Lecture 6: The Absolute Galois Group (G2S2, Novosibirsk, 2018)

Gareth Jones

University of Southampton, UK

August 4, 2018

Introduction

The absolute Galois group $\mathbb{G}$ is the automorphism group of the field $\overline{\mathbb{Q}}$ of algebraic numbers.

It is a very important group, since it describes the entire Galois theory of algebraic number fields.

It is also very complicated, and there are some difficult open problems associated with it, such as the Inverse Galois Problem, which asks whether every finite group is the Galois group of some algebraic number field.

By Belyĭ's Theorem, a compact Riemann surface (= algebraic curve) is defined over $\overline{\mathbb{Q}}$ if and only if it is obtained from a dessin.

$\mathbb{G}$ acts on the coefficients of the rational functions defining Belyĭ pairs and dessins, so it has an induced action on dessins.

This action is faithful, so one can 'see' the Galois theory of algebraic numbers fields by studying the action of $\mathbb{G}$ on dessins.

Basic Galois Theory

For simplicity, all fields in this lecture are subfields of $\mathbb{C}$.
$\alpha \in \mathbb{C}$ is algebraic if $f(\alpha) = 0$ for some non-zero $f[x] \in \mathbb{Q}[x]$, or equivalently $\mathbb{Q}(\alpha)$ is a finite extension field of $\mathbb{Q}$.

The algebraic numbers form a field $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$.

They include $1/2$, $\sqrt{2}$, i, $\sqrt[43]{191 - 41\sqrt{-17}}$, etc, but not $e, \pi, \ldots$.

A field K is a Galois extension of $\mathbb{Q}$ if every embedding $K \to \overline{\mathbb{Q}}$ is an automorphism of K. Equivalently, every irreducible $f(x) \in \mathbb{Q}[x]$ with a root in K splits (has all its roots) in K. The finite Galois extensions of $\mathbb{Q}$ are the splitting fields of the polynomials in $\mathbb{Q}[x]$.

Example Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$, a root of $f(x) = x^3 - 2$, so $\alpha \in \overline{\mathbb{Q}}$. The other roots are $\alpha\omega^{\pm 1}$ where $\omega = e^{2\pi i/3}$. The field $\mathbb{Q}(\alpha)$ is not Galois over $\mathbb{Q}$: it contains only one root of f, and it can be embedded in $\overline{\mathbb{Q}}$ as the isomorphic field $\mathbb{Q}(\alpha\omega) \neq \mathbb{Q}(\alpha)$. However, the splitting field $K = \mathbb{Q}(\alpha, \omega)$ of f is Galois over $\mathbb{Q}$: any embedding in $\overline{\mathbb{Q}}$ permutes the roots of f, so it preserves K.

The Fundamental Theorem of Galois Theory

For any field extension $K \supseteq F$, the Galois group $G = \operatorname{Gal} K/F$ is the group of automorphisms of K fixing F pointwise. For any subgroup $H \leq G$, $\operatorname{Fix} H$ is the subfield of K fixed by H.

Theorem

Let $K \supseteq F$ be a finite Galois extension, and let $G = \operatorname{Gal} K/F$. 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. Its inverse is given by $H \mapsto L = \operatorname{Fix} H$. We have

$$|K : L| = |H| \quad \text{and} \quad |L : F| = |G : H|.$$

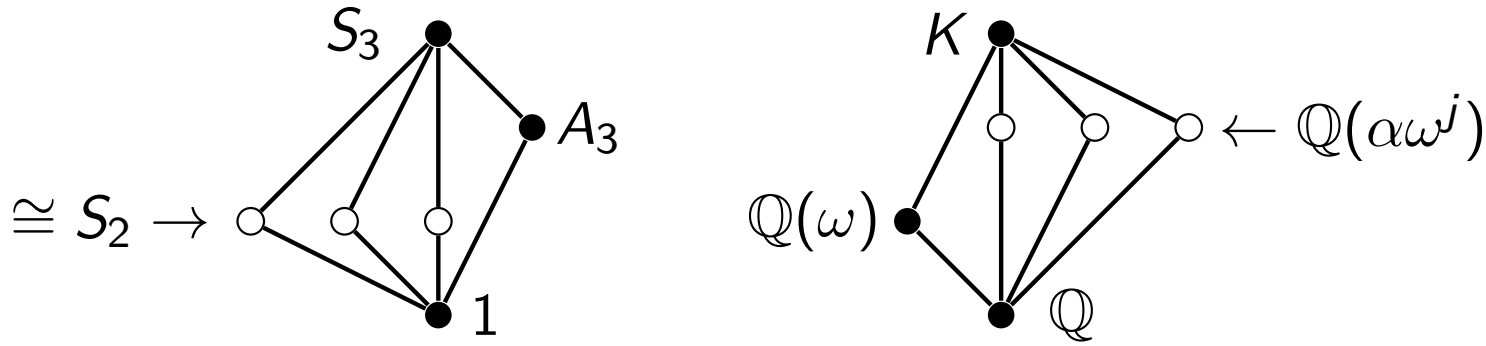
Such an extension $L \supseteq F$ is Galois if and only if the corresponding subgroup H is normal in G, in which case $\operatorname{Gal} L/F \cong G/H$.

