CYCLOTOMIC COMPLETIONS OF POLYNOMIAL RINGS

KAZUO HABIRO

Abstract. The main object of study in this paper is the completion 
\( \mathbb{Z}[q]^N = \varprojlim_n \mathbb{Z}[q]/((1-q)(1-q^2) \cdots (1-q^n)) \) of the polynomial ring \( \mathbb{Z}[q] \),
which arises from the study of a new invariant of integral homology 3-
spheres with values in \( \mathbb{Z}[q]^N \) announced by the author, which unifies all
the \( sl_2 \) Witten-Reshetikhin-Turaev invariants at various roots of unity.
We show that any element of \( \mathbb{Z}[q]^N \) is uniquely determined by its power
series expansion in \( q - \zeta \) for each root \( \zeta \) of unity. We also show that
any element of \( \mathbb{Z}[q]^N \) is uniquely determined by its values at the roots
of unity. These results may be interpreted that \( \mathbb{Z}[q]^N \) behaves like a
ring of “holomorphic functions defined on the set of the roots of unity”.
We will also study the generalizations of \( \mathbb{Z}[q]^N \), which are completions
of the polynomial ring \( R[q] \) over a commutative ring \( R \) with unit with
respect to the linear topologies defined by the principal ideals generated
by products of powers of cyclotomic polynomials.

Contents

1. Introduction 2
2. Preliminaries 5
3. Monic completions of polynomial rings 6
  3.1. Definitions and basic properties 6
  3.2. Injectivity of the homomorphism \( \rho^R_{M,M'} \) 7
4. Injectivity of \( \rho^R_S \) 9
5. Expansions at roots of unity 10
6. Values at roots of unity 12
7. Remarks 14
  7.1. Units in \( \mathbb{Z}[q]^N \) 14
  7.2. A localization of \( \mathbb{Z}[q]^N \) 15
  7.3. Modules 16
  7.4. Non-surjectivity of \( \rho^R_{S,(n)} \) 16
  7.5. The ring \( \mathbb{Q}[q]^\infty \) 17
References 17

Date: September 6, 2002.
2000 Mathematics Subject Classification. Primary 13B35; Secondary 13B25, 57M27.
Key words and phrases. completion of polynomial rings, cyclotomic polynomials,
Witten-Reshetikhin-Turaev invariant.
1. Introduction

The main object of study in this paper is the completion
\[ Z[q]^N = \lim_{n \to 0} Z[q]/(q)_n \]
of the polynomial ring \( Z[q] \) in an indeterminate \( q \), where we use the notation
\[ (q)_n = (1 - q)(1 - q^2) \cdots (1 - q^n) \in Z[q], \quad n \geq 0. \]
Each element \( a \in Z[q]^N \) is expressed as an infinite sum
\[ a = \sum_{n \geq 0} a_n(q)_n, \]
where \( a_n \in Z[q] \) for \( n \geq 0 \).

Some specific instances of the series (2) and some variants which can define elements of \( Z[q]^N \) can be found in the literature. Zagier [13] studied the series \( \sum_{n \geq 0} (q)_n \), which was introduced by Kontsevich, and observed that it can be expanded in \( q - \zeta \) for any root \( \zeta \) of unity. Clearly, this is the case also for any elements of \( Z[q]^N \). Some of the formulae given by Lawrence and Zagier [4] and by Le [5] for the values of the \( sl_2 \) Witten-Reshetikhin-Turaev invariants [9] [12] of some particular 3-manifolds, including the Poincaré homology sphere, were expressed as infinite series similar to (2), and have well-defined values at the roots of unity.

The ring \( Z[q]^N \) arises from the new invariant \( I(M) \) of an integral homology 3-sphere \( M \) that we announced in [1] (see also [8]). (The ring \( Z[q]^N \) is denoted \( \hat{Z}[q] \) in [1].) The invariant \( I(M) \) takes values in \( Z[q]^N \) and unifies all the \( sl_2 \) Witten-Reshetikhin-Turaev invariants \( \tau_\zeta(M) \) defined at various roots \( \zeta \) of unity; i.e., for any root \( \zeta \) of unity we have
\[ I(M)|_{q=\zeta} = \tau_\zeta(M). \]
As we explained in [1], the existence of the invariant \( I(M) \) generalizes the previous integrality results [3] [6] [7] [10] on the Witten-Reshetikhin-Turaev invariant for integral homology spheres.

The present paper was at first intended to provide the results on the ring \( Z[q]^N \) announced in [1] and those necessary for the future papers [2] in which we will prove the existence of \( I(M) \). From purely algebraic interests, however, we will also study some generalizations of \( Z[q]^N \) as follows.

Let \( R \) be a commutative ring with unit, and let \( R[q] \) denote the polynomial ring over \( R \) in an indeterminate \( q \). For each \( n \in \mathbb{N} = \{1, 2, \ldots\} \) let \( \Phi_n(q) \) denote the \( n \)th cyclotomic polynomial
\[ \Phi_n(q) = \prod_{(i,n)=1} (q - \zeta^i) \in Z[q], \]
where \( \zeta \) is a primitive \( n \)th root of unity. If \( S \subset \mathbb{N} \) is a subset, we set
\[ \Phi_S = \{ \Phi_n(q) \mid n \in S \} \subset Z[q], \]
and let $\Phi_S^*$ denote the multiplicative set in $\mathbb{Z}[q]$ generated by $\Phi_S$, which we will regard as a directed set with respect to the divisibility relation $|$. The principal ideals $(f(q)) \subset R[q]$ for $f(q) \in \Phi_S^*$ define a linear topology of the ring $R[q]$. Define a commutative $R$-algebra $R[q]^S$ by

$$(3) \quad R[q]^S = \varprojlim_{f(q) \in \Phi_S^*} R[q]/(f(q)),$$

which we will call the $(S\text{-})$cyclo
tomic completion of $R[q]$. Since the sequence $(-1)^n(q_n), n \geq 0,$ is cofinal to the directed set $\Phi_S^*$, the definition (3) is consistent with (1). Note that if $S$ is finite, then $R[q]^S$ is identified with the $\left(\prod \Phi_S\right)$-adic completion of $R[q]$, where $\prod \Phi_S = \prod_{f(q) \in \Phi_S^*} f = \prod_{n \in S} \Phi_n(q)$. In particular, we have $R[q]^{(1)} \simeq R[[q - 1]]$ and $R[q]^{(2)} \simeq R[[q + 1]]$. In general, we have a natural isomorphism

$$\mathbb{Z}[q]^S \simeq \varprojlim_{S' \subset S, |S'| < S} \mathbb{Z}[q]^{S'},$$

where $S'$ runs through all the finite subsets of $S$.

We are interested in the behavior of natural homomorphisms among the cyclotomic completions $R[q]^S$ for various $R$ and $S$, and also those among the $R[q]^S$ and some other rings. First of all, if $g: R \to R'$ is a ring homomorphism, then for each $S \subset \mathbb{N}$ the homomorphism $g_S: R[q] \to R'[q]$, induced by $g$, induces a ring homomorphism $g_S: R[q]^S \to R'[q]^S$. If $g$ is injective (resp. surjective), then so is $g_S$ (see Lemma [3.1]).

More interesting homomorphisms among cyclotomic completions are induced by inclusions $S' \subset S \subset \mathbb{N}$. In this case, $\Phi_S^*$ is a directed subset of $\Phi_S^*$, and hence $\text{id}_{R[q]}$ induces an $R$-algebra homomorphism

$$\rho_{S,S'}^R: R[q]^S \to R[q]^{S'}.$$

The rings $R[q]^S$ for $S \subset \mathbb{N}$ and the homomorphisms $\rho_{S,S'}^R$ form a presheaf of rings over the set $\mathbb{N}$ with the discrete topology; i.e., we have $R[q]^0 = \{0\}$ and $\rho_{S,S''}^R = \rho_{S'',S'}^R \cdot \rho_{S,S''}^R$ if $S'' \subset S' \subset S \subset \mathbb{N}$.

We will state a sufficient condition for $\rho_{S,S'}^R$ to be injective using a certain graph defined on the set $S$. For each subset $S \subset \mathbb{N}$, let $\Gamma_R(S)$ denote the graph (with loop-edges) whose set of vertices is $S$, and in which two elements $n, n' \in S$ are adjacent if and only if either

1. $n = n'$,
2. $n/n'$ is an integer power of a prime $p$ such that $R$ is $p$-adically separated, i.e., $\bigcap_{j \geq 0} p^j R = \{0\}$, or
3. $R = \{0\}$.

