Forum of Mathematics, Sigma (2026), **xx**:xx 1–48
doi:10.1017/fmsX

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Categorification of characteristic structures

Peter A. Brooksbank[1], Heiko Dietrich[2], Joshua Maglione[3], E.A. O'Brien[4] and James B. Wilson[5]

[1]Bucknell University, USA; E-mail: pbrooksb@bucknell.edu.

[2]Monash University, Australia; E-mail: heiko.dietrich@monash.edu.

[3]University of Galway, Ireland; E-mail: joshua.maglione@universityofgalway.ie.

[4]University of Auckland, New Zealand; E-mail: e.obrien@auckland.ac.nz.

[5]Colorado State University, USA; E-mail: James.Wilson@ColoState.Edu.

Received: 10 Feb 2025; **Accepted:** 15 Dec 2025

Keywords: Categorification; Characteristic Structure; Isomorphism Problem

MSC Codes: *Primary* – 18N25, 08A35; *Secondary* – 20-08

Abstract

We develop a representation theory of categories as a means to explore characteristic structures in algebra. Characteristic structures play a critical role in isomorphism testing of groups and algebras, and their construction and description often rely on specific knowledge of the parent object and its automorphisms. In many cases, questions of reproducibility and comparison arise. Here we present a categorical framework that addresses these questions. We prove that every characteristic structure is the image of a functor equipped with a natural transformation. This shifts the local description in the parent object to a global one in the ambient category. Through constructions in representation theory, such as tensor products, we can combine characteristic structure across multiple categories. Our results are constructive and stated in the language of a constructive type theory which facilitates their implementation in proof checkers.

Contents

1. Introduction

The problem of deciding when two algebraic structures are isomorphic is fundamental to algebra and computer science. It encompasses issues of decidability and complexity, and it tests the limits of our theories and algorithms. An initial tactic in deciding isomorphism is to identify substructures that are

invariant under isomorphisms because doing so reduces the search space. We first discuss groups, where the literature is most developed (see, for example, [7, 9, 21, 35]), but our results apply to monoids, loops, rings, and non-associative algebras.

A subgroup H of a group G is *characteristic* if $\varphi(H) = H$ for every automorphism $\varphi : G \to G$; it is *fully invariant* if $\psi(H) \leqslant H$ for every homomorphism $\psi : G \to G$. We use the language of categories, following [28], and a type of natural transformation to describe our main results (details are given in Section 5.1).

Definition 1.1. Let A be a category, and let B be a subcategory with inclusion functor $\mathcal{I} : \mathsf{B} \to \mathsf{A}$. A *counital* is a natural transformation $\iota : C \Rightarrow \mathcal{I}$ for some functor $C : \mathsf{B} \to \mathsf{A}$. The class of all such counitals is denoted $\mathrm{Counital}(\mathsf{B}, \mathsf{A})$. For an object X of B, the X-component of ι is the morphism $\iota_X : C(X) \to \mathcal{I}(X)$ in A.

A special case of our results, for the category of groups, can be stated as follows.

Theorem 1. *For the category* Grp *of groups and subcategory* $\overleftrightarrow{\mathsf{Grp}}$ *of groups and their isomorphisms, the following equalities of sets hold:*

$$\begin{aligned} \{H \leqslant G \mid H \text{ characteristic in } G\} &= \left\{ \mathrm{Im}(\iota_G) \;\middle|\; \iota \in \mathrm{Counital}\left(\overleftrightarrow{\mathsf{Grp}}, \mathsf{Grp}\right) \right\}; \\ \{H \leqslant G \mid H \text{ fully invariant in } G\} &= \{\mathrm{Im}(\iota_G) \mid \iota \in \mathrm{Counital}(\mathsf{Grp}, \mathsf{Grp})\}. \end{aligned}$$

Theorem 1 contrasts a "recognizable" description of characteristic (fully invariant) subgroups with a "constructive" one. For a fixed group G, the sets on the left are of the form $\{H \mid P(G, H)\}$, where P is the appropriate logical predicate that allows us to recognize when a subgroup H belongs to the set; those on the right are of the form $\{f(\iota) \mid \iota \in \mathrm{Counital}(\ldots, \mathsf{Grp})\}$, where $f(\iota) = \mathrm{Im}(\iota_G)$ allows us to construct members of the subset by applying a function. Also, the descriptions on the left are "local" since they reference just a single parent group, whereas those on the right are "global" since they apply to the ambient categories.

The characterization of characteristic subgroups by natural transformations allows one to recast the lattice theory of characteristic subgroups into the globular compositions of natural transformations as explored in [4, 27]. We now explore other implications of Theorem 1.

1.1. Constraining isomorphism by characteristic subgroups

Characteristic subgroups constrain isomorphisms in the following sense:

Fact 1.2. *Let G be a group with characteristic subgroup $H \leqslant G$. If $\alpha, \beta : G \to \tilde{G}$ are isomorphisms, then $\alpha(H) = \beta(H)$.*

It is therefore useful for an isomorphism test to locate characteristic subgroups of a group G: every hypothetical isomorphism from G to $\tilde{G}$ must then assign such a subgroup H to a unique corresponding subgroup $\tilde{H}$ of $\tilde{G}$. This raises at least two issues. First, if the task is to construct isomorphisms, then we should assume that $\mathrm{Aut}(G)$ is not yet known. How then do we verify that H is characteristic? Is there an alternative definition of the characteristic property that does not directly reference $\mathrm{Aut}(G)$? A second issue is how to determine the possible $\tilde{H} \leqslant \tilde{G}$ when we know only that H is characteristic in G. For familiar characteristic subgroups such as the center $\zeta(G)$ this is possible because the definition is already global to all groups. Hence, a hypothetical isomorphism $\alpha : G \to \tilde{G}$ must satisfy $\alpha(\zeta(G)) = \zeta(\tilde{G})$, and typically $\zeta(G)$ and $\zeta(\tilde{G})$ can be constructed without explicit knowledge of $\mathrm{Aut}(G)$ or $\mathrm{Aut}(\tilde{G})$. However, the following family of examples, first explored by Rottlaender [29], exhibits groups whose characteristic subgroups have no known global definition, so it is difficult to utilize Fact 1.2.

Example 1.3. Let p be a prime and $m < p$ a positive integer. Let $q \equiv 1 \bmod p$ be a prime and denote by $\mathbb{F}_q$ the field with q elements. Let $\theta \in \mathrm{GL}_m(\mathbb{F}_q)$, with $\theta^p = 1$, be diagonalizable with m eigenvalues $a_1, \ldots, a_m$, each different from 1, satisfying the following property: if there exists $u \in \{1, \ldots, p-1\}$ with $a_i^u = a_j$ for all $i \neq j$, then $p \nmid (u^k - 1)$ for $k \in \{1, \ldots, m\}$. For $m = 2$, this requires $a_1 \neq a_2^{\pm 1}$.

The cyclic group C_p of order p acts on the vector space $V = \mathbb{F}_q^m$ via θ. The condition on θ means that each eigenspace in V is a characteristic subgroup of the semidirect product $G_\theta = C_p \ltimes_\theta V$ determined by θ, and exactly m of the $1 + q + q^2 + \cdots + q^{m-1}$ order q subgroups of G_θ are characteristic. Two such groups G_θ and G_τ may be isomorphic even if the eigenvalues of θ and τ are different. For example, this occurs when $\tau = \theta^j$ for some j coprime to p. Thus, the correspondence between characteristic subgroups of G_θ and G_τ is not *a priori* clear. □

One of the goals of this work is to reinterpret the definition of a characteristic subgroup in a way that is independent of automorphisms and which is unambiguously defined for all groups. We do this by formulating the characteristic condition on the entire category of groups, thereby providing a categorification of the property of being characteristic. Moreover, our formulation pairs well with—and indeed is motivated by—the necessities of computation (see Section 1.3). To address this, we employ methods from theorem-checking, specifically type-theoretic techniques [18, 26, 34]; these have recently become accessible through systems such as Agda [2], Coq [11], and Lean [23].

1.2. A local-to-global problem

Our approach is to transform the local characteristic property of subgroups into an equivalent global property of the category of all groups and their isomorphisms. Calculations now take place within the category instead of within individual groups, which opens up new ways to search for characteristic subgroups. Our approach also facilitates an *a priori* verification of the global characteristic property, rather than the usual *a posteriori* check that requires knowledge of automorphisms. The process is analogous to proving that $\zeta(G)$ is characteristic without employing specific properties of G. Our methods extend to *every characteristic subgroup*, even those discovered via bespoke calculations.

The traditional model of a category A involves both objects and morphisms. By sometimes focusing only on morphisms, we work with categories as an algebraic structure with a partial binary associative product on A—given by composition of its morphisms—and with identities $\mathbb{1}_\mathsf{A} = \{\mathrm{id}_X \mid X \text{ an object in } \mathsf{A}\}$. It is partial because not every pair of morphisms is composable, in which case the product is undefined. This perspective yields an algebraic framework for our computations.

The morphisms of a category can act on the morphisms of another category either on the left or the right. Although several interpretations of "category action" appear in the literature [5, §2], [25], [14, 1.271–274], there is no single established meaning. Our formulation uses *partial functions* that are purposefully undefined for some inputs; see Section 2.5 for a precise definition. Let A, B, and X be categories. A left A-*action* on X is a partial function, where $a \cdot x$ is defined for some morphisms a of A and x of X, that satisfies two conditions inspired by group actions. The first is that $(a\acute{a}) \cdot x = a \cdot (\acute{a} \cdot x)$, whenever defined, for all morphisms $a, \acute{a}$ of A and x of X. The second is that $\mathbb{1}_\mathsf{A} \cdot x = \{x\}$; to simplify notation we write $\mathbb{1}_\mathsf{A} \cdot x = x$. As in the theory of bimodules of rings, an (A, B)-*biaction* on X is a left A-action and a right B-action on X such that for every morphism a in A, b in B, and x in X,

$$a \cdot (x \cdot b) = (a \cdot x) \cdot b$$

whenever both sides of the equation are defined. For (A, B)-biactions on categories X and Y, an (A, B)-*morphism* is a partial function $\mathcal{M} : \mathsf{Y} \to \mathsf{X}$ such that

$$\mathcal{M}(a \cdot y \cdot b) = a \cdot \mathcal{M}(y) \cdot b$$

whenever $a \cdot y \cdot b$ is defined for morphisms a in A, b in B, and y in Y.

We write $\mathsf{A} \leqslant \mathsf{B}$ to indicate that A is a subcategory of B, and denote the identity functor of A by $\mathrm{id}_{\mathsf{A}} : \mathsf{A} \to \mathsf{A}$. A *counit* is a counital of the form $\eta : C \Rightarrow \mathrm{id}_{\mathsf{A}}$. The following specialization of one of our principal results to groups describes how characteristic subgroups relate to counits and morphisms of category biactions.

Theorem 2. *Let G be a group and $H \leqslant G$ with inclusion $\iota_G : H \hookrightarrow G$. There exist categories A and B, where $\overleftrightarrow{\mathsf{Grp}} \leqslant \mathsf{A} \leqslant \mathsf{Grp}$, such that the following are equivalent.*

(1) *H is characteristic in G.*

(2) *There is a functor $C : \mathsf{A} \to \mathsf{A}$ and a counit $\eta : C \Rightarrow \mathrm{id}_{\mathsf{A}}$ such that $H = \mathrm{Im}(\eta_G)$.*

(3) *There is an (A, B)-morphism $\mathcal{M} : \mathsf{B} \to \mathsf{A}$ such that $\iota_G = \mathcal{M}(\mathrm{id}_G \cdot \mathbb{1}_{\mathsf{B}})$.*

We emphasize that the category B in Theorem 2 need not be a subcategory of Grp; see Section 8 for an example. Moreover, our results apply to characteristic substructures of varieties of algebraic structures, which include monoids, loops, rings, and non-associative algebras. This generalization (Theorem 2-cat) and its dual version (Theorem 2-dual) are proved in Section 6. We now illustrate how natural transformations arise from characteristic substructures.

Example 1.4. The derived subgroup $\gamma_2(G)$ of a group G determines the inclusion homomorphism $\lambda_G : \gamma_2(G) \hookrightarrow G$ and a functor $\mathcal{D} : \mathsf{Grp} \to \mathsf{Grp}$ mapping groups to their derived subgroup and mapping homomorphisms to their restriction onto the derived subgroups. For every group homomorphism $\varphi : G \to H$, observe that $\lambda_H \mathcal{D}(\varphi) = \mathrm{id}_{\mathsf{Grp}}(\varphi)\lambda_G$, so $\lambda : \mathcal{D} \Rightarrow \mathrm{id}_{\mathsf{Grp}}$ is a natural transformation.

The center $\zeta(G)$ of G yields the inclusion homomorphism $\rho_G : \zeta(G) \hookrightarrow G$. To define a functor with object map $G \mapsto \zeta(G)$, we must restrict the type of homomorphisms between groups since homomorphisms need not map centers to centers. (Consider, for example, an embedding $\mathbb{Z}/2 \hookrightarrow \mathrm{Sym}(3)$.) Since every isomorphism maps center to center, we restrict to $\overleftrightarrow{\mathsf{Grp}}$, defining a functor $\mathcal{Z} : \overleftrightarrow{\mathsf{Grp}} \to \overleftrightarrow{\mathsf{Grp}}$ mapping $G \mapsto \zeta(G)$ and mapping each homomorphism to its restriction. If $\mathcal{I} : \overleftrightarrow{\mathsf{Grp}} \to \mathsf{Grp}$ is the inclusion functor, then $\rho : \mathcal{I}\mathcal{Z} \Rightarrow \mathcal{I}$ is a natural transformation. □

1.3. Applications to computation

Part of the motivation for our work comes from computational challenges that arise in contemporary isomorphism tests in algebra. One of these is to develop new ways to discover characteristic subgroups. Standard constructions—such as the commutator subgroup, the center, and the Fitting subgroup—can be applied to any group. However, these subgroups often contribute little to resolving isomorphism. Many ideas have been introduced to search for new structures; see, for example, [7, 9, 21]. Often these involve detailed computations with individual groups, and their application is *ad hoc*. Indeed, a primary motivation for this study is to systematize the disparate techniques currently used to search for characteristic subgroups.

Theorem 2 provides the framework for a systematic search for characteristic subgroups. An (A, B)-morphism generalizes the familiar and much studied category theory notion of adjoint functor pairs. We show in Section 4.6 that category actions offer a flexible way to implement the behavior of natural transformations in a computer algebra system. To exploit the full power of the categorical interpretation of characteristic subgroups, we work in a suitably general algebraic framework that allows a seamless transfer of information from one category to another. The familiar examples from Sections 7 and 8 demonstrate how to identify characteristic structure in a category and transfer it back to groups.

A second challenge concerns reproducibility and comparison of characteristic subgroups. Algorithms to decide isomorphism between groups G and H often, as a first step, generate lists of characteristic subgroups for G and H, respectively. To exploit these lists, any hypothetical isomorphism $G \to H$ must map the first list to the second (Fact 1.2). We observed in Example 1.3 that it is not always possible to determine a 'canonical ordering' of characteristic subgroups such that this is guaranteed. In practice,

some constructions employ randomization or make labelling choices that vary from one run to the next. These variations can limit the utility of characteristic subgroups in deciding isomorphism.

Our proposed solution is to develop algorithms that return the natural transformation (or a morphism of biactions) from Theorem 2 instead of the characteristic subgroup itself. This will allow us, in principle, to extend the reach of a specific characteristic subgroup of a given group to an entire category, in much the same way that the commutator subgroup and center behave. The natural transformation can then be applied to a group $\tilde{G}$ to produce a characteristic subgroup $\tilde{H}$ that corresponds to H in the sense of Fact 1.2: every isomorphism $G \to \tilde{G}$ necessarily maps H to $\tilde{H}$, so allowing a meaningful comparison of characteristic subgroups.

A third challenge is verifiability: in a computer algebra system, subgroups are often given by monomorphisms which are defined on a given generating set. The construction of such a monomorphism usually invokes computations that *prove* the claimed properties (such as homomorphism or characteristic image). We present our work in a framework that combines these computations, data, and proofs, by employing an intuitionistic Martin-Löf type theory; such a model also allows machine verification of proofs. In this setting, if a computer algebra system returns a counital ι, then this counital comes with a "type" that *certifies* that each morphism ι_G of ι yields a characteristic substructure.

1.4. Structure of this paper

In Section 2, we discuss the required background for our foundations (type theory). In Section 3, we first review varieties of algebraic structures and then show how to model categories as terms of the variety of *abstract categories*.

Section 4 studies category actions. In particular, we define *capsules* (category modules) and describe a computational model for natural transformations as category bimorphisms (Proposition 4.10). This also allows us to describe counitals (Theorem 4.11) and adjoint functor pairs (Theorem 4.13) in the language of bicapsules and bimorphisms.

In Section 5, we explain how characteristic structures can be described by counitals. The functors involved in this construction are defined on categories with one object, but Theorem 5.4—which we call the *Extension Theorem*—allows us to extend these functors to larger categories. This theorem is the essential ingredient for proving our main results. We also generalize Theorem 1 to varieties of algebras (Theorem 1-cat).

In Section 6, we generalize Theorem 2 to varieties of algebras (Theorem 2-cat). We show that characteristic substructures can be described as certain counits, and as bimorphism actions on capsules. We also prove the dual version of this result for characteristic quotients (Theorem 2-dual).

In Section 7, we use our framework to provide categorical descriptions of common characteristic subgroups, including verbal and marginal subgroups.

In Section 8, we describe a cross-category translation of counitals and explain, in categorical terms, how a counital for a category of groups can be constructed from a counital for a category of algebras.

In Section 9, we report on an implementation of some of the concepts introduced in this work.

Table 1 summarizes notation used throughout the paper.

2. Type theory and certifying characteristic structure

The emergence of randomized methods in computational algebra has elevated the significance of certification. Certificates are used to upgrade Monte Carlo algorithms to Las Vegas algorithms, where every output (other than failure) is correct [12, §3.2.1]. Usually this certification occurs *a posteriori*, which can present an intractable obstacle. Suppose an algorithm constructs a characteristic subgroup H

Symbol	Description
E	variety of algebraic structures
$\mathsf{A}, \mathsf{B}, \mathsf{C}, \mathsf{D}$	Abstract categories or categories that act
$\mathsf{X}, \mathsf{Y}, \mathsf{Z}$	Capsules
Δ, Σ	Bicapsules
id_X	Identity morphism of type X
$\mathbb{1}_{\mathsf{A}}$	Identity morphisms of A
$\mathcal{F}, \mathcal{G}$	Morphisms between categories
$\mathcal{I}, \mathcal{J}, \mathcal{K}, \mathcal{L}$	Inclusion functors
$\mathcal{M}, \mathcal{N}, \mathcal{R}, \mathcal{S}$	Capsule morphisms
A^X	Functions $X \to A$
A^n	Functions $\{1, \ldots, n\} \to A$
Ω	Signature
Alge_Ω	Type of Ω-algebras
$\mathrm{Alge}_{\Omega,\mathcal{L}}$	Type of Ω-algebras in the variety for the laws $\mathcal{L}$
$\bot$	The void type
$B^?$	The type $B \sqcup \{\bot\}$
$f(a) \succeq b$	If $f(a)$ is defined, then $f(a) = b$
$f\blacktriangleleft, \blacktriangleleft f$	Source and target of a morphism
$f\triangleleft, \triangleleft f$	Guards for a category action
$\overset{\leftrightarrow}{\mathsf{A}}, \overset{\twoheadrightarrow}{\mathsf{A}}, \overset{\hookrightarrow}{\mathsf{A}}$	The iso-, epi-, and mono-morphisms of A (resp.)

Table 1: A guide to notation

of a group G with inclusion $\iota\colon H \hookrightarrow G$. To certify that H is characteristic, we must verify that

$$(\forall \varphi \in \mathrm{Aut}(G))\ \ (\forall h \in H)\ \ (\exists k \in H)\ \ \varphi(\iota(h)) = \iota(k). \tag{2.1}$$

An obstacle to certification is that the algorithm may not know $\mathrm{Aut}(G)$ explicitly. The very construction of $\mathrm{Aut}(G)$ is often one of the key reasons to find characteristic subgroups in the first place. What is needed is *a priori* certification.

Of course, certain constructions yield subgroups of G which are guaranteed to be characteristic; these include $\zeta(G)$ and $\gamma_2(G)$. Their constructions, and the reasons they produce characteristic subgroups, apply to all groups. A careful examination of these reasons on the categorical level leads to the key insight of this paper: there is a uniform categorical description of the characteristic property. As we shall see, this insight ultimately leads to the possibility of *a priori* certification.

To put this into practice, we develop a constructive version of our main results using type theory language. Specifically, we use an intuitionistic Martin-Löf type theory (MLTT), a model of computation capable of expressing aspects of proofs that can be machine verified. An advantage of this approach is that certificate data can be verified by practical type-checkers. An MLTT employs the "propositions as types" paradigm (Curry–Howard Correspondence), where types correspond to propositions and terms are programs that correspond to proofs. The remainder of this section is a concise treatment of type theory from [18, Chapters 10–13], [34, Chapter 3].

2.1. Types

Informally, *types* annotate data by signalling which syntax rules apply to the data. We write $a : A$ and say "a is a *term* of type A" or "a inhabits A". For example, $a : \mathbb{N}$ signals that a can only be used as a natural number. A type A is *inhabited* if there exists at least one term $a : A$ and *uninhabited* if no term

of type A exists. The *void* type $\perp$ has no inhabitants by definition. Deciding whether a type is inhabited or not is computationally undecidable [18, pp. 66–67]. Therefore, in computational settings, types are permitted to be neither inhabited nor uninhabited. Type annotations enable us to use symbols according to their logical purpose; for example, $a : A$ is analogous to $a \in A$, but type theories do not have the axioms of set theory.

Types are introduced from two sources. Some are predefined by the *context*: they are given *a priori*, such as the type of natural numbers $\mathbb{N}$. Others are created using *type-builders*: these construct new types from existing ones. We use both $A \to B$ and B^A to denote the type of functions, and set $\mathrm{Dom}(A \to B) = A$ and $\mathrm{Codom}(A \to B) = B$. If n is a natural number, then an inhabitant of type A^n can be interpreted as an n-tuple $(a_1, \ldots, a_n)$ with each $a_i : A$, or alternatively as a function $\{1, \ldots, n\} \to A$. There is a unique function $\perp \to A$ (akin to the uniqueness of a function $\varnothing \to A$), so A^0 is a type with a single inhabitant—it is *not* void.

The notation $\prod_{i:I} A_i$ together with projection maps $\pi_i : (\prod_{i:I} A_i) \to A_i$ is used for Cartesian products, and $\bigsqcup_{i:I} A_i$ together with inclusion maps $\iota_i : A_i \to \bigsqcup_{i:I} A_i$ is used for disjoint unions. (The tradition in type theory is to use $\sum_{i:I} A_i$ instead of $\bigsqcup_{i:I} A_i$, but this conflicts with algebraic uses of Σ.)

2.2. Propositions as types

In set theory, propositions are part of the existing foundations. In type theory, propositions co-evolve with the theory as special types. A proposition P in logic is associated to a type $\hat{P}$: Type. (Only in this section do we distinguish propositions P in logic from propositions as types with the notation $\hat{P}$.) If the type $\hat{P}$ is inhabited by data $p : \hat{P}$, then the term p is regarded as a proof that P is true. For example, an implication $P \Rightarrow Q$ (here $\Rightarrow$ means "implies" with weakening and contraction laws) can be proved by means of a function $f : \hat{P} \to \hat{Q}$, where $\hat{P}$ and $\hat{Q}$ are the respective types associated with P and Q, because it suffices to assume P and derive a proof of Q. Likewise, if we assume that there is a term $p : \hat{P}$ and apply the function f, then it produces a term $f(p) : \hat{Q}$.

In classical logic, it is only the existence of a proof for a proposition that is relevant. Analogously, in type theory, $\hat{P}$: Type is a *mere proposition*, written $\hat{P}$: Prop, if it has at most one inhabitant.

Consider the function $\hat{P} : A \to$ Prop. Now $(\forall a \in A)(P(a))$ and $(\exists a \in A)(P(a))$ are expressed by terms of type $\prod_{a:A} \hat{P}_a$: Prop and $\| \bigsqcup_{a:A} \hat{P}_a \|$: Prop, respectively, where $\|A\|$ *truncates* a type to a single term if it has any terms [34, §3.7]. The negation of a proposition P is $P \Rightarrow$ False, which accords with functions of type $\hat{P} \to \perp$. For additional details, see [18, Chapters 12–13], [34, Chapter 3].

2.3. Equality

In Zermelo set theories, all data are sets and there is a single notion of equality afforded by the *Axiom of extensionality*: two sets are equal if, and only if, they have the same elements. In type theory, terms and types are separate entities, and this single axiom is replaced by several distinct notions of equality more representative of computational behavior. Each type theory is built on a rewriting system (such as a λ-calculus or combinatory logic). Employing the language of [18, §1D and §2D], we judge data as equal if their normal forms in this rewriting system coincide; and $s := t$ followed by some sentences M means that "within the given scope M, the variable s should be substituted by the data t".

Type theories include axioms that allow equality after taking normal forms to count as (*definitional*) *equality*–the type theory sees no difference between the data [18, p. 193]. For example, if we build the type $\mathbb{Z}/n$ which depends on a term $n : \mathbb{N}$, then some type systems judge that $\mathbb{Z}/(m+m)$ is equal to $\mathbb{Z}/2m$ because $m + m$ and $2m$ have the same normal form. But the function $\gcd(m, 2m)$ is more complicated and its normal form may differ from m. Hence, the type system does not judge $\mathbb{Z}/\gcd(m, 2m)$ as equal to $\mathbb{Z}/m$; neither does it assert they are not equal; instead it withholds judgment.

To construct an equality that mimics set theory, Per Martin-Löf developed a notion of propositional equality that imitates the *Leibniz Law* [13]:

$$(s = t) \iff [(\forall P(x))\ P(s) \iff P(t)]\,,$$

where $P(x)$ runs over all predicates of a single variable x. For every type A and terms $s, t : A$, we define an auxiliary type $s =_A t$, where terms are proofs that s equals t, with the rule that, given a function $f : A \to B$, there is a function

$$\mathrm{path}(f) : (s =_A t) \to (f(s) =_B f(t)). \tag{2.2}$$

For example, a proof $p : (\gcd(m, 2m) =_{\mathbb{N}} m)$ can be transported along a path to $q : (\mathbb{Z}/\gcd(m, 2m) =_{\mathbb{Z}/m} \mathbb{Z}/m)$ allowing programs to treat these types as equal. Thus, computational evidence enhances the reach of equality, see [18, §3.5], [34].

For readability we often omit the subscript A in $s =_A t$. By slight abuse of notation, writing "$s = t$" as a logical statement in text should be interpreted as "the type $s =_A t$ is inhabited".

