JOURNAL OF ALGEBRAS **136**, 497–529 (1991)

# Matrices, Relations, and Group Representations

AURELIO CARBONI

*Department of Mathematics, University of Milan,*
*Via C. Saldini 50, Milano, Italy*

*Communicated by Saunders MacLane*

Received March 3, 1988

Motivated by the search for a good notion of a "selfdual" object in a symmetric monoidal category, we give an abstract notion of commutative separable algebra in a symmetric monoidal category $\mathscr{V}$, such that when $\mathscr{V}$ is the category of modules over a commutative ring $k$ we obtain the usual commutative separable algebras. Developing the calculus based on such an abstract notion we are able to prove that the dual category of separable algebras in any compact closed, additive category with coequalizers is in fact *a boolean pretopos*. We apply this result to give a simple characterization of the *categories* of continuous representations of profinite groups in discrete finite dimensional $k$-vector spaces. Finally we show that the same calculus can be applied to symmetric monoidal categories of relations to give an essentially algebraic characterization of such categories. © 1991 Academic Press, Inc.

## INTRODUCTION

Tannaka's problem is well known (see, e.g., [CH, SR]): given a group $G$ and the symmetric monoidal category $\mathrm{Rep}_k(G)$ of finite dimensional representations of $G$ over a field $k$, how to reconstruct $G$ from $\mathrm{Rep}_k(G)$? The answer he gave is the following: let

$$\begin{array}{c}\mathrm{Rep}_k(G)\\ \big\downarrow{\scriptstyle \omega_G}\\ k\text{-}\mathrm{Vect}_{f.d.}\end{array}$$

be the strong monoidal functor which assigns to each representation of $G$ the underlying vector space and let $\mathrm{End}^{\otimes}(\omega_G)$ be the monoid of the monoidal endotransformations of $\omega_G$. Due to the compact-closedness of $k$-$\mathrm{Vect}_{f.d.}$ one has that $\mathrm{End}^{\otimes}(\omega_G)=\mathrm{Aut}^{\otimes}(\omega_G)$ and there exists a canonical homomorphism $G\to\mathrm{Aut}^{\otimes}(\omega_G)$; then one can prove that this homomorphism is in fact an iso when $G$ is compact in the continuous case, in particular when $G$ is finite, or when $G$ is algebraic.



0021-8693/91 \$3.00

What is not completely satisfactory in such a way of reconstructing the group is that it is strongly dependent on the *functor* $\omega_G$ and not just on the *category* $\mathrm{Rep}_k(G)$. Even without looking for particular counterexamples, it is clear that if we want to avoid ambiguities we have to reconstruct not just the group $G$ but, at least when $G$ is finite, *the whole topos* $S_{\text{fin}}^G$ *of permutation representations of* $G$ as a subcategory of $\mathrm{Rep}_k(G)$ by means of the free vector space functor:

$$\begin{array}{ccc} S_{\text{fin}}^G & \xrightarrow{F} & \mathrm{Rep}_k(G) \\ {\scriptstyle \omega_G}\downarrow & & \downarrow{\scriptstyle \omega_G} \\ S_{\text{fin}} & \xrightarrow[F]{} & k\text{-}\mathrm{Vect}_{f.d.} \end{array}$$

Then standard category theory will tell us how to reconstruct $G$ and the whole situation will be completely determined, since the functor $\omega_G\colon S_{\text{fin}}^G \to S_{\text{fin}}$ can be proved to be essentially unique, provided it satisfies nice exactness conditions.

Following such a program we can consider the simplest possible case, i.e., when $G=1$. In this case what we have to reconstruct is the *topos of finite sets* out of the category of finite dimensional vector spaces! And it is quite clear that if we solve the problem for $G=1$ we can solve it for all (finite) $G$, using what we know of the categories of linear representations of finite groups.

The above kind of situation often occurs in mathematics and the general picture is the following: we have a "linear" category $\mathscr{L}$, we know that there is a topos $\mathscr{E}$ of "sets" embedded *not fully* in $\mathscr{L}$ which supports the linear category $\mathscr{L}$ in some nice way, and we ask how to reconstruct $\mathscr{E}$ out of $\mathscr{L}$. Clearly such a question is the first one we should answer before asking ourselves a more ambitious question: can we elementarily *characterize* the class of linear categories we are interested in, in terms of structures (such as a symmetric monoidal closed structure) and of properties (such as additivity) that a linear category can have? Clearly the first basic class of such categories is the categories $k$-mod of modules over a commutative ring $k$.

The case of a commutative ring can be usefully generalized to the case of a cocomplete symmetric monoidal closed category $\mathscr{V}$, which means looking at the bicategory $\mathbf{B}=\mathscr{V}$-Mod of $\mathscr{V}$-categories and $\mathscr{V}$-profunctors between them. Again the base topos of sets is embedded in $\mathbf{B}$ and the problem of recovering it arises. We will discuss this kind of generalization with the simplest possible example, namely that of the cocomplete symmetric monoidal closed category 2 of "truth values."

In the following we want to illustrate the idea, which goes back to Grothendieck, that the notion of a *commutative separable algebra* should be the answer to such kinds of questions. Clearly we need to have a notion of commutative separable algebra abstract enough to be interpreted in any symmetric monoidal category. Such a notion has already been worked out (see, e.g., [DM-I, M]), but something more should be done if we want to prove properties of the category of commutative separable algebras in the abstract setting, as for instance that the dual of the category of commutative separable algebras enjoys good exactness properties.

After introducing in Section 1 our abstract notion motivated by the search for a good notion of selfduality and after investigating the first basic properties, we show in Section 2 that such a notion agrees with the classical one in the category of projective modules over a commutative ring. In Sections 3, 4, and 5 we develop the calculus based on our abstract notion to prove that the dual category of commutative separable algebras in any compact closed, preadditive category with coequalizers is a pretopos. In Section 6 we show that if the category is additive then the dual category of commutative separable algebras is a *boolean* pretopos, and we apply this result to give a simple characterization of *categories* of continuous representations of profinite groups in discrete finite dimensional $k$-vector spaces, $k$ being a separably closed field. In Section 7 we extend our abstract notion to the case of symmetric monoidal categories enriched over ordered sets and we show that this provides an essentially algebraic characterization of categories of relations.

In working in a symmetric monoidal category we will forget associativity and identity isomorphisms; we will denote by $I$ the identity of the tensor product and by $c_{X,Y}$ the symmetry isomorphisms; composition will be written diagrammatically.

## 1. Duality

Recall that the category $k$-mod of semimodules over a commutative semiring $k$ is a symmetric monoidal closed category (the identity $I$ of the tensor product being $k$ itself as 1-dimensional semimodule) and that the functor "free $k$-semimodule"

$$F : \mathscr{S} \to k\text{-mod}$$

is strong monoidal: $F(X \times Y) \simeq F(X) \otimes F(Y)$ and $(*) \simeq I$; thus the diagonal and the terminal maps in $\mathscr{S}$ give rise to a cocommutative coalgebra structure on $F(X)$:

$$F(X) \xrightarrow{\Delta_X} F(X) \otimes F(X), \qquad F(X) \xrightarrow{\perp_X} I.$$

Hence the functor $F$ factors through the category $\mathrm{CCoalg}_k$ of cocommutative coalgebras:

$$\mathscr{S} \to \mathrm{CCoalg}_k$$

and one can prove that *$F$ factors fully and faithfully provided $k$ has no nontrivial idempotents* (see [W]). But now, how can we recognize the coalgebra structure on $F(X)$ arising from the diagonal in sets among all other possible ones? Clearly $F(X)$ has another canonical structure, namely that of a commutative, associative, and distributive *multiplication*,

$$F(X) \otimes F(X) \xrightarrow{\nabla_X} F(X),$$

given by pointwise multiplication and having an identity

$$I \xrightarrow{\perp_X} F(X)$$

iff $X$ is a *finite set*. These two structures relate to each other in the following way: multiplication $\nabla_X$ and counit $\top_X$ compose to produce a bilinear form (*trace*),

$$\varepsilon_{F(X)} : F(X) \otimes F(X) \xrightarrow{\nabla_X} F(X) \xrightarrow{\top_X} I,$$

which tries to be the counit for an adjunction $F(X) \dashv F(X)$, proving that $F(X)$ is a strong selfdual object (for the abstract notion of duality in a symmetric monoidal category see, e.g., [K-L]), and in fact it is when $X$ is finite, the unit being

$$\eta_{F(X)} : I \xrightarrow{\perp_X} F(X) \xrightarrow{\Delta_X} F(X) \otimes F(X)$$

and the adjointness equations

$$(1 \otimes \eta)(\varepsilon \otimes 1) = 1 = (\eta \otimes 1)(1 \otimes \varepsilon) \tag{C}$$

being satisfied since one can easily check that the following equations hold:

$$(1 \otimes \Delta)(\nabla \otimes 1) = \nabla \Delta = (\Delta \otimes 1)(1 \otimes \nabla). \tag{D}$$

The easy proof that Eqs. (C) follow from (D) and the unit and counit equations for multiplication and comultiplication are left to the reader. Notice also that Eqs. (D) hold as well when *$X$ is not finite*, the only obstruction in proving Eqs. (C) being then the lack of the unit of the multiplication.

So, the free $k$-semimodule functor $F : \mathscr{S} \to k$-mod factors through a full subcategory of $\mathrm{CCoalg}_k$, namely the one determined by those cocommutative coalgebras for which there exists a multiplication satisfying axiom (D). Notice that:

LEMMA 1. *In any symmetric monoidal category $\mathscr{V}$, if a coalgebra $\langle A, \triangle, \top \rangle$ admits a multiplication $\nabla: A \otimes A \to A$ satisfying axiom* (D), *then $\nabla$ is associative.*

*Proof.* From axiom (D) and the counit we have:

$$\nabla = \nabla \triangle (1 \otimes \top) = (\triangle \otimes 1)(1 \otimes \nabla \top) = (1 \otimes \triangle)(\nabla \top \otimes 1).$$

Hence

$$\begin{aligned}(\nabla \otimes 1)\nabla &= (1 \otimes \triangle \otimes 1)(\nabla \top \otimes 1 \otimes 1)(\triangle \otimes 1)(1 \otimes \nabla \top)\\ &= (1 \otimes \triangle \otimes 1)(1 \otimes 1 \otimes \triangle \otimes 1)(\nabla \top \otimes 1 \otimes 1 \otimes 1)(1 \otimes \nabla \top)\\ &= (1 \otimes \triangle \otimes 1)(1 \otimes \triangle \otimes 1 \otimes 1)(1 \otimes 1 \otimes 1 \otimes \nabla \top)(\nabla \top \otimes 1)\\ &= (1 \otimes \triangle \otimes 1)(1 \otimes 1 \otimes \nabla \top)(1 \otimes \triangle)(\nabla \top \otimes 1) = (1 \otimes \nabla)\nabla \quad \blacksquare\end{aligned}$$

Further evidence of the power of axiom (D) is that for a cocommutative coalgebra to admit a commutative multiplication $\nabla$ satisfying axiom (D) is a *property* rather than a structure, provided the following axiom holds:

$$\triangle \nabla = 1. \tag{U}$$

LEMMA 2. *In a symmetric monoidal category $\mathscr{V}$ a cocommutative comultiplication $A \xrightarrow{\triangle} A \otimes A$ can admit at most one commutative multiplication $A \otimes A \xrightarrow{\nabla} A$ satisfying axioms* (D) *and* (U).

