Bull. Austral. Math. Soc. 05A15, 05A19
Vol. 42 (1990) [185–189]

A NATURAL PROOF OF THE CYCLOTOMIC IDENTITY

D.E. Taylor

The cyclotomic identity

$$(1-ax)^{-1} = \prod_{n\geqslant 1} (1-x^n)^{-M(a,n)},$$

where $M(a,n) = 1/n \sum_{d|n} \mu(d)a^{n/d}$ and μ is the classical Möbius function, is shown to be a consequence of a natural isomorphism of species.

1. Introduction

In this note we give a natural combinatorial proof of the cyclotomic identity:

$$(1-ax)^{-1} = \prod_{n\geqslant 1} (1-x^n)^{-M(a,n)},$$

where $M(a,n) = 1/n \sum_{d|n} \mu(d)a^{n/d}$ and μ is the classical Möbius function.

A combinatorial proof of this identity has previously been given by Metropolis and Rota [**2, 3**]. Their proof uses a sequence of bijections between structures built from linear and cyclic orders. But some of the bijections they use depend on a choice of labelling and are not natural in the categorical sense. The Metropolis-Rota proof has been translated into the language of species (à la Joyal [**1**]) by Varadarajan and Wehrhahn [**5**]. The lemmas which depend on a choice of labelling give an equipotence rather than an isomorphism of species. However the species identity which corresponds to the cyclotomic identity is in fact an isomorphism of species, not just an equipotence. It is the purpose of this note to give a short proof of this result.

Recently Nelson [**4**] has generalised this proof to obtain an identity for each group G satisfying certain finiteness conditions. The cyclotomic identity corresponds to the case $G = \mathbb{Z}$.

Received 26th October, 1989

https://doi.org/10.1017/S0004972700028355 Published online by Cambridge University Press

2. Species

A *species* $\mathbf{S}$ is a functor from the category of finite sets and bijections to the category of finite sets. The generating function of $\mathbf{S}$ is the formal power series

$$\#\mathbf{S}(x) = \sum_{n=0}^{\infty} |\mathbf{S}[n]| \frac{x^n}{n!},$$

where $[n] = \{1, 2, \ldots, n\}$. The elements of $\mathbf{S}(N)$ are called the $\mathbf{S}$-structures on N.

The $\mathbf{S}$-structures $\sigma \in \mathbf{S}(N)$ and $\tau \in \mathbf{S}(N')$ are said to be of the same *type* if there is a bijection $u : N \to N'$ such that $\tau = \mathbf{S}(u)\sigma$.

In what follows we write $\mathbf{S} \equiv \mathbf{T}$ to indicate that the species $\mathbf{S}$ and $\mathbf{T}$ are naturally isomorphic.

Species were introduced by Joyal [**1**] to provide a combinatorial underpinning for the calculus of formal power series. He showed that the usual operations on power series such as addition, multiplication, substitution, *et cetera*, have species analogues. Refer to [**1**] for the details. The important point is that passing from a species to its generating function respects these operations.

A sequence of species $\mathbf{S}_0$, $\mathbf{S}_1$, $\mathbf{S}_2$, ... is said to be *summable* if for each finite set N there are only finitely many $\mathbf{S}_i$ such that $\mathbf{S}_i(N) \neq \emptyset$. In this case the sum of the sequence is the species $\sum_{i=0}^{\infty} \mathbf{S}_i$, where $\left(\sum_{i=0}^{\infty} \mathbf{S}_i\right)(N)$ is the disjoint union of the sets $S_i(N)$ and the action on bijections is defined in the obvious way.

The species $\mathbf{I}$ such that $\mathbf{I}(N) = \emptyset$ for $N \neq \emptyset$ and $\mathbf{I}(\emptyset) = \{\emptyset\}$ is the identity element for multiplication; its generating function is 1. The species $\mathbf{X}$ has just one structure on each singleton and no structures on any other set. Its generating function is x and we have $\mathbf{S}(\mathbf{X}) \equiv \mathbf{S}$ for all $\mathbf{S}$.