2.4. Subtypes and inclusion functions

Sets are a special case of types: we write $S : \mathrm{Set}$ for a type S if the type $s =_S t$ is a mere proposition for all $s, t : S$. Let A be a type. If $P : A \to \mathrm{Prop}$, then

$$\{a : A \mid P(a)\} := \bigsqcup_{a:A} P(a),$$

is the *subtype* of A defined by P. We also write this as $B := \{a : A \mid P(a)\} \subset A$. Terms of type B have the form $\langle a, p\rangle$ for $a : A$ and $p : \mathrm{Prop}$, where p is a proof that $P(a)$ is inhabited. We sometimes use set theory notation to improve readability when describing a subtype. For more details, see [34, §3.5]. For a typed function $f : A \to B$, the image $\{f(a) \mid a : A\}$ is shorthand for $\{b : B \mid (\exists a : A)(f(a) = b)\}$.

Subtypes have an associated inclusion function $\alpha : B \to A$ where $\alpha(\langle a, p\rangle) := a$. A subtlety is that if $C \subset B$ with inclusion map $\beta : C \to B$, then the composition $\alpha\beta : C \to A$ is injective but does not show directly that $C \subset A$. A term of type $C := \bigsqcup_{b:B} Q(b)$, with $Q : B \to \mathrm{Prop}$, has the form $\langle\langle a, p\rangle, q\rangle$, which differs from terms of type B. A small modification addresses the fact that the relation $\subset$ is not strictly transitive. Define a subtype $C' := \bigsqcup_{a:A} R(a)$, where $R(a) := \bigsqcup_{p:P(a)} Q(a)$, and inclusion $\gamma : C' \to A$. Now construct a map $\sigma : C \to C'$ given by

$$\langle\langle a, p\rangle, q\rangle \mapsto \langle a, \langle p, q\rangle\rangle,$$

where $a : A$ and $\langle p, q\rangle : R(a)$. Thus, $\alpha\beta = \gamma\sigma$, and the composition $\alpha\beta$ is equivalent to γ. Hence, $\subset$ is transitive up to this equivalence.

2.5. Partial functions

In type theory, functions are ultimately programs so they may fail to halt. Since our concern lies with algebraic obstacles rather than decidability, we confine our model to algebras that have decidable operations, such as polynomial and integer operations, look-up tables, and strongly normalizing rewriting systems. Thus, all functions are total: given an input, they produce an output. However, it is helpful to identify inputs we regard as "undefined", or "leading to errors". For example, a division operator may allow 0 as an input and return an error token as output. We call such functions *partial functions* and regard them as "undefined" at such inputs.

To accommodate such partial operations, we extend types by adjoining the symbol $\perp$ (the void type) to represent "undefined". For a type A, we define

$$A^? := A \sqcup \{\perp\} \tag{2.3}$$

with inclusion $\iota_A : A \hookrightarrow A^?$. For $a : A^?$, we write $a : A$ in this setting as shorthand for "there exists $a' : A$ such that $a = \iota_A(a')$". This allows us to define an endofunctor Q on the category of types that maps a morphism $f : A \to B$ to $f^? : A^? \to B^?$, such that $f^?(a) = f(a)$ for $a : A$ and $f^?(\perp) = \perp$. The canonical projection $\mu : QQ \Rightarrow Q$, with components $\mu_A : (A^?)^? \to A?$, is a natural isomorphism. Hence, it suffices to work with single applications of Q, and $\perp$ will serve as the designated symbol for undefined elements throughout.

This discussion also motivates a notion of "directional equality" similar to that in [14, 1.12]. For $a, b : A^?$, define

$$(a \succcurlyeq b) := [(a : A) \to (a = b)] := [((\exists a' : A)(a = \iota_A(a'))) \to (\iota_A(a') = b)]. \tag{2.4}$$

By slight abuse of notation, for function terms $f, g : A^? \to B^?$ we denote function extensionality also by $f = g$, that is, we define

$$(f = g) := \big[(\forall a : A^?)\ (f(a) = g(a))\big].$$

2.6. Certifying that the trivial group is characteristic

As an illustration, we present a type verifying the characteristic property of the trivial subgroup. Let G : Group be a group with identity $1 : G$. Let $H := \{x : G \mid x = 1\}$ be the subtype of G representing the trivial subgroup. Recall that terms of H have the form $\langle x, p\rangle$, where $x : G$ and p is a term of type $x = 1$, and there is a map $\iota : H \to G$, $\langle x, p\rangle \mapsto x$. If $h, k : H$, then $\iota(h) = \iota(k) = 1$, and, by (2.2), for every $\varphi : \mathrm{Aut}(G)$ there is an invertible function of type

$$\varphi(1) =_G 1 \iff \varphi(\iota(h)) =_G \iota(k). \tag{2.5}$$

The latter function depends on h and k, but we suppress this dependency to simplify the exposition. Let $\mathrm{idLaw}(\varphi) : \varphi(1) =_G 1$ be a proof that $\varphi : \mathrm{Aut}(G)$ fixes $1 : G$. Using (2.5), we define the term

$$\mathrm{idMap}(\varphi) : \prod_{h:H} \left\| \bigsqcup_{k:H} \varphi(\iota(h)) =_G \iota(k) \right\|$$

that takes as input $h : H$ and produces $\langle 1, \mathrm{idLaw}(\varphi)\rangle : \| \bigsqcup_{k:H} \varphi(\iota(h)) =_G \iota(k) \|$. Therefore we obtain the term

$$\mathrm{idMap} : \prod_{\varphi:\mathrm{Aut}(G)} \prod_{h:H} \left\| \bigsqcup_{k:H} \varphi(\iota(h)) =_G \iota(k) \right\|,$$

which certifies that H is characteristic in G; compare to (2.1). Recall that in MLTT, types correspond to propositions, and terms are programs that correspond to proofs. Thus, the term idMap is not an exhaustive tuple listing $\mathrm{Aut}(G)$, but a program (function) that takes as input $\varphi : \mathrm{Aut}(G)$ and $h : H$, and produces $k : H$ and $p : \varphi(\iota(h)) =_G \iota(k)$.

3. Algebraic structures and varieties

To interpret characteristic structure as computable categorical information, we treat categories as algebraic structures. (Computational categories should not be confused with categorical semantics of computation.) For our purpose, it suffices to use operations that may only be partially defined, so categories are important examples, as are monoids, groups, groupoids, rings, and non-associative algebras. We give an abridged account and refer to [10, §II.2], [1, Chapter 3] for details.

3.1. Intentional and extensional formulations of algebra

It is natural to ask if algebraic structures such as groups and rings, that are introduced in standard texts such as [19] using *extensional* set theory, have logically consistent *intentional* formulations in foundations such as MLTT. While it is not within our purview to consider alternative foundations of algebra, we briefly compare type-theoretic formulations of groups with their long-standing and rigorous treatment in *computational* algebra.

Although systems such as GAP [15], Macauley [16], Magma [8], and SageMath [31] are not designed to use types robustly, they nevertheless facilitate a treatment of groups that is more intentional than extensional. In these systems, groups can be represented in many different ways, but for practical reasons *they are generally not treated as sets of elements*. For instance, a group G may be specified by a generating set Y of permutations. Algorithms such as the *product replacement* [12, §3.2.2] can then be used to select "random" elements of G as words in Y. However, basic questions such as membership—*does a permutation belong to G?*—often require clever algorithms to answer [12, Chapter 4].

Even the question of whether two elements in a group are equal is often not immediate. (There are models, such as finitely-presented groups, where this question is not decidable.) In standard models for computation with groups, effective equality testing is usually available, but it is not always done by simply asking if two pieces of data are identical. For example, do elements a and b of $G = \langle Y \rangle$ coincide in $G/\zeta(G)$? Equivalently, is $ab^{-1} \in \zeta(G)$? Even if we do not know generators for $\zeta(G)$, we can answer the latter question efficiently by deciding whether ab^{-1} commutes with every element of Y. In this sense, asking whether $a = b$ in computational algebra (where a program settles the question) is closer to writing $a = b$ in type theory (where evidence is provided by a proof) than it is to the (trivial) question in set theory (cf. Section 2.3).

3.2. Operators, grammars, and signatures

Informally, a grammar is a description of rules for formulas.

Definition 3.1. An *operator* is a symbol with a grammar, which we describe using the Backus–Naur Form (BNF) [26, p. 24]. The *valence* of an operator ω, written $|\omega|$, is the number of parameters in its grammar. A set Ω of operators is a *signature*.

Example 3.2. A signature for additive formulas specifies three operators:

```
<Add> ::= (<Add> + <Add>) | 0 | (-<Add>)
```

The bivalent addition (+) depends on terms to the left and right; zero (0) depends on nothing; and univalent negation (−) is followed by a term. □

It is easy to reject $+ - + 2\,3\,7$ since it is not meaningful. However, we might write $2 + 3 - 7$ intending $(2 + 3) + (-7)$; the BNF grammar `<Add>` accepts only the latter.

The purpose of the signature is to formulate important algebraic concepts such as homomorphisms. To declare that a function $f : A \to B$ is a homomorphism between additive groups, we use the signature

of Example 3.2 as follows:

$$f((x+y)) = (f(x) + f(y)), \qquad f(0) = 0, \qquad f((-x)) = (-f(x)).$$

3.3. Algebraic structures

An algebra is a single type with a signature [10, §II.2].

Definition 3.3. An *algebraic structure* with signature Ω is a type A and a function $\omega \mapsto \omega_A$, where $\omega : \Omega$ and $\omega_A : A^{|\omega|} \to A$. A *homomorphism* between algebraic structures A and B, each having signature Ω, is a function $f : A \to B$ such that, for every $\omega : \Omega$ and $a_1, \ldots, a_{|\omega|} : A$,

$$f(\omega_A(a_1, \ldots, a_{|\omega|})) = \omega_B(f(a_1), \ldots, f(a_{|\omega|})).$$

As in Section 2.2, we extend these propositions to types as follows:

$$\begin{aligned} \mathrm{Alge}_\Omega &:= \bigsqcup_{A:\mathrm{Type}} \prod_{\omega:\Omega} (A^{|\omega|} \to A) \\ \mathrm{Hom}_\Omega(A,B) &:= \bigsqcup_{f:A\to B} \prod_{\omega:\Omega} \prod_{a:A^{|\omega|}} f(\omega_A(a_1,\ldots,a_{|\omega|})) =_B \omega_B(f(a_1),\ldots,f(a_{|\omega|})). \end{aligned}$$

Terms of type Alge_Ω are Ω-*algebras*.

For example, consider the additive group signature from Example 3.2. The underlying structure of an additive group can be described by a type (set) A together with assignments of the operators in `Add` such as `(<Add> + <Add>)` to $+_A : A \times A \to A$. The nullary operator `0` is then identified with a term $0 : A$.

3.4. Free algebras and formulas

We now extend signatures to include variables that allow us to work with formulas.

Definition 3.4. Let Ω be a signature and let X be a type whose terms are *variables*. The *free* Ω-algebra in variables X, denoted by $\Omega\langle X\rangle$, is the type of every formula in X constructed using the operators in Ω.

Example 3.5. To describe formulas in variables x, y and z, we extend the additive signature $\Omega = \mathtt{Add}$ of Example 3.2 as follows:

```
<Add<X>> ::= (<Add<X>> + <Add<X>> ) | 0 | (-<Add<X>> ) | x | y | z.
```

Here, $x+y$ and $(-x)+(0+z)$ have type $\mathtt{Add}\langle X\rangle$, but $x-$ and $x+7$ do not. The operations on the formulas $\Phi_1(X), \Phi_2(X) : \mathtt{Add}\langle X\rangle$ are:

$$\begin{aligned} \Phi_1(X) +_{\mathtt{Add}\langle X\rangle} \Phi_2(X) &:= (\Phi_1(X) + \Phi_2(X)) \\ 0_{\mathtt{Add}\langle X\rangle} &:= 0 \\ -_{\mathtt{Add}\langle X\rangle}\Phi_1(X) &:= (-\Phi_1(X)). \end{aligned}$$

Thus, $\mathtt{Add}\langle X\rangle$ is the free additive algebra, but it lacks laws such as $x + y = y + x$ and $x + (-x) = 0$. We explain how to impose these laws in Section 3.5. □

Fact 3.6. *Let A be an Ω-algebra and $a : A^X$, where X is a type whose terms are variables. There is a unique homomorphism* $\mathrm{eval}_a : \Omega\langle X\rangle \to A$ *that satisfies* $\mathrm{eval}_a(x) = a_x$.

Consequently, we write $\Phi(a) := \mathrm{eval}_a(\Phi)$ for formulas $\Phi : \Omega\langle X\rangle$ and $a : A^X$.

Remark 3.7. The construction in Fact 3.6 is categorical in nature, and we use it in Section 7 to construct characteristic subgroups. The category of Ω-algebras has objects of type Alge_Ω together with homomorphisms. The pair of functors (given only by their object maps)

$$X \mapsto \Omega\langle X\rangle \quad \text{and} \quad \langle A : \mathrm{Type},\ (\omega : \Omega) \mapsto (\omega_A : A^{|\omega|} \to A)\rangle \mapsto A$$

forms an *adjoint functor pair* between the categories of types and Ω-algebras; see Section 4.5 for related discussion.

3.5. Laws and varieties

Let Ω be a signature. We now describe the variety of Ω-algebras whose operators satisfy a list of (equational) laws such as the axioms of a group. Let X be a type for variables. A *law* is a term of type $\Omega\langle X\rangle^2$. We index laws by a type L, so they are terms $\mathcal{L} : L \to \Omega\langle X\rangle^2$ and are written $\ell \mapsto (\Lambda_{1,\ell}, \Lambda_{2,\ell})$.

An Ω-algebra A is in the *variety* for the laws $\mathcal{L} : L \to \Omega\langle X\rangle^2$ if

$$(\forall a : A^X)\ (\forall \ell : L)\ \Lambda_{1,\ell}(a) = \Lambda_{2,\ell}(a).$$

We write $\mathrm{Alge}_{\Omega,\mathcal{L}}$ for the type of all Ω-algebras in the variety for the laws $\mathcal{L}$; this is a subtype of Alge_Ω. The category of Ω-algebras in the variety for $\mathcal{L}$ has object type $\mathrm{Alge}_{\Omega,\mathcal{L}}$ and morphism type

$$\mathrm{Hom}_{\Omega,\mathcal{L}} := \bigsqcup_{A:\mathrm{Alge}_{\Omega,\mathcal{L}}} \bigsqcup_{B:\mathrm{Alge}_{\Omega,\mathcal{L}}} \mathrm{Hom}_\Omega(A, B),$$

with $\mathrm{Hom}_\Omega(A, B)$ as in Definition 3.3.

Example 3.8. The signature Ω for groups is the following:

$$\texttt{<G> ::= (<G><G>) | 1 | (<G>)}^{-1}.$$

The variety of groups uses three laws, indexed by $L := \{\texttt{asc}, \texttt{id}, \texttt{inv}\}$ with variables $X := \{x, y, z\}$, where for example

$$\Lambda_{1,\texttt{asc}} := x(yz) \quad \text{and} \quad \Lambda_{2,\texttt{asc}} := (xy)z.$$

Thus, $\Lambda_{1,\texttt{asc}}(g, h, k) = g(hk)$ and $\Lambda_{2,\texttt{asc}}(g, h, k) = (gh)k$, and associativity is imposed on the Ω-algebra G by requiring a term ("proof") of type

$$\prod_{g:G} \prod_{h:G} \prod_{k:G} g(hk) =_G (gh)k.$$

Encoding $1x = x$ and $x^{-1}x = 1$ as additional laws gives a complete description of the variety of groups. Laws need not be algebraically independent: for example, $x1 = x$ and $xx^{-1} = 1$ are often also encoded. □

For clarity, henceforth we write laws as propositions. For example, we write $g(hk) = (gh)k$ rather than terms of a mere proposition type.

3.6. Categories as algebraic structures

We cannot always compose a pair of morphisms in a category: composition may be a partial function. Hence, the morphisms need not form an algebraic structure under composition. We address this limitation by identifying precisely when the operators yield partial functions.

Example 3.9. The type of each function is given as

$$\mathrm{Fun} := \bigsqcup_{A:\mathrm{Type}} \bigsqcup_{B:\mathrm{Type}} (A \to B).$$

Technically, to quantify over all types, we shift to a larger universe Type_1; see Remark 3.17. For $f : A \to B$ and $g : \mathrm{Fun}$, define

$$f\blacktriangleleft := \mathrm{id}_A, \qquad \blacktriangleleft f := \mathrm{id}_B, \qquad fg := \begin{cases} f \circ g & f\blacktriangleleft = \blacktriangleleft g, \\ \bot & \text{otherwise.} \end{cases} \tag{3.1}$$

where $f \circ g$ is the usual composition of functions. The condition $f\blacktriangleleft = \blacktriangleleft g$ guards against composing non-composable functions (one can think of $f\blacktriangleleft = \blacktriangleleft g$ as saying "what enters f must match what exits g"). Note that $\blacktriangleleft(f\blacktriangleleft) = \blacktriangleleft \mathrm{id}_A = \mathrm{id}_A = f\blacktriangleleft$, and similarly $(\blacktriangleleft f)\blacktriangleleft = \blacktriangleleft f$. □

The definitions in (3.1) motivate an algebraic structure on $\mathrm{Fun}^?$. We define the *composition signature*:

```
<Comp> ::= (<Comp><Comp>) | (◀<Comp>) | (<Comp>◀) | ⊥
```
(3.2)

Definition 3.10. Let Ω be the composition signature of (3.2). An *abstract category* A is an Ω-algebra on a type C satisfying the law

$$f(gh) = (fg)h$$

in variables f, g, h, together with the following *source–target* laws and $\bot$-*sink* laws:

$$\begin{array}{lll} \blacktriangleleft(f\blacktriangleleft) = f\blacktriangleleft & (\blacktriangleleft f)f = f & \blacktriangleleft(fg) = \blacktriangleleft(f(\blacktriangleleft g)) \\ (\blacktriangleleft f)\blacktriangleleft = \blacktriangleleft f & f(f\blacktriangleleft) = f & (fg)\blacktriangleleft = ((f\blacktriangleleft)g)\blacktriangleleft \end{array}$$

$$\bot\blacktriangleleft = \bot \qquad \blacktriangleleft\bot = \bot \qquad f\bot = \bot \qquad \bot f = \bot.$$

We refer to the operators $(-)\blacktriangleleft$ and $\blacktriangleleft(-)$ in Definition 3.10 as *guards*. Note that $\blacktriangleleft f = \bot$ or $f\blacktriangleleft = \bot$ if, and only if, $f = \bot$; this follows from the laws $(\blacktriangleleft f)f = f$ and $f(f\blacktriangleleft) = f$.

Conventional categories can be treated as abstract categories. First, the morphisms of the category can be packaged as a disjoint union into a common type A, which possibly requires an enlarged universe. Then we use $A^?$ as the carrier type for the abstract category A, where the nullary operator $\bot : \Omega$ is identified with the term $\bot$ in $A^?$; see (2.3). We write $a : \mathsf{A}$ to indicate that a is a term of the carrier type $A^?$. Henceforth, we assume that all abstract categories have carrier types of the form $A^?$.

A useful subtype of an abstract category A is the type of *identities*:

$$\mathbb{1}_{\mathsf{A}} := \{a\blacktriangleleft \mid a : \mathsf{A},\ a \neq \bot\}.$$

Since $\blacktriangleleft(a\blacktriangleleft) = a\blacktriangleleft$ and $(\blacktriangleleft a)\blacktriangleleft = \blacktriangleleft a$, we also have $\mathbb{1}_{\mathsf{A}} = \{\blacktriangleleft a \mid a : \mathsf{A},\ a \neq \bot\}$.

Lemma 3.11. *The following hold in every abstract category.*

(a) *The guards are idempotents, namely*

$$((-)\blacktriangleleft)\blacktriangleleft = (-)\blacktriangleleft, \qquad \blacktriangleleft(\blacktriangleleft(-)) = \blacktriangleleft(-).$$

(b) *Terms f and g satisfy*

$$\blacktriangleleft(fg) \succeq \blacktriangleleft f, \qquad (fg)\blacktriangleleft \succeq g\blacktriangleleft.$$

Proof. For a term f in an abstract category,

$$\blacktriangleleft(\blacktriangleleft f) = \blacktriangleleft((\blacktriangleleft f)\blacktriangleleft) = (\blacktriangleleft f)\blacktriangleleft = \blacktriangleleft f.$$

A similar argument shows $(f\blacktriangleleft)\blacktriangleleft = f\blacktriangleleft$, so (a) holds. For (b), it remains to consider terms f, g such that $\blacktriangleleft(fg)$ is not $\bot$. This means that fg is not $\bot$, and hence $f\blacktriangleleft = \blacktriangleleft g$ with both $f\blacktriangleleft$ and $\blacktriangleleft g$ not $\bot$. Now

$$\blacktriangleleft(fg) = \blacktriangleleft(f(\blacktriangleleft g)) = \blacktriangleleft(f(f\blacktriangleleft)) = \blacktriangleleft f,$$

as claimed. The other formula follows similarly. □

Let C be a category with object type C_0. Form the type of all morphisms of C:

$$\mathsf{C}_1 := \bigsqcup_{U:\mathsf{C}_0} \bigsqcup_{V:\mathsf{C}_0} \mathsf{C}_1(U, V). \tag{3.3}$$

For objects $U, V : \mathsf{C}_0$, there is an inclusion map (see Section 2.1)

$$\iota_{UV} : \mathsf{C}_1(U, V) \hookrightarrow \mathsf{C}_1.$$

Thus, for each $\varphi : \mathsf{C}_1$, there exist unique $U, V : \mathsf{C}_0$ and $f : \mathsf{C}_1(U, V)$ such that $\varphi = \iota_{UV}(f)$.

Proposition 3.12. *Let* C *be a category. The type* $\mathsf{C}_1^?$ *from* (3.3) *of all morphisms of* C *with the composition signature from* (3.2) *forms an abstract category.*

Proof. Let $f, g : \mathsf{C}_1^?$. If $f = \bot$ or $g = \bot$, then all the equations in Definition 3.10 become $\bot = \bot$. It remains to consider the case that $f, g, h : \mathsf{C}_1$. If $f : U \to V$ in C, then $\blacktriangleleft(f\blacktriangleleft) = \mathrm{id}_{\mathrm{Codom}\,\mathrm{id}_U} = \mathrm{id}_U = f\blacktriangleleft$. Similarly, $(\blacktriangleleft f)\blacktriangleleft = \blacktriangleleft f$, and $\blacktriangleleft(f\blacktriangleleft) = f\blacktriangleleft$ and $(\blacktriangleleft f)\blacktriangleleft = \blacktriangleleft f$.

Observe that $(\blacktriangleleft f)f$ is defined and equals $\mathrm{id}_V\, f = f$; also $f(f\blacktriangleleft)$ is defined and equals $f\,\mathrm{id}_U = f$. For $g : \mathsf{C}_1(U', V')$, the expression $\blacktriangleleft(fg)$ is defined whenever $f\blacktriangleleft = \blacktriangleleft g$, and $f(\blacktriangleleft g)$ is defined whenever $f\blacktriangleleft = \blacktriangleleft(\blacktriangleleft g)$. Since $\blacktriangleleft(-)$ is idempotent by Lemma 3.11(a), both $\blacktriangleleft(fg)$ and $f(\blacktriangleleft g)$ are defined when $f\blacktriangleleft = \blacktriangleleft g$. Thus, $f\blacktriangleleft = \blacktriangleleft g$ implies

$$\blacktriangleleft(fg) = \mathrm{id}_V = \blacktriangleleft(f(f\blacktriangleleft)) = \blacktriangleleft(f(\blacktriangleleft g)),$$

so $\blacktriangleleft(fg) = \blacktriangleleft(f(\blacktriangleleft g))$. Similar arguments hold for $(fg)\blacktriangleleft = ((f\blacktriangleleft)g)\blacktriangleleft$ and for $f(gh) = (fg)h$. □

Example 3.13. Let A be an abstract category with $\mathbb{1}_\mathsf{A} := \{e_1, \ldots, e_6\}$ and additional morphisms $a_{12}, a_{23}, a_{13}, \acute{a}_{13}, b_{45}, b_{54}$, where $x_{ij}\blacktriangleleft = e_j$ and $\blacktriangleleft x_{ij} = e_i$. Using the composition signature from (3.2), A is an algebraic structure with multiplication defined in Table 2, where each instance of $\bot$ is omitted. It is not easy to discern structure from this table, so two additional visualizations of A are given in Figure 1, again with $\bot$ omitted. The first is the Cayley graph of the multiplication with undefined products omitted. The second is the Peirce decomposition, which we now discuss. □

3.7. Peirce decomposition of abstract categories

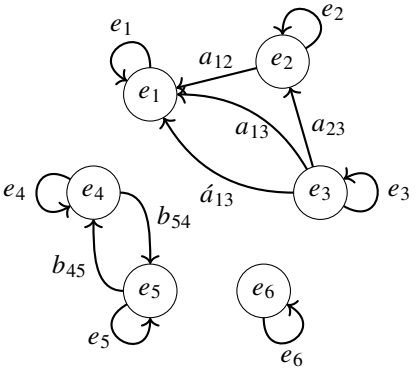
Treating categories as algebraic structures allows us to frame aspects of category theory in algebraic terms. Our goal is an elementary representation theory of categories. In particular, we seek matrix-like structures—known as Peirce decompositions in ring theory—for abstract categories.

One can recover from an abstract category A notions of objects and morphisms by considering the identities $\mathbb{1}_\mathsf{A}$. Using the laws in Definition 3.10, if $e : \mathbb{1}_\mathsf{A}$, then $e = e\blacktriangleleft$ and so $ee = e(e\blacktriangleleft) = e$; more

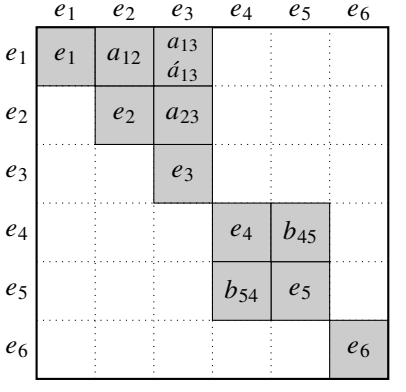
x	e_1	e_2	e_3	e_4	e_5	e_6	a_{12}	a_{23}	a_{13}	$\acute{a}_{13}$	b_{45}	b_{54}
$x\blacktriangleleft$	e_1	e_2	e_3	e_4	e_5	e_6	e_2	e_3	e_3	e_3	e_5	e_4
$\blacktriangleleft x$	e_1	e_2	e_3	e_4	e_5	e_6	e_1	e_2	e_1	e_1	e_4	e_5

$\cdot$	e_1	e_2	e_3	e_4	e_5	e_6	a_{12}	a_{23}	a_{13}	$\acute{a}_{13}$	b_{45}	b_{54}
e_1	e_1						a_{12}		a_{13}	$\acute{a}_{13}$		
e_2		e_2						a_{23}				
e_3			e_3									
e_4				e_4							b_{45}	
e_5					e_5							b_{54}
e_6						e_6						
a_{12}		a_{12}						a_{13}				
a_{23}			a_{23}									
a_{13}			a_{13}									
$\acute{a}_{13}$			$\acute{a}_{13}$									
b_{45}					b_{45}							e_4
b_{54}				b_{54}							e_5	

Table 2: The multiplication table for A



(a) Cayley graph



(b) Peirce decomposition

Figure 1: Visualizing the abstract category A in Example 3.13

generally,

$$(\forall e : \mathbb{1}_{\mathsf{A}})\ \ (\forall f : \mathbb{1}_{\mathsf{A}})\quad ef = \begin{cases} e & \text{if } f = e, \\ \bot & \text{otherwise.} \end{cases}$$

In algebraic terms, the subtype $\mathbb{1}_{\mathsf{A}}$ is a type of pairwise orthogonal idempotents. For subtypes X and Y of A, define

$$XY := \{xy \mid x : X, y : Y,\ x\blacktriangleleft = \blacktriangleleft y\}.$$

Fact 3.14. *If $a : \mathsf{A}$, then $\mathbb{1}_{\mathsf{A}}\{a\} = \{a\} = \{a\}\mathbb{1}_{\mathsf{A}}$; we write simply $\mathbb{1}_{\mathsf{A}}a = a = a\mathbb{1}_{\mathsf{A}}$.*

Given $e, f : \mathbb{1}_{\mathsf{A}}$, we define three subtypes:

$$\begin{aligned} &\text{(left slice)} && e\mathsf{A} := \{a : \mathsf{A} \mid e = {\blacktriangleleft}a\}; \\ &\text{(right slice)} && \mathsf{A}f := \{a : \mathsf{A} \mid a{\blacktriangleleft} = f\}; \\ &\text{(hom-set)} && e\mathsf{A}f := \{a : \mathsf{A} \mid e = {\blacktriangleleft}a,\ a{\blacktriangleleft} = f\}. \end{aligned}$$

These subtypes appear in Figure 2 in the left, middle, and right images, respectively. If $e{\blacktriangleleft} = {\blacktriangleleft}a$ for $a : \mathsf{A}$, then $ea = (e{\blacktriangleleft})a = ({\blacktriangleleft}a)a = a$.

