HAL open science

Mould theory and the double shuffle Lie algebra structure

Adriana Salerno, Leila Schneps

To cite this version:

Adriana Salerno, Leila Schneps. Mould theory and the double shuffle Lie algebra structure. Periods in Quantum Field Theory and Arithmetic, Jun 2020, Madrid, Spain. hal-02994290

HAL Id: hal-02994290

https://hal.science/hal-02994290v1

Submitted on 7 Nov 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Mould theory and the double shuffle Lie algebra structure

Adriana Salerno and Leila Schneps

Abstract. The real multiple zeta values $\zeta(k_1, \ldots, k_r)$ are known to form a $\mathbb{Q}$-algebra; they satisfy a pair of well-known families of algebraic relations called the double shuffle relations. In order to study the algebraic properties of multiple zeta values, one can replace them by formal symbols $Z(k_1, \ldots, k_r)$ subject only to the double shuffle relations. These form a graded Hopf algebra over $\mathbb{Q}$, and quotienting this algebra by products, one obtains a vector space. A complicated theorem due to G. Racinet proves that this vector space carries the structure of a Lie coalgebra; in fact Racinet proved that the dual of this space is a Lie algebra, known as the double shuffle Lie algebra $\mathfrak{ds}$.

J. Ecalle developed a new theory to explore combinatorial and algebraic properties of the formal multiple zeta values. His theory is sketched out in some publications (essentially [E1] and [E2]). However, because of the depth and complexity of the theory, Ecalle did not include proofs of many of the most important assertions, and indeed, even some interesting results are not always stated explicitly. The purpose of the present paper is to show how Racinet's theorem follows in a simple and natural way from Ecalle's theory. This necessitates an introduction to the theory itself, which we have pared down to only the strictly necessary notions and results.

§1. Introduction

In his doctoral thesis from 2000, Georges Racinet ([R1], see also [R2]) proved a remarkable theorem using astute combinatorial and algebraic reasoning. His proof was later somewhat simplified and streamlined by H. Furusho ([F]), but it remains really difficult to grasp the essential key that makes it work. The purpose of this article is to show how Ecalle's theory of moulds yields a very different and natural proof of the same result. The only difficulty is to enter into the universe of moulds and learn its language; the theory is equipped with a sort of standard all-purpose "toolbox" of objects and identities which, once acquired, serve to prove all kinds of results, in particular the one we consider in this paper. Therefore, the goal of this article is not only to present the mould-theoretic proof of Racinet's theorem, but also to provide an initiation into mould theory in general. Ecalle's seminal article on the subject is [E1], and a detailed introduction with complete proofs can be found in [S]; the latter text will be referred to here for some basic lemmas.

We begin by recalling the definitions necessary to state Racinet's theorem.

Definition. Let u, v be two monomials in x and y. Then the commutative *shuffle product* $\mathrm{sh}(u, v)$ is defined recursively by $\mathrm{sh}(u, v) = \{\{u\}\}$ if $v = 1$ and $\{\{v\}\}$ if $u = 1$, where $\{\{\cdot\}\}$ denotes a multiset, i.e. an unordered list with possible repetitions; otherwise, writing $u = Xu'$ and $v = Yv'$ where $X, Y \in \{x, y\}$ represents the first letter of the word, we have

the recursive rule

$$\mathrm{sh}(Xu, Yv) = \{\{X \cdot \mathrm{sh}(u, Yv)\}\} \cup \{\{Y \cdot \mathrm{sh}(Xu, v)\}\}, \tag{1.1}$$

where $\cup$ denotes the union of the two multisets which preserves repetitions and $X \cdot \mathrm{sh}(u, v)$ means we multiply every member in the multiset $\mathrm{sh}(u, v)$ on the left by X.

For example,

$$\begin{aligned}
\mathrm{sh}(xy, x) &= \{\{x \cdot \mathrm{sh}(y, x)\}\} \cup \{\{x \cdot \mathrm{sh}(xy, 1)\}\} \\
&= \{\{x \cdot \{\{yx, xy\}\}\ \}\} \cup \{\{x \cdot \{\{xy\}\}\ \}\} \\
&= \{\{xyx, xxy\}\} \cup \{\{xxy\}\} \\
&= \{\{xyx, xxy, xxy\}\}
\end{aligned}$$

If u, v are two words ending in y, we can write them uniquely as words in the letters $y_i = x^{i-1}y$. The *stuffle product* of u, v is defined by $\mathrm{st}(u, v) = \{\{u\}\}$ if $v = 1$ and $\{\{v\}\}$ if $u = 1$, and

$$\mathrm{st}(y_i u, y_j v) = \{\{y_i \cdot \mathrm{st}(u, y_j v)\}\} \cup \{\{y_j \cdot \mathrm{st}(y_i u, v\})\} \cup \{\{y_{i+j} \cdot \mathrm{st}(u, v)\}\}, \tag{1.2}$$

where y_i and y_j are respectively the first letters of the words u and v written in the y_j.

For example,

$$\begin{aligned}
\mathrm{st}(y_1y_2, y_1) &= \{\{y_1 \cdot \mathrm{st}(y_2, y_1)\}\} \cup \{\{y_1 \cdot \mathrm{st}((y_1y_2, 1)\}\} \cup \{\{y_2 \cdot \mathrm{st}(y_2, 1)\}\} \\
&= \{\{y_1y_2y_1, y_1y_1y_2, y_1y_3\}\} \cup \{\{y_1y_1y_2\}\} \cup \{\{y_2y_2\}\} \\
&= \{\{y_1y_2y_1, y_1y_1y_2, y_1y_3, y_1y_1y_2, y_2y_2\}\}
\end{aligned}$$

Definition. The *double shuffle space* $\mathfrak{ds}$ is the space of polynomials $f \in \mathbb{Q}\langle x, y\rangle$, the polynomial ring on two non-commutative variables x and y, of degree ≥ 3 that satisfy the following two properties:

(1) The coefficients of f satisfy the *shuffle relations*

$$\sum_{w \in \mathrm{sh}(u,v)} (f|w) = 0, \tag{1.3}$$

where u, v are words in x, y and $\mathrm{sh}(u, v)$ is the set of words obtained by shuffling them. This condition is equivalent to the assertion that f lies in the free Lie algebra $\mathrm{Lie}[x, y]$, a fact that is easy to see by using the characterization of Lie polynomials in the non-commutative polynomial ring $\mathbb{Q}\langle x, y\rangle$ as those that are "Lie-like" under the coproduct Δ defined by $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $\Delta(y) = y \otimes 1 + 1 \otimes y$, i.e. such that $\Delta(f) = f \otimes 1 + 1 \otimes f$ (cf. [Se, Ch. III, Thm. 5.4]). Indeed, when the property of being Lie-like under Δ is expressed explicitly on the coefficients of f it is nothing other than the shuffle relations (1.3).

(2) Let $f_* = \pi_y(f) + f_{\mathrm{corr}}$, where $\pi_y(f)$ is the projection of f onto just the words ending in y, and

$$f_{\mathrm{corr}} = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} (f|x^{n-1}y)y^n. \tag{1.4}$$

Considering f_* as being rewritten in the variables $y_i = x^{i-1}y$, the coefficients of f_* satisfy the *stuffle relations*:

$$\sum_{w \in \mathrm{st}(u,v)} (f_*|w) = 0, \tag{1.5}$$

where u and v are words in the y_i.

The double shuffle space $\mathfrak{ds}$ is the one defined by Racinet in [R1] (which he denoted $\mathfrak{dm}$, for the French term "double mélange"). It should not be confused with the bigraded space Dsh studied in [IKZ]. The space Dsh is a linearized version of $\mathfrak{ds}$, which has also been the subject of a great deal of study, but is more often denoted $\mathfrak{ls}$ (cf. for example [Br]).

For every $f \in \mathrm{Lie}[x,y]$, define a derivation D_f of $\mathrm{Lie}[x,y]$ by setting it to be

$$D_f(x) = 0, \quad D_f(y) = [y, f]$$

on the generators. Define the *Poisson (or Ihara) bracket* on (the underlying vector space of) $\mathrm{Lie}[x,y]$ by

$$\{f,g\} = [f,g] + D_f(g) - D_g(f). \tag{1.6}$$

This definition corresponds naturally to the Lie bracket on the space of derivations of $\mathrm{Lie}[x,y]$; indeed, it is easy to check that

$$[D_f, D_g] = D_f \circ D_g - D_g \circ D_f = D_{\{f,g\}}. \tag{1.7}$$

Racinet's Theorem. *The double shuffle space $\mathfrak{ds}$ is a Lie algebra under the Poisson bracket.*

The goal of this paper is to give the mould-theoretic proof of this result, which first necessitates rephrasing the relevant definitions in terms of moulds. The paper is organized as follows. In §2, we give basic definitions from mould theory that will be used throughout the rest of the paper, and in §3 we define dimorphy and consider the main dimorphic subspaces related to double shuffle. In §4 we give the dictionary between mould theory and the double shuffle situation. In §5 we give some of the definitions and basic results on the group aspect of mould theory. In §6 we describe the special mould *pal* that lies at the heart of much of mould theory, and introduce Ecalle's fundamental identity. The final section §7 contains the simple and elegant proof of the mould version of Racinet's theorem. Sections §§2, 3, 5 and 6 can serve as a short introduction to the basics of mould theory; a much more complete version with full proofs and details is given in [S], which is cited for some results. Every mould-theory definition in this paper is due to Ecalle, as are all of the statements, although some of these are not made explicitly in his papers, but used as assumptions. Our contribution has been firstly to provide complete proofs of many statements which are either nowhere proved in his articles or proved by arguments that are difficult to understand (at least by us), secondly to pick a path through the dense forest of his results that leads most directly to the desired theorem, and thirdly, to give the dictionary that identifies the final result with Racinet's theorem above.

In order to preserve the expository flow leading to the proof of the main theorem, we have chosen to consign the longer and more technical proofs to appendices or, for those that already appear in [S], to simply give the reference.

Acknowledgements. The authors wish to thank the ICMAT and the Women in Numbers group for hosting wonderful workshops, the referees for the careful reading of this paper and the many improvements that resulted, and Jean Ecalle for his guidance. Salerno was partially supported by the NSF-AWM Mentoring Travel grant.

§2. Definitions for mould theory

This section constitutes what could be called the "first drawer" of the mould toolbox, with only the essential definitions of moulds, some operators on moulds, and some mould symmetries. We work over a base field K, and let $u_1, u_2, \ldots$ be a countable set of indeterminates, and $v_1, v_2, \ldots$ another. The definitions below arise from Ecalle's papers (see especially [E1], and are also developed at length in [S] and [Cr].

Moulds. A *mould* in the variables u_i is a family $A = (A_r)_{r\geq 0}$ of functions of the u_i, where each A_r is a function of $u_1, \ldots, u_r$. We call A_r the *depth* r component of the mould. In this paper we let $K = \mathbb{Q}$, and in fact we consider only rational-function valued moulds, i.e. we have $A_r(u_1, \ldots, u_r) \in \mathbb{Q}(u_1, \ldots, u_r)$ for $r \geq 0$. Note that $A_0(\emptyset)$ is a constant. We often drop the index r when the context is clear, and write $A(u_1, \ldots, u_r)$. Moulds can be added and multiplied by scalars componentwise, so the set of moulds forms a vector space. A mould in the v_i is defined identically for the variables v_i.

Let ARI (resp. $\overline{\text{ARI}}$) denote the space of moulds in the u_i (resp. in the v_i) such that $A_0(\emptyset) = 0$*. These two vector spaces are obviously isomorphic, but they will be equipped with very different Lie algebra structures. We use superscripts on ARI to denote the type of moulds we are dealing with; in particular ARI^{pol} denotes the space of polynomial-valued moulds, and ARI^{rat} denotes the space of rational-function moulds.

Operators on moulds. We will use the following operators on moulds in ARI:

$$\text{neg}(A)(u_1, \ldots, u_r) = A(-u_1, \ldots, -u_r) \tag{2.1}$$

$$\text{push}(A)(u_1, \ldots, u_r) = A(-u_1 - \cdots - u_r, u_1, \ldots, u_{r-1}) \tag{2.2}$$

$$\text{mantar}(A)(u_1, \ldots, u_r) = (-1)^{r-1} A(u_r, \ldots, u_1). \tag{2.3}$$

We also introduce the swap, which is a map from *ARI* to $\overline{ARI}$ given by

$$\text{swap}(A)(v_1, \ldots, v_r) = A(v_r, v_{r-1} - v_r, v_{r-2} - v_{r-1}, \ldots, v_1 - v_2), \tag{2.4}$$

* Écalle works with *bimoulds*, which are moulds that are simultaneously in the variables u_i and v_i. However, while bimoulds are well-adapted to the study of certain more complex objects such as multizeta values colored by roots of unity, they do not arise naturally in the context of the simple multizeta values used here, and we found that using moulds in only the u_i or only the v_i made the proofs and the notation considerably simpler.

and its inverse, also called swap, from $\overline{ARI}$ to ARI:

$$\mathrm{swap}(A)(u_1,\dots,u_r) = A(u_1+\cdots+u_r, u_1+\cdots+u_{r-1},\dots,u_1+u_2,u_1). \tag{2.5}$$

Thanks to this formulation, which is not ambiguous since to know which swap is being used it suffices to check whether swap is being applied to a mould in ARI or one in $\overline{ARI}$, we can treat swap like an involution: $\mathrm{swap}\circ\mathrm{swap} = \mathrm{id}$.

