ORIGINAL PAPER

Automorphism groups of Cayley evolution algebras

C. Costoya[1] · V. Muñoz[2] · A. Tocino[3] · A. Viruel[2]

Abstract

In this paper we introduce a new species of evolution algebras that we call Cayley evolution algebras. We show that if a field $\Bbbk$ contains sufficiently many elements (for example if $\Bbbk$ is infinite) then every finite group G is isomorphic to $\mathrm{Aut}(X)$ where X is a finite-dimensional absolutely simple Cayley evolution $\Bbbk$-algebra.

Keywords Evolution algebra · Finite group · Automorphism group · Graph

Mathematics Subject Classification 05C25 · 17A36 · 17D99

1 Introduction

The question of whether any finite group may be realised as the full automorphism group of a finite-dimensional simple algebra (over an algebraically closed field $\Bbbk$ of characteristic zero) was raised by Popov in [13]. Years later, in the celebrated paper by Gordeev and Popov [9], a positive answer was given in a more general setting: if $\Bbbk$ is a field containing sufficiently many elements, every linear algebraic $\Bbbk$-group is isomorphic to the full automorphism group of a finite-dimensional simple $\Bbbk$-algebra (which is neither associative nor commutative).

Using techniques from Rational Homotopy Theory, in [6, Proposition 4.2, Corollary 4.11(2)] it was shown that every group G is the full automorphism group of an infinite number of non-isomorphic differential graded $\mathbb{Q}$-algebras M_n, $n \geq 1$ (that are associative and commutative in the graded sense). Moreover, if the group G is finite, then for every

✉ V. Muñoz
vicente.munoz@ucm.es

C. Costoya
cristina.costoya@udc.es

A. Tocino
alicia.tocino@uma.es

A. Viruel
viruel@uma.es

[1] CITIC, CITMAGA, Departamento de Ciencias de la Computación y Tecnologías de la Información, Universidade da Coruña, 15071-A Coruna, Spain

[2] Departamento de Álgebra, Geometría y Topología, Universidad de Málaga, 29071 Malaga, Spain

[3] Departamento de Matemática Aplicada, Universidad de Málaga, 29071 Malaga, Spain

integer $n \geq 1$, M_n is an elliptic algebra, which means that it is finitely generated with finite-dimensional cohomology over $\mathbb{Q}$.

In this paper, we place ourselves in the framework of evolution algebras, which are commutative and non-associative algebras. Recall that a $\Bbbk$-algebra X is called absolutely simple, if for every field extension $\mathbb{F}/\Bbbk$, the $\mathbb{F}$-algebra $X_{\mathbb{F}} = X \otimes_{\Bbbk} \mathbb{F}$ is simple. Then our main result is:

Theorem A *Let G be a finite group and let $\Bbbk$ be a not necessarily finite field with multiplicative group of order $|\Bbbk^*| \geq 2|G|$. Then, there exists an absolutely simple evolution $\Bbbk$-algebra X such that $\mathrm{Aut}(X_{\mathbb{F}}) \cong G$ for every field extension $\mathbb{F}/\Bbbk$.*

The proof of Theorem A is postponed to Sect. 4 and relies on the *good* properties of Cayley evolution algebras, which are new objects introduced in this work (see Definition 3.1). They are constructed out of any finite-dimensional associative $\Bbbk$-algebra $\mathcal{A}$, $\Bbbk$ an arbitrary field. In the special case that $\mathcal{A} = \Bbbk[G]$, a group algebra with G finite group, the associated Cayley evolution algebras will be closely related to classical Cayley graphs.

We end this section by pointing out that our main result is an improvement of our previous result [5, Theorem 1.1] where finite groups were realised by regular, but not simple (see Remark 3.6), evolution algebras (see also [15] for an independent proof in char $\Bbbk = 0$).

2 Background on evolution algebras

We present here the definitions on evolution algebras that are needed in the following sections. We mainly follow the notation in [3], although the reader is encouraged to also check [16], a classical reference on the subject. Other properties of evolution algebras appear in [1, 2, 12].

Let $\Bbbk$ be a field. An automorphism of $\Bbbk$-algebra is a linear isomorphism which commutes with the multiplication of the algebra. In this work we consider only finite-dimensional algebras. We now recall the definition of an evolution algebra [16, Definition 1], [3, Definitions 1.2.1]:

Definition 2.1 Let X be a $\Bbbk$-algebra. We say that X is an *evolution $\Bbbk$-algebra* if X admits a basis $B = \{b_i \mid i \in \Lambda\}$ such that $b_i b_j = 0$ for $i \neq j$. Such a basis B is called a *natural basis*.

Observe that given an evolution $\Bbbk$-algebra X, it may admit more than one natural basis (see for example [3, Example 1.6.3]). On the other hand, for a given $\Bbbk$-vector space X spanned by a basis $B = \{b_i \mid i \in \Lambda\}$, an evolution $\Bbbk$-algebra with natural basis B is completely determined by just giving $b_i^2 := b_i b_i \in X$ as a linear combination of elements in B, for every $i \in \Lambda$, and declaring $b_i b_j = 0$ for $i \neq j$. This motivates the following definition [3, Definition 1.2.1]:

Definition 2.2 Let X be an evolution algebra with a fixed natural basis B. The scalars $\omega_{ki} \in \Bbbk$ such that $b_i^2 := b_i b_i = \sum_{k \in \Lambda} \omega_{ki} b_k$ are called the *structure constants* of X relative to B, and the matrix $M_B(X) := (\omega_{ki})$ is said to be the *structure matrix* of X relative to B.