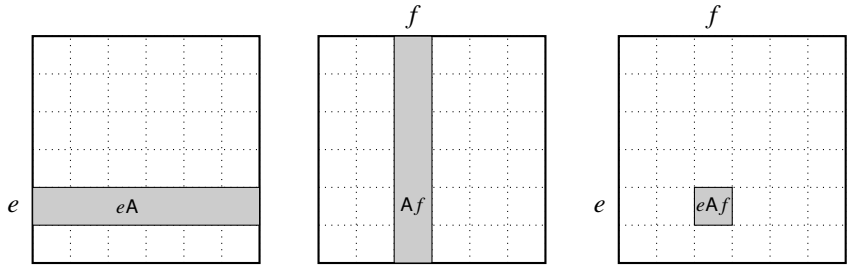


Figure 2: Visualizing the Peirce decomposition of A

If $a : \mathsf{A}$, then $a : \mathsf{A}(a{\blacktriangleleft})$, from which we deduce the following.

Proposition 3.15. *If* A *is an abstract category, then* $a \mapsto ({\blacktriangleleft}a)a$, $a \mapsto a(a{\blacktriangleleft})$, *and* $a \mapsto ({\blacktriangleleft}a)a(a{\blacktriangleleft})$ *induce invertible functions* (*denoted by "*$\leftrightarrow$*"*) *of the following types:*

$$\mathsf{A} \longleftrightarrow \bigsqcup_{e:\mathbb{1}_{\mathsf{A}}} e\mathsf{A}, \qquad \mathsf{A} \longleftrightarrow \bigsqcup_{f:\mathbb{1}_{\mathsf{A}}} \mathsf{A}f \qquad \mathsf{A} \longleftrightarrow \bigsqcup_{e:\mathbb{1}_{\mathsf{A}}} \bigsqcup_{f:\mathbb{1}_{\mathsf{A}}} e\mathsf{A}f.$$

Proposition 3.15, which we use to prove Theorem 5.4, allows us to draw upon intuition from matrix algebras. The morphisms of a category appear in its multiplication table, as in Table 2. Products of morphisms and slices are defined, as with matrix products, only when the inner indices agree. In this model, $\mathbb{1}_{\mathsf{A}}$ can be visualized as the identity matrix, where the entries on the diagonal are the individual identities $e : \mathbb{1}_{\mathsf{A}}$. In Figure 1b, that product is represented in a matrix-like form respecting the conditions of the Peirce decomposition.

Remark 3.16. While types for categories and abstract categories differ, every theorem stated in one setting translates to a corresponding theorem in the other. More precisely, the translation is a model-theoretic *definable interpretation* [24, §1.4]: there is a prescribed formula that translates every theorem and its proof between the two theories. Example 3.13 shows how the model of categories with both objects and morphisms may be interpreted as definable types in the theory of categories with only morphisms (abstract categories). Conversely, if A is an abstract category, then we obtain a category C with object type $\mathsf{C}_0 := \mathbb{1}_{\mathsf{A}}$ as follows. For objects $e, f : \mathsf{C}_0$, we define

$$\mathsf{C}_1(e, f) := f\mathsf{A}e,$$

where the identity morphisms of C are $e : \mathsf{C}_1(e, e)$. To compose morphisms $fae : \mathsf{C}_1(e, f)$ with $gbf : \mathsf{C}_1(f, g)$ for objects $e, f, g : \mathsf{C}_0$, we define

$$(gbf)(fae) := gbae : \mathsf{C}_1(e, g).$$

Hence, we no longer distinguish between categories and abstract categories.

3.8. Varieties as categories

Proposition 3.12 shows that a category is an algebraic structure with the composition signature. Conversely, for every signature Ω, the type $\mathrm{Alge}_{\Omega,\mathcal{L}}$ of Ω-algebras in the variety for the laws $\mathcal{L}$ forms a category with morphism type $\mathrm{Hom}_{\Omega,\mathcal{L}}$ (Section 3.5). Indeed, as in Proposition 3.12, $\mathrm{Alge}_{\Omega,\mathcal{L}}$ is an abstract category on $(\mathrm{Hom}_{\Omega,\mathcal{L}})^?$, and is therefore an algebraic structure with the composition signature.

Freyd originally explored the concept of *essentially algebraic structures* using partial functions, but did not include $\perp$ as an operator (see [14, §1.2]). This required dealing with implications such as "if $f\blacktriangleleft = \blacktriangleleft g$ then $(fg)\blacktriangleleft = g\blacktriangleleft$", which in turn entails working in a *quasi-variety*. But a quasi-variety is not closed under homomorphic images, so no analogue of Noether's Isomorphism Theorem (see Theorem 3.18) exists. An earlier version of this paper used this approach, but implementing our methods revealed the simpler approach of transforming categories into varieties (see Section 9).

We reserve E to denote a variety treated as category.

Remark 3.17. Regarding categories as algebras could lead to a paradox of Russell type. The paradox is avoided either by limiting Π-types to forbid some quantifications [33] or by creating an increasing tower of universe types and pushing the larger categories into the next universe [34, §9.9]. Both resolutions allow us to define categories and algebras computationally.

Under the correspondence of Remark 3.16, morphisms between abstract categories yield functors between categories, but the converse need not follow. A functor $\mathcal{F} : \mathsf{C} \to \mathsf{D}$ between categories retains the homomorphism properties of most of the operators: $\mathcal{F}(c\blacktriangleleft) = \mathcal{F}(c)\blacktriangleleft$, $\mathcal{F}(\blacktriangleleft c) = \blacktriangleleft\mathcal{F}(c)$, and $\mathcal{F}(\perp) = \perp$. But it relaxes composition to a directional equality:

$$\mathcal{F}(cc') \succcurlyeq \mathcal{F}(c)\mathcal{F}(c').$$

This translation serves two of our goals. The first is an elementary representation theory for categories: by regarding categories as "monoids with partial operators", we mimic monoid actions. The second is to treat a category as a single data type with operations defined on it. This is considerably easier to implement as a computer program. Both GAP and Magma are designed for such algebras. While there are advantages to the usual description of categories, the translation to abstract categories is essential for our approach to computing with and within categories.

We conclude this section with Noether's Isomorphism Theorem, see [10, Theorem II.3.7]; it guarantees that images and coimages exist in a variety.

Theorem 3.18 (Noether's Isomorphism Theorem)**.** *Let $\varphi : E_1 \to E_2$ be a morphism of Ω-algebras. There exists an Ω-algebra* $\mathrm{Coim}(\varphi)$ *and epimorphism* $\mathrm{coim}(\varphi) : E_1 \twoheadrightarrow \mathrm{Coim}(\varphi)$*, an Ω-algebra* $\mathrm{Im}(\varphi)$ *and monomorphism* $\mathrm{im}(\varphi) : \mathrm{Im}(\varphi) \hookrightarrow E_2$*, and an isomorphism $\psi : \mathrm{Coim}(\varphi) \to \mathrm{Im}(\varphi)$ such that the following diagram commutes:*

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \varphi\ } & E_2 \\ {\scriptstyle \mathrm{coim}(\varphi)}\downarrow & & \uparrow{\scriptstyle \mathrm{im}(\varphi)} \\ \mathrm{Coim}(\varphi) & \xrightarrow{\ \psi\ } & \mathrm{Im}(\varphi) \end{array}$$

The morphism $\mathrm{im}(\varphi)$ from Theorem 3.18 is the *image* of φ, and the morphism $\mathrm{coim}(\varphi)$ is the *coimage* of φ. These maps possess universal properties [28, §E.5].

3.9. Subobjects and images

We close with a list of facts about varieties, which we use heavily in Section 5. We first define a preorder that enables abbreviation of compositions of multiple homomorphisms. To motivate this, assume

$\varphi : E_1 \to E_2$ is a homomorphism of algebras. Theorem 3.18 states there exists $\theta : E_1 \to \mathrm{Im}(\varphi)$ such that $\varphi = \mathrm{im}(\varphi)\theta$. We denote this by $\varphi \ll \mathrm{im}(\varphi)$ and make the following more general definition. For morphisms $a, b : \mathsf{E}$,

$$a \ll b \iff [(\exists c : \mathsf{E})\ \ a = bc]\,, \tag{3.4}$$
$$a \gg b \iff [(\exists d : \mathsf{E})\ \ a = db]\,. \tag{3.5}$$

Two monomorphisms $a, b : \mathsf{E}$ are *equivalent* if $a \ll b$ and $b \ll a$. Similarly, epimorphisms $c, d : \mathsf{E}$ are *equivalent* if $c \gg d$ and $d \gg c$.

Lemma 3.19. *Let* E *be a variety. For morphisms* $a, b : \mathsf{E}$*, if* $a\blacktriangleleft = \blacktriangleleft b$*, then* $a\,\mathrm{im}(b) \ll \mathrm{im}(ab)$.

Proof. By Theorem 3.18, there exist isomorphisms $\psi_b, \psi_{ab} : \mathsf{E}$ such that

$$b = \mathrm{im}(b)\psi_b \mathrm{coim}(b), \qquad ab = \mathrm{im}(ab)\psi_{ab}\mathrm{coim}(ab).$$

By the universal property of coimages, there exists a unique morphism $\pi : \mathsf{E}$ such that $\mathrm{coim}(ab) = \pi\,\mathrm{coim}(b)$. Therefore

$$a\,\mathrm{im}(b)\psi_b\mathrm{coim}(b) = ab = \mathrm{im}(ab)\psi_{ab}\mathrm{coim}(ab) = \mathrm{im}(ab)\psi_{ab}\pi\,\mathrm{coim}(b).$$

Since $\mathrm{coim}(b)$ is an epimorphism, $a\,\mathrm{im}(b) = \mathrm{im}(ab)\psi_{ab}\pi\psi_b^{-1} \ll \mathrm{im}(ab)$. □

Lemma 3.20. *Let* E *be a variety. For morphisms* $a, b : \mathsf{E}$*, if* $a\blacktriangleleft = \blacktriangleleft b$*, then* $\mathrm{im}(ab) \ll \mathrm{im}(a)$*. If* a *is also monic, then* $\mathrm{im}(ab) \ll a\,\mathrm{im}(b)$.

Proof. The first claim follows from the universal property of images, so we assume a is monic. By Theorem 3.18, there exists an isomorphism $\psi_b : \mathsf{E}$ such that

$$b = \mathrm{im}(b)\psi_b\mathrm{coim}(b).$$

Since $a\,\mathrm{im}(b)$ is monic and $ab = (a\,\mathrm{im}(b))(\psi_b\mathrm{coim}(b))$, by the universal property of images, there exists a morphism $\iota : \mathsf{E}$ such that $\mathrm{im}(ab) = a\,\mathrm{im}(b)\iota \ll a\,\mathrm{im}(b)$. □

Varieties have a *coproduct* [28, p. 81] given by the *free product* [28, p. 183]. An example concerning groups is given in [28, Corollary 4.5.7]. We list some facts concerning coproducts in varieties.

Fact 3.21. *Let* I *be a type. In a variety* E*, the following hold for all* $e : \mathbb{1}_{\mathsf{E}}$ *and* $a : I \to e\mathsf{E}$.

(a) *There exists a coproduct morphism* $\coprod_{i:I} a_i$ *and morphisms* $\iota : I \to \left(\coprod_{i:I} a_i\right)\mathsf{E}$ *satisfying* $\left(\coprod_{i:I} a_i\right)\iota_j = a_j$ *for each* $j : I$.

(b) *If* I *is uninhabited, then* $f := \left(\coprod_{i:I} a_i\right)\blacktriangleleft$ *is the identity on the free algebra on the empty set. In particular,* $\coprod_{i:I} a_i$ *is the unique morphism inhabiting* $e\mathsf{E}f$.

(c) *If* $b : \mathsf{E}$ *such that* $b\blacktriangleleft = \blacktriangleleft a_i$ *for all* $i : I$*, then* $\coprod_{i:I}(ba_i) = b\coprod_{i:I} a_i$.

(d) *If* $b : I \to \mathsf{E}$ *with* $a_i\blacktriangleleft = \blacktriangleleft b_i$ *for all* $i : I$*, then* $\coprod_{i:I}(a_i b_i) \ll \coprod_{i:I} a_i$.

(e) *If* $J \subset I$*, then* $\coprod_{j:J} a_j \ll \coprod_{i:I} a_i$.

Finally, if a is monomorphism satisfying $\blacktriangleleft a = e$, for some identity e, then $a\blacktriangleleft$ can be regarded as a subobject of the object associated to e. Given a collection $\{a_i \mid i : I\}$ of such monomorphisms, consider the smallest subobject containing all set-wise images of the $a_i\blacktriangleleft$. The coproduct allows us to effectively "glue" together all of the monomorphisms, but the result is not a monomorphism. To obtain

a monomorphism, we take the image of the coproduct, namely

$$\operatorname{im}\left(\coprod_{i:I} a_i\right). \tag{3.6}$$

4. Category actions, capsules, and counits

Theorem 2 asserts that characteristic subgroups arise from categories acting on other categories. In this section we define category actions and introduce the notion of a *capsule*. We also elucidate the connection between capsules and the more familiar category notions of units, counits, and adjoint functor pairs. Recall from our discussion following Definition 3.10 that an (abstract) category A is on an underlying type $A^?$, hence $\bot : \mathsf{A}$.

4.1. Category actions

Our formulation of category actions generalizes the familiar notion for groups and also actions of monoids and groupoids [20, §I.4]. The technical aspects of the definition concern the additional guards, denoted $\triangleleft$, needed to express where products are defined. Their use is similar to the guards $\blacktriangleleft$ introduced for abstract categories in Definition 3.10.

Definition 4.1. Let A be an abstract category with guards $(-)\blacktriangleleft$ and $\blacktriangleleft(-)$. Let X be a type. A (*left*) *category action* of A on X consists of a type $\triangleleft X$, functions $(-)\triangleleft : \mathsf{A} \to (\triangleleft X)^?$ and $\triangleleft(-) : X^? \to (\triangleleft X)^?$ that output $\bot$ if, and only if, the input is $\bot$, and a function $\cdot : \mathsf{A} \times X^? \to X^?$ that satisfies the following rules:

(1) $(\forall a : \mathsf{A})$ $(\forall x : X^?)$ $[(a\triangleleft = \triangleleft x) \iff ((\exists y : X)\ a \cdot x = y)]$;
(2) $(\forall a : \mathsf{A})$ $(\forall x : X^?)$ $[(a\blacktriangleleft)\triangleleft = a\triangleleft$ and $((a\blacktriangleleft) \cdot x) \succeq x]$; and
(3) $(\forall a, b : \mathsf{A})$ $(\forall x : X^?)$ $((ab) \cdot x) \succeq (a \cdot (b \cdot x))$.

Given a left action of A on a type Y, a function $\mathcal{M} : X^? \to Y^?$ is an A-*morphism* if $\mathcal{M}(a \cdot x) = a \cdot \mathcal{M}(x)$ whenever $a : \mathsf{A}$ and $x : X$ with $a\triangleleft = \triangleleft x$; that is, $\mathcal{M}(a \cdot x) \succeq a \cdot \mathcal{M}(x)$.

Right category actions are similarly defined. We unpack the symbolic expressions in Definition 4.1. Condition (1) states that the functions $(-)\triangleleft$ and $\triangleleft(-)$ serve as guards for the function $\cdot : \mathsf{A} \times X^? \to X^?$: namely, (1) characterizes precisely when $\cdot$ is defined. The first part of condition (2) asserts that $(-)\triangleleft$ respects the $(-)\blacktriangleleft$ identity of A; the second part states that identity morphisms of A act as identities. Condition (3) is the familiar group action axiom in the setting of partial functions.

For subtypes $S \subset \mathsf{A}$ and $Y \subset X$, we write

$$S \cdot Y := \{s \cdot y \mid s : S,\ y : Y,\ s\triangleleft = \triangleleft y\}.$$

From Definition 4.1, an A-morphism $\mathcal{M} : X^? \to Y^?$ maps a term $b : (\mathsf{A} \cdot X)$ to a term of Y; we say that $\mathcal{M}$ is *defined* on $\mathsf{A} \cdot X$.

Definition 4.2. The category action of A on X is *full* if $e \cdot x \mapsto \triangleleft(e \cdot x)$ defines a bijection from $\mathbb{1}_{\mathsf{A}} \cdot X$ to $\mathsf{A}\triangleleft = \{a\triangleleft \mid a : \mathsf{A}\}$. Thus, the action is full if, and only if, for every $a : \mathsf{A}$ there exists $x : X$ such that $a\triangleleft = \triangleleft x$.

Recall from Remark 3.16 that we identify categories and abstract categories. We say that a category C acts on a type X if its morphism type $\mathsf{C}_1^?$ acts on X (cf. Proposition 3.12).

Example 4.3. Let C be a category with object type C_0 and morphism type $\mathsf{C}_1^?$. Set $X = \triangleleft X = \mathsf{C}_0$. Define $(-)\triangleleft : \mathsf{C}_1^? \to \mathsf{C}_0^?$ via $f\triangleleft := \operatorname{Dom} f$ and define $\triangleleft(-) : \mathsf{C}_0^? \to \mathsf{C}_0^?$ via $\triangleleft U := U$. Let $\cdot : \mathsf{C}_1^? \times \mathsf{C}_0^? \to \mathsf{C}_0^?$ be

defined by

$$f \cdot U := \begin{cases} \operatorname{Codom} f & \text{if } f\triangleleft = \triangleleft U, \\ \bot & \text{otherwise.} \end{cases}$$

This defines a full left action of C on C_0. A full right action is defined similarly. □

Remark 4.4. Let C be a category and let $X = \mathsf{C}_1$. The definition of category action in [14, 1.271–1.274] is similar to ours, but it requires $\triangleleft X = \mathbb{1}_{\mathsf{C}} = \{f\blacktriangleleft \mid f : \mathsf{C}_1\}$ and $\triangleleft x = \blacktriangleleft x$ and $f\triangleleft = f\blacktriangleleft$ for every $x : X$ and $f : \mathsf{C}_1$. Thus, for $f, g : \mathsf{C}_1$ and $x : X$, both $f \cdot x$ and $g \cdot x$ are defined (neither is $\bot$) only when $f\blacktriangleleft = \triangleleft x = g\blacktriangleleft$; this is too restrictive for our purposes.

4.2. Capsules

As identified in Section 1.2, we focus on the action of one category A on another category X; we call these "category modules" *capsules*. Note the subtle change in notation from X to X to emphasize this setting. In this case, X already has a candidate type for $\triangleleft\mathsf{X}$, namely $\blacktriangleleft\mathsf{X} = \mathbb{1}_{\mathsf{X}}$. Since a category has its own operation of composition, the action by A respects composition. For example, given a group homomorphism $\varphi : G \to H$, we get an action $g \cdot h := \varphi(g)h$ that satisfies $g \cdot (hh') = (g \cdot h)h'$.

Definition 4.5. A category X is a *left* A*-capsule* if there is a full left A-action on X with $\triangleleft\mathsf{X} = \mathbb{1}_{\mathsf{X}}$ such that the following hold:

(a) $(\forall x : \mathsf{X})\quad (\triangleleft x = \blacktriangleleft x)$;
(b) $(\forall a : \mathsf{A})\quad (\forall x, y : \mathsf{X})\qquad (a \cdot (xy) = (a \cdot x)y)$.

A *right* A*-capsule* is similarly defined. We present our results below for left A-capsules, but they can be formulated for both.

Much of our intuition on actions draws on familiar themes in representation theory. A reader may be assisted by translating "A-capsule" to "A-module" and considering the matching statement for modules. We write ${}_{\mathsf{A}}\mathsf{X}$ to indicate the presence of a left A-capsule action on X.

From now on, if a category A acts on itself, then we assume it is by the (left) *regular action*, where $\cdot : \mathsf{A} \times \mathsf{A} \to \mathsf{A}$ is given by composition in A. Moreover, a category action on another category is implicitly understood to be on the morphisms. We now show that capsules arise from morphisms between categories.

Proposition 4.6. *A category* X *is a left* A*-capsule of a category* A *if, and only if, there is a morphism* $\mathcal{F} : \mathsf{A} \to \mathsf{X}$ *such that* $a \cdot x = \mathcal{F}(a)x$ *for all* $a : \mathsf{A}$ *and* $x : \mathsf{X}$*. Furthermore, the morphism* $\mathcal{F}$ *is unique.*

The following lemma proves one direction of Proposition 4.6.

Lemma 4.7. *Every morphism* $\mathcal{F} : \mathsf{A} \to \mathsf{X}$ *of categories makes* X *a left* A*-capsule, where for each* $a : \mathsf{A}$ *and* $x : \mathsf{X}$*, the guard is defined by* $a\triangleleft := \mathcal{F}(a)\blacktriangleleft$ *and the action is defined by* $a \cdot x := \mathcal{F}(a)x$*.*

Proof. Condition (1) of Definition 4.1 is satisfied by the defined action.

For the first part of condition (2), let $a : \mathsf{A}$. Since $\mathcal{F}$ is a morphism and $(-)\blacktriangleleft$ is everywhere defined, $\mathcal{F}(a\blacktriangleleft) = \mathcal{F}(a)\blacktriangleleft$. Hence, by Lemma 3.11(a),

$$(a\blacktriangleleft)\triangleleft = \mathcal{F}(a\blacktriangleleft)\blacktriangleleft = (\mathcal{F}(a)\blacktriangleleft)\blacktriangleleft = \mathcal{F}(a)\blacktriangleleft = a\triangleleft\,.$$

For the second part of condition (2), let $a : \mathsf{A}$ and $x : \mathsf{X}$ with $a\triangleleft = \triangleleft x$, so $\mathcal{F}(a)\blacktriangleleft = \blacktriangleleft x$ by definition. Thus,

$$(a\blacktriangleleft) \cdot x = \mathcal{F}(a\blacktriangleleft)x = (\mathcal{F}(a)\blacktriangleleft)x = (\blacktriangleleft x)x = x,$$

so $(a\blacktriangleleft)\cdot x \succcurlyeq x$ for every $a : \mathsf{A}$ and $x : \mathsf{X}$.

For condition (3), let $a, b : \mathsf{A}$ and $x : \mathsf{X}$ with $a\blacktriangleleft = \blacktriangleleft b$ and $(ab)\triangleleft = \triangleleft x$, so $(ab)\cdot x$ is defined and $(ab)\blacktriangleleft = b\blacktriangleleft$. We need to show that $(ab)\cdot x = a\cdot(b\cdot x)$. Since $\mathcal{F}$ is a morphism,

$$(ab)\triangleleft = (\mathcal{F}(ab))\blacktriangleleft = \mathcal{F}((ab)\blacktriangleleft) = \mathcal{F}(b\blacktriangleleft) = \mathcal{F}(b)\blacktriangleleft = b\triangleleft\,.$$

Hence, $(ab)\triangleleft = \triangleleft x$ implies $b\triangleleft = \triangleleft x$. Thus, $\mathcal{F}(b)x$ is defined. Also, $a\blacktriangleleft = \blacktriangleleft b$ implies $\mathcal{F}(a)\blacktriangleleft = \blacktriangleleft(\mathcal{F}(b))$, so

$$a\triangleleft = \mathcal{F}(a)\blacktriangleleft = \blacktriangleleft(\mathcal{F}(b)) = \blacktriangleleft(\mathcal{F}(b)x) = \blacktriangleleft(b\cdot x) = \triangleleft(b\cdot x).$$

It follows that $a\cdot(b\cdot x)$ is defined. Since $\mathcal{F}$ is a morphism,

$$a\cdot(b\cdot x) = \mathcal{F}(a)(\mathcal{F}(b)x) = \mathcal{F}(ab)x = (ab)\cdot x,$$

and therefore $(ab)\cdot x \succcurlyeq a\cdot(b\cdot x)$ for every $a, b : \mathsf{A}$ and $x : \mathsf{X}$.

To see that the action is full, consider $a : \mathsf{A}$ and define $x = \mathcal{F}(a)\blacktriangleleft$. By the laws of an abstract category, $a\triangleleft = \mathcal{F}(a)\blacktriangleleft = \blacktriangleleft(\mathcal{F}(a)\blacktriangleleft) = \blacktriangleleft x = \triangleleft x$. Finally, $(a\cdot x)y = \mathcal{F}(a)xy = a\cdot(xy)$, so X is a left A-capsule. □

Our proof of the reverse direction of Proposition 4.6 uses the following result.

Lemma 4.8. *Let X be a left A-capsule. For every $a : \mathsf{A}$, there is a unique $e : \mathbb{1}_{\mathsf{X}}$ such that $a\cdot e$ is the unique term of type $a\cdot\mathbb{1}_{\mathsf{X}}$.*

Proof. Let $a : \mathsf{A}$. If $a = \bot$, then $\bot$ is the unique $x : \mathsf{X}$ with $a\triangleleft = \bot = \triangleleft x$. Now suppose a is not $\bot$. Since the action is full, there exists $x : \mathsf{X}$ such that $a\triangleleft = \triangleleft x$, so $a\cdot x$ is defined. Since X is a left A-capsule, $a\triangleleft = \triangleleft x = \blacktriangleleft x$, so

$$\triangleleft(\blacktriangleleft x) = \blacktriangleleft(\blacktriangleleft x) = \blacktriangleleft x.$$

Hence, $a\cdot(\blacktriangleleft x)$ is defined and has type $a\cdot\mathbb{1}_{\mathsf{X}}$. Suppose $e : \mathbb{1}_{\mathsf{X}}$ and $f : \mathbb{1}_{\mathsf{X}}$ with $a\triangleleft = \triangleleft e = \triangleleft f$, so that $a\cdot e : a\cdot\mathbb{1}_{\mathsf{X}}$ and $a\cdot f : a\cdot\mathbb{1}_{\mathsf{X}}$. Then

$$e = \blacktriangleleft e = \triangleleft e = \triangleleft f = \blacktriangleleft f = f,$$

so $a\cdot e = a\cdot f$, and there is exactly one term with type $a\cdot\mathbb{1}_{\mathsf{X}}$. □

Under the assumptions of Lemma 4.8, we simplify notation and identify $a\cdot\mathbb{1}_{\mathsf{X}}$ with its unique term.

