A brief introduction to Dessins d'Enfants

Aryan Hemmati*

Abstract

1 Crash course through the required Galois theory

Definition 1. (Algebraic extension): A field extension L/K is said to be algebraic if any element $x \in L$ is algebraic over K; that is, there exists some non-zero $P \in K[X]$ such that $P(x) = 0$.

Example 1. The field extension $\mathbb{C}/\mathbb{R}$ is algebraic, while the field extension $\mathbb{R}/\mathbb{Q}$ is not algebraic (why?)

Extreme attention in number theory is towards studying the structure of algebraic closure of $\mathbb{Q}$, also known as field of algebraic numbers. An element $x \in \mathbb{Q}^{\text{alg}}$ is called an algebraic integer if it's root of some monic polynomial with integer coefficients (these definitions generalize to algebraic number fields.)

Definition 2. An algebraic extension L/K is termed the algebraic closure of K if it is also algebraically closed. Such algebraic extension exists and is unique up to isomorphism over K, and is denoted as K^{alg} or $\bar{K}$.

Definition 3. (Separable extension): An algebraic extension L/K is separable if for any $x \in L$, the minimal polynomial of x over K is separable; that is, it has no repeated roots as a polynomial over L. It can be proven that any $P \in K[X]$ is separable if and only if its formal derivative is non-zero as a polynomial in $K[X]$.

Theorem 1. Every algebraic extension of a field F is separable if $\text{char}(F) = 0$. This is since in characteristic zero, any irreducible polynomial is in fact separable. This implies that minimal polynomials are separable. Note that the converse is not true. In fact, this also holds for some fields of positive characteristic. Such fields are generally called perfect fields. A field of positive characteristic p is perfect iff $x \mapsto x^p$ is an automorphism.

Definition 4. Let L/K be a field extension. Then $K^{\text{sep}} := \{x \in L \mid x \text{ algebraic and separable over } K\}$ is a unique (up to isomorphism over K) subfield of L (why?) separable over K and containing all other separable extensions of K within L. (obvious by definition) This is therefore called as the separable closure of K in L.

Definition 5. (Normal extension): An algebraic field extension L/K is normal or quasi-Galois if any polynomial $P \in K[X]$ irreducible over K that has a root in L, splits into linear factors in L. This is equivalent to the minimal polynomial of any $x \in L$ over K splitting in L (decomposing to linear factors as a polynomial over L).

Definition 6. Let L/K be an algebraic field extension. Then there exists at least one normal extension of L (why?) Therefore there exists a minimal normal extension of L, called the normal closure of L/K.

*aryanhemmati1382@gmail.com

Definition 7. (Galois extension): An algebraic field extension L/K is said to be a Galois extension if it is separable and normal. This is equivalent to $|\mathrm{Aut}(L/K)| = [L : K]$, by a celebrated theorem of Emil Artin.

Note. By the preceding discussion, the algebraic closure K^{alg} of a field of characteristic zero is indeed Galois. Moreover, the algebraic closure K^{alg} of an arbitrary field is Galois iff K is a perfect field.

Definition 8. (Galois group): Let L/K be a Galois field extension. Then the group of automorphisms of L fixing K is called the Galois group of L/K (denoted by $\mathrm{Gal}(L/K)$). Galois group of a non-Galois extension L/K is defined as Galois group of its Galois completion (the minimal Galois extension containing L/K).

By the fundamental theorem of Galois theory, studying the Galois group of a field extension helps us know about the intermediate fields of the extension, especially when the main field L is quite hard to understand.

Definition 9. Let I be a poset (indexing set) and $\{G_i\}_{i\in I}$ be a family of groups, $\{\varphi_{i,j} : G_i \to G_j\}_{(i,j)\in I\times I, i\geq j}$ be a family of homomorphisms (the transition maps). Then the pair $(\{G_i\}, \{\varphi_{i,j}\})$ is an inverse system if:

1. $\varphi_{i,i} \equiv id_{G_i} \quad , \quad \forall i \in I$
2. $\varphi_{i,j} \equiv \varphi_{i,k} \circ \varphi_{k,j} \quad , \quad \forall i \geq k \geq j$

Given an inverse system, one can define the inverse limit of the system as a subgroup of the direct product:

$$\varprojlim_{i\in I}(G_i) := \left\{ \{g_i\}_{i\in I} \in \prod_{i\in I} G_i \;\middle|\; \varphi_{i,j}(g_i) = g_j, \forall i \geq j \right\} \leq \prod_{i\in I} G_i$$

Definition 10. A topological group is a topological space G equipped with a compatible group structure; that is, the inverse map $\iota : G \to G$ and the multiplication map $\mathfrak{m} : G \times G \to G$ are continuous with respect to topologies of G and $G \times G$. The definition generalizes if there is a differentiable structure on G.