Let us now introduce some notation necessary for the Lie algebra structures on ARI and $\overline{\mathrm{ARI}}$.

Flexions. Let $\mathbf{w} = (u_1,\cdots,u_r)$. For every possible way of cutting the word $\mathbf{w}$ into three (possibly empty) subwords $\mathbf{w} = \mathbf{abc}$ with

$$\mathbf{a} = (u_1,\dots,u_k),\quad \mathbf{b} = (u_{k+1},\dots,u_{k+l}),\quad \mathbf{c} = (u_{k+l+1},\dots,u_r),$$

set

$$\begin{cases} \mathbf{a}\rceil = (u_1,u_2,\cdots,u_{k-1},u_k+u_{k+1}+\cdots+u_{k+l}) & \text{if } \mathbf{b}\neq\emptyset, \text{ otherwise } \mathbf{a}\rceil = \mathbf{a} \\ \lceil\mathbf{c} = (u_{k+1}+\cdots+u_{k+l+1}, u_{k+l+2},\cdots,u_r) & \text{if } \mathbf{b}\neq\emptyset, \text{ otherwise } \lceil\mathbf{c} = \mathbf{c}. \end{cases}$$

If now $\mathbf{w} = (v_1,\dots,v_r)$ is a word in the v_i, then for every decomposition $\mathbf{w} = \mathbf{abc}$ with

$$\mathbf{a} = (v_1,\dots,v_k),\quad \mathbf{b} = (v_{k+1},\dots,v_{k+l}),\quad \mathbf{c} = (v_{k+l+1},\dots,v_r),$$

we set

$$\begin{cases} \mathbf{b}\rfloor = (v_{k+1}-v_{k+l+1}, v_{k+2}-v_{k+l+1},\dots,v_{k+l}-v_{k+l+1}) & \text{if } \mathbf{c}\neq\emptyset, \text{ otherwise } \mathbf{b}\rfloor = \mathbf{b} \\ \lfloor\mathbf{b} = (v_{k+1}-v_k, v_{k+2}-v_k,\dots,v_{k+l}-v_k) & \text{if } \mathbf{a}\neq\emptyset, \text{ otherwise } \lfloor\mathbf{b} = \mathbf{b}. \end{cases}$$

Operators on pairs of moulds. For $A,B\in\mathrm{ARI}$ or $A,B\in\overline{\mathrm{ARI}}$, we set

$$\mathrm{mu}(A,B)(\mathbf{w}) = \sum_{\mathbf{w}=\mathbf{ab}} A(\mathbf{a})B(\mathbf{b}) \tag{2.6}$$

$$\mathrm{lu}(A,B) = \mathrm{mu}(A,B) - \mathrm{mu}(B,A). \tag{2.7}$$

For any mould $B\in\mathrm{ARI}$, we define two operators on ARI, $\mathrm{amit}(B)$ and $\mathrm{anit}(B)$, defined by

$$\big(\mathrm{amit}(B)\cdot A\big)(\mathbf{w}) = \sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{b},\mathbf{c}\neq\emptyset}} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b})$$

$$\big(\mathrm{anit}(B)\cdot A\big)(\mathbf{w}) = \sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{a},\mathbf{b}\neq\emptyset}} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}). \tag{2.8}$$

For any mould $B\in\mathrm{ARI}$, the operators $\mathrm{amit}(B)$ and $\mathrm{anit}(B)$ are derivations of ARI for the lu-bracket (see [S], Prop. 2.2.1). We define a third derivation, $\mathrm{arit}(B)$, by

$$\big(\mathrm{arit}(B)\cdot A\big)(\mathbf{w}) = \mathrm{amit}(B)\cdot A - \mathrm{anit}(B)\cdot A. \tag{2.9}$$

If $B \in \overline{\mathrm{ARI}}$ we have derivations of $\overline{\mathrm{ARI}}$ given by

$$\big(\mathrm{amit}(B)\cdot A\big)(\mathbf{w}) = \sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{b},\mathbf{c}\neq\emptyset}} A(\mathbf{ac})B(\mathbf{b}\rfloor)$$

$$\big(\mathrm{anit}(B)\cdot A\big)(\mathbf{w}) = \sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{a},\mathbf{b}\neq\emptyset}} A(\mathbf{ac})B(\lfloor\mathbf{b}), \tag{2.10}$$

and again we define the derivation $\mathrm{arit}(B)$ as in (2.9). Finally, for $A, B \in \mathrm{ARI}$ or $A, B \in \overline{\mathrm{ARI}}$, we set

$$\mathrm{ari}(A, B) = \mathrm{arit}(B)\cdot A + \mathrm{lu}(A, B) - \mathrm{arit}(A)\cdot B. \tag{2.11}$$

Remark. The condition $\mathbf{b} \neq \emptyset$ in the definitions of *amit* and *anit* above are not necessary in (2.8) and (2.10), since we are assuming that $B \in \mathrm{ARI}$, so it has the property that $B(\emptyset) = 0$; this means that including decompositions with $\mathbf{b} = \emptyset$ in the sum would not actually change the values. However, we chose to reproduce Écalle's definition, which also applies to moulds with non-zero value in depth 0, so as to make it easier to consult his articles and recognize the same definitions.

Since $\mathrm{arit}(B)$ is a derivation for lu, the ari-operator is easily shown to be a Lie bracket. Note that although we use the same notation ari for the Lie brackets on both ARI and $\overline{\mathrm{ARI}}$, they are two different Lie brackets on two different spaces. Indeed, while some formulas and properties (such as mu, or alternality, see (2.12) below) are written identically for ARI and $\overline{\mathrm{ARI}}$, others, in particular all those that use flexions, are very different, since the definitions of upper flexions (on the u_i) and lower flexions (on the v_i are very different. This can be seen in the following examples.

Examples. We give a few of the expressions above explicitly in low depth. The moulds $\mathrm{amit}(B)\cdot A$ and $\mathrm{amit}(B)\cdot A$ are all zero in depth 1. Let $A, B \in \mathrm{ARI}$ and let us compute the mould $\mathrm{amit}(B)\cdot A$ in depth 2. The only possible decomposition of $\mathbf{w} = (u_1, u_2)$ as $\mathbf{abc}$ with $\mathbf{b}, \mathbf{c} \neq 0$ is $\mathbf{abc} = (\emptyset)(u_1)(u_2)$, so using the upper flexions as in (2.8), we have $\lceil\mathbf{c} = (u_1 + u_2)$ and

$$\big(\mathrm{amit}(B)\cdot A\big)(u_1, u_2) = A(u_1 + u_2)B(u_1).$$

(Note that if we don't include the condition $\mathbf{b} \neq 0$ in the sum, we would also consider the decomposition $\mathbf{abc} = (u_1)(\emptyset)(u_2)$ so we would add on the term $A(u_1, u_2)B(\emptyset)$, but as pointed out in the remark above, this term is zero since $B \in \mathrm{ARI}$.)

Now let us compute the mould $\mathrm{anit}(B)\cdot A$ in depth 3. Let $\mathbf{w} = (u_1, u_2, u_3)$. The decompositions $\mathbf{w} = \mathbf{abc}$ with $\mathbf{a}, \mathbf{b} \neq 0$ are given by $(u_1)(u_2)(u_3)$, $(u_1, u_2)(u_3)(\emptyset)$ and $(u_1)(u_2, u_3)(\emptyset)$, so

$$\big(\mathrm{anit}(B)\cdot A\big)(u_1, u_2, u_3) = A(u_1+u_2, u_3)B(u_2)+A(u_1, u_2+u_3)B(u_3)+A(u_1+u_2+u_3)B(u_2, u_3).$$

If $A, B \in \overline{\mathrm{ARI}}$, we again compute $\mathrm{amit}(B)\cdot A$ in depth 2 and $\mathrm{anit}(B)\cdot A$ in depth 3, but now using the lower flexions of (2.10); we obtain the expressions

$$\big(\mathrm{amit}(B)\cdot A\big)(v_1, v_2) = A(v_2)B(v_1 - v_2)$$

$$\big(\mathrm{anit}(B)\cdot A\big)(v_1,v_2,v_3) = A(v_1,v_3)B(v_2-v_1)+A(v_1,v_2)B(v_3-v_2)+A(v_1)B(v_2-v_1,v_3-v_1).$$

Symmetries. A mould in ARI (resp. $\overline{\mathrm{ARI}}$) is said to be *alternal* if for all words $\mathbf{u},\mathbf{v}$ in the u_i (resp. v_i),

$$\sum_{\mathbf{w}\in\mathrm{sh}(\mathbf{u},\mathbf{v})} A(\mathbf{w}) = 0. \tag{2.12}$$

The relations in (2.12) are known as the *alternality* relations, and they are identical for moulds in ARI and $\overline{\mathrm{ARI}}$. Let us now define the *alternility relations.* Écalle defined families of alternility relations for moulds in ARI and in $\overline{\mathrm{ARI}}$ (and indeed, for general bimoulds), but for the purposes of this article we only need to introduce these relations on moulds in $\overline{\mathrm{ARI}}$. Just as the alternality conditions are the mould equivalent of the shuffle relations, the alternility conditions on $\overline{\mathrm{ARI}}$ are the mould equivalent of the stuffle relations, translated in terms of the alphabet $\{v_1,v_2,\ldots\}$ as follows. Let $Y_1=(y_{i_1},\ldots,y_{i_r})$ and $Y_2=(y_{j_1},\ldots,y_{j_s})$ be two sequences; for example, we consider $Y_1=(y_i,y_j)$ and $Y_2=(y_k,y_l)$. Let w be a word in the stuffle product $\mathrm{st}\big(Y_1,Y_2\big)$, which in our example is the 13-element multiset

$$\{\{(y_i,y_j,y_k,y_l),(y_i,y_k,y_j,y_l),(y_i,y_k,y_l,y_j),(y_k,y_i,y_j,y_l),(y_k,y_i,y_l,y_j),(y_k,y_l,y_i,y_j),$$
$$(y_i,y_{j+k},y_l),(y_{i+k},y_j,y_l),(y_i,y_k,y_{j+l}),(y_{i+k},y_l,y_j),(y_k,y_i,y_{j+l}),(y_k,y_{i+l},y_j),$$
$$(y_{i+k},y_{j+l})\}\}. \tag{2.13}$$

To each such word we associate an alternility term for the mould A, given by associating the tuple (v_1,v_2,v_3,v_4) to the ordered tuple (y_i,y_j,y_k,y_l) and taking

$$\frac{1}{(v_i-v_j)}\big(A(\ldots,v_i,\ldots)-A(\ldots,v_j,\ldots)\big) \tag{2.14}$$

for each contraction occurring in the word w. For instance in our example we have the six alternility terms

$$A(v_1,v_2,v_3,v_4),A(v_1,v_3,v_2,v_4),A(v_1,v_3,v_4,v_2),A(v_3,v_1,v_2,v_4),$$
$$A(v_3,v_1,v_4,v_2),A(v_3,v_4,v_1,v_2) \tag{2.15}$$

corresponding to the first six words in (2.13), the six terms

$$\frac{1}{(v_2-v_3)}\big(A(v_1,v_2,v_4)-A(v_1,v_3,v_4)\big),\quad \frac{1}{(v_1-v_3)}\big(A(v_1,v_2,v_4)-A(v_3,v_2,v_4)\big),$$
$$\frac{1}{(v_2-v_4)}\big(A(v_1,v_3,v_2)-A(v_1,v_3,v_4)\big),\quad \frac{1}{(v_1-v_3)}\big(A(v_1,v_4,v_2)-A(v_3,v_4,v_2)\big),$$
$$\frac{1}{(v_2-v_4)}\big(A(v_3,v_1,v_2)-A(v_3,v_1,v_4)\big),\quad \frac{1}{(v_1-v_4)}\big(A(v_3,v_1,v_2)-A(v_3,v_4,v_2)\big) \tag{2.16}$$

corresponding to the next six words, and the final term

$$\frac{1}{(v_1-v_3)(v_2-v_4)}\big(A(v_1,v_2)-A(v_3,v_2)-A(v_1,v_4)+A(v_3,v_4)\big) \tag{2.17}$$

corresponding to the final word with the double contraction. Let us write $A_{\mathbf{w}}$ for the alternility term of A associated to a word $\mathbf{w}$ in the stuffle product $\mathrm{st}(Y_1,Y_2)$; note that the alternility terms (for example those in (2.15), (2.16) and (2.17) associated to the words $\mathbf{w}$ in the list (2.13)) are not all terms of the form $A(\mathbf{w})$ or even linear combinations of such terms (due to the denominators). However, the alternality terms $A_{\mathbf{w}}$ are all polynomials in the v_i, since the zeros of the denominators all correspond to zeros of the numerator.

