# Galois Graphs: Walks, Trees and Automorphisms 

JOSEP M. BRUNAT<br>brunat@ma2.upc.es<br>JOAN-C. LARIO lario@ma2.upc.es<br>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 $\Phi$. Symmetry is also considered, relating the Galois group $\operatorname{Gal}(\bar{k} / k)$ 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: $\left(j_{1}, j_{2}\right)$ is an arc with multiplicity $n$ if $\Phi\left(j_{1}, y\right)$ 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 $\Phi\left(j_{1}, y\right)$ is the zero polynomial.
We will refer to $G(\Phi)$ as the Galois graph of $\Phi$. 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 $\Phi$. In Section 3 we will discuss walks, distances and cycles, providing detection and counting results from

[^0]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 $\operatorname{Gal}(\bar{k} / k)$ 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 $\operatorname{Gal}(\bar{k} / k)$ 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 $v$ 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 $v$, 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 $\infty$ which means that $j$ is a root of the polynomial

$$
F(x)=\operatorname{gcd}\left(f_{0}(x), \ldots, f_{v}(x)\right)
$$

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

$$
G(\Phi)=G\left(\Phi_{0}\right) \oplus G\left(\Phi_{1}\right)
$$

where $G\left(\Phi_{0}\right)$ and $G\left(\Phi_{1}\right)$ are arc-disjoint and $G\left(\Phi_{1}\right)$ is locally finite (i.e., each vertex has finite valency). The arcs of $G\left(\Phi_{0}\right)$ are all the pairs $\left(j_{1}, j_{2}\right),\left(j_{2}, j_{1}\right)$ with $F\left(j_{1}\right)=0$ and $j_{2} \in \bar{k}$. According to the above, the structure of $G(\Phi)$ is completely determined by the structure of $G\left(\Phi_{1}\right)$, so we can (and do) restrict ourselves to studying locally finite Galois graphs.

Now, the degree $v$ of $\Phi(x, y)$ in one of the indeterminates is an upper bound of the outvalencies 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 $\operatorname{gcd}\left(f_{1}(x), \ldots\right.$, $\left.f_{v}(x)\right)$.

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

$$
D(x)=\operatorname{Resultant}\left(\Phi(x, y), \Phi_{y}^{\prime}(x, y), y\right)
$$

where $\Phi_{y}^{\prime}(x, y)$ means the partial derivative of $\Phi(x, y)$ with respect to $y$. The leading coefficients of $\Phi(x, y)$ and $\Phi_{y}^{\prime}(x, y)$ as polynomials in the indeterminate $y$ are $f_{v}(x)$ and $v f_{v}(x)$ respectively, so $f_{v}(x)$ is a factor of $D(x)$. Thus, the vertices with out-valency $<v$ are also roots of $D(x)$. Conversely, if $D(j)=0$, then either $f_{v}(j)=0$ or the polynomials $\Phi(j, y)$ and $\Phi_{y}^{\prime}(j, y)$ have a common root, i.e., either $j$ has out-valency $<v$ 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 $\left(j_{1}, j_{2}\right)$, ( $j_{2}, j_{1}$ ) 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 $f_{v}(x)=1$, so every vertex has out-valency 3. The discriminant is $D(x)=27\left(1-x^{3}\right)$, and the loops are the roots of $L(x)=2 x^{3}-1$. 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 $e_{i}=\left(j_{i-1}, j_{i}\right)$ 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 $\infty$ when there is none, and it is denoted by $d\left(j_{1}, j_{2}\right)$. Since $\Phi$ is assumed to be symmetric, note that $d\left(j_{1}, j_{2}\right)=d\left(j_{2}, j_{1}\right)$.

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

$$
\begin{aligned}
& \psi_{0}^{j}(y)=y-j \\
& \psi_{1}^{j}(y)=\Phi(j, y) \\
& \psi_{n}^{j}(y)=\operatorname{Resultant}\left(\psi_{n-1}^{j}(t), \Phi(t, y), t\right), \quad \text { if } n \geq 2
\end{aligned}
$$

