\tau - 1)/\tau$ fixes $\omega = \zeta_3 = e^{2\pi i/3}$, corresponding to the hexagonal lattice $\Lambda(1, \zeta_3)$. These are hyperbolic rotations through π and $2\pi/3$ around i and ζ_3 respectively. The sides of F are paired by X and by the element $Z : \tau \mapsto \tau + 1$ of Γ. If use these two elements to identify equivalent pairs of boundary points of F, then isomorphism classes of elliptic curves correspond to points in the resulting quotient space $F/\Gamma = \mathbf{H}/\Gamma$.

One can show that X and Y generate Γ, in the sense that every element of Γ can be written as a product of powers of X and Y: for instance $Z = XY^{-1}$, where we compose transformations from right to left. It is clear that $X^2 = Y^3 = 1$, and one can show that these are defining relations for Γ, in the sense that all equations between elements of Γ can be deduced from them. To summarise this concisely, we say that Γ has a presentation

$$\Gamma = \langle\, X, Y \mid X^2 = Y^3 = 1 \,\rangle,$$

where we list the generators first and then the defining relations. This presentation shows that Γ is the free product $C_2 * C_3$ of its cyclic subgroups $\langle\, X \mid X^2 = 1 \,\rangle \cong C_2$ and $\langle\, Y \mid Y^3 = 1 \,\rangle \cong C_3$ of orders 2 and 3, since it is obtained by combining the presentations of these two groups with no additional relations.

There is an important class of subgroups of Γ called the congruence subgroups. For each integer $n \geq 2$, the reduction mod (n) is a ring homomorphism $\mathbf{Z} \to \mathbf{Z}_n$ which induces group homomorphisms $SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}_n)$ and $\phi_n : \Gamma = PSL_2(\mathbf{Z}) \to PSL_2(\mathbf{Z}_n) = SL_2(\mathbf{Z}_n)/\{\pm I\}$. We define the *principle congruence subgroup* $\Gamma(n)$ of Γ to be the kernel $\ker \phi_n$ of ϕ_n. This is a normal subgroup of finite index in Γ. (More generally, a *congruence subgroup* of Γ is any subgroup containing $\Gamma(n)$ for some n; these subgroups are important in number theory.) One can show that ϕ_n is an epimorphism, so that $\Gamma/\Gamma(n) \cong PSL_2(\mathbf{Z}_n)$. A particularly important congruence subgroup is $\Gamma(2)$, consisting of the elements

$$T : \tau \mapsto \frac{a\tau + b}{c\tau + d}$$

of Γ where a and d are odd and b and c are even. One can show that $\Gamma(2)$ is a free group of rank 2, freely generated by the elements $\tau \mapsto \tau/(-2\tau + 1)$ fixing 0 and sending 1 to -1, and $\tau \mapsto (-\tau + 2)/(-2\tau + 3)$ fixing 1 and sending 2 to 0.

Exercise 1.3. Show that Γ acts transitively on the rational projective line $\hat{\mathbf{Q}} = \mathrm{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. Show that $\Gamma(2)$ has three orbits on $\hat{\mathbf{Q}}$, and deduce that $\Gamma/\Gamma(2)$ is isomorphic to S_3, the symmetric group of degree 3.

Since isomorphism classes of elliptic curves correspond to orbits of Γ on $\mathbf{H}$, it would be useful to have a 'well-behaved' function of τ which takes a single value on each orbit of Γ, and takes different values on different orbits. The functions g_2 and g_3 can be regarded as functions $g_2(\tau)$ and $g_3(\tau)$ of τ by evaluating them on the lattice $\Lambda = \Lambda(1, \tau)$ with modulus τ. Unfortunately, if we replace Λ with a similar lattice $\mu\Lambda$, corresponding to an isomorphic elliptic curve, these functions are multiplied by μ^{-4} and μ^{-6} respectively. There is a similar problem with the discriminant function $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$. However, the *elliptic modular function*

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

(which is not in fact an elliptic function!) is invariant under similarity of lattices, so it takes the same value for all elliptic curves in a given isomorphism class. It is independent of the choice of basis of a lattice, so it is invariant under the action of Γ, that is,

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

for all $\tau \in \mathbf{H}$ and all $T \in \Gamma$. One can show that it is holomorphic on $\mathbf{H}$ (since g_2 and g_3 are, with $\Delta \neq 0$), and that it induces a bijection between orbits of Γ on $\mathbf{H}$ and elements of $\mathbf{C}$.

Exercise 1.4. Evaluate J at $\tau = i$ and at $\tau = \zeta_3$ $(= e^{2\pi i/3})$, and find the corresponding elliptic curves.

An alternative is to put each elliptic curve E into Legendre form

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

and to 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, since it depends on which of the roots of the cubic polynomial p we send to 0 and 1. For instance, if we replace x with $1 - x$, so that the right-hand side becomes $(1-x)(-x)(1-x-\lambda) = -x(x-1)(x-(1-\lambda))$, and replace y with iy, so that the left-hand side becomes $-y^2$, we obtain an isomorphic elliptic curve but now λ has been replaced with $1 - \lambda$. A similar substitution (find it!) replaces λ with $1/\lambda$. These two substitutions generate a group isomorphic to S_3 (corresponding to the permutations of the roots e_j of p), giving rise to six possible values

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

(For some λ, there may be repetitions among these values.)

One can define Λ uniquely as a function of τ by noting that $\wp'(z) = 0$ at $z = \omega_1/2$, $\omega_2/2$ and $(\omega_1 + \omega_2)/2$ (proof?), so the roots e_1, e_2 and e_3 of p are at $x = \wp(\omega_1/2), \wp(\omega_2/2)$ and

$\wp((\omega_1+\omega_2)/2)$. An affine transformation $x \mapsto ax+b$ sending, say, e_2 and e_3 to 0 and 1 sends e_1 to

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

This depends only on τ, since if we replace Λ with a similar lattice $\mu\Lambda$ the resulting powers of μ cancel. The function $\lambda(\tau)$ is holomorphic on $\mathbf{H}$, and is invariant under the congruence subgroup $\Gamma(2)$ of Γ, but not under Γ: the elements of the six cosets of $\Gamma(2)$ in Γ send λ to the six values listed above.

The functions λ and J are related by the equation

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

showing the (generically) 6-to-1 relationship between values of λ and of J.

Background material for these topics, including proofs of the unproved assertions, can be found in:

G. A. Jones and D. Singerman, *Complex Function Theory, an Algebraic and Geometric Viewpoint*, Cambridge University Press, 1987.

2. Embeddings of graphs, bipartite maps and monodromy groups

2.1. Bipartite maps

Let $\mathcal{G} = (V, E)$ be a connected finite graph, with V and E the sets of vertices and edges. We will not assume that $\mathcal{G}$ is simple, so we allow loops and multiple edges.

A *map* $\mathcal{M}$ is an embedding $\mathcal{G} \to X$ of $\mathcal{G}$ in a connected surface X, so that the faces (connected components of $X \setminus \mathcal{G}$) are simply connected, that is, homeomorphic to an open disc. We will assume that X is oriented, so it is orientable and a particular orientation has been chosen. (There is a theory of maps on non-orientable surfaces, but we will restrict attention to those which are orientable, since all Riemann surfaces have this property.)

We say that $\mathcal{G}$ is *bipartite* if its vertices can be coloured black or white so that every edge joins a black vertex to a white vertex; this is equivalent to the property that every circuit has even length. We will assume for the moment that $\mathcal{G}$ is bipartite (since the graphs arising from Belyi functions have this property), though later we will relax this condition. A *bipartite map* $\mathcal{B}$ is a map in which the embedded graph $\mathcal{G}$ is bipartite. Every dessin is a bipartite map, since the vertices can be coloured black or white as they cover 0 or 1, and the edges cover the unit interval so they join black and white vertices.

Example 2.1. The equation $J = 4(1-\lambda+\lambda^2)^3/27\lambda^2(1-\lambda)^2$ gives rise to a Belyi function $\beta(z) = 4(1-z+z^2)^3/27z^2(1-z)^2$, corresponding to a dessin $\mathcal{B}_1$ on the sphere $\hat{\mathbf{C}}$. The triple zeros of β at $\zeta_6^{\pm 1}$ give two 3-valent black vertices, the double zeros of $\beta - 1$ at $-1, 1/2, 2$ give three 2-valent white vertices, and the double poles of β at $0, 1, \infty$ give three 4-gonal faces. Since β has degree 6, there are six edges.

Example 2.2. The quotient $\mathcal{B}_2 = \mathcal{B}_1/C_2$ of $\mathcal{B}_1$ by a half-turn around the vertex $1/2$ is a bipartite map on the sphere, with one 3-valent black vertex, two white vertices of valencies 2 and 1, three edges, and two faces.

Example 2.3. The *complete bipartite graph* $K_{m,n}$ has m black and n white vertices, each black and white pair joined by a single edge. There is an embedding $\mathcal{B}_3$ of $K_{3,3}$ on a torus with three hexagonal faces.

If $\mathcal{B}$ is a bipartite map then the orientation of X gives a pair of permutations x and y of E, sending each edge $e \in E$ to the next edge around its incident black or white vertex respectively. (Note that these are in general *not* automorphisms.) The black and white vertices correspond to the cycles of x and y, with valency equal to cycle-length, and the faces correspond to the cycles of xy, with face-size twice the cycle-length. The orders l, m and n of these permutations are the least common multiples of their cycle-lengths. We then have the relations $x^l = y^m = (xy)^n = 1$, or equivalently $x^l = y^m = z^n = xyz = 1$, where we define $z = (xy)^{-1}$. We call the triple (l, m, n) the *type* of $\mathcal{B}$. Thus in the above examples, $\mathcal{B}_1$ and $\mathcal{B}_2$ have type $(3, 2, 2)$ while $\mathcal{B}_3$ has type $(3, 3, 3)$.

The *monodromy group* of a bipartite map $\mathcal{B}$ is the subgroup $G = \langle x, y \rangle$ generated by x and y in the symmetric group $\operatorname{Sym} E$ of all permutations of R. Since $\mathcal{G}$ is connected, this permutation group G is transitive on E. It follows that the action of G on E is equivalent to its action by right multiplication on the cosets $G_e g$ in G of a stabiliser $G_e = \{g \in G \mid eg = e\}$, where $e \in E$. We say that G (or any transitive permutation group) is *regular*, or *acts regularly*, if each stabiliser is the trivial subgroup, $G_e = 1$.