*Proof.* Suppose that $\nabla'$ is another commutative multiplication on $A$ satisfying axiom (D) and (U); then:

$$\begin{aligned}\nabla' \triangle &= \nabla' \triangle \nabla \triangle = (\triangle \otimes 1)(1 \otimes \nabla')(\triangle \otimes 1)(1 \otimes \nabla)\\ &= (\triangle \otimes 1)(\triangle \otimes 1 \otimes 1)(1 \otimes 1 \otimes \nabla')(1 \otimes \nabla)\\ &= (\triangle \otimes 1)(c_{A,A} \otimes 1)(1 \otimes c_{A,A})(\triangle \otimes 1 \otimes 1)(1 \otimes 1 \otimes \nabla')(1 \otimes \nabla)\\ &= (\triangle \otimes 1)c_{A \otimes A, A}(\triangle \otimes 1 \otimes 1)(1 \otimes 1 \otimes \nabla')(1 \otimes \nabla)\\ &= c_{A,A}(1 \otimes \triangle)(\triangle \otimes 1 \otimes 1)(1 \otimes 1 \otimes \nabla')(1 \otimes \nabla)\\ &= c_{A,A}(\triangle \otimes 1)(1 \otimes \nabla) = c_{A,A}\nabla \triangle = \nabla \triangle.\end{aligned}$$

Hence composing with $\triangle$ and using axiom (U) we get $\nabla' = \nabla$. $\blacksquare$

Another useful consequence of axioms (D) and (U) is given by the following:

LEMMA 3. *In a symmetric monoidal category $\mathscr{V}$ if a commutative multiplication $\nabla: A \otimes A \to A$ admits a coassociative comultiplication $\triangle: A \to A \otimes A$ satisfying axioms* (D) *and* (U), *then $\triangle$ is cocommutative.*

*Proof.*

$$\begin{aligned}\triangle c_{A,A} &= \triangle c_{A,A} \nabla \triangle c_{A,A} = \triangle c_{A,A}(1 \otimes \triangle)(\nabla \otimes 1) c_{A,A}\\ &= \triangle(\triangle \otimes 1) c_{A\otimes A,A} c_{A\otimes A,A}(1 \otimes \nabla) = \triangle(\triangle \otimes 1) c_{A,A\otimes A}(1 \otimes \nabla)\\ &= \triangle(1 \otimes \triangle) c_{A,A\otimes A}(1 \otimes \nabla) = \triangle c_{A,A}(\triangle \otimes 1)(1 \otimes \nabla)\\ &= \triangle c_{A,A} \nabla \triangle = \triangle. \quad \blacksquare\end{aligned}$$

*Remarks.* (1) Notice that axiom (U) holds for the pointwise multiplication and the diagonal map on the free $k$-semimodule $F(X)$ over any commutative semiring $k$.

(2) Let us stress that the above lemmas can be *dualized* in the sense that if we interchange multiplication with comultiplication in the hypotheses then the conclusion with the same interchange holds.

(3) In Lemma 2 coassociativity has not been used in the proof and cocommutativity cannot be avoided as can be shown by the example of the algebra of matrices.

## 2. Commutative Separable Algebras

One can now ask a deeper uniqueness question: given a symmetric monoidal category $\mathscr{V}$, how many cocommutative coalgebra (resp. algebra) structures are there on each object $A$ for which there exists an algebra (resp. coalgebra) structure satisfying axioms (D) and (U)? When $\mathscr{V}$ is $k$-mod, $k$ a commutative ring, the answer is provided by the following

Theorem. *In the symmetric monoidal category of projective k-modules, those commutative k-algebras $\langle A, \nabla, \perp \rangle$ for which there exists a coalgebra structure $\langle A, \triangle, \top \rangle$ satisfying axioms* (D) *and* (U) *are precisely commutative separable k-algebras.*

*Proof.* The proof is fairly straightforward if we assume the general definition over a commutative ring $k$ given in [DM-I]. According to such a definition a $k$-algebra $\langle A, \nabla, \perp \rangle$ is separable if there exists a "comultiplication" $\triangle : A \to A \otimes A$ satisfying axiom (U) and which is a left $A \otimes A^{\circ}$-module homomorphism, which is equivalent to axiom (D). So, using the above lemmas we only have to show that such a comultiplication has a *counit* $\top : A \to I$. First notice that a separable algebra $A$ which is a projective module is also a *finite dimensional* $k$-module (see, e.g., [DM-I, p. 47]); hence $A$ has a strong dual $A^*$. Define the counit as the *trace* of the multiplication $\nabla$

$$\top = A \xrightarrow{1 \otimes \eta_A} A \otimes A \otimes A^* \xrightarrow{\nabla \otimes 1} A \otimes A^* \xrightarrow{c_{A,A^*}} A^* \otimes A \xrightarrow{\varepsilon_A} I$$

($\eta_A$ and $\varepsilon_A$ being the adjunction maps for the dual object of $A$); we need to prove $\triangle(1\otimes\top)=1$; using axiom (D) we get:

$$\begin{aligned}\triangle(1\otimes\top) &= \triangle(1\otimes 1\otimes\eta)(1\otimes\nabla\otimes 1)(1\otimes c_{A,A^*})(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\triangle\otimes 1\otimes 1)(1\otimes\nabla\otimes 1)(1\otimes c_{A,A^*})(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\nabla\otimes 1)(\triangle\otimes 1)(1\otimes c_{A,A^*})(1\otimes\varepsilon).\end{aligned}$$

Now, using axiom (U), duality equations, commutativity, and again axiom (D) we get:

$$\begin{aligned}1 = \triangle\nabla &= \triangle(1\otimes\eta\otimes 1)(1\otimes 1\otimes\varepsilon)\nabla\\ &= \triangle(1\otimes\eta\otimes 1)(\nabla\otimes 1\otimes 1)(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\triangle\otimes 1\otimes 1)\, c_{A,A\otimes A\otimes A^*}(\nabla\otimes 1\otimes 1)(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\triangle\otimes 1\otimes 1)(1\otimes\nabla\otimes 1)\, c_{A,A\otimes A^*}(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\nabla\otimes 1)(\triangle\otimes 1)(c_{A,A}\otimes 1)\, c_{A,A\otimes A^*}(1\otimes\varepsilon)\\ &= (1\otimes\eta)(\nabla\otimes 1)(\triangle\otimes 1)(1\otimes c_{A,A^*})(1\otimes\varepsilon) = \triangle(1\otimes\top). \quad \blacksquare\end{aligned}$$

*Remarks.* (1) Notice that the unit $\perp$ does not enter in the proof and that by defining the *transfer* of a comultiplication $\triangle$ on a finite dimensional projective $k$-module $A$ as

$$\perp = I \xrightarrow{\eta} A\otimes A^* \xrightarrow{\triangle\otimes 1} A\otimes A\otimes A^* \xrightarrow{1\otimes c_{A,A^*}} A\otimes A^*\otimes A \xrightarrow{1\otimes\varepsilon} A,$$

we can prove mimicking the above theorem that if $A$ is equipped with a commutative multiplication $\nabla$ satisfying axioms (D) and (U) then $\perp$ is the unit of $\nabla$. Hence for finitely generated projective modules both unit and counit can be deduced from $\nabla$, $\triangle$, the axioms (D) and (U), and commutativity. On the other hand the existence of unit and counit and just axiom (D) imply that $A$ is finite dimensional projective, since the argument of Section 1 shows that $A$ has a strong dual, namely $A$ itself.

(2) Axiom (D) has already appeared in the literature without axiom (U) and without any connection with separable algebras; however, it was observed that it implies selfduality (see [L, p. 151]). A *Frobenius doctrine* is an endo-1-cell $A$ in a bicategory $\mathscr{V}$ equipped with a monad structure $\langle A, \nabla, \perp\rangle$ and a comonad structure $\langle A, \triangle, \top\rangle$ satisfying four equations which when $\mathscr{V}$ has just one object, i.e., is a monoidal category, reduce to:

$$(1\otimes\triangle)(\nabla\otimes 1)(1\otimes\top) = \nabla = (\triangle\otimes 1)(1\otimes\nabla)(\top\otimes 1),$$

$$(\perp\otimes 1)(1\otimes\triangle)(\nabla\otimes 1) = \triangle = (1\otimes\top)(\triangle\otimes 1)(1\otimes\nabla).$$

Easily one has that axiom (D) implies the above equations. Conversely,

$$\begin{aligned}\nabla\triangle &= \nabla(\perp\otimes 1)(\triangle\otimes 1)(1\otimes\nabla) = (\perp\otimes 1\otimes 1)(1\otimes\nabla)(\triangle\otimes 1)(1\otimes\nabla)\\ &= (\perp\otimes 1\otimes 1)(\triangle\otimes 1\otimes 1)(1\otimes 1\otimes\nabla)(1\otimes\nabla)\\ &= (\perp\otimes 1\otimes 1)(\triangle\otimes 1\otimes 1)(1\otimes\nabla\otimes 1)(1\otimes\nabla)\\ &= (((\perp\otimes 1)(\triangle\otimes 1)(1\otimes\nabla))\otimes 1)(1\otimes\nabla) = (\triangle\otimes 1)(1\otimes\nabla),\end{aligned}$$

and similarly $\nabla\triangle = (1\otimes\triangle)(\nabla\otimes 1)$. Notice that two of the four equations are redundant and that commutativity has never been used. Also, from the example of [L] it seems appropriate to name axiom (D) (without axiom (U) and without commutativity) as the "Frobenius" axiom, even if it has been independently discovered in another context in [C-W].

We conclude this section with the following

DEFINITION. Let $\mathscr{V}$ be a symmetric monoidal category. A *commutative separable algebra* in $\mathscr{V}$ is an object $A$ equipped with a commutative algebra structure $\langle A, \nabla, \perp\rangle$ and a cocommutative coalgebra structure $\langle A, \triangle, \top\rangle$ satisfying axioma (D) and (U).

The above definition is a bit redundant since from the lemmas and remarks of Section 1 it follows that it is enough to ask for associativity and commutativity of one of the two structures. Half of axiom (D) is also redundant since in the presence of commutativity and cocommutativity one of the two equations can be deduced from the other. Notice also that *the notion of a commutative separable algebra is disjoint from the notion of a bialgebra* [S, p. 51], since if an object $A$ has a commutative separable algebra structure which also satisfies the equations for a bialgebra, then $A$ must be isomorphic to the identity $I$: from the equations $\nabla\top = \top\otimes\top$, $\perp\triangle = \perp\otimes\perp$, $\top = 1$ of a bialgebra, and axiom (D) it follows easily using Eqs. (C) of Section 1 that $\top$ and $\perp$ are inverses to each other. However, axioms (D) and (U) force the remaining axiom $\nabla\triangle = (\triangle\otimes\triangle)(1\otimes c_{A,A}\otimes 1)(\nabla\otimes\nabla)$ of a bialgebra, since using commutativity and assciativity we get:

$$\begin{aligned}&(\triangle\otimes\triangle)(1\otimes c_{A,A}\otimes 1)(\nabla\otimes\nabla)\\ &\quad= (\triangle\otimes 1)(1\otimes 1\otimes\triangle)\,c_{A\otimes A\otimes A,A}(\nabla\otimes 1\otimes 1)\\ &\quad= (\triangle\otimes 1)(1\otimes 1\otimes\triangle)(1\otimes\nabla\otimes 1)(\nabla\otimes 1)c_{A,A}\\ &\quad= (\triangle\otimes 1)(1\otimes 1\otimes\triangle)(\nabla\otimes 1\otimes 1)(\nabla\otimes 1)c_{A,A}\\ &\quad= (1\otimes\triangle)(\nabla\otimes 1)c_{A,A} = \nabla\triangle.\end{aligned}$$

## 3. Abstract Galois Theory

Recalling the fundamental theorem of Grothendieck Galois Theory that the dual category of the category of commutative separable algebras over a field $k$ is equivalent to the *topos* of continuous representations in finite sets of the profinite fundamental group of $k$, the natural question arises of giving an abstract proof of such a theorem. In other words, if $\mathscr{V}$ is any symmetric monoidal category and if $\mathrm{Sep}(\mathscr{V})$ is the category of commutative separable algebras in $\mathscr{V}$, when is it possible to prove that the dual of the category $\mathrm{Sep}(\mathscr{V})$ is a *Galois category* (see [SGA-1]) or at least is a *pretopos* (see [SGA-4, exp 6])? Clearly to prove such a theorem we have to develop the calculus based on our abstract definition of commutative separable algebra and we first clarify some consequences of the duality.

