Pré-Publicações do Departamento de Matemática Universidade de Coimbra Preprint Number 09–36

GALOIS THEORY AND COMMUTATORS

TOMAS EVERAERT AND TIM VAN DER LINDEN

ABSTRACT: We prove that the relative commutator with respect to a subvariety of a variety of Ω -groups can be described in terms of categorical Galois theory. This extends the known correspondence between Fröhlich's and Janelidze and Kelly's notions of central extension. As an example we study the reflection of the category of loops to the category of groups where we obtain an interpretation of the associator as a relative commutator.

KEYWORDS: categorical Galois theory, semi-abelian category, commutator, associator, higher central extension.

AMS SUBJECT CLASSIFICATION (2010): 18E10, 17D10, 20J.

Introduction

This article concerns the connection between universal algebra and categorical algebra which arises when the concept of *relative commutator* is analysed from a Galois-theoretic point of view. It may be seen as a continuation of Janelidze and Kelly's work [21] on a general theory of *central extensions*, which gives a categorical interpretation of the relative notion of central extension introduced by Fröhlich [15] in the universal-algebraic context of Higgins's Ω -groups [18]. We shall explain how, in a formally precise way, the relative commutator studied in [7] corresponds to a two-dimensional version of those relative central extensions.

Relative central extensions in varieties of Ω -groups. Fröhlich's definition involves a variety of Ω -groups \mathcal{A} and a chosen subvariety \mathcal{B} of \mathcal{A} . Let $I: \mathcal{A} \to \mathcal{B}$ be the left adjoint to the inclusion functor, and $\eta: 1_{\mathcal{A}} \Rightarrow I$ the unit of the adjunction. Then $[-]_{\mathcal{B}}: \mathcal{A} \to \mathcal{A}$ denotes the **variety subfunctor** associated to I, which maps an object A of \mathcal{A} to the object $[A]_{\mathcal{B}}$ defined through the short exact sequence

$$0 \longrightarrow [A]_{\mathcal{B}} \xrightarrow{\mu_A} A \xrightarrow{\eta_A} IA \longrightarrow 0,$$

Received 6th October 2009.

Research supported by CMUC, FCT and FWO.

and a morphism $a: A' \to A$ to its (co)restriction $[a]_{\mathcal{B}}: [A']_{\mathcal{B}} \to [A]_{\mathcal{B}}$. For instance, when \mathcal{A} is the variety Gp of all groups and \mathcal{B} is the subvariety Ab of abelian groups, IA is the abelianisation A/[A, A] of A, and $[A]_{\mathsf{Ab}}$ is the commutator subgroup [A, A]. Of course, A is in Ab if and only if $[A]_{\mathsf{Ab}} = [A, A] = 0$.

An extension $f: A \to B$ in \mathcal{A} being a surjection, it is central with respect to \mathcal{B} if and only if for any parallel pair of morphisms $a_0, a_1: A' \to A$, the condition $f \circ a_0 = f \circ a_1$ implies that $[a_0]_{\mathcal{B}} = [a_1]_{\mathcal{B}}$. For instance, in the case of groups vs. abelian groups, a surjective group homomorphism f is central with respect to Ab exactly when it is central in the classical sense, i.e., the commutator [K, A] of A with the kernel K of f is trivial.

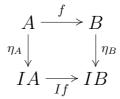
The Galois-theoretic approach. Janelidze and Kelly understood how this relative concept of central extension may be described in terms of *categorical Galois theory*. Introduced by Janelidze (in [19]; see also [3]) this general approach to Galois theory not only captures, e.g., the case of field extensions, but similar concepts in other parts of mathematics as well—indeed also Fröhlich's relative central extensions, as explained in the article [21]. In the context where we shall need it, their definition of central extension involves a semi-abelian category \mathcal{A} (in the sense of [22]: pointed, Barr exact and Bourn protomodular with binary sums) and a **Birkhoff subcategory** \mathcal{B} of \mathcal{A} : full and reflective in \mathcal{A} , and closed in \mathcal{A} under formation of subobjects and regular quotients. The adjunction

$$\mathcal{A}_{\overleftarrow{\searrow}}^{\stackrel{I}{\longrightarrow}}\mathcal{B}$$
(A)

together with the classes $|\mathsf{Ext}\mathcal{A}|$ and $|\mathsf{Ext}\mathcal{B}|$ of **extensions** (i.e., regular epimorphisms) in \mathcal{A} and in \mathcal{B} form a so-called *Galois structure*

$$\Gamma = (\mathcal{A}_{\prec \stackrel{I}{\searrow}}^{I}\mathcal{B}, |\mathsf{Ext}\mathcal{A}|, |\mathsf{Ext}\mathcal{B}|).$$

An extension $f: A \to B$ in \mathcal{A} is trivial (with respect to \mathcal{B}) or \mathcal{B} -trivial when the induced commutative square



is a pullback. And f is central (with respect to \mathcal{B}) or \mathcal{B} -central when there exists an extension $g: C \to B$ such that the pullback g^*f of f along gis \mathcal{B} -trivial.

In the present context, if f is central then one necessarily has that either one of the projections f_0 , f_1 in the kernel pair $(R[f], f_0, f_1)$ of f is \mathcal{B} -trivial (i.e., f is normal with respect to \mathcal{B}) [21, Theorem 4.8]. When \mathcal{A} is a variety of Ω -groups, it is a semi-abelian category, and a Birkhoff subcategory \mathcal{B} of \mathcal{A} is the same thing a subvariety. Then an extension is \mathcal{B} -central in the Galois-theoretic sense if and only if it is \mathcal{B} -central in Fröhlich's sense [21, Theorem 5.2]. More precisely, the definition of central extensions as we presented it above for Ω -groups is equally valid in semi-abelian categories [4, Theorem 2.1].