If either one of the above conditions holds, then we write $n \leftrightarrow_R n'$. For example, in $\Gamma_\mathbb{Z}(\mathbb{N})$ two vertices $n, n'$ are adjacent if and only if $n/n'$ is an integer power of a prime, and hence the graph $\Gamma_\mathbb{Z}(\mathbb{N})$ is connected; while the graph $\Gamma_\mathbb{Q}(\mathbb{N})$ is discrete, i.e., two distinct vertices are never adjacent. Theorem [4.2] states that if $S' \subset S \subset \mathbb{N}$ are subsets such that for any $n \in S$
there is a sequence $S' \ni n' \iff_R \cdots \iff_R n$ in $S$, then the homomorphism $\rho_{S,S'}^R$ is injective. A nonempty subset $S \subset \mathbb{N}$ is said to be $\iff_R$-connected if the graph $\Gamma_R(S)$ is connected. It follows that if $S \subset \mathbb{N}$ is $\iff_R$-connected, then for any nonempty subset $S' \subset S$ the homomorphism $\rho_{S,S'}^R$ is injective. In particular, since $\mathbb{N}$ is $\iff\mathbb{Z}$-connected, for each $n \in \mathbb{N}$ the homomorphism

$$\rho_{\mathbb{N},\{n\}}^\mathbb{Z}: \mathbb{Z}[q]^\mathbb{N} \rightarrow \mathbb{Z}[q]^{\{n\}} ( = \lim_{j \geq 0} \mathbb{Z}[q]/(\Phi_n(q)^j))$$

is injective.

If $\zeta$ is a primitive $n$th root of unity, then the homomorphism $\sigma_{\mathbb{N},\zeta}^\mathbb{Z}: \mathbb{Z}[q]^\mathbb{N} \rightarrow \mathbb{Z}[\zeta][[q - \zeta]],$

which is induced by the inclusion $\mathbb{Z}[q] \subset \mathbb{Z}[\zeta]_q$ and factors through $\rho_{\mathbb{N},\{n\}}^\mathbb{Z}$, is injective (Theorem 5.4). In other words, each element of $\mathbb{Z}[q]^\mathbb{N}$ is uniquely determined by its power series expansion in $q - \zeta$. In particular, the invariant $I(M)$ of an integral homology sphere $M$ is completely determined by its expansion in $q - \zeta$ for one root $\zeta$ of unity, which in the case $\zeta = 1$ is the Ohtsuki series $[\bar{1}]$. Since $\mathbb{Z}[\zeta][[q - \zeta]]$ is an integral domain, it follows that so is $\mathbb{Z}[q]^\mathbb{N}$ (Corollary 5.3).

We are also interested in the homomorphism

$$\tau_{S,T}^R: R[q]^S \rightarrow P_T(R) = \prod_{n \in T} R[q]/(\Phi_n(q))$$

for $T \subset S \subset \mathbb{N}$, induced by the homomorphism $R[q] \rightarrow P_T(R), f(q) \mapsto (f(q) \mod (\Phi_n(q)))_{n \in T}$, where $R$ is a subring of the field $\bar{\mathbb{Q}}$ of algebraic numbers. If $S$ is $\iff_R$-connected, and for some $n \in S$ there are infinitely many elements $m \in T$ with $m \iff_R n$, then $\tau_{S,T}^R$ is injective (Theorem 6.1). In particular, if $T \subset \mathbb{N}$ contains infinitely many prime powers, then $\tau_{\mathbb{N},T}^R: \mathbb{Z}[q]^\mathbb{N} \rightarrow P_T(\mathbb{Z})$ is injective. Hence it follows that if $Z$ is a set of roots of unity containing infinitely many elements of prime power order, then the homomorphism

$$\tau_{S,Z}^R: \mathbb{Z}[q]^S \rightarrow P_Z(\mathbb{Z}) = \prod_{\zeta \in Z} \mathbb{Z}[\zeta],$$

induced by $\mathbb{Z}[q] \rightarrow P_Z(\mathbb{Z}), f(q) \mapsto (f(\zeta))_{\zeta \in Z}$, is injective (Theorem 6.3). In other words, each element in $\mathbb{Z}[q]^\mathbb{N}$ is uniquely determined by its values at roots of unity in such a set $Z$. In particular, it follows that the invariant $I(M)$ of an integral homology sphere $M$ is completely determined by the Witten-Reshetikhin-Turaev invariants $\tau_\zeta(M)$ with $\zeta \in Z$.

Recall that a holomorphic function defined in a region is determined either by the power series expansion at one point or by its values at any infinitely many points contained in a compact set in the region. The properties of $\mathbb{Z}[q]^\mathbb{N}$ described above may be interpreted that $\mathbb{Z}[q]^\mathbb{N}$ behaves like the ring of “holomorphic functions defined in the set of the roots of unity”. These properties are not as obvious as they might first appear; the ring $\bar{\mathbb{Q}}[q]^\mathbb{N}$, which
contains \( \mathbb{Z}[q]^N \) as a subring, is quite contrasting. We have an isomorphism
\[
\mathbb{Q}[q]^N \cong \prod_{n \in \mathbb{N}} \mathbb{Q}[q]^{\{n\}},
\]
see Section 7.3. It follows that \( \rho_{\mathbb{Q},\{n\}}^N \) for \( n \in \mathbb{N} \) and \( \tau_{\mathbb{Q},\mathbb{N}}^\mathbb{N} \) are not injective (but surjective), and that \( \mathbb{Q}[q]^\mathbb{N} \) is not an integral domain.

The results stated above are more or less generalized in the later sections.

The rest of the paper is organized as follows. In Section 2 we fix some notations. Section 3 deals with what we might call “monic completions” of \( R[q] \), which are generalizations of cyclotomic completions defined using monic polynomials instead of cyclotomic polynomials. In Section 4 we apply the results in Section 3 to cyclotomic completions, and study the conditions for the homomorphisms \( \rho_R^{R,S'} \) to be injective. In Section 5 we consider the power series expansion of the elements of \( R[q]^S \) in \( q - \zeta \) with \( \zeta \in R \) root of unity of order contained in \( S \). In Section 6 we study the homomorphisms \( \tau_{R,S,T}^R \) and \( \tau_{R,S,Z}^R \). In Section 7 we give some remarks.

2. Preliminaries

Throughout the paper, rings are unital and commutative, and homomorphisms of rings are unital. By “homomorphism” we will usually mean a ring homomorphism. Two rings that are considered to be canonically isomorphic to each other will often be identified. Also, if a ring \( R \) embeds into another ring \( R' \) in a natural way, we will often regard \( R \) as a subring of \( R' \).

If \( R \) is a ring and \( I \subseteq R \) is an ideal, then the \( I \)-adic completion of \( R \) will be denoted by
\[
R^I = \lim_{\leftarrow j} R/I^j,
\]
and if \( J \subseteq I \) is another ideal, then let
\[
\rho_{J,I}^R: R^J \to R^I
\]
denote the homomorphism induced by \( \text{id}_R \). These notation should not cause confusions with \( R[q]^S \) and \( \rho_{S,S'}^R \) defined in the introduction. We will further generalize these notations in the later sections. The ring \( R \) is said to be \( I \)-adically separated (resp. \( I \)-adically complete) if the natural homomorphism \( R \to R^I \) is injective (resp. an isomorphism). Recall that \( R \) is \( I \)-adically separated if and only if \( \bigcap_{j \geq 0} I^j = (0) \).

Let \( \mathbb{N} = \{1, 2, \ldots\} \) denote the set of positive integers. We regard \( \mathbb{N} \) as a directed set with respect to the divisibility relation \( | \). We will not use the letter \( \mathbb{N} \) for the same set \( \{1, 2, \ldots\} \) when it is considered as an ordered set with the usual order \( \leq \).

The letter \( q \) will always denote an indeterminate.
3. Monic completions of polynomial rings

3.1. Definitions and basic properties. For a ring $R$ let $\mathcal{M}_R$ denote the set of the monic polynomials in $R[q]$, which is a directed set with respect to the divisibility relation $|$. For a subset $M \subseteq \mathcal{M}_R$, let $M^*$ denote the multiplicative set in $R[q]$ generated by $M$, which is a directed subset of $\mathcal{M}_R$. The principal ideals $(f)$, $f \in M^*$, define a linear topology of the ring $R[q]$, and let

$$R[q]^M = \lim_{\substack{\longrightarrow \cr f \in M^*}} R[q]/(f)$$

denote the completion. (If $M = \{1\}$, then (4) implies $R[q]^{\{1\}} = R[q]/(1) = 0$, which notationally contradicts to the previous definition $R[q]^{\{1\}} = R[[q - 1]]$. In the rest of the paper, however, “$R[q]^{\{1\}}$ will always mean $R[[q - 1]]$.)