Given a symmetric monoidal category $\mathscr{V}$ we consider a new category $\mathrm{Sep}_l(\mathscr{V})$ whose objects are commutative separable algebras in $\mathscr{V}$ and whose morphisms are just morphisms of $\mathscr{V}$; when $\mathscr{V}$ is the symmetric monoidal category of projective $k$-modules, $k$ a commutative ring, then $\mathrm{Sep}_l(\mathscr{V})$ is the category of commutative separable $k$-algebras and *linear* maps between them. Clearly $\mathscr{W} = \mathrm{Sep}_l(\mathscr{V})$ is a *symmetric monoidal category* since one can easily verify that the tensor product of two commutative separable algebras is again a commutative separable algebra, and is canonically endowed with the following structure:

Definition 1. A *well supported compact closed* (wscc) *structure* on a symmetric monoidal category $\mathscr{W}$ is given by four maps on each object $X$,

$$\perp_X: I \to X, \qquad \nabla_X: X \otimes X \to X$$

and

$$\top_X: X \to I, \qquad \Delta_X: X \to X \otimes X,$$

satisfying the following axioms:

(1) $\langle X, \nabla_X, \perp_X \rangle$ is a commutative monoid object and $\langle X, \Delta_X, \top_X \rangle$ is a cocommutative comonoid object;

(2) the monoid and comonoid structures on a tensor product are pointwise (i.e., $\nabla_{X \otimes Y} = (1 \otimes c_{X,Y} \otimes 1)(\nabla_X \otimes \nabla_Y)$, etc.) and the ones on $I$ are both the identity;

(3) multiplication and comultiplication satisfy the following equations:

$$\nabla \Delta = (\Delta \otimes 1)(1 \otimes \nabla) \tag{D}$$

$$\Delta \nabla = 1. \tag{U}$$

Given a wscc-structure on a symmetric monoidal category $\mathscr{W}$, let $\mathrm{Map}(\mathscr{W})$ be the category of comonoid homomorphisms and let $\mathrm{Alg}(\mathscr{W})$ be the category of monoid homomorphisms. We will denote comonoid homomorphisms with lowercase latin letters and we will call them "maps." Notice that if $\mathscr{W}$ is $\mathrm{Sep}_l(\mathscr{V})$ then $\mathrm{Alg}(\mathscr{W})$ is the category of commutative separable algebras in $\mathscr{V}$ and $\mathrm{Map}(\mathscr{W})$ is the category of commutative separable algebras in $\mathscr{V}$ but *with morphisms the coalgebra homomorphisms.*

THEOREM 1. *If $\mathscr{W}$ is a symmetric monoidal category equipped with a* wscc-*structure, then*:

(1) $\mathrm{Map}(\mathscr{W})$ *has finite products and* $\mathrm{Alg}(\mathscr{W})$ *has finite sums;*

(2) *the definitions*

$$R \cdot S \overset{\mathrm{def}}{=} \triangle_X(R \otimes S) \nabla_Y, \qquad \top_{X,Y} \overset{\mathrm{def}}{=} \top_X \bot_Y$$

*give to each* hom-*set $\mathscr{W}(X, Y)$ the structure of a commutative monoid;*

(3) *$\mathscr{W}$ is compact closed and canonically the involution $(-)^\circ$: $\mathscr{W} \to \mathscr{W}^{\mathrm{op}}$ is the identity on objects;*

(4) *if $R : X \to Y$ is a comultiplication homomorphism then*

$$(R \otimes 1) \nabla = (1 \otimes R^\circ) \nabla R;$$

(5) $\bot^\circ = \top$ *and* $\nabla^\circ = \triangle$;

(6) *if $f : X \to Y$ is a map as well as a monoid homomorphism then $f$ is an orthogonal isomorphism, i.e., $ff^\circ = 1$ and $f^\circ f = 1$; in particular $c^\circ_{X,Y} = c_{Y,X}$;*

(7) *if $f : X \to Y$ is a map which is invertible in $\mathscr{W}$, then $f^{-1} = f^\circ$, and hence $f$ is invertible in* $\mathrm{Map}(\mathscr{W})$; *it follows that $f$ is in fact in* $\mathrm{Alg}(\mathscr{W})$;

(8) *if $A : X \to X$ is an endomorphism such that $A \cdot A = A = A \cdot 1_X$ then $A$ is a symmetric idempotent and a comultiplication homomorphism.*

*Proof.* (1) One can show easily that $\mathrm{Alg}(\mathscr{W})$ is again a symmetric monoidal category. Moreover, $\nabla_X$ and $\bot_X$ are algebra maps: just repeat the proof that in commutative rings the multiplication and the unit maps are ring homomorphisms. The statement about $\mathrm{Alg}(\mathscr{W})$ follows now from the known argument that in commutative rings the tensor product is the categorical sum. As for $\mathrm{Map}(\mathscr{W})$, just dualize the previous argument.

(2) Obvious: the commutative monoid equations for the product so defined on each hom-set follow from the same equations for the $\langle \triangle, \nabla, \top, \bot \rangle$-structure on each object.

(3) It is well known [K-L] that a symmetric monoidal category $\mathscr{W}$ is compact closed when each object $X$ has an adjoint $X^*$ in the bicategory with one object whose hom-category is $\mathscr{W}$; that is, there are two maps,

$$\eta_X : I \to X \otimes X^* \qquad \text{and} \qquad \varepsilon_X : X^* \otimes X \to I,$$

satisfying the equations

$$(1 \otimes \eta)(\varepsilon \otimes 1) = 1 \qquad \text{and} \qquad (\eta \otimes 1)(1 \otimes \varepsilon) = 1. \tag{C}$$

In our situation the obvious candidates for $\eta$ and $\varepsilon$ are

$$\eta_X = I \xrightarrow{\perp_X} X \xrightarrow{\triangle_X} X \otimes Y \qquad \text{and} \qquad \varepsilon_X = X \otimes X \xrightarrow{\nabla_X} X \xrightarrow{\top_X} I.$$

It is straightforward to verify that $\eta$ and $\varepsilon$ so defined satisfy the Eqs. (C): basically this follows from axiom (3) plus unit and counit axioms. So, $\mathscr{W}$ is compact closed and there is a natural bijection

$$(-)^\wedge : \mathscr{W}(Z \otimes X, Y) \to \mathscr{W}(Z, Y \otimes X),$$

whose inverse we denote by $(-)^\vee$, defined for $Z \otimes X \xrightarrow{R} Y$, $Z \xrightarrow{S} Y \otimes Z$, by:

$$(R)^\wedge = (1 \otimes \eta_X)(R \otimes 1) \qquad \text{and} \qquad (S)^\vee = (S \otimes 1)(1 \otimes \varepsilon_X).$$

Naturality in $Y$ and $Z$ means

$$[(H \otimes 1)R]^\wedge = H(R)^\wedge \qquad \text{and} \qquad (H \otimes 1)S^\vee = (HS)^\vee \tag{N$_1$}$$

and

$$(RK)^\wedge = (R)^\wedge\,(K \otimes 1) \qquad \text{and} \qquad S^\vee K = [S(K \otimes 1)]^\vee. \tag{N$_2$}$$

Moreover, if $R : X \to Y$ is any arrow, by defining

$$R^\circ = (1_Y \otimes \eta_X)(1_Y \otimes R \otimes 1_X)(\varepsilon_Y \otimes 1_X) : Y \to X$$

we can prove that we get an *involution* on $\mathscr{W}$ which is the identity on objects, i.e., a functor $(-)^\circ : \mathscr{W} \to \mathscr{W}^{\mathrm{op}}$ which is the identity on objects and satisfies $(R^\circ)^\circ = R$. More, we can prove that the bijection $(-)^\wedge$ is natural also with respect to the variable $X$:

$$[(1 \otimes S)R]^\wedge = (R)^\wedge\,(1 \otimes S^\circ). \tag{N$_3$}$$

(4) We have: $(R\triangle)^{\vee}=(R\otimes 1)(\triangle)^{\vee}$, by naturality, and again by naturality:

$$[\triangle(R\otimes R)]^{\vee}=[\triangle(1\otimes R)(R\otimes 1)]^{\vee}=[\triangle(1\otimes R)]^{\vee}R$$
$$=[\triangle(1\otimes(R^{\circ})^{\circ})]^{\vee}R=(1\otimes R^{\circ})(\triangle)^{\vee}R.$$

Thus if $R$ is a comultiplication homomorphism and if $(\triangle)^{\vee}=\nabla$ we get the statement. But:

$$(\triangle)^{\vee}=(\triangle\otimes 1)(1\otimes\varepsilon)=(\triangle\otimes 1)(1\otimes\nabla)(1\otimes\top)=\nabla\triangle(1\otimes\top)=\nabla.$$

(5) Easily one has $\perp^{\circ}=\top$. As for the second equation, using the definition of the involution, instances of axioms (1) and (2), and associativity of $\nabla$ we can compute $\nabla^{\circ}$ as

$$\nabla^{\circ}=(1\otimes\perp\otimes\perp)(1\otimes\triangle\otimes\triangle)(1\otimes 1\otimes c_{X,X}\otimes 1)(\nabla\otimes 1\otimes 1\otimes 1)$$
$$(\nabla\otimes 1\otimes 1)(\top\otimes 1\otimes 1);$$

since the two middle factors commute we can apply axiom (3); then using functoriality of the tensor product we can apply the unit axiom of $\nabla$ so that the last expression reduces to

$$(1\otimes\perp)(\triangle\otimes\triangle)(1\otimes c_{X,X}\otimes 1)(\nabla\otimes 1\otimes 1)(\top\otimes 1\otimes 1)$$
$$=(1\otimes\perp)(\triangle\otimes 1)(1\otimes 1\otimes\triangle)(1\otimes c_{X,X}\otimes 1)(\nabla\otimes 1\otimes 1)(\top\otimes 1\otimes 1);$$

now, using commutativity of $\nabla$ and $\triangle$ and coherence conditions of the symmetry isomorphisms, this last becomes

$$(1\otimes\perp)(\triangle\otimes 1)(1\otimes 1\otimes\triangle)\,c_{X\otimes X\otimes X,X}(\nabla\otimes 1\otimes 1)(\top\otimes 1\otimes 1);$$

since $(\triangle\otimes 1)(1\otimes 1\otimes\triangle)=(1\otimes\triangle)(\triangle\otimes 1\otimes 1)$, we can apply naturality of symmetry isomorphisms to get

$$(1\otimes\perp)(1\otimes\triangle)\,c_{X\otimes X,X}(1\otimes\triangle\otimes 1)(\nabla\otimes 1\otimes 1)(\top\otimes 1\otimes 1),$$

which by axiom (3) and the counit axiom gives

$$(1\otimes\perp)(1\otimes\triangle)\,c_{X\otimes X,X}(\nabla\otimes 1);$$

now using commutativity of $\nabla$ and $\triangle$ and coherence conditions of symmetry we can prove that

$$(1\otimes\triangle)\,c_{X\otimes X,X}(\nabla\otimes 1)=(1\otimes\triangle)(\nabla\otimes 1);$$

thus by applying once again axiom (3) and the unit axiom we get $\triangle$.

(6) If $f: X \to Y$ is a map then $f$ is a comultiplication homomorphism; hence by (4) $(f \otimes 1) \nabla = (1 \otimes f^\circ) \nabla f$; since $f$ is a monoid homomorphism if and only if $f^\circ$ is a map then the same equation holds for $f^\circ$; now, $f^\circ$ is a counit homomorphism; hence $f$ is a unit homomorphism; thus

$$1 = (\perp \otimes 1) \nabla = (\perp f \otimes 1) \nabla = (\perp \otimes 1)(f \otimes 1) \nabla = (\perp \otimes 1)(1 \otimes f^\circ) \nabla f$$
$$= f^\circ(\perp \otimes 1) \nabla f = f^\circ f;$$

and since also $f^\circ$ is a unit homomorphism, we get

$$1 = (\perp \otimes 1) \nabla = (\perp f^\circ \otimes 1) \nabla = (\perp \otimes 1)(f^\circ \otimes 1) \nabla = (\perp \otimes 1)(1 \otimes f) \nabla f^\circ$$
$$= f(\perp \otimes 1) \nabla f^\circ = f f^\circ.$$

The last sentence of the statement follows now because one can easily show that $c_{X,Y}$ is a map and a monoid homomorphism.

(7) If $f: X \to Y$ is an invertible map then

$$1 = \triangle(f^{-1} f \otimes 1) \nabla = \triangle(f^{-1} \otimes 1)(f \otimes 1) \nabla = \triangle(f^{-1} \otimes 1)(1 \otimes f^\circ) \nabla f$$
$$= \triangle(f^{-1} \otimes f^\circ) \nabla f = \triangle(f^\circ \otimes f^{-1}) \nabla f = \triangle(f^\circ \otimes 1)(1 \otimes f^{-1}) \nabla f$$
$$= f^\circ \triangle(1 \otimes f)(1 \otimes f^{-1}) \nabla f = f^\circ f;$$

hence $f^{-1} = f^\circ$.

