ABOUT CATEGORIZATION OF CYCLOTOMIC INTEGERS AND TENSORED $N$-COMPLEXES

DJALAL MIRMOHADES

ABSTRACT. We prove that the ideal used in recent works to categorify the cyclotomic integers is generated by a cyclotomic polynomial. Moreover, we publish a proof by T. Ekedahl that the $q$-binomial relations used in the tensor product of $N$-complexes makes it necessary for the category to be enriched over the cyclotomic integers.

1. ACKNOWLEDGEMENTS

It was during my master’s thesis that I started to investigate the question posed as Theorem 3.1. I could not prove it, nor find any counterexamples. Finally, the problem reached Ekedahl in October 2010 who swiftly replied by mail with the proof published here.

About four years later at a conference in Montreal, Khovanov asked if someone could work on categorification of the ring of cyclotomic integers.

Motivated by Ekedahl’s proof, I started to look for a suitable ideal in a some product category of $N$-complexes so that I could apply the methods in the proof by Ekedahl to prove that the decategorified ideal is generated by the cyclotomic polynomial. The resulting paper [Mir] however only dealt with two distinct primes, and a simple calculation was sufficient to show that the ideal is principal.

However, without Ekedahl’s solution, I would most likely not have worked on [Mir], and I would certainly not have written this paper. So I would like to acknowledge my gratitude to Torsten Ekedahl.

2. ABOUT CATEGORIZATION OF CYCLOTOMIC INTEGERS

Recently, Laugwitz & Qi in [LQ] constructed a monoidal category together with a thick ideal such that in the ring $\mathbb{Z}[q, q^{-1}]$, this ideal is generated by certain elements of the form $(q^m - 1)/(q^{m/p_k} - 1)$, $p_k|m$. Here, we show that this ideal is generated by $\Phi_m(q)$. This result generalizes the case in [Mir] Last step of main Theorem where $m$ is equal to a product of two primes. Note that we can do the calculations in $\mathbb{Z}[q]$ instead of $\mathbb{Z}[q, q^{-1}]$ because in the quotient ring we have $q^m = 1$, hence $q^{-1} = q^{m-1}$.

We refer to [LQ, Mir] and the references within them for a more detailed introduction to the subject.

Lemma 2.1. Any maximal ideal of $\mathbb{Z}[x]$ contains a prime number.

Proof (unknown origin). Let $I$ be an ideal of $\mathbb{Z}[x]$. If $I \cap \mathbb{Z} = (0)$, we need to show that $I$ cannot be maximal. Let $I'$ be the ideal of $\mathbb{Q}[x]$ generated by $I$. We have $I' = (f(x))$ for a polynomial $f$ coming from $\mathbb{Z}[x]$ of content 1. The polynomial $f$ has degree $> 0$, because if 1 could be written as a linear combination of polynomials from $I$ in $\mathbb{Q}[x]$, then $I \cap \mathbb{Z} \neq (0)$. But any $h \in I$ is of the form $gf$ for some $g \in \mathbb{Z}[x]$. It follows from Gauss lemma that $g \in \mathbb{Z}[x]$. This shows that $I \subseteq (f(x))$ in $\mathbb{Z}[x]$. To see that $(f(x))$ is not maximal in $\mathbb{Z}[x]$, pick an $m \in \mathbb{Z}$ such that $f(m) \neq 0, \pm 1.$
Evaluation at \( m \) then induces a map

\[
\mathbb{Z}[x] \rightarrow \mathbb{Z}/(f(m))
\]

which has kernel strictly between \((f(x))\) and \(\mathbb{Z}[x]\). Hence, any maximal ideal \( I \) of \(\mathbb{Z}[x] \) has \( I \cap \mathbb{Z} = (n) \) for some integer \( n > 0 \). But since \( n \) is the characteristic of the field \(\mathbb{Z}[x]/I\), it must be prime. \(\square\)

**Lemma 2.2.** An ideal \( I \) of \(\mathbb{Z}[x] \) is the unit ideal if and only if, for every prime \( p \), the canonical homomorphism \(\mathbb{Z}[x] \rightarrow \mathbb{Z}/(p)[x] \) maps \( I \) to the unit ideal in \(\mathbb{Z}/(p)[x] \).

**Proof.** The canonical homomorphisms \(\mathbb{Z}[x] \rightarrow \mathbb{Z}/(p)[x] \) maps the unit ideal to a unit ideal. So assume \( I \) is not the unit ideal of \(\mathbb{Z}[x] \), then by Zorn’s lemma \( I \) lies in a maximal ideal \( M \), and by Lemma 2.1, there is a prime \( p \in M \). But then, the image of \( M \) in \(\mathbb{Z}/(p)[x] \) cannot be the unit ideal. \(\square\)

**Lemma 2.3.** For a prime \( p \), and distinct positive integers \( n \) and \( m \) not divisible by \( p \), we have \(\gcd(\Phi_n(q), \Phi_m(q)) = 1 \) in the principal ideal domain \(\mathbb{Z}/(p)[q] \).

