USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Categorías (finitamente) universales

Daniel Lugaresi Palomares

2024/2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO EN MATEMÁTICAS

Traballo Fin de Grao

Categorías (finitamente) universales

Daniel Lugaresi Palomares

Xullo, 2025

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álgebra
Título: Categorías (finitamente) universales
Breve descrición do contido
Introducción a las técnicas del problema de realización de grupos: ejemplos de categorías (finitamente) universales.
Bibliografía
Babai L. (1995). Automorphism groups, isomorphism, reconstruction, in:Handbook of combinatorics, Elsevier Sci. B. V, Amsterdam, volume 2, 1447-1540. Costoya C., Viruel A. (2014) Every finite group is the group of self homotopy equivalences of an elliptic space, Acta Mathematica, 213, 49-62. Costoya C., Viruel A. (2018) On the realizability of group actions, Adv. Math. 336, 299-315. Gareth, A.J. (2021) Realisation of groups as automorphism groups in permutational categories, Ars Math. Contemp. 21 (1). Riehl, E. (2016) Category theory in context, Aurora Dover Modern Math originals. Dover Publications. 234 pp.
Recomendacións

Índice

Resumo

Un dos problemas clásicos que impulsou importantes avances en álxebra é o Problema Inverso de Galois, proposto por Hilbert en 1892. Inspirado por este problema e seguindo unha lóxica semellante, xorde a comezos do século XX o *problema de realización de grupos*, que formula unha cuestión aparentemente sinxela: dada unha categoría $\mathcal{C}$ e un grupo G, existe algún obxecto de $\mathcal{C}$ cuxo grupo de automorfismos sexa isomorfo a G? Cando isto ocorre para todo grupo (finito), dise que a categoría é (finitamente) universal. Un dos primeiros avances neste ámbito débese a R. Frucht, quen en 1939 demostrou que a categoría dos grafos simples finitos é finitamente universal [12]. Dende entón, o problema foi estudado en diversas categorías [3] e continúa a ser, a día de hoxe, un tema de interese na investigación en álxebra.

O obxectivo deste traballo é introducir o problema de realización de grupos, presentar as ferramentas máis relevantes para o seu estudo e aplicar estas técnicas para abordar, por primeira vez na literatura, a universalidade finita da categoría dos *aneis de fusión*, estruturas alxébricas que xorden de forma natural tanto en álxebra como en certos contextos da física teórica dentro do marco actual de investigación.

Abstract

One of the classical problems that has driven significant advances in algebra is the Inverse Galois Problem, proposed by Hilbert in 1892. Inspired by this problem and following a similar logical framework, the group realization problem emerged in the early 20th century, posing a seemingly simple question: given a category $\mathcal{C}$ and a group G, does there exist an object in $\mathcal{C}$ whose automorphism group is isomorphic to G? When this holds for all (finite) groups, the category is said to be (finitely) universal. One of the earliest breakthroughs in this area is due to R. Frucht, who in 1939 proved that the category of finite simple graphs is finitely universal [12]. Since then, the problem has been studied in many categories [3] and remains an active area of

research in Algebra.

The aim of this paper is to introduce the group realization problem, present the most relevant tools for its study and then apply these techniques to address, for the first time in the literature, the finite universality of the category of fusion rings — algebraic structures that naturally arise both in algebra and in certain theoretical physics contexts within the current research framework.

Introdución

Un dos problemas clásicos que deu lugar a importantes desenvolvementos en álxebra é o *Problema Inverso de Galois*, proposto por Hilbert no ano 1892. Este problema formula a seguinte cuestión: dado un grupo finito G, atopar unha extensión de corpos finita $L|_{\mathbb{Q}}$ tal que o seu grupo de Galois sexa isomorfo a G. Trátase dun problema aínda aberto en xeral e a súa relevancia é tal que conta cunha entrada específica na *Mathematics Subject Classification* (MSC 12F12). Este tipo de cuestións, nas que se parte dun grupo abstracto e se procura "realizalo" como o grupo de simetrías dun certo obxecto matemático, serve de inspiración para formulacións análogas en contextos diversos.

Neste traballo ocupámonos do que se coñece como o *Problema de Realización de grupos*, que segue a mesma estrutura lóxica que o problema inverso de Galois. Dada unha categoría fixada $\mathcal{C}$, sabemos que o conxunto dos automorfismos dun obxecto X en $\mathcal{C}$ forma sempre un grupo. Unha cuestión natural que xorde inmediatamente é a seguinte:

Problema. *Dada unha categoría $\mathcal{C}$ e un grupo G, decidir se existe algún $X \in \mathrm{obx}(\mathcal{C})$ tal que o seu grupo de automorfismos sexa isomorfo a G.*

Se ocorre para un grupo G fixado, dicimos que dito grupo é realizable en $\mathcal{C}$. No caso de que a resposta sexa afirmativa para todo grupo G, dicimos que a categoría $\mathcal{C}$ é *universal* e, se se verifica para grupos finitos, falamos de *categoría finitamente universal*.

As categorías (finitamente) universais constitúen unha liña de traballo cun papel destacado nas matemáticas, como evidencian os traballos publicados en revistas de elevado prestixio internacional. Así, un dos primeiros exemplos destacados desta liña de investigación atopámolo no traballo de Robert Frucht, quen demostrou en 1939 [12] que todo grupo finito é isomorfo ao grupo de automorfismos dun grafo simple finito, é dicir, que a categoría dos grafos simples finitos é finitamente universal. Máis tarde, no ano 1960, Gert Sabidussi ampliou este resultado permitindo grafos infinitos, e conseguiu así realizar calquera grupo (non necesariamente finito) como o grupo de automorfismos dun grafo [22]. Dende entón, moitos autores exploraron estruturas distintas co mesmo obxectivo: realizar tódolos grupos finitos (ou, en ocasións, tódolos grupos) como grupos de simetrías da estrutura considerada. Entre os exemplos máis significativos destacan: retículos

distributivos (Birkhoff, 1946, [6]), superficies de Riemann (Greenberg, 1960, [13]), planos proxectivos (Mendelsohn, 1972, [19]), corpos (Fried e Kollár, 1978, [11]), variedades hiperbólicas de volume finito en dimensión fixa (Belolipetsky e Lubotzky, 2005, [5]), espacios elípticos (Costoya e Viruel, 2014, [9]), álxebras conmutativas diferenciais graduadas (Costoya, Méndez e Viruel, 2020, [8]), entre outros (véxase a introducción de [17]).

O noso obxectivo será desenvolver os conceptos fundamentais da teoría de categorías (finitamente) universais e as técnicas do problema de realización de grupos, así como revisar algún dos resultados máis importantes de universalidade. En concreto, detendrémonos no teorema de Frucht, que constitúe unha das ferramentas clave no estudo deste tipo de problemas. No resto do traballo estudaremos, por primeira vez na literatura, a universalidade dunha categoría en concreto: a dos *aneis de fusión*. Estes aneis son estruturas alxébricas de especial interese dentro da investigación en matemáticas [2, 10, 1]; aínda que tamén aparecen en certas ramas da física en auxe, como poden ser a computación cuántica [25] ou a teoría conforme de campos [4].

A continuación, descríbese o contenido de cada capítulo e a organización do traballo. No Capítulo 1 realizarase un breve repaso dos conceptos de teoría de categorías, grupos e aneis necesarios para desenvolver os contidos posteriores.
No Capítulo 2 motívase o problema de realización de grupos, danse as definicións principais e estúdase dito problema en dúas categorías: a dos grupos, que non é finitamente universal, e en contraposición, a dos grafos simples finitos, chegando ao resultado de Frucht, do que comentaremos o seu papel clave nas demostracións de universalidade.
Despois, no Capítulo 3, dase ao lector unha introdución aos aneis de fusión, construíndoos a partir dunha estrutura alxébrica ben coñecida: os aneis asociativos e unitarios. Estúdanse tamén as súas propiedades e proporciónase, a modo de motivación e sen entrar en detalle, un dos exemplos destacados da álxebra en que aparecen este tipo de aneis de xeito natural: o anel de Grothendieck da categoría das representacións de dimensión finita dun grupo finito G sobre $\mathbb{C}$.
No Capítulo 4 preséntase unha construción alternativa e equivalente dos aneis de fusión partindo dun conxunto de regras de fusión, definindo con ela o concepto de morfismo de fusión e a categoría asociada. Finalmente, introdúcense os automorfismos internos dun anel de fusión, analizando as súas propiedades principais. A importancia deste capítulo reside en que se proporcionan as ferramentas necesarias para o estudo da universalidade finita da categoría dos aneis de fusión.
Na última parte do traballo, o Capítulo 5, próbase, por primeira vez na literatura, que a categoría dos aneis de fusión é finitamente universal. Máis concretamente, demóstrase, por un lado, que todo grupo abeliano finito é realizable como o grupo de automorfismos internos dun anel de fusión asociativo; e por outro lado, que todo grupo finito é realizable como o grupo de automorfismos dun anel de fusión non asociativo. Estes resultados constitúen unha achega orixinal ao estudo do *Problema de realización de grupos*.

Capítulo 1

Teoría de categorías

Neste primeiro capítulo, introduciremos a linguaxe de categorías que empregaremos ao longo do traballo e lembraremos algúns conceptos de interese relativos a categorías xa coñecidas como son a dos grupos ou a dos aneis unitarios.

1.1. Categorías e funtores

O propósito desta primeira sección é dar as definicións dos conceptos de *categoría* e *funtor*, así como outras nocións fundamentais da teoría de categorías que serán necesarias en capítulos posteriores. Seguiremos [15].

Definición 1.1. Unha categoría $\mathcal{C}$ é unha *clase de obxectos* $\mathrm{obx}(\mathcal{C})$ equipada con:

- Un conxunto $\mathrm{Hom}_{\mathcal{C}}(A,B)$ para cada $A,B \in \mathrm{Obx}(\mathcal{C})$. A cada elemento deste conxunto chamarémolo *morfismo (de dominio A e codominio B).*
- Unha *lei de composición*, isto é, para cada $A,B,C \in \mathrm{Obx}(\mathcal{C})$, unha aplicación:

$$\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \xrightarrow{\ \circ\ } \mathrm{Hom}_{\mathcal{C}}(A,C)$$

$$(f,g) \longmapsto gf,$$

que debe satisfacer os seguintes tres axiomas: se $A,B,C,D \in \mathrm{Obx}(\mathcal{C})$,

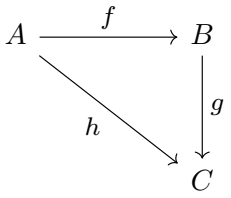
I) Se $(A,B) \neq (C,D)$, entón $\mathrm{Hom}_{\mathcal{C}}(A,B) \cap \mathrm{Hom}_{\mathcal{C}}(C,D) = \emptyset$.

II) A composición é asociativa, isto é, $(hg)f = h(gf)$ para todo $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ e $h \in \mathrm{Hom}_{\mathcal{C}}(C,D)$.

III) Existe elemento unidade, o que quere dicir que para cada $A \in \mathrm{obx}(\mathcal{C})$, existe un único elemento $1_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ tal que $f1_A = f$ se $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ e $1_A g = g$ se $g \in \mathrm{Hom}_{\mathcal{C}}(B,A)$.

Observación 1.2. Sexa $\mathcal{C}$ unha categoría arbitraria e $A, B \in \mathrm{Obx}(\mathcal{C})$. Denotaremos por *frecha* de A en B a cada elemento $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Podemos definir os diagramas conmutativos entre obxectos da mesma maneira que en teoría de conxuntos. Por exemplo, dados $A, B, C \in \mathrm{obx}(\mathcal{C})$ e f unha frecha de A en B, g unha frecha de B en C e h unha frecha de A en C, o diagrama



dise que *conmuta* ou que *é conmutativo* se $gf = h$.

Exemplo 1.3. Vexamos algúns exemplos de categorías xa coñecidos.

- Os conxuntos forman unha categoría que denotaremos $\mathcal{C} = \mathsf{Set}$. Os obxectos son precisamente os conxuntos e, para cada $A, B \in \mathrm{obx}(\mathsf{Set})$, defínese $\mathrm{Hom}_{\mathsf{Set}}(A, B)$ como o conxunto de aplicacións de A en B. A lei de composición é a composición de aplicacións.
- Os grupos tamén forman unha categoría, $\mathcal{C} = \mathsf{Grp}$, onde os obxectos son os grupos e para cada $G, G' \in \mathrm{obx}(\mathcal{C})$, $\mathrm{Hom}_{\mathsf{Grp}}(G, G')$ é o conxunto de homomorfismos de grupos entre G e G'. A lei de composición é a composición de aplicacións (véxase a Sección 1.3.1).
- $\mathcal{C} = \mathsf{Ab}$ é a categoría dos grupos abelianos. É a categoría Grp restrinxida aos grupos abelianos.
- $\mathcal{C} = \mathsf{Ring}$ é a categoría dos aneis unitarios, onde $R \in \mathrm{obx}(\mathcal{C})$ é un anel unitario e tomamos os homomorfismos de aneis e a composición de aplicacións para completar a definición (véxase a Sección 1.3.2).
- Para cada corpo K, $\mathcal{C} = \mathsf{Vect}_K$ a categoría dos espazos vectoriais finito-dimensionais sobre K, onde os obxectos son ditos espazos, os morfismos son as aplicacións lineais entre eles e a lei de composición é a composición de aplicacións.

Notemos que en todos estes exemplos o elemento unidade é sempre a aplicación identidade.

Observación 1.4. En xeral, non se pode pensar en $\mathrm{obx}(\mathcal{C})$ como un conxunto. No caso en que $\mathrm{obx}(\mathcal{C})$ sexa un conxunto, a categoría $\mathcal{C}$ dise que é *pequena*. Por exemplo, Set non é pequena.

Definición 1.5. Sexa $\mathcal{C}$ unha categoría e $A, B \in \mathrm{Obx}(\mathcal{C})$. Unha frecha $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ denomínase *isomorfismo* se existe $g \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ tal que $fg = 1_B$ e $gf = 1_A$.

Observación 1.6. Nas condicións da definición anterior, de existir dita g, é unica e denotarémola $g = f^{-1}$. En efecto, sexa h unha frecha de A en B tal que $fg = 1_B = fh$, entón $(gf)g = (gf)h$,

logo $1_A g = 1_A h$ e así $g = h$. Por outro lado, notemos que $ff^{-1} = 1_B$ e $f^{-1}f = 1_A$, de forma que $(f^{-1})^{-1} = f$. Ademais, $(h^{-1}f^{-1})(fh) = h^{-1}(f^{-1}f)h = h^{-1}(1_A h) = h^{-1}h = 1_B$ e viceversa, co que, pola unicidade, $(fh)^{-1} = h^{-1}f^{-1}$.

Definición 1.7. Sexa $\mathcal{C}$ unha categoría e $A \in \mathrm{obx}(\mathcal{C})$. Unha frecha $f \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ dise que é un *automorfismo* de A se f é un isomorfismo.

Proposición 1.8. *Sexa $\mathcal{C}$ unha categoría e $A \in \mathrm{obx}(\mathcal{C})$. O conxunto de automorfismos de A, $\mathrm{Aut}_{\mathcal{C}}(A)$, ten estrutura de grupo coa lei de composición da categoría en cuestión.*

Demostración. Comprobemos as propiedades. Sexan $f, g, h \in \mathrm{Aut}_{\mathcal{C}}(A)$.

(I) *Asociatividade*: por definición, $(fg)h = f(gh)$.

(II) *Elemento neutro*: $f = 1_A \in \mathrm{Aut}_{\mathcal{C}}(A)$ é o elemento neutro.

(III) *Inversos*: f^{-1} existe por definición de isomorfismo, como vimos na Observación 1.6.

□

É sinxelo caracterizar os grupos de automorfismos das categorías do Exemplo 1.3 como aqueles morfismos que teñen inversa respecto á composición de funcións, pois se pode comprobar fácilmente que dita inversa é tamén un morfismo na categoría en cuestión.

Definición 1.9. Consideremos $\mathcal{C}$ e $\mathcal{D}$ dúas categorías. Un *funtor (covariante)* F de $\mathcal{C}$ en $\mathcal{D}$, $F : \mathcal{C} \to \mathcal{D}$, está formado por unha aplicación $F : \mathrm{obx}(\mathcal{C}) \to \mathrm{obx}(\mathcal{D})$ (coa notación $F(A) = FA$) e ademais, para cada $A, B \in \mathrm{obx}(\mathcal{C})$, unha aplicación $F : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(FA, FB)$ inducida por F que cumpre:

- $F(1_A) = 1_{FA}$,
- $F_{AC}(gf) = F_{BC}(g)F_{AB}(f)$ para cada $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ e $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$.

Definición 1.10. Tomemos $\mathcal{C}, \mathcal{D}$ dúas categorías e F un funtor de $\mathcal{C}$ en $\mathcal{D}$. F dise *fiel* se a aplicación inducida F_{AB} é inxectiva para todo $A, B \in \mathrm{obx}(C)$. F dise *pleno* se F_{AB} é sobrexectiva para todo $A, B \in \mathrm{obx}(C)$.

1.2. Algúns tipos especiais de categorías

Co obxectivo de introducir un exemplo a modo de motivación no Capítulo 3, será necesario definir certos tipos especiais de categorías. Dado que o estudo en profundidade destes conceptos escápase dos obxectivos do traballo, deselvolverémolos brevemente buscando comprender as ideas clave, e remitimos ao lector interesado en profundizar máis ás referencias empregadas [20] e [18].

Definición 1.11. Sexa $\mathcal{A}$ unha categoría. $\mathcal{A}$ dise *aditiva* se cada conxunto $\mathrm{Hom}_{\mathcal{A}}(A, B)$ está dotado dunha estrutura de grupo abeliano e satisfai os seguintes axiomas:

1. A composición é bilinear respecto á estrutura de grupo abeliano.
2. Existe un *obxecto* 0, de forma que existe un único morfismo $f : A \to 0$ e outro $g : 0 \to A$, para todo $A \in \mathrm{obx}(\mathcal{A})$.
3. Para cada par de obxectos $A, B \in \mathrm{obx}(\mathcal{A})$, existe un obxecto *suma directa* $A \oplus B \in \mathrm{Obx}(\mathcal{A})$.

Definición 1.12. Sexa $\mathcal{A}$ unha categoría aditiva. Defínese o *núcleo* dun morfismo $f : A \to B$, $\mathrm{Ker}(f)$, como un obxecto K xunto cun morfismo $k : K \to A$ tal que $fk = 0$ e de forma que é único salvo isomorfismos. Defínese o *conúcleo* dun morfismo $f : A \to B$, $\mathrm{Coker}(f)$, como un obxecto C xunto cun morfismo $c : B \to C$ tal que $cf = 0$ e de forma que é único salvo isomorfismos. Cómpre notar que o núcleo e o conúcleo dun morfismo non sempre existen.

Definición 1.13. Sexa $\mathcal{A}$ unha categoría aditiva. $\mathcal{A}$ dise *abeliana* se existen o núcleo e o conúcleo de todo morfismo $f : A \to B$ e este admite unha factorización canónica a través dos mesmos. Diremos ademais que un morfismo $f : A \to B$ é un *monomorfismo* se $\mathrm{Ker}(f) = 0$ e un *epimorfismo* se $\mathrm{Coker}(f) = 0$.

Observación 1.14. Nunha categoría abeliana, se temos un morfismo $f : A \to B$ con

$$\ker(f) : K \xrightarrow{k} A \quad \text{e} \quad \mathrm{coker}(f) : B \xrightarrow{c} C,$$

podemos definir a *coimaxe* de f como

$$\mathrm{coim}(f) := \mathrm{coker}(k),$$

e a *imaxe* de f como:

$$\mathrm{im}(f) := \ker(c).$$

En xeral, pódese probar que existe un isomorfismo canónico $\phi : \mathrm{coim}(f) \to \mathrm{im}(f)$, de forma que a factorización canónica de f é a seguinte:

$$A \to \mathrm{coim}(f) \xrightarrow{\phi} \mathrm{im}(f) \to B.$$

Definición 1.15. Sexa $\mathcal{A}$ una categoría abeliana. Un obxecto $S \in \mathrm{Obx}(\mathcal{A})$ dise *simple* se todo monomorfismo $f : A \to S$ en $\mathcal{A}$ é isomorfo á inclusión $0 \hookrightarrow S$ ou á unidade $1_S : S \hookrightarrow S$. De xeito intuitivo, S non ten subobxectos propios non triviais, só o 0 e el mesmo.

Definición 1.16. Sexa $\mathcal{A}$ unha categoría abeliana. Dicimos que $\mathcal{A}$ é *semisimple* se todo obxecto de $\mathcal{A}$ é suma directa finita de obxectos simples. Deste xeito e tendo en conta a definición anterior, podemos atopar unha "base" de obxectos simples $\{S_i\}_{i \in I}$ de maneira que tódolos obxectos de $\mathcal{A}$ poden descompoñerse como suma directa deles.

Definición 1.17 (Categoría monoidal ríxida)**.** Una *categoría monoidal ríxida* é una *categoría monoidal* $(\mathcal{C}, \otimes, \mathbf{1})$, ou sexa, dotada dun obxecto unidade $\mathbf{1} \in \mathrm{Obx}(\mathcal{C})$ e dun funtor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ chamado *produto tensorial*; na que ademais cada obxecto $X \in \mathrm{Obx}(\mathcal{C})$ posúe un *dual pola esquerda* X^* e un *dual pola dereita* ${}^*X$, xunto cos respectivos morfismos chamados *evaluación* e *coevaluación*:

$$\mathrm{ev}_X : X^* \otimes X \to \mathbf{1}, \qquad \mathrm{coev}_X : \mathbf{1} \to X \otimes X^*,$$
$$\mathrm{ev}'_X : X \otimes {}^*X \to \mathbf{1}, \qquad \mathrm{coev}'_X : \mathbf{1} \to {}^*X \otimes X,$$

tales que:

$$(Id_X \otimes \mathrm{ev}_X) \circ (\mathrm{coev}_X \otimes Id_X) = Id_X,$$
$$(\mathrm{ev}'_X \otimes Id_X) \circ (Id_X \otimes \mathrm{coev}'_X) = Id_X.$$

1.3. Teoría de grupos e aneis

Como se expuxo no Exemplo 1.3, os grupos e os aneis unitarios conforman as súas respectivas categorías. En todo este texto empregaranse conceptos fundamentais da teoría de grupos e aneis, polo que cómpre establecer a notación e lembrar aqueles elementos de interese e algúns resultados xa coñecidos. As referencias utilizadas nesta sección son [14], [21] e [16].

1.3.1. Grupos e a súa categoría

Definición 1.18. Un *grupo* $(G, \cdot)$ é un conxunto G dotado dunha operación binaria $\cdot : G \times G \to G$ que é asociativa e para a que existe un elemento neutro 1 e un elemento inverso g^{-1} para cada elemento $g \in G$. Se ademais é conmutativa, G dirase *abeliano*. Xeralmente nos referimos ao grupo $(G, \cdot)$ polo nome G do conxunto subxacente.
A *orde* do grupo é a cardinalidade do conxunto G. Diremos que G é finito se a súa orde é finita.

Observación 1.19. Na maioría dos casos en que tratemos con grupos abelianos, cambiaremos a notación *multiplicativa* (operación: $\cdot$, neutro: 1 e inversos: g^{-1}) pola notación *aditiva* (operación: $+$, neutro: 0 e *opostos*: $-g$).

Notación 1.20. Sexa G un grupo. Empregaremos a seguinte notación:

- $H \leq G$ para denotar un subgrupo H de G, ou $H \triangleleft G$ se o subgrupo é normal.
- Denotaremos a orde de G por $|G|$ ou por $\mathrm{ord}(G)$.

Dados G e H grupos, defínese un *homomorfismo de grupos* como unha aplicación $f : G \to H$ que preserva a operación, é dicir, tal que $f(ab) = f(a)f(b)$, para cada $a, b \in G$. É sinxelo comprobar que todo homomorfismo de grupos $f : G \to H$ cumpre $f(1) = 1$, que a identidade é

un homomorfismo de grupos e que o conxunto $\mathrm{Hom}_{\mathsf{Grp}}(G, H)$ de homomorfismos de grupos entre G e H é pechado para a composición de aplicacións.

Deste xeito, pódese definir a categoría $\mathcal{C} = \mathsf{Grp}$, como se fixo no Exemplo 1.3.

Conceptos de interese

Teorema 1.21. (Orde e existencia de subgrupos.) *Sexa G un grupo finito. Entón:*

1. *A orde de todo subgrupo de G divide á orde de G, en particular, a orde de todo elemento $g \in G$ divide á orde de G.*
2. *Se G é un grupo cíclico de orde n, entón para cada divisor $d|n$, G ten un único subgrupo de orde d.*

Definición 1.22. Sexa G un grupo. Defínese o *centro* de G, $Z(G)$, como o conxunto de elementos que conmutan con calquera outro, isto é,

$$Z(G) = \{a \in G : ax = xa, \quad \text{para todo} \quad x \in G\}.$$

Proposición 1.23. *Sexa G un grupo. Entón $Z(G)$ é un subgrupo normal de G e se $G/Z(G)$ é cíclico, entón G é abeliano.*

Enunciaremos agora os teoremas de isomorfía e o de correspondencia de grupos para fixar a notación.