Connections with homological algebra. There are close connections between the Janelidze–Kelly theory of central extensions and some recent developments in homological algebra, which are worth exploring before we go deeper into the link with commutator theory. Already in the work of Fröhlich, Lue and Furtado-Coelho [15, 24, 16] in the varietal context, the relation between the derived functors of the reflector $I: \mathcal{A} \to \mathcal{B}$ and the notion of \mathcal{B} central extension is emphasised. This relation is particularly explicit in the Hopf formula

$$H_2(B,\mathcal{B}) \cong \frac{K \cap [A]_{\mathcal{B}}}{[K,A]_{\mathcal{B}}}$$

which gives an interpretation of a derived functor of I (the left hand side of the equation) in terms of commutators (the equation's right hand side). Here the short exact sequence

$$0 \longrightarrow K \xrightarrow{k} A \xrightarrow{f} B \longrightarrow 0 \tag{B}$$

is a **presentation** of B, i.e., A is projective, and the commutator $[K, A]_{\mathcal{B}}$ is the smallest ideal J of A such that the induced map $A/J \to B$ is central.

Similar ideas are known to work in the context of semi-abelian categories [8, 11, 12].

The relative theory of central extensions may be used to prove higherdimensional versions of the Hopf formula, which express the higher homology groups $H_n(B, \mathcal{B})$ in terms of higher-dimensional central extensions [10, 6]. Just like the concept of central extension which is defined with respect to an adjunction (**A**), one may consider double central extensions which are defined with respect to the reflection of extensions to central extensions the adjunction

$$\mathsf{Ext}\mathcal{A}_{\overleftarrow{\mathbb{Z}}}^{I_1}\mathsf{CExt}_{\mathcal{B}}\mathcal{A}$$

where $\mathsf{Ext}\mathcal{A}$ denotes the category of extensions and commutative squares between them, and $\mathsf{CExt}_{\mathcal{B}}\mathcal{A}$ its full subcategory determined by those extensions which are \mathcal{B} -central. Together with well-chosen classes of *double extensions*, this adjunction forms a Galois structure Γ_1 , and Galois theory provides us with a notion of *relative double central extension* with respect to \mathcal{B} . This construction may be repeated ad infinitum, so that notions of *n-fold central extension* are obtained, but for the present purposes the second step is sufficient. Thus double central extensions, first introduced by Janelidze for groups [20], appear naturally in the study of (co)homology [6, 10, 13, 17, 25], and turn out to be precisely what we need to understand how the relative commutator works.

The relative commutator. Given a variety of Ω -groups \mathcal{A} and a subvariety \mathcal{B} of \mathcal{A} , the objects of \mathcal{B} and the \mathcal{B} -central extensions are often defined in terms of some kind of commutator. (Such as, in the case of groups, the classical commutator [-, -], which is used to characterise abelian groups and central extensions.) One may take the opposite point of view, and ask whether the subvariety \mathcal{B} (and the \mathcal{B} -central extensions) determine a notion of commutator. In his paper [7], the first author does exactly this: he introduces a relative commutator $[-, -]_{\mathcal{B}}$ with respect to \mathcal{B} which is such that an object A of \mathcal{A} is in \mathcal{B} if and only if $[A, A]_{\mathcal{B}} = 0$. Moreover, an extension $f: A \to B$ in \mathcal{A} with kernel K is \mathcal{B} -central if and only if $[K, A]_{\mathcal{B}} = 0$. For example, if \mathcal{A} is the variety PXMod of precrossed modules (which is indeed a variety—see, e.g., [23]) and \mathcal{B} is the subvariety XMod of crossed modules then $[-, -]_{\mathcal{B}}$ is the *Peiffer commutator* $\langle -, - \rangle$.

In view of the above ideas, a relation between this relative commutator and the concept of higher central extension was to be expected. Morally, the fact that we need *double* central extensions here is simply a consequence of the commutator's having two arguments. Indeed, the objects of the Birkhoff subcategory \mathcal{B} of \mathcal{A} are those objects A for which the commutator $[A, A]_{\mathcal{B}}$ of A with itself is zero: to characterise the zero-dimensional \mathcal{B} -central extensions of \mathcal{A} , the commutator has to take no non-trivial arguments. To characterise a one-dimensional \mathcal{B} -central extension $f: A \to B$ with kernel K as an extension f such that $[K, A]_{\mathcal{B}}$ is zero, one non-trivial argument of the commutator is needed; so it is natural to expect that a commutator with two non-trivial arguments corresponds to the two-dimensional \mathcal{B} -central extensions of \mathcal{A} .

Structure of the text. In the first section we recall the definition of the relative commutator introduced in [7], as well as some basic notations and examples. In Section 2 we sketch the needed categorical background: semi-abelian categories, categorical Galois theory and the concept of double central extension. We characterise double central extensions in terms of double equivalence relations and the zero-dimensional commutator (Proposition 2.9). Section 3 contains the main result of the article, Theorem 3.1, which gives an interpretation of the relative commutator in terms of double central extensions. Finally, in Section 4, we study a non-classical example: the relative commutator of loops with respect to groups. The category Loop of loops and loop homomorphisms does not form a variety of Ω -groups, hence lies beyond the scope of the theory introduced in [7]. Nevertheless the concept of relative commutator arises naturally here when the reflection to the category Gp of groups is considered (Theorem 4.7).

1. The relative commutator

A variety of Ω -groups [18] is a pointed variety of universal algebras (it has exactly one constant) that has amongst its operations and identities those of the variety of groups. It is well-known that any such variety is semiabelian [22]. Examples include the varieties Gp of groups, Rng of non-unital rings, XMod of crossed modules, PXMod of precrossed modules, CommAlg of commutative algebras, _RMod of modules over a ring R and Lie_K of Lie algebras over a field K.

We shall denote finite ordered sets (x_1, x_2, \ldots, x_r) , (a_1, a_2, \ldots, a_s) ,... by \boldsymbol{x} , \boldsymbol{a} , etc. Instead of $(x_1y_1, x_2y_2, \ldots, x_ry_r)$ we shall write \boldsymbol{xy} . $w(x_1, x_2, \ldots, x_r)$

and $w(a_1, a_2, \ldots, a_s)$ become $w(\boldsymbol{x})$ and $w(\boldsymbol{a})$, for terms (words) w. If 1 is the unit of a group operation we shall write **1** instead of $(1, \ldots, 1)$. Also, $a_1, a_2, \ldots, a_s \in A$ will be abbreviated to $\boldsymbol{a} \in A$.

