
Journal of Algebraic Combinatorics **10** (1999), 135–148

Galois Graphs: Walks, Trees and Automorphisms

JOSEP M. BRUNAT brunat@ma2.upc.es
JOAN-C. LARIO lario@ma2.upc.es
Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Pau Gargallo, 5, 08028-Barcelona, Catalunya, Spain

Received December 2, 1996; Revised March 25, 1998

Abstract. Given a symmetric polynomial $\Phi(x, y)$ over a perfect field k of characteristic zero, the Galois graph $G(\Phi)$ is defined by taking the algebraic closure $\bar{k}$ as the vertex set and adjacencies corresponding to the zeroes of $\Phi(x, y)$. Some graph properties of $G(\Phi)$, such as lengths of walks, distances and cycles are described in terms of Φ. Symmetry is also considered, relating the Galois group $\mathrm{Gal}(\bar{k}/k)$ to the automorphism group of certain classes of Galois graphs. Finally, an application concerning modular curves classifying pairs of isogeny elliptic curves is revisited.

Keywords: Galois, graph, digraph, tree, automorphism

1. Introduction

Let k be a perfect field of characteristic zero and let $\bar{k}$ denote the algebraic closure of k. To a given polynomial $\Phi(x, y)$ with two indeterminates and coefficients in k, we attach the following directed graph $G(\Phi)$:

- vertices: $j \in \bar{k}$,
- arcs: (j_1, j_2) is an arc with multiplicity n if $\Phi(j_1, y)$ has j_2 as a root with multiplicity n.

To make the definition consistent, the multiplicity of every $j_2 \in \bar{k}$ is taken to be 1 whenever $\Phi(j_1, y)$ is the zero polynomial.

We will refer to $G(\Phi)$ as the *Galois graph* of Φ. Note that if $\Phi(x, y)$ is a constant polynomial, then $G(\Phi)$ is the complete or the null graph depending on whether the constant is zero or not. From now on, we will put to one side these degenerate cases and assume that $\Phi(x, y)$ is a non-constant polynomial. As we will be mainly interested in properties of non directed graphs, it is natural to assume (and we do from now on) that $\Phi(x, y)$ is a symmetric polynomial. Nevertheless, Sections 2 and 3 can easily be adapted to the nonsymmetric case.

Our aim is to explore some properties of $G(\Phi)$ in terms of the polynomial $\Phi(x, y)$. In the next section, we classify what we call singular vertices of $G(\Phi)$. These are vertices destroying the regularity of $G(\Phi)$ and form a finite set easily described from Φ. In Section 3 we will discuss walks, distances and cycles, providing detection and counting results from

Research of the authors was supported in part by the CICYT grant TIC 97-0963 and DGICYT grant PB96-0970-C02-02, respectively.

recursive sequences of polynomials. The notion of a *k-graph* is introduced in Section 4. A k-graph is a graph with vertices in $\bar{k}$ such that the Galois automorphisms of $\mathrm{Gal}(\bar{k}/k)$ are graph automorphisms. For instance, Galois graphs $G(\Phi)$ are k-graphs. Then, for a finite k-tree T, we show that the vertices in the center $Z(T)$ are algebraic numbers of degree 1 or 2 over k, and that $Z(T)$ is contained in the *kernel* of T, the subgraph induced by the vertices of minimum degree. Moreover, we show that the kernel is a connected subgraph. In Section 5, we deal with the action of $\mathrm{Gal}(\bar{k}/k)$ on k-trees providing criteria to decide whether the Galois automorphisms embed surjectively on the graph automorphism group. Finally, in the last section we present an application concerning the Galois graphs resulting from the modular curves $X_0(N)$. These curves classify pairs of isomorphism classes of cyclic isogenies of degree N between elliptic curves and are defined by the classical modular polynomials $\Phi_N(x, y)$. For an introduction to modular curves and modular polynomials we refer to [5, 6]. For algebraic and graph-theoretical notions we refer to [2] and [1, 4], respectively.

2. Singular vertices

In this section we show that Galois graphs $G(\Phi)$ are almost regular. Let ν be the degree of $\Phi(x, y)$ in one of the indeterminates. A vertex is said to be *singular* if:

- its out-valency is not ν, or
- it is the origin of a multiple arc, or
- it is a loop vertex.

We shall characterize the singular vertices as the roots of a certain polynomial and so only a finite number exists.

The symmetric polynomial $\Phi(x, y)$ can be written as

$$\Phi(x, y) = \sum_{r=0}^{\nu} f_r(x) y^r = \sum_{r=0}^{\nu} f_r(y) x^r,$$

for some polynomials $f_r(x)$ in $k[x]$. The out-valency of a vertex j in $G(\Phi)$ is the degree of the polynomial $\Phi(j, y)$ and it coincides with the maximum subscript r such that $f_r(j) \neq 0$ provided that $\Phi(j, y)$ is a non-zero polynomial. When $\Phi(j, y) = 0$, the out-valency of j is ∞ which means that j is a root of the polynomial

$$F(x) = \gcd(f_0(x), \ldots, f_\nu(x)).$$

Note that the out-valency of a vertex is infinite if and only if the in-valency is infinite, although if both are finite they can be distinct (see Example 1 below). Letting $q_r(x) = f_r(x)/F(x)$ for $0 \leq r \leq \nu$, we have

$$\Phi(x, y) = F(x) \sum_{r=0}^{\nu} q_r(x) y^r = F(y) \sum_{r=0}^{\nu} q_r(y) x^r,$$

so $\Phi(x, y) = \Phi_0(x, y)\Phi_1(x, y)$, where $\Phi_0(x, y) = F(x)F(y)$, and $\Phi_1(x, y)$ is a symmetric polynomial such that $\Phi_1(j, y) \neq 0$ for all j in $\bar{k}$. Then, the graph $G(\Phi)$ admits the

decomposition

$$G(\Phi) = G(\Phi_0) \oplus G(\Phi_1),$$

where $G(\Phi_0)$ and $G(\Phi_1)$ are arc-disjoint and $G(\Phi_1)$ is locally finite (i.e., each vertex has finite valency). The arcs of $G(\Phi_0)$ are all the pairs (j_1, j_2), (j_2, j_1) with $F(j_1) = 0$ and $j_2 \in \bar{k}$. According to the above, the structure of $G(\Phi)$ is completely determined by the structure of $G(\Phi_1)$, so we can (and do) restrict ourselves to studying locally finite Galois graphs.