In Example 2.1, $G \cong D_3$, the dihedral group of order 6, acting regularly. The relations $x^3 = y^2 = (xy)^2 = 1$ show that G is a quotient of D_3, and since G is transitive on the six edges we have $|G : G_e| = 6$, so $G \cong D_3$ and $G_e = 1$.

In Example 2.2, G is again isomorphic to D_3, but this time acting on the vertices of a triangle (number the edges of $\mathcal{B}_2$ and the vertices of a triangle to see this); now $G_e \cong C_2$, so G does not act not regularly.

In Example 2.3, $G \cong C_3 \times C_3$ acting regularly. We have $x^3 = y^3 = 1$, and by inspection $xy = yx$, so G is a quotient of $C_3 \times C_3$. Now $K_{3,3}$ has $3^2 = 9$ edges, so arguing as in Example 1 we deduce that G acts regularly.

We define an *algebraic bipartite map* to be a 4-tuple (G, x, y, E) where $G = \langle x, y \rangle$ is a 2-generator transitive permutation group acting on a set E. We can then reconstruct a bipartite map $\mathcal{B}$ by taking E to be the edge-set, with the cycles of x, y and $z = (xy)^{-1}$ giving the black vertices, white vertices and faces, the cyclic order within the cycles giving the orientation, and containment in cycles giving incidence of edges with vertices and faces. The resulting bipartite map $\mathcal{B}$ has monodromy group G. This gives us a correspondence between topological and algebraic bipartite maps, and allows us to apply the theory of groups and their actions.

Exercise 2.1. If $x = (1, 2, \ldots, N)$ and $y = (1, 2)$ in S_N, draw the corresponding bipartite map $\mathcal{B}$ and find its monodromy group G.

2.2 Automorphisms of bipartite maps

An *automorphism* of a bipartite map $\mathcal{B}$ is a permutation of E commuting with x and y, or equivalently with G. For instance, we can see various rotations for $\mathcal{B}_1$ and $\mathcal{B}_3$, and also translations for $\mathcal{B}_3$, but only the identity for $\mathcal{B}_2$. The automorphisms of $\mathcal{B}$ form a group $\operatorname{Aut} \mathcal{B}$, equal to the centraliser $C = C(G) = \{c \in \operatorname{Sym} E \mid cg = gc \text{ for all } g \in G\}$ of G in $\operatorname{Sym} E$.

A permutation group is *semiregular* (or *fixed-point-free*) if its stabilisers are trivial, *regular* if it is transitive and semiregular. Thus it is semiregular, transitive or regular if at most, at least, or exactly one group element takes one point to another.

Theorem 2.1. *Let G be any transitive permutation group, acting on a set E, and let $C = C(G)$ be its centraliser in* $\operatorname{Sym} E$.

(i) *C acts semiregularly.*

(ii) *C acts regularly if and only if G does.*

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

Proof. (i) Let $c \in C$ fix $e \in E$. Since G is transitive, any element of E has the form $e' = eg$ for some $g \in G$, so $e'c = egc = ecg = eg = e'$, that is, $c = 1$.

(ii) If C acts regularly then it is transitive, so its centraliser is semiregular by applying (i) to C; but G centralises C, so G is semiregular, and being transitive it must be regular. Conversely, if G acts regularly its action is equivalent to the action on itself by right multiplication, $\rho_g : e \mapsto eg$; but then left multiplication $\lambda_c : e \mapsto c^{-1}e$ commutes with G by associativity ($c^{-1}(eg) = (c^{-1}e)g$), and this action is transitive, so C is transitive and hence regular by (i).

(iii) $\lambda_c \mapsto c$ gives an isomorphism $C \to G$. □

Exercise 2.2. Show that $C \cong N_G(G_e)/G_e$, where $N_G(G_e)$ is the normaliser of G_e in G.

We say that a bipartite map $\mathcal{B}$ is *regular* if $\mathrm{Aut}\,\mathcal{B}$ (or equivalently its monodromy group G) acts regularly on its edge-set E. Thus our examples $\mathcal{B}_1$ and $\mathcal{B}_3$ are regular, but $\mathcal{B}_2$ is not.

Exercise 2.3. If $\mathcal{B}$ is a regular bipartite map of type (l, m, n) with N edges, what is its genus? Are there finitely or infinitely many regular bipartite maps of a given type and genus?

We define an *isomorphism* $\iota : \mathcal{B} \to \mathcal{B}'$ of bipartite maps to consist of a group isomorphism $\theta : G \to G', x \mapsto x', y \mapsto y'$ and a compatible bijection $\phi : E \to E'$, where 'compatible' means that $\phi(eg) = \phi(e)\theta(g)$ for $g = x, y$ (equivalently for all $g \in G$) and all $e \in E$. We write $\mathcal{B} \cong \mathcal{B}'$ if there is an isomorphism $\mathcal{B} \to \mathcal{B}'$.

Theorem 2.2. *Every bipartite map $\mathcal{B}$ is isomorphic to the quotient $A\backslash\tilde{\mathcal{B}}$ for some regular bipartite map $\tilde{\mathcal{B}}$ and subgroup $A \leq \mathrm{Aut}\,\tilde{\mathcal{B}}$.*

Proof. Let G be the monodromy group of $\mathcal{B}$, let $\tilde{\mathcal{B}}$ be the dessin corresponding to the regular representation of G, so $\tilde{\mathcal{B}}$ is regular with $\mathrm{Aut}\,\tilde{\mathcal{B}} = \{\lambda_g \mid g \in G\} \cong G$, and let A consist of the automorphisms of $\tilde{\mathcal{B}}$ given by left multiplication λ_g where $g \in G_e$, so that $A \cong G_e$. The orbits of A (acting by left multiplication) on $E = G$ are the cosets $G_e g$ of G_e in G, and G acts on these (by right multiplication) to give a bipartite map $A\backslash\tilde{\mathcal{B}}$. It is now straightforward to check that $\mathcal{B} \cong A\backslash\tilde{\mathcal{B}}$. □

This means that we can study all bipartite maps by studying the regular ones and their automorphism groups. We call $\tilde{\mathcal{B}}$, as constructed above, the *canonical regular cover* of $\mathcal{B}$. For instance, in our examples we have $\tilde{\mathcal{B}}_2 = \mathcal{B}_1$ since $\mathcal{B}_2 \cong A\backslash\mathcal{B}_1$ with $A \cong C_2$.

Exercise 2.4. Find $G, C, \tilde{\mathcal{B}}$ and A if $\mathcal{B}$ is a path of N edges, with vertices alternately black and white.

2.3. Maps

Until now we have considered only bipartite maps, but one can extend the theory to deal with maps which are not necessarily bipartite. Given any map $\mathcal{M}$, if we colour its vertices black and insert a white vertex in every edge of $\mathcal{M}$, we obtain a bipartite map $\mathcal{B} = \mathcal{M}^{\mathrm{bip}}$ on the same surface, where the white vertices have valency 2. (This is the analogue of replacing a Belyi function β with a new Belyi function $4\beta(1-\beta)$, so that the point $1 \in \hat{\mathbf{C}}$ is covered only by double points.) The set E of edges of $\mathcal{B}$ corresponds to the set Ω of *darts*, or directed edges, of $\mathcal{M}$; the permutation x acts on these darts by rotating them around the vertices of $\mathcal{M}$ they point to, while y reverses the direction of each dart, so that $y^2 = 1$.

For example, consider the well-known planar map $\mathcal{M}$ which depicts Monsieur Mathieu. Start with a path of two edges, drawn vertically, for his body, add a loop to the top vertex for his head, an edge at the middle vertex for his arm (he has only one), and two edges at the bottom vertex for his legs. These last three edges end in three vertices representing a

hand and two feet. Subdividing the six edges of $\mathcal{M}$ as above, we get a bipartite map $\mathcal{B}$ of type $(3, 2, 11)$ with 12 edges. The monodromy group G is not obvious, but if we number the edges $1, 2, \ldots, 12$ and give the resulting permutations x and y to a program such as GAP, we find that they generate a group $G \cong M_{12}$, the simple Mathieu group of order 95040; the stabiliser G_e of an edge is the simple Mathieu group M_{11} of order 7920, the smallest of the 26 sporadic simple groups. The bipartite map $\mathcal{B}$ has genus 0, but its canonical regular cover $\tilde{\mathcal{B}}$ has genus 3601 (see Exercise 2.3). This dessin $\tilde{\mathcal{B}}$ corresponds to a Belyi function on an algebraic curve defined over $\mathbf{Q}(\sqrt{-11})$, given by an equation of degree 12 with very large coefficients (it takes about a page to write out the equation). It is surprising that such a simple sketch as $\mathcal{M}$ can lead to such sophisticated mathematical structures, and this is one of the reasons why Grothendieck gave the name *dessins d'enfants* (children's drawings) to this subject.

The Galois group of the field $\mathbf{Q}(\sqrt{-11})$ is of order 2, generated by complex conjugation, and if we let this act on the coefficients of the equation and the Belyi function, it sends $\tilde{\mathcal{B}}$, $\mathcal{B}$ and $\mathcal{M}$ to their mirror images. It is hardly surprising that complex conjugation acts in this example by reflection, but later we will see much more interesting actions of Galois groups on dessins.

The algebraic theory of maps is developed in:

G. A. Jones and D. Singerman, Theory of maps on orientable surfaces, *Proc. London Math. Soc.* (3) 37 (1978), 273–307.

There are many papers on the connections between maps and Belyi functions in the following conference proceedings:

L. Schneps (ed.), *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Note Ser. 200 (1994).

For instance:

G. A. Jones and D. Singerman, Maps, hypermaps and triangle groups, pp. 115–145.

There are further papers on this topic in the following two-volume proceedings:

P. Lochak and L. Schneps (eds.), *Geometric Galois Actions I, II*, London Math. Soc. Lecture Note Ser. 242, 243 (1997).

For instance, in volume II:

G. A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups, pp. 25–65.

For information on the sporadic simple groups, including the Mathieu groups, see:

M. Aschbacher, *Sporadic Groups*, Cambridge University Press, 1994.

J. H. Conway *et al.*, *ATLAS of Finite Groups*, Oxford University Press, 1985.

3. Galois theory

3.1. Basic Galois Theory

Every field F has an algebraic closure $\overline{F}$, a minimal extension of F over which every polynomial $f \in F[x]$ splits into linear factors. It is unique up to isomorphisms fixing F, and is an algebraic extension of F, that is, every $\alpha \in \overline{F}$ is a root of some non-zero $f \in F[x]$, or equivalently $|F(\alpha) : F| < \infty$. An important case, motivated by Belyi's Theorem, is where F is the rational field $\mathbf{Q}$, so that we can take $\overline{\mathbf{Q}} = \{\alpha \in \mathbf{C} \mid f(\alpha) = 0, 0 \neq f \in \mathbf{Q}[x]\}$, the field of algebraic numbers.

