Compositions of n-homomorphisms

Darij Grinberg

April 13, 2026

Abstract. We study n-homomorphisms in the sense of Khudaverdian–Voronov, but generalized to maps from arbitrary rings to arbitrary commutative rings. We show that the sum of an n-homomorphism and an m-homomorphism is an $(n+m)$-homomorphism, and that the composition of an n-homomorphism and an m-homomorphism is an nm-homomorphism. The proofs are entirely combinatorial.

This note is a long answer to one of my own MathOverflow questions. The answer (which was obtained with the help of GPT-5.4, though written up entirely on my own) did not fit in a MathOverflow post, so I have made it into a note.

Acknowledgments. I have used GPT-5.4 via Christian Stump's convenient `https://sciencebench.ai/` front-end. I thank Christian for his work on this.

0.1. n-homomorphisms

The notion of an n-homomorphism is a generalization of the notion of a pseudorepresentation, which was introduced by Taylor in [Taylor91] (based on an idea of Wiles [Wiles88, proof of Lemma 2.2.3]).

We first introduce some notations. *Rings* are always understood to be associative and unital (but not necessarily commutative); ring morphisms preserve the unity (unless we speak of "nonunital ring morphisms"). For any nonnegative integer n, we let $[n]$ denote the set $\{1, 2, \ldots, n\}$, and we let S_n denote the n-th symmetric group (i.e., the group of permutations of this set $[n]$). If σ is a permutation of a finite set (e.g., of $[n]$), then $(-1)^{\sigma}$ shall denote the sign of σ. (If $\sigma \in S_n$, then $(-1)^{\sigma} = (-1)^{\ell(\sigma)}$, where $\ell(\sigma)$ is the number of inversions of σ.) The *cycles* of a permutation σ shall be understood in the usual combinatorial sense; for example, the permutation

$$\begin{aligned} [7] &\to [7], \\ i &\mapsto 8 - i \end{aligned}$$

of [7] has the four cycles $(1,7)$, $(2,6)$, $(3,5)$ and (4). (Fixed points are 1-cycles.) Note that cycles are only well-defined up to cyclic rotation; for example, $(2,6)$ and $(6,2)$ are the same cycle.

In [BucRee97], Buchstaber and Rees defined the notion of an *n-homomorphism* between commutative rings; it was studied further in [BucRee01], [BucRee04] and [KhuVor20] (among other works), although mostly only for commutative $\mathbb{Q}$-algebras. We shall here generalize it to a notion of n-homomorphisms from an arbitrary (not necessarily commutative) ring A to a commutative ring B. We define it as follows:

Definition 0.1. Let A be a ring, and let B be a commutative ring. Let $f : A \to B$ be any $\mathbb{Z}$-linear map.

(a) We say that f is *central* if we have

$$f\left(aa'\right) = f\left(a'a\right) \qquad \text{for all } a, a' \in A.$$

(b) If f is central, and if n is a nonnegative integer, then we define the $\mathbb{Z}$-multilinear map $f_n : A^n \to B$ by

$$f_n\left(a_1, a_2, \ldots, a_n\right) = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) \tag{1}$$

(we will see in a moment why this is well-defined). For example, for $n = 3$, this is saying that

$$\begin{aligned} f_3\left(a_1, a_2, a_3\right) &= f\left(a_1\right) f\left(a_2\right) f\left(a_3\right) - f\left(a_1\right) f\left(a_2 a_3\right) - f\left(a_2\right) f\left(a_1 a_3\right) \\ &\quad - f\left(a_3\right) f\left(a_1 a_2\right) + f\left(a_1 a_2 a_3\right) + f\left(a_1 a_3 a_2\right) \end{aligned}$$

(here, the first addend corresponds to the permutation $\sigma = \mathrm{id} \in S_3$ with its three cycles $(1), (2), (3)$; the second addend corresponds to the transposition $t_{2,3} \in S_3$ that swaps 2 and 3 and has two cycles (1) and $(2,3)$; the following two addends similarly correspond to the transpositions $t_{1,3}$ and $t_{1,2}$; and the last two addends correspond to the two 3-cycles in S_3).

Note that the right hand side of (1) is well-defined, since the centrality of f ensures that the value $f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right)$ does not depend on where we start indexing the cycle c (indeed, if we replace the cycle $(i_1, i_2, \ldots, i_k)$ by its cyclic rotation $\left(i_p, i_{p+1}, \ldots, i_k, i_1, i_2, \ldots, i_{p-1}\right)$, then the centrality of f shows that $f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) = f\left(a_{i_p} a_{i_{p+1}} \cdots a_{i_k} a_{i_1} a_{i_2} \cdots a_{i_{p-1}}\right)$).

The map f_n is called the *n-Frobenius map* of f. For instance, for all $a, b, c \in A$, we have

$$\begin{aligned} f_0() &= 1; \\ f_1(a) &= f(a); \\ f_2(a,b) &= f(a) f(b) - f(ab); \\ f_3(a,b,c) &= f(a) f(b) f(c) - f(a) f(bc) \\ &\qquad - f(b) f(ac) - f(c) f(ab) + f(abc) + f(acb). \end{aligned}$$

As we will soon see (Proposition 0.6), the map f_n can also be defined recursively by

$$\begin{aligned} & f_n(a_1, a_2, \ldots, a_n) \\ & = f(a_n) f_{n-1}(a_1, a_2, \ldots, a_{n-1}) \\ & \qquad - \sum_{i=1}^{n-1} f_{n-1}(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}). \end{aligned} \tag{2}$$

(c) Let n be a nonnegative integer. We say that f is an *n-homomorphism* (or *Frobenius n-homomorphism*) if f is central and satisfies $f_{n+1} = 0$ (identically).

Example 0.2. The only 0-homomorphism is the zero map. The 1-homomorphisms are just the nonunital ring homomorphisms. The 2-homomorphisms are the central maps $f : A \to B$ that satisfy

$$\begin{aligned} & f(a) f(b) f(c) - f(a) f(bc) - f(b) f(ac) - f(c) f(ab) + f(abc) + f(acb) \\ & = 0 \qquad \text{for all } a, b, c \in A. \end{aligned}$$

An example of an n-homomorphism is the trace map $\operatorname{Tr} : B^{n \times n} \to B$ from the matrix ring $B^{n \times n}$ (sending each $n \times n$-matrix to its trace). Indeed, the fact that $\operatorname{Tr}_{n+1} = 0$ on $B^{n \times n}$ is known as the *fundamental trace identity* for $n \times n$-matrices, and goes back to Frobenius; proofs can be found (e.g.) in [Laue87, Corollary], [Dotsen11, Theorem 1], [Morel19, §VII.7.3.2] or [Proces76, Theorem 4.3 (b)].

This general concept of an n-homomorphism also covers another classical notion: that of a pseudocharacter, as considered (e.g.) in [Dotsen11], [Morel19, §VII.7.3], [Bellai10, Definition 2.2], [Rouqui96], [Chenev08], generalizing the pseudorepresentations introduced by Taylor in [Taylor91] (which, in turn, were based on an idea of Wiles [Wiles88, proof of Lemma 2.2.3]). Again, much of the literature requires that A is a $\mathbb{Q}$-algebra or at least $n!$ is invertible. If we turn a blind eye to this requirement, then n-homomorphisms are more or less the same as pseudocharacters: A $\mathbb{Z}$-linear map $f : A \to B$ from a ring A to a commutative ring B is an n-homomorphism if and only if the corresponding B-linear map

$$\widetilde{f} : B \otimes_{\mathbb{Z}} A \to B,$$
$$b \otimes a \mapsto bf(a)$$

is a pseudocharacter of degree n. Conversely, a B-linear map $f : A \to B$ from a B-algebra A to its (commutative) base ring B is a pseudocharacter of degree n if and only if it is an n-homomorphism. Thus, the concept of an n-homomorphism and that of a pseudocharacter of degree n subsume each other (again ignoring the invertibility requirement). Apparently the two respective communities (pseudocharacters and n-homomorphisms) are mostly unaware of one another, even though both credit Frobenius for the original idea.

In this note, I will prove certain basic (but nontrivial) properties of n-homomorphisms in full generality, most importantly [KhuVor20, Theorem 3.2], without assuming A commutative or $n!$ invertible. The method used in [KhuVor20] becomes unusable in this generality, so one is forced to do combinatorics.

The first main result of this note is a generalization of the first part of [KhuVor20, Theorem 3.2] (also part of [Rouqui96, Lemme 2.8]):[1]

Theorem 0.3. Let A and B be two rings, with B commutative. Let $n, m \in \mathbb{N}$. Let $f : A \to B$ be an n-homomorphism, and let $g : A \to B$ be an m-homomorphism. Then, $f + g$ is an $(n+m)$-homomorphism.

In short: the sum of an n-homomorphism with an m-homomorphism is an $(n+m)$-homomorphism.