The *alternility relation* associated to the pair (Y_1,Y_2) on A is the sum of the alternility terms associated to words in the stuffle of Y_1 and Y_2; it is given by

$$\sum_{\mathbf{w}\in\mathrm{st}(Y_1,Y_2)} A_{\mathbf{w}} = 0. \tag{2.18}$$

Let $A_{r,s}$ denote the left-hand side of (2.18). Note that indeed, $A_{r,s}$ does not depend on the actual sequences Y_1 and Y_2, but merely on the number of letters in Y_1 and in Y_2. For example when $r=s=2$, the alternility sum $A_{2,2}$ is given by the sum of the terms (2.15)-(2.17) above. Furthermore, like for the shuffle, we may assume that $r\le s$ by symmetry. Thus we have the following definition: a mould in $\overline{\mathrm{ARI}}$ is said to be *alternil* if it satisfies the alternility relation $A_{r,s}=0$ for all pairs of integers $1\le r\le s$.

§3. Lie subalgebras of ARI

In this section, we show that the spaces of moulds satisfying certain important symmetry properties are closed under the ari-bracket. In particular, we introduce the following *dimorphic spaces* investigated by Écalle, where the term dimorphy refers to the double description of a mould by a symmetry property on it and another one on its swap.

Definitions. Let ARI_{al} denote the set of alternal moulds. Let $\mathrm{ARI}_{al/al}$ (resp. $\mathrm{ARI}_{al/il}$) denote the set of alternal moulds with alternal (resp. alternil) swap. Let ARI_{al*al} (resp. ARI_{al*il}) denote the set of alternal moulds whose swap is alternal (resp. alternil) up to addition of a constant-valued mould. Finally, let $\mathrm{ARI}_{\underline{al}/\underline{al}}$ (resp. $\mathrm{ARI}_{\underline{al}*\underline{al}}$, $\mathrm{ARI}_{\underline{al}/\underline{il}}$, $\mathrm{ARI}_{\underline{al}*\underline{il}}$) denote the subspace of $\mathrm{ARI}_{al/al}$ (resp. ARI_{al*al}, $\mathrm{ARI}_{al/il}$, ARI_{al*il}) consisting of moulds A such that A_1 is an even function, i.e. $A(-u_1)=A(u_1)$.

The first main theorem of this paper is the following result, which is used constantly in Ecalle's work although no explicit proof appears to have been written down, and the proof is by no means as easy as one might imagine.

Theorem 3.1. *The subspace* $\mathrm{ARI}_{al}\subset\mathrm{ARI}$ *of alternal moulds forms a Lie algebra under the* ari*-bracket, as does the subspace* $\overline{\mathrm{ARI}}_{al}$ *of* $\overline{\mathrm{ARI}}$.

The full proof is given in Appendix A. The idea is as follows: if $C=\mathrm{ari}(A,B)$, then by (2.11) it is enough to show separately that if A and B are alternal then $\mathrm{lu}(A,B)$ is alternal

and $\mathrm{arit}(B)\cdot A$ is alternal. This is done via a combinatorial manipulation that is fairly straightforward for lu but actually quite complicated for arit.

We next have a simple but important result on polynomial-valued moulds.

Proposition 3.2. *The subspace* ARI^{pol} *of polynomial-valued moulds in* ARI *forms a Lie algebra under the* ari-*bracket.*

Proof. This follows immediately from the definitions of mu, arit and ari in (2.6)-(2.9), as all the operations and flexions there are polynomial. ♢

Now we give another key theorem, the first main result concerning dimorphy. This result, again, is used repeatedly by Ecalle but we were not able to find a complete proof in his papers, so we have reconstructed one here (see also [S, §2.5]).

Theorem 3.3. *The subspaces* $\mathrm{ARI}_{\underline{al}/\underline{al}}$ *and* $\mathrm{ARI}_{\underline{al}*\underline{al}}$ *form Lie algebras under the* ari-*bracket.*

The proof is based on the following two propositions.

Proposition 3.4. *If* $A\in\mathrm{ARI}_{\underline{al}*\underline{al}}$*, then* A *is* neg-*invariant and* push-*invariant.*

The proof of this proposition is deferred to Appendix B.

Proposition 3.5. *If* A *and* B *are both* push-*invariant moulds, then*

$$\mathrm{swap}\Big(\mathrm{ari}\big(\mathrm{swap}(A),\mathrm{swap}(B)\big)\Big)=\mathrm{ari}(A,B), \tag{3.1}$$

Proof. Explicit computation using the flexions shows that for all moulds $A,B\in\mathrm{ARI}$ we have the general formula:

$$\mathrm{swap}\big(\mathrm{ari}(\mathrm{swap}(A),\mathrm{swap}(B))\big)=\mathrm{axit}\big(B,-\mathrm{push}(B)\big)\cdot A-\mathrm{axit}\big(A,-\mathrm{push}(A)\big)\cdot B+\mathrm{lu}(A,B), \tag{3.2}$$

where here ari is the Lie bracket on $\overline{\mathrm{ARI}}$, and axit is the operator on ARI defined for a general pair of moulds $B,C\in\mathrm{ARI}$ by the formula

$$\mathrm{axit}(B,C)\cdot A=\mathrm{amit}(B)\cdot A+\mathrm{anit}(C)\cdot A.$$

(See [S, §4.1] for complete details of this flexion computation.) Comparing with (2.9) shows that $\mathrm{arit}(B)=\mathrm{axit}(B,-B)$. Thus if A and B are push-invariant, (3.2) reduces to

$$\mathrm{swap}\Big(\mathrm{ari}\big(\mathrm{swap}(A),\mathrm{swap}(B)\big)\Big)=\mathrm{arit}(B)\cdot A-\mathrm{arit}(A)\cdot B+\mathrm{lu}(A,B),$$

which is exactly $\mathrm{ari}(A,B)$ by (2.11). ♢

Proof of Theorem 3.3. Using these two propositions, the proof becomes reasonably easy. We first consider the case where $A,\ B\in\mathrm{ARI}_{\underline{al}/\underline{al}}$. In particular A and B are alternal. Set $C=\mathrm{ari}(A,B)$. The mould C is alternal by Theorem 3.1. By Proposition 3.4, we know that A and B are push-invariant, so by Proposition 3.5 we have

$\mathrm{swap}(C) = \mathrm{swap}\big(\mathrm{ari}(A,B)\big) = \mathrm{ari}\big(\mathrm{swap}(A), \mathrm{swap}(B)\big)$. But this is also alternal by Theorem 3.1, so $C \in \mathrm{ARI}_{al/al}$. Furthermore, it follows directly from the defining formula for the ari-bracket, which is additive in the mould depths, that if C is an ari-bracket of two moulds in ARI, i.e. with constant term equal to 0, we must have $C(u_1) = 0$, so $C \in \mathrm{ARI}_{\underline{al}/\underline{al}}$.

Now we consider the more general situation where $A, B \in \mathrm{ARI}_{\underline{al}*\underline{al}}$. Let A_0, B_0 be the constant-valued moulds such that $\mathrm{swap}(A) + A_0$ and $\mathrm{swap}(B) + B_0$ are alternal. From the definitions (2.6)-(2.9), we see that for any constant-valued mould M_0, we have $\mathrm{arit}(M_0) \cdot M = 0$. Indeed if M_0 is constant-valued, say with constant value c_r in depth r, then

$$\big(arit(M_0) \cdot M\big)(\mathbf{w}) = \sum_{\substack{\mathbf{w}=\mathbf{abc} \\ \mathbf{b},\mathbf{c}\neq 0}} M(\mathbf{a}\lceil\mathbf{c})M_0(\mathbf{b}) - \sum_{\substack{\mathbf{w}=\mathbf{abc} \\ \mathbf{a},\mathbf{b}\neq 0}} M(\mathbf{a}\rceil\mathbf{c})M_0(\mathbf{b}).$$

Writing $\mathbf{w} = \mathbf{abc} = (u_1, \ldots, u_i)(u_{i+1}, \ldots, u_{i+j})(u_{i+j+1}, \ldots, u_r)$, we can rewrite this as

$$\sum_{i=0}^{r-2}\sum_{j=1}^{r-1} c_j M(u_1, \ldots, u_i, u_{i+1} + \cdots + u_{i+j+1}, u_{i+j+2}, \ldots, u_r)$$

$$-\sum_{i=1}^{r-1}\sum_{j=1}^{r-1} c_j M(u_1, \ldots, u_{i-1}, u_i + \cdots + u_{i+j}, u_{i+j+1}, \ldots, u_r).$$

But by renumbering i as $i+1$ in the first sum shows that these two sums are in fact equal, so their difference is zero. An analogous computation shows that $\mathrm{arit}(M) \cdot M_0 = \mathrm{lu}(M, M_0)$. Thus by (2.11), we have $\mathrm{ari}(M, M_0) = 0$, so we find that

$$\mathrm{ari}(A + A_0, B + B_0) = \mathrm{ari}(A, B) + \mathrm{ari}(A, B_0) + \mathrm{ari}(A_0, B) + \mathrm{ari}(A_0, B_0) = \mathrm{ari}(A, B). \quad (3.3)$$

Now, A and B are push-invariant by Proposition 3.4, and constant-valued moulds are always push-invariant, so $A + A_0$ and $B + B_0$ are also push-invariant; thus we have

$$\begin{aligned}\mathrm{swap}(C) &= \mathrm{swap}\big(\mathrm{ari}(A,B)\big) \\ &= \mathrm{swap}\big(\mathrm{ari}(A + A_0, B + B_0)\big) \quad \text{by (3.3)} \\ &= \mathrm{ari}\big(\mathrm{swap}(A + A_0), \mathrm{swap}(B + B_0)\big) \quad \text{by (3.1).}\end{aligned}$$

But since swap preserves constant-valued moulds, we have $\mathrm{swap}(A + A_0) = \mathrm{swap}(A) + A_0$ and $\mathrm{swap}(B + B_0) = \mathrm{swap}(B) + B_0$. These two moulds are alternal by hypothesis, so by Theorem 3.1, their ari-bracket is alternal, i.e. $\mathrm{swap}(C)$ is alternal. Since as above we have $C(u_1) = 0$, we find that in fact C is not just in $\mathrm{ARI}_{\underline{al}*\underline{al}}$ but in $\mathrm{ARI}_{\underline{al}/\underline{al}}$. This completes the proof of Theorem 3.3. $\diamondsuit$

We will see in the next section that the double shuffle space $\mathfrak{ds}$ defined in §1 is isomorphic to the space of polynomial-valued moulds $\mathrm{ARI}^{pol}_{\underline{al}*\underline{il}}$, with the alternality property translating shuffle and the alternility property translating stuffle. Thus dimorphy is closely connected to double shuffle, but much more general, since the symmetry properties of alternality or alternility on itself or its swap can hold for any mould, not just polynomial ones.

§4. Dictionary with the Lie algebra and double shuffle framework

Let $C_i = ad(x)^{i-1}y \in \mathbb{Q}\langle x, y\rangle$, where $ad(x)y = [x, y]$. By Lazard elimination (see [Bo, Prop. 10a]), the subring $\mathbb{Q}\langle C_1, C_2, \ldots\rangle$, which we denote simply by $\mathbb{Q}\langle C\rangle$, is free on the C_i. Let $\mathbb{Q}_0\langle C\rangle$ denote the subspace of polynomials in the C_i with constant term equal to 0. Define a linear map

$$\begin{aligned} ma : \mathbb{Q}_0\langle C\rangle &\xrightarrow{\sim} \mathrm{ARI}^{pol} \\ C_{a_1}\cdots C_{a_r} &\mapsto A_{a_1,\ldots,a_r} \end{aligned} \tag{4.1}$$

where $A_{a_1,\ldots,a_r}$ is the polynomial mould concentrated in depth r defined by

$$A_{a_1,\ldots,a_r}(u_1,\ldots,u_r) = (-1)^{a_1+\cdots+a_r-r}u_1^{a_1-1}\cdots u_r^{a_r-1}. \tag{4.2}$$

This map ma is trivially invertible and thus an isomorphism of vector spaces. Let $\mathrm{Lie}[C]$ denote the free Lie algebra $\mathrm{Lie}[C_1, C_2, \ldots]$ on the C_i. Note that, again by Lazard elimination, we can write $\mathrm{Lie}[x, y] = \mathbb{Q}x \oplus \mathrm{Lie}[C]$. Since by its definition, all elements of the double shuffle space $\mathfrak{ds} \subset \mathrm{Lie}[x, y]$ are polynomials of degree ≥ 3, we have

$$\mathfrak{ds} \subset \mathrm{Lie}[C] \subset \mathbb{Q}_0\langle C\rangle.$$

Definition. Let $\mathcal{MT}_0$ denote the Lie algebra whose underlying space is the space of polynomials $\mathbb{Q}_0\langle C\rangle$, equipped with the Poisson bracket (1.6), and let $\mathfrak{mt}$ denote the subspace of Lie polynomials in the C_i, i.e. the vector space $\mathrm{Lie}[C]$ equipped with the Poisson bracket. Observe that $\mathfrak{mt}$ is closed under the Poisson bracket since if f, g are Lie then so are $D_f(g)$, $D_g(f)$ and $[f, g]$, so $\mathfrak{mt}$ is a Lie algebra. The letters "M-T" stand for *twisted Magnus* (cf. [R1]). Let $\mathcal{MT}$ denote the universal enveloping algebra of $\mathfrak{mt}$. It is isomorphic as a vector space to $\mathbb{Q}\langle C\rangle$, and like all universal enveloping algebras, it is equipped with a pre-Lie* law $\odot$. In the special case where $g \in \mathfrak{mt}$, the pre-Lie law on $\mathcal{MT}$ reduces to the expression $f \odot g = fg - D_g(f)$, so that we have $f \odot g - g \odot f = \{f, g\}$ as befits the pre-Lie law of a universal enveloping algebra. Let us also define the twisted Magnus group as the exponential $MT = \exp^{\odot}(\mathfrak{mt})$, where $exp^{\odot}(f) = \sum_{n\geq 0} \frac{1}{n!} f^{\odot n}$. Note that $f^{\odot n} = f^{\odot(n-1)} \odot f = f^n - D_f(f^{\odot n})$, which gives an explicit recursive expression for $f^{\odot n}$.

