EXPANSIONS AND QUADRATICITY FOR GROUPS

DROR BAR-NATAN

ABSTRACT. First year students learn that the Taylor expansion Z_T carries functions into power series, and that it has some nice algebraic properties (e.g. multiplicativity, $Z_T(fg) = Z_T(f)Z_T(g)$). It is less well known that the same game can be played within arbitrary groups: there is a natural way to say "a Taylor expansion Z for elements of an arbitrary group G", and a natural way to carry the algebraic properties of the Taylor expansion to this more general context. In the case of a general G "Taylor expansions" (expansions with the same good properties as Z_T) may or may not exist, may or may not be unique, may or may not separate group elements, and a further good property which is hidden in the case of Z_T, "quadraticity", may or may not hold.

The purpose of this expository note is to properly define all the notions in the above paragraph, to enumerate some classes of groups whose theory of expansions we either understand or wish to understand, to indicate the relationship between these notions and the notions of "finite type invariants" and "unipotent" and "Mal'cev" completions, and to point out (with references) that our generalization of "expansions" to arbitrary groups is merely the tip of an iceberg, for almost everything we say can be generalized further to "expansions for arbitrary algebraic structures".

This paper is written at two formality levels. Material in "print" fonts is at the fully formal level. Material in handriting fonts is at conversation level. At this level I write what I think is true, but at times it may be imprecise, incomplete, or plain wrong.

CONTENTS

Date: first edition in future, this edition May. 18, 2016. The arXiv:????.???? edition may be older. Electronic version and related files at `http://drorbn.net/AcademicPensieve/Projects/ExQu`.

2010 *Mathematics Subject Classification.* 57M25, 20E99.

Key words and phrases. Expansions, Group Rings, Groups, Homomorphic Expansions, Projectivization, Quadratic Algebras .

This work was partially supported by NSERC grant RGPIN 262178.

1. Introduction

1.1. **The Taylor Expansion.** Before the real thing, which commences in Section 1.2, we start with a brief reminder on the classical Taylor expansion, which serves as a motivation for Section 1.2.

Let $\tilde{R} = C^\infty(V)$ the the algebra of smooth real-valued functions on some vector space V over $\mathbb{R}$, and let I be the ideal within $\tilde{R}$ of functions that vanish at 0: $I := \{f \in \tilde{R} \colon f(0) = 0\}$. Let $I^0 := \tilde{R}$, $I^1 := I$, and for $n > 1$ let I^n be the nth power of I: the set of all products of the form $f_1 f_2 \dots f_n$, where $f_i \in I$ for every i. Then I^n is the space of smooth functions that "vanish at least n times at 0", and hence the quotient I^n/I^{n+1} is "functions vanishing n times, while regarding as 0 functions that vanish more than n times", which is precisely "homogeneous polynomials of degree n". Thus the space

$$\hat{\mathcal{A}}(\tilde{R}) := \prod_{n\geq 0} I^n/I^{n+1} \tag{0}$$

can be identified as the space of power series on V. The "Taylor expansion" is a linear map $Z_T \colon \tilde{R} \to \hat{\mathcal{A}}(\tilde{R})$, and one may show that it is characterised by the following three properties (see Proposition 1.11 on page 8):

(1) *Z_T is an expansion:* If $f \in I^n$ then $Z_T(f)$ begins with $[f]$, the class of f within I^n/I^{n+1}. Namely,
$$Z_T(f) = (0, \dots, 0, \underbrace{[f]}_{\text{in degree } n}, *, *, \dots), \tag{1}$$
where "$*$" stands for "something arbitrary".

(2) *Z_T is multiplicative:*
$$Z_T(fg) = Z_T(f) Z_T(g), \tag{2}$$
where the product on the left is the pointwise product of functions and the product on the right is the product of power series.

(3) *Z_T is co-multiplicative:* If g is a smooth function of two variables $x, y \in V$ then its Taylor expansion $Z_T^x(g)$ with respect to the variable x is a smooth function of the variable y (namely, each coefficient of each homogeneous polynomial appearing in $Z_T^x(g)$ is a smooth function of y). Thus there is an iterated Taylor expansion $Z_T^{x,y}(g) := Z_T^y(Z_T^x(g))$, and it can be interpreted as taking values in the space of power series in two variables x, y. With all this and with $f \in \tilde{R}$, we have that
$$Z_T^{x,y}(f(x+y)) = (Z_T(f))(x+y).$$
Alternatively, with $\square$ denoting the operation $f(x) \mapsto f(x+y)$, defined on both functions and power series (and doubling the number of variables in each case), we have that
$$Z_T^{x,y} \circ \square = \square \circ Z_T. \tag{3}$$

1.2. **General Expansions.** A space "of power series" $\hat{\mathcal{A}}(R)$ can be defined as in Equation (0) whenever R is a ring and I is an ideal

[1] So in fact, our motivating example, the Taylor expansion, is not a special case of our definitions but only a close associate which is obtained when our definitions are restated for arbitrary rings. We can make the analogy a bit closer. The algebra $\tilde{R} = C^\infty(V)$ of functions under pointwise multiplication is isomorphic, via the Fourier transform and ignoring issues of analysis, to the algebra $R = C^\infty(V^*)$ of functions under convolutions. The latter algebra R is a continuous version of the group ring of V^*, and with this loose identification the definitions in this section match with the Taylor series example.

in R. Yet in this paper we restrict to the case when the ring R is the group ring of a group G.[1] So let G be an arbitrary discrete group whose identity element is denoted e. While G is arbitrary, some groups are more interesting than others, for our purpose. We advise our readers to inspect the left-most column of Table 1 on page 6 to gain a feel for the kind of groups we care more about. A particularly good example to keep in mind is the pure braid group PB_n on n strands, which we discuss in Section 1.5.

Let $R \coloneqq \mathbb{Q}G = \{\sum_{i=1}^k a_i g_i \colon a_i \in \mathbb{Q},\, g_i \in G\}$ be the group ring of G over the rational numbers $\mathbb{Q}$, and let $I = I_G$ be the augmentation ideal of $\mathbb{Q}G$:

$$I = \left\{ \sum a_i g_i \colon \sum a_i = 0 \right\} = \langle g - e \colon g \in G \rangle \,.$$

We declare that I^0 is $R = \mathbb{Q}G$ and also consider all higher powers I^n of I.

Definition 1.1. The polynomial algebra[2] $\mathcal{A}(G)$ of the group G is the direct sum

$$\mathcal{A}(G) \coloneqq \bigoplus_{n\geq 0} \mathcal{A}(G)_n \coloneqq \bigoplus_{n\geq 0} I^n/I^{n+1}.$$

The power series algebra $\hat{\mathcal{A}}(G)$ of G is the graded completion of the polynomial algebra $\mathcal{A}(G)$ of G. Thus

$$\hat{\mathcal{A}}(G) = \prod_{n\geq 0} \mathcal{A}(G)_n = \prod_{n\geq 0} I^n/I^{n+1}.$$

We note that the product $I^m \otimes I^n \to I^{m+n}$ induced by the product of R descends to a product $\mu\colon (I^m/I^{m+1}) \otimes (I^n/I^{n+1}) \to I^{m+n}/I^{m+n+1}$ and hence $\mathcal{A}(G)$ is in fact a graded algebra over $\mathbb{Q}$. We denote the identity element $[e] \in I^0/I^1$ of $\mathcal{A}(G)$ by 1, and note that there is a map $G \to \mathcal{A}_1(G)$ by $g \mapsto \bar{g} \coloneqq [g-e] \in I/I^2$.

Also note that $\mathcal{A}$ is a functor: a group homomorphism $\phi\colon G \to H$ induces a morphism $\phi\colon \mathbb{Q}G \to \mathbb{Q}H$ for which $\phi(I_G) \subset I_H$ and hence $\phi(I_G^n) \subset I_H^n$ for all n. Hence we get an induced map $\phi\colon \mathcal{A}(G) \to \mathcal{A}(H)$ which is easily seen to be a morphism of graded algebras. Likewise $\hat{\mathcal{A}}$ is a functor too.

$\hat{\mathcal{A}}(G)$ sometimes remembers much of the structure of G, and sometimes forgets much of it, as we shall see below. Yet always, for any group G whatsoever, it makes sense to seek a "Taylor expansion for G" — a map $Z\colon G \to \hat{\mathcal{A}}(G)$ satisfying the three properties that characterize the ordinary Taylor expansion. These are Definitions 1.2, 1.5, and 1.7 below.

Definition 1.2. A map $Z\colon G \to \hat{\mathcal{A}}(G)$ is called "an expansion"[3] if its homonymous uniquely defined linear extension $Z\colon \mathbb{Q}G \to \hat{\mathcal{A}}(G)$ has the "universality"[4] property that if $f \in I^n$ then $Z(f)$ begins with $[f]$, the class of f within I^n/I^{n+1}. Namely, if

$$Z(f) = (0, \dots, 0, \underbrace{[f]}_{\text{in degree } n}, *, *, \dots), \qquad (4)$$

where "$*$" stands for "something arbitrary".

Aside. One may think of expansions as "algorithms for progressively transmitting further and further details of a mathematical image". The best way to visualize that is to recall how real-life pictures are progressively transmitted over slow communication channels.

Think a picture of Brook Taylor, as it would gradually appear in a web browser connected to the internet over a slow modem:

Here the space of all pictures plays the role of R, and I^{n+1} is "the information we

[2] Quillen has a paper [Qu] devoted to the study of $\mathcal{A}(G)$, but he never names that ring beyond "the associated graded ring of a group ring".

[3] I learned this notion from Xiao-Song Lin's [Li].