In this context, a normal subobject N of an object A is usually called an **ideal**. The meet of ideals is their intersection, and also the join is easy to compute: if M and N are ideals of A then $M \vee N$ is the (internal) product

$$M \cdot N = \{mn \mid m \in M, n \in N\}$$

with the Ω -group structure induced by A. A priori, $M \vee N$ contains all $w(\boldsymbol{mn})$ where w is a term, $\boldsymbol{m} \in M$ and $\boldsymbol{n} \in N$; but $w(\boldsymbol{mn})$ may be written as the product of $w(\boldsymbol{mn})w(\mathbf{1n})^{-1} \in M$ with $w(\mathbf{1n}) \in N$, which explains why $M \vee N = M \cdot N$. (To see that $w(\boldsymbol{mn})w(\mathbf{1n})^{-1}$ is indeed an element of M, apply the quotient map $A \to A/M$ to it.) Given an ideal J of $M \cdot N$, the induced quotient of $M \cdot N$ is denoted

$$q_J \colon M \cdot N \to \frac{M \cdot N}{J};$$

we write R_J for the kernel pair of q_J .

Suppose that \mathcal{A} is a variety of Ω -groups and \mathcal{B} is a subvariety of \mathcal{A} . Then \mathcal{B} is completely determined by a set of identities of terms of the form $w(\boldsymbol{x}) = 1$. The set of all corresponding terms $w(\boldsymbol{x})$ forms a group

$$W = W_{\mathcal{B}} = \{ w(\boldsymbol{x}) \mid w(\boldsymbol{b}) = 1, \forall B \in \mathcal{B}, \forall \boldsymbol{b} \in B \}.$$

An object B belongs to \mathcal{B} if and only if $w(\mathbf{b}) = 1$ for all $w \in W$ and $\mathbf{b} \in B$ and, consequently,

$$[A]_{\mathcal{B}} = \{w(\boldsymbol{a}) \mid w \in W, \boldsymbol{a} \in A\}$$

for any A in \mathcal{A} .

Now we are in a position to recall the definition of the relative commutator introduced in [7].

Definition 1.1. Let \mathcal{A} be a variety of Ω -groups and \mathcal{B} a subvariety of \mathcal{A} . For any object A of \mathcal{A} and any pair of ideals M and N of A, the commutator $[M, N]_{\mathcal{B}}$ is the ideal of $M \cdot N$ generated by the set

{
$$w(\boldsymbol{m}\boldsymbol{n})w(\boldsymbol{n})^{-1}w(\boldsymbol{m})^{-1}w(\boldsymbol{p}) \mid w \in W, \boldsymbol{m} \in M, \boldsymbol{n} \in N, \boldsymbol{p} \in M \cap N$$
}.

Examples 1.2. We already mentioned that in the case of groups vs. abelian groups, $[M, N]_{Ab}$ is the classical commutator [M, N]. It is shown in [7] that,

more generally, for any variety of Ω -groups \mathcal{A} , the commutator $[M, N]_{\mathsf{Ab}\mathcal{A}}$ relative to the subvariety $\mathsf{Ab}\mathcal{A}$ of abelian Ω -groups in \mathcal{A} is the Higgins commutator from [18]. Proposition 2.3 in [7] states that the commutator $[M, N]_{\mathsf{XMod}}$ of two precrossed submodules M and N of a precrossed module A is precisely the Peiffer commutator $\langle M, N \rangle$ of M and N. For any $k \geq 2$, a description of the commutator $[M, N]_{\mathsf{Sol}_k}$ of groups vs. solvable groups of class at most k, and of $[M, N]_{\mathsf{Nil}_k}$, the commutator of groups vs. nilpotent groups of class at most k can be found in [9].

2. Double central extensions

In this section we sketch the categorical and Galois-theoretic background needed for the definition of double central extension, and we explain how those double central extensions can be characterised in terms of zero-dimensional commutators and double equivalence relations (Proposition 2.9). More on these subjects may, for instance, be found in the articles [6, 10, 25].

2.1. Semi-abelian categories. Recall that a regular epimorphism is a coequaliser of some pair of arrows. A category is regular when it is finitely complete with coequalisers of kernel pairs and with pullback-stable regular epimorphisms. In a regular category, any morphism may be factored as a regular epimorphism followed by a monomorphism, and this image factorisation is unique up to isomorphism. A category is Barr exact when it is regular and such that any internal equivalence relation is effective, i.e., it is the kernel pair of its coequaliser. A pointed and regular category is Bourn protomodular when the (Regular) Short Five Lemma holds: this means that for any commutative diagram

$$\begin{array}{c} K[f'] \xrightarrow{\ker f'} A' \xrightarrow{f'} B' \\ {}^{k} \downarrow & a \downarrow & \downarrow b \\ K[f] \xrightarrow{\ker f} A \xrightarrow{f} B \end{array}$$

such that f and f' are regular epimorphisms, k and b being isomorphisms implies that a is an isomorphism. A **semi-abelian** category is pointed, Barr exact and Bourn protomodular with binary coproducts [22].

Since a regular epimorphism is always the cokernel of its kernel in a semiabelian category, the following notion of short exact sequence is appropriate. A short exact sequence is any sequence

$$K \xrightarrow{k} A \xrightarrow{f} B$$

with $k = \ker f$ and f a regular epimorphism. We denote this situation

$$0 \longrightarrow K \xrightarrow{k} A \xrightarrow{f} B \longrightarrow 0.$$

2.2. Double extensions. Let \mathcal{A} be a semi-abelian category. Recall that an extension in \mathcal{A} is a regular epimorphism. The category $\mathsf{Ext}\mathcal{A}$ has for its objects the extensions in \mathcal{A} , and for its arrows the commutative squares between extensions. Since $\mathsf{Ext}\mathcal{A}$ need no longer be semi-abelian, we usually make all constructions involving exact sequences etc. in the semi-abelian category $\mathsf{Arr}\mathcal{A}$ of all arrows in \mathcal{A} which contains $\mathsf{Ext}\mathcal{A}$ as a full subcategory.