Proof of Proposition 4.6. By Lemma 4.7, it remains to prove the forward direction and uniqueness. Suppose that X is a left A-capsule. By Lemma 4.8, for each $a : \mathsf{A}$ there is a unique $\mathcal{F}(a\blacktriangleleft) : \mathbb{1}_{\mathsf{X}}$ such that $(a\blacktriangleleft)\cdot\mathcal{F}(a\blacktriangleleft)$ is defined. Since X is a left A-capsule and $\mathcal{F}(a\blacktriangleleft)$ is an identity,

$$(a\blacktriangleleft)\triangleleft = a\triangleleft = \triangleleft\mathcal{F}(a\blacktriangleleft) = \blacktriangleleft\mathcal{F}(a\blacktriangleleft) = \mathcal{F}(a\blacktriangleleft).$$

Thus, $a\cdot\mathcal{F}(a\blacktriangleleft)$ is also defined. Put $\mathcal{F}(a) := a\cdot\mathcal{F}(a\blacktriangleleft)$. If $x : \mathsf{X}$, then $a\cdot x$ is defined whenever

$$\blacktriangleleft x = \triangleleft x = a\triangleleft = \mathcal{F}(a\blacktriangleleft) = \mathcal{F}(a\blacktriangleleft)\blacktriangleleft\,.$$

Hence, $\mathcal{F}(a\blacktriangleleft)x$ is also defined in X. Because $\mathcal{F}(a\blacktriangleleft)$ is an identity, $\mathcal{F}(a\blacktriangleleft)x = x$. Since X is a left A-capsule, $a\cdot x = a\cdot(\mathcal{F}(a\blacktriangleleft)x) = (a\cdot\mathcal{F}(a\blacktriangleleft))x = \mathcal{F}(a)x$. Hence, it remains to prove that $\mathcal{F} : \mathsf{A}\to\mathsf{X}$ is a morphism of categories.

For $a, b : \mathsf{A}$, by the action laws

$$\mathcal{F}(ab) = (ab)\cdot\mathcal{F}((ab)\blacktriangleleft) = (ab)\cdot\mathcal{F}(b\blacktriangleleft) \succcurlyeq a\cdot(b\cdot\mathcal{F}(b\blacktriangleleft)) = a\cdot\mathcal{F}(b).$$

Thus, $\mathcal{F}(ab) \succeq a \cdot \mathcal{F}(b)$. But X is a left A-capsule, so Fact 3.14 implies that

$$a \cdot \mathcal{F}(b) = a \cdot (\mathbb{1}_{\mathsf{X}}\mathcal{F}(b)) = (a \cdot \mathbb{1}_{\mathsf{X}})\mathcal{F}(b) = \mathcal{F}(a)\mathcal{F}(b). \tag{4.1}$$

Hence, $\mathcal{F}(ab) \succeq \mathcal{F}(a)\mathcal{F}(b)$. By Lemma 3.11(b) and (4.1) for all $a : \mathsf{A}$,

$$\mathcal{F}(a)\blacktriangleleft \;=\; (a \cdot \mathcal{F}(a\blacktriangleleft))\blacktriangleleft \;=\; (\mathcal{F}(a)\mathcal{F}(a\blacktriangleleft))\blacktriangleleft \;=\; \mathcal{F}(a\blacktriangleleft)\blacktriangleleft \;=\; \mathcal{F}(a\blacktriangleleft).$$

Similarly, $\mathcal{F}(\blacktriangleleft a) = \blacktriangleleft\mathcal{F}(a)$. Hence, $\mathcal{F}$ is a morphism.

Lastly, we prove uniqueness of $\mathcal{F}$. Suppose there exists $\mathcal{G} : \mathsf{A} \to \mathsf{X}$ such that $a \cdot x = \mathcal{G}(a)x$ for every $a : \mathsf{A}$ and $x : \mathsf{X}$ whenever $a\triangleleft = \triangleleft x$. Since $a\triangleleft = \mathcal{F}(a\blacktriangleleft)$, it follows that $\mathcal{G}(a)\blacktriangleleft = \mathcal{F}(a\blacktriangleleft)$, so $\mathcal{G}(a) = \mathcal{G}(a)\mathcal{F}(a\blacktriangleleft) = a \cdot \mathcal{F}(a\blacktriangleleft) = \mathcal{F}(a)$. □

If B is a subcategory of A with inclusion $\mathcal{I} : \mathsf{B} \to \mathsf{A}$, then the (left) *regular action* of B on A is defined to be the action given by $\mathcal{I}$. In other words, the regular action of B on A is given by $b \cdot a = \mathcal{I}(b)a$ for $a : \mathsf{A}$ and $b : \mathsf{B}$. By Lemma 4.7, each regular action defines a capsule. With regular actions we sometimes omit the "$\cdot$".

4.3. Category biactions and cyclic bicapsules

We now define the concepts appearing in Theorem 2(3).

Definition 4.9. Let A and B be categories and let X and Y be types.

(a) An (A, B)-*biaction* on X is a left A-action on X and a right B-action on X such that $a \cdot (x \cdot b) = (a \cdot x) \cdot b$ for every $a : \mathsf{A}$, $b : \mathsf{B}$, and $x : X$. Hence, writing $a \cdot x \cdot b$ is unambiguous. If, in addition, X is a left A-capsule and right B-capsule, then X is an (A, B)-*bicapsule*.

(b) Suppose there are (A, B)-biactions on X and Y. An (A, B)-*morphism* is a function $\mathcal{M} : X^? \to Y^?$ such that $\mathcal{M}(a \cdot x \cdot b) = a \cdot \mathcal{M}(x) \cdot b$, whenever $a : \mathsf{A}$, $x : X$, $b : \mathsf{B}$ with $a\triangleleft = \triangleleft x$ and $x\triangleleft = \triangleleft b$; that is, $\mathcal{M}(a \cdot x \cdot b) \succeq a \cdot \mathcal{M}(x) \cdot b$.

We sometimes write ${}_{\mathsf{A}}X_{\mathsf{B}}$ for an (A, B)-biaction on X for clarity. Notice that an (A, B)-morphism $\mathcal{M} : X^? \to Y^?$ must be defined on $\mathsf{A} \cdot X \cdot \mathsf{B}$. As with capsule morphisms, we do not need to establish guards. We abbreviate (A, A)-bicapsule to A-*bicapsule*, (A, A)-morphism to A-*bimorphism*, and (A, A)-biaction to A-*biaction*. Just as ring homomorphisms are not always linear maps, morphisms of capsules need not be morphisms of categories since they need not send identities to identities.

Motivated by Proposition 4.6, we show that bicapsules provide a computationally useful perspective to record natural transformations of functors. If $\mathcal{F}, \mathcal{G} : \mathsf{A} \to \mathsf{B}$ are functors and $\mu : \mathcal{G} \Rightarrow \mathcal{F}$ is a natural transformation, then, using Remark 3.16, the natural transformation property written with guards is

$$\mathcal{F}(a)\mu_{a\blacktriangleleft} = \mu_{\blacktriangleleft a}\mathcal{G}(a)$$

for every morphism a in A.

Proposition 4.10. *In the following statements, the category* A *is also regarded as an* A*-bicapsule via its regular action.*

(a) *For every natural transformation* $\mu : \mathcal{G} \Rightarrow \mathcal{F}$ *between functors* $\mathcal{F}, \mathcal{G} : \mathsf{A} \to \mathsf{X}$*, the assignment*

$$a \cdot x \cdot a' := \mathcal{F}(a)x\mathcal{G}(a') \qquad\qquad (a, a' : \mathsf{A},\ x : \mathsf{X})$$

makes X *into an* A*-bicapsule, and the assignment* $\mathcal{M}(a) := a \cdot \mu_{a\blacktriangleleft}$ *defines an* A*-bimorphism* $\mathcal{M} : \mathsf{A} \to \mathsf{X}$.

(b) *Conversely, for every category* X *and* A*-bimorphism* $\mathcal{M} : \mathsf{A} \to \mathsf{X}$*, the assignments*

$$\mathcal{F}(a) := a \cdot \mathbb{1}_{\mathsf{X}}, \qquad \mathcal{G}(a) := \mathbb{1}_{\mathsf{X}} \cdot a \qquad (a : \mathsf{A})$$

define functors $\mathcal{F}, \mathcal{G} : \mathsf{A} \to \mathsf{X}$*, and the assignment*

$$\mu_{a\blacktriangleleft} := \mathcal{M}(a\blacktriangleleft) \qquad (a : \mathsf{A})$$

defines a natural transformation $\mu : \mathcal{G} \Rightarrow \mathcal{F}$*.*

Proof. (a) By Lemma 3.11(b) for all $a, b, c : \mathsf{A}$,

$$\mathcal{M}(ab) = (ab) \cdot \mu_{(ab)\blacktriangleleft} = \mathcal{F}(ab)\mu_{(ab)\blacktriangleleft} \succcurlyeq \mathcal{F}(a)\mathcal{F}(b)\mu_{b\blacktriangleleft} = a \cdot \mathcal{M}(b).$$

Since μ is a natural transformation,

$$\begin{aligned}\mathcal{M}(bc) &= \mathcal{F}(bc)\mu_{(bc)\blacktriangleleft} = \mu_{\blacktriangleleft(bc)}\mathcal{G}(bc)\\ &\succcurlyeq \mu_{\blacktriangleleft b}\mathcal{G}(b)\mathcal{G}(c) = \mathcal{F}(b)\mu_{b\blacktriangleleft}\mathcal{G}(c) = \mathcal{M}(b) \cdot c.\end{aligned}$$

Thus, $\mathcal{M}(abc) \succcurlyeq a \cdot \mathcal{M}(b) \cdot c$, so $\mathcal{M}$ is an A-bimorphism.

(b) By Proposition 4.6, the left and right actions determine functors $\mathcal{F}, \mathcal{G} : \mathsf{A} \to \mathsf{X}$. For $e : \mathbb{1}_{\mathsf{A}}$, define $\mu_e := \mathcal{M}(e)$. For $a : \mathsf{A}$

$$\begin{aligned}\mathcal{F}(a)\mu_{a\blacktriangleleft} &= \mathcal{F}(a)\mathcal{M}(a\blacktriangleleft) = a \cdot \mathcal{M}(a\blacktriangleleft) = \mathcal{M}(a(a\blacktriangleleft)) = \mathcal{M}(a)\\ &= \mathcal{M}((\blacktriangleleft a)a) = \mathcal{M}(\blacktriangleleft a) \cdot a = \mathcal{M}(\blacktriangleleft a)\mathcal{G}(a) = \mu_{\blacktriangleleft a}\mathcal{G}(a).\end{aligned}$$

It follows that μ is a natural transformation. □

We summarize the conclusion in Proposition 4.10(b), namely $\mu_e = \mathcal{M}(e)$ for every $e : \mathbb{1}_{\mathsf{A}}$, by writing $\mu := \mathcal{M}(\mathbb{1}_A)$. While $\mathbb{1}_{\mathsf{A}}$ consists of many terms, each of the types $x \cdot \mathbb{1}_{\mathsf{A}}$ and $\mathbb{1}_{\mathsf{A}} \cdot x$ is inhabited by a unique term, so $\mathbb{1}_{\mathsf{A}}$ plays a role similar to multiplying by 1. Since $\mathcal{M} : \mathsf{A} \to \mathsf{X}$ is an A-bimorphism,

$$(\forall a : \mathsf{A}) \qquad \mathcal{M}(a) = a \cdot \mathcal{M}(\blacktriangleleft a) = \mathcal{M}(a\blacktriangleleft) \cdot a,$$

which shows that $\mathcal{M}$ is determined by $\mathcal{M}(\mathbb{1}_{\mathsf{A}})$. We write

$$\mathsf{A} \cdot \mu \cdot \mathsf{A} := \{a \cdot \mu_e \cdot \acute{a} \mid a, \acute{a} : \mathsf{A}, e : \mathbb{1}_{\mathsf{A}},\ a\triangleleft = \triangleleft\mu_e,\ \mu_e\triangleleft = \triangleleft\acute{a}\}\,. \tag{4.2}$$

The bicapsule in (4.2) is the *cyclic* A-bicapsule determined by $\mu = \mathcal{M}(\mathbb{1}_{\mathsf{A}})$.

4.4. Units and counits

A *unit* in a category A is a natural transformation $\mu : \mathrm{id}_{\mathsf{A}} \Rightarrow \mathcal{H}$, where $\mathcal{H} : \mathsf{A} \to \mathsf{A}$ is a functor. Similarly, a *counit* is a natural transformation $\nu : \mathcal{H} \Rightarrow \mathrm{id}_{\mathsf{A}}$. We will prove that units and counits are responsible for all characteristic structure. It therefore makes sense to translate these into capsule actions. We show that a unit μ is characterized as an (A, B)-bimorphism $\mathcal{M} : \mathsf{A} \to \mathsf{B}$ and a counit ν by an (A, B)-morphism $\mathcal{N} : \mathsf{B} \to \mathsf{A}$. As the relationship is dual, and we emphasize substructures instead of quotients, we consider this relationship only for counits.

Theorem 4.11. *Let* A *and* B *be categories.*

(a) *If both* A *and* B *are* (A, B)*-bicapsules and* $\mathcal{N} : \mathsf{B} \to \mathsf{A}$ *is an* (A, B)*-morphism, then* $\mathcal{F}(b) := \mathbb{1}_{\mathsf{A}} \cdot b$ *and* $\mathcal{G}(a) := a \cdot \mathbb{1}_{\mathsf{B}}$ *define functors* $\mathcal{F} : \mathsf{B} \to \mathsf{A}$ *and* $\mathcal{G} : \mathsf{A} \to \mathsf{B}$*, and* $\nu := \mathcal{N}\mathcal{G}(\mathbb{1}_{\mathsf{A}})$ *is a counit* $\nu : \mathcal{F}\mathcal{G} \Rightarrow \mathrm{id}_{\mathsf{A}}$.

(b) *If* $\mathcal{F} : \mathsf{B} \to \mathsf{A}$ *and* $\mathcal{G} : \mathsf{A} \to \mathsf{B}$ *are functors and* $\nu : \mathcal{F}\mathcal{G} \Rightarrow \mathrm{id}_{\mathsf{A}}$ *is a counit, then* A *and* B *are* (A, B)*-bicapsules, where* $a \cdot y \cdot b := \mathcal{G}(a)yb$ *and* $a \cdot x \cdot b = \mathcal{F}\mathcal{G}(a)x\mathcal{F}\mathcal{G}\mathcal{F}(b)$ *for* $a, x : \mathsf{A}$ *and* $b, y : \mathsf{B}$*. Also,* $\mathcal{N}'(b) := \mathcal{F}(b)\nu_{\mathcal{F}(b)\blacktriangleleft}$ *is an* (A, B)*-morphism* $\mathsf{B} \to \mathsf{A}$ *such that* $\mathcal{N}'\mathcal{G}(e) = \nu_{\mathcal{F}\mathcal{G}(e)}$ *for all* $e : \mathbb{1}_{\mathsf{A}}$.

Proof. (a) By Proposition 4.6, the maps $\mathcal{F}$ and $\mathcal{G}$ define functors where $x \cdot b = x\mathcal{F}(b)$ and $a \cdot y = \mathcal{G}(a)y$, for $a, x : \mathsf{A}$ and $b, y : \mathsf{B}$. Put $\nu = \mathcal{N}(\mathcal{G}(\mathbb{1}_A))$. For $a : \mathsf{A}$,

$$a\nu_{a\blacktriangleleft} = a\mathcal{N}\mathcal{G}(a\blacktriangleleft) = a\mathcal{N}(\mathcal{G}(a)\blacktriangleleft) = \mathcal{N}(a \cdot (\mathcal{G}(a))\blacktriangleleft) = \mathcal{N}(\mathcal{G}(a)(\mathcal{G}(a))\blacktriangleleft) = \mathcal{N}\mathcal{G}(a),$$

and

$$\nu_{\blacktriangleleft a}\mathcal{F}\mathcal{G}(a) = \mathcal{N}\mathcal{G}(\blacktriangleleft a) \cdot \mathcal{G}(a) = \mathcal{N}(\blacktriangleleft\mathcal{G}(a)) \cdot \mathcal{G}(a) = \mathcal{N}((\blacktriangleleft\mathcal{G}(a))\mathcal{G}(a)) = \mathcal{N}\mathcal{G}(a).$$

Hence, $a\nu_{a\blacktriangleleft} = \nu_{\blacktriangleleft a}\mathcal{F}\mathcal{G}(a)$ for all $a : \mathsf{A}$, so $\nu : \mathcal{F}\mathcal{G} \Rightarrow \mathrm{id}_{\mathsf{A}}$ is a natural transformation.

We show that $\mathcal{N}'(b) := \mathcal{F}(b)\nu_{\mathcal{F}(b)\blacktriangleleft}$ yields an (A, B)-morphism $\mathcal{N}' : \mathsf{B} \to \mathsf{A}$. First, if $a : \mathsf{A}$ and $y : \mathsf{B}$ with $a\triangleleft = \triangleleft y$, then

$$\begin{aligned}
\mathcal{N}'(a \cdot y) &= \mathcal{N}'(\mathcal{G}(a)y) \\
&= \mathcal{F}(\mathcal{G}(a)y)\nu_{\mathcal{F}(\mathcal{G}(a)y)\blacktriangleleft} \\
&= \mathcal{F}\mathcal{G}(a)\mathcal{F}(y)\nu_{(\mathcal{F}\mathcal{G}(a)\mathcal{F}(y))\blacktriangleleft} \\
&= \mathcal{F}\mathcal{G}(a)\mathcal{F}(y)\nu_{\mathcal{F}(y)\blacktriangleleft} \\
&= \mathcal{F}\mathcal{G}(a)\mathcal{N}'(y) \\
&= a \cdot \mathcal{N}'(y).
\end{aligned}$$

Next, if $b : \mathsf{B}$ such that $y\triangleleft = \triangleleft b$, then

$$\begin{aligned}
\mathcal{N}'(yb) &= \mathcal{F}(yb)\nu_{\mathcal{F}(yb)\blacktriangleleft} \\
&= \nu_{\blacktriangleleft\mathcal{F}(yb)}\mathcal{F}\mathcal{G}\mathcal{F}(yb) \\
&= \nu_{\blacktriangleleft(\mathcal{F}(y)\mathcal{F}(b))}\mathcal{F}\mathcal{G}\mathcal{F}(y)\mathcal{F}\mathcal{G}\mathcal{F}(b) \\
&= \nu_{\blacktriangleleft\mathcal{F}(y)}\mathcal{F}\mathcal{G}\mathcal{F}(y)\mathcal{F}\mathcal{G}\mathcal{F}(b) \\
&= \mathcal{F}(y)\nu_{\mathcal{F}(y)\blacktriangleleft}\mathcal{F}\mathcal{G}\mathcal{F}(b) \\
&= \mathcal{N}'(y)\mathcal{F}\mathcal{G}\mathcal{F}(b) \\
&= \mathcal{N}'(y) \cdot b.
\end{aligned}$$

Finally, consider $e : \mathbb{1}_{\mathsf{A}}$. Since functors map identities to identities, we deduce that

$$\mathcal{N}'(\mathcal{G}(e)) = \mathcal{F}\mathcal{G}(e)\nu_{\mathcal{F}\mathcal{G}(e)\blacktriangleleft} = \nu_{\mathcal{F}\mathcal{G}(e)}.$$

□

4.5. Adjoint functor pairs

Adjoint functor pairs are an important special case of natural transformations. We give one of many equivalent definitions [28, §4.1].

Definition 4.12. Let A and B be categories. An *adjoint functor pair* is a pair of functors $\mathcal{F} : \mathsf{B} \to \mathsf{A}$ and $\mathcal{G} : \mathsf{A} \to \mathsf{B}$ with the following property. For every object U in B and V in A, there is an invertible function

$$\Psi_{UV} : \mathsf{A}_1(\mathcal{F}(U), V) \to \mathsf{B}_1(U, \mathcal{G}(V))$$

that is *natural* in the following sense: if $b : \mathsf{B}_1(X, U)$ and $a : \mathsf{A}_1(V, Y)$ for objects X in B and Y in B then, for $x : \mathsf{A}_1(\mathcal{F}(U), V)$,

$$\Psi_{XY}(ax\mathcal{F}(b)) = \mathcal{G}(a)\Psi_{UV}(x)b. \tag{4.3}$$

We say $\mathcal{F}$ is *left-adjoint* to $\mathcal{G}$ and $\mathcal{G}$ is *right-adjoint* to $\mathcal{F}$ and write $\mathcal{F} : \mathsf{B} \dashv_\Psi \mathsf{A} : \mathcal{G}$.

We now characterize adjoint functor pairs in terms of bicapsules. A reader may find it useful to review the translation between categories and abstract categories in Remark 3.16. The invertibility of Ψ_{UV} in Definition 4.12 is equivalent to a pseudo-inverse property of morphisms of bicapsules.

For types X and Y, functions $\mathcal{M} : X^? \to Y^?$ and $\mathcal{N} : Y^? \to X^?$ are *pseudo-inverses* if, for $x : X^?$ and $y : Y^?$, $\mathcal{M}\mathcal{N}\mathcal{M}(x) = \mathcal{M}(x)$ and $\mathcal{N}\mathcal{M}\mathcal{N}(y) = \mathcal{N}(y)$.

Theorem 4.13. *Let* A *and* B *be categories.*

(a) *If* A *and* B *are* (A, B)*-bicapsules and* $\mathcal{M} : \mathsf{A} \to \mathsf{B}$ *and* $\mathcal{N} : \mathsf{B} \to \mathsf{A}$ *are* (A, B)*-morphisms that are pseudo-inverses, then* $\mathcal{F} : \mathsf{B} \dashv_\Psi \mathsf{A} : \mathcal{G}$ *where*

$$\begin{aligned} \mathcal{F} &: \mathsf{B} \to \mathsf{A}, \quad \mathcal{F}(b) := \mathbb{1}_\mathsf{A} \cdot b, \\ \mathcal{G} &: \mathsf{A} \to \mathsf{B}, \quad \mathcal{G}(a) := a \cdot \mathbb{1}_\mathsf{B}, \end{aligned}$$

and for $x : \mathsf{A}_1(\mathcal{F}(U), V)$ *and* $y : \mathsf{B}_1(U, \mathcal{G}(V))$ *the bijections* Ψ_{UV} *and* Ψ_{UV}^{-1} *are given by*

$$\Psi_{UV}(x) := \mathcal{M}(x) \qquad\qquad \Psi_{UV}^{-1}(x) := \mathcal{N}(y).$$

(b) *If* $\mathcal{F} : \mathsf{B} \dashv_\Psi \mathsf{A} : \mathsf{G}$ *is an adjoint functor pair, then* A *and* B *are* (A, B)*-bicapsules with actions defined by*

$$a \cdot y := \mathcal{G}(a)y \quad \text{and} \quad x \cdot b := x\mathcal{F}(b)$$

for $a, x : \mathsf{A}$ *and* $b, y : \mathsf{B}$*. Furthermore,* Ψ *yields a pair of* (A, B)*-morphisms* $\mathcal{M} : \mathsf{A} \to \mathsf{B}$ *and* $\mathcal{N} : \mathsf{B} \to \mathsf{A}$ *that are pseudo-inverses, where*

$$\begin{aligned} \mathcal{M}(x) &:= \Psi_{UV}(x), & x : \mathsf{A} \cdot \mathbb{1}_\mathsf{B} &:= \bigsqcup_{\mathrm{id}_V : \mathbb{1}_\mathsf{A}} \bigsqcup_{\mathrm{id}_U : \mathbb{1}_\mathsf{B}} \mathsf{A}_1(\mathcal{F}(U), V), \\ \mathcal{N}(y) &:= \Psi_{UV}^{-1}(y), & y : \mathbb{1}_\mathsf{A} \cdot \mathsf{B} &:= \bigsqcup_{\mathrm{id}_V : \mathbb{1}_\mathsf{A}} \bigsqcup_{\mathrm{id}_U : \mathbb{1}_\mathsf{B}} \mathsf{B}_1(U, \mathcal{G}(V)). \end{aligned}$$

Proof. (a) Since A and B are (A, B)-bicapsules, by Proposition 4.6 there are functors $\mathcal{F} : \mathsf{B} \to \mathsf{A}$ and $\mathcal{G} : \mathsf{A} \to \mathsf{B}$ defining the right B-capsule A_B and the left A-capsule ${}_\mathsf{A}\mathsf{B}$ respectively. Since $\mathcal{M}$ and $\mathcal{N}$ are pseudo-inverses and capsule actions are full, $\mathcal{M}$ inverts $\mathcal{N}$ on $\mathsf{A} \cdot \mathbb{1}_\mathsf{B}$ and $\mathcal{N}$ inverts $\mathcal{M}$ on $\mathbb{1}_\mathsf{A} \cdot \mathsf{B}$. For objects U of B and V of A, let $e = \mathrm{id}_U$ and $f = \mathrm{id}_V$, so that $\mathsf{A}_1(\mathcal{F}(U), V) = f\mathsf{A} \cdot e$ and $\mathsf{B}_1(U, \mathcal{G}(V)) = f \cdot \mathsf{B}e$. Define $\Psi_{UV}(x) := \mathcal{M}(x)$ for $x : \mathsf{A}_1(\mathcal{F}(U), V)$. For $y : \mathsf{B}_1(U, \mathcal{G}(V))$, the map $y \mapsto \mathcal{N}(y)$ inverts Ψ_{UV}, so the result follows.

(b) By Proposition 4.6, we can exchange functors for capsules, so $\mathcal{F} : \mathsf{B} \to \mathsf{A}$ affords a right B-capsule A_B. We enrich this action by adding the left regular action by A to produce an (A, B)-bicapsule ${}_\mathsf{A}\mathsf{A}_\mathsf{B}$. We do likewise with $\mathcal{G} : \mathsf{A} \to \mathsf{B}$ producing a second (A, B)-capsule ${}_\mathsf{A}\mathsf{B}_\mathsf{B}$.

