ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 30, Number 1, Spring 2000

A COMBINATORIAL IDENTITY OF SUBSET-SUM POWERS IN RINGS

ROY MALTBY

ABSTRACT. Escott showed that, for any set of n natural numbers, the sum of the kth powers of the sums of subsets of even cardinality is equal to the sum of the kth powers of the sums of subsets of odd cardinality for $k = 1, \dots, n-1$. We present a new proof of this fact which shows that this result holds in noncommutative rings as well.

The main application of Theorem 1 is to the Prouhet-Tarry-Escott problem, which is to determine, for each $d \in \mathbf{N}$, the least m such that there exist $(a_1, \dots, a_m) \in \mathbf{N}^m$ and $(b_1, \dots, b_m) \in \mathbf{N}^m$ not permutations of each other so that $\sum_{i=1}^m a_i^k = \sum_{i=1}^m b_i^k$ for all $k \leq d$. (We use $\mathbf{N}$ to denote the set of natural numbers, and for every $n \in \mathbf{N}$ we use $\mathbf{n}$ to denote the set $\{1, \dots, n\}$.) In [**3**], this author describes in detail one method of applying Theorem 1 to the Prouhet-Tarry-Escott problem. For a thorough discussion of the Prouhet-Tarry-Escott problem, see Borwein and Ingall's recent paper [**1**].

Dorwart and Brown [**2**, p. 624] attribute Theorem 1 to Escott. Here we give a fuller presentation of the old proof sketched by Borwein and Ingalls following their Proposition 1 in [**1**]. This proof has similarities to the one presented by Wright [**4**]. This proof shows that the theorem holds for natural numbers, and we follow it with a proof that the identity holds in noncommutative rings as well.

Theorem 1. *For any $n \in \mathbf{N}$ and $\alpha_1, \dots, \alpha_n \in \mathbf{N}$,*

$$\sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ odd}}} \left(\sum_{i \in I} \alpha_i \right)^k = \sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ even}}} \left(\sum_{i \in I} \alpha_i \right)^k,$$

for all $k < n$.

Received by the editors on December 20, 1996.

Proof. Let $m \in \mathbf{N}$ and $a_1, \dots, a_m, b_1, \dots, b_m \in \mathbf{N}$. Observe that in $\mathbf{Z}[x]$,

$$(x-1)^n \,\Big|\, \sum_{i=1}^{m} x^{a_i} - \sum_{i=1}^{m} x^{b_i}$$

if and only if

$$\sum_{i=1}^{m} 1^{a_i} - \sum_{i=1}^{m} 1^{b_i} = 0$$

and

$$(x-1)^{n-1} \,\Big|\, \frac{d}{dx}\biggl(\sum_{i=1}^{m} x^{a_i} - \sum_{i=1}^{m} x^{b_i}\biggr).$$

In fact, these conditions are equivalent to

$$\sum_{i=1}^{m} 1^{a_i} - \sum_{i=1}^{m} 1^{b_i} = 0$$

and

$$(x-1)^{n-1} \,\Big|\, x\frac{d}{dx}\biggl(\sum_{i=1}^{m} x^{a_i} - \sum_{i=1}^{m} x^{b_i}\biggr),$$

which simplify to

$$\sum_{i=1}^{m} 1^{a_i} - \sum_{i=1}^{m} 1^{b_i} = 0$$

and

$$(x-1)^{n-1} \,\Big|\, \sum_{i=1}^{m} a_i x^{a_i} - \sum_{i=1}^{m} b_i x^{b_i}.$$

Repeating the reasoning above, we see that this last divisibility statement is equivalent to saying that

$$\sum_{i=1}^{m} a_i 1^{a_i} - \sum_{i=1}^{m} b_i 1^{b_i} = 0$$

and

$$(x-1)^{n-2} \,\Big|\, \sum_{i=1}^{m} a_i^2 x^{a_i} - \sum_{i=1}^{m} b_i^2 x^{b_i}.$$

Repeating this reasoning n times, we see that

$$(x-1)^n \,\Big|\, \sum_{i=1}^{m} x^{a_i} - \sum_{i=1}^{m} x^{b_i}$$

if and only if

$$\sum_{i=1}^{m} a_i^k - \sum_{i=1}^{m} b_i^k = 0$$

for all $k < n$.