[4] The origin of the word "universality" is in the subject of finite type invariants of knots [BN1], where the analogous property means that Z is a "universal finite type invariant".

allow ourselves to forget in the nth transmition step". So if $P \in R$ is our picture of Brook Taylor, then its projection to R/I^n is what we see after the $(n-1)$-st transmission step. For the next transmission step we need to transmit enough to recover the projection of P to R/I^{n+1}, but it would be wastefull to retransmit what we have sent before, which is in R/I^n. So we wish to transmit the "new" information in R/I^{n+1}: only that part of R/I^{n+1} that is 0 in R/I^n. That is the kernel of the projection $R/I^{n+1} \to R/I^n$, which is I^n/I^{n+1}. So we need a map $Z = \prod Z_n\colon R \to \prod I^n/I^{n+1}$ where Z_n is "the information tansmitted in step n". Finally, Z_n should have the property that if P is a picture all of whose details are forgettable until step n (namely, it is in I^n), then nothing about it should be transmitted until step n and then on step n we must transmit everything about P that is relevant to step n, and that's precisely the class of P in I^n/I^{n+1}. This last sentence is exactly condition (4).

When we see a picture gradually appearing on a web browser, it is precisely because somebody has already chosen an expansion Z for the space R of all pictures (Z is not unique and there is no canonical choice for Z).

It is often beneficial to try to find an expansion Z that is compatible with various operations that one may wish to apply to images P: re-colourations, rotations, or the concatanation of several images. Expansions that are compatible with the available operations are what we call "Taylor expansions": see Definition 1.8 below.

Proposition 1.3 (proof below). *Any group G has an expansion (in general, non-unique).*

Hence the real interest is not in expansions in general, but in expansions with extra properties as in the definitions that follow.

Proof of Proposition 1.3. For any natural number n the quotient I^n/I^{n+1} is a linear subspace of $\mathbb{Q}G/I^{n+1}$ and hence there is a (non-unique) projection $p_n\colon \mathbb{Q}G/I^{n+1} \to I^n/I^{n+1}$ which is a one-sided inverse of the inclusion map. Let $\pi_n\colon \mathbb{Q}G \to \mathbb{Q}G/I^{n+1}$ be the quotient map, and for $g \in G$ set $Z(g) := \sum_{n=0}^{\infty} p_n(\pi_n g) \in \prod I^n/I^{n+1} = \hat{\mathcal{A}}(G)$. It is easy to check that Z is an expansion. $\square$

Even before completing the definition of a "Taylor" expansion for a general group, we can already ponder whether a group has "powerful" expansions.

Definition 1.4. We say that a group G has a faithful expansion if it has an injective expansion $Z\colon G \to \hat{\mathcal{A}}(G)$.

Proposition **??** in Section 2 implies that if one expansion for a group G is injective, then so is every other expansion for G.

MORE: Same as residually torsion-free nilpotent?

A summary of what we know about the faithfulness of expansions for specific groups is in Table 1 on page 6.

Next is the analogue of (2):

Definition 1.5. An expansion $Z\colon G \to \hat{\mathcal{A}}(G)$ is said to be "multiplicative" if $Z(g_1g_2) = Z(g_1)Z(g_2)$ for every $g_1, g_2 \in G$.

Before we can state Definition 1.7, the analogue of (3), we need the following proposition:

Proposition 1.6 (Proof in Section 2.5)**.** *If G and H are groups, then $\mathcal{A}(G\times H) \cong \mathcal{A}(G) \otimes \mathcal{A}(H)$ and hence $\hat{\mathcal{A}}(G\times H) \cong \hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(H)$, where everything is interpreted in the (completed) graded sense:*

$$\hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(H) = \prod_n \bigoplus_{p+q=n} \mathcal{A}(G)_p \otimes \mathcal{A}(H)_q.$$

MORE: "Naturality".

Now given a group G let $\Box\colon G \to G$ be the "diagonal" map $g \mapsto (g,g)$ and let the same symbol $\Box$ also denote the functorially-induced morphism $\Box\colon \hat{\mathcal{A}}(G) \to \hat{\mathcal{A}}(G\times G) \cong \hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(G)$. The analogue of (3) is:

Definition 1.7. An expansion $Z\colon G \to \hat{\mathcal{A}}(G)$ is said to be "co-multiplicative" if the following diagram is commutative:

$$\begin{tikzcd} G \arrow[r, "\Box"] \arrow[d, "Z"] & G \times G \arrow[d, "Z\otimes Z"] \\ \hat{\mathcal{A}}(G) \arrow[r, "\Box"] & \hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(G). \end{tikzcd} \tag{5}$$

This amounts to saying that for every $g \in G$, $\zeta := Z(G)$ is group-like, namely, it satisfies $\Box\zeta = \zeta \otimes \zeta$.

Finally, we come to the definition of "Taylor":

Definition 1.8. We say that a group G is "Taylor" if it has a Taylor expansion — an $\hat{\mathcal{A}}(G)$-valued multiplicative and co-multiplicative expansion.

MORE: Really, $\Box$ makes $\mathcal{A}$ into a bialgebra and we seek a bialgebra morphism.

A summary of what we know about the Taylor property for specific groups is in Table 1 on page 6.

Remark 1.9. As a matter of convenience, we fixed our ground ring to be $\mathbb{Q}$, though our definitions make sense over arbitrary ground rings. In practice, raw expansions and multiplicative often exist also over $\mathbb{Z}$, yet Taylor expansions often require characteristic 0. See e.g. Remark 4.3.

Aside. Why Care About Expansions? Groups are sometimes complicated. It is sometimes difficult to decide if a group element g is trivial or not. Given an expansion Z, compute $Z(g)$ and (at least if Z is faithful) the question is susceptable to a degree-by-degree study, where often at least the low degrees are easy. It is sometimes difficult to decide if a certain equation, written within a group G, has solution. E.g., is $g \in G$ a square of some $h \in G$? Likewise, given g_1 and g_2, is there h such that $g_2 = h^{-1}g_1h$? Namely, are g_1 and g_2 conjugate? Given a multiplicative Z such questions become similarly susceptable to a degree-by-degree study.

1.3. **Quadraticity.** If an expansion is to be useful, we must understand its target space, $\hat{\mathcal{A}}(G)$. Clearly, as every element in I^n is a product of elements in I, the degree n piece $\mathcal{A}(G)_n = I^n/I^{n+1}$ is generated by products of elements in $\mathcal{A}(G)_1 = I/I^2$. So $\mathcal{A}(G)$ is generated by the degree 1 elements in it. $\mathcal{A}(G)$ is especially simple if all the relations between its generators are in degree 2.

Definition 1.10. Following [Lee], we say that the group G is "quadratic" if the $\mathbb{Q}$-algebra $\mathcal{A}(G)$ is a quadratic algebra [PP]. Namely, if $\mathcal{A}(G)$ is the algebra freely generated by $\mathcal{A}(G)_1$ modulo the ideal generated by the kernel of the multiplication map $\mu_{11}\colon \mathcal{A}(G)_1 \otimes \mathcal{A}(G)_1 \to \mathcal{A}(G)_2$:

$$\mathcal{A}(G) = \left\langle \frac{I}{I^2} \right\rangle \Big/ \!\! \Big/ \left\langle \ker\left(\frac{I}{I^2} \otimes \frac{I}{I^2} \to \frac{I^2}{I^3} \right) \right\rangle .$$

A summary of what we know about the quadraticity of specific groups is in Table 1 on page 6.

1.4. **Some Basic Examples.**

1.4.1. *The Infinite Cyclic Group $\mathbb{Z}$.* As our first example we take the group $\mathbb{Z}$, which we write in multiplicative notation: $G = \langle x \rangle = \{x^k \colon k \in \mathbb{Z}\}$. Then $\mathbb{Q}G = \mathbb{Q}[x, x^{-1}]$ can be identified as the ring of Laurent polynomials in a variable x. The augmentation ideal I of $\mathbb{Q}G$ is the ideal $\langle \tilde{x} \rangle$ generated by the single element $\tilde{x} = x - 1$; indeed, clearly $\langle \tilde{x} \rangle \subset I$, and the identities $x^k - 1 = (x^{k-1} + x^{k-2} + \cdots + 1)\tilde{x}$ and $x^{-k} - 1 = -(x^{-1} + x^{-2} + \cdots + x^{-k})\tilde{x}$ (for positive k) prove that $x^k - 1 \in \langle \tilde{x} \rangle$ for any k, and therefore $I \subset \langle \tilde{x} \rangle$. Therefore $\mathcal{A}(G) = \bigoplus \langle \tilde{x} \rangle^n / \langle \tilde{x} \rangle^{n+1} = \bigoplus \langle \tilde{x}^n \rangle / \langle \tilde{x}^{n+1} \rangle = \mathbb{Q}[\bar{x}]$ is a polynomial ring in one variable $\bar{x}$, where $\bar{x}$ is the class of $\tilde{x}$ in I/I^2 (and $\bar{x}^n$ is the class of $\tilde{x}^n$ in I^n/I^{n+1}). Thus $\hat{\mathcal{A}}(G) = \mathbb{Q}[\![\bar{x}]\!]$ is the ring of power series in $\bar{x}$.

A homomorphic expansion $Z\colon G \to \mathbb{Q}[\![\bar{x}]\!]$ is determined by its value $\xi = Z(x)$ on the generator x of G. Condition (4) is satisfied iff $\xi = 1 + \bar{x} + O(\bar{x})^2$ (note that such ξ's are always invertible in $\mathbb{Q}[\![\bar{x}]\!]$, so $Z(x^{-1}) = \xi^{-1}$

✔:=Yes, ✘:=No, ∼:=it Depends
?:=Unknown (to the author).
Superscripts: see "table footnotes" below.