(8) From the definition of the local product we have

$$A \triangle = \triangle(1 \otimes A) \nabla \triangle = \triangle(1 \otimes A)(\triangle \otimes 1)(1 \otimes \nabla) = \triangle(\triangle \otimes A)(1 \otimes \nabla)$$
$$= \triangle(\triangle \otimes 1)(1 \otimes 1 \otimes A)(1 \otimes \nabla) = \triangle(1 \otimes \triangle)(1 \otimes 1 \otimes A)(1 \otimes \nabla)$$
$$= \triangle(1 \otimes A);$$

from commutativity of $\triangle$ it follows that $A \triangle = \triangle(A \otimes 1)$ as well. Now

$$\triangle(A \otimes A) = \triangle(1 \otimes A)(A \otimes 1) = A \triangle(A \otimes 1) = AA\triangle;$$

hence

$$A = \triangle(A \otimes A) \nabla = AA \triangle \nabla = AA,$$

so $A$ is idempotent as well as a comultiplication homomorphism; thus

$$A = \triangle(A \otimes 1) \nabla = \triangle(1 \otimes A^\circ) \nabla A = A^\circ A;$$

hence $A = A^\circ$. ∎

*Remarks.* If $f : X \to Y$ is a map or more generally just a comultiplication homomorphism, then the following *projection formula* holds for the local product in $\mathscr{W}(X, Y)$:

$$f^\circ R \cdot S = f^\circ(R \cdot fS)$$

and dually:

$$Rf \cdot S = (R \cdot Sf^\circ)f.$$

(2) Notice that the tensor product in $\mathscr{W}$ can be reconstructed from the cartesian structure of $\mathrm{Map}(\mathscr{W})$ and the local product in $\mathscr{W}$, since one can easily show that

$$R \otimes S = (pSp^\circ) \cdot (pRp^\circ),$$

where the $p$'s denote the appropriate projections.

COROLLARY. *In any symmetric monoidal category $\mathscr{V}$ the dual of the category of commutative separable algebras is isomorphic to the category of commutative separable algebras with morphisms the coalgebra homomorphisms.*

## 4. The Galois Category of a Symmetric Monoidal Category

DEFINITION 1. Let $\mathscr{V}$ be a symmetric monoidal category; the Galois Category of $\mathscr{V}$ is the category $\mathrm{Gal}(\mathscr{V})$ of commutative separable algebras in $\mathscr{V}$ and coalgebra homomorphisms between them.

The aim of this section is to prove that under suitable hypotheses on $\mathscr{V}$ the category $\mathrm{Gal}(\mathscr{V})$ is a pretopos. Using the machinery developed in the last section it will be enough to prove the same statement for the category $\mathrm{Map}(\mathscr{W})$, where $\mathscr{W}$ is a symmetric monoidal category equipped with a wscc-structure. First we investigate the left exactness of $\mathrm{Map}(\mathscr{W})$, which reduces to investigating the existence of equalizers, since we have already proved the existence of finite products.

DEFINITION 2. Let $\mathscr{W}$ be a symmetric monoidal category equipped with a wscc-structure. $\mathscr{W}$ is said to be functionally complete if for each endomorphism $A : X \to X$ such that $A \cdot A = A = A \cdot 1_X$ there exists a map $i : X' \to X$ such that $ii^\circ = 1$ and $i^\circ i = A$.

*Remarks.* (1) It is easy to see that the splitting of $A$ given by $i$ and $i^\circ$ is unique up to a unique isomorphism which is also a map: it is enough to show that if $j$ is a map such that $jj^\circ = 1$ then $j^\circ$ is a comultiplication homomorphism. Hence $ij^\circ$ is also a comultiplication homomorphism; moreover, if $j^\circ j = A$ then $ij^\circ$ is a counit homomorphism: $ij^\circ\top = ij^\circ j\top = ii^\circ i\top = i\top = \top$.

(2) Let us call *coreflexives* the endomorphisms $A$ of $X$ which "think" that the identity arrow $1_X$ of $X$ is the unit for the local product in $\mathscr{W}(X, X)$ and which are idempotents for the local product; call $\mathrm{Cor}(X)$ the set of such endomorphisms. Then $\mathrm{Cor}(X)$ is a commutative submonoid of the monoid $\mathscr{W}(X, X)$ with respect to composition. In particular if $A$ and $B$ are two coreflexives then $A \cdot B = AB$.

LEMMA 1. *Let $\mathscr{W}$ be a symmetric monoidal category equipped with a functional complete* wscc-*structure. Then*:

(1) $\mathrm{Map}(\mathscr{W})$ *is left exact*;

(2) *a commutative square $qf = gp$ is a pullback in* $\mathrm{Map}(\mathscr{W})$ *iff $qq^\circ \cdot gg^\circ = 1$ and $pf^\circ = g^\circ q$; in particular a map $i$ is a mono in* $\mathrm{Map}(\mathscr{W})$ *if and only if $ii^\circ = 1$ in $\mathscr{W}$.*

*Proof.* (1) We just need to show that $\mathrm{Map}(\mathscr{W})$ has equalizers. First observe that if $R$ is an endomorphism of $X$ then the endomorphism $A = 1 \cdot R$ has the property that $1 \cdot A = A$, since the local product is associative and axiom (U) can be stated in terms of the local product as $1 \cdot 1 = 1$. Now, let $f, g : X \to Y$ be a parallel pair of maps and consider the endomorphism of $X$ given by $A = 1 \cdot fg^\circ$. From the above remark it follows that $1 \cdot A = A$; and $A \cdot A = 1 \cdot fg^\circ \cdot fg^\circ$, again from commutativity of the local product and axiom (U); hence:

$$\begin{aligned} A \cdot A &= \triangle(1 \otimes \triangle)(1 \otimes fg^\circ \otimes fg^\circ)(1 \otimes \nabla)\nabla \\ &= \triangle(1 \otimes \triangle)(1 \otimes f \otimes f)(1 \otimes g^\circ \otimes g^\circ)(1 \otimes \nabla)\nabla \\ &= \triangle(1 \otimes f)(1 \otimes \triangle)(1 \otimes \nabla)(1 \otimes g^\circ)\nabla = \triangle(1 \otimes f)(1 \otimes g^\circ)\nabla = A. \end{aligned}$$

So, $A$ satisfies the conditions of the functional completeness axiom and there exists a map $i$ such that $ii^\circ = 1$ and $i^\circ i = A$; $i$ is the equalizer of $f$, $g$ in $\mathrm{Map}(\mathscr{W})$. First notice that $A$ is symmetric; now using the projection formula [Sect. 3, Remark 2] we get

$$\begin{aligned} Ag &= (1 \cdot fg^\circ)\, g = g \cdot f, \\ Af &= A^\circ f = (1 \cdot gf^\circ)\, f = f \cdot g. \end{aligned}$$

Hence $if = ig$. If $h : Z \to X$ is a map such that $hf = hg$, then consider $x = hi^\circ$; $x$ is a map, since

$$x\triangle = hi^\circ\triangle = h\triangle i^\circ\triangle(1 \otimes ii^\circ) = h\triangle(i^\circ \otimes i^\circ) = \triangle(x \otimes x),$$

using [Sect. 3, Theorem 1(4)] and the fact that $ii^\circ = 1$; and

$$\begin{aligned} x\top &= hi^\circ\top = hi^\circ i\top = h\Delta(1\otimes fg^\circ)\,\nabla\top = \Delta(h\otimes hfg^\circ)\,\nabla g\top \\ &= \Delta(h\otimes hgg^\circ)\,\nabla g\top = h\Delta(1\otimes g)(1\otimes g^\circ)\,\nabla g\top \\ &= h\Delta(g\otimes g)\,\nabla\top = hg\top = \top. \end{aligned}$$

So, $x$ is a map and easily one has that $xi = h$; $x$ is also unique since $i$ is a mono; thus $\mathrm{Map}(\mathscr{W})$ has all finite limits.

(2) From the definition of products and equalizers in $\mathrm{Map}(\mathscr{W})$, a pullback of

$$X \xrightarrow{p} Z \xleftarrow{f} Y$$

is a splitting $\langle i, i^\circ\rangle$ of the coreflexive $A = \Delta(1\otimes p_X pf^\circ p_Y^\circ)\nabla$; hence putting $i = \Delta(g\otimes q)$ we get

$$1 = ii^\circ = \Delta(g\otimes q)(g^\circ\otimes q^\circ)\,\nabla = gg^\circ\cdot qq^\circ.$$

Now an easy computation shows that

$$A = (\Delta\otimes 1)(1\otimes pf^\circ\otimes 1)(1\otimes\nabla),$$

from which

$$(g^\circ\otimes q^\circ)\,\nabla\Delta(g\otimes f) = (\Delta\otimes 1)(1\otimes g^\circ f\otimes 1)(1\otimes\nabla);$$

but again it is not hard to show that

$$(g^\circ\otimes q^\circ)\,\nabla\Delta(g\otimes q) = (\Delta\otimes 1)(1\otimes g^\circ q\otimes 1)(1\otimes\nabla).$$

Now precomposing with $(\perp\otimes 1)$ and postcomposing with $(1\otimes\top)$ and using the definition of the involution we get $(pf^\circ)^\circ = (g^\circ q)^\circ$; hence $pf^\circ = g^\circ q$.

As for the converse, if $g$ and $q$ are two maps satisfying the stated equations it is easily seen that $i = \Delta(g\otimes q)$ is a map such that $ii^\circ = 1$ and $i^\circ i = A$ so that $\Delta(g\otimes q)$ is the equalizer of $p_X p$ and $p_Y f$; hence $gp = qf$ is a pullback. ∎

COROLLARY. *If $\mathscr{V}$ is a symmetric monoidal category in which idempotents split then* $\mathrm{Gal}(\mathscr{V})$ *is left exact and the forgetful functor* $\mathrm{Gal}(\mathscr{V})\to\mathscr{V}$ *preserves monomorphisms.*

*Proof.* We need to prove that $\mathscr{W} = \mathrm{Sep}_l(\mathscr{V})$ satisfies the functional completeness axiom. Let $X$ be a commutative separable algebra of $\mathscr{V}$ and let $A: X\to X$ be an endomorphism of $X$ in $\mathscr{V}$ satisfying $A\cdot A = A = A\cdot 1$.

Then $A$ is a symmetric idempotent and let $X' \xrightarrow{i} X \xrightarrow{p} X'$ be a splitting of $A$ in $\mathscr{V}$; we need to show that $X'$ has a commutative separable algebra structure for which $i$ is a coalgebra homomorphism and $p = i^\circ$. Using the fact that a splitting of $A$ is an equalizer or a coequalizer of the pair $A$ and 1 and that $\triangle(A \otimes A) = A\triangle$ as well as that $A = A^\circ$ (see Sect. 3, Theorem 1 (8)), we can prove that there exists a unique comultiplication $\triangle'$ on $X'$ for which $i$ is a homomorphism and a unique multiplication $\nabla'$ on $X'$ for which $p$ is a homomorphism. Easily one has that they are associative, commutative, and satisfy axiom (U). Equation (D) for $\triangle'$ and $\nabla'$ can be proved as follows: first observe that $i$ is also a multiplication homomorphism and similarly that $p$ is also a comultiplication homomorphism; then

$$\begin{aligned}\nabla'\triangle' &= \nabla' ip\triangle' = (i \otimes i)\ \nabla\triangle(p \otimes p) = (i \otimes i)(\triangle \otimes 1)(1 \otimes \nabla)(p \otimes p)\\ &= (i\triangle \otimes i)(p \otimes \nabla p) = (\triangle' \otimes 1)(i \otimes i \otimes i)(p \otimes p \otimes p)(1 \otimes \nabla')\\ &= (\triangle' \otimes 1)(1 \otimes \nabla').\end{aligned}$$

Define now the counit $\top'$ as $\top' = i\top$ and unit $\bot'$ as $\bot' = \bot p$; it is straightforward to prove the needed equations. Finally, let us show that $p = i^\circ$:

$$\begin{aligned}p^\circ &= (1 \otimes \bot\triangle)(1 \otimes p \otimes 1)(\nabla'\top' \otimes 1) = (1 \otimes \bot\triangle)(ip \otimes p \otimes 1)(\nabla' i\top \otimes 1)\\ &= (1 \otimes \bot\triangle)(i \otimes 1 \otimes 1)(\nabla pi\top \otimes 1) = i(1 \otimes \bot\triangle)(\nabla \otimes 1)(A \otimes 1)(\top \otimes 1)\\ &= i\triangle(A \otimes 1)(\top \otimes 1) = iA\triangle(\top \otimes 1) = iA = i,\end{aligned}$$

since (see the proof of Sect. 3, Theorem 1(8)) $\triangle(A \otimes 1) = A\triangle$. ∎

To reach the goal of proving that $\mathrm{Gal}(\mathscr{V})$ is a pretopos we will use stronger assumptions on $\mathscr{V}$. In the case of the category of finite dimensional vector spaces the following theorem is usually proved using the existence of a separable closure of a field.