Now, the degree ν of $\Phi(x, y)$ in one of the indeterminates is an upper bound of the out-valencies and the vertices with out-valency $<\nu$ are those which are roots of the polynomial $f_\nu(x)$. In particular, the isolated vertices are the roots of the polynomial $\gcd(f_1(x), \ldots, f_\nu(x))$.

Let j be the origin of a multiple arc. In this case, the polynomial $\Phi(j, y)$ has a multiple root which is a root of the discriminant

$$D(x) = \text{Resultant}(\Phi(x, y),\ \Phi'_y(x, y),\ y)\,,$$

where $\Phi'_y(x, y)$ means the partial derivative of $\Phi(x, y)$ with respect to y. The leading coefficients of $\Phi(x, y)$ and $\Phi'_y(x, y)$ as polynomials in the indeterminate y are $f_\nu(x)$ and $\nu f_\nu(x)$ respectively, so $f_\nu(x)$ is a factor of $D(x)$. Thus, the vertices with out-valency $<\nu$ are also roots of $D(x)$. Conversely, if $D(j) = 0$, then either $f_\nu(j) = 0$ or the polynomials $\Phi(j, y)$ and $\Phi'_y(j, y)$ have a common root, i.e., either j has out-valency $<\nu$ or it is the origin of a multiple arc.

Finally, the vertices j with a loop are the roots of $L(x) = \Phi(x, x)$.

Putting all this together, the singular vertices are characterized as the roots of the polynomial $S(x) = F(x)D(x)L(x)$, so they are in number less than or equal to $\deg S(x)$.

If a subgraph of $G(\Phi)$ does not have singular vertices, then every pair of arcs (j_1, j_2), (j_2, j_1) is considered as an *edge* and the subgraph as an (undirected simple) graph.

To end this section, we provide a first example of a Galois graph. For future reference, the connected component in $G(\Phi)$ of a vertex j will be denoted by $G(\Phi, j)$.

Example 1 Take $\Phi(x, y) = x^3 + y^3 - 1$ over $\mathbf{Q}$. We have $f_\nu(x) = 1$, so every vertex has out-valency 3. The discriminant is $D(x) = 27(1 - x^3)$, and the loops are the roots of $L(x) = 2x^3 - 1$. Figure 1 gives some connected components of $G(\Phi)$, where the absence of arrows represents edges. Note that all connected components apart from $G(\Phi, 0)$ and $G(\Phi, \sqrt[3]{1/2})$ do not have singular vertices, and therefore can be considered as undirected graphs.

3. Walks, distances and cycles

A *walk* of length n (or a n-walk) in $G(\Phi)$ is a sequence

$$j_0, e_1, j_1, e_2, j_2, \ldots, j_{n-1}, e_{n-1}, j_n,$$

where $e_i = (j_{i-1}, j_i)$ are arcs of $G(\Phi)$. A *path* is a walk with no vertex repetition. A vertex j_2 is said to be *n-reachable* from a vertex j_1 if there is a n-walk with j_1 and j_2 as, respectively,

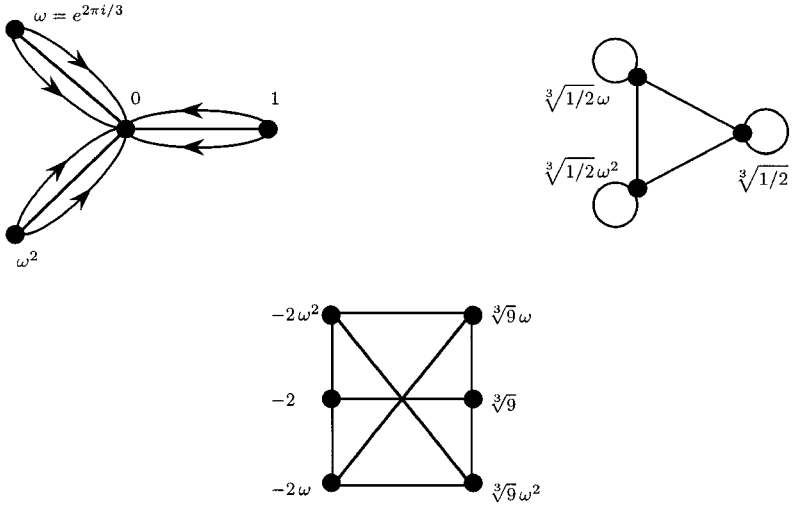

Figure 1. Some connected components of $G(\Phi)$ where $\Phi(x, y) = x^3 + y^3 - 1$.

the starting and end point vertices. The *distance* between distinct vertices j_1 and j_2 is defined as the minimum length of a path from j_1 to j_2, or ∞ when there is none, and it is denoted by $d(j_1, j_2)$. Since Φ is assumed to be symmetric, note that $d(j_1, j_2) = d(j_2, j_1)$.

