Galois Groups as Tree Automorphisms

1 Definitions

1.1 Trees

Definition 1.1. A **tree** T is an undirected graph in which any two vertices are connected by exactly one path. We often refer to the vertices of a tree as **nodes**. We denote by $\mathrm{N}(T)$ to be the set of all nodes of T and we denote by $\mathrm{E}(T)$ to be the set of all edges of T.

Remark 1. Throughout this document, we only consider trees which at most countably many nodes and edges.

Definition 1.2. A **rooted tree** is a tree T in which a special node is singled out. In this case, we refer to the singled out node as the **root** of T and we often denote it by r (if context isn't clear, then we will denote it by r_T).

Definition 1.3. Let T be a rooted tree. We say $\ell \in \mathrm{N}(T)$ is a **leaf** of T if ℓ is not the root and if $\deg \ell = 1$ (meaning it is the boundary of exactly one edge in T). We denote by $\mathrm{L}(T)$ to be the set of leaves of T by $\mathrm{L}(T)$. An **internal node** of T a node which isn't a leaf. We denote by $\mathrm{N}^\circ(T)$ to be the set of all internal nodes of T.

1.1.1 Height, Ancestors, and Descendants

Definition 1.4. Let T be a rooted tree and let $\mathrm{n} \in \mathrm{N}(T)$. The **height** of n in T, denoted $h_T(\mathrm{n})$ (or more simply $h(\mathrm{n})$ if T is understood from context), is the number of edges along the unique path between n and the root (if there are countably infinitely many edges along the unique path from n to r, then we say n has height infinity and we write $h(\mathrm{n}) = \infty$). The **height** of the root of T is $h(\mathrm{r}) = 0$. For all $i \in \mathbb{N} \cup \{\infty\}$, we denote

$$\mathrm{N}_i(T) := \{\mathrm{n} \in \mathrm{N}(T) \mid h(\mathrm{n}) = i\}.$$

If e is an edge of T whose endpoints are n_1 and n_2 which have heights h_1 and h_2 respectively, then the **height** of e is given by $h(\mathrm{e}) = \max\{h_1, h_2\}$. For all $i \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, we denote

$$\mathrm{E}_i(T) := \{\mathrm{e} \in \mathrm{E}(T) \mid h(\mathrm{e}) = i\}.$$

The **height** of T, denoted $h(T)$, is the supremum of the heights of all nodes of T.

Definition 1.5. Let T be a rooted tree and let $\mathrm{n}_1, \mathrm{n}_2 \in \mathrm{N}(T)$ such that $h(\mathrm{n}_2) > h(\mathrm{n}_1)$. If the unique path from n_1 to n_2 does not contain the root, then we say n_1 is an **ancestor** of n_2, and similarly we say n_2 is a **descedant** of n_1. If $h(\mathrm{n}_2) = h(\mathrm{n}_1) + 1$, then we say n_1 is a **parent** of n_2, and similarly we say n_2 is a **child** of n_1. We say a node n in T is **prolific** if it has more than one child.

Remark 2. Ancestory gives rise to a partial order on $\mathrm{N}(T)$: if $\mathrm{n}_1, \mathrm{n}_2 \in \mathrm{N}(T)$, then we write $\mathrm{n}_1 \leq \mathrm{n}_2$ if n_1 is an ancestor of n_2. The pair $(\mathrm{N}(T), \leq)$ is easily seen to form a partially ordered set. We say a node n is the **greatest common ancestor** of nodes n_1 and n_2, denoted $\mathrm{n} = \gcd(\mathrm{n}_1, \mathrm{n}_2)$ if $\mathrm{n} \leq \mathrm{n}_1, \mathrm{n}_2$ and for all other nodes n' such that $\mathrm{n}' \leq \mathrm{n}_1, \mathrm{n}_2$, we have $\mathrm{n}' \leq \mathrm{n}$. Note that greatest common ancestors need not exist when T has infinite height.