To encode Ψ, we define an (A, B)-bimorphism $\mathcal{M} : \mathsf{A} \to \mathsf{B}$ by $\mathcal{M}(x) := \Psi_{UV}(x)$ for $x : A_1(\mathcal{F}(U), V)$. This defines $\mathcal{M}$ on

$$\bigsqcup_{U : \mathsf{B}_0} \bigsqcup_{V : \mathsf{A}_0} \mathsf{A}_1(\mathcal{F}(U), V) = \bigsqcup_{e : \mathbb{1}_\mathsf{B}} \bigsqcup_{f : \mathbb{1}_\mathsf{A}} f\mathsf{A} \cdot e = \mathsf{A} \cdot \mathbb{1}_\mathsf{B}.$$

For all other values, $\mathcal{M}$ is undefined. Now (4.3) shows that on $\mathsf{A} \cdot \mathbb{1}_{\mathsf{B}}$ with $a : \mathsf{A}_1(V, Y)$, $b : \mathsf{B}_1(X, U)$, and $x : \mathsf{A}_1(\mathcal{F}(U), V)$,

$$\mathcal{M}(ax \cdot b) = \Psi_{UV}(ax\mathcal{F}(b)) = \mathcal{G}(a)\Psi_{XY}(x)b = a \cdot \mathcal{M}(x)b,$$

so $\mathcal{M}$ is an (A, B)-bimorphism. We define $\mathcal{N} : \mathsf{B} \to \mathsf{A}$ analogously: if $y : \mathbb{1}_{\mathsf{A}} \cdot \mathsf{B}$, then $\mathcal{N}(y) := \Psi^{-1}(y)$ (for suitable subscripts of Ψ), and otherwise $\mathcal{N}(y)$ is undefined. Therefore, for $x : \mathsf{A} \cdot \mathbb{1}_{\mathsf{B}}$ and $y : \mathbb{1}_{\mathsf{A}} \cdot \mathsf{B}$,

$$\begin{aligned}(\mathcal{M}\mathcal{N}\mathcal{M})(x) &= \Psi(\Psi^{-1}(\Psi(x))) = \Psi(x) = \mathcal{M}(x)\\ (\mathcal{N}\mathcal{M}\mathcal{N})(y) &= \Psi^{-1}(\Psi(\Psi^{-1}(y))) = \Psi^{-1}(y) = \mathcal{N}(y).\end{aligned}$$ □

4.6. A computational model for natural transformations

We use the algebraic perspective of Section 3.6 to discuss briefly a model for computing with natural transformations. The next definition formalizes how to treat morphisms of a category as functors between two other categories.

Definition 4.14. Let N, A and B be abstract categories. A *natural map* of N from A to B consists of functions $\cdot : \mathbb{1}_{\mathsf{N}} \times \mathsf{A} \to \mathsf{B}$ and $\bullet : \mathsf{N} \times \mathbb{1}_{\mathsf{A}} \to \mathsf{B}$ that satisfy the following properties:

(1) $(\forall x, y : \mathsf{A})$ $(\forall e : \mathbb{1}_{\mathsf{N}})$ $e \cdot (xy) \succeq (e \cdot x)(e \cdot y)$;
(2) $(\forall x : \mathsf{A})$ $(\forall e : \mathbb{1}_{\mathsf{N}})$ $e \cdot (x\blacktriangleleft) = (e \cdot x)\blacktriangleleft$ and $e \cdot (\blacktriangleleft x) = \blacktriangleleft(e \cdot x)$;
(3) $(\forall x : \mathsf{A})$ $(\forall s : \mathsf{N})$ $(s \bullet (\blacktriangleleft x))((s\blacktriangleleft) \cdot x) = ((\blacktriangleleft s) \cdot x)(s \bullet (x\blacktriangleleft))$;
(4) $(\forall f : \mathbb{1}_{\mathsf{A}})$ $(\forall s, t : \mathsf{N})$ $(st) \bullet f \succeq (s \bullet f)(t \bullet f)$.

The use of $\succeq$ in (1) and (4) depends only on xy and st, respectively, being defined. For the composition signature Ω from (3.2), conditions (1) and (2) imply that there is a function $\mathbb{1}_{\mathsf{N}} \to \mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$ given by $e \mapsto (x \mapsto e \cdot x)$ where $\mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$ is the type of morphisms between abstract categories; see also Definition 3.10. This function $\mathbb{1}_{\mathsf{N}} \to \mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$ enables us to treat the objects of N as functors from A to B. As illustrated in Example 4.15, conditions (3) and (4) are equivalent to the commutative diagrams in Figure 3 in the shaded $(2, 2)$ and $(3, 1)$ entries, respectively.

Example 4.15. We illustrate how the four conditions of Definition 4.14 translate to categories with objects and morphisms. Let A and B be two such categories, and let Ω be the composition signature from (3.2). Then $\mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$ is the type of functors from A to B. Let N be the category whose objects are the functors in $\mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$ and whose morphisms are natural transformations. Let $\eta : \mathcal{F} \Rightarrow \mathcal{G}$ be a natural transformation between $\mathcal{F}, \mathcal{G} : \mathrm{Hom}_{\Omega}(\mathsf{A}, \mathsf{B})$. Treating N as an abstract category, the guards are defined as follows: $\eta\blacktriangleleft := (\mathrm{id}_{\mathcal{F}} : \mathcal{F} \Rightarrow \mathcal{F})$ and $\blacktriangleleft\eta := (\mathrm{id}_{\mathcal{G}} : \mathcal{G} \Rightarrow \mathcal{G})$. Define $\cdot : \mathbb{1}_{\mathsf{N}} \times \mathsf{A} \to \mathsf{B}$ by $(\mathrm{id}_{\mathcal{F}}, \varphi) \longmapsto \mathcal{F}(\varphi)$, and $\bullet : \mathsf{N} \times \mathbb{1}_{\mathsf{A}} \to \mathsf{B}$ by $(\eta, \mathrm{id}_X) \longmapsto \eta_X$. Now the conditions of Definition 4.14 become:

(1) $(\forall a, b : \mathsf{A})$ $(\forall\, \mathrm{id}_{\mathcal{F}} : \mathbb{1}_{\mathsf{N}})$ $\mathcal{F}(ab) \succeq \mathcal{F}(a)\mathcal{F}(b)$;
(2) $(\forall a : \mathsf{A})$ $(\forall\, \mathrm{id}_{\mathcal{F}} : \mathbb{1}_{\mathsf{N}})$ $\mathcal{F}(a\blacktriangleleft) = (\mathcal{F}(a))\blacktriangleleft$ and $\mathcal{F}(\blacktriangleleft a) = \blacktriangleleft(\mathcal{F}(a))$;
(3) $(\forall (a : X \to Y) : \mathsf{A})$ $(\forall (\eta : \mathcal{F} \Rightarrow \mathcal{G}) : \mathsf{N})$ $\eta_Y\mathcal{F}(a) = \mathcal{G}(a)\eta_X$;
(4) $(\forall\, \mathrm{id}_X : \mathbb{1}_{\mathsf{A}})$ $(\forall \eta, \epsilon : \mathsf{N})$ $(\eta\epsilon)_X \succeq \eta_X\epsilon_X$. □

The theory of functors and natural transformations is equivalent to that of natural maps on abstract categories, but the latter allows us to use multiple encodings of functors and natural transformations such as those available in computer algebra systems. If, for example, we compute the derived subgroup $\gamma_2(G)$ of a group G in Magma, then the system may use an encoding for $\gamma_2(G)$ that differs from that supplied for G. In such cases, Magma also returns an inclusion homomorphism $\lambda_G : \gamma_2(G) \hookrightarrow G$.

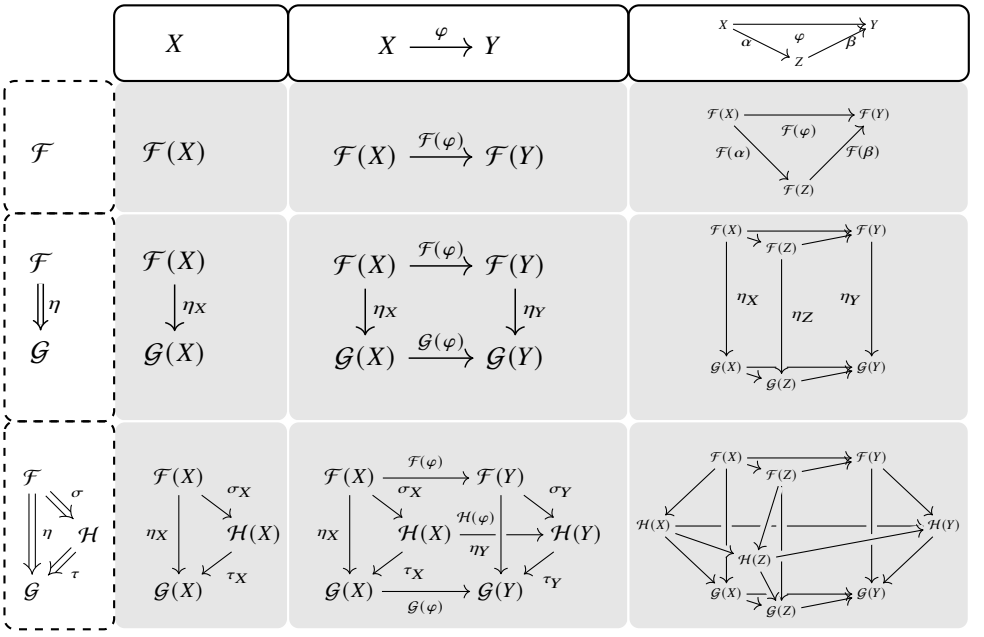


Figure 3: A natural map of N (displayed in the left dotted column) from A (displayed in top row) to B (shaded gray)

5. The Extension Theorem

One of our goals is a categorification of characteristic subgroups and their analogues in varieties of algebraic structures. We start by translating the characteristic condition into the language of natural transformations.

5.1. Natural transformations express characteristic subgroups

Suppose that H is a characteristic subgroup of a group G. Hence, every automorphism $\varphi : G \to G$ restricts to an automorphism $\varphi|_H : H \to H$ of H. In categorical terms, we now treat $\mathsf{A} := \mathsf{Aut}(G)$ as the subcategory of Grp consisting of a single object G and all isomorphisms $G \to G$. Likewise, we treat $\mathsf{B} := \mathsf{Aut}(H)$ as a subcategory of Grp. The restriction defines a functor $C : \mathsf{A} \to \mathsf{B}$. Of course, $\mathsf{Aut}(G)$ and $\mathsf{Aut}(H)$ are also groups and C is a group homomorphism, but the discussion below justifies the functor language.

Now we use the fact that H is a subgroup of G (by using the inclusion map $\rho_G : H \hookrightarrow G$). That $\varphi(H)$ is a subgroup of H can be expressed as $\varphi\rho_G = \rho_G\varphi|_H = \rho_G C(\varphi)$. Recognizing the different categories, we use the inclusion functors $\mathcal{I} : \mathsf{A} \to \mathsf{Grp}$ and $\mathcal{J} : \mathsf{B} \to \mathsf{Grp}$ to deduce the following:

$$\mathcal{I}(\varphi)\rho_G = \rho_G \mathcal{J} C(\varphi).$$

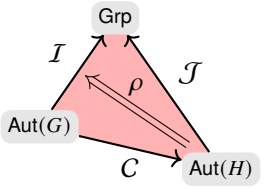
Thus, a characteristic subgroup determines a natural transformation

$$\rho : \mathcal{J}C \Rightarrow \mathcal{I}.$$

The next definition generalizes Definition 1.1.

Definition 5.1. Fix a variety E with subcategories A and B and inclusion functors $\mathcal{I} : \mathsf{A} \to \mathsf{E}$ and $\mathcal{J} : \mathsf{B} \to \mathsf{E}$. A *counital* is a natural transformation $\rho : \mathcal{J}C \Rightarrow \mathcal{I}$ for some functor $C : \mathsf{A} \to \mathsf{B}$. The counital $\rho : \mathcal{J}C \Rightarrow \mathcal{I}$ is *monic* if ρ_X is a monomorphism for all objects X in A.

A common way to illustrate categories, functors, and natural transformations uses a 2-dimensional diagram where categories are vertices, functors are directed edges, and natural transformations are oriented 2-cells. The next diagram illustrates the counital discussed above.



We now generalize the notion of a characteristic subgroup to an arbitrary algebra in a variety.

Definition 5.2. Let E be a variety and $G, H : \mathsf{E}$. Let A be a subcategory of E whose objects are those of E. We denote by $\mathsf{A}(G)$ the full subcategory of A with a single object G. Let $\mathcal{I} : \mathsf{A}(G) \to \mathsf{A}$ and $\mathcal{J} : \mathsf{A}(H) \to \mathsf{A}$ be inclusions. A monomorphism $\iota : H \hookrightarrow G$ is A-*invariant* if there is a functor $C : \mathsf{A}(G) \to \mathsf{A}(H)$ and a monic counital $\eta : \mathcal{J}C \Rightarrow \mathcal{I}$ such that η_G is equivalent to ι (see Section 3.9 for the definition of equivalence).

Using the language of Definition 5.2, a characteristic subgroup H of a group G determines and is determined by a $\overleftrightarrow{\mathsf{Grp}}$-invariant monomorphism $H \hookrightarrow G$. For fully invariant subgroups, the corresponding monomorphism is Grp-invariant.

5.2. The extension problem and representation theory

In Section 5.1, we observed that a characteristic subgroup H of G determines a functor $C : \mathsf{A} \to \mathsf{B}$ and a natural transformation $\rho : \mathcal{J}C \Rightarrow \mathcal{I}$, where A and B are categories with one object, namely G and H respectively. If a group $\hat{G}$ is isomorphic to G, then, by Fact 1.2, $\hat{G}$ has a characteristic subgroup corresponding to H. It seems plausible that we may be able to extend the functor C to more groups and, hence, to larger categories. We now make this notion of extension precise and generalize it to the setting of varieties of algebras.

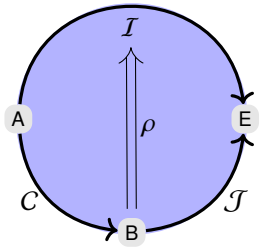
Fix a variety E. Let A, B, and C be subcategories of E where $\mathsf{A} \leqslant \mathsf{C}$. We have inclusion functors $\mathcal{I} : \mathsf{A} \to \mathsf{E}$, $\mathcal{J} : \mathsf{B} \to \mathsf{E}$, $\mathcal{K} : \mathsf{C} \to \mathsf{E}$ and $\mathcal{L} : \mathsf{A} \to \mathsf{C}$ such that $\mathcal{I} = \mathcal{K}\mathcal{L}$. Suppose that $\rho : \mathcal{J}C \Rightarrow \mathcal{I}$ is a monic counital as depicted in Figure 4(a). The extension problem asks whether there is a functor $\mathcal{D} : \mathsf{C} \to \mathsf{E}$ and a natural transformation $\sigma : \mathcal{D} \Rightarrow \mathcal{K}$ such that

$$\rho_X = \sigma_{\mathcal{L}(X)}\tau_X \tag{5.1}$$

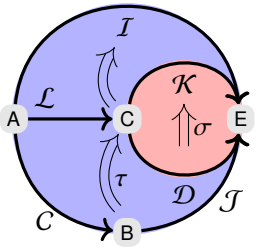
for some invertible morphism $\tau_X : \mathcal{J}C(X) \to \mathcal{D}\mathcal{L}(X)$ for all objects X of A. This is depicted in Figure 4(b).

For now, we are concerned only with the existence and construction of such extensions. For use within an isomorphism test, it will be necessary to develop tools to compute efficiently with categories; the data types of Section 4.6 are designed for that purpose.

In light of Proposition 4.10, we can explore the natural transformations from Figure 4 through the lens of actions. Recall that concatenation always denotes regular actions. The natural transformation ρ defined above is encoded as an A-bimorphism $\mathcal{R} : \mathsf{A} \to \mathsf{E}$, where $\rho = \mathcal{R}(\mathbb{1}_{\mathsf{A}})$, and this bimorphism defines a cyclic A-bicapsule $\Delta := \mathsf{A}\rho \cdot \mathsf{A}$ via (4.2), which we fix throughout.



(a) A diagram of a counital



(b) A diagram of an extension

Figure 4: Extending a counital

Our goal in part is to extend the cyclic A-bicapsule Δ to a cyclic C-bicapsule Σ. Specifically, we will define $\Sigma := \mathsf{C}\sigma \cdot \mathsf{C}$, where $\sigma : \mathcal{D} \Rightarrow \mathcal{K}$ is depicted in Figure 4(b). This is the content of Theorem 5.4, but given in the general setting of algebras in a variety. By construction (Proposition 4.10), the left actions on Δ and Σ are regular; hence, we focus on right actions.

Example 5.3. For the purposes of illustration, we consider a familiar construction that is similar to our context, namely Frobenius reciprocity and Morita condensation [30, Theorem 25A.19]. Here E is a ring, and A and C are subrings. Considering a Peirce decomposition of E, let $\mathbb{1}_A$ and $\mathbb{1}_C$ be idempotents in E such that $\mathbb{1}_A\mathbb{1}_C = \mathbb{1}_A = \mathbb{1}_C\mathbb{1}_A$. Then $C = \mathbb{1}_C E \mathbb{1}_C$ is a (non-unital) subring of E, and $A = \mathbb{1}_A E \mathbb{1}_A$ is a subring of both C and E. Furthermore, $\mathbb{1}_A E \mathbb{1}_C = \mathbb{1}_A C$ is an (A, C)-bimodule and $C\mathbb{1}_A = \mathbb{1}_C E \mathbb{1}_A$ is a (C, A)-bimodule. Suppose Δ is a right A-module and Σ a right C-module. The theory of induction and restriction provides us, respectively, with a right C-module and a right A-module: namely,

$$\mathrm{Ind}_A^C(\Delta) := \Delta \otimes_A (\mathbb{1}_A C) \quad \text{and} \quad \mathrm{Res}_A^C(\Sigma) := \Sigma \otimes_C (C\mathbb{1}_A).$$

Thus, $A \to (\mathbb{1}_A C) \otimes_C (C\mathbb{1}_A)$ yields a map $\Delta \cong \Delta \otimes_A A \to \mathrm{Res}_A^C(\mathrm{Ind}_A^C(\Delta))$. If, for example, $C\mathbb{1}_A C = C$, then $\Delta \cong \mathrm{Res}_A^C(\mathrm{Ind}_A^C(\Delta))$. □

Guided by the Peirce decomposition from Example 5.3, we seek similar constructions for categories and capsules. Recall that E contains a subcategory C that contains a subcategory A. This containment implies that $\mathbb{1}_\mathsf{A}$ is contained in (or rather embeds under the inclusion functors into) $\mathbb{1}_\mathsf{C}$. The bicapsule action of A on Δ induces a C-bicapsule, denoted $\mathrm{Ind}_\mathsf{A}^\mathsf{C}(\Delta)$. By mimicking modules, we can consider a formal extension process. We form the type $\Delta \otimes_\mathsf{A} \mathsf{C}$ whose terms are pairs, denoted $\delta \otimes c$ for $\delta : \Delta$ and $c : \mathsf{C}$, subject to the equivalence relation $(\delta \cdot a) \otimes c = \delta \otimes (ac)$. Then we equip this type with the right C-action $(\delta \otimes c) \cdot c' = \delta \otimes (cc')$. Defining $\mathsf{A}\backslash\mathsf{C} := \{\mathsf{A}c \mid c : \mathsf{C}\}$, we write

$$\Delta \otimes_\mathsf{A} \mathsf{C} := \coprod_{\mathsf{A}c : \mathsf{A}\backslash\mathsf{C}} \Delta \otimes_\mathsf{A} \mathsf{A}c.$$

We return to this construction in Section 8. Finally, since $\Delta = \mathsf{A}\rho \cdot \mathsf{A}$ and C are both subtypes of E, the product in E defines a map $\Delta \times \mathsf{C} \to \mathsf{E}$ that factors through $\Delta \otimes_\mathsf{A} \mathsf{C}$. The image of the map is a cyclic C-bicapsule Σ embedded in E, with corresponding C-bimorphism $\mathcal{S} : \mathsf{C} \to \mathsf{E}$. The following theorem states that this is always possible if A is full in C. Table 3 summarizes some of the notation fixed throughout this section.

Theorem 5.4 (Extension)**.** *Let* $\mathsf{E}, \mathsf{C}, \mathsf{A}, \Delta$ *be as in Table 3. If* A *is full in* C*, then there is a cyclic* C*-bicapsule* Σ *on* E *and unique cyclic* A*-bicapsules* Υ, Λ *on* E *such that*

$$\Delta = \mathrm{Res}_\mathsf{A}^\mathsf{C}(\Sigma) \otimes_\mathsf{A} \Upsilon \quad \textit{and} \quad \mathrm{Res}_\mathsf{A}^\mathsf{C}(\Sigma) = \Delta \otimes_\mathsf{A} \Lambda.$$

E	variety of algebraic structures
B, C	subcategories of E
A	full subcategory of C

bimorphism	monic counital	cyclic bicapsule
$\mathcal{R} : \mathsf{A} \to \mathsf{E}$	$\rho := \mathcal{R}(\mathbb{1}_{\mathsf{A}})$	$\Delta := A\rho \cdot A$
$\mathcal{S} : \mathsf{C} \to \mathsf{E}$	$\sigma := \mathcal{S}(\mathbb{1}_{\mathsf{C}})$	$\Sigma := C\sigma \cdot C$

Table 3: Data for the proof of Theorem 5.4

We briefly describe the idea of the proof. We start with a cyclic A-bicapsule Δ with associated A-bimorphism $\mathcal{R} : \mathsf{A} \to \mathsf{E}$. We seek an extension of $\mathcal{R}$ to a C-bimorphism $\mathcal{S} \colon \mathsf{C} \to \mathsf{E}$ that satisfies $\mathcal{S}\mathcal{L} = \mathcal{R}$, where $\mathcal{L} \colon \mathsf{A} \to \mathsf{C}$ is the inclusion functor. If this holds, then, for every $e : \mathbb{1}_{\mathsf{A}}$ and every $c : \mathsf{C}$ with $c\blacktriangleleft = \blacktriangleleft\mathcal{R}(e)$,

$$c \cdot \mathcal{R}(e) = c \cdot \mathcal{S}\mathcal{L}(e) = \mathcal{S}(c \cdot e) = \mathcal{S}(c) = \mathcal{S}(\blacktriangleleft c) \cdot c.$$

We now derive some necessary conditions for a putative $\mathcal{S}$ of this type. Recall from (3.4) that the notation $\alpha \ll \beta$ for morphisms α and β implies that there is a morphism γ such that $\alpha = \beta\gamma$. Applying Lemma 3.20 to $c \cdot \mathcal{R}(e) = \mathcal{S}(c\blacktriangleleft) \cdot c$ yields $\operatorname{im}(c \cdot \mathcal{R}(e)) \ll \operatorname{im}(\mathcal{S}(\blacktriangleleft c))$. For $f : \mathbb{1}_{\mathsf{C}}$ define

$$\mathbb{U}_{\mathsf{C}}(f) := \bigsqcup_{e:\mathbb{1}_{\mathsf{A}}} f\mathsf{C} \cdot e.$$

The left A-actions on C and E are regular, as is the left C-action on E. Hence, for $\langle e, c\rangle : \mathbb{U}_{\mathsf{C}}(f)$,

$$c\triangleleft = (c \cdot \mathbb{1}_{\mathsf{E}})\blacktriangleleft = (c\blacktriangleleft) \cdot \mathbb{1}_{\mathsf{E}} = e \cdot \mathbb{1}_{\mathsf{E}}.$$

Therefore $c\triangleleft = e \cdot \mathbb{1}_{\mathsf{E}} = \blacktriangleleft(e \cdot \mathcal{R}(e)) = \blacktriangleleft\mathcal{R}(e) = \triangleleft\mathcal{R}(e)$, so $c \cdot \mathcal{R}(e)$ is defined. Since $\operatorname{im}(c \cdot \mathcal{R}(e)) \ll \operatorname{im}(\mathcal{S}(f))$ holds for every $\langle e, c\rangle : \mathbb{U}_{\mathsf{C}}(f)$, we can make a single inclusion (see (3.6)):

$$\operatorname{im}\left(\bigsqcup_{\langle e,c\rangle \in \mathbb{U}_{\mathsf{C}}(f)} \operatorname{im}(c \cdot \mathcal{R}(e))\right) \ll \operatorname{im}(\mathcal{S}(f)). \tag{5.2}$$

Observe that (5.2) also holds if, instead of $\mathcal{R} = \mathcal{S}\mathcal{L}$, we assume that there exists $\mathcal{T} : \mathsf{A} \to \mathsf{E}$ such that $\mathcal{R}(a) = \operatorname{Res}^{\mathsf{C}}_{\mathsf{A}}(\mathcal{S})(a)\mathcal{T}(a\blacktriangleleft)$ for all $a : \mathsf{A}$; here $\operatorname{Res}^{\mathsf{C}}_{\mathsf{A}}(\mathcal{S})(a) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot a)$ denotes the restriction of $\mathcal{S}$ to A. This motivates us to choose $\mathcal{S}$ such that $\mathcal{S}(c)$ is defined as the left hand side of (5.2), and then solve for a suitable $\mathcal{T}$.

In the language of bimorphisms, Theorem 5.4 asserts that there exists an A-bimorphism $\mathcal{T} \colon \mathsf{A} \to \mathsf{E}$ such that, for $a : \mathsf{A}$,

$$\mathcal{R}(a) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot (\blacktriangleleft a))\mathcal{T}(a) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot a)\mathcal{T}(a\blacktriangleleft) \tag{5.3}$$

where $\mathcal{S}$ is the C-bimorphism corresponding to Σ; we use this language in its proof. The second equality in (5.3) reflects the tensor product over A shown in Theorem 5.4.

5.3. Building blocks

We prove Theorem 5.4 in Section 5.4 using the three intermediate results presented in this section.

Lemma 5.5. *Let* C *and* E *be as in Table 3. For* $\sigma : \prod_{f:\mathbb{1}_\mathsf{C}} (f \cdot \overleftrightarrow{\mathsf{E}})$*, the following are equivalent.*

(1) *There is a* C*-bicapsule* Σ *on* E *such that the function* $\mathcal{S} : \mathsf{C} \to \Sigma$ *given by* $\mathcal{S}(c) := c \cdot \sigma_{c\blacktriangleleft}$ *is a* C*-bimorphism.*

(2) *For all* $c : \mathsf{C}$*,* $c \cdot \sigma_{c\blacktriangleleft} \ll \sigma_{\blacktriangleleft c}$*.*

Proof. We assume (1) holds and prove (2). By Proposition 4.10(b), there exists a unique functor $\mathcal{G} : \mathsf{C} \to \mathsf{E}$ that induces the action of C on the right of E. Since $\mathcal{S}$ is a function and a C-bimorphism by assumption, $c\triangleleft = \triangleleft\sigma_{c\blacktriangleleft}$ for all $c : \mathsf{C}$, and

$$c \cdot \sigma_{c\blacktriangleleft} = \mathcal{S}(c) = \mathcal{S}((\blacktriangleleft c) \cdot c) = \mathcal{S}(\blacktriangleleft c) \cdot c = ((\blacktriangleleft c) \cdot \sigma_{(\blacktriangleleft c)\blacktriangleleft}) \cdot c = \sigma_{\blacktriangleleft c}\mathcal{G}(c).$$

Thus, (2) holds.

