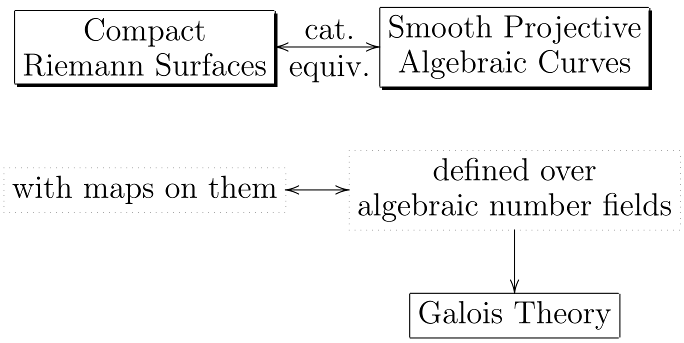
Lecture 2

by Prof. Gareth Jones

notes by Tuomas Puurtinen

1 Introduction



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 1.1 *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.

1.1 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

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

where $\sum'$ means the sum over $\omega \neq 0$. 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 1.2 *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 $\mathrm{Im}\,\tau > 0$, i.e. τ is the upper half place $\mathbb{H} = \{\, \tau \in \mathbb{C} \mid \mathrm{Im}\,\tau > 0 \,\}$.

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 1.3 *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).*