Definition 11. (Profinite group): A topological group that is isomorphic to the inverse limit of an inverse system of discrete finite groups (finite groups equipped with the discrete topology) is termed a profinite group. This is equivalent to this topological group being compact and totally disconnected.

Definition 12. Given a group G, the profinite completion of G is defined as $\widehat{G} := \varprojlim_{N\lhd G\,,\,[N:G]<\infty} G/N$.

Example 2. An important example of a profinite completion is $\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ where $\mathbb{N}$ is partially ordered by divisibility and the transition maps of the inverse system are the quotient maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ where $m \mid n$.

Note. There exists a canonical homomorphism $G \to \widehat{G}$ defined by $g \in G \mapsto \{[g]_N \in G/N\}_{N\lhd G\,,\,[N:G]<\infty}$. One can show that for any arbitrary group G, the image of this homomorphism is dense in $\widehat{G}$.

Theorem 2. Galois group of any Galois field extension is a profinite group. Furthermore, any profinite group arises as Galois group of some Galois field extension, due to a result by William. C. Waterhause.

Proof. Let L/K be a Galois field extension. Define $\mathcal{L} := \{L_i \mid i \in I\}$ to be the family of all intermediate subfields $K \subseteq L_i \subseteq L$ such that each L_i/K is a finite Galois extension. Therefore $L = \bigcup_{i \in I} L_i$. One sees that:

1. $\mathrm{Gal}(L/L_i) \triangleleft \mathrm{Gal}(L/K)$. Furthermore, $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_i) \cong \mathrm{Gal}(L_i/K)$ is finite for every $i \in I$
2. $\forall i, j \in I, \exists k \in I : \mathrm{Gal}(L/L_k) \leq \mathrm{Gal}(L/L_i) \cap \mathrm{Gal}(L/L_j)$
3. $\bigcap_{i \in I} \mathrm{Gal}(L/L_i) = \{1\}$

Therefore, the collection $\{\mathrm{Gal}(L/L_i) \triangleleft \mathrm{Gal}(L/K) \mid i \in I\}$ defines a fundamental system of neighborhoods of the identity element of $\mathrm{Gal}(L/K)$ (which is the identity automorphism id_L) and therefore induces a unique topology compatible with the group structure of $\mathrm{Gal}(L/K)$. This topology is called the Krull topology on Galois group and thus $\mathrm{Gal}(L/K)$ equipped with this topology is a topological group Furthermore, $\mathrm{Gal}(L/K) = \varprojlim_{i \in I} \mathrm{Gal}(L_i/K)$.

Definition 13. (Absolute Galois group): Let K be an arbitrary field and K^{alg} be its algebraic closure. Also let K^{sep} be the separable closure of K in K^{alg}. Then the absolute Galois group of K (denoted by G_K) is defined as $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Note that if K is a perfect field, then $G_K = \mathrm{Gal}(G^{\mathrm{alg}}/G)$ (as is the case for $K = \mathbb{Q}$).

Example 3. Absolute Galois group $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is a cyclic group of two elements, corresponding to identity and conjugation automorphisms. Absolute Galois group of any finite field is isomorphic to $\widehat{\mathbb{Z}}$.

Therefore it is mainly believed that studying absolute Galois group of $\mathbb{Q}$ would enable us to understand its algebraic closure quite better, since there is no explicit description of this very important field.

2 Studying $G_{\mathbb{Q}}$ by its geometric actions

In his Esquisse d'un programme, Grothendieck suggests that one should try to give a description of the absolute Galois group of the rational numbers, by studying its action on the geometry of $\mathbb{Q}$-varieties (for any field K, a K-variety is a scheme of finite type over K.) He then offers two such geometric objects for studying the geometric action of fundamental group, first being the Étale fundamental group of the tower of moduli space $\mathfrak{M}_{g,n}$ of algebraic curves of genus g with n punctures (preferably nodes) and the other being combinatorial objects so simple he resembles them to children's drawings: Dessins d'Enfants. We now proceed by observing an example of a geometric action of $G_{\mathbb{Q}}$:

Definition 14. (Algebraic group): Let G be a K-variety where K is an arbitrary field. Then the quadruple $(G, \mathfrak{m}, \iota, \mathfrak{1})$ is an algebraic group if $\mathfrak{m} : G \times_K G \to G, \iota : G \to G, \mathfrak{1} : \mathrm{Spec}(K) = \{0\} \to G$ and the constant morphism $\mathfrak{o} : G \to \mathrm{Spec}(K) = \{0\}$ are morphisms of varieties such that the following diagrams commute:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\mathrm{id}_G \times \mathfrak{m}} & G \times G \\ {\scriptstyle \mathfrak{m} \times \mathrm{id}_G}\downarrow & & \downarrow{\scriptstyle \mathfrak{m}} \\ G \times G & \xrightarrow[\mathfrak{m}]{} & G \end{array} \quad , \quad \begin{array}{ccc} G & \xrightarrow{(\mathfrak{1}, \mathrm{id}_G)} & G \times G \\ {\scriptstyle (\mathrm{id}_G, \mathfrak{1})}\downarrow & \searrow^{\mathrm{id}_G} & \downarrow{\scriptstyle \mathfrak{m}} \\ G \times G & \xrightarrow[\mathfrak{m}]{} & G \end{array} \quad , \quad \begin{array}{ccc} G & \xrightarrow{(\iota, \mathrm{id}_G)} & G \times G \\ {\scriptstyle (\mathrm{id}_G, \iota)}\downarrow & \searrow^{\mathfrak{1} \circ \mathfrak{o}} & \downarrow{\scriptstyle \mathfrak{m}} \\ G \times G & \xrightarrow[\mathfrak{m}]{} & G \end{array}$$

Example 4. Consider the underlying multiplicative group $\mathbb{G}_m$ of a field K. This is then a K-variety (since $\mathbb{G}_m = \mathrm{Spec}(K[X, X^{-1}])$ is an affine K-variety) and also an algebraic group via the field operations.

Now the absolute Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ trivially acts on $\mathbb{Q}^{\mathrm{alg}}$ but this action is tautological and hence not beneficial. Perhaps a more interesting action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ is its action on the multiplicative group of the field of rational numbers, which is indeed a $\mathbb{Q}$-variety. Let us denote by $\mu_n = \langle \xi_n \rangle$ the set of all n-th roots of unity (roots of the equation $x^n = 1$ in $\mathbb{C}$). Note that since elements of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ are automorphisms of $\mathbb{Q}^{\mathrm{alg}}$, they would map any root of unity to another root of unity and therefore constitute an action on μ_n. More generally one could deduce that if $P \in \mathbb{Q}[X]$ is a polynomial and $V(P)$ is its (multi)-set of roots then $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ acts on $V(P)$ by mapping roots of P to roots of P. Similarly one can see that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ also acts on affine algebraic varieties. We now turn back to the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ on μ_n. First, remember the following theorem:

Remind. A K-scheme $X \to \mathrm{Spec}(K)$ is geometrically integral if $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\bar{K})$ is integral for an algebraic closure $K \subseteq \bar{K}$.

Theorem 3. Let X be a quasi-compact and geometrically integral scheme over a field K. Let $\bar{K}$ be an algebraic closure and $\bar{K}^{\mathrm{sep}}$ be the separable closure of K within $\bar{K}$. Also let $\bar{X} := X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K^{\mathrm{sep}})$ and let $\bar{x}$ be a geometric point of $\bar{X}$ with values in $\bar{K}$. Then the maps $\bar{X} \to X$ and $X \to \mathrm{Spec}(K)$ induce maps $\pi_1(\bar{X}, \bar{x}) \to \pi_1(X, \bar{x})$ and $\pi_1(X, \bar{x}) \to \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Then the following sequence of profinite groups is exact:

$$1 \longrightarrow \pi_1(\bar{X}, \bar{x}) \longrightarrow \pi_1(X, \bar{x}) \longrightarrow \mathrm{Gal}(K^{\mathrm{sep}}/K) \longrightarrow 1$$

Therefore for a perfect field K there exist the homotopy exact sequence of the Étale fundamental group given by:

$$1 \longrightarrow \pi_1^{\text{ét}}(\mathbb{G}_m(K^{\mathrm{sep}})) \longrightarrow \pi_1^{\text{ét}}(\mathbb{G}_m(K)) \longrightarrow \mathrm{Gal}(K^{\mathrm{sep}}/K) \longrightarrow 1$$

Therefore since this is exact, $\pi_1^{\text{ét}}(\mathbb{G}_m(K)) \cong \pi_1^{\text{ét}}(\mathbb{G}_m(K^{\mathrm{sep}})) \rtimes \mathrm{Gal}(K)$. Remind that for a complex smooth algebraic variety X this variety can be realized as a complex manifold $X(\mathbb{C})$ and then $\pi_1^{\text{ét}}(X, x) = \widehat{\pi_1(X(\mathbb{C}), x)}$. Note that in the case of $\mathbb{G}_m(K^{\mathrm{sep}}) = \mathrm{Spec}(K^{\mathrm{sep}}[X, X^{-1}])$, one can see that $(\mathbb{G}_m(K^{\mathrm{sep}}))(\mathbb{C}) \cong \mathbb{A}^1 \setminus \{0\}$. Therefore $\pi_1((\mathbb{G}_m(K^{\mathrm{sep}}))(\mathbb{C})) = \pi_1(\mathbb{A}^1 \setminus \{0\}) = \mathbb{Z}$ which implies that $\pi_1^{\text{ét}}(\mathbb{G}_m(K^{\mathrm{sep}})) = \widehat{\mathbb{Z}}$.