Teorema 1.24. (Primeiro teorema de isomorfía.) *Sexa $f : G \to H$ un homomorfismo de grupos. Entón*

$$G/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

Teorema 1.25. (Segundo teorema de isomorfía.) *Sexa G un grupo e H, K subgrupos normais de G tales que K é á súa vez un subgrupo normal de H. Tense*

$$\frac{G/K}{H/K} \cong G/H.$$

Teorema 1.26. (Teorema de correspondencia de grupos.) *Sexa G un grupo e H un subgrupo normal de G. Os subgrupos de G/H son os grupos cociente da forma K/H tales que K é un subgrupo de G con $H \subset K$.*

Definición 1.27. Sexa G un grupo e X un conxunto. Unha *acción de grupo (pola esquerda) de G sobre X* é unha aplicación $f : G \times X \to X$, coa notación $f(g, x) = gx$ que verifica:

1. $g(g'x) = (gg')x$, para todo $g, g' \in G$ e para todo $x \in X$.
2. $1x = x$, para todo $x \in X$.

A acción pola dereita defínese de xeito análogo.

Grupo libre

Sexa X un conxunto e X^{-1} un conxunto bixectivo con X tal que $X \cap X^{-1} = \emptyset$. Tomemos tamén un conxunto $\{1\}$ tal que $\{1\} \cap (X \cup X^{-1}) = \emptyset$.

Definición 1.28. Definimos as *palabras* en X como as expresións da forma $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$, con $\varepsilon_i \in \{0, 1, -1\}$, para cada $i \in \{1, \ldots, n\}$. A palabra $1 \cdots 1$ é a *palabra baleira*. O conxunto $F(X)$ de *palabras reducidas* (*i.e.*, eliminando os 1 e os elementos consecutivos iguais con superíndices opostos), xunto coa palabra baleira e coa operación *xustaposición* (entendendo por isto pegar as palabras e logo calcular a reducida) é un grupo, chamado *grupo libre sobre* X.

Proposición 1.29. (Propiedade universal do grupo libre.) *O grupo libre $F(X)$ é o único grupo tal que dado un grupo G e unha aplicación $f : X \to G$ existe un único homomorfismo de grupos $h : F(X) \to G$ con $h \circ \iota = f$ (con ι a aplicación inclusión).*

Definición 1.30. Unha *presentación (libre)* de grupo é unha expresión da forma $\langle X \mid R \rangle$ onde X é un conxunto e R é un subconxunto do grupo libre sobre X. Toda presentación de grupo define un grupo da forma $\langle X \mid R \rangle = F(X)/R_{\triangleleft}$, sendo $R_{\triangleleft}$ o subgrupo normal de $F(X)$ xerado por $R \subset F(X)$. O conxunto X denomínase *conxunto de xeradores* e R *conxunto de relacións*.

Proposición 1.31. *Todo grupo G admite unha presentación. Isto é, todo grupo é cociente dun grupo libre.*

Grupos abelianos

Definición 1.32. Nas condicións da Definición 1.28, o *conmutador* de dous elementos $x, x' \in X$ é a palabra $[x, x'] = xx'x^{-1}(x')^{-1}$. Consideremos $R = \{[x, x'] : x, x' \in X\}$. Así, o *grupo abeliano libre* sobre X é o grupo dado pola presentación $F_{ab}(X) = \langle X \mid R \rangle$.

Teorema 1.33. (Teorema de estrutura de grupos abelianos finitos). *Sexa G un grupo abeliano finito de orde $|G| = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, con $p_1, \ldots, p_m$ números primos e $\alpha_1, \ldots, \alpha_n$ enteiros positivos. Entón*

$$G \cong G_{(p_1)} \oplus \cdots \oplus G_{(p_m)},$$

onde, para cada $i \in \{1, \ldots, m\}$,

$$G_{p_i} = \mathbb{Z}_{p_i^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{k_n}},$$

para certos enteiros positivos $k_1, \ldots, k_n$. Denótase por $\mathbb{Z}_{p_i^{k_j}}$ ao grupo cíclico de orde $p_i^{k_j}$, $\mathbb{Z}/p_i^{k_j}\mathbb{Z}$.

Definición 1.34. Sexa G un grupo abeliano finito. Definimos $\mathrm{Tor}_2(G)$ como o conxunto de elementos de G de orde 2, engadindo $0 \in \mathrm{Tor}_2(G)$.

Observación 1.35. Notemos que $\mathrm{Tor}_2(G)$ é un subgrupo de G para todo grupo abeliano finito G, pois se $h, g \in \mathrm{Tor}_2(G)$, entón

$$2(h+g) = 2h + 2g = 0 + 0 = 0,$$

co que $h + g \in \mathrm{Tor}_2(G)$; a asociatividade herédase de G, o elemento neutro é $0 \in \mathrm{Tor}_2(G)$ e o oposto dun elemento de orde 2 é el mesmo.

Proposición 1.36. *Sexa $\{G_i\}_{i\in I}$ un conxunto de grupos abelianos finitos, onde o cardinal $|I| = n$. Entón*

$$\mathrm{Tor}_2\left(\bigoplus_{i\in I} G_i\right) = \bigoplus_{i\in I} \mathrm{Tor}_2(G_i).$$

Demostración. Sexa $(g_1, \ldots, g_n) \in \mathrm{Tor}_2\left(\bigoplus_{i\in I} G_i\right)$. Entón $2(g_1, \ldots, g_n) = 0$, co que $(2g_1, \ldots, 2g_n) = 0$ e así $2g_i = 0$, para todo $i \in I$. Recíprocamente, se $(g_1, \ldots, g_n) \in \bigoplus_{i\in I} \mathrm{Tor}_2(G_i)$, entón $(2g_1, \ldots, 2g_n) = 0$, co que $2(g_1, \ldots, g_n) = 0$, e así $(g_1, \ldots, g_n) \in \mathrm{Tor}_2\left(\bigoplus_{i\in I} G_i\right)$. □

Proposición 1.37. (Xeralización de [21], Theorem 2.30) *Sexa $\{G_i\}_{i\in I}$ un conxunto finito de grupos abelianos finitos e $\{H_i\}_{i\in I}$ un conxunto de subgrupos normais de forma que $H_i \triangleleft G_i$, para cada $i \in I$. Entón*

$$\frac{\bigoplus_{i\in I} G_i}{\bigoplus_{i\in I} H_i} \cong \bigoplus_{i\in I} G_i/H_i.$$

Demostración. A aplicación

$$\begin{aligned} \textstyle\bigoplus_{i\in I} G_i &\longrightarrow \textstyle\bigoplus_{i\in I} G_i/H_i \\ (g_1, \ldots, g_n) &\longmapsto (g_1 + H_1, \ldots, g_n + H_n), \end{aligned}$$

é un homomorfismo de grupos. En efecto, é evidente tendo en conta que, para cada $i \in I$, $(g_i + H_i) + (h_i + H_i) = (g_i + h_i)H_i$. Ademais, como cada aplicación $\phi_i : G_i \to G_i/H_i$ con $g_i \mapsto g_i + H_i$ é sobrexectiva, ϕ tamén o é. Por último, calculemos o núcleo de ϕ:

$$\mathrm{Ker}(\phi) = \left\{ (g_1, \ldots, g_n) \in \bigoplus_{i\in I} G_i : g_i \in H_i, \quad \text{para todo} \quad i \in I \right\} = \bigoplus_{i\in I} H_i.$$

Finalmente, aplicando o Primeiro Teorema de isomorfía (Teorema 1.24), concluímos a proba. □

1.3.2. Aneis e a súa categoría

Definición 1.38. Un *anel* é un conxunto R dotado de dúas operacións binarias $+ : R \times R \to R$ (suma) e $\cdot : R \times R \to R$ (produto), de forma que $(R, +)$ é un grupo abeliano e a operación $\cdot$ é distributiva respecto de $+$. Ademais:

- Se $\cdot$ é asociativa, diremos que o anel é *asociativo*.
- Se existe elemento neutro 1 para o produto, diremos que o anel é *unitario*.

No caso en que $(R, \cdot)$ cumpra as dúas condicións anteriores, diremos que R é un *anel asociativo e unitario*. Por último, se $\cdot$ é conmutativa, R dise que é un *anel conmutativo*.

Ao igual que cos grupos, denotaremos un anel $(R, +, \cdot)$ polo nome R do conxunto subxacente.

Consideraremos de agora en adiante aneis unitarios.

Definimos o concepto de *homomorfismo de aneis* como unha aplicación entre dous aneis R e S, $f : R \to S$, que preserva o neutro multiplicativo, a suma e o produto, ou sexa, $f(1) = 1$ e, para todo $x, y \in A$, $f(x + y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$. É sinxelo comprobar que a composición de homomorfismos de aneis é un homomorfismo de aneis e que a identidade tamén o é.

Desta maneira, obtemos a categoría $\mathcal{C} = \mathsf{Ring}$ dos aneis unitarios como no Exemplo 1.3.

Necesitaremos máis adiante o concepto de *anti-isomorfismo de aneis*.

Definición 1.39. Sexan R e S dous aneis calquera e $f : R \to S$ unha bixección. Entón f dise que é un *anti-isomorfismo de aneis* se preserva o neutro multiplicativo e a suma e ademais cumpre:

$$f(x \cdot y) = f(y) \cdot f(x), \quad \text{para todo} \quad x, y \in R \quad \text{(Anti-produto)}.$$

Anel grupo

Definición 1.40. Sexa R un anel asociativo e unitario e G un grupo. Chamamos *anel grupo de G sobre R* ao anel $(R[G], +, \cdot)$, onde:

$$R[G] = \left\{ \sum_{g \in G} a_g g : a_g \in R, \quad \text{e case todo} \quad a_g = 0 \right\}.$$

Notemos que as expresións $\sum_{g \in G} a_g g$ son formais e denotan as combinacións lineais sobre R dos elementos de G. A suma e a multiplicación defínense do xeito esperado:

$$\sum_{g \in G} a_g g \; + \; \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) gh.$$

Observación 1.41. É sinxelo comprobar que $R[G]$ é un anel asociativo e unitario, sendo o neutro para a suma $0 = \sum_{g \in G} 0_R g$, onde 0_R denota o neutro para a suma do anel R; e os elementos

opostos $-(\sum_{g\in G} a_g g) = \sum_{g\in G}(-a_g)g$. Por último, o neutro para o produto é $1 = \sum_{g\in G} 1_R g$, onde 1_R é o neutro para o produto do anel R.
Notemos que se identificamos cada elemento do anel $r \in R$ e cada elemento do grupo $g \in G$ cos respectivos $r1_G$ (1_G é o neutro do grupo G) e $1_R g$, podemos considerar R como un subanel de $R[G]$ e G como un subgrupo do grupo de unidades de $R[G]$, que denotaremos $\mathcal{U}(R[G])$.

Exemplo 1.42. Consideremos o grupo (cíclico) multiplicativo $\mathbb{Z}/2\mathbb{Z} = \{\mathbf{1}, \tau\}$ e o anel asociativo e unitario $\mathbb{Z}$. Entón, podemos construír o anel grupo $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$, onde os elementos teñen a seguinte expresión:

$$a + b\tau,\ a, b \in \mathbb{Z}.$$

Se $a, b \in \mathbb{Z}$, a suma sería da forma:

$$(a + b\tau) + (c + d\tau) = (a + c) + (b + d)\tau,$$

onde os elementos entre parénteses súmanse como no anel $\mathbb{Z}$. E a multiplicación:

$$(a + b\tau)(c + d\tau) = ac + bc\tau + ad\tau + bd\tau^2 = (ac + bd) + (bc + ad)\tau,$$

onde os elementos entre parénteses súmanse e multiplícanse como no anel.

Consideracións de teoría de módulos sobre aneis

Fixemos A un anel conmutativo e unitario.

Definición 1.43. Un *$A-$módulo* é un grupo abeliano G equipado cunha operación externa $A \times G \to G$, $(a, g) \mapsto ag$ que satisfai, para cada $g, h \in G$ e cada $a, b \in A$,

- $(ab)g = a(bg)$,
- $(a + b)g = ag + bg$,
- $a(g + h) = ag + ah$,
- $1_A g = g$.

En particular, se A é un corpo, entón un $A-$módulo é un $A-$espazo vectorial.

Observación 1.44. Un grupo abeliano G é equivalente a un $\mathbb{Z}-$módulo mediante

$$n \cdot g = \begin{cases} \overbrace{g + \cdots + g}^{n)}, & \text{se } n > 0, \\ 0, & \text{se } n = 0, \\ \underbrace{(-g) + \cdots + (-g)}_{-n)}, & \text{se } n < 0, \end{cases}$$

con $n \in \mathbb{Z}$.

Capítulo 2

O problema de realización de grupos: categorías (finitamente) universais.

Dada unha categoría fixada $\mathcal{C}$, sabemos que o conxunto dos automorfismos dun obxecto $X \in \mathrm{obx}(\mathcal{C})$ forma sempre un grupo (véxase a Proposición 1.8), que se denota por $\mathrm{Aut}_{\mathcal{C}}(X)$. Unha cuestión natural que xorde inmediatamente é a seguinte:

Problema 2.1. *Dada unha categoría $\mathcal{C}$ e un grupo G, decidir se existe algún $X \in \mathrm{obx}(\mathcal{C})$ tal que o seu grupo de automorfismos $\mathrm{Aut}_{\mathcal{C}}(X)$ sexa isomorfo a G.*

No caso de que a resposta sexa afirmativa para todo grupo G, dicimos que a categoría $\mathcal{C}$ é *universal* e, se se verifica para grupos finitos, falamos de *categoría finitamente universal*.

Tal e como comentamos na introdución, as categorías (finitamente) universais, cuxo estudo comeza a principios do século XX, conforman un campo de estudo de gran relevancia dentro do panorama actual da investigación matemática. Ao longo deste capítulo, veremos que non toda categoría posúe esta propiedade; de feito, a propia categoría dos grupos serve como contraexemplo. En contraste, analizaremos o traballo de Frucht, probando que a categoría dos grafos simples finitos é finitamente universal, resultado que constitúe un pilar fundamental no desenvolvemento do estudo deste tipo de categorías. A referencia principal empregada nesta parte do capítulo é [3].

Recordamos as definicións xa vistas no parágrafo de introducción:

Definición 2.2. Sexa $\mathcal{C}$ unha categoría. Un grupo G dise *realizable* en $\mathcal{C}$ se existe $X \in \mathrm{obx}(\mathcal{C})$ tal que $\mathrm{Aut}_{\mathcal{C}}(X)$ e G son isomorfos.

Exemplo 2.3. O grupo multiplicativo $G = \mathbb{Z}/2\mathbb{Z}$ é realizable na categoría dos grupos $\mathcal{C} = \mathsf{Grp}$. En efecto, sexa o grupo

$$\mathbb{Z}/3\mathbb{Z} = \langle g \mid g^3 = 1 \rangle = \{1, g, g^2\}.$$

Calculemos os posibles automorfismos de $\mathbb{Z}/3\mathbb{Z}$. En primeiro lugar temos sempre o automorfismo identidade $\sigma_1 = Id_{\mathbb{Z}/3\mathbb{Z}} \in \mathrm{Aut}_{\mathcal{C}}(\mathbb{Z}/3\mathbb{Z})$. Por outro lado, se $\sigma_2 \in \mathrm{Aut}_{\mathcal{C}}(\mathbb{Z}/3\mathbb{Z})$ é distinto da identidade, como necesariamente $\sigma_2(1) = 1$ e ten que ser bixectiva, a única opción que temos é que $\sigma_2(g) = g^2$, e queda determinado o automorfismo, con $\sigma_2(g^2) = \sigma_2(g)\sigma_2(g) = g^4 = g^3g = 1g = g$. Así,

$$\mathrm{Aut}_{\mathcal{C}}(\mathbb{Z}/3\mathbb{Z}) = \{\sigma_1, \sigma_2\},$$

onde o neutro para a composición é σ_1 e $\sigma_2^2 = \sigma_1$. Como hai un único grupo de orde 2 salvo isomorfismos, $\mathrm{Aut}_{\mathcal{C}}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Definición 2.4. Sexa $\mathcal{C}$ unha categoría arbitraria. Dicimos que $\mathcal{C}$ é *(finitamente) universal* se para todo grupo (finito) G existe $X \in \mathrm{obx}(\mathcal{C})$ tal que $\mathrm{Aut}_{\mathcal{C}}(X) \cong G$. Equivalentemente, unha categoría $\mathcal{C}$ é (finitamente) universal se, e só se todo grupo (finito) é realizable en $\mathcal{C}$.

Dada a natureza combinatoria dos grafos e o feito de que todo grupo finito pode realizarse como grupo de automorfismos dun grafo finito, o esquema básico da maior parte das demostracións de universalidade consiste en tomar un grafo cun grupo de automorfismos dado, e codificalo noutro tipo de estrutura: nun corpo, nun espazo racional, nunha álxebra de evolución, etc. Esta codificación baséase na construción dun funtor que sexa suficientemente "bo" e que permita trasladar información dende a categoría universal coñecida á categoría que se desexa estudar:

Teorema 2.5. *Sexa $\mathcal{C}$ unha categoría (finitamente) universal e $\mathcal{D}$ outra categoría arbitraria. Se existe un funtor $F : \mathcal{C} \to \mathcal{D}$ que é fiel e pleno, enton $\mathcal{D}$ é (finitamente) universal.*

Demostración. Primeiro, se F é fiel e pleno, entón a aplicación F_{AB} asociada a F (véxase a Definición 1.9), con $A, B \in \mathrm{obx}(\mathcal{C})$, é bixectiva e cumpre, por definición de funtor,

$$F_{AC}(gf) = F_{BC}(g)F_{AB}(f) \quad \text{para cada} \quad f \in \mathrm{Hom}_{\mathcal{C}}(A, B) \quad \text{e} \quad g \in \mathrm{Hom}_{\mathcal{C}}(B, C).$$

Notemos entón que se $X \in \mathrm{obx}(\mathcal{C})$, a aplicación F_{XX} induce un isomorfismo de grupos de forma que $\mathrm{Aut}_{\mathcal{C}}(X) \overset{F_{XX}}{\cong} \mathrm{Aut}_{\mathcal{D}}(FX)$. Agora, tomemos G un grupo finito. Por ser $\mathcal{C}$ finitamente universal, existe $X \in \mathrm{obx}(\mathcal{C})$ tal que $\mathrm{Aut}_{\mathcal{C}}(X) \cong G$. Polo isomorfismo anterior,

$$\mathrm{Aut}_{\mathcal{D}}(FX) \cong \mathrm{Aut}_{\mathcal{C}}(X) \cong G,$$

co que G é realizable en $\mathcal{D}$. Dado que G era arbitrario, $\mathcal{D}$ é finitamente universal. □

2.1. Existencia de categorías non finitamente universais: $\mathcal{C} = \mathsf{Grp}$

Acabamos de ver que existen grupos finitos realizables na categoría dos grupos (véxase o Exemplo 2.3). Sen embargo, como veremos nesta sección, non todo grupo finito pode ser realizado

en dita categoría, concluíndo que nin sequera a propia categoría dos grupos, $\mathcal{C} = \mathsf{Grp}$, é capaz de realizar tódolos grupos finitos.

Definición 2.6. Dado G un grupo e $a \in G$, a aplicación $\gamma_a : G \to G$ definida por $\gamma_a(x) = axa^{-1}$, para todo $x \in G$ denomínase *conxugación (pola esquerda) por* a. Chamaremos *automorfismos interiores de* G ao conxunto $\mathrm{Inn}(G) = \{\gamma_a : a \in G\}$.

Recordemos que $Z(G)$ denota o centro do grupo G introducido na Definición 1.22.

Lema 2.7. *Sexa G un grupo e $a \in G$. Tense que:*

1. *A aplicación γ_a é un automorfismo de grupos.*
2. *O conxunto $\mathrm{Inn}(G)$ é un grupo coa composición de aplicacións.*
3. *$G/Z(G) \cong \mathrm{Inn}(G)$.*

Demostración. 1. Para ver que $\gamma_a \colon G \to G$, definida por $\gamma_a(x) = axa^{-1}$, é un isomorfismo de grupos, primeiro comprobamos que é un homomorfismo. Dado $x, y \in G$, temos:

$$\gamma_a(xy) = a(xy)a^{-1} = (ax)(a^{-1}a)(ya^{-1}) = (axa^{-1})(aya^{-1}) = \gamma_a(x)\gamma_a(y),$$

polo que γ_a conserva a operación, é dicir, é un homomorfismo. Para ver que é sobrexectiva, tomamos $x \in G$ e consideramos:

$$\gamma_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = x,$$

así que $\mathrm{Im}(\gamma_a) = G$, polo que γ_a é sobrexectiva. Finalmente, para demostrar que é inxectiva:

$$\mathrm{Ker}(\gamma_a) = \{x \in G : \gamma_a = 1\} = \{x \in G : axa^{-1} = 1\} = \{x \in G : x = aa^{-1}\} = \{1\}.$$

Concluímos que γ_a é un isomorfismo.

2. Imos ver agora que o conxunto $\mathrm{Inn}(G) = \{\gamma_a : a \in G\}$ forma un subgrupo de $\mathrm{Aut}(G)$:

   - *Clausura por composición*: para $a, b \in G$ e $x \in G$,

     $$(\gamma_a \circ \gamma_b)(x) = \gamma_a(bxb^{-1}) = abx(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = \gamma_{ab}(x),$$

     así que $\gamma_a \circ \gamma_b = \gamma_{ab} \in \mathrm{Inn}(G)$.
   - *Asociatividade*: séguese da asociatividade da composición de funcións.
   - *Elemento neutro*: $\gamma_1(x) = 1x1^{-1} = x$ para todo $x \in G$, logo $\gamma_1 = Id_G$ é o neutro.
   - *Inversos*:

     $$(\gamma_{a^{-1}} \circ \gamma_a)(x) = \gamma_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = x,$$

     polo que $\gamma_{a^{-1}} = \gamma_a^{-1}$, e γ_a é invertible en $\mathrm{Inn}(G)$.

3. Para demostrar que $G/Z(G) \cong \mathrm{Inn}(G)$, definimos a aplicación:

$$\begin{aligned} G &\longrightarrow \mathrm{Inn}(G) \\ a &\longmapsto \gamma_a. \end{aligned}$$

Esta aplicación é un homomorfismo, xa que

$$f(ab) = \gamma_{ab} = \gamma_a \circ \gamma_b = f(a)f(b),$$

segundo vimos anteriormente.

Estudamos agora o núcleo:

$$\begin{aligned} \ker(f) &= \{a \in G : \gamma_a = Id_G\} = \{a \in G : axa^{-1} = x \text{ para todo } x \in G\} \\ &= \{a \in G : ax = xa \text{ para todo } x \in G\} = Z(G). \end{aligned}$$

Como $\mathrm{Im}(f) = \mathrm{Inn}(G)$, aplicando o primeiro teorema de isomorfía (Teorema 1.24) temos:

$$G/Z(G) \cong \mathrm{Inn}(G). \qquad \square$$

Teorema 2.8. *A categoría $\mathcal{C} = \mathsf{Grp}$ non é finitamente universal.*

Demostración. Por redución ao absurdo, supoñamos que $\mathcal{C} = \mathsf{Grp}$ é finitamente universal. Entón, para cada $p \in \mathbb{Z}$ impar, o grupo multiplicativo $G = \mathbb{Z}/p\mathbb{Z} = \langle g \mid g^p = 1 \rangle$ cumpre que existe un grupo $G' \in \mathrm{obx}(\mathsf{Grp})$ tal que $\mathrm{Aut}_{\mathsf{Grp}}(G') \cong \mathbb{Z}/p\mathbb{Z}$.

Agora ben, empregando o Lema 2.7, $\mathrm{Inn}(G') \subset \mathrm{Aut}_{\mathsf{Grp}}(G')$, co que podemos definir o homomorfismo inclusión para ver $\mathrm{Inn}(G')$ como un subgrupo de $\mathrm{Aut}_{\mathsf{Grp}}(G')$:

$$\iota : G'/Z(G') \cong \mathrm{Inn}(G') \lhook\joinrel\longrightarrow \mathrm{Aut}_{\mathsf{Grp}}(G') \cong \mathbb{Z}/p\mathbb{Z}.$$

Agora, o feito de que $\mathrm{Aut}_{\mathsf{Grp}}(G') \cong \mathbb{Z}/p\mathbb{Z}$ indica que $\mathrm{Aut}_{\mathsf{Grp}}(G')$ é cíclico e, polo tanto, todo subgrupo tamén o é, en particular $\mathrm{Inn}(G')$.

Distingamos dous casos:

- Se $\mathrm{Inn}(G')$ non é trivial, entón existe $a \in G'$ con $a \notin Z(G')$ tal que $\mathrm{Inn}(G') = \langle \gamma_a \rangle$ (posto que $\gamma_a = Id_{G'}$ para todo $a \in Z(G')$). Agora ben, como $a \notin Z(G')$, existe $b \in G'$ tal que non conmuta con a. Finalmente, dado $\gamma_b \in \mathrm{Inn}(G')$, existe $s \in \mathbb{Z}$ tal que $\gamma_b = (\gamma_a)^s$, e como $ab \neq ba$,

$$\begin{aligned} a \neq bab^{-1} = \gamma_b(a) = (\gamma_a)^s(a) &= \underbrace{(\gamma_a \circ \cdots \circ \gamma_a)}_{\text{s)}}(a) \\ &= \underbrace{a \cdots a}_{\text{s)}}\ a\ \underbrace{a^{-1} \cdots a^{-1}}_{\text{s)}} = a^s a a^{-s} = a^{s+1-s} = a, \end{aligned}$$

o cal é unha contradición.