We now assume (2) holds and prove (1). First, we show that $x : \mathsf{E}$ satisfying $c \cdot \sigma_{c\blacktriangleleft} = \sigma_{\blacktriangleleft c}x$ is unique. Suppose $y : \mathsf{E}$ satisfies $c \cdot \sigma_{c\blacktriangleleft} = \sigma_{\blacktriangleleft c}y$, so $\sigma_{\blacktriangleleft c}x = \sigma_{\blacktriangleleft c}y$. Since $\sigma_{\blacktriangleleft c}$ is a monomorphism, $x = y$. We denote this unique morphism by $u_c : \mathsf{E}$. Since $\sigma_{\blacktriangleleft c}u_c$ is defined for all $c : \mathsf{C}$,

$$\blacktriangleleft u_{\blacktriangleleft c} = (\sigma_{\blacktriangleleft(\blacktriangleleft c)})\blacktriangleleft = (\sigma_{\blacktriangleleft c})\blacktriangleleft = \blacktriangleleft u_c.$$

Next, we define a right C-capsule structure on E as follows. Let $\triangleleft(-) : \mathsf{C} \to \mathbb{1}_\mathsf{E}$ be given by $\triangleleft c := \blacktriangleleft u_c$, and let $(-)\triangleleft : \mathsf{E} \to \mathbb{1}_\mathsf{E}$ be given by $x\triangleleft := x\blacktriangleleft$. For all $c : \mathsf{C}$ and $x : \mathsf{E}$, let $x \cdot c := xu_c$, which is defined if, and only if, $x\blacktriangleleft = \blacktriangleleft u_c$. Condition (2) of Definition 4.1 follows from $\triangleleft(\blacktriangleleft c) = \blacktriangleleft u_{\blacktriangleleft c} = \blacktriangleleft u_c = \triangleleft c$ and $u_e : \mathbb{1}_\mathsf{E}$ for all $e : \mathbb{1}_\mathsf{C}$ since σ_e is monic. Lastly, let $c, d : \mathsf{C}$ with $c\blacktriangleleft = \blacktriangleleft d$. Now $(cd) \cdot \sigma_{(cd)\blacktriangleleft} = \sigma_{\blacktriangleleft(cd)}u_{cd} = \sigma_{\blacktriangleleft c}u_{cd}$ and, since we have a regular left action,

$$(cd) \cdot \sigma_{(cd)\blacktriangleleft} = c \cdot (d \cdot \sigma_{(cd)\blacktriangleleft}) = c \cdot (d \cdot \sigma_{d\blacktriangleleft}) = c \cdot \sigma_{\blacktriangleleft d}u_d = \sigma_{\blacktriangleleft c}u_cu_d.$$

Since $\sigma_{\blacktriangleleft c}$ is a monomorphism, $u_{cd} = u_cu_d$. Hence, this defines a right C-capsule on E since $\triangleleft c = \blacktriangleleft u_c : \mathbb{1}_\mathsf{E}$ for all $c : \mathsf{C}$. Since C acts regularly on E on the left, there exists a C-bicapsule Σ on E by Proposition 4.6, with the regular left and right actions just defined. Finally, we prove that $\mathcal{S}$ is a C-bimorphism. For all $c, x, y : \mathsf{C}$,

$$\mathcal{S}(cx) = (cx) \cdot \sigma_{(cx)\blacktriangleleft} = (cx) \cdot \sigma_{x\blacktriangleleft} = c \cdot (x \cdot \sigma_{x\blacktriangleleft}) = c \cdot \mathcal{S}(x),$$

provided $c\blacktriangleleft = \blacktriangleleft x$. If $y\blacktriangleleft = \blacktriangleleft c$, then

$$\begin{aligned}\mathcal{S}(yc) &= (yc) \cdot \sigma_{(yc)\blacktriangleleft} = (yc) \cdot \sigma_{c\blacktriangleleft} = y \cdot (c \cdot \sigma_{c\blacktriangleleft}) = y \cdot (\sigma_{\blacktriangleleft c}u_c) = (y \cdot \sigma_{y\blacktriangleleft})u_c \\ &= \mathcal{S}(y) \cdot c.\end{aligned}$$

□

Lemma 5.6. *For* $\mathsf{E}, \mathsf{C}, \mathcal{R}$ *as in Table 3, define* $\sigma : \coprod_{f:\mathbb{1}_\mathsf{C}} (f \cdot \overleftrightarrow{\mathsf{E}})$ *via*

$$\sigma_f := \mathrm{im}\left(\coprod_{\langle e,x\rangle : \mathbb{U}_\mathsf{C}(f)} \mathrm{im}(x \cdot \mathcal{R}(e)) \right).$$

For each $c : \mathsf{C}$*, there is a unique* $y : \mathsf{E}$ *satisfying* $c \cdot \sigma_{c\blacktriangleleft} = \sigma_{\blacktriangleleft c}y$*.*

Proof. Let $c : \mathsf{C}$, so $c\triangleleft = c\blacktriangleleft$, and $c\blacktriangleleft = \triangleleft\sigma_{c\blacktriangleleft}$ by definition of σ. We show that $c \cdot \sigma_{c\blacktriangleleft} \ll \sigma_{\blacktriangleleft c}$. By Lemma 3.19,

$$(\forall \langle e, x\rangle : \mathbb{U}_\mathsf{C}(f)) \qquad c \cdot \mathrm{im}(x \cdot \mathcal{R}(e)) \ll \mathrm{im}(c \cdot (x \cdot \mathcal{R}(e))) = \mathrm{im}((cx) \cdot \mathcal{R}(e)).$$

Thus, by Fact 3.21(d),

$$\coprod_{\langle e,x\rangle:\mathbb{U}_{\mathsf{C}}(f)} (c \cdot \mathrm{im}(x \cdot \mathcal{R}(e))) \ll \coprod_{\langle e,x\rangle:\mathbb{U}_{\mathsf{C}}(f)} \mathrm{im}((cx) \cdot \mathcal{R}(e)). \tag{5.4}$$

Therefore, using (3.6),

$$\begin{aligned} c \cdot \mathrm{im}\left(\coprod_{\langle e,x\rangle} \mathrm{im}(x \cdot \mathcal{R}(e))\right) &\ll \mathrm{im}\left(c \cdot \coprod_{\langle e,x\rangle} \mathrm{im}(x \cdot \mathcal{R}(e))\right) && \text{(Lemma 3.19)} \\ &= \mathrm{im}\left(\coprod_{\langle e,x\rangle} (c \cdot \mathrm{im}(x \cdot \mathcal{R}(e)))\right) && \text{(Fact 3.21(c))} \\ &\ll \mathrm{im}\left(\coprod_{\langle e,x\rangle} \mathrm{im}((cx) \cdot \mathcal{R}(e))\right) && \text{(Equation (5.4))} \end{aligned}$$

where all of the coproducts are over $\langle e,x\rangle : \mathbb{U}_{\mathsf{C}}(c\blacktriangleleft)$. By Fact 3.21(e),

$$\mathrm{im}\left(\coprod_{\langle e,x\rangle:\mathbb{U}_{\mathsf{C}}(c\blacktriangleleft)} \mathrm{im}((cx) \cdot \mathcal{R}(e))\right) \ll \mathrm{im}\left(\coprod_{\langle e,z\rangle:\mathbb{U}_{\mathsf{C}}(\blacktriangleleft c)} \mathrm{im}(z \cdot \mathcal{R}(e))\right).$$

Putting this together, we deduce that

$$c \cdot \sigma_{c\blacktriangleleft} = c \cdot \mathrm{im}\left(\coprod_{\langle e,x\rangle:\mathbb{U}_{\mathsf{C}}(c\blacktriangleleft)} \mathrm{im}(x \cdot \mathcal{R}(e))\right) \ll \mathrm{im}\left(\coprod_{\langle e,z\rangle:\mathbb{U}_{\mathsf{C}}(\blacktriangleleft c)} \mathrm{im}(z \cdot \mathcal{R}(e))\right) = \sigma_{\blacktriangleleft c},$$

so $c \cdot \sigma_{c\blacktriangleleft} = \sigma_{c\blacktriangleleft} y$ for some $y : \mathsf{E}$. Since $\sigma_{\blacktriangleleft c}$ is monic, y is unique. □

Proposition 5.7. *Let* $\mathsf{E}, \mathsf{C}, \mathsf{A}, \mathcal{R}$ *be as in Table 3. If* A *is full in* C*, then* $\mathcal{S} : \mathsf{C} \to \mathsf{E}$ *defined by*

$$\mathcal{S}(c) := c \cdot \mathrm{im}\left(\coprod_{\langle e,x\rangle:\mathbb{U}_{\mathsf{C}}(c\blacktriangleleft)} \mathrm{im}(x \cdot \mathcal{R}(e))\right)$$

is a C*-bimorphism, and there exists a unique* $\lambda : \prod_{f:\mathbb{1}_{\mathsf{A}}} f \overleftrightarrow{\mathsf{E}} f$ *such that for all* $a : \mathsf{A}$*,*

$$\mathcal{R}(a) = \mathcal{S}(a \cdot \mathbb{1}_{\mathsf{C}})\lambda_{a\blacktriangleleft} \quad \text{and} \quad \mathcal{S}(a \cdot \mathbb{1}_{\mathsf{C}}) = \mathcal{R}(a)\lambda_{a\blacktriangleleft}^{-1}.$$

Proof. Take $e, f : \mathbb{1}_{\mathsf{A}}$, and recall that A acts regularly on both the left and right of C. Since A is full in C, these actions are full, so

$$f \cdot \mathsf{C} \cdot e = \mathbb{1}_{\mathsf{C}} \cdot (f\mathsf{A}e) = (f\mathsf{A}e) \cdot \mathbb{1}_{\mathsf{C}}.$$

Since the left actions of A on C and on E and the left action of C on E are regular, for each $a : \mathsf{A}$ and $x : \mathsf{E}$ with $a\triangleleft = \triangleleft x$,

$$(a \cdot \mathbb{1}_{\mathsf{C}}) \cdot x = a \cdot x. \tag{5.5}$$

Fix $a : \mathsf{A}$. Set $c = a \cdot \mathbb{1}_{\mathsf{C}}$, so $(c\blacktriangleleft)\mathsf{C} = (a\blacktriangleleft) \cdot \mathsf{C}$. Thus, since the A-action on C is full,

$$\mathbb{U}_{\mathsf{C}}(c\blacktriangleleft) := \bigsqcup_{e:\mathbb{1}_{\mathsf{A}}} ((c\blacktriangleleft)\mathsf{C} \cdot e) = \bigsqcup_{e:\mathbb{1}_{\mathsf{A}}} ((a\blacktriangleleft) \cdot \mathsf{C} \cdot e) = ((a\blacktriangleleft)\mathsf{A}) \cdot \mathbb{1}_{\mathsf{C}}, \tag{5.6}$$

where $(a\blacktriangleleft)\mathsf{A}$ acts on $\mathbb{1}_\mathsf{C}$ in the final expression. Therefore

$$\begin{aligned}
\mathcal{S}(a\cdot\mathbb{1}_\mathsf{C}) &= a\cdot\operatorname{im}\left(\coprod_{\langle e,x\rangle:\mathbb{U}_\mathsf{C}((a\blacktriangleleft)\cdot\mathbb{1}_\mathsf{C})}\operatorname{im}(x\cdot\mathcal{R}(e))\right) && \text{(Equation (5.5))}\\
&= a\cdot\operatorname{im}\left(\coprod_{a':(a\blacktriangleleft)\mathsf{A}}\operatorname{im}(a'\cdot\mathcal{R}(a'\blacktriangleleft))\right) && \text{(Equation (5.6))}\\
&= a\cdot\operatorname{im}\left(\coprod_{a':(a\blacktriangleleft)\mathsf{A}}\operatorname{im}(\mathcal{R}(a\blacktriangleleft)\cdot a')\right) && \text{(A-bimorphism, $\blacktriangleleft a'=a\blacktriangleleft$)}\\
&\ll a\cdot\mathcal{R}(a\blacktriangleleft)=\mathcal{R}(a). && \text{(Lemma 3.20, Fact 3.21(c))}
\end{aligned}$$

For the application of Lemma 3.20 in the last step, recall that $\mathcal{R}(e)$ is monic for $e:\mathsf{A}$ by our assumption (Table 3).

We establish the other direction as follows:

$$\begin{aligned}
\mathcal{R}(a\blacktriangleleft) &\ll \operatorname{im}(\mathcal{R}(a\blacktriangleleft))=\operatorname{im}((a\blacktriangleleft)\cdot\mathcal{R}(a\blacktriangleleft)) && \text{(Theorem 3.18)}\\
&\ll \coprod_{a':(a\blacktriangleleft)\mathsf{A}}\operatorname{im}(a'\cdot\mathcal{R}(a'\blacktriangleleft)) && \text{(Fact 3.21(e))}\\
&\ll \operatorname{im}\left(\coprod_{a':(a\blacktriangleleft)\mathsf{A}}\operatorname{im}(a'\cdot\mathcal{R}(a'\blacktriangleleft))\right). && \text{(Theorem 3.18)}
\end{aligned}$$

Acting with $a:\mathsf{A}$ from the left, we obtain $\mathcal{R}(a)\ll\mathcal{S}(a\cdot\mathbb{1}_\mathsf{C})$.

From both computations, there exist $\lambda,\mu:\prod_{f:\mathbb{1}_\mathsf{A}}f\mathsf{E}f$ such that

$$\mathcal{R}(a)=\mathcal{S}(a\cdot\mathbb{1}_\mathsf{C})\lambda_{a\blacktriangleleft},\qquad\qquad \mathcal{S}(a\cdot\mathbb{1}_\mathsf{C})=\mathcal{R}(a)\mu_{a\blacktriangleleft}.$$

It remains to show that $\mu_{a\blacktriangleleft}=\lambda_{a\blacktriangleleft}^{-1}$ for all $a:\mathsf{A}$ and λ is unique. For all $e:\mathbb{1}_\mathsf{A}$, $\mathcal{R}(e)$ is monic by the assumptions in Theorem 5.4, and $\mathcal{S}(e\cdot\mathbb{1}_\mathsf{C})$ is also monic by the definition of $\mathcal{S}$. Since $\mathcal{R}(e)$ is monic,

$$\mathcal{R}(e)=\mathcal{S}(e\cdot\mathbb{1}_\mathsf{C})\lambda_e=\mathcal{R}(e)\mu_e\lambda_e$$

implies $\mu_e\lambda_e:\mathbb{1}_\mathsf{E}$. Similarly, $\lambda_e\mu_e:\mathbb{1}_\mathsf{E}$ because $\mathcal{S}(e\cdot\mathbb{1}_\mathsf{C})$ is monic and

$$\mathcal{S}(e\cdot\mathbb{1}_\mathsf{C})=\mathcal{R}(e)\mu_e=\mathcal{S}(e\cdot\mathbb{1}_\mathsf{C})\lambda_e\mu_e.$$

The uniqueness of λ follows since $\mathcal{R}(e)$ is monic. □

5.4. Proof of Theorem 5.4

Let $\mathcal{S}:\mathsf{C}\to\mathsf{E}$ be the C-bimorphism in Proposition 5.7. This proposition shows that there exists a unique $\lambda:\prod_{f:\mathbb{1}_\mathsf{A}}f\overleftrightarrow{\mathsf{E}}f$ such that for all $a:\mathsf{A}$,

$$\mathcal{R}(a)=\mathcal{S}(a\cdot\mathbb{1}_\mathsf{C})\lambda_{a\blacktriangleleft}. \tag{5.7}$$

Since $\mathcal{R}$ is an A-bimorphism,

$$(a\cdot\mathbb{1}_\mathsf{E})\cdot\mathcal{R}(a\blacktriangleleft)=\mathcal{R}(a)=\mathcal{R}(\blacktriangleleft a)\cdot(\mathbb{1}_\mathsf{E}\cdot a). \tag{5.8}$$

Let Σ be the C-bicapsule on E defined by the C-bimorphism $\mathcal{S}$. Both Δ and Σ are bicapsules, so applying (5.7) to (5.8) yields

$$(a \cdot \mathbb{1}_{\mathsf{E}})\mathcal{S}((a\blacktriangleleft) \cdot \mathbb{1}_{\mathsf{C}})\lambda_{a\blacktriangleleft} = \mathcal{S}((\blacktriangleleft a) \cdot \mathbb{1}_{\mathsf{C}})\lambda_{\blacktriangleleft a}(\mathbb{1}_{\mathsf{E}} \cdot a). \tag{5.9}$$

Since the left C-action on E and the left A-action on C are regular, $a \cdot \mathbb{1}_{\mathsf{E}} = (a \cdot \mathbb{1}_{\mathsf{C}}) \cdot \mathbb{1}_{\mathsf{E}}$. Thus, $(a \cdot \mathbb{1}_{\mathsf{E}})\mathcal{S}((a\blacktriangleleft) \cdot \mathbb{1}_{\mathsf{C}}) = \mathcal{S}(a \cdot \mathbb{1}_{\mathsf{C}}) = \mathcal{S}((\blacktriangleleft a) \cdot \mathbb{1}_{\mathsf{C}})(\mathbb{1}_{\mathsf{E}} \cdot (\mathbb{1}_{\mathsf{C}} \cdot a))$. Applying this to (5.9) and using the monic property of $\mathcal{S}((\blacktriangleleft a) \cdot \mathbb{1}_{\mathsf{C}})$, we deduce that

$$(\mathbb{1}_{\mathsf{E}} \cdot (\mathbb{1}_{\mathsf{C}} \cdot a))\lambda_{a\blacktriangleleft} = \lambda_{\blacktriangleleft a}(\mathbb{1}_{\mathsf{E}} \cdot a).$$

Since the actions are capsules, λ defines a natural transformation. By Proposition 4.10(a), the function $a \mapsto (\mathbb{1}_{\mathsf{E}} \cdot (\mathbb{1}_{\mathsf{C}} \cdot a))\lambda_{a\blacktriangleleft}$ defines an A-bimorphism $\mathcal{T} : \mathsf{A} \to \mathsf{E}$. Thus, $\mathcal{T}(a\blacktriangleleft) = \lambda_{a\blacktriangleleft} : \overleftrightarrow{\mathsf{E}}$, and therefore

$$\mathcal{R}(a) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot a)\mathcal{T}(a\blacktriangleleft) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot (\blacktriangleleft a))(\mathbb{1}_{\mathsf{E}} \cdot (\mathbb{1}_{\mathsf{C}} \cdot a))\mathcal{T}(a\blacktriangleleft) = \mathcal{S}(\mathbb{1}_{\mathsf{C}} \cdot (\blacktriangleleft a))\mathcal{T}(a).$$

The uniqueness of $\mathcal{T}$ follows from Proposition 4.10(b) and the uniqueness of λ. □

5.5. *Proof of Theorem 1 for varieties*

Recall that $\mathrm{Counital}(\mathsf{B}, \mathsf{E})$ denotes the type of all counitals $\iota : \mathcal{K}C \Rightarrow \mathcal{I}$, where $\mathsf{B} \leqslant \mathsf{E}$ and C are categories, $C : \mathsf{B} \to \mathsf{C}$ is a functor, and $\mathcal{I} : \mathsf{B} \to \mathsf{E}$ and $\mathcal{K} : \mathsf{C} \to \mathsf{E}$ are inclusion functors. Let $\mathrm{Unital}(\mathsf{B}, \mathsf{E})$ be the type of all unitals $\pi : \mathcal{I} \Rightarrow \mathcal{K}C$; these are the duals of counitals. Recall from Theorem 3.18 that im and coim produce categorical morphisms, and from Section 3.9 the equivalence relations on monomorphisms and epimorphisms. Invariance of monomorphisms is defined in Definition 5.2.

Our use of set theory notation in the following generalization of Theorem 1 is justified because we compare subsets of a fixed algebra.

Theorem 1-cat. *Let* E *be a variety. For every* $G : \mathsf{E}$*, the following equalities of sets hold up to equivalence:*

$$\{\iota : H \hookrightarrow G \mid \iota \textit{ is } \overleftrightarrow{\mathsf{E}}\textit{-invariant}\} = \left\{\mathrm{im}(\eta_G) \mid \eta : \mathrm{Counital}\left(\overleftrightarrow{\mathsf{E}}, \mathsf{E}\right)\right\}; \tag{1}$$

$$\{\pi : G \twoheadrightarrow Q \mid \pi \textit{ is } \overleftrightarrow{\mathsf{E}}\textit{-invariant}\} = \left\{\mathrm{coim}(\tau_G) \mid \tau : \mathrm{Unital}\left(\overleftrightarrow{\mathsf{E}}, \mathsf{E}\right)\right\}; \tag{2}$$

$$\{\iota : H \hookrightarrow G \mid \iota \textit{ is } \mathsf{E}\textit{-invariant}\} = \{\mathrm{im}(\eta_G) \mid \eta : \mathrm{Counital}(\mathsf{E}, \mathsf{E})\}; \tag{3}$$

$$\{\pi : G \twoheadrightarrow Q \mid \pi \textit{ is } \mathsf{E}\textit{-invariant}\} = \{\mathrm{coim}(\tau_G) \mid \tau : \mathrm{Unital}(\mathsf{E}, \mathsf{E})\}. \tag{4}$$

Proof. We prove (1) in detail; the proof of (3) is analogous but requires replacing $\overleftrightarrow{\mathsf{E}}$ with E. The proofs of (2) and (4) are dual to the proofs of (1) and (3), respectively. Recall that the single-object category $\mathsf{Aut}(G)$ consists of G and all its automorphisms. It is a subcategory of E and a full subcategory of $\overleftrightarrow{\mathsf{E}}$. Let $\mathcal{I} : \mathsf{Aut}(G) \to \mathsf{E}$, $\mathcal{L} : \mathsf{Aut}(G) \to \overleftrightarrow{\mathsf{E}}$, and $\mathcal{K} : \overleftrightarrow{\mathsf{E}} \to \mathsf{E}$ be the inclusion functors with $\mathcal{K}\mathcal{L} = \mathcal{I}$.

Let $\iota : H \hookrightarrow G$ be an $\overleftrightarrow{\mathsf{E}}$-invariant morphism in E. Consider the single-object category $\mathsf{Aut}(H)$ with inclusion functor $\mathcal{J} : \mathsf{Aut}(H) \to \mathsf{E}$. As in Section 5.1, we obtain a natural transformation $\rho : \mathcal{J}C \Rightarrow \mathcal{I}$ with (restriction) functor $C : \mathsf{Aut}(G) \to \mathsf{Aut}(H)$, so $\rho : \mathrm{Counital}(\mathsf{Aut}(G), \mathsf{E})$ is a monic counital.

We now use Proposition 4.10 to pass to the associated cyclic $\mathsf{Aut}(G)$-bicapsule $\Delta := \mathsf{Aut}(G) \cdot \rho \cdot \mathsf{Aut}(G)$. Recall that the left action is defined by $\mathcal{I}$, hence it is regular, and the right action is defined by $\mathcal{J}C$. By construction, Δ satisfies the conditions of Theorem 5.4 since $\mathsf{Aut}(G)$ is full in $\overleftrightarrow{\mathsf{E}}$. We extend Δ to a cyclic $\overleftrightarrow{\mathsf{E}}$-bicapsule $\Sigma = \overleftrightarrow{\mathsf{E}} \cdot \sigma \cdot \overleftrightarrow{\mathsf{E}}$ where $\sigma : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{K}$ is a monic counital extending ρ. Thus, there exists an isomorphism $\tau_G : \mathcal{J}C(G) \to \mathcal{D}\mathcal{L}(G)$ such that $\iota = \rho_G = \sigma_{\mathcal{L}(G)}\tau_G$; see (5.1). Since $\mathcal{L}$ is the

inclusion functor, there exists an isomorphism $\tau' : \mathsf{E}$ such that $\iota = \sigma_G\tau'$, so ι and σ_G are equivalent. Hence, ι and $\mathrm{im}(\sigma_G)$ are equivalent. Since $\sigma : \mathrm{Counital}(\overleftrightarrow{\mathsf{E}}, \mathsf{E})$, this proves the "$\subseteq$" part of (1).

For the converse, consider $\eta : \mathrm{Counital}(\overleftrightarrow{\mathsf{E}}, \mathsf{E})$, say $\eta : \mathcal{HD} \Rightarrow \mathcal{K}$ for some functor $\mathcal{D} : \overleftrightarrow{\mathsf{E}} \to \mathsf{C}$, subcategory $\mathsf{C} \leqslant \mathsf{E}$, and inclusion $\mathcal{H} : \mathsf{C} \to \mathsf{E}$. If $\varphi : \mathsf{Aut}(G)$, then $\mathcal{L}(\varphi) : \overleftrightarrow{\mathsf{E}}$, and so $\mathcal{KL}(\varphi)\eta_G = \eta_G\mathcal{HDL}(\varphi)$. Since $G = \mathcal{L}(G) = \mathcal{K}(G)$, the morphism $\eta_G : \mathcal{HD}(G) \to G$ is characteristic, and therefore so is its monic image $\mathrm{im}(\eta_G)$. This proves the "$\supseteq$" part of (1). □

6. Categorification of characteristic substructure

The final step in our work is to describe the source of all characteristic subgroups, and more generally of characteristic substructures in algebras in fixed varieties. In Section 5, we showed that characteristic structure arises naturally from counitals. Now we demonstrate that all counitals are derived from counits. In particular, in Section 6.3, we prove the following generalization of Theorem 2 to varieties of algebras.

Theorem 2-cat. *Fix a variety* E. *Let* G *be an object in* E *with subobject* H *and inclusion* $\iota : H \hookrightarrow G$. *There exist categories* A *and* B, *where* $\overleftrightarrow{\mathsf{E}} \leqslant \mathsf{A} \leqslant \mathsf{E}$, *such that the following are equivalent.*

(1) H *is characteristic in* G.

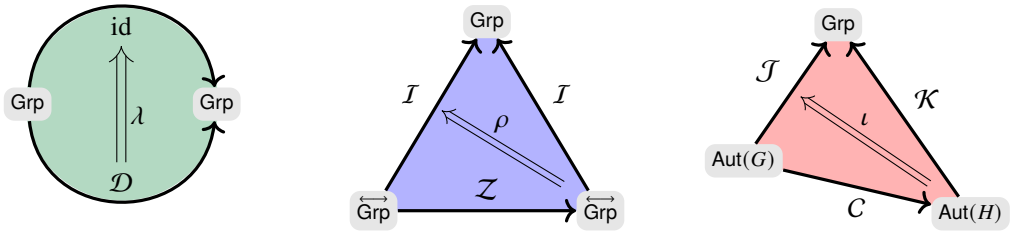
(2) *There is a functor* $C : \mathsf{A} \to \mathsf{A}$ *and a counit* $\eta : C \Rightarrow \mathrm{id}_{\mathsf{A}}$ *such that* $H = \mathrm{Im}(\eta_G)$.

(3) *There is an* (A, B)*-morphism* $\mathcal{M} : \mathsf{B} \to \mathsf{A}$ *such that* $\iota = \mathcal{M}(\mathrm{id}_G \cdot \mathbb{1}_{\mathsf{B}})$.

Our proof relies on the Extension Theorem 5.4 and additional consideration of counitals.