THEOREM. *Let $\mathscr{V}$ be a compact closed category with coequalizers; then* $\mathrm{Gal}(\mathscr{V})$ *is an exact category and the forgetful functor* $\mathrm{Gal}(\mathscr{V}) \to \mathscr{V}$ *preserves monomorphisms and coequalizers.*

*Proof.* To show that $\mathrm{Gal}(\mathscr{V})$ is an *exact category* in the sense of Barr [B] let us first recall that $\mathrm{Gal}(\mathscr{V})$ is left exact by the previous lemma; so, we can say what an *equivalence relation*

$$R \underset{r_1}{\overset{r_0}{\rightrightarrows}} X$$

is in $\mathrm{Gal}(\mathscr{V})$: it is a *jointly monic pair* (which can be expressed by $\triangle(r_0 r_0^\circ \otimes r_1 r_1^\circ)\nabla = 1$ using the wscc-structure on $\mathscr{W} = \mathrm{Sep}_l(\mathscr{V})$), which is *reflexive* (i.e., there exists a map $\rho\colon X \to R$ such that $\rho r_0 = 1 = \rho r_1$), *symmetric* (i.e., there exists a map $\sigma\colon R \to R$ such that $\sigma r_0 = r_1$ and $\sigma r_1 = r_0$), and *transitive* (i.e., there exists a map $\tau : R \times_X R \to R$ such that $\tau r_0 = r_0' r_0$ and $\tau r_1 = r_1'$, $r_0'$ and $r_1'$ being the projections $R \times_X R \to R$ from the pullback of $r_0$ and $r_1$ in $\mathrm{Gal}(\mathscr{V})$). Now let

$$R \overset{r_0}{\underset{r_1}{\rightrightarrows}} X \xrightarrow{p} Y$$

be the coequalizer of $r_0$, $r_1$ in $\mathscr{V}$. Certainly $Y$ has a unique cocommutative coalgebra structure $\langle Y, \triangle, \top\rangle$ for which $p$ is a homomorphism and $p$ is the coequalizer in coalgebras; we need to show that $\langle Y, \triangle, \top\rangle$ is in fact a *commutative separable algebra.* Since $\mathscr{V}$ is *closed,* then for any $Z$ the diagram

$$R \otimes Z \overset{r_0 \otimes 1}{\underset{r_0 \otimes 1}{\rightrightarrows}} X \otimes Z \xrightarrow{p \otimes 1} Y \otimes Z$$

is a coequalizer diagram. Since $r_0, r_1$ is a *reflexive* pair also

$$R \otimes R \overset{r_0 \otimes r_0}{\underset{r_1 \otimes r_1}{\rightrightarrows}} X \otimes X \xrightarrow{p \otimes p} Y \otimes Y$$

is a coequalizer diagram. Consider now the arrow

$$(r_0^\circ \otimes r_1^\circ)\nabla : X \otimes X \to R;$$

we want to show that such an arrow coequalizes $r_0 \otimes r_0$ and $r_1 \otimes r_1$; due to the characterization of pullbacks in $\mathrm{Gal}(\mathscr{V})$ contained in Lemma 1 it is enough to show that in any left exact category a pullback of $(r_0 \times r_0)$ and $\langle r_0, r_1\rangle$ is as well a pullback of $(r_1 \times r_1)$ and $\langle r_0, r_1\rangle$, which can be easily checked using that $\langle r_0, r_1\rangle$ is a symmetric and transitive relation. So, *a fortiori* the arrow $(r_0^\circ \otimes r_1^\circ)\,\nabla\top$ coequalizes $r_0 \otimes r_0$ and $r_1 \otimes r_1$; hence there exists a unique arrow

$$\varepsilon' : Y \otimes Y \to I$$

such that $(p \otimes p)\varepsilon' = (r_0^\circ \otimes r_1^\circ)\,\nabla\top$. Easily one can prove that the following equations are true:

$$\triangle'\varepsilon' = \top' \qquad \text{and} \qquad (\triangle' \otimes 1)(1 \otimes \varepsilon') = (1 \otimes \triangle')(\varepsilon' \otimes 1)$$

(using reflexivity for the first equation). By defining $\nabla' = (\triangle' \otimes 1)(1 \otimes \varepsilon')$ one can prove as in [LA] that $\triangle'$ and $\nabla'$ satisfy axioms (D) and (U). Using now that $\mathscr{V}$ is compact closed, we can conclude as in the theorem of Section 2 that the above structure on $Y$ is a commutative separable algebra structure. It remains to show that the kernel pair of $p$ in $\mathrm{Gal}(\mathscr{V})$ is $\langle r_0, r_1\rangle$ and that coequalizers are stable under pullback. Since

$$(pp^\circ \otimes 1)\ \nabla\top = (p\otimes p)\ \nabla\top = (r_0^\circ \otimes r_1^\circ)\ \nabla\top = (r_0^\circ r_1 \otimes 1)\ \nabla\top,$$

from compact closedness we get $pp^\circ = r_0^\circ r_1$; since $\langle r_0, r_1\rangle$ is monic, the characterization of pullbacks in $\mathrm{Gal}(\mathscr{V})$ mentioned above ensures that the kernel pair of $p$ is $\langle r_0, r_1\rangle$. As for the stability of coequalizers in $\mathrm{Gal}(\mathscr{V})$, first observe that from their definition and the closedness of $\mathscr{V}$ it easy to see that they are stable under products; hence it is enough to show that they are stable under pulling back along monos. So let

$$\begin{tikzcd} X \arrow[r, "p"] \arrow[d, "g"'] & U \arrow[d, "f"] \\ Y \arrow[r, "q"'] & V \end{tikzcd}$$

be a pullback diagram in $\mathrm{Gal}(\mathscr{V})$, where $q$ is a regular epi and $f$ (hence $g$) is a mono. First observe that $p$ is an *epimorphism in* $\mathscr{V}$ (hence in $\mathrm{Gal}(\mathscr{V})$): let $x$, $y$ be morphisms of $\mathscr{V}$ such that $px = py$; then $g^\circ px = g^\circ py$; but from the characterization of pullbacks in $\mathrm{Gal}(\mathscr{V})$ we get $g^\circ p = qf^\circ$, so that $qf^\circ x = qf^\circ y$; recalling the construction of regular epis in $\mathrm{Gal}(\mathscr{V})$, we have that $q$ is an epi in $\mathscr{V}$, hence $f^\circ x = f^\circ y$; finally, since $f$ is a mono in $\mathrm{Gal}(\mathscr{V})$, i.e., $ff^\circ = 1$, we get $x = y$. So $\mathrm{Gal}(\mathscr{V})$ is a left exact category in which for every object $X$ the equivalence relations on $X$ correspond bijectively to quotient objects of $X$ and a pullback of a regular epi is an *epi*; it is quite easy to prove that in any such category every arrow factors through a regular epi and a mono. Let $p'i = p$ be the factorization of $p$ into a regular epi followed by a mono in $\mathrm{Gal}(\mathscr{V})$; since $i$ is a mono, i.e., $ii^\circ = 1$, we have that $p' = pi^\circ$; since $pi^\circ i = p'i = p$ and $p$ is an epi in $\mathscr{V}$, we have $i^\circ i = 1$; hence $p$ is a regular epi. ▮

*Remarks.* (A) The hypotheses of the theorem are satisfied by the following examples:

(1) $\mathscr{V}$ is the category $k\text{-Vect}_{f.d.}$ of finite dimensional vector spaces on a field $k$.

(2) $\mathscr{V}$ is the category $\mathrm{Rep}_k(G)$ of finite dimensional linear representations of a finite group $G$.

(3) $\mathscr{V}$ is the *category of motifs* $M(k)$, which is compact closed and is abelian *modulo* the standard conjectures in Algebraic Geometry (see [SR, MN]).

(B) In the following examples the hypotheses are not verified;

however, we can still prove under different assumptions on $\mathscr{V}$ that Gal($\mathscr{V}$) is an exact category:

(1) The classical Galois Theory has been generalized in the direction of considering an arbitrary commutative ring $k$ as the ring of coefficients (see, e.g., [M] and the reference there). The obstruction here is the following: a commutative separable algebra in $k$-mod is certainly a finitely generated projective module and the category $\mathscr{V}$ of such modules is compact closed, but does not have coequalizers. $\mathscr{V}$ has the splitting of idempotents, so that Gal($\mathscr{V}$) is left exact; about the exactness, we can observe that in the proof of the theorem above the assumption that $\mathscr{V}$ is compact closed can be weakened to just closedness and still we will be able to prove something, namely that every equivalence relation in Gal($\mathscr{V}$) has a coequalizer in *cocommutative coseparable coalgebras*; this last notion means a cocommutative coalgebra for which there exists a (unique, commutative) multiplication satisfying axioms (D) and (U) (see e.g., [LA] or [M], where it is called *locally strongly separable algebra*). Such a notion corresponds to the *infinite Galois Theory* and could be developed abstractly by defining Gal($\mathscr{W}$) for any symmetric monoidal category $\mathscr{W}$ to be the category of cocommutative coseparable coalgebras and coalgebra homomorphisms between them and proving that under suitable hypotheses on $\mathscr{W}$ the category Gal($\mathscr{W}$) is actually a *Grothendieck topos.* These hypotheses on $\mathscr{W}$ should be the ones true for $\mathscr{W} = k$-Mod, namely that $\mathscr{W}$ is a closed cocomplete category and that the subcategory $\mathscr{V}$ of $\mathscr{W}$ determined by strongly dualizable objects is a generating category for $\mathscr{W}$ in an appropriate sense. In developing such an abstract theory it could be useful to notice the remarkable resemblance of the infinite Galois Theory with the abstract theory of partial maps as developed in [C] as it has been useful to notice the resemblance of the ordinary Galois Theory with the abstract theory of relations developed in [C-W].

(2) Other symmetric monoidal categories which do not satisfy the hypotheses of the theorem are the categories of relations and of sup-lattices. However, our abstract theory applies as well if we consider other properties that such categories have and it will be done in the corresponding section.