Definition 2.3 An evolution $\Bbbk$-algebra X is called *regular* (or perfect, or idempotent) if $X = X^2$. An evolution algebra X is called *simple* if $X^2 \neq 0$ and 0 is the only proper ideal.

Notice that an evolution algebra X is regular if and only if for any natural basis B, the structure matrix $M_B(X)$ is a regular (or invertible) matrix. It is also clear that if X simple then X is regular, but the converse is not always true (see Proposition 3.5).

Every evolution algebra has a directed graph and a weighted (or coloured) graph attached depending on the chosen natural basis [16, Definition 15], [7, Definition 2.2]:

Definition 2.4 Let X be an evolution $\Bbbk$-algebra, and $B = \{b_1, \ldots, b_n\}$ its natural basis. The directed graph $\Gamma(X, B) = (V, E)$ with set of vertices $V = \{1, \ldots, n\}$ and set of edges $E = \{(i, j) \in V \times V : \omega_{ij} \neq 0\}$ is called the directed graph attached to the evolution algebra X relative to B. The directed graph $\Gamma^w(X, B) = (V, E, w)$ with $\Gamma(X, B) = (V, E)$ and weight function $w \colon E \to \Bbbk$, given by $w(i, j) = \omega_{ij}$, is called the weighted graph attached to the evolution algebra X relative to B.

3 The Cayley evolution algebra of a $\Bbbk$-algebra

We now explain how, to a given associative $\Bbbk$-algebra $\mathcal{A}$, we can associate an evolution $\Bbbk$-algebra that takes into account the inner product of $\mathcal{A}$:

Definition 3.1 Let $\mathcal{A}$ be a finite-dimensional associative $\Bbbk$-algebra with basis $B = \{b_i : i \in \Lambda\}$ together with a function $f : B \to \Bbbk$ (a set-theoretical map). We define the *Cayley evolution $\Bbbk$-algebra associated to f*, that we denote by $\mathrm{Cay}(f)$, as the evolution $\Bbbk$-algebra with $\mathrm{Cay}(f) \cong \mathcal{A}$, as a $\Bbbk$-vector space, furnished with natural basis B and structure constants given by $b_i \cdot b_i = \sum_{b_j \in B} f(b_j) b_i b_j$, where $x \cdot y$ denotes the product in $\mathrm{Cay}(f)$ and xy the inner product in $\mathcal{A}$.

Remark 3.2 Observe that fixing a function $f : B \to \Bbbk$ is equivalent to choosing a vector $w = \sum f(b_i) b_i$. Therefore, the Cayley evolution algebra associated to f could also be defined as the Cayley evolution algebra associated to a vector $w \in \mathcal{A}$ with $\mathrm{Cay}(w) \cong \mathcal{A}$, as $\Bbbk$-vector space, furnished with natural basis B and structure constants given by $b_i \cdot b_i = \sum_{b_j \in B} w^*(b_j) b_i b_j$, where w^* is the dual of w.

Remark 3.3 Given a finite-dimensional associative $\Bbbk$-algebra $\mathcal{A}$ with basis B, the isomorphism type of the evolution $\Bbbk$-algebra $\mathrm{Cay}(f)$ strongly depends on the choice of $f : B \to \Bbbk$. For example, if $\mathcal{A}$ is a non-degenerate evolution algebra with natural basis B, then the constant map given by $f_0(b_i) = 0$ converts $\mathrm{Cay}(f_0)$ into a degenerated evolution algebra, whereas the constant map given by $f_1(b_i) = 1$ transforms $\mathrm{Cay}(f_1) \cong \mathcal{A}$. A more elaborated example is constructed in Example 4.9 to illustrate how the isomorphism type of the Cayley evolution algebra depends on the choice of the basis.

From now on, let us fix a unital finite-dimensional associative $\Bbbk$-algebra $\mathcal{A}$, with basis B, and a function $f : B \to \Bbbk$. We now prove several properties of the Cayley evolution $\Bbbk$-algebra associated to f, $\mathrm{Cay}(f)$. First we show how units in $\mathcal{A}$ give rise to automorphisms of $\mathrm{Cay}(f)$.

Proposition 3.4 *If $x \in \mathcal{A}$ is a unit such that $xB = B$ then the left-multiplication by x induces $\psi_x \in \mathrm{Aut}\big(\mathrm{Cay}(f)\big)$. If moreover B consists of units in $\mathcal{A}$, then ψ_x acts freely on B for $x \neq 1$.*

Proof Given a unit $x \in \mathcal{A}$, we construct the map $\psi_x : \mathrm{Cay}(f) \to \mathrm{Cay}(f)$ given by $\psi_x(a) = xa$. Observe that ψ_x maps the natural basis B to itself since $\psi_x(B) = xB = B$. Hence it is an automorphism of $\mathrm{Cay}(f)$ as $\Bbbk$–vector space. Now, to check that ψ_x is an automorphism of evolution algebras, on the one hand we have that $\psi_x(b_i \cdot b_i) = \psi_x(\sum_{b_j \in B} f(b_j) b_i b_j) = \sum_{b_j \in B} f(b_j) x(b_i b_j) = \sum_{b_j \in B} f(b_j)(x b_i) b_j = \sum_{b_j \in B} f(b_j) \psi_x(b_i) b_j = \psi_x(b_i) \cdot \psi_x(b_i)$.