Definition 6.1. Fix a category E with subcategories A and B and inclusion functors $\mathcal{I} : \mathsf{A} \to \mathsf{E}$ and $\mathcal{J} : \mathsf{B} \to \mathsf{E}$. A counital $\eta : \mathcal{JC} \Rightarrow \mathcal{I}$ is *isosceles* if $\mathsf{A} = \mathsf{B}$ and $\mathcal{I} = \mathcal{J}$, and *flat* if, in addition, $\mathsf{A} = \mathsf{B} = \mathsf{E}$ and $\mathcal{I} = \mathcal{J} = \mathrm{id}_{\mathsf{E}}$. Otherwise, it is *scalene*.

Example 6.2. We mention three examples in Grp and illustrate their natural transformations in Figure 5. The first two are the derived subgroup and the center of a group G, as considered in Example 1.4. For the third example, we consider an arbitrary characteristic subgroup H of G. As discussed in Section 5.2, define $\mathsf{Aut}(G)$ to be the category with one object G and its morphisms are the automorphisms of G. Hence, $\mathsf{Aut}(G)$ and $\mathsf{Aut}(H)$ are subcategories of Grp with inclusion functors $\mathcal{J}$ and $\mathcal{K}$, respectively. We define a functor $C : \mathsf{Aut}(G) \to \mathsf{Aut}(H)$ by mapping G to H and automorphisms of G to their restriction to H, and so obtain a natural transformation $\iota : \mathcal{KC} \Rightarrow \mathcal{J}$. □



(a) The derived subgroup (b) The center (c) A characteristic subgroup

Figure 5: Natural transformations from Example 6.2

In our study of characteristic structure we use induced actions from Theorem 6.5 to pass from a scalene counital to one that is isosceles. We then work with isosceles counitals to determine an intermediate class of isosceles counitals known as *internal* counitals. Finally, we show that an internal counital is completely determined by a morphism of bicapsules.

Counits are common in many categorical contexts; for example, they occur for every adjoint functor pair. The case of flat counitals coincides precisely with the stricter class of fully-invariant substructures.

6.1. Composing counitals

In this section, we describe two ways to construct new counitals from given counitals by composing natural transformations and functors in different ways. These are two instances of a much larger theory; see [4, 27]. Figure 4 illustrates the usual composition of natural transformations. We now describe how to compose a functor with a natural transformation. Consider functors $\mathcal{F}, \mathcal{G} : \mathsf{B} \to \mathsf{A}$, $\mathcal{H} : \mathsf{C} \to \mathsf{B}$, and $\mathcal{K} : \mathsf{A} \to \mathsf{D}$ for categories A, B, C, and D, and a natural transformation $\eta : \mathcal{F} \Rightarrow \mathcal{G}$. Define $\eta\mathcal{H} : \mathcal{F}\mathcal{H} \Rightarrow \mathcal{G}\mathcal{H}$ by setting $(\eta\mathcal{H})_X := \eta_{\mathcal{H}(X)}$ for each object X in C. Similarly, define $\mathcal{K}\eta : \mathcal{K}\mathcal{F} \Rightarrow \mathcal{K}\mathcal{G}$ by setting $(\mathcal{K}\eta)_Y := \mathcal{K}(\eta_Y)$ for each Y in B. The effects of $\eta\mathcal{H}$ and $\mathcal{K}\eta$ are displayed in Figure 6.

(a) A diagram for $\eta\mathcal{H}$

(b) A diagram for $\mathcal{K}\eta$

Figure 6: Composing natural transformations with functors

The composition we describe next is specific to natural transformations of a particular form, which include counitals. It composes two natural transformations that share a functor and reflects our expectation that the characteristic relation is transitive. In Grp, for example, given a counital describing a characteristic subgroup H of G, and a counital describing a characteristic subgroup K of H, we expect to have a counital that prescribes how K is characteristic in G.

To that end, suppose E is a variety with subcategories A, B, and C, and respective inclusions $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{K}$. Suppose $\eta : \mathcal{J}\mathcal{C} \Rightarrow \mathcal{I}$ and $\mu : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{J}$ are natural transformations. Define $\mu \triangledown \eta : \mathcal{K}\mathcal{D}\mathcal{C} \Rightarrow \mathcal{I}$ by

$$(\mu \triangledown \eta)_X := \eta_X \mu_{C(X)}$$

for all objects X in A, see Figure 7. This construction reflects the fact that being a characteristic substructure is a transitive property.

6.2. Categorifying isosceles counitals

All extensions used in our proof of Theorem 1-cat lead to isosceles counitals. Counits—namely, counitals $\mathcal{J}\mathcal{C} \Rightarrow \mathcal{I}$ in which $\mathcal{J} = \mathcal{I}$ is the identity functor—are one source of isosceles counitals. This hints at a way to characterize characteristic subgroups.

We now prove that all counitals arising from characteristic subgroups extend to isosceles counitals, thereby proving Theorem 2-cat. The most direct proof might utilize *Kan lifts*, the dual of the better known *Kan extensions* [28, Chapter 6], but we give a self-contained proof.

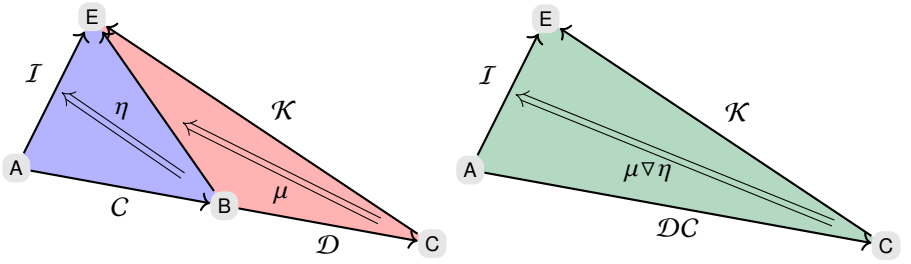


Figure 7: The $\triangledown$-composition of counitals explains transitivity

Definition 6.3. Let $\mathcal{I} : \mathsf{A} \to \mathsf{C}$ be an inclusion functor of categories, let $C : \mathsf{A} \to \mathsf{C}$ be a functor, and let $\iota : C \Rightarrow \mathcal{I}$ be a natural transformation. If, for every object X in A, the morphism $\iota_X : C(X) \to \mathcal{I}(X)$ in C is a morphism in A (more precisely, the image of a morphism in A under $\mathcal{I}$), then ι is *internal*.

The property of being internal is strong. Take, for example, $\mathsf{A} = \overleftrightarrow{\mathsf{C}}$, so the morphisms are exclusively isomorphisms. If ι is internal, then $\iota_X : C(X) \to X$ is an isomorphism. Such an ι does not identify a new substructure. In other words, A has too few morphisms for our purposes. By extending the types of morphisms, we prove in Proposition 6.4 that every monic isosceles counital lifts to an internal one; see Figure 8 for an illustration.

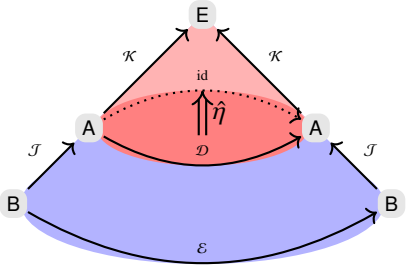


Figure 8: Extending an isosceles counital to an internal one

Proposition 6.4. *Let* E *be a category with subcategory* B *and inclusion* $\mathcal{I}$*. Suppose every object in* E *is also an object in* B*. Let* $\eta : \mathcal{I}\mathcal{E} \Rightarrow \mathcal{I}$ *be a monic isosceles counital with* $\mathcal{E} : \mathsf{B} \to \mathsf{B}$*. There exists a category* A *with inclusions* $\mathcal{J} : \mathsf{B} \to \mathsf{A}$ *and* $\mathcal{K} : \mathsf{A} \to \mathsf{E}$*, a functor* $\mathcal{D} : \mathsf{A} \to \mathsf{A}$*, and an internal monic isosceles counital* $\hat{\eta} : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{K}$ *such that* $\mathcal{J}\mathcal{E} = \mathcal{D}\mathcal{J}$*,* $\mathcal{I} = \mathcal{K}\mathcal{J}$*, and* $\hat{\eta}\mathcal{J} = \eta$*.*

Proof. We define a subcategory A of E as follows: its objects are the objects of E; its morphisms are given as finite compositions of morphisms $\mathcal{I}(\varphi) : \mathsf{E}$, where φ is a morphism in B, and morphisms $\eta_X : \mathsf{E}$, where X an object in B. Hence, we have inclusions $\mathcal{J} : \mathsf{B} \to \mathsf{A}$ and $\mathcal{K} : \mathsf{A} \to \mathsf{E}$ such that $\mathcal{I} = \mathcal{K}\mathcal{J}$. Since both A and B have the same objects as E, it follows that $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{K}$ are the identities on objects. Moreover, $\mathcal{K}$ is the identity on morphisms.

We now construct a functor $\mathcal{D} : \mathsf{A} \to \mathsf{A}$ such that $\mathcal{J}\mathcal{E} = \mathcal{D}\mathcal{J}$. It suffices to define $\mathcal{D}$ on morphisms and then verify that $\mathcal{D}$ is a functor. Set

$$\mathcal{D}(\varphi) := \begin{cases} \mathcal{J}\mathcal{E}(\varphi') & \varphi = \mathcal{J}(\varphi') \text{ for a morphism } \varphi' \text{ in } \mathsf{B}, \\ \eta_{\mathcal{E}(X)} & \varphi = \eta_X \text{ for some object } X \text{ in } \mathsf{B}, \\ \mathcal{D}(\sigma)\mathcal{D}(\tau) & \varphi = \sigma\tau. \end{cases}$$

If $\mathcal{D}$ is well defined, then $\mathcal{D}(\varphi)$ is a morphism in A, and $\mathcal{J}\mathcal{E} = \mathcal{D}\mathcal{J}$ by construction. To verify that $\mathcal{D}$ is well defined, it suffices to consider the case where η_X (with X an object in B) is also a morphism in B: specifically, there is a morphism $\beta : \mathsf{B}$ such that $\eta_X = \mathcal{I}(\beta)$. Since $\mathcal{I}$ is the identity on objects, $\beta : \mathcal{E}(X) \to X$. We will show that $\eta_{\mathcal{E}(X)} = \mathcal{K}\mathcal{D}(\eta_X) = \mathcal{I}\mathcal{E}(\beta)$. To see this, we apply η to the morphism $\beta : \mathcal{E}(X) \to X$ and obtain the following diagram (see shaded entry $(2, 2)$ of Figure 3).

$$\begin{array}{ccc} \mathcal{I}\mathcal{E}\mathcal{E}(X) & \xrightarrow{\mathcal{I}\mathcal{E}(\beta)} & \mathcal{I}\mathcal{E}(X) \\ \downarrow{\scriptstyle \eta_{\mathcal{E}(X)}} & & \downarrow{\scriptstyle \eta_X} \\ \mathcal{I}\mathcal{E}(X) & \xrightarrow{\mathcal{I}(\beta)} & \mathcal{I}(X) \end{array}$$

Since $\eta_X = \mathcal{I}(\beta)$, the diagram implies that $\eta_X\eta_{\mathcal{E}(X)} = \eta_X\mathcal{I}\mathcal{E}(\beta)$. Since η_X is monic by assumption, $\mathcal{I}\mathcal{E}(\beta) = \eta_{\mathcal{E}(X)}$. This proves that $\mathcal{D}$ is well defined.

We claim that there exists a natural transformation $\hat{\eta} : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{K}$ such that $\hat{\eta}\mathcal{J} = \eta$. Since the objects of A are those of B, we define $\hat{\eta}_X$ to be η_X and show that this yields the required counital. First, we consider the case that $\varphi : X \to Y$ is a morphism in B. Then $\mathcal{K}\mathcal{D}\mathcal{J}(\varphi) = \mathcal{K}\mathcal{J}\mathcal{E}(\varphi) = \mathcal{I}\mathcal{E}(\varphi)$, so

$$\hat{\eta}_Y\mathcal{K}\mathcal{D}(\mathcal{J}(\varphi)) = \eta_Y\mathcal{I}\mathcal{E}(\varphi) = \mathcal{I}(\varphi)\eta_X = \mathcal{K}(\mathcal{J}(\varphi))\hat{\eta}_X.$$

Now we assume $\varphi = \eta_X : \mathcal{I}\mathcal{E}(X) \to \mathcal{I}(X)$ for some object X in B. Since $\mathcal{I}$ is the identity on objects and $\mathcal{K}$ is the identity on morphisms,

$$\hat{\eta}_{\mathcal{I}(X)}\mathcal{K}\mathcal{D}(\eta_X) = \hat{\eta}_X\mathcal{K}\mathcal{D}(\eta_X) = \eta_X\mathcal{K}(\eta_{\mathcal{E}(X)}) = \eta_X\eta_{\mathcal{E}(X)} = \mathcal{K}(\eta_X)\hat{\eta}_{\mathcal{E}(X)}.$$

Lastly, we consider the case of an arbitrary finite composition $\varphi = \varphi_1 \cdots \varphi_n$ where each φ_k is either $\mathcal{J}(\varphi'_k)$ for some morphism φ'_k in B or a morphism η_X for some object X in B. It suffices to consider only the case where $n = 2$, say $\varphi = \varphi_1\varphi_2$ with $\varphi_2 : X \to Z$ and $\varphi_1 : Z \to Y$. Now

$$\begin{aligned} \hat{\eta}_Y\mathcal{K}\mathcal{D}(\varphi) &= \hat{\eta}_Y\mathcal{K}\mathcal{D}(\varphi_1)\mathcal{K}\mathcal{D}(\varphi_2) \\ &= \mathcal{K}(\varphi_1)\hat{\eta}_Z\mathcal{K}\mathcal{D}(\varphi_2) \\ &= \mathcal{K}(\varphi_1)\mathcal{K}(\varphi_2)\hat{\eta}_X \\ &= \mathcal{K}(\varphi)\hat{\eta}_X. \end{aligned}$$

Thus, $\hat{\eta} : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{K}$. Since η is monic, so is $\hat{\eta}$. Also, $\hat{\eta}_X$ is a morphism in A for every object X, so it is internal, as claimed. □

We now prove that every characteristic substructure of an algebra in a variety is induced by a morphism of category biactions.

Theorem 6.5. *Let X be an object in a variety E. Let Y be characteristic in X with inclusion $\iota : Y \to X$. There exist subcategories A and B with $\overleftrightarrow{\mathsf{E}} \leqslant \mathsf{A}, \mathsf{B} \leqslant \mathsf{E}$, and an (A, B)-morphism $\mathcal{M} : \mathsf{B} \to \mathsf{A}$ such that $\mathcal{M}(\mathrm{id}_X \cdot \mathbb{1}_{\mathsf{B}}) = \iota$.*

Proof. Let $\mathcal{I} : \overleftrightarrow{\mathsf{E}} \to \mathsf{E}$ be the inclusion functor. The proof of Theorem 1-cat shows that there exists a functor $\mathcal{E} : \overleftrightarrow{\mathsf{E}} \to \overleftrightarrow{\mathsf{E}}$ and a monic counital $\eta : \mathcal{I}\mathcal{E} \Rightarrow \mathcal{I}$ such that $\eta_X = \iota$. We use Proposition 6.4 (with $\mathsf{B} = \overleftrightarrow{\mathsf{E}}$) to create a category A generated from $\overleftrightarrow{\mathsf{E}}$ and η, an inclusion functor $\mathcal{K} : \mathsf{A} \to \mathsf{E}$, a functor $\mathcal{D} : \mathsf{A} \to \mathsf{A}$, and an internal monic counital $\hat{\eta} : \mathcal{K}\mathcal{D} \Rightarrow \mathcal{K}$ with $\hat{\eta}_Z = \eta_Z$ for all objects in $\overleftrightarrow{\mathsf{E}}$. Lastly, we apply Proposition 4.10(a) to $\hat{\eta}$ to obtain an A-bimorphism $\mathcal{N} : \mathsf{A} \to \mathsf{E}$ such that $\hat{\eta} = \mathcal{N}(\mathbb{1}_{\mathsf{A}})$. Since $\hat{\eta}$ is internal, there exists an A-bimorphism $\mathcal{M} : \mathsf{A} \to \mathsf{A}$ such that $\mathcal{N} = \mathcal{K}\mathcal{M}$. Hence, $\hat{\eta} = \mathcal{K}\mathcal{M}(\mathbb{1}_{\mathsf{A}})$. With $\mathsf{B} := \mathsf{A}$, it follows that $\mathcal{M}(\mathrm{id}_X \cdot \mathbb{1}_{\mathsf{B}}) = \hat{\eta}_X = \eta_X = \iota$, as claimed. □

6.3. Proofs of main theorems

Having developed the required theory, we can now complete the proofs of our main results. Theorem 1 is a special case of Theorem 1-cat, which we proved in the previous section.

Proof of Theorem 2-cat. If (1) holds, then Theorem 6.5 yields (3). If (3) holds, then (2) follows from Theorem 4.11(a) and the fact that $\iota = \mathcal{M}(\mathrm{id}_G \cdot \mathbb{1}_{\mathsf{B}})$. If (2) holds, then (1) follows from Theorem 1-cat. □

Theorem 2 follows from Theorem 2-cat.

6.4. Duality

Recall from Section 5.5 that a natural transformation $\eta : \mathcal{I} \Rightarrow \mathcal{D}$ is a unital if $\mathcal{I}$ is an inclusion functor. If $\mathcal{I} = \mathrm{id}$, then $\eta : \mathrm{id} \Rightarrow \mathcal{D}$ is a *unit*. A unital $\eta : \mathcal{I} \Rightarrow \mathcal{D}$ is *epic* if $\eta_X : \mathcal{I}(X) \to \mathcal{D}(X)$ is epic for all objects X. Units and unitals are the duals of counits and counitals.

We state a dual analogue of Theorem 2-cat for characteristic quotients of algebras in varieties; its proof follows *mutatis mutandis* from that of Theorem 2-cat.

Theorem 2-dual. *Let* E *be a variety, and let* G *be an object of* E *with quotient* Q *and projection* π. *There exist categories* A *and* B, *where* $\overleftrightarrow{\mathsf{E}} \leqslant \mathsf{A} \leqslant \mathsf{E}$, *such that the following are equivalent.*

(1) Q *is a characteristic quotient of* G.

(2) *There is a functor* $\mathcal{U} : \mathsf{A} \to \mathsf{A}$ *and a unit* $\epsilon : \mathrm{id}_{\mathsf{A}} \Rightarrow \mathcal{U}$ *such that* $Q = \mathrm{Coim}(\epsilon_G)$.

(3) *There is an* (A, B)*-morphism* $\mathcal{M} : \mathsf{A} \to \mathsf{B}$ *such that* $\pi = \mathcal{M}(\mathbb{1}_{\mathsf{A}} \cdot \mathrm{id}_G)$.

Although a characteristic subgroup of a group G is associated with a characteristic quotient of G, and vice versa, there are subtle differences in other categories of algebraic structures.

Example 6.6. Let $\mathbb{Q}$ be the ring of rational numbers and $\mathbb{Z}$ its subring of integers. If $\varphi : \mathbb{Q} \to \mathbb{Q}$ is a homomorphism of unital rings, then $\varphi(1) = 1$. This forces $\varphi = \mathrm{id}_{\mathbb{Q}}$, so $\mathbb{Z}$ is fully invariant in $\mathbb{Q}$. Since $\mathbb{Q}$ is a field, its only quotients are itself and the trivial ring. Hence, $\mathbb{Q}$ has many fully-invariant substructures, but only two fully-invariant quotients. More generally, if R is a unital ring, then the kernel of a ring homomorphism with domain R is not necessarily a unital subring of R. □

By contrast, the kernel of every group homomorphism is a normal subgroup. Up to equivalence of natural transformations in Cat, invariant structures of groups are *self-dual*. The next proposition provides a categorical description of this observation for Grp; we use it in Section 7.

Proposition 6.7. *The following hold for categories* $\overleftrightarrow{\mathsf{Grp}} \leqslant \mathsf{A} \leqslant \mathsf{Grp}$ *and* $\mathsf{B} \leqslant \mathsf{Grp}$ *with inclusion functors* $\mathcal{I} : \mathsf{A} \to \mathsf{Grp}$ *and* $\mathcal{J} : \mathsf{B} \to \mathsf{Grp}$.

(a) *Given a unital* $\pi : \mathcal{I} \Rightarrow \mathcal{J}\mathcal{U}$, *there is a sub category* $\mathsf{C} \leqslant \mathsf{Grp}$ *with inclusion* $\mathcal{K}$, *and a functor* $C : \mathsf{A} \to \mathsf{C}$ *such that* $\ker(\pi) : \mathcal{K}C \Rightarrow \mathcal{I}$ *is a counital where* $C(G) = \ker(\pi_G)$ *and* $(\ker(\pi))_G : \ker(\pi_G) \hookrightarrow G$ *is the inclusion for every group* G.

(b) *Given a counital* $\iota : \mathcal{J}C \Rightarrow \mathcal{I}$, *there is a subcategory* $\mathsf{C} \leqslant \mathsf{Grp}$ *with inclusion* $\mathcal{K}$, *and a functor* $\mathcal{U} : \mathsf{A} \to \mathsf{C}$ *such that* $\mathrm{coker}(\iota) : \mathcal{I} \Rightarrow \mathcal{K}\mathcal{U}$ *is a unital where* $\mathcal{U}(G) = G/\mathrm{Im}(\iota_G)$ *and* $(\mathrm{coker}(\iota))_G : G \twoheadrightarrow G/\mathrm{Im}(\iota_G)$ *for every group* G.

(c) *With the notation of* (a) *and* (b), *there are unique invertible* $\mu, \tau : \mathsf{A}$ *such that* $\mathrm{coker}(\ker(\pi)) = \mu(\mathrm{im}(\pi))$ *and* $\ker(\mathrm{coker}(\iota)) = \iota\tau$.

Proof. (a) For every morphism $\varphi : G \to H$ in A, there is an induced morphism $\varphi' : \mathrm{Im}(\pi_G) \to \mathrm{Im}(\pi_H)$ such that $\varphi'\pi_G = \pi_H\varphi$, so

$$\pi_H\varphi(\ker(\pi_G)) = \varphi'\pi_G(\ker(\pi_G)) = 1.$$

Therefore $\varphi(\ker(\pi_G)) \leqslant \ker(\pi_H)$. In particular, the restriction

$$\varphi|_{\ker(\pi_G)} : \ker(\pi_G) \to \ker(\pi_H)$$

is well defined. Let C be the category whose objects are $\ker(\pi_G)$ for all groups G and whose morphisms are $\varphi|_{\ker(\pi_G)}$ for all morphisms $\varphi : G \to H$ in A. Let $\mathcal{K} : \mathsf{C} \to \mathsf{Grp}$ be the inclusion functor. Moreover, there is a functor $C : \mathsf{A} \to \mathsf{C}$ given by $C(G) = \ker(\pi_G)$ and $C(\varphi) = \varphi|_{\ker(\pi_G)}$. If we define $\iota_G : \ker(\pi_G) \hookrightarrow G$ to be the associated inclusion map for the kernel, then $\iota : \mathcal{K}C \Rightarrow \mathcal{I}$ is the required counital.

(b) The proof is dual to that of (a).

(c) Consider the unital $\pi : \mathcal{I} \Rightarrow \mathcal{J}\mathcal{U}$. By Theorem 3.18, for each group G there is an isomorphism

$$\mu : \mathcal{U}(G) = \mathrm{Im}\pi_G \to G/\ker\pi_G = \mathrm{coker}(\ker\pi_G).$$

Thus, $\mathrm{coker}(\ker(\pi)) = \mu(\mathrm{im}(\pi))$; likewise, for $\ker(\mathrm{coker}(\iota))$ and ι. □

7. Categorification of standard characteristic subgroups

Theorem 2 states that every characteristic subgroup can be studied in three ways: as a group, as a natural transformation, and as a morphism of category biactions. In this section, we describe common characteristic subgroups using all three forms. In so doing, we reveal insights gained from the categorical perspective.

Throughout, we use the following notation for restriction and induction. Let $\varphi : G \to H$ be a homomorphism of groups, and let $C(G)$ and $C(H)$ be subgroups of H and G, respectively. If the restriction of φ to $C(G)$ maps into $C(H)$, then we denote it by

$$\varphi|_C : C(G) \to C(H), \quad c \mapsto \varphi(c). \tag{7.1}$$

Similarly, if φ maps a normal subgroup $Q(G)$ of G into a normal subgroup $Q(H)$ of H, then the *induction* of φ via Q is

$$\varphi|^Q : G/Q(G) \to H/Q(H), \quad gQ(G) \mapsto \varphi(g)Q(H). \tag{7.2}$$

7.1. Abelianization and derived subgroups

Figure 9 gives the three perspectives on the derived subgroup. We develop this example so that we may also treat the lower central series and all verbal subgroups in Section 7.2.

The counital $\lambda : \mathcal{D} \Rightarrow \mathrm{id}_{\mathsf{Grp}}$ of Example 6.2 associated with the derived subgroup $\gamma_2(G)$ of a group G can be constructed also as the kernel of the unital associated with abelianization. We explore the category biaction interpretation. Let Abel be the category of abelian groups, a subcategory of Grp with inclusion $\mathcal{I} : \mathsf{Abel} \to \mathsf{Grp}$. We define a morphism $\mathcal{A} : \mathsf{Grp} \to \mathsf{Abel}$ given by $\varphi \mapsto \varphi|^{\gamma_2}$. The functors $\mathcal{A}$ and $\mathcal{I}$ turn the categories Grp and Abel into $(\mathsf{Grp}, \mathsf{Abel})$-bicapsules.

We show that $\mathcal{A} : \mathsf{Grp} \to \mathsf{Abel}$ is a $(\mathsf{Grp}, \mathsf{Abel})$-morphism. Let φ and τ be group homomorphisms, and let α be a homomorphism of abelian groups. Now

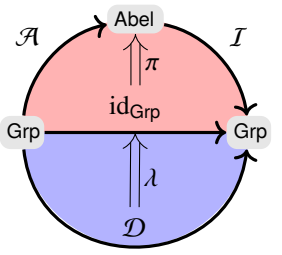
$$\mathcal{A}(\alpha \cdot \varphi\tau) = (\mathcal{I}(\alpha)\varphi\tau)|^{\gamma_2} = \alpha\ \varphi|^{\gamma_2}\ \tau|^{\gamma_2} = \alpha\mathcal{A}(\varphi) \cdot \tau.$$

To obtain the counital associated with the derived subgroup, we apply Proposition 6.7 and take the kernel of $\mathcal{A}(\mathbb{1}_{\mathsf{Grp}})$. Since the unital-counital pair obtained through this process is a unit-counit pair, we obtain the well-known observation that the derived subgroup is fully invariant.

