USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Grupos de permutacións na clasificación de álxebras de evolución idempotentes

Alexandre Lago Pereira

2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO EN MATEMÁTICAS

Traballo Fin de Grao

Grupos de permutacións na clasificación de álxebras de evolución idempotentes

Alexandre Lago Pereira

Xullo, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Grupos de permutacións na clasificación de álxebras de evolución idempotentes
Breve descrición do contido
Unha álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ é unha $\mathbb{K}$-álxebra dotada dunha base que verifica que o produto de dous elementos distintos sempre é nulo. As álxebras de evolución idempotentes de dimensión finita teñen a propiedade de que o seu grupo de automorfismos, $\mathrm{Aut}(\mathcal{E})$, é finito e admite unha representación mediante permutacións. No contexto do problema de realización de grupos xorde a pregunta natural de se toda representación mediante permutacións dun grupo finito G pode realizarse a través dunha álxebra de evolución idempotente de dimensión finita. Neste traballo intrudúcese a teoría necesaria para comprender o problema e trátanse os resultados principais que aparecen na literatura.
Recomendacións
Outras observacións

Índice

Resumo

Unha álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ é unha $\mathbb{K}$-álxebra dotada dunha base B que verifica que o produto de calquera par de elementos distintos de B sempre é nulo. As álxebras de evolución idempotentes de dimensión finita teñen a propiedade de que o seu grupo de automorfismos, $\mathrm{Aut}(\mathcal{E})$, é finito e admite unha representación mediante permutacións. No contexto do problema de realización de grupos xorde a pregunta natural de se toda representación mediante permutacións dun grupo finito G pode realizarse a través dunha álxebra de evolución idempotente de dimensión finita. Neste traballo intrudúcese a teoría necesaria para comprender o problema e trátanse os resultados principais que aparecen na literatura.

Abstract

An evolution algebra $\mathcal{E}$ over a field $\mathbb{K}$ is a $\mathbb{K}$-algebra equipped with a basis B such that the product of any pair of distinct elements from B is always zero. Finite-dimensional idempotent evolution algebras have the property that their automorphism group, $\mathrm{Aut}(\mathcal{E})$, is finite and admits a representation by permutations. In the context of the group realization problem, a natural question arises: can every permutation representation of a finite group G be realized through a finite-dimensional idempotent evolution algebra? This work introduces the necessary theory to understand the problem and discusses the main results found in the literature.

Introdución

As *álxebras de evolución* son un tipo de estruturas alxébricas introducidas por Tian e Vojtechovsky no ano 2006 (véxase [9]) co obxectivo de modelizar certos mecanismos de herdanza xenética non mendeliana. Trátanse de álxebras conmutativas, en xeral non asociativas, dotadas dunha base, chamada *base natural*, na que o produto de calquera par de elementos distintos sempre é nulo. Estas estruturas presentan diversas conexións con outras ramas da álxebra, como a teoría de grupos ou a teoría de grafos (véxase, por exemplo, [8]).

No espírito da teoría de Galois, que estuda a estrutura dun corpo a través do seu grupo de automorfismos, é posible estudar unha álxebra de evolución $\mathcal{E}$ a través do seu grupo de automorfismos, $\mathrm{Aut}(\mathcal{E})$. Neste contexto, autores como Sriwongsa e Zou, [7], suxeriron a posibilidade de clasificar determinados tipos de álxebras de evolución a partir do seu grupo de automorfismos.

Dentro deste marco conceptual se sitúa o presente Traballo de Fin de Grao, centrado no estudo dunha clase concreta de álxebras de evolución, que son as *idempotentes*, ou sexa, aquelas que verifican que $\mathcal{E}^2 = \mathcal{E}$. Esta clase particular de álxebras presenta unha estrutura suficientemente ríxida como para estudar en detalle o seu grupo de automorfismos. Concretamente, as álxebras de evolución idempotentes verifican a importante propiedade de que a súa base natural é única agás por permutacións e multiplicación por escalares non nulos. Este feito facilita significativamente a caracterización dos seus automorfismos, o que nos permitirá representar $\mathrm{Aut}(\mathcal{E})$ como un cociente do grupo simétrico S_n e estudar a súa estrutura.

Unha das ferramentas básicas que empregaremos para abordar este problema é a teoría de grafos. Veremos que a cada álxebra de evolución $\mathcal{E}$ lle podemos asociar un grafo dirixido Γ relativo a unha base natural, que reflicte parte da estrutura multiplicativa da álxebra. Esta asociación non é puramente estética: como se mostra no artigo [6], existe unha sucesión exacta de grupos que relaciona o grupo de automorfismos de $\mathcal{E}$ co grupo de automorfismos do grafo, $\mathrm{Aut}(\Gamma)$, mais o chamado *grupo diagonal* de Γ, que está relacionado coas raíces da unidade:

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Aut}(\Gamma).$$

Esta sucesión exacta permítenos estudar de forma sinxela, por exemplo, cando Φ_B, a repre-

sentación do grupo de automorfismos de $\mathcal{E}$, é inxectiva, o que sucede precisamente cando $\mathrm{Diag}(\Gamma)$ é o grupo trivial. Esta condición está relacionada con propiedades combinatorias do grafo, como o seu *balance*, e ofrécenos información relevante sobre a propia álxebra de evolución. Ademais, baixo certas hipóteses adicionais de transitividade, a anterior sucesión exacta permítenos chegar a unha caracterización máis forte do grupo $\mathrm{Aut}(\mathcal{E})$.

Finalmente, estudaremos a posibilidade de substituír a condición de idempotencia por outras condicións máis débiles, como a chamada *propiedade 2LI*, que é suficiente para garantir algunhas das propiedades das álxebras de evolución idempotentes, mais non todas. Este feito lévanos a reflexionar sobre a rixidez estrutural destas álxebras e as consecuencias que certas relaxacións poden ter na súa simetría.

Este traballo pretende así contribuír á comprensión das álxebras de evolución, empregando ferramentas da teoría de grafos e a teoría de grupos para estudar e clasificar os seus grupos de automorfismos.

Capítulo 1

Grupos e grupos de permutacións

O obxectivo deste capítulo é repasar os conceptos básicos da teoría de grupos e introducir algunhas nocións e resultados que utilizaremos ó longo dos seguintes capítulos para desenvolver os contidos do traballo.

1.1. Grupos: definicións e exemplos

Un **grupo** é unha estrutura alxébrica formada por un conxunto non baleiro G dotado dunha operación binaria interna $\cdot : G \to G$ que satisfai as seguintes propiedades:

1. *Asociatividade:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para calquera $a, b, c \in G$.
2. *Elemento neutro:* Existe un elemento $e \in G$ tal que $e \cdot a = a \cdot e = a$ para todo $a \in G$.
3. *Elemento inverso:* Para cada $a \in G$, existe un elemento $a^{-1} \in G$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Se ademais $a \cdot b = b \cdot a$ para todo $a, b \in G$, entón dicimos que o grupo é **abeliano**.

O elemento neutro e é único e denótase 1. O inverso dun elemento $a \in G$ tamén é único. Para simplificar a notación, escribiremos ab en lugar de $a \cdot b$ sempre que non cause confusión.

Un **subgrupo** dun grupo G é un subconxunto non baleiro $H \subset G$ que é un grupo coa operación $\cdot$ restrinxida a H. Equivalentemente, H é un subgrupo de G se cumpre as seguintes condicións:

1. Se $a, b \in H$ entón $ab \in H$.
2. Se $a \in H$ entón $a^{-1} \in H$.

Se H é un subgrupo de G, entón escribimos $H < G$. Un subgrupo $H < G$ dise **normal** se $aH = Ha$ para todo $a \in G$, ou equivalentemente, se $aha^{-1} \in H$ para todo $h \in H$ e todo $a \in G$. Se H é un subgrupo normal de G, entón escribimos $H \lhd G$.

Se H é un subgrupo de G, entón H induce en G a seguinte relación de equivalencia:

$$a \sim b \quad \text{se} \quad ab^{-1} \in H.$$

Observemos que a clase de equivalencia dun elemento $a \in H$ é o conxunto $aH = \{ah : h \in H\}$. Se $H \lhd G$, entón o conxunto cociente G/H é un grupo coa operación:

$$aH \cdot bH := abH.$$

Nese caso, o elemento neutro de G/H é $1H = H$ e o inverso de aH é o elemento $a^{-1}H$.

Un **homomorfismo** entre dous grupos G e G' é unha aplicación $\varphi : G \to G'$ que cumpre que $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in G$. Se ademais φ é bixectivo, entón φ^{-1} tamén é un homomorfismo de grupos, e dicimos que φ é un **isomorfismo**. Se existe un isomorfismo $\varphi : G \to G'$, entón diremos que os grupos G e G' son **isomorfos**, e escribiremos $G \simeq G'$. Un **automorfismo** de G é un isomorfismo $G \to G$.

Se $\varphi : G \to G'$ é un homomorfismo de grupos, entón o conxunto $\mathrm{Ker}\varphi := \{x \in G : \varphi(x) = 1\}$ é un subgrupo normal de G chamado **núcelo** de φ, e o conxunto $\mathrm{Im}\varphi := \{\varphi(x) : x \in G\}$ é un subgrupo de G' chamado **imaxe** de φ. Tense que φ é inxectivo se, e soamente se, $\mathrm{Ker}\varphi = 1$. Ademais, tense o seguinte isomorfismo de grupos:

$$\frac{G}{\mathrm{Ker}\varphi} \simeq \mathrm{Im}\varphi.$$

Unha **sucesión exacta de grupos** é unha cadea de homomorfismos de grupos:

$$\cdots \longrightarrow G_{i-1} \xrightarrow{\varphi_{i-1}} G_i \xrightarrow{\varphi_i} G_{i+1} \longrightarrow \cdots$$

que cumpre que $\mathrm{Im}(\varphi_{i-1}) = \mathrm{Ker}(\varphi_i)$ para cada i. Esta condición garante que os elementos de G_i que se anulan ó aplicar φ_i son exactamente as imaxes por φ_{i-1} de elementos de G_{i-1}.Unha **sucesión exacta curta** é unha sucesión exacta da forma:

$$1 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 1.$$

Neste caso, a exactitude equivale a que φ sexa inxectivo, $\mathrm{Im}\varphi = \mathrm{Ker}\psi$ e ψ sexa sobrexectivo. En particular,

$$A \simeq \mathrm{Im}\varphi \qquad \text{e} \qquad \frac{B}{\mathrm{Im}\varphi} \simeq \frac{B}{\mathrm{Ker}\psi} \simeq C.$$

Exemplo 1.1. Algúns exemplos fundamentais son os seguintes:

1. O conxunto dos números enteiros $\mathbb{Z}$ é un grupo coa operación $+$, e o elemento neutro é o número 0.

2. Se G e H son dous grupos, entón o produto cartesiano $G \times H$ é un grupo coa operación

$$(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2,\ h_1 h_2).$$

   O elemento neutro é $(1_G, 1_H)$, onde 1_G e 1_H denotan os elementos neutros de G e H respectivamente, e o inverso do elemento (g, h) é o elemento (g^{-1}, h^{-1}). Se ambos grupos son abelianos, entón o produto tamén o é.

3. Se $\mathbb{K}$ é un corpo, entón o conxunto $\mathbb{K}^\times := \mathbb{K}\backslash\{0\}$ é un grupo co produto, chamado **grupo multiplicativo de** $\mathbb{K}$. O subconxunto:

$$\boldsymbol{\mu}_n(\mathbb{K}) = \{\mu \in \mathbb{K}^\times : \mu^n = 1\}$$

   é un subgrupo de $\mathbb{K}^\times$ chamado **grupo das raíces n-ésimas da unidade** en $\mathbb{K}$. Observemos que $\boldsymbol{\mu}_1$ é o grupo trivial, que normalmente denotaremos por 1.

4. Na teoría de categorías, un obxecto X dunha categoría $\mathcal{C}$ pode ter diversos morfismos en si mesmo. Un **automorfismo** de X é un isomorfismo $X \to X$, é dicir, un morfismo $f : X \to X$ para o cal existe outro morfismo $f^{-1} : X \to X$ tal que $f \circ f^{-1} = id_X = f^{-1} \circ f$. O conxunto de todos os automorfismos de X, denotado por $\mathrm{Aut}(X)$, é un grupo coa composición de aplicacións. ◇

No capítulo 2 empregaremos o seguinte resultado que involucra o grupo das raíces m-ésimas da unidade nun corpo $\mathbb{K}$, e que constitúe un exemplo significativo do concepto de automorfismo de grupos:

Lema 1.2. *Sexan $\mathbb{K}$ un corpo e $\boldsymbol{\mu}_m(\mathbb{K})$ o grupo multiplicativo das raíces m-esimas da unidade para certo enteiro positivo impar m. Entón a aplicación:*

$$\begin{aligned} \alpha : \boldsymbol{\mu}_m(\mathbb{K}) &\longrightarrow \boldsymbol{\mu}_m(\mathbb{K}) \\ \mu &\longmapsto \mu^2 \end{aligned}$$

é un automorfismo de grupos. Dado $\mu \in \boldsymbol{\mu}_m(\mathbb{K})$, o elemento $\alpha^{-1}(\mu)$ denótase $\mu^{\frac{1}{2}}$.

Demostración. Dados $\mu, \mu' \in \boldsymbol{\mu}_m(\mathbb{K})$, tense que:

$$\alpha(\mu\mu') = (\mu\mu')^2 = \mu^2 \mu'^2 = \alpha(\mu)\alpha(\mu'),$$

ou sexa, α é un homomorfismo de grupos.

Por outra parte, como m é impar, entón m é da forma $2s+1$ para s algún enteiro non negativo. Consideremos a aplicación:

$$\begin{aligned} \beta : \boldsymbol{\mu}_m(\mathbb{K}) &\longrightarrow \boldsymbol{\mu}_m(\mathbb{K}) \\ \mu &\longmapsto \mu^{s+1} \end{aligned}$$

Dado $\mu \in \boldsymbol{\mu}_m(\mathbb{K})$ tense que $\mu^m = 1$ e polo tanto:

$$\begin{aligned} \alpha\beta(\mu) = \alpha(\mu^{s+1}) = (\mu^{s+1})^2 = \mu^{2s+2} = \mu^m\mu = \mu, \\ \beta\alpha(\mu) = \beta(\mu^2) = (\mu^2)^{s+1} = \mu^{2s+2} = \mu^m\mu = \mu. \end{aligned}$$

Ou sexa, α e β son aplicacións bixectivas e inversas a unha da outra. En particular concluímos que α é un automorfismo. □

1.2. Grupos finitos

Se G é un grupo finito, entón o cardinal de G chámase **orde** de G e denótase por $|G|$. Noutro caso, dise que G é un grupo de orde infinita.

Se G é un grupo finito e H é un subgrupo de G, entón o grupo H e o conxunto G/H son finitos. O cardinal de G/H chámase **índice** de H en G, e denótase $(G : H)$. O teorema de Lagrange establece a seguinte identidade:

$$|G| = (G : H)|H|.$$

Reciprocamente, se G é un grupo e H é un subgrupo finito de G tal que G/H é un conxunto finito, entón G é finito e verifícase a mesma igualdade.

A **orde dun elemento** $a \in G$ é o menor enteiro positivo n (se existe) que satisfai que $a^n = 1$, e denótase $|a|$. Se a é un elemento de G de orde n e m é un enteiro tal que $a^m = 1$, entón $n \mid m$.

A continuación demostraremos un resultado elemental sobre a orde dun elemento nun grupo, que empregaremos no capítulo 2 para a demostración doutro resultado:

Lema 1.3. *Sexan G un grupo e $a \in G$ un elemento de orde n. Dado $k \in \mathbb{Z}$:*

$$|a^k| = \frac{n}{\gcd\{n,k\}}.$$

Demostración. Sexa $m = |a^k|$, e sexa $d = \gcd\{n,k\} > 0$, de xeito que $n = rd$ e $k = sd$ para certos enteiros r e s, necesariamente positivos, tales que $\gcd\{r,s\} = 1$. Debemos ver que $m = r$.

Vexamos que $r \mid m$. Como $|a^k| = m$ entón $1 = (a^k)^m = a^{km}$, e como ademais $|a| = n$, entón $n \mid km$. Ou sexa, existe un número enteiro λ tal que $km = \lambda n$. Entón $sdm = \lambda rd$, e como $d \neq 0$ entón $sm = \lambda r$. Particularmente, $r \mid sm$. Pero como ademais $\gcd\{r, s\} = 1$, entón $r \mid m$.

Vexamos que $m \mid r$. Efectivamente, tense que:

$$(a^k)^r = a^{kr} = a^{sdr} = a^{ns} = (a^n)^s = 1^s = 1,$$

e como $|a^k| = m$, entón $m \mid r$.

Como r e m son números enteiros positivos tales que $r \mid m$ e $m \mid r$, entón $r = m$, que era o que tiñamos que probar. □

Tamén demostraremos os seguintes dous lemas, que serán de utilidade no capítulo 2 para probar algúns resultados que involucran a orde de certos grupos finitos, motivo polo cal os incluímos nesta sección:

Lema 1.4. *Se* n, m *son enteiros positivos tales que* $n \mid m$ *entón* $2^n - 1 \mid 2^m - 1$.

Demostración. Supoñamos que $m = kn$ para certo enteiro k necesariamente positivo. Entón:

$$\begin{aligned} 2^m - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)((2^n)^{k-1} + (2^n)^{k-2} + \cdots + 2^n + 1), \end{aligned}$$

e polo tanto $2^n - 1 \mid 2^m - 1$, como queriamos ver. □

Lema 1.5. *Se* n, m *son enteiros positivos, entón* $\gcd\{2^n - 1, 2^m - 1\} = 2^{\gcd\{n,m\}} - 1$.

Con máis xeneralidade, se $\{n_1 \dots n_k\}$ *é un conxunto finito de números enteiros positivos, entón* $\gcd\{2^{n_1} - 1 \dots 2^{n_k} - 1\} = 2^{\gcd\{n_1 \dots n_k\}} - 1$.

Demostración. En primeiro lugar vexamos que se n, m son enteiros positivos, entón $\gcd\{2^n - 1, 2^m - 1\} = 2^{\gcd\{n,m\}} - 1$.

Sexan $t = \gcd\{2^n - 1, 2^m - 1\} > 0$ e $d = \gcd(n, m) > 0$. Polo teorema de Bézout, existen $s, t \in \mathbb{Z}$ tales que $d = sn + tm$.

Como $t \mid 2^n - 1$ e $t \mid 2^m - 1$ entón:

$$2^n \equiv 2^m \equiv 1 \pmod{t},$$

e polo tanto:

$$2^d = 2^{sn+tm} \equiv 1 \pmod{t},$$

ou sexa, $t \mid 2^d - 1$.

Ademais, polo lema anterior tense que, como $d \mid n$, entón $2^d - 1 \mid 2^n - 1$, e como $d \mid m$, entón $2^d - 1 \mid 2^m - 1$. Polo tanto, $2^d - 1$ divide o valor $t = \gcd\{2^n - 1, 2^m - 1\}$, isto é, $2^d - 1 \mid t$.

Acabamos de probar que $t \mid 2^d - 1$ e $2^d - 1 \mid t$, e como tanto t como $2^d - 1$ son números enteiros positivos, entón $t = 2^d - 1$, é dicir, que $\gcd\{2^n - 1, 2^m - 1\} = 2^{\gcd\{n,m\}} - 1$.

Agora vexamos que se $\{n_1 \dots n_k\}$ é un conxunto finito de números enteiros positivos, entón $\gcd\{2^{n_1} - 1 \dots 2^{n_k} - 1\} = 2^{\gcd\{n_1 \dots n_k\}} - 1$. Verémolo por indución sobre $k \geq 2$. Para $k = 2$ acabamos de probalo. Ademais, se o resultado é certo para calquera conxunto finito de $k - 1$ números enteiros positivos, entón, para o conxunto $\{n_1 \dots n_k\}$ verifícase que:

$$\begin{aligned}
\gcd\{2^{n_1} - 1 \dots 2^{n_k} - 1\} &= \gcd\{\gcd\{2^{n_1} - 1 \dots 2^{n_{k-1}} - 1\}, 2^{n_k} - 1\} \\
&= \gcd\{2^{\gcd\{n_1 \dots n_{k-1}\}} - 1, 2^{n_k} - 1\} \\
&= 2^{\gcd\{\gcd\{n_1 \dots n_{k-1}\}, n_k\}} - 1 \\
&= 2^{\gcd\{n_1 \dots n_k\}} - 1,
\end{aligned}$$

que era o que queriamos demostrar. □

1.3. Grupos de permutacións e transitividade

Unha **permutación** do conxunto $N = \{1 \dots n\}$ é unha aplicación bixectiva $\sigma : N \to N$. O conxunto de todas as permutacións do conxunto N é un grupo coa composición de aplicacións chamado **grupo simétrico** de n elementos. Este grupo denótase S_n, é abeliano para $n = 2$ e non abeliano para $n \geq 3$. Calquera subgrupo de S_n chámase **grupo de permutacións**.