1.1.2 Ancestors and Descendants

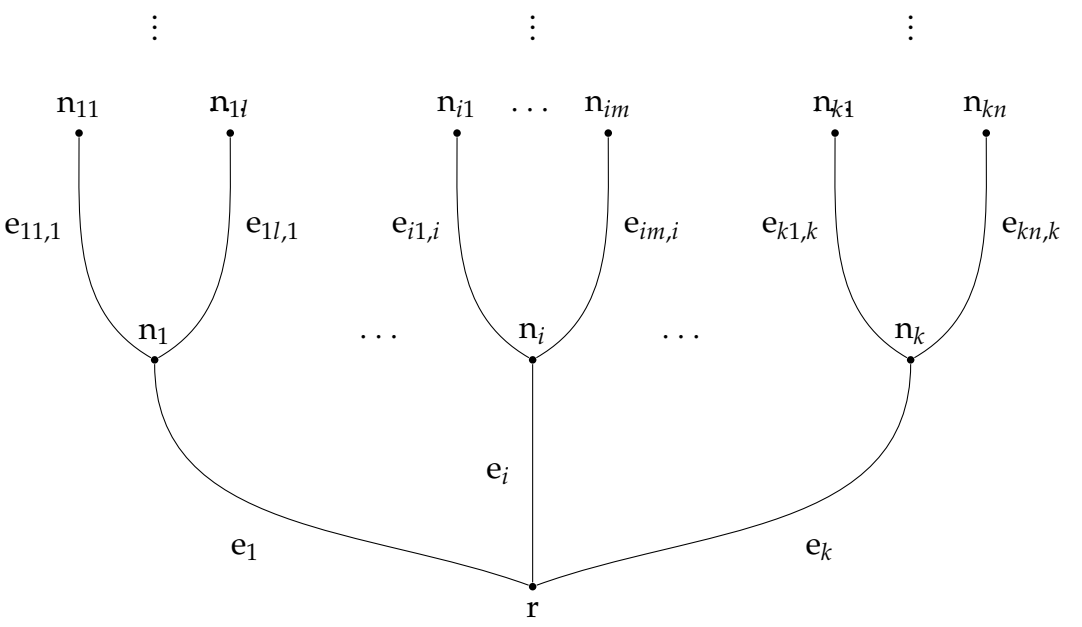
Let T be a rooted tree and let $\mathrm{n}_1, \mathrm{n}_2 \in \mathrm{N}(T)$ such that $h(\mathrm{n}_2) \geq h(\mathrm{n}_1)$. If the unique path from n_1 to n_2 does not contain the root, then we say n_1 is an **ancestor** of n_2, and similarly we say n_2 is a **descedant** of n_1 (if $\mathrm{n}_1 = \mathrm{n} = \mathrm{n}_2$, then we say n is an ancestor and descendant of itself). If $h(\mathrm{n}_2) = h(\mathrm{n}_1) + 1$, then we say n_1 is a **parent** of n_2, and similarly we say n_2 is a **child** of n_1. In this case, the unique path from n_1 to n_2 is an edge e, and we say e has **height** $h(\mathrm{n}_1)$ (we also denote this by $h(\mathrm{e})$). We say a node n in T is **prolific** if it has more than one child.

Ancestory gives rise to a partial order on $\mathrm{N}(T)$: if $\mathrm{n}_1, \mathrm{n}_2 \in \mathrm{N}(T)$, then we write $\mathrm{n}_1 \leq \mathrm{n}_2$ if n_1 is an ancestor of n_2 (if $\mathrm{n}_1 \neq \mathrm{n}_2$, then we also write $\mathrm{n}_1 < \mathrm{n}_2$). The pair $(\mathrm{N}(T), \leq)$ is easily seen to form a partially ordered set. We say a node n is the **greatest common ancestor** of nodes n_1 and n_2, denoted $\mathrm{n} = \gcd(\mathrm{n}_1, \mathrm{n}_2)$, if $\mathrm{n} \leq \mathrm{n}_1, \mathrm{n}_2$ and for all other nodes n' such that $\mathrm{n}' \leq \mathrm{n}_1, \mathrm{n}_2$, we have $\mathrm{n}' \leq \mathrm{n}$.