Group(s) G	**Faithful** Z**?**	**Taylor** Z**?**	**Quadratic?**	**See**
1. Finite / torsion groups	✘[1]	✔[2]	✔[2]	Sec. 2.3
2. Free Abelian groups $\mathbb{Z}^n$	✔	✔	✔	Sec. 1.4.2
3. Free groups FG_n	✔	✔	✔	Sec. 1.4.3
4. LOT and LOF groups	∼	✔	✔	Sec. 4.1
5. Knot and pure tangle groups	∼	✔	✔	Sec. 4.2
6. Link groups	✘[3]	✔	✔	Sec. 4.3
7. 2-Knots groups	∼	✔	✔	
8. Pure braid groups PB_n	✔	✔	✔	Sec. 1.5
9. Hyperplane arrangement groups	?	✔	✔	
10. Reduced free groups RF_n	✔	✔	✘	Sec. 4.4
11. Reduced (homotopy) pure braid groups RPB_n	✔	✔	✘	
12. Pure v-braid groups PvB_n	?	✘	✔	
13. Pure w-braid groups PwB_n	✔	✔	✔	
14. Pure f-braid groups PfB_n				Merkov
15. Annular braids				
16. Elliptic pure braid groups PB_n^1 (braids on the torus)	?	✔	✘	
17. Higher genus pure braid groups $PB_n^{>1}$ (braids on high genus surfaces)	?	?	✘	arXiv:math/0309245?
18. Braid commutators $[PuB_n, PuB_n]$				
19. v-Braid commutators $[PvB_n, PvB_n]$				
20. w-Braid commutators $[PwB_n, PwB_n]$				
21. Hilden braids				
22. Mexican plait braids				Kurpita-Murasugi
23. Cactus groups				
24. Fundamental groups of surfaces		✔	✔	
25. Mapping class groups				
26. Torelli groups				Hain
27. Right-angled Artin groups		✔	✔	
28. General Artin groups				
29. Groups from BEER				arXiv:math/0509661
30. Groups from Brochier				arXiv:1209.0417
31. Poly-free groups				arXiv:math/0603470

MORE: Make sure that all statements are referenced. Additional columns: $H^2 = 0$?, extensibly Taylor?. Hierarchical structure for group list? Add tangles / homology cylinders / w-tangles etc., modulo C_n, Y_n, etc. Add tangles mod concordance, homology cylinders mod homology cobordism.

Table 1. Some groups and their expansion properties.

Table footnotes. 1. Except $G = \{e\}$. 2. In an empty manner. 3. Except $G = \mathbb{Z}^n$.

makes sense). Indeed, (4) with $n = 0, 1$ and $f = 1, t$ forces the first two coefficients of ξ to be as stated, and if ξ is as stated and $f = t^n \in I^n$ then $Z(f) = Z((x-1)^n) = (\xi - 1)^n = (\bar{x} + O(\bar{x})^2)^n = \bar{x}^n + O(\bar{x})^{n+1}$, sufficiently proving (4). Quite clearly, Z is faithful.

DRAFT! See http://drorbn.net/AcademicPensieve/Projects/ExQu/

We leave it to the reader to verify that the map $\square\colon \mathbb{Q}[\![\bar{x}]\!] = \hat{\mathcal{A}}(G) \to \hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(G) = \mathbb{Q}[\![\bar{x}_1, \bar{x}_2]\!]$ is the substitution $\bar{x} \to \bar{x}_1 + \bar{x}_2$. Therefore the commutativity of (5) starting with $x \in G$ in the upper left corner is the equation $\xi(\bar{x}_1 + \bar{x}_2) = \xi(\bar{x}_1)\xi(\bar{x}_2)$, whose unique solution within power series satisfying our initial condition is $\xi(\bar{x}) = \exp(\bar{x})$. Therefore there is a unique Taylor expansion for $G = \langle x \rangle$ and it is given by $Z(x^k) = e^{k\bar{x}}$.

1.4.2. *Abelian Groups.* Similar analysis shows that if $G = \mathbb{Z}^m = \langle x_1, \dots, x_m \colon x_i x_j = x_j x_i \rangle$, then $\mathbb{Q}G = \mathbb{Q}[x_i, x_i^{-1}]$ is the ring of Laurent polynomials in m variables, the augmentation ideal $I = \langle \tilde{x}_1, \dots, \tilde{x}_m \rangle$ is generated by the m elements $\tilde{x}_i = x_i - 1$, and $\hat{\mathcal{A}}(G) = \mathbb{Q}[\![\bar{x}_1, \dots, \bar{x}_m]\!]$ is the ring of power series in the variables $\bar{x}_i$, the images of $\tilde{x}_i$ in I/I^2. There is a unique Taylor expansion for G and it is given by $Z(x_i) = e^{\bar{x}_i}$. This expansion is faithful.

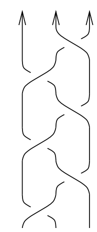
If G is finitely generated Abelian, then it is of the form $\mathbb{Z}^m \times T$, for some torsion group T. By Proposition 1.6, $\hat{\mathcal{A}}(G) = \hat{\mathcal{A}}(\mathbb{Z}^m)\hat{\otimes}\hat{\mathcal{A}}(T)$. By Corollary 2.4 below we find that $\mathcal{A}(T) = 0$. Hence there is a unique Taylor expansion for G, it is given by $Z(x_i) = e^{\bar{x}_i}$ with x_i and $\bar{x}_i$ as before, and it is faithful iff the torsion part T is trivial.

The case of general Abelian groups serves as Example 2.9.

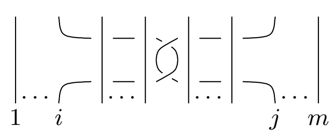
1.4.3. *Free Groups.* We leave it to the reader to verify that if G is a free group on some set of generators $\{x_\gamma\}_{\gamma\in\Gamma}$ then $\mathcal{A}(G)$ is the free associative algebra generated by $\bar{x_\gamma} = x_\gamma - e$ in I/I^2. One noteworthy expansion for G is the Magnus expansion Z_M, the multiplicative extension of $x_\gamma \mapsto 1 + \bar{x_\gamma}$ and $x_\gamma^{-1} \mapsto 1 - \bar{x_\gamma} + \bar{x_\gamma}^2 - \dots$. It is faithful (e.g. [MKS]), it is defined over $\mathbb{Z}$, but it is not Taylor. Another noteworthy expansion is the exponential expansion Z_E, the multiplicative extension of $x_\gamma^{\pm 1} \mapsto \exp(\pm\bar{x_\gamma})$. By Proposition [?] and the faithfulness of Z_M, the exponential expansion is also faithful. Z_E is Taylor, though it is only defined over $\mathbb{Q}$. Z_E is *not* the unique Taylor expansion for G — we leave it to the reader to verify that if $\{f_\gamma\}_{\gamma\in\Gamma}$ are Lie power series in the generators of $\mathcal{A}(G)$ which vanish in degree 1, then $x_\gamma^{\pm 1} \mapsto \exp(\pm(\bar{x_\gamma} + f_\gamma))$ always defines a (faithful) Taylor expansion for G.

1.5. **The First Sophisticated Example: Pure Braids and Vassiliev Invariants.** As an illustrative example, we discuss the pure braid group on m strands, PB_m. Our purpose is only to highlight the results; the proofs are merely cited.

The group PB_m is the fundamental group of the configuration space $C_m = \{z \in \mathbb{C}^m \colon i \neq j \Rightarrow z_i \neq z_j\}$ of m distinct points in the plane. A pure braid can be visualized as on the right.



The group PB_m is generated by the love-behind-the-bars elements $\{\sigma_{ij} \colon 1 \leq i < j \leq m\}$,

$\sigma_{ij} =$ 

,

subject to the relations (see Kassel-Turaev, [KT, Section 1.3])

$$\sigma_{ij}^{\sigma_{kl}} = \begin{cases} \sigma_{ij} & l < i \vee i < k < l < j, \\ \sigma_{ij}^{\sigma_{kj}^{-1}} & l = i, \\ \sigma_{ij}^{\sigma_{lj}^{-1}\sigma_{ij}^{-1}} & i = k < l < j, \\ \sigma_{ij}^{\sigma_{lj}\sigma_{kj}\sigma_{lj}^{-1}\sigma_{kj}^{-1}} & k < i < l < j, \end{cases}$$

where in a group $x^y := y^{-1}xy$ denotes conjugation.

The generators $\mathcal{A}(PB_m)_1$ of $\mathcal{A}(PB_m)$ are elements t_{ij}, the equivalence classes of $\sigma_{ij} - 1$ in I/I^2 (though we also allow $i > j$ by declaring $t_{ij} = t_{ji}$). The relations of $\mathcal{A}(PB_m)$ can be derived from the relations of PB_m, and come out to be $[t_{ij}, t_{kl}] = 0$ whenever i, j, k, l are distinct, and $[t_{ij} + t_{ik}, t_{jk}] = 0$ whenever i, j, k are distinct. Hence $\mathcal{A}(PB_m)$

is the well-known "Drinfel'd-Kohno algebra" [Dr1, Dr2, Koh1, Koh2].

Note that the augmentation ideal I is always generated by differences of group elements, and that any two pure braids differ by finitely many "crossing changes" ⤯ $\leftrightarrow$ ⤰. Hence for PB_m, the ideal I is generated by differences ⤫ $:=$ ⤯ $-$ ⤰ as in the theory of finite type (Vassiliev) invariants (e.g., [BN1, BN2]). Hence I^n is generated by "n-singular pure braids" (pure braids with n double points ⤫), hence $(\mathbb{Q}PB_m/I^{n+1})^*$ is precisely the space of type n invariants, and a little further inspection of the definitions shows that an expansion for PB_m is precisely what is called within the language of finite type invariants "a Universal Finite Type Invariant (UFTI) for PB_m".