If $M' \subset M \subseteq \mathcal{M}_R$, then $(M')^*$ is a directed subset of $M^*$, and hence $\text{id}_{R[q]}$ induces a homomorphism

$$\rho_{M,M'}^R : R[q]^M \to R[q]^{M'}$$

We also extend the notation in the obvious way to $\rho_{M,I}^R : R[q]^M \to R[q]^I$ for $M \subseteq \mathcal{M}_R$ a subset and $I \subseteq R$ an ideal, etc., if it is well defined. (The general rule is that $\rho_{X,Y}^R : R[q]^X \to R[q]^Y$ is a homomorphism induced by $\text{id}_{R[q]}$.)

If $M \subseteq \mathcal{M}_R$ is finite, then the directed set $M^*$ is cofinal to the sequence $(\prod M)^j$, $j \geq 0$. Hence $R[q]^M$ is naturally isomorphic to the $(\prod M)$-adic completion $R[q](\prod M)$ of $R[q]$. In particular, if $f \in \mathcal{M}_R$, then we have

$$R[q]^{\langle f \rangle} \simeq R[q]^{(f)} = \lim_{\substack{\longrightarrow \cr j}} R[q]/(f)^j.$$  

If $M \subseteq \mathcal{M}_R$ is infinite, then $R[q]^M$ is not an ideal-adic completion in general, see for example Proposition 6.2.

If $M \subseteq \mathcal{M}_R$, then the rings $R[q]^{M'}$ for finite subsets $M'$ of $M$ and the natural homomorphisms $\rho_{M',M''}^R$ for finite $M', M''$ with $M'' \subset M' \subset M$ form an inverse system of rings, of which the inverse limit is naturally isomorphic to $R[q]^M$; i.e., we have

$$R[q]^M \simeq \lim_{\substack{\longrightarrow \cr M' \subseteq M, \ |M'| < \infty}} R[q]^{M'}.$$  

Let $h : R \to R'$ be a ring homomorphism. Note that if $h$ is injective (resp. surjective), then so is the induced homomorphism $h_q : R[q] \to R'[q]$.

**Lemma 3.1.** Let $h : R \to R'$ be a ring homomorphism and let $M \subseteq \mathcal{M}_R$ be at most countable. If $h$ is injective (resp. surjective), then so is the homomorphism

$$h_M : R[q]^M \to R'[q]^{h(M)}$$

induced by $h_q$. 


Similarly, we first show that if \( \rho \) is a homomorphism from some ideal \( I \) to \( M \), then \( \rho \) is cofinal to \( M \). Note that the sequence \( h(g_0)h(g_1) \cdots \) is cofinal to \( h(M^*) = h(M)^* \). Since each \( g_n \) is monic, each \( a \in R[q]^M \) is uniquely expressed as an infinite sum

\[
a = \sum_{n \geq 0} a_n g_n,
\]

where \( a_n \in R[q] \), \( \deg a_n < \deg g_{n+1} - \deg g_n \) for \( n \geq 0 \). From this presentation of elements of \( R[q]^M \), the result follows immediately. \( \square \)

### 3.2. Injectivity of the homomorphism \( \rho_{M,M}^R \)

Let \( R \) be a ring, \( I \subset R \) an ideal, and \( f, g \in M \). Let \( \sqrt{I} \) denote the radical of \( I \). We write \( f \not\supseteq_R g \), or simply \( f \not\Rightarrow g \), if \( f \in \sqrt{\langle g \rangle + I[q]} \), i.e., if \( f^m \in \langle g \rangle + I[q] \) for some \( m \geq 0 \).

For \( f, g \in M \), we write \( f \not\Rightarrow_R g \), or simply \( f \not\Rightarrow g \), if we have \( f \not\Rightarrow_R g \) for some ideal \( I \subset R \) with \( \bigcap_{j \geq 0} I^j = \{0\} \). Then \( \Rightarrow_R \) defines a relation on the set \( M \). Obviously, \( g|f \) implies \( f \Rightarrow g \). Note also that if \( f \Rightarrow g \), \( f|f' \), and \( g'|g \), then \( f' \Rightarrow g' \).

**Proposition 3.2.** Let \( R \) be a ring, and \( f, g \in M \) with \( f \Rightarrow_R g \). Then the homomorphism \( \rho_{(f,g),(f)}^R : R[q](f) \rightarrow R[q](f) \) is injective.

**Proof.** We first show that if \( f \not\Rightarrow g \) and \( R \) is \( I \)-adically complete, then \( \rho_{(f,g),(f)}^R \) is an isomorphism. Since \( R \simeq R^I \) and \( f \) is monic, we have

\[
R[q](f) \simeq R^I[q](f) = \lim_{\leftarrow i} (\lim_{\rightarrow j} R/I^j)[q]/(f^i) \\
\simeq \lim_{\leftarrow i} (\lim_{\rightarrow j} R[q]/((f^i) + I^j[q])) \simeq R[q](f + I[q]).
\]

Similarly, \( R[q](f,g) \simeq R[q](f,g) + I[q] \). Since \( f \not\Rightarrow g \), we have \( ((f^m) + I[q]) \subset (f^m) + I[q] \subset (f,g) + I[q] \) for some \( m \geq 1 \), while we obviously have \( (f,g) + I[q] \subset (f) + I[q] \). Hence the \( ((f^m) + I[q]) \)-adic topology and the \( ((f,g) + I[q]) \)-adic topology of \( R[q] \) are the same. Hence \( \rho_{(f,g),(f)}^R : R[q](f + I[q]) \rightarrow R[q](f) \) is an isomorphism.

Now consider the general case, where we have \( f \not\Rightarrow_R g \) and \( R \) is \( I \)-adically separated. We have a commutative diagram

\[
\begin{array}{ccc}
R[q](f,g) & \xrightarrow{\rho_{(f,g),(f)}^R} & R[q](f) \\
\downarrow & & \downarrow \\
R^I[q](f,g) & \xrightarrow{\rho_{(f,g),(f)}^R} & R^I[q](f)
\end{array}
\]
where vertical arrows are induced by the inclusion \( R \subset R' \), and hence are injective. Let \( \bar{I} \) denote the closure of \( I \) in \( R' \). Since \( R' \) is \( \bar{I} \)-adically complete and clearly \( f \overset{\bar{I}}{\to} R' g \), the above-proved case implies that \( \rho^{R'}_{(fg),t} \) is an isomorphism. Hence \( \rho^R_{(fg),t} \) is injective. \( \Box \)

For two subsets \( M, M' \subset M_{\bar{R}} \), we write \( M' \prec M \) if \( M' \subset M \) and for each \( f \in M \) there is a sequence \( M' \ni f_0 \Rightarrow f_1 \Rightarrow \cdots \Rightarrow f_r = f \) in \( M \).

Suppose that \( M_0 \prec M \subset M_{\bar{R}} \). Set

\[
\mathcal{F}(M, M_0) = \{ M' \subset M \mid M_0 \subset M', |M' \setminus M_0| < \infty \},
\]

and

\[
\mathcal{F}^\prec(M, M_0) = \{ M' \in \mathcal{F}(M, M_0) \mid M_0 \prec M' \} \subset \mathcal{F}(M, M_0).
\]

We will regard \( \mathcal{F}(M, M_0) \) as a directed set with respect to \( \subset \), and \( \mathcal{F}^\prec(M, M_0) \) as a partially-ordered subset of \( \mathcal{F}(M, M_0) \). Note that if \( M', M'' \in \mathcal{F}^\prec(M, M_0) \) and \( M'' \subset M' \), then we have \( M'' \prec M' \).

**Lemma 3.3.** If \( M_0 \prec M \subset M_{\bar{R}} \), then \( \mathcal{F}^\prec(M, M_0) \) is a cofinal directed subset of \( \mathcal{F}(M, M_0) \).

**Proof.** It suffices to show that if \( M' \in \mathcal{F}(M, M_0) \), then there is \( M'' \in \mathcal{F}^\prec(M, M_0) \) with \( M' \subset M'' \). For each \( g \in M' \setminus M_0 \) choose a sequence \( M_0 \ni g_0 \Rightarrow \cdots \Rightarrow g_r = g \) in \( M \) and set \( U_g = \{ g_1, \ldots, g_r \} \). Set \( M'' = M_0 \cup \bigcup_{g \in M' \setminus M_0} U_g \). Then we have \( M'' \in \mathcal{F}^\prec(M, M_0) \) and \( M' \subset M'' \). \( \Box \)

**Theorem 3.4.** If \( R \) is a ring and \( M_0 \prec M \subset M_{\bar{R}} \), then the homomorphism \( \rho^R_{M,M_0} : R[q]^M \to R[q]^{M_0} \) is injective.