Un caso importante de permutacións son os ciclos. Un **r-ciclo** é unha permutación $\sigma \in S_n$ para a cal existen r elementos distintos $a_1, \dots, a_r \in \{1, \dots, n\}$ tales que:

$$\begin{aligned}
\sigma(a_1) &= a_2, \\
\sigma(a_2) &= a_3, \\
&\dots \\
\sigma(a_{r-1}) &= a_r, \\
\sigma(a_r) &= a_1,
\end{aligned}$$

e de tal maneira que σ deixa fixos o resto de elementos. Normalmente, representamos os r-ciclos de forma abreviada como $\sigma = (a_1 \dots a_r)$. Os 2-ciclos chámanse **transposicións**.

Exemplo 1.6 (Produto de ciclos e transposicións)**.** O 3-ciclo de S_4 $\sigma = (132)$ é a permutación:

$$\sigma(1) = 3,$$
$$\sigma(2) = 1,$$
$$\sigma(3) = 2,$$
$$\sigma(4) = 4.$$

A transposición $\tau = (14)$ é a permutación:

$$\tau(1) = 4,$$
$$\tau(2) = 2,$$
$$\tau(3) = 3,$$
$$\tau(4) = 1.$$

É fácil ver que $\tau\sigma = (1324)$ e $\sigma\tau = (1432)$. ◇

Un resultado importante establece que calquera permutación de S_n pode descompoñerse como produto de transposicións. Esta descomposición non é única, pero conserva a paridade, o que quere dicir que se σ se pode descompoñer como produto dun número par (impar) de transposicións, entón calquera descomposición de σ consta dun número par (impar) de transposicións.

Se σ se expresa como produto dun número par de transposicións, entón dise que σ é unha permutación **par**. O conxunto formado por todas as permutacións pares de S_n é un subgrupo de S_n chamado **grupo alternado** de n elementos, e denótase por A_n.

A continuación introduciremos o concepto de grupo de permutacións transitivo, que será clave na última parte do capítulo 4:

Definición 1.7. Sexan n e k enteiros positivos tales que $k \leq n$. Un grupo de permutacións $P < S_n$ dise **k-transitivo** se, para calquera par de k-uplas $(x_1 \dots x_k)$ e $(y_1 \dots y_k)$ formadas por elementos distintos de $\{1 \dots n\}$, existe unha permutación $\sigma \in P$ tal que $(y_1 \dots y_k) = (\sigma(x_1) \dots \sigma(x_k))$. Se $k = 1$ entón diremos que o grupo de permutacións é **transitivo** en lugar de 1-transitivo.

Verifícase o seguinte resultado:

Proposición 1.8. *Se $P < S_n$ é un grupo de permutacións k-transitivo, entón é k'-transitivo para calquera enteiro positivo $k' < k$.*

Demostración. Dadas dúas k'-uplas de elementos distintos de $\{1 \dots n\}$, $(x_1 \dots x_{k'})$ e $(y_1 \dots y_{k'})$, podemos completalas con outros $k - k'$ elementos distintos $x_{k'+1} \dots x_k$ e $y_{k'+1} \dots y_k$ de $\{1 \dots n\}$,

dando lugar a dúas k-uplas $(x_1 \dots x_{k'}, x_{k'+1} \dots x_k)$ e $(y_1 \dots y_{k'}, y_{k'+1} \dots y_k)$. Como P é k-transitivo, entón existe unha permutación $\sigma \in P$ tal que

$$(y_1 \dots y_{k'}, y_{k'+1} \dots y_k) = (\sigma(x_1) \dots \sigma(x_{k'}), \sigma(x_{k'+1}) \dots \sigma(x_k)).$$

Particularmente, $(y_1 \dots y_{k'}) = (\sigma(x_1) \dots \sigma(x_{k'}))$. □

Un importante exemplo de grupo 2-transitivo é o seguinte (véxase [3]):

Exemplo 1.9. O grupo alternado de 4 elementos, A_4, é 2-transitivo.

Para probalo, tomemos (x_1, x_2) e (y_1, y_2) dous pares de elementos distintos de $\{1, 2, 3, 4\}$, e vexamos que existe unha permutación $\sigma \in A_n$ tal que $(y_1, y_2) = (\sigma(x_1), \sigma(x_2))$. Distinguiremos catro casos:

- Se os elementos x_1, x_2, y_1, y_2 son todos distintos, entón chega tomar $\sigma = (x_1 y_1)(x_2 y_2)$.
- Se $x_1 = y_1$ e $x_2 \neq y_2$, entón podemos tomar z o elemento de $\{1, 2, 3, 4\} \backslash \{x_1, y_1, x_2 = y_2\}$ e definir $\sigma = (x_2 y_2)(y_2 z)$.
- Se $x_1 \neq y_1$ e $x_2 = y_2$, entón podemos tomar z o elemento de $\{1, 2, 3, 4\} \backslash \{x_1 = y_1, x_2, y_2\}$ e definir $\sigma = (x_1 y_1)(y_1 z)$.
- Se $x_1 = y_1$ e $x_2 = y_2$, chega tomar $\sigma = 1$. ◇

De xeito análogo podemos ver que A_n é 2-transitivo para calquera $n > 4$ arbitrario. Destacamos este feito xa que os grupos de pemutacións 2-transitivos xogarán un papel moi significativo na última parte do capítulo 4.

Capítulo 2

Grafos dirixidos. Automorfismos diagonais

Neste capítulo introduciremos as nocións de grafo dirixido finito, grupo diagonal dun grafo dirixido finito e outros conceptos relacionados, que serán algunhas das ferramentas fundamentais que empregaremos ó longo do noso traballo. Todas as definicións e resultados deste capítulo están tomados de [6] e de [1]. Cómpre sinalar que os grafos que consideraremos neste traballo son todos grafos dirixidos finitos, e por simplicidade moitas veces referirémonos a eles soamente como grafos.

2.1. Grafos dirixidos: definicións e exemplos

Un **grafo (dirixido finito)** é un par $\Gamma = (V, E)$ formado por un conxunto finito V cuxos elementos se chaman *vértices* e un conxunto $E \subset V \times V$ cuxos elementos se chaman *arestas*.

Un **morfismo** entre dous grafos $\Gamma = (V, E)$ e $\Gamma' = (V', E')$ é unha aplicación $\sigma : V \to V'$ que cumpre que $(\sigma(i), \sigma(j)) \in E'$ se $(i, j) \in E$. Se σ é bixectiva e σ^{-1} é un morfismo de grafos, entón dise que σ é un **isomorfismo** de grafos. Un **automorfismo** dun grafo Γ é un isomorfismo de Γ en si mesmo. Trivialmente, o conxunto $\mathrm{Aut}(\Gamma)$ formado polos automorfismos dun grafo Γ é un grupo coa composición de aplicacións.

Exemplo 2.1 (Morfismo de grafos)**.** Consideremos o grafo $\Gamma = (V, E)$ dado por:

$$V = \{v_1, v_2, v_3\} \quad \text{e} \quad E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3)\},$$

e mais o grafo $\Gamma' = (V', E')$ dado por:

$$V' = \{v_1', v_2', v_3'\} \quad \text{e} \quad E' = \{(v_2', v_3'), (v_2', v_1'), (v_3', v_1'), (v_3', v_3')\},$$

representados na figura 2.1.

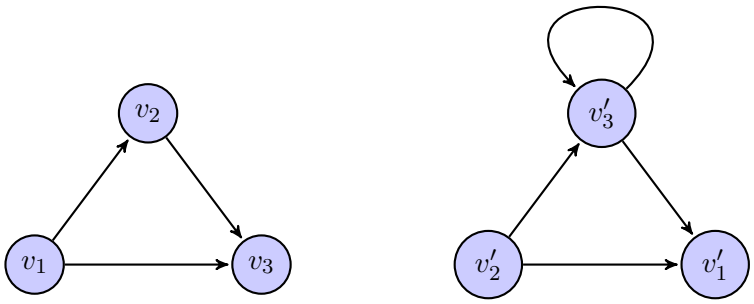

Figura 2.1: Grafos Γ e Γ' do exemplo 2.1.

Claramente, a aplicación $\sigma : V \to V'$ definida como:

$$\sigma(v_1) = v'_2,$$
$$\sigma(v_2) = v'_3,$$
$$\sigma(v_3) = v'_1,$$

é un morfismo de grafos bixectivo. Non obstante, a aplicación σ^{-1} non é un morfismo de grafos, xa que $(v'_3, v'_3) \in E'$ pero en cambio $(\sigma^{-1}(v'_3), \sigma^{-1}(v'_3)) = (v_2, v_2) \notin E$. Entón σ é un morfismo de grafos bixectivo, que non é un isomorfismo de grafos. $\diamond$

Dado un grafo $\Gamma = (V, E)$, introducimos as seguintes definicións:

- Un **subgrafo** é un grafo $\Gamma' = (V', E')$ que verifica $V' \subset V$ e $E' \subset E$.
- Un **camiño** é unha secuencia $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$, onde $n \geq 0$, $v_0, \ldots, v_n \in V$, $e_1, \ldots, e_n \in E$, e para cada $i = 1, \ldots, n$ cúmprese que $e_i = (v_{i-1}, v_i)$ ou $e_i = (v_i, v_{i-1})$. Un **ciclo** é un camiño $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ tal que $v_0 = v_n$.
- O **grao de entrada** dun vértice $v \in V$ é o enteiro non negativo:

  $$\deg^-(v) = \#\{w \in V \mid (w, v) \in E\},$$

  mentres que o **grao de saída** é:

  $$\deg^+(v) = \#\{w \in V \mid (v, w) \in E\}.$$

  Dicimos que un vértice v é unha **fonte** se $\deg^-(v) = 0$, é dicir, se non ten arestas entrantes, e un **sumidoiro** se $\deg^+(v) = 0$, ou sexa, se non ten arestas saíntes.

- Definimos o **balance** do camiño $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ como o número enteiro:

$$b(\gamma) = \#\{i \mid 1 \leq i \leq n \text{ e } e_i = (v_{i-1}, v_i)\} - \#\{i \mid 1 \leq i \leq n \text{ e } e_i = (v_i, v_{i-1})\}.$$

  É dicir, $b(\gamma)$ obtense sumando $+1$ se a aresta e_i vai na dirección çorrecta"de v_{i-1} a v_i e -1 sevai na dirección contraria, sumando ó longo do camiño.

- O **balance do grafo** Γ defínese como o máximo común divisor dos valores absolutos dos balances dos ciclos en Γ:

$$b(\Gamma) = \gcd\{\, |b(\gamma)| : \gamma \text{ é un ciclo en } \Gamma \,\}.$$

- Por último, diremos que un grafo Γ é **conexo** se para calquera par de vértices $v, w \in V$ existe un camiño:

$$\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$$

  con $v_0 = v$ e $v_n = w$. Diremos que γ é un camiño de v a w.

  Calquera grafo Γ é a **unión disxunta** das súas compoñentes conexas, onde por **compoñente conexa** entendemos un subgrafo conexo maximal de Γ.

Ilustremos con algúns exemplos os conceptos que acabamos de definir:

Exemplo 2.2. A figura 2.2 representa o grafo de vértices $V = \{v_1, v_2, v_3, v_4\}$ e arestas $E = \{(v_1, v_2), (v_2, v_1), (v_1, v_3), (v_3, v_1), (v_1, v_4), (v_2, v_4), (v_3, v_4)\}$. O vértice v_4 non ten arestas saíntes, é dicir, $\deg^+(v_4) = 0$, e polo tanto é un sumidoiro. ◇

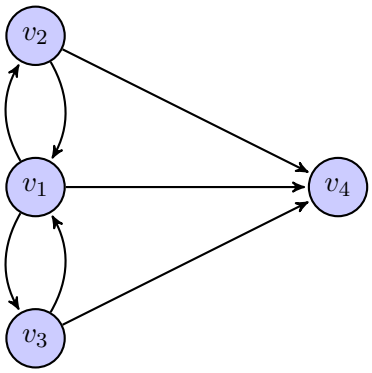

Figura 2.2: Grafo con sumidoiro.

Exemplo 2.3. A figura 2.3 representa o grafo de vértices $V = \{v_1, v_2, v_3, v_4\}$ e arestas $E = \{(v_1, v_2), (v_2, v_1), (v_1, v_3), (v_3, v_1), (v_4, v_1), (v_4, v_2), (v_4, v_3)\}$. O vértice v_4 non ten arestas entrantes, é dicir, $\deg^-(v_4) = 0$, e polo tanto é unha fonte. ◇

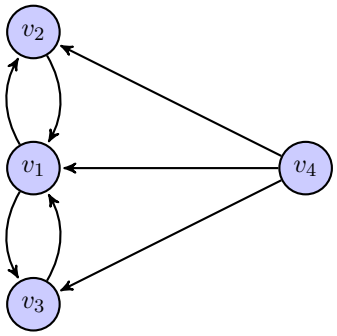

Figura 2.3: Grafo con fonte.

Exemplo 2.4. A figura 2.4 representa o grafo de vértices $V = \{v_1, v_2, v_3, v_4\}$ e arestas $E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3), (v_3, v_4), (v_4, v_1)\}$. Por simplicidade, denotemos por e_{ij} a aresta (v_i, v_j). Consideremos os seguintes camiños en Γ:

$$\gamma_1 = (v_1, e_{12}, v_2, e_{23}, v_3, e_{34}, v_4, e_{41}, v_1)$$
$$\gamma_2 = (v_1, e_{13}, v_3, e_{34}, v_4, e_{41}, v_1)$$

Está claro que $b(\gamma_1) = 4$ e $b(\gamma_2) = 3$. Como $b(\Gamma)$ é un enteiro positivo que divide o valor $\gcd\{b(\gamma_1), b(\gamma_2)\} = \gcd\{4, 3\} = 1$, entón $b(\Gamma) = 1$. ◇

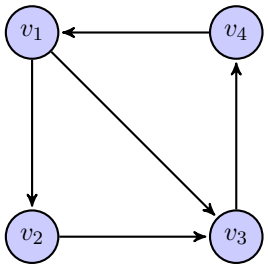

Figura 2.4: Grafo con balance 1.

2.2. O grupo diagonal dun grafo

Sexan $\mathbb{K}$ un corpo e $\Gamma = (V, E)$ un grafo. Definimos o **grupo diagonal de Γ** en $\mathbb{K}$ como o conxunto:

$$\mathrm{Diag}_{\mathbb{K}}(\Gamma) := \{\psi : V \to \mathbb{K}^\times \mid \psi(w) = \psi(v)^2 \text{ se } (v, w) \in E\}$$

A partir de agora, entenderemos que estamos traballando sobre o corpo $\mathbb{K}$ aínda que non o indiquemos explicitamente, e escribiremos $\mathrm{Diag}(\Gamma)$ en lugar de $\mathrm{Diag}_{\mathbb{K}}(\Gamma)$. Do mesmo xeito, denotaremos o grupo multiplicativo das raíces m-ésimas da unidade en $\mathbb{K}$ por $\boldsymbol{\mu}_m$ en lugar de $\boldsymbol{\mu}_m(\mathbb{K})$ sen causar confusión.

O seguinte resultado establece que, efectivamente, Diag(Γ) é un grupo:

Proposición 2.5. *Se* $\Gamma = (V, E)$ *é un grafo, entón* Diag(Γ) *é un grupo coa operación:*

$$(\psi\psi')(v) = \psi(v)\psi'(v)$$

e o seu elemento neutro é a aplicación $1 : V \to \mathbb{K}^\times$ *dada por* $1(v) = 1$ *para todo* $v \in V$*.*

Demostración. Vexamos cada parte da demostración por separado.

- *A operación está ben definida.* Dados $\psi, \psi' \in \mathrm{Diag}(\Gamma)$, para calquera aresta $(v, w) \in E$:

$$(\psi\psi')(w) = \psi(w)\psi'(w) = \psi(v)^2\psi'(v)^2 = (\psi(v)\psi'(v))^2 = (\psi\psi')(v)^2,$$

  é dicir, que $\psi\psi' \in \mathrm{Diag}(\Gamma)$.

- *Asociatividade.* Dados $\psi, \psi', \psi'' \in \mathrm{Diag}(\Gamma)$, para todo $v \in V$ cúmprese que:

$$\begin{aligned}((\psi\psi')\psi'')(v) &= (\psi\psi')(v)\psi''(v)\\ &= (\psi(v)\psi'(v))\psi''(v)\\ &= \psi(v)(\psi'(v)\psi''(v))\\ &= \psi(v)(\psi'\psi''(v))\\ &= (\psi(\psi'\psi''))(v),\end{aligned}$$

  é dicir, $(\psi\psi')\psi'' = \psi(\psi'\psi'')$.

- *Elemento neutro.* Para cada $v \in V$ arbitrario verifícanse as seguintes igualdades:

$$\begin{aligned}(1\psi)(v) &= 1(v)\psi(v) = 1 \cdot \psi(v) = \psi(v),\\ (\psi 1)(v) &= \psi(v)1(v) = \psi(v) \cdot 1 = \psi(v);\end{aligned}$$

  ou sexa, que $1\psi = \psi = \psi 1$ para todo $\psi \in \mathrm{Diag}(\Gamma)$, o que quere dicir que 1 é o elemento neutro de Diag(Γ).

- *Elemento inverso.* Dado calquera $\psi \in \mathrm{Diag}(\Gamma)$, pódese definir a aplicación $\psi' : V \to \mathbb{K}^\times$ como $\psi'(v) = \dfrac{1}{\psi(v)}$, posto que $\psi(V) \subset \mathbb{K}^\times$. Se $(v, w) \in E$ entón:

$$\psi'(w) = \frac{1}{\psi(w)} = \frac{1}{\psi(v)^2} = \psi'(v)^2,$$

  e polo tanto $\psi' \in \mathrm{Diag}(\Gamma)$. Ademais, para todo $v \in V$, $\psi\psi'(v) = 1 = \psi'\psi(v)$, ou sexa, $\psi' = \psi^{-1}$.

Polo tanto, Diag(Γ) é un grupo. □

O seguinte resultado presenta unha relación entre o grupo diagonal dun grafo Γ e os grupos diagonais das súas compoñentes conexas, e será de utilidade á hora de estudar o grupo diagonal de grafos non conexos:

Proposición 2.6. *Sexa Γ un grafo e sexan $\Gamma_1 \dots \Gamma_k$ as súas compoñentes conexas. Entón:*

$$\mathrm{Diag}(\Gamma) \simeq \mathrm{Diag}(\Gamma_1) \times \cdots \times \mathrm{Diag}(\Gamma_k).$$

Demostración. Supoñamos que $\Gamma = (V, E)$ e que $\Gamma_i = (V_i, E_i)$ para cada $i = 1, \dots, k$. Definimos a aplicación:

$$\begin{aligned} r : \mathrm{Diag}(\Gamma) &\longrightarrow \mathrm{Diag}(\Gamma_1) \times \cdots \times \mathrm{Diag}(\Gamma_k) \\ \psi &\longmapsto r(\psi) := (\psi|_{V_1}, \dots, \psi|_{V_n}) \end{aligned}$$

Vexamos que r é un isomorfismo de grupos.

- *r está ben definido.* Para cada $\psi \in \mathrm{Diag}(\Gamma)$ e cada $i = 1, \dots, k$, a restrición $\psi|_{V_i}$ é un elemento de $\mathrm{Diag}(\Gamma_i)$, xa que se $(v, w) \in E_i$, en particular $(v, w) \in E$, e en consecuencia $\psi|_{V_i}(w) = \psi(w) = \psi(v)^2 = \psi|_{V_i}(v)^2$.

- *r é un homomorfismo.* Dados $\psi, \psi' \in \mathrm{Diag}(\Gamma)$, para cada $i = 1, \dots, k$ arbitrario cúmprese que $(\psi\psi')|_{V_i} = \psi|_{V_i}\psi'|_{V_i}$, e polo tanto $r(\psi\psi') = r(\psi)r(\psi')$.

- *r é inxectivo.* Sexa $\psi \in \mathrm{Ker}(r)$. Dado un elemento $v \in V$ arbitrario, terase que v pertence ó conxunto de vértices dunha única compoñente conexa de Γ. Supoñamos que $v \in V_i$. Entón $\psi(v) = \psi|_{V_i}(v) = 1$. Concluímos que $\psi = 1$, de xeito que $\mathrm{Ker}(r) = 1$ e r é inxectivo.