It is well known that a multiplicative and co-multiplicative (i.e., Taylor) expansion / UFTI Z exists for PB_m. However I still don't know a simple group-theoretic proof of that fact. Indeed the simplest formula I know for such a Z is

$$Z(\gamma) = \sum_{\substack{n\geq 0 \\ 0<t_1<\ldots<t_n<1 \\ 1\leq i_1<j_1, i_2<j_2, \ldots, i_n<j_n\leq m}} \prod_{\alpha=1}^{n} \frac{t_{i_\alpha j_\alpha}}{2\pi i} d\log(z_{i_\alpha} - z_{j_\alpha}),$$

with z_i denoting the ith coordinate of a smooth braid-representative $\gamma\colon [0,1]\to C_m$. This formula, which was probably first written by Kohno [Koh1, Koh2], is far from obvious, and it contains in it the seeds for the Kontsevich integral [Ko, BN1, CDM], for the Drinfel'd theory of associators [Dr1, Dr2], and for our current understanding of multiple ζ-values [LM, Br].

Finally, for PB_m, Z is faithful, or in finite type language, "finite type invariants separate pure braids". See [Koh2, BN2].

1.6. What We Do in this Paper. MORE.

1.7. Back to Taylor. For the sake of completeness, we conclude this introduction with the following proposition:

Proposition 1.11. *The three properties of the Taylor expansion of smooth functions enumerated at the beginning of the introduction characterize the Taylor expansion. In other words, if $Z'\colon \tilde{R}\to\hat{\mathcal{A}}(\tilde{R})$ is linear and satisfies Equations (1), (2), and (3), then $Z' = Z_T$*

Proof. The Taylor expansion is elementary and well known and for us it is merely a motivating example. Hence we only indicate the main steps of the proof and leave the details to the reader. Without loss of generality $V=\mathbb{R}^k$ with coordinates $x_1,\ldots x_k$. As Z' is an expansion (1), it is enough to show that $Z'(p)=p$ whenever p is a polynomial in $x_1,\ldots x_k$. As it is multiplicative (2), it is enough to show that $Z'(x_i)=x_i$ for $i=1,\ldots,k$. Let $f_i := Z'(x_i)$. By (1), $f_i = x_i + (\text{higher degrees})$. Also, x_i satisfies $\square(x_i) = x_i + y_i$ and so by (3) we have that $f_i(x+y) = f_i(x) + f_i(y)$. It is easy to check that the only power series f_i satisfying these two conditions are $f_i = x_i$. $\square$

We note that all three conditions are necessary for Proposition 1.11. Indeed if $\Upsilon\colon \hat{\mathcal{A}}(\tilde{R})\to\hat{\mathcal{A}}(\tilde{R})$ is an arbitrary degree-increasing linear operator (no conditions at all, so there are plenty of choices) then $Z' := \Upsilon\circ Z_T$ is an expansion (satisfies (1)) while generally breaking (2) and (3), and if f_i are of the form $f_i = x_i + (\text{higher degrees})$ then setting $Z'(x_i) := f_i$ defines a multiplicative expansion uniquely, and unless $f_i = x_i$, it will not be co-multiplicative.

1.8. Disclaimer. I am far from an expert on group theory. Rather than "the authoritative paper on expansions", this note should be viewed as a challenge to others to write a better one, or perhaps, to send me the reference to an already-existing such paper.

1.9. Acknowledgement. I wish to thank Iva Halacheva, Peter Lee, Gwenael Massuyeau, Alexander Suciu, Huan Vo, and He Wang for their help with this paper.

2. Some Soft Facts about Power Series and Expansions

2.1. **Alternative Definitions.** We can define expansions somewhat more abstractly, note that $\mathbb{Q}G$ is filtered by the sequence $I^0 \supset I^1 \supset I^2 \supset \dots$ and that $\hat{\mathcal{A}}(G)$ is the (completed) associated graded space of that filtration, $\hat{\mathcal{A}}(G) = \widehat{\operatorname{gr}}\,\mathbb{Q}G$. Note that graded spaces are automatically also filtered, with the nth filtration space being the product of the degree m subspaces over all $m \geq n$. Note also that $\widehat{\operatorname{gr}}$ is a functor on the category of filtered spaces and that $\widehat{\operatorname{gr}} \circ \widehat{\operatorname{gr}}$ is naturally equivalent to $\widehat{\operatorname{gr}}$. With all this in mind, condition (4) is equivalent to the following:

$$Z\colon \mathbb{Q}G \to \widehat{\operatorname{gr}}\,\mathbb{Q}G \text{ is a filtration preserving linear map so that } \widehat{\operatorname{gr}}\,Z\colon \widehat{\operatorname{gr}}\,\mathbb{Q}G \to \widehat{\operatorname{gr}}\widehat{\operatorname{gr}}\,\mathbb{Q}G = \widehat{\operatorname{gr}}\,\mathbb{Q}G \text{ is the identity map of } \widehat{\operatorname{gr}}\,\mathbb{Q}G = \hat{\mathcal{A}}(G). \tag{6}$$

Even more abstractly, we can form the "unipotent completion" of G, $\widehat{\mathbb{Q}G} := \varprojlim_{n\to\infty} \mathbb{Q}G/I^n$, the inverse limit of the system

$$\mathbb{Q}G/I^1 \leftarrow \mathbb{Q}G/I^2 \leftarrow \mathbb{Q}G/I^3 \leftarrow \cdots .$$

The space $\widehat{\mathbb{Q}G}$ is filtered, with the type n subspace being the inverse limit $\varprojlim_{m\geq n} I^n/I^m$. One may verify that $\operatorname{gr}\widehat{\mathbb{Q}G} = \hat{\mathcal{A}}(G)$ and that the following is an equivalent definition of "an expansion":

$$\text{An expansion is a filtration preserving vector space isomorphism } Z\colon \widehat{\mathbb{Q}G} \to \hat{\mathcal{A}}(G) \text{ for which } \widehat{\operatorname{gr}}\,Z \text{ is the identity.} \tag{7}$$

Indeed, the limit of the projections $\mathbb{Q}G \to \mathbb{Q}G/I^n$ is a homomorphism $\iota\colon \mathbb{Q}G \to \widehat{\mathbb{Q}G}$. Composing ι with an expansion in the sense of (7) produces an expansion in the sense of (6), and it is easy to verify that every expansion in the sense of (6) arises in this way.

2.2. **Degrees 0 and 1.**

Proposition 2.1. *The degrees 0 and 1 parts of any expansion Z are uniquely determined by the universality condition (4) to be $Z(g) = 1 + \bar{g} = (1, \bar{g}) = (1, [g-1]) \in \mathbb{Q} \oplus (I/I^2) = \mathcal{A}_{\leq 1}(G)$.*

Proof. We have that $I^0 = G$, so by (4) at $n = 0$ we have that $Z(g) = (g + I^1, \dots) = (e + I^1, \dots)$, as $g - e \in I^1$. But then by (4) at $n = 1$ we must have $Z(g) - Z(e) = Z(g - e) = (0, [g - e], \dots) = (0, \bar{g}, \dots)$. This forces $Z(g) = 1 + \bar{g}$. □

2.3. **Some Trivialities About the Polynomial Algebra $\mathcal{A}(G)$.** For $g \in G$ we let $\tilde{g} := g - e \in \mathbb{Q}G$. It is clear that $\tilde{g} \in I$ and that elements of the form $\tilde{g}$ generate I. And as I/I^2 generates $\mathcal{A}(G)$, the classes $\bar{g}$ of the $\tilde{g}$'s in I/I^2 generate $\mathcal{A}(G)$.

Proposition 2.2. *In I/I^2, $\overline{gh} = \bar{g} + \bar{h}$ for any $g, h \in G$. In particular, in I/I^2, $\overline{g^k} = k\bar{g}$ for any $k \in \mathbb{Z}$ and $\overline{g^h} = \overline{h^{-1}gh} = \bar{g}$.*

Proof. In $\mathbb{Q}G$, $\widetilde{gh} = gh - e = (g - e) + (h - e) + (g - e)(h - e) = \tilde{g} + \tilde{h} + \tilde{g}\tilde{h}$, and modulo I^2 the last term drops out. □

Corollary 2.3. *If G is generated by some elements $\{g_\gamma\}$, or even merely normally generated by these elements*[5]*, then $\mathcal{A}(G)$ is generated by $\{\bar{g}_\gamma\}$.*

Corollary 2.4. *If a group G is torsion then $\mathcal{A}(G) = 0$ (justifying Table 1 line 1).*

Proof. Indeed if G is torsion and $g \in G$, then $g^k = e$ for some k, hence $k\bar{g} = \overline{g^k} = g^k - e = 0$, hence $\bar{g} = 0$, hence all the generators of $\mathcal{A}(G)$ vanish. □

There is an easy "graded variant" of Proposition 2.2; we care about it because many of the groups we care about are defined by relations involving conjugation, and expansions carry these conjugations into graded algebras:

[5]Meaning, generated by the g_γ's and their conjugates.