Proposition 1 The vertex $j_{2}$ is n-reachable from $j_{1}$ if and only if $\psi_{n}^{j_{1}}\left(j_{2}\right)=0$. 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, $\psi_{n-1}^{j_{1}}(t)=a_{0} \prod_{i=1}^{r}\left(t-t_{i}\right)^{n_{i}}$ for some constant $a_{0} \neq 0$. Now, $\psi_{n}^{j_{1}}(y)$ is $\prod_{i=1}^{r} \Phi\left(t_{i}, y\right)^{n_{i}}$ up to some power of $a_{0}$. Therefore, $\psi_{n}^{j_{1}}\left(j_{2}\right)=0$ 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 $\Phi\left(t_{i}, y\right)$ 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 $\operatorname{rad} f(x)=f(x) / \operatorname{gcd}\left(f(x), f^{\prime}(x)\right)$. 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

$$
\begin{aligned}
& \chi_{0}^{j}(y)=y-j \\
& \chi_{n}^{j}(y)=\operatorname{rad} \psi_{n}^{j}(y) / \operatorname{rad} \prod_{k=0}^{n-1} \operatorname{gcd}\left(\psi_{k}^{j}(y), \psi_{n}^{j}(y)\right), \quad \text { if } n \geq 1
\end{aligned}
$$

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 $\operatorname{gcd}\left(\psi_{k}^{j}(y), \psi_{n}^{j}(y)\right)$ 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

$$
\begin{aligned}
& \bar{\chi}_{0}^{j}(y)=\chi_{0}^{j}(y) \\
& \bar{\chi}_{1}^{j}(y)=\chi_{1}^{j}(y) \\
& \bar{\psi}_{n}^{j}(y)=\operatorname{rad} \operatorname{Resultant}\left(\bar{\chi}_{n-1}^{j}(t), \Phi(y, t), t\right), \quad \text { if } n \geq 1 ; \\
& \bar{\chi}_{n}^{j}(y)=\bar{\psi}_{n}^{j}(y) /\left(\operatorname{gcd}\left(\bar{\psi}_{n-1}^{j}(y), \bar{\chi}_{n-1}^{j}(y)\right) \operatorname{gcd}\left(\bar{\psi}_{n}^{j}(y), \bar{\chi}_{n-2}^{j}(y)\right)\right), \quad \text { if } n \geq 2 .
\end{aligned}
$$

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 $\Phi(x, y)=x^{3}+y^{3}+$ $x y-1$ 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 $\Phi(x, y)=x^{3}+y^{3}+x y-1$.

|  | Type (a) vertices | Type (b) vertices |
| :--- | :---: | :---: |
| $\chi_{0}^{0}(y)=$ | $y$ |  |
| $\chi_{1}^{0}(y)=$ | $\left(y^{2}+y+1\right)$ | $(y-1)$ |
| $\chi_{2}^{0}(y)=$ | $\left(y^{4}-y^{2}+1\right)$ | $\left(y^{2}+1\right)$ |
| $\chi_{3}^{0}(y)=$ | $\left(y^{4}-2 y^{3}+2 y^{2}-4 y+4\right)$ | $\left(y^{2}+2 y+2\right)$ |
| $\chi_{4}^{0}(y)=$ | $\left(y^{8}+3 y^{6}+4 y^{5}+4 y^{4}+6 y^{3}+19 y^{2}-10 y+25\right)$ | $\left(y^{4}-3 y^{2}+2 y+5\right)$ |



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


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

In order to detect non-obvious (i.e. of length $\geq 3$ ) 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

$$
a_{r}(j)=\operatorname{Resultant}\left(\operatorname{Resultant}\left(\chi_{r}^{j}(x), \Phi(x, y), x\right), \chi_{r}^{j}(y), y\right)
$$

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 $\operatorname{Resultant}\left(\chi_{r}^{j}(x), \Phi\left(x, j_{2}\right), x\right)=0$ and $\chi_{r}^{j}\left(j_{2}\right)=0$. The first condition is equivalent to the existence of some $j_{1}$ such that $\chi_{r}^{j}\left(j_{1}\right)=0$ and $\Phi\left(j_{1}, j_{2}\right)=0$. 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

$$
b_{r}(j)=\operatorname{Resultant}\left(\frac{\psi_{r}^{j}(y)}{\operatorname{gcd}\left(\psi_{r}^{j}(y), \chi_{r}^{j}(y)\right)}, \chi_{r}^{j}(y), y\right)
$$