Theorem 4.1. (Racinet) *The linear isomorphism (4.1) is a Lie algebra isomorphism*

$$ma : \mathcal{MT}_0 \xrightarrow{\sim} \mathrm{ARI}^{pol}, \tag{4.3}$$

and it restricts to a Lie algebra isomorphism of the Lie subalgebras

$$ma : \mathfrak{mt} \xrightarrow{\sim} \mathrm{ARI}^{pol}_{al}. \tag{4.4}$$

Proof. In view of the fact that ma is invertible as a linear map, the isomorphism (4.3) follows from the following identity relating the Poisson bracket and the ari-bracket on

* A pre-Lie law must satisfy the defining relation $\big((f \odot g) \odot h\big) - \big(f \odot (g \odot h)\big) = \big(f \odot h) \odot g\big) - \big(f \odot (h \odot g)\big)$.

polynomial-valued moulds, which was proven by Racinet in his thesis ([R1, Appendix A], see also [S, Corollary 3.3.4]):

$$ma\big(\{f,g\}\big) = \mathrm{ari}\big(ma(f), ma(g)\big), \tag{4.5}$$

The isomorphism (4.4), identifying Lie polynomials with alternal polynomial moulds, follows from a standard argument that we indicate briefly, as it is merely an adaptation to $\mathrm{Lie}[C]$ of the similar argument following the definition of the shuffle relations in (1.3). Let Δ denote the standard cobracket on $\mathbb{Q}\langle C\rangle$ defined by $\Delta(C_i) = C_i \otimes 1 + 1 \otimes C_i$. Then the Lie subspace $\mathrm{Lie}[C]$ of the polynomial algebra $\mathbb{Q}\langle C\rangle$ is the space of primitive elements for Δ, i.e. elements $f \in \mathrm{Lie}[C]$ satisfying $\Delta(f) = f \otimes 1 + 1 \otimes f$. This condition on f is given explicitly on the coefficients of f by the family of shuffle relations

$$\sum_{D \in \mathrm{sh}(C_{a_1}\cdots C_{a_r}, C_{b_1}\cdots C_{b_s})} (f|D) = 0,$$

where $(f|D)$ denotes the coefficient in the polynomial f of the monomial D in the C_i. But these conditions are exactly equivalent to the alternality relations

$$\sum_{D \in \mathrm{sh}((a_1,\ldots,a_r),(b_1,\ldots,b_s))} ma(f)(D) = 0,$$

proving (4.4). $\diamondsuit$

Theorem 4.3. *The linear isomorphism (4.4) restricts to a linear isomorphism of the subspaces*

$$ma : \mathfrak{ds} \xrightarrow{\sim} \mathrm{ARI}^{pol}_{\underline{al}*\underline{il}}. \tag{4.6}$$

Proof. By (4.4), since $\mathfrak{ds} \subset \mathfrak{mt}$, we have $ma : \mathfrak{ds} \hookrightarrow \mathrm{ARI}^{pol}_{al}$. If an element $f \in \mathfrak{ds}$ has a depth 1 component, i.e. if the coefficient of $x^{n-1}y$ in f is non-zero, then n is odd; this is a simple consequence of solving the depth 2 stuffle relations (see [C, Theorem 2.30 (i)] for details). Thus, if the mould $ma(f)$ has a depth 1 component, it will be an even function, since by the definition of ma the degree of $ma(f)(u_1)$ is equal to the degree of f minus 1. This shows that ma maps $\mathfrak{ds}$ to moulds that are even in depth 1, i.e.

$$ma : \mathfrak{ds} \hookrightarrow \mathrm{ARI}^{pol}_{\underline{al}}.$$

It remains only to show that if $f \in \mathfrak{ds}$ then $\mathrm{swap}\big(ma(f)\big)$ is alternil up to addition of a constant mould, i.e. that the stuffle conditions (1.5) imply the alternility of $\mathrm{swap}\big(ma(f)\big)$.

By additivity, we may assume that f is of homogeneous degree n. Let C be the constant mould concentrated in depth n given by $C(u_1,\ldots,u_n) = \frac{(-1)^{n-1}}{n}(f|x^{n-1}y)$, and let $A = \mathrm{swap}\big(ma(f)\big) + C$. Écalle showed (see [R1, Appendix A] or [S, (3.2.6)] for full details) that we have the following explicit expression for $\mathrm{swap}\big(ma(f)\big)$. If for $r \geq 1$ we write the depth r part of f_* as

$$(f_*)^r = \sum_{\mathbf{a}=(a_1,\ldots,a_r)} c_{\mathbf{a}}\, y_{a_1}\cdots y_{a_r}, \tag{4.7}$$

then $\mathrm{swap}\big(ma(f)\big)$ is given by

$$\mathrm{swap}\big(ma(f)\big)(v_1,\dots,v_r) = \sum_{\mathbf{a}=(a_1,\dots,a_r)} c_{\mathbf{a}}\, v_1^{a_1-1}\cdots v_r^{a_r-1}. \tag{4.8}$$

Note that since f is homogeneous of degree n, the associated mould $A = \mathrm{swap}\big(ma(f)\big)+C$ is concentrated in depths $\leq n$. We will use this close relation between the polynomial f_* and the mould A to show that the stuffle relations (1.5) on f_* are equivalent to the alternility of A.

For any pair of integers $1 \leq r \leq s$, let $A_{r,s}$ denote the alternility sum associated to the mould A as in (2.18). By definition, A is alternil if and only if $A_{r,s} = 0$ for all pairs $1 \leq r \leq s$. Recall from §2 that the alternility sum $A_{r,s}$ is a polynomial in $v_1,\dots,v_{r+s}$ obtained by summing up polynomial terms in one-to-one correspondence with the terms of the stuffle of two sequences of lengths r and s. By construction, the coefficient of a monomial $w = v_1^{b_1-1}\cdots v_{r+s}^{b_{r+s}-1}$ in the alternility term corresponding to to a given stuffle term is equal to the coefficient in f_* of the stuffle term itself. This follows from a direct calculation obtained by expanding the alternility terms; for example, the alternility term corresponding to the stuffle term (y_i, y_{j+k}, y_l) in (2.13) is given by

$$\frac{1}{v_2-v_2}\big(A(v_1,v_2,v_4) - A(v_1,v_3,v_4)\big)$$

(see (2.15)), whose polynomial expansion is given by

$$\sum_{\mathbf{a}=(a_1,a_2,a_3)} c_{\mathbf{a}} v_1^{a_1-1}\Big(\sum_{m=0}^{a_2-2} v_2^m v_3^{a_2-2-m}\Big) v_4^{a_3-1},$$

and the coefficient of the monomial $v_1^{i-1}v_2^{j-1}v_3^{k-1}v_4^{l-1}$ in this alternility term corresponds to $a_1-1=i-1$, $m=j-1$, $a_2-2-m=k-1$ and $a_3-1=l-1$, i.e. $a_1=i$, $a_2=j+k$, $a_3=l$, so it is equal to $c_{i,j+k,l}$ which is exactly the coefficient $(f_*|y_iy_{j+k}y_l)$ in (4.7). The alternility sum is equal to zero if and only the coefficient of each monomial in $v_1,\dots,v_{r+s}$ is equal to zero, which is thus equivalent to the full set of stuffle relations on f_*. $\diamondsuit$

In view of (4.5) and (4.6), a mould-theoretic proof of Racinet's theorem consists in proving that $\mathrm{ARI}^{pol}_{\underline{al}*\underline{il}}$ is a Lie algebra under the ari-bracket. To prove this mould-theoretic version, we need to make use of the Lie group GARI associated to ARI, defined in the next section. In §6 we give the necessary results from Ecalle's theory, and the theorem is proved in §7.

§5. The group GARI

In this section we introduce several notions on the group GARI of moulds with constant term 1, which are group analogs of the Lie notions introduced in §2. To move from the Lie algebra ARI to the associated group GARI, Ecalle introduces a pre-Lie law on ARI, defined as follows:

$$\mathrm{preari}(A,B) = \mathrm{arit}(B)\cdot A + \mathrm{mu}(A,B), \tag{5.1}$$

where arit and mu are as defined in (2.9) and (2.6). Indeed, if $A, B \in \mathrm{ARI}$ then $\mathrm{preari}(A,B)$ also lies in ARI, and it is straightforward to check that preari satisfies the defining condition of pre-Lie laws given in §4. Using preari, Écalle defined an exponential map on ARI in the standard way:

$$\exp_{\mathrm{ari}}(A) = \sum_{n\geq 0} \frac{1}{n!}\,\mathrm{preari}(\underbrace{A,\dots,A}_{n}), \tag{5.2}$$

where

$$\mathrm{preari}(\underbrace{A,\dots,A}_{n}) = \mathrm{preari}(\mathrm{preari}(\underbrace{A,\dots,A}_{n-1}),A).$$

This map is the exponential isomorphism $\exp_{\mathrm{ari}} : \mathrm{ARI} \to \mathrm{GARI}$, where GARI is nothing other than the group of all moulds with constant term equal to 1, equipped with the multiplication law, denoted gari, that comes as always from the Campbell-Hausdorff law $\mathrm{ch}(\cdot,\cdot)$ on ARI:

$$\mathrm{gari}\big(\exp_{\mathrm{ari}}(A), \exp_{\mathrm{ari}}(B)\big) = \exp_{\mathrm{ari}}(\mathrm{ch}(A,B)). \tag{5.3}$$

The gari-inverse of a mould $B \in \mathrm{GARI}$ is denoted $\mathrm{inv}_{\mathrm{gari}}(B)$. The inverse isomorphism of $\exp_{\mathrm{ari}}$ is denoted by $\log_{\mathrm{ari}}$.

Like all Lie algebras, ARI is equipped with an action of the associated group GARI, namely the standard adjoint action, denoted $\mathrm{Ad}_{\mathrm{ari}}$ (Ecalle denotes it simply adari, but we have modified it to stress the fact that it represents the adjoint action of the group *GARI* on *ARI*):

$$\begin{aligned}\mathrm{Ad}_{\mathrm{ari}}(A)\cdot B &= \mathrm{gari}\big(\mathrm{preari}(A,B), \mathrm{inv}_{\mathrm{gari}}(A)\big)\\ &= \frac{d}{dt}|_{t=0}\ \mathrm{gari}\big(A, \exp_{\mathrm{ari}}(tB), \mathrm{inv}_{\mathrm{gari}}(A)\big)\\ &= B + \mathrm{ari}\big(\log_{\mathrm{ari}}(A), B\big) + \frac{1}{2}\mathrm{ari}\big(\log_{\mathrm{ari}}(A), \mathrm{ari}\big(\log_{\mathrm{ari}}(A), B\big) + \cdots\end{aligned} \tag{5.4}$$

Finally, to any mould $A \in \mathrm{GARI}$ (i.e. any mould in the u_i with constant term 1), Ecalle associates an automorphism $\mathrm{ganit}(A)$ of the ring of all moulds in the u_i under the mu-multiplication which is just the exponential of the derivation $\mathrm{anit}\big(\log_{\mathrm{ari}}(A)\big)$.