1.1.3 Ordered Trees

Definition 1.6. An **ordered tree** is a rooted tree T in which a total ordering is specified for the children of each internal node. This is sometimes called a "plane tree" because an ordering of the children is equivalent to an embedding of the tree in the plane, with the root being at the bottom and the children of each internal node being above that internal node (or sometimes we represent the root being on the top and the children of each internal node being below that node).

Example 1.1. Here is a visual representation of an ordered tree:



The children of n_i are $\mathrm{n}_{i1}, \ldots, \mathrm{n}_{im}$. The way the tree is embedded in the plane indicates that $\mathrm{n}_{i1} < \cdots < \mathrm{n}_{im}$.

1.2 R-Trees

Throughout this subsection, let R be a commutative ring and let A be an R-algebra.

Definition 1.7. An **R-tree** in A is a rooted tree T equipped with labeling functions

$$\eta_T \colon \mathrm{N}(T) \to A \quad \text{and} \quad \varepsilon_T \colon \mathrm{E}(T) \to R[X],$$

such that the following property holds: if $\mathrm{e} \in \mathrm{E}(T)$ is an edge with boundary nodes $\mathrm{n} < \mathrm{n}'$ (so n' is a child of n), then

$$\varepsilon_T(\mathrm{e})(\eta_T(\mathrm{n}')) = \eta_T(\mathrm{n}). \tag{1}$$

If T is understood from context, then we simplify our notation and write $\eta = \eta_T$ and $\varepsilon = \varepsilon_T$. Also for each $h \geq 0$ we denote

$$\mathcal{N}_{\eta,h} = \mathcal{N}_h = \eta(\mathrm{N}_h(T)) \quad \text{and} \quad \mathcal{E}_{\varepsilon,h} = \mathcal{E}_h = \varepsilon(\mathrm{E}_h(T)).$$

Remark 3. If $\eta(\mathrm{n}) = a$, $\eta(\mathrm{n}') = a'$, and $\varepsilon(\mathrm{e}) = f$, then we often say n is labeled by a, n' is labeled by a', and e is labeled by f. In this case, (1) says $f(a') = a$.

Example 1.2. Let T be an R-tree in A. If B is another R-algebra and $\sigma \colon A \to B$ is an R-algebra homomorphism, then we obtain a tree σT in B where $(\sigma T)_n = \{\sigma a \mid a \in T_n\}$. For instance, if $\mathfrak{a}$ is an ideal of A, then we obtain an R-tree $\overline{T}$ in $A/\mathfrak{a}$ where $\overline{T}_n = \{\overline{a} \mid a \in T_n\}$.

1.2.1 Galois Trees

Definition 1.8. Let T be an R-tree in A. We say T is **Galois** if the following conditions hold:

1. The labeling function $\eta \colon \mathrm{N}(T) \to A$ is injective with $\eta(\mathrm{r}) = 0$;
2. For each $n \geq 1$, we have $\mathcal{E}_n = \{f_n\}$ for some non-constant monic polynomial $f_n \in R[X]$ of degree $d_n \geq 2$ (every edge with height n is labeled by f_n). Furthermore, we have $\mathcal{N}_{n+1} = f_n^{-1}(\mathcal{N}_n)$.

Let T be an R-tree in A which is Galois and let G be a subgroup of $\mathrm{Aut}_R(A)$, the group of all R-algebra automorphisms of A. Then we get a tree representation of G on T which can be described as follows: Let $\sigma \in G$ and let $\mathrm{n} \in \mathrm{N}_n(T)$. We set $\sigma\mathrm{n}$ to be the unique node in $\mathrm{N}_n(T)$ such that $\eta(\sigma\mathrm{n}) = \sigma(\eta(\mathrm{n}))$.