3 Riemann Surfaces

Definition 15. A Riemann surface is a connected complex manifold of codimension 1. Therefore a Riemann surface consists of a connected surface locally biholomorphic to an open subset of $\mathbb{C}$.

Definition 16. Let $p : \widetilde{X} \to X$ be a covering map. Then for any $x \in X$ the fundamental group $\pi_1(X, x)$ acts on $p^{-1}(x)$ as follows: Any loop $\gamma \in \pi_1(X, x)$ lifts with a choice of base point $x_0 \in p^{-1}(x)$, to a path $\widetilde{\gamma} : I \to \widetilde{M}$ with $\widetilde{\gamma}(0) = x_0$ and $\widetilde{\gamma}(1) \in p^{-1}(x_0)$. Therefore any $\gamma \in \pi_1(X, x)$ induces a mapping $f_\gamma : p^{-1}(x_0) \to p^{-1}(x_0)$ and this mapping is invertible, therefore a bijection. This is called the monodromy action of the covering map p. Finally, the correspondence $\gamma \to f_\gamma$ is a group homomorphism $\pi_1(X, x) \to \mathrm{Aut}(p^{-1}(x))$ by operation of loop concatenation. This homomorphism is called the monodromy group of the covering.

Definition 17. Any simply connected covering of a topological space X is called "the" universal covering space of X. Any connected, path-connedcted and semilocally simply-connected space admits a universal cover. It can be proven that universal cover is the unique maximal element of isomorphism classes of coverings of X equipped with the order of covering (and the unique minimal element is obviously isomorphism class of X). Furthermore, this poset is opposite to the poset of subgroups of $\pi_1(X,x)$. This correspondence is called the Galois correspondence. A covering is then regular/Galois if the image $p_*(\pi_1(\widetilde{X},\widetilde{x}))$ is a normal subgroup of $\pi_1(X,x)$. Therefore the lifting correspondence $\frac{\pi_1(X,x)}{p_*(\pi_1(\widetilde{X},\widetilde{x}))} \to p^{-1}(x)$ is a group homomorphism and a bijection. Therefore the Galois criterion is equivalent to $\mid \mathrm{Aut}(\widetilde{X}/X) \mid = \mid p^{-1}(x) \mid$ for finite connected coverings.

Definition 18. Let $\Omega \subseteq \mathbb{C}$ be an open set and $f : \Omega \to \mathbb{C}$ be a holomorphic function. If f is not constant, $V(f')$ has no limit point in Ω. (because of the identity theorem) Therefore critical points of f are isolated by open balls $B(z_i, r_i)$. Let $\partial B(z,r)$ be the boundary circle of a sufficiently small open ball (not containing any zeroes or critical points) about an arbitrary point $z \in \Omega$ considered as a curve with positive orientation. Then the winding number of $f(\partial B(z,r))$ with respect to z is a positive integer called the ramification index of z_i and is denoted by $e_z(f)$. In general, $e_z(f)$ can be negative (orientation-reversing map) and infinite. The notion of ramification index generalizes to any map between Riemann surfaces. Especially, if X, Y are compact Riemann surfaces and $f : X \to Y$ is proper and analytic, then $e_z(f) \geq 1, \forall z \in X$. Even more, one can change the local coordinates (in $\mathbb{C}$) in such a way that f becomes the map $x \mapsto x^{e_z(f)}$ and therefore, ramification index locally characterizes the map. This characterization also shows that the set $\{z \in X \mid e_z(f) \neq 1\} \subset X$ is discrete, hence finite (since X is compact). These points are called branch points and their images in Y are called ramification points.