Categories:
Grp: groups
Abel: abelian groups

Abelianization:
$\mathcal{A}(G) = G/\gamma_2(G)$
$\pi_G : G \twoheadrightarrow \mathcal{A}(G)$

Derived subgroup:
$\mathcal{D}(G) = \gamma_2(G)$
$\lambda_G : \mathcal{D}(G) \hookrightarrow G$



$\mathsf{Grp} \xrightarrow{\mathcal{A}} \mathsf{Abel}$

$G \downarrow f H \mapsto G/\gamma_2(G) \downarrow f|^{\gamma_2} H/\gamma_2(H)$

$\pi = \mathcal{A}(\mathbb{1}_{\mathsf{Grp}})$

$\mathsf{Grp} \xrightarrow{\mathcal{D}} \mathsf{Grp}$

$\mathcal{D} = \ker(\pi)$

$\lambda = \mathcal{D}(\mathbb{1}_{\mathsf{Grp}})$

Figure 9: Three perspectives on the derived subgroup

7.2. Verbal subgroups

We generalize the approach taken in Section 7.1. Let Ω be the group signature from Example 3.8. To each set W of words from the free group $\Omega\langle X\rangle$ we associate a category $\mathsf{Var}(W)$ as follows (see Section 3.4). For each word $w : W$, group G, and X-tuple $g : G^X$, define $w_G : G^X \to G$ by $g \mapsto \mathrm{eval}_g(w)$. Define $\mathsf{Var}(W)$ to be the full subcategory of Grp with objects

$$\{G : \mathsf{Grp} \mid (\forall g : G^X)(\forall w : W)\ w_G(g) = 1\}$$

with inclusion functor $\mathcal{I} : \mathsf{Var}(W) \to \mathsf{Grp}$. The category $\mathsf{Var}(W)$ is the *group variety* with laws W. Let $\mathrm{Rad}_W(G)$ be the minimal normal subgroup of a group G such that $G/\mathrm{Rad}_W(G)$ is in $\mathsf{Var}(W)$. Let $\mathcal{R} : \mathsf{Grp} \to \mathsf{Var}(W)$ be the functor such that $\mathcal{R}(G)$ is the largest quotient of G contained in $\mathsf{Var}(W)$, where the functor carries G to $G/\mathrm{Rad}_W(G)$, and morphisms φ are sent to $\varphi|^{\mathrm{Rad}_W}$.

Proposition 7.1. *The functors $\mathcal{R}$ and $\mathcal{I}$ form an adjoint functor pair $\mathcal{R} : \mathsf{Grp} \dashv \mathsf{Var}(W) : \mathcal{I}$.*

Proof. By Proposition 4.6, the functors $\mathcal{R}$ and $\mathcal{I}$ turn both $\mathsf{Var}(W)$ and Grp into $(\mathsf{Var}(W), \mathsf{Grp})$-bicapsules. The functor $\mathcal{R}$ is a $(\mathsf{Var}(W), \mathsf{Grp})$-morphism: for morphisms α in $\mathsf{Var}(W)$ and φ, τ in Grp,

$$\mathcal{R}(\alpha\varphi \cdot \tau) = (\alpha\varphi\mathcal{I}(\tau))|^{\mathrm{Rad}_W} = \alpha|^{\mathrm{Rad}_W}\ \varphi|^{\mathrm{Rad}_W}\ \tau = \alpha \cdot \mathcal{R}(\varphi)\tau.$$

Since $\mathcal{R}$ and $\mathcal{I}$ are pseudo-inverses, the result follows from Theorem 4.13(a). □

The adjoint functor pair in Proposition 7.1 categorifies verbal subgroups. The dual version of Theorem 4.11 describes how to obtain the unit $\pi : \mathrm{id}_{\mathsf{Grp}} \Rightarrow \mathcal{I}\mathcal{R}$ from $\mathcal{R}$. Applying Proposition 6.7, the kernel of π yields a counit $\iota : \mathcal{V} \Rightarrow \mathrm{id}_{\mathsf{Grp}}$ for some functor $\mathcal{V} : \mathsf{Grp} \to \mathsf{Grp}$. If G is a group, then $\mathcal{V}(G)$ is the W-*verbal* subgroup. We conclude that all verbal subgroups are fully invariant. Thus, from Proposition 7.1, we get an *exact sequence* of natural transformations

$$\mathcal{V} \overset{\ker(\pi)}{\Longrightarrow} \mathrm{id}_{\mathsf{Grp}} \overset{\pi}{\Longrightarrow} \mathcal{I}\mathcal{R}.$$

The corresponding diagram appears in Figure 10.

7.3. Marginal subgroups

Now we consider characteristic subgroups such as the center $\zeta(G)$ of a group G. As seen in Example 1.4, there are group homomorphisms $\varphi : G \to H$ for which $\varphi(\zeta(G)) \not\leq \zeta(H)$, so, unlike verbal subgroups,

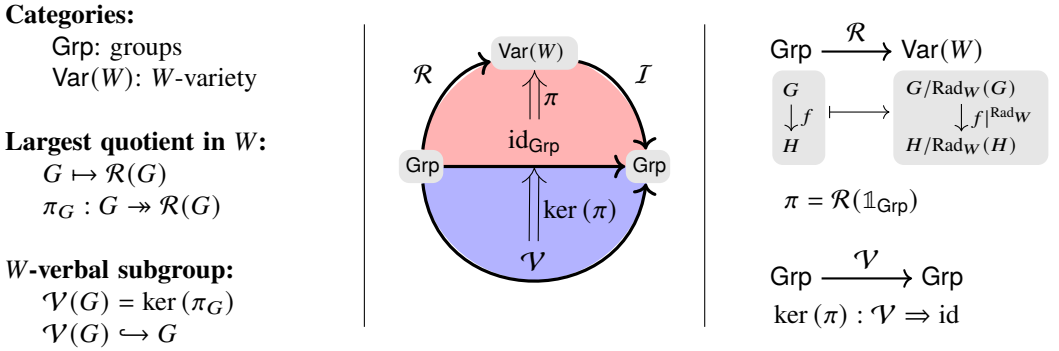


Figure 10: Three perspectives on verbal subgroups

the center is not fully invariant. This fact is revealed by the categorification of the center—it does not yield a counit between functors $\mathsf{Grp} \to \mathsf{Grp}$, but rather a proper counital between functors of the form $\overrightarrow{\mathsf{Grp}} \to \mathsf{Grp}$, where $\overrightarrow{\mathsf{Grp}}$ is the category of groups whose morphisms are epimorphisms. We establish this fact more generally for the class of *marginal subgroups* introduced by P. Hall [17].

Example 7.2 (Hall's Isoclinism)**.** For an integer $n > 0$ we write G^n for the n-fold direct product of a group G. The commutator map $\kappa : G^2 \to G$ is given by $(g, h) \mapsto [g, h] := g^{-1}h^{-1}gh$. We define a congruence relation $\equiv$ on G and write $x \equiv z$ if and only if $[x, z] = [y, z]$ for all $y : G$. Factoring through this congruence relation and restricting the outputs to the verbal subgroups, we obtain a map $* : (G/\zeta(G))^2 \to \gamma_2(G)$ such that the following diagram commutes.

$$\begin{array}{ccc} G^2 & \xrightarrow{\kappa} & G \\ \downarrow & & \uparrow \\ (G/\zeta(G))^2 & \xrightarrow{*} & \gamma_2(G) \end{array}$$

Two groups are *isoclinic* if their commutator maps are equivalent. □

For each group G and each word w, there is a unique minimal normal subgroup $w^*(G)$ such that the map $\overline{w}_G : (G/w^*(G))^n \to G$ given by

$$(g_1 w^*(G), \ldots, g_n w^*(G)) \longmapsto w_G(g_1, \ldots, g_n)$$

is non-degenerate: namely, fixing any $n - 1$ entries of the n-tuple argument of $\overline{w}_G$ yields an injective map $G/w^*(G) \to G$. Here w_G is as defined in Section 7.2.

For a set W of words, the associated *marginal subgroup* of a group G is defined as $W^*(G) := \bigcap_{w:W} w^*(G)$. Clearly, $W^*(G)$ is characteristic in G. The image of $\overline{w}_G$, and thus also w_G, is the verbal subgroup $w(G)$ associated with w.

Hall [17] introduced the general notion of *isologism* for word-map equivalence. We extend this language to categories. Each word w determines a category $\overrightarrow{\mathsf{Log}}_w$ with maps $\overline{w}_G : (G/w^*(G))^n \to w(G)$ as objects, where the morphisms are pairs (φ_1, φ_2) of group epimorphisms such that the following diagram commutes.

$$\begin{array}{ccc} (G/w^*(G))^n & \xrightarrow{\overline{w}_G} & w(G) \\ \downarrow{\scriptstyle \varphi_1^n} & & \downarrow{\scriptstyle \varphi_2} \\ (H/w^*(H))^n & \xrightarrow{\overline{w}_H} & w(H) \end{array}$$

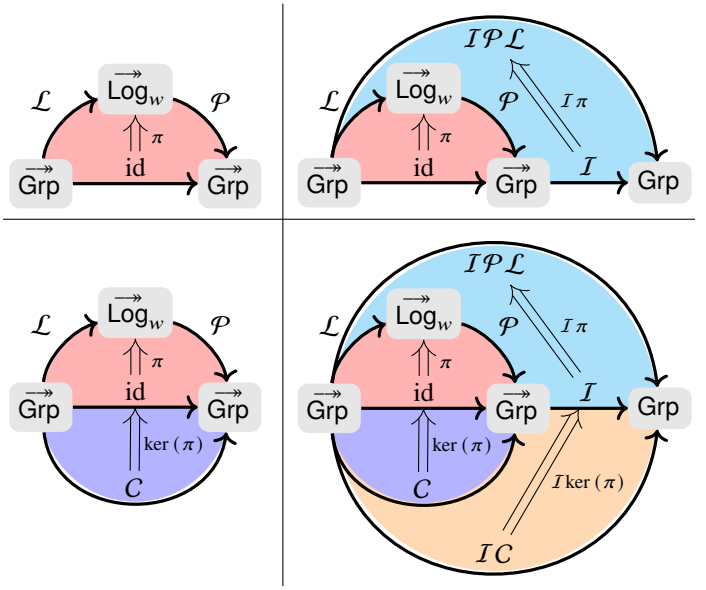


Figure 11: Marginal subgroups and quotients categorified

We define two functors. The first is $\mathcal{L} : \overrightarrow{\mathsf{Grp}} \to \overrightarrow{\mathsf{Log}}_w$ given by $G \mapsto \overline{w}_G$ and $\varphi \mapsto (\varphi|^{w^*}, \varphi|_w)$. The second is $\mathcal{P} : \overrightarrow{\mathsf{Log}}_w \to \overrightarrow{\mathsf{Grp}}$ given by $\overline{w}_G \mapsto G/w^*(G)$ and $(\varphi_1, \varphi_2) \mapsto \varphi_1$. For a group G, let $\pi_G : G \twoheadrightarrow G/w^*(G)$ be the usual projection homomorphism. Now $\pi : \mathrm{id}_{\overrightarrow{\mathsf{Grp}}} \Rightarrow \mathcal{P}\mathcal{L}$ is a unit. Let $\mathcal{I} : \overrightarrow{\mathsf{Grp}} \to \mathsf{Grp}$ be the inclusion functor. Then the unital $\mathcal{I}\pi : \mathcal{I} \Rightarrow \mathcal{I}\mathcal{P}\mathcal{L}$ is a categorification of marginal quotients.

To categorify the marginal subgroup, we take the kernel of π via Proposition 6.7 and compose with $\mathcal{I}$: namely, $\mathcal{I}\ker(\pi) : \mathcal{I}C \Rightarrow \mathcal{I}$ for some functor $C : \overrightarrow{\mathsf{Grp}} \to \overrightarrow{\mathsf{Grp}}$. Figure 11 displays the various morphisms and their relationships. This construction demonstrates that marginal subgroups are not just characteristic, but invariant under all epimorphisms.

The construction applies to other algebraic structures by simply involving formulas in the appropriate signature. However, the notion of congruence does not always yield a substructure, so the structures are more naturally expressed as characteristic quotients.

8. Composite characteristic structures

We now address one remaining powerful feature of our categorical description of characteristic structure. It relates to a comment we made after Theorem 2: a characteristic subgroup may arise from (A, B)-morphisms $\mathsf{B} \to \mathsf{A}$ where B is *not* a category of groups. We give one illustration of how this "transferability" explains techniques currently used in isomorphism tests.

In [35, §4], it is shown that a p-group G of class at most 2 with exponent p has a characteristic subgroup induced by the Jacobson radical of an algebra associated to the bilinear commutator map of G. Here we construct that characteristic subgroup using a tensor product of capsules, as described in Section 5.2.

8.1. From groups to bimaps

Fix an odd prime p, and let $\mathsf{G} := \overleftrightarrow{\mathsf{Grp}}_{2,p}$ be the category whose objects are p-groups of class at most 2 with exponent p, and whose morphisms are isomorphisms. The objects of G are groups G with exponent p and central derived subgroup, so $\gamma_2(G) \leqslant \zeta(G)$.

Let $\mathbb{F}_p$ be the field with p elements, and let $\mathsf{B} := \overleftrightarrow{\mathsf{Bi}}\ (\mathbb{F}_p)$ be the category of alternating $\mathbb{F}_p$-bilinear maps. The objects of B are bilinear maps $b : V \times V \to W$, where V and W are $\mathbb{F}_p$-spaces, such that $b(u, v) = -b(v, u)$ for all vectors u, v. For objects $b : V \times V \to W$ and $b' : V' \times V' \to W'$ in B, a morphism $\varphi : b \to b'$ is a pair of invertible linear maps $(\alpha : V \to V', \beta : W \to W')$ such that, for all $u, v \in V$,

$$b'(\alpha u, \alpha v) = \beta b(u, v).$$

Define a functor $\mathcal{B} : \mathsf{G} \to \mathsf{B}$ that takes a group G to

$$b_G : G/\gamma_2(G) \times G/\gamma_2(G) \to \gamma_2(G), \quad (x\gamma_2(G), y\gamma_2(G)) \mapsto [x, y],$$

and a homomorphism $\varphi : G \to H$ to the pair $(\varphi|^{\gamma_2},\ \varphi|_{\gamma_2})$, as defined in (7.1) and (7.2). Since G has exponent p and $\gamma_2(G) \leqslant \zeta(G)$ by assumption, b_G is an alternating $\mathbb{F}_p$-bilinear map.

Next, define a functor $\mathcal{G} : \mathsf{B} \to \mathsf{G}$ that takes an $\mathbb{F}_p$-bilinear map $b : V \times V \to W$ to the group G_b on $V \times W$ with binary operation

$$(v_1, w_1) \cdot (v_2, w_2) = \left(v_1 + v_2, w_1 + w_2 + \frac{1}{2} b(v_1, v_2)\right).$$

A morphism (α, β) from $b : V \times V \to W$ to $b' : V' \times V' \to W'$ in B induces a group isomorphism, denoted $\alpha \boxtimes \beta$, mapping $G_b = V \times W$ to $G_{b'} = V' \times W'$ by

$$(\alpha \boxtimes \beta)(v, w) := (\alpha u, \beta w).$$

Lemma 8.1. *The functor $\mathcal{B} : \mathsf{G} \to \mathsf{B}$ is a (G, B)-morphism.*

Proof. The functor $\mathcal{B}$ induces a left G-action on (the morphisms of) B, and $\mathcal{G}$ induces a right B-action on G, so B and G are (B, G)-bicapsules. Let λ, μ be morphisms of G and let (α, β) be a morphism of B such that $\lambda\mu \cdot (\alpha, \beta) = \lambda\mu(\alpha \boxtimes \beta)$ is not $\perp$. Now

$$\begin{aligned} \mathcal{B}(\lambda\mu \cdot (\alpha, \beta)) &= \big((\lambda\mu(\alpha \boxtimes \beta))|^{\gamma_2},\ (\lambda\mu(\alpha \boxtimes \beta))|_{\gamma_2}\big) \\ &= \big(\lambda|^{\gamma_2}\mu|^{\gamma_2}\alpha,\ \lambda|_{\gamma_2}\mu|_{\gamma_2}\beta\big) \\ &= \lambda \cdot \mathcal{B}(\mu)(\alpha, \beta), \end{aligned}$$

so $\mathcal{B}$ is a (G, B)-morphism. □

By applying the dual version of Theorem 4.11(a), we obtain a unit $\mathrm{id}_{\mathsf{G}} \Rightarrow \mathcal{B}\mathcal{G}$. There is also a counit $\mathrm{id}_{\mathsf{G}} \Leftarrow \mathcal{B}\mathcal{G}$. Together these give a categorical interpretation of the *Baer correspondence* [3].

8.2. From bimaps to algebras

Let $\mathsf{A} := \overleftrightarrow{\mathsf{Alge}}\ (\mathbb{F}_p)$ be the category of $\mathbb{F}_p$-matrix algebras with algebra isomorphisms. Using [35, §4], define a functor $\mathcal{A} : \mathsf{B} \to \mathsf{A}$ by

$$\mathcal{A}(b) = \{f \in \mathrm{End}(V) \mid (\exists f^* \in \mathrm{End}(V)^{\mathrm{op}})(\forall u, v \in V)\ b(fu, v) = b(u, f^*v)\}.$$

Invertible morphisms (α, β) in B from $b : V \times V \to W$ to $b' : V' \times V' \to W'$ are sent to

$$\mathcal{A}(\alpha, \beta) : f \in \mathcal{A}(b) \mapsto f^{\alpha^{-1}} \in \mathcal{A}(b').$$

Fact 8.2. *The functor $\mathcal{A}$ is a (B, A)-morphism.*

8.3. From matrix algebras to semisimple algebras

Every matrix algebra A over a field is Artinian, so the quotient of A by its Jacobson radical $\mathrm{Jac}(A)$ is semisimple. The map $A \mapsto A/\mathrm{Jac}(A)$ is a functor from A to the category $\mathsf{S} := \overleftrightarrow{\mathsf{SSAlge}}\,(\mathbb{F}_p)$ of semisimple $\mathbb{F}_p$-algebras. It is also an (A, S)-morphism.

8.4. Combining capsules

Recall that

$$\mathsf{G} = \overleftrightarrow{\mathsf{Grp}}_{2,p}, \qquad \mathsf{B} = \overleftrightarrow{\mathsf{Bi}}\,(\mathbb{F}_p), \qquad \mathsf{A} = \overleftrightarrow{\mathsf{Alge}}\,(\mathbb{F}_p), \qquad \mathsf{S} = \overleftrightarrow{\mathsf{SSAlge}}\,(\mathbb{F}_p).$$

Denote by Δ the bicapsule associated to the (G, B)-morphism in Lemma 8.1. Denote by Γ and Υ, respectively, the bicapsules associated to the (B, A)- and (A, S)-morphisms in Fact 8.2 and Section 8.3. These three capsules can now be combined to produce the (G, S)-capsule

$$\Delta \otimes_{\mathsf{B}} \Gamma \otimes_{\mathsf{A}} \Upsilon = \mathsf{G} \cdot \mu \cdot \mathsf{S}.$$

The resulting generator μ of this cyclic bicapsule is a unital. By Theorem 2-dual this provides the characteristic subgroup used in [22] and [35, §4].

9. Implementation

At the suggestion of the referee, we developed code in Agda [2] that focuses on the central topic of this paper: modeling characteristic structure as categories acting on categories. Our documented implementation is available at [6]. We encountered challenges in achieving both computational utility and verification and believe it is useful to identify them.

Refining the decision hierarchy. A main goal of the implementation was to build the category of all homomorphisms of an algebraic structure. This requires a decidable composition test: to compose $f : A \to B$ and $g : C \to D$, we must decide whether $B = C$. The question is decidable if B and C are simple types, but is undecidable for dependent types. For the particular dependent types used in our implementation, equality is decidable by case-splitting, but this has a high combinatorial cost. A 'decidable universe tower' could potentially address this issue.

Refining types for carrier sets. In many computational settings, the carrier set is not fixed in advance, but instead is generated by operations. One such setting is free algebras, which are equivalent to inductive types. Another is finite presentations (with explicit relations), which can be handled using higher inductive types. However, a third setting crucial in computational algebra is when we form a quotient by recognition (with no explicit relations). One such instance appears in Section 3.1. This presents significant difficulties from a type theory perspective.

Extending tactics to loop invariants. Computer algebra systems typically rely on mutable data, while theorem provers emphasize functional, stateless constructs. Many stateful algorithms can be reformulated as loops with invariant properties, where loop termination provides the desired proof. Developing tactics and types that express such invariants directly, without expanding them into recursion, would enhance both efficiency and usability.

Using systems such as Agda reduces the risk of misinterpreting code or relying on unverified results. Yet complex type systems sometimes create the illusion that stronger claims have been proved than actually are. Implementing explicit inhabitants and test cases often revealed gaps in our formal proofs. It is of course tempting to use "proof holes" (such as `postulate` in Agda or `sorry` in Lean) to bypass seemingly "obvious" proofs, but this can undermine the computational benefits of formalization. The development of our implementation made this clear: avoiding postulates forced repeated reformulation and showed us that treating categories as varieties, rather than as the essentially algebraic structures we initially studied, was essential. This conceptual shift strengthened our main results and simplified their exposition. The result was not only completely verified proofs, but also a deeper understanding of the algebra underlying categories.

Note that we avoid postulates for proofs, but our Agda code uses the tag `{-# OPTIONS --allow-unsolved-metas #-}` which averts warnings about potential holes in our code: these are confined to proofs of negation only, and satisfy the type-checker's need to return something if a contradiction is raised. Since contradictions cannot arise, such holes are *unreachable* and do not represent a gap.

Acknowledgements. We thank the referee for careful reading and valuable comments; the suggestion to develop a proof-of-concept implementation especially informed our understanding of the theory and its applications. We thank Chris Liu for fruitful discussions. We thank John Power and Mima Stanojkovski for comments on a draft.

Conflicts of interest. None.

Financial Support. Brooksbank was supported by NSF grant DMS-2319371. Maglione was supported by DFG grant VO 1248/4-1 (project number 373111162) and DFG-GRK 2297. O'Brien was supported by the Marsden Fund of New Zealand Grant 23-UOA-080 and by a Research Award of the Alexander von Humboldt Foundation. Wilson was supported by a Simons Foundation Grant identifier #636189 and by NSF grant DMS-2319370.

References

[1] J. Adámek and J. Rosický, *Locally presentable and accessible categories*, London Mathematical Soc. Lecture Note Ser., vol. 189, Cambridge University Press, Cambridge, 1994.
[2] The Agda Development Team, *The Agda user manual*, 2005–2023. Available at http://agda.readthedocs.io.
[3] R. Baer, Groups with abelian central quotient group, *Trans. Amer. Math. Soc.* **44** (1938), no. 3, 357–386.
[4] J. C. Baez, An introduction to n-categories, in *Category theory and computer science* (Santa Margherita Ligure, 1997), Lecture Notes in Comput. Sci., vol. 1290, Springer-Verlag, Berlin, 1997, pp. 1–33.
[5] J. E. Bergner and P. Hackney, Reedy categories which encode the notion of category actions, *Fund. Math.* **228** (2015), 193–222.
[6] P. A. Brooksbank, H. Dietrich, J. Maglione, E. A. O'Brien, and J. B. Wilson, Characteristic structure in Agda, 2025. Available at https://github.com/algeboy/Glassbox.
[7] B. Eick, C. R. Leedham-Green, and E. A. O'Brien, Constructing automorphism groups of p-groups, *Comm. Algebra* **30** (2002), no. 5, 2271–2295.
[8] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265.
[9] P. A. Brooksbank, E. A. O'Brien, and J. B. Wilson, Testing isomorphism of graded algebras, *Trans. Amer. Math. Soc.* **372** (2019), no. 11, 8067–8090.
[10] P. M. Cohn, *Universal algebra*, 2nd ed., D. Reidel Publishing Co., Dordrecht–Boston, Mass., 1981.
[11] The Coq Development Team, *The Coq proof assistant reference manual*, 2004. Available at https://coq.inria.fr/documentation.
[12] D. F. Holt, B. Eick, and E. A. O'Brien, *Handbook of computational group theory*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.
[13] F. Feldman, Leibniz and "Leibniz' Law", *The Philosophical Review* **79** (1970), no. 4, 510–522.
[14] P. J. Freyd and A. Scedrov, *Categories, allegories*, North-Holland Math. Library, vol. 39, North-Holland Publishing Co., Amsterdam, 1990.
[15] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.15.1, 2025. Available at https://www.gap-system.org.
[16] D. Grayson, M. Stillman, and D. Eisenbud, *Macaulay2*. Available at http://www2.macaulay2.com.
[17] P. Hall, Verbal and marginal subgroups, *J. Reine Angew. Math.* **182** (1940), 156–157.

[18] J. R. Hindley and J. P. Seldin, *Lambda-calculus and Combinators, An introduction*, Cambridge University Press, Cambridge, 2008.
[19] T. W. Hungerford, *Algebra*, Grad. Texts in Math., vol. 73, Springer-Verlag, New York–Berlin, 1980.
[20] M. Kilp, U. Knauer, and A. V. Mikhalev, *Monoids, acts and categories*, De Gruyter Exp. Math., Walter de Gruyter & Co, Berlin, 2000.
[21] J. Maglione, Filters compatible with isomorphism testing, *J. Pure Appl. Algebra* **225** (2021), no. 3.
[22] J. Maglione, Longer nilpotent series for classical unipotent subgroups, *J. Group Theory* **18** (2015), no. 4, 569–585.
[23] L. de Moura and S. Ullrich, The Lean 4 Theorem Prover and Programming Language, in *Automated Deduction — CADE 28*, Lecture Notes in Comput. Sci., vol. 12699, Springer, Cham, 2021, pp. 625–635.
[24] D. Marker, *Model Theory: An Introduction*, Grad. Texts in Math., vol. 217, Springer-Verlag, New York, 2002.
[25] nLab authors, *Action*, revision 74, 2023. Available at https://ncatlab.org.
[26] B. C. Pierce, *Types and programming languages*, MIT Press, Cambridge, MA, 2002.
[27] A. J. Power, An n-categorical pasting theorem, in *Category Theory (Como 1990)*, Lecture Notes in Math., Springer, Berlin, Heidelberg, 1991, pp. 326–358.
[28] E. Riehl, *Category theory in context*, Aurora Dover Mod. Math. Orig., Dover Publications, Inc., Mineola, NY, 2016.
[29] A. Rottlaender, Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen, *Math. Z.* **28** (1928), no. 1, 641–653.
[30] L. H. Rowen, *Graduate algebra: noncommutative view*, Grad. Stud. Math., vol. 91, American Mathematical Society, Providence, RI, 2008.
[31] The Sage Developers, *SageMath, the Sage Mathematics Software System*. Available at https://www.sagemath.org.
[32] Á. Seress, *Permutation group algorithms*, Cambridge Tracts in Math., vol. 152, Cambridge University Press, Cambridge, 2003.
[33] D. Tucker, Paradoxes and Restricted Quantification: A Non-Hierarchical Approach, *Thought: A Journal of Philosophy* **7** (2018), 190–199.
[34] The Univalent Foundations Program, *Homotopy Type Theory: Univalent Foundations of Mathematics*, Institute for Advanced Study, 2013. Available at https://homotopytypetheory.org/book.
[35] J. B. Wilson, More characteristic subgroups, Lie rings, and isomorphism tests for p-groups, *J. Group Theory* **16** (2013), no. 6, 875–897.