Theorem 1.1. *Let K be a field, let $\overline{K}$ be an algebraic closure of K, and let $G = \mathrm{Gal}(\overline{K}/K)$. Suppose $f_1, \dots, f_n$ is a sequence of polynomials in $K[X]$ such that*

$$f_{[n]} := f_1 \circ f_2 \circ \cdots \circ f_n$$

is separable and irreducible over K. Let T be the K-tree in $\overline{K}$ whose nodes of height h are in bijection with (and labeled by) the set of roots of $f_{[m]}$ in $\overline{K}$ and whose edges of height h are labeled by f_h and correspond to for each $1 \leq m \leq n$. Suppose $\mathfrak{n}$ and $\mathfrak{n}'$ are nodes which are labeled by b and b' such that $\mathfrak{n}$ has height h and $\mathfrak{n}'$ has height $h+1$. Then is a node of height h and labeled by b and $\mathfrak{n}'$ is a node of height $h+1$, then we Then T is a transitive G-tree.

Proof. Let d_n denote the degree of f_n. We need to show that f_n restricts to a d_n-to-1 map from $\mathcal{N}_n$ to $\mathcal{N}_{n-1}$. To see that it does, let $\alpha \in \mathcal{N}_{n-1}$ and note that $f_n - \alpha$ is separable since $f_n - \alpha \mid f_{[n]}$ and since $f_{[n]}$ is separable. In particular, there are d_n distinct β's in $\overline{K}$ such that $f_n(\beta) = \alpha$; moreover each such β belongs to $\mathcal{R}_n$ since

$$\begin{aligned} f_{[n]}(\beta) &= (f_{[n-1]} \circ f_n)(\beta) \\ &= f_{[n-1]}(f_n(\beta)) \\ &= f_{[n-1]}(\alpha) \\ &= 0. \end{aligned}$$

It follows that $(\mathcal{R}_n, f_n)$ is a tree in $\overline{K}$. To see that it is a G-tree, note that if $\sigma \in G$, then $\sigma f_n = f_n \sigma$ since σ fixes the coefficients of f_n. Also note that the action of G on $\overline{K}$ restricts to a transitive action on $\mathcal{R}_n$ since $f_{[n]}$ is irreducible. □

Example 1.3. Let p be a prime and let G be the absolute Galois group of $\mathbb{Q}$. Let f_1 be the pth cyclotomic polynomial and let $f_n = X^p$ for each $n \geq 2$. Note that $f_{[n]}$ is the p^nth cyclotomic polynomial. In particular, each $f_{[n]}$ is separable and irreducible over $\mathbb{Q}$. Thus if we set $\mathcal{R}_n$ to be the set of primitive p^nth roots of unity in $\mathbb{C}$, then Theorem (1.1) implies $(\mathcal{R}_n, f_n)$ is a transitive G-tree in $\overline{\mathbb{Q}}$.

1.2.2 Galois Trees coming from p-Eisenstein Polynomials

Lemma 1.2. *Let R be a ring and let $\mathfrak{p}$ be a prime ideal of R. Suppose that f and g be monic $\mathfrak{p}$-Eistenstein polynomials in $R[X]$ of degrees m and n respectively. If $m \geq 2$, then the composite $f \circ g$ is a monic $\mathfrak{p}$-Eisenstein polynomial.*