**Proof.** By (3.3) and Lemma 3.3 we have

\[
R[q]^M \simeq \varprojlim_{M' \in \mathcal{F}(M, M_0)} R[q]^{M'} \simeq \varprojlim_{M' \in \mathcal{F}^\prec(M, M_0)} R[q]^{M'}.
\]

Hence it suffices to prove the theorem assuming that \( |M \setminus M_0| = 1 \). Let \( g \in M \setminus M_0 \) be the unique element.

First we assume that \( M_0 = \{ f_1, \ldots, f_n \} \ (n \geq 1) \) is finite. Set \( f = f_1 \cdots f_n \). Since \( f_i \Rightarrow g \) for some \( i \in \{ 1, \ldots, n \} \), we have \( f \Rightarrow g \). By Proposition 3.2, \( \rho^R_{(fg),t} \) is injective. Since \( R[q]^{M_0} = R[q]^{(f)} \) and \( R[q]^M = R[q]^{(fg)} \), it follows that \( \rho^R_{M,M_0} \) is injective.

Now assume that \( M_0 \) is infinite. Choose an element \( g_0 \in M_0 \) with \( g_0 \Rightarrow g \). We have \( R[q]^{M_0} \simeq \varprojlim_{U \in \mathcal{F}(M_0, \{ g_0 \})} R[q]^U \) and \( R[q]^M \simeq \varprojlim_{U \in \mathcal{F}(M_0, \{ g_0 \})} R[q]^{U \cup \{ g \}} \).

For each \( U \in \mathcal{F}(M_0, \{ g_0 \}) \) we have \( U \prec U \cup \{ g \} \). Hence it follows from the above-proved case that the homomorphism \( \rho^R_{U \cup \{ g \},U} : R[q]^{U \cup \{ g \}} \to R[q]^U \) is injective. Since \( \rho^R_{M,M_0} \) is the inverse limit of the \( \rho^R_{U \cup \{ g \},U} \) for \( U \in \mathcal{F}(M_0, \{ g_0 \}) \), it is injective. \( \Box \)
A subset $M \subseteq \mathcal{M}_R$ is said to be $\Rightarrow^R$-connected if $M$ is not empty and for each $f, f' \in M$ there is a sequence $f = f_0 \Rightarrow_R f_1 \Rightarrow_R \cdots \Rightarrow_R f_r = f'$ ($r \geq 0$) in $M$. Note that if $M$ is $\Rightarrow^R$-connected, then for any nonempty subset $M' \subseteq M$ we have $M' \prec M$. The following follows immediately from Theorem 3.4.

**Corollary 3.5.** If $R$ is a ring, and $M \subseteq \mathcal{M}_R$ is a $\Rightarrow^R$-connected subset, then for any nonempty subset $M' \subset M$ the homomorphism $\rho^R_{M,M'}$: $R[q]^M \to R[q]^M'$ is injective.

### 4. Injectivity of $\rho^R_{S,S'}$

If $R$ a ring, and $S \subset \mathbb{N}$ is a subset, then we have $R[q]^S = R[q]^S$. If $S' \subset S$, then we have

$$\rho^R_{S,S'} = \rho^R_{\Phi_S,\Phi_{S'}}: R[q]^S \to R[q]^S'.$$

We will use the following well-known properties of cyclotomic polynomials.

**Lemma 4.1.** (1) Let $n \in \mathbb{N}$, $p$ a prime, and $e \geq 1$. Then we have

$$\Phi_{p^n}(q) \equiv \Phi_n(q)^d \pmod{(p)},$$

in $\mathbb{Z}[q]$, where $d = \deg \Phi_{p^n}(q)/\deg \Phi_n(q)$. (We have $d = (p - 1)p^{e-1}$ if $(n,p) = 1$ and $d = p^e$ if $p|n$.)

(2) If $m,n \in \mathbb{N}$, and $n/m \in \mathbb{Q}$ is not an integer power of a prime, then we have $(\Phi_n(q), \Phi_m(q)) = (1)$ in $\mathbb{Z}[q]$.

For $m,n \in \mathbb{N}$, we define $c_{m,n} \in \{0,1\} \cup \{p \mid p \text{ prime}\}$ by

1. $c_{n,n} = 0$,
2. $c_{m,n} = p$ if $p$ is a prime and $n/m = p^j$ for some $j \in \mathbb{Z} \setminus \{0\}$, and
3. $c_{m,n} = 1$ if $n/m$ is not an integer power of a prime.

Note that $c_{m,n} = c_{n,m}$ for all $m,n \in \mathbb{N}$. It is straightforward to see that $m \Rightarrow_R n$ if and only if $R$ is $(c_{m,n})$-adically separated.

Lemma 4.3 implies that for each $m,n \in \mathbb{N}$ we have $\Phi_m(q) \in \sqrt{(\Phi_n(q), c_{m,n})}$ in $R[q]$, i.e., $\Phi_m(q) \Rightarrow^R \Phi_n(q)$. It follows that if $m \leftrightarrow_R n$, then we have $\Phi_m(q) \Rightarrow_R \Phi_n(q)$. Note also that if $S \subset \mathbb{N}$ is $\leftrightarrow^R$-connected, then $\Phi_S$ is $\Rightarrow^R$-connected. The following follows immediately from Theorem 3.4 and Corollary 3.5.

**Theorem 4.2.** Let $R$ be a ring and let $S' \subset S \subset \mathbb{N}$. Suppose that each connected component of the graph $\Gamma_R(S)$ contains at least one vertex of $\Gamma_R(S')$. (In other words, for each element $n \in S$, there is a sequence $S' \ni n' \leftrightarrow_R \cdots \leftrightarrow_R n$ in $S$.) Then the homomorphism $\rho^R_{S,S'}$ is injective.

In particular, if $S \subset \mathbb{N}$ is $\leftrightarrow^R$-connected, then for any nonempty subset $S' \subset S$ the homomorphism $\rho^R_{S,S'}$: $R[q]^S \to R[q]^S'$ is injective. More particularly, for any nonempty subset $S' \subset \mathbb{N}$ the homomorphism $\rho^\mathbb{Z}_{S',S'}$: $\mathbb{Z}[q]^{S'} \to \mathbb{Z}[q]^{S'}$ is injective.
We remark that the special case of Theorem 4.2 where \( R = \mathbb{Z}, S = \mathbb{N}, \) and \( S' = \{1\} \) is obtained also by P. Vogel. Another proof of a special case of Theorem 4.2 is sketched in Remark 5.3.

For each \( n \in \mathbb{N} \) set \( \langle n \rangle = \{ m \in \mathbb{N} \mid m|n \} \). Since \( \prod_{n|n} \Phi_m(q) = q^n - 1 \), we have
\[
R[q]\langle n \rangle = R[q]^{(q^n-1)} = \lim_{j \to n} R[q]/(q^n - 1)^j.
\]

Note that the set \( \langle n \rangle \) is \( \iff \)-connected if and only if for each prime factor \( p \) of \( n \) the ring \( R \) is \( p \)-adically separated. A subset \( S \subset \mathbb{N} \) will be called \( R \)-admissible if \( S \) is a \( \iff \)-connected, directed subset of \( \mathbb{N} \) such that \( n \in S \) implies \( \langle n \rangle \subset S \). Note that a subset \( S \subset \mathbb{N} \) is finite and \( R \)-admissible if and only if there is \( n \in \mathbb{N} \) such that \( S = \langle n \rangle \) and \( R \) is \( p \)-adically separated for each prime factor \( p \) of \( n \). Note also that an \( R \)-admissible subset \( S \subset \mathbb{N} \) satisfies \( S = \bigcup_{n \in S} \langle n \rangle \), and hence we have \( R[q]^S \cong \lim_{\leftarrow n \in S} R[q]\langle n \rangle \). The following easily follows from Theorem 4.2.

