Publl. RIMS, Kyoto Univ.
40 (2004), 1127–1146

Cyclotomic Completions of Polynomial Rings[†]

By

Kazuo HABIRO[*]

Abstract

For a subset $S \subset \mathbb{N} = \{1, 2, \dots\}$ and a commutative ring R with unit, let $R[q]^S$ denote the completion $\varprojlim_{f(q)} R[q]/(f(q))$, where $f(q)$ runs over all the products of the powers of cyclotomic polynomials $\Phi_n(q)$ with $n \in S$. We will show that under certain conditions the completion $R[q]^S$ can be regarded as a "ring of analytic functions" defined on the set of roots of unity of order in S. This means that an element of $R[q]^S$ vanishes if it vanishes on a certain type of infinite set of roots of unity, or if its power series expansion at one root of unity vanishes. In particular, the completion $\mathbb{Z}[q]^{\mathbb{N}} \simeq \varprojlim_n \mathbb{Z}[q]/((1-q)(1-q^2)\cdots(1-q^n))$ enjoys this property.

§1. Introduction

For $n \in \mathbb{N} = \{1, 2, \dots\}$, let $\Phi_n(q) \in \mathbb{Z}[q]$ denote the nth cyclotomic polynomial. Let S be a subset of $\mathbb{N}$. Set $\Phi_S = \{\Phi_n(q) \mid n \in S\} \subset \mathbb{Z}[q]$, and let Φ_S^* denote the multiplicative set in $\mathbb{Z}[q]$ generated by Φ_S. Let R be a commutative ring with unit. 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 completion $R[q]^S$ of $R[q]$ by

$$R[q]^S = \varprojlim_{f(q) \in \Phi_S^*} R[q]/(f(q)), \tag{1.1}$$

which we will call the *S-cyclotomic completion* of $R[q]$. If S is finite, then $R[q]^S$ is just the $(\prod_{n \in S} \Phi_n(q))$-adic completion of $R[q]$.

Communicated by T. Kawai. Received October 29, 2003. Revised March 1, 2004, June 21, 2004, July 8, 2004.
2000 Mathematics Subject Classification(s): Primary 13B35; Secondary 13B25, 57M27
Key words: completion of polynomial ring, cyclotomic polynomial, Witten-Reshetikhin-Turaev invariant

[†] This article is an invited contribution to a special issue of Publications of RIMS commemorating the fortieth anniversary of the founding of the Research Institute for Mathematical Sciences.

[*] Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan.

The main results of this paper can be rephrased as follows: Under certain conditions, the ring $R[q]^S$ behaves like a "ring of analytic functions" defined on the set of the roots of unity of order contained in S. In the following two paragraphs, we will explain two properties that justify the above claim, by restricting to the special case $R = \mathbb{Z}$ and $S = \mathbb{N}$.

The first property states that *an element $f(q) \in \mathbb{Z}[q]^{\mathbb{N}}$ is a function on the set of all the roots of unity.* Let $Z_{\mathbb{N}} \subset \mathbb{C}$ denote the subset of all roots of unity, and let $\mathbb{Z}[Z_{\mathbb{N}}]$ denote the subring of $\mathbb{C}$ generated by the elements of $Z_{\mathbb{N}}$. If $f(q) \in \mathbb{Z}[q]^{\mathbb{N}}$ and $\zeta \in Z_{\mathbb{N}}$, then the *evaluation* $f(\zeta)$ of $f(q)$ at ζ is well defined, since $q - \zeta$ divides $\Phi_n(q)$ with $n = \operatorname{ord}\zeta$. Hence there is a well defined map

$$\epsilon\colon\ \mathbb{Z}[q]^{\mathbb{N}} \to \operatorname{Map}(Z_{\mathbb{N}}, \mathbb{Z}[Z_{\mathbb{N}}])$$

such that $\epsilon(f(q)) = (f(\zeta))_{\zeta \in Z_{\mathbb{N}}}$. By Theorem 6.2, the map ϵ is injective, and we can regard $\mathbb{Z}[q]^{\mathbb{N}}$ as a subring of $\operatorname{Map}(Z_{\mathbb{N}}, \mathbb{Z}[Z_{\mathbb{N}}])$. Hence the elements of $\mathbb{Z}[q]^{\mathbb{N}}$ can be regarded as functions defined on the roots of unity. Moreover, Theorem 6.2 implies for example that $f(q) \in \mathbb{Z}[q]^{\mathbb{N}}$ vanishes if $f(q)$ vanishes at infinitely many roots of unity of prime power order.

The second property is a kind of *analytic continuation.* For ζ each root of unity, there is an *expansion homomorphism*

$$\sigma_\zeta\colon\ \mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Z}[\zeta][[q - \zeta]],$$

induced by $\mathbb{Z}[q] \to \mathbb{Z}[\zeta][q]$, since $(q - \zeta)^i$ divides $\Phi_{\operatorname{ord}\zeta}(q)^i$ for $i \geq 0$. For $f(q) \in \mathbb{Z}[q]^{\mathbb{N}}$, $\sigma_\zeta(f(q))$ can be regarded as the power series expansion of $f(q)$ at ζ. By Theorem 5.2, the homomorphism σ_ζ is injective. In other words, the function $\epsilon(f(q))$ is completely determined by its expansion at each root of unity. We remark here that the injectivity of σ_1 is also proved independently by P. Vogel. The non-surjectivity of σ_ζ is proved in Section 7.4.

The above-mentioned properties do *not* hold for a general ring R. For example, the analogues of the homomorphisms ϵ and σ_ζ over the rational numbers, are not injective; nevertheless, the natural homomorphism $\mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Q}[q]^{\mathbb{N}}$ is injective. For more details, see Section 7.5.