We now introduce a recursive sequence of polynomials associated with the graph $G(\Phi)$ which allows us to have control over reachability and the number of walks in $G(\Phi)$ joining two vertices. Let $j \in \bar{k}$ and define

$$\psi_0^j(y) = y - j;$$
$$\psi_1^j(y) = \Phi(j, y);$$
$$\psi_n^j(y) = \text{Resultant}\big(\psi_{n-1}^j(t), \Phi(t, y), t\big), \quad \text{if } n \geq 2.$$

Proposition 1 *The vertex j_2 is n-reachable from j_1 if and only if $\psi_n^{j_1}(j_2) = 0$. Moreover, the number of n-walks from j_1 to j_2 coincides with the multiplicity of the root j_2 in $\psi_n^{j_1}(y)$.*

Proof: The proof is by induction on n, the claim being easily checked for $n = 0, 1$. For $n \geq 2$, let $t_1, \ldots, t_r$ be the vertices $(n-1)$-reachable from j_1 and n_i the number of $(n-1)$-walks from j_1 to t_i. By the induction hypothesis, $\psi_{n-1}^{j_1}(t) = a_0 \prod_{i=1}^r (t - t_i)^{n_i}$ for some constant $a_0 \neq 0$. Now, $\psi_n^{j_1}(y)$ is $\prod_{i=1}^r \Phi(t_i, y)^{n_i}$ up to some power of a_0. Therefore, $\psi_n^{j_1}(j_2) = 0$ if and only if j_2 is adjacent from some t_i, that is to say, if j_2 is n-reachable from j_1. The multiplicity, say m_i, of j_2 as a root of $\Phi(t_i, y)$ is the number of 1-walks from t_i to j_2. Thus, $n_i m_i$ is the number of n-walks from j_1 to j_2 through t_i. Therefore $\sum_{i=1}^r n_i m_i$ is the number of n-walks from j_1 to j_2 and it is also the multiplicity of j_2 as a root of $\psi_n^j(y)$. □

A slight modification of the above permits the characterization of the vertices whose distance to a fixed vertex is constant. Recall that the *radical* of a polynomial $f(x) \in \bar{k}[x]$ is defined by $\operatorname{rad} f(x) = f(x)/\gcd(f(x), f'(x))$. This is a separable polynomial with the same roots as $f(x)$. Now, fix a vertex j of $G(\Phi)$ and define the sequence of univariate polynomials

$$\chi_0^j(y) = y - j;$$
$$\chi_n^j(y) = \operatorname{rad} \psi_n^j(y)/\operatorname{rad} \prod_{k=0}^{n-1} \gcd\big(\psi_k^j(y), \psi_n^j(y)\big), \quad \text{if } n \geq 1.$$

We have:

Proposition 2 *The roots of $\chi_n^j(y)$ are the vertices at distance n from j. Moreover, the number of paths from j to such a vertex coincides with its multiplicity in $\psi_n^j(y)$.*

Proof: The case $n = 0$ is obvious, so let $n \geq 1$. The vertices at distance n from j are the vertices n-reachable from j which are not k-reachable for $0 \leq k \leq n-1$. The roots of $\operatorname{rad} \psi_n^j(y)$ are the vertices n-reachable from j and have multiplicity one. On the other hand, the roots of $\gcd(\psi_k^j(y), \psi_n^j(y))$ are the vertices which are simultaneously k-reachable and n-reachable from j. Then, the roots of the denominator are the vertices n-reachable from j which are k-reachable for some $0 \leq k \leq n-1$, and they have multiplicity one. Therefore, we conclude that the roots of $\chi_n^j(y)$ are the vertices at distance n from j.

If j_1 is at distance n from j, a n-walk from j to j_1 is a n-path. Hence the second claim follows from Proposition 1. □

Note that a connected component $G(\Phi, j)$ is finite if and only if $\chi_n^j(y)$ is a non-zero constant polynomial for some $n \geq 0$. In this case the diameter of $G(\Phi, j)$ is $\leq n$.

It is possible to give an alternative construction for the above distance polynomials as follows. Define

$$\bar{\chi}_0^j(y) = \chi_0^j(y);$$
$$\bar{\chi}_1^j(y) = \chi_1^j(y);$$
$$\bar{\psi}_n^j(y) = \operatorname{rad} \text{ Resultant } \big(\bar{\chi}_{n-1}^j(t), \Phi(y,t),\ t\big), \quad \text{if } n \geq 1;$$
$$\bar{\chi}_n^j(y) = \bar{\psi}_n^j(y)\big/\big(\gcd\big(\bar{\psi}_{n-1}^j(y), \bar{\chi}_{n-1}^j(y)\big) \gcd\big(\bar{\psi}_n^j(y), \bar{\chi}_{n-2}^j(y)\big)\big), \quad \text{if } n \geq 2.$$

The roots of $\bar{\psi}_n^j(y)$ are the vertices adjacent to vertices at distance $n-1$ from j, so are vertices at distance $n-2, n-1$ or n from j, including all the vertices at distance n. By dividing by the product of the gcd's, only the vertices at distance n remain. Thus, we have a result analogous to Proposition 2 for the polynomials $\bar{\chi}_n^j$. In fact, $\chi_n^j(y) = a_n \bar{\chi}_n^j(y)$ for a constant a_n.

Example 2 Consider the Galois graph attached to the polynomial $\Phi(x, y) = x^3 + y^3 + xy - 1$ over the field of rational numbers $\mathbf{Q}$. Figure 2 displays part of the connected component $G(\Phi, 0)$, and the polynomials $\chi_n^0(y)$ for $0 \leq n \leq 4$ can be read from Table 1.

Table 1. Polynomials $\chi_n^0(y)$ for the graph $G(\Phi)$ where $\Phi(x, y) = x^3 + y^3 + xy - 1$.