The second main result generalizes the second part of [KhuVor20, Theorem 3.2]:

Theorem 0.4. Let A, B and C be three rings, with B and C commutative. Let $n, m \in \mathbb{N}$. Let $f : B \to C$ be an n-homomorphism, and let $g : A \to B$ be an m-homomorphism. Then, $f \circ g$ is an nm-homomorphism.

In short: the composition of an n-homomorphism with an m-homomorphism is an nm-homomorphism.

The proofs will use some auxiliary results that may well be useful on their own. In particular, Theorem 0.11 is a formula for the n-Frobenius maps of a composition of two central maps; this formula was found by the GPT-5.4 LLM when I asked it for a proof of Theorem 0.4.

[1] The notation $\mathbb{N}$ denotes the set of all nonnegative integers (including 0).

Remark 0.5. It is worth mentioning the "aspirational" properties of n-homomorphisms and pseudocharacters, as they can be helpful. A pseudocharacter of degree n wishes to be the character of an n-dimensional representation of the algebra (in the sense that the latter are always instances of the former, and in some sense "generic" ones; see, e.g., [Dotsen11, Proposition 2]). An n-homomorphism wishes to be a sum of n ring homomorphisms (see [KhuVor20, §1.2]). The former wish can be fulfilled under certain restrictive conditions (see, e.g., [Morel19, §VII.7.3.4]). I don't know when and to what extent the latter can be fulfilled. However, when it can be fulfilled, Theorem 0.3 becomes obvious, and Theorem 0.4 also becomes easy (if $f : B \to C$ is a sum of n (nonunital) ring homomorphisms, and if g is an m-homomorphism, then $f \circ g$ is an nm-homomorphism, as can be easily proved using Theorem 0.3). Sadly, this approach seems to be unsuited for the generality in which we have stated the above theorems.

0.2. Recursion and explicit formula

First, I will pay a debt from Definition 0.1 **(b)**, by proving the equivalence of the two definitions of n-Frobenius maps:

Proposition 0.6. Let A be a ring, and let B be a commutative ring. Let $f : A \to B$ be a central $\mathbb{Z}$-linear map.

The recursive definition (2) of f_n (with the base case $f_0\left(\right) := 1$) is equivalent to the explicit definition (1).

Proof sketch. We use (1) as the definition of f_n. Thus, we must prove that f_n satisfies the recursion (2).

Let $n \geq 1$ and $a_1, a_2, \ldots, a_n \in A$. Then, (1) becomes

$$\begin{aligned} & f_n\left(a_1, a_2, \ldots, a_n\right) \\ & = \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) \\ & = \sum_{i=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(i) = n}} (-1)^{\sigma} \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) \end{aligned} \tag{3}$$

(since each $\sigma \in S_n$ satisfies $\sigma(i) = n$ for a unique element $i \in \{1, 2, \ldots, n\}$). We shall now rewrite the addends of the outer sum here, showing that they correspond (up to sign) to the addends on the right hand side of (2).

We start with the addend for $i = n$.

Each permutation $\tau \in S_{n-1}$ can be extended to a permutation $\widehat{\tau} \in S_n$ by setting $\widehat{\tau}(n) := n$ and $\widehat{\tau}(i) := \tau(i)$ for all $i < n$. The assignment $\tau \mapsto \widehat{\tau}$

defines a bijection from S_{n-1} to $\{\sigma \in S_n \mid \sigma(n) = n\}$. Let us use this bijection to reindex a sum:

$$\begin{aligned}
&\sum_{\substack{\sigma \in S_n;\\ \sigma(n)=n}} (-1)^{\sigma} \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\\
&= \sum_{\tau \in S_{n-1}} \underbrace{(-1)^{\widehat{\tau}}}_{\substack{=(-1)^{\tau}\\ \text{(since } \widehat{\tau} \text{ has the same}\\ \text{inversions as } \tau)}} \underbrace{\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \widehat{\tau}}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)}_{\substack{=f(a_n) \prod\limits_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \tau}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\\ \text{(since the cycles of } \widehat{\tau} \text{ are the cycles of } \tau\\ \text{plus the additional 1-cycle } (n))}}\\
&= \sum_{\tau \in S_{n-1}} (-1)^{\tau} f(a_n) \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \tau}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\\
&= f(a_n) \underbrace{\sum_{\tau \in S_{n-1}} (-1)^{\tau} \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \tau}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)}_{\substack{=f_{n-1}(a_1,a_2,\ldots,a_{n-1})\\ \text{(by the definition of } f_{n-1})}}\\
&= f(a_n) f_{n-1}(a_1,a_2,\ldots,a_{n-1}). \qquad (4)
\end{aligned}$$

Now, let $i \in \{1,2,\ldots,n-1\}$. Let us define $n-1$ elements $a'_1, a'_2, \ldots, a'_{n-1}$ of A by

$$\begin{aligned}
&\left(a'_1, a'_2, \ldots, a'_{n-1}\right)\\
&:= \left(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}\right). \qquad (5)
\end{aligned}$$

That is, we set $a'_i := a_i a_n$ and

$$a'_r := a_r \qquad \text{for all } r \neq i. \qquad (6)$$

Let $t_{i,n} \in S_n$ be the transposition that swaps i with n.

Let $\tau \in S_{n-1}$ be any permutation. Then, the permutation $\widehat{\tau} \in S_n$ (defined above) sends n to n. Hence, the permutation $\widehat{\tau} \circ t_{i,n} \in S_n$ sends $i \overset{t_{i,n}}{\mapsto} n \overset{\widehat{\tau}}{\mapsto} n$. Moreover, this permutation $\widehat{\tau} \circ t_{i,n}$ has "almost" the same cycles as τ: Namely, let

$$d = (j_1, j_2, \ldots, j_\ell)$$

be the cycle of τ that contains i, indexed in such a way that $i = j_\ell$. (If τ fixes i, then this is a 1-cycle, i.e., we have $\ell = 1$.) Then, the cycles of $\widehat{\tau} \circ t_{i,n}$ are exactly the cycles of τ, except that the cycle d is replaced by

$$d' := (j_1, j_2, \ldots, j_\ell, n).$$

(To see this, just observe that $\widehat{\tau} \circ t_{i,n}$ transforms the inputs j_ℓ and n as follows: $j_\ell = i \overset{t_{i,n}}{\mapsto} n \overset{\widehat{\tau}}{\mapsto} n$ and $n \overset{t_{i,n}}{\mapsto} i = j_\ell \overset{\widehat{\tau}}{\mapsto} j_1$. On all other inputs, $\widehat{\tau} \circ t_{i,n}$ does not differ from τ, since $t_{i,n}$ only affects the inputs i and n.) In other words, the cycles of $\widehat{\tau} \circ t_{i,n}$ are exactly the cycle $d' = (j_1, j_2, \ldots, j_\ell, n)$ and the cycles of τ distinct from d. Therefore,

$$\begin{aligned} &\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \widehat{\tau}\circ t_{i,n}}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) \\ &= f\left(a_{j_1} a_{j_2} \cdots a_{j_\ell} a_n\right) \cdot \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \tau \\ \text{distinct from } d}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right). \end{aligned} \tag{7}$$

However, for each cycle $c = (i_1, i_2, \ldots, i_k)$ of τ distinct from d, we have

$$a_{i_1} a_{i_2} \cdots a_{i_k} = a'_{i_1} a'_{i_2} \cdots a'_{i_k} \tag{8}$$

(because $c \neq d$ ensures that c does not contain i, and therefore all elements $i_1, i_2, \ldots, i_k$ of c are distinct from i and thus satisfy $a'_{i_1} = a_{i_1}$ and $a'_{i_2} = a_{i_2}$ and so on (by (6)); hence, $a'_{i_1} a'_{i_2} \cdots a'_{i_k} = a_{i_1} a_{i_2} \cdots a_{i_k}$). Meanwhile, the cycle $d = (j_1, j_2, \ldots, j_\ell)$ of τ contains i only as its last entry $j_\ell = i$, and therefore all the previous elements $j_1, j_2, \ldots, j_{\ell-1}$ of d are distinct from i and thus satisfy $a'_{j_1} = a_{j_1}$ and $a'_{j_2} = a_{j_2}$ and so on (by (6)), whereas its last entry satisfies $a'_{j_\ell} = a'_i = a_i a_n = a_{j_\ell} a_n$ (since $i = j_\ell$). Therefore,

$$a'_{j_1} a'_{j_2} \cdots a'_{j_{\ell-1}} a'_{j_\ell} = a_{j_1} a_{j_2} \cdots a_{j_{\ell-1}} a_{j_\ell} a_n = a_{j_1} a_{j_2} \cdots a_{j_\ell} a_n.$$

In other words,

$$a_{j_1} a_{j_2} \cdots a_{j_\ell} a_n = a'_{j_1} a'_{j_2} \cdots a'_{j_{\ell-1}} a'_{j_\ell} = a'_{j_1} a'_{j_2} \cdots a'_{j_\ell}. \tag{9}$$