- Se $\mathrm{Inn}(G') = \{Id_{G'}\}$ entón, como $\mathrm{Inn}(G') \cong G'/Z(G')$, terase que $G'/Z(G')$ é o grupo trivial, co que $G' = Z(G')$ e G' é abeliano. Agora ben, isto implica que a aplicación

$$\begin{aligned} i : G' &\longrightarrow G' \\ h &\longmapsto i(h) = h^{-1}, \end{aligned}$$

é un homomorfismo de grupos. En efecto, se $g, h \in G'$, $i(hg) = (hg)^{-1} = g^{-1}h^{-1} = h^{-1}g^{-1} = i(h)i(g)$, por ser G' abeliano. Así pois, $i \in \mathrm{Aut}_{\mathsf{Grp}}(G')$, pero $i^2 = Id_{G'}$ e $|i| = 2$. Sen embargo, dado que a orde de todo elemento dun grupo divide á orde do grupo, $|i| \Big| |\mathrm{Aut}_{\mathsf{Grp}}(G')|$, ou sexa que $2|p$, pero p era impar por hipótese, logo chegamos a unha contradición.

□

Observación 2.9. Notemos que, esencialmente, o motivo que impide que a categoría $\mathcal{C} = \mathsf{Grp}$ sexa finitamente universal é que hai grupos finitos G, para os que non podemos atopar ningún obxecto $X \in \mathrm{obx}(\mathsf{Grp})$ tal que o grupo dos automorfismos interiores $\mathrm{Inn}(X)$ (como subgrupo de $\mathrm{Aut}_{\mathsf{Grp}}(X)$) se corresponda con algún subgrupo de G. Deste modo non se pode establecer o isomorfismo entre $\mathrm{Aut}_{\mathsf{Grp}}(X)$ e G. En resumo, non todo grupo finito G é realizable como os automorfismos interiores doutro grupo finito H.

2.2. Existencia de categorías finitamente universais: $\mathcal{C} = \mathsf{Graphs}$

A pesar de que na sección anterior comprobamos que non toda categoría é finitamente universal, si existen categorías que cumpren esta propiedade, sendo Frucht quen atopou a primeira, como xa comentamos no parágrafo introdutorio. Nesta sección, desenvolveremos os conceptos necesarios de teoría de grafos para definir a categoría dos grafos simples finitos, $\mathcal{C} = \mathsf{Graphs}$, probaremos o resultado de Frucht e comentaremos o seu interese nas probas de universalidade. Os contenidos das dúas primeiras partes desta sección foron extraídos na súa maioría de [7].

2.2.1. Grafos e a súa categoría

Primeiro comezaremos establecendo as nocións de interese da teoría de grafos que imos empregar nesta sección e definiremos a categoría dos grafos simples finitos.

Definición 2.10. Un *grafo (finito) non dirixido* $\mathcal{G}$ é un par $(V(\mathcal{G}), E(\mathcal{G}))$ formado por dous conxuntos finitos $V(\mathcal{G}) \neq \emptyset$ e $E(\mathcal{G})$, cuxos elementos son da forma

$$\{u, v\} \in E(\mathcal{G}), \quad u, v \in V(\mathcal{G}).$$

Cada elemento de $V(\mathcal{G})$ denomínase *vértice* e cada elemento de $E(\mathcal{G})$ denomínase *arista*. Podemos representar gráficamente un grafo $\mathcal{G}$ debuxando os vértices como puntos e as aristas como liñas que os unen.

Observación 2.11. Se o grafo non dirixido $\mathcal{G}$ do que se está a falar se sobreentende, denotaremos por comodidade $V \equiv V(\mathcal{G})$ e $E \equiv E(\mathcal{G})$. Ademais, cada arista $\{u, v\} \in E$ denotarémola por uv, onde u diremos que é o *comezo* de uv e v o seu *final*.

Definición 2.12. Sexa $\mathcal{G} = (V, E)$ un grafo non dirixido.

(1) Se dous vértices $u, v \in V$ forman unha arista de $\mathcal{G}$, isto é, $uv \in E$, dise que son *adxacentes*.

(2) Unha arista da forma $uu \in E$ denomínase *lazo*.

(3) Dous vértices $u, v \in V$ dise que están *unidos* pola arista $e \in \mathcal{G}$ se o comezo de e é u e o seu final é v.

(4) Dúas aristas dinse *adxacentes* se comparten o comezo de unha e o final da outra, ou sexa, se son da forma $uv, vw \in E$.

(5) O grafo $\mathcal{G}$ dise *simple* se non presenta lazos nin aristas múltiples (ou sexa, dous vértices están unidos, ao sumo, por unha única arista).

(6) O número de elementos de V é a *orde* de G e o de E o *tamaño* de $\mathcal{G}$.

(7) Un *camiño* en $\mathcal{G}$ é unha sucesión $(v_1, \ldots, v_{n+1})$ de vértices e unha sucesión $(e_1, \ldots, e_n)$ de aristas tales que $e_i = v_i v_{i+1}$, para cada $i \in \{1, \ldots, n\}$. Diremos que a *lonxitude* do camiño é n.

Definición 2.13. Sexa $\mathcal{G} = (V, E)$ un grafo. O *grao* de $u \in V$, $d(u)$, é o número de aristas da forma $uv \in E$ tales que $v \in V$. Se o grafo é simple, coincide co número de vértices $v \in V$ tales que uv é unha arista de $\mathcal{G}$.

Definición 2.14. Dicimos que un vértice $u \in V$ dun grafo simple finito $\mathcal{G} = (V, E)$ é *final* se $d(u) = 1$.

Definición 2.15. Sexan $\mathcal{G}, \mathcal{H}$ dous grafos simples finitos. Un *morfismo de grafos* é unha aplicación $f : V(\mathcal{G}) \to V(\mathcal{H})$ que preserva a adxacencia, isto é, se $uv \in E(\mathcal{G})$, entón $f(u)f(v) \in E(\mathcal{H})$. O morfismo f dise que é un *isomorfismo de grafos* se f é bixectiva e $uv \in E(\mathcal{G})$ se, e só se, $f(u)f(v) \in E(\mathcal{H})$. Se ademais $\mathcal{H} = \mathcal{G}$, f dise que é un *automorfismo de grafos*.

Lema 2.16. *Sexa $\mathcal{G} = (V, E)$ un grafo simple finito, e $f : V(\mathcal{G}) \to V(\mathcal{G})$ un automorfismo de grafos. Entón $d(u) = d(f(u))$ para todo $u \in V$.*

Demostración. Por ser f un automorfismo de grafos non dirixidos, $uv \in E$ se, e só se, $f(u)f(v) \in E$, de forma que para cada $v' \in V$, $uv' \in E$ se, e só se $f(u)f(v') \in E$, co que o número de elementos

$v' \in V$ tales que $uv' \in E$ coincide co de $f(v') \in V$ (todos distintos por ser f inxectiva) tales que $f(u)f(v') \in E$. □

Proposición 2.17. *A composición de morfismos de grafos é un morfismo de grafos.*

Demostración. Tomemos $\mathcal{G}, \mathcal{H}, \mathcal{K}$ grafos simples finitos e $f : V(\mathcal{G}) \to V(\mathcal{H})$, $g : V(\mathcal{H}) \to V(\mathcal{K})$ morfismos de grafos. Vexamos que a composición preserva a adxacencia: se $uv \in E(\mathcal{G})$, entón $f(u)f(v) \in E(\mathcal{H})$, co que $g(f(u))g(f(v)) \in E(\mathcal{K})$. □

Definición 2.18. Coa proposición anterior e tendo en conta que a identidade é trivialmente un morfismo de grafos, definimos a categoría dos grafos simples finitos $\mathcal{C} = \mathsf{Graphs}$, onde os obxectos son os grafos simples finitos e, para cada $\mathcal{G}, \mathcal{H} \in \mathrm{Obx}(\mathsf{Graphs})$, $\mathrm{Hom}_{\mathsf{Graphs}}(\mathcal{G}, \mathcal{H})$ é o conxunto de morfismos de grafos de $\mathcal{G}$ en $\mathcal{H}$, coa composición de aplicacións.

Por último, podemos caracterizar os automorfismos $f \in \mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G})$ como os morfismos dun grafo en si mesmo que teñen inversa respecto á composición f^{-1}. En efecto, tendo en conta a Definición 1.5 e a Definición 1.7, basta ver que f^{-1} é un automorfismo de grafos: $uv \in E(\mathcal{G})$ se, e só se

$$uv = f(f^{-1}(u))f(f^{-1}(v)) \in E(\mathcal{G}),$$

se e só se, por ser f un automorfismo de grafos,

$$f^{-1}(u)f^{-1}(v) \in E(\mathcal{G}).$$

Dende aquí é evidente que a definición categórica de automorfismo en $\mathcal{C} = \mathsf{Graphs}$ é equivalente á dada na Definición 2.15.

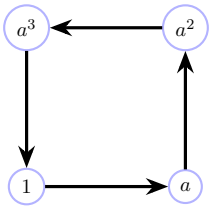
2.2.2. O grafo de Cayley

Arthur Cayley introduciu, en 1878, un tipo especial de grafos que permiten representar os grupos finitos e que serán de utilidade á hora de probar que a categoría $\mathcal{C}$=Graphs é finitamente universal.

Definición 2.19. Sexa G un grupo finito que admite a presentación libre $G = \langle H \mid R \rangle$, con xeradores $H = \{h_1, \ldots, h_n\}$. Chamamos *grafo de Cayley de G asociado a H*, $\mathrm{Cay}(G, H)$, ao grafo $(V, \overrightarrow{H})$, con $V = G$ e $\overrightarrow{H}$ o conxunto de aristas *coloreadas* polos elementos de H. Isto último significa que os elementos de $\overrightarrow{H}$ son os pares ordenados (g, gh_i) para cada $g \in G$ e $h_i \in H$, $i = 1, \ldots, n$. Neste senso, diremos que a arista (g, gh_i) está *coloreada* por h_i ou que ten *cor* i. Podemos denotar a arista (g, gh_i) por $g \to gh_i$.

A definición anterior permite representar calquera grupo finito coñecendo un conxunto de xeradores e engadindo unha etiqueta a cada arista segundo a cor que teña asociada:

Exemplo 2.20. Lembremos que o grupo multiplicativo $G = \mathbb{Z}/p\mathbb{Z},\ p > 2$, admite a presentación libre $\mathbb{Z}/p\mathbb{Z} = \langle a \mid a^p = 1\rangle$. Por exemplo, se $p = 4$, $\mathrm{Cay}(G, \{a\})$ ten vértices $V = G = \{1, a, a^2, a^3\}$ e aristas coloreadas $\overrightarrow{\{a\}} = \{(1, 1 \cdot a), (a, a \cdot a), (a^2, a^2 \cdot a), (a^3, a^3 \cdot a)\}$. Neste caso só temos unha cor (con etiqueta a, pois o único xerador é a) co que se pode representar G como:



Na Figura 2.1 pódese observar a representación do grafo de Cayley asociado ao grupo $\mathbb{Z}/2\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z}$ (grupo de Klein) dado por $\langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle$ e, na Figura 2.2, a representación do grupo simétrico S_3 cos xeradores:

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

de forma que $\tau^2 = Id_{S_3}$ e $\sigma^3 = Id_{S_3}$.

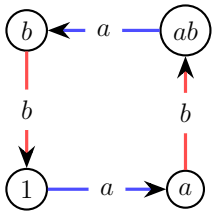


Figura 2.1: Grafo de Cayley do grupo de Klein

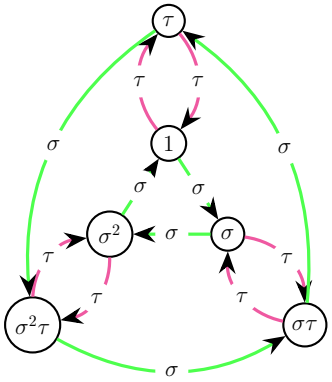


Figura 2.2: Grafo de Cayley de S_3.

Definición 2.21. Sexa un grupo finito $G = \langle H \mid R\rangle$, con $H = \{h_1, \ldots, h_n\}$. Un *automorfismo de grafos de Cayley* é unha permutación θ do conxunto de vértices G tal que, para cada $i \in \{1, \ldots, n\}$, se $k_1, k_2 \in G$ e $h_i \in H$, entón $k_1 h_i = k_2$ se, e só se, $\theta(k_1)h_i = \theta(k_2)$. Isto é, o seguinte diagrama conmuta, para todo $k \in G$ e para todo $h_i \in H$:

$$\begin{array}{ccc} k & \xmapsto{h_i} & kh_i \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ \theta(k) & \xmapsto{h_i} & \theta(k)h_i \end{array}$$

Observación 2.22. Pódese comprobar de forma sinxela que o conxunto de automorfismos de grafos de Cayley dun grupo finito G é, en efecto, un grupo coa composición de aplicacións. Denotarémolo por $\mathrm{Aut}(\mathrm{Cay}(G,H))$.

Teorema 2.23. *Sexa $G = \langle H \mid R\rangle$ un grupo finito con $H = \{h_1, \ldots, h_n\}$ un conxunto de xeradores. Entón* $\mathrm{Aut}(\mathrm{Cay}(G,H)) \cong G$.

Demostración. Dado $k \in G$, a aplicación $\varphi_k : \mathrm{Cay}(G,H) \to \mathrm{Cay}(G,H)$ dada por $\varphi_k(g) = kg$ é un automorfismo de grafos de Cayley. En efecto, fixemos $h_i \in H$ e tomemos $(g, gh_i) \in \overrightarrow{H}$. Entón,

$$\varphi_k(gh_i) = k(gh_i) = (kg)h_i = \varphi_k(g)h_i.$$

Agora, vexamos que a aplicación

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(\mathrm{Cay}(G,H)) \\ h &\longmapsto \phi(h) = \varphi_h, \end{aligned}$$

é un isomorfismo de grupos. Imos por partes:

- *É un homomorfismo.* Consideremos $h, g \in G$ e outro $k \in G$. Tense que

$$\begin{aligned} \phi(hg)(k) = \varphi_{hg}(k) = hgk = \varphi_h(gk) = \varphi_h(\varphi_g(k)) \\ = \varphi_h(\phi(g)(k)) = \phi(h)(\phi(g)(k)) = (\phi(h) \circ \phi(g))(k). \end{aligned}$$

- *Inxectividade.* Dados $h, g \in G$, temos $\phi(h) = \phi(g)$ se, e só se, $\varphi_h = \varphi_g$. Sexa agora $a \in G$, $\varphi_h(a) = \varphi_g(a)$, co que $ha = ga$, así que $h = g$.

- *Sobrexectividade.* Sexa $\theta \in \mathrm{Aut}(\mathrm{Cay}(G,H))$. Temos que atopar $h \in G$ tal que $\varphi_h = \theta$. Imos comprobar que $h = \theta(1)$. En efecto, como $G = \langle H \mid R\rangle$, entón cada $k \in G$ pódese escribir como:

$$k = h_{k_1}^{a_1} \cdots h_{k_n}^{a_n}, \text{ con } a_i \in \mathbb{Z}.$$

  Notemos que para cada h_i^a, con $a \in \mathbb{Z}$, tense que

$$\theta(kh_i^a) = \theta(kh_i^{a-1})h_i = \theta(kh_i^{a-2})h_i^2 = \cdots = \theta(k)h_i^a, \quad \text{para cada} \quad k \in G. \tag{2.1}$$

  co cal,

$$\theta(k) = \theta(1k) = \theta(1h_{k_1}^{a_1} \cdots h_{k_n}^{a_n}) \underset{(2.1)}{=} \cdots = \theta(1)h_{k_1}^{a_1} \cdots h_{k_n}^{a_n} = \theta(1)k = hk,$$

  e finalmente $\theta(k) = \varphi_h(k)$.

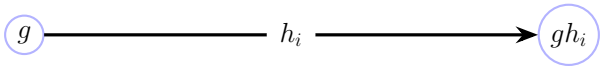
□

2.2.3. O Teorema de Frucht

En 1939, Robert Frucht probou, manipulando adecuadamente os grafos de Cayley, que todo grupo finito é isomorfo ao grupo de automorfismos dalgún grafo $\mathcal{G} \in \mathrm{Obx}(\mathsf{Graphs})$. No que segue, demostraremos este resultado baseándonos no proceso de substitución de frechas levado a cabo por Frucht en [12].

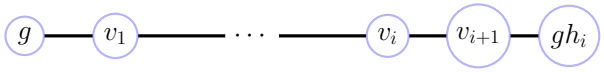
Substitución de frechas

Dado un grupo finito $G = \langle H \mid R \rangle$, con xeradores $H = \{h_1, \ldots, h_n\}$, podemos transformar o seu grafo de Cayley $\mathrm{Cay}(G, H)$ nun grafo simple mediante un proceso denominado *substitución de frechas*. Comeza do seguinte modo: por separado, centrémonos en cada arista (g, gh_i) (con etiqueta fixa $i \in \{1, \ldots, n\}$).

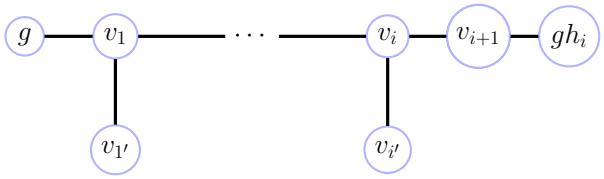


O proceso consiste en engadir un camiño de lonxitude $i+2$ para codificar o sentido e a etiqueta (cor) da arista:

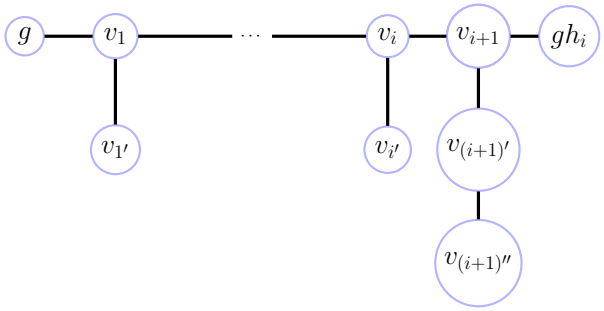
(1) Introducimos $v_1, \ldots, v_{i+1}$ vértices na arista (quitando a frecha que marca o sentido e a etiqueta).



(2) En $v_1, \ldots, v_i$ engadimos un camiño de lonxitude 1 que chegan a novos vértices $v_{1'}, \ldots, v_{i'}$.



(3) En v_{i+1} engadimos un camiño de lonxitude 2, con dous novos vértices $v_{(i+1)'}$ e $v_{(i+1)''}$.



Desta forma, as aristas $v_1v_1', \ldots, v_iv_i'$ codifican a cor i e as outras dúas o sentido, xa que queren dicir que a dirección orixinal era do vértice que conecta con v_i ao vértice que conecta con v_{i+1}. Este novo grafo denotarase por $\mathcal{G}_{SF}(G,H) = (V,E)$ e é un grafo simple finito, logo $\mathcal{G}_{SF}(G,H) \in \text{obx}(\mathsf{Graphs})$.

Exemplo 2.24. O grafo de Cayley do grupo de Klein (do Exemplo 2.20, véxase a Figura 2.1) tras realizar o proceso de substitución de frechas descrito anteriormente, daría lugar ao grafo simple da Figura 2.3.

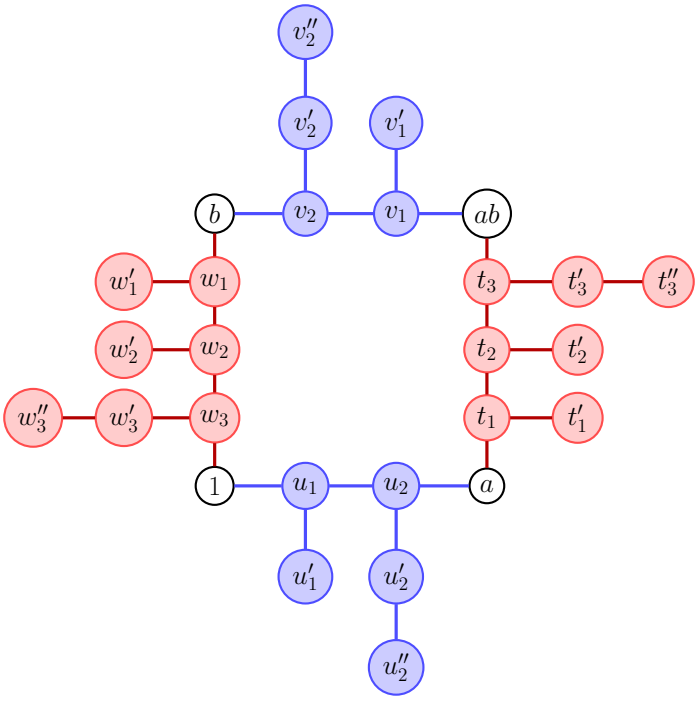


Figura 2.3: Grafo de Cayley asociado ao grupo de Klein tras a substitución de frechas.

Observación 2.25. Dado un grafo de Cayley, $\text{Cay}(G,H)$, asociado a un grupo finito $G = \langle H \mid R \rangle$, con $H = \{h_1, \ldots, h_n\}$, denotaremos cada vértice $v \in \mathcal{G}_{SF}(G,H) \setminus G$ como segue: para un $i \in \{1, \ldots, n\}$ fixado, $v = v_j^{gi}$ é o $j-$ésimo vértice engadido na arista que unía, no grafo $\text{Cay}(G,H)$, os vértices $g \to gh_i$, onde $j \in \{1, \ldots, i, 1' \ldots, i', i{+}1, (i{+}1)', (i{+}1)''\}$. Os novos vértices engadidos cumpren que o seu grao, por construción, é

$$d(v_j^{gi}) = \begin{cases} 3 & \text{se } j \in \{1, \ldots, i+1\}, \\ 1 & \text{se } j \in \{1', \ldots, i', (i+1)''\}, \\ 2 & \text{se } j = (i+1)'. \end{cases}$$

Teorema 2.26. (Teorema de Frucht). *A categoría $\mathcal{C} =$ Graphs é finitamente universal.*

Demostración. Sexa $G = \langle H \mid R\rangle$ un grupo finito onde $H = \{h_1, \ldots, h_n\}$ é o conxunto de xeradores. Consideremos o grafo de Cayley asociado $\mathrm{Cay}(G, H)$. Polo Teorema 2.23, terase que

$$\mathrm{Aut}(\mathrm{Cay}(G, H)) \cong G.$$

Por substitución de frechas, obtemos o grafo simple $\mathcal{G}_{SF}(G, H)$ que denotamos $\mathcal{G}_{SF}$ para simplificar a notación. Dado que G se realiza a través de $\mathrm{Cay}(G, H)$, basta probar que $\mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}_{SF}) \cong \mathrm{Aut}(\mathrm{Cay}(G, H))$ e entón xa estará. Con este propósito, definamos a aplicación

$$\begin{aligned} \mathrm{Aut}(\mathrm{Cay}(G, H)) &\xrightarrow{\ \phi\ } \mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}_{SF}) \\ \theta &\longmapsto \phi(\theta) : \mathcal{G}_{SF} \longrightarrow \mathcal{G}_{SF} \\ & \qquad v \longmapsto \phi(\theta)(v), \end{aligned}$$

dada do seguinte modo: se $v \in G$, $\phi(\theta)(v) = \theta(v)$ e se $v = v_j^{gi} \in \mathcal{G}_{SF} \setminus G$ (véxase a Observación 2.25), definimos $\phi(\theta)(v_j^{gi}) = v_j^{\theta(g)i}$.

Vexamos que ϕ está ben definida e que é un automorfismo de grupos:

(1) *Está ben definida.* Hai que ver que $\phi(\theta)$ preserva a adxacencia: se $uv \in E(\mathcal{G}_{SF})$ é unha arista, entón, se u e v non pertencen ao grafo orixinal, uv é da forma $v_j^{gi}v_k^{gi}$ e a arista de chegada é $v_j^{\theta(g)i}v_k^{\theta(g)i}$, co que se preserva a adxacencia. No caso en que algún nodo pertenza ao grafo orixinal, poñamos primeiro $u = g \in G$, uv debe ser da forma gv_1^{gi}, logo a arista de chegada é $\theta(g)v_1^{\theta(g)i}$, preservando tamén a adxacencia. E por último, se uv é da forma $v_{i+1}^{gi}gh_i$, entón a imaxe por $\phi(\theta)$ é, por ser θ un automorfismo de grafos de Cayley, $v_{i+1}^{\theta(g)i}\theta(g)h_i$, conservando a adxacencia. Así, $\phi(\theta)$ é un automorfismo de grafos.

(2) *É un homomorfismo de grupos.* Sexan $\theta_1, \theta_2 \in \mathrm{Aut}(\mathrm{Cay}(G, H))$ e un vértice arbitrario $v \in \mathcal{G}_{SF}$. Se $v \in G$,

$$\phi(\theta_1\theta_2)(v) = \theta_1(\theta_2(v)) = \phi(\theta_1)(\phi(\theta_2)(v)) = (\phi(\theta_1)\phi(\theta_2))(v).$$

E se $v_j^{gi} \in \mathcal{G}_{SF} \setminus G$,

$$\phi(\theta_1\theta_2)(v_j^{gi}) = \theta_1(v_j^{\theta_2(g)i}) = v_j^{(\theta_1(\theta_2(g)))i} = \phi(\theta_1)(v_j^{\theta_2(g)i}) = (\phi(\theta_1)\phi(\theta_2))(v_j^{gi}).$$

(3) *Inxectividade.* Calulemos o núcleo de ϕ:

$$\mathrm{Ker}(\phi) = \{\theta \in \mathrm{Aut}(\mathrm{Cay}(G, H)) : \phi(\theta)(v) = v, \text{ para todo } \ v \in \mathcal{G}_{SF}\}.$$

Como necesariamente debe ocurrir, para que $\theta \in \mathrm{Ker}(\phi)$, que cada $v \in G$ cumpra $\phi(\theta(v)) = \theta(v) = v$; entón $\theta = Id_{\mathrm{Cay}(G,H)}$ e polo tanto o núcleo é trivial, co que ϕ é inxectiva.