The analogous objects exist for moulds in the v_i. If preari denotes the pre-Lie law on $\overline{\mathrm{ARI}}$ given by (5.1) (but for the derivation arit of ARI), then the formula (5.2) defines an analogous exponential isomorphism $\overline{\mathrm{ARI}} \to \overline{\mathrm{GARI}}$, where $\overline{\mathrm{GARI}}$ consists of all moulds in

the variables v_i with constant term 1 and multiplication determined by (5.3) (note that this definition depends on that of arit, so just as the Lie bracket ari is different for ARI and $\overline{\mathrm{ARI}}$, the multiplication is different for GARI and $\overline{\mathrm{GARI}}$). As above, we let the automorphism $\mathrm{ganit}(A)$ of $\overline{\mathrm{GARI}}$ associated to each $A \in \overline{\mathrm{GARI}}$ be defined as the exponential of the derivation $\mathrm{anit}\big(\log_{\mathrm{ari}}(A)\big)$ of $\overline{\mathrm{ARI}}$.

Definition. A mould $A \in \mathrm{GARI}$ (resp. $\overline{\mathrm{GARI}}$) is *symmetral* if for all words $\mathbf{u}, \mathbf{v}$ in the u_i (resp. in the v_i), we have

$$\sum_{\mathbf{w} \in \mathrm{sh}(\mathbf{u},\mathbf{v})} A(\mathbf{w}) = A(\mathbf{u})A(\mathbf{v}). \tag{5.7}$$

Following Ecalle, we write GARI_{as} (resp. $\overline{\mathrm{GARI}}_{as}$) for the set of symmetral moulds in GARI (resp. $\overline{\mathrm{GARI}}$). The property of *symmetrality* is the group equivalent of alternality; in particular,

$$A \in \mathrm{ARI}_{al} \text{ (resp. } \overline{\mathrm{ARI}}_{al}) \;\Leftrightarrow\; \exp_{\mathrm{ari}}(A) \in \mathrm{GARI}_{as} \text{ (resp. } \overline{\mathrm{GARI}}_{as}). \tag{5.8}$$

Remark. Let MT denote the *twisted Magnus group* of power series in $\mathbb{Q}\langle\langle C_1, C_2, \ldots\rangle\rangle$ with constant term 1, identified with the exponential of the twisted Magnus Lie algebra $\mathfrak{mt}$ defined by

$$\exp^{\odot}(f) = \sum_{n \geq 0} \frac{1}{n!} f^{\odot n}$$

for $f \in \mathfrak{mt}$, where $\odot$ is the pre-Lie law

$$f \odot g = fg + D_f(g) \tag{5.9}$$

defined for $f, g \in \mathfrak{mt}$ (see §4). The group MT is equipped with the twisted Magnus multiplication

$$\big(f \odot g\big)(x, y) = f(x, gyg^{-1})g(x, y). \tag{5.10}$$

Notice that it makes sense to use the same symbol $\odot$ for (5.9) and (5.10), because in fact $\odot$ is the multiplication on the completion of the universal enveloping algebra of $\mathfrak{mt}$, and (5.9) and (5.10) merely represent the particular expressions that it takes on two elements of $\mathfrak{mt}$ resp. two elements of MT.

The multiplication (5.10) corresponds to the gari-multiplication in the sense that the map ma defined in (4.1) yields a group isomorphism $MT \xrightarrow{\sim} \mathrm{GARI}^{pol}$. If $g \in MT$, then the automorphism $\mathrm{ganit}\big(ma(g)\big)$ is the GARI-version of the automorphism of MT given by mapping $x \mapsto x$ and $y \mapsto yg$.

The fact of having non-polynomial moulds in GARI gives enormously useful possibilities of expanding the familiar symmetries and operations (derivations, shuffle and stuffle relations etc.) to a broader situation. In particular, the next section contains some of Ecalle's most important results in mould multizeta theory, which make use of moulds with denominators and have no analog within the usual polynomial framework.

§6. The mould pair *pal*/*pil* and Ecalle's fundamental identity

In this section we enter into the "second drawer" of Ecalle's powerful toolbox, with the mould pair *pal*/*pil* and Ecalle's fundamental identity.

Definition. Let *dupal* be the mould defined explicitly by the following formulas: $dupal(\emptyset) = 0$ and for $r \geq 1$,

$$dupal(u_1, \ldots, u_r) = \frac{B_r}{r!} \frac{1}{u_1 \cdots u_r} \left(\sum_{i=0}^{r-1} (-1)^i \binom{r-1}{i} u_{i+1} \right), \tag{6.1}$$

where B_r denotes the r-th Bernoulli number. This mould is actually quite similar to a power series often studied in classical situations. Indeed, if we define dar to be the mould operator defined by

$$\mathrm{dar} \cdot A(u_1, \ldots, u_r) = u_1 \cdots u_r \; A(u_1, \ldots, u_r),$$

then $\mathrm{dar} \cdot dupal$ is a polynomial-valued mould, so it is the image of a power series under *ma*; explicitly

$$\mathrm{dar} \cdot dupal = ma\Big(x - \frac{\mathrm{ad}(-y)}{\exp(\mathrm{ad}(-y)) - 1}(x)\Big).$$

Ecalle gave several equivalent definitions of the key mould *pal*, but the most recent one (see [E2]) appears to be the simplest and most convenient. If we define dur to be the mould operator defined by

$$\mathrm{dur} \cdot A(u_1, \ldots, u_r) = (u_1 + \cdots + u_r)\, A(u_1, \ldots, u_r),$$

then the mould *pal* is defined recursively by

$$\mathrm{dur} \cdot pal = \mathrm{mu}(pal, dupal). \tag{6.2}$$

Calculating the first few terms of *pal* explicitly, we find that

$$\begin{cases} pal(\emptyset) = 1 \\ pal(u_1) = \frac{1}{2u_1} \\ pal(u_1, u_2) = \frac{u_1 + 2u_2}{12 u_1 u_2 (u_1 + v_2)} \\ pal(u_1, u_2, u_3) = \frac{-1}{24 u_1 u_3 (u_1 + u_2)}. \end{cases}$$

Let $pil = \mathrm{swap}(pal)$. The most important result concerning *pal*, necessary for the proof of Ecalle's fundamental identity below, is the following.

Theorem 6.1. *The moulds pal and pil are symmetral.*

In [E1,§4.2], the mould *pil* (called $\mathfrak{ess}$) is given an independent definition which makes it easy to prove that it is symmetral. Similarly, it is not too hard to prove that *pal* is

symmetral using the definition (6.2). The real difficulty is to prove that *pil* (as defined in [E1]) is the swap of *pal* (as defined in (6.2)). Ecalle sketched beautiful proofs of these two facts in [E2], and the details are fully written out in [S,§§4.2,4.3].

Before proceeding to the fundamental identity, we need a useful result in which a very simple v-mould is used to give what amounts to an equivalent definition of alternility.*

Proposition 6.2. *Let pic be the v-mould defined by* $\mathrm{pic}(v_1,\dots,v_r) = 1/v_1\cdots v_r$. *Then for any alternal mould $A \in \overline{\mathrm{ARI}}$, the mould* $\mathrm{ganit}(pic)\cdot A$ *is alternil.*

Proof. The proof is deferred to Appendix C. ♢

We now come to Ecalle's fundamental identity.

Ecalle's fundamental identity: For any push-invariant mould A, we have

$$\mathrm{swap}\big(\mathrm{Ad}_{\mathrm{ari}}(pal)\cdot A\big) = \mathrm{ganit}(pic)\cdot\big(\mathrm{Ad}_{\mathrm{ari}}(pil)\cdot\mathrm{swap}(A)\big). \tag{6.3}$$

The proof of this fundamental identity actually follows as a consequence of (3.2) and a more general fundamental identity, similar but taking place in the group GARI and valid for all moulds. It is given in full detail in [S, Thm. 4.5.2].

§7. The main theorem

In this section we give Ecalle's main theorem on dimorphy, which shows how the mould *pal* transforms moulds with the double symmetry $\underline{al} * \underline{al}$ to moulds that are $\underline{al} * \underline{il}$. We then show how Racinet's theorem follows directly from this. We first need a useful lemma.

Lemma 7.1. *If C is a constant-valued mould, then*

$$\mathrm{ganit}(pic)\cdot\mathrm{Ad}_{\mathrm{ari}}(pil)\cdot C = C. \tag{7.1}$$

Proof. [B, Corollary 4.43] We apply the fundamental identity (6.3) in the case where $A = \mathrm{swap}(A) = C$ is a constant-valued mould, obtaining

$$\mathrm{swap}\big(\mathrm{Ad}_{\mathrm{ari}}(pal)\cdot C\big) = \mathrm{ganit}(pic)\cdot\mathrm{Ad}_{\mathrm{ari}}(pil)\cdot C.$$

So it is enough to show that the left-hand side of this is equal to C, i.e. that $\mathrm{Ad}_{\mathrm{ari}}(pal)\cdot C = C$, since a constant mould is equal to its own swap. As we saw just before (3.3), the definitions (2.6)-(2.9) imply that $\mathrm{ari}(A,C) = 0$ for all $A \in \mathrm{ARI}$. Now, by (5.4) we see that $\mathrm{Ad}_{\mathrm{ari}}(pal)\cdot C$ is a linear combination of iterated ari-brackets of $\log_{\mathrm{ari}}(pal)$ with C, but since $pal \in \mathrm{GARI}$, $\log_{\mathrm{ari}}(pal) \in \mathrm{ARI}$, so $\mathrm{ari}(\log_{\mathrm{ari}}(pal), C) = 0$, i.e. all the bracketed terms in (5.4) are 0. Thus $\mathrm{Ad}_{\mathrm{ari}}(pal)\cdot C = C$. This concludes the proof. ♢

* This is just one example of a general identity valid for *flexion units*, see [E1, p. 64] where Ecalle explains the notion of alternality twisted by a flexion unit and asserts that alternility is merely alternality twisted by the flexion unit $1/v_1$.

We can now state the main theorem on moulds.

Theorem 7.2. *The action of the operator* $\mathrm{Ad}_{\mathrm{ari}}(pal)$ *on the Lie subalgebra* $\mathrm{ARI}_{\underline{al}*\underline{al}} \subset \mathrm{ARI}$ *yields a Lie isomorphism of subspaces*

$$\mathrm{Ad}_{\mathrm{ari}}(pal) : \mathrm{ARI}_{\underline{al}*\underline{al}} \xrightarrow{\sim} \mathrm{ARI}_{\underline{al}*\underline{il}}. \tag{7.2}$$

Thus in particular $\mathrm{ARI}_{\underline{al}*\underline{il}}$ *forms a Lie algebra under the* ari-*bracket.*

Proof. The proof we give appears not to have been published anywhere by Ecalle, but we learned its outline from him through a personal communication to the second author, for which we are grateful.

Note first that $\mathrm{Ad}_{\mathrm{ari}}(pal)$ preserves the depth 1 component of moulds in ARI, so if A is even in depth 1 then so is $\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A$. We first consider the case where $A \in \mathrm{ARI}_{\underline{al}/\underline{al}}$, i.e. $swap(A)$ is alternal without addition of a constant correction. By (5.8), the mould $\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A$ is alternal, since pal is symmetral by Theorem 6.1. By Proposition 3.4, A is push-invariant, so Ecalle's fundamental identity (6.3) holds. Since $A \in \mathrm{ARI}_{\underline{al}/\underline{al}}$, $\mathrm{swap}(A)$ is alternal, and by Theorem 6.1, pil is alternal; thus by (5.8), $\mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \mathrm{swap}(A)$ is alternal. Then by Proposition 6.2, $\mathrm{ganit}(pic) \cdot \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \mathrm{swap}(A)$ is alternil, and finally by (6.3), $\mathrm{swap}\big(\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A\big)$ is alternil, which proves that $\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A \in \mathrm{ARI}_{\underline{al}/\underline{il}}$ as desired.

We now consider the general case where $A \in \mathrm{ARI}_{\underline{al}*\underline{al}}$. Let C be the constant-valued mould such that $\mathrm{swap}(A) + C$ is alternal. As above, we have that $\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A$ is alternal, so to conclude the proof of the theorem it remains only to show that its swap is alternil up to addition of a constant mould, and we will show that this constant mould is exactly C. As before, since $\mathrm{swap}(A) + C \in \overline{\mathrm{ARI}}$ is alternal, the mould

$$\mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \big(\mathrm{swap}(A) + C\big) = \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \mathrm{swap}(A) + \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot C$$

is also alternal. Thus by Proposition 6.2, applying $\mathrm{ganit}(pic)$ to it yields the alternil mould

$$\mathrm{ganit}(pic) \cdot \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \mathrm{swap}(A) + \mathrm{ganit}(pic) \cdot \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot C.$$

By Lemma 7.1, this is equal to

$$\mathrm{ganit}(pic) \cdot \mathrm{Ad}_{\mathrm{ari}}(pil) \cdot \mathrm{swap}(A) + C, \tag{7.3}$$

which is thus alternil. Now, since A is push-invariant by Proposition 3.4, we can apply (6.3) and find that (7.3) is equal to

$$\mathrm{swap}\big(\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A\big) + C,$$

which is thus also alternil. Therefore $\mathrm{swap}\big(\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A\big)$ is alternil up to a constant, which precisely means that $\mathrm{Ad}_{\mathrm{ari}}(pal) \cdot A \in \mathrm{ARI}_{\underline{al}*\underline{il}}$ as claimed. Since $\mathrm{Ad}_{\mathrm{ari}}(pal)$ is invertible (with inverse $\mathrm{Ad}_{\mathrm{ari}}\big(\mathrm{inv}_{\mathrm{gari}}(pal)\big)$) and by the analogous arguments this inverse takes $\mathrm{ARI}_{\underline{al}*\underline{il}}$ to $\mathrm{ARI}_{\underline{al}*\underline{al}}$, this proves that (7.2) is an isomorphism. ♢

Corollary 7.3. $\mathrm{ARI}^{pol}_{\underline{al}*\underline{il}}$ *forms a Lie algebra under the* ari-*bracket.*

Proof. By Proposition 3.2, ARI^{pol} is a Lie algebra under the ari-bracket, so since $\mathrm{ARI}_{\underline{al}*\underline{il}}$ is as well by Theorem 7.2, their intersection also forms a Lie algebra. ♢

In view of (4.5) and (4.6), this corollary is equivalent to Racinet's theorem that $\mathfrak{ds}$ is a Lie algebra under the Poisson bracket.