**Corollary 4.3.** Let \( R \) be a ring, and let \( S \subset \mathbb{N} \) be \( R \)-admissible. Then for each \( m, n \in S \) with \( m|n \) the homomorphism \( \rho_{(n), (m)}^R : R[q]^{(n)} \to R[q]^{(m)} \) is injective. Hence \( R[q]^S \) can be regarded as the intersection \( \bigcap_{n \in S} R[q]\langle n \rangle \), where the \( R[q]^{(n)} \), \( n \in S \), are regarded as \( R \)-subalgebras of \( R[q]^{(1)} = R[[q-1]] \).

In particular, if \( m, n \in \mathbb{N} \) and \( m|n \), then \( \rho_{(n), (m)}^\mathbb{Z} : \mathbb{Z}[q]^{(n)} \to \mathbb{Z}[q]^{(m)} \) is injective. We have \( \mathbb{Z}[q]^\mathbb{N} = \bigcap_{n \in \mathbb{N}} \mathbb{Z}[q]\langle n \rangle \).

We will see in Proposition 7.7 that if \( m|n \) and \( m \neq n \), then \( \rho_{(n), (m)}^\mathbb{Z} \) is not surjective.

5. **Expansions at roots of unity**

For an integral domain \( R \) of characteristic 0 let \( Z^R \) denote the set of the roots of unity in \( R \). If \( S \subset \mathbb{N} \), then set \( Z^S_R = \{ \zeta \in Z^R \mid \text{ord} \zeta \in S \} \). For a subset \( Z \subset Z^R \) set
\[
R[q]^Z = R[q]^{M_Z},
\]
where \( M_Z = \{ q - \zeta \mid \zeta \in Z \} \subset \mathcal{M}_R \). If \( Z' \subset Z \), then set
\[
\rho_{Z, Z'}^R = \rho_{M_Z, M_{Z'}}^R : R[q]^Z \to R[q]^{Z'}.
\]
(Although we have \( 1 \in Z \) and \( 1 \in \mathbb{N} \), the notation \( R[q]^{\{1\}} \) is not ambiguous because 1 is the unique primitive 1st root of unity.)

For a subset \( Z \subset Z^R \) set \( N_Z = \{ \text{ord} \zeta \mid \zeta \in Z \} \), and in particular set \( N_R = N_{Z^R} \). If \( S \subset N_R \), then we have
\[
R[q]^S \cong R[q]^{Z^S_R}.
\]

**Lemma 5.1.** Let \( R \) be an integral domain of characteristic 0, and let \( \zeta, \zeta' \in Z^R \). Then the following conditions are equivalent.

1. \( (q - \zeta) \Rightarrow_R (q - \zeta') \),
(2) $R$ is $(\zeta - \zeta')$-adically separated,
(3) $\text{ord}(\zeta^{-1}\zeta')$ is a power of some prime $p$ such that $R$ is $p$-adically separated.

**Proof.** If (1) holds, then we have $(q - \zeta)^m \in (q - \zeta') + I[q]$ for some $m \geq 0$ and $R$ is $I$-adically separated. It follows that $(\zeta' - \zeta)^m \in I$, and hence $R$ is $(\zeta' - \zeta)$-adically separated. Hence we have (2).

The other implications (2) $\Rightarrow$ (1) and (2) $\Leftrightarrow$ (3) are straightforward. □

Let $\Leftrightarrow_R$ denote the relation on $Z^R$ such that for $\zeta, \zeta' \in Z^R$ we have $\zeta \Leftrightarrow_R \zeta'$ if and only if either one of the conditions in Lemma 5.1 holds. The following follows immediately from Corollary 3.4.

**Theorem 5.2.** Let $R$ be an integral domain of characteristic 0 and let $Z \subset Z^R$ be an $\Leftrightarrow_R$-connected subset. Then for any nonempty subset $Z' \subset Z$ the homomorphism $\rho_{Z,Z'}^R : R[q]^Z \to R[q]^Z'$ is injective.

If $\zeta, \zeta' \in Z^R$, then $\zeta \Leftrightarrow_R \zeta'$ implies $\text{ord} \zeta \Leftrightarrow_R \text{ord} \zeta'$. (The converse, however, does not holds.) It follows that if $Z \subset Z^R$ is $\Leftrightarrow_R$-connected, then $N_Z$ is $\Leftrightarrow_R$-connected.

**Remark 5.3.** We sketch below another proof using Theorem 5.2 of the special case of Theorem 1.2 where $S$ is $\Leftrightarrow_R$-connected and $R$ is an integral domain of characteristic 0 such that $R$ is $p$-adically separated for any prime $p$. Let $k$ be the quotient field of $R$ and let $\bar{k}$ be the algebraic closure of $k$. Let $\tilde{R} \subset \bar{k}$ be the $R$-subalgebra generated by the elements of $Z_S^\tilde{R}$. In view of Lemma 3.1, it suffices to see that $\rho_{S,S'}^\tilde{R}$ is injective. Since $\Leftrightarrow_R$-connectivity of $S$ implies that of $Z_S$, the homomorphism $\rho_{S,S'}^\tilde{R}$ is injective by Theorem 5.2.

**Theorem 5.4.** Let $R$ be an integral domain of characteristic 0, $S \subset N$ a $\Leftrightarrow_R$-connected subset, and $n \in S$. Assume that $R$ is $p$-adically separated for each odd prime factor $p$ of $n$, and also that if $4|n$, then $R$ is 2-adically separated. Let $\zeta$ be a primitive $n$th root of unity, which may or may not be contained in $R$. Then the homomorphism

$$\sigma_{S,\zeta}^R : R[q]^S \to R[\zeta][q - \zeta]$$

induced by $R[q] \subset R[\zeta][q]$ is injective.

In particular, for any root $\zeta$ of unity the homomorphism $\sigma_{N,\zeta}^N : Z[q]^N \to Z[\zeta][q - \zeta]$ is injective.

**Proof.** The homomorphism $\sigma_{S,\zeta}^R$ is the composition of the following three homomorphisms

$$R[q]^S \xrightarrow{\rho_{S,(n)}^\tilde{R}} R[q]^{\{n\}} \xrightarrow{i} R[\zeta][q]^{\{n\}} \xrightarrow{\rho_{\{n\},(q-\zeta)}^R} R[\zeta][q - \zeta],$$

the first two arrows of which are injective by Theorem 1.2 and Lemma 3.1, respectively. Hence it suffices to prove that $\rho_{\{n\},(q-\zeta)}^R$ is injective. We may assume $\zeta \in R$, hence $R = R[\zeta].$
For each $m$ with $m|n$, set $Z_m = Z_{m,n}^R = \{ \zeta \in Z^R : \text{ord}_m \zeta = m \}$. By $R[q]^{(n)} \simeq R[q]^n$ and Theorem [5.2], it suffices to prove that the set $Z_n$ is $\iff$-connected. The case $n = 1$ is trivial, so we assume not. Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be a factorization into prime powers, where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$. There is a bijection

$$Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}} \cong Z_n, \quad (\xi_1, \ldots, \xi_r) \mapsto \xi_1 \cdots \xi_r.$$

It suffices to show that if $(\xi_1, \ldots, \xi_r), (\xi_1', \ldots, \xi_r') \in Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}}$ satisfies $\xi_j = \xi_j'$ for all $j \in \{1, \ldots, r\} \setminus \{i\}$ and $\xi_i \neq \xi_i'$ for some $i$, then we have $\xi_1 \cdots \xi_r \iff \xi_1' \cdots \xi_r'$, which is equivalent to that $\xi_i \iff \xi_i'$. Since $Z_2 = \{-1\}$ contains only one element, the case $p_1 = 2$ and $e_1 = 1$ does not occur. We have $(\xi_i - \xi_i') \in \sqrt{(p_1)}$, and hence $\xi_i \iff \xi_i'$.

**Corollary 5.5.** Let $R$ be an integral domain of characteristic 0, and $S \subset \mathbb{N}$ a $\iff_R$-connected subset. Suppose that there is $n \in S$ such that $R$ is $p$-adically separated for each odd prime factor $p$ of $n$, and if $4|n$, then $R$ is also 2-adically separated. Then the ring $R[q]^S$ is an integral domain.

In particular, $Z[q]^S$ is an integral domain for any nonempty subset $S \subset \mathbb{N}$.

**Proof.** The result follows from Theorem 5.4 and the fact that the formal power series ring $R[\zeta][[q - \zeta]]$ is an integral domain. \qed

6. **VALUES AT ROOTS OF UNITY**

**Theorem 6.1.** Let $R$ be a subring of the field $\overline{\mathbb{Q}}$ of algebraic numbers, $S \subset \mathbb{N}$ a $\iff_R$-connected subset, and $T \subset S$ a subset. Suppose that for some $n \in S$ there are infinitely many elements $m \in T$ with $m \iff_R n$. Then the homomorphism $\tau_{S,T}^R: R[q]^S \to P_T(R)$ is injective.