- *r é sobrexectivo.* Para cada $i = 1, \dots, k$ sexa $\psi_i \in \mathrm{Diag}(\Gamma_i)$ un elemento arbitrario, e definamos a aplicación $\psi : V \to \mathbb{K}^\times$ da seguinte maneira:

  $$\psi(v) := \psi_i(v) \text{ se } v \in V_i.$$

  En primeiro lugar, ψ está ben definida, pois cada elemento $v \in V$ pertence ó conxunto de vértices dunha única compoñente conexa de Γ. Ademais, dada unha aresta $(v, w) \in E$, terase que (v, w) pertence ó conxunto de arestas dalgunha compoñente conexa de Γ, digamos E_i; entón $v, w \in V_i$ e ademais $\psi(w) = \psi_i(w) = \psi_i(v)^2 = \psi(v)^2$. Consecuentemente, $\psi \in \mathrm{Diag}(\Gamma)$. Ademais, para cada $i = 1, \dots, k$ terase que $\psi|_{V_i} = \psi_i$ e polo tanto $r(\psi) = (\psi_1, \dots, \psi_k)$.

Acabamos de ver que r é un isomorfismo e polo tanto $\mathrm{Diag}(\Gamma) \simeq \mathrm{Diag}(\Gamma_1) \times \cdots \times \mathrm{Diag}(\Gamma_k)$. □

Máis abaixo veremos que se Γ é un grafo conexo e sen fontes, entón o grupo $\mathrm{Diag}(\Gamma)$ é isomorfo ó grupo das raíces N-ésimas da unidade $\boldsymbol{\mu}_N$ para certo número natural N relacionado co balance de Γ. O seguinte resultado, en cuxa demostración adaptamos as ideas de [5, Theorem 4.8], ofrece unha primeira intuición da relación que existe entre os elementos do grupo diagonal e as raíces da unidade en $\mathbb{K}$:

Teorema 2.7. *Sexan $\Gamma = (V, E)$ un grafo sen fontes e $\psi \in \mathrm{Diag}(\Gamma)$. Dado $v \in V$, $\psi(v)$ é unha raíz m-ésima da unidade para algún enteiro positivo impar m.*

Demostración. Supoñamos que $V = \{v_1, \ldots, v_n\}$ e que $v = v_i$. Denotemos $i_0 = i$. Como o grafo Γ non ten fontes, entón existirá algún índice $i_1 \in \{1, \ldots, n\}$ tal que $(v_{i_1}, v_{i_0}) \in E$. Analogamente, existirá algún índice $i_2 \in \{1, \ldots, n\}$ tal que $(v_{i_2}, v_{i_1}) \in E$. Procedendo sucesivamente da mesma maneira, construiremos unha sucesión de índices $\{i_k\}_{k=0}^{\infty}$ formada por elementos do conxunto $\{1, \ldots, n\}$ que para todo $k \in \mathbb{N}$ cumpre que $(v_{i_{k+1}}, v_{i_k}) \in E$, e en particular $\psi(v_{i_k}) = \psi(v_{i_{k+1}})^2$, xa que $\psi \in \mathrm{Diag}(\Gamma)$.

Agora ben, no conxunto $\{i_k\}_{k=0}^{n}$ debe haber necesariamente dous elementos repetidos, e polo tanto podemos considerar r e s os menores enteiros tales que $0 \leq r < s \leq n$ e $i_r = i_s$ (obsérvese o grafo da figura 2.5). Terase que:

$$\psi(v_{i_r}) = \psi(v_{i_{r+1}})^2 = \psi(v_{i_{r+2}})^{2^2} = \cdots = \psi(v_{i_s})^{2^{s-r}} = \psi(v_{i_r})^{2^{s-r}},$$

de xeito que $\psi(v_{i_r})^{2^{s-r}-1} = 1$. Ademais:

$$\psi(v) = \psi(v_{i_0}) = \psi(v_{i_1})^2 = \cdots = \psi(v_{i_r})^{2^r}.$$

Polo tanto:

$$\psi(v)^{2^{s-r}-1} = (\psi(v_{i_r})^{2^r})^{2^{s-r}-1} = (\psi(v_{i_r})^{2^{s-r}-1})^{2^r} = 1^{2^r} = 1.$$

Se denotamos $m = 2^{s-r} - 1$, teremos m é impar e $\psi(v)$ é unha raíz m-ésima da unidade. □

Acabamos de probar que se Γ é un grafo sen fontes, $\psi \in \mathrm{Diag}(\Gamma)$ e $v \in V$, entón $\psi(v)$ é unha raíz impar da unidade, e, en particular, $|\psi(v)|$, a orde de $\psi(v)$ no grupo multiplicativo $\mathbb{K}^\times$, é un número impar.

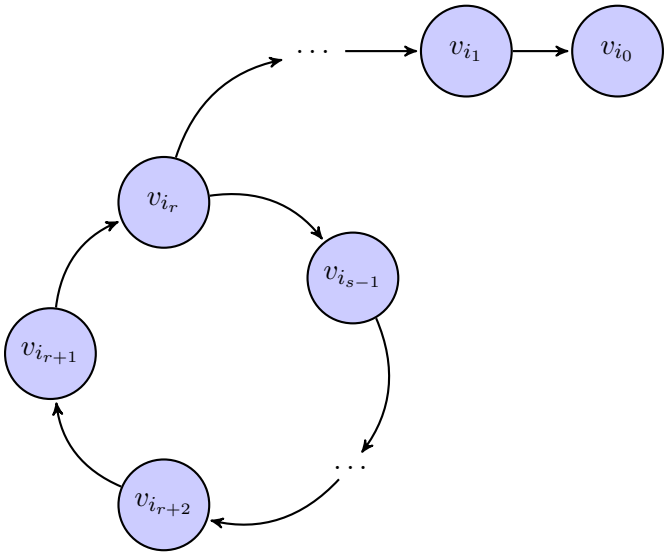

Figura 2.5: Grafo do teorema 2.7.

O seguinte resultado nos permitirá probar que se ademais Γ é conexo, entón todos os elementos $\psi(v)$, con $\psi \in \mathrm{Diag}(\Gamma)$ e $v \in V$, teñen a mesma orde en $\mathbb{K}^\times$:

Proposición 2.8. *Sexan $\Gamma = (V, E)$ un grafo e $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ un camiño en Γ, e sexa $\psi \in \mathrm{Diag}(\Gamma)$ tal que cada elemento $\psi(v_i)$ é unha raíz impar da unidade. Entón $\psi(v_n) = \psi(v_0)^{2^{b(\gamma)}}$.*

Demostración. Vexamos a demostración por indución sobre n. En primeiro lugar, debemos ver que o resultado é certo para $n = 1$, ou sexa, para un camiño da forma $\gamma = (v_0, e_1, v_1)$. Distinguiremos dous casos:

Caso 1. Se $e_1 = (v_0, v_1)$ entón $b(\gamma) = 1$ e ademais:

$$\psi(v_1) = \psi(v_0)^2 = \psi(v_0)^{2^{b(\gamma)}}.$$

Caso 2. Se $e_1 = (v_1, v_0)$ entón $b(\gamma) = -1$ e $\psi(v_0) = \psi(v_1)^2$. Grazas ó lema 1.2 podemos escribir:

$$\psi(v_1) = \psi(v_0)^{2^{-1}} = \psi(v_0)^{2^{b(\gamma)}}.$$

Agora supoñamos que o resultado é certo para camiños de lonxitude $n-1$ e vexámolo para $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ un camiño de lonxitude n.

Consideremos o camiño $\gamma' = (v_0, e_1, v_1, \ldots, v_{n-2}, e_{n-1}, v_{n-1})$. Resulta claro que:

$$b(\gamma) = \begin{cases} b(\gamma') + 1 & \text{se } e_n = (v_{n-1}, v_n) \\ b(\gamma') - 1 & \text{se } e_n = (v_n, v_{n-1}) \end{cases}$$

Distinguiremos dous casos:

Caso 1. Se $e_n = (v_{n-1}, v_n)$ entón:

$$\psi(v_n) = \psi(v_{n-1})^2 = (\psi(v_0)^{2^{b(\gamma')}})^2 = \psi(v_0)^{2^{b(\gamma')+1}} = \psi(v_0)^{2^{b(\gamma)}}.$$

Caso 2. Se $e_n = (v_n, v_{n-1})$ entón $\psi(v_{n-1}) = \psi(v_n)^2$ e polo tanto:

$$\psi(v_n) = \psi(v_{n-1})^{2^{-1}} = (\psi(v_0)^{2^{b(\gamma')}})^{2^{-1}} = \psi(v_0)^{2^{b(\gamma')-1}} = \psi(v_0)^{2^{b(\gamma)}}.$$

o que remata a proba. □

A partir da proposición anterior deducimos o seguinte resultado, que adiantabamos antes:

Proposición 2.9. *Sexa $\Gamma = (V, E)$ un grafo conexo e sen fontes e sexa $\psi \in \mathrm{Diag}(\Gamma)$. Entón, dados $u, v \in V$, $\psi(u)$ e $\psi(v)$ teñen a mesma orde no grupo multiplicativo $\mathbb{K}^\times$.*

Demostración. Como o grafo Γ é conexo, entón existirá $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ un camiño de u a v. Podemos supoñer que $b(\gamma) \geq 0$ sen perda de xeneralidade, xa que se fose $b(\gamma) < 0$, entón poderíamos considerar o camiño de v a u $\gamma^{-1} = (v_n, e_{n-1}, v_{n-1}, \ldots, v_1, e_1, v_0)$, cuxo balance é $b(\gamma^{-1}) = -b(\gamma) > 0$, e facer un razoamento análogo.

Supoñamos pois que γ é un camiño de u a v con $b(\gamma) \geq 0$. Pola proposición 2.8, tense que $\psi(v) = \psi(u)^{2^{b(\gamma)}}$. Se $b(\gamma) = 0$ entón $\psi(v) = \psi(u)$ e o resultado dedúcese trivialmente. Se $b(\gamma) > 0$, entón polo lema 1.3 terase que:

$$|\psi(v)| = \frac{|\psi(u)|}{\gcd\{|\psi(u)|, 2^{b(\gamma)}\}},$$

onde $2^{b(\gamma)}$ é un número par e $|\psi(u)|$ é un número impar (a consecuencia do teorema 2.7). Polo tanto $\gcd\{|\psi(u)|, 2^{b(\gamma)}\} = 1$, e de aí $|\psi(v)| = |\psi(u)|$. □

Finalmente, xa estamos en condicións de formular a relación que existe entre o grupo $\mathrm{Diag}(\Gamma)$ e as raíces da unidade en $\mathbb{K}$. Recordemos que se m é un enteiro positivo, entón $\boldsymbol{\mu}_m$ denota o subrgupo de $\mathbb{K}^\times$ formado polos elementos $\mu \in \mathbb{K}^\times$ tales que $\mu^m = 1$.

Teorema 2.10. *Sexa $\Gamma = (V, E)$ un grafo conexo e sen fontes, e sexa $N = 2^{b(\Gamma)} - 1$. Entón* $\mathrm{Diag}(\Gamma) \simeq \boldsymbol{\mu}_N$.

Demostración. Fixado un elemento $a \in V$, definimos a aplicación:

$$\begin{aligned} \Phi_a : \mathrm{Diag}(\Gamma) &\longrightarrow \mathbb{K}^\times \\ \psi &\longmapsto \Phi_a(\psi) := \psi(a) \end{aligned}$$

Vexamos que Φ_a é un homomorfismo de grupos inxectivo, e que a súa imaxe é precisamente $\boldsymbol{\mu}_N$. Procedamos por partes:

- Φ_a *é un homomorfismo de grupos.* Dados $\psi\psi' \in \mathrm{Diag}(\Gamma)$:

$$\Phi_a(\psi\psi') = (\psi\psi')(a) = \psi(a)\psi'(a) = \Phi_a(\psi)\Phi_a(\psi').$$

- Φ_a *é inxectivo.* Sexa $\psi \in \mathrm{Diag}(\Gamma)$ tal que $\Phi_a(\psi) = 1$, ou sexa, tal que $\psi(a) = 1$. Como Γ é un grafo conexo entón, dado $v \in V$ arbitrario, existirá γ un camiño de a a v, e pola proposición 2.8 entón:
$$\psi(v) = \psi(a)^{2^{b(\gamma)}} = 1^{2^{b(\gamma)}} = 1.$$
Como $\psi(v) = 1$ para todo $v \in V$, entón $\psi = 1$. Concluímos que $\mathrm{Ker}\Phi_a = 1$, o que quere dicir que o homomorfismo de grupos Φ_a é inxectivo.

- *Vexamos que* $\mathrm{Im}\Phi_a \subset \boldsymbol{\mu}_N$. Sexa $\psi \in \mathrm{Diag}(\Gamma)$. Observemos que se $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ é un ciclo de Γ arbitrario ($v_0 = v_n$), entón $\psi(v_0) = \psi(v_n) = \psi(v_0)^{2^{b(\gamma)}}$, e polo tanto:
$$\psi(v_0)^{2^{b(\gamma)}-1} = 1.$$
Deste xeito, $|\psi(v_0)|$, a orde de $\psi(v_0)$ en $\mathbb{K}^\times$, divide a $2^{b(\gamma)} - 1$. Agora ben, pola proposición 2.9 tense que $|\psi(v_0)| = |\psi(a)|$. Polo tanto, $|\psi(a)|$ divide a $2^{b(\gamma)} - 1$ para calquera ciclo γ de Γ. Daquela, $|\psi(a)|$ divide o valor:
$$\begin{aligned} &\gcd\{2^{b(\gamma)} - 1 : \gamma \text{ é un ciclo de } \Gamma\} = \\ &\quad = 2^{\gcd\{b(\gamma):\gamma \text{ é un ciclo de } \Gamma\}} - 1 \\ &\quad = 2^{b(\Gamma)} - 1 \\ &\quad = N, \end{aligned}$$
onde a primeira igualdade é consecuencia do lema 1.5. Polo tanto, $\psi(a)^N = 1$, ou sexa, $\Phi_a(\psi) = \psi(a) \in \boldsymbol{\mu}_N$.

- *Vexamos que* $\boldsymbol{\mu}_N \subset \mathrm{Im}\Phi_a$. Sexa $\mu \in \boldsymbol{\mu}_N$, e definamos $\psi : V \to \mathbb{K}^\times$ da seguinte maneira:
$$\psi(v) := \begin{cases} \mu & \text{se } v = a \\ \mu^{2^{b(\gamma)}} & \text{se } v \neq a, \text{ para algún camiño } \gamma \text{ de } a \text{ a } v \end{cases}$$

En primeiro lugar, ψ está ben definida, pois se $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ e $\hat{\gamma} = (\hat{v}_0, \hat{e}_1, \hat{v}_1, \ldots, \hat{v}_{k-1}, \hat{e}_k, \hat{v}_k)$ son dous camiños de a a v, entón o camiño:

$$\gamma\hat{\gamma}^{-1} := (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n = \hat{v}_k, \hat{e}_k, \hat{v}_{k-1}, \ldots, \hat{v}_1, \hat{e}_1, \hat{v}_0)$$

é un ciclo que comeza e acaba en a, e o seu balance é $b(\gamma\hat{\gamma}^{-1}) = b(\gamma) - b(\hat{\gamma})$. Terase que $b(\Gamma) \mid b(\gamma\hat{\gamma}^{-1})$, e grazas ó lema 1.4 entón:

$$N = 2^{b(\Gamma)} - 1 \mid 2^{b(\gamma\hat{\gamma}^{-1})} - 1 = 2^{b(\gamma)-b(\gamma')} - 1.$$

Agora, como $\mu \in \boldsymbol{\mu}_N$ entón $\mu^N = 1$, e como ademais $N \mid 2^{b(\gamma)-b(\gamma')} - 1$, entón tamén se verifica que $\mu^{2^{b(\gamma)-b(\gamma')}-1} = 1$, é dicir:

$$\mu^{2^{b(\gamma)-b(\gamma')}} = \mu.$$

Elevando ambos termos a $2^{b(\gamma')}$ obtemos que:

$$\mu^{2^{b(\gamma)}} = (\mu^{2^{b(\gamma)-b(\gamma')}})^{2^{b(\gamma')}} = \mu^{2^{b(\gamma')}},$$

e de aí concluímos que o valor $\psi(v)$ está ben definido.

Ademais, temos que $\psi \in \mathrm{Diag}(\Gamma)$, xa que, dada unha aresta $e = (v, w) \in E$, e tomado un camiño arbitrario $\gamma = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n)$ de a a v, verifícase que $\gamma' = (v_0, e_1, v_1, \ldots, v_{n-1}, e_n, v_n, e, w)$ é un camiño de a a w con $b(\gamma') = b(\gamma) + 1$, e polo tanto:

$$\psi(w) = \mu^{2^{b(\gamma')}} = \mu^{2^{b(\gamma)+1}} = (\mu^{2^{b(\gamma)}})^2 = \psi(v)^2.$$

Ou sexa, acabamos de demostrar que ψ é un elemento de $\mathrm{Diag}(\Gamma)$ tal que $\Phi_a(\psi) = \mu$, e de aí concluímos que $\boldsymbol{\mu}_N \subset \mathrm{Im}\Phi_a$

Vimos que Φ_a é un homomorfismo de grupos inxectivo entre $\mathrm{Diag}(\Gamma)$ e $\mathbb{K}^\times$, cuxa imaxe é precisamente $\boldsymbol{\mu}_N$. Daquela:

$$\mathrm{Diag}(\Gamma) \simeq \boldsymbol{\mu}_N,$$

que era o que tiñamos que probar. □

Como consecuencia do teorema anterior deducimos dous importantes corolarios:

Corolario 2.11. *Se $\Gamma = (V, E)$ é un grafo conexo e sen fontes que contén un ciclo da forma $\gamma = (v, e, v)$, entón* $\mathrm{Diag}(\Gamma) = 1$.

Demostración. Tense que $b(\Gamma)$ divide o valor $b(\gamma) = 1$, e polo tanto $b(\Gamma) = 1$. Do teorema anterior deducimos que $\mathrm{Diag}(\Gamma) \simeq \boldsymbol{\mu}_1 = 1$, ou sexa, que $\mathrm{Diag}(\Gamma)$ é o grupo trivial. □

Corolario 2.12. *Se* Γ *é un grafo sen fontes, entón* $\mathrm{Diag}(\Gamma)$ *é un grupo finito.*

Demostración. Sexan $\Gamma_1, \ldots, \Gamma_k$ as compoñentes conexas de Γ, e para cada $i = 1, \ldots, k$ sexa $N_i = 2^{b(\Gamma_i)} - 1$. Cada compoñente Γ_i é un grafo conexo e sen fontes, e polo tanto $\mathrm{Diag}(\Gamma_i) \simeq \boldsymbol{\mu}_{N_i}$. Ademais, pola proposición 2.6, $\mathrm{Diag}(\Gamma) \simeq \mathrm{Diag}(\Gamma_1) \times \cdots \times \mathrm{Diag}(\Gamma_k)$. Entón:

$$\mathrm{Diag}(\Gamma) \simeq \boldsymbol{\mu}_{N_1} \times \cdots \times \boldsymbol{\mu}_{N_k},$$

e, en particular, $\mathrm{Diag}(\Gamma)$ é un grupo finito. □

Capítulo 3

Álxebras de evolución: definicións e estrutura

Neste capítulo introducimos a noción de *álxebra de evolución* sobre un corpo, que consitúe o principal obxecto de estudo do noso traballo, así como o concepto de *matriz de estrutura* dunha álxebra de evolución, unha ferramenta que nos permitirá estudar algunhas propiedades deste tipo de álxebras mediante invariantes asociados ás matrices. Na última sección do capítulo definiremos o concepto de *idempotencia* dunha álxebra de evolución, unha importante propiedade que será clave para garantir algúns dos resultados que desenvolveremos no capítulo 4.

3.1. Álxebras sobre un corpo: definicións e exemplos

Unha **álxebra sobre un corpo** $\mathbb{K}$, ou $\mathbb{K}$-álxebra, é un $\mathbb{K}$-espazo vectorial $\mathcal{A}$ dotado dunha operación binaria interna $\cdot : \mathcal{A}\times\mathcal{A} \to \mathcal{A}$ que satisfai as seguintes propiedades para todo $x, y, z \in \mathcal{A}$ e todo $\lambda \in \mathbb{K}$:

1. *Distributividade pola dereita:* $x \cdot (y + z) = x \cdot y + x \cdot z$,
2. *Distributividade pola esquerda:* $(x + y) \cdot z = x \cdot z + y \cdot z$,
3. *Compatibilidade co produto escalar:* $x \cdot (\lambda y) = (\lambda x) \cdot y = \lambda(x \cdot y)$.