Example. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\alpha, \omega)$, where $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\omega = e^{2\pi i/3}$ as in the earlier example.

Then $G = \mathrm{Gal}\, K/\mathbb{Q} \cong S_3$, permuting the roots $\alpha\omega^j$ ($j = 0, \pm 1$) of $f(x) = x^3 - 2$.

Like S_3, G has one normal subgroup of index 2 (corresponding to A_3), three non-normal subgroups of index 3 (each the stabiliser of a root, $\cong S_2$), and the (normal) identity subgroup of index 6.

Therefore K contains one Galois extension of $\mathbb{Q}$ of degree 2 (this is $\mathbb{Q}(\omega)$, the splitting field of $x^2 + x + 1$), three non-Galois extensions of degree 3 (the fields $\mathbb{Q}(\alpha\omega^j)$), and one of degree 6 ($K$ itself).



● Galois/normal ○ not Galois/normal

The absolute Galois group

The absolute Galois group $\mathbb{G}$ is the Galois group $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$.

It is an infinite group, built up from finite groups, as follows.

Let $\mathcal{K}$ be the set of finite Galois extensions K of $\mathbb{Q}$ in $\mathbb{C}$. These are the splitting fields of the polynomials in $\mathbb{Q}[x]$.

Theorem
(i) *$\overline{\mathbb{Q}}$ is the union of the fields $K \in \mathcal{K}$.*
(ii) *Each $K \in \mathcal{K}$ is invariant under $\mathbb{G}$.*

Proof. (i) $|K : \mathbb{Q}| < \infty$ for all $K \in \mathcal{K}$, so if $\alpha \in K$ then $|\mathbb{Q}(\alpha) : \mathbb{Q}| \leq |K : \mathbb{Q}| < \infty$ and hence $\alpha \in \overline{\mathbb{Q}}$. Conversely, each $\alpha \in \overline{\mathbb{Q}}$ is a root of some $f(x) \in \mathbb{Q}[x]$, so α is in its splitting field.

(ii) Elements of $\mathbb{G}$ permute the roots of polynomials in $\mathbb{Q}[x]$ and hence preserve their splitting fields (generated by these roots).

Structure of the absolute Galois group

Since $\overline{\mathbb{Q}} = \cup_{K \in \mathcal{K}} K$ by (i), each $g \in \mathbb{G}$ is uniquely determined by its restrictions g_K to the fields $K \in \mathcal{K}$, and these determine g.

Since $\mathbb{G}$ preserves each $K \in \mathcal{K}$ by (ii), each g_K is an element of the Galois group $G_K := \mathrm{Gal}\, K/\mathbb{Q}$.

These restrictions g_K are not independent of each other: if $K, L \in \mathcal{K}$ and $K \supseteq L$ then by the Fundamental Theorem G_K preserves L, so restriction from K to L gives a homomorphism $\rho_{K,L} : G_K \to G_L,\ g_K \mapsto g_L$. Moreover $\rho_{K,L}$ is an epimorphism, so every element of G_L extends (in $|K : L|$ ways) to an element of G_K.

Thus we can make the identification

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

This is the projective limit or inverse limit $\lim_{\leftarrow} G_K$ of the groups G_K and epimorphisms $\rho_{K,L}$, a profinite group, that is, a projective limit of finite groups. (A class of groups are of current interest.)

The Krull topology

The Fundamental Theorem of Galois Theory gives a bijection between subfields and subgroups, valid for finite extensions.

For infinite Galois extensions, such as $\overline{\mathbb{Q}} \supset \mathbb{Q}$, there is a similar bijection, but between subfields and closed subgroups, where we regard $\mathbb{G}$ as a topological group, one in which multiplication and inversion are continuous operations.

To define a topology on $\mathbb{G}$, first put the discrete topology on each G_K, so every subset of G_K is both open and closed. This defines a product topology on $\Pi := \prod_{K \in \mathcal{K}} G_K$, the weakest topology in which the projections $\Pi \to G_K$ are continuous. By Tychonoff's Theorem, as a product of compact spaces G_K, Π is compact.