	Type (a) vertices	Type (b) vertices
$\chi_0^0(y) =$	y	
$\chi_1^0(y) =$	$(y^2 + y + 1)$	$(y - 1)$
$\chi_2^0(y) =$	$(y^4 - y^2 + 1)$	$(y^2 + 1)$
$\chi_3^0(y) =$	$(y^4 - 2y^3 + 2y^2 - 4y + 4)$	$(y^2 + 2y + 2)$
$\chi_4^0(y) =$	$(y^8 + 3y^6 + 4y^5 + 4y^4 + 6y^3 + 19y^2 - 10y + 25)$	$(y^4 - 3y^2 + 2y + 5)$

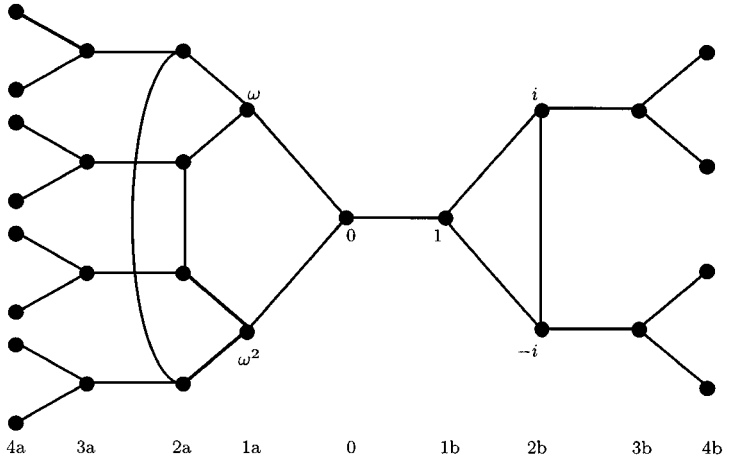

Figure 2. Part of the connected component $G(\Phi, 0)$ where $\Phi(x, y) = x^3 + y^3 + xy - 1$.

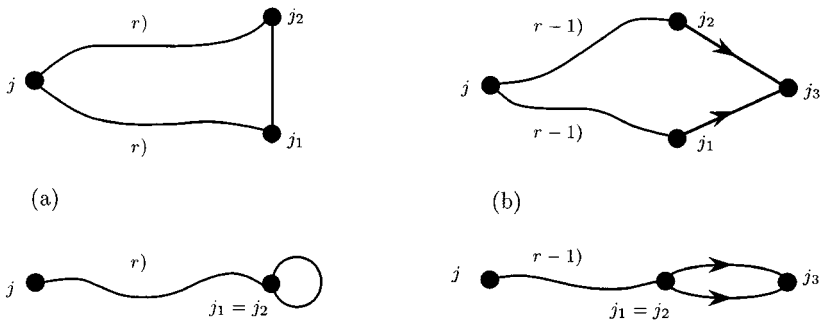

Figure 3. Illustrations of Lemma 3.1 (a) and Lemma 3.2 (b).

In order to detect non-obvious (i.e. of length ≥ 3) cycles in $G(\Phi)$ and characterize finite subtrees of $G(\Phi)$, we need the following two Lemmas. They provide necessary and sufficient conditions for the existence of a certain types of adjacencies, as illustrated in figure 3.

Given a fixed $j \in \bar{k}$, for $r \geq 0$ set

$$a_r(j) = \text{Resultant}\big(\text{Resultant}\big(\chi_r^j(x), \Phi(x, y), x\big), \chi_r^j(y), y\big).$$

Lemma 1 *The equality $a_r(j) = 0$ holds if and only if there are either two distinct adjacent vertices at distance r from j, or a loop vertex at distance r from j.*

Proof: The condition $a_r(j) = 0$ is equivalent to the existence of some j_2 such that $\text{Resultant}(\chi_r^j(x),\ \Phi(x, j_2),\ x) = 0$ and $\chi_r^j(j_2) = 0$. The first condition is equivalent to the existence of some j_1 such that $\chi_r^j(j_1) = 0$ and $\Phi(j_1, j_2) = 0$. Thus, $a_r(j) = 0$ if and only if there exist two adjacent vertices j_1, j_2 at distance r from j, the case $j_1 = j_2$ corresponding to the existence of a loop vertex. □

Analogously, for $j \in \bar{k}$ and $r \geq 0$ define

$$b_r(j) = \text{Resultant}\left(\frac{\psi_r^j(y)}{\gcd\big(\psi_r^j(y), \chi_r^j(y)\big)},\ \chi_r^j(y), y\right).$$

Lemma 2 *Suppose that $r \geq 2$ and $b_{r-1}(j) \neq 0$. Then, $b_r(j) = 0$ if and only if either there are two distinct vertices at distance $r-1$ from j simultaneously adjacent to a vertex at distance r from j, or there is a vertex at distance $r-1$ which is the origin of a multi-arc with end-vertex at distance r from j.*

Proof: For $0 \leq s \leq r$, let $q_s(y) = \psi_s^j(y)/\gcd(\psi_s^j(y), \chi_s^j(y))$. Suppose first that $b_r(j) = 0$. Then $q_r(j_3) = \chi_r^j(j_3) = 0$ for some $j_3 \in \bar{k}$. Since j_3 is also a root of $\gcd(\psi_r^j(y), \chi_r^j(y))$, it follows that the multiplicity of j_3 as a root of $\psi_r^j(y)$ is ≥ 2. Hence, by Proposition 1, there are two distinct paths from j to j_3. Now, condition $b_{r-1}(j) \neq 0$ implies $q_{r-1}(j') \neq 0$ for all vertices j' at distance $r-1$ from j, and the multiplicity of each j' as a root of $\psi_{r-1}^j(y)$ is one. Hence, there is only one path from j to j'. Thus, there exist two vertices j_1, j_2 at distance $r-1$ from j both of them adjacent to j_3, and the case $j_1 = j_2$ corresponds to a multiple arc.

Conversely, if j_1, j_2, j_3 exist as in figure 3(b), we have $\chi_r^j(j_3) = 0$ and the multiplicity of j_3 as a root of $\psi_r^j(y)$ is ≥ 2. Hence, $q_r(j_3) = 0$ and j_3 is a common root of $q_r(y)$ and $\chi_r(y)$. (Note that, in this part, the hypothesis $b_{r-1}(j) \neq 0$ is not needed.) □

For $n \geq 0$, let $G(\Phi, j, n)$ be the subgraph of $G(\Phi)$ induced by the vertices of $G(\Phi)$ at distance $\leq n$ from j, and suppose that it does not have singular vertices, so it is considered as an undirected simple graph. To decide whether $G(\Phi, j, n)$ is a tree, we define

$$A_n(j) = \prod_{r=0}^{n} a_r(j);$$

$$B_n(j) = \prod_{r=0}^{n} b_r(j).$$

Then, we have:

Proposition 3 *Suppose that $G(\Phi, j, n)$ does not have singular vertices. Then $G(\Phi, j, n)$ is a tree if and only if $A_n(j)B_n(j) \neq 0$.*

Proof: First, let us suppose that $A_n(j)B_n(j) = 0$. It is sufficient to show that there are two distinct paths between two vertices. If $A_n(j) = 0$, then some $a_r(j) = 0$ and, since $G(\Phi, j, n)$ has no singular vertices, Lemma 1 implies that there are two distinct adjacent vertices j_1, j_2 at distance r from j. Therefore, we find two distinct paths from j to j_1, one of length r and the other of length $r + 1$, the last edge being (j_2, j_1).