Appendix A.

Proof of Theorem 3.1. We cut it into two separate results as explained in the main text.

Proposition A.1. *If A, B are alternal moulds then $C = \mathrm{lu}(A, B)$ is alternal.*

Proof. We have

$$C(\mathbf{w}) = \mathrm{lu}(A, B)(\mathbf{w}) = \sum_{\mathbf{w}=\mathbf{ab}} \big(A(\mathbf{a})B(\mathbf{b}) - B(\mathbf{a})A(\mathbf{b})\big),$$

so we need to show that the following sum vanishes:

$$\begin{aligned} \sum_{\mathbf{w}\in\mathrm{sh}(\mathbf{u},\mathbf{v})} C(\mathbf{w}) &= \sum_{\mathbf{w}\in\mathrm{sh}(\mathbf{u},\mathbf{v})} \mathrm{lu}(A, B)(\mathbf{w}) \\ &= \sum_{\mathbf{w}\in\mathrm{sh}(\mathbf{u},\mathbf{v})} \sum_{\mathbf{w}=\mathbf{ab}} \big(A(\mathbf{a})B(\mathbf{b}) - B(\mathbf{a})A(\mathbf{b})\big). \end{aligned} \tag{A.0}$$

This sum breaks into three pieces: the terms where $\mathbf{a}$ contain letters from both $\mathbf{u}$ and $\mathbf{v}$, the case where $\mathbf{a}$ contains only letters from $\mathbf{u}$ or from $\mathbf{v}$ but $\mathbf{b}$ contains letters from both, and finally the cases $\mathbf{a} = \mathbf{u}$, $\mathbf{b} = \mathbf{v}$ and $\mathbf{a} = \mathbf{v}, \mathbf{b} = \mathbf{u}$.

The first type of terms add up to zero because we can break up the sum into smaller sums where $\mathbf{a}$ lies in the shuffle of the first i letters of $\mathbf{u}$ and j letters of $\mathbf{b}$, and these terms already sum to zero since A and B are alternal.

The second type of term adds up to zero for the same reason, because even though $\mathbf{a}$ may contain only letters from one of $\mathbf{u}$ and $\mathbf{v}$, $\mathbf{b}$ must contain letters from both and therefore the same reasoning holds.

The third type of term yields $A(\mathbf{u})B(\mathbf{v}) - B(\mathbf{u})A(\mathbf{v})$ when $\mathbf{a} = \mathbf{u}$,$\mathbf{b} = \mathbf{v}$ and $A(\mathbf{v})B(\mathbf{u}) - B(\mathbf{v})A(\mathbf{u})$ when $\mathbf{a} = \mathbf{v}$, $\mathbf{b} = \mathbf{u}$, which cancel out. Thus the sum $(A.0)$ adds up to zero. $\diamondsuit$

Proposition A.2. *If A and B are alternal moulds in* ARI*, then $C = \mathrm{arit}(B) \cdot A$ is alternal.*

Proof. By definition, C is alternal if

$$\sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} C(\mathbf{w}) = 0,$$

for all pairs of non-trivial words $\mathbf{x}, \mathbf{y}$.

Pick an arbitrary pair of non-trivial words $\mathbf{x}, \mathbf{y}$, of appropriate length (that is, so that their lengths add up to the length of A plus the length of B). We will be shuffling $\mathbf{x}$ and $\mathbf{y}$ together, and the resulting word is then broken up into three parts (all possible ones) in order to compute the flexions. Thus, if we break up $\mathbf{w} = \mathbf{abc}$, $\mathbf{a}$ must be a shuffle of some parts at the beginning of each word $\mathbf{x}, \mathbf{y}$, $\mathbf{b}$ must come from shuffling their middles, and $\mathbf{c}$ can only come from shuffling the last parts. Then we can rewrite this computation as follows:

$$\sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} \mathrm{arit}(B)\cdot A(\mathbf{w}) = \sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} \left(\sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{c}\neq\emptyset}} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b}) - \sum_{\substack{\mathbf{w}=\mathbf{abc}\\ \mathbf{a}\neq\emptyset}} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}) \right)$$

$$= \sum_{\substack{\mathbf{x}=\mathbf{x_1x_2x_3}\\ \mathbf{y}=\mathbf{y_1y_2y_3},\mathbf{x_3y_3}\neq\emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2}),\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b})$$

$$- \sum_{\substack{\mathbf{x}=\mathbf{x_1x_2x_3}\\ \mathbf{y}=\mathbf{y_1y_2y_3},\mathbf{x_1y_1}\neq\emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2}),\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}).$$

Now for a fixed splitting of each $\mathbf{x}$ and $\mathbf{y}$ into three parts, we have the following possibilities.

Case I. Both $\mathbf{x_2} = \mathbf{y_2} = \emptyset$. Then $B(\emptyset) = 0$ so we are done.

Case II. Both $\mathbf{x_2}$ and $\mathbf{y_2}$ are nonempty. The trick here is that because of the flexion operations, no matter how $\mathbf{b} = \mathrm{sh}(\mathbf{x_2}, \mathbf{y_2})$ is shuffled, the part being added together with the last letter in $\mathbf{a}$ and the first letter in $\mathbf{c}$ remains the same. Thus, if we further fix a particular $\mathbf{a}$ and $\mathbf{c}$, we get that

$$\sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b}) = A(\mathbf{a}\lceil\mathbf{c}) \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} B(\mathbf{b}) = 0$$

and

$$\sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}) = A(\mathbf{a}\rceil\mathbf{c}) \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} B(\mathbf{b}) = 0,$$

by alternality of B. And thus,

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b}) = 0$$

and

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}) = 0.$$

Case III. Either $\mathbf{x_2} = \emptyset$ or $\mathbf{y_2} = \emptyset$, but not both. Without loss of generality, assume $\mathbf{x_2} = \emptyset$. Then we have:

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{b}=\mathbf{y_2},\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\lceil\mathbf{c})B(\mathbf{b}) = B(\mathbf{y_2}) \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\lceil\mathbf{c})$$

And similarly

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{b}=\mathbf{y_2},\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\rceil\mathbf{c})B(\mathbf{b}) = B(\mathbf{y_2}) \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{a}\rceil\mathbf{c})$$

Recall that by definition

$$\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}) = \mathrm{sh}(\mathbf{x_1'},\mathbf{y_1})(\text{last letter in } \mathbf{x_1}) + \mathrm{sh}(\mathbf{x_1},\mathbf{y_1'})(\text{last letter in } \mathbf{y_1})$$

and

$$\mathrm{sh}(\mathbf{x_3},\mathbf{y_3}) = (\text{first letter in } \mathbf{x_3})\mathrm{sh}(\mathbf{x_3'},\mathbf{y_3}) + (\text{first letter in } \mathbf{y_3})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3'}).$$

Thus,

$$\mathbf{a}\lceil\mathbf{c} = \mathrm{sh}(\mathbf{x_1},\mathbf{y_1})(\text{sum of letters in } \mathbf{y_2} \text{ plus first letter in } \mathbf{x_3})\mathrm{sh}(\mathbf{x_3'},\mathbf{y_3}) \tag{A.1}$$

or

$$\mathbf{a}\lceil\mathbf{c} = \mathrm{sh}(\mathbf{x_1},\mathbf{y_1})(\text{sum of letters in } \mathbf{y_2} \text{ plus first letter in } \mathbf{y_3})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3'}) \tag{A.2}$$

and

$$\mathbf{a}\rceil\mathbf{c} = \mathrm{sh}(\mathbf{x_1'},\mathbf{y_1})(\text{sum of letters in } \mathbf{y_2} \text{ plus last letter in } \mathbf{x_1})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3}) \tag{A.3}$$

or

$$\mathbf{a}\rceil\mathbf{c} = \mathrm{sh}(\mathbf{x_1},\mathbf{y_1'})(\text{sum of letters in } \mathbf{y_2} \text{ plus last letter in } \mathbf{y_1})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3}). \tag{A.4}$$

Recall that, since $\mathbf{x_2}$ is assumed to be empty, then for a given $\mathbf{x_1},\mathbf{x_3}$, we can let $\overline{\mathbf{x_1}},\overline{\mathbf{x_3}}$ be so that $\overline{\mathbf{x_1}}$ is $\mathbf{x_1}$ with an additional letter given by the first letter of $\mathbf{x_3}$ and $\overline{\mathbf{x_3}}$ is defined in the logical way. That means that equations $(A.1)$ and $(A.3)$ are exactly the same. Thus, we get direct cancellation for all possible choices of $\mathbf{x_1},\mathbf{x_3}$ (this is compatible with the restrictions on nonemptiness given by the definition).

We cannot do the same for $(A.2)$ and $(A.4)$, since $\mathbf{y_2}$ is assumed to be nonempty. For these, notice that if we keep $\mathbf{y}$ fixed and sum over all possible partitions of $\mathbf{x} = \mathbf{x_1}\mathbf{x_2}\mathbf{x_3}$ where $\mathbf{x_2} = \emptyset$, and $\mathbf{x_3} \neq \emptyset$ we get that each

$$\mathbf{a}\lceil\mathbf{c} = \mathrm{sh}(\mathbf{x_1},\mathbf{y_1})(\text{sum of letters in } \mathbf{y_2} \text{ plus first letter in } \mathbf{y_3})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3'})$$

could be seen as a term in the shuffle $\mathrm{sh}(\mathbf{x},\mathbf{y_1}\lceil\mathbf{y_3})$. To see this, suppose that

$$\mathbf{x} = u_1\cdots u_k|u_{k+1}\cdots u_l = \mathbf{x_1}|\mathbf{x_3}$$

and that

$$\mathbf{y} = u_{l+1}\cdots u_{l+i}|u_{l+i+1}\cdots u_{l+j}|u_{l+j+1}\cdots u_n = \mathbf{y_1}|\mathbf{y_2}|\mathbf{y_3}.$$

Then

$$\mathbf{a}\lceil\mathbf{c} = \mathrm{sh}((u_1\cdots u_k),(u_{l+1}\cdots u_{l+i}))(u_{l+i+1}+\cdots+u_{l+j}+u_{l+j+1})\mathrm{sh}((u_{k+1}\cdots u_l),(u_{l+j+2}\cdots u_n)).$$

And so if we allow the k to shift from 1 to l, this is essentially the shuffling of the words $u_1 \cdots u_l = \mathbf{x}$ and $u_{l+1} \cdots u_{l+i}(u_{l+i+1} + \cdots + u_{l+j} + u_{l+j+1})u_{l+j+2} \cdots u_n = \mathbf{y_1} \lceil \mathbf{y_3}$. Thus we have

$$\sum_{\substack{\mathbf{x}=\mathbf{x_1}\mathbf{x_3} \\ \mathbf{x_3}\neq\emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}) \\ \mathbf{b}=\mathbf{y_2},\mathbf{c}=y_{first}\mathrm{sh}(\mathbf{x_3},\mathbf{y'_3})}} A(\mathbf{a}\lceil\mathbf{c}) = \sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y_1}\lceil\mathbf{y_3})} A(\mathbf{w}) = 0$$

by alternality of A.

A similar argument holds for the terms corresponding to the other flexion (the terms corresponding to equation $(A.4)$).