Using (9) and (8), we can rewrite (7) as

$$\begin{aligned} &\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \widehat{\tau}\circ t_{i,n}}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right) \\ &= f\left(a'_{j_1} a'_{j_2} \cdots a'_{j_\ell}\right) \cdot \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \tau \\ \text{distinct from } d}} f\left(a'_{i_1} a'_{i_2} \cdots a'_{i_k}\right) \\ &= \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \tau}} f\left(a'_{i_1} a'_{i_2} \cdots a'_{i_k}\right). \end{aligned} \tag{10}$$

Finally,

$$(-1)^{\widehat{\tau}\circ t_{i,n}} = \underbrace{(-1)^{\widehat{\tau}}}_{\substack{=(-1)^{\tau} \\ \text{(since } \widehat{\tau} \text{ has the same} \\ \text{inversions as } \tau\text{)}}} \underbrace{(-1)^{t_{i,n}}}_{\substack{=-1 \\ \text{(since transpositions} \\ \text{have sign } -1\text{)}}} = -(-1)^{\tau}. \tag{11}$$

Forget that we fixed τ. Thus, for each permutation $\tau \in S_{n-1}$, we have constructed a permutation $\widehat{\tau} \circ t_{i,n} \in S_n$ that sends i to n and satisfies (10) and (11). Moreover, the assignment $\tau \mapsto \widehat{\tau} \circ t_{i,n}$ defines a bijection from S_{n-1} to $\{\sigma \in S_n \mid \sigma(i) = n\}$ (because if $\sigma \in S_n$ sends i to n, then $\sigma \circ t_{i,n}^{-1}$ sends n to n and thus has the form $\widehat{\tau}$ for a unique $\tau \in S_{n-1}$). Let us use this bijection to reindex a sum:

$$\begin{aligned}
&\sum_{\substack{\sigma\in S_n; \\ \sigma(i)=n}} (-1)^{\sigma} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) \\
&= \sum_{\tau\in S_{n-1}} \underbrace{(-1)^{\widehat{\tau}\circ t_{i,n}}}_{\substack{=-(-1)^{\tau} \\ \text{(by (11))}}} \underbrace{\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \widehat{\tau}\circ t_{i,n}}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)}_{\substack{= \prod\limits_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \tau}} f\left(a'_{i_1}a'_{i_2}\cdots a'_{i_k}\right) \\ \text{(by (10))}}} \\
&= -\underbrace{\sum_{\tau\in S_{n-1}} (-1)^{\tau} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \tau}} f\left(a'_{i_1}a'_{i_2}\cdots a'_{i_k}\right)}_{\substack{=f_{n-1}\left(a'_1,a'_2,\ldots,a'_{n-1}\right) \\ \text{(by the definition of } f_{n-1}\text{)}}} \\
&= -f_{n-1}\left(a'_1, a'_2, \ldots, a'_{n-1}\right) \\
&= -f_{n-1}\left(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}\right) \qquad (12)
\end{aligned}$$

(by (5)).

Forget that we fixed i. So we have proved (12) for each $i \in \{1, 2, \ldots, n-1\}$. Now, splitting off the $i = n$ addend from the outer sum on the right hand side of (3), we obtain

$$f_n(a_1, a_2, \ldots, a_n) = \underbrace{\sum_{\substack{\sigma \in S_n; \\ \sigma(n) = n}} (-1)^\sigma \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f(a_{i_1} a_{i_2} \cdots a_{i_k})}_{\substack{= f(a_n) f_{n-1}(a_1, a_2, \ldots, a_{n-1}) \\ (\text{by } (4))}}$$
$$+ \sum_{i=1}^{n-1} \underbrace{\sum_{\substack{\sigma \in S_n; \\ \sigma(i) = n}} (-1)^\sigma \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f(a_{i_1} a_{i_2} \cdots a_{i_k})}_{\substack{= -f_{n-1}(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}) \\ (\text{by } (12))}}$$
$$= f(a_n) f_{n-1}(a_1, a_2, \ldots, a_{n-1}) - \sum_{i=1}^{n-1} f_{n-1}(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}).$$

This proves (2). Thus, Proposition 0.6 is proved. □

0.3. Symmetry of n-Frobenius maps

Next, we note something simple:

Proposition 0.7. Let A be a ring, and let B be a commutative ring. Let $f : A \to B$ be a central $\mathbb{Z}$-linear map. Let $n \in \mathbb{N}$. Then, the map $f_n : A^n \to B$ is symmetric in its n inputs. That is, if $\tau \in S_n$ is any permutation and $a_1, a_2, \ldots, a_n \in A$, then

$$f_n\left(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}\right) = f_n(a_1, a_2, \ldots, a_n).$$

Proof. Let $\tau \in S_n$ and $a_1, a_2, \ldots, a_n \in A$. Then, (1) yields

$$f_n(a_1, a_2, \ldots, a_n) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f(a_{i_1} a_{i_2} \cdots a_{i_k})$$
$$= \sum_{\sigma \in S_n} (-1)^\sigma \prod_{\substack{c = (j_1, j_2, \ldots, j_k) \\ \text{is a cycle of } \sigma}} f(a_{j_1} a_{j_2} \cdots a_{j_k}) \qquad (13)$$

and

$$f_n\left(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}\right) = \sum_{\sigma \in S_n} (-1)^\sigma \prod_{\substack{c = (i_1, i_2, \ldots, i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{\tau(i_1)} a_{\tau(i_2)} \cdots a_{\tau(i_k)}\right). \qquad (14)$$

However, recall that conjugate permutations have the same cycle type. More concretely: If $\sigma \in S_n$ is any permutation, then the cycles of the permutation $\tau \circ \sigma \circ \tau^{-1}$ are in bijection with the cycles of σ: Namely, if $(i_1, i_2, \ldots, i_k)$ is a cycle of σ, then $(\tau(i_1), \tau(i_2), \ldots, \tau(i_k))$ is a cycle of $\tau \circ \sigma \circ \tau^{-1}$, and this gives a 1-to-1 correspondence between the cycles of σ and the cycles of $\tau \circ \sigma \circ \tau^{-1}$. Thus, if $\sigma \in S_n$ is any permutation, then

$$\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{\tau(i_1)} a_{\tau(i_2)} \cdots a_{\tau(i_k)}\right) = \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right).$$

Substituting this into (14), we obtain

$$\begin{aligned} & f_n\left(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}\right) \\ &= \sum_{\sigma \in S_n} \underbrace{(-1)^{\sigma}}_{\substack{=(-1)^{\tau\circ\sigma\circ\tau^{-1}} \\ \text{(since conjugate permutations} \\ \text{have the same sign)}}} \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right) \\ &= \sum_{\sigma \in S_n} (-1)^{\tau\circ\sigma\circ\tau^{-1}} \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right) \\ &= \sum_{\sigma \in S_n} (-1)^{\sigma} \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \sigma}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right) \end{aligned}$$

(here, we have substituted σ for $\tau \circ \sigma \circ \tau^{-1}$ in the sum, because conjugation by τ is a bijection from S_n onto itself). Comparing this with (13), we obtain $f_n\left(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}\right) = f_n(a_1, a_2, \ldots, a_n)$. This proves Proposition 0.7. □

The proof of Proposition 0.7 can be somewhat generalized, essentially replacing the permutation τ by a bijection between two finite sets of integers. We record the result, since it will prove useful later on:

Proposition 0.8. Let A be a ring, and let B be a commutative ring. Let $f : A \to B$ be a central $\mathbb{Z}$-linear map.

Let $U = \{u_1, u_2, \ldots, u_n\}$ be a finite set of integers (with $u_1, u_2, \ldots, u_n$ distinct). Let S_U denote the group of all permutations of U. Let a_u be an element of A for each $u \in U$. Then,

$$f_n(a_{u_1}, a_{u_2}, \ldots, a_{u_n}) = \sum_{\alpha \in S_U} (-1)^{\alpha} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \alpha}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right).$$

Proof. Let $\tau : [n] \to U$ be the map that sends each $i \in [n]$ to u_i. This map τ is a bijection (indeed, it is surjective because $U = \{u_1, u_2, \ldots, u_n\}$, and it is injective since $u_1, u_2, \ldots, u_n$ are distinct). Hence, for each permutation $\sigma \in S_n$, the composition $\tau \circ \sigma \circ \tau^{-1}$ is a permutation of U. Thus, we obtain a map

$$\begin{aligned} S_n &\to S_U, \\ \sigma &\mapsto \tau \circ \sigma \circ \tau^{-1}, \end{aligned} \tag{15}$$

which is easily seen to be a group isomorphism. Intuitively speaking, $\tau \circ \sigma \circ \tau^{-1}$ is what you obtain if you take the permutation σ of $[n]$ and rename each element $i \in [n]$ (say, in the two-line notation of σ, or in the cycle decomposition of σ) as $\tau(i)$. In particular, the cycles of the permutation $\tau \circ \sigma \circ \tau^{-1}$ (for a given $\sigma \in S_n$) are in bijection with the cycles of σ: Namely, if $(i_1, i_2, \ldots, i_k)$ is a cycle of σ, then $(\tau(i_1), \tau(i_2), \ldots, \tau(i_k))$ is a cycle of $\tau \circ \sigma \circ \tau^{-1}$, and this gives a 1-to-1 correspondence between the cycles of σ and the cycles of $\tau \circ \sigma \circ \tau^{-1}$. Thus, if $\sigma \in S_n$ is any permutation, then

$$\begin{aligned} &\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{\tau(i_1)} a_{\tau(i_2)} \cdots a_{\tau(i_k)}\right) \\ &= \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right). \end{aligned} \tag{16}$$

Moreover, if $\sigma \in S_n$ is any permutation, then

$$(-1)^{\sigma} = (-1)^{\tau\circ\sigma\circ\tau^{-1}}. \tag{17}$$

(This is easiest to see by factoring σ into a product of transpositions; see [Grinbe15, Exercise 5.12].)