If $B_n(j) = 0$, then take r as the first index such that $b_r(j) = 0$. Note that $r \geq 1$ due to the fact that $b_0(j) \neq 0$. By Lemma 2, there are two distinct vertices j_1, j_2 at distance $r - 1$ from j, both adjacent to a vertex j_3 with $d(j, j_3) = r$. Therefore, we also find in this case two paths from j to j_3, one through j_1 and another through j_2.

Conversely, suppose that $G(\Phi, j, n)$ has a cycle. Choose j_3 to be a vertex belonging to a cycle in $G(\Phi, j, n)$ and at a maximum distance, say r, from j. If $b_s(j) = 0$ for some $s < r$, we are done. So, suppose that $b_s(j) \neq 0$ for all $s < r$. Let j_1 and j_2 be distinct vertices adjacent to j_3 of the cycle. If $d(j, j_1) = d(j, j_2) = r - 1$, then Lemma 2 implies $b_r(j) = 0$ and $B_n(j) = 0$. Otherwise, j_1 or j_2 is at distance r from j, and, by applying Lemma 1 we get $a_r(j) = 0$ and $A_n(j) = 0$. □

4. *k*-graphs and *k*-trees

Let $H = (V, E)$ be a graph with $V \subset \bar{k}$. We say that H is a *k-graph* if the map

$$\rho: \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(H), \quad \sigma \mapsto \sigma_{|V}$$

is well-defined and a group homomorphism. In other words, H is a k-graph if the automorphisms of $G_k = \mathrm{Gal}(\bar{k}/k)$ act as automorphisms of the graph H. The automorphisms of H in the image of ρ will be called *Galois automorphisms* of H.

The class of k-graphs is larger than that of Galois graphs. Indeed, if $\sigma \in G_k$ and j_2 is a root of $\Phi(j_1, y)$, then j_2^σ is a root of $\Phi(j_1^\sigma, y)$ with the same multiplicity, so σ acts on $G(\Phi)$ as a graph automorphism. The study of the symmetry of Galois graphs fits well in the more general setting of k-graphs.

The algebraic *degree* of a $j \in \bar{k}$ is defined as the degree of its minimum polynomial over k. The *kernel* of a graph H, denoted in the sequel by $\mathrm{Ker}H$, is the graph induced by the set of vertices in H with minimum degree. The degree of the vertices in $\mathrm{Ker}H$ will be denoted by $\deg \mathrm{Ker}H$.

Lemma 3 *If H is a k-graph, then $\mathrm{Ker}H$ is a k-graph.*

Proof: If $j \in \mathrm{Ker}H$ and $\sigma \in G_k$, then $j^\sigma \in H$ since H is a k-graph, and the degrees of j^σ and j coincide. Hence, $j^\sigma \in \mathrm{Ker}H$. Therefore the Galois automorphisms of H apply the induced subgraph $\mathrm{Ker}H$ on itself and they act on $\mathrm{Ker}H$ as graph automorphisms. □

As for the connected components of k-graphs, the property of being also a k-graph admits the following characterization:

Proposition 4 *Let H be a k-graph, j a vertex of H, and $H(j)$ its connected component. Then the following statements are equivalent*:
(i) $j^{G_k} \subset H(j)$;
(ii) $\mathrm{Ker}H(j)$ *is a k-graph*;
(iii) $H(j)$ *is a k-graph.*

Proof: (i)⇒(iii) By hypothesis, j and j^σ are in the same connected component of H for all σ in G_k. Moreover, σ applies the connected component of j on the connected component of j^σ. Hence, $H(j)^\sigma = H(j^\sigma) = H(j)$ and $H(j)$ is a k-graph.

(iii)⇒(ii) by Lemma 3.

(ii)⇒(i) Let $j_1 \in \mathrm{Ker}H(j)$. Since $\mathrm{Ker}H(j)$ is a k-graph, $j_1^{G_k} \subset \mathrm{Ker}H(j) \subset H(j) = H(j_1)$. By applying (i)⇒(iii), we have that $H(j) = H(j_1)$ is a k-graph. □

By applying the above proposition to a rational j in k, we obtain the following corollary.

Corollary 1 *If $j \in k$ is a vertex of a k-graph H, then $H(j)$ is a k-graph.*

Note that this provides us with an easy way to construct k-graphs, just by taking connected components of rational vertices in Galois graphs.

We now focus on k-trees. First, we consider finite k-trees. As we shall see, in this case the center determines the degree of the kernel. Recall that the *eccentricity* of a vertex j in a finite connected graph is the maximum of the distances from j to any vertex, and the *center* of the graph is the set of vertices with minimum eccentricity. It is known that the center $Z(T)$ of a finite tree T consists of a unique vertex or two adjacent vertices (see [1]). Moreover, $Z(T)^\sigma = Z(T)$ for all automorphisms of T, in particular if T is a k-tree, $Z(T)^\sigma = Z(T)$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$.

Proposition 5 *If T is a finite k-tree, then the following assertions hold*:
(i) *if $Z(T) = \{c\}$, then $c \in k$ and* $\deg \mathrm{Ker}\ T = 1$;
(ii) *if $Z(T) = \{c_1, c_2\} \not\subset k$, then c_1 and c_2 are quadratic conjugates and* $\deg \mathrm{Ker}\ T = 2$;
(iii) $Z(T) \subset \mathrm{Ker}\ T$.