The subgroup $\mathbb{G}$ of Π inherits an induced topology, the Krull topology, in which two elements of $\mathbb{G}$ are 'close together' if they agree on a large subfield of $\overline{\mathbb{Q}}$. The equations $\rho_{K,L}(g_K) = g_L$ define $\mathbb{G}$ as a closed subset of Π, so it is also compact.

The absolute Galois group and the Cantor set

As a compact topological group, one might hope that $\mathbb{G}$ may be 'smooth', perhaps a Lie group like S^1 or $SO(3)$.

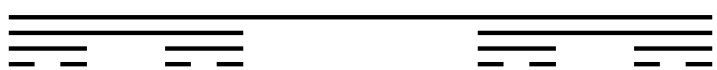
However, the opposite is true: $\mathbb{G}$ is fractal, rather than smooth.

In fact, $\mathbb{G}$ is homeomorphic to the Cantor ternary set C.

This is formed by removing the middle third of the closed unit interval $I = [0, 1]$ to leave the union $[0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$ of two closed intervals, then removing their middle thirds to leave $[0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$, and so on. After infinitely many iterations, what is left is C. More precisely

$$C = \left\{ x = 0 \cdot x_1 x_2 \ldots = \sum_{i=1}^{\infty} x_i 3^{-i} \in \mathbb{R} \mid \text{each } x_i = 0 \text{ or } 2 \right\},$$

the set of real numbers $x \in [0, 1]$ with a base 3 expansion consisting entirely of digits $x_i = 0$ or 2.



The action of the absolute Galois group on Belyĭ pairs

By Belyĭ's Theorem a compact Riemann surface X is defined over $\overline{\mathbb{Q}}$ if and only if there is a Belyĭ function $\beta : X \to \Sigma$.

In this case, β can also be chosen to be defined over $\overline{\mathbb{Q}}$, in the sense that it is a rational function of the coordinates of points in X, with coefficients in $\overline{\mathbb{Q}}$.

This Belyĭ pair (X, β) determines a dessin $\mathcal{B} = \beta^{-1}(\mathcal{B}_1)$ on X.

Applying any $g \in \mathbb{G}$ to the coefficients of the polynomials and rational functions defining X and β gives a pair (X^g, β^g).

X^g is a compact Riemann surface and β^g is a Belyĭ function, so (X^g, β^g) is a Belyĭ pair, corresponding to a dessin $\mathcal{B}^g$.

This gives an action of $\mathbb{G}$ on (isomorphism classes of) dessins.

Of course, if (X, β) is defined over $\mathbb{Q}$ it is fixed by every $g \in \mathbb{G}$.

However, there are examples where (X, β) is moved by some g.

An example of an orbit of $\mathbb{G}$ on Belyĭ pairs

Let X be the elliptic curve E_λ given by $w^2 = z(z-1)(z-\lambda)$ where $\lambda = 1/\sqrt[3]{2} \in \mathbb{R}$, so X is defined over $K = \mathbb{Q}(\lambda, \omega = e^{2\pi i/3}) \in \mathcal{K}$; the Belyĭ function $\beta : (z, w) \mapsto 4z^3(1-z^3)$ is defined over $\mathbb{Q}$.

$G_K = \mathrm{Gal}\, K/\mathbb{Q} \cong S_3$, permuting the roots $\lambda, \lambda\omega, \lambda\overline{\omega}$ of $2z^3 - 1$.

Composing with the epimorphism $\mathbb{G} \to G_K$ gives an action of $\mathbb{G}$, sending $X = E_\lambda$ to the elliptic curves $X^g = E_\mu$ for $\mu = \lambda, \lambda\omega, \lambda\overline{\omega}$.

The polynomial defining β is invariant under $\mathbb{G}$, so it also defines a Belyĭ function β^g on each E_μ, giving three Belyĭ pairs (E_μ, β).

On any elliptic curve E_λ the J-function takes the value

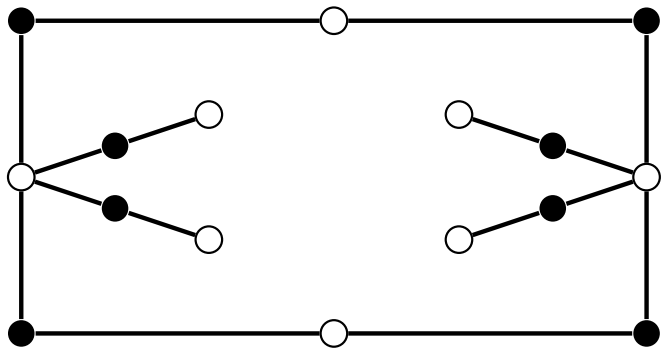
$$J(\tau) = \frac{4(1-\lambda+\lambda^2)^3}{27\lambda^2(1-\lambda)^2}.$$

Assigning λ the three values of μ gives J distinct values, so these curves E_μ are mutually non-isomorphic, as are the three Belyĭ pairs.