But each $i \in [n]$ satisfies $a_{u_i} = a_{\tau(i)}$ (since the definition of τ yields $\tau(i) = u_i$, thus $a_{\tau(i)} = a_{u_i}$). Therefore,

$$\begin{aligned}
& f_n\left(a_{u_1}, a_{u_2}, \ldots, a_{u_n}\right) \\
&= f_n\left(a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}\right) \\
&= \sum_{\sigma \in S_n} \underbrace{(-1)^{\sigma}}_{\substack{=(-1)^{\tau\circ\sigma\circ\tau^{-1}} \\ \text{(by (17))}}} \underbrace{\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} f\left(a_{\tau(i_1)} a_{\tau(i_2)} \cdots a_{\tau(i_k)}\right)}_{\substack{= \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1}a_{j_2}\cdots a_{j_k}\right) \\ \text{(by (16))}}} \\
&\qquad \left(\text{by (1), applied to } a_{\tau(i)} \text{ instead of } a_i\right) \\
&= \sum_{\sigma \in S_n} (-1)^{\tau\circ\sigma\circ\tau^{-1}} \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \tau\circ\sigma\circ\tau^{-1}}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right) \\
&= \sum_{\alpha \in S_U} (-1)^{\alpha} \prod_{\substack{c=(j_1,j_2,\ldots,j_k) \\ \text{is a cycle of } \alpha}} f\left(a_{j_1} a_{j_2} \cdots a_{j_k}\right)
\end{aligned}$$

(here, we have substituted α for $\tau \circ \sigma \circ \tau^{-1}$ in the sum, since the map (15) is a bijection). Renaming the index $(j_1, j_2, \ldots, j_k)$ as $(i_1, i_2, \ldots, i_k)$ on the right hand side, we can rewrite this as

$$f_n\left(a_{u_1}, a_{u_2}, \ldots, a_{u_n}\right) = \sum_{\alpha \in S_U} (-1)^{\alpha} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \alpha}} f\left(a_{i_1} a_{i_2} \cdots a_{i_k}\right).$$

Thus, Proposition 0.8 is proved. □

0.4. The sum of two n-homomorphisms

The proof of Theorem 0.3 will require two lemmas:

Lemma 0.9. Let A be a ring, and let B be a commutative ring. Let $f : A \to B$ be any central $\mathbb{Z}$-linear map. Let $m \in \mathbb{N}$ be such that $f_m = 0$. Then, $f_n = 0$ for all $n \geq m$.

Proof sketch. If some positive integer n satisfies $f_{n-1} = 0$, then $f_n = 0$ as well (by the recursion (2)). Hence, Lemma 0.9 follows easily by induction on n. □

Lemma 0.10. Let A and B be two rings, with B commutative. Let $f : A \to B$ and $g : A \to B$ be two central $\mathbb{Z}$-linear maps. Let $a_1, a_2, \ldots, a_p \in A$ be some elements.

For any subset $I = \{i_1, i_2, \ldots, i_k\}$ of $[p]$ (with $i_1, i_2, \ldots, i_k$ distinct) and any central map $h : A \to B$, let us define

$$h_I(a) := h_k\left(a_{i_1}, a_{i_2}, \ldots, a_{i_k}\right) \in B.$$

(This is well-defined, i.e., does not depend on the order in which we label the elements of I as $i_1, i_2, \ldots, i_k$, because Proposition 0.7 shows that the map h_k is symmetric.)

Then,

$$(f+g)_p\left(a_1, a_2, \ldots, a_p\right) = \sum_{U \sqcup V = [p]} f_U(a) \cdot g_V(a).$$

Here, the notation "$U \sqcup V = [p]$" means that U and V are two disjoint sets whose union is $[p]$ (that is, U is a subset of $[p]$, and V is its complement in $[p]$).

Proof of Lemma 0.10 (sketched). From (1) (applied to $f+g$ and p instead of f and n), we have

$$\begin{aligned}
&(f+g)_p\left(a_1, a_2, \ldots, a_p\right) \\
&= \sum_{\sigma \in S_p} (-1)^\sigma \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} \underbrace{(f+g)\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)}_{=f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)+g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)} \\
&= \sum_{\sigma \in S_p} (-1)^\sigma \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} \left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) + g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right). \qquad (18)
\end{aligned}$$

Now, fix a permutation $\sigma \in S_p$. If we expand the product

$$\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} \left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) + g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right), \qquad (19)$$

then we obtain a sum over all ways to choose, for each cycle $c = (i_1, i_2, \ldots, i_k)$ of σ, one of the two addends of the sum $f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) + g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)$. Such "ways to choose" can be viewed as colorings of the cycles of σ, in which each cycle is either colored red (meaning that the $f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)$ addend is chosen) or colored blue (meaning that the $g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)$ addend is chosen). Thus, the expanded form of (19) can be written as follows:

$$\begin{aligned}
&\prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} \left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) + g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right) \\
&= \sum_{\substack{\text{coloring of all cycles of } \sigma \\ \text{in red and blue}}} \prod_{\substack{c=(i_1,i_2,\ldots,i_k) \\ \text{is a cycle of } \sigma}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \text{ is red;} \\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \text{ is blue.} \end{cases}
\end{aligned}$$

Equivalently, instead of coloring cycles, we can just as well color the **elements** of these cycles red and blue (viz., all elements of all red cycles are colored red, while all elements of all blue cycles are colored blue). These colorings are not arbitrary, but must have the property that each cycle is either completely red (i.e., all its elements are red) or completely blue (i.e., all its elements are blue); in other words, they must have the property that σ sends red elements to red elements and blue elements to blue elements. Thus, the above expanded form of (19) can be rewritten as follows:

$$\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)+g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)$$

$$= \sum_{\substack{\text{coloring of all elements of } [p]\\ \text{in red and blue;}\\ \sigma \text{ sends red elements to red elements}\\ \text{and blue elements to blue elements}}} \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \text{ is red;}\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \text{ is blue}\end{cases}$$

(where "c is red" means that all elements of c are red, and likewise for "blue").

Of course, a coloring of all elements of $[p]$ in red and blue is the same thing as a decomposition of $[p]$ into two disjoint subsets U and V (where U is the set of all red elements and V is the set of all blue elements); in other words, it is a choice of two sets U and V such that $U \sqcup V = [p]$. Moreover, the condition "σ sends red elements to red elements" is simply saying that $\sigma(U) \subseteq U$, whereas the condition "σ sends blue elements to blue elements" is saying that $\sigma(V) \subseteq V$. Hence, our above expanded form of (19) can be rewritten as follows:

$$\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)+g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)$$

$$= \sum_{\substack{U\sqcup V=[p];\\ \sigma(U)\subseteq U;\\ \sigma(V)\subseteq V}} \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c \subseteq V\end{cases} \qquad (20)$$

(where "$c \subseteq U$" means that all elements of c belong to U, and likewise for "$c \subseteq V$").

Forget that we fixed σ. We thus have proved (20) for each $\sigma \in S_p$. Now, (18) becomes

$$\begin{aligned}
&(f+g)_p\left(a_1,a_2,\ldots,a_p\right)\\
&=\sum_{\sigma\in S_p}(-1)^{\sigma}\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of }\sigma}}\left(f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)+g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)\\
&=\sum_{\sigma\in S_p}(-1)^{\sigma}\sum_{\substack{U\sqcup V=[p];\\ \sigma(U)\subseteq U;\\ \sigma(V)\subseteq V}}\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of }\sigma}}\begin{cases}f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq V\end{cases}\\
&\qquad\qquad(\text{by (20)})\\
&=\sum_{U\sqcup V=[p]}\sum_{\substack{\sigma\in S_p;\\ \sigma(U)\subseteq U;\\ \sigma(V)\subseteq V}}(-1)^{\sigma}\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of }\sigma}}\begin{cases}f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq V\end{cases}
\end{aligned}\tag{21}$$

(here, we have interchanged the two summation signs).