Proof:

(i) The center $Z(T)$ is fixed for all automorphism, so $c^\sigma = c$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Hence, $c \in k$ and $\deg \mathrm{Ker}\ T = 1$.
(ii) Suppose that $c_1 \notin k$. For some $\sigma \in \mathrm{Gal}(\bar{k}/k)$, we have $c_1^\sigma \neq c_1$. Now, $Z(T)^\sigma = Z(T)$ implies $c_1^\sigma = c_2$. Analogously, $c_2^\sigma = c_1$ and $c_2 \notin k$. Hence, the polynomial $p(x) = (x - c_1)(x - c_2) \in k[x]$ is irreducible and, therefore, c_1, c_2 are quadratic over k. We claim that T does not have a vertex in k. Indeed, let $j \in k$ be a vertex of T. Because

c_1 and c_2 are adjacent and T is a tree, the distances $d(c_1, j)$ and $d(c_2, j)$ differ by 1, say $d(c_2, j) = r$, and $d(c_1, j) = r + 1$. We have

$$r = d(c_2, j) = d\left(c_1^\sigma, j^\sigma\right) = d(c_1, j) = r + 1,$$

which is a contradiction.

(iii) If $Z(T) \subset k$, then the vertices in $Z(T)$ are of minimum degree and $Z(T) \subset \text{Ker } T$; otherwise, by applying (ii), $Z(T) \subset \text{Ker } T$. □

In the case of k-trees which are not necessarily finite, we have the following Proposition:

Proposition 6 *If T is a k-tree, then the following assertions hold*:

(i) $\deg \text{Ker } T \in \{1, 2\}$;

(ii) *if* $\deg \text{Ker } T = 2$, *then there is a vertex in* Ker T *adjacent to its conjugate*;

(iii) $k(j_1) = k(j_2)$ *for all* $j_1, j_2 \in \text{Ker } T$;

(iv) Ker T *is a k-tree*;

Proof: Take $j \in \text{Ker } T$ and let M be the minimal subtree of T which contains the set j^{G_k} of all the conjugates of j. The tree M is finite and, for all $\sigma \in G_k$, we have $(j^{G_k})^\sigma = j^{G_k}$, so $M^\sigma = M$ and M is a finite k-tree. Therefore, Proposition 5 can be applied to M. Since $\deg \text{Ker } T = \deg \text{Ker} M \in \{1, 2\}$, it follows (i).

If $\deg \text{Ker } T = 2$, then $Z(M)$ consists of two conjugate and adjacent vertices, which are in Ker T and (ii) holds.

The proof of (iii) and (iv) depends on $Z(M)$. First, assume $Z(M) \subset k$ and let $c \in Z(M)$. Then $k(j_1) = k(c) = k$ for all $j_1 \in \text{Ker } T$ and (iii) holds. To show (iv), take $j_1, j_2 \in \text{Ker } T$ and the path P from j_1 to j_2. Since $j_1, j_2 \in k$, the path P is fixed for all Galois automorphisms σ. Hence, $j^\sigma = j$ for all $j \in P$. It follows that $j \in \text{Ker } T$ and Ker T is a subtree of T. From Lemma 3 it is also a k-graph.

Second, suppose $Z(M) = \{c_1, c_2\} \not\subset k$. Observe that, since c_1 and c_2 are quadratic conjugate, $k(c_1) = k(c_2)$. Let now $j \in \text{Ker } T$ and fix a Galois automorphism $\sigma \in \text{Gal}(\bar{k}/k)$ as before. Interchanging c_1 and c_2 if necessary, we can assume that $d(j, c_1^\sigma) = d(j, c_2) = d(j, c_1) + 1$. There is a path, say P, in T from j to j^σ. If $\tau \in \text{Gal}(k(c_1)/k)$, the path P^σ is either P or the reverse of P. Then τ acts on P either as the identity or as σ, so $k(j) = k(c_1)$. Thus, (iii) is satisfied.

To show (iv), let j_1 be a vertex of the path, say P_1, from $j \in \text{Ker } T$ to c_1 and consider the path P from j to j^σ. It is clear that P contains P_1. Now, every $\tau \in \text{Gal}(\bar{k}/k)$ acts on P either as the identity or as σ. Hence j_1 has exactly one conjugate, j_1^σ, which tells us that j_1 is quadratic over k. Moreover, P_1 is a path in Ker T and Ker T is a k-tree. □

5. Automorphisms

For a given k-graph H, the representation

$$\rho: \text{Gal}(\bar{k}/k) \longrightarrow \text{Aut}(H), \quad \sigma \mapsto \sigma_{|V}$$

is in general far from being surjective and it appears natural to ask how to determine the image of ρ. As for the kernel, it is clear that ρ factors through $\mathrm{Gal}(k(H)/k)$, where $k(H)$ denotes the extension obtained by adjoining the vertices of H to the field k.

In order to determine the image of ρ, we will make some restrictions on the k-graphs under consideration. Indeed, we will analyze the situation for finite k-trees with some extra conditions.

For a finite k-tree, say T, we need to consider the filtration

$$\mathrm{Ker}\, T = T_0 \subset T_1 \subset \cdots \subset T_{r-1} \subset T_r = T,$$

where T_s is the subtree of T induced by the vertices at distance at most s from Ker T, and s runs the integers 0 through the eccentricity of the kernel $r = \max\{d(j, \mathrm{Ker}\, T) \mid j \in T\}$. Since Ker T is a k-tree, and the Galois action preserves distances, it follows that each T_s is also a k-tree.

Our assumption on T will be null if the eccentricity of Ker T is 0, otherwise the following hypothesis (H) will apply:

H1: all the leaves of T are at distance r from Ker T;
H2: $\mathrm{Gal}(k(T_s)/k(T_{s-1})) \simeq \{f \in \mathrm{Aut}(T_s) : f_{|T_{s-1}} = id\}$, for $1 \leq s \leq r$.