A double extension is a commutative square

$$\begin{array}{ccc} X \xrightarrow{c} C \\ d & & \downarrow^{g} \\ D \xrightarrow{f} Z \end{array} \tag{C}$$

such that all its maps and the comparison map $(d, c): X \to D \times_Z C$ to the pullback of f with g are regular epimorphisms. The category of double extensions in \mathcal{A} and commutative cubes between them is denoted $\mathsf{Ext}^2\mathcal{A}$. The basic categorical properties of higher-dimensional extensions are explored in [10] and [6].

2.3. Double relations. Given two (internal) equivalence relations R and S on an object X, a double equivalence relation C on R and S is an equivalence relation C on S of which the "object part" is R, as in the next diagram.



For instance, $R \Box S$ denotes the largest double equivalence relation on Rand S. In the concrete case of a variety of universal algebras it consists of all quadruples $(x, y, z, t) \in X^4$ in the configuration

$$\begin{pmatrix} x & y \\ z & t \end{pmatrix},$$

i.e., where (x, z), $(y, t) \in R$ and (x, y), $(z, t) \in S$. We shall be especially interested in the special case where C is induced by a double extension (**C**) as follows: R = R[c] is the kernel pair of c, S = R[d] is the kernel pair of dand $C = R[c] \Box R[d]$. It is easily seen that then the rows and columns of the induced diagram

$$R[c] \square R[d] \xrightarrow{p_1} R[d] \xrightarrow{p} R[g]$$

$$\xrightarrow{r_0} \bigvee r_1 \qquad d_0 \bigvee d_1 \qquad g_0 \bigvee g_1$$

$$R[c] \xrightarrow{c_1} X \xrightarrow{c} C$$

$$r \bigvee \qquad d \bigvee \qquad \downarrow g$$

$$R[f] \xrightarrow{f_1} D \xrightarrow{f} Z$$

are exact, i.e., consist of effective equivalence relations with their coequalisers.

2.4. Birkhoff subcategories. Given a semi-abelian category \mathcal{A} , a **Birkhoff subcategory** \mathcal{B} of \mathcal{A} is full and reflective in \mathcal{A} , and closed in \mathcal{A} under formation of subobjects and regular quotients.

Example 2.5. Recall from [5] that a variety of universal algebras \mathcal{A} is semiabelian if and only if it has a unique constant 1 and, for some natural number $n \geq 1$, n binary terms t_i and an (n + 1)-ary term t such that $t_i(x, x) = 1$ and $t(t_1(x, y), t_2(x, y), \ldots, t_n(x, y), y) = x$. This is the case, precisely when the variety is pointed and *BIT speciale* in the sense of [26] or *classically ideal determined* in the sense of [27].

A Birkhoff subcategory \mathcal{B} of \mathcal{A} is the same thing as a subvariety. Since x = y in \mathcal{A} if and only if $t_i(x, y) = 1$ for all i, the subvariety \mathcal{B} is completely determined by a set of identities of terms of the form w(x) = 1, as in the case of varieties of Ω -groups.

2.6. The centralisation functor. Let \mathcal{B} be a Birkhoff subcategory of \mathcal{A} . The full subcategory of $\mathsf{Ext}\mathcal{A}$ determined by the \mathcal{B} -central extensions is denoted $\mathsf{CExt}_{\mathcal{B}}\mathcal{A}$. The inclusion $\mathsf{CExt}_{\mathcal{B}}\mathcal{A} \subset \mathsf{Ext}\mathcal{A}$ has a left adjoint, the centralisation functor, which is denoted $I_1 \colon \mathsf{Ext}\mathcal{A} \to \mathsf{CExt}_{\mathcal{B}}\mathcal{A}$. It may be described in terms of one-dimensional commutators as follows.

Let $f: A \to B$ be an extension with kernel K. Note that f is \mathcal{B} -central if and only if for the kernel pair $(R[f], f_0, f_1)$ of f, the (co)restrictions

$$[f_0]_{\mathcal{B}}, [f_1]_{\mathcal{B}} \colon [R[f]]_{\mathcal{B}} \to [A]_{\mathcal{B}}$$

of the two projections are equal: $[f_0]_{\mathcal{B}} = [f_1]_{\mathcal{B}}$. Indeed, if the latter condition holds and $f \circ a_0 = f \circ a_1$ for some $a_0, a_1 \colon A' \to A$, then there exists a map $a \colon A' \to R[f]$ such that $f_0 \circ a = a_0$ and $f_1 \circ a = a_1$, which implies $[a_0]_{\mathcal{B}} = [a_1]_{\mathcal{B}}$. The converse is obvious.

Since $[f_0]_{\mathcal{B}}$ and $[f_1]_{\mathcal{B}}$ are jointly monomorphic and have a common splitting, $[f_0]_{\mathcal{B}}$ is equal to $[f_1]_{\mathcal{B}}$ exactly when either one of these maps is an isomorphism. Hence the kernel $[K, A]_{\mathcal{B}}$ of $[f_0]_{\mathcal{B}}$ measures how far f is from being central: fis \mathcal{B} -central if and only if $[K, A]_{\mathcal{B}}$ is zero. This one-dimensional commutator $[K, A]_{\mathcal{B}}$ may be considered as a normal subobject of A via the composite $\mu_{A^{\circ}}[f_1]_{\mathcal{B}^{\circ}}$ ker $[f_0]_{\mathcal{B}}: [K, A]_{\mathcal{B}} \to A$, as depicted in the following diagram.

$$[K, A]_{\mathcal{B}}$$

$$\ker [f_0]_{\mathcal{B}} \bigvee$$

$$0 \longrightarrow [R[f]]_{\mathcal{B}} \xrightarrow{\mu_{R[f]}} R[f] \xrightarrow{\eta_{R[f]}} IR[f] \longrightarrow 0$$

$$[f_0]_{\mathcal{B}} \bigcup [f_1]_{\mathcal{B}} \xrightarrow{f_0} \bigcup f_1 \qquad If_0 \bigcup If_1$$

$$0 \longrightarrow [A]_{\mathcal{B}} \xrightarrow{\mu_A} A \xrightarrow{\eta_A} IA \longrightarrow 0$$

Examples 2.7. Here are two examples, taken from [10] and [7]. If $f: A \to B$ is an extension of precrossed modules with kernel K then the commutator $[K, A]_{\mathsf{XMod}}$ relative to the subvariety of crossed modules is the Peiffer commutator $\langle K, A \rangle$. If f is an extension of groups then the commutator $[K, A]_{\mathsf{Sol}_2}$ relative to the subvariety Sol_2 of all groups which are solvable of class at most 2 is [[K, A], [A, A]].