Putting all of these cases together, we see that indeed, C is alternal. $\diamondsuit$

Proposition A.3. *If A and B are alternal moulds in $\overline{\mathrm{ARI}}$, then $C = \mathrm{arit}(B) \cdot A$ is alternal.*

Proof. As with the proof for ARI_{al}, we have to show that

$$\sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} C(\mathbf{w}) = 0,$$

for all pairs of non-trivial words $\mathbf{x}, \mathbf{y}$. Again, this can be rewritten as follows:

$$\begin{aligned}
\sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} \mathrm{arit}(B) \cdot A(\mathbf{w}) &= \sum_{\mathbf{w}=\mathrm{sh}(\mathbf{x},\mathbf{y})} \left(\sum_{\substack{\mathbf{w}=\mathbf{abc} \\ \mathbf{c}\neq\emptyset}} A(\mathbf{ac})B(\mathbf{b}\rfloor) - \sum_{\substack{\mathbf{w}=\mathbf{abc} \\ \mathbf{a}\neq\emptyset}} A(\mathbf{ac})B(\lfloor\mathbf{b}) \right) \\
&= \sum_{\substack{\mathbf{x}=\mathbf{x_1}\mathbf{x_2}\mathbf{x_3} \\ \mathbf{y}=\mathbf{y_1}\mathbf{y_2}\mathbf{y_3},\mathbf{x_3}\mathbf{y_3}\neq\emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}) \\ \mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2}),\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{ac})B(\mathbf{b}\rfloor) \\
&- \sum_{\substack{\mathbf{x}=\mathbf{x_1}\mathbf{x_2}\mathbf{x_3} \\ \mathbf{y}=\mathbf{y_1}\mathbf{y_2}\mathbf{y_3},\mathbf{x_1}\mathbf{y_1}\neq\emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}) \\ \mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2}),\mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} A(\mathbf{ac})B(\lfloor\mathbf{b})
\end{aligned}$$

Again, for a fixed splitting of each $\mathbf{x}$ and $\mathbf{y}$ into three parts, we have the following possibilities.

Case I. Both $\mathbf{x_2} = \mathbf{y_2} = \emptyset$. Then $B(\emptyset) = 0$ so we are done.

Case II. Both $\mathbf{x_2}$ and $\mathbf{y_2}$ are nonempty.

Here, no matter how $\mathbf{b} = \mathrm{sh}(\mathbf{x_2}, \mathbf{y_2})$ is shuffled, the part being subtracted from $\mathbf{b}$, which is either the last letter in $\mathbf{a}$ or the first letter in $\mathbf{c}$, remains the same if we fix a particular $\mathbf{a}$ and $\mathbf{c}$. Thus, we get that

$$\mathbf{b}\rfloor_i = \mathrm{sh}(\mathbf{x_2}, \mathbf{y_2})_i - \text{first letter in } \mathbf{c} = \mathrm{sh}((\mathbf{x_{2_k}} - \text{first letter in } \mathbf{c}), (\mathbf{y_{2_k}} - \text{first letter in } \mathbf{c}))_i$$

and

$$\lfloor\mathbf{b}_i = \mathrm{sh}(\mathbf{x_2}, \mathbf{y_2})_i - \text{last letter in } \mathbf{a} = \mathrm{sh}((\mathbf{x_{2_k}} - \text{last letter in } \mathbf{a}), (\mathbf{y_{2_k}} - \text{last letter in } \mathbf{a}))_i.$$

Thus,

$$\sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{ac})B(\mathbf{b}\rfloor) = A(\mathbf{ac}) \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} B(\mathbf{b}\rfloor) = 0$$

and

$$\sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{ac})B(\lfloor\mathbf{b}) = A(\mathbf{ac}) \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} B(\lfloor\mathbf{b}) = 0,$$

by alternality of B. And thus,

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{ac})B(\mathbf{b}\rfloor) = 0$$

and

$$\sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})\\ \mathbf{c}=\mathrm{sh}(\mathbf{x_3},\mathbf{y_3})}} \sum_{\mathbf{b}=\mathrm{sh}(\mathbf{x_2},\mathbf{y_2})} A(\mathbf{ac})B(\lfloor\mathbf{b}) = 0.$$

Case III. Either $\mathbf{x_2} = \emptyset$ or $\mathbf{y_2} = \emptyset$, but not both. Without loss of generality, assume $\mathbf{x_2} = \emptyset$.

Recall, again, that by definition

$$\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}) = \mathrm{sh}(\mathbf{x_1'},\mathbf{y_1})(\text{last letter in } \mathbf{x_1}) + \mathrm{sh}(\mathbf{x_1},\mathbf{y_1'})(\text{last letter in } \mathbf{y_1})$$

and

$$\mathrm{sh}(\mathbf{x_3},\mathbf{y_3}) = (\text{first letter in } \mathbf{x_3})\mathrm{sh}(\mathbf{x_3'},\mathbf{y_3}) + (\text{first letter in } \mathbf{y_3})\mathrm{sh}(\mathbf{x_3},\mathbf{y_3'}).$$

Since $\mathbf{x_2} = \emptyset$, we can see that

$$\mathbf{b}\rfloor_i = \mathbf{y_{2_i}} - \text{first letter in } \mathbf{c}$$

and

$$\lfloor\mathbf{b}_i = \mathbf{y_{2_i}} - \text{last letter in } \mathbf{a}.$$

For a given $\mathbf{x_1}, \mathbf{x_3}$, we can let $\overline{\mathbf{x_1}}, \overline{\mathbf{x_3}}$ be so that $\overline{\mathbf{x_1}}$ is $\mathbf{x_1}$ with an additional letter given by the first letter of $\mathbf{x_3}$ and $\overline{\mathbf{x_3}}$ is defined in the logical way. That means that

$$A(\mathrm{sh}(\overline{\mathbf{x_1}}',\mathbf{y_1})(\text{last letter in } \overline{\mathbf{x_1}})\mathrm{sh}(\overline{\mathbf{x_3}},\mathbf{y_3}))B(\lfloor\mathbf{b})$$

and

$$A(\mathrm{sh}(\mathbf{x_1},\mathbf{y_1})(\text{first letter in } \mathbf{x_3})\mathrm{sh}(\mathbf{x_3'},\mathbf{y_3}))B(\mathbf{b}\rfloor)$$

are identical (for each fixed shuffling).

Thus, we get direct cancellation for all possible choices of $\mathbf{x_1}, \mathbf{x_3}$ (this is compatible with the restrictions on nonemptiness given by the definition).

The only terms that have not cancelled out are the ones coming from the second term in the shuffle equations above. Now, suppose that

$$\mathbf{x} = v_1 \cdots v_k | v_{k+1} \cdots v_l = \mathbf{x_1}|\mathbf{x_3}$$

and that

$$\mathbf{y} = v_{l+1} \cdots v_{l+i} | v_{l+i+1} \cdots v_{l+j} | v_{l+j+1} \cdots v_n = \mathbf{y_1} | \mathbf{y_2} | \mathbf{y_3},$$

and fix this splitting of $\mathbf{y}$. Then

$$\mathbf{ac} = \mathrm{sh}(v_1 \cdots v_k, v_{l+1} \cdots v_{l+i}) v_{l+j+1} \mathrm{sh}(v_{k+1} \cdots v_l, v_{l+j+2} \cdots v_n).$$

And so if we allow the k to shift from 1 to l, this is essentially the shuffling of the words $v_1 \cdots v_l = \mathbf{x}$ and $v_{l+1} \cdots v_{l+i}, v_{l+j+1}, v_{l+j+2} \cdots v_n = \mathbf{y_1 y_3}$. Notice that this shuffling fixes $\mathbf{b}\rfloor$, since

$$\mathbf{b}\rfloor = (v_{l+i+1} - v_{l+j+1}, \ldots, v_{l+j} - v_{l+j+1}).$$

Thus we have

$$\sum_{\substack{\mathbf{x}=\mathbf{x_1}\mathbf{x_3} \\ \mathbf{x_3} \neq \emptyset}} \sum_{\substack{\mathbf{a}=\mathrm{sh}(\mathbf{x_1},\mathbf{y_1}), \mathbf{b}=\mathbf{y_2} \\ \mathbf{c}=y_{first}\mathrm{sh}(\mathbf{x_3},\mathbf{y'_3})}} A(\mathbf{ac}) B(\mathbf{b}\rfloor) = B(\mathbf{b}\rfloor) \sum_{w=\mathrm{sh}(\mathbf{x},\mathbf{y_1 y_3})} A(w) = 0$$

by alternality of A.

A similar argument holds for the terms corresponding to the other flexion. Combining all the cases, we see that indeed, C is alternal. $\diamondsuit$

Appendix B.

Proof of Proposition 3.4. By additivity, we may assume that A is concentrated in a fixed depth d, meaning that $A(u_1, \dots, u_r) = 0$ for all $r \neq d$. We use the following two lemmas.

Lemma B.1. *If $A \in \mathrm{ARI}_{al}$, then*

$$A(u_1, \dots, u_r) = (-1)^{r-1} A(u_r, \dots, u_1);$$

in other words, A is mantar*-invariant. Similarly, if $A \in \overline{\mathrm{ARI}}_{al}$ then again A is* mantar*-invariant*

Proof. We give the argument for ARI; the result in $\overline{\mathrm{ARI}}$ comes from the identical computation with u_i replaced by v_i. We first show that the sum of shuffle relations

$$\begin{aligned}\mathrm{sh}\big((1),(2,\dots,r)\big) - \mathrm{sh}\big((2,1),(3,\dots,r)\big) + \mathrm{sh}\big((3,2,1),(4,\dots,r)\big) + \cdots \\ +(-1)^{r-2}\mathrm{sh}\big((r-1,\dots,2,1),(r)\big) = (1,\dots,r) + (-1)^r(r,\dots,1).\end{aligned}$$

Indeed, using the recursive formula for shuffle, we can write the above sum with two terms for each shuffle, as

$$\begin{aligned}(1,\dots,r) &+ 2\cdot\mathrm{sh}\big((1),(3,\dots,r)\big) \\ &- 2\cdot\mathrm{sh}\big((1),(3,\dots,r)\big) - 3\cdot\mathrm{sh}\big((2,1),(4,\dots,r)\big) \\ &+ 3\cdot\mathrm{sh}\big((2,1),(4,\dots,r)\big) + 4\cdot\mathrm{sh}\big((3,2,1),(5,\dots,r)\big) \\ &+ \cdots + (-1)^{r-3}(r-1)\cdot\mathrm{sh}\big((r-2,\dots,1),(r)\big) \\ &+ (-1)^{r-2}(r-1)\cdot\mathrm{sh}\big((r-2,\dots,1),(r)\big) + (-1)^{r-2}(r,r-1,\dots,1) \\ &= (1,\dots,r) + (-1)^r(r,\dots,1).\end{aligned}$$

Using this, we conclude that if A satisfies the shuffle relations, then

$$A(u_1,\dots,u_r) + (-1)^r A(u_r,\dots,u_1) = 0,$$

which is the desired result. ♢

Lemma B.2. *If $A \in \mathrm{ARI}_{\underline{al}*\underline{al}}$, then A is* neg $\circ$ push*-invariant.*

Proof. We first consider the case where $A \in \mathrm{ARI}_{\underline{al}/\underline{al}}$. Using the easily verified identity

$$\mathrm{neg} \circ \mathrm{push} = \mathrm{mantar} \circ \mathrm{swap} \circ \mathrm{mantar} \circ \mathrm{swap}, \tag{B.1}$$

and the fact that by Lemma B.1, if $A \in \mathrm{ARI}_{\underline{al}/\underline{al}}$, then both A and $\mathrm{swap}(A)$ are mantar-invariant, we have

$$\begin{aligned}\mathrm{neg} \circ \mathrm{push}(A)(u_1,\dots,u_r) &= \mathrm{mantar} \circ \mathrm{swap} \circ \mathrm{mantar} \circ \mathrm{swap}(A)(u_1,\dots,u_r) \\ &= \mathrm{mantar} \circ \mathrm{swap} \circ \mathrm{swap}(A)(u_1,\dots,u_r) \\ &= \mathrm{mantar}(A)(u_1,\dots,u_r) \\ &= A(u_1,\dots,u_r),\end{aligned} \tag{B.2}$$

so A is neg $\circ$ push-invariant.

Now suppose that $A \in \mathrm{ARI}_{\underline{al}*\underline{al}}$, so A is alternal and $\mathrm{swap}(A) + A_0$ is alternal for some constant mould A_0. By additivity, we may assume that A is concentrated in depth r. First suppose that r is odd. Then $\mathrm{mantar}(A_0)(v_1, \ldots, v_r) = (-1)^{r-1} A_0(v_r, \ldots, v_1)$, so since A_0 is a constant mould, it is mantar-invariant. But $\mathrm{swap}(A) + A_0$ is alternal, so it is also mantar-invariant by Lemma B.1; thus $\mathrm{swap}(A)$ is mantar-invariant, and the identity $\mathrm{neg} \circ \mathrm{push} = \mathrm{mantar} \circ \mathrm{swap} \circ \mathrm{mantar} \circ \mathrm{swap}$ shows that A is neg $\circ$ push-invariant as in $(B.2)$.