**Proof.** Let \( \varphi \) denote Euler’s totient function and \( k \) denote the least common multiple of \( n \) and \( m \). The integer \( p^{\varphi(k)} - 1 \) is then divisible by \( k \), \( n \) and \( m \). Let \( GF_{p^{\varphi(k)}} \) denote a splitting field of \( q^{p^{\varphi(k)}} - q \) over \(\mathbb{Z}/(p) \). Since the polynomial \(\Phi_n(q)\Phi_m(q) \) is a divisor of \((q^{p^{\varphi(k)}} - 1)q \) in \(\mathbb{Z}[q] \), it has only simple roots in \( GF_{p^{\varphi(k)}} \). This proves the lemma. \(\square\)

**Theorem 2.4.** Let \( n = p_1p_2\cdots p_t \), where \( p_k \) are distinct primes. In the ring \(\mathbb{Z}[q] \), we have the following equality of ideals

\[
\left(\frac{[n]_q}{[n/p_1]_q}\right) + \left(\frac{[n]_q}{[n/p_2]_q}\right) + \cdots + \left(\frac{[n]_q}{[n/p_t]_q}\right) = (\Phi_n(q))
\]

where \( [n]_q = (q^n - 1)/(q - 1) \) and \(\Phi_n \) denotes the \( n \)-th cyclotomic polynomial.

**Proof.** Recall that \( q^n - 1 = \prod_{d|n} \Phi_d(q) \), hence

\[
[n]_q/[n/p_k]_q = (q^n - 1)/(q^{n/p_k} - 1) = \prod_{d|n/p_k} \Phi_d(q).
\]

Since \(\Phi_n(q) \) divides every generator \( [n]_q/[n/p_k]_q \), it is equivalent to show that the polynomials \( [n]_q/[n/p_k]_q\Phi_n(q), 1 \leq k \leq t \) generate the unit ideal in \(\mathbb{Z}[q] \). We use Lemma 2.2 so we need to show this in \(\mathbb{Z}/(p)[q] \) for an arbitrary prime \( p \). Since \(\mathbb{Z}/(p)[q] \) is a PID, it is enough to show that \(\gcd([n]_q/[n/p_1]_q, \cdots, [n]_q/[n/p_t]_q) = \Phi_n(q) \).

In the case \( p \nmid n \), the minimum multiplicity of \(\Phi_m(q) \) in \( [n]_q/[n/p_k]_q \) over \( 1 \leq k \leq t \) is equal to 1 if \( m = n \) and equal to 0 otherwise. It then follows from Lemma 2.3 that the \(\gcd \) of the generators is equal to \(\Phi_n(q) \).

In the case \( p \mid n \), we again use Lemma 2.3. We only need to count the multiplicities of \(\Phi_m(q) \) where \( p \nmid m \), because by [Nag, p. 160] (assuming \( p \nmid m \)) and the fact that we work over characteristic \( p \), we have

\[
\Phi_{pm}(q) = \frac{\Phi_m(q^p)}{\Phi_m(q)} = \Phi_m(q)^{p-1}.
\]

Moreover, when \( p_k = p \)

\[
[n]_q/[n/p_k]_q = (q^n - 1)/(q^{n/p} - 1) = (q^{n/p} - 1)^{p-1} = \prod_{d|n/p} \Phi_d(q)^{p-1}
\]
and when \( p_k \neq p \)

\[
[n]_q/[u/p_k]_q = (q^{n/p} - 1)^p/(q^{n/p_k} - 1)^p = \prod_{d|n/p_k, \ p_k \nmid d} \Phi_d(q)^p.
\]

The multiplicity of \( \Phi_{n/p}(q) \) in \([n]_q/[u/p_k]_q\) is then equal to \( p - 1 \) when \( p_k = p \) and equal to \( p \) otherwise. Hence the minimum multiplicity over \( 1 \leq k \leq t \) is equal to \( p - 1 \), which is equal to the multiplicity of \( \Phi_{n/p}(q) \) in \( \Phi_n(q) \). The minimum multiplicity of \( \Phi_m(q) \), where \( m \neq n/p \) and \( p \nmid m \) is equal to 0 for the same reason as before.

\[\square\]

### 3. About tensored \( N \)-complexes

To define a tensor product for \( N \)-complexes, Kapranov [Kap] uses \( q \)-commutativity in the construction of the total complex. Assuming that \( q \) is a primitive \( N \)th root of unity (that is \( \Phi_N(q) = 0 \)) implies that \((\frac{N}{i})_q = 0 \) for \( 0 < i < N \). This turns the total complex into an \( N \)-complex. See [Kap, Prop. 1.8–1.10] for details.