On the other hand, for $b_i \neq b_j$, we have that $\psi_x(b_i \cdot b_j) = \psi_x(0) = x0 = 0$ and we are going to prove that $\psi_x(b_i) \cdot \psi_x(b_j)$ is also zero. Suppose that it is not, hence $\psi_x(b_i) \cdot \psi_x(b_j) = xb_i \cdot xb_j \neq 0$, and since xb_i and xb_j are elements in the natural basis B, they must be equal. But x is a unit in $\mathcal{A}$, which leads to the contradiction $b_i = b_j$.

Now, suppose that B consists of units in $\mathcal{A}$. If ψ_x fixes an element $b \in B$, then $\psi_x(b) = xb = b$, so we obtain that $x = 1$ since b is a unit. □

Let us define $\mathrm{supp}(f : B \to \Bbbk) := \{b \in B : f(b) \neq 0\}$.

Proposition 3.5 *Suppose that B consists of units in $\mathcal{A}$, and that $\mathrm{supp}(f)$ generates $\mathcal{A}$ as an algebra. If the Cayley evolution $\Bbbk$-algebra associated to f, $\mathrm{Cay}(f)$, is regular, then $\mathrm{Cay}(f)$ is also simple.*

Proof Suppose that $\mathrm{Cay}(f)$ is regular but not simple. Then, according to [4, Corollary 4.6], the elements in B can be reordered, namely $B = \{b_1, b_2, \ldots, b_r, \ldots, b_n\}$, $1 \leq r < n$, such that the structure matrix of $\mathrm{Cay}(f)$ becomes

$$M_B(\mathrm{Cay}(f)) = \left(\begin{array}{ccc|ccc} * & \cdots & * & * & \cdots & * \\ \vdots & r \times r & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \\ \hline & & & * & \cdots & * \\ & \mathbf{0} & & \vdots & \ddots & \vdots \\ & & & * & \cdots & * \end{array} \right).$$

Let $S = \mathrm{supp}(f)$ and consider an element $b \in B \setminus \{b_1, \ldots, b_r\}$. Since S generates $\mathcal{A}$ as algebra, and B consists of units in $\mathcal{A}$, the product $b_1^{-1}b = \sum_k \lambda_k \prod_{i=1}^{l_k} s_{i,k}$, where $\lambda_k \in \Bbbk$ and $s_{i,k} \in S$. Then, $b = b_1 b_1^{-1} b = b_1 \left(\sum_k \lambda_k \prod_{i=1}^{l_k} s_{i,k} \right) = \sum_k \lambda_k b_1 \left(\prod_{i=1}^{l_k} s_{i,k} \right)$.

We claim that $b_1 \left(\prod_{i=1}^{l_k} s_{i,k} \right) \in Span(\{b_1, \ldots, b_r\})$. Indeed, for $j \in \{1, \ldots, r\}$,

$$b_j \cdot b_j = \sum_{b_k \in B} f(b_k) b_j b_k = \sum_{s \in S} f(s) b_j s,$$

thus, by the shape of $M_B(\mathrm{Cay}(f))$, we conclude that $b_j s \in Span(\{b_1, \ldots, b_r\})$ for all $j \in \{1, \ldots, r\}$ and for all $s \in S$. Even more, given $\prod_{i=1}^{l_k} s_{i,k}$, for $s_{i,k} \in S$, an inductive argument shows that $b_j \left(\prod_{i=1}^{l_k} s_{i,k} \right) \in Span(\{b_1, \ldots, b_r\})$ for all $j \in \{1, \ldots, r\}$. In particular, we obtain that $b \in Span(\{b_1, \ldots, b_r\})$. This leads to a contradiction as B is a linearly independent set, hence $\mathrm{Cay}(f)$ is simple. □

Remark 3.6 As we mentioned in Introduction, the evolution algebras obtained in [6] are regular but not simple. Recall that associated to a simple graph $\mathcal{G} = (V, E)$, we construct an evolution algebra $\mathcal{X}(G)$ over any field $\Bbbk$ with natural basis $B = \{b_v, v \in V\} \cup \{b_e, e \in E\}$ (see [6, Definition 3.2]). In particular, the multiplication for the elements associated to the vertices of the graph is given by $b_v^2 = b_v$, for all $v \in V$. Hence, for I_r the identity matrix of order $r = |V|$, and I_s the identity matrix of order $s = |E|$, the structure matrix of $\mathcal{X}(G)$

becomes

$$
M_B(\mathcal{X}(G)) =
\left(
\begin{array}{c|ccc}
 & * & \cdots & * \\
I_r & \vdots & \ddots & \vdots \\
 & * & \cdots & * \\
\hline
0 & & I_s &
\end{array}
\right)
$$

which by [4, Corollary 4.6], implies that $\mathcal{X}(G)$ is not simple for $r, s > 0$.