An extension $K \supseteq F$ is *Galois*, or *normal*, if each embedding $e : K \to \overline{F}$ fixing F satisfies $e(K) = K$. (Strictly speaking, Galois means normal and separable, where 'separable' means that irreducible polynomials have distinct roots; however, we can ignore this distinction and avoid problems about separability by assuming from now on that all fields discussed have characteristic 0, since in this case all extensions are separable.)

Example 3.1. Let $F = \mathbf{Q}$ and $K = \mathbf{Q}(\zeta_n)$, the nth cyclotomic field, where $\zeta_n = \exp(2\pi i/n)$. Each embedding of K in $\overline{\mathbf{Q}}$ sends ζ_n to some nth root of unity $\zeta_n^j \in K$, so $e(K) = K$ and the extension is Galois.

Example 3.2. Let $F = \mathbf{Q}$ and $K = \mathbf{Q}(\alpha)$, where $\alpha = 2^{1/3} \in \mathbf{R}$. There is an embedding $e : K \to \overline{\mathbf{Q}}$ sending α to $\alpha\zeta_3$, which is not real and hence not in K, so $e(K) \neq K$ and the extension is not Galois.

The following result is useful and not difficult to prove:

Theorem 3.1. *An extension $K \supseteq F$ is finite and Galois if and only if K is the splitting field of some $f \in F[x]$.* □

The *Galois group* $\operatorname{Gal} K$ of a field K is the group of field automorphisms of K. If H is a subgroup of $\operatorname{Gal} K$, then $\operatorname{Fix} H$ denotes the subfield fixed pointwise by H. If F is a subfield of K, then $\operatorname{Gal} K/F$ denotes the subgroup of $\operatorname{Gal} K$ fixing F pointwise.

In Theorem 3.1, $G = \operatorname{Gal} K/F$ permutes the roots of f faithfully, so we can embed G in the symmetric group S_n, where $n = \deg(f)$. It can also be shown that $|G| = |K : F|$.

Example 3.3. Let $F = \mathbf{Q}$ and $K = \mathbf{Q}(\alpha, \zeta_3)$, where α is as in Example 3.2. Then K is the splitting field of $f(x) = x^3 - 2 \in \mathbf{Q}[x]$. This extension has degree $|K : F| = 6$: for instance, we can take 1, α, α^2, ζ_3, $\alpha\zeta_3$, $\alpha^2\zeta_3$ as a basis for K over F. The three roots $\alpha_j = \alpha\zeta_3^j$ of f in K are permuted faithfully by $G = \operatorname{Gal} K/F$, giving an embedding of G in S_3. Since $|G| = |K : F| = 6 = |S_3|$ we have $G \cong S_3$.

Theorem 3.2 (Fundamental Theorem of Finite Galois Theory). *Let $K \supseteq F$ be a finite Galois extension, and let $G = \operatorname{Gal} K/F$. Then there is an order-reversing bijection $L \mapsto H = \operatorname{Gal} K/L$ between the subfields L of K containing F and the subgroups H of G. The inverse of this bijection is given by $H \mapsto L = \operatorname{Fix} H$. We have $|K : L| = |H|$ and $|L : F| = |G : H|$. The extension $L \supseteq F$ is Galois if and only if H is normal in G, in which case $\operatorname{Gal} L/F \cong G/H$.* □

In Example 3.1, for instance, $\operatorname{Gal} \mathbf{Q}(\zeta_n)/\mathbf{Q} = \{\theta_j : \zeta_n \mapsto \zeta_n^j \mid (j, n) = 1\}$, isomorphic to the multiplicative group $U_n = \mathbf{Z}_n^*$ of units mod (n). This group has order $|U_n| = \phi(n) =$

$|\mathbf{Q}(\zeta_n) : \mathbf{Q}|$. Since U_n is abelian, all its subgroups are normal, so all subfields of $\mathbf{Q}(\zeta_n)$ are Galois extensions of $\mathbf{Q}$.

In Example 3.3, the normal subgroup $H = A_3 \cong C_3$ of index 2 in $G = S_3$ corresponds to the subfield $L = \mathbf{Q}(\zeta_3)$ of K, a Galois extension of $\mathbf{Q}$ with $\operatorname{Gal} L/\mathbf{Q} \cong A_3$ and $\operatorname{Gal} K/L \cong S_3/A_3 \cong C_2$. There is also a conjugacy class of three subgroups of index 3 in G, the stabilisers of the roots α_j of f, corresponding to the subfields $L = \mathbf{Q}(\alpha_j)$; these are non-Galois extensions of $\mathbf{Q}$ of degree 3, with $\operatorname{Gal} K/L \cong C_2$. There are no other proper subgroups of G, so we have described all the subfields of K.

Exercise 3.1. Find the splitting field K for the polynomial $f(x) = x^n - 2 \in \mathbf{Q}[x]$, describe $\operatorname{Gal} K/\mathbf{Q}$, and find the subgroups fixing ζ_n and $\alpha = 2^{1/n} \in \mathbf{R}$.

3.2. The absolute Galois group

The *absolute Galois group* of a field F is $\operatorname{Gal} \overline{F}/F$. We will refer to $\mathbf{G} = \operatorname{Gal} \overline{\mathbf{Q}}/\mathbf{Q}$ as simply the *absolute Galois group*. Let $\mathcal{K}$ denote the set of finite Galois extensions K of $\mathbf{Q}$ in $\overline{\mathbf{Q}}$, the splitting fields of the polynomials in $\mathbf{Q}[x]$ by Theorem 3.1. For each $K \in \mathcal{K}$ let G_K denote $\operatorname{Gal} K/\mathbf{Q}$, a finite group of order $|K : \mathbf{Q}|$.

Theorem 3.3. (i) $\overline{\mathbf{Q}}$ *is the union of the fields* $K \in \mathcal{K}$.

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

Proof. (i) Each $K \in \mathcal{K}$ is a finite extension of $\mathbf{Q}$, so if $\alpha \in K$ then $|\mathbf{Q}(\alpha) : \mathbf{Q}| \leq |K : \mathbf{Q}| < \infty$ and hence $\alpha \in \overline{\mathbf{Q}}$. Conversely, each $\alpha \in \overline{\mathbf{Q}}$ is a root of a non-zero polynomial in $\mathbf{Q}[x]$ and hence lies in its splitting field $K \in \mathcal{K}$.

(ii) This follows from the fact that each $K \in \mathcal{K}$ is a Galois extension of $\mathbf{Q}$. □

This imples that each $g \in \mathbf{G}$ is uniquely determined by its restrictions $g_K \in G_K$ to the fields $K \in \mathcal{K}$. If $K, L \in \mathcal{K}$ and $K \supseteq L$ then since the extension $L \supseteq \mathbf{Q}$ is Galois, G_K leaves L invariant, so the restriction mapping gives a group-homomorphism $\rho_{K,L} : G_K \to G_L,\ g_K \mapsto g_L = g_K|_L$. In the notation of Theorem 3.2, $\ker \rho_{K,L}$ is the normal subgroup $H = \operatorname{Gal} K/L$ of G_K. The image of $\rho_{K,L}$ has order $|G_K : H| = |L : F| = |\operatorname{Gal} L/F| = |G_L|$, so $\rho_{K,L}$ is an epimorphism, that is, every element of G_L extends (in $|H| = |K : L|$ ways) to an element of G_K.

We have shown that any $g \in \mathbf{G}$ determines an element $g_K \in G_K$ for each $K \in \mathcal{K}$, so that $\rho_{K,L}(g_K) = g_L$ whenever $K \supseteq L$. Conversely, given $g_K \in G_K$ for each $K \in \mathcal{K}$, satisfying this condition, we obtain an element $g \in \mathbf{G}$ by defining $g(\alpha) = g_K(\alpha)$ where $\alpha \in K \in \mathcal{K}$: this is well-defined, since if $\alpha \in K_i$ $(i = 1, 2)$ where each $K_i \in \mathcal{K}$, then α is contained in the subfield $K = K_1 K_2$ generated by K_1 and K_2; this field is in $\mathcal{K}$, and contains each K_i, so $g_{K_1}(\alpha) = g_K(\alpha) = g_{K_2}(\alpha)$. Thus we can make the identification

$$\mathbf{G} = \{g = (g_K) \in \prod_{K \in \mathcal{K}} G_K \mid \rho_{K,L}(g_K) = g_L \text{ whenever } K \supseteq L\}$$

of $\mathbf{G}$ with the subgroup of the cartesian product $\mathbf{\Pi} = \prod_{K \in \mathcal{K}} G_K$ consisting of the elements $g = (g_K)$ whose coordinates g_K are compatible with the restriction homomorphisms $\rho_{K,L}$. This is the *projective* or *inverse limit*

$$\mathbf{G} = \varprojlim G_K$$

of the groups G_K and homomorphisms $\rho_{K,L}$, a *profinite* group, that is, a projective limit of finite groups. For more on the theory of profinite groups, see the books on the subject by A. Lubotzky & D. Segal, or by J. S. Wilson.

Exercise 3.2. Show that $\cup_{n\geq 1}\mathbf{Q}(\zeta_n)$ is a subfield of $\overline{\mathbf{Q}}$, and describe its Galois group.

Exercise 3.3. What are the cardinalities of $\overline{\mathbf{Q}}$ and of $\mathbf{G}$?

3.3. The Krull topology

Unlike in finite extensions, not every subgroup of $\mathbf{G}$ corresponds to a subfield of $\overline{\mathbf{Q}}$. We need to put a topology on $\mathbf{G}$ so that subfields correspond to closed subgroups.

