2.3 More on Dessins

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

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

**Theorem 2.2** Every dessin $B$ is isomorphic to $A \backslash \tilde{B}$ for some regular dessin $\tilde{B}$ and subgroup $A \subseteq \text{Aut } \tilde{B}$.

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

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

**Exercise 2.4** Let $B$ consist of a path of $N$ edges, alternately white, black, white, etc. $\bullet \circ \bullet \circ \bullet \circ \cdots$ Find $G$, $C$, $\tilde{B}$ and $A$ for this dessin.

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

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

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

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

The algebraic theory is similar to that for bipartite maps.

2.4 Example

$\mathcal{M}$, Monsieur Mathieu:

Here $|\Omega| = 12$. So

$$x = (123)(456)(7)(8910)(11)(12)$$

and


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

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

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

3 Galois Theory

3.1 Basic Galois Theory

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

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

Important case: $\bar{\mathbb{Q}} := \{ \alpha \in \mathbb{C} \mid f(\alpha) = 0 \text{ for some non-zero } f \in \mathbb{Q}[x] \}$ the field of algebraic numbers. Motivation: Belyi’s Theorem.

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

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

Example 3.1 $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_n)$ the $n^{th}$ cyclotomic field, $\zeta_n = \exp(\frac{2\pi i}{n})$. Any embedding $e : K \hookrightarrow \bar{\mathbb{Q}}$ sends $\zeta_n$ to some $\zeta'_n \in K$, so $e(K) = K$. This is Galois extension.

Example 3.2 $F = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$, $\alpha = 2^{1/3} \in \mathbb{R}$. There is an embedding $e : K \hookrightarrow \bar{\mathbb{Q}}$ sending $\alpha$ to $\alpha \zeta_3 \notin K$. This extension is not Galois.

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

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

In theorem 3.1 $G = \text{Gal} K/F$ permutes the roots of $f$ faithfully so we can embed $G$ in $S_n$, $n = \deg(f) =$”no. of roots of $f$”, and $|G| = |K : F|$.
**Example 3.3**  \( K = \mathbb{Q}(\zeta_3, \alpha_3), \alpha = 2^{1/3} \in \mathbb{R} \) as before, \( F = \mathbb{Q} \).  \( K \) is the splitting field of \( f(x) = x^3 - 2 \). Degree is \( |K : F| = 6 \), basis \( 1, \alpha, \alpha^2, \zeta_3, \alpha \zeta_3, \alpha^2 \zeta_3 \).  

\( f \) has three roots \( \alpha_j = \alpha \zeta_j^3 \) \((j = 0, 1, 2)\) permuted faithfully by \( G = \text{Gal} \ K/F \), so \( G \hookrightarrow S_3 \). Since \( |G| = |K : F| = 6 \) and \( |S_3| = 6 \), \( G \cong S_3 \).

**Theorem 3.2 (Fundamental Theorem of Galois Theory)**  Let \( K \supseteq F \) be a finite Galois extension, \( G = \text{Gal} \ K/F \). There is an order-reversing bijection \( L \mapsto H = \text{Gal} \ K/L \) between fields \( L \) such that \( K \supseteq L \supseteq F \), and subgroups \( H \leq G \). The inverse sends each \( H \) to \( L = \text{fix} \ H \). We have \( |K : L| = |H| \) and \( |L : F| = |G : H| \). \( L \supseteq F \) is Galois iff \( H \trianglelefteq G \), in which case \( \text{Gal} \ L/F \cong G/H \).

\[
\begin{array}{ccc}
K & \longrightarrow & G \\
\downarrow & & \downarrow \\
L & \longrightarrow & H \\
\downarrow & & \downarrow \\
F & \longrightarrow & 1
\end{array}
\]

In example 1,

\[ \text{Gal} \ \mathbb{Q}(\zeta_n)/\mathbb{Q} = \{ \theta_j : \zeta_n \mapsto \zeta_n^j \mid (j, n) = 1 \} \cong \mathbb{Z}_n^\ast, \]

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

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

**Exercise 3.1**  Find the splitting field \( K \) of \( x^n - 2 \), describe the Galois group of \( K \), and find the subgroups fixing \( 2^{1/n} \in \mathbb{R} \) and \( \zeta_n \).

### 3.2 The Absolute Galois Group

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

**Theorem 3.3**

(i) \( \bar{\mathbb{Q}} \) is the union of all the fields \( K \in \mathcal{K} \).

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

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

(ii) Follows by definition of "Galois".

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

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

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

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

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

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

**Exercise 3.2** Show that $\bigcup_{n \geq 1} \mathbb{Q}(\zeta_n)$ is a subfield of $\bar{\mathbb{Q}}$, and describe its Galois group.

**Exercise 3.3** What are the cardinalities of $\bar{\mathbb{Q}}$ and $\mathcal{G}$?

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

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

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

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

The Fundamental Theorem (3.1) extends to the extension $\bar{\mathbb{Q}} \supseteq \mathbb{Q}$ provided we restrict the bijection to the closed subgroups of $\mathcal{G}$, not all subgroups.
Exercise 3.5 In any topological group, every open subgroup is closed, and every closed subgroup of finite index is open.