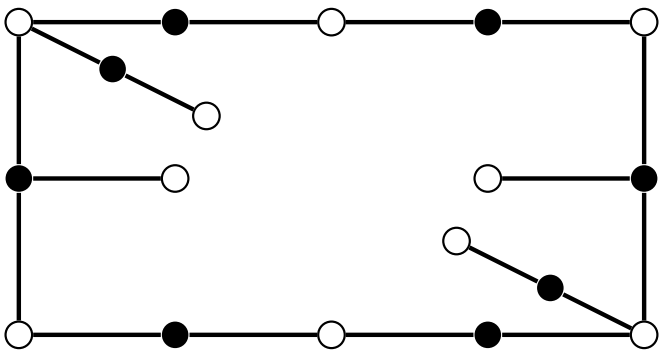
The corresponding orbit of $\mathbb{G}$ on dessins

The dessins $\mathcal{B}_\mu = \beta^{-1}(\mathcal{B}_1)$ corresponding to the Belyĭ pairs (E_μ, β) in this example are as follows (identify opposite sides to form a torus). They form an orbit of $\mathbb{G}$, acting as $G_K \cong S_3$.

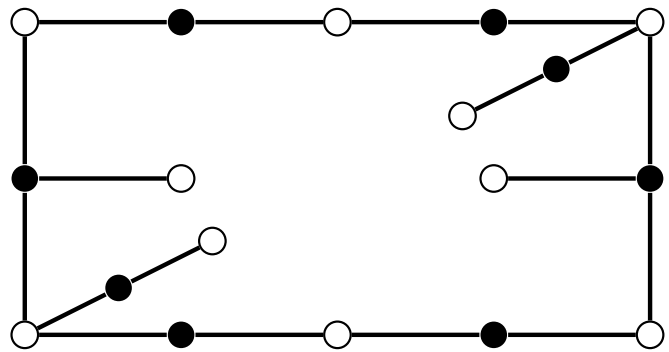
$\mathcal{B}_\lambda$



$\mathcal{B}_{\lambda\omega}$



$\mathcal{B}_{\lambda\overline{\omega}}$



$\mathcal{B}_{\lambda\overline{\omega}}$ is the mirror image of $\mathcal{B}_{\lambda\omega}$.

Invariants of $\mathbb{G}$

Theorem (Streit and J, 1997)

$\mathbb{G}$ *preserves the following properties of dessins:*

- *numbers of black and white vertices and faces;*
- *valencies of black and white vertices and faces;*
- *genus;*
- *monodromy group;*
- *orientation-preserving automorphism group.*

However, it does not preserve

- full automorphism group (possibly reversing orientation);
- number and lengths of Petrie polygons (closed zig-zag paths, turning first left and first right at alternate vertices);
- isomorphism class.

Equivalence of Belyĭ pairs: define $(X, \beta) \equiv (X', \beta')$ if there is an isomorphism $\iota : X \to X'$ of Riemann surfaces with $\beta' \circ \iota = \beta$.
This is equivalent to isomorphism of the corresponding dessins.

Theorem (Grothendieck, 1984)

$\mathbb{G}$ acts faithfully on equivalence classes of Belyĭ pairs.

Proof. If $1 \neq g \in \mathbb{G}$, then g moves some $a \in \overline{\mathbb{Q}}$.
Since $\overline{\mathbb{Q}}$ is algebraically closed, there is some $\lambda \in \overline{\mathbb{Q}}$ satisfying

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

so the elliptic curve $X = E_\lambda$ has $J(X) = a$.
Then $X^g = E_{g(\lambda)}$, with $J(X^g) = g(a) \neq a = J(X)$, so $X^g \ncong X$.
Since X is defined over $\overline{\mathbb{Q}}$ there is a Belyĭ function β on X, also defined over $\overline{\mathbb{Q}}$. Since $X \ncong X^g$ we have $(X, \beta) \not\equiv (X, \beta)^g$. □

Corollary

$\mathbb{G}$ acts faithfully on isomorphism classes of dessins.

In fact, this proves:

Corollary

$\mathbb{G}$ *acts faithfully on isomorphism classes of dessins of genus* 1*.*

More generally, we have:

Theorem (González-Diez and Girondo, 2007)

$\mathbb{G}$ *acts faithfully on isomorphism classes of dessins of any genus.*

Even more surprisingly, we have:

Theorem (Schneps, 1994)

$\mathbb{G}$ *acts faithfully on isomorphism classes of plane trees.*

It is remarkable that such simple combinatorial objects (maps of genus 0 with one face) can faithfully represent such a large, complicated and important group as $\mathbb{G}$.