The discrete topology on each G_K (in which every subset is open) defines a product topology on $\mathbf{\Pi} = \prod_{K\in\mathcal{K}} G_K$, the weakest topology in which the projections $\mathbf{\Pi} \to G_K$ are all continuous. As a subset of $\mathbf{\Pi}$, $\mathbf{G}$ inherits a topology, the *Krull topology*. Intuitively, two elements of $\mathbf{G}$ are 'close together' if they agree on a large subfield of $\overline{\mathbf{Q}}$. Multiplication and inversion are clearly continuous functions in each factor G_K, so they are also continuous in $\mathbf{\Pi}$ and $\mathbf{G}$, which are therefore topological groups.

Exercise 3.4. Show that $\mathbf{G}$ is a closed subgroup of $\mathbf{\Pi}$, and that $\mathbf{\Pi}$ and $\mathbf{G}$ are compact Hausdorff spaces.

Warning: the topology on $\mathbf{G}$ is not pleasant: the structure is fractal rather than smooth, and in fact $\mathbf{G}$ can be shown to be homeomorphic to the Cantor set

$$\left\{ \sum_{n=1}^{\infty} a_n 3^{-n} \in [0,1] \mid \text{each } a_n = 0 \text{ or } 2 \right\}.$$

With this topology, the Galois correspondence applies to the extension $\overline{\mathbf{Q}} \supset \mathbf{Q}$ as in Theorem 3.2, except that the bijection is now between subfields L and *closed* subgroups H of $\mathbf{G}$.

Exercise 3.5. Show that in any topological group, each open subgroup is closed, and each closed subgroup of finite index is open.

Many books cover basic Galois Theory; those considering infinite extensions include:

N. Jacobson, *Basic Algebra I, II*, Freeman, 1985, 1989.

S. Lang, *Algebra*, Addison-Wesley, 1965.

For a description and topological characterisation of the Cantor set, see §2-15 of:

J. G. Hocking and G. S. Young, *Topology*, Addison-Wesley, 1961.

For the theory of profinite groups, see:

A. Lubotzky and D. Segal, *Subgroup Growth*, Birkhäuser, 2003.

J. S. Wilson, *Profinite Groups*, Oxford University Press, 1998.

4. From dessins to holomorphic structures

4.1. Coverings

We can generalise the idea of an isomorphism between algebraic bipartite maps, as defined in Lecture 2. A *morphism* or *covering* $\gamma : \mathcal{B} = (G, x, y, E) \to \mathcal{B}' = (G', x', y', E')$ consists of a homomorphism $\theta : G \to G'$ sending $x \mapsto x', y \mapsto y'$ and a compatible function $\phi : E \to E'$, that is, $\phi(eg) = \phi(e)\theta(g)$ for $g = x, y$, or equivalently for all $g \in G$, and for all $e \in E$.

Example 4.1. We considered a covering $\mathcal{B}_1 \to \mathcal{B}_2 = C_2\backslash\mathcal{B}_1$ in Examples 2.1 and 2.2. More generally, if $A \leq \operatorname{Aut}\mathcal{B}$ then we have a covering $\mathcal{B} \to \mathcal{B}' = A\backslash\mathcal{B}$, with G', x', y' the induced actions of G, x, y on $E' = A\backslash E$ (see Theorem 2.2). We call such a covering, induced by a group of automorphisms, a *regular* or *normal* covering.

Exercise 4.1. Show that in any covering, θ and ϕ must be epimorphisms.

A covering γ is an isomorphism if θ and ϕ are bijections, in which case it is an automorphism if $\mathcal{B} = \mathcal{B}'$. Recall Exercise 2.2: the automorphisms of $\mathcal{B}$ form a group $\operatorname{Aut}\mathcal{B} = C(G) \cong N_G(G_e)/G_e$, where $C(G)$ is the centraliser of G in $\operatorname{Sym} E$.

Compositions of coverings are coverings, and the identity is a covering, so algebraic bipartite maps and their coverings form a category. The analogue of a covering for (topological) bipartite maps is a surface covering $X \to X'$, preserving the orientation, such that black vertices, white vertices, edges and faces on X' to lift to the same on X, and there is branching only over vertices and face-centres. Topological bipartite maps and their coverings form a category, and Lecture 2 describes a functor from topological to algebraic bipartite maps. It is easy to define a functor in the opposite direction, but we will try to do better by constructing a functor from algebraic to holomorphic bipartite maps, that is, topological bipartite maps on Riemann surfaces.

4.2. Triangle groups and universal bipartite maps

We will consider bipartite maps $\mathcal{B}$ of a fixed type (l, m, n), so $x^l = y^m = z^n = xyz = 1$ in the monodromy group G of $\mathcal{B}$. To do this we consider the (abstract) group

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

so G is a quotient of Δ by $X \mapsto x$, etc. We can then regard $\mathcal{B}$ as a transitive action of Δ on E, using the composition of homomorphisms $\Delta \to G \to \operatorname{Sym} E$, and conversely any transitive action of Δ gives rise to an algebraic bipartite map, with black vertices, white vertices and faces corresponding to the cycles of X, Y and Z. (However, note that this may give rise to maps of types (l', m', n') dividing (l, m, n), meaning that $l' \mid l$ etc.)

The transitive actions of Δ form a subcategory of the category of algebraic bipartite maps, with bipartite maps $\mathcal{B}$ corresponding to conjugacy classes of *map subgroups*, namely the edge-stabilisers $\Delta_e \leq \Delta$. A bipartite map $\mathcal{B}$ is compact if and only if Δ_e has finite index in Δ. Coverings $\mathcal{B} \to \mathcal{B}'$ correspond to inclusions $\Delta_e \leq \Delta_{e'}$, and $\operatorname{Aut}\mathcal{B} \cong N_\Delta(\Delta_e)/\Delta_e$ (Exercise 2.2), so a covering $\mathcal{B} \to \mathcal{B}'$ is regular if and only if $\Delta_e \leq \Delta_{e'}$ is a normal inclusion. Theorem 2.1 and Exercise 2.2 also give:

Theorem 4.1. *A bipartite map $\mathcal{B}$ is regular if and only if Δ_e is a normal subgroup of Δ, in which case* $\mathrm{Aut}\,\mathcal{B} \cong G \cong \Delta/\Delta_e$. □

Example 4.2. Let $\mathcal{B}$ correspond to the regular representation of the group $G = C_n \times C_n = \langle x, y \mid x^n = y^n = 1, xy = yx \rangle$. The elements x, y and xy have order n, so $\mathcal{B}$ has type (n, n, n) and we take $\Delta = \Delta(n, n, n)$. The map subgroups Δ_e are all equal, coinciding with the kernel of the epimorphism $\Delta \to G, X \mapsto x$ etc. This is a normal subgroup of Δ, and since G is abelian it contains the commutator subgroup Δ' of Δ; both subgroups have index n^2 in Δ, so $\Delta_e = \Delta'$. This map has automorphism group $\mathrm{Aut}\,\mathcal{B} \cong G \cong C_n \times C_n$.

The triangle group of type (l, m, n), denoted by $\langle l, m, n \rangle$ in Jürgen's lectures, has the same presentation as Δ, so these two groups are isomorphic. We may therefore identify the abstract group Δ with the geometric group $\langle l, m, n \rangle$ by taking a triangle T with angles π/l, π/m, π/n, and representing X, Y and Z as rotations through $2\pi/l$, $2\pi/m$ and $2\pi/n$ about the vertices of T.

We will assume that $l^{-1} + m^{-1} + n^{-1} < 1$ (the most typical case), so that Δ acts on $\mathbf{H}$; there are similar arguments involving $\mathbf{C}$ or $\hat{\mathbf{C}}$ if $l^{-1} + m^{-1} + n^{-1} = 1$ or > 1. The hyperbolic plane $\mathbf{H}$ is tessellated by the images of T under the extended triangle group $\Delta[l, m, n]$, generated by reflections in the sides of T, and $\Delta(l, m, n)$ is the even subgroup of index 2, preserving the orientation of $\mathbf{H}$.

We can colour the vertices of this tessellation black, white or red as they are images of the vertex of T fixed by X, Y or Z. Every triangle has one vertex of each colour, with valencies $2l, 2m$ or $2n$. If we delete the red vertices and their incident edges, we get a bipartite map $\mathcal{B}_\infty(l, m, n)$, the *universal bipartite map of type* (l, m, n) on $\mathbf{H}$. It is regular, with $\mathrm{Aut}\,\mathcal{B}_\infty(l, m, n) = \Delta(l, m, n)$, and has edge-stabilisers $\Delta_e = 1$.

Theorem 4.2. *Any bipartite map $\mathcal{B}$ of type dividing (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 of* $\mathrm{Aut}\,\mathcal{B}_\infty(l, m, n)$.

Proof. Given $\mathcal{B} = (G, x, y, E)$, take the group A induced by Δ_e where $e \in E$, as in Theorem 2.2. □

4.3. Holomorphic structures

The map $A\backslash\mathcal{B}_\infty(l, m, n)$ in Theorem 4.2 has extra holomorphic structure, so let us denote it by $\mathcal{B}^{\mathrm{hol}}$: since $\mathbf{H}$ is a Riemann surface, and Δ_e acts as a discontinuous group of automorphisms of $\mathbf{H}$ (since Δ does), it follows that $\mathcal{B}^{\mathrm{hol}}$ lies on a Riemann surface $X = \Delta_e\backslash\mathbf{H}$.

Morphisms $\mathcal{B} \to \mathcal{B}'$ of algebraic maps correspond to inclusions $\Delta_e \leq \Delta_{e'}$ of map subgroups of Δ, so they induce branched coverings $X \to X'$ of the corresponding Riemann surfaces. In particular, taking $\Delta_{e'} = \Delta$, corresponding to the trivial bipartite map $\mathcal{B}'$ with one edge, we get a covering $X \to X' = \Delta\backslash\mathbf{H} \cong \hat{\mathbf{C}}$ branched over just three points, corresponding to the orbits of Δ consisting of the black, white and red vertices. If X is compact then this is a Belyi function, so Belyi's Theorem implies:

Theorem 4.3. *If $\mathcal{B}$ is a finite algebraic map, then the Riemann surface X underlying $\mathcal{B}^{\mathrm{hol}}$ is defined, as a smooth projective algebraic curve, over $\overline{\mathbf{Q}}$.* □

Example 4.3. If $\mathcal{B}$ is as in Example 4.2 then X is the nth degree Fermat curve, with affine model $x^n + y^n = 1$ and Belyi function $\beta : (x, y) \mapsto x^n$. The black and white vertices of $\mathcal{B}^{\rm hol}$ are the points $v_j = (0, \zeta_n^j)$ and $w_k = (\zeta_n^k, 0)$ on X, with $j, k \in \{0, 1, \ldots, n-1\}$. The edge $v_j w_k$ consists of the points $(r\zeta_n^k, s\zeta_n^j)$ where $r, s \in [0, 1]$ satisfy $r^n + s^n = 1$.