Note that under hypothesis (H1), the tree T_{s-1} is obtained from T_s by deleting all its leaves and, therefore, the restriction of every $f \in \mathrm{Aut}\, T_s$ to T_{s-1} yields to an automorphism of T_{s-1}.

The following result shows that in this particular setting, the property of being a Galois automorphism can be decided just by checking it over the kernel.

Proposition 7 *Let T be a finite k-tree which satisfies* (H), *and denote its representation by ρ: $\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(T)$. Then, we have*:

$$\mathrm{Im}\,\rho = \{f \in \mathrm{Aut}(T) : \textit{ there is } \sigma \in \mathrm{Gal}(\bar{k}/k) \textit{ such that } f_{|\mathrm{Ker}T} = \rho(\sigma)_{|\mathrm{Ker}T}\}.$$

Proof: Let r be the eccentricity of Ker T. The case $r = 0$ is immediate, so we assume $r \geq 1$. For $1 \leq s \leq r$, let

$$H_s = \left\{f \in \mathrm{Aut}(T_s) : f_{|T_{s-1}} = id\right\},$$

$$\Gamma_s = \{f \in \mathrm{Aut}(T_s) : \text{ there is } \sigma \in \mathrm{Gal}(\bar{k}/k) \text{ such that } f_{|\mathrm{Ker}T} = \rho(\sigma)_{|\mathrm{Ker}T}\}.$$

Our claim is $\mathrm{Im}\,\rho = \Gamma_r$. The inclusion $\mathrm{Im}\,\rho \subset \Gamma_r$ holds in general due to the fact that Ker T is a k-tree. We shall show that $[\Gamma_r : \mathrm{Im}\,\rho] = 1$ by induction on $r \geq 1$.

The tree T_{r-1} satisfies the induction hypothesis, so we have $\mathrm{Im}\,\rho_{r-1} = \Gamma_{r-1}$, where ρ_{r-1}: $\mathrm{Gal}(k(T_{r-1})/k) \longrightarrow \mathrm{Aut}(T_{r-1})$ is the corresponding natural representation. Since we have the inclusion

$$H_r \simeq \mathrm{Gal}(k(T_r)/k(T_{r-1})) \subset \mathrm{Gal}(k(T_r)/k) \simeq \mathrm{Im}\,\rho_r,$$

we can write the equality

$$[\Gamma_r : \mathrm{Im}\,\rho] = \frac{[\Gamma_r : H_r]}{[\mathrm{Im}\,\rho : H_r]}.$$

Calculating the above denominator, we obtain

$$\frac{|\mathrm{Im}\,\rho|}{|H_r|} = \frac{|\mathrm{Gal}(k(T_r)/k)|}{|\mathrm{Gal}(k(T_r)/k(T_{r-1}))|} = |\mathrm{Gal}(k(T_{r-1})/k)| = |\mathrm{Im}\,\rho_{r-1}| = |\Gamma_{r-1}|,$$

and

$$[\Gamma_r : \mathrm{Im}\,\rho] = \frac{[\Gamma_r : H_r]}{|\Gamma_{r-1}|}.$$

It is easy to check that the map

$$\Gamma_r/H_r \longrightarrow \Gamma_{r-1}$$

defined by sending each coset fH_r to the restriction of f to T_{r-1} is well-defined and injective. Thus, we have $[\Gamma_r : \mathrm{Im}\,\rho] = 1$. □

Corollary 2 *Let T be as above and assume that* $\mathrm{Ker}\,T = Z(T)$. *Then, ρ is surjective.*

Proof: By Proposition 5, the center $Z(T)$ contains either only one or two rational vertices in k, or two conjugate quadratic vertices over k. In both cases, all automorphisms of T act on $\mathrm{Ker}\,T$ as Galois automorphisms. Hence, the above proposition shows that $\Gamma_r = \mathrm{Aut}(T)$ and ρ is surjective. □

Example 3 Take the modular polynomial

$$\Phi_2(x, y) = x^3 + y^3 - x^2y^2 + 2^4 3 \cdot 31(x^2y + xy^2) - 2^4 3^4 5^3(x^2 + y^2) + 3^4 5^3 4027xy + 2^8 3^7 5^6(x + y) - 2^{12} 3^9 5^9.$$

After computing the first distance polynomials as in Section 3, we consider the induced subgraph T of the connected component $G(\Phi, -1/15)$ shown in figure 4, where

A	$-1/15$	E	$272223782641/164025$
B	$13997521/225$	F	$4733169839/3515625$
C	$111284641/50625$	G	$-147281603041/215233605$
D	$56667352321/15$	H	$1114544804970241/405$

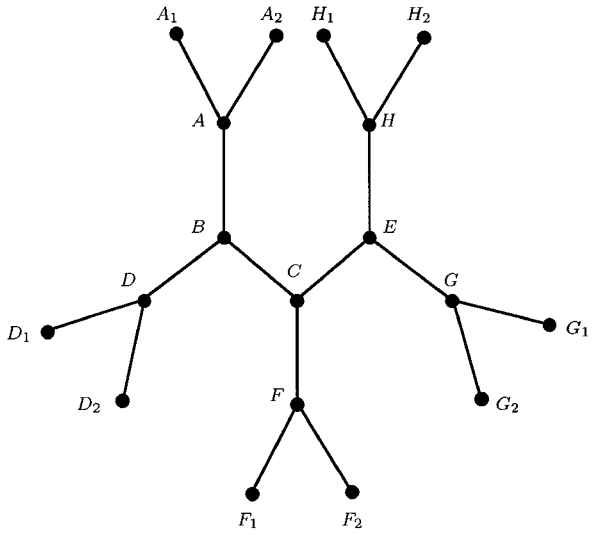

Figure 4. The graph T from the Example 3.