Now, fix a decomposition $U\sqcup V=[p]$ of the set $[p]$ into two disjoint subsets U and V. Then, any permutation $\sigma\in S_p$ satisfying $\sigma(U)\subseteq U$ and $\sigma(V)\subseteq V$ can be "decomposed" into a pair (α,β) consisting of a permutation $\alpha:=\sigma\mid_U$ of U and a permutation $\beta:=\sigma\mid_V$ of V. To put it more formally: There is a bijection

from $\left\{\text{permutations } \sigma\in S_p \text{ satisfying } \sigma(U)\subseteq U \text{ and } \sigma(V)\subseteq V\right\}$
to $S_U\times S_V$

(where S_X denotes the group of permutations of any set X) that sends each σ to $(\alpha,\beta):=(\sigma\mid_U,\ \sigma\mid_V)$. Moreover, the cycles of the former permutation σ are simply the cycles of the two "component" permutations α and β, and it is easy to see that the sign of σ is given by

$$(-1)^{\sigma}=(-1)^{\alpha}(-1)^{\beta}$$

(this follows, e.g., by writing α and β as products of transpositions). Hence,

$$\begin{aligned}
&\sum_{\substack{\sigma\in S_p;\\ \sigma(U)\subseteq U;\\ \sigma(V)\subseteq V}} (-1)^\sigma \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq V\end{cases}\\
&= \sum_{(\alpha,\beta)\in S_U\times S_V} (-1)^\alpha (-1)^\beta \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \alpha \text{ or of } \beta}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq V\end{cases}\\
&= \sum_{(\alpha,\beta)\in S_U\times S_V} (-1)^\alpha (-1)^\beta \left(\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \alpha}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)\\
&\qquad \left(\prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \beta}} g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)\\
&= \left(\sum_{\alpha\in S_U} (-1)^\alpha \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \alpha}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right)\\
&\qquad \left(\sum_{\beta\in S_V} (-1)^\beta \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \beta}} g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right)\right). \qquad (22)
\end{aligned}$$

However, if we write the set U in the form $U=\{u_1,u_2,\ldots,u_r\}$ (with $u_1,u_2,\ldots,u_r$ distinct), then

$$\begin{aligned}
f_U(a) &= f_r\left(a_{u_1},a_{u_2},\ldots,a_{u_r}\right) \qquad \text{(by the definition of } f_U\text{)}\\
&= \sum_{\alpha\in S_U} (-1)^\alpha \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \alpha}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) \qquad (23)
\end{aligned}$$

(by Proposition 0.8, applied to r instead of n). Thus, we have shown that

$$\sum_{\alpha\in S_U} (-1)^\alpha \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \alpha}} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) = f_U(a).$$

Similarly,

$$\sum_{\beta\in S_V} (-1)^\beta \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \beta}} g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right) = g_V(a).$$

Substituting these two equalities into (22), we obtain

$$\sum_{\substack{\sigma\in S_p;\\ \sigma(U)\subseteq U;\\ \sigma(V)\subseteq V}} (-1)^\sigma \prod_{\substack{c=(i_1,i_2,\ldots,i_k)\\ \text{is a cycle of } \sigma}} \begin{cases} f\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq U;\\ g\left(a_{i_1}a_{i_2}\cdots a_{i_k}\right), & \text{if } c\subseteq V \end{cases}$$
$$= f_U(a)\cdot g_V(a). \qquad (24)$$

Now forget that we fixed the decomposition $U\sqcup V=[p]$. Now, substituting (24) into (21), we obtain

$$(f+g)_p\left(a_1,a_2,\ldots,a_p\right) = \sum_{U\sqcup V=[p]} f_U(a)\cdot g_V(a).$$

This proves Lemma 0.10. □

Proof of Theorem 0.3 (sketched). The map f is central (being an n-homomorphism). Similarly, g is central. Thus, it is easy to see that $f+g$ is central. It remains to show that $(f+g)_{n+m+1}=0$.

Let $p:=n+m+1$. Let $a_1,a_2,\ldots,a_p\in A$. Then, Lemma 0.10 yields

$$(f+g)_p\left(a_1,a_2,\ldots,a_p\right) = \sum_{U\sqcup V=[p]} f_U(a)\cdot g_V(a), \qquad (25)$$

where the notations are as defined in Lemma 0.10.

Now, fix any decomposition $U\sqcup V=[p]$ of $[p]$ into two disjoint subsets U and V. We shall show that

$$f_U(a)\cdot g_V(a)=0. \qquad (26)$$

[*Proof:* From $U\sqcup V=[p]$, we obtain

$$|U|+|V| = |U\sqcup V| = |[p]| = p = n+m+1 > n+m.$$

Hence, we must have $|U|>n$ or $|V|>m$ (since otherwise, we would have both $|U|\leq n$ and $|V|\leq m$, and therefore we could add these two inequalities together and obtain $|U|+|V|\leq n+m$, which would contradict $|U|+|V|>n+m$). We WLOG assume that $|U|>n$ (since the $|V|>m$ case is analogous). Thus, $|U|\geq n+1$. But $f_{n+1}=0$ (since f is an n-homomorphism). Hence, Lemma 0.9 (applied to $|U|$ and $n+1$ instead of n and m) yields $f_{|U|}=0$ (since $|U|\geq n+1$). Now, let us write the set U in the form $U=\{u_1,u_2,\ldots,u_r\}$ (with $u_1,u_2,\ldots,u_r$ distinct). Then, $r=|U|$ and therefore $f_r=f_{|U|}=0$. But the definition of f_U (see Lemma 0.10) yields

$$f_U(a) = \underbrace{f_r}_{=0}\left(a_{u_1},a_{u_2},\ldots,a_{u_r}\right)=0.$$

Hence, $f_U(a) \cdot g_V(a) = 0 \cdot g_V(a) = 0$. This proves (26).]

Forget that we fixed the decomposition $U \sqcup V = [p]$. We have thus shown that (26) holds for each such decomposition. In other words, all addends on the right hand side of (25) are 0. Hence, the whole right hand side is 0, and so we can rewrite (25) as

$$(f+g)_p (a_1, a_2, \ldots, a_p) = 0.$$

Since $a_1, a_2, \ldots, a_p$ were chosen arbitrarily, this proves that $(f+g)_p = 0$. In other words, $(f+g)_{n+m+1} = 0$ (since $p = n+m+1$). This completes the proof of Theorem 0.3. □

0.5. The composition formula

Next, we introduce some notations. A *set partition* (henceforth just *partition*) of a finite set J means a set $\{J_1, J_2, \ldots, J_k\}$ of disjoint nonempty subsets of J whose union is $J_1 \cup J_2 \cup \cdots \cup J_k = J$. These subsets $J_1, J_2, \ldots, J_k$ are called the *blocks* of the partition. For instance, the five partitions of [3] are[2]

$$\begin{gathered} \{\{1,2,3\}\} \qquad (\text{with 1 block}) \qquad \text{and} \\ \{\{1,2\},\{3\}\} \text{ and } \{\{1,3\},\{2\}\} \text{ and } \{\{2,3\},\{1\}\} \\ (\text{with 2 blocks each}) \qquad \text{and} \\ \{\{1\},\{2\},\{3\}\} \qquad (\text{with 3 blocks}). \end{gathered}$$

Note that $\{\{1,3\},\{2\}\}$ and $\{\{2\},\{3,1\}\}$ are the same partition. We let Π_J denote the set of all partitions of the finite set J. Note that the empty set $\varnothing$ has a unique partition, which has 0 blocks; that is, $\Pi_\varnothing = \{\varnothing\}$.

Let us agree to always write partitions with their blocks distinct: e.g., when we say "$\{P_1, P_2, \ldots, P_k\} \in \Pi_J$", we shall understand that $P_1, P_2, \ldots, P_k$ are distinct.

The following formula (discovered by GPT-5.4) will be crucial to our proof of Theorem 0.4:

Theorem 0.11. Let A, B and C be three rings, with B and C commutative. Let $g : A \to B$ and $f : B \to C$ be two central $\mathbb{Z}$-linear maps. Let $h := f \circ g : A \to C$. Let $a_1, a_2, \ldots, a_n \in A$. For any subset $P = \{p_1, p_2, \ldots, p_r\}$ of $[n]$ (with $p_1, p_2, \ldots, p_r$ distinct), we set

$$b_P := g_r (a_{p_1}, a_{p_2}, \ldots, a_{p_r}). \tag{27}$$

(This is well-defined, i.e., does not depend on the order in which we label the elements of P as $p_1, p_2, \ldots, p_r$, because Proposition 0.7 shows that the map g_r is symmetric.) Then,

$$h_n (a_1, a_2, \ldots, a_n) = \sum_{\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[n]}} f_k (b_{P_1}, b_{P_2}, \ldots, b_{P_k}).$$

[2]Recall that for any integer $r \geq 0$, we let $[r]$ denote the set $\{1, 2, \ldots, r\}$.

(The expression $f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right)$ here is well-defined, i.e., does not depend on the order in which we label the blocks of π as $P_1, P_2, \ldots, P_k$, because Proposition 0.7 shows that the map f_k is symmetric.)