4 Cayley evolution algebras of group algebras

In this section we refine the results in Sect. 3. We fix a finite group G and we consider the group algebra over $\Bbbk$, $\mathcal{A} = \Bbbk[G]$. Now, we take as a basis $B = G$ and a function $f : G \to \Bbbk$. In this setting, observe that the structure constants of $\mathrm{Cay}(f)$ with respect to G can be given by $g \cdot g = \sum_{k \in G} f(g^{-1}k)k$.

Our first result is a straightforward consequence of Proposition 3.4.

Proposition 4.1 *G acts faithfully on $\mathrm{Cay}(f)$ as a permutation group over its natural basis by left-multiplication. That is, $G \leq \mathrm{Aut}(\mathrm{Cay}(f))$.*

Proof The elements of G are units in $\mathcal{A} = \Bbbk[G]$ and since $G^2 = G$, then $GB = B$. Hence by Proposition 3.4, $\psi_g \in \mathrm{Aut}\big(\mathrm{Cay}(f)\big)$. Moreover, for any $g, h \in G$, $\psi_g \circ \psi_h = \psi_{gh}$, thus the units $G \subset \mathcal{A}$ produce a subgroup of automorphisms which is isomorphic to G. □

We now recall the definition of Cayley graph [17, Definition 4-5].

Definition 4.2 Let G be a finite group, and S be a subset of G. The *Cayley graph* of G with respect to S is the directed graph $\mathrm{Cay}(G, S)$ with vertex set G and edges (g, gs) for each $g \in G$ and $s \in S$. Moreover, we can assign a colour c_s to each edge (g, gs), $s \in S$, where $c_s \neq c_{s'}$ if $s \neq s'$. Hence, we obtain an *edge-coloured directed graph*, the coloured Cayley graph. In this work we will denote it by $\mathrm{Cay}^{cor}(G, S)$.

The Cayley evolution algebras that we have previously introduced are closely related to Cayley graphs. By comparing Definitions 2.4 and 4.2 we immediately obtain:

Lemma 4.3 *Let $S = \mathrm{supp}(f)$, and assume $f|_S$ is injective. Then $\Gamma\big(\mathrm{Cay}(f), G\big) = \mathrm{Cay}(G, S)$ as abstract directed graphs while $\Gamma^w\big(\mathrm{Cay}(f), G\big) = \mathrm{Cay}^{cor}(G, S)$ as edge-coloured directed graphs.*

One of the key features of the coloured Cayley graph $\mathrm{Cay}^{cor}(G, S)$ is that whenever S generates G, the group G can be represented as the full group of automorphisms of $\mathrm{Cay}^{cor}(G, S)$, that is $G \cong \mathrm{Aut}(\mathrm{Cay}^{cor}(G, S))$ [17, Theorem 4-8]. In a similar way we prove:

Proposition 4.4 *Suppose that the evolution $\Bbbk$-algebra $\mathrm{Cay}(f)$ is regular, $S = \mathrm{supp}(f)$ generates G and $f|_S$ injective. If S contains two elements of coprime order, then $G \cong \mathrm{Aut}(\mathrm{Cay}(f))$.*

Proof First of all, we make use of the identification $\Gamma\big(\mathrm{Cay}(f), S\big) = \mathrm{Cay}(G, S)$ as abstract directed graphs, according to Lemma 4.3. Now, since $\mathrm{Cay}(f)$ is regular, by [8, Theorem 3.2], there exists an exact sequence

$$1 \hookrightarrow \mathrm{Diag}(\mathrm{Cay}(G, S)) \to \mathrm{Aut}(\mathrm{Cay}(f)) \to \mathrm{Aut}(\mathrm{Cay}(G, S)),$$

with $\mathrm{Diag}(\mathrm{Cay}(G, S)) = \mu_N = \{k \in \mathbb{K}; k^N = 1\}$ for $N = 2^{\mathrm{b}(\mathrm{Cay}(G,S))} - 1$ where $\mathrm{b}(\mathrm{Cay}(G, S))$ is the balance of $\mathrm{Cay}(G, S)$ (see [8, Section 2] and [8, Theorem 2.7]).

We first calculate $\mathrm{Diag}(\mathrm{Cay}(G, S))$. Notice that for every $s \in S$, the graph $\mathrm{Cay}(G, S)$ has a directed cycle of length the order of the element s, $o(s)$. Therefore, if $s_1, s_2 \in S$ are elements such that $\gcd(o(s_1), o(s_2)) = 1$, we obtain

$$1 \leq \mathrm{b}(\mathrm{Cay}(G, S)) = \gcd\{|\mathrm{b}(\gamma)| : \gamma \text{ cycle in } \mathrm{Cay}(G, S)\} \leq \gcd(o(s_1), o(s_2)) = 1.$$