(4) *Sobrexectividade.* Sexa $\varphi \in \mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}_{SF})$. Estudemos como se comporta en cada arista. Para isto, teñamos en conta as seguintes propiedades:

(CI) φ é un automorfismo de grafos non dirixidos, logo polo Lema 2.16 presérvase o grao de cada vértice.

(CII) Por preservación da adxacencia, a imaxe por φ dunha sucesión de vértices distintos que formen un camiño de lonxitude arbitraria n en $\mathcal{G}_{SF}$ debe ser outra sucesión de vértices que formen un camiño de lonxitude n en $\mathcal{G}_{SF}$.

Por (CII), a imaxe por φ do camiño de lonxitude $i+2$ engadido na arista (g, gh_i), debe ser outro camiño de lonxitude $i+2$. Ademais, non pode ser un camiño dentro do grafo de Cayley orixinal porque este non ten vértices finais (e o grao debe preservarse), co que se debe corresponder con outro camiño de lonxitude $i+2$ engadido noutra arista da forma (k, kh_i), con $k \in G$. Así, φ leva aristas de cor i en aristas de cor i.
Agora, por (CI), os graos deben preservarse, de forma que, pola Observación 2.25, como $v^{gi}_{(i+1)'}$ é o único vértice con grao 2 dentro do camiño de lonxitude $i+2$, $\varphi(v^{gi}_{(i+1)'}) = v^{ki}_{(i+1)'}$. Agora ben, por preservación da adxacencia, como $v^{gi}_{(i+1)'}$ e $v^{gi}_{(i+1)''}$ son adxacentes, logo $\varphi(v^{gi}_{(i+1)'})$ e $\varphi(v^{gi}_{(i+1)''})$ tamén o son. Notemos que $\varphi(v^{gi}_{(i+1)'}) = v^{ki}_{(i+1)'}$ e os únicos vértices adxacentes con $v^{ki}_{(i+1)'}$ son $v^{ki}_{(i+1)''}$ e $v^{ki}_{(i+1)}$, pero $d(v^{ki}_{(i+1)}) = 3$ e $d(v^{ki}_{(i+1)''}) = 1$. Como $v^{gi}_{(i+1)''}$ ten grao 1, debe ser $\varphi(v^{gi}_{(i+1)''}) = v^{ki}_{(i+1)''}$. Análogamente, $\varphi(v^{gi}_{(i+1)}) = v^{ki}_{(i+1)}$. Así, probamos que os vértices que codifican a dirección seguen codificando dirección.
Notemos agora que $\varphi(gh_i)$ e $v^{ki}_{(i+1)}$ deben ser adxacentes pola adxacencia de gh_i e $v^{gi}_{(i+1)}$. Como os únicos vértices adxacentes con $v^{ki}_{(i+1)}$ son v^{ki}_i e kh_i, pero $d(v^{ki}_i) = 3$ e $d(kh_i) = d(gh_i)$ (que deben ter o mesmo grao par, pois no grafo de Cayley hai unha frecha que entra no vértice e outra que sae por cada xerador), entón

$$\varphi(gh_i) = kh_i. \tag{2.2}$$

O seguinte paso é notar que $v^{ki}_{(i+1)}$ e $\varphi(v^{gi}_i)$ deben ser adxacentes, co que un razoamento análogo ao dos pasos previos leva a que $\varphi(v^{gi}_i) = v^{ki}_i$. Deste xeito, realizando o proceso consecutivamente, por preservación do grao, debe ocurrir que $\varphi(v^{gi}_j) = v^{ki}_j$, para todo $j \in \{1, \dots, i-1\}$. Análogamente, $\varphi(v^{gi}_j) = v^{ki}_j$, para todo $j \in \{1', \dots, i'\}$. O que acabamos de probar é que

$$\varphi(v^{gi}_j) = v^{\varphi(g)i}_j, \text{ para todo } j \in \{1, \dots, i+1, 1', \dots, (i+1)', (i+1)''\}. \tag{2.3}$$

Razoando da mesma maneira que en tódolos casos anteriores,

$$\varphi(g) = k. \tag{2.4}$$

Sexa entón a aplicación

$$\begin{aligned} \mathrm{Cay}(G,H) &\longrightarrow \mathrm{Cay}(G,H) \\ g &\longmapsto \theta(g) = \varphi(g). \end{aligned}$$

Polas Ecuacións (2.2) e (2.4), está ben definida e é un automorfismo de grafos de Cayley. Ademais, se $v_j^{gi} \in \mathcal{G}_{SF} \setminus G$, terase que

$$\phi(\theta)(v_j^{gi}) = v_j^{\theta(g)i} = v_j^{\varphi(g)i} \underset{(2.3)}{=} \varphi(v_j^{gi}),$$

co que θ é o antecedente por ϕ do automorfismo de grafos non dirixidos φ.

□

Do Teorema de Frucht extráese directamente o seguinte Corolario, co que facemos notar a súa importancia nas demostracións de universalidade, xa comentada ao comezo do capítulo:

Corolario 2.27. *Sexa $\mathcal{C}$ unha categoría arbitraria. Entón, se existe un funtor F : $\mathsf{Graphs} \to \mathcal{C}$ fiel e pleno, $\mathcal{C}$ é finitamente universal.*

Demostración. Polo Teorema 2.26, Graphs é finitamente universal co que o Teorema 2.5 garante, por existir o funtor do enunciado, que $\mathcal{C}$ é finitamente universal. □

Capítulo 3

Introdución aos aneis de fusión

Os aneis de fusión son estruturas alxébricas que xorden de maneira natural en diversos contextos da álxebra moderna, entre os cales destaca a teoría de representacións de grupos finitos. En particular, o anel de Grothendieck da categoría das representacións de dimensión finita dun grupo finito G sobre $\mathbb{C}$ constitúe un exemplo canónico deste tipo de estrutura. Neste capítulo, familiarizaremos ao lector co concepto de *anel de fusión* e desenvolveremos brevemente o exemplo anterior a modo de motivación.

3.1. Definición e propiedades

Esta primeira sección está dedicada a introducir o concepto de *anel de fusión* e estudar as súas propiedades básicas, empregando para iso a referencia [10].
No que segue denotamos $\mathbb{Z}_+ = \{m \in \mathbb{Z} : m \geq 0\}$, o conxunto dos enteiros non negativos. Ademais, δ_{ij} (ou $\delta_{i,j}$) denotará a delta de Kronecker nos índices i e j.

Definición 3.1. Sexa $(A, +, \cdot)$ un anel asociativo e unitario tal que o grupo abeliano $(A, +)$ é libre como $\mathbb{Z}$-módulo. Chámase $\mathbb{Z}_+-$*base* de A a unha base $B_+ = \{b_i\}_{i \in I}$ que cumpre:

$$b_i b_j = \sum_{k \in I} c_{ij}^k b_k, \text{ con } c_{ij}^k \in \mathbb{Z}_+, \text{ para todos } i, j \in I.$$

Observación 3.2. Dado que a multiplicación debe estar ben definida dentro do anel, dedúcese que, para cada $i, j \in I$, o conxunto $\{k \in I : c_{ij}^k \neq 0\}$ debe ser finito.

Definición 3.3. Un $\mathbb{Z}_+-$*anel* é un anel cunha $\mathbb{Z}_+-$*base* fixada (A, B_+), no que o neutro para o produto 1 é unha combinación lineal non negativa dos elementos da base. Se ademais $1 \in B_+$ dise que (A, B_+) é *unital*.

Definición 3.4. Sexa (A, B_+) un $\mathbb{Z}_+-$anel, con $B_+ = \{b_i\}_{i\in I}$, e sexa

$$I_0 = \{i \in I : b_i \text{ aparece na expresión de 1 na base } B_+\}.$$

Definimos o morfismo de grupos $\tau : (A, +) \to (\mathbb{Z}, +)$ dado polos elementos da base:

$$\tau(b_i) = \begin{cases} 1, \text{ se } i \in I_0, \\ 0, \text{ se } i \notin I_0. \end{cases}$$

Proposición 3.5. *Sexa (A, B_+) un $\mathbb{Z}_+-$anel. Entón, para cada $i, j \in I_0$ (introducido na Definición 3.4), con $i \neq j$, cúmprese que $b_i^2 = b_i$ e $b_i b_j = 0$.*

Demostración. Sexa $I_0 = \{b_{i_1}, \ldots, b_{i_r}\}$. Podemos escribir $1 \in A$ como

$$1 = \alpha_{i_1} b_{i_1} + \cdots + \alpha_{i_r} b_{i_r}, \quad \alpha_{i_j} > 0 \text{ para todo } j \in \{1, \ldots, r\}. \tag{3.1}$$

Fixemos agora $b_{i_s} \in I_0$, con $s \in \{1, \ldots, r\}$, e multipliquemos pola dereita a expresión anterior por b_{i_s}. Obtemos:

$$b_{i_s} = \sum_{j=1}^{r} \alpha_{i_j} b_{i_j} b_{i_s} = \sum_{j=1}^{r} \alpha_{i_j} \left(\sum_{k=1}^{n} c_{i_j i_s}^k \right) b_k$$

$$= \sum_{j=1}^{r} \sum_{k=1}^{n} \alpha_{i_j} c_{i_j i_s}^k b_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{r} \alpha_{i_j} c_{i_j i_s}^k \right) b_k.$$

Como $\{b_i\}_{i\in I}$ é unha base, a expresión de b_{i_s} é única. Así, para cada $k \neq i_s$ tense

$$\sum_{j=1}^{r} \alpha_{i_j} c_{i_j i_s}^k = 0, \quad \text{e} \quad \sum_{j=1}^{r} \alpha_{i_j} c_{i_j i_s}^{i_s} = 1.$$

Agora, como estamos nun $\mathbb{Z}_+$-anel, tódolos coeficientes $c_{ij}^k \geq 0$, e como $\alpha_{i_j} > 0$ para todo j, dedúcese que

$$c_{i_t i_s}^k = 0, \quad \text{para todo } t \in \{1, \ldots, r\}, \text{ e todo } k \neq i_s. \tag{3.2}$$

De forma análoga, multiplicando pola esquerda por b_{i_s} na ecuación (3.1):

$$b_{i_s} = \sum_{j=1}^{r} \alpha_{i_j} b_{i_s} b_{i_j} = \sum_{j=1}^{r} \alpha_{i_j} \left(\sum_{k=1}^{n} c_{i_s i_j}^k \right) b_k$$

$$= \sum_{j=1}^{r} \sum_{k=1}^{n} \alpha_{i_j} c_{i_s i_j}^k b_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{r} \alpha_{i_j} c_{i_s i_j}^k \right) b_k.$$

Pola unicidade da expresión, temos de novo:

$$\sum_{j=1}^{r} \alpha_{i_j} c^{k}_{i_s i_j} = 0 \text{ para todo } k \neq i_s, \quad \text{e} \quad \sum_{j=1}^{r} \alpha_{i_j} c^{i_s}_{i_s i_j} = 1.$$

E, como antes,

$$c^{k}_{i_s i_t} = 0, \quad \text{para todo } t \in \{1, \ldots, r\}, \text{ e todo } k \neq i_s. \tag{3.3}$$

Combinando as ecuacións (3.2) e (3.3), dedúcese que os únicos coeficientes non nulos dos produtos $b_{i_j} b_{i_s}$ (con $j \in \{1, \ldots, r\}$) son os $c^{i_s}_{i_s i_s}$. Ademais, como

$$1 = \sum_{j=1}^{r} \alpha_{i_j} c^{i_s}_{i_s i_j} = \alpha_{i_s} c^{i_s}_{i_s i_s},$$

obtense $c^{i_s}_{i_s i_s} = 1$, e en consecuencia:

$$b_{i_j} b_{i_s} = 0 \text{ para } j \neq s, \quad \text{e} \quad b^2_{i_s} = b_{i_s}.$$

□

Definición 3.6. Sexa A un conxunto. Unha aplicación bixectiva $f : A \to A$ dise unha *involución* se $f^2 = Id_A$.

Definición 3.7. Un *anel base* é unha terna $(A, B_+, *)$ onde (A, B_+) é un $\mathbb{Z}_+-$anel equipado cunha involución $* : I \to I$ tal que os elementos da base B_+ cumpren:

$$\tau(b_i b_j) = \begin{cases} 1, \text{ si } j = i^* \\ 0, \text{ si } j \neq i^* \end{cases}.$$

E ademais tal que a extensión natural de $*$ no anel A dada por

$$a = \sum_{i \in I} \alpha_i b_i \longmapsto a^* = \sum_{i \in I} \alpha_i b_{i^*}, \ \alpha_i \in \mathbb{Z},$$

sexa un anti-isomorfismo involutivo (véxase a Definición 1.39) no anel A. Notemos que $b_{i^*} = b^*_i$, co que se empregarán ambas notacións indistintamente.

Proposición 3.8. (Propiedades dos aneis base). *Sexa $(A, B_+, *)$ un anel base, entón*

(AB1) $1 = \sum_{i \in I_0} b_i$.

(AB2) $i^* = i$ *para todo* $i \in I_0$.

(AB3) $\tau(x) = \tau(x^*)$ *para todo* $x \in A$.

(AB4) (Reciprocidade de Frobenius). *Os coeficientes $c^{k^*}_{ij}$ son invariantes por permutacións cíclicas de $i, j, k \in I$.*

Demostración. Comecemos probando (AB1). Se $1 \in A$ descompón no anel como

$$1 = \sum_{i \in I_0} \alpha_i b_i, \ \alpha_i > 0,$$

entón, para cada $j \in I_0$, tense que

$$\alpha_j = \sum_{i \in I_0} \alpha_i \delta_{ji} = \sum_{i \in I_0} \alpha_i \tau(b_j b_i^*) = \tau\left(\sum_{i \in I_0} \alpha_i b_j b_i^*\right) = \tau\left(b_j \left(\sum_{i \in I_0} \alpha_i b_i^*\right)\right) = \tau\left(b_j \cdot 1\right) = \tau(b_j) = 1.$$

A propiedade (AB2) dedúcese da Proposición 3.5, pois $b_i^2 = b_i$ e desta maneira,

$$\tau(b_i^2) = \tau(b_i b_i) = \tau(b_i) = 1,$$

de forma que, por unicidade, $i = i^*$, para todo $i \in I_0$.

Imos agora con (AB3). Temos que, para un $x \in A$ fixo,

$$x^* = \sum_{i \in I} \alpha_i b_i^*, \quad \alpha_i \in \mathbb{Z},$$

logo podemos expresar

$$\tau(x^*) = \tau\left(\sum_{i \in I} \alpha_i b_i^*\right) = \sum_{i \in I} \alpha_i \tau(b_i^*) \underset{(\dagger)}{=} \sum_{i \in I} \alpha_i \tau(b_i) = \tau\left(\sum_{i \in I} \alpha_i b_i\right) = \tau(x).$$

onde a igualdade (†) é consecuencia de que $b_i \in I_0$ sé e só se $b_i^* (= b_{i^*}) \in I_0$, o cal dedúcese directamente de (AB2).

Para probar (AB4), comecemos vendo que $c_{ij}^{k^*} = \tau(b_i b_j b_k)$. En efecto, se primeiro descompoñemos

$$b_i b_j = \sum_{k \in I} c_{ij}^k b_k,$$

podemos, fixado $k \in I$, multiplicar por b_k e obter

$$b_i b_j b_k = \sum_{l \in I} c_{ij}^l b_l b_k.$$

Finalmente, aplicando o homomorfismo de grupos τ,

$$\tau(b_i b_j b_k) = \sum_{l \in I} c_{ij}^l \tau(b_l b_k) = \sum_{l \in I} c_{ij}^l \delta_{k^* k} = c_{ij}^{k^*}.$$

Agora, probemos que, para cada $x, y \in A$, tense que $\tau(xy) = \tau(yx)$. Isto é sinxelo utilizando a estrutura de $\mathbb{Z}$-módulo:

$$\tau(xy) = \tau\left(\sum_{i \in I} \alpha_i b_i \cdot \sum_{j \in I} \beta_j b_j\right) = \sum_{i \in I} \sum_{j \in I} \alpha_i \beta_j \tau(b_i b_j)$$

$$= \sum_{i \in I} \sum_{j \in I} \alpha_i \beta_j \tau(b_j b_i) = \tau\left(\left(\sum_{j \in I} \beta_j b_j\right) \cdot \left(\sum_{i \in I} \alpha_i b_i\right)\right) = \tau(yx).$$

Notemos que a igualdade $\tau(b_i b_j) = \tau(b_j b_i)$ séguese trivialmente do feito de que $i \mapsto i^*$ é unha involución. Das dúas propiedades probadas conclúese que $c_{ij}^{k^*}$ é invariante por permutacións cíclicas de $i, j, k \in I$. □

Definición 3.9. (Anel de fusión). Diremos que un anel base $(A, B_+, *)$ é un *anel de multifusión* se ten unha base de rango numerable. Se ademais é unital, *i.e.*, $1 \in B_+$, diremos que é un *anel de fusión.*

Observación 3.10. Un anel de multifusión é de fusión se, e só se o cardinal $|I_0| = 1$. Isto é evidente xa que 1 está en na base considerada se, e só se se cumpre a condición pedida.

3.2. O anel de Grothendieck de $\mathcal{C} = \mathsf{Rep}_{\mathbb{C}}(G)$

Esta sección inclúese co propósito de motivar ao lector, mostrando como os aneis de fusión aparecen de xeito natural en álxebra. Con todo, o estudo detallado da teoría de representacións non forma parte do obxectivo principal deste traballo. Para unha exposición máis ampla sobre o tema, remitimos ao lector interesado ás referencias usadas [10], [23] e [24].

3.2.1. O anel de Grothendieck

Os conceptos necesarios relativos ás categorías foron introducidos na Sección 1.2.

Definición 3.11. Sexa $\mathcal{C}$ unha categoría abeliana e semisimple. O seu *grupo de Grothendieck*, que se denota por $K_0(\mathcal{C})$, defínese como o grupo abeliano libre xerado polo conxunto

$$\{[S_\beta] : S_\beta \in B\},$$

onde B é unha base de obxectos simples de $\mathcal{C}$, e $[S_\beta]$ designa a *clase de isomorfismo* de S_β, isto é, a clase de equivalencia dos obxectos isomorfos a S_β. Ademais, este grupo está dotado da seguinte relación:

$$[X] = [Y] + [Z] \quad \text{sempre que } X \cong Y \oplus Z.$$

Exemplo 3.12. Considérese a categoría $\mathcal{C} = \mathsf{Vect}_{\mathbb{C}}$ (Exemplo 1.3). É abeliana e semisimple, pois todo espazo vectorial sobre $\mathbb{C}$ é isomorfo a $\mathbb{C}^n$. O único obxecto simple (salvo isomorfismos) é $\mathbb{C}$. O grupo de Grothendieck $K_0(\mathsf{Vect}_{\mathbb{C}})$ identifica clases de obxectos coa súa dimensión, mediante o homomorfismo:

$$K_0(\mathsf{Vect}_{\mathbb{C}}) \xrightarrow{\quad\phi\quad} \mathbb{Z}$$

$$[V] \longmapsto \dim_{\mathbb{C}}(V),$$

que é un isomorfismo de grupos. O seu inverso está dado por $n \mapsto n \cdot [\mathbb{C}]$, polo que

$$[V] = [\mathbb{C}^n] = n \cdot [\mathbb{C}].$$

Definición 3.13. Nas condicións da Definición 3.11, se ademais $\mathcal{C}$ é monoidal, o produto entre clases de isomorfismo

$$[X] \cdot [Y] := [X \otimes Y],$$

induce, ao estendelo bilinealmente, un anel conmutativo e unitario, que denominaremos *anel de Grothendieck de* $\mathcal{C}$.

3.2.2. A categoría $\mathcal{C} = \mathsf{Rep}_{\mathbb{C}}(G)$

Fixado G un grupo finito e $\mathbb{C}$ o corpo dos números complexos, defínese a *categoría das representaciones finito-dimensionales de G sobre $\mathbb{C}$*, $\mathcal{C} = \mathsf{Rep}_{\mathbb{C}}(G)$, do seguinte xeito:

- **Obxectos**: pares (V, ρ_V) onde V é un $K-$espazo vectorial de dimensión finita e $\rho_V : G \to \mathrm{GL}(V)$ é un morfismo de grupos, ao que nos referimos como *representación linear de G*.
- **Morfismos**: serán as aplicacións lineais $f : V \to W$ que satisfán

$$f(\rho_V(g)(v)) = \rho_W(g)(f(v)), \quad \text{para todo } g \in G,\ v \in V.$$

Diremos que unha representación ρ_V é *irreducible* se non existe ningún subespazo $W \subsetneq V$ con $W \neq \{0\}$ que sexa $G-$*estable*, isto é, tal que $\rho(g)(W) \subseteq W$ para todo $g \in G$.

A continuación enunciaremos un resultado fundamental. Non incluiremos a demostración completa, mais ofreceremos unha idea do seu argumento co obxectivo de proporcionar ao lector non experto a intuición que facilite a comprensión do teorema.

Teorema 3.14. *A categoría $\mathsf{Rep}_{\mathbb{C}}(G)$ é abeliana, semisimple e monoidal ríxida.*

Idea da demostración. A categoría é abeliana: o obxecto nulo é o espazo vectorial $\{0\}$ dotado da representación trivial. Ademais, todo morfismo é unha aplicación linear compatible coas accións de G, polo que admite núcleo e conúcleo. Tamén, a suma directa de obxectos (V_1, ρ_1) e (V_2, ρ_2) constrúese sobre $V_1 \oplus V_2$, coa representación $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$ definida por

$$(\rho_1 \oplus \rho_2)(g)(v_1, v_2) = (\rho_1(g)v_1,\ \rho_2(g)v_2).$$

A categoría é semisimple segundo o Teorema de Maschke (véxase [23]), que garante que toda representación finitamente xerada de G sobre $\mathbb{C}$ é suma directa de representacións irreducibles. Estas últimas son precisamente os obxectos simples da categoría.

Finalmente, $\mathsf{Rep}_{\mathbb{C}}(G)$ é monoidal ríxida: o obxecto unidade é $(\mathbb{C}, \rho_{\mathrm{triv}})$, onde $\rho_{\mathrm{triv}}(g) = 1$ para todo $g \in G$. O produto tensorial defínese como o produto tensorial de espazos vectoriais xunto co produto tensorial de representacións:

$$\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2), \quad (\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2).$$

O dual dun obxecto (V, ρ_V) é (V^*, ρ_V^*), onde $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ e

$$\rho_V^*(g)(\varphi) := \varphi \circ \rho_V(g^{-1}), \quad \text{para } \varphi \in V^*.$$

Isto define unha acción natural de G sobre o dual, o que completa a estrutura monoidal ríxida. □

Definición 3.15. O anel de Grothendieck de $\mathsf{Rep}_{\mathbb{C}}(G)$, $K_0(\mathsf{Rep}_{\mathbb{C}}(G))$, denominarase *anel de representación complexo de G*.

Imos agora a introducir tódalas ferramentas necesarias para demostrar que $K_0(\mathsf{Rep}_{\mathbb{C}}(G))$ é un anel de fusión.

Proposición 3.16. *Sexa K un corpo e V, W $K-$espazos vectoriais. Entón*

1. $V^{**} \cong V$,
2. $(V \otimes W)^* \cong W^* \otimes V^*$.

Dado $(V, \rho_V) \in \mathrm{Obx}(\mathsf{Rep}_{\mathbb{C}}(G))$, o *subespazo invariante de V* defínese como

$$V^G := \{v \in V : \rho(g)(v) = v, \text{ para todo } \ g \in G\},$$

e a súa dimensión coincide coa cantidade de copias que hai en V da representación trivial.

As seguintes propiedades, cuxas demostracións se poden consultar en [24], serán fundamentais no que segue:

Proposición 3.17. *1.* (Lema de Schur). *Para calquera grupo finito G e calquera par de representacións irreducibles (V, ρ_V) e (W, ρ_W), temos:*

$$\mathrm{Hom}_{\mathsf{Rep}_{\mathbb{C}}(G)}(V, W) = \begin{cases} \mathbb{C}, & \text{se } V \cong W; \\ \{0\}, & \text{se } V \ncong W. \end{cases}$$

2. Dada unha representación (V, ρ_V), o seu dual (V^*, ρ_V^*) é irreducible se, e só se, (V, ρ_V) é irreducible.

Lema 3.18. *Sexa G un grupo finito e $(V, \rho_V), (W, \rho_W) \in \mathrm{Obx}(\mathsf{Rep}_{\mathbb{C}}(G))$. Entón, a representación trivial aparece con multiplicidade 1 en $V \otimes W$ se, e só se $W \cong V^*$.*

Idea da demostración. Imos dar unha idea de como se pode probar só cos resultados vistos ata agora, sen utilizar a denominada *teoría de caracteres* (véxase [23]). Primeiro, é sinxelo comprobar que a representación trivial aparece en $V \otimes W$ se, e só se hai algún vector $G-$invariante en $V \otimes W$ distinto do trivial, ou sexa, $(V \otimes W)^G \neq \{0\}$. Agora, notemos que, pola definición de $\mathrm{Hom}_{\mathsf{Rep}_{\mathbb{C}}(G)}(V, W)$, é isomorfo ao subespazo V^G. Tamén se ten:

$$\mathrm{Hom}_{\mathsf{Rep}_{\mathbb{C}}(G)}(V^*, W) \cong \mathrm{Hom}_{\mathsf{Rep}_{\mathbb{C}}(G)}(\mathbb{C}, V \otimes W) \cong (V \otimes W)^G.$$

Por último, aplicando o Lema de Schur, como (V, ρ_V) e (W, ρ_W) son irreducibles,

$$\dim((V \otimes W)^G) = \begin{cases} 1, & \text{se } W \cong V^*, \\ 0, & \text{noutro caso.} \end{cases}$$

□

Teorema 3.19. *O anel $K_0(\mathsf{Rep}_{\mathbb{C}}(G))$ é, para todo grupo finito G, un anel de fusión.*

Demostración. Denotemos por $\{[V_i] : i \in I = \{1, \ldots, r\}\}$ o conxunto de clases de isomorfismo das representacións irreducibles de G, onde $V_i \equiv (V_i, \rho_{V_i})$. Entón, $K_0(\mathsf{Rep}_{\mathbb{C}}(G))$ é o grupo abeliano libre xerado por esas clases, coa relación:

$$[V] = \sum_{i=1}^{r} m_i [V_i] \quad \text{se} \quad V \cong \bigoplus_{i=1}^{r} V_i^{m_i}.$$

Esta estrutura esténdese naturalmente ao anel de representación complexo de G, dotado do produto:

$$[V_i] \cdot [V_j] := [V_i \otimes V_j] = \sum_{k=1}^{r} c_{ij}^k [V_k],$$

onde os coeficientes $c_{ij}^k \in \mathbb{Z}_{\geq 0}$ son as multiplicidades de V_k en $V_i \otimes V_j$.