Given any extension $f: A \to B$ with kernel K, its centralisation $I_1 f$ is now obtained through the diagram with exact rows

Considering this diagram as a short exact sequence

$$0 \longrightarrow K[\eta_f^1] \xrightarrow{\mu_f^1} f \xrightarrow{\eta_f^1} I_1 f \longrightarrow 0$$

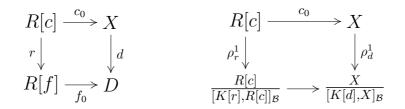
in the semi-abelian category of arrows Arr \mathcal{A} we obtain a description of the unit η^1 of the adjunction and its kernel μ^1 .

Thus the Galois structure Γ induces a new Galois structure

$$\Gamma_{1} = (\mathsf{Ext}\mathcal{A}_{\prec \perp}^{\stackrel{I_{1}}{\longrightarrow}} \mathsf{CExt}_{\mathcal{B}}\mathcal{A}, |\mathsf{Ext}^{2}\mathcal{A}|, |\mathsf{Ext}\mathsf{CExt}_{\mathcal{B}}\mathcal{A}|)$$

where $\mathsf{ExtCExt}_{\mathcal{B}}\mathcal{A}$ consists of all double extensions which lie in $\mathsf{CExt}_{\mathcal{B}}\mathcal{A}$.

2.8. Double central extensions. By definition, a double extension is a **double central extension** when it is a covering with respect to the Galois structure Γ_1 . This means that the double extension (**C**), considered as a map $(c, f): d \to g$ in the category $\mathsf{Ext}\mathcal{A}$, is central if and only if the first projection



of its kernel pair—the left hand side square—is a trivial extension with respect to Γ_1 . (Alternatively, one could use the square of second projections.) This means that the comparison map to its reflection into $\mathsf{CExt}_{\mathcal{B}}\mathcal{A}$ —the right hand side square—is a pullback. For this to happen, the natural map

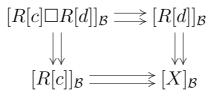
$$[K[r], R[c]]_{\mathcal{B}} \to [K[d], X]_{\mathcal{B}}$$
(D)

must be an isomorphism. This, in turn, is equivalent to the square

being a pullback, because $[K[r], R[c]]_{\mathcal{B}}$ and $[K[d], X]_{\mathcal{B}}$ are by definition the kernels of the vertical maps in this square. Note that, equivalently, we could have chosen second projections for the vertical maps. Thus we proved the following characterisation of double central extensions, which is a relative version of the result in Section 1.9 of [25].

Proposition 2.9. Let \mathcal{A} be a semi-abelian category and \mathcal{B} a Birkhoff subcategory of \mathcal{A} . A double extension (C) is central with respect to \mathcal{B} if and only

if any of the induced commutative squares in



is a pullback.

3. The commutator in terms of categorical Galois theory

Now we are ready to prove our main theorem: a characterisation of the relative commutator from Definition 1.1 in Galois-theoretic terms.

Theorem 3.1. Let \mathcal{A} be a variety of Ω -groups and \mathcal{B} a subvariety of \mathcal{A} . Given any two ideals M and N of an object A of \mathcal{A} , the commutator $[M, N]_{\mathcal{B}}$ is zero if and only if the double extension

$$\begin{array}{cccc} M \cdot N \xrightarrow{q_M} & \underbrace{M \cdot N}{M} \\ q_N & & \downarrow \\ & \underbrace{M \cdot N}{N} \longrightarrow 0 \end{array} \end{array}$$
 (E)

is central.

Proof: First note that the above square is indeed a double extension: the comparison map

$$(q_N, q_M): M \cdot N \to \frac{M \cdot N}{N} \times \frac{M \cdot N}{M}$$

to the induced pullback is a surjection, because

$$(q_N(mn), q_M(m'n')) = (q_N(m), q_M(n'))$$

= $(q_N(mn'), q_M(mn'))$

for all $m, m' \in M, n, n' \in N$.

Now suppose that $[M, N]_{\mathcal{B}}$ is zero. By Proposition 2.9, it suffices to prove that any of the commutative squares in

is a pullback. Now $R_M \Box R_N$ consists of all

$$\begin{pmatrix} mn & mn' \\ m'n & m'n'p \end{pmatrix}$$

where $m, m' \in M, n, n' \in N$ and $p \in M \cap N$. Hence $[R_M \Box R_N]_{\mathcal{B}}$ contains all quadruples

$$\begin{pmatrix} w(\boldsymbol{mn}) & w(\boldsymbol{mn'}) \\ w(\boldsymbol{m'n}) & w(\boldsymbol{m'n'p}) \end{pmatrix}$$

where $w \in W$, $m, m' \in M$, $n, n' \in N$ and $p \in M \cap N$. We have to prove that two of those quadruples coincide as soon as three out of four of their elements do. This is the case because the assumption implies

$$w(\mathbf{m}'\mathbf{n}'\mathbf{p}) = w(\mathbf{m}')w(\mathbf{n}')w(\mathbf{p})$$

= $w(\mathbf{m}')w(\mathbf{n}')$
= $w(\mathbf{m}')w(\mathbf{n})w(\mathbf{n})^{-1}w(\mathbf{m})^{-1}w(\mathbf{m})w(\mathbf{n}')$
= $w(\mathbf{m}'\mathbf{n})w(\mathbf{m}\mathbf{n})^{-1}w(\mathbf{m}\mathbf{n}'),$

so that the fourth element depends fully on the other three.