Example 0.12. Let us set $n = 3$ in Theorem 0.11. Then, the theorem says that

$$\begin{aligned}
& h_3\left(a_1, a_2, a_3\right) \\
& = \sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[3]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \\
& = f_1\left(b_{\{1,2,3\}}\right) + f_2\left(b_{\{1,2\}}, b_{\{3\}}\right) + f_2\left(b_{\{1,3\}}, b_{\{2\}}\right) \\
& \qquad + f_2\left(b_{\{2,3\}}, b_{\{1\}}\right) + f_3\left(b_{\{1\}}, b_{\{2\}}, b_{\{3\}}\right) \\
& = f_1\left(g_3\left(a_1, a_2, a_3\right)\right) + f_2\left(g_2\left(a_1, a_2\right), g_1\left(a_3\right)\right) + f_2\left(g_2\left(a_1, a_3\right), g_1\left(a_2\right)\right) \\
& \qquad + f_2\left(g_2\left(a_2, a_3\right), g_1\left(a_1\right)\right) + f_3\left(g_1\left(a_1\right), g_1\left(a_2\right), g_1\left(a_3\right)\right).
\end{aligned}$$

Proof of Theorem 0.11. I would welcome an inclusion/exclusion argument using cycles of permutations, but GPT-5.4 suggests an induction proof instead, and that shall do.

We induct on n.

Base case: For $n = 0$, the claim of Theorem 0.11 is saying that $h_0() = f_0()$ (since $\Pi_{[0]} = \Pi_\varnothing = \{\varnothing\}$), which is clear because both sides equal 1.

Strictly speaking, this is enough to complete the base case, but let us also check the $n = 1$ case.

For $n = 1$, the claim of Theorem 0.11 is saying that $h_1\left(a_1\right) = f_1\left(b_{\{1\}}\right)$. Since $f_1 = f$ and $h_1 = h$ and $b_{\{1\}} = g_1\left(a_1\right) = g\left(a_1\right)$, this boils down to $h\left(a_1\right) = f\left(g\left(a_1\right)\right)$, which follows from $h = f \circ g$. Thus, the base case is proved.

Induction step: Let $n \geq 2$. Assume (as induction hypothesis) that Theorem 0.11 holds for $n - 1$ instead of n. We must now prove it for n.

The induction hypothesis yields

$$h_{n-1}\left(a_1, a_2, \ldots, a_{n-1}\right) = \sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n-1]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right). \tag{28}$$

Moreover, for each $i \in [n-1]$, we define $n - 1$ elements $a_1^{(i)}, a_2^{(i)}, \ldots, a_{n-1}^{(i)}$ of A by

$$\begin{aligned}
& \left(a_1^{(i)}, a_2^{(i)}, \ldots, a_{n-1}^{(i)}\right) \\
& := \left(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}\right)
\end{aligned} \tag{29}$$

(these are what we called $a'_1, a'_2, \ldots, a'_{n-1}$ in (5)), and then the induction hypothesis (applied to these $n - 1$ elements) yields

$$h_{n-1}\left(a_1^{(i)}, a_2^{(i)}, \ldots, a_{n-1}^{(i)}\right) = \sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n-1]}} f_k\left(b_{P_1}^{(i)}, b_{P_2}^{(i)}, \ldots, b_{P_k}^{(i)}\right), \tag{30}$$

where for any subset $P = \{p_1, p_2, \ldots, p_r\}$ of $[n-1]$ (with $p_1, p_2, \ldots, p_r$ distinct), we set

$$b_P^{(i)} := g_r \left(a_{p_1}^{(i)}, a_{p_2}^{(i)}, \ldots, a_{p_r}^{(i)} \right). \tag{31}$$

Note that if P is a subset of $[n-1]$ and if $i \in [n-1]$ is such that $i \notin P$, then

$$b_P = b_P^{(i)}. \tag{32}$$

(Indeed, let P be a subset of $[n-1]$, and let $i \in [n-1]$ be such that $i \notin P$. Then, writing P as $P = \{p_1, p_2, \ldots, p_r\}$ (with $p_1, p_2, \ldots, p_r$ distinct), we see that each $k \in [r]$ satisfies $p_k \neq i$ (since $i \notin P = \{p_1, p_2, \ldots, p_r\}$) and therefore $a_{p_k}^{(i)} = a_{p_k}$ (since (29) shows that $a_j^{(i)} = a_j$ for all $j \neq i$). Hence, the right hand side of (31) equals the right hand side of (27). Therefore, the same holds for the left hand sides as well. In other words, we have $b_P^{(i)} = b_P$. This proves (32).)

Note also that (27) yields $b_{\{n\}} = g_1(a_n) = g(a_n)$.

Next, we observe that each subset P of $[n-1]$ satisfies

$$b_{P \cup \{n\}} = b_P b_{\{n\}} - \sum_{i \in P} b_P^{(i)}. \tag{33}$$

(Indeed, let P be a subset of $[n-1]$. Write P as $P = \{p_1, p_2, \ldots, p_r\}$ (with $p_1, p_2, \ldots, p_r$ distinct). Then $P \cup \{n\} = \{p_1, p_2, \ldots, p_r, n\}$ (with $p_1, p_2, \ldots, p_r, n$ distinct because $P \subseteq [n-1]$), hence

$$b_{P \cup \{n\}} = g_{r+1} \left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}, a_n \right) \qquad \text{(by (27))}. \tag{34}$$

But each $i \in [r]$ satisfies

$$\begin{aligned} b_P^{(p_i)} &= g_r \underbrace{\left(a_{p_1}^{(p_i)}, a_{p_2}^{(p_i)}, \ldots, a_{p_r}^{(p_i)} \right)}_{\substack{= \left(a_{p_1}, a_{p_2}, \ldots, a_{p_{i-1}}, a_{p_i} a_n, a_{p_{i+1}}, a_{p_{i+2}}, \ldots, a_{p_r} \right) \\ \text{(indeed, all } k \neq i \text{ satisfy } p_k \neq p_i \text{ (since } p_1, p_2, \ldots, p_r \text{ are distinct)} \\ \text{and thus } a_{p_k}^{(p_i)} = a_{p_k} \text{ (by (29)),} \\ \text{whereas } a_{p_i}^{(p_i)} = a_{p_i} a_n \text{ (again by (29)))}}} \qquad \text{(by (31))} \\ &= g_r \left(a_{p_1}, a_{p_2}, \ldots, a_{p_{i-1}}, a_{p_i} a_n, a_{p_{i+1}}, a_{p_{i+2}}, \ldots, a_{p_r} \right). \end{aligned} \tag{35}$$

Now, the recursion (2) (applied to g, $r+1$ and $\left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}, a_n \right)$ instead of f,

n and $(a_1, a_2, \ldots, a_n)$) yields

$$\begin{aligned} & g_{r+1}\left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}, a_n\right) \\ & = \underbrace{g\left(a_n\right)}_{=b_{\{n\}}} \underbrace{g_r\left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}\right)}_{=b_P} \\ & \qquad - \sum_{i=1}^{r} \underbrace{g_r\left(a_{p_1}, a_{p_2}, \ldots, a_{p_{i-1}}, a_{p_i} a_n, a_{p_{i+1}}, a_{p_{i+2}}, \ldots, a_{p_r}\right)}_{\substack{=b_P^{(p_i)} \\ \text{(by (35))}}} \\ & = b_{\{n\}} b_P - \sum_{i=1}^{r} b_P^{(p_i)} = b_{\{n\}} b_P - \sum_{j \in P} b_P^{(j)} \end{aligned}$$

(here, we have substituted j for p_i in the sum, since $P = \{p_1, p_2, \ldots, p_r\}$ with $p_1, p_2, \ldots, p_r$ distinct). Thus, we can rewrite (34) as

$$b_{P \cup \{n\}} = \underbrace{b_{\{n\}} b_P}_{\substack{=b_P b_{\{n\}} \\ \text{(since } B \text{ is} \\ \text{commutative)}}} - \underbrace{\sum_{j \in P} b_P^{(j)}}_{= \sum_{i \in P} b_P^{(i)}} = b_P b_{\{n\}} - \sum_{i \in P} b_P^{(i)}.$$

This proves (33).)

Let del : $\Pi_{[n]} \to \Pi_{[n-1]}$ be the map that transforms each partition π of $[n]$ into a partition of $[n-1]$ by deleting the element n from the block of π that contains it (and deleting this block if it becomes empty). For instance, for $n = 4$, we have

$$\operatorname{del}\left(\{\{1,4\}, \{2,3\}\}\right) = \{\{1\}, \{2,3\}\} \qquad \text{and}$$
$$\operatorname{del}\left(\{\{1\}, \{2,3\}, \{4\}\}\right) = \{\{1\}, \{2,3\}\}.$$

Thus, we can split the sum on the right hand side of Theorem 0.11 as follows:

$$\begin{aligned} & \sum_{\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[n]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \\ & = \sum_{\omega = \{Q_1, Q_2, \ldots, Q_\ell\} \in \Pi_{[n-1]}} \ \sum_{\substack{\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[n]}; \\ \operatorname{del}(\pi) = \omega}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right). \end{aligned} \tag{36}$$

Now, fix a partition $\omega = \{Q_1, Q_2, \ldots, Q_\ell\} \in \Pi_{[n-1]}$.