We have $\mathrm{Aut}\,\mathcal{B} \cong \mathrm{Aut}\,\mathcal{B}^{\rm hol} \cong N_\Delta(\Delta_e)/\Delta_e \leq N_{PSL_2\mathbf{R}}(\Delta_e)/\Delta_e \cong \mathrm{Aut}\,X$, so the automorphisms of $\mathcal{B}$ induce automorphisms of X.

Example 4.4. If $\mathcal{B}$ is as in Examples 4.2 and 4.3 then $\mathrm{Aut}\,\mathcal{B} \cong C_n \times C_n$, acting on X by multiplying the coordinates x and y by nth roots of 1. However, in this case $\mathrm{Aut}\,X$ is larger, a semidirect product of $C_n \times C_n$ by S_3: the extra S_3 comes from forgetting the colours (black, white, red) of the vertices of the induced triangulation of X, and allowing all possible permutations of the colours. Algebraically, this is best seen by writing X in projective form $x^n + y^n + z^n = 0$ and permuting the coordinates.

Exercise 4.2. Explain Example 4.4 by giving a geometric description of $N_{PSL_2\mathbf{R}}(\Delta_e)$.

4.4. Non-cocompact triangle groups

Suppose that we want to consider bipartite maps of type $(3, 2, n)$ for all n, not just for some fixed n. Equivalently, by removing white vertices of valency 2, we consider all trivalent maps (not necessarily bipartite). We take

$$\Delta = \Delta(3, 2, \infty) = \langle X, Y, Z \mid X^3 = Y^2 = Z^\infty = XYZ = 1\rangle = \langle X, Y \mid X^3 = Y^2 = 1\rangle$$

(a free product $C_3 * C_2$), where we regard the relation $Z^\infty = 1$ as vacuous. We obtain the same algebraic theory as before, but with no restrictions on the face-sizes n, and the same applies to other types besides $(3, 2, \infty)$.

In the above case we take the triangle T to have a black vertex at ζ_3 with angle $\pi/3$, a white vertex at i with angle $\pi/2$, and a red vertex at ∞ on $\partial\mathbf{H}$ with angle $\pi/\infty = 0$, called an *ideal vertex*. Reflections in the sides of T generate the extended triangle group $\Delta[3, 2, \infty]$, and the images of T under this group tessellate $\mathbf{H}$, with red vertices at the images of ∞, i.e. on $\mathrm{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$ (see Exercise 1.3). The triangle group Δ is the even subgroup of index 2 in $\Delta[3, 2, \infty]$.

Exercise 4.3. Show that $\Delta[3, 2, \infty] = PGL_2(\mathbf{Z})$, consisting of the transformations

$$\tau \mapsto \frac{a\tau + b}{c\tau + d} \quad \text{where } a, b, c, d \in \mathbf{Z},\ ad - bc = 1,$$

and

$$\tau \mapsto \frac{a\overline{\tau} + b}{c\overline{\tau} + d} \quad \text{where } a, b, c, d \in \mathbf{Z},\ ad - bc = -1.$$

Deleting the red vertices and their incident edges gives a bipartite map $\mathcal{B}_\infty(3, 2, \infty)$, the *universal bipartite map of type* $(3, 2, \infty)$, and removing its white vertices gives the *universal trivalent map*. Both of these maps are regular, with the modular group $\Gamma = PSL_2(\mathbf{Z}) = \Delta(3, 2, \infty)$ as their automorphism group.

As before, given a bipartite map $\mathcal{B}$ of type $(3,2,n)$ for some n, we can construct a holomorphic bipartite map $\mathcal{B}^{\rm hol}$ on $\Delta_e\backslash\mathbf{H}$ by taking the quotient of $\mathcal{B}_\infty(3,2,\infty)$ by an appropriate subgroup Δ_e of $\Delta = \Delta(3,2,\infty)$. However, in this case there are punctures at the face-centres, corresponding to the red vertices on $\partial\mathbf{H}$ but not on $\mathbf{H}$, so we compactify the surface by inserting these points, one for each orbit of Δ_e on $\mathrm{P}^1(\mathbf{Q})$. This gives us a compact Riemann surface X, isomorphic to that obtained earlier from $\Delta(3,2,n)$.

Similarly, we can deal with bipartite maps of all types by using

$$\Delta = \Delta(\infty,\infty,\infty) = \langle X,Y,Z \mid XYZ = 1\rangle = \langle X,Y \mid -\rangle,$$

a free group of rank 2. This time we take T to have three ideal vertices on $\partial\mathbf{H}$: a black vertex at 0, a white vertex at 1, and a red vertex at ∞. Reflections in the sides of T generate the extended triangle group $\Delta[\infty,\infty,\infty]$, and its even subgroup $\Delta(\infty,\infty,\infty)$ is the principal congruence subgroup $\Gamma(2)$ of level 2 in Γ. The images of T under $\Delta[\infty,\infty,\infty]$ tessellate $\mathbf{H}$, with black, white and red vertices at orbits $[0],[1]$ and $[\infty]$ of $\Gamma(2)$ on $\mathrm{P}^1(\mathbf{Q})$, i.e. at the points p/q with p even and q odd, p and q both odd, or p odd and q even (see Exercise 1.3 again). Deleting the red vertices and their incident edges gives $\mathcal{B}_\infty = \mathcal{B}_\infty(\infty,\infty,\infty)$, the *universal bipartite map*, with $\Gamma(2)$ as its automorphism group. Its vertices are the points $p/q \in \mathbf{Q}$ with q odd, coloured black or white as p is even or odd, and there is an edge from p/q to r/s if and only if $ps - qr = \pm 1$. The analogue of Theorem 4.2 is:

Theorem 4.4. *Any bipartite map $\mathcal{B}$ is isomorphic to a quotient of $\mathcal{B}_\infty$ by a subgroup A of* $\mathrm{Aut}\,\mathcal{B}_\infty = \Gamma(2)$. □

Exercise 4.4. Draw $\mathcal{B}_\infty$.

For connections between maps and triangle groups, see:

G. A. Jones and D. Singerman, Maps, hypermaps and triangle groups, in L. Schneps (ed.), *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Note Ser. 200 (1994), pp. 115–145.

For more details about holomorphic structures on maps, see:

J. Wolfart, *ABC for polynomials, dessins d'enfants and uniformization — a survey*, to appear. See the Jyväskylä Summer School website, course MA1.

For a comprehensive study of connections between maps and many other areas of mathematics, see:

S. K. Lando and A. K. Zvonkin, *Graphs on Surfaces and their Applications*, Springer, 2004.

5. Quasiplatonic surfaces and automorphisms

5.1. Quasiplatonic surfaces

Any compact Riemann surface X of genus $g > 1$ is uniformised by a torsion-free Fuchsian group K, which is unique up to conjugation in $PSL_2(\mathbf{R})$. As in Jürgen's lectures, isomorphisms $X \to X'$ of Riemann surfaces lift to isometries of $\mathbf{H}$ conjugating K to the corresponding group K'. Similarly, if we take $X = X'$ we see that automorphisms of X lift to isometries normalising K; since K acts trivially on its quotient space, we have $\operatorname{Aut} X \cong N(K)/K$, where $N(K)$ is the normaliser of K in $PSL_2(\mathbf{R})$.

The situation is similar for genus $g = 1$, as explained in Lecture 1 on elliptic curves. Here we must replace $\mathbf{H}$ with $\mathbf{C}$, and K with a lattice Λ, which is unique up to similarity. We find that $\operatorname{Aut} X \cong N(\Lambda)/\Lambda$, where $N(\Lambda)$ is the normaliser of Λ (regarded as a group of translations) in the automorphism group $AGL_1(\mathbf{C}) = \{z \mapsto az + b \mid a, b \in \mathbf{C}, a \neq 0\}$ of the Riemann surface $\mathbf{C}$. There is no problem when $g = 0$, since the only compact Riemann surface of genus 0 is $\hat{\mathbf{C}}$, and this is simply connected.

We say that a compact Riemann surface of genus $g > 1$ is *quasiplatonic* if it uniformised by a normal subgroup of a triangle group.

Theorem 5.1. *If X is a compact Riemann surface then the following are equivalent:*
(a) X is quasiplatonic;
(b) $N(K)$ is a triangle group;
(c) X has a Belyi function $\beta : X \to \hat{\mathbf{C}}$ which is a regular covering;
(d) X is obtained from a regular dessin.

Proof. (a) $\Rightarrow$ (b). $N(K)$ is a Fuchsian group, and any Fuchsian group containing a triangle group is also a triangle group, by Teichmüller theory.

(b) $\Rightarrow$ (c). The inclusion $K \leq N(K)$ induces a Belyi function $X \cong K\backslash\mathbf{H} \to N(K)\backslash\mathbf{H} \cong \hat{\mathbf{C}}$, regular since the inclusion is normal.

(c) $\Rightarrow$ (d). Using β to lift the trivial dessin (on the unit interval) to X gives the required regular dessin.

(d) $\Rightarrow$ (a). As explained in earlier lectures, regular dessins correspond to normal subgroups of triangle groups. □

Example 5.1. We have seen that the nth degree Fermat curve corresponds to a regular dessin, and is uniformised by a normal subgroup of the triangle group $\Delta(n, n, n)$, so for $n > 3$ it is a quasiplatonic surface.

Exercise 5.1. What are the analogues of the quasiplatonic surfaces for genus $g = 1$?

Property (d) suggests that quasiplatonic surfaces are natural generalisations of the platonic solids, hence their name. They can be characterised as the local maxima for $|\operatorname{Aut} X|$ in the sense that within the Teichmüller space of compact Riemann surfaces of genus g, all other surfaces sufficiently close to X have smaller automorphism groups. This follows from the rigidity of triangle groups.

5.2. Hurwitz groups and surfaces

Here we look for *global* maxima for $|\mathrm{Aut}\, X|$:

Problem. For a given genus $g > 1$, what are the most symmetric Riemann surfaces?