Proposition 2.5. *If $d > 0$ and g and h are elements of a graded algebra and h is invertible, then the degree d part of $g^h = h^{-1}gh$ depends on the parts of g at most up to degree d and on the parts of h at most up to degree $d-1$. Precisely, if we modify g by a degree $\leq d$ element γ and h by a degree $\geq d$ element η (so that the modified $h+\eta$ is still invertible) then*

$$(g+\gamma)^{(h+\eta)} = g^h + \gamma$$

in degrees $\leq d$. □

2.4. **A-Expansions.** Expansions are valued in $\hat{\mathcal{A}}(G)$, a space with a simple general abstract definition. Yet for concrete groups, it is sometimes difficult to describe $\mathcal{A}(G)$ in concrete terms. It is often the case that it is easy to guess a graded space A and show that it is "no smaller" than $\mathcal{A}(G)$; it then remains to affirm that the guess is right — namely, that $A \cong \mathcal{A}(G)$. In the current section we will see that we can achieve this affirmation by constructing an $\hat{A}$-valued "A-expansion". The first example where this technique is useful is within the proof of Proposition 1.6 in the next section, where the "unknown" is $\mathcal{A}(G \times H)$ and the "guess" is $\mathcal{A}(G) \otimes \mathcal{A}(H)$.

Definition 2.6. (Compare with Definition 1.2 and consult the diagram on the right).

$$\begin{tikzcd} & \hat{A} \arrow[d, shift right, "\hat\pi"'] \\ \mathbb{Q}G \arrow[ur, "Z_A"] \arrow[r, dashed, "\hat\pi\circ Z_A"] & \hat{\mathcal{A}}(G) \arrow[u, dashed, shift right, "\widehat{\operatorname{gr}} Z_A"'] \end{tikzcd}$$

Let G be a group, and A a graded vector space along with a degree-respecting surjection $\pi\colon A \to \mathcal{A}(G)$ (equivalently, $\hat\pi\colon \hat{A} \to \hat{\mathcal{A}}(G)$, where $\hat{A}$ is the graded completion of A). An A-expansion (for G) is a map $Z_A\colon G \to \hat{A}$ whose homonymous (uniquely defined) linear extension $Z_A\colon \mathbb{Q}G \to \hat{A}$ has the property that if $a \in A$ is of degree n and $f \in I^n$ is such that $\pi a = [f]$ in I^n/I^{n+1}, then $Z_A(f)$ begins with a. Namely,

$$Z_A(f) = (0, \ldots, 0, \underbrace{a}_{\text{in degree } n}, *, *, \ldots). \tag{8}$$

In the language of (6), the above definition is equivalent to the following:

$$\begin{array}{l} Z_A\colon \mathbb{Q}G \to \hat{A} \text{ is a filtration} \\ \text{preserving linear map so that} \\ \widehat{\operatorname{gr}}\, Z_A \circ \hat\pi\colon \hat{A} \to \hat{A} \text{ is the identity} \\ \text{map of } \hat{A}. \end{array} \tag{9}$$

Proposition 2.7. *If Z_A is an A-expansion for a group G, then $\pi\colon A \xrightarrow{\sim} \mathcal{A}(G)$ is an isomorphism and $Z := \hat\pi \circ Z_A$ is an expansion. (Hence finding an A-expansion both identifies $\mathcal{A}(G)$ and defines an ordinary expansion).*

Proof. The surjectivity of π is given and its injectivity follows from $\widehat{\operatorname{gr}}\, Z_A \circ \hat\pi = Id$, so it is an isomorphism. Given this (9) becomes (6). □

If we seek multiplicative expansions, then A should be an algebra and π a morphism of algebras, and we seek a multiplicative A-expansion Z_A so that $Z = \hat\pi \circ Z_A$ would be a multiplicative expansion. Likewise if we seek Taylor expansions, then in addition A should be a bialgebra and π a morphism of bialgebras, and we seek a co-multiplicative Z_A.

Claim 2.8. *If A is a graded algebra generated by its degree 1 elements, and π and Z_A are multiplicative and satisfy the conditions of an A-expansion in degrees 0 and 1 (namely, π is surjective and Equation (8) holds in these degrees), then Z_A is an A-expansion (in all degrees).*

Proof. Follows from the fact that $\mathcal{A}(G)$ is generated by its degree 1 elements. □

Example 2.9. Let G be an arbitrary Abelian group, written multiplicatively: $G = \langle x_\gamma\rangle_{\gamma\in\Gamma} \Big/ \left\{\prod_\gamma x_\gamma^{a_{r\gamma}} = e\right\}_{r\in R}$, where $\{x_\gamma\}$ is a set of commuting generators indexed by some set Γ, where $\left\{\prod_\gamma x_\gamma^{a_{r\gamma}} = e\right\}$ is a set of relations indexed by some set R, and where $(a_{r\gamma})$ is a matrix of coefficients in $\mathbb{Z}$ having the property that for any any fixed $r \in R$, $a_{r\gamma} \neq 0$ only for finitely many $\gamma \in \Gamma$.

By Corollary 2.3 we know that $\mathcal{A}(G)$ is generated by the elements $\bar{x_\gamma}$, and by Proposition 2.2 we know that for every r, $\sum_\gamma a_{r\gamma}\bar{x_\gamma} = 0$. It is fair to guess that these are the only relations in $\mathcal{A}(G)$. To confirm this, we let A be the Abelian algebra over $\mathbb{Q}$ with degree 1 generators t_γ for each $\gamma\in\Gamma$ and relations $\sum_\gamma a_{r\gamma}t_\gamma$ for each $r\in R$. The map $\pi\colon A\to\mathcal{A}(G)$ by $t_\gamma\mapsto\bar{x_\gamma}$ is well-defined and surjective, and we can construct a homomorphic A-expansion Z_A by setting $Z_A(x_\gamma)=e^{t_\gamma}$ — it is well defined by because in an Abelian algebra a product of exponentials is the exponential of a sum hence $Z_A(\prod_\gamma x_\gamma^{a_{r\gamma}})=\prod_\gamma e^{a_{r\gamma}t_\gamma}=\exp(\sum_\gamma a_{r\gamma}t_\gamma)=\exp(0)=e$, and it is easy to verify that it satisfies the condition (8) in degree 1.

Hence by Proposition 2.7 we know that we have identified all the relations in $\mathcal{A}(G)$ and that we have constructed a homomorphic expansion for G. $\boxed{2.9}$

2.5. **Products and Almost-Direct Products.** We aim to prove Proposition 1.6, asserting that $\mathcal{A}(G\times H)\cong\mathcal{A}(G)\otimes\mathcal{A}(H)$, using the technique of the previous section.

Proof of Proposition 1.6. Without further comment we will identify G and H as commuting subgroups of $GH:=G\times H$ using the coordinate inclusions, and likewise $\mathbb{Q}G$ and $\mathbb{Q}H$ as commuting subalgebras of $\mathbb{Q}(GH)=\mathbb{Q}G\otimes\mathbb{Q}H$. Let I_G, I_H, and I_{GH} denote the augmentation ideals of $\mathbb{Q}G$, $\mathbb{Q}H$, and $\mathbb{Q}(GH)$ respectively. Our first task is to compare these ideals and their powers.

Clearly, $I_{GH}=I_G(\mathbb{Q}H)+(\mathbb{Q}G)I_H$: the "$\supset$" inclusion is obvious, and the "$\subset$" inclusion follows from $gh-e=(g-e)h+(h-e)$. By expanding powers it follows that

$$I_{GH}^n=(I_G(\mathbb{Q}H)+(\mathbb{Q}G)I_H)^n=\sum_{p+q=n}I_G^pI_H^q. \quad (10)$$

Let $A=\mathcal{A}(G)\otimes\mathcal{A}(H)$, and let $\pi\colon A\to\mathcal{A}(GH)$ be the composition

$$\mathcal{A}(G)\otimes\mathcal{A}(H)\to\mathcal{A}(GH)\otimes\mathcal{A}(GH)\xrightarrow{\mu}\mathcal{A}(GH)$$

of the maps induced by the coordinate inclusions and the multiplication map μ. The map π is clearly graded, and it follows from (10) that it is surjective. Finally, if Z_G and Z_H are expansions for G and H (these exist by Proposition 1.3), it is easy to check that $Z_A:=Z_G\otimes Z_H$, more precisely defined by $Z_A(gh)=\sum_{p,q}Z_G(g)_p\otimes Z_H(h)_q$ is an A-expansion, where $Z_G(g)_p$ and $Z_H(h)_q$ denote the degree p and degree q of $Z_G(g)$ and $Z_H(h)$, respectively. Hence by Proposition 2.7 π is an isomorphism. $\square$

The only place in the above proof where we have used the fact that G and H commute within GH was in Equation (10). Indeed, without this commutativity we have that I_{GH}^n is a sum of 2^n products whose factors are $I_G(\mathbb{Q}H)$ and $(\mathbb{Q}G)I_H$ taken in an arbitrary order, and we have no way of 'sorting' such products to the form $I_G^pI_H^q$. Yet there is a further situation in which an analog of Proposition 1.6 holds:

Definition 2.10. A semi-direct product of groups $G\rtimes H$ is called "almost-direct" if the action of H on G descends to the trivial action of H on the Abelianization of G. In other words, if for any $g\in G$ and $h\in H$, $g^h\equiv g$ modulo (G,G), where $g^h:=h^{-1}gh$ and (G,G) denotes the group generated by all commutators of pairs of elements in G.