In particular, if $R$ is a subring of the ring of algebraic integers, then, for any subset $T \subset \mathbb{N}$ containing infinitely many prime powers, $\tau_{S,T}^R: R[q]^S \to P_T(R)$ is injective.

**Proof.** Suppose for contradiction that there is a nonzero element $a \in R[q]^S$ with $\tau_{S,T}^R(a) = 0$. By Theorem [1.2], $\rho_{S,\{n\}}^R(a) \neq 0$. Hence we can write $\rho_{S,\{n\}}^R(a) = \sum_{j=1}^{\infty} a_j \Phi_n(q)^j$, where $l \geq 0$ and $a_j \in R[q]$ for $j \geq l$ with $a_j \not\in (\Phi_n(q))$. There are infinitely many elements $m_1, m_2, \ldots \in T$ with $m_i \iff_R n$ and $n/m_i$. For each $i$, $m_i/n$ is a power of a prime $p_i$ such that $R$ is $p_i$-adically separated. It follows from $\tau_{S,T}^R(a) = 0$ that $\Phi_{m_i}(q)^{a_i}$ in $R[q]^S$ for each $i$. Since $R$ is an integral domain of characteristic 0, we can show by induction that $\Phi_{m_1}(q) \cdots \Phi_{m_k}(q)a$ in $R[q]^S$ for each $k \geq 0$, and hence we have $\Phi_{m_1}(q) \cdots \Phi_{m_k}(q)|\rho_{S,\{n\}}^R(a)$ in $R[q]^S$. By (3) we have $\Phi_{m_i}(q) \in (p_i, \Phi_n(q))$ for each $i$. Hence we have $\Phi_{m_1}(q) \cdots \Phi_{m_k}(q) \in (p_1 \cdots p_k, \Phi_n(q))$. In other words, for each $k \geq 0$, $a_i = a_i \text{ mod } (\Phi_n(q)) \in R[q]/(\Phi_n(q))$ is divisible by $p_1 \cdots p_k$. Note that $R[q]/(\Phi_n(q)) = R \oplus Rq \oplus \cdots \oplus Rq^{d-1}$ with $d = \deg \Phi_n(q)$, and $a_i$ is expressed as a polynomial in $q$ of degree $< d$, each coefficient of which is divisible by $p_1 \cdots p_k$ in $R$ for $k \geq 0$. \qed
Since \( R \) is a subring of \( \mathbb{Q} \) and each \( p_i \) is a non-unit in \( R \), it follows that the coefficients of \( \bar{a}_i \) are zero. Consequently, we have \( a_i \in (\Phi_n(q)) \).

**Proposition 6.2.** Let \( R \) be a subring of \( \mathbb{Q} \), and \( S \subset \mathbb{N} \) an infinite subset. Then the completion \( R[q]^S \) of \( R[q] \) is not an ideal-adic completion, i.e., there is no ideal \( I \) in \( R[q] \) such that \( R \) is the direct product of the injective homomorphisms defined by \( \bar{a} \). Then \( \bar{a} \) is injective.

**Proof.** Let \( I \subset R[q] \) be a nonzero ideal, and \( f(q) \in I \) a nonzero element. Then there are only finitely many elements \( n \in S \) with \( \Phi_n(q) | f(q) \). For each \( n \in R \), the power \( f(q)^j \) for \( j \geq 1 \) is divisible by \( \Phi_n(q) \) if and only if \( f(q) \) is divisible by \( \Phi_n(q) \). It follows that \( f(q)^j \) does not converge to 0 as \( j \to 0 \) in \( R[q] \) with the topology defining the completion \( R[q]^S \). Hence we have \( R[q]^S \nless \lim_{\to} R[q]/P \).

Let \( R \) be a subring of \( \mathbb{Q} \), and let \( Z \subset Z^Q \) be a subset. Set \( P_Z(R) = \prod_{\zeta \in Z} R[\zeta] \), which generalizes the definition of \( P_Z(\mathbb{Z}) \). If \( S \subset \mathbb{N} \) is a subset and \( Z \subset Z^Q_S \), then let

\[
\tau_{S,Z}^R : R[q]^S \to P_Z(R)
\]

denote the homomorphism induced by \( R[q] \to P_Z(R) \), \( f(q) \mapsto (f(\zeta))_{\zeta \in Z} \).

**Theorem 6.3.** Let \( R \) be a subring of \( \mathbb{Q} \), and let \( S \subset \mathbb{N} \) and \( Z \subset Z^Q \) be subsets. Suppose that there is an element \( n \in S \) such that for infinitely many \( \zeta \in Z \) we have \( \text{ord} \zeta \nless_R n \). Then the homomorphism \( \tau_{S,Z}^R : R[q]^S \to P_Z(R) \) is injective.

In particular, if \( R \) is a subring of the ring of algebraic integers, and \( Z \subset Z^Q \) is a subset containing infinitely many elements of prime power orders, then \( \tau_{S,Z}^R : R[q]^S \to P_Z(R) \) is injective.

**Proof.** Set \( N_Z = \{ \text{ord} \zeta | \zeta \in Z \} \subset \mathbb{N} \). Let \( \gamma : P_{N_Z}(R) \to P_Z(R) \) be the homomorphism defined by \( \gamma((f_n(q))_{n \in N_Z}) = (f_{n,\zeta}(\zeta))_{\zeta \in Z} \). Since \( \gamma \) is the direct product of the injective homomorphisms \( R[q]/(\Phi_n(q)) \to \prod_{\zeta \in Z \text{ord} \zeta = n} R[\zeta], f(q) \mapsto (f(\zeta))_{\zeta} \), it follows that \( \gamma \) is injective. We have \( \tau_{S,Z}^R = \gamma \tau_{S,N_Z}^R \), where \( \tau_{S,N_Z}^R : R[q]^S \to P_{N_Z}(R) \) is injective by Theorem 6.1. Hence \( \tau_{S,Z}^R \) is injective.

**Conjecture 6.4.** For any infinite subset \( Z \subset Z^Q \), the homomorphism \( \tau_{N,Z}^R : \mathbb{Z}[q]^N \to P_Z(\mathbb{Z}) \) is injective.

If \( Z' \subset Z \subset Z^R \), then we have a homomorphism \( \tau_{Z,Z'}^R : R[q]^{Z'} \to P_Z(R) \), induced by \( R[q] \to P_Z(R), f(q) \mapsto (f(\zeta))_{\zeta} \).
Theorem 6.5. Let $R$ be a subring of $\mathbb{Q}$, let $Z \subset Z^R$ a $\leftrightarrow_R$-connected subset, and let $Z' \subset Z$. Suppose that for some $\zeta \in Z$ there are infinitely many elements $\xi \in Z'$ with $\xi \leftrightarrow_R \zeta$. Then the homomorphism $\tau_{Z,Z'}^R: R[q]^Z \to P_{Z'}(R)$ is injective.

Proof. The proof is similar to that of Theorem 6.1 with the cyclotomic polynomials replaced with the polynomials $q - \zeta$ with $\zeta$ a roots of unity. The details are left to the reader. \hfill \Box

7. Remarks

7.1. Units in $\mathbb{Z}[q]^S$. If $R$ is a ring and $S \subset M_R$ is a subset consisting of monic polynomials with the constant terms being units in $R$, then the element $q$ is invertible in $R[q]^S$. In particular, we have an explicit formula for $q^{-1} \in R[q]^N$ as follows.

Proposition 7.1. For any ring $R$ the element $q \in R[q]^N$ is invertible with the inverse

$$q^{-1} = \sum_{n \geq 0} q^n(q)_n.$$ 

Proof. $q \sum_{n \geq 0} n(q)_n = \sum_{n \geq 0} q^{n+1}(q)_n = \sum_{n \geq 0}(1 - (1 - q^{n+1}))q_n = \sum_{n \geq 0}((q)_n - (q)_{n+1}) = (q)_0 = 1$. \hfill \Box

For each subset $S \subset \mathbb{N}$ the inclusion $\mathbb{Z}[q] \subset \mathbb{Z}[q,q^{-1}]$ induces an isomorphism

$$\mathbb{Z}[q]^S \simeq \lim_{\mathcal{F} \in \Phi_S^*} \mathbb{Z}[q,q^{-1}]/(\mathcal{F}),$$

via which we will identify these two rings. If $S \neq \emptyset$, then, since $\bigcap_{f \in \Phi_S} (f) = (0)$ in $\mathbb{Z}[q,q^{-1}]$, the natural homomorphism $\mathbb{Z}[q,q^{-1}] \to \mathbb{Z}[q]^S$ is injective and regarded as inclusion.