We have $\mathrm{Aut}\, X \cong N(K)/K$. Now $N(K)$ is a Fuchsian group, and it contains K with finite index, equal to the ratio of the areas of their fundamental regions. The region for K has fixed area $(= 4\pi(g-1))$, so for a given g, maximising $|\mathrm{Aut}\, X|$ is equivalent to minimising the area for $N(K)$. It can be shown that, among all Fuchsian groups, this area is minimised by the (essentially unique) triangle group

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

Exercise 5.2. Show that $\Delta(3,2,7)$ has a fundamental region of area $\pi/21$, and that this is the smallest for any triangle group acting on $\mathbf{H}$.

This minimality property implies Hurwitz's bound

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

attained if and only if $X = K\backslash\mathbf{H}$ for some torsion-free normal subgroup K of finite index in $\Delta = \Delta(3,2,7)$, in which case $\mathrm{Aut}\, X \cong \Delta/K$. The compact surfaces X and the finite groups $G = \mathrm{Aut}\, X$ arising in this way are called *Hurwitz surfaces* and *Hurwitz groups*. These surfaces are all quasiplatonic.

Example 5.2. The modular group $\Gamma = PSL_2(\mathbf{Z}) = \Delta(3,2,\infty)$ maps onto $G = PSL_2(7) = PSL_2(\mathbf{Z}_7)$ by reducing coefficients mod (7). The generator $Z : \tau \mapsto \tau + 1$ of Γ maps to an element $z : \tau \mapsto \tau + 1$ of order 7 in G, so G is an epimorphic image Δ/K of $\Delta(3,2,7)$ for some K. Now G has order 168 $(= 7(7^2-1)/2)$, so the surface $X = K\backslash\mathbf{H}$ 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 $\mathrm{Aut}\, X \cong PSL_2(7)$. It carries a trivalent regular map, with 24 heptagonal faces.

Exercise 5.3. Prove that there is no Hurwitz group of genus 2.

5.3. Kernels and epimorphisms

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

Proposition 5.2. *If Δ is a finitely generated group and G is a finite group, then the number $n_\Delta(G)$ of normal subgroups K of Δ with $\Delta/K \cong G$ is given by*

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

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

Proof. These normal subgroups K are the kernels of the epimorphisms $\theta : \Delta \to G$. Two epimorphisms $\theta, \theta' : \Delta \to G$ have the same kernel if and only if $\theta' = \alpha \circ \theta$ for some $\alpha \in \mathrm{Aut}\, G$, so $n_\Delta(G)$ is the number of orbits of $\mathrm{Aut}\, G$ acting by composition on the epimorphisms. Since these are epimorphisms, $\alpha \circ \theta = \theta$ if and only if $\alpha = 1$, so $\mathrm{Aut}\, G$ acts semiregularly and hence all its orbits have size $|\mathrm{Aut}\, G|$. There are only finitely many ways of mapping the generators of Δ into G, so $\mathrm{Epi}\,(\Delta, G)$ is finite and the result follows. □

For many finite groups G, $|\mathrm{Aut}\, G|$ is known, or is easily computed, so it remains to find $|\mathrm{Epi}\,(\Delta, G)|$. In the case of a triangle group

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

finding an epimorphism $\theta : \Delta \to G$ for some G is equivalent to finding a triple $x, y, z \in G$ such that

(a) $x^l = y^m = z^n = xyz = 1$ (so there is a homomorphism $\theta : \Delta \to G, X \mapsto x$, etc), and
(b) x, y and z (or equivalently any two of them) generate G (so θ is an epimorphism).

If we want $K = \ker \theta$ to be torsion-free, then we also require

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

This is because the torsion elements of Δ are the conjugates of the powers of X, Y and Z, so if none of these is in K (apart from 1) then K is torsion-free.

5.4. Direct counting.

Example 5.3. Let us count normal subgroups K of $\Delta = \Delta(5, 2, \infty)$ with $\Delta/K \cong G = A_5$, or equivalently, 5-valent regular maps $\mathcal{M}$ with $\mathrm{Aut}\, \mathcal{M} \cong A_5$. We first count epimorphisms $\Delta \to A_5$. Now A_5 has 24 elements of order 5 (the 5-cycles) and 15 elements of order 2 (the double transpositions), so there are $24 \times 15 = 360$ ways of mapping X, Y to elements x, y of order 5 and 2 in A_5. These must generate a subgroup H of order divisible by 10, and the only possibilities are $H \cong D_5$ and $H = A_5$. There are six subgroups $H \cong D_5$ in A_5 (normalisers of Sylow 5-subgroups), each generated by $4 \times 5 = 20$ pairs x, y, so there are $6 \times 20 = 120$ pairs x, y generating subgroups $H < A_5$. The remaining $360 - 120 = 240$ pairs must generate A_5, so there are 240 epimorphisms $\Delta \to A_5$. Now $\mathrm{Aut}\, A_5 = S_5$ has order $5! = 120$, so it has $240/120 = 2$ orbits on these epimorphisms, and hence there are two normal subgroups K of Δ with $\Delta/K \cong A_5$.

One class of epimorphisms is represented by

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

corresponding to a regular 5-valent map with $60/3 = 20$ triangular faces: clearly this is the icosahedron. The other class is represented by

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

corresponding to a regular 5-valent map with $60/5 = 12$ pentagonal faces. By Exercise 2.3 this has genus

$$g = 1 + \frac{N}{2}\Big(1 - \frac{1}{l} - \frac{1}{m} - \frac{1}{n}\Big) = 1 + \frac{60}{2}\Big(1 - \frac{1}{5} - \frac{1}{2} - \frac{1}{5}\Big) = 4.$$

This is the *great dodecahedron* $\mathcal{G}$ (the polytope $\{5, 5/2\}$ in Coxeter's notation), formed by taking the underlying graph of an icosahedron and attaching a pentagonal face to the 5-cycle around each vertex. An immersion (not an embedding) of this map in $\mathbf{R}^3$ can be bought in toy-shops as an alternative form of Rubik's cube.

The quasiplatonic surface $X = K\backslash\mathbf{H}$ underlying $\mathcal{G}$ is Bring's curve, given in $\mathrm{P}^4(\mathbf{C})$ by the equations

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

The full automorphism group of X is isomorphic to S_5, acting by permuting coordinates; this lifts to the triangle group $\Delta(5, 2, 4)$, which contains $\Delta(5, 2, 5)$ with index 2. The even permutations induce $\mathrm{Aut}\,\mathcal{G} \cong A_5$, while the odd permutations send $\mathcal{G}$ to its dual map $\mathcal{G}^*$, which is distinct from but isomorphic to $\mathcal{G}$ (compare this with the tetrahedron, where $\Delta = \Delta(3, 2, 3)$).

5.5. Counting by character theory

For larger or more complicated groups G, direct counting is of little use, and one needs more subtle methods, such as character theory. For simplicity, however, I will retain $G = A_5$ as the basic example.

A (complex) *representation* of a group G is a homomorphism $\rho : G \to GL(V)$ where V is a vector space over $\mathbf{C}$, so G acts by linear transformations on V. Representations ρ and ρ' on V and V' are *equivalent* if there is an isomorphism $V \to V'$ commuting with the actions of G. A representation ρ is *irreducible* if there are no G-invariant subspaces of V other than 0 and V. A standard theorem of representation theory states that a finite group G has c isomorphism classes of irreducible representations, where c is the number of conjugacy classses in G.

The *character* of a representation ρ is the function $\chi = \chi_\rho : G \to \mathbf{C}, g \mapsto \mathrm{tr}(\rho(g))$, the trace (sum of eigenvalues) of the linear transformation $\rho(g)$. Conjugate elements have the same eigenvalues, and hence the same trace, so χ is constant on each conjugacy class. The *irreducible characters* of G are the characters of its irreducible representations. The *character table* of G is the $c \times c$ array giving the values of the irreducible characters on the conjugacy classes. These are known for many groups G, e.g. see the *ATLAS of Finite Groups*. The following result is proved in many books on representation theory:

Proposition 5.3. *If $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ are conjugacy classes in a finite group G, then the number of solutions of the equation $xyz = 1$ in G, with $x \in \mathcal{X}, y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, is given by*

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

where the sum is over the irreducible complex characters χ of G. □

Here $|\mathcal{X}|.|\mathcal{Y}|.|\mathcal{Z}|/|G|$ is a rough estimate, based on probabilistic conssiderations, and the sum is a correction term since groups do not behave randomly.

In $G = A_5$ there are five conjugacy classes: the identity $\{1\}$, the fifteen double transpositions, the twenty 3-cycles, and two classes of twelve 5-cycles (forming a single class in S_5). It follows that there are five irreducible characters. On the identity element they take

the values $\chi(1) = 1, 3, 3, 4, 5$, on the double transpositions they take the values $1, 1, 1, 0, 1$, on the 3-cycles they take the values $1, 0, 0, 1, -1$, and on the two classes of 5-cycles they take the values $1, (1 \pm \sqrt{5})/2, (1 \mp \sqrt{5})/2, -1, 0$.

Example 5.5. Let us count normal subgroups K of $\Delta = \Delta(3, 3, 5)$ with $\Delta/K \cong A_5$. We first consider epimorphisms $\Delta \to A_5$. There is one choice for the conjugacy classes $\mathcal{X}$ and $\mathcal{Y}$ of elements of order 3, and there are two choices for the class $\mathcal{Z}$ of elements of order 5. In either case, we find that there are

$$\frac{20.20.12}{60}\Big(1 + \frac{-1}{4}\Big) = 60$$

triples $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ such that $xyz = 1$, so there are 120 such triples in all. Since A_5 has no proper subgroups of order divisible by 15, each triple generates A_5. Since $|\mathrm{Aut}\, A_5| = 120$ they form a single orbit, represented by $x = (1, 2, 3)$, $y = (3, 4, 5)$, $z = (1, 3, 5, 4, 2)$. It follows that there is a single normal subgroup K in Δ with $\Delta/K \cong A_5$, corresponding to a single regular bipartite map $\mathcal{B}$ of type $(3, 3, 5)$ with $\mathrm{Aut}\, \mathcal{B} \cong A_5$. This has genus

$$g = 1 + \frac{60}{2}\Big(1 - \frac{1}{3} - \frac{1}{3} - \frac{1}{5}\Big) = 5.$$

It is a double covering of the dodecahedron, branched over its 12 face-centres; the faces are thus 10-gons, with vertices alternately coloured black and white.