Unha $\mathbb{K}$-álxebra $\mathcal{A}$ dise **asociativa** se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ para todos $x, y, z \in \mathcal{A}$; **conmutativa** se $x \cdot y = y \cdot x$ para todos $x, y \in \mathcal{A}$; e **unitaria** se existe un elemento $1 \in \mathcal{A}$ tal que $1 \cdot x = x \cdot 1 = x$ para todo $x \in \mathcal{A}$.

A partir de agora, para simplificar a notación, escribiremos simplemente xy en lugar de $x \cdot y$.

Unha **base dunha álxebra** $\mathcal{A}$ é unha base de $\mathcal{A}$ como espazo vectorial, é dicir, un subconxunto $B \subset \mathcal{A}$ tal que todo elemento de $\mathcal{A}$ pode escribirse de forma única como combinación linear de elementos de B.

Se $B = \{e_i\}_{i \in I}$ é unha base de $\mathcal{A}$, entón a estrutura multiplicativa de $\mathcal{A}$ queda determinada polas **constantes de estrutura** $c_{ij}^k \in \mathbb{K}$, determinadas por:

$$e_i e_j = \sum_{k \in I} c_{ij}^k \, e_k.$$

Unha $\mathbb{K}$-álxebra $\mathcal{A}$ dise de **tipo finito** se ten dimensión finita como $\mathbb{K}$-espazo vectorial, é dicir, se admite unha base finita. No noso traballo só consideraremos álxebras de tipo finito, e a partir de agora referirémonos a elas simplemente como álxebras.

Un **morfismo de álxebras** entre dúas $\mathbb{K}$-álxebras $\mathcal{A}$ e $\mathcal{A}'$ é unha aplicación $\varphi : \mathcal{A} \to \mathcal{A}'$ que é linear e multiplicativa, ou sexa, $\varphi(xy) = \varphi(x)\varphi(y)$ para todo $x, y \in \mathcal{A}$. Se ademais φ é bixectiva, entón o seu inverso φ^{-1} tamén é linear e multiplicativo, e polo tanto un morfismo de álxebras. Nese caso, dise que φ é un **isomorfismo**. Un **automorfismo** dunha $\mathbb{K}$-álxebra $\mathcal{A}$ é un isomorfismo $\varphi : \mathcal{A} \to \mathcal{A}$. O conxunto de todos os automorfismos de $\mathcal{A}$ é un grupo coa composición de aplicacións e denotámolo por $\mathrm{Aut}(\mathcal{A})$.

Obsérvese que para verificar que unha aplicación $\varphi : \mathcal{A} \to \mathcal{A}'$ é un (iso)morfismo de álxebras, chega con comprobar que é (isomorfismo) linear sobre unha base $B = \{e_i\}$ de $\mathcal{A}$ e que se conserva o produto entre elementos da base (é dicir, $\varphi(e_i e_j) = \varphi(e_i)\varphi(e_j)$ para todo i, j), xa que para o resto de elementos o argumento esténdese por linearidade.

Exemplo 3.1. Algúns exemplos fundamentais son os seguintes:

1. O conxunto $M_n(\mathbb{K})$ das matrices cadradas de orde n con entradas nun corpo $\mathbb{K}$ é unha álxebra asociativa e unitaria coas operacións usuais de suma, produto por escalar e produto matricial.
2. O conxunto $\mathbb{K}[X]$ dos polinomios con coeficientes en $\mathbb{K}$ é unha álxebra asociativa, conmutativa e unitaria coas operacións usuais de suma, produto por escalar e produto entre polinomios.
3. $\mathbb{R}^3$ é unha álxebra non asociativa coas operacións usuais de suma e produto por escalar, mais o produto vectorial. ◇

Exemplo 3.2. Consideramos a álxebra $M_2(\mathbb{R})$ das matrices cadradas de orde 2 reais.

1. A aplicación $\varphi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ definida para cada $A \in M_2(\mathbb{R})$ como $\varphi(A) = A^T$, onde A^T é a trasposta da matriz A, verifica que:

$$\varphi(AB) = (AB)^T = B^T A^T = \varphi(B)\varphi(A).$$

Como non necesariamente $\varphi(B)\varphi(A) = \varphi(A)\varphi(B)$, entón φ non é multiplicativa, e polo tanto non é un morfismo de álxebras.

2. Sexa $P \in M_2(\mathbb{R})$ unha matriz non singular, e consideremos a aplicación $\varphi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ definida para cada $A \in M_2(\mathbb{R})$ como $\varphi(A) = PAP^{-1}$. Está claro que φ é unha aplicación linear, e ademais verifícase que:

$$\varphi(AB) = PABP^{-1} = (PAP^{-1})(PBP^{-1}) = \varphi(A)\varphi(B).$$

Como φ é linear e multiplicativa, entón é un morfismo de álxebras.

Ademais, φ é unha aplicación bixectiva, cuxa inversa está definida para cada $A \in M_2(\mathbb{R})$ como $\varphi^{-1}(A) = P^{-1}AP$. Entón φ é un automorfismo de $M_2(\mathbb{R})$. ◇

Cómpre destacar que a aplicación φ do apartado (1.) do exemplo anterior é un automorfismo linear de $M_2(\mathbb{R})$, é dicir, un automorfismo de $M_2(\mathbb{R})$ como espazo vectorial, a pesar de que non é un automorfismo de álxebras.

Cando falemos dun automorfismo dunha álxebra $\mathcal{A}$, referirémonos a un automorfismo de álxebras de $\mathcal{A}$, e por automorfismo linear de $\mathcal{A}$ entenderemos un automorfismo de $\mathcal{A}$ como espazo vectorial. O exemplo anterior mostra que, en xeral, os automorfismos lineais de $\mathcal{A}$ non son automorfismos de álxebras.

Outro concepto importante é o de *ideal* dunha álxebra. Se $\mathcal{A}$ é unha $\mathbb{K}$-álxebra, un **ideal** de $\mathcal{A}$ é un subespazo vectorial $\mathcal{I}$ que verifica que $\mathcal{A} \cdot \mathcal{I} \subset \mathcal{I}$.

Un exemplo importante de ideal, que será de utilidade na sección 4.1, para tratar os conceptos de conexión e descompoñibilidade en álxebras de evolución, é o seguinte:

Proposición 3.3. *Se $\mathcal{A}$ é unha $\mathbb{K}$-álxebra, entón o conxunto:*

$$\operatorname{ann}(\mathcal{A}) := \{x \in \mathcal{A} : x\mathcal{A} = 0\}$$

*é un ideal de $\mathcal{A}$, e chámase **aniquilador** de $\mathcal{A}$.*

Demostración. Primeiro vexamos que $\operatorname{ann}(\mathcal{A})$ é un subespazo vectorial de $\mathcal{A}$. Dados $x, y \in \operatorname{ann}(\mathcal{A})$ e $\alpha, \beta \in \mathbb{K}$, para calquera $z \in \mathcal{A}$ cúmprese que:

$$(\alpha x + \beta y)z = \alpha xz + \beta yz = 0,$$

e polo tanto $\alpha x + \beta y \in \operatorname{ann}(\mathcal{A})$. Daquela, $\operatorname{ann}(\mathcal{A})$ é un subespazo vectorial de $\mathcal{A}$.

Agora vexamos que $\mathcal{A} \cdot \operatorname{ann}(\mathcal{A}) \subset \mathcal{A}$. Efectivamente, dados $x \in \mathcal{A}$ e $y \in \operatorname{ann}(\mathcal{A})$, para cada $z \in \mathcal{A}$ arbitrario cúmprese que:

$$(xy)z = x(yz) = x \cdot 0 = 0,$$

e polo tanto $xy \in \operatorname{ann}(\mathcal{A})$. Daquela, $\mathcal{A} \cdot \operatorname{ann}(\mathcal{A}) \subset \mathcal{A}$. □

3.2. Álxebras de evolución

Nesta sección introduciremos por fin o concepto fundamental do que trataremos ó longo do resto do noso traballo, e que constitúe o noso principal obxecto de estudo, que é o de *álxebra de evolución*. Primeiro definiremos este e outros conceptos relacionados e ilustrarémolos con exemplos significativos, e despois trataremos a propiedade de *idempotencia*. As definicións e os resultados que veremos ata o final do capítulo están tomados de [5].

Recordemos que todas as álxebras das que tratamos no noso traballo son de tipo finito, aínda que non o indiquemos explicitamente.

3.2.1. Definición e exemplos

Definición 3.4. Unha **álxebra de evolución** sobre un corpo $\mathbb{K}$ é unha $\mathbb{K}$-álxebra $\mathcal{E}$ que admite unha base finita $B = \{e_1, \ldots, e_n\}$ tal que $e_i e_j = 0$ sempre que $i \neq j$. Dicimos que B é unha **base natural** de $\mathcal{E}$.

Observemos que se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$, e $x, y \in \mathcal{E}$ son dous elementos da forma:

$$x = \sum_{i=1}^{n} x_i e_i \quad \text{e} \quad y = \sum_{j=1}^{n} y_j e_j,$$

entón, pola distributividade do produto e a compatibilidade coa multiplicación por escalares:

$$xy = \left(\sum_{i=1}^{n} x_i e_i \right) \left(\sum_{j=1}^{n} y_j e_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \, e_i e_j.$$

Agora ben, como $e_i e_j = 0$ sempre que $i \neq j$, entón a expresión anterior redúcese a:

$$xy = \sum_{i=1}^{n} x_i y_i \, e_i^2.$$

É dicir, o produto de dous elementos arbitrarios de $\mathcal{E}$ redúcese a unha suma de como moito n termos, e depende unicamente dos cadrados dos elementos da base natural. Polo tanto, coñecer as expresións de $e_1^2, \ldots, e_n^2$ permite determinar completamente a estrutura multiplicativa de $\mathcal{E}$. Este feito motiva a seguinte definición:

Definición 3.5. Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$, chamamos **matriz de estrutura asociada a $\mathcal{E}$ relativa á base B** á matriz $M_B(\mathcal{E}) = (\alpha_{ij}) \in \mathcal{M}_n(\mathbb{K})$ determinada polas expresións:

$$e_i^2 = \sum_{j=1}^{n} \alpha_{ij} e_j$$

para cada $i = 1, \ldots, n$.

Observemos que os coeficientes α_{ij} son únicos xa que B é unha base de $\mathcal{E}$, e polo tanto cada elemento e_i^2 se expresa de forma única como combinación linear de $e_1, \ldots, e_n$.

Vexamos un exemplo do cálculo da matriz de estrutura dunha álxebra de evolución:

Exemplo 3.6 (Cálculo da matriz de estrutura)**.** Consideremos a álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ con base natural $B = \{e_1, e_2, e_3\}$ e cuxo produto está determinado por:

$$\begin{aligned} e_1^2 &= e_1 + e_2, \\ e_2^2 &= 2e_2 + 3e_3, \\ e_3^2 &= e_1, \end{aligned}$$

(ademais de $e_i e_j = 0$ se $i \neq j$). A matriz de estrutura de $\mathcal{E}$ relativa á base B é:

$$M_B(\mathcal{E}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 3 \\ 1 & 0 & 0 \end{pmatrix}.$$

Observemos que a matriz $M_B(\mathcal{E})$ é suficiente para determinar a estrutura multiplicativa de $\mathcal{E}$. $\diamond$

Antes de continuar coa seguinte sección, destacamos un feito importante que satisfán os automorfismos das álxebras de evolución, que recollemos na seguinte proposición:

Proposición 3.7. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$ e $\varphi \in \mathrm{Aut}(\mathcal{E})$, entón $\varphi(B) = \{\varphi(e_1), \ldots, \varphi(e_n)\}$ é unha base natural de $\mathcal{E}$.*

Demostración. Como, particularmente, φ é un automorfismo linear de $\mathcal{E}$ (un automorfismo de $\mathcal{E}$ como espazo vectorial) entón $\{\varphi(e_1), \ldots, \varphi(e_n)\}$ será unha base de $\mathcal{E}$. Só falta ver que dita base é natural. Agora ben, como φ satisfai a propiedade multiplicativa, entón, para cada $i \neq j$:

$$\varphi(e_i)\varphi(e_j) = \varphi(e_i e_j) = \varphi(0) = 0$$

que era o que faltaba por demostrar. $\square$

Este feito, que será importante na demostración do corolario 3.19, non se verifica en xeral para automorfismos lineais de $\mathcal{E}$ que non sexan multiplicativos:

Exemplo 3.8. Consideremos a álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3\}$ e produto dado por :

$$\begin{aligned} e_1^2 &= e_2, \\ e_2^2 &= e_1, \\ e_3^2 &= 0. \end{aligned}$$

Sexa $\varphi : \mathcal{E} \to \mathcal{E}$ a aplicación linear determinada por:

$$\begin{aligned}\varphi(e_1) &= e_1 + e_2,\\ \varphi(e_2) &= e_2,\\ \varphi(e_3) &= e_3.\end{aligned}$$

Como $\varphi(B) = \{e_1 + e_2, e_2, e_3\}$ é, trivialmente, unha base de $\mathcal{E}$, entón deducimos que φ é un automorfismo linear de $\mathcal{E}$. Non obstante, φ non é un automorfismo de álxebras de $\mathcal{E}$, xa que non é multiplicativo. Por exemplo:

$$\varphi(e_1)\varphi(e_2) = (e_1 + e_2)e_2 = e_1e_2 + e_2^2 = e_2^2 = e_1 \neq 0 = \varphi(0) = \varphi(e_1e_2)$$

Precisamente, como $\varphi(e_1)\varphi(e_2) \neq 0$, entón $\varphi(B)$ non é unha base natural de $\mathcal{E}$. ◇

3.2.2. Idempotencia

Do mesmo xeito que vimos que o produto nunha álxebra de evolución $\mathcal{E}$ queda completamente determinado pola súa matriz de estrutura, cabe preguntarse que outras propiedades de $\mathcal{E}$ poden describirse ou caracterizarse a partir desta matriz. Este tipo de correspondencias son de especial interese xa que permiten estudar propiedades alxébricas a través de invariantes asociados ás matrices. Un exemplo deste tipo de propiedades é o de *idempotencia*, que introducimos na seguinte definición:

Definición 3.9. Dada unha $\mathbb{K}$-álxebra de evolución $\mathcal{E}$, definimos o seguinte subespazo:

$$\mathcal{E}^2 = \operatorname{span}\{xy : x, y \in \mathcal{E}\}.$$

Diremos que $\mathcal{E}$ é **idempotente** se $\mathcal{E}^2 = \mathcal{E}$.

O seguinte lema presenta unha caracterización máis sinxela do subespazo $\mathcal{E}^2$, que resulta útil para comprobar se unha álxebra de evolución é idempotente:

Lema 3.10. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución e $B = \{e_1, \ldots, e_n\}$ é unha base natural de $\mathcal{E}$, entón:*

$$\mathcal{E}^2 = \operatorname{span}\{e_1^2, \ldots, e_n^2\}.$$

Demostración. Dados dous elementos de $\mathcal{E}$ arbitrarios, $x = \sum_{i=1}^n x_i e_i$ e $y = \sum_{i=1}^n y_i e_i$, sabemos que:

$$xy = \sum_{i=1}^n x_i y_i e_i^2,$$

e consecuentemente $xy \in \text{span}\{e_1^2, \ldots, e_n^2\}$. Deducimos entón que:

$$\{xy : x, y \in \mathcal{E}\} \subset \text{span}\{e_1^2, \ldots, e_n^2\},$$

e daquela:

$$\mathcal{E}^2 = \text{span}\{xy : x, y \in \mathcal{E}\} \subset \text{span}\{e_1^2, \ldots, e_n^2\}.$$

O contido recíproco é trivialmente certo, e polo tanto verifícase a igualdade. □

Fagamos uso do resultado anterior e vexamos algúns exemplos de álxebras de evolución idempotentes e non idempotentes:

Exemplo 3.11 (Álxebra de evolución non idempotente)**.** Consideremos a álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ con base natural $B = \{e_1, e_2, e_3\}$ cuxo produto está determinado por:

$$\begin{aligned} e_1^2 &= e_2, \\ e_2^2 &= 0, \\ e_3^2 &= 0. \end{aligned}$$

Verifícase que

$$\mathcal{E}^2 = \text{span}\{e_1^2,\ e_2^2,\ e_3^2\} = \text{span}\{e_2\},$$

mentres que $\mathcal{E} = \text{span}\{e_1, e_2, e_3\}$. Daquela, $\mathcal{E}^2 \subsetneq \mathcal{E}$, e polo tanto $\mathcal{E}$ non é idempotente. ◇

Exemplo 3.12 (Álxebra de evolución idempotente)**.** Considérese a álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ con base natural $B = \{e_1, e_2\}$ e produto definido por:

$$\begin{aligned} e_1^2 &= e_1 + e_2, \\ e_2^2 &= e_2. \end{aligned}$$

Tense que:

$$\mathcal{E}^2 = \text{span}\{e_1^2, e_2^2\} = \text{span}\{e_1 + e_2, e_2\} = \text{span}\{e_1, e_2\} = \mathcal{E}$$

e polo tanto $\mathcal{E}$ é idempotente. ◇

Na seguinte proposición, que reformula a observación [5, Remark 4.2], presentamos unha caracterización da idempotencia dunha álxebra de evolución en termos da súa matriz de estrutura:

Proposición 3.13. *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$ e matriz de estrutura $M_B(\mathcal{E})$. As seguintes afirmacións son equivalentes:*

1. *$\mathcal{E}$ é idempotente, é dicir, $\mathcal{E}^2 = \mathcal{E}$.*
2. *O conxunto $\{e_1^2, \ldots, e_n^2\}$ é unha base de $\mathcal{E}$.*

3. A matriz $M_B(\mathcal{E})$ é non singular.

Demostración. (1. $\implies$ 2.) Supoñamos que $\mathcal{E}^2 = \mathcal{E}$. Polo lema 3.10, entón $\mathcal{E} = \text{span}\{e_1^2, \ldots, e_n^2\}$, é dicir, $\{e_1^2, \ldots, e_n^2\}$ é un conxunto de xeradores de $\mathcal{E}$. Agora ben, como o conxunto $\{e_1^2, \ldots, e_n^2\}$ consta de n elementos e $\dim_{\mathbb{K}}(\mathcal{E}) = n$, entón esa condición é suficiente para garantir que $\{e_1^2, \ldots, e_n^2\}$ é unha base de $\mathcal{E}$.

(2. $\implies$ 1.) Supoñamos que $\{e_1^2, \ldots, e_n^2\}$ é unha base de $\mathcal{E}$. Como a inclusión $\mathcal{E}^2 \subset \mathcal{E}$ sempre se satisfai, entón só falta ver que $\mathcal{E} \subset \mathcal{E}^2$. Sexa x un elemento arbitrario de $\mathcal{E}$. Como $\{e_1^2, \ldots, e_n^2\}$ é unha base de $\mathcal{E}$, entón x pode expresarse como $x = \sum_{i=1}^n x_i e_i^2$ para certos coeficientes $x_1, \ldots, x_n \in \mathbb{K}$. Observemos que:

$$x = \left(\sum_{i=1}^n x_i e_i\right) \cdot \left(\sum_{j=1}^n e_j\right),$$

xa que $e_i e_j = 0$ sempre que $i \neq j$. Polo tanto x é un elemento de $\mathcal{E}^2$. Concluímos que $\mathcal{E}^2 = \mathcal{E}$, como queriamos ver.

(2. $\iff$ 3.) Como $\dim_{\mathbb{K}}(\mathcal{E}) = n$ e o conxunto $\{e_1^2, \ldots, e_n^2\}$ consta de n elementos, entón $\{e_1^2, \ldots, e_n^2\}$ será unha base de $\mathcal{E}$ se, e só se, é un conxunto linealmente independente. Isto é equivalente a que a matriz $M_B(\mathcal{E})$, cuxas filas son coordenadas dos elementos $e_1^2, \ldots, e_n^2$ respecto a base B, sexa non singular. □

A proposición anterior proporciona un criterio sinxelo para comprobar se unha álxebra de evolución é idempotente sen máis que observar a súa matriz de estrutura. Vexamolo no seguinte exemplo:

Exemplo 3.14 (Matrices de estrutura dos exemplos anteriores)**.** A matriz de estrutura do exemplo 3.11 é

$$M_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

que ten determinante nulo. Polo tanto, a álxebra de evolución asociada non é idempotente.