Proof. Write

$$f(X) = X^m + a_{m-1}X^{m-1} \cdots + a_0 \quad \text{and} \quad g(X) = X^n + b_{n-1}X^{n-1} \cdots + b_0$$

where $a_i, b_j \in R$ for each $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$. Then f and g being $\mathfrak{p}$-Eisteinstein means $a_i, b_j \in \mathfrak{p}$ for all i, j and $a_0, b_0 \notin \mathfrak{p}^2$. The composite $f \circ g$ is given by

$$\begin{aligned} (f \circ g)(X) &= f(g(X)) \\ &= g(X)^m + \sum_{i=1}^{m-1} a_i g(X)^i \\ &= (X^n + b_{n-1}X^{n-1} \cdots + b_0)^m + \sum_{i=1}^{m-1} a_i (X^n + b_{n-1}X^{n-1} \cdots + b_0)^i + a_0 \\ &\equiv X^{mn} + b_0^m + a_{m-1}b_0^{m-1} + \cdots + a_0 \bmod \mathfrak{p}^2 \\ &\equiv X^{mn} + a_0 \bmod \mathfrak{p}^2 \end{aligned}$$

where we used the fact that $m \geq 2$ to obtain the last line. Clearly we also have $f \circ g \equiv X^{mn} \bmod \mathfrak{p}$, and thus it follows that $f \circ g$ is $\mathfrak{p}$-Eisenstein. □

Example 1.4. Let K be a number field, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let (f_n) be a sequence of monic $\mathfrak{p}$-Eistenstein polynomials in $\mathcal{O}_K[X]$ such that $d_n \geq 2$ for all $n \in \mathbb{N}$ where $d_n = \deg f_n$. Then by Lemma (1.2), each $f_{[n]}$ is a monic $\mathfrak{p}$-Eisenstein polynomial in $\mathcal{O}_K[X]$. In particular, each $f_{[n]}$ is irreducible over K; hence separable as well since K is perfect. Setting $\mathcal{R}_n$ to be the set of roots of $f_{[n]}$ for each $n \in \mathbb{N}$, we see that $(\mathcal{R}_n, f_n)$ is a G-tree in $\overline{\mathbb{Q}}$ by Theorem (1.1).

1.3 Trees in a Variety

Example 1.5. Let E be the elliptic curve given by the Weierstrass equation

$$E : y^2 = x^3 + x.$$

We set $T_0 = \{\mathcal{O}\}$ and for each $n \geq 1$ we set $T_n = E[2^n] \backslash T_{n-1}$. Define $f_1 \colon E \to E$ by

$$f_1[x : y : z] = [x(x^2 + 1) : 1 : 0]$$

$$f_1(\boldsymbol{x}) = f_1(x, y) =$$

We also $f_0 =$Define $f \colon E \to E$ by

$$\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{f}(x, y) = \left(\frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} \right) = 2\boldsymbol{x}$$

$$f([x : y : 1]) = \left[\frac{x^4 - 2x^2 + 1}{4y^2} : \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} : 1 \right] = \left[2y(x^4 - 2x^2 + 1) : x^6 + 5x^4 - 5x^2 - 1 : 1 \right]$$

Therefore

$$\begin{aligned} f([x : y : z]) &= f([x/z : y/z : 1]) \\ &= \left[2(y/z)((x/z)^4 - 2(x/z)^2 + 1) : (x/z)^6 + 5(x/z)^4 - 5(x/z)^2 - 1 : 1 \right] \\ &= \left[2yz(x^4z^2 - 2x^2z^4 + z^6) : x^6 + 5x^4z^2 - 5x^2z^4 - z^6 : z^6 \right] \\ &= \left[2yz^3(x^4 - 2x^2z^2 + z^4) : x^6 + 5x^4z^2 - 5x^2z^4 - z^6 : z^6 \right] \end{aligned}$$

for all $\boldsymbol{x} \in E$. We set $T_0 = \{\mathcal{O}\}$ and for each $n \geq 1$ we set $T_n = E[2^n] \backslash T_{n-1}$. Observe that