## 5. Matrices

To prove that the Galois Category Gal($\mathscr{V}$) of a compact closed category $\mathscr{V}$ with coequalizers is a *pretopos* we need to consider another property that $\mathscr{V}$ can have, namely that $\mathscr{V}$ is also *preadditive.* Certainly the first three examples mentioned in the remarks at the end of the last section satisfy this condition. We will use the technique of considering the category $\mathscr{W} = \mathrm{Sep}_l(\mathscr{V})$ equipped with the canonical wscc-structure:

LEMMA 1. *If $\mathscr{V}$ is a (compact)-closed symmetric monoidal category which is preadditive, then $\mathscr{W} = \mathrm{Sep}_l(\mathscr{V})$ enjoys the following properties with respect to the canonical* wscc-*structure*:

(1) *$\mathscr{W}$ is preadditive*;

(2) *the injections $i_X : X \to X \oplus Y$ are maps and projections $p_X : X \oplus Y \to X$ are algebra homomorphisms.*

*Proof.* If $\langle X, \triangle, \nabla, \top, \perp \rangle$ and $\langle Y, \triangle', \top', \top', \perp' \rangle$ are commutative separable algebras of $\mathscr{V}$, then the direct sum $X \oplus Y$ has a unique commutative separable algebra structure for which the injections are coalgebra homomorphisms and the projections are algebra homomorphisms: just define the comultiplication on $X \oplus Y$ as the unique arrow induced on the direct sum by $\triangle(i_X \otimes i_X)$ and $\triangle(i_Y \otimes i_Y)$; similarly for the counit; the multiplication and the unit can be defined in the same way using the projections. Associativity, commutativity, and unit axioms are easily checked as well as axiom (U). To prove axiom (D), first observe that injections are also multiplication homomorphisms $(i_X \otimes i_X) \nabla = \nabla i_X$, since composing both sides with projections we get equal morphisms

$$(i_X \otimes i_X) \nabla p_X = (i_X p_X \otimes i_X p_X) \nabla = \nabla = \nabla i_X p_X,$$

using that additivity implies $i_X p_X = 1$;

$$\begin{aligned}(i_X \otimes i_X) \nabla p_Y &= (i_X p_Y \otimes i_X p_Y) \nabla = (0_{X,Y} \otimes 0_{X,Y}) \nabla = 0_{X \otimes Y} \nabla \\ &= 0_{X \otimes X, Y \otimes Y} \nabla = 0_{X \otimes X, Y} = \nabla i_X p_Y,\end{aligned}$$

using that additivity implies that the composite $i_X p_Y$ is the zero arrow $0_{X,Y}$ and that closedness implies that tensoring preserves zero maps. In a similar way we can also prove that projections are comultiplication homomorphisms. From this one easily has

$$\begin{aligned}(p_X i_X \otimes p_X i_X)(\triangle \otimes 1)((1 \otimes \nabla) &= (p_X \otimes p_X)(\triangle \otimes 1)(1 \otimes \nabla) i_X \otimes i_X) \\ &= (p_X \otimes p_X) \nabla \triangle (i_X \otimes i_X) = \nabla p_X i_X \triangle,\end{aligned}$$

and similarly with $p_Y i_Y$; now adding both sides of the two equations and using that additivity and closedness imply that

$$(p_X i_X \otimes p_X i_X) + (p_Y i_Y \otimes p_Y i_Y) = 1,$$

we get axiom (D). So, $\mathscr{W}$ has biproducts such that injections are maps and projections are algebra homomorphisms. Notice that due to the closedness of $\mathscr{V}$, the zero object $Z$ of $\mathscr{V}$ has a unique commutative separable algebra structure, so that is also a zero object in $\mathscr{W}$. ∎

The above lemma motivates the following:

DEFINITION 1. Let $\mathscr{W}$ be a symmetric monoidal category equipped with a wscc-structure. The wscc-structure on $\mathscr{W}$ is called distributive if:

(1) $\mathscr{W}$ is preadditive;

(2) injections $i_X : X \to X \oplus Y$ are maps and projections $p_X : X \oplus Y \to X$ are algebra homomorphisms. ∎

LEMMA 2. *Let $\mathscr{W}$ be a symmetric monoidal category equipped with a distributive* wscc-*structure. Then*:

(1) Map($\mathscr{W}$) *has finite sums stable under products*;

(2) *if $\mathscr{W}$ is functionally complete, then in* Map($\mathscr{W}$) *the initial object is strict, the injections are mono, and the sums are disjoint and universal.*

*Proof.* (1) It is enough to show that the codiagonal $\delta_X : X \oplus X \to X$ is a map and the sum $f \oplus g$ of maps is a map. This is a straightforward calculation, since to prove the needed equations it is enough to show that composing with injections on both sides of the equations we get equality; this follows by the condition requiring injections to be maps. So Map($\mathscr{W}$) has sums. Stability of sums under products means that the canonical arrow

$$\begin{pmatrix} 1 \otimes i_Y \\ 1 \otimes i_Z \end{pmatrix} : (X \otimes Y) \oplus (X \otimes Z) \to X \otimes (Y \oplus Z)$$

is invertible in Map($\mathscr{W}$). But this arrow is a map and is invertible in $\mathscr{W}$ since $\mathscr{W}$ is (compact)-closed; hence by Section 3, Theorem 1(7) we get that it is invertible in Map($\mathscr{W}$). Finally the initial arrow $0_X : Z \to X$ is easily seen to be a map, so that Map($\mathscr{W}$) has an initial object $Z$ and with considerations such as the above ones we can see that the canonical arrow $Z \to X \otimes Z$ is invertible in Map($\mathscr{W}$).

(2) First notice that projections are the opposites of injections:

$$\begin{aligned} i^\circ &= (\perp \triangle \otimes 1)(1 \otimes i \otimes 1)(1 \otimes \triangledown \top) = (\perp \triangle \otimes 1)(ip \otimes 1 \otimes 1)(1 \otimes \triangledown \top) \\ &= (\perp \times 1)(i \otimes 1)(\triangle \otimes 1)(1 \otimes \triangledown)(1 \otimes \top)\, p = (\perp \otimes 1)(i \otimes 1) \triangledown p \\ &= (\perp \otimes 1)(ip \otimes p) \triangledown = (\perp \otimes 1)(1 \otimes p) \triangledown = p(\perp \otimes 1) \triangledown = p. \end{aligned}$$

We can also see easily that the opposite of the initial map $0_X : Z \to X$ is the terminal map so that the zero arrow $0_{X,Y} : X \to Y$ is $0_{X,Y} = 0_X^\circ 0_Y$. Now, if the wscc-structure of $\mathscr{W}$ is functionally complete, then Map($\mathscr{W}$) is left exact and by the characterization of pullbacks of Section 4, Lemma 1(2) it is immediately seen that injections are mono ($i_X i_X^\circ = 1$), sums are disjoint

($i_X i_Y^\circ = 0_X^\circ 0_Y$), and similarly that the initial object is strict. As for the universality, since sums are stable under products, it is enough to show that sums are universal along monos. This can be shown by a tedious but straightforward computation which uses besides the previous remarks, the remaining equation of additivity, namely $i_X^\circ i_X + i_Y^\circ i_Y = 1$. ∎

The following theorem sumarizes all the matter so far developed:

THEOREM. *Let $\mathscr{V}$ be a symmetric monoidal category; then:*

(1) Gal($\mathscr{V}$) *is isomorphic to the dual category of the category of commutative separable algebras in* $\mathscr{V}$; Gal($\mathscr{V}$) *is a cartesian category and the forgetful functor* Gal($\mathscr{V}$) $\to \mathscr{V}$ *reflects isomorphisms;*

(2) *if idempotents split in* $\mathscr{V}$ *then* Gal($\mathscr{V}$) *is left exact and the forgetful functor preserves monomorphisms;*

(3) *if* $\mathscr{V}$ *is closed and preadditive, then* Gal($\mathscr{V}$) *has finite sums stable under products and the forgetful functor preserves them; if, moreover, idempotents split in* $\mathscr{V}$, *then* Gal($\mathscr{V}$) *is a left exact category with finite sums which are disjoint and universal and it has a strict initial object;*

(4) *if* $\mathscr{V}$ *is a compact closed category with coequalizers, then* Gal($\mathscr{V}$) *is an exact category and the forgetful functor preserves coequalizers; hence from* (3) *if* $\mathscr{V}$ *is also preadditive, then* Gal($\mathscr{V}$) *is a pretopos.*

## 6. GROUP REPRESENTATIONS

Let $G$ be a profinite group, let $k$ be a field, and let $\mathrm{Rep}_k^c(G)$ be the category of continuous representations of $G$ in discrete finite dimensional $k$-vector spaces. Recall that a representation of $G$ in a discrete vector space $V$ is *continuous* if the stabilizer of each vector of $V$ is an open subgroup of $G$. We will show that the theory so far developed provides a precise characterization of such categories.

To reach such a goal we first have to prove a further property that the categories of the form Gal($\mathscr{V}$) can have for convenient $\mathscr{V}$'s, namely the one given by the following:

THEOREM 1. *If* $\mathscr{V}$ *is a compact closed, additive category with (co)-equalizers, then* Gal($\mathscr{V}$) *is a boolean pretopos.*

*Proof.* Booleaness of Gal($\mathscr{V}$) can be proved as follows. Since $\mathscr{V}$ is compact closed, we have an involution $(-)^*$ and denote by $\eta$ and $\varepsilon$ the unit and counit arrows; then notice that the bilinear map $\nabla\top : X \otimes X \to I$ gives rise to an isomorphism $\alpha_X : X \to X^* = (1 \otimes \eta)(\nabla\top \otimes 1)$, so that given a subobject $i : Y \hookrightarrow X$ of $X$ in Gal($\mathscr{V}$) we can define the subobject $Y^\perp$ of $X$ *orthogonal* to $Y$ as the kernel of the composite $\alpha_X i^*$. Notice that the $\alpha$'s are natural, i.e., $R^\circ\alpha = \alpha R^*$, so that $j : Y^\perp \to X$ can also be described as the kernel of $i^\circ\alpha$ and, $\alpha$ being invertible, also as the kernel of $i^\circ$. Now, $i^\circ$ is a split epi in $\mathscr{V}$; hence by the usual arguments that can be carried out in *additive* categories, the diagram

$$Y^\perp \xrightarrow{j} X \xrightarrow{i^\circ} Y$$

is a split short exact sequence, so that there exists an arrow $p : X \to Y^\perp$ for which $jp = 1$ and $pj + i^\circ i = 1$ (just consider the arrow $t = 1 - i^\circ i$, observe that $ti^\circ = 0$, and deduce that there exists a unique $p$ such that $pj = 1 - i^\circ i$), thus exhibiting $X$ as the direct sum of $Y^\perp$ and $Y$. We only need to show that $Y^\perp$ has a (unique) commutative separable algebra structure for which $j$ is a map and $p = j^\circ$: the fact that $ji^\circ = 0$ will then imply that $j$ is a *complement* of $i$ in Gal($\mathscr{V}$), due to the description of limits in Gal($\mathscr{V}$) (see Sect. 4, Lemma 1(2)).

Since $j = \ker(i^\circ)$, $p = \operatorname{coker}(i)$, and since $i$ is a comultiplication homomorphism, using that tensoring preserves the zero arrows, we get that there exist unique arrows $\triangle'$ and $\nabla'$ such that

$$p\triangle' = \triangle(p \otimes p) \qquad \text{and} \qquad \nabla' j = (j \otimes j)\nabla;$$

similarly, since $ipj\top = 0$ and $\perp pji^\circ = 0$, there exist unique $\top'$ and $\perp'$ such that

$$p\top' = pj\top \qquad \text{and} \qquad \perp' j = \perp pj.$$

To show that $j$ is a comultiplication homomorphism as well, first observe that using the distributivity of the tensor with local sums we get

$$\begin{aligned} \triangle &= \triangle[(i^\circ i + pj) \otimes (i^\circ i + pj)] \\ &= \triangle[(i^\circ i \otimes i^\circ i) + (i^\circ i \otimes pj) + (pj \otimes i^\circ i) + (pj \otimes pj)] \\ &= \triangle(i^\circ i \otimes i^\circ i) + \triangle(i^\circ i \otimes pj) + \triangle(pj \otimes i^\circ i) + \triangle(pj \otimes pj) \\ &= \triangle(i^\circ \otimes i^\circ) + \triangle(pj \otimes pj), \end{aligned}$$

since the two middle terms vanish, as can be seen using the functoriality of the tensor and the results of Section 3, Theorem 1(4), (5). So, using that $i$ is a mono in Gal($\mathscr{V}$), so that $i^\circ$ is also a comultiplication homomorphism (see Sect. 4, Remark (1)) and that $p$ is a comultiplication homomorphism, we get

$$j\triangle = j\triangle(i^\circ i \otimes i^\circ i) + j\triangle(pj \otimes pj) = ji^\circ\triangle(i \otimes i) + jp\triangle'(j \otimes j) = \triangle'(j \otimes j).$$

Finally, to show that $j$ is a counit homomorphism first notice that

$$p\top' = pj\top = (1 - i^\circ i)\top = \top - i^\circ\top,$$

since $i$ is a counit homomorphism; hence,

$$\top' = jp\top' = j\top - ji^\circ\top = j\top.$$

Now the equations for a commutative separable algebra structure on $Y^\perp$ are easily checked as well as $p = j^\circ$. ∎

Now recall that from Grothendieck Galois Theory we know that if $k$ is a *separably closed field*, then $\mathrm{Gal}(k\text{-Vect}_{f.d.})$ is equivalent to the category of finite sets; i.e., each finite dimensional vector space $V$ over $k$ has *an essentially unique* commutative separable algebra structure, so that modulo the choice of a basis for $V$ a commutative separable algebra structure on $V$ must be isomorphic to the one described in Section 1.