Example 5.6. Let us try the same with $\Delta = \Delta(5, 5, 3)$. There are two choices for each of the classes $\mathcal{X}$ and $\mathcal{Y}$, and there is one choice for $\mathcal{Z}$. In each of these four cases, we get

$$\frac{20.12.12}{60}\Big(1 + \frac{1}{4}\Big) = 60$$

triples $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ such that $xyz = 1$, so there are 240 such triples in all. Again, each triple generates A_5. Under automorphisms they form two orbits: in one, represented by $x = (1, 2, 4, 3, 5)$, $y = (1, 4, 3, 2, 5)$, $z = (1, 2, 3)$, x and y are in the same conjugacy class; in the other, represented by $x = (1, 2, 3, 4, 5)$, $y = (1, 3, 2, 4, 5)$, $z = (1, 2, 3)$, they are not. Thus there are two normal sugroups K of Δ with $\Delta/K \cong A_5$, corresponding to two regular bipartite maps $\mathcal{B}$ of type $(5, 5, 3)$ with $\mathrm{Aut}\, \mathcal{B} \cong A_5$. They have genus

$$g = 1 + \frac{60}{2}\Big(1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{5}\Big) = 9.$$

The first, where x and y are conjugate, is a double covering of the icosahedron, branched over its 20 face-centres; the faces are thus 6-gons, with vertices alternately coloured black and white. But how do we describe the other one?

Exercise 5.4. How many regular bipartite maps of type $(5, 5, 5)$ have automorphism group A_5?

Quasiplatonic surfaces are considered in detail in:

J. Wolfart, *ABC for polynomials, dessins d'enfants and uniformization — a survey*, to appear. See the Jyväskylä Summer School website, course MA1.

For a proof of Hurwitz's bound, and basic properties of Hurwitz groups, see §5.11 of:

G. A. Jones and D. Singerman, *Complex Function Theory, an Algebraic and Geometric Viewpoint*, Cambridge University Press, 1987.

Regular maps, especially those of low genus, are considered in Chapter 8 of:

H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, Springer, 1957.

For basic representation theory, including a proof of Proposition 5.2 in Chapter 28, see:

G. James and M. Liebeck, *Representations and Characters of Groups*, Cambridge University Press, 1993.

For character tables of many finite groups, especially the simple groups, see:

J. H. Conway *et al.*, *ATLAS of Finite Groups*, Oxford University Press, 1985.

6. Regular embeddings of complete bipartite graphs

This lecture, and also Jürgen's last lecture, will be rather different in nature compared with the earlier lectures. In those, we described some fairly classical material, ranging from the late 18th century to the late 20th century. In the last two lectures we will describe some very recent research we have been involved in, some of it still on-going, in order to give you a flavour of current developments in one particular area of dessins d'enfants.

6.1. Regular maps

Theorem 2.2 states that every bipartite map $\mathcal{B}$ is a quotient of a regular bipartite map $\tilde{\mathcal{B}}$ (its canonical regular cover) by a subgroup $A \leq \mathrm{Aut}\,\tilde{\mathcal{B}}$; $\tilde{\mathcal{B}}$ has the same type as $\mathcal{B}$, and is finite if and only if $\mathcal{B}$ is finite. There is a similar result for maps. This shows that it is important to understand regular maps, regular bipartite maps, and their automorphism groups. One can try to classify such maps by their type, automorphism group, genus or underlying graph.

(a) **Classifying by type.** Lecture 5 gives some ideas on how to do this. Regular bipartite maps $\mathcal{B}$ of type (l, m, n) correspond to normal subgroups K in the triangle group $\Delta(l, m, n)$, with finite bipartite maps corresponding to those subgroups K of finite index. A theorem of Mal'cev implies that in the euclidean and hyperbolic cases, there are infinitely many normal subgroups of finite index in Δ, and hence infinitely many finite regular bipartite maps $\mathcal{B}$ of type (l, m, n). A group is said to be *residually finite* if the intersection of its normal subgroups of finite index is the trivial subgroup; if such a group is infinite, then it must have infinitely many normal subgroups of finite index, since the intersection of finitely many of them has finite index. Mal'cev's theorem asserts that any finitely generated linear group is residually finite, where 'linear' means isomorphic to a subgroup of $GL_n(F)$ for some field F. In our case, Δ is finitely generated, and is infinite in the euclidean and hyperbolic cases. The euclidean triangle groups can be regarded as linear groups by identifying each affine transformation $z \mapsto az + b$ of $\mathbf{C}$ with the matrix $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathbf{C})$. The hyperbolic triangle groups are subgroups of $PSL_2(\mathbf{R})$, and we can prove that they are residually finite by applying Mal'cev's theorem to their inverse images in $SL_2(\mathbf{R})$.

Example 6.1. By applying this to $\Delta(3, 2, 7)$ we see that there are infinitely many Hurwitz groups. There are several results giving infinite families of explicit examples of these groups. For instance, Macbeath has shown that $PSL_2(q)$ is a Hurwitz group if and only if $q = 7$, or $q = p$ for some prime $p \equiv \pm 1 \bmod (7)$, or $q = p^3$ for some prime $p \equiv \pm 2, \pm 3 \bmod (7)$; by Dirichlet's Theorem on primes in arithmetic progressions, there are infinitely many prime powers q satisfying these conditions. Similarly Conder has shown that A_n is a Hurwitz group for all $n \geq 168$ (and also for some smaller values of n).

(b) **Classifying by group.** Again, Lecture 5 gives some ideas on how to do this. Given a finite group G, we look for pairs of elements x, y generating G, for instance by using the character formula (Proposition 5.3) to count bipartite maps of a given type with automorphism group G. As an example, it can be shown (by rather tedious inspection) that every nonabelian finite simple group is generated by a pair x, y satisfying $y^2 = 1$, so it is isomorphic to $\mathrm{Aut}\,\mathcal{M}$ for some regular map $\mathcal{M}$.

One difficulty with this approach is that a given group may have many generating pairs. For instance, Dixon has shown that if a pair of elements x, y in $G = S_n$ are chosen at random, then they generate S_n or A_n with probabilities approaching $\frac{3}{4}$ or $\frac{1}{4}$ as $n \to \infty$. (These are the probabilities that at least one of them is odd, or both are even.) There are similar results for other families of simple (or nearly simple) groups.

(c) **Classifying by genus.** The regular maps of genus 0 are well known (the platonic solids, together with the regular n-gons and their dual maps), and those of genus 1 are easily described as quotients of the universal maps of appropriate types on $\mathbf{C}$ (see Exercise 5.1, and also Chapter 8 of the book by Coxeter and Moser). The Hurwitz bound $|\mathrm{Aut}\, X| \leq 84(g-1)$ (see §5.2) implies that for each genus $g \geq 2$ there can be only finitely many regular dessins, and for small values of g it is feasible to classify them, either by hand or by computer. While the summer school was taking place, Marston Conder announced a classification by computer of the regular maps of genus g for $2 \leq g \leq 200$; there seems to be little consistent pattern, the number of regular maps depending heavily on the factorisation of $g-1$. Schlage-Puchta and Wolfart have smoothed out these variations by showing that the number of regular dessins of genera from 2 to g grows asymptotically like $g^{\log g}$.

(d) **Classifying by graph.** Here we try to solve the following general problem:

Given a graph (or class of graphs) $\mathcal{G}$, classify all regular maps on orientable surfaces with underlying graph $\mathcal{G}$.

(There is a similar problem for nonorientable surfaces, but this is of less interest for the study of dessins.) Equivalently, we can look for subgroups G of $\mathrm{Aut}\, \mathcal{G}$ which act transitively on the vertices of $\mathcal{G}$, and for which the stabiliser G_v of a vertex v is cyclic, acting regularly on the neighbours of v, since the automorphism group of any regular embedding of $\mathcal{G}$ must satisfy these conditions. Such a group exists only if $\mathcal{G}$ is arc-transitive, that is, $\mathrm{Aut}\, \mathcal{G}$ acts transitively on the arcs (directed edges) of $\mathcal{G}$. The problem of classifying regular embeddings has been solved for several classes of arc-transitive graphs.

Example 6.2. Let $\mathcal{G}$ be the complete graph K_n, consisting of n vertices, every distinct pair joined by an edge. There are obvious examples of regular embeddings of K_n on the sphere for $n = 1, 2, 3$ and 4, and these are easily seen to be unique. For each of $n = 5$ and $n = 7$ there is a chiral (mirror-image) pair of regular embeddings of K_n on a torus, obtained as quotients of the universal bipartite maps of types $(4, 2, 4)$ and $(6, 2, 3)$ by removing the 2-valent white vertices.

Exercise 6.1. Can you get a regular embedding of K_7 from the bipartite map representing the 7-point Fano plane $\mathrm{P}^2(F_2)$ on the torus? Can you get two of them?

There is no corresponding example for $n = 6$, and this is explained by the following result.

Theorem 6.1 (Biggs, 1971). *The complete graph K_n has a regular orientable embedding if and only if n is a prime power.*

The examples constructed by Biggs are based on the finite fields $F = F_n$ of order n, which exist (and are unique up to isomorphism) if and only if n is a prime power. We let $\mathcal{G}$ have vertex set $V = F$, and choose a generator α for the multiplicative group F^*,

which is a cyclic group of order $n-1$. We then define the cyclic order of neighbours of each vertex v to be $v+1, v+\alpha, v+\alpha^2, \ldots, v+\alpha^{n-2}$. This defines an oriented surface around v, and by taking the union of these we obtain an oriented map $\mathcal{M} = \mathcal{M}(\alpha)$, which is regular with $\mathrm{Aut}\,\mathcal{M} \cong AGL_1(F)$, the 1-dimensional affine group over F consisting of the transformations $v \mapsto av + b$ with $a, b \in F$ and $a \neq 0$.

Theorem 6.2 (James and Jones, 1985). *The maps $\mathcal{M}(\alpha)$ are the only regular embeddings of K_n. We have $\mathcal{M}(\alpha) \cong \mathcal{M}(\alpha')$ if and only if α and α' are conjugate under the Galois group of the field F, so if $n = p^e$ for some prime p then there are, up to isomorphism, $\phi(n-1)/e$ regular oriented embeddings of K_n.*

Here $\phi(n-1)$ is the number of choices for a generator α of the group $F^* \cong C_{n-1}$, and e is the order of the Galois group $\mathrm{Gal}\,F \cong C_e$, generated by the Frobenius automorphism $t \mapsto t^p$ of F.