If $\mathbf{S}_0$, $\mathbf{S}_1$, $\mathbf{S}_2$, ... is summable, the product

$$\prod_{i=0}^{\infty} (\mathbf{I} + \mathbf{S}_i)$$

is well-defined. A structure of this product species on a finite set N consists of a sequence $(K_1, K_2, \ldots, K_m)$ of disjoint subsets of N whose union is N and an $(\mathbf{I} + \mathbf{S}_i)$-structure on K_i for all i. The condition that $\mathbf{S}_0$, $\mathbf{S}_1$, $\mathbf{S}_2$, ... be summable ensures that each finite set carries only a finite number of $\mathbf{S}_i$-structures and that

$$\#\Big(\prod_{i=0}^{\infty} (\mathbf{I} + \mathbf{S}_i)\Big)(x) = \prod_{i=0}^{\infty} (1 + \#\mathbf{S}_i(x)).$$

We use $\mathbf{Sym}$ to denote the species of permutations. That is, $\mathbf{Sym}\,(N)$ is the set of all permutations of N and for every bijection $u : N \to N'$, $\mathbf{Sym}\,(u) : \mathbf{Sym}\,(N) \to$

https://doi.org/10.1017/S0004972700028355 Published online by Cambridge University Press

Sym (N') sends σ to $u\sigma u^{-1}$. Its generating function is $(1-x)^{-1}$. A related species is **Circ**, the species of all circular permutations. The **Circ**-structures on N are the permutations of N having only one cycle.

The fact that every permutation can be written as a product of uniquely determined disjoint cycles translates into the species identity

$$\mathbf{Sym} \equiv \mathbf{Exp}\ (\mathbf{Circ}),$$

where **Exp** denotes the species that has exactly one structure on each finite set — so called because $\#\mathbf{Exp}\ (x) = \exp(x)$.

3. The Cyclotomic Identity

Let A be a finite set. We also use A to denote the constant species such that $A(\emptyset) = A$ and $A(N) = \emptyset$ for $N \neq \emptyset$. If $|A| = a$, the generating function of **Sym** $(A \cdot \mathbf{X})$ is $(1-ax)^{-1}$. Our intention is to find a species factorisation of **Sym** $(A \cdot \mathbf{X})$.

The **Sym** $(A \cdot \mathbf{X})$-structures on a set N can be regarded as pairs (π, f), where $\pi \in$ **Sym** (N) and $f : N \to A$. We think of (π, f) as a *coloured permutation* (with colours from A).

First consider the coloured permutations (π, f) with $\pi \in \mathbf{Circ}(N)$. The group **Sym** (N) acts on them by conjugation. That is, $\sigma \in$ **Sym** (N) sends (π, f) to $(\sigma\pi\sigma^{-1}, f\sigma^{-1})$. The orbits of **Sym** (N) are called *necklaces*. In species terminology a necklace is a type of structure for $\mathbf{Circ}(A \cdot \mathbf{X})$.

The *period* of the necklace ξ represented by (π, f) is the least positive integer d such that π^d fixes f. In particular, f is constant on every orbit of $\langle \pi^d \rangle$ on N. The necklaces on N of period $|N|$ are said to be *primitive*. The number of primitive necklaces of period n with colours from A depends only on n and a and so we denote this number by $M(a,n)$. An explicit formula for $M(a,n)$ is well-known and easily found. Indeed, if π_0 is a fixed element of $\mathbf{Circ}[n]$, then by counting the number of coloured permutations (π_0, f) we find that $a^n = \sum_{d|n} dM(a,d)$. By Möbius inversion we have

$$M(a,n) = \frac{1}{n} \sum_{d|n} \mu(d) a^{n/d}.$$

If (π, f) is a coloured permutation of period d, then π induces a permutation $\bar{\pi}$ on the orbits $N/\langle \pi^d \rangle$ of $\langle \pi^d \rangle$ and as f is constant on these orbits it induces a function $\bar{f} : N/\langle \pi^d \rangle \to A$. The coloured permutation $(\bar{\pi}, \bar{f})$ represents a primitive necklace, called the necklace *associated* with (π, f).

If η is a primitive necklace, we define $\mathbf{Circ}(A \cdot \mathbf{X})_\eta$ to be the species of coloured permutations whose associated primitive necklace is η.