Por outra parte, a matriz de estrutura do exemplo 3.12 é

$$M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

que ten determinante non nulo. Daquela, a álxebra de evolución asociada é idempotente. ◇

A continuación veremos que as álxebras de evolución idempotentes posúen, esencialmente, unha única base natural. Máis concretamente, demostraremos que se unha álxebra de evolución

idempotente admite dúas bases naturais, entón ambas coinciden agás por unha permutación dos seus elementos e a multiplicación de cada un por un escalar non nulo. Antes diso, debemos introducir a noción de *soporte*:

Definición 3.15. Sexan $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución e $B = \{e_1, \ldots, e_n\}$ unha base natural de $\mathcal{E}$, e sexa x un elemento de $\mathcal{E}$. Supoñamos que $x = \sum_{i=1}^{n} x_i e_i$. Chamamos **soporte do elemento x na base B** ó conxunto de índices:

$$sop_B(x) := \{i \in \{1, \ldots, n\} : x_i \neq 0\}.$$

Reformulamos a observación [5, Remark 4.3] no seguinte lema:

Lema 3.16. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e $x, y \in \mathcal{E}$ son elementos tales que $xy = 0$, entón $sop_B(x) \cap sop_B(y) = \emptyset$.*

Demostración. Supoñamos que $x = \sum_{i=1}^{n} x_i e_i$ e $y = \sum_{i=1}^{n} y_i e_i$. Tense que:

$$0 = xy = \sum_{i=1}^{n} x_i y_i e_i^2.$$

Agora ben, como $\mathcal{E}^2 = \mathcal{E}$ entón os elementos $\{e_1^2, \ldots, e_n^2\}$ son linearmente independentes e polo tanto $x_i y_i = 0$ para todo $i = 1, \ldots, n$. Entón, para cada $i = 1, \ldots, n$, $x_i = 0$ ou $y_i = 0$, de onde $sop_B(x) \cap sop_B(y) = \emptyset$. □

A condición de que $\mathcal{E}$ sexa idempotente é esencial para garantir o resultado anterior. Se suprimimos esa condición, entón o lema deixa de ser válido, como pon de manifesto o seguinte exemplo:

Exemplo 3.17. Consideremos a álxebra de evolución $\mathcal{E}$ sobre un corpo $\mathbb{K}$ con base natural $B = \{e_1, e_2, e_3\}$ e cuxo produto está definido por:

$$\begin{aligned} e_1^2 &= e_2, \\ e_2^2 &= e_3, \\ e_3^2 &= 0. \end{aligned}$$

Observemos que $\mathcal{E}$ non é idempotente, xa que:

$$\mathcal{E}^2 = \operatorname{span}\{e_1^2, e_2^2, e_3^2\} = \{e_2, e_3\} \subsetneq \mathcal{E}.$$

Agora consideremos os elementos $x = e_1 + e_3$ e $y = e_2 + e_3$. Verifícase que:

$$xy = (e_1 + e_3)(e_2 + e_3) = e_1e_2 + e_1e_3 + e_3e_2 + e_3^2 = e_3^2 = 0,$$

pero non obstante, $sop_B(x) \cap sop_B(y) = \{e_3\} \neq \emptyset$. ◇

O lema 3.16 permítenos probar o seguinte teorema, que afirma, como anticipamos antes, que as álxebras de evolución idempotentes teñen unha única base natural agás permutacións e multiplicación por escalares non nulos.

Teorema 3.18. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución idempotente e $B = \{e_1, \dots, e_n\}$ e $B' = \{f_1, \dots, f_n\}$ son dúas bases naturais de $\mathcal{E}$, entón existen unha única permutación $\sigma \in S_n$ e escalares non nulos $\mu_1, \dots, \mu_n \in \mathbb{K}^\times$ tales que $f_i = \mu_i e_{\sigma(i)}$ para cada $i = 1, \dots, n$.*

Demostración. Primeiro probaremos a existencia. Para cada $i, j = 1, \dots, n$, $i \neq j$, tense que $f_i f_j = 0$, e polo lema 3.16 entón:

$$sop_B(f_i) \cap sop_B(f_j) = \emptyset.$$

Ou sexa, os conxuntos de índices $\{sop_B(f_i)\}_{i=1}^n$ son disxuntos dous a dous, e ademais son non baleiros, xa que cada f_i é un elemento non nulo de $\mathcal{E}$. Necesariamente, o soporte de cada elemento f_i consta dun único elemento distinto de $\{1, \dots, n\}$. Entón existirá unha permutación $\sigma \in S_n$ tal que $sop_B(f_i) = \{\sigma(i)\}$ para todo $i = 1, \dots, n$, e daquela $f_i = \mu_i e_{\sigma(i)}$ para algún $\mu_i \in \mathbb{K}^\times$.

Para probar a unicidade, supoñamos que $\tau \in S_n$ e $\lambda_1, \dots, \lambda_n \in \mathbb{K}^\times$ tamén son tales que $f_i = \lambda_i e_{\tau(i)}$ para cada $i = 1, \dots, n$. Entón, dado $i = 1, \dots, n$:

$$\mu_i e_{\sigma(i)} = f_i = \lambda_i e_{\tau(i)}.$$

Como $\{e_1, \dots, e_n\}$ é un conxunto linearmente independente, entón deducimos que $\sigma(i) = \tau(i)$ e $\mu_i = \lambda_i$. Como isto é certo para cada $i = 1, \dots, n$, entón $\sigma = \tau$. □

Unha importante consecuencia do teorema anterior é o seguinte corolario, que establece unha propiedade fundamental do grupo de automorfismos dunha álxebra de evolución idempotente, e que consitúé un dos piares básicos da teoría que desenvolveremos no capítulo seguinte. En termos xerais, este resultado establece unha relación entre os automorfismos dunha álxebra de evolución idempotente n-dimensional e o grupo das permutacións de n elementos. No capítulo seguinte exploraremos en profundidade esta relación.

Corolario 3.19. *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \dots, e_n\}$, e sexa $\varphi \in \mathrm{Aut}(\mathcal{E})$. Entón existe unha única permutación $\sigma \in S_n$ tal que $\varphi(e_i) \in \mathbb{K}^\times e_{\sigma(i)}$ para cada $i = 1, \dots, n$.*

Demostración. Se φ é un automorfismo de $\mathcal{E}$, entón $\varphi(B) = \{\varphi(e_1), \dots, \varphi(e_n)\}$ é unha base natural de $\mathcal{E}$ en virtude da proposición 3.7, e o resultado dedúcese inmediatamente a partir do teorema anterior. □

Capítulo 4

Álxebras de evolución vía grafos: estrutura e automorfismos

Neste capítulo introduciremos o concepto de grafo asociado a unha álxebra de evolución $\mathcal{E}$ relativo a unha base natural, unha importante ferramenta que nos permitirá estudar as propiedades das álxebras de evolución idempotentes a través de grafos asociados a elas, valéndonos da teoría desenvolvida nos capítulos anteriores.

Concretamente, na sección 4.1 presentaremos o concepto de *descompoñibilidade* dunha álxebra de evolución, e veremos que está estreitamente relacionado coa conectividade do seu grafo asociado no caso das álxebras de evolución idempotentes, a diferenza do que sucede para as non idempotentes, como ilustraremos a continuación cun exemplo significativo. Posteriormente, na sección 4.2 demostraremos unha serie de resultados que nos permitirán estudar o grupo de automorfismos dunha álxebra de evolución idempotente a través do seu grafo asociado, e na sección 4.3, aplicaremos estes resultados a unha clase concreta de álxebras de evolución idempotentes cuxo grupo de automorfismos satisfai certa condición de transitividade, ilustrando algunha das aplicacións desta teoría.

A seguinte definición e os resultados teóricos do capítulo están tomados de [5] e [6]. Na maior parte dos casos, adaptaremos as demostracións orixinais ó noso contexto para facilitar a presentación e o desenvolvemento do traballo.

Definición 4.1. Sexan $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$ e (α_{ij}) a matriz de estrutura asociada a $\mathcal{E}$ relativa a dita base. Definimos o **grafo asociado a $\mathcal{E}$ relativo á base B** como o grafo $\Gamma(\mathcal{E}, B) = (V, E)$ dado por:

$$V := \{1, \ldots, n\} \quad \text{e} \quad E := \{(i, j) \in V \times V : \alpha_{ij} \neq 0\}.$$

Antes de presentar os resultados teóricos deste capítulo, ilustremos a noción que acabamos de introducir con algúns exemplos sinxelos, que nos suxerirán a conveniencia de traballar con álxebras de evolución idempotentes.

En primeiro lugar, sería desexable que a conectividade do grafo asociado a unha álxebra de evolución $\mathcal{E}$ non dependese da base natural escollida, é dicir, que ou ben o grafo asociado a $\mathcal{E}$ relativo a calquera base natural fose conexo, ou ben non fose conexo para ningunha base natural de $\mathcal{E}$. Na sección 4.1 veremos que este é o caso para as álxebras de evolución idempotentes, a diferenza do que sucede se suprimimos a condición de idempotencia, como revela o seguinte exemplo:

Exemplo 4.2 (Conexión de grafos en álxebras de evolución non idempotentes)**.** Sexa $\mathcal{E}$ a $\mathbb{K}$-álxebra de evolución que admite a base natural $B = \{e_1, e_2, e_3\}$ e cuxo produto vén dado por:

$$\begin{aligned} e_1^2 &= e_2 + e_3, \\ e_2^2 &= 0, \\ e_3^2 &= 0. \end{aligned}$$

Observemos que $\mathcal{E}$ non é idempotente xa que:

$$\mathcal{E}^2 = \operatorname{span}\{e_1^2,\ e_2^2,\ e_3^2\} = \operatorname{span}\{e_2 + e_3\} \subsetneq \operatorname{span}\{e_1, e_2, e_3\} = \mathcal{E}.$$

O grafo asociado a $\mathcal{E}$ relativo á base B, representado na figura 4.1, é claramente conexo.

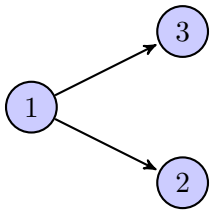

Figura 4.1: Grafo $\Gamma(\mathcal{E}, B)$ do exemplo 4.2

Agora consideremos a base de $\mathcal{E}$ $B' = \{f_1 = e_1, f_2 = e_2 + e_3, f_3 = e_3\}$. Verifícase que B' é natural, xa que:

$$\begin{aligned} f_1 f_2 &= e_1(e_2 + e_3) = e_1e_2 + e_1e_3 = 0 + 0 = 0, \\ f_1 f_3 &= e_1e_3 = 0, \\ f_2 f_3 &= (e_2 + e_3)e_3 = e_2e_3 + e_3^2 = e_3^2 = 0. \end{aligned}$$

Ademais:

$$f_1^2 = f_2,$$
$$f_2^2 = 0,$$
$$f_3^2 = 0.$$

Claramente, o grafo asociado a $\mathcal{E}$ relativo á base B', representado na figura 4.2, non é conexo.

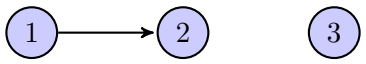

Figura 4.2: Grafo $\Gamma(\mathcal{E}, B')$ do exemplo 4.2

$\diamond$

Os seguintes exemplos mostran outra importante propiedade que satisfán as álxebras evolución idempotentes, e que tampouco se verifica se suprimimos a condición de idempotencia. Trátase de que os grafos asociados ás álxebras de evolución idempotentes non teñen fontes, como demostraremos na sección 4.2. Este feito, aparentemente trivial, resulta ser moi conveniente, e será crucial para demostrar a finitude do grupo de automorfismos dunha álxebra de evolución idempotente.

Exemplo 4.3 (Grafo asociado a unha álxebra de evolución idempotente)**.** Consideremos a $\mathbb{K}$-álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3\}$ cuxo produto está dado por:

$$e_1^2 = e_2 + e_3,$$
$$e_2^2 = e_3,$$
$$e_3^2 = e_1.$$

Observemos que $\mathcal{E}$ é idempotente, xa que $\{e_1^2, e_2^2, e_3^2\} = \{e_2 + e_3, e_3, e_1\}$ é trivialmente unha base de $\mathcal{E}$, e o grafo asociado a $\mathcal{E}$ relativo á base B, representado na figura 4.3, non ten fontes. $\diamond$

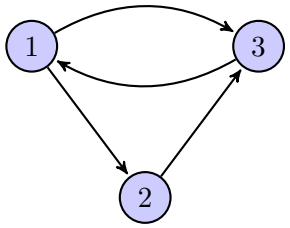

Figura 4.3: Grafo do exemplo 4.3.

Exemplo 4.4 (Grafo asociado a unha álxebra de evolución non idempotente)**.** Consideremos a $\mathbb{K}$-álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3\}$ cuxo produto está dado por:

$$e_1^2 = e_3,$$
$$e_2^2 = e_3,$$
$$e_3^2 = e_1.$$

Observemos que $\mathcal{E}$ non é idempotente, xa que $\{e_1^2, e_2^2, e_3^2\} = \{e_1, e_3\}$ non é unha base de $\mathcal{E}$, e o grafo asociado a $\mathcal{E}$ relativo á base B, representado na figura 4.4, si ten unha fonte, o vértice 2. $\diamond$

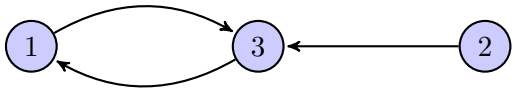

Figura 4.4: Grafo do exemplo 4.4.

4.1. Estructura das álxebras de evolución: descompoñibilidade

Como xa anticipamos na introdución do capítulo, esta sección está dedicada a estudar o concepto de *descompoñibilidade* en álxebras de evolución, mais a súa relación coa conectividade do seu grafo asociado relativo a unha base natural. Na seguinte definición formulamos de maneira precisa este concepto:

Definición 4.5. Unha $\mathbb{K}$-álxebra de evolución $\mathcal{E}$ dise **descompoñible** se existen $\mathcal{I}$ e $\mathcal{J}$ dous ideais non nulos de $\mathcal{E}$ tales que $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$. Se $\mathcal{E}$ non é descompoñible, entón dise que é **indescompoñible**.

O seguinte teorema presenta, parcialmente, a relación que existe entre a descompoñibilidade dunha álxebra de evolución e a conectividade do seu grafo asociado:

Teorema 4.6. *Sexan $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución e $B = \{e_1, \ldots, e_n\}$ unha base natural arbitraria. Se $\mathcal{E}$ é indescompoñible, entón $\Gamma(\mathcal{E}, B)$ é conexo.*

Demostración. Supoñamos que $\Gamma(\mathcal{E}, B)$ non é conexo e vexamos que entón $\mathcal{E}$ é descompoñible.

Como $\Gamma(\mathcal{E}, B)$ non é conexo, entón existirá unha partición $\{I, J\}$ do conxunto de vértices $V = \{1, \ldots, n\}$ formada por dous conxuntos non baleiros I e J tales que ningunha aresta de $\Gamma(\mathcal{E}, B)$ conecta un nodo de I cun nodo de J. Se (α_{ij}) é a matriz de estrutura de $\mathcal{E}$ relativa á base B, entón a condición anterior equivale a dicir que $\alpha_{ij} = 0 = \alpha_{ji}$ sempre que $i \in I$ e $j \in J$.

Sexan $\mathcal{I} = \operatorname{span}\{e_i : i \in I\}$ e $\mathcal{J} = \operatorname{span}\{e_j : j \in J\}$, e vexamos que $\mathcal{I}$ e $\mathcal{J}$ son ideais non nulos de $\mathcal{E}$ tales que $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$.

- *$\mathcal{I}$ e $\mathcal{J}$ son ideais de $\mathcal{E}$.* Só probaremos que $\mathcal{I}$ é un ideal de $\mathcal{E}$, xa que a demostración para $\mathcal{J}$ sería análoga.

  Por construción, $\mathcal{I}$ é un subespazo vectorial de $\mathcal{E}$, e polo tanto só falta por comprobar que $\mathcal{E}\cdot\mathcal{I}\subset\mathcal{I}$. Agora, dados $x=\sum_{i=1}^{n}x_ie_i\in\mathcal{E}$ e $y=\sum_{i\in I}y_ie_i\in\mathcal{I}$ arbitrarios, tense que:

$$\begin{aligned}xy&=(\sum_{i=1}^{n}x_ie_i)(\sum_{i\in I}y_ie_i)\\&=\sum_{i\in I}x_iy_ie_i^2\\&=\sum_{i\in I}x_iy_i(\sum_{j=1}^{n}\alpha_{ij}e_j)\\&\overset{(*)}{=}\sum_{i\in I}x_iy_i(\sum_{j\in I}\alpha_{ij}e_j)\\&=\sum_{j\in I}(\sum_{i\in I}x_iy_i\alpha_{ij})e_j,\end{aligned}$$

  onde en $(*)$ utilizamos o feito de que $\alpha_{ij}=0$ se $j\in J$, ou sexa, se $j\notin I$. Da expresión anterior deducimos que $xy\in\mathcal{I}$, e concluímos que $\mathcal{E}\cdot\mathcal{I}\subset\mathcal{I}$, que era o que tiñamos que probar.

- *$\mathcal{I}$ e $\mathcal{J}$ son non nulos.* Efectivamente, como $I\neq\emptyset$, entón o conxunto $\{e_i : i\in I\}$ é non baleiro, e como $\mathcal{I}=\text{span}\{e_i : i\in I\}$, daquela $\mathcal{I}\neq 0$. Analogamente, $\mathcal{J}\neq 0$.

- *Vexamos que $\mathcal{E}=\mathcal{I}\oplus\mathcal{J}$.* Claramente:

$$\begin{aligned}\mathcal{E}&=\text{span}e_i : i=1,\dots,n\}\\&=\text{span}\{\{e_i : i\in I\}\cup\{e_j : j\in J\}\}\\&=\text{span}\{\{e_i : i\in I\}\}+\text{span}\{\{e_j : j\in J\}\}\\&=\mathcal{I}+\mathcal{J}.\end{aligned}$$

  Polo tanto, só falta ver que $\mathcal{I}\cap\mathcal{J}=0$. Efectivamente, se $x\in\mathcal{I}\cap\mathcal{J}$, entón existen escalares $\{x_i\}_{i\in I}\subset\mathbb{K}$ e $\{x'_j\}_{j\in J}\subset\mathbb{K}$ tales que:

$$\sum_{i\in I}x_ie_i=x=\sum_{j\in J}x'_je_j,$$

  e polo tanto:

$$\sum_{i\in I}x_ie_i-\sum_{j\in J}x'_je_j=0.$$

  Mais como $\{e_1,\dots,e_n\}=\{e_i : i\in I\}\cup\{e_j : j\in J\}$ (unión disxunta) é un conxunto linearmente independente, entón deducimos que $x_i=0$ para todo $i\in I$ e $x'_j=0$ para todo $j\in J$, de xeito que $x=0$.

Como $\mathcal{I}$ e $\mathcal{J}$ son ideais non nulos de $\mathcal{E}$ tales que $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$, entón $\mathcal{E}$ é descompoñible. □

En xeral, o recíproco deste teorema non é certo: a conectividade do grafo asociado a unha álxebra de evolución $\mathcal{E}$ non é suficiente para garantir a súa indescompoñibilidade. Con todo, no teorema 4.8 veremos que isto si se verifica baixo a hipótese adicional de que o aniquilador de $\mathcal{E}$ sexa nulo. Recordemos que o aniquilador dunha álxebra arbitraria $\mathcal{A}$ é o ideal:

$$\operatorname{ann}(\mathcal{A}) = \{x \in \mathcal{A} : x\mathcal{A} = 0\}.$$

Para o caso das álxebras de evolución, temos a seguinte caracterización máis sinxela:

Proposición 4.7. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución con base natural $B = \{e_1, \ldots, e_n\}$, entón:*

$$\operatorname{ann}(\mathcal{E}) = \operatorname{span}\{e_i : e_i^2 = 0\}.$$

Demostración. ($\supset$) Se e_i é tal que $e_i^2 = 0$, entón, dado un elemento $x = \sum_{j=1}^n x_j e_j \in \mathcal{E}$ arbitrario:

$$e_i x = \sum_{j=1}^n x_j e_i e_j = x_i e_i^2 = 0,$$

e polo tanto $e_i \in \operatorname{ann}(\mathcal{E})$. Daquela, $\operatorname{span}\{e_i : e_i^2 = 0\} \subset \operatorname{ann}(\mathcal{E})$.

($\subset$) Dado un elemento $x = \sum_{j=1}^n x_j e_j \in \operatorname{ann}(\mathcal{E})$ arbitrario, para cada $i = 1, \ldots, n$ terase que:

$$0 = x e_i = \sum_{j=1}^n x_j e_j e_i = x_i e_i^2.$$

Se $x_i \neq 0$, entón $e_i^2 = 0$, e polo tanto os escalares non nulos na expresión $\sum_{j=1}^n x_j e_j$ corresponden a elementos de $\{e_i : e_i^2 = 0\}$. É dicir, x é unha combinación linear de $\{e_i : e_i^2 = 0\}$, e consecuentemente, $x \in \operatorname{span}\{e_i : e_i^2 = 0\}$. □

O seguinte resultado complementa o teorema 4.6:

Teorema 4.8. *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución tal que* $\operatorname{ann}(\mathcal{E}) = 0$*, e sexa $B = \{e_1, \ldots, e_n\}$ unha base natural de $\mathcal{E}$ tal que $\Gamma(\mathcal{E}, B)$ é conexo. Entón $\mathcal{E}$ é indescompoñible.*

Demostración. Supoñamos que $\mathcal{E}$ é descompoñible e vexamos que entón $\Gamma(\mathcal{E}, B)$ non é conexo.