Este anel é claramente un $\mathbb{Z}_+-$anel con base $B_+ = \{[V_i] : i \in I\}$, e é unital xa que a unidade do produto tensorial é $(\mathbb{C}, \rho_{\text{triv}})$, que pertence á base.

Para verificar que se trata dun anel de fusión, resta definir unha involución $* : I \to I$ como require a Definición 3.7. Tal involución vén dada, para cada $[V_i] \in B_+$, por:

$$[V_i]^* := [V_i^*],$$

é dicir, pola clase da representación dual $(V_i^*, \rho_{V_i}^*)$.

Supoñamos, sen perda de xeneralidade, que $[V_1] = [\mathbb{C}]$. Entón:

$$\tau([V_i] \cdot [V_j]) = \tau\left(\sum_{k=1}^{r} c_{ij}^k [V_k]\right) = \sum_{k=1}^{r} c_{ij}^k \tau([V_k]) \overset{(\circledcirc)}{=} c_{ij}^1,$$

onde $(\circledcirc)$ é consecuencia de que o anel é unital e $\tau([V_k]) = \delta_{k1}$. Agora ben, c_{ij}^1 é a multiplicidade de $\mathbb{C}$ en $V_i \otimes V_j$ co que, polo Lema 3.18:

$$c_{ij}^1 = \begin{cases} 1 & \text{se } j = i^*, \\ 0 & \text{se } j \neq i^*. \end{cases}$$

Finalmente, grazas á Proposición 3.16, $*$ define un anti-isomorfismo involutivo de aneis, o que conclúe a demostración. □

Capítulo 4

A categoría dos aneis de fusión

Ao longo deste capítulo presentarase unha definición alternativa de *anel de fusión*, partindo do que coñecemos como *regra de fusión*, que resultará máis útil á hora de definir o concepto de *morfismo de fusión* e construír a categoría correspondente. Esta definición de *anel de fusión*, que se basea na presentada en [2], ten un carácter máis combinatorio ca alxébrico e admite aneis non asociativos, aínda que é equivalente, no caso asociativo, á exposta no capítulo anterior. Porén, considerar este novo enfoque facilitaranos notablemente a análise da universalidade finita da categoría dos aneis de fusión.
Na parte final do capítulo, abordaremos o estudo das unidades nos aneis de fusión e, a partir delas, definiremos os seus automorfismos internos, o que nos permitirá realizar unha análise similar á realizada coa categoría dos grupos no Capítulo 2.
Cómpre destacar que a maior parte dos resultados e as definicións incluídos neste capítulo non aparecen explícitamente na literatura, ata onde sabemos, e polo tanto, constitúen unha achega novidosa ao estudo dos aneis de fusión e das súas propiedades.

4.1. Construción alternativa dun anel de fusión

Como comentamos no parágrafo introdutorio, é conveniente, para o noso caso, tomar unha definición alternativa de *anel de fusión*. Presentaremos entón nesta sección un enfoque combinatorio similar ao que aparece en [2] e probaremos que coincide, no caso asociativo, coa definición dada no capítulo anterior. Ilustraremos as definicións e os resultados a través do exemplo do anel grupo sobre $\mathbb{Z}$ (véxase a Definición 1.40).

Definición 4.1. Un *conxunto punteado* é un par $(\mathcal{I}, \mathbf{o})$, onde $\mathcal{I}$ é un conxunto e $\mathbf{o} \in \mathcal{I}$ é un elemento fixado, chamado *elemento distinguido*. Un *morfismo de conxuntos punteados* entre $(\mathcal{I}_1, \mathbf{o}_1)$ e $(\mathcal{I}_2, \mathbf{o}_2)$ é unha aplicación $f\colon \mathcal{I}_1 \to \mathcal{I}_2$ tal que $f(\mathbf{o}_1) = \mathbf{o}_2$.

Definición 4.2. Sexa $(\mathcal{I}, \mathbf{o})$ un conxunto punteado numerable. Unha *regra de fusión asociativa* en $(\mathcal{I}, \mathbf{o})$ é un conxunto de enteiros non negativos

$$N = \{N_{\alpha,\beta}^{\gamma} \in \mathbb{Z}_+ : \alpha, \beta, \gamma \in \mathcal{I}\},$$

cuxos elementos satisfán os seguintes axiomas:

(F1) *Base.* Para cada par de elementos $\alpha, \beta \in \mathcal{I}$, o conxunto $\{\gamma \in \mathcal{I} : N_{\alpha,\beta}^{\gamma} \neq 0\}$ é finito.

(F2) *Asociatividade.* Para todo $\alpha, \beta, \gamma \in \mathcal{I}$, cúmprese que

$$\sum_{\lambda \in \mathcal{I}} N_{\alpha,\beta}^{\lambda} N_{\lambda,\gamma}^{\mu} = \sum_{\lambda \in \mathcal{I}} N_{\beta,\gamma}^{\lambda} N_{\alpha,\lambda}^{\mu} \ ,$$

para todo $\mu \in \mathcal{I}$.

(F3) *Existencia de unidade.* Para todo $\alpha, \beta \in \mathcal{I}$, tense $N_{\alpha,\mathbf{o}}^{\beta} = N_{\mathbf{o},\alpha}^{\beta} = \delta_{\alpha,\beta}$.

(F4) *Dualidade.* Para todo $\alpha \in \mathcal{I}$ existe un único $\alpha^* \in \mathcal{I}$ tal que $N_{\alpha,\beta}^{\mathbf{o}} = N_{\beta,\alpha}^{\mathbf{o}} = \delta_{\alpha^*,\beta}$ para todo $\beta \in \mathcal{I}$.

(F5) *Anti-involución.* Para todo $\alpha, \beta, \gamma \in \mathcal{I}$, $N_{\alpha,\beta}^{\gamma} = N_{\beta^*,\alpha^*}^{\gamma^*}$.

Proposición 4.3. *(Reciprocidade de Frobenius). Sexa N unha regra de fusión asociativa en $(\mathcal{I}, \mathbf{o})$. Entón para todo $\alpha, \beta, \gamma \in \mathcal{I}$, $N_{\alpha,\beta}^{\gamma} = N_{\alpha^*,\gamma}^{\beta} = N_{\gamma,\beta^*}^{\alpha}$.*

Demostración. Notemos primeiro que, polo axioma (F4), $(\alpha^*)^* = \alpha$. Comezaremos probando que $N_{\alpha,\beta}^{\gamma} = N_{\gamma,\beta^*}^{\alpha}$:

$$N_{\alpha,\beta}^{\gamma} = \sum_{\lambda \in \mathcal{I}} N_{\alpha,\beta}^{\lambda} \delta_{\lambda\gamma} \underset{(F4)}{=} \sum_{\lambda \in \mathcal{I}} N_{\alpha,\beta}^{\lambda} N_{\lambda,\gamma^*}^{\mathbf{o}} \underset{(F2)}{=} \sum_{\lambda \in \mathcal{I}} N_{\beta,\gamma^*}^{\lambda} N_{\alpha,\lambda}^{\mathbf{o}}$$

$$\underset{(F4)}{=} \sum_{\lambda \in \mathcal{I}} N_{\beta,\gamma^*}^{\lambda} N_{\lambda,\alpha}^{\mathbf{o}} = \sum_{\lambda \in \mathcal{I}} N_{\beta,\gamma^*}^{\lambda} \delta_{\lambda\alpha^*} = N_{\beta,\gamma^*}^{\alpha^*} \underset{(F5)}{=} N_{\gamma,\beta^*}^{\alpha}.$$

A segunda igualdade é sinxela de comprobar de xeito similar facendo uso do anterior:

$$N_{\alpha^*,\gamma}^{\beta} = \sum_{\lambda \in \mathcal{I}} N_{\alpha^*,\gamma}^{\lambda} \delta_{\lambda\beta^*} \underset{(F4)}{=} \sum_{\lambda \in \mathcal{I}} N_{\alpha^*,\gamma}^{\lambda} N_{\lambda,\beta^*}^{\mathbf{o}} \underset{(F2)}{=} \sum_{\lambda \in \mathcal{I}} N_{\gamma,\beta^*}^{\lambda} N_{\alpha^*,\lambda}^{\mathbf{o}}$$

$$\underset{(F4)}{=} \sum_{\lambda \in \mathcal{I}} N_{\gamma,\beta^*}^{\lambda} N_{\lambda,\alpha^*}^{\mathbf{o}} = \sum_{\lambda \in \mathcal{I}} N_{\gamma,\beta^*}^{\lambda} \delta_{\lambda\alpha} = N_{\gamma,\beta^*}^{\alpha} = N_{\beta,\gamma}^{\alpha}.$$

□

Observación 4.4. Supoñamos que se cumpren os axiomas da Definición 4.2 salvo (F2). Entón non necesariamente se ten a reciprocidade de Frobenius. En efecto, sexa o conxunto punteado

$(\{0,1,2\},0)$ e o conxunto de enteiros non negativos indexados en $\alpha,\beta,\gamma \in \{0,1,2\}$ como segue:

$$\begin{aligned}
&N_{0,\alpha}^{\beta} = N_{\alpha,0}^{\beta} = \delta_{\alpha\beta},\\
&N_{1,2}^{0} = N_{2,1}^{0} = 1,\\
&N_{1,2}^{1} = N_{1,2}^{2} = 2,\ N_{1,1}^{2} = N_{2,2}^{1} = 1,\\
&N_{2,1}^{1} = N_{2,1}^{2} = 1,\ N_{1,1}^{1} = N_{2,2}^{2} = 1.
\end{aligned}$$

Por construción, tense os axiomas (F1),(F3),(F4) e (F5). Agora ben, se $\alpha = 1, \beta = 2, \gamma = 1$ e $\mu = 2$,

$$N_{1,2}^{0}N_{0,1}^{2} + N_{1,2}^{1}N_{1,1}^{2} + N_{1,2}^{2}N_{2,1}^{2} = 1\cdot 0 + 2\cdot 1 + 2\cdot 1 = 4,$$

mentres que

$$N_{2,1}^{0}N_{1,0}^{2} + N_{2,1}^{1}N_{1,1}^{2} + N_{2,1}^{2}N_{1,2}^{2} = 1\cdot 0 + 1\cdot 1 + 1\cdot 2 = 3,$$

e por tanto non se cumpre o axioma (F2). É sinxelo ver entón que non se cumpre a reciprocidade de Frobenius tendo en conta que $1^* = 2$ e $2^* = 1$. Por exemplo, se $\alpha = 1$, $\beta = 2$ e $\gamma = 1$:

$$N_{1,2}^{1} = 2 \neq 1 = N_{1,1}^{1} = N_{1,2^*}^{1}.$$

Definición 4.5. Sexa $(\mathcal{I},\mathbf{o})$ un conxunto punteado numerable. Unha *regra de fusión non asociativa en* $(\mathcal{I},\mathbf{o})$ é un conxunto de enteiros non negativos N que cumpren tódolos axiomas da Definición 4.2 salvo (F2). Engádese neste caso como axioma:

(F6) *Reciprocidade de Frobenius.* Para todo $\alpha,\beta,\gamma \in \mathcal{I}$, $N_{\alpha,\beta}^{\gamma} = N_{\alpha^*,\gamma}^{\beta} = N_{\gamma,\beta^*}^{\alpha}$.

Definición 4.6. (Anel asociado a unha regra de fusión). Sexa $(\mathcal{I},\mathbf{o})$ un conxunto punteado numerable, e $N = \{N_{\alpha,\beta}^{\gamma} \in \mathbb{Z}_+ : \alpha,\beta,\gamma \in \mathcal{I}\}$ unha regra de fusión (asociativa ou non asociativa) sobre $(\mathcal{I},\mathbf{o})$. Construímos o grupo abeliano libre xerado polo conxunto $\mathcal{B} = \{[\alpha] : \alpha \in \mathcal{I}\}$:

$$\mathcal{F}(N) = \left\{ \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha] : n_\alpha \in \mathbb{Z},\ \text{e case todo } n_\alpha = 0 \right\}.$$

Equipando este $\mathbb{Z}$-módulo cunha operación de multiplicación definida sobre os elementos da base

$$[\alpha]\cdot[\beta] = \sum_{\gamma\in I} N_{\alpha,\beta}^{\gamma}[\gamma], \tag{4.1}$$

obténse unha estrutura de anel, chamada *anel de fusión asociado á regra de fusión* N.

Observación 4.7. Notemos que, desta maneira, dados dous elementos calquera de $\mathcal{F}(N)$, a suma e o produto que estamos considerando son, respectivamente:

$$\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha] + \sum_{\alpha\in\mathcal{I}} n'_\alpha[\alpha] = \sum_{\alpha\in\mathcal{I}} (n_\alpha + n'_\alpha)[\alpha],$$

e

$$\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)\cdot\left(\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right) = \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\alpha]\cdot[\beta]).$$

Proposición 4.8. *Nas condicións da Definición 4.6, a multiplicación en $\mathcal{F}(N)$ está ben definida e proporciona unha estrutura de anel coas operacións indicadas na observación anterior.*

Demostración. Temos que ver que $(\mathcal{F}(N), +, \cdot)$ está ben definido e que se ten a propiedade distributiva de $\cdot$ sobre $+$.

- O Axioma (F1) asegura que a multiplicación está ben definida en termos da base, xa que a suma na Ecuación (4.1) ten un número finito de sumandos non triviais.
- O produto é distributivo respecto da suma: primeiro, dados enteiros $n, m \in \mathbb{Z}$ e $[\alpha], [\beta] \in \mathcal{B}$, pola estrutura de $\mathbb{Z}-$módulo tense que

$$\begin{aligned}(n+m)([\alpha]\cdot[\beta]) &= (n+m)\sum_{\gamma\in\mathcal{I}} N_{\alpha,\beta}^{\gamma}[\gamma] = n\sum_{\gamma\in\mathcal{I}} N_{\alpha,\beta}^{\gamma}[\gamma] + m\sum_{\gamma\in\mathcal{I}} N_{\alpha,\beta}^{\gamma}[\gamma] \\ &= n([\alpha]\cdot[\beta]) + m([\alpha]\cdot[\beta]).\end{aligned}$$

  Sexan agora tres elementos calquera de $\mathcal{F}(N)$, expresámolos en termos da base e operamos:

$$\begin{aligned}\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)\left(\sum_{\beta\in\mathcal{I}} n'_\beta[\beta] + \sum_{\beta\in\mathcal{I}} n''_\beta[\beta]\right) &= \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)\left(\sum_{\beta\in\mathcal{I}} (n'_\beta + n''_\beta)[\beta]\right) \\ &= \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha(n'_\beta + n''_\beta)([\alpha]\cdot[\beta]) \\ &= \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\alpha]\cdot[\beta]) + \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n''_\beta([\alpha]\cdot[\beta]) \\ &= \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)\left(\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right) \\ &\quad + \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)\left(\sum_{\beta\in\mathcal{I}} n''_\beta[\beta]\right).\end{aligned}$$

□

Observación 4.9. Podemos notar as seguintes propiedades para os aneis de fusión así construídos:

- Se se cumpre o Axioma (F2), entón o anel $\mathcal{F}(N)$ é asociativo. En efecto, comprobémolo para os elementos da base: se $\alpha, \beta, \gamma \in \mathcal{I}$,

$$\begin{aligned}([\alpha]\cdot[\beta])\cdot[\gamma] &= \left(\sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}[\lambda]\right)\cdot[\gamma] = \sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}([\lambda]\cdot[\gamma]) = \sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}\left(\sum_{\mu\in\mathcal{I}} N_{\lambda,\gamma}^{\mu}[\mu]\right) \\ &= \sum_{\lambda\in\mathcal{I}}\sum_{\mu\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}N_{\lambda,\gamma}^{\mu}[\mu] = \sum_{\mu\in\mathcal{I}}\sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}N_{\lambda,\gamma}^{\mu}[\mu] \underset{\text{(F2)}}{=} \sum_{\mu\in\mathcal{I}}\sum_{\lambda\in\mathcal{I}} N_{\beta,\gamma}^{\lambda}N_{\alpha,\lambda}^{\mu}[\mu] \\ &= \sum_{\lambda\in\mathcal{I}} N_{\beta,\gamma}^{\lambda}\sum_{\mu\in\mathcal{I}} N_{\alpha,\lambda}^{\mu}[\mu] = \sum_{\lambda\in\mathcal{I}} N_{\beta,\gamma}^{\lambda}([\alpha]\cdot[\lambda]) = [\alpha]\cdot\left(\sum_{\lambda\in\mathcal{I}} N_{\beta,\gamma}^{\lambda}[\lambda]\right) \\ &= [\alpha]\cdot([\beta]\cdot[\gamma]).\end{aligned}$$

- O axioma (F3) asegura que $[\mathbf{o}]$ é a identidade multiplicativa en $\mathcal{F}(N)$. Sexa $\alpha \in \mathcal{I}$:

$$[\alpha]\cdot[\mathbf{o}] = \sum_{\gamma\in\mathcal{I}} N_{\alpha,\mathbf{o}}^{\gamma}[\gamma] \underset{\text{(F3)}}{=} \sum_{\gamma\in\mathcal{I}} \delta_{\alpha\gamma}[\gamma] = [\alpha],$$

  e compróbase do mesmo xeito que $[\mathbf{o}]\cdot[\alpha] = [\alpha]$.

- O Axioma (F5) asegura que $[i]^* := [i^*]$ define un anti-isomorfismo de aneis involutivo sobre $\mathcal{F}(N)$. En efecto, a aplicación $* : \mathcal{F}(N) \to \mathcal{F}(N)$ dada por

$$\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)^* = \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]^* = \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha^*],$$

  é unha involución:

$$\left(\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)^*\right)^* = \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha^*]\right)^* = \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha^*]^* = \sum_{\alpha\in\mathcal{I}} n_\alpha[(\alpha^*)^*] = \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha].$$

  Ademais, é un anti-isomorfismo no anel $\mathcal{F}(N)$. En efecto, é evidente que $[\mathbf{o}]^* = [\mathbf{o}]$ e tense, para a suma:

$$\begin{aligned}\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha] + \sum_{\alpha\in\mathcal{I}} n'_\alpha[\alpha]\right)^* &= \left(\sum_{\alpha\in\mathcal{I}} (n_\alpha + n'_\alpha)[\alpha]\right)^* = \sum_{\alpha\in\mathcal{I}} (n_\alpha + n'_\alpha)[\alpha^*] \\ &= \sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha^*] + \sum_{\alpha\in\mathcal{I}} n'_\alpha[\alpha^*] = \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)^* + \left(\sum_{\alpha\in\mathcal{I}} n'_\alpha[\alpha]\right)^*,\end{aligned}$$

  e para o anti-produto:

$$\begin{aligned}\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right)^* &= \left(\sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\alpha]\cdot[\beta])\right)^* = \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\alpha]\cdot[\beta])^* \\ &= \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta \left(\sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^{\lambda}[\lambda]\right)^* = \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}}\sum_{\lambda\in\mathcal{I}} n_\alpha n'_\beta N_{\alpha,\beta}^{\lambda}[\lambda^*] \\ &\underset{\text{(F5)}}{=} \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}}\sum_{\lambda\in\mathcal{I}} n_\alpha n'_\beta N_{\beta^*,\alpha^*}^{\lambda^*}[\lambda^*] = \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta \left(\sum_{\gamma\in\mathcal{I}} N_{\beta^*,\alpha^*}^{\gamma}[\gamma]\right) \\ &= \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\beta^*]\cdot[\alpha^*]) = \sum_{\beta\in\mathcal{I}} n'_\beta[\beta^*]\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha^*] \\ &= \left(\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right)^* \left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right)^*.\end{aligned}$$

Observación 4.10. Coa observación anterior conclúese que, dada unha regra de fusión **asociativa** N dun conxunto punteado numerable $(\mathcal{I},\mathbf{o})$, $\mathcal{F}(N)$ é un $\mathbb{Z}_+-$anel unital onde a base numerable é $\mathcal{B} = \{[\alpha] : \alpha \in \mathcal{I}\}$. Está ademais dotado do anti-isomorfismo involutivo $*$ e, como o neutro $[\mathbf{o}]$ está na base, é evidente que $\mathcal{F}(N)$ é un anel de fusión segundo a Definición 3.9.

Proposición 4.11. *As definicións de anel de fusión (Definición 3.9) e a definición de anel de fusión asociado a unha regra de fusión asociativa dun conxunto punteado (Definición 4.6) son equivalentes.*

Demostración. A observación anterior pon de manifesto que a segunda definición implica a primeira. Comprobaremos entón que a primeira implica a segunda. Sexa $(A, B_+, *)$ un anel de fusión. Vexamos que existe un conxunto punteado $(\mathcal{I}, \mathbf{o})$ e un conxunto de regras de fusión N tal que o anel de fusión asociado a N é A. Basta considerar $\mathcal{I} = I$ o conxunto de índices que indexa a base B_+ co elemento distinguido $\mathbf{o} = i \in I$ tal que $b_{\mathbf{o}} = 1$, que está en B_+ por definición de anel de fusión. Agora, $N = \{c_{ij}^k : i, j, k \in I\}$ é un conxunto de regras de fusión. En efecto, vexamos que se satisfán os axiomas:

(F1) É consecuencia da Observación 3.2.

(F2) Sexan $i, j, k \in I$ fixados. Pola asociatividade do anel A, tense que

$$(b_i b_j) b_k = b_i (b_j b_k).$$

Desenvolvendo cada lado da igualdade obtemos

$$(b_i b_j) b_k = \left(\sum_{l \in I} c_{ij}^l b_l \right) b_k = \sum_{l \in I} c_{ij}^l (b_l b_k) = \sum_{l \in I} c_{ij}^l \left(\sum_{\lambda \in I} c_{lk}^\lambda b_\lambda \right)$$

$$= \sum_{l \in I} \sum_{\lambda \in I} c_{ij}^l c_{lk}^\lambda b_\lambda = \sum_{\lambda \in I} \sum_{l \in I} c_{ij}^l c_{lk}^\lambda b_\lambda,$$

por un lado e

$$b_i (b_j b_k) = b_i \left(\sum_{l \in I} c_{jk}^l b_l \right) = \sum_{l \in I} c_{jk}^l (b_i b_l) = \sum_{l \in I} c_{jk}^l \left(\sum_{\lambda \in I} c_{il}^\lambda b_\lambda \right)$$

$$= \sum_{l \in I} \sum_{\lambda \in I} c_{jk}^l c_{il}^\lambda b_\lambda = \sum_{\lambda \in I} \sum_{l \in I} c_{jk}^l c_{il}^\lambda b_\lambda,$$

por outro. Agora ben, por unicidade da expresión de $(b_i b_j) b_k = b_i (b_j b_k)$ na base $\{b_i\}_{i \in I}$ do $\mathbb{Z}-$módulo $(A, +)$, terase que

$$\sum_{l \in I} c_{ij}^l c_{lk}^\lambda = \sum_{l \in I} c_{jk}^l c_{il}^\lambda \ , \quad \text{para todo} \ \ \lambda \in I.$$

(F3) Podemos escribir

$$b_i = b_i \cdot 1 = b_i \cdot b_{\mathbf{o}} = \sum_{k \in I} c_{i\mathbf{o}}^k b_k.$$

Agora ben, como $\{b_i\}_{i \in I}$ é base de $(A, +)$ entón, por unicidade da expresión, $c_{i\mathbf{o}}^k = \delta_{ik}$. Análogamente, $c_{\mathbf{o}i}^k = \delta_{ik}$.

(F4) Basta empregar o homomorfismo de grupos τ, xa que por linearidade:

$$\tau(b_ib_j) = \tau\left(\sum_{k\in I} c_{ij}^k b_k\right) = \sum_{k\in I} c_{ij}^k \tau(b_k) = \sum_{k\in I} c_{ij}^k \delta_{k\mathbf{o}} = c_{ij}^{\mathbf{o}}.$$

Agora, pola Definición 3.7, $c_{ij}^{\mathbf{o}} = \tau(b_ib_j) = \delta_{i^*j}$ e entón o elemento dual i^* de $i \in I$ é o dado pola involución $i \mapsto i^*$.