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 $q_{s}(y)=\psi_{s}^{j}(y) / \operatorname{gcd}\left(\psi_{s}^{j}(y), \chi_{s}^{j}(y)\right)$. Suppose first that $b_{r}(j)=$ 0 . Then $q_{r}\left(j_{3}\right)=\chi_{r}^{j}\left(j_{3}\right)=0$ for some $j_{3} \in \bar{k}$. Since $j_{3}$ is also a root of $\operatorname{gcd}\left(\psi_{r}^{j}(y), \chi_{r}^{j}(y)\right)$, it follows that the multiplicity of $j_{3}$ as a root of $\psi_{r}^{j}(y)$ is $\geq 2$. Hence, by Proposition 1 , there are two distinct paths from $j$ to $j_{3}$. Now, condition $b_{r-1}(j) \neq 0$ implies $q_{r-1}\left(j^{\prime}\right) \neq 0$ for all vertices $j^{\prime}$ at distance $r-1$ from $j$, and the multiplicity of each $j^{\prime}$ as a root of $\psi_{r-1}^{j}(y)$ is one. Hence, there is only one path from $j$ to $j^{\prime}$. 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 $\chi_{r}^{j}\left(j_{3}\right)=0$ and the multiplicity of $j_{3}$ as a root of $\psi_{r}^{j}(y)$ is $\geq 2$. Hence, $q_{r}\left(j_{3}\right)=0$ 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

$$
\begin{aligned}
& A_{n}(j)=\prod_{r=0}^{n} a_{r}(j) \\
& B_{n}(j)=\prod_{r=0}^{n} b_{r}(j) .
\end{aligned}
$$

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 $\left(j_{2}, j_{1}\right)$.

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 $d\left(j, j_{3}\right)=r$. 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 $d\left(j, j_{1}\right)=d\left(j, j_{2}\right)=r-1$, 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. $\boldsymbol{k}$-graphs and $\boldsymbol{k}$-trees

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

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

is well-defined and a group homomorphism. In other words, $H$ is a $k$-graph if the automorphisms of $G_{k}=\operatorname{Gal}(\bar{k} / k)$ act as automorphisms of the graph $H$. The automorphisms of $H$ in the image of $\rho$ 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 $\Phi\left(j_{1}, y\right)$, then $j_{2}^{\sigma}$ is a root of $\Phi\left(j_{1}^{\sigma}, y\right)$ with the same multiplicity, so $\sigma$ 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 $\operatorname{Ker} H$, is the graph induced by the set of vertices in $H$ with minimum degree. The degree of the vertices in $\operatorname{Ker} H$ will be denoted by deg $\operatorname{Ker} H$.

Lemma 3 If $H$ is a $k$-graph, then $\operatorname{Ker} H$ is a $k$-graph.
Proof: If $j \in \operatorname{Ker} H$ and $\sigma \in G_{k}$, then $j^{\sigma} \in H$ since $H$ is a $k$-graph, and the degrees of $j^{\sigma}$ and $j$ coincide. Hence, $j^{\sigma} \in \operatorname{Ker} H$. Therefore the Galois automorphisms of $H$ apply the induced subgraph $\operatorname{Ker} H$ on itself and they act on $\operatorname{Ker} H$ 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) $\operatorname{Ker} H(j)$ is a $k$-graph;
(iii) $H(j)$ is a k-graph.

Proof: (i) $\Rightarrow$ (iii) By hypothesis, $j$ and $j^{\sigma}$ are in the same connected component of $H$ for all $\sigma$ in $G_{k}$. Moreover, $\sigma$ applies the connected component of $j$ on the connected component of $j^{\sigma}$. Hence, $H(j)^{\sigma}=H\left(j^{\sigma}\right)=H(j)$ and $H(j)$ is a $k$-graph.
(iii) $\Rightarrow$ (ii) by Lemma 3 .
(ii) $\Rightarrow$ (i) Let $j_{1} \in \operatorname{Ker} H(j)$. Since $\operatorname{Ker} H(j)$ is a $k$-graph, $j_{1}^{G_{k}} \subset \operatorname{Ker} H(j) \subset H(j)=$ $H\left(j_{1}\right)$. By applying $(\mathrm{i}) \Rightarrow($ iii $)$, we have that $H(j)=H\left(j_{1}\right)$ 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 $\sigma \in \operatorname{Gal}(\bar{k} / k)$.