Which partitions $\pi \in \Pi_{[n]}$ satisfy $\operatorname{del}(\pi) = \omega$? In other words, which partitions of $[n]$ become ω after we remove the element n (and the block that contains it, in case it becomes empty)? Stated this way, the question is trivial: those partitions that can be obtained from ω either by adding a new block $\{n\}$ or by inserting n into one of the existing blocks $Q_1, Q_2, \ldots, Q_\ell$. Thus, there are precisely $\ell + 1$ partitions $\pi \in \Pi_{[n]}$ that satisfy $\operatorname{del}(\pi) = \omega$: namely, the one partition

$$\{Q_1, Q_2, \ldots, Q_\ell, \{n\}\}$$

and the ℓ partitions

$$\left\{Q_1, Q_2, \ldots, Q_j \cup \{n\}, \ldots, Q_\ell\right\} \qquad \text{for } j \in [\ell]$$

(the notation "$Q_1, Q_2, \ldots, Q_j \cup \{n\}, \ldots, Q_\ell$" means "take the list $Q_1, Q_2, \ldots, Q_\ell$ and replace its j-th entry by $Q_j \cup \{n\}$"). Hence,

$$\begin{aligned} &\sum_{\substack{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n]};\\ \operatorname{del}(\pi)=\omega}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \\ &= f_{\ell+1}\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_\ell}, b_{\{n\}}\right) \\ &\qquad + \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}\right) \end{aligned} \tag{37}$$

(where "$b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}$" means "take the list $b_{Q_1}, b_{Q_2}, \ldots, b_{Q_\ell}$ and replace its j-th entry by $b_{Q_j \cup \{n\}}$").

Now, let $j \in [\ell]$. Then, $Q_j \subseteq [n-1]$ (since Q_j is a block of $\omega \in \Pi_{[n-1]}$) and thus

$$b_{Q_j \cup \{n\}} = b_{Q_j} b_{\{n\}} - \sum_{i \in Q_j} b^{(i)}_{Q_j}$$

(by (33), applied to $P = Q_j$). Hence,

$$\begin{aligned} &f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}\right) \\ &= f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}} - \sum_{i \in Q_j} b^{(i)}_{Q_j}, \ldots, b_{Q_\ell}\right) \\ &= f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \\ &\qquad - \sum_{i \in Q_j} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b^{(i)}_{Q_j}, \ldots, b_{Q_\ell}\right) \end{aligned} \tag{38}$$

(since the map f_ℓ is $\mathbb{Z}$-multilinear and thus, in particular, linear in its j-th argument). Moreover, for each $k \in [\ell] \setminus \{j\}$ and each $i \in Q_j$, we have $Q_k \cap Q_j = \varnothing$ (since ω is a set partition, so that its blocks are disjoint) and thus $i \notin Q_k$ (since $i \in Q_j$) and therefore $b_{Q_k} = b^{(i)}_{Q_k}$ (by (32), applied to $P = Q_k$). Hence, in the sum on the right hand side of (38), we can replace each b_{Q_k} by $b^{(i)}_{Q_k}$. Thus, (38) rewrites as

$$
\begin{aligned}
& f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}\right) \\
& = f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \\
& \qquad - \sum_{i \in Q_j} f_\ell \underbrace{\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_j}, \ldots, b^{(i)}_{Q_\ell}\right)}_{=\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_\ell}\right)} \\
& = f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \\
& \qquad - \sum_{i \in Q_j} f_\ell\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_\ell}\right). \qquad (39)
\end{aligned}
$$

Forget that we fixed j. Summing the equality (39) over all $j \in [\ell]$, we find

$$
\begin{aligned}
& \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}\right) \\
& = \sum_{j=1}^{\ell} \left(f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \right. \\
& \qquad \left. - \sum_{i \in Q_j} f_\ell\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_\ell}\right) \right) \\
& = \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \\
& \qquad - \sum_{j=1}^{\ell} \sum_{i \in Q_j} f_\ell\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_\ell}\right). \qquad (40)
\end{aligned}
$$

In this equality, we can replace the two summation signs $\sum\limits_{j=1}^{\ell} \sum\limits_{i \in Q_j}$ by $\sum\limits_{i=1}^{n-1}$ (since the sets $Q_1, Q_2, \ldots, Q_\ell$ form a set partition of $[n-1]$, so that each $i \in [n-1]$ appears in exactly one of these sets). Thus, this equality simplifies to

$$
\begin{aligned}
& \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j \cup \{n\}}, \ldots, b_{Q_\ell}\right) \\
& = \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_j} b_{\{n\}}, \ldots, b_{Q_\ell}\right) \\
& \qquad - \sum_{i=1}^{n-1} f_\ell\left(b^{(i)}_{Q_1}, b^{(i)}_{Q_2}, \ldots, b^{(i)}_{Q_\ell}\right). \qquad (41)
\end{aligned}
$$

Substituting this into (37), we find

$$\begin{aligned}
&\sum_{\substack{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n]};\\ \operatorname{del}(\pi)=\omega}} f_k\left(b_{P_1},b_{P_2},\ldots,b_{P_k}\right)\\
&= f_{\ell+1}\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell},b_{\{n\}}\right)\\
&\qquad + \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_j}b_{\{n\}},\ldots,b_{Q_\ell}\right)\\
&\qquad - \sum_{i=1}^{n-1} f_\ell\left(b^{(i)}_{Q_1},b^{(i)}_{Q_2},\ldots,b^{(i)}_{Q_\ell}\right). \qquad (42)
\end{aligned}$$

However, the recursion (2) (applied to $\ell+1$ and $\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell},b_{\{n\}}\right)$ instead of n and $(a_1,a_2,\ldots,a_n)$) yields

$$\begin{aligned}
&f_{\ell+1}\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell},b_{\{n\}}\right)\\
&= f\left(b_{\{n\}}\right) f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell}\right)\\
&\qquad - \sum_{i=1}^{\ell} f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_i}b_{\{n\}},\ldots,b_{Q_\ell}\right)\\
&= f\left(b_{\{n\}}\right) f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell}\right)\\
&\qquad - \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_j}b_{\{n\}},\ldots,b_{Q_\ell}\right).
\end{aligned}$$

In other words,

$$\begin{aligned}
&f_{\ell+1}\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell},b_{\{n\}}\right)\\
&\qquad + \sum_{j=1}^{\ell} f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_j}b_{\{n\}},\ldots,b_{Q_\ell}\right)\\
&= f\left(b_{\{n\}}\right) f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell}\right).
\end{aligned}$$

Substituting this into (42), we obtain

$$\begin{aligned}
&\sum_{\substack{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n]};\\ \operatorname{del}(\pi)=\omega}} f_k\left(b_{P_1},b_{P_2},\ldots,b_{P_k}\right)\\
&= f\left(b_{\{n\}}\right) f_\ell\left(b_{Q_1},b_{Q_2},\ldots,b_{Q_\ell}\right)\\
&\qquad - \sum_{i=1}^{n-1} f_\ell\left(b^{(i)}_{Q_1},b^{(i)}_{Q_2},\ldots,b^{(i)}_{Q_\ell}\right). \qquad (43)
\end{aligned}$$

Forget that we fixed ω. So we have proved (43) for each partition $\omega = \{Q_1, Q_2, \ldots, Q_\ell\} \in \Pi_{[n-1]}$. Now, (36) becomes

$$\begin{aligned}
&\sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \\
&= \sum_{\omega=\{Q_1,Q_2,\ldots,Q_\ell\}\in\Pi_{[n-1]}} \sum_{\substack{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n]};\\ \operatorname{del}(\pi)=\omega}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \\
&= \sum_{\omega=\{Q_1,Q_2,\ldots,Q_\ell\}\in\Pi_{[n-1]}} \left(f\left(b_{\{n\}}\right) f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_\ell}\right) \right. \\
&\qquad \left. - \sum_{i=1}^{n-1} f_\ell\left(b_{Q_1}^{(i)}, b_{Q_2}^{(i)}, \ldots, b_{Q_\ell}^{(i)}\right) \right) \qquad \text{(by (43))} \\
&= f\left(\underbrace{b_{\{n\}}}_{=g(a_n)}\right) \underbrace{\sum_{\omega=\{Q_1,Q_2,\ldots,Q_\ell\}\in\Pi_{[n-1]}} f_\ell\left(b_{Q_1}, b_{Q_2}, \ldots, b_{Q_\ell}\right)}_{\substack{=\sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n-1]}} f_k\left(b_{P_1},b_{P_2},\ldots,b_{P_k}\right) \\ =h_{n-1}(a_1,a_2,\ldots,a_{n-1}) \\ \text{(by (28))}}} \\
&\qquad - \sum_{i=1}^{n-1} \underbrace{\sum_{\omega=\{Q_1,Q_2,\ldots,Q_\ell\}\in\Pi_{[n-1]}} f_\ell\left(b_{Q_1}^{(i)}, b_{Q_2}^{(i)}, \ldots, b_{Q_\ell}^{(i)}\right)}_{\substack{=\sum_{\pi=\{P_1,P_2,\ldots,P_k\}\in\Pi_{[n-1]}} f_k\left(b_{P_1}^{(i)},b_{P_2}^{(i)},\ldots,b_{P_k}^{(i)}\right) \\ =h_{n-1}\left(a_1^{(i)},a_2^{(i)},\ldots,a_{n-1}^{(i)}\right) \\ \text{(by (30))}}} \\
&= \underbrace{f\left(g\left(a_n\right)\right)}_{\substack{=h(a_n) \\ \text{(since } f\circ g=h)}} h_{n-1}\left(a_1, a_2, \ldots, a_{n-1}\right) \\
&\qquad - \sum_{i=1}^{n-1} h_{n-1} \underbrace{\left(a_1^{(i)}, a_2^{(i)}, \ldots, a_{n-1}^{(i)}\right)}_{\substack{=(a_1,a_2,\ldots,a_{i-1},a_ia_n,a_{i+1},a_{i+2},\ldots,a_{n-1}) \\ \text{(by (29))}}} \\
&= h\left(a_n\right) h_{n-1}\left(a_1, a_2, \ldots, a_{n-1}\right) \\
&\qquad - \sum_{i=1}^{n-1} h_{n-1}\left(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}\right).
\end{aligned}$$