$$E[2] = \{\mathcal{O}, (0, 0), (-i, 0), (i, 0)\}$$

2 Some Identities Involving Composition

2.1 Chain Rule

Recall the chain rule says $(f \circ g)' = (f' \circ g)g'$. More generally, suppose (f_n) be a sequence of polynomials in $K[X]$, and write

$$f_{[n]} := f_n \circ f_{n-1} \circ \cdots \circ f_1$$

for each $n \in \mathbb{N}$. Then we have

$$\begin{aligned} f'_{[n]} &= (f_n \circ f_{[n-1]})' \\ &= (f'_n \circ f_{[n-1]}) f'_{[n-1]} \\ &= (f'_n \circ f_{[n-1]})(f'_{n-1} \circ f_{[n-2]}) f'_{[n-2]} \\ &\vdots \\ &= (f'_n \circ f_{[n-1]})(f'_{n-1} \circ f_{[n-2]}) \cdots (f'_2 \circ f_1) f'_1 \end{aligned}$$

In particular, if $\deg f_i = 1$ for all i, then $f'_{[n]} = \prod_{i=1}^{n} f'_i$. For instance, suppose $f_1 = X + 1$, $f_2 = 2X + 2$, and $f_3 = 3X - 1$. Then

$$\begin{aligned} f_{[3]} &= f_3 \circ f_2 \circ f_1 \\ &= 3((2X + 1) + 2) - 1 \\ &= 6X + 6, \end{aligned}$$

On the other hand, if at least two of the f_i have degree > 2, then this factorization tells us that $f'_{[n]}$ is reducible. Thus for example, suppose $f_1 = X^2 + 2$, $f_2 = X^3 - X + 1$, and $f_3 = X - 1$. Then we have

$$\begin{aligned} f_{[3]} &= f_3 \circ f_2 \circ f_1 \\ &= ((X^2 + 2)^3 - (X^2 + 2) + 1) - 1 \\ &= X^6 + 6X^4 + 11X^2 + 6 \\ &= (X - i)(X + i)(X - i\sqrt{2})(X + i\sqrt{2})(X - i\sqrt{3})(X + i\sqrt{3}) \end{aligned}$$

If one calculates this derivative in the usual way, one will find that it equals

$$\begin{aligned} f'_{[3]} &= (f'_3 \circ f_{[2]})(f'_2 \circ f_{[1]})f'_1 \\ &= ((3X^2 - 1) \circ f_1)2X \\ &= (3(X^2 + 2)^2 - 1)2X. \end{aligned}$$

Thus if we ever need to cook up an example of a polynomial whose derivative has many factors, then $f_{[n]}$ is a good candidate to consider. The factors of $f'_{[n]}$ tell us where the critical points of $f_{[n]}$ are; namely α is a critical point of $f_{[n]}$ if and only if $f'_i(f_{[i-1]}(\alpha)) = 0$ for some i if and only if $f_{[i-1]}(\alpha)$ is a critical point of f_i for some i.

2.2 Degree

Another obvious identity:

$$\deg f_{[n]} = \prod_{i=1}^{n} \deg f_n.$$

2.3 Algebraic Properties

Next let's record some algebraic properties of $\circ$. We have

1. $(g_1 \circ f)(g_2 \circ f) = (g_1 g_2) \circ f$
2. $g_1 \circ f + g_2 \circ f = (g_1 + g_2) \circ f$

2.4 Substitution

Recall that the Fundamental Theorem of Calculus tells us that

$$\int_0^1 f' \mathrm{d}t = f(1) - f(0).$$

In particular, we have $\int_0^g f \mathrm{d}t = f \circ g - f(0)$. Thus $(\int_0^g f)' = (f \circ g)' = (f' \circ g)g'$ and we can solve $\int (f \circ g)\mathrm{d}x$ via u-substitution. Namely, we set $u = g$ (so $\mathrm{d}u = g'\mathrm{d}x = u'\mathrm{d}x$), then this integral becomes $\int f(u)u'\mathrm{d}u =$