The species version of the cyclotomic identity is based on the following lemma.

https://doi.org/10.1017/S0004972700028355 Published online by Cambridge University Press

LEMMA. *If η has period d, then* $\mathbf{Circ}(A\cdot\mathbf{X})_\eta$ *and* $\mathbf{Circ}(\mathbf{X}^d)$ *are naturally isomorphic species.*

PROOF: Choose a representative $(\pi_0, f_0) \in \mathbf{Circ}(A\cdot\mathbf{X})(D)$ for η. If $(\pi, f) \in \mathbf{Circ}(A\cdot\mathbf{X})_\eta(N)$, we will define $\theta_N(\pi, f) \in \mathbf{Circ}(\mathbf{X}^d)(N)$ and show that θ is a natural isomorphism. It turns out that there are many natural isomorphisms between $\mathbf{Circ}(A\cdot\mathbf{X})_\eta$ and $\mathbf{Circ}(\mathbf{X}^d)$. In order to describe one we first choose an element $s \in D$.

Because $(\bar\pi, \bar f)$ represents η, and η is primitive, there is a unique orbit $\{e_1, e_2 \ldots, e_k\}$ of $\langle\pi^d\rangle$ on N such that for all i and j

$$f(\pi^i(e_j)) = f_0(\pi_0^i(s)).$$

Thus N is the disjoint union of the k subsets $\{\pi^i(e_j) \mid 0 \leqslant i < d\}$, each of which carries a linear order induced by π. Moreover, these k subsets are permuted cyclically by π. That is, (π, f) determines a $\mathbf{Circ}(\mathbf{X}^d)$-structure $\theta_N(\pi, f)$ on N. If $u : N \to N'$ is a bijection, then $\{u(e_j) \mid 1 \leqslant j \leqslant k\}$ is an orbit of $\langle(u\pi u^{-1})^d\rangle$ on N' and $(fu^{-1})\left((u\pi u^{-1})^i u(e_j)\right) = f_0(\pi_0^i(s))$. Thus θ_N defines an isomorphism of species. ∎

THEOREM. $\mathbf{Sym}\ (A\cdot\mathbf{X}) \equiv \prod_{d\geqslant 1} \mathbf{Sym}\ (\mathbf{X}^d)^{M(A,d)}$

PROOF: Let Δ be the set of primitive necklaces. Every coloured circular permutation is associated with a unique primitive necklace and thus

$$\mathbf{Circ}(A\cdot\mathbf{X}) \equiv \sum_{\eta\in\Delta} \mathbf{Circ}(A\cdot\mathbf{X})_\eta.$$

By definition there are $M(a,d)$ primitive necklaces of period d and thus by the Lemma we have

$$\mathbf{Circ}(A\cdot\mathbf{X}) \equiv \sum_{d=1}^{\infty} M(a,d)\mathbf{Circ}(\mathbf{X}^d).$$

Applying **Exp** and using the fact that **Sym** $\equiv$ **Exp** (**Circ**) yields the isomorphism

$$\mathbf{Sym}\ (A\cdot\mathbf{X}) \equiv \prod_{d=1}^{\infty} \mathbf{Sym}\ (\mathbf{X}^d)^{M(a,d)}.$$

This completes the proof. ∎

The cyclotomic identity follows from this theorem on taking generating functions.

REFERENCES

[1] André Joyal, 'Une théorie combinatoire des series formelles', *Adv. in Math.* **42** (1981), 1–82.

[2] N. Metropolis and Gian-Carlo Rota, 'Witt vectors and the algebra of necklaces', *Adv. in Math.* **50** (1983), 95–125.

[3] N. Metropolis and Gian-Carlo Rota, 'The cyclotomic identity', *Contemporary Math.* **34** (1984), 19–27.

[4] A. M. Nelson, 'A generalized cyclotomic identity', *University of Sydney Research Report* **89–7** (1989).

[5] K. Varadarajan and K. Wehrhahn, 'Aperiodic rings, necklace rings and Witt vectors', *Adv. in Math.* **81** (1990), 1–29.

Department of Pure Mathematics
University of Sydney
NSW 2006 Australia