Lemma 1. *If $k$ is a separably closed field then the* $k$-Vect *enriched category* $\mathrm{Rep}_k^c(G)$ *equipped with the forgetful functor*

$$\begin{array}{c} \mathrm{Rep}_k^c(G) \\ \downarrow{\scriptstyle \omega_G} \\ k\text{-}\mathrm{Vect}_{f.d.} \end{array}$$

*enjoys the following properties:*

(1) $\mathrm{Rep}_k^c(G)$ *is a compact closed, exact (thus abelian) category and $\omega_G$ is an exact, faithful, strong monoidal functor;*

(2) *the objects equipped with a commutative separable algebra structure in* $\mathrm{Rep}_k^c(G)$ *generate;*

(3) *if $X$ is an object equipped with a commutative algebra structure, then the vector space of equivariant maps $k \to X$ is spanned by the finite set of coalgebra homomorphisms $k \to X$.*

*Proof.* Everything being standard, we only need a few comments on items (2) and (3). If

$$\langle \alpha : G \to \mathrm{Aut}(V) \rangle$$

is a representation of $G$ in the $k$-vector space $V$, then $\triangle_V$, $\top_V$, $\nabla_V$, $\perp_V$ are equivariant maps iff for each $g \in G$ the automorphism $\alpha_g$ of $V$ is an algebra and a coalgebra homomorphism; but this precisely means that $\alpha_g$ is induced by a permutation on the basis of $V$, so that the Galois Category of $\mathrm{Rep}_k^c(G)$ is equivalent the topos of continuous representation of $G$ in finite sets.

If $T = \langle \alpha : G \to \mathrm{Aut}(V) \rangle$ is a continuous representation of $G$ then let $B = \{v_1, ..., v_n\}$ be a basis of $V$ and consider for each $v_i$ the stabilizer $H_i$ of $v_i$; since the representation is continuous, the $H_i$ are normal subgroups of finite index of $G$; so let $G_i$ be the finite groups $G_i = G/H_i$, let $U$ be the finite set $U = \{\langle [u], i \rangle \mid [u] \in G_i\}$, and let $X$ be the vector space generated by $U$; $X$ is nothing but the sum $\sum_{i=1}^n F(G_i)$ in $\mathrm{Rep}_k^c(G)$ where the $F(G_i)$ are the free vector spaces on $G_i$ equipped with the action induced on the basis; so $G$ acts on $U$ by multiplication on the first component and consider $X$ equipped with the induced (continuous) action; let $p : X \to V$ be the linear map whose definition on generators is $p([u], i) = \alpha(u)(v_i) \stackrel{\text{def}}{=} uv_i$; $r$ is well defined, since if $u \simeq u'$ (mod $H_i$) then $u^{-1}u' \in H_i$ so that $u^{-1}u'v_i = v_i$, hence $uv_i = u'v_i$; easily one verifies that $p$ is equivariant; clearly $p$ is surjective, since it has a splitting $s$ defined as $s(v_i) = \langle 1, i \rangle$ (which is *not* equivariant), and $X$ is equipped with a commutative separable algebra structure in $\mathrm{Rep}_k^c(G)$. So, in $\mathrm{Rep}_k^c(G)$ every object is *canonically* a quotient of a sum of objects equipped with a separable algebra structure and one can see that every map between two objects arises from a map between their canonical presentations.

Item (3) means that if $V$ is a vector space with an action of $G$ induced by a permutation representation of $G$ on the basis, then every equivariant map $k \to V$ is a linear combination of vectors of the basis which are fixed under the action of $G$. ∎

Our aim is to prove that in fact the above properties *characterize* the categories of linear representations of profinite groups over any separably closed field $k$ as follows:

THEOREM 2. *Let $\mathscr{V}$ be a small category enriched over finite dimensional k-vector spaces and suppose that*:

(1) *$\mathscr{V}$ is compact closed and exact (thus abelian)*;

(2) *there exists an exact, strong monoidal and faithful functor*

$$\omega : \mathscr{V} \to k\text{-Vect};$$

(3) *the objects of $\mathscr{V}$ equipped with a commutative separable algebra structure generate*;

(4) *if $X$ is equipped with a commutative separable algebra structure, then the vector space $\mathscr{V}$ $(I, X)$ is spanned by the finite set of coalgebra homomorphisms $I \to X$*;

*then there exists a profinite group G and a strict monoidal equivalence*

$$\mathrm{Rep}_k^c(G) \simeq \mathscr{V}$$

*which identifies $\omega$ to the forgetful functor; moreover the functor $\omega$ is unique up to a natural isomorphism.*

*Proof.* Since $\omega$ is strong monoidal and faithful and since $k$ is separably closed, the category $\mathrm{Sep}_I(\mathscr{V})$ is equivalent to a subcategory of $\mathscr{V}$; hence the composite

$$\mathrm{Gal}(\mathscr{V}) \to \mathscr{V} \to k\text{-}\mathrm{Vect}_{f.d.}$$

factors through the free vector space functor $S_{\mathrm{fin}} \to k\text{-}\mathrm{Vect}_{f.d.}$ into a functor

$$\omega : \mathrm{Gal}(\mathscr{V}) \to S_{\mathrm{fin}}.$$

Since $\mathscr{V}$ is compact closed and abelian, from Theorem1 we know that $\mathrm{Gal}(\mathscr{V})$ is a boolean pretopos and that $\omega$ restricts to a pretopos morphism which from Section 3, Theorem 1(7) reflects isomorphisms; so, $\mathrm{Gal}(\mathscr{V}) \xrightarrow{\omega} S_{\mathrm{fin}}$ is a *Galois category*, and hence from the characterization theorem of Grothendieck (see [SGA-1, p. 118]) we have that there exists a profinite group $G$ and an equivalence

$$\mathrm{Gal}(\mathscr{V}) \simeq \mathrm{Rep}_k^c(G)$$

which identifies $\omega : \mathrm{Gal}(\mathscr{V}) \to S_{\mathrm{fin}}$ to the forgetful functor $\omega_G$ and moreover that the functor $\omega$ is unique up to a natural isomorphism.

It remains to show that everything is determined by $\omega_G$. From (4) we know that $\omega_G$ determines the restriction $\mathrm{Sep}_I(\mathscr{V}) \to k\text{-Vect}$ of $\omega$, since if $X$ and $Y$ are objects of $\mathscr{V}$ equipped with a commutative separable algebra structure, then $\mathscr{V}(X, Y) \simeq \mathscr{V}(I, X \otimes Y)$ by duality; but property (4) ensures that $\mathscr{V}(I, X \otimes Y)$ is spanned by $\mathrm{Gal}(\mathscr{V})(I, X \otimes Y)$. So, $\mathrm{Sep}_I(\mathscr{V}) \to k\text{-}\mathrm{Vect}_{f.d.}$ is determined by $\omega_G$ and is equivalent to the full subcategory of $\mathrm{Rep}_k^c(G)$ determined by the continuous representations of $G$ on discrete finite sets. Property (3) then ensures that from $\omega_G$ we can reconstruct the whole of $\omega$. ∎

Notice that if we drop conditions (3) and (4) in the theorem, we are still able to prove that there exists a profinite group $G$ such that $\mathrm{Gal}(\omega)$ is isomorphic to $\omega_G$: $[G, S_{\mathrm{fin}}]_c \to S_{\mathrm{fin}}$($[G, S_{\mathrm{fin}}]_c$ being the category of continuous representations of $G$ in finite discrete sets); axioms (3) and (4) are needed to reconstruct $\mathscr{V}$ as $\mathrm{Rep}_k^c(G)$.

## 7. Relations and Sup-Lattices

The construction of the category of relations is a basic one in mathematics. From the recent developments of category theory it is well understood that the categories $\mathscr{E}$ where the construction of the category $\mathrm{Rel}(\mathscr{E})$ of relations in $\mathscr{E}$ can be carried out and the usual elementary properties of relations and functions can be proved, are precisely the *regular* categories in the sense of [B], i.e., left exact categories for which kernel pairs have pull-back stable coequalizers. Clearly the problem of having an elementary characterization of those categories which appear as categories of relations arises. In the case of additive relations this problem was first discussed by MacLane (see [ML]), and Puppe [P] gave a solution. The more general case of relations defined in regular categories has been discussed in the Perugia Notes of Lawvere (see [L1]), and Freyd gave a solution to the problem of their characterization in terms of the theory of "allegories" (see [F1]). Other characterizations have been carried out by various authors, including the writer (see [C-W]), but the one contained in [C-W] is basically in terms of the abstract notion of a commutative separable algebra used here; there the motivations were to have a more transparent theory of relations, formulated in the flexible and meaningful language of linear algebra; however, the real meaning of the basic axiom we found then (which is axiom (D)) was not completely clear to us, unit the discovery of the theorem in Section 2. So, we now would like to give a bird's-eye view of the axiom in the study of relations with the fuller consciousness given by the understanding of it in genuine linear algebra carried out in the last sections, referring to the quoted paper for a more detailed study.

The basic idea is the same as in Section 1: the category of relations is a symmetric monoidal category and we still have the regular category $\mathscr{E}$ embedded *not fully* in $\mathrm{Rel}(\mathscr{E})$ by means of the *graph* functor

$$\Gamma : \mathscr{E} \to \mathrm{Rel}(\mathscr{E});$$

$\Gamma$ is a strong monoidal functor and since $\mathscr{E}$ is cartesian, it factors through the category of cocommutative coalgebras in $\mathrm{Rel}(\mathscr{E})$; easily one can check that *$\Gamma$ factor fully and faithfully*, which means that *a relation is the graph of a (unique) function iff it is a coalgebra homomorphism with respect to the coalgebra structures given by the graphs of the diagonal and of the terminal maps.* Again the problem arises of recognizing the coalgebra structure on an object $X$ of $\mathrm{Rel}(\mathscr{E})$ arising from the diagonal and the terminal in $\mathscr{E}$ among all possible coalgebra structures.

First observe that $\mathrm{Rel}(\mathscr{E})$ is not merely a monoidal category, but has the richer structure of an *order enriched* monoidal category, meaning that each hom-set is in fact an ordered set and composition and tensor are order preserving in each variable. With this richer structure it is a basic fact that *a relation $R$ is the graph of a (unique) function iff it has a right adjoint $R^*$* ($R \dashv R^*$), i.e., *a relation $R^*$ in the opposite direction such that* $1 \leqslant RR^*$ and $R^*R \leqslant 1$. So, a condition on the graphs $\triangle_X$ of the diagonal and $\top_X$ of the terminal must be to have right adjoints $\triangledown_X$ and $\bot_X$.

This last condition certainly characterizes those coalgebra structures in Rel($\mathscr{E}$) which arise from the diagonal in $\mathscr{E}$. So, it looks like we pointed out enough structure to be able to characterize those order enriched symmetric monoidal categories $\mathscr{V}$ which appear as categories of relations: on each object $X$ of $\mathscr{V}$ should be given a cocommutative coalgebra structure

$$\triangle_X : X \to X \otimes X \qquad \text{and} \qquad \top_X : X \to I$$

such that $\triangle_X$ and $\top_X$ have right adjoints $\triangledown_X$ and $\bot_X$; however, as we start to work with this definition we would struggle with the two possibilities we have to define the category $\mathscr{E}$ of "functions" out of the category $\mathscr{V}$ of "relations": one is the category of coalgebra homomorphisms with respect to the given coalgebra structure on each object, and the other is the category determined by the arrows of $\mathscr{V}$ which have right adjoints; this latter is completely determined by $\mathscr{V}$ as an order enriched category, whereas the first depends upon the tensor product and the choice of the coalgebra structure on each object: certainly we neglected part of the structure!