Proposition 2.11. *(Compare [Pa, Theorem 3.1] and [FR, Section 3]). If $G\rtimes H$ is almost-direct then as vector spaces, $\hat{\mathcal{A}}(G\times H)\cong\hat{\mathcal{A}}(G)\hat{\otimes}\hat{\mathcal{A}}(H)$.*

Proof. It is enough to re-prove Equation (10) in the present case. The inclusion $\supset$ is trivial, and so following the discussion above it is sufficient to show that in an arbitrary ordered product of factors each of which is $\mathbb{Q}G$, $\mathbb{Q}H$, I_G, or I_H we can sort the $\mathbb{Q}G$ and I_G factors to the left and all the $\mathbb{Q}H$ and I_H factors to the right by a series of $\subset$ inclusions, without decreasing the total number of I_G / I_H factors appearing. For this we use the equalities / inclusions $HG=GH$, $(\mathbb{Q}H)I_G=I_G(\mathbb{Q}H)$, and $I_H(\mathbb{Q}G)\subset I_{GH}=I_G(\mathbb{Q}H)+I_H$ which are easily shown to hold in an arbitrary semi-direct product, and the inclusion $I_HI_G\subset I_GI_H+I_G^2H$ which is a property of almost-direct products as follows:

$$(h-e)(g-e)=(g-e)(h-e)+(g^{h^{-1}}-g)h$$

$$\in I_G I_H + I_G^2 H. \qquad \square$$

MORE: a description of $\mathcal{A}(GH)$ as an algebra.

2.6. More About the Polynomial Algebra $\mathcal{A}(G)$.

If x and y are elements of a group, we denote their group-commutator by $(x,y) := xyx^{-1}y^{-1}$. If a and b are elements of an algebra, we denote their algebra-commutator by $[a,b] = ab - ba$. In our context, these two notions are compatible:

Proposition 2.12. *If $x, y \in G$, then $\widetilde{(x,y)} \in I^2$ and in $\mathcal{A}(G)_2 = I^2/I^3$, $\widetilde{(x,y)} = [\bar{x}, \bar{y}]$.*

Proof. In $\mathbb{Q}G$ and since e is central, $[\tilde{x}, \tilde{y}] = \widetilde{[x,y]} = \widetilde{(x,y)}yx$. Hence $\widetilde{(x,y)}yx \in I^2$, hence $\widetilde{(x,y)}(yx - e) \in I^3$, hence modulo I^3, $\widetilde{(x,y)} = \widetilde{(x,y)}yx = [\tilde{x}, \tilde{y}] = [\bar{x}, \bar{y}]$. $\square$

The above proposition has a stronger variant:

Proposition 2.13. *If $x, y \in G$ are such that $\tilde{x} \in I^m$ and $\tilde{y} \in I^n$, then $\widetilde{(x,y)} \in I^{m+n}$ and in $\mathcal{A}(G)_{m+n}$, $\widetilde{(x,y)} = [\tilde{x}, \tilde{y}]$.*

Proof. Same proof, with I^2 replaced with I^{m+n} and I^3 with I^{m+n+1}. $\square$

2.7. More About Expansions $Z\colon G \to \hat{\mathcal{A}}(G)$.

MORE Existance in the plain case, uniqueness, A-expansions.

MORE: Something about GT/GRT.

MORE: Something about expansions of nilpotent quotients.

MORE: Something about left- and right-exactness.

MORE: Add section, "computability".

3. Degree by Degree Constructions

Summary. Using standard deformation theory techniques, we show that if $H^2(G, \mathbb{Q}) = 0$ then G has a Taylor expansion that can be constructed inductively.

An "expansion to degree d" (sometimes, "partial expansion"), often denoted Z_d, is the same as an expansion (Definition 1.2), except that it takes values in the part $\mathcal{A}_{\leq d}(G)$ of degrees at most than d of $\mathcal{A}(G)$ (equivalently, in $\mathcal{A}(G)/\mathcal{A}_{>d}(G)$), and that the condition for an expansion, Equation (4), is imposed only for $n \leq d$. It similarly makes sense to speak of "multiplicative" and "Taylor" expansions, and of A-expansions to degree d.

Note that by Proposition 2.1, for any group G and any $g \in G$ we must set $Z_1(g) = 1 + \bar{g}$; this definition is Taylor to degree 1.

We say that a multiplicative (or Taylor or A-) expansion to degree d named Z_d is "extendible" if we can find a Z_{d+1}, a multiplicative (or Taylor or A-) expansion to degree $d+1$, whose restriction to degrees $\leq d$ is Z_d. (By an argument similar to the proof of Proposition 1.3, all partial expansions are extendible as "plain expansions", without multiplicativity or a Taylor property).

We say that a group G has the mutiplicative extension property (or the Taylor extension property) is for every $d \geq 1$ every multiplicative (or Taylor) expansion to degree d is extendible.

Example 3.1. Free groups have the multiplicative / Taylor extension property. For the multiplicative extension property, simply extend any expansion to degree d by choosing degree $d+1$ values for the extension on the generators in an arbitrary manner. For the Taylor extension property use the fact cited below in Capsule 3.4 that group-like elements to degree d always extend to group-like elements to degree $d+1$.

We give a very brief definition of the second cohomology $H^2 = H^2(G; V)$ of a group G, with coefficients in some vector space V over some field $\mathbb{F}$ (which we will later fix to be $\mathbb{Q}$). Further information can be found e.g. in Weibel's [We].

Given a group G, let $C^k := C^k(G; V) := \{\varphi\colon G^k \to V\}$ be the set of k-ary V-valued functions on G, for $k = 1, 2, 3$. Define $d^1\colon C^1 \to C^2$ and $d^2\colon C^2 \to C^3$ on $\phi \in C^1$ and $\epsilon \in C^2$ as follows:

$$(d^1\phi)(g_1, g_2) := \phi(g_1) - \phi(g_1 g_2) + \phi(g_2),$$

$$(d^2\epsilon)(g_1,g_2,g_3) \coloneqq \epsilon(g_2,g_3) - \epsilon(g_1g_2,g_3) + \epsilon(g_1,g_2g_3) - \epsilon(g_1,g_2).$$

It is easy to verify that $d^1/\!\!/d^2 = 0$, and hence it makes sense to set $H^2 \coloneqq H^2(G;V) \coloneqq \ker(d^2)/\operatorname{im}(d^1)$.

Our plan is to extend expansions. As a first step, we prove a general "extension" lemma. Let (B,η) be an augmented $\mathbb{F}$-algebra (an $\mathbb{F}$-algebra B along with a multiplicative $\eta\colon B \to \mathbb{F}$), and let C be an ideal within B which is trivial as a B-bimodule; namely, such that $bc = cb = \eta(b)c$ for every $b \in B$ and $c \in C$. Let $\pi\colon B \to B/C$ be the projection. It is a morphism of augmented algebras.

Lemma 3.2. *If $H^2(G;C) = 0$, then every multiplicative map $Z_0\colon G \to B/C$ for which $Z_0/\!\!/\eta = 1$ can be lifted to a multiplicative $Z\colon G \to B$ for which $Z/\!\!/\eta = 1$.*

$$\begin{tikzcd} & B \arrow[d, "\pi"] \\ G \arrow[ur, dashed, "\exists Z"] \arrow[r, "Z_0"'] & B/C \end{tikzcd}$$

Proof. Pick an arbitrary, possibly not-multiplicative, lift $Z'\colon G \to B$. Its failure to be multiplicative is measured by a functional $\epsilon' \coloneqq \epsilon(Z') \in C^2(G;C)$, where

$$\epsilon(Z')(g_1,g_2) \coloneqq Z'(g_1g_2) - Z'(g_1)Z'(g_2) \quad (11)$$

(the multiplicativity of π implies that $\epsilon'/\!\!/\pi = 0$, so ϵ' takes values in C). We claim that $d^2\epsilon' = 0$. Indeed, in the diamond

$$\begin{tikzcd} & Z'(g_1g_2)Z'(g_3) \arrow[dl, dash, "\epsilon'(g_1g_2,g_3)"'] \arrow[dr, dash, "\epsilon'(g_1,g_2)"] & \\ Z'(g_1g_2g_3) \arrow[dr, dash, "\epsilon'(g_1,g_2g_3)"] & & Z'(g_1)Z'(g_2)Z'(g_3) \arrow[dl, dash, "\epsilon'(g_2,g_3)"'] \\ & Z'(g_1)Z'(g_2g_3) & \end{tikzcd}$$

the quantity indicated on each edge is the difference of the quantity on the vertex to its left with the quantity on the vertex to its right (for the two edges on the right, we use the triviallity of the action of B on C and the condition $Z_0/\!\!/\eta = 1$). Hence by telescoping the sum of the upper two edge-quantities is equal to the sum of the bottom two. That is, $d^2\epsilon' = 0$.

As $H^2(G;C) = 0$, we can find $\phi \in C^1(G;C)$ such that $d_1\phi = \epsilon'$. Set $Z \coloneqq Z' + \phi$. Studying (11) (and again using the triviallity of the action of B on C and the condition $Z_0/\!\!/\eta = 1$) we find that

$$\epsilon(Z) = \epsilon(Z') - d^1\phi = \epsilon' - \epsilon' = 0,$$

which means that Z is multiplicative. $\square$

The road is now clear.

Theorem 3.3. *If $H^2(G;\mathbb{Q}) = 0$ then G has the multiplicative extension property: every multiplicative partial expansion Z_d, for $d \geq 1$, can be extended. In particular, G has a multiplicative (full) expansion Z.*

Proof. If $H^2(G;\mathbb{Q}) = 0$ then $H^2(G;V) = 0$ for any $\mathbb{Q}$-vector space V. For the first statement of the theorem, take $B = \mathcal{A}_{\leq d+1}(G)$, $C = \mathcal{A}_{d+1}(G)$, $B/C = \mathcal{A}_{\leq d}(G)$, and use the lemma. The second statement is proven by induction starting from the fact that Z_1 always exists. $\square$

MORE. It would be nice to relate the above with standard group cohomology techniques: Ext groups, group extensions, Schur multipliers.