Como $\mathcal{E}$ é descompoñible, entón existen dous ideais non nulos $\mathcal{I}, \mathcal{J}$ tales que $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$. Para cada $i = 1, \ldots, n$, existirán dous elementos $e_i' \in \mathcal{I}$ e $e_i'' \in \mathcal{J}$ tales que $e_i = e_i' + e_i''$. Sexan $I = \{i \in \{1, \ldots, n\} : e_i' \neq 0\}$ e $J = \{j \in \{1, \ldots, n\} : e_j'' \neq 0\}$. Imos ver que I e J son conxuntos non baleiros e forman unha partición de $\{1, \ldots, n\}$ de xeito tal que os vértices de $\Gamma(\mathcal{E}, B)$ contidos en I non están conectados con aqueles contidos en J.

- *Vexamos que* $I \cup J = \{1, \ldots, n\}$. Dado $i = 1, \ldots, n$ tense que:

$$0 \neq e_i = e'_i + e''_i.$$

e polo tanto, $e'_i \neq 0$ ou $e''_i \neq 0$, é dicir, $i \in I$ ou $i \in J$. Deducimos entón que $I \cup J = \{1, \ldots, n\}$.

- *A unión* $I \cup J$ *é disxunta.* En primeiro lugar observemos que se $i \neq j$, entón:

$$\begin{aligned} 0 = e_i e_j &= (e'_i + e''_i)(e'_j + e''_j) \\ &= e'_i e'_j + e'_i e''_j + e''_i e'_j + e''_i + e''_j. \end{aligned}$$

Por ser $e'_i e''_j, e''_i e'_j \in \mathcal{I} \cap \mathcal{J} = 0$, a expresión anterior redúcese a:

$$0 = e'_i e'_j + e''_i e''_j.$$

Como $e'_i e'_j \in \mathcal{I}$ e $e''_i e''_j \in \mathcal{J}$, e tendo en conta que a suma $\mathcal{I} \oplus \mathcal{J}$ é directa, deducimos que $e'_i e'_j = 0$ e $e''_i e''_j = 0$. Ou sexa, $e'_i e'_j = 0$ e $e''_i e''_j = 0$ sempre que $i \neq j$.

Utilizando este feito, imos ver que o conxunto $B_{\mathcal{I}} := \{e_i : i \in I\}$ é unha base de $\mathcal{I}$.

Primeiro probaremos que $B_{\mathcal{I}}$ é un conxunto de xeradores de $\mathcal{I}$. Sexa $x \in \mathcal{I}$ e supoñamos que $x = \sum_{i=1}^{n} x_i e_i$. Entón:

$$x = \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} x_i e'_i + \sum_{i=1}^{n} x_i e''_i,$$

onde x e $\sum_{i=1}^{n} x_i e'_i$ son elementos de $\mathcal{I}$ e $\sum_{i=1}^{n} x_i e''_i$ é un elemento de $\mathcal{J}$. Como a suma $\mathcal{I} \oplus \mathcal{J}$ é directa, deducimos que $\sum_{i=1}^{n} x_i e''_i = 0$, e ademais:

$$x = \sum_{i=1}^{n} x_i e'_i = \sum_{i \in I} x_i e'_i.$$

Daquela, $x \in \operatorname{span}\{e'_i : i \in I\}$, como queriamos ver.

Agora veremos que $B_{\mathcal{I}}$ é un conxunto de elementos linearmente independentes. Razoaremos por redución ó absurdo. Supoñamos que os elementos $\{e'_i : i \in I\}$ non fosen linearmente independentes: entón existirían un índice $i \in I$ e escalares $\{\lambda_j\}_{\substack{j \in I \\ j \neq i}} \subset \mathbb{K}$ tales que $e'_i = \sum_{\substack{j \in I \\ j \neq i}} \lambda_j e'_j$. Como $e'_i e'_j = 0$ se $j \neq i$, entón:

$$e'^2_i = \sum_{\substack{j \in I \\ j \neq i}} \lambda_j e'_j e'_i = 0.$$

Deducimos que, para cada elemento $x = \sum_{j=1}^{n} x_j e_j \in \mathcal{E}$ arbitrario:

$$\begin{aligned} e_i' x &= e_i' \sum_{j=1}^{n} x_j e_j \\ &= e_i' \sum_{j=1}^{n} x_j e_j' + e_i' \sum_{j=1}^{n} x_j e_j'' \\ &= \sum_{j=1}^{n} x_j e_i' e_j' + \sum_{j=1}^{n} x_j e_i' e_j'' \\ &\overset{(*^1)}{=} \sum_{j=1}^{n} x_j e_i' e_j' \\ &\overset{(*^2)}{=} x_i e_i'^2 \\ &= x_i \cdot 0 \\ &= 0, \end{aligned}$$

onde a igualdade $(*^1)$ é consecuencia de que $e_i' e_j'' \in \mathcal{I} \cap \mathcal{J} = 0$ para cada $j = 1, \ldots, n$ e $(*^2)$ derívase de que $e_i' e_j' = 0$ sempre que $i \neq j$. Acabamos de ver que $e_i' \mathcal{E} = 0$, e polo tanto $e_i' \in \operatorname{ann}(\mathcal{E}) = 0$. Entón $e_i' = 0$, contradicindo o feito de que $i \in I$. Deducimos que os elementos $\{e_i' : i \in I\}$ deben ser linearmente independentes.

Analogamente pode demostrarse que o conxunto $B_{\mathcal{J}} := \{e_j : j \in J\}$ é unha base de $\mathcal{J}$. Particularmente:

$$n = \dim_{\mathbb{K}} \mathcal{E} = \dim_{\mathbb{K}} \mathcal{I} + \dim_{\mathbb{K}} \mathcal{J} = \#B_{\mathcal{I}} + \#B_{\mathcal{J}} = |I| + |J|.$$

Como I e J son tales que $I \cup J = \{1, \ldots, n\}$ e $|I| + |J| = n$, entón os conxuntos I e J deben ser necesariamente disxuntos. É dicir, a unión $I \cup J$ é disxunta, como tiñamos que ver.

Do razoamento anterior deducimos en particular que $e_i' = 0$ sempre que $e_i'' \neq 0$, e reciprocamente, $e_i' \neq 0$ sempre que $e_i'' = 0$. Polo tanto, para cada $i = 1, \ldots, n$, ou ben $e_i = e_i'$ (se $i \in I$), ou ben $e_i = e_i''$ (no caso de que $i \in J$). Daquela, $B = B_{\mathcal{I}} \cup B_{\mathcal{J}}$ (unión disxunta).

- *I e J son non baleiros.* Se o conxunto I fose baleiro, entón teríamos que $B = B_{\mathcal{J}}$, e polo tanto $\mathcal{E} = \mathcal{J}$ e $\mathcal{I} = 0$, contradecindo a hipótese de que o ideal $\mathcal{I}$ era non nulo. Necesariamente, I debe ser non baleiro, e analogamente poderiamos demostrar que J tampouco é baleiro.

- *Os vértices de $\Gamma(\mathcal{E}, B)$ contidos en I non están conectados cos de J.* Denotemos por (α_{ij})

a matriz de estrutura asociada a $\mathcal{E}$ relativa á base B. Se $i \in I$ entón $e_i = e'_i$, e ademais:

$$\begin{aligned} e_i^2 &= \sum_{j=1}^{n} \alpha_{ij} e_j \\ &= \sum_{j \in I} \alpha_{ij} e_j + \sum_{j \in J} \alpha_{ij} e_j, \end{aligned}$$

sendo $e_i^2 = e_i'^2$ e $\sum_{j\in I} \alpha_{ij} e_j$ elementos de $\mathcal{I}$ e $\sum_{j\in J} \alpha_{ij} e_j$ un elemento de $\mathcal{J}$. Como a suma $\mathcal{I} \oplus \mathcal{J}$ é directa, entón deducimos que $e_i^2 = \sum_{j\in I} \alpha_{ij} e_j$ e asemade:

$$\sum_{j \in J} \alpha_{ij} e_j = 0.$$

Como os elementos $\{e_j : j \in J\}$ son linearmente independentes, entón deducimos que $\alpha_{ij} = 0$ para todo $j \in J$.

Acabamos de ver que $\alpha_{ij} = 0$ sempre que $i \in I$ e $j \in J$. Ou sexa, se $i \in I$ e $j \in J$, entón o par (i, j) non é unha aresta de $\Gamma(\mathcal{E}, B)$. Un argumento análogo proba tamén que, se $i \in I$ e $j \in J$, entón (j, i) tampouco é unha aresta de $\Gamma(\mathcal{E}, B)$.

Como $\{I, J\}$ é unha partición non trivial dos vértices de $\Gamma(\mathcal{E}, B)$ de xeito tal que ningunha aresta do grafo conecta un nodo de I cun nodo de J, entón non pode existir ningún camiño entre os nodos de $\Gamma(\mathcal{E}, B)$ contidos en I e aqueles contidos en J. Polo tanto, $\Gamma(\mathcal{E}, B)$ non é conexo. □

Insistimos en que o teorema anterior non é válido se suprimimos a hipótese $\operatorname{ann}(\mathcal{E}) = 0$, como se pode ver no seguinte exemplo, que retoma o caso do exemplo 4.2:

Exemplo 4.9 (Exemplo 4.2 revisitado)**.** Vimos que a álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3\}$ cuxo produto está dado por:

$$\begin{aligned} e_1^2 &= e_2 + e_3, \\ e_2^2 &= 0, \\ e_3^2 &= 0, \end{aligned}$$

admite outra base natural B' tal que $\Gamma(\mathcal{E}, B)$ é un grafo conexo mentres que $\Gamma(\mathcal{E}, B')$ non o é. Como $\Gamma(\mathcal{E}, B')$ non é conexo, deducimos do teorema 4.6 que $\mathcal{E}$ é descompoñible.

Trátase pois dun exemplo de álxebra de evolución descompoñible que admite unha base natural cuxo grafo asociado relativo a dita base si é conexo. Isto débese, precisamente, a que $\operatorname{ann}(\mathcal{E}) \neq 0$. Efectivamente, pola proposición 4.7:

$$\operatorname{ann}(\mathcal{E}) = \operatorname{span}\{e_i : e_i^2 = 0\} = \operatorname{span}\{e_2, e_3\} \neq 0,$$

e polo tanto non se garanten as hipóteses do teorema 4.8. ◇

Convenientemente, a condición $\operatorname{ann}(\mathcal{E}) = 0$ sempre verifica no caso das álxebras de evolución idempotentes, como establece a seguinte proposición:

Proposición 4.10. *Se $\mathcal{E}$ é unha álxebra de evolución idempotente, entón* $\operatorname{ann}(\mathcal{E}) = 0$.

Demostración. Sexa $B = \{e_1, \ldots, e_n\}$ unha base natural de $\mathcal{E}$. Como $\mathcal{E}^2 = \mathcal{E}$, entón $\{e_1^2, \ldots, e_n^2\}$ é unha base de $\mathcal{E}$. Entón $e_i^2 \neq 0$ para todo $i = 1, \ldots, n$, e polo tanto, grazas á proposición 4.7 podemos escribir:

$$\operatorname{ann}(\mathcal{E}) = \operatorname{span}\{e_i : e_i^2 = 0\} = 0$$

que era o que queriamos probar. □

Os teoremas 4.6 e 4.8, mais a proposición anterior, permiten probar a seguinte equivalencia para o caso de álxebras de evolución idempotentes:

Teorema 4.11. *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución idempotente. Entón son equivalentes:*

1. *$\mathcal{E}$ é indescompoñible.*
2. *$\Gamma(\mathcal{E}, B)$ é conexo para algunha base natural B de $\mathcal{E}$.*
3. *$\Gamma(\mathcal{E}, B)$ é conexo para calquera base natural B de $\mathcal{E}$.*

Demostración. (1. $\implies$ 3.) Dada B unha base natural arbitraria de $\mathcal{E}$, $\Gamma(\mathcal{E}, B)$ será conexo polo teorema 4.6.

(3. $\implies$ 2.) Trivial.

(2. $\implies$ 1.) Como $\operatorname{ann}(\mathcal{E}) = 0$ e $\Gamma(\mathcal{E}, B)$ é conexo para certa base natural B de $\mathcal{E}$, entón $\mathcal{E}$ será indescompoñible grazas ó teorema 4.8. □

Do teorema anterior deducimos que se $\mathcal{E}$ é unha álxebra de evolución idempotente, entón, ou ben o seu grafo asociado relativo a calquera base natural é conexo, ou ben non é conexo para ningunha base natural de $\mathcal{E}$.

4.2. Automorfismos das álxebras de evolución: finitude

Nesta sección desenvolveremos a teoría que nos permitirá estudar o grupo de automorfismos das álxebras de evolución idempotentes a partir das propiedades dos seus grafos asociados. Recordemos que por $\operatorname{Aut}(\mathcal{E})$ denotamos o grupo dos automorfismos de álxebras de $\mathcal{E}$, é dicir, os isomorfismos de $\mathcal{E}$ en si mesma que preservan tanto a estrutura linear coma o produto.

Comezamos probando un feito sinxelo que, como anunciamos na introdución do capítulo, resultará ser moi conveniente para probar que o grupo de automorfismos dunha álxebra de evolución idempotente é finito:

Proposición 4.12. *Sexan $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e $\Gamma = (V, E)$ o grafo asociado a $\mathcal{E}$ relativo a dita base. Entón Γ non ten fontes.*

Demostración. Sexa $M_B(\mathcal{E}) = (\alpha_{ij})$ a matriz de estrutura asociada a $\mathcal{E}$ relativa á base B. Entón $M_B(\mathcal{E})$ é non singular en virtude da proposición 3.13, e polo tanto, para cada $j = 1, \ldots, n$, existirá algún índice $i = 1, \ldots, n$ tal que $\alpha_{ij} \neq 0$ (se non fose así, entón $det(M_B(\mathcal{E})) = 0$, contradecindo que $M_B(\mathcal{E})$ é non singular); entón $(i, j) \in E$, e consecuentemente o nodo j non é unha fonte de Γ. Concluímos entón que o grafo Γ non ten fontes. □

Observemos que, se $\mathcal{E}$ non é idempotente, entón o seu grafo asociado si pode ter fontes, como vimos no exemplo 4.4.

Unha consecuencia importante desta proposición é que, se Γ é o grafo asociado a unha álxebra de evolución idempotente $\mathcal{E}$ relativo a unha base natural, entón o grupo $\mathrm{Diag}(\Gamma)$ é finito (véxase o corolario 2.12). Este feito será especialmente relevante na demostración do teorema 4.18.

A continuación presentaremos os resultados que nos permitirán estudar o grupo de automorfismos de $\mathcal{E}$ a través das propiedades do seu grafo asociado. Antes de introducilos, debemos recordar que se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e $\varphi \in \mathrm{Aut}(\mathcal{E})$, entón existe unha única permutación $\sigma \in S_n$ tal que $\varphi(e_i) \in \mathbb{K}^\times e_{\sigma(i)}$ para cada $i = 1, \ldots, n$ (véxase o corolario 3.19). O teorema 4.14 ampliará este resultado e presentará unha afirmación aínda máis forte. A demostración deste teorema será, en gran medida, unha consecuencia do seguinte lema, que establece unha propiedade clave dos automorfismos dunha álxebra de evolución idempotente, á cal recorreremos en diversas ocasións máis adiante.

Lema 4.13. *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e matriz de estrutura asociada (α_{ij}) relativa a dita base. Entón:*

1. *Sexa $\varphi \in \mathrm{Aut}(\mathcal{E})$, e sexan $\sigma \in S_n$ e $\mu_1, \ldots, \mu_n \in \mathbb{K}^\times$ a permutación e os escalares non nulos tales que $\varphi(e_i) = \mu_i e_{\sigma(i)}$ para cada $i = 1, \ldots, n$. Entón verifícase a seguinte relación:*

$$\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$$

   para cada $i, j = 1, \ldots, n$.

2. *Sexan σ unha permutación de S_n e φ o automorfismo linear de $\mathcal{E}$ (automorfismo de $\mathcal{E}$ como $\mathbb{K}$-espazo vectorial) determinado por $\varphi(e_i) = \mu_i e_{\sigma(i)}$ para todo $i = 1, \ldots, n$, para certos escalares non nulos $\mu_1, \ldots, \mu_n \in \mathbb{K}^\times$ tales que $\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$ para cada $i, j = 1, \ldots, n$. Entón $\varphi \in \mathrm{Aut}(\mathcal{E})$.*

Demostración. (1.) Para cada $i = 1, \ldots, n$ arbitrario, tense que:

$$\varphi(e_i^2) = \varphi(\sum_{j=1}^{n} \alpha_{ij} e_j) = \sum_{j=1}^{n} \alpha_{ij} \varphi(e_j) = \sum_{j=1}^{n} \alpha_{ij} \mu_j e_{\sigma(j)},$$

e ó mesmo tempo:

$$\varphi(e_i^2) = \varphi(e_i)^2 = (\mu_i e_{\sigma(i)})^2 = \mu_i^2 e_{\sigma(i)}^2 = \mu_i^2 \sum_{j=1}^{n} \alpha_{\sigma(i)j} e_j = \sum_{j=1}^{n} \mu_i^2 \alpha_{\sigma(i)\sigma(j)} e_{\sigma(j)}.$$

Entón:

$$\sum_{j=1}^{n} \alpha_{ij} \mu_j e_{\sigma(j)} = \sum_{j=1}^{n} \mu_i^2 \alpha_{\sigma(i)\sigma(j)} e_{\sigma(j)},$$

e como $\{e_1, \ldots, e_n\}$ é un conxunto linearmente independente deducimos:

$$\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$$

para cada $j = 1, \ldots, n$.

(2.) Supoñamos que φ é un automorifsmo linear de $\mathcal{E}$ que satisfai as condicións do enunciado. Para ver que $\varphi \in \mathrm{Aut}(\mathcal{E})$, só falta ver que φ é multiplicativo, ou sexa, que conserva o produto en $\mathcal{E}$. Ademais, é suficiente con comprobalo para os elementos da base, xa que para o resto de elementos o argumento esténdese por linearidade.

Por unha parte, se $i \neq j$ entón:

$$\varphi(e_i e_j) = \varphi(0) = 0 = \mu_i \mu_j 0 = (\mu_i e_i)(\mu_j e_j) = \varphi(e_i)\varphi(e_j).$$

Por outra parte, dado $i = 1, \ldots, n$, de xeito análogo á proba da primeira parte demostramos que:

$$\varphi(e_i^2) = \sum_{j=1}^{n} \alpha_{ij} \mu_j e_{\sigma(j)},$$

e tamén:

$$\varphi(e_i)^2 = \sum_{j=1}^{n} \mu_i^2 \alpha_{\sigma(i)\sigma(j)} e_{\sigma(j)}.$$

Como $\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$ para todo $i, j = 1, \ldots, n$ entón deducimos que $\varphi(e_i^2) = \varphi(e_i)^2$.

Entón φ conserva o produto dos elementos da base e en consecuencia $\varphi \in \mathrm{Aut}(\mathcal{E})$, como queriamos ver. □

Como anticipamos, o lema anterior permite demostrar de forma sinxela o seguinte teorema, que amplía o corolario 3.19:

Teorema 4.14. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e Γ é o grafo asociado a $\mathcal{E}$ relativo a dita base, entón tense o seguinte homomorfismo de grupos:*

$$\begin{aligned} \Phi_B : \mathrm{Aut}(\mathcal{E}) &\longrightarrow \mathrm{Aut}(\Gamma) \\ \varphi &\longmapsto \Phi_B(\varphi) := \sigma_\varphi \end{aligned}$$

onde, para cada $\varphi \in \mathrm{Aut}(\mathcal{E})$, σ_φ é a única permutación de S_n tal que $\varphi(e_i) \in \mathbb{K}^\times e_{\sigma_\varphi(i)}$ para cada $i = 1, \ldots, n$.

Demostración. Debemos ver que a aplicación Φ_B está ben definida (concretamente, que $\mathrm{Im}\Phi_B \subset \mathrm{Aut}(\Gamma)$) e que é un homomorfismo de grupos. Procedamos por partes:

- *A aplicación Φ_B está ben definida.* Debemos ver que $\mathrm{Im}\Phi_B \subset \mathrm{Aut}(\Gamma)$. Denotemos por (α_{ij}) a matriz de estrutura de $\mathcal{E}$ relativa á base B.