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

## Proof:

(i) The center $Z(T)$ is fixed for all automorphism, so $c^{\sigma}=c$ for $\operatorname{all} \sigma \in \operatorname{Gal}(\bar{k} / k)$. Hence, $c \in k$ and $\operatorname{deg} \operatorname{Ker} T=1$.
(ii) Suppose that $c_{1} \notin k$. For some $\sigma \in \operatorname{Gal}(\bar{k} / k)$, we have $c_{1}^{\sigma} \neq c_{1}$. Now, $Z(T)^{\sigma}=Z(T)$ $\operatorname{implies} c_{1}^{\sigma}=c_{2}$. Analogously, $c_{2}^{\sigma}=c_{1}$ and $c_{2} \notin k$. Hence, the polynomial $p(x)=$ $\left(x-c_{1}\right)\left(x-c_{2}\right) \in k[x]$ 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 $d\left(c_{1}, j\right)$ and $d\left(c_{2}, j\right)$ differ by 1 , say $d\left(c_{2}, j\right)=r$, and $d\left(c_{1}, j\right)=r+1$. We have

$$
r=d\left(c_{2}, j\right)=d\left(c_{1}^{\sigma}, j^{\sigma}\right)=d\left(c_{1}, j\right)=r+1
$$

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

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) $\operatorname{deg} \operatorname{Ker} T \in\{1,2\}$;
(ii) if $\operatorname{deg} \operatorname{Ker} T=2$, then there is a vertex in $\operatorname{Ker} T$ adjacent to its conjugate;
(iii) $k\left(j_{1}\right)=k\left(j_{2}\right)$ for all $j_{1}, j_{2} \in \operatorname{Ker} T$;
(iv) $\operatorname{Ker} T$ is a $k$-tree;

Proof: Take $j \in \operatorname{Ker} T$ 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 $\left(j^{G_{k}}\right)^{\sigma}=j^{G_{k}}$, so $M^{\sigma}=M$ and $M$ is a finite $k$-tree. Therefore, Proposition 5 can be applied to $M$. Since $\operatorname{deg} \operatorname{Ker} T=\operatorname{deg} \operatorname{Ker} M \in\{1,2\}$, it follows (i).

If $\operatorname{deg} \operatorname{Ker} T=2$, 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 $k\left(j_{1}\right)=k(c)=k$ for all $j_{1} \in \operatorname{Ker} T$ and (iii) holds. To show (iv), take $j_{1}, j_{2} \in$ 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 $\sigma$. Hence, $j^{\sigma}=j$ for all $j \in P$. It follows that $j \in \operatorname{Ker} T$ and $\operatorname{Ker} T$ is a subtree of $T$. From Lemma 3 it is also a $k$-graph.
Second, suppose $Z(M)=\left\{c_{1}, c_{2}\right\} \not \subset k$. Observe that, since $c_{1}$ and $c_{2}$ are quadratic conjugate, $k\left(c_{1}\right)=k\left(c_{2}\right)$. Let now $j \in \operatorname{Ker} T$ and fix a Galois automorphism $\sigma \in \operatorname{Gal}(\bar{k} / k)$ as before. Interchanging $c_{1}$ and $c_{2}$ if necessary, we can assume that $d\left(j, c_{1}^{\sigma}\right)=d\left(j, c_{2}\right)=$ $d\left(j, c_{1}\right)+1$. There is a path, say $P$, in $T$ from $j$ to $j^{\sigma}$. If $\tau \in \operatorname{Gal}\left(k\left(c_{1}\right) / k\right)$, the path $P^{\sigma}$ is either $P$ or the reverse of $P$. Then $\tau$ acts on $P$ either as the identity or as $\sigma$, so $k(j)=k\left(c_{1}\right)$. Thus, (iii) is satisfied.

To show (iv), let $j_{1}$ be a vertex of the path, say $P_{1}$, from $j \in \operatorname{Ker} T$ to $c_{1}$ and consider the path $P$ from $j$ to $j^{\sigma}$. It is clear that $P$ contains $P_{1}$. Now, every $\tau \in \operatorname{Gal}(\bar{k} / k)$ acts on $P$ either as the identity or as $\sigma$. Hence $j_{1}$ has exactly one conjugate, $j_{1}^{\sigma}$, which tells us that $j_{1}$ is quadratic over $k$. Moreover, $P_{1}$ is a path in $\operatorname{Ker} T$ and $\operatorname{Ker} T$ is a $k$-tree.