and the pairs (A_1, A_2), (D_1, D_2), (F_1, F_2), (G_1, G_2), and (H_1, H_2) are respectively the roots of the polynomials

$$x^2 - 2^4 3 \cdot 2081x + 3361^3/15$$
$$x^2 - 2^4 3^2 6203 \cdot 61471 \cdot 259925329x - 235130881^3/15$$
$$x^2 + 2^4 3 \cdot 17489 \cdot 26387 \cdot 213131/5^{16}x + 193^3 769^3 2593^3/(3^2 5^{20})$$
$$x^2 + 2^4 101 \cdot 1811 \cdot 2129521 \cdot 3324077/3^{32}x + 23^6 3433009^3/(3^{40}5)$$
$$x^2 - 2^4 3 \cdot 17 \cdot 97583 \cdot 95108797967742721x - 1346881^3 127681^3/(3^4 5).$$

The graph T is a k-tree, and its kernel is the subtree induced by the rational vertices A, B, C, D, E, F, and G. Observe that the eccentricity of Ker T is 1 and that the hyphotesis (H) of Proposition 7 is satisfied. In this case, we find that the Galois automorphisms of T form a group isomorphic to C_2^5, which is a subgroup of Aut $(T) \simeq C_2 + C_2[C_2[C_2]]$ of order 2^8, where the brackets stand for the wreath product (see [4]).

6. Application

Let $G = (V, E)$ be a k-graph and denote by $\rho: \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(G)$ the representation $\rho(\sigma) = \sigma_{|V}$. A mapping f from G to a graph H is a morphism of graphs if $j_1 \sim j_2$ implies $f(j_1) \sim f(j_2)$ for all $j_1, j_2 \in G$, where $\sim$ means adjacency. A surjective morphism of graphs $f: G \to H$ will be called G_k-*equivariant* if for all $j_1, j_2 \in G$ and $\sigma \in \mathrm{Gal}(\bar{k}/k)$,

$$f(j_1) = f(j_2) \Rightarrow f\left(j_1^\sigma\right) = f\left(j_2^\sigma\right);$$
$$f(j_1) \sim f(j_2) \Rightarrow f\left(j_1^\sigma\right) \sim f\left(j_2^\sigma\right).$$

The morphism f induces an action on H as follows:

$$\rho \otimes f : \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(H), \quad \sigma \mapsto f \circ \rho(\sigma) \circ f^{-1}.$$

Indeed, it is easy to check that $\rho \otimes f$ is well-defined and a group homomorphism. We call this action on H the twisted action by f, or simply the quotient action. Note that in general this new action on H does not make it a k-graph.

Proposition 8 *Assume that $G(\Phi_1\Phi_2, j)$ is a k-graph such that*:
(i) *$G(\Phi_1, j)$, $G(\Phi_2, j)$ are trees*,
(ii) *there are G_k-equivariant projectors $\pi_i : G(\Phi_1\Phi_2, j) \to G(\Phi_i, j)$, $i = 1, 2$.*
Then $G(\Phi_1\Phi_2, j)$ has a vertex over a compositum of at most two quadratic fields.

Proof: From the hypothesis we know that the Galois orbit of j is a subset of vertices in $G(\Phi_1\Phi_2, j)$. Note that for each σ in $G_k = \mathrm{Gal}(\bar{k}/k)$ we can view the connected components $G(\Phi_i, j^\sigma)$ as subgraphs of $G(\Phi_1\Phi_2, j)$. Consider $\pi_1(j^{G_k}) \subset G(\Phi_1, j)$ and let T_1 denote the minimal subtree of $G(\Phi_1, j)$ that connects the vertices of $\pi_1(j^{G_k})$. Analogously, define T_2 making use of the projector π_2. Since each $\rho \otimes \pi_i$ restricts to an automorphism of T_i, the centers $Z(T_i)$ satisfy

$$(\rho \otimes \pi_i)(Z(T_i)) \subset Z(T_i), \quad \text{for } i = 1, 2.$$

As a consequence, and by using the fact that the projectors are G_k-equivariant, G_k permutes the set of vertices $\Sigma = \pi_1^{-1}(Z(T_1)) \cap \pi_2^{-1}(Z(T_2))$. Indeed, as for $v \in \Sigma$ and $\sigma \in G_k$, we have $\pi_i(v) \in Z(T_i)$ so $(\rho \otimes \pi_i)(\sigma)(\pi_i(v)) = \pi_i(v^\sigma) \in Z(T_i)$ which yields to $v^\sigma \in \Sigma$. Moreover, the Galois action on the centers determines the Galois action on Σ, each automorphism $\sigma_{|\Sigma}$ being of order 1 or 2. □

Proposition 8 admits an obvious generalization for any finite product of symmetric polynomials. As a particular case, we reobtain Elkies' result on the field of definition for k-elliptic curves without complex multiplication [3]. A k-elliptic curve E is an elliptic curve defined over $\bar{k}$ which is isogenous to all its Galois conjugates. By taking $\Phi_i(x, y)$ as the classical modular polynomials $\Phi_p(x, y)$, one describes the graph of prime p-powers isogenies between elliptic curves. Let j be the modular invariant of E. In the absence of complex multiplication (CM), $G(\Phi_p, j)$ is a tree. Then, in order to define the corresponding projectors, one uses the properties of factorization of isogenies between non-CM elliptic curves. The conclusion is that each k-elliptic curve without CM is $\bar{k}$-isogenous to a k-elliptic curve defined over a compositum of quadratic fields.

References

1. G. Chartrand and L. Lesniak, *Graphs and Digraphs*, 3rd edition, Chapman & Hall, London, 1996.
2. P.M. Cohn, *Algebra*, Vol.1/2, John Wiley & Sons, Chichester, 1989.
3. N.D. Elkies, "A Remark on Elliptic K-Curves," 1993, Preprint.
4. F. Harary, *Graph Theory*, Addison-Wesley, Reading, MA, 1972.
5. J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer–Verlag, New York, 1986.
6. J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer–Verlag, New York, 1994.