One basic question is the uniqueness of the structure of a commutative coalgebra on each object of $\mathscr{V}$. In the case of relations there is an elementary condition on the category which ensures the uniqueness of the commutative separable algebra structure on each object: just observe that in the category Rel($\mathscr{E}$) of relations, the cocommutative coalgebra structures on each object $X$ given by the graphs $\triangle_X$ of the diagonal and $\top_X$ of the terminal in the base category $\mathscr{E}$ enjoy an obvious *categorical* property, namely the $\triangle$'s and the $\top$'s are the components of *lax natural, monoidal transformations*

$$\triangle : 1_{\mathscr{V}} \Rightarrow 1_{\mathscr{V}} \otimes 1_{\mathscr{V}} \qquad \text{and} \qquad \top : 1_{\mathscr{V}} \Rightarrow I_{\mathscr{V}},$$

where $I_{\mathscr{V}}$ denotes the constant functor whose value is the identity object $I$; lax naturality means that for each relation $R : X \to Y$ we have

$$R \triangle Y \leqslant \triangle_X (R \otimes R) \qquad \text{and} \qquad R \top_Y \leqslant \top_X, \tag{LN}$$

and monoidalness means that

$$\triangle_{X \otimes Y} = (\triangle X \otimes \triangle_Y)(1 \otimes c_{X,Y} \otimes 1) \qquad \text{and} \qquad \top_{X \otimes Y} = \top_X \otimes \top_Y; \tag{M}$$

moreover the $I$th component of $\top$ determined as

$$\top_I = 1_I. \tag{Id}$$

LEMMA 1. *Let $\mathscr{V}$ be a symmetric monoidal category enriched over ordered sets. If $\mathscr{V}$ is equipped with a pair of lax natural, monoidal transformations $\triangle : 1_{\mathscr{V}} \Rightarrow 1_{\mathscr{V}} \otimes 1_{\mathscr{V}}$ and $\top : 1_{\mathscr{V}} \Rightarrow I_{\mathscr{V}}$ satisfying axioms* (Id) *and counit, then such a pair is unique.*

*Proof.* If $\triangle'$ and $\top'$ is any other such a pair for which axiom (Id) holds, then certainly $\top = \top'$ due to lax naturality and axiom (Id); then using again lax naturality and monoidalness it is easy to see that the two comultiplications on each object are homomorphisms with respect to each other; so, having the same counit, the comultiplication version of the Eckman–Hilton argument shows that they are equal.[1] ∎

We are not yet finished: the category of coalgebra homomorphisms still depends on the structure of the tensor product on $\mathscr{V}$, whereas the category of arrows with right adjoint depends on the local order of $\mathscr{V}$ and it seems that we are not yet able to show what is true in categories of relations. A relation is a coalgebra homomorphism with respect to the coalgebra structure given by the graphs of the diagonal and the terminal maps iff it has a right adjoint. So, we are forced to look for something else we neglected and that would allow us to prove such a statement.

Another basic fact about categories of relations which has not appeared yet is the operation of *transposition* of a relation or, more generally, the fact that *the symmetric monoidal category of relations is compact closed, and the involution is the identity on objects.* From the discussion in Section 1, we know that such a structure is equivalent to giving the adjunction arrows

$$\eta_X : I \to X \otimes X \qquad \text{and} \qquad \varepsilon_X : X \otimes X \to I$$

satisfying the adjunction equations (see Section 1, (C)). As in the case of commutative rings, by defining $\eta_X$ and $\varepsilon_X$ as $\eta_X = \perp_X \triangle_X$ and $\varepsilon_X = \nabla_X \top_X$, we can prove that the adjunction equations are verified since also in the case of relations the basic equations

$$(1 \otimes \triangle)(\nabla \otimes 1) = \nabla \triangle = (\triangle \otimes 1)(1 \otimes \nabla) \tag{D}$$

hold for the graph of the diagonal and its adjoint, as one can easily verify. Notice that due to the adjunction $\triangle \dashv \nabla$, we already have that $\nabla \triangle \leqslant (\triangle \otimes 1)(1 \otimes \nabla)$: from the coassociativity $\triangle(\triangle \otimes 1) = \triangle(1 \otimes \triangle)$ of $\triangle$ and from the adjunctions $\triangle \dashv \nabla$ and $(1 \otimes \triangle) \dashv (1 \otimes \nabla)$ we get the

[1] This argument has been basically suggested by G. M. Kelly.

claimed inequality. Notice also that one of the two equations (D) forces the other.

The axioms which emerge from the above discussion are summarized by the following:

DEFINITION 1. A symmetric monoidal category $\mathscr{V}$ enriched over ordered sets is called a "bicategory of relations" when it is equipped with two lax natural, monoidal transformations

$$\triangle : 1_{\mathscr{V}} \otimes 1_{\mathscr{V}} \qquad \text{and} \qquad \top : 1_{\mathscr{V}} \Rightarrow I_{\mathscr{V}}$$

satisfying the following axioms:

(1) the components $\triangle_X$ and $\top_X$ satisfy the equations for a cocommutative coalgebra;

(2) $\top_I = 1_I$;

(3) each component $\triangle_X$ and $\top_X$ has a right adjoint $\nabla_X$ and $\perp_X$;

(4) the inequality given by coassociativity and adjointness is in fact an equality:

$$\nabla \triangle = (\triangle \otimes 1)(1 \otimes \nabla).$$

In [C-W] it is shown that the above definition is correct: in a bicategory of relations $\mathscr{V}$ we can prove that an arrow is a coalgebra homomorphism iff has a right adjoint, iff the transpose is a right adjoint; moreover, modulo a "functional completeness" axiom (see Sect. 4, Definition 2) we can show that the subcategory $\mathscr{E} = \mathrm{Map}(\mathscr{V})$ of $\mathscr{V}$ determined by coalgebra homomorphisms (equivalently by arrows with right adjoint) is a regular category and that $\mathrm{Rel}(\mathscr{E}) \simeq \mathscr{V}$. It can also be proved that the above definition is a bit redundant, since it is not hard to see that coassociativity and cocommutativity of $\triangle_X$ follow from lax naturality, monoidalness, and axiom (3): since every arrow with right adjoint is in fact a *strict* coalgebra homomorphism, we get: $\triangle_X \triangle_{X \otimes X} = \triangle_X(\triangle_X \otimes \triangle_X)$; so from the monoidalness of $\triangle$ we get

$$\triangle_X(\triangle_X \otimes \triangle_X)(1 \otimes c_{X,X} \otimes 1) = \triangle_X(\triangle_X \otimes \triangle_X),$$

from which using the counit we can prove cocommutativity and coassociativity. The above discussion motivates the following:

DEFINITION 2. An adjoint commutative separable algebra in an order enriched, symmetric monoidal category $\mathscr{V}$ is a cocommutative coalgebra

$$\triangle : X \to X \otimes X \qquad \text{and} \qquad \top : X \to I$$

such that:

(A) $\triangle$ and $\top$ have right adjoints $\triangledown$ and $\perp$;

(D) the inequality given by coassociativity of $\triangle$ and by the adjunction $\triangle \dashv \triangledown$ is in fact an equality

$$\triangledown \triangle = (1 \otimes \triangle)(\triangledown \otimes 1).$$

Notice that from the above axioms it follows that the unit $1 \leqslant \triangle \triangledown$ of the adjunction is an equality,

$$\triangle \triangledown = 1, \tag{U}$$

since $\triangle \triangledown = \triangle (1 \otimes 1) \triangledown \leqslant \triangle (\top \perp \otimes 1) \triangledown = \triangle (\top \otimes 1)(\perp \otimes 1) \triangledown = 1$.

If $\mathscr{V}$ is an order enriched symmetric monoidal category, let us define the Adjoint Galois Category of $\mathscr{V}$ to be the order enriched, symmetric monoidal category $\mathrm{Gal}^a(\mathscr{V})$ given by adjoint commutative separable algebras in $\mathscr{V}$ and lax coalgebra homomorphisms between them. From the above discussion on relations we have that $\mathrm{Gal}^a(\mathrm{Rel}(\mathscr{E})) \simeq \mathrm{Rel}(\mathscr{E})$; the above definition is further supported by the following lemma, whose proof follows from [C-W, Remark 4.7 and Remark 2.9(iv)] and [J-T, Chap. V, Sect. 5], noting that by Prop. 1, p. 35 of [J-T], the arrow $\top : X \to I$ is automatically open once it admits an adjoint:

LEMMA 2. (1) *If $\mathscr{E}$ is an exact category and* $\mathrm{Ord}(\mathscr{E})$ *is the order enriched symmetric monoidal category of ordered objects in $\mathscr{E}$ and ideals between them, then*

$$\mathrm{Gal}^a(\mathrm{Ord}(\mathscr{E})) \simeq \mathrm{Rel}(\mathscr{E});$$

(2) *If $\mathscr{E}$ is an elementary topos and* $\mathrm{SL}(\mathscr{E})$ *is the order enriched symmetric monoidal category of sup-lattices in $\mathscr{E}$, then*

$$\mathrm{Gal}^a(\mathrm{Sl}(\mathscr{E})) \simeq \mathrm{Rel}(\mathscr{E}).$$

## ACKNOWLEDGMENTS

I would like to express particular thanks to: André Joyal and Bill Lawvere, whose encouragement and comments have been extremely useful; Bob Walters, who developed with me the abstract notion of well supported compact closed structure (see [W]) while I was in Sydney in January 1987 under the Australian Research Grants Scheme; and Mike Johnson, for reading the paper and pointing out many incomprehensible sentences I wrote.

## REFERENCES


[C] A. CARBONI, Bicategories of partial maps, *Cahiers Topologie Géom. Différentielle Catégoriques* **18-2** (1987), 111–126.

[CH] C. CHEVALLEY, "The Theory of Lie Groups," p. 211, Princeton Univ. Press, Princeton, NJ, 1946.

[C-W] A. CARBONI AND R. WALTERS, Cartesian bicategories I, *J. Pure Appl. Algebra* **49(1, 2)** (1987), 11–32.

[B] M. BARR, Exact categories, *in* "Exact Categories and Categories of Sheaves," pp. 1–120, Springer SLN, Vol. 236, Springer-Verlag, New York/Berlin, 1971.

[DM-I] F. DEMEYER AND E. INGRAHAM, "Separable Algebras over Commutative Rings," Springer SLN, Vol. 181, Springer-Verlag, New York/Berlin, 1971.

[D-P] A. DOLD AND D. PUPPE, Duality, trace, and transfer, *in* "Proceedings of the International Conference on Geometric Topology (1980)," p. 81–102, Polish Scientific Publishers.

[F] P. FREYD, On canonizing category theory, or, on functorialiing model theory, pamphlet, University of Pennsylvania (1974).

[J-T] A. JOYAL AND M. TIERNEY, An extension of the Galois theory of Grothendieck, *Mem. Amer. Math. Soc.* **51** (1984), 309.

[K-L] G. M. KELLY AND M. L. LAPLAZA, Coherence for compact closed categories, *J. Pure Appl. Algebra* **19** (1980), 193–213.

[L] F. W. LAWVERE, Ordinal sums and equational doctrines, *in* "Seminar on Triples and Categorical Homology Theory," Springer SLN, Vol. 80, Springer-Verlag, New York/Berlin, 1969.

[L1] F. W. LAWVERE, "Teoria delle Categorie sopra un Topos di base," University of Perugia, 1973.

[LA] R. G. LARSON, Coseparable Hopf algebras, *J. Pure Appl. Algebra* **3** (1973), 261–267.

[M] MAGID, "The Separable Galois Theory of Commutative Rings," New York, 1974.

[ML] S. MACLANE, An algebra of additive relations, *Proc. Nat. Acad. Sci. USA* **47**, No. 7 (1961), 1043–1051.

[MN] JU I. MANIN, Correspondences, motives and monoidal transformations, *Math. USSR-Sb* **6** (1968), 439–470.

[P] D. PUPPE, Korrespondenzen in Abelschen Kategorien, *Math. Ann.* **148** (1962), 1–30.

[S] M. E. SWEEDLER, "Hopf Algebras," Benjamin, New York, 1969.

[SGA-1] A. GROTHENDIECK, "Revêtements Etales et Groupe Fondamental," Springer SLN, Vol. 224, Springer-Verlag, New York/Berlin, 1971.

[SGA-4] M. ARTIN, A. GROETHENDIECK, AND J. L. VERDIER, "Théorie des Topos et Cohomologie Etale des Schémas," Springer SLN, Vol. 270, Springer-Verlag, New York/Berlin, 1972.

[SR] N. SAAVEDRA RIVANO, "Catégories Tannakiennes," Springer SLN, Vol. 265, Springer-Verlag, New York/Berlin, 1972.

[W] R. WALTERS, The tensor product of matrices, Talk at Louvain Meeting on Category Theory and its Applications (1987).