Hence $N = 2^{\mathrm{b}(\mathrm{Cay}(G,S))-1} = 1$, and $\mathrm{Diag}(\mathrm{Cay}(G, S)) = \mu_1 = \{1\}$ so,

$$\mathrm{Aut}(\mathrm{Cay}(f)) \leq \mathrm{Aut}(\mathrm{Cay}(G, S)).$$

Therefore, elements in $\mathrm{Aut}(\mathrm{Cay}(f))$ can be thought as those graph automorphisms of $\mathrm{Cay}(G, S)$ that preserve the structure matrix $M_G(\mathrm{Cay}(f))$ in the following sense. Let $\psi \in \mathrm{Aut}(\mathrm{Cay}(f))$ and $g \in G$ an arbitrary element. As ψ preserves the product in $\mathrm{Cay}(f)$, for $g \cdot g = \sum_{k \in G} f(g^{-1}k)k$, we have that

$$\psi(g \cdot g) = \sum_{k \in G} f(g^{-1}k)\psi(k) \tag{1}$$

must coincide with $\psi(g) \cdot \psi(g) = \sum_{k \in G} f(\psi(g)^{-1}k)k$. Since ψ can be thought as a graph automorphism of $\mathrm{Cay}(G, S)$, ψ is in particular a permutation of the elements in G, which allows us to express

$$\psi(g) \cdot \psi(g) = \sum_{k \in G} f(\psi(g)^{-1}\psi(k))\psi(k). \tag{2}$$

Comparing both (1) and (2) we deduce that $f(g^{-1}k) = f(\psi(g)^{-1}\psi(k))$ for arbitrary $g, k \in G$. In other words, ψ is an automorphism of the weighted graph $\Gamma^w\big(\mathrm{Cay}(f), G\big)$ which, by Lemma 4.3 coincides with $\mathrm{Cay}^{cor}(G, S)$. That is,

$$\mathrm{Aut}(\mathrm{Cay}(f)) \leq \mathrm{Aut}(\mathrm{Cay}^{cor}(G, S)) \cong G.$$

Since $G \leq \mathrm{Aut}(\mathrm{Cay}(f))$ by Proposition 4.1, we conclude that $G \cong \mathrm{Aut}(\mathrm{Cay}(f))$. $\square$

We prove now that if the field $\mathbb{K}$ is large enough compared with $|G|$ (for instance, if $\mathbb{K}$ is infinite), it is then possible to construct $\mathrm{Cay}(f)$, a Cayley evolution $\mathbb{K}$-algebra associated to the function $f : G \to \mathbb{K}$, fulfilling hypotheses from Lemma 4.3 and Proposition 4.4.

The following lemma makes the condition "large enough compared with an integer" precise. Recall that a polynomial $P \in \mathbb{K}[X_1, \ldots, X_m]$ is said to be homogeneous of degree $n \in \mathbb{N}$, denoted by $\deg(P) = n$, if P is a linear combination of monomials $X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}$ such that $\sum d_i = n$.

Lemma 4.5 *Let $\mathbb{K}$ be a not necessarily finite field with multiplicative group of order $|\mathbb{K}^*|$, and let n and m be positive integers such that $|\mathbb{K}^*| \geq 2n$ and $n \geq m$. Then, for any homogeneous polynomial of degree n in m variables*

$$P = \sum_{i=1}^{m} \lambda_i X_i^n + Q \in \mathbb{K}[X_1, \ldots, X_m],$$

with $\lambda_i \neq 0$ for all i, and where every monomial in Q involves at least two different variables, there exists a choice of non-zero pairwise distinct values $k_1, \ldots, k_m \in \Bbbk^*$ such that $P(X_i = k_i : i = 1, \ldots, m) \neq 0$.

Proof Fix $n \geq m$ and $P \in \Bbbk[X_1, \ldots, X_m]$ as in the hypotheses. Since $|\Bbbk^*| \geq m$, we can choose $k_1, \ldots, k_{m-1} \in \Bbbk^*$ pairwise distinct values. Hence, the polynomial $\widetilde{P}(X_m) := P(X_i = k_i : i < m)$ is a non-trivial polynomial of degree n, and therefore the equation $\widetilde{P}(X_m) = 0$ admits a most n different non-zero solutions. That is, there exist at most $\kappa_1, \ldots, \kappa_n \in \Bbbk^*$ such that $\widetilde{P}(X_m = \kappa_r) = 0$, for $r = 1, \ldots, n$. Since $|\Bbbk^*| \geq 2n > m - 1 + n$, there exists a non-zero value $k_m \in \Bbbk^*$ such that $k_m \neq k_j$ for $j = 1, \ldots, m - 1$ and $k_m \neq \kappa_r$ for $r = 1, \ldots, n$. Then, $k_1, \ldots, k_m \in \Bbbk^*$ are non-zero pairwise distinct values and $P(X_i = k_i : i = 1, \ldots, m) \neq 0$.   □

Theorem 4.6 *Let $\Bbbk$ be a not necessarily finite field with multiplicative group of order $|\Bbbk^*|$ and let G be a finite group. If $|\Bbbk^*| \geq 2|G|$, then for any non-empty $S \subset G$ there exists a function $f : G \to \Bbbk$ such that:*

(1) $S = \mathrm{supp}(f)$
(2) $f|_S$ *is injective*
(3) $\mathrm{Cay}(f)$ *is regular.*