Conversely, suppose that any of the commutative squares in (**F**) is a pullback. Then, since for any $w \in W$ and $p \in M \cap N$, both

(1)	1	and	(1)	1
$\backslash 1$	$w(\mathbf{p})$	and	(1	1)

are in $[R_M \Box R_N]_{\mathcal{B}}$, we have that $w(\mathbf{p}) = 1$. Also, for any $w \in W$, $\mathbf{m} \in M$ and $\mathbf{n}' \in N$, we have that both

$$\begin{pmatrix} w(\boldsymbol{m}) & w(\boldsymbol{mn'}) \\ 1 & w(\boldsymbol{n'}) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} w(\boldsymbol{m}) & w(\boldsymbol{mn'}) \\ 1 & w(\boldsymbol{m})^{-1}w(\boldsymbol{mn'}) \end{pmatrix}$$

are in $[R_M \Box R_N]_{\mathcal{B}}$, hence $w(\boldsymbol{mn'}) = w(\boldsymbol{m})w(\boldsymbol{n'})$.

Using Theorem 3.1, one can extend the relative notion of commuting subobjects so that \mathcal{A} is allowed to be any semi-abelian category \mathcal{A} and \mathcal{B} any Birkhoff subcategory of \mathcal{A} . Taking, for normal subobjects M and N of an object A in \mathcal{A} , their commutator $[M, N]_{\mathcal{B}}$ to be the smallest normal subobject J of $M \vee N$ such that $q_J M$ and $q_J N$ commute thus provides one with a categorical notion of relative commutator, which will be studied in more detail in [14].

4. Example: the associator of loops

We now illustrate this approach with example of loops vs. groups. Note that loops do not constitute a variety of Ω -groups, so that Definition 1.1 is not applicable. Nevertheless, the variety **Loop** is semi-abelian. The commutator $[-, -]_{\mathcal{B}}$ defined above in terms of double central extensions characterises the associator of loops when \mathcal{B} is taken to be the subvariety **Gp** of groups. Since indeed loops are "non-associative groups" it makes sense for the reflection to **Gp** to induce a commutator $[M, N]_{\mathsf{Gp}}$ which measures how well the elements of two given normal subloops M and N of a loop A associate with each other.

4.1. Basic definitions and properties. Recall that a loop is an algebraic structure $(A, \cdot, \backslash, /, 1)$ where the multiplication \cdot and the left and right division \backslash and / satisfy the axioms

$$y = x \cdot (x \setminus y) \qquad \qquad y = x \setminus (x \cdot y)$$
$$x = (x/y) \cdot y \qquad \qquad x = (x \cdot y)/y$$

and 1 is a unit for the multiplication, $x \cdot 1 = x = 1 \cdot x$. We shall sometimes write xy for $x \cdot y$. The variety of loops is denoted **Loop**. It is known to be semi-abelian [2], and easily seen to be such using the description recalled in Example 2.5: take n = 1, t(x, y) = xy and $t_1(x, y) = x/y$.

Suppose that M and N are normal subloops of a loop A. Then the argument showing that $M \vee N = M \cdot N$ given in the case of Ω -groups is still valid, as indeed $w(\boldsymbol{mn})$ is the product of $w(\boldsymbol{mn})/w(\boldsymbol{n})$ with $w(\boldsymbol{n})$.

4.2. The associator. The **associator** of three elements x, y, z of a loop A is the unique element [x, y, z] of A such that $(xy)z = [x, y, z] \cdot x(yz)$. Hence [x, y, z] is equal to ((xy)z)/(x(yz)). Given three normal subloops L, M and N of A, we write [L, M, N] for the normal subloop of A generated by the elements [x, y, z], where either (x, y, z) or any of its permutations is in $L \times M \times N$: it is the smallest normal subloop J of A such that $q_J L$, $q_J M$ and $q_J N$ "associate".

The **associator of** A is its normal subloop [A, A, A]. A loop A is a group if and only if its associator is trivial, and the reflection gpA of any loop A into Gp is given by A/[A, A, A]. Thus we see that $[A]_{Gp} = [A, A, A]$. 4.3. Characterisation of the Gp-central extensions of loops. The adjunction

$$\mathsf{Loop}_{\overbrace{\supset}}^{\mathsf{gp}}\mathsf{Gp}$$

induces a notion of central extension of loops, relative to the subvariety of groups. It may be characterised in terms of an associator as follows.

Proposition 4.4. In the category of loops, let $f: A \to B$ be an extension with kernel K. The extension f is central with respect to Gp if and only if the associator [K, A, A] is zero. Hence

$$[K,A]_{\mathsf{Gp}} = [K,A,A].$$

Proof: By definition, f is a central extension if and only if the induced split epimorphisms of loops

$$[f_0]_{\mathsf{Gp}}, [f_1]_{\mathsf{Gp}} \colon [R[f], R[f], R[f]] \to [A, A, A]$$

are equal.

Let (k, a, a') be an element of $K \times A \times A$ and suppose that $[f_0]_{\mathsf{Gp}} = [f_1]_{\mathsf{Gp}}$. Then

$$[k, a, a'] = f_0[(k, 1), (a, a), (a', a')] = f_1[(k, 1), (a, a), (a', a')] = [1, a, a'] = 1.$$

Similarly, also [a, k, a'] = 1 and [a, a', k] = 1, which means that [K, A, A] = 0. Conversely, assume that [K, A, A] = 0. First note that this implies that

$$(ak)/(a'k) = a/a' \qquad \forall a, a' \in A, k \in K.$$
 (G)

Indeed, it follows from the assumption that

$$ak = ((a/a')a')k = (a/a')(a'k).$$

Now, for any element (a, a') of R[f] we can write a' = ak, where $k = a \setminus a'$ is in K. Thus we see that [R[f], R[f], R[f]] is generated by all elements of the form [(a, ak), (a', a'k'), (a'', a''k'')] where $(a, a', a'') \in A^3$ and $(k, k', k'') \in K^3$. We have to show for any such generator that [a, a', a''] = [ak, a'k', a''k'']. We shall do this in three steps, first eliminating k'', then k', and finally k.