## 5. Automorphisms

For a given $k$-graph $H$, the representation

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

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

In order to determine the image of $\rho$, 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

$$
\text { Ker } T=T_{0} \subset T_{1} \subset \cdots \subset T_{r-1} \subset T_{r}=T
$$

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 $r=\max \{d(j, \operatorname{Ker} T) \mid j \in T\}$. 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 $\operatorname{Ker} T$ is 0 , otherwise the following hypothesis (H) will apply:

H1: all the leaves of $T$ are at distance $r$ from $\operatorname{Ker} T$;
$\mathrm{H} 2: \operatorname{Gal}\left(k\left(T_{s}\right) / k\left(T_{s-1}\right)\right) \simeq\left\{f \in \operatorname{Aut}\left(T_{s}\right): f_{\mid T_{s-1}}=i d\right\}, \quad$ 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 $f \in$ 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 $(\mathrm{H})$, and denote its representation by $\rho: \operatorname{Gal}(\bar{k} / k) \longrightarrow \operatorname{Aut}(T)$. Then, we have:

$$
\operatorname{Im} \rho=\left\{f \in \operatorname{Aut}(T): \text { there is } \sigma \in \operatorname{Gal}(\bar{k} / k) \text { such that } f_{\mid \operatorname{Ker} T}=\rho(\sigma)_{\mid \mathrm{Ker} T}\right\}
$$

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

$$
\begin{aligned}
H_{s} & =\left\{f \in \operatorname{Aut}\left(T_{s}\right): f_{\mid T_{s-1}}=i d\right\} \\
\Gamma_{s} & =\left\{f \in \operatorname{Aut}\left(T_{s}\right): \text { there is } \sigma \in \operatorname{Gal}(\bar{k} / k) \text { such that } f_{\mid \operatorname{Ker} T}=\rho(\sigma)_{\mid \operatorname{Ker} T}\right\}
\end{aligned}
$$

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

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

$$
H_{r} \simeq \operatorname{Gal}\left(k\left(T_{r}\right) / k\left(T_{r-1}\right)\right) \subset \operatorname{Gal}\left(k\left(T_{r}\right) / k\right) \simeq \operatorname{Im} \rho_{r}
$$

we can write the equality

$$
\left[\Gamma_{r}: \operatorname{Im} \rho\right]=\frac{\left[\Gamma_{r}: H_{r}\right]}{\left[\operatorname{Im} \rho: H_{r}\right]} .
$$

Calculating the above denominator, we obtain

$$
\frac{|\operatorname{Im} \rho|}{\left|H_{r}\right|}=\frac{\left|\operatorname{Gal}\left(k\left(T_{r}\right) / k\right)\right|}{\left|\operatorname{Gal}\left(k\left(T_{r}\right) / k\left(T_{r-1}\right)\right)\right|}=\left|\operatorname{Gal}\left(k\left(T_{r-1}\right) / k\right)\right|=\left|\operatorname{Im} \rho_{r-1}\right|=\left|\Gamma_{r-1}\right|,
$$

and

$$
\left[\Gamma_{r}: \operatorname{Im} \rho\right]=\frac{\left[\Gamma_{r}: H_{r}\right]}{\left|\Gamma_{r-1}\right|}
$$

It is easy to check that the map

$$
\Gamma_{r} / H_{r} \longrightarrow \Gamma_{r-1}
$$

defined by sending each coset $f H_{r}$ to the restriction of $f$ to $T_{r-1}$ is well-defined and injective. Thus, we have $\left[\Gamma_{r}: \operatorname{Im} \rho\right]=1$.

Corollary 2 Let $T$ be as above and assume that $\operatorname{Ker} T=Z(T)$. Then, $\rho$ 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 $\operatorname{Ker} T$ as Galois automorphisms. Hence, the above proposition shows that $\Gamma_{r}=\operatorname{Aut}(T)$ and $\rho$ is surjective.

Example 3 Take the modular polynomial

$$
\begin{aligned}
\Phi_{2}(x, y)= & x^{3}+y^{3}-x^{2} y^{2}+2^{4} 3 \cdot 31\left(x^{2} y+x y^{2}\right)-2^{4} 3^{4} 5^{3}\left(x^{2}+y^{2}\right) \\
& +3^{4} 5^{3} 4027 x y+2^{8} 3^{7} 5^{6}(x+y)-2^{12} 3^{9} 5^{9}
\end{aligned}
$$

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 $\left(A_{1}, A_{2}\right),\left(D_{1}, D_{2}\right),\left(F_{1}, F_{2}\right),\left(G_{1}, G_{2}\right)$, and $\left(H_{1}, H_{2}\right)$ are respectively the roots of the polynomials

