Galois Groups as Tree Automorphisms

1 Definitions

1.1 Trees in a Ring

Definition 1.1. Let R be a ring. A **tree** in R sequence of pairs $((\mathcal{R}_n, f_n))_{n\in\mathbb{N}}$ where $(\mathcal{R}_n)_{n\in\mathbb{N}}$ is a sequence of pairwise disjoint subsets of R and where $(f_n)_{n\in\mathbb{N}}$ is a sequence of polynomials in $R[X]$ such that f_n restricts to a d_n-to-1 map from $\mathcal{R}_n$ to $\mathcal{R}_{n-1}$ for each $n \geq 2$ where $d_n = \deg(f_n)$.

Remark 1. To clean notation further, we often write "let $(\mathcal{R}_n, f_n)$ be a tree in R" to mean "let $((\mathcal{R}_n, f_n))_{n\in\mathbb{N}}$ be a tree in R".

Definition 1.2. Let R be a ring, let $(\mathcal{R}_n, f_n)$ be a tree in R, and let G be a subgroup of $\mathrm{Aut}(R)$, the group of all automorphisms of R. We say $(\mathcal{R}_n, f_n)$ is an G-**tree** in R if for each $n \in \mathbb{N}$ the following two conditions are satisfied:

1. If $\sigma \in G$, then $\sigma f_n = f_n \sigma$.
2. The natural action of G on R restricts to a transitive action of G on $\mathcal{R}_n$ for each $n \in \mathbb{N}$.

1.2 Galois Trees

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_n) be 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 for each $n \in \mathbb{N}$. Let $\mathcal{R}_n$ be the set of roots of $f_{[n]}$ in $\overline{K}$. Then $(\mathcal{R}_n, f_n)$ is a G-tree in $\overline{K}$.

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 $\mathcal{R}_n$ to $\mathcal{R}_{n-1}$. To see that it does, let $\alpha \in \mathcal{R}_{n-1}$ 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 1.1. 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 G-tree in $\overline{\mathbb{Q}}$.

1.2.1 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. $\square$

Example 1.2. 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).