Recall that a multiplicative expansion Z is "Taylor" if $Z(g)$ is group-like for every $g \in G$ (Definition 1.7. Before we can prove the "Taylor" version of Theorem 3.3, we need to recall a few well-known facts about group-like elements in a bi-algebra.

Capsule 3.4. (consider moving to an earlier location) (Following many sources starting with [MM]. A quick introduction is at [CDM, Appendix A.2]). In a graded degree-completed connected co-commutative bialgebra A, ζ is called "group-like" if it satisfies $\Box\zeta = \zeta \otimes \zeta$, and ϕ is "primitive" if $\Box\phi = \phi \otimes 1 + 1 \otimes \phi$. Group-like elements form a group (denoted $A_{\exp}$) under multiplication, and primitive elements form a graded Lie algebra (denoted A_{prim}) under the commutator bracket. There is a bijection between group-like and primitive elements: if ϕ is primitive then $\exp(\phi)$ is group-like, and if ζ is group-like, $\log\phi$ makes sense and is primitive. Both notions make sense "up to degree d" (or "modulo degrees higher than d"), and the bijection persists. A primitive up to degree d element always extends to a primitive up to degree $d+1$ element: simply extend by 0 at degree $d+1$. The same extension property is true for group-like elements: take the logarithm, extend by 0, and exponentiate back again. Finally, if ζ is group-like to degree d and ϕ is of degree d, then $\zeta+\phi$ is group-like to degree d iff ϕ is primitive. $\boxed{3.4}$

Theorem 3.5. *If $H^2(G;\mathbb{Q})=0$ then G has the Taylor extension property: every partial Taylor expansion Z_d, for $d\geq 1$, can be extended. In particular, G has a (full) Taylor expansion Z.*

Proof. Use the same procedures as in the proof of Theorem 3.3 and Lemma 3.2, yet note that at each stage the lift Z' can be chosen to be group-like (by the extension property for group-like elements above), and then ϵ' is primitive as the least-degree difference of two group-like elements. As $H^2(G;\mathcal{A}_{prim}(G))=0$, we can choose ϕ to be primitive, and then $Z=Z'+\phi$ remains group-like. □

In rare ocassions, the existence of Taylor expansions for a group G implies the same for a quotient of G:

Definition 3.6. We say that a normal subgroup R of a group G is "robust" if it is normally generated within G by elements r_i whose images in $\mathbb{Q}\otimes G^{ab}$ are linearly independent.

Theorem 3.7. *If G has the multiplicative (or Taylor) extension property and R is a robust normal subgroup of G, then G/R also has the multiplicative (or Taylor) extension property.*

Proof. As every group has expansions to degree 1, it is enough to prove an extension lemma

MORE: Finish this!

Are there examples beyond LOT groups?

Is it true that Lemma 3.2 is an iff and that if R is robust and $H^2(G)=0$ then $H^2(G/R)=0$?

4. Some Specific Families of Groups

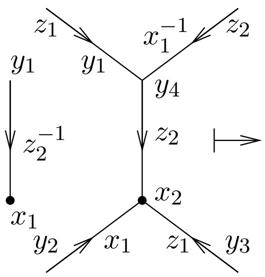
MORE: Sort in: homologically trivial braids in the torus / in genus g, upper McCool.

4.1. LOT and LOF groups.

Summary. Howie [Ho1, Ho2] defines a class of groups associated with certain "labelled oriented graphs" Γ, and studies in detail the case when Γ is a tree, calling the resulting class of groups "LOT groups", showing that they are the fundamental groups of ribbon d-knots, for $d\geq 2$. We allow forests instead of just trees, call the resulting class "LOF groups", and study their expansions.

Following Howie [Ho1, Section 3], a "labeled oriented graph" Γ is a quintuple $\Gamma=(V,E,\iota,\tau,\lambda)$, where V and E are sets of "vertices" and "edges" respectively (finite, in [Ho1], but not necessarily so, for us), where ι and τ are maps $E\to V$ which map every edge $a\in E$ to its initial vertex $\iota(a)$ and terminal vertex $\tau(a)$[6], and where $\lambda\colon E\to V^{\pm 1}:=\{a,a^{-1}\colon a\in V\}$ puts an additional "label", which is either a vertex or the formal inverse of a vertex, conventionaly marked near the middle of the edge. To such Γ we associate a group $G(\Gamma)$, defined as the group whose set of generators is V and whose relations correspond to the edges of Γ, where the relation for an edge a with $\iota(a)=x$, $\tau(a)=y$, and $\lambda(a)=z^{\pm 1}$, namely for $x\xrightarrow{z^{\pm 1}}y$, is $x=z^{\mp 1}yz^{\pm 1}=y^{z^{\pm 1}}$, or "the tail is the head conjugated by the middle"[7]. Here is a simple example of a lalebled graph with two connected components, and the corresponding group presentation:

[6] Having established notation we will use graph theoretic language with no further comment.



$$\longmapsto \left\langle \begin{array}{c} x_1, x_2, y_1, y_2, y_3, y_4, z_1, z_2\colon \\ r_1\colon y_1 = x_1^{z_2^{-1}},\ r_2\colon y_2 = x_2^{x_1}, \\ r_3\colon y_3 = x_2^{z_1},\ r_4\colon y_4 = x_2^{z_2}, \\ r_5\colon z_1 = y_4^{y_1},\ r_6\colon z_2 = y_4^{z_1^{-1}} \end{array} \right\rangle$$

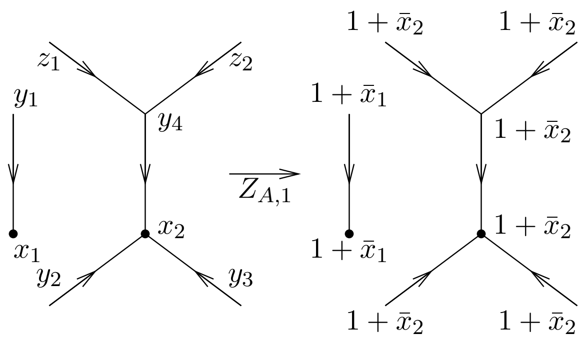
We say that Γ is a tree if its underlying graph $(V, E, \iota.\tau)$ is a tree. In this case, Howie [Ho1, Ho2] calls $G(\Gamma)$ a LOT (Labelled Oriented Tree) group. Howie shows that such groups are precisely the fundamental groups of ribbon d-knots in S^{d+2}, for $d \geq 2$.

We say that Γ is a forest of rank n if its underlying graph $(V, E, \iota.\tau)$ is a disjoint union of n trees, and call the corresponding groups "LOF groups" of rank n (note that the labeling λ can jump across components). One may show (see also [BN3, Comment 3.10]) that such groups are precisely the fundamental groups of ribbon knottings of wedge sums of n based d-spheres in S^{d+2}, for $d \geq 2$.

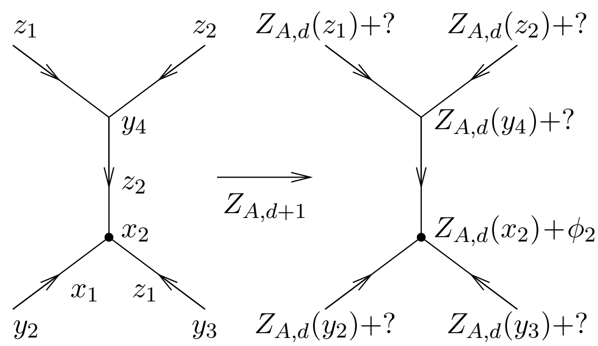
For any Γ, the edge relations in $G \coloneqq G(\Gamma)$ imply that it is normally generated by one generator for each connected component of Γ, and hence by Corollary 2.3 $\mathcal{A} \coloneqq \mathcal{A}(G)$ is generated by one generator for each component of Γ. If Γ is not a forest, that's all that we can say at this point. If Γ is a forest, let $\{x_i\}_{i=1}^n \subset V$ be some choice of roots for the components of Γ. Then $\mathcal{A}$ is generated by the elements $\bar{x}_i = [x_i - 1]$ in $\mathcal{A}_1 = I/I^2$, and we guess that the $\bar{x}_i$'s freely generate $\mathcal{A}$. To verify this we set $A \coloneqq FA(\bar{x}_i)$, the free associative algebra generated by the $\bar{x}_i$'s, note the obvious projection $\pi\colon A \to \mathcal{A}$, and construct (below) an A-expansion $Z_A\colon G \to A$ (see Section 2.4).

We construct Z_A degree by degree, in the spirit of Section 3 (though without using the results of that section).

The beginning of the construction is forced by Proposition 2.1: we must have $Z_1(g) = 1 + \bar{g} \in \mathcal{A}_{\leq 1}(G)$ for every $g \in G$, so we must have $Z_{A,1}(y) = 1 + \bar{y} \in A_{\leq 1}$ for every generator y of G. If y is one of these generators and x_i is the root of the tree that y belongs to, then by the relations, y is conjugate to x_i, so by Proposition 2.2, $\bar{y} = \bar{x}_i$ in $\mathcal{A}_{\leq 1}(G)$ and we must set $Z_{A,1}(y) = 1 + \bar{x}_i$. So considering the example before to degree 1, we must have:



Now assume that we found and extension $Z_{A,d}$ of $Z_{A,1}$ to degree d; we aim to extend it further to degree $d+1$. Using Capsule 3.4 find $\phi_i \in A_{d+1}$ so that on the roots x_i we'd have that $Z_{A,d+1}(x_i) \coloneqq Z_{A,d}(x_i) + \phi_i$ is group like. So far we have (dropping one connected component to save space):



But now the values of $Z_{A,d+1}$ on the immediate neighbors of the roots ((y_2, y_3, y_4) in the partial example) are determined: they have to be conjugates of the values on the roots as specified by the edge relations. The values of

[7]Note that the relation corresponding to $x \xrightarrow{z^{-1}} y$ is equivalent to the relation for $x \xleftarrow{z} y$, so we could have restricted, as Howie [Ho1] does, to middle labels with positive powers, at the cost of reversing some edge orientations.

the conjugators (x_1, z_1, z_2) in these edge relations might already be specified only to degree d, but by Proposition 2.5, that is enough. Continuing in this way the values of $Z_{A,d+1}$ on farther and farther neighbors of the roots are determined, and eventually $Z_{A,d+1}$ is fully determined and is a Taylor expansion to degree $d+1$.