  Sexa $\varphi \in \mathrm{Aut}(\mathcal{E})$ dado por $\varphi(e_i) = \mu_i e_{\sigma(i)}$ para cada $i = 1, \ldots, n$, de xeito que $\Phi_B(\varphi) = \sigma$. Polo lema 4.13:

  $$\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$$

  para cada $i, j = 1, \ldots, n$. Como os escalares $\mu_1, \ldots, \mu_n$ son non nulos, entón:

  $$\alpha_{ij} \neq 0 \iff \alpha_{\sigma(i)\sigma(j)} \neq 0.$$

  Ou sexa, $(i, j) \in E$ se, e só se, $(\sigma(i), \sigma(j)) \in E$, o que equivale a dicir que $\Phi_B(\varphi) = \sigma$ é un elemento de $\mathrm{Aut}(\Gamma)$.

- *Φ_B é un homomorfismo de grupos.* Sexan $\varphi, \varphi' \in \mathrm{Aut}(\mathcal{E})$. Fixado $i = 1, \ldots, n$:

  $$\varphi'(e_i) \in \mathbb{K}^\times e_{\sigma_{\varphi'}(i)},$$

  e polo tanto

  $$\varphi\varphi'(e_i) = \varphi(\varphi'(e_i)) \in \mathbb{K}^\times e_{\sigma_\varphi(\sigma_{\varphi'}(i))} = \mathbb{K}^\times e_{\sigma_\varphi \sigma_{\varphi'}(i).}$$

  Pero ademais:

  $$\varphi\varphi'(e_i) \in \mathbb{K}^\times e_{\sigma_{\varphi\varphi'}(i)}.$$

  Entón existen dous escalares non nulos $\lambda, \mu \in \mathbb{K}^\times$ tales que:

  $$\lambda e_{\sigma_\varphi \sigma_{\varphi'}(i)} = \varphi\varphi'(e_i) = \mu e_{\sigma_{\varphi\varphi'}(i)}.$$

  Como $\{e_1, \ldots, e_n\}$ é un conxunto linearmente independente, entón $\lambda = \mu$ e $e_{\sigma_{\varphi\varphi'}(i)} = e_{\sigma_\varphi \sigma_{\varphi'}(i)}$; en particular, $\sigma_\varphi \sigma_{\varphi'}(i) = \sigma_{\varphi\varphi'}(i)$. Como isto se verifica para cada $i = 1, \ldots, n$, entón $\sigma_\varphi \sigma_{\varphi'} = \sigma_{\varphi\varphi'}$, ou sexa:

  $$\Phi_B(\varphi)\Phi_B(\varphi') = \Phi_B(\varphi\varphi').$$

Concluímos que Φ_B está ben definida e é un homomorfismo de grupos, como tiñamos que probar. □

Acabamos de ver que cada automorfismo de $\mathcal{E}$ induce un automorfismo de grafos de Γ. A continuación veremos que cada elemento de $\mathrm{Diag}(\Gamma)$ induce á súa vez un automorfismo de $\mathcal{E}$:

Teorema 4.15. *Sexa $\mathcal{E}$ unha álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e grafo asociado $\Gamma = (V, E)$ relativo a dita base. Tense o seguinte homomorfismo inxectivo de grupos:*

$$\begin{aligned} \iota : \mathrm{Diag}(\Gamma) &\longrightarrow \mathrm{Aut}(\mathcal{E}) \\ \psi &\longmapsto \iota(\psi) = \hat{\psi} \end{aligned}$$

onde $\hat{\psi}$ é o automorfismo de $\mathcal{E}$ determinado por $\hat{\psi}(e_i) = \psi(i)e_i$ para cada $i = 1, \ldots, n$.

Demostración. Dividiremos a demostración en tres partes:

- *ι está ben definido.* Sexan $\psi \in \mathrm{Diag}(\Gamma)$ e $\varphi = \hat{\psi}$. Debemos comprobar que $\varphi \in \mathrm{Aut}(\mathcal{E})$.

  Como os escalares $\psi(1), \ldots, \psi(n)$ son non nulos e $\{e_1, \ldots, e_n\}$ é unha base de $\mathcal{E}$, entón $\{\varphi(e_1), \ldots, \varphi(e_n)\} = \{\psi(1)e_1, \ldots, \psi(n)e_n\}$ é unha base de $\mathcal{E}$, e en consecuencia φ é un automorfismo linear de $\mathcal{E}$, é dicir, un automorfismo de $\mathcal{E}$ como espazo vectorial. Daquela, só falta por comprobar que φ conserva o produto en $\mathcal{E}$.

  Agora ben, como ψ é un elemento de $\mathrm{Diag}(\Gamma)$, entón $\psi(j) = \psi(i)^2$ sempre que $(i, j) \in E$, ou sexa, sempre que $\alpha_{ij} \neq 0$. Polo tanto, se $\alpha_{ij} \neq 0$ satisfaise a seguinte identidade:

  $$\psi(j)\alpha_{ij} = \psi(i)^2\alpha_{ij}.$$

  Ademais, a mesma igualdade verifícase trivialmente sempre que $\alpha_{ij} = 0$. En virtude do lema 4.13, o automorfismo de $\mathcal{E}$ determinado por $\varphi(e_i) = \psi(i)e_i$ é un elemento de $\mathrm{Aut}(\mathcal{E})$. Ou sexa, $\varphi \in \mathrm{Aut}(\mathcal{E})$ como queriamos ver.

- *ι é un homomorfismo de grupos.* Sexan $\psi, \psi' \in \mathrm{Diag}(\Gamma)$. Para cada $i = 1, \ldots, n$:

  $$\begin{aligned} (\hat{\psi\psi'})(e_i) = (\psi\psi'(i))e_i = \psi(i)\psi'(i)e_i = \psi'(i)(\psi(i)e_i) = \\ = \psi'(i)\hat{\psi}(e_i) = \hat{\psi}(\psi'(i)e_i) = \hat{\psi}(\hat{\psi'}(e_i)) = (\hat{\psi} \circ \hat{\psi'})(e_i). \end{aligned}$$

  Como $(\hat{\psi\psi'})(e_i) = (\hat{\psi} \circ \hat{\psi'})(e_i)$ para cada elemento da base e_i, entón a mesma igualdade se verifica para o resto de elementos de $\mathcal{E}$, e concluímos que que $\iota(\psi\psi') = (\hat{\psi\psi'}) = \hat{\psi} \circ \hat{\psi'} = \iota(\psi) \circ \iota(\psi')$.

- ι *é inxectivo.* Sexa $\psi \in \mathrm{Ker}\iota$, ou sexa, sexa $\psi \in \mathrm{Diag}(\Gamma)$ tal que $\hat{\psi} = id_{\mathcal{E}}$. Para cada $i = 1, \ldots, n$ tense a seguinte igualdade:

  $$e_i = \hat{\psi}(e_i) = \psi(i)e_i,$$

  e polo tanto $\psi(i) = 1$ para todo $i = 1, \ldots, n$. Daquela ψ é o elemento neutro de $\mathrm{Diag}(\Gamma)$. Entón $\mathrm{Ker}\iota = 1$ e polo tanto ι é un homomorfismo inxectivo.

Entón ι é un homomorfismo de grupos inxectivo, como tiñamos que probar. □

Unha vez definidos os homomorfismos $\iota : \mathrm{Diag}(\Gamma) \to \mathrm{Aut}(\mathcal{E})$ e $\Phi_B : \mathrm{Aut}(\mathcal{E}) \to \mathrm{Aut}(\Gamma)$, estamos en condicións de enunciar o seguinte importante teorema:

Teorema 4.16. *Sexa $\mathcal{E}$ unha álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$ e grafo asociado $\Gamma = (V, E)$ relativo a dita base. A seguinte sucesión é exacta:*

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Aut}(\Gamma).$$

Demostración. Xa vimos no teorema anterior que ι era inxectivo, e polo tanto só falta comprobar que $\mathrm{Im}\iota = \mathrm{Ker}\Phi_B$.

- *Vexamos que* $\mathrm{Im}\iota \subset \mathrm{Ker}\Phi_B$. Sexa $\varphi \in \mathrm{Im}\iota$, e supoñamos que $\varphi = \iota(\psi)$ con $\psi \in \mathrm{Diag}(\Gamma)$, de xeito que $\varphi(e_i) = \psi(i)e_i$ para todo $i = 1, \ldots, n$. Entón $\varphi(e_i) \in \mathbb{K}^\times e_i$ para todo $i = 1, \ldots, n$, e polo tanto está claro que $\Phi_B(\varphi) = 1$.

- *Vexamos que* $\mathrm{Ker}\Phi_B \subset \mathrm{Im}\iota$. Sexa $\varphi \in \mathrm{Ker}\Phi_B$. Entón $\varphi(e_i) \in \mathbb{K}^\times e_i$ para cada $i = 1, \ldots, n$, ou sexa, existen escalares non nulos $\mu_1, \ldots, \mu_n \in \mathbb{K}^\times$ tales que $\varphi(e_i) = \mu_i e_i$ para cada $i = 1, \ldots, n$. Definimos $\psi : V \to \mathbb{K}^\times$ como $\psi(i) = \mu_i$ para todo $i = 1, \ldots, n$, de xeito que $\varphi(e_i) = \psi(i)e_i$.

  Polo lema 4.13, para cada $i, j = 1, \ldots, n$ verifícase a seguinte igualdade:

  $$\mu_j \alpha_{ij} = \mu_i^2 \alpha_{ij}.$$

  Obsérvese que se $(i, j) \in E$, entón $\alpha_{ij} \neq 0$, e deducimos que $\mu_j = \mu_i^2$. É dicir, $\psi(j) = \psi(i)^2$ sempre que $(i, j) \in E$. Ou sexa, $\psi \in \mathrm{Diag}(\Gamma)$. Como ademais $\varphi = \iota(\psi)$, entón $\varphi \in \mathrm{Im}\iota$.

Como ι é inxectivo e $\mathrm{Im}\iota = \mathrm{Ker}\Phi_B$, entón a sucesión

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Aut}(\Gamma)$$

é exacta. □

O seguinte corolario dedúcese trivialmente a partir do teorema anterior:

Corolario 4.17. *Sexa $\mathcal{E}$ unha álxebra de evolución idempotente con base natural B e grafo asociado $\Gamma = (V, E)$ relativo a dita base. Entón tense unha sucesión exacta curta:*

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1.$$

Unha consecuencia inmediata deste corolario é o seguinte teorema ([5, Theorem 4.8]), que afirma, como adiantamos en varias ocasións, que o grupo de automorfismos dunha álxebra de evolución idempotente é finito, e do cal presentamos unha demostración máis concisa que no artigo orixinal. A nosa demostración, a diferenza da que presenta o artigo, baséase na sucesión exacta do corolario anterior e fai uso explícito da finitude do grupo diagonal dun grafo asociado a unha álxebra de evolución idempotente.

Teorema 4.18. *Se $\mathcal{E}$ é unha $\mathbb{K}$-álxebra de evolución idempotente, entón $\mathrm{Aut}(\mathcal{E})$ é un grupo finito.*

Demostración. Sexan B unha base natural de $\mathcal{E}$ e Γ o grafo asociado a $\mathcal{E}$ relativo á base B. Consideremos a sucesión exacta curta:

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1.$$

Terase que:

$$\frac{\mathrm{Aut}(\mathcal{E})}{\mathrm{Ker}\Phi_B} \simeq \mathrm{Im}\Phi_B,$$

onde $\mathrm{Im}\Phi_B$ é un subgrupo de S_n, e en particular, un grupo finito. Polo tanto, para ver que $\mathrm{Aut}(\mathcal{E})$ é finito, é suficiente con ver que $\mathrm{Ker}\Phi_B$ o é.

Agora ben, como $\mathcal{E}$ é idempotente, entón Γ non ten fontes en virtude da proposición 4.12, e daquela o grupo $\mathrm{Diag}(\Gamma)$ é finito a consecuencia do teorema 2.10. Polo tanto, o grupo $\mathrm{Ker}\Phi_B = \mathrm{Im}\iota \simeq \mathrm{Diag}(\Gamma)$ tamén é finito, que era precisamente o que tiñamos que probar. □

Cómpre observar que se a álxebra de evolución $\mathcal{E}$ non é idempotente, entón o grupo $\mathrm{Aut}(\mathcal{E})$ non ten por que ser finito, como revela o seguinte exemplo, tomado de [5]:

Exemplo 4.19 (Álxebra de evolución non idempotente con grupo de automorfismos infinito)**.** Consideremos a $\mathbb{R}$-álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3\}$ cuxo produto vén dado por:

$$e_1^2 = e_2^2 = e_3^2 = e_3.$$

O grafo asociado a $\mathcal{E}$ relativo á base B está representado na figura 4.5.

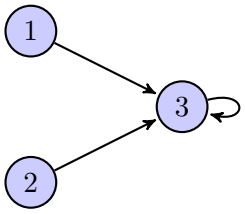

Figura 4.5: Grafo do exemplo 4.19.

Observemos que $\mathcal{E}$ non é idempotente, xa que $\{e_1^2, e_2^2, e_3^2\} = \{e_3\}$ non é unha base de $\mathcal{E}$. Imos ver que $\mathrm{Aut}(\mathcal{E})$ é o grupo formado por todos os automorfismos lineais $\varphi : \mathcal{E} \to \mathcal{E}$ da forma:

$$\begin{aligned}\varphi(e_1) &= \alpha e_1 + \beta e_2,\\ \varphi(e_2) &= \gamma e_1 + \delta e_2,\\ \varphi(e_3) &= e_3,\end{aligned}$$

tales que a matriz

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$$

é ortogonal, os cales constitúen un grupo infinito.

En primeiro lugar, supoñamos que φ é un automorfismo de $\mathcal{E}$, e supoñamos que φ está determinado por:

$$\varphi(e_j) = \sum_{i=1}^{3} a_{ij} e_i$$

para cada $j \in \{1, 2, 3\}$. Terase que:

$$\sum_{i=1}^{3} a_{i3} e_i = \varphi(e_3) = \varphi(e_3^2) = \varphi(e_3)^2 = \sum_{i=1}^{3} a_{i3}^2 e_i^2 = (\sum_{i=1}^{3} a_{i3}^2) e_3,$$

e polo tanto $a_{13} = a_{23} = 0$ e $a_{33}^2 = a_{33}$. Como $\varphi(e_3) \neq 0$, entón necesariamente $a_{33} \neq 0$ e en consecuencia $a_{33} = 1$. Daquela:

$$\varphi(e_3) = e_3.$$

Por outra banda, se $j = 1$ ou 2 tense que:

$$0 = \varphi(0) = \varphi(e_j e_3) = \varphi(e_j)\varphi(e_3) = (\sum_{i=1}^{3} a_{ij} e_i) e_3 = a_{3j} e_3^2 = a_{3j} e_3,$$

de onde $a_{3j} = 0$. Ou sexa, $a_{31} = a_{32} = 0$. Se denotamos $\alpha = a_{11}$, $\beta = a_{21}$, $\gamma = a_{12}$ e $\delta = a_{22}$, teremos que:

$$\begin{aligned}\varphi(e_1) &= \alpha e_1 + \beta e_2,\\ \varphi(e_2) &= \gamma e_1 + \delta e_2.\end{aligned}$$

Ademais:

$$e_3 = \varphi(e_3) = \varphi(e_1^2) = (\alpha e_1 + \beta e_2)^2 = (\alpha^2 e_1^2 + \beta^2 e_2^2) = (\alpha^2 + \beta^2)e_3,$$

e polo tanto $\alpha^2 + \beta^2 = 1$. Analogamente:

$$e_3 = \varphi(e_3) = \varphi(e_2^2) = (\gamma e_1 + \delta e_2)^2 = (\gamma^2 e_1^2 + \delta^2 e_2^2) = (\gamma^2 + \delta^2)e_3,$$

e daquela $\gamma^2 + \delta^2 = 1$. Igualmente:

$$0 = \varphi(0) = \varphi(e_1 e_2) = (\alpha e_1 + \beta e_2)(\gamma e_1 + \delta e_2) = \alpha\gamma e_1^2 + \beta\delta e_2^2 = (\alpha\gamma + \beta\delta)e_3,$$

de xeito que $\alpha\gamma + \beta\delta = 0$. Ademais, as condicións $\alpha^2 + \beta^2 = 1$, $\gamma^2 + \delta^2 = 1$ e $\alpha\gamma + \beta\delta = 0$ equivalen a que a matriz

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

sexa ortogonal.

Reciprocamente, se φ é un automorfismo linear da forma indicada anteriormente, entón é inmediato comprobar que $\varphi(e_i e_j) = \varphi(e_i)\varphi(e_j)$ para cada $i, j = 1, \ldots, n$, e polo tanto $\varphi(xy) = \varphi(x)\varphi(y)$ para cada $x, y \in \mathcal{E}$, de xeito que $\varphi \in \mathrm{Aut}(\mathcal{E})$. ◇

Observación 4.20. Antes de rematar a sección, queremos destacar que os resultados comprendidos entre o lema 4.13 e o corolario 4.17, ambos incluídos, se deducen directamente do corolario 3.19, que é unha consecuencia directa do teorema 3.18, sen necesidade de recorrer a propiedades adicionais.

Concretamente, a condición de idempotencia que esiximos en ditos resultados, soamente é necesaria para garantir a aplicabilidade do teorema 3.18, que asegura que as álxebras de evolución idempotentes teñen unha única base natural agás permutacións e produto por escalares non nulos. En particular, os resultados mencionados seguen sendo válidos aínda que substituamos a condición de idempotencia por outra condición máis débil, baixo a cal siga sendo válido o teorema 3.18. En particular, seguiríamos tendo a sucesión exacta curta:

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1.$$

Non obstante, se prescindimos da condición de idempotencia, non podemos concluír que Γ non teña fontes nin deducir a finitude dos grupos $\mathrm{Diag}(\Gamma)$ e $\mathrm{Aut}(\mathcal{E})$. Trataremos estas cuestións con maior detalle no capítulo 5.

4.3. Grupos transitivos

Nesta sección estudaremos o grupo de automorfismos dunha álxebra de evolución idempotente $\mathcal{E}$ baixo certas hipóteses adicionais de transitividade (véxase a definición 1.7) que nos permitirán

chegar a unha caracterización máis forte do grupo $\mathrm{Aut}(\mathcal{E})$. Os contidos desta sección están tomados de [4].

Os resutlados fundamentais dos que faremos uso son o lema 4.13, a sucesión exacta curta:

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1$$

do corolario 4.17, mais o teorema 2.10.

Verifícase o seguinte resultado:

Lema 4.21. *Se $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é un grupo 2-transitivo, entón:*

1. *Ou ben $\alpha_{ij} = 0$ para todo $i \neq j$, ou ben $\alpha_{ij} \neq 0$ para todo $i \neq j$.*
2. *Ou ben $\alpha_{ii} = 0$ para todo i, ou ben $\alpha_{ii} \neq 0$ para todo i.*

Demostración. (1.) Sexan $i \neq j$ e $r \neq s$ dous pares de índices distintos arbitrarios. Como $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 2-transitivo, entón existirá unha permutación $\sigma \in \Phi_B(\mathrm{Aut}(\mathcal{E}))$ tal que $(r, s) = (\sigma(i), \sigma(j))$. Sexa $\varphi \in \mathrm{Aut}(\mathcal{E})$ tal que $\sigma = \Phi_B(\varphi)$, e sexan $\mu_1, \ldots, \mu_n \in \mathbb{K}^\times$ os escalares tales que $\varphi(e_k) = \mu_k e_{\sigma(k)}$ para todo $k = 1, \ldots, n$. Polo lema 4.13:

$$\mu_j \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)} = \mu_i^2 \alpha_{rs}.$$

Como μ_i e μ_j son non nulos, entón $\alpha_{ij} = 0$ se, e só se, $\alpha_{rs} = 0$. Polo tanto, ou ben todos os coeficientes α_{ij} (con $i \neq j$) son nulos, ou ben todos son non nulos.