Definition 19. A branched/ramified covering of a connected topological space X is a covering of $X \setminus D$ where $D \subset X$ is a discrete subset. A ramified covering can be unramified by the following procedure: For each ramified point (finite where X is compact) $y_1, \cdots, y_k$, add as many points to X as there are cycles in p_{γ_i} and map them all to y_i, where p is the covering map and γ_i is a generator of fundamental group $\pi_1(X,x)$ where x is ramified (case of punctured Riemann sphere as an example)

Definition 20. A meromorphic function of a Riemann surface X is a holomorphic mapping $f : X \to \bar{\mathbb{C}}$ where $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ is the Riemann sphere. If $X = \mathbb{C}$, then every meromorphic function is a rational function. Furthermore, if it has a single pole in ∞, then it is a polynomial. Riemann-Roch theorem then proves that there are many non-constant meromorphic functions on each Riemann surface. This can be used to prove the following:

Theorem 4. Each Riemann surface can be realized as an algebraic curve in a complex projective space; that is, it can be given by a system of polynomial equations. In fact, if we consider two linearly independent meromorphic functions f_1, f_2 on X, these functions are always related by a polynomial relation $P(f_1, f_2) = 0$. Hence, any pair of linearly independent functions determines a mapping (f_1, f_2) from the Riemann surface to a plane algebraic curve.

Therefore a Riemann surface is synonym to a complex algebraic curve! Furthermore, maps of Riemann surfaces can also be realized as maps between complex algebraic curves.

Definition 21. If a Riemann surface X can be realized as a complex algebraic curve defined by a system of equations with coefficients in a subfield $K \subseteq \mathbb{C}$, then X is said to be defined over K. Special interest is in the case where K is a number field or more specifically, where $K = \mathbb{Q}^{\text{alg}}$.

Now we can state the following wonderful theorem:

Theorem 5. (Belyi theorem): A Riemann surface/complex algebraic curve X is defined over $\mathbb{Q}^{\text{alg}}$ if and only if there exist a covering $f : X \to \bar{\mathbb{C}}$ ramified only over $\{0, 1, \infty\}$. This morphism is then also defined over $\mathbb{Q}^{\text{alg}}$.

Proof. The if part is due to Grothendieck's' isomorphism ${\pi_1}^{\text{alg}/\bar{\mathbb{Q}}}(\mathbb{P}^1{}_{\bar{\mathbb{Q}}} - \{0, 1, \infty\}) \cong {\pi_1}^{\text{alg}/\bar{\mathbb{C}}}(\mathbb{P}^1{}_{\bar{\mathbb{C}}} - \{0, 1, \infty\})$

Definition 22. A meromorphic function $f : X \to \bar{\mathbb{C}}$ unramified outside $\{0, 1, \infty\}$ is a Belyi function. A pair (X, f) is then called a Belyi pair. Thus the category of covers of $\bar{\mathbb{C}}$ is equivalent to the category of beyli pairs.

A Belyi pair gives rise to a specific CW-complex on the Riemann surface. Color all pre-images $f^{-1}(0)$ as black vertices and all pre-images $f^{-1}(1)$ as white vertices and take this as a 0-skeleton. Then take all pre-images $f^{-1}([0, 1])$ as edges between the vertices and take these to be the 1-skeleton. The resulting graph is then bipartite and is 2-cell embedded in X. Furthermore, each face of the embedding has a unique pre-image of ∞ (a pole of f) and the multiplicity of this pole is then equal to the valency of the corresponding face. All the critical points of f on X (except centers) are then contained in the colored vertices. Even more, the multiplicity of a critical point at a vertex is equal to the valency of that vertex, with vertices of valency 1 are not critical points. The resulting embedded graph has as additional structure of a cyclic order on edges meeting every vertex. Monodromy action associates to each element of the fundamental group of $\bar{\mathbb{C}} - \{0, 1, \infty\}$ with respect to $\frac{1}{2}$ a permutation of the edges in the dessin: A loop at $\frac{1}{2}$ lifts to a path in the covering X starting at one edge of the dessin and ending in another. Furthermore any two edges are mapped by this permutation and thus the action induces a cyclic order of vertices. This gives rise to an equivalency between category of Belyi pairs and the category of dessins. The covers are permuted by the Galois group $\text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$, so this group also acts on the set of dessins, and one consequence of Belyi's theorem is that the action is faithful.

Dessin	$\hat{X}$	Equation for the cover
	$\mathbb{P}^1(\mathbb{C})$	$\beta_1(x) = x^3$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_2(x) = 1 - \beta_1(x) = 1 - x^3$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_3(x) = \frac{(4-x)(1+2x)^2}{27x}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_4(x) = 1 - \beta_3(x) = \frac{4(x-1)^3}{27x}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_5(x) = \frac{x^3+3x^2}{4}$
	$\mathbb{P}^1(\mathbb{C})$	$\beta_6(x) = \frac{x^3}{x^3-1}$
	$y^2 = x^3 + 1$	$\beta_7(x, y) = \frac{1}{2}(1 + y)$