Now, specifically, put $m = 2^{n-1}$ and for each $I \subseteq \mathbf{n}$ such that $|I|$ is even, put a different one of $a_1, \ldots, a_m$ equal to $\sum_{i \in I} \alpha_i$. Then do likewise for $b_1, \ldots, b_m$, except with the condition that $|I|$ be odd rather than even. Now

$$\prod_{i=1}^{n}(1 - x^{\alpha_i}) = \sum_{i=1}^{m} x^{a_i} - \sum_{i=1}^{m} x^{b_i}.$$

It is clear that

$$(1-x)^n \,\Big|\, \prod_{i=1}^{n}(1 - x^{\alpha_i}),$$

so the previous paragraph allows us to conclude that

$$\sum_{i=1}^{n} a_i^k - \sum_{i=1}^{n} b_i^k = 0$$

for all $k < n$. In other words,

$$\sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ odd}}} \left(\sum_{i \in I} \alpha_i \right)^k = \sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ even}}} \left(\sum_{i \in I} \alpha_i \right)^k$$

for all $k < n$. $\square$

Now we present a new proof which shows that the identity holds in any (not necessarily commutative) ring. This may be a better proof than the old proof of Theorem 1 repeated above, even if one is only interested in the ring of integers.

Theorem 2. *Let R be any ring. For any $n \in \mathbf{N}$ and $a_1, \ldots, a_n \in R$,*

$$\sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ odd}}} \left(\sum_{i \in I} a_i \right)^k = \sum_{\substack{I \subseteq \mathbf{n} \\ |I| \text{ even}}} \left(\sum_{i \in I} a_i \right)^k$$

for all $k < n$.

Proof. When $k = 0$, the formula says that $\mathbf{n}$ has as many subsets of odd size as it does of even size. This well-known result is easily verified by fixing $p \in \mathbf{n}$ and observing that the map f is a bijection between the set of odd-cardinality subsets of $\mathbf{n}$ and the set of even-cardinality subsets of $\mathbf{n}$ if f is defined by:

$$f(I) = \begin{cases} I \smallsetminus \{p\} & p \in I, \\ I \cup \{p\} & p \notin I. \end{cases}$$

Let $k < n$, $k \geq 1$. Then

$$\begin{aligned} \sum_{I \subseteq \mathbf{n}} (-1)^{|I|} \left(\sum_{i \in I} a_i \right)^k &= \sum_{I \subseteq \mathbf{n}} (-1)^{|I|} \sum_{(i_1, \ldots, i_k) \in I^k} \prod_{j=1}^{k} a_{i_j} \\ &= \sum_{I \subseteq \mathbf{n}} \sum_{(i_1, \ldots, i_k) \in I^k} (-1)^{|I|} \prod_{j=1}^{k} a_{i_j} \\ &= \sum_{(i_1, \ldots, i_k) \in \mathbf{n}^k} c_{i_1, \ldots, i_k} \prod_{j=1}^{k} a_{i_j} \end{aligned}$$

where, for all $(i_1, \ldots, i_k) \in \mathbf{n}^k$,

$$\begin{aligned} c_{i_1, \ldots, i_k} &= \sum_{\{i_1, \ldots, i_k\} \subseteq I \subseteq \mathbf{n}} (-1)^{|I|} \\ &= \sum_{J \subseteq \mathbf{n} \smallsetminus \{i_1, \ldots, i_k\}} (-1)^{|\{i_1, \ldots, i_k\} \cup J|} \\ &= (-1)^{|\{i_1, \ldots, i_k\}|} \sum_{J \subseteq \mathbf{n} \smallsetminus \{i_1, \ldots, i_k\}} (-1)^{|J|}. \end{aligned}$$

But we know that

$$\sum_{J \subseteq \mathbf{n} \smallsetminus \{i_1, \dots, i_k\}} (-1)^{|J|} = 0$$

since we know by the reasoning at the start of this proof that $\mathbf{n} \smallsetminus \{i_1, \dots, i_k\}$ has just as many subsets of even cardinality as it does of odd cardinality. So every $c_{i_1, \dots, i_k} = 0$. Hence,

$$\sum_{I \subseteq \mathbf{n}} (-1)^{|I|} \left(\sum_{i \in I} a_i \right)^k = 0. \qquad \square$$

REFERENCES

1. Peter Borwein and Colin Ingalls, *The Prouhet-Tarry-Escott problem revisited*, Enseign. Math. **40** (1994), 3–27.

2. H.L. Dorwart and O.E. Brown, *The Tarry-Escott problem*, MAA Monthly **44** (1937), 613–626.

3. Roy Maltby, *Pure product polynomials and the Prouhet-Tarry-Escott problem*, Math. Comp. **66** (1997), 1323–1340.

4. E.M. Wright, *Prouhet's* 1851 *solution of the Tarry-Escott problem of* 1910, Amer. Math. Monthly **66** (1959), 199–201.

Excel Geophysics, Box 5056, 303 21st Street SE, High River, Alberta, Canada T1V 1M3
E-mail address: rmaltby@telusplanet.net