(F5) Lembremos que, pola Proposición 3.8, $c_{ij}^{k^*} = \tau(b_ib_jb_k)$, $\tau(x) = \tau(x^*)$, $\tau(xy) = \tau(yx)$ e que $(b_ib_j)^* = b_j^*b_i^*$ (isto último por ser $*$ un anti-isomorfismo de aneis). Entón:

$$c_{ij}^k = \tau(b_ib_jb_k^*) = \tau((b_ib_jb_k^*)^*) = \tau(b_k(b_ib_j)^*) = \tau(b_kb_j^*b_i^*) = \tau(b_j^*b_i^*b_k) = c_{j^*i^*}^{k^*}.$$

(F6) A reciprocidade de Frobenius está probada de dúas formas, unha nesta sección e outra na Sección 3.1, na Proposición 3.8.

Concluíndo, dado que a base é $B_+ = \{b_i\}_{i\in I}$, que o anel de fusión asociado a N, $\mathcal{F}(N)$, constrúese a partir do $\mathbb{Z}-$módulo libre xerado por B_+ e que a multiplicación dos elementos da base coincide nas dúas definicións (sen máis que observar as expresións), $\mathcal{F}(N) = A$. □

Proposición 4.12. *Sexa G un grupo numerable (ou finito) con elemento neutro $\mathbf{1} \in G$ (coa notación multiplicativa), e consideremos $(G, \mathbf{1})$ como un conxunto punteado numerable. Entón, o conxunto de enteiros non negativos $N_G = \{N_{\alpha,\beta}^\gamma : \alpha, \beta, \gamma \in G\}$ dado por*

$$N_{\alpha,\beta}^\gamma = \begin{cases} 1, & \text{se } \alpha\beta = \gamma \text{ (co produto en } G), \\ 0, & \text{en caso contrario}, \end{cases}$$

define una regra de fusión asociativa sobre $(G, \mathbf{1})$ onde $\alpha^* = \alpha^{-1}$. Ademais, o anel de fusión $\mathcal{F}(N_G)$ é isomorfo ao anel de grupo $\mathbb{Z}[G]$.

Demostración. Para ver que é unha regra de fusión asociativa, verifiquemos os axiomas:

(F1) Sexan $\alpha, \beta \in G$, o conxunto $\{\gamma \in \mathcal{I} : N_{\alpha,\beta}^\gamma \neq 0\} = \{\gamma \in \mathcal{I} : \alpha\beta = \gamma\} = \{\alpha\beta\}$, que é finito.

(F2) Temos que comprobar que dados $\alpha, \beta, \gamma \in G$,

$$\sum_{\lambda\in\mathcal{I}} N_{\beta,\gamma}^\lambda N_{\alpha,\lambda}^\mu = \sum_{\lambda\in\mathcal{I}} N_{\alpha,\beta}^\lambda N_{\lambda,\gamma}^\mu \ ,$$

para todo $\mu \in \mathcal{I}$. Fixados $\alpha, \beta, \gamma \in G$, terase que, para $\lambda \in G$, os coeficientes $N_{\beta,\gamma}^\lambda$ son nulos salvo cando $\lambda = \beta\gamma$, de forma que o único sumando do lado esquerdo que pode non ser nulo para algún $\mu \in G$ é $N_{\beta,\gamma}^{\beta\gamma} N_{\alpha,\beta\gamma}^\mu$. Análogamente, no lado dereito obtemos que o único sumando que posiblemente non é nulo é $N_{\alpha,\beta}^{\alpha\beta} N_{\alpha\beta,\gamma}^\mu$. Do mesmo xeito, ambos sumandos anularanse cando $\mu \neq \alpha\beta\gamma$ e valerán 1 cando $\mu = \alpha\beta\gamma$, o que conclúe a igualdade.

(F3) Dado que o 1 é o neutro do grupo G, $\alpha 1 = 1\alpha = \alpha$, de forma que $N_{\alpha,1}^{\beta} = N_{1,\alpha}^{\beta} = \delta_{\alpha\beta}$.

(F4) Sexa $\alpha \in G$ arbitrario, o inverso $\alpha^{-1} \in G$ é o único elemento que cumpre $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$ e así, $N_{\alpha,\beta}^{1} = N_{\beta\alpha}^{1} = \delta_{\alpha^{-1}\beta}$.

(F5) Tense que $\beta^*\alpha^* = \beta^{-1}\alpha^{-1} = (\alpha\beta)^{-1}$. Entón, por unicidade do neutro, $(\alpha\beta)^{-1} = \gamma^{-1}$ se e só se $\alpha\beta = \gamma$, de forma que $N_{\alpha\beta}^{\gamma} = N_{\beta^{-1}\alpha^{-1}}^{\gamma^{-1}} = N_{\beta^*\alpha^*}^{\gamma^*}$.

Por ser asociativa a regra de fusión, cumpre a Reciprocidade de Frobenius tamén.

Comprobemos agora que, en efecto, $\mathcal{F}(N_G)$ é isomorfo a o anel grupo $\mathbb{Z}[G]$ (Definición 1.40). O anel de fusión xerado pola base $\{[g] : g \in G\}$ é da forma

$$\mathcal{F}(N_G) = \left\{ \sum_{g\in G} n_g[g] : n_g \in \mathbb{Z} \text{ e } n_g = 0, \text{ para case todo } g \in G \right\}.$$

Co cal, as definicións son equivalentes, así como as operacións, polo que basta considerar a aplicación $f : \mathcal{F}(N) \to \mathbb{Z}[G]$ dada por $f([g]) = g$, estendida naturalmente como

$$f\left(\sum_{g\in G} n_g[g]\right) = \sum_{g\in G} a_g f([g]) = \sum_{g\in G} a_g g,$$

que é trivialmente un isomorfismo de aneis. □

4.2. Morfismos de fusión

Nesta sección, definiremos as aplicacións que conservan a estrutura entre aneis de fusión e estudaremos as súas propiedades, co obxectivo de definir a categoría dos aneis de fusión e caracterizar os seus grupos de automorfismos.

Empregaremos o termo *regra de fusión* cando queiramos referirnos indistintamente a regras de fusión asociativas e a regras de fusión non asociativas.

Definición 4.13. Sexa $(\mathcal{I}_i, \mathbf{o}_i)$ un conxunto punteado numerable e N_i unha regra de fusión sobre $(\mathcal{I}_i, \mathbf{o}_i)$, para $i = 1, 2$. Un morfismo de conxuntos punteados $f\colon (\mathcal{I}_1, \mathbf{o}_1) \to (\mathcal{I}_2, \mathbf{o}_2)$ dise que é un *morfismo de regras de fusión* se para cada $\alpha, \beta \in \mathcal{I}_1$,

$$N_{f(\alpha),f(\beta)}^{\kappa} = \begin{cases} \sum_{\gamma\in f^{-1}(\{\kappa\})} N_{\alpha,\beta}^{\gamma}, & \text{se } \kappa \in f(\mathcal{I}_1) \subset \mathcal{I}_2, \\ 0, & \text{se } \kappa \in \mathcal{I}_2 \setminus f(\mathcal{I}_1) \subset \mathcal{I}_2. \end{cases}$$

Ademais, se $(\mathcal{I}_1, \mathbf{o}_1) = (\mathcal{I}_2, \mathbf{o}_2)$ e f é bixectiva, diremos que é un *automorfismo de regras de fusión.*

Definición 4.14. Nas condicións da definición anterior, se f é un morfismo de regras de fusión, chamamos *morfismo de fusión asociado a* f á aplicación $F(f)\colon \mathcal{F}(N_1) \to \mathcal{F}(N_2)$ estendida pola conservación das operacións da estrutura. Isto é, para cada $a \in \mathcal{F}(N_1)$:

$$F(f)(a) = F(f)\left(\sum_{\alpha\in\mathcal{I}_1} n_\alpha[\alpha]\right) = \sum_{\alpha\in\mathcal{I}_1} n_\alpha[f(\alpha)].$$

De xeito que para cada $\alpha, \beta \in \mathcal{I}_1$,

$$F(f)([\alpha][\beta]) = F(f)\left(\sum_{\lambda\in\mathcal{I}_1} N^\lambda_{\alpha,\beta}[\lambda]\right) = \sum_{\lambda\in\mathcal{I}_1} N^\lambda_{\alpha,\beta}[f(\lambda)].$$

Exemplo 4.15. Sexa N unha regra de fusión sobre o conxunto punteado $(\mathcal{I}, \mathbf{o})$. Entón, a aplicación identidade no anel de fusión $Id_{\mathcal{F}(N)}$, é un morfismo de fusión asociado ao morfismo de regras de fusión dado pola identidade $Id_{\mathcal{I}}$.

As dúas proposicións seguintes séguense inmediatamente da Definición 4.13.

Proposición 4.16. *Sexa* $(\mathcal{I}_i, \mathbf{o}_i)$ *un conxunto punteado numerable e* N_i *unha regra de fusión sobre* $(\mathcal{I}_i, \mathbf{o}_i)$*, para* $i = 1, 2$*. Todo morfismo de fusión* $F(f)$ *asociado a un morfismo de regras de fusión* $f : (\mathcal{I}_1, \mathbf{o}_1) \to (\mathcal{I}_2, \mathbf{o}_2)$ *é un homomorfismo de aneis.*

Demostración. Sexa $F(f)$ o morfismo de fusión asociado a f e $a, b \in \mathcal{F}(N)$. Por un lado, $F(f)([\mathbf{o}_1]) = [f(\mathbf{o}_1)] = [\mathbf{o}_2]$. Por outro lado, para a suma, se $a, b \in \mathcal{F}(N_1)$,

$$\begin{aligned} F(f)(a+b) &= F(f)\left(\sum_{\alpha\in\mathcal{I}_1} n_\alpha[\alpha] + \sum_{\alpha\in\mathcal{I}_1} n'_\alpha[\alpha]\right) = \sum_{\alpha\in\mathcal{I}_1} (n_\alpha + n'_\alpha)[f(\alpha)] \\ &= \sum_{\alpha\in\mathcal{I}_1} n_\alpha[f(\alpha)] + \sum_{\alpha\in\mathcal{I}_1} n'_\alpha[f(\alpha)] = F(f)(a) + F(f)(b). \end{aligned}$$

Para o produto, vexamos o que ocurre primeiro cos elementos da base. Sexan $\alpha, \beta \in \mathcal{I}_1$,

$$F(f)([\alpha][\beta]) = F(f)\left(\sum_{\lambda\in\mathcal{I}_1} N^\lambda_{\alpha,\beta}[\lambda]\right) = \sum_{\lambda\in\mathcal{I}_1} N^\lambda_{\alpha,\beta}[f(\lambda)].$$

Por outro lado,

$$\begin{aligned} F(f)([\alpha])F(f)([\beta]) = [f(\alpha)][f(\beta)] &= \sum_{\kappa\in\mathcal{I}_2} N^\kappa_{f(\alpha),f(\beta)}[\kappa] \\ &= \sum_{\kappa\in f(\mathcal{I}_1)} N^\kappa_{f(\alpha),f(\beta)}[\kappa] \quad + \sum_{\kappa\in\mathcal{I}_2\setminus f(\mathcal{I}_1)} N^\kappa_{f(\alpha),f(\beta)}[\kappa]. \end{aligned}$$

Agora ben, por ser f un automorfismo de regras de fusión, a segunda suma é cero. Empregando entón a definición de morfismo de regras de fusión,

$$F(f)([\alpha])F(f)([\beta]) = \sum_{\kappa\in f(\mathcal{I}_1)} N^{\kappa}_{f(\alpha),f(\beta)}[\kappa] = \sum_{\kappa\in f(\mathcal{I}_1)} \left(\sum_{\gamma\in f^{-1}(\{\kappa\})} N^{\gamma}_{\alpha,\beta} \right) [f(\lambda)]$$
$$= \sum_{\lambda\in\mathcal{I}_1} N^{\lambda}_{\alpha,\beta}[f(\lambda)] = F(f)([\alpha][\beta]).$$

Finalmente, a extensión a calquera par de elementos de $\mathcal{F}(N)$ é sinxela:

$$F(f)\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right) = F(f)\left(\sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta([\alpha][\beta])\right) = \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta F(f)([\alpha][\beta])$$
$$= \sum_{\alpha\in\mathcal{I}}\sum_{\beta\in\mathcal{I}} n_\alpha n'_\beta F(f)([\alpha])F(f)([\beta])$$
$$= \sum_{\alpha\in\mathcal{I}} n_\alpha F(f)([\alpha]) \sum_{\beta\in\mathcal{I}} n'_\beta F(f)([\beta])$$
$$= F(f)\left(\sum_{\alpha\in\mathcal{I}} n_\alpha[\alpha]\right) F(f)\left(\sum_{\beta\in\mathcal{I}} n'_\beta[\beta]\right).$$

□

Proposición 4.17. *A composición de morfismos de fusión é un morfismo de fusión.*

Demostración. Sexa $(\mathcal{I}_i, \mathbf{o}_i)$ un conxunto punteado numerable e N_i unha regra de fusión sobre $(\mathcal{I}_i, \mathbf{o}_i)$, con $i = 1, 2, 3$. Consideremos, para cada $i = 1, 2, 3$ o anel de fusión asociado a N_i, $\mathcal{F}(N_i)$. Tomemos ademais dous morfismos de regras de fusión $f_1 : (\mathcal{I}_1, \mathbf{o}_1) \to (\mathcal{I}_2, \mathbf{o}_2)$ e $f_2 : (\mathcal{I}_2, \mathbf{o}_2) \to (\mathcal{I}_3, \mathbf{o}_3)$ e os morfismos de fusión asociados $F(f_1)\colon \mathcal{F}(N_1) \to \mathcal{F}(N_2)$ e $F(f_2)\colon \mathcal{F}(N_2) \to \mathcal{F}(N_3)$. Comecemos vendo que $f_2 \circ f_1$ é un morfismo de regras de fusión. En efecto, pola Definición 4.14, $f_2(f_1(\mathbf{o}_1)) = f_2(\mathbf{o}_2) = \mathbf{o}_3$ e, para cada $\alpha, \beta \in \mathcal{I}_1$, tense:

$$N^{\widetilde{\kappa}}_{f_2(f_1(\alpha)),f_2(f_1(\beta))} = \begin{cases} \sum_{\widetilde{\gamma}\in f_2^{-1}(\{\widetilde{\kappa}\})} N^{\widetilde{\gamma}}_{f_1(\alpha),f_1(\beta)}, & \text{se } \widetilde{\kappa} \in f_2(\mathcal{I}_2), \\ 0, & \text{se } \widetilde{\kappa} \in \mathcal{I}_3 \setminus f(\mathcal{I}_2). \end{cases}$$

Agora, como f_1 é un morfismo de regras de fusión,

$$N^{\widetilde{\kappa}}_{f_2(f_1(\alpha)),f_2(f_1(\beta))} = \begin{cases} \sum_{\widetilde{\gamma}\in f_2^{-1}(\{\widetilde{\kappa}\})} \left(\sum_{\gamma\in f_1^{-1}(\{\widetilde{\gamma}\})} N^{\gamma}_{\alpha,\beta} \right), & \text{se } \widetilde{\kappa} \in f_2(\mathcal{I}_2) \text{ e } \widetilde{\gamma} \in f_1(\mathcal{I}_1), \\ 0, & \text{noutro caso.} \end{cases}$$

Notemos que se $\widetilde{\gamma} \in f_1(\mathcal{I}_1)$, entón $\widetilde{\kappa} = f_2(\widetilde{\gamma}) \in f_2(f_1(\mathcal{I}_1))$, logo

$$N^{\widetilde{\kappa}}_{f_2(f_1(\alpha)),f_2(f_1(\beta))} = \begin{cases} \sum_{\gamma\in f_2^{-1}(f_2^{-1}(\{\widetilde{\kappa}\}))} N^{\gamma}_{\alpha,\beta}, & \text{se } \widetilde{\kappa} \in f_2(f_1(\mathcal{I}_2)), \\ 0, & \text{noutro caso.} \end{cases}$$

Así, $f_2 \circ f_1$ é un morfismo de regras de fusión, do que se segue que $F(f_2 \circ f_1)$ é un morfismo de fusión. Finalmente, sexa $\alpha \in \mathcal{I}_1$,

$$F(f_2 \circ f_1)([\alpha]) = (f_2 \circ f_1)([\alpha]) = f_2(f_1([\alpha])) = f_2(F(f_1)([\alpha])) = (F(f_2) \circ F(f_1))([\alpha]),$$

co que

$$F(f_2 \circ f_1) = F(f_2) \circ F(f_1).$$

□

Definición 4.18. Tendo en conta a Proposición 4.17 e o Exemplo 4.15, podemos definir a categoría dos aneis de fusión $\mathcal{C} = \mathsf{Fus}$ como segue: os obxectos son os aneis de fusión asociados a unha regra de fusión nun conxunto punteado numerable, para cada $\mathcal{F}(N_1), \mathcal{F}(N_2) \in \mathrm{obx}(\mathcal{C})$, $\mathrm{Hom}_{\mathsf{Fus}}(\mathcal{F}(N_1), \mathcal{F}(N_2))$ é o conxunto de morfismos de fusión de $\mathcal{F}(N_1)$ en $\mathcal{F}(N_2)$; e a lei de composición é a dada pola composición de aplicacións.

Caractericemos agora os automorfismos en $\mathcal{C} = \mathsf{Fus}$. Sexa $(\mathcal{I}, \mathbf{o})$ un conxunto punteado numerable e N un conxunto de regras de fusión en $(\mathcal{I}, \mathbf{o})$. Para empezar, se $f : (\mathcal{I}, \mathbf{o}) \to (\mathcal{I}, \mathbf{o})$ é un automorfismo de regras fusión (Definición 4.13), entón $f^{-1}(\mathbf{o_1}) = f^{-1}(f(\mathbf{o_1})) = \mathbf{o_1}$ e, ademais,

$$N^{\gamma}_{\alpha,\beta} = N^{f(f^{-1}(\gamma))}_{f(f^{-1}(\alpha)),f(f^{-1}(\beta))} = N^{f^{-1}(\gamma)}_{f^{-1}(\alpha),f^{-1}(\beta)}, \text{ para todo } \gamma \in \mathcal{I}_1.$$

Notemos que como f é bixectivo, $\mathcal{I}_1 \setminus f^{-1}(\mathcal{I}_1) = \emptyset$. Así, f^{-1} é un automorfismo de regras de fusión. Agora, observemos que, pola Proposición 4.17,

$$F(f) \circ F(f^{-1}) = F(f \circ f^{-1}) = Id_{\mathcal{F}(N_1)},$$

e viceversa, co que $F(f)^{-1} = F(f^{-1})$. Conclúese directamente que $F(f)^{-1}$ é un morfismo de fusión. Deste xeito e tendo en conta a Definición 1.7, caracterizamos de dúas formas os automorfismos de $\mathcal{C} = \mathsf{Fus}$ (que denominaremos *automorfismos de fusión*):

(AF1) Son aqueles morfismos de fusión $F(f) : \mathcal{F}(N) \to \mathcal{F}(N)$ que posúen inversa para a composición de aplicacións.

(AF2) Son os morfismos de fusión $F(f) : \mathcal{F}(N) \to \mathcal{F}(N)$ tales que f é un automorfismo de regras de fusión.

Notemos finalmente que, pola Proposición 4.16, o grupo de automorfismos de fusión $\mathrm{Aut}_{\mathsf{Fus}}(\mathcal{F}(N))$ é un subgrupo de $\mathrm{Aut}_{\mathsf{Ring}}(\mathcal{F}(N))$.

Exemplo 4.19. Todo automorfismo de fusión é un automorfismo de aneis, pero non necesariamente coinciden ambos grupos. Por exemplo, consideremos o grupo multiplicativo $\mathbb{Z}/2\mathbb{Z} = \{\mathbf{1}, \tau\}$ e o seu anel de grupo sobre $\mathbb{Z}$, $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$, xa detallado no Exemplo 1.42. Pola Proposición 4.12, podemos ver $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ como un anel de fusión sobre o conxunto punteado $(\mathbb{Z}/2\mathbb{Z}, \mathbf{1})$. Neste caso,

dado que os isomorfismos de conxuntos punteados deben cumprir $f(\mathbf{1}) = \mathbf{1}$, o único posible é a identidade. Así pois, todo automorfismo de fusión debe cumprir, para calquera $n, m \in \mathbb{Z}$,

$$f(n + m\tau) = nf(\mathbf{1}) + mf(\tau) = n + m\tau,$$

co que $\mathrm{Aut}_{\mathsf{Fus}}(\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]) = \{Id\}$. Sen embargo, $f\colon \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}] \to \mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$ dado por $f([\tau]) = -[\tau]$ é un automorfismo de aneis que non é un automorfismo de fusión.

Sabemos que todo morfismo de fusión é un morfismo de aneis (Proposición 4.16), pero o recíproco non é certo (Exemplo 4.19). A seguinte proposición dá unha condición suficiente para que un morfismo de aneis sexa un morfismo de fusión.

Proposición 4.20. *Sexa $(\mathcal{I}, \mathbf{o})$ un conxunto punteado numerable, N unha regra de fusión sobre $(\mathcal{I}, \mathbf{o})$ e consideremos un morfismo de conxuntos punteados que é unha permutación dos índices $f : (\mathcal{I}, \mathbf{o}) \to (\mathcal{I}, \mathbf{o})$. Se $F(f)$ é un homomorfismo de aneis, entón é un morfismo de fusión.*

Demostración. Por ser $F(f)$ un homomorfismo de aneis, se $\alpha, \beta \in \mathcal{I}$,

$$F(f)([\alpha][\beta]) = F(f)([\alpha])F(f)([\beta]).$$

Agora ben, por un lado,

$$f([\alpha][\beta]) = f\left(\sum_{\lambda\in\mathcal{I}} N^{\lambda}_{\alpha,\beta}[\mu]\right) = \sum_{\lambda\in\mathcal{I}} N^{\lambda}_{\alpha,\beta} f([\lambda]) = \sum_{\lambda\in\mathcal{I}} N^{\lambda}_{\alpha,\beta}[f(\lambda)],$$

e por outro, empregando a bixectividade de f,

$$f([\alpha])f([\beta]) = [f(\alpha)][f(\beta)] = \sum_{\lambda\in\mathcal{I}} N^{f(\lambda)}_{f(\alpha),f(\beta)}[f(\lambda)].$$

Finalmente, pola unicidade da expresión de $F(f)([\alpha][\beta]) = F(f)([\alpha])F(f)([\beta])$ na base $\{[\alpha] : \alpha \in \mathcal{I}\}$ do $\mathbb{Z}-$módulo $(\mathcal{F}(N), +)$, temos que

$$N^{f(\lambda)}_{f(\alpha),f(\beta)} = N^{\lambda}_{\alpha,\beta}, \text{ para todo } \lambda \in \mathcal{I}.$$

Así, f é un morfismo de regras de fusión □

Proposición 4.21. *Sexa G un grupo numerable con elemento neutro $\mathbf{1} \in G$ (notación multiplicativa), e consideremos o anel de grupo sobre $\mathbb{Z}$ asociado, $\mathbb{Z}[G]$, como un anel de fusión, como na Proposición 4.12. Entón,* $\mathrm{Aut}_{\mathsf{Fus}}(\mathbb{Z}[G]) \cong \mathrm{Aut}_{grp}(G)$.

Demostración. Lembremos que na Proposición 4.12 tomábamos $(G, \mathbf{1})$ como o conxunto punteado numerable sobre o que se definía o anel de fusión $\mathbb{Z}[G]$. Así, todo automorfismo de grupos $f \in \mathrm{Aut}_{\mathsf{Grp}}(G)$ é un morfismo de regras de fusión. En efecto, $f(\mathbf{1}) = \mathbf{1}$ e se $\alpha, \beta, \gamma \in G$, tense

$$N^{\gamma}_{\alpha,\beta} = \begin{cases} 1, & \text{se } \alpha\beta = \gamma, \\ 0, & \text{en caso contrario.} \end{cases}$$

E tamén

$$N_{f(\alpha),f(\beta)}^{f(\gamma)} = \begin{cases} 1, & \text{se } f(\alpha)f(\beta) = f(\gamma), \\ 0, & \text{en caso contrario.} \end{cases}$$

Agora ben, como f é un automorfismo de grupos,

$$f(\alpha\beta) = f(\alpha)f(\beta) = f(\gamma).$$

Pola inxectividade, isto é equivalente a que $\alpha\beta = \gamma$, co que

$$N_{f(\alpha),f(\beta)}^{f(\gamma)} = N_{\alpha,\beta}^{\gamma}.$$

Notemos que, por ser f bixectiva, $G \setminus f(G) = \emptyset$. Agora ben, cada $f \in \mathrm{Aut}_{\mathsf{Grp}}(G)$ induce entón un automorfismo de fusión $F(f) \in \mathrm{Aut}_{fus}(\mathbb{Z}[G])$. Sexa a aplicación

$$\begin{aligned} \mathrm{Aut}_{\mathsf{Grp}}(G) &\xrightarrow{F} \mathrm{Aut}_{Fus}(\mathbb{Z}[G]) \\ f &\longmapsto F(f) : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] \\ &\qquad \textstyle\sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g f(g) \end{aligned}$$

Polo feito ata agora, está ben definida. Vexamos que é un isomorfismo de grupos:

- $F(f \circ g) = F(f) \circ F(g)$, segundo o visto na Proposición 4.17.
- Comprobemos a inxectividade:

  $$\mathrm{Ker}(F) = \{f \in \mathrm{Aut}_{\mathsf{Grp}}(G) : F(f) = Id_{\mathbb{Z}[G]}\},$$

  logo se $f \in \mathrm{Ker}(F)$, $F(f)(g) = f(g) = g$ para todo $g \in G$, entón $f = Id_G$ e o núcleo é trivial.
- Para a sobrexectividade, como cada $F(f) \in \mathrm{Aut}_{\mathsf{Fus}}(\mathbb{Z}[G])$ ven inducida por un morfismo de regras de fusión $f \in \mathrm{Aut}_{\mathsf{Grp}}(G)$ (Definición 4.13), entón f é o antecedente buscado.