For a ring $R$ let $U(R)$ denote the (multiplicative) group of the units in $R$. If $S \neq \emptyset$, then we have

$$U(\mathbb{Z}[q,q^{-1}]) \subset U(\mathbb{Z}[q]^N).$$

It is well known that $U(\mathbb{Z}[q,q^{-1}]) = \{\pm q^i \mid i \in \mathbb{Z}\}$. If we regard $\mathbb{Z}[q]^N$ and the $\mathbb{Z}[q]^{(n)}$ as subrings of $\mathbb{Z}[q]^{(1)} = \mathbb{Z}[q - 1]$ as in Corollary 4.3, then we have

$$U(\mathbb{Z}[q]^N) = \bigcap_{n \in \mathbb{N}} U(\mathbb{Z}[q]^{(n)}).$$

Conjecture 7.2. We have $U(\mathbb{Z}[q]^N) = \{\pm q^i \mid i \in \mathbb{Z}\}$.

Remark 7.3. One might expect that Conjecture 7.2 would generalize to any infinite, $\mathbb{Z}$-admissible subset $S \subset \mathbb{N}$, but this is not the case. For odd $m \geq 3$ consider the element $\gamma_m = \sum_{i=0}^{m-1}(-1)^iq^i \in \mathbb{Z}[q]$, which is known to define a unit in the ring $\mathbb{Z}[q]/(q^n - 1)$ with $(n,2m) = 1$ and is called an “alternating unit”, see [11]. For such $n$, it follows that there are $u,v \in \mathbb{Z}[q]$ such that
\[ \gamma_m u = 1 + v \Phi_n(q) \]. Since \( 1 + v \Phi_n(q) \) is a unit in \( \mathbb{Z}[q]^{(n)} \), it follows that \( \gamma_m \) is a unit in \( \mathbb{Z}[q]^{(n)} \). Set \( S = \{ n \in \mathbb{N} \mid (n, 2m) = 1 \} \). Then it is straightforward to check that \( \gamma_m \) defines a unit in \( \mathbb{Z}[q]^S \) (hence also in \( \mathbb{Z}[q]^{S'} \) for any \( S' \subset S \)). Consequently, we have \( U(\mathbb{Z}[q]^S) \subseteq \{ \pm q^i \mid i \in \mathbb{Z} \} \).

### 7.2. A localization of \( \mathbb{Z}[q]^N \)

In some application \[ \mathbb{Z}[q]^N \] will be natural to consider the following type of localization of \( \mathbb{Z}[q]^N \). Recall from Proposition 7.3 that \( \mathbb{Z}[q]^N \) is an integral domain. Let \( Q(\mathbb{Z}[q]^N) \) denote the quotient field of \( \mathbb{Z}[q]^N \). We will consider the the \( \mathbb{Z}[q]^N \)-subalgebra \( \mathbb{Z}[q]^N[\Phi^{-1}_N] \) of \( Q(\mathbb{Z}[q]^N) \) generated by the elements \( \Phi_n(q)^{-1} \) for \( n \in \mathbb{N} \). Alternatively, \( \mathbb{Z}[q]^N[\Phi^{-1}_N] \) may be defined as the subring of \( Q(\mathbb{Z}[q]^N) \) consisting of the fractions \( f(q)/g(q) \) with \( f(q) \in \mathbb{Z}[q]^N \) and \( g(q) \in \Phi_N^* \). Similarly, let \( \mathbb{Z}[q,q^{-1}][\Phi^{-1}_N] \) denote the \( \mathbb{Z}[q,q^{-1}] \)-subalgebra of the quotient field \( Q(q)(\subset Q(\mathbb{Z}[q]^N)) \) of \( \mathbb{Z}[q,q^{-1}] \) generated by the elements \( \Phi_n(q)^{-1} \) for \( n \in \mathbb{N} \), which may alternatively defined as the subring of \( Q(q) \) consisting of the fractions \( f(q)/g(q) \) with \( f(q) \in \mathbb{Z}[q,q^{-1}] \) and \( g(q) \in \Phi_N^* \).

**Proposition 7.4.** We have \( \mathbb{Z}[q]^N[\Phi^{-1}_N] = \mathbb{Z}[q]^N + \mathbb{Z}[q,q^{-1}][\Phi^{-1}_N] \).

**Proof.** The inclusion \( \supset \) is obvious; we will show the other inclusion. Since

\[
\mathbb{Z}[q]^N[\Phi^{-1}_N] = \bigcup_{f(q) \in \Phi_N^*} \frac{1}{f(q)} \mathbb{Z}[q]^N,
\]

it suffices to show that for each \( f(q) \in \Phi_N^* \) we have

\[
\frac{1}{f(q)} \mathbb{Z}[q]^N \subset \mathbb{Z}[q]^N + \frac{1}{f(q)} \mathbb{Z}[q,q^{-1}].
\]

By multiplying \( f(q) \), we need show that

\[
\mathbb{Z}[q]^N \subset f(q)^2 \mathbb{Z}[q]^N + \mathbb{Z}[q,q^{-1}],
\]

which follows from \( \mathbb{Z}[q]^N \simeq \lim_{\rightarrow_{g(q) \in \Phi_N^*}} \mathbb{Z}[q,q^{-1}]/(f(q)g(q)) \). \( \square \)

**Proposition 7.5.** We have

\[ \mathbb{Z}[q]^N \cap \mathbb{Z}[q,q^{-1}][\Phi^{-1}_N] = \mathbb{Z}[q,q^{-1}] \).

**Proof.** The inclusion \( \supset \) is obvious; we will show the other inclusion. Suppose that \( f(q) = g(q)/h(q) \in \mathbb{Z}[q]^N \cap \mathbb{Z}[q,q^{-1}][\Phi^{-1}_N] \), where \( g(q) \in \mathbb{Z}[q,q^{-1}] \) and \( h(q) \in \Phi_N^* \) and \( g(q) \) and \( h(q) \) are coprime. We will show that \( f(q) \in \mathbb{Z}[q,q^{-1}] \), i.e., \( h(q)g(q) \) in \( \mathbb{Z}[q,q^{-1}] \). Assume for contradiction that \( h(q) \neq 1 \). Choose \( n \in \mathbb{N} \) such that \( \Phi_n(q)^h(q) \). We have \( g(q) = f(q)h(q) \). Since \( \Phi_n(q)^h(q) \), we have \( \Phi_n(q)^g(q) \), which is a contradiction. Hence we have \( h(q) = 1 \), and we obviously have \( h(q)g(q) \). \( \square \)
7.3. Modules. We can define cyclotomic completions also for any \( \mathbb{Z} \)-modules as follows. Let \( A \) be a \( \mathbb{Z} \)-module, and let \( A[q] \) denote the \( \mathbb{Z}[q] \)-module of polynomials in \( q \) with coefficients in \( A \). For each \( S \subset \mathbb{N} \) let \( A[q]^S \) denote the completion

\[
A[q]^S = \lim_{f \in \Phi_S} A[q]/fA[q].
\]

If \( A \) is a ring, then this definition of \( A[q]^S \) is compatible with the previous one. Some results in the present paper can be generalized to the \( A[q]^S \).

For example, Theorem 4.2 is generalized as follows. Let \( \iff_A \) denote the relation on \( \mathbb{N} \) such that \( m \iff_A n \) if and only if either we have \( A = 0 \), or \( m/n \) is an integer power of a prime \( p \) with \( A \) being \( p \)-adically separated.

**Theorem 7.6.** Let \( A \) be a \( \mathbb{Z} \)-module, and let \( S' \subset S \subset \mathbb{N} \) be subsets. Suppose that for each \( n \in S \) there is a sequence \( S' \ni n' \iff_A \cdots \iff_A n \) in \( S \). Then the homomorphism \( \rho_{S,S'}^A : A[q]^S \to A[q]^{S'} \) induced by \( \id_{A[q]} \) is injective.

**Proof.** One way to prove Theorem 7.6 is to modify Section 3 and the proof of Theorem 4.2. We roughly sketch the necessary modifications. Section 3 is generalized as follows. For two elements \( f, g \in M_R \) and an \( R \)-module, we write \( f \Rightarrow_A g \) if \( f \Rightarrow_A g \) for some ideal \( I \) with \( A \) being \( I \)-adically separated. Then Proposition 3.2 with \( R \) replaced with an \( R \)-module \( A \) holds. Generalizations of Theorem 3.4 and Corollary 3.5 to \( R \)-modules is straightforward. Theorem 7.6 follows immediately from the generalized version of Corollary 3.4.