Consider an associator [ak, a'k', a''k'']. Then

$$[ak, a'k', a''k''] = ((ak \cdot a'k')(a''k''))/((ak)(a'k' \cdot a''k''))$$

and $(ak \cdot a'k')(a''k'') = (ak \cdot a'k')a'' \cdot k''$ while $(ak)(a'k' \cdot a''k'') = (ak)((a'k' \cdot a'')k'') = (ak)(a'k' \cdot a'') \cdot k''$ so that [ak, a'k', a''k''] = [ak, a'k', a''] by (**G**). Write $k'a'' = a''\overline{k'}$ where $\overline{k'} = a'' \setminus (k'a'') \in K$. Since $(ak \cdot a'k')a'' = ((ak \cdot a')k')a'' = (ak \cdot a')(k'a'') = (ak \cdot a')(a''\overline{k'}) = (ak \cdot a')a'' \cdot \overline{k'}$ and

$$(ak)(a'k' \cdot a'') = (ak)(a' \cdot k'a'') = (ak)(a' \cdot a''\overline{k'}) = (ak)(a'a'' \cdot \overline{k'}) = (ak \cdot a'a'') \cdot \overline{k'},$$

using (**G**) we find that $[ak, a'k', a''] = [ak, a', a'']$. Finally,

$$(ak \cdot a')a'' = (a \cdot ka')a'' = (a \cdot a'\overline{k})a'' = (aa' \cdot \overline{k})a''$$
$$= aa' \cdot \overline{k}a'' = aa' \cdot a''\overline{k} = (aa' \cdot a'') \cdot \overline{k}$$

and

$$ak \cdot a'a'' = a(k \cdot a'a'') = a(ka' \cdot a'') = a(a'\overline{k} \cdot a'') = a(a' \cdot \overline{k}a'')$$
$$= a(a' \cdot a''\overline{\overline{k}}) = a(a'a'' \cdot \overline{\overline{k}}) = (a \cdot a'a'') \cdot \overline{\overline{k}},$$

for some $\overline{k}, \overline{\overline{k}} \in K$, from which we infer—again using (**G**)—that [a, a', a''] = [ak, a'k', a''k''].

One way to apply this result occurs when computing of the homology of loops with respect to groups: the second homology group of a loop B may be written in a Hopf formula as a quotient of associators.

Corollary 4.5 (Hopf formula for loops vs. groups). If B is a loop and (**B**) a projective presentation of B, then

$$H_2(B, \mathsf{Gp}) \cong \frac{K \cap [A, A, A]}{[K, A, A]},$$

where the left hand side homology group is the comonadic homology of B with coefficients in the reflector $gp: Loop \rightarrow Gp$ and relative to the comonad induced by the forgetful/free adjunction to Set.

Proof: This is an instance of [12, Theorem 6.9]; see also [10] and [8].

4.6. The relative commutator is an associator. We now use the characterisation of Gp-central extensions of loops to interpret the commutator $[-,-]_{Gp}$ in terms of associator elements. Let A be a loop and let M and N be normal subloops of A. As in the case of Ω -groups, the induced commutative square (**E**) is indeed a double extension of loops: the proof given with Theorem 3.1 is still valid. We have to find out when this double extension is Gp-central.

Theorem 4.7. If M and N are normal subloops of a loop A then

$$[M, N]_{\mathsf{Gp}} = [M, N, M \cdot N].$$

Proof: We have to show that the associator $[M, N, M \cdot N]$ is zero if and only if (**E**) is central. This happens when the two projections

$$\left[K[q_N\circ(q_M)_0]\cap K[q_N\circ(q_M)_1], R_M\right]_{\mathsf{Gp}} \to [N, M \cdot N]_{\mathsf{Gp}}$$

arising through the diagram

and corresponding to (**D**) are equal to each other. Proposition 4.4 tells us that they are the restrictions of the kernel pair projections $(q_M)_0$ and $(q_M)_1$ to maps

$$q_0, q_1 \colon \left[K[q_N \circ (q_M)_0] \cap K[q_N \circ (q_M)_1], R_M, R_M \right] \to [N, M \cdot N, M \cdot N].$$

If $q_0 = q_1$ then, for any $m, m' \in M$ and $n, n' \in N$,

$$[n, m, m'n'] = q_0[(n, n), (m, 1), (m'n', n')]$$

= $q_1[(n, n), (m, 1), (m'n', n')]$
= $[n, 1, n'] = 1.$

Similarly, [m, n, m'n'], [m, m'n', n], [n, m'n', m], [m'n', m, n] and [m'n', n, m] also vanish so that $[M, N, M \cdot N] = 0$.

Conversely, suppose that $[M, N, M \cdot N]$ is zero. We have to prove that then the morphism q_0 is equal to q_1 . Note that any element of the intersection $K[q_N \circ (q_M)_0] \cap K[q_N \circ (q_M)_1]$ may be written as (n, np) with $n \in N$ and $p \in$ $M \cap N$, and any element of R_M as (nm, nmm') with $m, m' \in M$ and $n \in N$. Hence it will be sufficient to prove that the identities

$$[n, n'm, n''m''] = [np, n'mm', n''m'''n'''],$$

$$[n''m'', n, n'm] = [n''m''m''', np, n'mm'],$$

and

$$[n'm, n''m'', n] = [n'mm', n''m''m''', np]$$

hold for all $p \in M \cap N$, m, m', m'', $m''' \in M$ and n, n', $n'' \in N$. This in its turn simplifies to proving that each of the commutators [nm, n'm', n''], [nm, n', n''m''] and [n, n'm', n''m''] is equal to [n, n', n''], since in that case we have that

$$[n, n'm, n''m''] = [n, n', n''] = [np, n', n''] = [np, n'mm', n''m''m''']$$

—and the other two identities can be derived in a similar fashion. We shall work out in detail that [nm, n'm', n''] = [n, n', n'']. The proofs of other two identities are quite similar and are left to the reader.