□

4.3. Unidades nos aneis de fusión

Nesta sección imos definir as unidades nos aneis de fusión, elementos especiais que nos permitirán introducir os equivalentes, neste contexto, da conxugación e dos automorfismos interiores dun grupo. Lembremos que estes últimos, tal e como se indicaba na Observación 2.9, constitúen a obstrucción principal para que a categoría dos grupos non poida ser finitamente universal.

Definición 4.22. Sexa N unha regra de fusión sobre un conxunto punteado numerable $(\mathcal{I}, \mathbf{o})$. Dado $\nu \in \mathcal{I}$, dicimos que $[\nu]$ é unha *unidade* no anel de fusión $\mathcal{F}(N)$ se $N_{\nu,\nu^*}^{\alpha} = N_{\nu^*,\nu}^{\alpha} = \delta_{\mathbf{o},\alpha}$ para todo $\alpha \in \mathcal{I}$. Isto é, $[\nu]$ é unha unidade en $\mathcal{F}(N)$ se, e só se, $[\nu][\nu^*] = [\nu^*][\nu] = [\mathbf{o}]$. O conxunto de unidades en $\mathcal{F}(N)$ denótase por $U(\mathcal{F}(N))$.

Observación 4.23. Notemos que se $[\nu] \in U(\mathcal{F}(N))$, entón $[\nu^*] \in U(\mathcal{F}(N))$, xa que $[(\nu^*)^*] = [\nu]$.

Para o que resta desta sección, N denotará unha regra de fusión **asociativa** sobre un conxunto punteado numerable $(\mathcal{I}, \mathbf{o})$.

Lema 4.24. *Sexa $[\nu] \in U(\mathcal{F}(N))$. Entón para todo $\alpha \in \mathcal{I}$ existe $\gamma \in \mathcal{I}$ tal que $[\nu][\alpha] = [\gamma]$.*

Demostración. Sexa $[\nu] \in U(\mathcal{F}(N))$ e $\alpha \in \mathcal{I}$. Entón,

$$[\nu] \cdot [\alpha] = \sum_{\gamma \in \mathcal{I}} N_{\nu,\alpha}^{\gamma} [\gamma],$$

onde tódolos coeficientes son non negativos. Empregando a asociatividade e que $[\nu]$ é unha unidade,

$$[\alpha] = [\mathbf{o}][\alpha] = [\nu^*]([\nu][\alpha]) = \sum_{\gamma \in \mathcal{I}} N_{\nu,\alpha}^{\gamma} [\nu^*][\gamma] = \sum_{\delta \in \mathcal{I}} \sum_{\gamma \in \mathcal{I}} N_{\nu,\alpha}^{\gamma} N_{\nu^*,\gamma}^{\delta} [\delta].$$

Agora ben, posto que $\mathcal{B} = \{[\nu] : \nu \in \mathcal{I}\}$ é unha base do $\mathbb{Z}-$módulo $(\mathcal{F}(N), +)$, a unicidade da expresión implica

$$\sum_{\gamma \in \mathcal{I}} N_{\nu,\alpha}^{\gamma} N_{\nu^*,\gamma}^{\alpha} = 1.$$

E como $N_{\nu,\alpha}^{\gamma} = N_{\nu^*,\gamma}^{\alpha}$ pola Reciprocidade de Frobenius, obtemos

$$\sum_{\gamma \in \mathcal{I}} (N_{\nu,\alpha}^{\gamma})^2 = 1,$$

o cal é posible en $\mathbb{Z}_+$ se, e só se tódolos sumandos, excepto un, son triviais e o sumando non trivial é igual a 1. Dito doutro modo, se, e só se $[\nu] \cdot [\alpha] = [\gamma]$ para algún $\gamma \in \mathcal{I}$. □

Lema 4.25. *Se $[\nu] \in U(\mathcal{F}(N))$, entón para todo $\alpha \in \mathcal{I}$ existe $\gamma \in \mathcal{I}$ tal que $[\alpha][\nu] = [\gamma]$.*

Demostración. É exactamente igual ca do Lema 4.24 pero multiplicando pola dereita en vez de pola esquerda. □

Lema 4.26. *Sexa $U(\mathcal{F}(N))$ o conxunto de unidades no anel de fusión $\mathcal{F}(N)$. Entón, a multiplicación en $\mathcal{F}(N)$ dá lugar a unha estrutura de grupo multiplicativo sobre $U(\mathcal{F}(N))$ na que o elemento neutro é $[\mathbf{o}]$ e, para calquera unidade $[\nu]$, o seu inverso en $U(\mathcal{F}(N))$ é $[\nu^*]$.*

Demostración. Sexa $[\nu],[\mu] \in U(\mathcal{F}(N))$. Segundo o Lema 4.24, existe $\gamma \in \mathcal{I}$ tal que $[\nu][\mu] = [\gamma]$. Como $[i]^* := [i^*]$ induce un anti-isomorfismo en $\mathcal{F}(N)$ (pola Observación 4.9),

$$[\gamma^*] = [\gamma]^* = ([\nu][\mu])^* = [\mu^*][\nu^*],$$

e a asociatividade dá lugar a

$$[\gamma][\gamma^*] = ([\nu][\mu])([\mu^*][\nu^*]) = [\nu]([\mu][\mu^*])[\nu] = [\nu][\mathbf{o}][\nu^*] = [\mathbf{o}].$$

Para $[\gamma^*][\gamma] = [\mathbf{o}]$ é análogo co Lema 4.25. Así, $[\gamma] \in U(\mathcal{F}(N))$. É dicir, a multiplicación en $U(\mathcal{F}(N))$ é pechada. Ademais, $\cdot$ é asociativa en $\mathcal{F}(N)$ co que tamén o será en $U(\mathcal{F}(N))$.

Por outro lado, o elemento neutro en $U(\mathcal{F}(N))$ é $[\mathbf{o}]$, xa que é trivialmente unha unidade e o neutro multiplicativo en $\mathcal{F}(N)$.

Finalmente, se $[\nu] \in U(\mathcal{F}(N))$, entón $[\nu^*] \in U(\mathcal{F}(N))$ (pola Observación 4.23) e $[\nu][\nu^*] = [\mathbf{o}]$ implica que $[\nu^*]$ actúa como $[\nu]^{-1}$ en $U(\mathcal{F}(N))$.

□

Exemplo 4.27. Sexa G un grupo numerable con elemento neutro $\mathbf{1} \in G$ (coa notación multiplicativa). Consideremos $\mathbb{Z}[G]$ como un anel de fusión como na Proposición 4.12. Entón $G \cong U(\mathbb{Z}[G])$. En efecto, pola Observación 1.41, G pode identificarse cun subgrupo de $\mathcal{U}(\mathbb{Z}[G])$ e resulta evidente que dito subgrupo é $U(\mathbb{Z}[G])$, por definición.

Definición 4.28. Sexa $[\nu] \in U(\mathcal{F}(N))$. Chámase *conxugación de fusión por* ν á aplicación:

$$\mathcal{F}(N) \xrightarrow{\psi_\nu} \mathcal{F}(N)$$

$$[\alpha] \longmapsto [\nu][\alpha][\nu^*].$$

Proposición 4.29. *Nas condicións da definición anterior,* ψ_ν *é un automorfismo de fusión para cada* $[\nu] \in U(\mathcal{F}(N))$.

Demostración. Fixado $[\nu] \in U(\mathcal{F}(N))$, polo Lema 4.24, existe un único $\gamma_1 \in \mathcal{I}$ tal que $[\nu][\alpha] = [\gamma_1]$ e polo Lema 4.25 existe un único $\gamma \in \mathcal{I}$ tal que $[\gamma_1][\nu^*] = [\gamma]$. É dicir, para cada $\alpha \in \mathcal{I}$ existe un único $\gamma \in \mathcal{I}$ tal que $[\nu][\alpha][\nu^*] = [\gamma]$. Polo tanto, podemos establecer unha bixección en $\mathcal{I}$ dada por $f_\nu(\alpha) = \gamma$. Agora ben, notemos o seguinte:

- Primeiro, se tomamos $\mathbf{o} \in \mathcal{I}$, temos que

  $$\psi_\nu([\mathbf{o}]) = [\nu][\mathbf{o}][\nu^*] = [\mathbf{o}],$$

  co que $f_\nu(\mathbf{o}) = \mathbf{o}$. Así, f_ν é un morfismo de conxuntos punteados.

- Para calquera $\alpha, \beta \in \mathcal{I}$,

$$\psi_\nu([\alpha][\beta]) = [\nu][\alpha][\beta][\nu^*] = [\nu][\alpha][\nu][\nu^*][\beta][\nu^*] = \psi_\nu([\alpha])\psi_\nu([\beta]).$$

Entón, pola Proposición 4.20, $F(f_\nu) = \psi_\nu$ e un morfismo de fusión. □

Definición 4.30. O conxunto de conxugacións de fusión por cada unidade,

$$\mathrm{Inn}(\mathcal{F}(N)) := \{\psi_\nu : [\nu] \in U(\mathcal{F}(N))\},$$

denomínase *automorfismos de fusión internos* de $\mathcal{F}(N)$.

Proposición 4.31. *Nas condicións da definición anterior,* $\mathrm{Inn}(\mathcal{F}(N))$ *ten estrutura de grupo coa composición de aplicacións e, polo tanto, é un subgrupo do grupo de automorfismos de fusión en* $\mathcal{F}(N)$.

Demostración. Vexamos primeiro que a composición é pechada en $\mathrm{Inn}(\mathcal{F}(N))$. Sexan $[\nu], [\mu] \in U(\mathcal{F}(N))$. Polo Lema 4.26, $[\nu][\mu] = [\gamma] \in U(\mathcal{F}(N))$, co que ψ_γ está ben definida. Agora, temos que, para cada $\alpha \in \mathcal{I}$,

$$(\psi_\nu \circ \psi_\mu)([\alpha]) = \psi_\nu([\mu][\alpha][\mu^*]) = ([\nu][\mu])[\alpha]([\mu^*][\nu^*]) = [\gamma][\alpha][\gamma^*] = \psi_\gamma([\alpha]).$$

Así, a composición de conxugacións de fusión é unha conxugación de fusión.

Por outro lado, a asociatividade séguese do feito de que a composición de aplicacións é asociativa. Notemos ademais que

$$\psi_{\mathbf{o}}([\beta]) = [\mathbf{o}][\beta][\mathbf{o}] = [\beta], \text{ para todo } \beta \in \mathcal{I}.$$

Co que $\psi_{\mathbf{o}} = Id_{\mathcal{F}(N)}$ é o elemento neutro en $\mathrm{Inn}(\mathcal{F}(N))$. Finalmente, se $[\nu] \in U(\mathcal{F}(N))$,

$$\psi_\nu \circ \psi_{\nu^*} = \psi_{\nu^*} \circ \psi_\nu = \psi_{\mathbf{o}} = Id_{\mathcal{F}(N)},$$

logo $\psi_\nu^{-1} = \psi_{\nu^*}$ e temos un inverso para cada elemento de $\mathrm{Inn}(\mathcal{F}(N))$. □

Exemplo 4.32. Sexa G un grupo numerable con elemento neutro $\mathbf{1} \in G$ (coa notación multiplicativa) e consideremos a $\mathbb{Z}[G]$ como un anel de fusión como na Proposición 4.12. Xa vimos que $\mathrm{Aut}_{\mathsf{Fus}}(\mathbb{Z}[G]) \cong \mathrm{Aut}_{\mathsf{Grp}}(G)$ na Proposición 4.21 e que $G \cong U(\mathbb{Z}[G])$ no Exemplo 4.27. Entón, para cada $g \in G$, o morfismo de fusión ψ_g da Definición 4.28 non é máis que o inducido pola conxugación (pola esquerda) por g (véxase a Definición 2.6).

Capítulo 5

Realización de grupos na categoría dos aneis de fusión

Este último capítulo está dedicado demostrar a universalidade finita da categoría dos aneis de fusión, $\mathcal{C} = \mathsf{Fus}$ (véxase a Definición 4.18). A partir de agora, dividiremos a categoría dos aneis de fusión en dous e denotaremos por AFus a (sub)categoría dos aneis de fusión **asociativos** e por NAFus a dos aneis de fusión **non asociativos**. Este capítulo divídese en dúas partes, presentando o estudo do problema de realización en cada unha das categorías anteriores.

Na primeira parte, retomamos a dificultade que impedía a universalidade finita da categoría $\mathcal{C} = \mathsf{Grp}$: non todo grupo finito G pode realizarse como o grupo de automorfismos interiores doutro grupo H (véxase o Teorema 2.8 e a Observación 2.9). Mostramos que esta limitación non aparece na categoría $\mathcal{C} = \mathsf{AFus}$ cando o grupo en cuestión é abeliano. Para iso, baseámonos no estudo da Sección 4.3 e utilizamos un anel de fusión particular, o chamado *anel de fusión de Haagerup-Izumi*, descrito en [25]. Isto permítenos realizar grupos abelianos finitos como grupos de automorfismos internos de aneis de fusión asociativos.

Na segunda parte, estudaremos a universalidade finita de $\mathcal{C} = \mathsf{NAFus}$ (e, polo tanto, de $\mathcal{C} = \mathsf{Fus}$) a través dun novo obxecto matemático: o anel de fusión asociado a un grafo simple. Esta construción aproveita o teorema de Frucht (Teorema 2.26) para demostrar que todo grupo finito pode realizarse como o grupo de automorfismos dun anel de fusión, que neste caso será **non asociativo**. Con esta construción, mostramos que a categoría $\mathcal{C} = \mathsf{Fus}$ é finitamente universal, resultado que, ata onde sabemos, non fora demostrado con anterioridade e que constitúe unha achega orixinal deste traballo.

5.1. Realizabilidade en $\mathcal{C} = \mathsf{AFus}$

Nesta sección resolveremos parcialmente o problema da realización de grupos finitos na categoría $\mathcal{C} = \mathsf{AFus}$. En concreto, resolveremos a dificultade exposta no Capítulo 2 (véxase a Observación 2.9) demostrando que todo grupo abeliano finito pode realizarse como grupo de automorfismos internos dun anel de fusión asociativo.

5.1.1. O anel de fusión de Haagerup-Izumi

Os conceptos de regra de fusión, Definición 4.2, e de anel de fusión, Definición 4.6, son esenciais para comprender con claridade a construción que se presentará a continuación.

Definición 5.1. Sexa $G = \{g_1 = \mathbf{1}, \dots, g_n\}$ un grupo abeliano finito (notación multiplicativa). Sexa $\{t_1\}$ un conxunto de forma que podemos considerar o conxunto finito (de xeito formal)

$$T = \{t_1 := \mathbf{1}t_1,\ t_2 := g_2t_1, \dots, t_n := g_nt_1\}.$$

Chamamos *anel de fusión de Haagerup-Izumi asociado a* G, que denotamos por $\mathrm{HI}(G)$, ao anel de fusión xerado polo conxunto punteado $(G \sqcup T, \mathbf{1})$ equipado coa regra de fusión N que induce en $\mathcal{F}(N)$ o seguinte produto $\times$ entre os elementos da base:

$$\begin{aligned} g_i \times g_j &= g_ig_j, \\ g_i \times t_j &= (g_ig_j)t_1, \\ t_i \times g_j &= (g_ig_j^{-1})t_1, \\ t_i \times t_j &= g_ig_j^{-1} + \sum_{k=1}^{n} t_k. \end{aligned}$$

Proposición 5.2. *Sexa G un grupo abeliano finito. Entón* $\mathrm{HI}(G)$ *é un anel de fusión, que é ademais asociativo.*

Demostración. Comecemos recordando a Proposición 4.11, pola que é suficiente probar que $(\mathcal{F}(N), +, \cdot)$ é un anel asociativo, que $\mathbf{1}$ é a unidade multiplicativa en $\mathcal{F}(N)$ e que existe un anti-isomorfismo involutivo $* : \mathcal{F}(N) \to \mathcal{F}(N)$.

- Asociatividade. Temos que comprobala para tódolos elementos da base. Empregaremos a asociatividade en G. Primeiro, supoñamos que temos tres elementos de G:

$$(g_i \times g_j) \times g_k = (g_ig_j) \times g_k = ((g_ig_j)g_k) = (g_i(g_jg_k)) = g_i \times (g_jg_k) = g_i \times (g_j \times g_k).$$

Agora, tomemos dous elementos de G e un de T:

$(g_i \times g_j) \times t_k = (g_i g_j) \times t_k = ((g_i g_j) g_k) t_1 = (g_i (g_j g_k)) t_1 = g_i \times (g_j g_k) t_1 = g_i \times (g_j \times t_k)$.

$(g_i \times t_j) \times g_k = (g_i g_j) t_1 \times g_k = ((g_i g_j) g_k^{-1}) t_k = (g_i (g_j g_k^{-1})) t_1 = g_i \times (g_j g_k^{-1}) t_1 = g_i \times (t_j \times g_k)$.

$(t_i \times g_j) \times g_k = (g_i g_j^{-1}) t_1 \times g_k = ((g_i g_j^{-1}) g_k^{-1}) t_1 \underset{(\circledast)}{=} (g_i (g_j g_k)^{-1}) t_1 = g_i \times (g_j g_k) = t_i \times (g_j \times g_k)$.

Continuando co proceso, se temos un elemento de G e dous de T:

$$(g_i \times t_j) \times t_k = (g_i g_j) t_1 \times t_k = ((g_i g_j) g_k^{-1}) + \sum_{l=1}^{n} t_l \underset{(\ddagger)}{=} (g_i (g_j g_k^{-1})) + \sum_{l=1}^{n} g_i g_l t_1$$

$$= g_i \times (g_j g_k^{-1} + \sum_{l=1}^{n} t_l) = g_i \times (t_j \times t_k).$$

$$(t_i \times g_j) \times t_k = (g_i g_j^{-1}) t_1 \times t_k = ((g_i g_j^{-1}) g_k^{-1}) + \sum_{l=1}^{n} t_l \underset{(\circledast)}{=} (g_i (g_j g_k)^{-1}) + \sum_{l=1}^{n} t_l = t_i \times (g_j g_k) t_1$$

$$= t_i \times (g_j \times t_k).$$

$$(t_i \times t_j) \times g_k = \left(g_i g_j^{-1} + \sum_{l=1}^{n} t_l \right) \times g_k = ((g_i g_j^{-1}) g_k) + \sum_{l=1}^{n} g_l g_k^{-1} t_1 \underset{(\ddagger),(\circledast)}{=} (g_i (g_j g_k^{-1})^{-1}) + \sum_{l=1}^{n} t_l$$

$$= t_i \times (g_j g_k^{-1}) t_1 = t_i \times (t_j \times t_k).$$

Por último, para o caso dos tres elementos en T, notemos primeiro que

$$(t_i \times t_j) \times t_k = \left(g_i g_j^{-1} + \sum_{l=1}^{n} t_l \right) \times t_k = ((g_i g_j^{-1}) g_k) t_1 + \sum_{l=1}^{n} \left(g_l g_k^{-1} + \sum_{\lambda=1}^{n} t_\lambda \right),$$

e, por outro lado,

$$t_i \times (t_j \times t_k) = t_i \times \left(g_j g_k^{-1} + \sum_{l=1}^{n} t_l \right) = (g_i (g_j g_k^{-1})^{-1}) t_1 + \sum_{l=1}^{n} \left(g_i g_l + \sum_{\lambda=1}^{n} t_\lambda \right)$$

$$\underset{(\ddagger),(\circledast)}{=} ((g_i g_j^{-1}) g_k) t_1 + \sum_{l=1}^{n} \left(g_l g_k^{-1} + \sum_{\lambda=1}^{n} t_\lambda \right).$$

Nas igualdades anteriores, en $(\circledast)$ empregamos o feito de que G é abeliano e en $(\ddagger)$ que en todo grupo G tense, para todo $g_i, g_k \in G$, $g_i G = G = G g_k^{-1}$, o cal é evidente pola existencia dos inversos de cada elemento de G.

- Que $\mathbf{1} \in G$ é a unidade multiplicativa en $\mathcal{F}(N)$ é evidente por ser $g\mathbf{1} = g = \mathbf{1}g$ para todo $g \in G$ e pola definición de $\mathrm{HI}(G)$.

- Comprobemos agora que todo elemento en $G \sqcup T$ ten un dual. Notemos primeiro que a unidade $\mathbf{1}$ está na base $G \sqcup T$, co que o homomorfismo de grupos $\tau : \mathrm{HI}(G) \to \mathbb{Z}$ (véxase a Definición 3.4) se trivializa e resulta, para cada $x \in G \sqcup T$,

$$\tau(x) = \begin{cases} 1, \text{ se } x = \mathbf{1}, \\ 0, \text{ noutro caso.} \end{cases}$$

Deste xeito, para os elementos de G, como $g \times g^{-1} = \mathbf{1}$, temos que $\tau(g \times g^{-1}) = \mathbf{1}$ e, pola propia construción de $\mathrm{HI}(G)$ (Definición 5.1), $\tau(g \times s) = 0$ para cada $s \in \mathrm{HI}(G)$ con $s \neq g$. Así, segundo a Definición 3.7, tomamos $g^* := g^{-1}$.

Centrémonos agora nos elementos de T. Sexa $i \in \{1, \ldots, n\}$ fixado e $t_i \in T$. Por definición,

$$t_i \times t_j = g_i g_j^{-1} + \sum_{k=1}^{n} t_k,$$

para cada $j \in \{1, \ldots, n\}$. Agora, por ser τ un homomorfismo de grupos,

$$\tau(t_i \times t_j) = \tau(g_i g_j^{-1}) + \sum_{k=1}^{n} \tau(t_k) = \tau(g_i g_j^{-1}).$$

Deste xeito, segundo o que comprobamos para os elementos de G, $\tau(t_i \times t_j) = 1$ se $j = i$ e $\tau(t_i \times t_j) = 0$, se $j \neq i$. Agora ben, tendo de novo en conta a definición de $\mathrm{HI}(G)$, $\tau(t_i \times s) = 0$, para todo $g \in G$. Finalmente, podemos definir $t_i^* := t_i$.

Co anterior, temos unha aplicación $* : G \sqcup T \to G \sqcup T$ que cumpre a primeira parte da Definición 3.7. Vexamos que a extensión natural ao anel é un anti-isomorfismo involutivo: que é involutivo é evidente por selo na base, e para comprobar que é un anti-isomorfismo de aneis, basta probar o anti-produto nos elementos da base. En efecto, considerando $g_i, g_j, t_i, t_j \in G \sqcup T$ e tendo en conta que G é abeliano:

$$(g_i \times g_j)^* = (g_i g_j)^* = (g_i g_j)^{-1} = g_j^{-1} g_i^{-1} = g_j^* \times g_i^*,$$

$$(g_i \times t_j)^* = ((g_i g_j) \cdot t_1)^* = (g_i g_j) \cdot t_1 = (g_j (g_i^{-1})^{-1}) \cdot t_1 = (t_j \times g_i^{-1}) = (t_j^* \times g_i^*),$$

$$(t_i \times g_j)^* = ((g_i g_j^{-1}) \cdot t_1)^* = (g_i g_j^{-1}) \cdot t_1 = (g_j^{-1} g_i) \cdot t_1 = (g_j^{-1} \times t_i) = (g_j^* \times t_i^*),$$

$$(t_i \times t_j)^* = (g_i g_j^{-1})^* + \sum_{k=1}^{n} t_k^* = (g_i g_j^{-1})^{-1} + \sum_{k=1}^{n} t_k = (g_j g_i^{-1}) + \sum_{k=1}^{n} t_k = (t_j^* \times t_i^*).$$

En conclusión, $\mathcal{F}(N)$ é un anel base unital cunha base de rango finito, co que é un anel de fusión (véxase a Definición 4.6).

□

5.1.2. Resultado principal

Unha vez introducidos os aneis $\mathrm{HI}(G)$ para cada grupo abeliano finito G, estamos en condicións de demostrar que todo grupo abeliano finito é isomorfo ao grupo de automorfismos internos dalgún anel de fusión asociativo $\mathcal{F}(N) \in \mathrm{obx}(\mathsf{AFus})$. Con iso, resolvemos o obstáculo sinalado no Capítulo 2 (véxase a Observación 2.9) no caso abeliano, o que constitúe un avance significativo na realización de grupos finitos como grupos de automorfismos de aneis de fusión asociativos.

Lema 5.3. *Sexa G un grupo abeliano finito. Entón o grupo de unidades (Definición 4.22)* $U(\mathrm{HI}(G)) \cong G$.

Demostración. Os únicos elementos $s \in G \sqcup T$ tales que o seu dual en $\mathcal{F}(N)$ cumpre $s \times s^* = 1$ son os elementos de G, co que a bixección $f : U(\mathrm{HI}(G)) \to G$ dada por $f(g) = g$ é trivialmente un isomorfismo de grupos. □

Lembramos que, para un grupo abeliano finito G, $\mathrm{Tor}_2(G)$ denota o subgrupo de G dos elementos de orde 2 (véxase Definición 1.34).