Finally, we assume that A is concentrated in even depth r. Here we have $\mathrm{mantar}(A_0) = -A_0$, so we cannot use the argument above; indeed $\mathrm{swap}(A) + A_0$ is mantar-invariant, but

$$\mathrm{mantar}(\mathrm{swap}(A)) = \mathrm{swap}(A) + 2A_0. \tag{B.3}$$

Instead, we note that if A is alternal then so is $\mathrm{neg}(A)$. Thus we can write A as a sum of an even and an odd function of the u_i via the formula

$$A = \frac{1}{2}(A + \mathrm{neg}(A)) + \frac{1}{2}(A - \mathrm{neg}(A)). \tag{B.4}$$

So it is enough to prove the desired result for all moulds concentrated in even depth r such that either $\mathrm{neg}(A) = A$ (even functions) or $\mathrm{neg}(A) = -A$ (odd functions). First suppose that A is even. Then since neg commutes with push and push is of odd order $r+1$ and neg is of order 2, we have

$$(\mathrm{neg} \circ \mathrm{push})^{r+1}(A) = \mathrm{neg}(A) = A. \tag{B.5}$$

However, we also have

$$\begin{aligned} \mathrm{neg} \circ \mathrm{push}(A) &= \mathrm{mantar} \circ \mathrm{swap} \circ \mathrm{mantar} \circ \mathrm{swap}(A) \\ &= \mathrm{mantar} \circ \mathrm{swap}\big(\mathrm{swap}(A) + 2A_0\big) \quad \text{by } (B.3) \\ &= \mathrm{mantar}\big(A + 2A_0\big) \\ &= A - 2A_0. \end{aligned}$$

Thus $(\mathrm{neg} \circ \mathrm{push})^{r+1}(A) = A - 2(r+1)A_0$, and this is equal to A by $(B.5)$, so $A_0 = 0$; thus in fact $A \in \mathrm{ARI}_{\underline{al}/\underline{al}}$ and that case is already proven.

Finally, if A is odd, i.e. $\mathrm{neg}(A) = -A$, the same argument as above gives $A - 2(r+1)A_0 = -A$, so $A = (r+1)A_0$, so A is a constant-valued mould concentrated in depth r, but this contradicts the assumption that A is alternal since constant moulds are not alternal, unless $A = A_0 = 0$. Note that this argument shows that all moulds in $\mathrm{ARI}_{\underline{al}*\underline{al}}$ that are not in $\mathrm{ARI}_{\underline{al}/\underline{al}}$ must be concentrated in odd depths. $\diamondsuit$

We can now complete the proof of Proposition 3.4*. Because $A = \mathrm{neg} \circ \mathrm{push}(A)$, we have $\mathrm{neg}(A) = \mathrm{push}(A)$, so in fact we only need to show that $\mathrm{neg}(A) = A$. As before,

* Ecalle states this result in [E1,§2.4] and there is also a proof in the preprint [E2,§12], but we were not able to follow the argument, so we have provided this alternative proof.

we may assume that A is concentrated in depth r. If $r = 1$, then A is an even function by assumption. If r is even, then as before we have $A = (\mathrm{neg} \circ \mathrm{push})^{2s+1}(A) = \mathrm{neg}(A)$. Finally, assume $r = 2s + 1$ is odd. Since we can write A as a sum of an even and an odd part as in (B.4), we may assume that $\mathrm{neg}(A) = -A$. Then, since A is alternal, using the shuffle $\mathrm{sh}\big((u_1, \ldots, u_{2s})(u_{2s+1})\big)$, we have

$$\sum_{i=0}^{2s} A(u_1, \ldots, u_i, u_{2s+1}, u_{i+1}, \ldots, u_{2s}) = 0.$$

Making the variable change $u_0 \leftrightarrow u_{2s+1}$ gives

$$\sum_{i=0}^{2s} A(u_1, \ldots, u_i, u_0, u_{i+1}, \ldots, u_{2s}) = 0. \tag{B.6}$$

Now consider the shuffle relation $\mathrm{sh}((u_1)(u_2, \ldots, u_{2s+1}))$, which gives

$$\sum_{i=1}^{2s+1} A(u_2, \ldots, u_i, u_1, u_{i+1}, \ldots, u_{2s+1}) = 0. \tag{B.7}$$

Set $u_0 = -u_1 - \cdots - u_{2s+1}$. Since $\mathrm{neg} \circ \mathrm{push}$ acts like the identity on A, we can apply it to each term of $(B.7)$ to obtain

$$\sum_{i=1}^{2s} -A(u_0, u_2, \ldots, u_i, u_1, u_{i+1}, \ldots, u_{2s}) - A(u_0, u_2, \ldots, u_{2s}, u_{2s+1}) = 0.$$

We apply $\mathrm{neg} \circ \mathrm{push}$ again to the final term of this sum in order to get the u_{2s+1} to disappear, obtaining

$$\sum_{i=1}^{2s} -A(u_0, u_2, \ldots, u_i, u_1, u_{i+1}, \ldots, u_{2s}) + A(u_1, u_0, u_2, \ldots, u_{2s-1}, u_{2s}) = 0.$$

Making the variable change $u_0 \leftrightarrow u_1$ in this identity yields

$$\sum_{i=1}^{2s} -A(u_1, u_2, \ldots, u_i, u_0, u_{i+1}, \ldots, u_{2s}) + A(u_0, u_1, u_2, \ldots, u_{2s-1}, u_{2s}) = 0. \tag{B.8}$$

Finally, adding $(B.6)$ and $(B.8)$ yields $2A(u_0, u_1, \ldots, u_{2s}) = 0$, so $A = 0$. This concludes the proof that $\mathrm{neg}(A) = A$ for all $A \in \mathrm{ARI}_{\underline{al}*\underline{al}}$, and thus, by Lemma B.2, that $\mathrm{push}(A) = A$. This concludes the proof of Proposition 3.4. $\diamondsuit$

Appendix C.

We follow Ecalle's more general construction of *twisted alternality* from [E1, pp. 57-64]. Let $\mathbf{e} \in \overline{\mathrm{ARI}}$ be a *flexion unit*, which is a mould concentrated in depth 1 satisfying

$$\mathbf{e}(v_1) = -\mathbf{e}(-v_1)$$

and

$$\mathbf{e}(v_1)\mathbf{e}(v_2) = \mathbf{e}(v_1 - v_2)\mathbf{e}(v_2) + \mathbf{e}(v_1)\mathbf{e}(v_2 - v_1).$$

Associate to $\mathbf{e}$ the mould $\mathbf{ez} \in \overline{\mathrm{GARI}}$ defined by

$$\mathbf{ez}(v_1, \ldots, v_r) = \mathbf{e}(v_1) \cdots \mathbf{e}(v_r).$$

Then a mould $A \in \overline{\mathrm{ARI}}$ is said to be $\mathbf{e}$-*alternal* if $A = \mathrm{ganit}(\mathbf{ez}) \cdot B$ where $B \in \overline{\mathrm{ARI}}$ is alternal. The conditions for $\mathbf{e}$-alternality can be written out using the explicit expression for ganit, using flexions, computed by Ecalle [E1, (2.36)]:

$$\big(\mathrm{ganit}(B) \cdot A\big)(\mathbf{w}) = \sum A(\mathbf{b}^1 \cdots \mathbf{b}^s) B(\lfloor \mathbf{c}^1) \cdots A(\lfloor \mathbf{c}^s), \tag{C.1}$$

where the sum runs over the decompositions of the word $\mathbf{w} = (u_1, \ldots, u_r)$ $(r \geq 1)$ as

$$\mathbf{w} = \mathbf{b}^1\mathbf{c}^1 \cdots \mathbf{b}^s\mathbf{c}^s, \quad (s \geq 1)$$

where all $\mathbf{b}^i$ and $\mathbf{c}^i$ are non-empty words except possibly for $\mathbf{c}^s$. For example in small depths, setting $C = \mathrm{ganit}(B) \cdot A$, we have

$$\begin{cases} C(v_1) = A(v_1) \\ C(v_1, v_2) = A(v_1, v_2) + A(v_1)B(v_2 - v_1) \\ C(v_1, v_2, v_3) = A(v_1, v_2, v_3) + A(v_1, v_2)B(v_3 - v_2) + \\ \qquad\qquad A(v_1)B(v_2 - v_1, v_3 - v_1) + A(v_1, v_3)B(v_2 - v_1). \end{cases}$$

Using the expression (C.1) for $\mathrm{ganit}(B) \cdot A$, the $\mathbf{e}$-alternality relations can be written explicitly as follows. Let $Y_1 = (y_1, \ldots, y_r)$ and $Y_2 = (y_{r+1}, \ldots, y_{r+s})$. Then for each word in the stuffle set $st(Y_1, Y_2)$, we construct the associated $\mathbf{e}$-*alternality term*, with an expression of the form

$$\big(C(\ldots, v_i, \ldots) - C(\ldots, v_j)\big)\mathbf{e}(v_i - v_j)$$

corresponding each contraction (cf. (2.14). For example, taking $Y_1 = (y_i, y_j)$ and $Y_2 = (y_k, y_l)$, the stuffle set $st(Y_1, Y_2)$ is given in (2.13), and the corresponding 13 $\mathbf{e}$-alternality terms are, first of all the six shuffle terms

$$C(v_1, v_2, v_3, v_4), C(v_1, v_3, v_2, v_4), C(v_1, v_3, v_4, v_2), C(v_3, v_1, v_2, v_4),$$

$$C(v_3, v_1, v_4, v_2), C(v_3, v_4, v_1, v_2)$$

(cf. (2.15)), then the six terms with a single contraction

$$\big(C(v_1,v_2,v_4)-C(v_1,v_3,v_4)\big)\mathbf{e}(v_2-v_3),\quad \big(C(v_1,v_2,v_4)-C(v_3,v_2,v_4)\big)\mathbf{e}(v_1-v_3),$$

$$\big(C(v_1,v_3,v_2)-C(v_1,v_3,v_4)\big)\mathbf{e}(v_2-v_4),\quad \big(C(v_1,v_4,v_2)-C(v_3,v_4,v_2)\big)\mathbf{e}(v_1-v_3),$$

$$\big(C(v_3,v_1,v_2)-C(v_3,v_1,v_4)\big)\mathbf{e}(v_2-v_4),\quad \big(C(v_3,v_1,v_2)-C(v_3,v_4,v_2)\big)\mathbf{e}(v_1-v_4)$$

(cf. (2.16)), and finally the single term with two contractions,

$$\big(C(v_1,v_2)-C(v_3,v_2)-C(v_1,v_4)+C(v_2,v_4)\big)\mathbf{e}(v_1-v_3)\mathbf{e}(v_2-v_4).$$

The $\mathbf{e}$-*alternality sum* $C_{r,s}$ is defined to be the sum of all the $\mathbf{e}$-alternality terms corresponding to words in the stuffle set $st(Y_1,Y_2)$; this sum is independent of the actual sequences Y_1,Y_2, depending only on their lengths r,s. The mould C is said to satisfy the $\mathbf{e}$-*alternality relations* if $C_{r,s}=0$ for all $1\le r\le s$. Comparing with (2.14-15) we see that the notion of alternality is nothing but the special case of $\mathbf{e}$-alternality for the flexion unit $\mathbf{e}(v_1)=1/v_1$. The associated mould $\mathbf{ez}$ is thus equal to *pic*, so we find that $\mathrm{ganit}(pic)\cdot A$ is alternil if A is alternal.

References

[B] S. Baumard, Aspects modulaires et elliptiques des relations entre multizêtas, Ph.D. dissertation, Paris, France, 2014.

[Bo] Bourbaki, N. Éléments de Mathématique. *Groupes et Algèbres de Lie*, Chapitres 2 et 3, 2nd ed., Springer (2006).

[Br] F. Brown, *Depth-graded motivic multiple zeta values*, arXiv: 1301.3053.

[C] S. Carr, Multizeta Values: Lie algebras and periods on $M_{0,n}$, Ph.D. Thesis, 2008. Available at http://math.unice.fr/ brunov/GdT/Carr.pdf.

[Cr] J. Cresson, Calcul Moulien, *Ann. Fac. Sci. Toulouse Math.* **XVIII** (2009), no. 2, 307-395.

[E1] J. Ecalle, The flexion structure and dimorphy: flexion units, singulators, generators, and the enumeration of multizeta irreducibles, in *Asymptotics in Dynamics, Geometry and PDEs; Generalized Borel Summation*, vol. II, O. Costin, F. Fauvet, F. Menous, D. Sauzin, eds., Edizioni della Normale, Pisa, 2011.

[E2] J. Ecalle, Eupolars and their bialternality grid, preprint 2014.

[F] H. Furusho, Double shuffle relation for associators, *Ann. of Math (2)* **174** (2011), no. 1, 341-360.

[R1] G. Racinet, Séries génératrices non-commutatives de polyzêtas et associateurs de Drinfel'd, Ph.D. dissertation, Paris, France, 2000.

[R2] G. Racinet, Doubles mélanges des polylogarithmes multiples aux racines de l'unité, *Publ. Math. Inst. Hautes Etudes Sci.* **No. 95** (2002), 185-231.

[S] L. Schneps, ARI, GARI, Zig and Zag: An introduction to Ecalle's theory of multizeta values, arXiv:1507.01534, 2014.

[Se] J-P. Serre, Lie Algebras and Lie Groups, Springer Lecture Notes **1500**, Springer-Verlag, 1965.