Let thus m and m' be elements of M and let n, n' and n'' be elements of N. Write $m'n'' = n''\overline{m'}$, $mn' = n'\overline{m}$ and then $\overline{m}n'' = n''\overline{\overline{m}}$, where $\overline{m'} = n'' \setminus (m'n'')$, $\overline{m} = n' \setminus (mn')$ and $\overline{\overline{m}} = n'' \setminus (\overline{m}n'')$ all lie in M. Then

$$[nm, n'm', n''] = ((nm \cdot n'm') \cdot n')/(nm \cdot (n'm' \cdot n''))$$

and

$$(nm \cdot n'm')n'' = ((nm \cdot n')m')n'' = (nm \cdot n') \cdot m'n'' = (nm \cdot n') \cdot n''\overline{m'}$$
$$= ((nm \cdot n')n'')\overline{m'} = ((n \cdot mn')n'')\overline{m'} = ((n \cdot n'\overline{m})n'')\overline{m'}$$
$$= ((nn' \cdot \overline{m})n'')\overline{m'} = (nn' \cdot \overline{m}n'')\overline{m'} = (nn' \cdot n''\overline{\overline{m}})\overline{m'}$$
$$= ((nn' \cdot n'')\overline{\overline{m}})\overline{m'} = (nn' \cdot n'') \cdot \overline{\overline{m}}\overline{m'}$$

while

$$nm \cdot (n'm' \cdot n'') = nm \cdot (n' \cdot m'n'') = nm \cdot (n' \cdot n''\overline{m'}) = nm \cdot (n'n'' \cdot \overline{m'})$$
$$= (nm \cdot n'n'')\overline{m'} = (n(m \cdot n'n''))\overline{m'} = (n(mn' \cdot n''))\overline{m'}$$
$$= (n(n'\overline{m} \cdot n''))\overline{m'} = (n(n' \cdot \overline{m}n''))\overline{m'} = (n(n' \cdot n''\overline{\overline{m}}))\overline{m'}$$
$$= (n(n'n'' \cdot \overline{\overline{m}}))\overline{m'} = ((n \cdot n'n'')\overline{\overline{m}})\overline{m'} = (n \cdot n'n'') \cdot \overline{\overline{m}}\overline{m'}$$

so that

$$(nn' \cdot n'') \cdot \overline{\overline{m}} \overline{m'} = ([n, n', n''] \cdot (n \cdot n'n'')) \cdot \overline{\overline{m}} \overline{m'} = [n, n', n''] \cdot ((n \cdot n'n'') \cdot \overline{\overline{m}} \overline{m'})$$

which implies that $[nm, n'm', n''] = [n, n', n''].$

References

- [1] F. Borceux and D. Bourn, *Mal'cev, protomodular, homological and semi-abelian categories*, Mathematics and its Applications, vol. 566, Kluwer Academic Publishers, 2004.
- [2] F. Borceux and M. M. Clementino, Topological semi-abelian algebras, Adv. Math. 130 (2005), 425–453.
- [3] F. Borceux and G. Janelidze, *Galois theories*, Cambridge Studies in Advanced Mathematics, vol. 72, Cambridge University Press, 2001.
- [4] D. Bourn and M. Gran, Central extensions in semi-abelian categories, J. Pure Appl. Algebra 175 (2002), 31–44.
- [5] D. Bourn and G. Janelidze, Characterization of protomodular varieties of universal algebras, Theory Appl. Categ. 11 (2003), no. 6, 143–147.
- [6] T. Everaert, *Higher central extensions and Hopf formulae*, J. Algebra, in press, published online 21 January 2009.
- [7] _____, Relative commutator theory in varieties of Ω-groups, J. Pure Appl. Algebra 210 (2007), 1–10.
- [8] T. Everaert and M. Gran, On low-dimensional homology in categories, Homology, Homotopy and Appl. 9 (2007), 275–293.
- [9] _____, Relative commutator associated with varieties of n-nilpotent and of n-solvable groups, Arch. Math. (Brno) **42** (2007), 387–396.
- [10] T. Everaert, M. Gran, and T. Van der Linden, Higher Hopf formulae for homology via Galois Theory, Adv. Math. 217 (2008), 2231–2267.
- [11] T. Everaert and T. Van der Linden, Baer invariants in semi-abelian categories I: General theory, Theory Appl. Categ. 12 (2004), no. 1, 1–33.
- [12] _____, Baer invariants in semi-abelian categories II: Homology, Theory Appl. Categ. 12 (2004), no. 4, 195–224.
- [13] _____, A note on double central extensions in exact Mal'tsev categories, Pré-Publicações DMUC 09-06 (2009), 1–8, submitted.
- [14] _____, Relative commutator theory in semi-abelian categories, in preparation, 2009.
- [15] A. Fröhlich, Baer-invariants of algebras, Trans. Amer. Math. Soc. 109 (1963), 221–244.
- [16] J. Furtado-Coelho, Homology and generalized Baer invariants, J. Algebra 40 (1976), 596–609.
- [17] J. Goedecke and T. Van der Linden, On satellites in semi-abelian categories: Homology without projectives, Math. Proc. Cambridge Philos. Soc., in press, published online 22 June 2009.
- [18] P. J. Higgins, Groups with multiple operators, Proc. London Math. Soc. 6 (1956), 366–416.
- [19] G. Janelidze, Pure Galois theory in categories, J. Algebra 132 (1990), 270–286.
- [20] _____, What is a double central extension? (The question was asked by Ronald Brown), Cah. Topol. Géom. Differ. Catég. XXXII (1991), no. 3, 191–201.
- [21] G. Janelidze and G. M. Kelly, Galois theory and a general notion of central extension, J. Pure Appl. Algebra 97 (1994), 135–161.
- [22] G. Janelidze, L. Márki, and W. Tholen, Semi-abelian categories, J. Pure Appl. Algebra 168 (2002), 367–386.
- [23] R. Lavendhomme and J. R. Roisin, Cohomologie non abélienne de structures algébriques, J. Algebra 67 (1980), 385–414.
- [24] A. S.-T. Lue, Baer-invariants and extensions relative to a variety, Math. Proc. Cambridge Philos. Soc. 63 (1967), 569–578.
- [25] D. Rodelo and T. Van der Linden, The third cohomology group classifies double central extensions, Pré-Publicações DMUC 08-55 (2008), 1–22, submitted.
- [26] A. Ursini, Osservazioni sulle varietà BIT, Boll. Unione Mat. Ital. 4 (1973), no. 7, 205–211.
- [27] _____, On subtractive varieties I, Algebra Universalis **31** (1994), 204–222.

Tomas Everaert

VAKGROEP WISKUNDE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2, 1050 BRUSSEL, BELGIUM *E-mail address*: teveraer@vub.ac.be

Tim Van der Linden

CENTRO DE MATEMÁTICA DA UNIVERSIDADE DE COIMBRA, 3001-454 COIMBRA, PORTUGAL *E-mail address*: tvdlinde@vub.ac.be

20