Teorema 5.4. *Sexa G un grupo abeliano finito. Entón, existe un anel de fusión asociativo $\mathcal{F}(N) \in \mathrm{obx}(\mathsf{Fus})$ tal que*

$$G/\operatorname{Tor}_2(G) \cong \mathrm{Inn}(\mathcal{F}(N)).$$

Demostración. Primeiro de todo, polo Lema 5.3, $U(\mathrm{HI}(G)) \cong G$, co que para cada $g_i \in G$, os automorfismos $\psi_{g_i} \in \mathrm{Inn}(\mathrm{HI}(G))$ (Definición 4.28), están ben definidos. Ademais, por ser G abeliano, cumpren

$$\begin{aligned}\psi_{g_i}(g_j) &= g_i \times g_j \times g_i^* = g_i g_j g_i^{-1} = g_j,\\ \psi_{g_i}(t_j) &= g_i \times t_j \times g_i^* = ((g_i g_j) \cdot t_1) \times g_i^* = (g_i g_j g_i) \cdot t_1 = (g_i^2 g_j) \cdot t_1,\end{aligned}$$

co que ψ_{g_i} será trivial se, e só se $(g_i^2 g_j) \cdot t_1 = t_j$, o que ocurrirá se e só se $g_i^2 g_j = g_j$ ou, equivalentemente, se e só se $g_i^2 = 1$.

Sexa agora a aplicación

$$\psi : G \to \mathrm{Inn}(\mathrm{HI}(G)),$$

dada por $\psi(g_i) = \psi_{g_i}$. Vexamos que é un homomorfismo de grupos: se $g_i, g_j \in G$,

$$\psi(g_i g_j) = \psi_{g_i g_j} = \psi_{g_i} \circ \psi_{g_j} = \psi(g_i) \circ \psi(g_j),$$

onde a segunda igualdade está probada na Proposición 4.31. Agora, se calculamos o núcleo de ψ,

$$\mathrm{Ker}(\psi) = \{g_i \in G : \psi_{g_i} = Id_{\mathrm{HI}(G)}\} \underset{(\circledast)}{=} \{g_i \in G : g_i^2 = 1\} = \mathrm{Tor}_2(G),$$

onde a igualdade ($\circledast$) séguese da equivalencia obtida máis arriba.

Isto garante que $\mathrm{Tor}_2(G)$ é un subgrupo normal de G por ser o núcleo dun homomorfismo de grupos. Finalmente, grazas ao primeiro teorema de isomorfía (Teorema 1.24), deducimos que

$$G/\operatorname{Tor}_2(G) \cong \mathrm{Inn}(\mathrm{HI}(G)).$$

□

Contamos xa con todos os elementos necesarios para probar que todo grupo abeliano finito pódese realizar como grupo de automorfismos internos dun anel de fusión.

Corolario 5.5. *Sexa G un grupo abeliano finito. Entón existe un anel de fusión $\mathcal{F}(N)$ tal que* $\mathrm{Inn}(\mathcal{F}(N)) \cong G$.

Demostración. Polo Teorema 1.33, podemos escribir G como

$$G \cong G_{(2)} \oplus H,$$

onde H é un grupo de orde impar e

$$G_{(2)} \cong \mathbb{Z}_{2^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{2^{k_n}},$$

para certos $k_1, \ldots, k_n$ enteiros positivos (notemos que $G_{(2)}$ é o grupo trivial no caso en que $2 \nmid G$). Definimos

$$\overline{G} \cong \mathbb{Z}_{2^{k_1+1}} \oplus \cdots \oplus \mathbb{Z}_{2^{k_n+1}} \oplus H.$$

Comprobemos agora que $G \cong \overline{G}/\operatorname{Tor}_2(\overline{G})$. Primeiro, pola Proposición 1.36, temos que

$$\operatorname{Tor}_2(\overline{G}) \cong \operatorname{Tor}_2(\mathbb{Z}_{2^{k_1+1}}) \oplus \ldots \oplus \operatorname{Tor}_2(\mathbb{Z}_{2^{k_n+1}}) \oplus \operatorname{Tor}_2(H).$$

Agora ben, como cada subgrupo $\mathbb{Z}_{2^{k_i}}$ é cíclico e $2|2^{k_i}$, polo Teorema 1.21, cada un destes grupos contén un único elemento de orde 2. Dito elemento é, precisamente, 2^{k_i}, pois $2 \cdot 2^{k_i} = 2^{k_i+1} = 0$ (ou sexa, $2^{k_i} + 2^{k_i} = 0$). Ademais, $\operatorname{Tor}_2(H) = \{0\}$, xa que é un grupo de orde impar. Deste xeito,

$$\operatorname{Tor}_2(\overline{G}) \cong \underbrace{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{n)}.$$

Notemos agora que, para cada $i \in \{1, \ldots, n\}$, polo teorema de correspondencia de grupos (Teorema 1.26), $2^{k_i}\mathbb{Z}/2^{k_i+1}\mathbb{Z}$ é un subgrupo de $\mathbb{Z}/2^{k_i+1}\mathbb{Z}$. Vexamos que ten orde 2: polo segundo teorema de isomorfía (Teorema 1.25),

$$\operatorname{ord}\left(\frac{\mathbb{Z}/2^{k_i+1}\mathbb{Z}}{2^{k_i}\mathbb{Z}/2^{k_i+1}\mathbb{Z}}\right) = \operatorname{ord}\left(\mathbb{Z}/2^{k_i}\mathbb{Z}\right) = 2^{k_i},$$

e ademais $\operatorname{ord}(\mathbb{Z}/2^{k_i+1}\mathbb{Z}) = 2^{k_i+1}$, co que

$$\operatorname{ord}(2^{k_i}\mathbb{Z}/2^{k_i+1}\mathbb{Z}) = \frac{\operatorname{ord}(\mathbb{Z}/2^{k_i+1}\mathbb{Z})}{\operatorname{ord}(\mathbb{Z}/2^{k_i}\mathbb{Z})} = 2^{k_i+1}/2^{k_i} = 2.$$

Como hai un único grupo de orde 2 salvo isomorfismos, $\mathbb{Z}/2\mathbb{Z} \cong 2^{k_i}\mathbb{Z}/2^{k_i+1}\mathbb{Z}$ e entón, aplicando de novo o segundo teorema de isomorfía (Teorema 1.25):

$$\frac{\mathbb{Z}_{2^{k_i+1}}}{\mathbb{Z}_{2^{k_i}}} \cong \frac{\mathbb{Z}/2^{k_i+1}\mathbb{Z}}{2^{k_i}\mathbb{Z}/2^{k_i+1}\mathbb{Z}} \cong \mathbb{Z}_{2^{k_i}}.$$

Empregando agora a Proposición 1.37,

$$\overline{G}/\operatorname{Tor}_2(\overline{G}) \cong \frac{\mathbb{Z}_{2^{k_1+1}} \oplus \cdots \oplus \mathbb{Z}_{2^{k_n+1}} \oplus H}{\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 \oplus \{0\}} \cong \frac{\mathbb{Z}_{2^{k_1+1}}}{\mathbb{Z}_2} \oplus \cdots \oplus \frac{\mathbb{Z}_{2^{k_n+1}}}{\mathbb{Z}_2} \oplus \frac{H}{\{0\}} \cong \mathbb{Z}_{2^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{2^{k_n}} \oplus H \cong G.$$

Finalmente, polo Teorema 5.4, tense que

$$\operatorname{Inn}(\operatorname{HI}(\overline{G})) \cong \overline{G}/\operatorname{Tor}_2(\overline{G}) \cong G.$$

□

5.2. Universalidade finita de $\mathcal{C} = \mathsf{NAFus}$

Ao considerar grupos finitos arbitrarios (non abelianos) non se poden empregar procedementos similares aos utilizados na sección anterior para estudar se son realizables en $\mathcal{C} = \mathsf{NAFus}$. Nesta sección, empregaremos unha ferramenta importante no estudo da universalidade finita de categorías: o teorema de Frucht, que nos garante a universalidade finita da categoría dos grafos finitos e simples. Para levar a cabo esta tarea, imos analizar como se relacionan os grafos cos aneis de fusión a partir dun novo obxecto: o *anel de fusión asociado a un grafo simple*.

Dado un grafo simple finito $\mathcal{G} = (V, E)$, consideremos o conxunto

$$\overline{E} = \{(v, w) : \{v, w\} \in E\},$$

de tódolos pares ordenados formados polas aristas de E. Sexa ademais un conxunto $\{\mathbf{o}\}$ tal que $\{\mathbf{o}\} \cap \left(\overline{E} \cup V\right) = \emptyset$. Finalmente, definimos

$$\mathcal{I}_{\mathcal{G}} = \overline{E} \cup V \cup \{\mathbf{o}\}.$$

Definición 5.6. Definimos a operación *concatenación* no $\mathbb{Z}-$módulo xerado por $\mathcal{I}_{\mathcal{G}}$ como segue:

- Se $(u, v), (w, t) \in \overline{E}$,

$$(u, v) \cdot (w, t) = \begin{cases} (u, t), & \text{se } v = w \text{ e } u \neq t, \\ \mathbf{o}, & \text{se } v = w \text{ e } u = t, \\ 0, & \text{noutro caso.} \end{cases} \tag{5.1}$$

- Se $v, w \in V$, entonces

$$v \cdot w = \begin{cases} (v, w), & \text{se } \{v, w\} \in E \text{ e } v \neq w, \\ \mathbf{o}, & \text{se } v = w, \\ 0, & \text{noutro caso.} \end{cases} \tag{5.2}$$

- Se $(u,v) \in \overline{E}$ e $w \in V$,

$$(u,v)\cdot w = \begin{cases} u, & \text{se } \ v = w, \\ 0, & \text{noutro caso.} \end{cases} \tag{5.3}$$

e tamén

$$w\cdot (u,v) = \begin{cases} v, & \text{se } \ w = u, \\ 0, & \text{noutro caso.} \end{cases} \tag{5.4}$$

Finalmente, a concatenación co elemento distinguido $\mathbf{o}$ defínese como segue: se $(u,v) \in \overline{E}$ e $w \in V$,

$$\begin{gathered} (u,v)\cdot \mathbf{o} = \mathbf{o}\cdot (u,v) = (u,v), \\ w\cdot \mathbf{o} = \mathbf{o}\cdot w = w, \\ \mathbf{o}\cdot \mathbf{o} = \mathbf{o}. \end{gathered} \tag{5.5}$$

Recordemos que na Definición 4.6 introducimos a noción de anel de fusión $\mathcal{F}(N)$ asociado a unha regra de fusión N.

Proposición 5.7. *Sexa $\mathcal{G} = (V,E)$ un grafo simple finito e $(\mathcal{I}_{\mathcal{G}}, \mathbf{o})$ o conxunto punteado dotado das regras que inducen a operación concatenación, que denotamos por $N_{\mathcal{G}}$. Entón, $N_{\mathcal{G}}$ é un conxunto de regras de fusión, e polo tanto $\mathcal{F}(N_{\mathcal{G}})$ é un anel de fusión, que denominaremos* anel de fusión asociado a $\mathcal{G}$.

Demostración. A proba redúcese a calcular $N_{\mathcal{G}}$ e probar que é un conxunto de regras de fusión. Tendo en conta a definición da concatenación, é sinxelo ver que, para cada $\gamma \in \mathcal{I}_{\mathcal{G}}$ fixado, os elementos $N^{\gamma}_{\alpha,\beta} \in N_{\mathcal{G}}$, con $\alpha, \beta \in \mathcal{I}_{\mathcal{G}}$ son da forma que se describe a continuación. Utilizaremos a notación $\delta_{i,j}$ para referirnos á delta de Kronecker:

- Se temos dúas aristas $(u,v),(w,t) \in \overline{E}$ distintas e incidentes, ou sexa $v = w$ e $u \neq t$, entón

$$N^{\gamma}_{(u,v),(v,t)} \underset{(5.1)}{=} \delta_{\gamma,(u,t)}.$$

- Para dous vértices $u, v \in V$ tales que $\{v,w\} \in E$, tense

$$N^{\gamma}_{v,w} \underset{(5.2)}{=} \delta_{\gamma,(v,w)}.$$

- Para unha arista $(u,v) \in E$, empregando as Ecuacións (5.3) e (5.4),

$$\begin{aligned} N^{\gamma}_{(u,v),v} &= \delta_{\gamma,u}, \\ N^{\gamma}_{u,(u,v)} &= \delta_{\gamma,v}. \end{aligned}$$

- Dada unha arista $(u,v) \in \overline{E}$ e un vértice $w \in V$, pola Ecuación (5.5),

$$\begin{aligned} &N^{\gamma}_{\mathbf{o},(u,v)} = N^{\gamma}_{(u,v),\mathbf{o}} = \delta_{\gamma,(u,v)}, \\ &N^{\gamma}_{\mathbf{o},w} = N^{\gamma}_{w,\mathbf{o}} = \delta_{\gamma,w}, \\ &N^{\gamma}_{\mathbf{o},\mathbf{o}} = \delta_{\gamma,\mathbf{o}}. \end{aligned} \tag{5.6}$$

- Finalmente, notemos que se $(u, v) \in \overline{E}$ e $w \in V$, empregando de novo a Ecuación (5.5),

$$\begin{aligned} N^{\mathbf{o}}_{w,\gamma} &= N^{\mathbf{o}}_{t,\gamma} = \delta_{\gamma,w}, \\ N^{\mathbf{o}}_{(u,v),\gamma} &= N^{\mathbf{o}}_{\gamma,(u,v)} = \delta_{\gamma,(v,u)}, \\ N^{\mathbf{o}}_{\mathbf{o},\gamma} &= N^{\mathbf{o}}_{\gamma,\mathbf{o}} = \delta_{\gamma,\mathbf{o}}. \end{aligned} \tag{5.7}$$

O resto dos elementos de $N_{\mathcal{G}}$ son todos cero. Deste xeito, pasemos a comprobar os axiomas da Definición 4.2.

(F1) É evidente por ser o grafo $\mathcal{G}$ finito.

(F3) A unidade é o elemento $\mathbf{o}$, como amosa a Ecuación (5.6).

(F4) Da Ecuación (5.7) dedúcese que os vértices $v \in V$ e o elemento $\mathbf{o}$ son autoduais. En canto a unha arista $(u, v) \in \overline{E}$, ten por dual $(v, u) \in \overline{E}$.

(F5) Temos que comprobar que, para todo $\alpha, \beta, \gamma \in \mathcal{I}_{\mathcal{G}}$, $N^{\gamma}_{\alpha,\beta} = N^{\gamma^*}_{\beta^*,\alpha^*}$. Teñamos primeiro en conta os que son distintos de cero. Tomemos $u, v \in V$ e $(u, v), (v, t) \in \overline{E}$.

$$\begin{aligned} N^{(u,v)}_{u,v} &= 1 = N^{(v,u)}_{v,u} = N^{(u,v)^*}_{v^*,u^*}, \\ N^{(u,t)}_{(u,v),(v,t)} &= 1 = N^{(t,u)}_{(t,v),(v,u)} = N^{(u,t)^*}_{(v,t)^*,(u,v)^*}, \\ N^{u}_{(u,v),v} &= 1 = N^{u}_{v,(v,u)} = N^{u^*}_{v^*,(u,v)^*}, \\ N^{v}_{u,(u,v)} &= 1 = N^{v}_{(v,u),u} = N^{v^*}_{(v,u)^*,u^*}. \end{aligned}$$

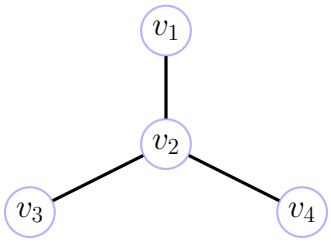
No caso de que apareza $\mathbf{o}$ como índice en $N^{\gamma}_{\alpha,\beta} \in N_{\mathcal{G}}$, é evidente que se ten (F5) polas Ecuacións (5.6) e (5.7). Finalmente, como o resto dos elementos de $N^{\gamma}_{\alpha,\beta} \in N_{\mathcal{G}}$ e os correspondentes $N^{\gamma^*}_{\beta^*,\alpha^*}$ son cero, cúmprese trivialmente para eles.

(F6) En principio, non temos asegurado que este anel sexa asociativo (Definición 4.5), co que temos que comprobar a reciprocidade de Frobenius. De novo, verémolo para os elementos distintos de 0, téndose entón directamente para o resto de elementos de $N_{\mathcal{G}}$. Sexa $u, v \in V$ e $(u, v), (v, t) \in \overline{E}$.

$$\begin{aligned} 1 &= N^{(u,v)}_{u,v} = N^{v}_{u,(u,v)} = N^{u}_{(u,v),v}, \\ 1 &= N^{(u,t)}_{(u,v),(v,t)} = N^{(v,t)}_{(v,u),(u,t)} = N^{(u,v)}_{(u,t),(t,v)}, \\ 1 &= N^{u}_{(u,v),v} = N^{v}_{(v,u),u} = N^{(u,v)}_{u,v}, \\ 1 &= N^{u}_{v,(v,u)} = N^{(v,u)}_{v,u} = N^{v}_{u,(u,v)}. \end{aligned}$$

Co que, tendo en conta que u e v son autoduais e que $(u, v)^* = (v, u)$ e $(v, t)^* = (t, v)$, xa estaría demostrado. No caso en que $\mathbf{o}$ apareza como índice, é evidente polas Ecuacións (5.6) e (5.7). □

Observación 5.8. En xeral, o anel de fusión $\mathcal{F}(N_{\mathcal{G}})$ non é asociativo. Por exemplo, se temos o seguinte grafo simple finito:



entón, $(v_1 \cdot v_3) \cdot v_3 = 0 \cdot v_3 = 0$, pero $v_1 \cdot (v_3 \cdot v_3) = v_1 \cdot \mathbf{o} = v_1$. Teñamos en conta que isto é posible facelo para todo grafo que non sexa completo, de maneira que este tipo de grafos non dan lugar a aneis de fusión asociativos.

O seguinte paso é estudar o que ocurre cos elementos de $\mathrm{Aut}_{\mathsf{Fus}}(\mathcal{F}(N_{\mathcal{G}}))$, para tratar de establecer algunha conexión cos automorfismos de $\mathcal{G}$.

Recordamos que na Definición 4.13 e Definición 4.14 introducimos, respectivamente, os morfismos de regras de fusión e morfismos de fusión.

Lema 5.9. *Sexa $\mathcal{G} = (V, E)$ un grafo simple finito. Entón, se $f : \mathcal{I}_{\mathcal{G}} \to \mathcal{I}_{\mathcal{G}}$ é un automorfismo de regras de fusión, a restrición $f_{|_V} : V \to V$ é un automorfismo de grafos.*

Demostración. Temos que ver que $f_{|_V}$ leva vértices en vértices e que preserva a adxacencia. Primeiramente, notemos que os únicos elementos autoduales en $\mathcal{F}(N_{\mathcal{G}})$ son os vértices, como vimos na proba da Proposición 5.7. Agora, por ser f un automorfismo de regras de fusión, o automorfismo de fusión $F(f)$ inducido en $\mathcal{F}(N_{\mathcal{G}})$ satisfai:

$$\mathbf{o} = f(\mathbf{o}) = F(f)(v \cdot v) = f(v) \cdot f(v),$$

logo $f(v)$ é o seu propio dual, de forma que $f(v)$ ten que ser un vértice de $\mathcal{G}$. Agora, como f é bixectiva, se $(u, v) \in \overline{E}$, entón $f((u, v)) \in \overline{E}$, e tendo en conta a definición de $\overline{E}$, f preserva a adxacencia. Notemos que, como f é un automorfismo de regras de fusión, f^{-1} tamén o é, e polo tanto a adxacencia consérvase tamén no sentido contrario. □

Lema 5.10. *Sexa $\mathcal{G} = (V, E)$ un grafo simple finito. Entón,*

$$\mathrm{Aut}_{\mathsf{Fus}}(\mathcal{F}(N_{\mathcal{G}})) \cong \mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}).$$

Demostración. Polo lema anterior, todo automorfismo de fusión induce un automorfismo de grafos. Resta entón comprobar que todo automorfismo de grafos pode estenderse a un automorfismo de fusión. Sexa $f : V \to V$ un automorfismo de grafos de $\mathcal{G}$ e consideremos a súa extension a $\mathcal{I}_{\mathcal{G}}$ dada, para cada $x \in \mathcal{I}_{\mathcal{G}}$, por

$$f^{\mathcal{I}_{\mathcal{G}}}(x) = \begin{cases} (f(u), f(w)), & \text{se } x = (u, w) \in \overline{E}, \\ \mathbf{o}, & \text{se } x = \mathbf{o}, \\ f(v), & \text{se } x = v \in V. \end{cases}$$

Así, $f^{\mathcal{I}_\mathcal{G}}$ está ben definida e é bixectiva por ser f un automorfismo de grafos. Ademais, é un automorfismo de regras de fusión sen máis que ter en conta a Definición 4.13. □

Teorema 5.11. *A categoría $\mathcal{C} = \mathsf{NAFus}$ é finitamente universal.*

Demostración. Polo teorema de Frucht (Teorema 2.26), dado G un grupo finito, existe un grafo simple finito $\mathcal{G}_{SF} \in \mathrm{Obx}(\mathsf{Graphs})$ tal que

$$\mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}_{SF}) \cong G.$$

Agora ben, por ser $\mathcal{G}_{SF}$ un grafo simple finito e polo Lema 5.10,

$$\mathrm{Aut}_{\mathsf{Fus}}(\mathcal{F}(N_{\mathcal{G}_{SF}})) \cong \mathrm{Aut}_{\mathsf{Graphs}}(\mathcal{G}_{SF}) \cong G.$$

Por outro lado, tendo en conta que o grafo $\mathcal{G}_{SF}$ asociado ao grafo de Cayley dun grupo finito non é completo, e a Observación 5.8, obtemos que $\mathcal{F}(N_{\mathcal{G}_{SF}})$ é non asociativo.

Finalmente, dado que G foi escollido arbitrariamente, concluímos que $\mathcal{C} = \mathsf{NAFus}$ é finitamente universal. □

Do resultado anterior séguese inmediatamente o seguinte corolario:

Corolario 5.12. *A categoría $\mathcal{C} = \mathsf{Fus}$ é finitamente universal.*

Bibliografía

[1] M. A. Alekseyev, W. Bruns, S. Palcoux, and F. V. Petrov. Classification of integral modular data up to rank 13, 2024. arXiv:2302.01613.

[2] T. B. Andersen. Rank 2 fusion rings are complete intersections. *Journal of Algebra*, 477:231–238, 2017.

[3] L. Babai. *Automorphism Groups, Isomorphism, Reconstruction.* Elsevier Science B.V., Amsterdam, The Netherlands, 1995.

[4] R. E. Behrend, P. A. Pearce, V. B. Petkova, and J.-B. Zuber. On the classification of bulk and boundary conformal field theories. *Physics Letters B*, 444(1-2):163–166, 1998.

[5] M. Belolipetsky and A. Lubotzky. Finite groups and hyperbolic manifolds. *Inventiones mathematicae*, 162(3):459–472, 2005.

[6] G. Birkhoff. Sobre los grupos de automorfismos. *Revista de la Unión Matemática Argentina*, 11(4):155–157, 1946.

[7] G. Chartrand, H. Jordon, V. Vatter, and P. Zhang. *Graphs & Digraphs.* CRC Press, Boca Raton, FL, USA, 6th edition, 2016.

[8] C. Costoya, D. Méndez, and A. Viruel. Realisability problem in arrow categories. *Collectanea Mathematica*, 71(3):383–405, 2020.

[9] C. Costoya and A. Viruel. Every finite group is the group of self-homotopy equivalences of an elliptic space. *Acta Mathematica*, 213(1):49–62, 2014.

[10] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik. *Tensor Categories*, volume 205 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, USA, 2015.

[11] E. Fried and J. Kóllar. Automorphism groups of algebraic number fields. *Mathematische Zeitschrift*, 163(2):121–123, 1978.

[12] R. Frucht. Herstellung von graphen mit vorgegebener abstrakter gruppe. *Compositio Mathematica*, 6:239–250, 1939.

[13] L. Greenberg. Conformal transformations of riemann surfaces. *American Journal of Mathematics*, 82(4):749–760, 1960.

[14] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, New York, NY, USA, 2nd edition, 1985.

[15] N. Jacobson. *Basic algebra II.* W. H. Freeman and Company, New York, NY, USA, 2nd edition, 1985.

[16] E. Jespers and Á. del Río. *Group Ring Groups, Volume 1: Orders and Generic Constructions of Units.* De Gruyter, Berlin, Germany, 2016.

[17] G. A. Jones. Realisation of groups as automorphism groups in permutational categories. *Ars Mathematica Contemporanea*, 21(1):P1.01, 2021.

[18] S. M. Lane. *Categories for the Working Mathematician.* Springer, New York, NY, USA, 2nd edition, 1998.

[19] E. Mendelsohn. Every group is the collineation group of some projective plane. *Journal of Geometry*, 2(2):97–106, 1972.

[20] E. Riehl. *Category Theory in Context.* Aurora Dover Modern Maths Originals. Dover Publications, Mineola, NY, USA, 2016.

[21] J. J. Rotman. *An Introduction to the Theory of Groups*, volume 148 of *Graduate Texts in Mathematics.* Springer, New York, NY, USA, 4th edition, 1995.

[22] G. Sabidussi. Graphs with given group and given graph-theoretical properties. *Canadian Journal of Mathematics*, 9:515–525, 1957.

[23] J.-P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, NY, USA, 1977.

[24] C. Teleman. Representation theory sheet 1. Lecture notes for Lent Term, Cambridge Tripos, 2005.

[25] G. Vercleyen and J. K. Slingerland. On low rank fusion rings. *Journal of Mathematical Physics*, 64(9):091703, 09 2023.