Proof For any function $f : G \to \Bbbk$, if we denote by X_g the variable such that $X_g = f(g)$, the structure coefficients of $\mathrm{Cay}(f)$ can be described by

$$g \cdot g = \sum_{h \in G} f(h) gh = \sum_{k \in G} f(g^{-1}k) k = \sum_{k \in G} X_{g^{-1}k} k,$$

and therefore, the structure matrix of $\mathrm{Cay}(f)$ becomes

$$M_B(\mathrm{Cay}(f)) = (X_{g^{-1}k})_{g,k \in G} \in M_{|G| \times |G|}(\Bbbk),$$

whose determinant is a homogeneous polynomial $P(X_g : g \in G)$ of degree $|G|$, that we now describe. Given $k \in G$, let $P_k := P(X_g = 0 : g \neq k) \in \Bbbk[X_k]$, thus $P = \sum_{k \in G} P_k + Q$ where Q is a homogeneous polynomial in $\Bbbk[X_g : g \in G]$ such that every monomial in Q involves at least two different variables. Since P is homogeneous, $P_k(X_k) = \lambda_k X_k^{|G|}$ for some $\lambda_k \in \Bbbk$. Following the notation of [10], we can think of the polynomials P_k as

$$P_k(X_k) = \det \left(A\big(\mathrm{Cay}(G, \{k\}), X_k\big) \right)$$

where $A\big(\mathrm{Cay}(G, \{k\}), X_k\big)$ denotes the variable adjacency matrix of the Cayley graph $\mathrm{Cay}(G, \{k\})$. And, according to [10, Theorem 2], as $\mathrm{Cay}(G, \{k\})$ is a directed graph consisting of a total of $\frac{|G|}{o(k)}$ disjoint directed cycles of length $o(k)$, which are also the strong components of $\mathrm{Cay}(G, \{k\})$, we obtain that

$$P_k(X_k) = \left(\det \big(A\big(o(k)\text{-cycle}, X_k\big) \big) \right)^{\frac{|G|}{o(k)}}.$$

Since the variable adjacency matrix of a directed $o(k)$-cycle is of the form

$$\begin{pmatrix} 0 & X_k & 0 & \ldots & 0 \\ 0 & 0 & X_k & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & X_k \\ X_k & 0 & 0 & \ldots & 0 \end{pmatrix} \in M_{o(k) \times o(k)}(\Bbbk)$$

we conclude that

$$P_k(X_k) = \left((-1)^{o(k)+1} X_k^{o(k)}\right)^{\frac{|G|}{o(k)}} = (-1)^{\frac{(o(k)+1)|G|}{o(k)}} X_k^{|G|}.$$

We proceed now to construct, for a given $S \subset G$, the desired function $f : G \to \Bbbk$. Let $P_S := P(X_g = 0 : g \notin S) \in \Bbbk[X_s : s \in S]$ which is a non-trivial homogeneous polynomial of degree $|G|$ on $|S|$ variables. As $|\Bbbk^*| \geq 2n$, Lemma 4.5 ensures the existence of non-zero pairwise distinct values $k_s \in \Bbbk^*$, $s \in S$, satisfying that $P_S(X_s = k_s : s \in S) \neq 0$. With that in mind, let $f : G \to \Bbbk$ be defined by

$$f(g) = \begin{cases} k_g, & \text{if } g \in S \\ 0, & \text{otherwise} \end{cases}$$

Notice that since all the values $k_s \in \Bbbk^*$, for $s \in S$, are non-zero and pairwise distinct, $S = \text{supp}(f)$ and $f|_S$ is injective. Finally,

$$\begin{aligned} \det\left(M_B(\text{Cay}(f))\right) &= P(X_g = f(g) : g \in G) \\ &= P_S(X_s = k_s : s \in S) \\ &\neq 0 \end{aligned}$$

hence $\text{Cay}(f)$ is regular.   □

Combining the results previously obtained, we give the proof of our main result.

Proof of Theorem A Let S be a set of generators of G containing coprime order elements. Observe that S is also a set of generators of $\Bbbk[G]$ as an algebra, and such S always exists, it suffices to consider a generating set S containing $1 \in S$, for example $S = G$. Considering the function $f : G \to \Bbbk$ given in Theorem 4.6, $\text{Cay}(f)$ is regular, $S = \text{supp}(f)$ and $f|_S$ is injective. Moreover, S contains coprime order elements, so by Proposition 4.4 we conclude that $\text{Aut}(\text{Cay}(f)) \cong G$. Moreover, since S generates $\Bbbk[G]$ and $\text{Cay}(f)$ is regular, by Proposition 3.5 we obtain that $\text{Cay}(f)$ is simple.

We now check that the simple evolution $\Bbbk$-algebra $X = \text{Cay}(f)$ above is indeed absolutely simple, and $\text{Aut}(X_{\mathbb{F}}) \cong G$ for every field extension $\mathbb{F}/\Bbbk$. In fact, since the function $f_{\mathbb{F}} : G \to \mathbb{F}$ induced by f also satisfies conclusions (1), (2), and (3) in Theorem 4.6, $\text{Aut}(\text{Cay}(f_{\mathbb{F}})) \cong G$, and $\text{Cay}(f_{\mathbb{F}})$ is simple. Finally, since $\mathbb{F}[G] = \Bbbk[G] \otimes_{\Bbbk} \mathbb{F}$ then $\text{Cay}(f_{\mathbb{F}}) = \text{Cay}(f) \otimes_{\Bbbk} \mathbb{F} = X_{\mathbb{F}}$, thus $X_{\mathbb{F}}$ is simple and $\text{Aut}(X_{\mathbb{F}}) \cong G$.