6.2 Complete bipartite graphs

Another class of arc-transitive graphs consists of the complete bipartite graphs $\mathcal{G} = K_{n,n}$: these have n black vertices and n white vertices, each black and white pair joined by an edge, so $|V| = 2n$ and $|E| = n^2$.

It is important to emphasise here that we are looking for embeddings $\mathcal{M}$ of $K_{n,n}$ which are regular as *maps*, so that $\mathrm{Aut}\,\mathcal{M}$ acts transitively on the *directed* edges of $\mathcal{M}$, ignoring the vertex-colours. Thus $\mathrm{Aut}\,\mathcal{M}$ is a semidirect product of G by C_2, where $G = \mathrm{Aut}\,\mathcal{B}$ is the automorphism group of the corresponding regular dessin $\mathcal{B}$, preserving the vertex colours, and the complement C_2 is generated by an automorphism of $\mathcal{M}$ which reverses an edge, thus transposing the colours. Note that G acts regularly on the edge-set E, so $|G| = |E| = n^2$.

Example 6.3. We have seen, in Examples 4.2, 4.3, 4.4 and 5.1 and in Jürgen's lectures, that the nth degree Fermat curve $x^n + y^n = 1$ has a Belyi function $\beta(x, y) = x^n$, and the corresponding dessin $\mathcal{B}$ is regular as a bipartite map, with $G = \mathrm{Aut}\,\mathcal{B} \cong C_n \times C_n$ acting by $(x, y) \mapsto (x\zeta_n^j, y\zeta_n^k)$. This is, in fact, regular as a map, with the automorphism $(x, y) \mapsto (y, x)$ transposing the vertex colours. The embedded graph is $K_{n,n}$, and we call this map the *standard embedding* $\mathcal{S}_n$ of $K_{n,n}$.

This example exists for each n, so if we define $\nu(n)$ to be number of regular embeddings of $K_{n,n}$, up to isomorphism, then $\nu(n) \geq 1$ for all n. This is unlike the situation with K_n, which has regular embeddings only when n is a prime power.

Theorem 6.3 (Nedela, Škoviera & Jones). *$\nu(n) = 1$ if and only if $(n, \phi(n)) = 1$.*

This is equivalent to the condition that $n = p_1 \ldots p_k$, where $p_1, \ldots, p_k$ are distinct primes, with p_i not dividing $p_j - 1$ if $i \neq j$. Burnside showed that these also are also the va;ues of n for which there is a unique *group* of order n, namely C_n; the proofs are similar, but independent of each other. Erdős has shown that these integers have asymptotic density

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

where γ is Euler's constant. This converges to 0 very slowly!

The proof of Theorem 6.3 uses the fact that a group G arises as $\mathrm{Aut}\,\mathcal{B}$ for some regular embedding of $K_{n,n}$ if and only if

(a) $G = XY$ and $X \cap Y = 1$ where $X = \langle x \rangle$ and $Y = \langle y \rangle$ have order n,

(b) there is an automorphism α of G transposing x and y.

Here x and uy act as rotations around a black vertex v and a white vertex w, and α is induced by conjugation by the automorphism of the map reversing the edge vw. Isomorphism classes of regular embeddings of $K_{n,n}$ correspond to orbits of $\mathrm{Aut}\,G$ on such pairs $x, y \in G$. This is the idea behind the proof of the following result.

Theorem 6.4 (Nedela, Škoviera & Jones). *If $n = p^e$ for a prime $p > 2$ then $\nu(n) = p^{e-1}$.*

Each of the maps enumerated in this theorem has genus $(n-1)(n-2)/2$, and has $2n$-gonal faces. The group $G = \mathrm{Aut}\,\mathcal{B}$ has the form

$$G_f := \langle g, h \mid g^n = h^n = 1,\ h^g = h^{1+p^f} \rangle$$

for some $f = 1, 2, \ldots, e$. As representatives of the orbits of $\mathrm{Aut}\,G$ on such pairs, we can take $x = g^u$ and $y = g^u h$ (or $y = (gh)^u$, sometimes more convenient for Galois theory), where $u = 1, 2, \ldots, p^{e-f}$ and $(u, p) = 1$. For each f there are $\phi(p^{e-f})$ such maps $\mathcal{M}$, so the total number is $\sum_{f=1}^{e} \phi(p^{e-f}) = p^{e-1}$. These correspond to distinct normal subgroups of index n^2 in $\Delta(n, n, n)$, all normal in $\Delta(n, 2, 2n)$ which contains $\Delta(n, n, n)$ with index 2. The case $f = e$ corresponds to the standard embedding, with $G_f = G_e \cong C_n \times C_n$.

An important ingredient in the proof is the following purely group-theoretic result:

Theorem 6.5 (Huppert, 1953). *If a p-group ($p > 2$) is a product of two cyclic groups, then it is metacyclic, i.e. an extension of one cyclic group by another*

In the situation in Theorem 6.4, we have $|G| = p^{2e}$, so G is a p-group, and (a) gives $G = XY$ with X and Y cyclic, so Huppert's Theorem applies to G; this allows us to deduce the above presentation for G, and eventually to classify the corresponding regular maps. Unfortunately, Huppert's Theorem does not apply when $p = 2$, and indeed there are extra embeddings for $n = 2^e$ which do not correspond to metacyclic groups: there is one, of genus 1 with 4-gonal faces, for $e = 2$ (can you draw it?), and there are four for each $e \geq 3$. When $p = 2$ we also have the maps associated as in the odd prime power case with the metacyclic groups G_f, but now the case $f = 1$ is excluded. Du, Kwak, Nedela, Škoviera and Jones have recently shown that the examples described here are the only ones for $n = 2^e$. An even more recent development (April 2006) is an extension of the classification to all integers n, using Sylow-type arguments to fit together the embeddings described above for the various prime powers dividing n. The resulting formula for $\nu(n)$ is very complicated, but it agrees with the results of computer searches for $n \leq 100$.

Lately, Jürgen and I have been working with Antoine Coste and Manfred Streit on some interesting Galois-theoretic problems concerning the dessins associated with these maps, and this will be the subject of Jürgen's last lecture.

References

N. L. Biggs, Automorphisms of imbedded graphs, *J. Combin. Theory Ser. B* 11 (1971), 132–138.

M. D. E. Conder, Generators for alternating and symmetric groups, *J. London Math. Soc.* (2) 22 (1980), 75–86.

A. D. Coste, G. A. Jones, M. Streit and J. Wolfart, Generalised Fermat hypermaps and Galois orbits, in preparation.

J. D. Dixon, The probability of generating the symmetric group, *Math. Z.* 110 (1969), 199–205.

S. F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2. I: Metacyclic case, *European J. Combinatorics*, to appear.

S. F. Du, G. A. Jones, J. H. Kwak, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is a power of 2. II: Non-metacyclic case, in preparation.

P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc.* 12 (1948), 75–78.

B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* 58 (1953), 243–264.

L. D. James and G. A. Jones, Regular orientable imbeddings of complete graphs, *J. Combinatorial Theory, Ser. B* 39 (1985), 353–367.

G. A. Jones, R. Nedela and M. Škoviera, Complete bipartite graphs with a unique regular embedding, *J. Combinatorial Theory, Ser. B*, to appear.

G. A. Jones, R. Nedela and M. Škoviera, Regular embeddings of $K_{n,n}$ where n is an odd prime power, *European J. Combinatorics*, to appear.

G. A. Jones, M. Streit and J. Wolfart, Galois action on families of generalised Fermat curves, submitted.

A. M. Macbeath, Generators of the linear fractional groups, in *1969 Number Theory, Proc. Sympos. Pure Math., vol. XII, Houston Texas 1967*, Amer. Math. Soc., pp. 14–32.

A. Mal'cev, On isomorphic matrix representations of infinite groups (Russian, English summary), *Mat. Sbornik N. S.* 8 (50), 405–422.

J.-C. Schlage-Puchta and J. Wolfart, How many quasiplatonic surfaces? *Arch. Math. (Basel)* 86 (2006), 129–132.

Further reading

In addition to the textbooks and papers mentioned in the notes for my lectures, the following books give useful background information on a number of topics relevant to dessins d'enfants. They are not all currently in print, but I hope that you can find many of them in university libraries. Gareth Jones

R. D. M. Accola, *Topics in the Theory of Riemann Surfaces*, Lecture Notes in Mathematics 1595, Springer, 1994.

A. F. Beardon, *The Geometry of Discrete Groups*, Springer, 1983.

E. Bujalance, A. F. Costa and E. Martinez, *Topics on Riemann Surfaces and Fuchsian Groups*, London Math. Soc. Lecture Note Series 287, Cambridge University Press, 2001.

A. Douady and R. Douady, *Algèbre et Théories Galoisiennes* (2 vols), CEDIC, Paris, 1979; *Algebra and Galois Theories*, Cassini, 2005.

H. Farkas and I. Kra, *Riemann Surfaces*, Springer, 1980.

O. Forster, *Lectures on Riemann Surfaces*, Springer, 1981.

J. Jost, *Compact Riemann Surfaces*, Springer Universitext, 1997.

K. Lamotke, *Riemannsche Flächen*, Springer, 2005.

W. Magnus, *Noneuclidean Tesselations and their Groups*, Academic Press, 1974.

R. Miranda, *Algebraic Curves and Riemann Surfaces*, American Math. Soc., 1995.

S. Nag, *The Complex Analytic Theory of Teichmüller Spaces*, Canadian Math. Soc. Monographs and Advanced Texts, Wiley-Interscience, 1988.

E. Reyssat, *Quelques Aspects des Surfaces de Riemann*, Progress in Mathematics 77, Birkhäuser, 1989.

B. Schoeneberg, *Elliptic Modular Functions*, Springer, 1974.

J-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, 1992.

G. Springer, *Introduction to Riemann Surfaces*, Addison-Wesley, 1957.

E. Vinberg (ed.), *Geometry II: Spaces of Constant Curvature*, Encyclopedia of Mathematical Sciences 29, Springer, 1993.

H. Zieschang, E. Vogt and H-D. Coldewey, *Surfaces and Planar Discontinuous Groups*, Lecture Notes in Mathematics 835, Springer, 1980.