On the other hand, the recursion (2) yields

$$\begin{aligned}
&h_n\left(a_1, a_2, \ldots, a_n\right) \\
&= h\left(a_n\right) h_{n-1}\left(a_1, a_2, \ldots, a_{n-1}\right) \\
&\qquad - \sum_{i=1}^{n-1} h_{n-1}\left(a_1, a_2, \ldots, a_{i-1}, a_i a_n, a_{i+1}, a_{i+2}, \ldots, a_{n-1}\right).
\end{aligned}$$

Comparing these two equalities, we find

$$h_n\left(a_1, a_2, \ldots, a_n\right) = \sum_{\pi=\{P_1, P_2, \ldots, P_k\} \in \Pi_{[n]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right).$$

This is precisely Theorem 0.11 for our n. So we have finished the induction step, and thus the proof of Theorem 0.11. □

0.6. The composition of n-homomorphisms

Proof of Theorem 0.4. Let $h := f \circ g : A \to C$. Thus, we must show that h is an nm-homomorphism. In other words, we must show that h is central and satisfies $h_{nm+1} = 0$.

Since g is central, it is easy to see that h is central as well (indeed, all $a, a' \in A$ satisfy

$$\begin{aligned}
h\left(aa'\right) &= f\left(g\left(aa'\right)\right) && \left(\text{since } h = f \circ g\right) \\
&= f\left(g\left(a'a\right)\right) && \left(\text{since } g \text{ is central, so } g\left(aa'\right) = g\left(a'a\right)\right) \\
&= h\left(a'a\right) && \left(\text{since } h = f \circ g\right),
\end{aligned}$$

which shows that h is central). Thus, it remains to prove that $h_{nm+1} = 0$.

Set $N := nm + 1$. Let $a_1, a_2, \ldots, a_N \in A$. We shall prove that $h_N\left(a_1, a_2, \ldots, a_N\right) = 0$.

For any subset $P = \{p_1, p_2, \ldots, p_r\}$ of $[N]$ (with $p_1, p_2, \ldots, p_r$ distinct), we set

$$b_P := g_r\left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}\right).$$

(This is well-defined for the same reason as in Theorem 0.11.) Then, Theorem 0.11 (applied to N instead of n) shows that

$$h_N\left(a_1, a_2, \ldots, a_N\right) = \sum_{\pi=\{P_1, P_2, \ldots, P_k\} \in \Pi_{[N]}} f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) \tag{44}$$

(where $f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right)$ is well-defined for the same reason as in Theorem 0.11).

However, we claim that any partition $\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[N]}$ satisfies

$$f_k\left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) = 0. \tag{45}$$

[*Proof:* Let $\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[N]}$ be any partition. Since f is an n-homomorphism, we have $f_{n+1} = 0$. Thus, if $k \geq n+1$, then $f_k = 0$ as well (by Lemma 0.9, applied to B, C, $n+1$ and k instead of A, B, m and n), and therefore (45) certainly holds in this case. Hence, for the rest of this proof of (45), we WLOG assume that $k < n+1$. Therefore, $k \leq n$, so that $n \geq k$. Now, since $\{P_1, P_2, \ldots, P_k\}$ is a partition of $[N]$, we have

$$|P_1| + |P_2| + \cdots + |P_k| = |[N]| = N = nm + 1 > \underbrace{n}_{\geq k} m \geq km.$$

Hence, at least one of the k addends $|P_1|, |P_2|, \ldots, |P_k|$ must be larger than m (because otherwise, we would have $|P_1| \leq m$ and $|P_2| \leq m$ and ... and $|P_k| \leq m$, and therefore, adding these k inequalities together, we would obtain $|P_1| + |P_2| + \cdots + |P_k| \leq \underbrace{m + m + \cdots + m}_{k \text{ times}} = km$, which would contradict $|P_1| + |P_2| + \cdots + |P_k| > km$). In other words, there exists some $j \in [k]$ such that $|P_j| > m$. Consider this j. Now, recall that g is an m-homomorphism; thus, $g_{m+1} = 0$. Write the set P_j as $P_j = \{p_1, p_2, \ldots, p_r\}$ (with $p_1, p_2, \ldots, p_r$ distinct); thus, $r = |P_j| > m$. Therefore, $r \geq m+1$. Hence, from $g_{m+1} = 0$, we obtain $g_r = 0$ (by Lemma 0.9, applied to g, $m+1$ and r instead of f, m and n).

But the definition of b_{P_j} yields $b_{P_j} = g_r \left(a_{p_1}, a_{p_2}, \ldots, a_{p_r}\right) = 0$ (since $g_r = 0$). Thus, $f_k \left(b_{P_1}, b_{P_2}, \ldots, b_{P_k}\right) = 0$ as well (since f_k is a $\mathbb{Z}$-multilinear map, and thus vanishes if any of the k inputs is 0). This proves (45).]

Now, substituting (45) into (44), we find

$$h_N \left(a_1, a_2, \ldots, a_N\right) = \sum_{\pi = \{P_1, P_2, \ldots, P_k\} \in \Pi_{[N]}} 0 = 0.$$

Since we have proved this for all $a_1, a_2, \ldots, a_N \in A$, we thus obtain $h_N = 0$. In other words, $h_{nm+1} = 0$ (since $N = nm+1$). As we said, this completes the proof of Theorem 0.4. □

References

[Bellai10] Joel Bellaiche, *Ribet's lemma, generalizations, and pseudocharacters*, 2010.
`https://people.brandeis.edu/~jbellaic/RibetHawaii3.pdf`

[BucRee97] V. M. Buchstaber, E. G. Rees, *Frobenius k-characters and n-ring homomorphisms*, Russian Math. Surveys (Uspekhi Mat. Nauk) **52** (1997), issue 2, pp. 159–160.

[BucRee01] V. M. Buchstaber, E. G. Rees, *The Gelfand map and symmetric products*, Selecta Mathematica 8 (2002), pp. 523–535. A preprint is available at arXiv:0109122v1.

[BucRee04] V. M. Buchstaber, E. G. Rees, *Rings of continuous functions, symmetric products, and Frobenius algebras*, Russian Math. Surveys **59** (2004), issue 1, pp. 125–145. A preprint is available at arXiv:math/0403357v1.

[Chenev08] Gaetan Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, arXiv:0809.0415v2.

[Dotsen11] Vladimir Dotsenko, *Pseudo-characters (an extended discussion of §7 in Mazur's paper)*, 2011.
`https://www.maths.tcd.ie/~vdots/research/files/Pseudo-characters.pdf`

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022, arXiv:2008.09862v3.

[KhuVor20] H. M. Khudaverdian, Th. Th. Voronov, *On the Buchstaber–Rees theory of "Frobenius n-homomorphisms" and its generalization*, arXiv:2002.02395v2.

[Laue87] Hartmut Laue, *A graph theoretic proof of the fundamental trace identity*, Discrete Math. **69** (1988), pp. 197–198.
A digitized version is available at `https://www.cip.ifi.lmu.de/~grinberg/algebra/laue-fundid.pdf` .

[Morel19] Sophie Morel, *Representation theory*, 2019.
`https://web.math.princeton.edu/~smorel/rep_theory_notes.pdf`

[Proces76] C. Procesi, *The invariant theory of $n \times n$ matrices*, Adv. in Math. **19** (1976), pp. 306–381.

[Rouqui96] Raphaël Rouquier, *Caractérisation des caractères et Pseudo-caractères*, Journal of Algebra **180** (1996), Issue 2, pp. 571–586.

[Taylor91] Richard Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. Journal **63** (1991), no. 2, pp. 281–332.

[Wiles88] Andrew Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), pp. 529–573.