In summary, we have proven the following:

Theorem 4.1. *If $G = G(\Gamma)$ is a LOF group and $\{x_i\}$ is a choice of roots for the components of Γ, then $\mathcal{A}(G)$ is a free associative algebra with generators $\{\bar{x}_i\}$ in bijection with the roots, and the Taylor expansions for G are in a bijection with choices of group-like elements $\{Z(x_i)\}$ in $\mathcal{A}(G)$, one for each root, such that to degree 1, $Z(x_i) = 1 + \bar{x}_i$.*

Remark 4.2. As $\mathcal{A}(G)$ is free, LOF groups are always quadratic.

Remark 4.3. Capsule 3.4 breaks over $\mathbb{Z}$, and indeed in general Taylor expansions for LOF groups do not exist over $\mathbb{Z}$. Otherwise our construction works in an almost verbatim manner to construct multiplicative expansions for LOF groups over $\mathbb{Z}$.

MORE. Faithfulness (ask Gwenael?)? $n = \infty$?

4.2. Knot and Pure Tangle.

4.3. Link Groups.

MORE: For link groups, state a theorem about the relationship with Milnor invariants; perhaps prove Stallings' using expansions?

4.4. Reduced Free Groups.

MORE.

5. Some Harder Facts about Power Series and Expansions

MORE: This section needs a detailed look.

The lower central series G_n of G is defined inductively by setting $G_1 := G$ and $G_{n+1} := (G, G_n) = \{(x,y) \colon x \in G,\ y \in G_n\}$. It is clear that $G = G_1 \rhd G_2 \rhd G_3 \rhd \ldots$, and that the quotients G_n/G_{n+1} are Abelian groups. It is well known that the group commutator (x,y) induces a structure of a graded Lie ring on $\mathcal{L}G := \bigoplus_n G_n/G_{n+1}$ (see e.g. [MKS]). Proposition 2.13 implies that the map $x \mapsto \bar{x}$ maps G_n to I^n and induces a Lie morphism $\mathcal{L}G \to \mathcal{A}(G)$ and hence an algebra morphism $\mathcal{U}(\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{L}G) \to \mathcal{A}(G)$, where $\mathcal{U}$ denotes the universal enveloping algebra. Quillen [Qu] proves that that morphism is in fact an isomorphism: $\mathcal{U}(\mathbb{Q}\otimes_{\mathbb{Z}}\mathcal{L}G) \cong \mathcal{A}(G)$.

Note that if $F = F(x_i)$ is a free group on some set of generators (x_i) and F_n denotes the lower central series of F, then F_1/F_2 is the free Abelian group with generators x_i and F_2/F_3 is the free Abelian group with generators (x_i, x_j) for $i < j$ (or allow (x_i, x_j) with arbitrary i, j, yet note that modulo F_3 and using Abelian notation, $(x_i, x_j) + (x_j, x_i) = 0$). We let $V = V(x_i)$ be the $\mathbb{Q}$-vector space with basis (x_i), and note that $\mathbb{Q}\otimes(F_1/F_2) \cong V$ and $\mathbb{Q}\otimes(F_2/F_3) \cong \bigwedge^2 V \subset V \otimes V$.

Definition 5.1. We say that a presentation $G = \langle x_i \mid r_k \rangle$ of a group G is "quadratically efficient" if the relations r_k, in themselves elements of the free group $F = F(x_i)$, all belong to the commutator subgroup $F_2 = (F,F)$ of F and their images ρ_k in $\mathbb{Q}\otimes(F_2/F_3) = \bigwedge^2 V$ are linearly independent.

Theorem 5.2. *If a group G has a quadratically efficient presentation $\langle x_i \mid r_k \rangle$ then it is quadratic and $\mathcal{A}(G) \cong TV/\langle \rho_k \rangle$ is the tensor algebra $TV = \bigoplus_n V^{\otimes n}$ of $V = V(x_i)$ modulo the ideal generated by the images ρ_k of the relations r_k in $\bigwedge^2 V \subset V^{\otimes 2}$.*

MORE: Examples and proof.

MORE Quillen's theorem (using expansions?). Must sort in Quillen's theorem and link up with existing literature, expecially with Suciu-Wang.

MORE Hutchings-Positselski-Lee.

6. Beyond Groups

MORE.

References

[BN1] D. Bar-Natan, *On the Vassiliev knot invariants,* Topology **34** (1995) 423–472.

[BN2] D. Bar-Natan, *Vassiliev and quantum invariants of braids,* in Proc. of Symp. in Appl. Math.

51 (1996) 129–144, *The interface of knots and physics,* (L. H. Kauffman, ed.), Amer. Math. Soc., Providence.

[BN3] D. Bar-Natan, *Balloons and Hoops and their Universal Finite Type Invariant, BF Theory, and an Ultimate Alexander Invariant,* Acta Mathematica Vietnamica **40-2** (2015) 271–329, arXiv:1308.1721.

[BND] D. Bar-Natan and Z. Dancso, *Finite Type Invariants of W-Knotted Objects I: Braids, Knots and the Alexander Polynomial,* http://www.math.toronto.edu/drorbn/LOP.html#WKO1, arXiv:1405.1956.

[Br] F. C. S. Brown, *Multiple Zeta Values and Periods of Moduli Spaces* $\overline{\mathfrak{M}}_{0,n}$, Ann. Sci. de l'ENS **42-3** (2009) 371–489, arXiv:math/0606419.

[CDM] S. Chmutov, S. Duzhin, and J. Mostovoy, *Introduction to Vassiliev Invariants,* Cambridge University Press, 2012.

[Dr1] V. G. Drinfel'd, *Quasi-Hopf Algebras,* Leningrad Math. J. **1** (1990) 1419–1457.

[Dr2] V. G. Drinfel'd, *On Quasitriangular Quasi-Hopf Algebras and a Group Closely Connected with* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$*,* Leningrad Math. J. **2** (1991) 829–860.

[En] B. Enriquez, *Elliptic Associators,* Sel. Math. New Ser. **20** (2014) 491–584, arXiv:1003.1012.

[FR] M. Falk and R. Randell, *The Lower Central Series of a Fiber-Type Arrangement,* Invent. Math. **82** (1985) 77–88.

[HL] N. Habegger and X-S. Lin, *The Classification of Links up to Link-Homotopy,* J. Amer. Math. Soc. **3** (1990) 389–419.

[Ho1] J. Howie, *On the Asphericity of Ribbon Disc Complements,* Trans. Amer. Math. Soc. **289-1** (1985) 281–302.

[Ho2] J. Howie, *Minimal Seifert Manifolds for Higher Ribbon Knots,* Geometry and Topology Monographs **1** 261–293, arXiv:math/9810185.

[Hu] P. Humbert, *Intégrale de Kontsevich elliptique et enchevêtrements en genre supérieur,* Ph.D. thesis, Strasbourg 2012.

[KT] C. Kassel and V. Turaev, *Braid Groups,* Graduate Texts in Mathematics **247**, Springer 2008.

[Koh1] T. Kohno, *Monodromy Representations of Braid Groups and Yang-Baxter Equations,* Ann. Inst. Fourier **37** (1987) 139–160.

[Koh2] T. Kohno, *Linear Representations of Braid Groups and Classical Yang-Baxter Equations,* Contemp. Math. **78** (1988) 339–363.

[Ko] M. Kontsevich, *Vassiliev's knot invariants,* Adv. in Sov. Math. **16(2)** (1993) 137–150.

[LM] T. Q. T. Le and J. Murakami, *On Kontsevich's Integral for the HOMFLY Polynomial and Relations of Multiple* ζ*-Numbers,* Topology and its Applications **62** (1995) 193–206.

[Lee] P. Lee, *The Pure Virtual Braid Group is Quadratic,* Selecta Mathematica **19-2** (2013) 461–508, arXiv:1110.2356.

[Li] X-S. Lin, *Power Series Expansions and Invariants of Links,* in *Geometric topology* (proceedings of the Georgia international topology conference), (W. H. Kazez, ed.), 184–202, Amer. Math. Soc. and International Press, Providence, 1997.

[MKS] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations,* Wiley, New York, 1966.

[MM] J. Milnor and J. Moore, *On the structure of Hopf algebras,* Ann. of Math. **81** (1965) 211–264.

[Pa] Ş. Papadima, *The Universal Finite-Type Invariant for Braids, with Integer Coefficients,* Topology and its Applications **118** (2002) 169–185.

[PP] A. Polishchuk and L. Positselski, *Quadratic Algebras,* University Lecture Series **37**, American Mathematical Society 2005.

[Qu] D. G. Quillen, *On the Associated Graded Ring of a Group Ring,* J. of Algebra **10** (1968) 411–418.

[We] C. A. Weibel, *An Introduction to Homological Algebra,* Cambridge University Press, Cambridge, 1994.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO ONTARIO M5S 2E4, CANADA
E-mail address: drorbn@math.toronto.edu
URL: http://www.math.toronto.edu/~drorbn