Alternatively, we can use Theorem 4.2 as follows. Since the case \( A = 0 \) is trivial, we assume not. Let \( A' = \mathbb{Z} \oplus A \) be the ring with the multiplication \( (m,a)(n,b) = (mn,mb+na) \) and with the unit \( (1,0) \). Then for \( m, n \in \mathbb{N} \) we have \( m \iff_A n \) if and only if \( m \iff_{A'} n \). Hence we can apply Theorem 4.2 to obtain the injectivity of \( \rho_{S,S'}^{A'} \). We can identify \( \rho_{S,S'}^{A'} \) with the direct product

\[
\rho_{S,S'}^Z \oplus \rho_{S,S'}^A : \mathbb{Z}[q]^S \oplus A[q]^S \to \mathbb{Z}[q]^{S'} \oplus A[q]^{S'}.
\]

Hence \( \rho_{S,S'}^A \) is injective. \( \Box \)

7.4. Non-surjectivity of \( \rho_{\mathbb{N},\{n\}}^Z \).

**Proposition 7.7.**

(1) If \( m, n \in \mathbb{N} \), \( m \iff \mathbb{Z} n \), and \( m \not\equiv n \), then the homomorphism \( \rho_{\{m,n\},\{m\}}^Z : \mathbb{Z}[q]^{\{m,n\}} \to \mathbb{Z}[q]^{\{m\}} \) is not surjective.

(2) If \( m|n \) and \( m \not\equiv n \), then the homomorphism \( \rho_{\{n\},\{m\}}^Z : \mathbb{Z}[q]^{\{n\}} \to \mathbb{Z}[q]^{\{m\}} \) is not surjective.

(3) For each nonempty, finite subset \( S \subset \mathbb{N} \), the homomorphism \( \rho_{\mathbb{N},S}^Z : \mathbb{Z}[q]^\mathbb{N} \to \mathbb{Z}[q]^S \) is not surjective.
Proof. (1) We have $m/n = p^e$ for some prime $p$ and an integer $e \neq 0$. Consider the following commutative diagram of natural homomorphisms.

$$
\begin{array}{ccc}
\mathbb{Z}[q]^{\{m,n\}} & \xrightarrow{\rho^{Z_{\{m,n\}}}} & \mathbb{Z}[q]^{\{m\}} \\
\downarrow & & \downarrow b \\
\mathbb{Z}[q]/(\Phi_n(q)) & \xrightarrow{c} & \mathbb{Z}_p[q]/(\Phi_n(q))
\end{array}
$$

It follows from $\mathbb{Z}_p[q]/(\Phi_n(q)) \simeq \varprojlim q^m z^m$, $\mathbb{Z}[q]/(\Phi_n(q), q^i)$, $\Phi_n(q) \in \sqrt{(\Phi_n(q), p)}$, and $p \in (\Phi_m(q), \Phi_n(q))$ that $b$ is a well-defined, surjective homomorphism. Since $c$ is not surjective, $\rho^{Z_{\{m,n\}}}$ is not surjective.

(2) We may assume that $n = pm$ for a prime $p$. The case $m = 1$ is contained in (1) above. There are isomorphisms $\mathbb{Z}[q]^{\langle m \rangle} \simeq \mathbb{Z}[q^m]^\langle 1 \rangle \otimes_{\mathbb{Z}[q^m]} \mathbb{Z}[q]$ and $\mathbb{Z}[q]^{\langle pm \rangle} \simeq \mathbb{Z}[q^m]^\langle p \rangle \otimes_{\mathbb{Z}[q^m]} \mathbb{Z}[q]$ induced by the isomorphism $\mathbb{Z}[q] \simeq \mathbb{Z}[q^m] \otimes_{\mathbb{Z}[q^m]} \mathbb{Z}[q]$. Then the case $m = 1$ implies the non-surjectivity of $\rho^{Z_{\{m,n\}}}$.

(3) This follows from (2) above, since $\rho^{Z_{\{n\}}}$ factors through $\rho^{Z_{\{n\},\langle m \rangle}}$ for some $n, m$ with $m/n$ and $m \neq n$.

\[\square\]

7.5. The ring $\mathbb{Q}[q]^S$. The structure of $\mathbb{Q}[q]^S$ for $S \subseteq \mathbb{N}$ is quite contrasting to that of $\mathbb{Z}[q]^S$. Note that $\mathbb{Z}[q]^S$ embeds into $\mathbb{Q}[q]^S$ by Lemma 3.1. (The following remarks holds if we replace $\mathbb{Q}$ with any ring $R$ such that each element of $S$ is a unit in $R$.)

Note that if $m, n \in S, m \neq n$, then $\langle \Phi_m(q)^i, \Phi_n(q)^j \rangle = (1)$ in $\mathbb{Z}[q]$ for any $i, j \geq 0$. Consequently, for each $f(q) = \prod_{n \in S} \Phi_n(q)^{\lambda(n)} \in \Phi_S^*$ with $\lambda(n) \geq 0$ we have by the Chinese Remainder Theorem

$$
\mathbb{Q}[q]/(f(q)) \simeq \prod_{n \in S} \mathbb{Q}[q]/(\Phi_n(q)^{\lambda(n)}).
$$

Taking the inverse limit, we obtain an isomorphism

$$
\mathbb{Q}[q]^S \xrightarrow{\sim} \prod_{n \in S} \mathbb{Q}[q]^{\langle n \rangle}.
$$

Since each $\mathbb{Q}[q]^{\langle n \rangle}$ is not zero, it follows that $\mathbb{Q}[q]^S$ is not an integral domain if $|S| > 1$. It also follows that $\rho^{Q_{S/\emptyset}}: \mathbb{Q}[q]^S \to \mathbb{Q}[q]^{S'}$ is not injective (but surjective) for each $S' \subseteq S$. Since for each $n \in S$ the (surjective) homomorphism $\mathbb{Q}[q]^{\langle n \rangle} \to \mathbb{Q}[q]/(\Phi_n(q))$ is not injective, the homomorphism $\tau^{Q_{S/\emptyset}}: \mathbb{Q}[q]^S \to \mathbb{Q}[q]/(\Phi_n(q))$ is not injective.

\textbf{References}

[1] K. Habiro, \textit{On the quantum sl$_2$ invariant of knots and integral homology spheres}, preprint.

[2] in preparation.

[3] R. J. Lawrence, \textit{Asymptotic expansions of Witten-Reshetikhin-Turaev invariants for some simple 3-manifolds}, J. Math. Phys. 36 (1995), no. 11, 6106–6129.
[4] and D. Zagier, *Modular forms and quantum invariants of 3-manifolds*, Asian J. Math. 3 (1999), no. 1, 93–107.

[5] T. T. Q. Le, *Quantum invariants of 3-manifolds: integrality, splitting, and perturbative expansion*, preprint. [math.QA/0004099](http://arxiv.org/abs/math.QA/0004099).

[6] H. Murakami, *Quantum SU(2)-invariants dominate Casson’s SU(2)-invariant*, Math. Proc. Cambridge Philos. Soc. 115 (1994), no. 2, 253–281.

[7] T. Ohtsuki, *A polynomial invariant of integral homology 3-spheres*, Math. Proc. Cambridge Philos. Soc. 117 (1995), no. 1, 83–112.

[8] (ed.), *Problems on invariants of knots and 3-manifolds*, preprint, available at [http://www.ms.u-tokyo.ac.jp/~tomotada/proj01](http://www.ms.u-tokyo.ac.jp/~tomotada/proj01).

[9] N. Reshetikhin and V. G. Turaev, *Invariants of 3-manifolds via link polynomials and quantum groups*, Invent. Math. 103 (1991), no. 3, 547–597.

[10] L. Rozansky, *On p-adic properties of the Witten-Reshetikhin-Turaev invariant*, preprint. [math.QA/9806075](http://arxiv.org/abs/math.QA/9806075).

[11] S. K. Sehgal, “Units in integral group rings”, Pitman Monogr. Surveys Pure Appl. Math., Longman, Essex, 1993.

[12] E. Witten, *Quantum field theory and the Jones polynomial*, Comm. Math. Phys. 121 (1989), no. 3, 351–399.

[13] D. Zagier, *Vassiliev invariants and a strange identity related to the Dedekind eta-function*, Topology 40 (2001), no. 5, 945–960.