□

We end this paper with some remarks on the non-uniqueness of the simple evolution algebras realizing finite groups.

Remark 4.7 Our construction of the simple evolution $\Bbbk$-algebra $\text{Cay}(f)$ such that $\text{Aut}(\text{Cay}(f)) \cong G$, for a fixed finite group G involves several choices: first, a generator set $S \subset G$ containing coprime order elements, which is not unique if $|G| > 1$. Secondly, a function $f : G \to \Bbbk$ such that $\text{Cay}(f)$ is regular, as in the proof of Theorem 4.6, which is not is unique either since any non-zero scalar multiple of $f : G \to \Bbbk$ will also work. An easy argument on the edge-coloured directed graphs $\Gamma^w\left(\text{Cay}(f), B\right) = \text{Cay}^{cor}(G, S)$ illustrates that both choices lead to non-isomorphic evolution $\Bbbk$-algebras with the same group of automorphism G.

Remark 4.8 For any evolution algebra Cay(f) built upon the group algebra $\mathcal{A} = \Bbbk[G]$ with fixed natural basis $B = G$, and any given $f : B \to \Bbbk$, the following holds

$$G \leq \mathrm{Aut}(\mathrm{Cay}(f)) \leq \mathrm{GL}(\Bbbk, |G|)$$

since $B = G$ is a group of units basis in $\mathcal{A} = \Bbbk[G]$ (see Proposition 4.1). The lower bound $G = \mathrm{Aut}(\mathrm{Cay}(f))$ is obtained when f is as in the proof of Theorem A (see also Theorem 4.6) while the upper bound $\mathrm{Aut}(\mathrm{Cay}(f)) = \mathrm{GL}(\Bbbk, |G|)$ is obtained when $f = 0$. Although it is not the purpose of this paper, we could raise the question of which intermediate groups H,

$$G \leq H \leq \mathrm{GL}(\Bbbk, |G|),$$

can be realized as automorphisms of simple Cayley evolution algebras. That is, $\mathrm{Aut}(\mathrm{Cay}(f)) = H$ for some function $f : G \to \Bbbk$.

We now highlight that not only $\mathrm{Aut}(\mathrm{Cay}(f))$ depends on how *good* or *bad* the function $f : G \to \Bbbk$ is, as Remark 4.8 illustrates, but it also depends on the group of units of $\mathcal{A} = \Bbbk[G]$. And in fact, since the isomorphism problem for group rings [14, Problem 1.1] has a negative answer in general [11], the group of units basis is not unique in a group algebra. The following example shows that the choice of the group of units basis as natural basis for Cay(f) might lead to non-isomorphic Cayley evolution algebras with non-isomorphic group of automorphisms:

Example 4.9 Let G_1 and G_2 be the finite groups of order $n = 2^{21}97^{28}$ denoted by respectively X and Y in [11, Theorem B]. Let $\Bbbk$ be a field (not necessarily finite) with multiplicative group of order $|\Bbbk^*| \geq 2 \cdot 2^{21}97^{28}$ and let $\mathcal{A} = \Bbbk[G_1]$ be the group $\Bbbk$-algebra. By [11, Theorem B], although G_1 and G_2 are non-isomorphic, they can both be the group of units basis of $\mathcal{A}$. Hence, following the proof of Theorem A, there exist functions $f_1 : G_1 \to \Bbbk$, and $f_2 : G_2 \to \Bbbk$, such that Cay(f_1) and Cay(f_2) are simple evolution $\Bbbk$-algebras with $\mathrm{Aut}(\mathrm{Cay}(f_1)) \cong G_1 \not\cong G_2 \cong \mathrm{Aut}(\mathrm{Cay}(f_2))$, and so Cay($f_1$) $\not\cong$ Cay(f_2).

Finally, it is also natural to ask whether the function $f : G \to \Bbbk$ defining Cay(f) can be chosen to be a significant one, for example a character, or more generally, a class function, that is $f(g^{-1}kg) = f(k)$ for all $g, k \in G$. We prove the following:

Proposition 4.10 *Let G be a finite group, $\mathcal{A} = \Bbbk[G]$, and $f : G \to \Bbbk$ be a class function. Then $\mathrm{Aut}(\mathrm{Cay}(f))$ contains two subgroups K_i, $i = 1, 2$, such that $K_1 \cong G$, $K_2 \cong G/Z(G)$ and $K_1 \cap K_2 = \{1\}$.*

Proof By Proposition 4.1, there exists $K_1 \cong G \leq \mathrm{Aut}(\mathrm{Cay}(f))$. Moreover, since the natural basis $B = G$ of Cay(f) consists of units in $\mathcal{A} = \Bbbk[G]$, Proposition 3.4 ensures that K_1 acts freely on the natural basis of Cay(f).