The following theorem shows that the assumption that \( \Phi_N(q) = 0 \) is not only sufficient in the above construction, but also necessary.

**Theorem 3.1.** In the ring \( \mathbb{Z}[q] \), we have the following equality of ideals

\[
\left( \begin{array}{c} n \\
1 \end{array} \right)_q + \left( \begin{array}{c} n \\
2 \end{array} \right)_q + \cdots + \left( \begin{array}{c} n \\
n - 1 \end{array} \right)_q = (\Phi_n(q))
\]

where \( \binom{n}{i}_q \) denote \( q \)-binomial coefficients and \( \Phi_n \) denotes the \( n \)th cyclotomic polynomial.

**Proof (T. Ekedahl).** The claim is that the ideal in \( \mathbb{Z}[q] \) generated by \( \binom{n}{i}_q, 0 < i < n \), is equal to \( \Phi_n(q) \), the \( n \)th cyclotomic polynomial (all \( \binom{n}{i}_q \) are clearly divisible by \( \Phi_n(q) \) as the factor \( \Phi_n(q) \) in \( q^n - 1 \) appearing in the numerator doesn’t cancel from the denominator). Hence an equivalent formulation is that the ideal \( I \) generated by \( \binom{n}{i}_q/\Phi_n(q) \) is equal to the unit ideal. If not it is contained in a maximal ideal and any maximal ideal of \( \mathbb{Z}[q] \) contains a prime number \( p \). Hence we may replace \( \mathbb{Z}[q] \) by \( \mathbb{Z}/p[q] \). As the latter ring is a PID, what we need to show is that the GCD of the \( \binom{n}{i}_q \) is equal to \( \Phi_n(q) \). Now we recall that \( q^{m-1} = 1 \) if \( q \nmid m \) and \( m = p^k \) if \( m \), if \( m, m' \) then \( \Phi_{m'}(q) = \Phi_m(q) = \Phi_{m'}(q) \) are relatively prime. Hence, for \( p \nmid d \) we have that the multiplicity with which \( \Phi_d \) divides \( q^{m-1} = 1 \) if \( d \nmid m \) and equal to \( \psi(k) := p^k + p^{k-1} + \cdots + 1 \) if \( d|m \) and \( k \) is the largest power of \( p \) dividing \( m \).

To show the result it is enough to show that for every \( d \) with \( p \nmid d \) the largest power of \( \Phi_d(q) \) which divides all \( \binom{n}{i}_q \) is 1 if \( n \neq p^k d \) and \( p^k \) if \( n = p^k d \). Assume therefore that \( p \nmid d \). Applied to \( i = 1 \) this gives \( d \nmid m \) and we write \( n = p^k m \) with \( p \nmid m \). Assume first that \( d \neq m \) and consider

\[
\binom{n}{p^k d}_q = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-p^k d+1} - 1)}{(q - 1)(q^2 - 1)\cdots(q^{p^k d} - 1)}
\]

Now, the multiplicity with which \( \Phi_d(q) \) divides \( q^{p^k d - j} - 1 \), for \( 0 \leq j < p^k d \) is equal to the same multiplicity for \( q^{p^k m - j} - 1 \) and hence the \( \Phi_d(q) \)-factors in the numerator and denominator cancel exactly. If instead \( n = p^k d \), then we use \( \binom{n}{p^k d}_q \) and the argument is the same except that we get an extra contribution of multiplicity \( p^k \) in \( q^n - 1 \).
Note that for a prime $p$ we have, by \[\text{Nag}, \text{p. 160}\]

$$\Phi_{np}(q) = \begin{cases} 
\Phi_n(q^p) & \text{if } p \mid n, \\
\frac{\Phi_n(q^p)}{\Phi_n(q)} & \text{if } p \nmid n.
\end{cases}$$

So in characteristic $p$ we get

$$\Phi_{np^k}(q) = \Phi_n(q^{p^k})/\Phi_n(q^{p^{k-1}}) = \Phi_n(q^{(p-1)p^{k-1}}) \text{ if } p \nmid n.$$

**References**

[Kap] M. M. Kapranov. On the $q$–analog of homological algebra, arXiv:q-alg/9611005.

[LQ] R. Laugwitz, Y. Qi. A categorification of cyclotomic rings, arXiv:1804.01478.

[Mir] D. Mirmohades. Categorification of the ring of cyclotomic integers for products of two primes, arXiv:1506.08755.

[Nag] T. Nagell. *Introduction to Number Theory*, Almqvist & Wiksell, 1951.