(2.) Sexan i e r dous índices arbitrarios. Como $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 2-transitivo, particularmente é transitivo, e polo tanto existe unha permutación $\sigma \in \Phi_B(\mathrm{Aut}(\mathcal{E}))$ tal que $\sigma(i) = r$. Sexa $\varphi \in \mathrm{Aut}(\mathcal{E})$ tal que $\sigma = \Phi_B(\varphi)$, e sexan $\mu_1, \ldots, \mu_n \in \mathbb{K}^\times$ os escalares tales que $\varphi(e_k) = \mu_k e_{\sigma(k)}$ para todo $k = 1, \ldots, n$. Polo lema 4.13:

$$\mu_i \alpha_{ii} = \mu_i^2 \alpha_{\sigma(i)\sigma(i)} = \mu_i^2 \alpha_{rr},$$

Como μ_i é non nulo, entón $\alpha_{ii} = 0$ se, e só se, $\alpha_{rr} = 0$. Polo tanto, ou ben todos os coeficientes α_{ii} son nulos, ou ben todos son non nulos. □

O lema anterior permite demostrar o seguinte teorema:

Teorema 4.22. *Se $n \geq 3$ e $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é un grupo 2-transitivo, entón Φ_B é inxectivo.*

Demostración. Observemos que os escalares α_{ij} non poden ser todos nulos e polo tanto deben existir dous índices r e s tales que $\alpha_{rs} \neq 0$. Distinguiremos dous casos:

Caso 1. Se $r = s$, entón $\alpha_{rr} \neq 0$ e polo tanto $\alpha_{ii} \neq 0$ para cada $i = 1, \ldots, n$ en virtude do lema anterior. Entón, cada compoñente conexa do grafo Γ_j contén un ciclo da forma $\gamma = (i, (i, i), i)$ (para i un vértice de Γ_j arbitrario, véxase a figura 4.6). Como $b(\gamma) = 1$ e $b(\Gamma_j) \mid b(\gamma)$, entón $b(\Gamma_j) = 1$, e daquela:

$$\mathrm{Diag}(\Gamma_j) \simeq \boldsymbol{\mu}_{2^{b(\Gamma_j)}-1} \simeq \boldsymbol{\mu}_1 = 1.$$

Polo tanto, se $\Gamma_1, \ldots, \Gamma_k$ son as compoñentes conexas de Γ, entón:

$$\mathrm{Ker}\Phi_B \simeq \mathrm{Diag}(\Gamma) \simeq \mathrm{Diag}(\Gamma_1) \times \cdots \times \mathrm{Diag}(\Gamma_k) \simeq 1 \times \cdots \times 1 \simeq 1.$$

Ou sexa, $\mathrm{Ker}\Phi_B$ é o grupo trivial e daquela o homomorfismo Φ_B é inxectivo.

Caso 2. Se $r \neq s$ entón deducimos a partir do lema anterior que $\alpha_{ij} \neq 0$ para todo $i \neq j$. Isto quere dicir que calquera par de vértices distintos de Γ están unidos por unha aresta en ambos sentidos, e particularmente Γ é un grafo conexo. Como $n \geq 3$, entón podemos tomar tres vértices arbitrarios distintos de Γ, i, j e k, e construír os seguintes ciclos:

$$\gamma_1 = (i, (i, j), j, (j, k), k, (k, i), i),$$
$$\gamma_2 = (i, (i, j), j, (j, i), i)$$

(véxase a figura 4.7). Observemos que $b(\gamma_1) = 3$ e $b(\gamma_2) = 2$. Daquela:

$$b(\Gamma) \mid \gcd\{b(\gamma_1), b(\gamma_2)\} = \gcd\{2, 3\} = 1,$$

e polo tanto $b(\Gamma) = 1$. En consecuencia:

$$\mathrm{Ker}\Phi_B \simeq \mathrm{Diag}(\Gamma) \simeq \boldsymbol{\mu}_{2^{b(\Gamma)}-1} = \boldsymbol{\mu}_1 = 1.$$

Ou sexa, $\mathrm{Ker}\Phi_B$ é o grupo trivial e daquela o homomorfismo Φ_B é inxectivo. □

Figura 4.6: Ciclo γ do caso 1 do teorema 4.22

O teorema anterior establece que se $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 2-transitivo, entón Φ_B é inxectivo, e particularmente $\mathrm{Aut}(\mathcal{E}) \simeq \Phi_B(\mathrm{Aut}(\mathcal{E}))$. Daquela, podemos identificar $\mathrm{Aut}(\mathcal{E})$ cun subgrupo de $\mathrm{Aut}(\Gamma)$, que á súa vez é un subgrupo de S_n. O seguinte teorema establece un resultado aínda máis forte:

Teorema 4.23. *Supoñamos que $n \geq 3$, $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 2-transitivo e $\alpha_{rr} \neq 0$ para algún $r = 1, \ldots, n$. Entón $\Phi_B(\mathrm{Aut}(\mathcal{E})) = S_n$.*

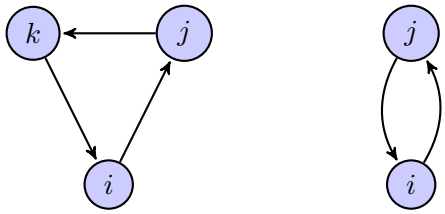

Figura 4.7: Ciclos γ_1 e γ_2 do caso 2 do teorema 4.22

Demostración. Sexa $\sigma \in S_n$. Debemos ver que existe un automorfismo $\varphi \in \mathrm{Aut}(\mathcal{E})$ tal que $\Phi_B(\varphi) = \sigma$.

Como $\alpha_{rr} \neq 0$ entón $\alpha_{ii} \neq 0$ para cada $i = 1, \ldots, n$ en virtude do lema 4.21. Polo tanto, para cada $i = 1, \ldots, n$ podemos definir o seguinte escalar non nulo:

$$\mu_i = \frac{\alpha_{ii}}{\alpha_{\sigma(i)\sigma(i)}}.$$

Definimos φ como o único automorfismo linear de $\mathcal{E}$ que satisfai que $\varphi(e_i) = \mu_i e_{\sigma(i)}$ para cada $i = 1, \ldots, n$. Vexamos que $\varphi \in \mathrm{Aut}(\mathcal{E})$, para o cal é suficiente demostrar que $\mu_j\ \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$ para cada $i, j = 1, \ldots, n$, en virtude do lema 4.13.

Sexan pois $i, j = 1, \ldots, n$. Se $i = j$ entón:

$$\mu_j \alpha_{ij} = \mu_i \alpha_{ii} = \frac{\alpha_{ii}}{\alpha_{\sigma(i)\sigma(i)}} \alpha_{ii} = \frac{\alpha_{ii}^2}{\alpha_{\sigma(i)\sigma(i)}^2} \alpha_{\sigma(i)\sigma(i)} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}.$$

Agora supoñamos que $i \neq j$. Como $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 2-transitivo, entón existe unha permutación $\sigma' \in \Phi_B(\mathrm{Aut}(\mathcal{E}))$ tal que $(\sigma(i), \sigma(j)) = (\sigma'(i), \sigma'(j))$. Sexa $\varphi' \in \mathrm{Aut}(\mathcal{E})$ tal que $\Phi_B(\varphi') = \sigma'$, e sexan $\mu'_1, \ldots, \mu'_n \in \mathbb{K}^\times$ os escalares non nulos que verifican que $\varphi'(e_k) = \mu'_k e_{\sigma'(k)}$ para cada $k = 1, \ldots, n$. Polo lema 4.13:

$$\mu'_i \alpha_{ii} = \mu_i'^2 \alpha_{\sigma'(i)\sigma'(i)},$$

e polo tanto:

$$\mu'_i = \frac{\alpha_{ii}}{\alpha_{\sigma'(i)\sigma'(i)}} = \frac{\alpha_{ii}}{\alpha_{\sigma(i)\sigma(i)}} = \mu_i.$$

Analogamente:

$$\mu'_j = \mu_j.$$

En consecuencia:

$$\mu_j \alpha_{ij} = \mu'_j \alpha_{ij} = \mu_i'^2 \alpha_{\sigma'(i)\sigma'(i)} = \mu_i^2 \alpha_{\sigma(i)\sigma(i)},$$

onde a segunda igualdade se deriva de que $\varphi' \in \mathrm{Aut}(\mathcal{E})$ a partir do lema 4.13. Ou sexa, $\mu_j\ \alpha_{ij} = \mu_i^2 \alpha_{\sigma(i)\sigma(j)}$ como queriamos ver.

En conclusión, dada unha permutación $\sigma \in S_n$, somos quen de construír un automorfismo $\varphi \in \mathrm{Aut}(\mathcal{E})$ tal que $\Phi_B(\varphi) = \sigma$. En consecuencia, deducimos que $S_n \subset \Phi_B(\mathrm{Aut}(\mathcal{E}))$. Como o contido $\Phi_B(\mathrm{Aut}(\mathcal{E})) \subset S_n$ é inmediato, entón $\Phi_B(\mathrm{Aut}(\mathcal{E})) = S_n$. □

Vimos que se $n \geq 3$ e $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é un grupo de permutacións 2-transitivo, entón Φ_B é inxectivo, e se ademais a matriz de estrutura de $\mathcal{E}$ verifica que $\alpha_{rr} \neq 0$ para algún $r = 1, \ldots, n$, entón $\Phi_B(\mathrm{Aut}(\mathcal{E})) = S_n$.

Do mesmo xeito que estudamos o caso 2-transitivo, tamén podemos estudar os casos doutros grupos de permutacións k-transitivos para $k > 2$. Por exemplo, un resultado de [4] afirma que se $n \geq 5$ e $\Phi_B(\mathrm{Aut}(\mathcal{E}))$ é 4-transitivo, entón Φ_B é inxectivo e $\Phi_B(\mathrm{Aut}(\mathcal{E})) = S_n$. Non trataremos este caso nin outros máis complexos en profundidade, xa que non dispoñemos de espazo para facelo.

Capítulo 5

Novas perspectivas: máis alá da idempotencia

Ata o momento, o noso traballo centrouse no estudo das álxebras de evolución idempotentes, caracterizadas pola súa forte rixidez estrutural: posúen unha única base natural agás por permutacións e multiplicación por escalares non nulos. Esta importante propiedade permitiunos describir con precisión os seus automorfismos (teorema 4.14) e chegar á seguinte sucesión exacta curta (teorema 4.16):

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1.$$

Agora ben, como sinalamos na observación 4.20, nos resultados comprendidos entre o lema 4.13 e o corolario 4.17, a condición de idempotencia só foi necesaria para garantir a unicidade da base natural. Deste xeito, os mesmos resultados seguen sendo válidos mesmo se substituímos a condición de idempotencia por algunha outra condición máis débil baixo a cal poidamos garantir a unicidade das bases naturais.

Neste contexto, introduciremos a propiedade 2LI para álxebras de evolución non dexeneradas, un caso das cales é o das álxebras de evolución idepotentes. Este capítulo está baseado fundamentalmente no artigo [2].

Advertimos que o obxectivo deste capítulo non é máis que sinalar novas vías de continuidade da teoría que levamos desenvolvendo ó longo do traballo, sen profundizar nos aspectos técnicos nin deternos nas demostracións de forma exhaustiva.

Definición 5.1. Unha álxebra de evolución $\mathcal{E}$ dise **non dexenerada** se verifica algunha das seguintes condicións equivalentes:

1. Existe unha base natural $B = \{e_1, \ldots, e_n\}$ de $\mathcal{E}$ tal que $e_i^2 \neq 0$ para todo $i = 1, \ldots, n$.

2. Toda base natural $B = \{e_1, \ldots, e_n\}$ de $\mathcal{E}$ cumpre $e_i^2 \neq 0$ para todo $i = 1, \ldots, n$.

3. O aniquilador de $\mathcal{E}$ é trivial, ou sexa, $\text{ann}(\mathcal{E}) = 0$.

Observemos que toda álxebra de evolución idempotente é non dexenerada. Efectivamente, se $\mathcal{E}$ é unha álxebra de evolución idempotente con base natural $B = \{e_1, \ldots, e_n\}$, entón $\{e_1^2, \ldots, e_n^2\}$ tamén é unha base de $\mathcal{E}$ grazas á proposición 3.13, e consecuentemente $e_i^2 \neq 0$ para todo $i = 1, \ldots, n$.

O seguinte resultado, demostrado no artigo [2], presenta unha caracterización das álxebras de evolución non dexeneradas que posúen unha única base natural (onde por *única* entendemos *única agás permutacións e multiplicación por escalares non nulos*):

Teorema 5.2 ([2], Corolario 2.7)**.** *Sexa $\mathcal{E}$ unha $\mathbb{K}$-álxebra de evolución non dexenerada sobre $\mathbb{K}$. Son equivalentes:*

1. *$\mathcal{E}$ posúe unha única base natural.*

2. *Existe unha base natural $B = \{e_1, \ldots, e_n\}$ tal que, para cada par de elementos distintos $e_i, e_j \in B$, o conxunto $\{e_i^2, e_j^2\}$ é linearmente independente.*

Este teorema motiva a seguinte definición:

Definición 5.3. Dicimos que unha $\mathbb{K}$-álxebra de evolución $\mathcal{E}$ satisfai a **propiedade 2LI** se admite unha base natural $B = \{e_1, \ldots, e_n\}$ tal que, para cada par de elementos distintos $e_i, e_j \in B$, o conxunto $\{e_i^2, e_j^2\}$ é linealmente independente.

Observemos que, en particular, calquera álxebra de evolución que satisfaga a propiedade 2LI é non dexenerada. Ademais, grazas ó teorema previo, esta propiedade non depende da base natural escollida.

Advertimos tamén que todas as álxebras de evolución idempotentes satisfán a propiedade 2LI, xa que se $B = \{e_1, \ldots, e_n\}$ é unha base natural dunha álxebra de evolución idempotente $\mathcal{E}$, entón $\{e_1^2, \ldots, e_n^2\}$ tamén é unha base de $\mathcal{E}$ e polo tanto cada subconxunto $\{e_i^2, e_j^2\}$ é linearmente independente. Ou doutra forma, o teorema 3.18 afirma precisamente que as álxebras de evolución idempotentes satisfán a condición equivalente (1.) do teorema 5.2.

Este teorema permítenos estender a análise que fixemos do grupo de automorfismos das álxebras de evolución idempotentes ó caso das álxebras de evolución coa propiedade 2LI. Non obstante, se prescindimos da condición de idempotencia, poderíamos perder certas propiedades desexables do grafo Γ asociado a unha álxebra de evolución $\mathcal{E}$ relativo a unha base natural, como a ausencia de fontes ou a finitude do grupo $\text{Diag}(\Gamma)$, así como a finitude de $\text{Aut}(\mathcal{E})$. Vexámolo no seguinte exemplo:

Exemplo 5.4 (Álxebra de evolución 2LI non idempotente)**.** Consideremos a $\mathbb{K}$-álxebra de evolución $\mathcal{E}$ con base natural $B = \{e_1, e_2, e_3, e_4, e_5\}$ cuxo produto está dado por:

$$\begin{aligned} e_1^2 &= e_2 + e_3 + e_4 + e_5, \\ e_2^2 &= e_3, \\ e_3^2 &= e_4, \\ e_4^2 &= e_5, \\ e_5^2 &= e_2, \end{aligned}$$

e cuxo grafo asociado relativo á base B está representado na figura 5.1. É trivial comprobar que calquera par de elementos distintos $e_i, e_j \in B$ satisfán que $\{e_i^2, e_j^2\}$ é un conxunto linearmente independente, e polo tanto $\mathcal{E}$ satisfai a propiedade 2LI. Non obstante, $\mathcal{E}$ non é idempotente, xa que:

$$\mathcal{E}^2 = \operatorname{span}\{e_1^2, \ldots, e_5^2\} = \operatorname{span}\{e_2, e_3, e_4, e_5\} \subsetneq \mathcal{E}$$

Ademais, está claro que o vértice 1 é unha fonte do grafo, e polo tanto deducimos que o teorema 4.12 non se satisfai en xeral para esta clase de álxebras de evolución. ◇

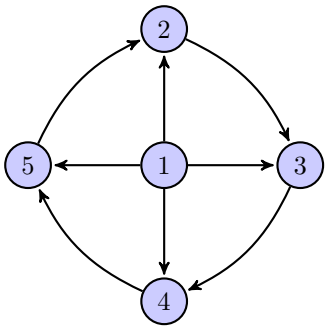

Figura 5.1: Grafo asociado a unha álxebra 2LI non idempotente.

Non obstante, e aínda que o grafo ten unha fonte, a seguinte proposición afirma que o grupo diagonal da álxebra de evolución do exemplo anterior si é finito (véxase Corolario 2.12):

Proposición 5.5. *Sexa* Γ *o grafo da figura 5.1. Entón* $\operatorname{Diag}(\Gamma)$ *é isomorfo a* $\mathbb{Z}_2$*.*

Demostración. Por definición,

$$\operatorname{Diag}(\Gamma) := \left\{ \psi : V \to \mathbb{K}^\times \;\middle|\; \psi(w) = \psi(v)^2 \text{ para todo } (v, w) \in E \right\}.$$

Polo tanto, as condicións que debe satisfacer un elemento $\psi \in \operatorname{Diag}(\Gamma)$ son as seguintes:

$$\begin{aligned} \psi(2) &= \psi(1)^2, \qquad \psi(3) = \psi(2)^2, \\ \psi(3) &= \psi(1)^2, \qquad \psi(4) = \psi(3)^2, \\ \psi(4) &= \psi(1)^2, \qquad \psi(5) = \psi(4)^2, \\ \psi(5) &= \psi(1)^2, \qquad \psi(2) = \psi(5)^2. \end{aligned}$$

Das catro primeiras deducimos:

$$\psi(2) = \psi(3) = \psi(4) = \psi(5) = \psi(1)^2.$$

Substituíndo en $\psi(3) = \psi(2)^2$, obtemos:

$$\psi(1)^2 = \psi(3) = \psi(2)^2 = (\psi(1)^2)^2 = \psi(1)^4,$$

e como $\psi(1) \neq 0$ entón deducimos:

$$\psi(1)^2 = 1.$$

Daquela, $\psi(1) = \pm 1$ e $\psi(2) = \psi(3) = \psi(4) = \psi(5) = (\pm 1)^2 = 1$.

Entón, calquera elemento $\psi \in \mathrm{Diag}(\Gamma)$ está determinado polo valor de $\psi(1)$, que pode ser 1 ou -1. En ambos casos, satisfanse as oito condicións anteriores, e polo tanto o grupo $\mathrm{Diag}(\Gamma)$ só consta de dous elementos. Particularmente, $\mathrm{Diag}(\Gamma)$ é un grupo finito e isomorfo a $\mathbb{Z}_2$. □

Observemos que se $\mathcal{E}$ é a álxebra de evolución 2LI do exemplo anterior, entón temos a sucesión exacta curta:

$$1 \longrightarrow \mathrm{Diag}(\Gamma) \xrightarrow{\iota} \mathrm{Aut}(\mathcal{E}) \xrightarrow{\Phi_B} \mathrm{Im}\Phi_B \longrightarrow 1,$$

e particularmente:

$$\frac{\mathrm{Aut}(\mathcal{E})}{\mathrm{Ker}\Phi_B} \simeq \mathrm{Im}\Phi_B.$$

Do mesmo xeito que razoamos na demostración do teorema 4.18, como $\mathrm{Im}\Phi_B$ e $\mathrm{Ker}\Phi_B \simeq \mathrm{Diag}(\Gamma)$ son grupos finitos, entón $\mathrm{Aut}(\mathcal{E})$ é un grupo finito.

Este exemplo lévanos a formular o seguinte problema, que, de ser resolto afirmativamente, implicaría a finitude do grupo de automorfismos das álxebras de evolución 2LI:

Conxectura 5.6. *Sexa $\mathcal{E}$ unha álxebra de evolución 2LI. Entón, o grupo diagonal do grafo asociado $\Gamma(\mathcal{E}, B)$ relativo a unha base natural B de $\mathcal{E}$ é finito.*

Bibliografía

[1] L. Babai. Automorphism groups, isomorphism, reconstruction. In *Handbook of combinatorics, Vol. 1, 2*, pages 1447–1540. Elsevier Sci. B. V., Amsterdam, 1995.

[2] N. Boudi, Y. Cabrera Casado, and M. Siles Molina. Natural families in evolution algebras. *Publ. Mat., Barc.*, 66(1):159–181, 2022.

[3] P. J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[4] C. Costoya, P. Mayorga, and A. Viruel. Permutation representations and automorphisms of evolution algebras. *arXiv preprint arXiv:2401.05924*, 2024.

[5] A. Elduque and A. Labra. Evolution algebras and graphs. *J. Algebra Appl.*, 14(7):1550103, 10, 2015.

[6] A. Elduque and A. Labra. Evolution algebras, automorphisms, and graphs. *Linear and Multilinear Algebra*, 0(0):1–12, 2019.

[7] S. Sriwongsa and Y. M. Zou. On automorphism groups of idempotent evolution algebras. *Linear Algebra Appl.*, 641:143–155, 2022.

[8] J. P. Tian. *Evolution algebras and their applications*, volume 1921 of *Lecture Notes in Mathematics*. Springer, Berlin, 2008.

[9] J. P. Tian and P. Vojtěchovský. Mathematical concepts of evolution algebras in non-Mendelian genetics. *Quasigroups Related Systems*, 14(1):111–122, 2006.