We now consider the following morphism $\rho : G \to \mathrm{Aut}(\mathrm{Cay}(f))$: for any $h \in G$, let $\rho(h)$ be the linear automorphism of Cay(f) = $\Bbbk[G]$ given by inner conjugation in G, that is, $\rho(h)(g) = hgh^{-1}$. Observe that $\rho(h)$ maps the natural basis $B = G$ of Cay(f) to itself, hence if $g \neq g'$ thus $g \cdot g' = 0$, then $\rho(h)(g) \neq \rho(h)(g')$ and $\rho(h)(g) \cdot \rho(h)(g') = 0$. Moreover

$$
\begin{aligned}
\rho(h)(g \cdot g) &= \rho(h) \left(\sum_{k \in G} f(g^{-1}k)k \right) \\
&= \sum_{k \in G} f(g^{-1}k)\rho(h)(k) \\
&= \sum_{k \in G} f(g^{-1}k)hkh^{-1} \\
&= \sum_{k \in G} f(hg^{-1}kh^{-1})hkh^{-1} \text{ (since } f \text{ is a class function)} \\
&= \sum_{k \in G} f(hg^{-1}h^{-1}hkh^{-1})hkh^{-1} \\
&= \sum_{k \in G} f(hg^{-1}h^{-1}k)k \\
&= \sum_{k \in G} f(\rho(h)(g)^{-1}k)k \\
&= \rho(h)(g) \cdot \rho(h)(g).
\end{aligned}
$$

Therefore, $\rho(h)$ is an actual automorphism of $\mathrm{Cay}(f)$ for every $h \in G$ and by construction $\rho(h) = \mathrm{Id}$ if and only if $h \in Z(G)$. Hence $\ker(\rho) = Z(G)$ and $K_2 = \mathrm{Im}(\rho) \cong G/Z(G)$.

Finally, notice that every $\rho(h) \in K_2$ fixes, at least, the element h in B, while every non-trivial element in K_1 acts freely on B. Therefore $K_1 \cap K_2 = \{1\}$. □

We obtain the following corollary:

Corollary 4.11 *Let $\mathcal{A} = \Bbbk[G]$, and $f \colon G \to \Bbbk$ be a class function satisfying that $\mathrm{Aut}(\mathrm{Cay}(f)) \cong G$. Then G is abelian.*

Proof According to Proposition 4.10, as $\mathrm{Aut}(\mathrm{Cay}(f)) \cong G$, the subgroup $G/Z(G)$ must be trivial.

□

References

1. Ahmed, H., Bekbaev, U., Rakhimov, I.: On classification of 2-dimensional evolution algebras and its applications. In: 5th International Conference on Mathematical Applications in Engineering 30–31 October 2019, Putrajaya, Malaysia, vol. 1489, pp. 012001. IOP Publishing Ltd (2020)
2. Alarafeen, A., Qaralleh, I., Ahmad, A.: Properties of nilpotent evolution algebras with no maximal nilindex. Eur. J. Pure Appl. Math. **14**(1), 278–300 (2021)
3. Cabrera C.Y.: Evolution algebras. Ph.D. thesis, University of Málaga, Spain (2016)
4. Cabrera, C.Y., Siles, M.M., Velasco, M.V.: Evolution algebras of arbitrary dimension and their decompositions. Linear Algebra Appl. **495**, 122–162 (2016)
5. Costoya, C., Ligouras, P., Tocino, A., Viruel, A.: Regular evolution algebras are universally finite. Proc. Am. Math. Soc. **150**(3), 919–925 (2022)
6. Costoya, C., Méndez, D., Viruel, A.: Realisability problem in arrow categories. Collect. Math. **71**, 383–405 (2020)
7. Elduque, A., Labra, A.: Evolution algebras and graphs. J. Algebra Appl. **14**(7), 1550103 (2015)
8. Elduque, A., Labra, A.: Evolution algebras, automorphisms, and graphs. Linear Multilinear Algebra **69**(2), 1–12 (2019)
9. Gordeev, N.L., Popov, V.L.: Automorphism groups of finite dimensional simple algebras. Ann. Math. **158**, 1041–1065 (2003)
10. Harary, F.: The determinant of the adjacency matrix of a graph. Siam Rev. **4**(3), 202–210 (1962)
11. Hertweck, M.: A counterexample to the isomorphism problem for integral group rings. Ann. Math. (2) **154**(1), 115–138 (2001)
12. Mukhamedov, F., Khakimov, O., Omirov, B., Qaralleh, I.: Derivations and automorphisms of nilpotent evolution algebras with maximal nilindex. J. Algebra Appl. **18**(12), 1950233 (2019)
13. Popov, V.L.: An analogue of M. Artin's conjecture on invariants for non-associative algebras. Am. Math. Soc. Transl. **169**, 121–143 (1995)
14. Sandling, R.: The isomorphism problem for group rings: A survey. In: Reiner, I., Roggenkamp, K.W. (eds.) Orders and Their Applications, pp. 256–288. Springer, Berlin (1985)
15. Sriwongsa, S., Zou, Y.M.: On automorphism groups of idempotent evolution algebras. Linear Algebra Appl. **641**, 143–155 (2022)
16. Tian, J.P.: Evolution Algebras and Their Applications. Lecture Notes in Mathematics, vol. 1921. Springer, Berlin (2008)
17. White, A.T.: Graphs, Groups and Surfaces, Volume 8 of North-Holland Mathematics Studies, 2nd edn. North-Holland Publishing Co., Amsterdam (1984)