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

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 $(T) \simeq C_{2}+C_{2}\left[C_{2}\left[C_{2}\right]\right]$ 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 $\rho: \operatorname{Gal}(\bar{k} / k) \longrightarrow \operatorname{Aut}(G)$ the representation $\rho(\sigma)=\sigma_{\mid V}$. A mapping $f$ from $G$ to a graph $H$ is a morphism of graphs if $j_{1} \sim j_{2}$ implies $f\left(j_{1}\right) \sim f\left(j_{2}\right)$ for all $j_{1}, j_{2} \in G$, where $\sim$ means adjacency. A surjective morphism of graphs $f: G \rightarrow H$ will be called $G_{k}$-equivariant if for all $j_{1}, j_{2} \in G$ and $\sigma \in \operatorname{Gal}(\bar{k} / k)$,

$$
\begin{aligned}
& f\left(j_{1}\right)=f\left(j_{2}\right) \Rightarrow f\left(j_{1}^{\sigma}\right)=f\left(j_{2}^{\sigma}\right) \\
& f\left(j_{1}\right) \sim f\left(j_{2}\right) \Rightarrow f\left(j_{1}^{\sigma}\right) \sim f\left(j_{2}^{\sigma}\right) .
\end{aligned}
$$

The morphism $f$ induces an action on $H$ as follows:

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

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 $G\left(\Phi_{1} \Phi_{2}, j\right)$ is a $k$-graph such that:
(i) $G\left(\Phi_{1}, j\right), G\left(\Phi_{2}, j\right)$ are trees,
(ii) there are $G_{k}$-equivariant projectors $\pi_{i}: G\left(\Phi_{1} \Phi_{2}, j\right) \rightarrow G\left(\Phi_{i}, j\right), i=1,2$.

Then $G\left(\Phi_{1} \Phi_{2}, j\right)$ 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 $G\left(\Phi_{1} \Phi_{2}, j\right)$. Note that for each $\sigma$ in $G_{k}=\operatorname{Gal}(\bar{k} / k)$ we can view the connected components $G\left(\Phi_{i}, j^{\sigma}\right)$ as subgraphs of $G\left(\Phi_{1} \Phi_{2}, j\right)$. Consider $\pi_{1}\left(j^{G_{k}}\right) \subset G\left(\Phi_{1}, j\right)$ and let $T_{1}$ denote the minimal subtree of $G\left(\Phi_{1}, j\right)$ that connects the vertices of $\pi_{1}\left(j^{G_{k}}\right)$. Analogously, define $T_{2}$ making use of the projector $\pi_{2}$. Since each $\rho \otimes \pi_{i}$ restricts to an automorphism of $T_{i}$, the centers $Z\left(T_{i}\right)$ satisfy

$$
\left(\rho \otimes \pi_{i}\right)\left(Z\left(T_{i}\right)\right) \subset Z\left(T_{i}\right), \quad \text { for } i=1,2
$$

As a consequence, and by using the fact that the projectors are $G_{k}$-equivariant, $G_{k}$ permutes the set of vertices $\Sigma=\pi_{1}^{-1}\left(Z\left(T_{1}\right)\right) \cap \pi_{2}^{-1}\left(Z\left(T_{2}\right)\right)$. Indeed, as for $v \in \Sigma$ and $\sigma \in G_{k}$, we have $\pi_{i}(v) \in Z\left(T_{i}\right)$ so $\left(\rho \otimes \pi_{i}\right)(\sigma)\left(\pi_{i}(v)\right)=\pi_{i}\left(v^{\sigma}\right) \in Z\left(T_{i}\right)$ which yields to $v^{\sigma} \in$ $\Sigma$. Moreover, the Galois action on the centers determines the Galois action on $\Sigma$, each automorphism $\sigma_{\mid \Sigma}$ 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 $(\mathrm{CM}), G\left(\Phi_{p}, j\right)$ 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

. G. Chartrand and L. Lesniak, Graphs and Digraphs, 3rd edition, Chapman \& Hall, London, 1996.
. P.M. Cohn, Algebra, Vol.1/2, John Wiley \& Sons, Chichester, 1989.
. 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.


[^0]:    Research of the authors was supported in part by the CICYT grant TIC 97-0963 and DGICYT grant PB96-0970-C02-02, respectively.