Here we would like to explain the original motivation of studying the cyclotomic completions. We should note first that some specific elements of $\mathbb{Z}[q]^{\mathbb{N}}$ have already appeared in the literature. Zagier [16] studied the series $\sum_{n\geq 0}(1-q)(1-q^2)\cdots(1-q^n)$, which was introduced by Kontsevich, and which can be regarded as an element of $\mathbb{Z}[q]^{\mathbb{N}}$ since we have an isomorphism

$$\mathbb{Z}[q]^{\mathbb{N}} \simeq \varprojlim_n \mathbb{Z}[q]/((1-q)(1-q^2)\cdots(1-q^n))$$

induced by $\mathrm{id}_{\mathbb{Z}[q]}$. Lawrence and Zagier [6] and Le [7] gave formulas for the sl_2 Witten-Reshetikhin-Turaev invariants [12, 15] for some particular integral homology spheres. These formulas were expressed as infinite series which can define elements of $\mathbb{Z}[q]^{\mathbb{N}}$.

The ring $\mathbb{Z}[q]^{\mathbb{N}}$ is used in the definition of the new invariant $I(M)$ of an integral homology 3-sphere M that we announced in [1] (where $\mathbb{Z}[q]^{\mathbb{N}}$ is denoted by $\widehat{\mathbb{Z}[q]}$), see also [11]. The invariant $I(M)$ takes values in $\mathbb{Z}[q]^{\mathbb{N}}$ and unifies all the Witten-Reshetikhin-Turaev invariants $\tau_\zeta(M)$ defined at all the roots of unity ζ, i.e., we have

$$\epsilon_\zeta(I(M)) = \tau_\zeta(M) \in \mathbb{Z}[\zeta], \quad \text{for all } \zeta \in Z_{\mathbb{N}}.$$

We may regard this result as saying that the Witten-Reshetikhin-Turaev invariants of an integral homology sphere, viewed as functions on roots of unity, is "analytic". (We note here that Lawrence [4, 5] have studied another kind of analyticity of the Witten-Reshetikhin-Turaev invariants.)

As we explained in [1], the existence of the invariant $I(M)$ generalizes the previous integrality results [9, 10, 4, 13] on the Witten-Reshetikhin-Turaev invariants of integral homology spheres. Using the injectivity of $\sigma_1\colon \mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Z}[[q-1]]$, we can show that the Ohtsuki series $\tau(M) \in \mathbb{Z}[[q-1]]$ [10], which was defined using only the $\tau_\zeta(M)$ with ζ the prime order roots of unity, determine the $\tau_\zeta(M)$ for ζ all the roots of unity. Recall that $\tau(M)$ can be regarded as a kind of "number theoretic expansion" at $q = 1$ of the Witten-Reshetikhin-Turaev invariants. For ζ a root of unity, the power series expansion $\epsilon_\zeta(I(M)) \in \mathbb{Z}[\zeta][[q-\zeta]]$ in $q-\zeta$ can be regarded as the "number theoretic expansion" at $q = \zeta$ of the Witten-Reshetikhin-Turaev invariants.

The present paper was at first intended to provide the results on the ring $\mathbb{Z}[q]^{\mathbb{N}}$ announced in [1] and those necessary for [2] in which we study completions of an integral form of the quantized enveloping algebra $U_q(sl_2)$, and for future papers [3] in which we will prove the existence of the invariant $I(M)$. However, we have generalized the subject of the paper mainly from purely algebraic point of view. Another practical reason for generalization is that it may be possible to define a generalization of $I(M)$ to rational homology spheres with values in $R[q]^S$ for some R and S which depend on the first homology group of M.

§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. Moreover, 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 $I \subset R$ is an ideal, then the I-adic completion of R will be denoted by

$$R^I = \varprojlim_j R/I^j,$$

and if $J \subset I$ is another ideal, then let

$$\rho^R_{J,I} \colon R^J \to R^I$$

denote the homomorphism induced by id_R. The notation R^I should not cause confusions with $R[q]^S$. 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 $\mathbb{N} = \{1, 2, \dots\}$ 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 $\{1, 2, \dots\}$ 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 $M \subset \mathcal{M}_R$, 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

$$R[q]^M = \varprojlim_{f \in M^*} R[q]/(f) \tag{3.1}$$

denote the completion. (If $M = \{1\}$, then (3.1) implies $R[q]^{\{1\}} = R[q]/(1) = 0$, which notationally contradicts 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 $M' \subset M \subset \mathcal{M}_R$, then $(M')^*$ is a directed subset of M^*, and hence $\mathrm{id}_{R[q]}$ induces a homomorphism

$$\rho^R_{M,M'} \colon R[q]^M \to R[q]^{M'}.$$

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

If $M \subset \mathcal{M}_R$ is finite, then the sequence $(\prod M)^j$, $j \geq 0$, is cofinal in the directed set M^*. 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

$$R[q]^{\{f\}} \simeq R[q]^{(f)} = \varprojlim_j R[q]/(f)^j.$$

If $M \subset \mathcal{M}_R$ is infinite, then $R[q]^M$ is not an ideal-adic completion in general, see for example Proposition 6.1.

If $M \subset \mathcal{M}_R$, then the rings $R[q]^{M'}$ for finite subsets M' of M and the natural homomorphisms $\rho^R_{M',M''}$ 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

$$R[q]^M \simeq \varprojlim_{M' \subset M,\, |M'| < \infty} R[q]^{M'}. \tag{3.2}$$

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

Lemma 3.1. *Let $h\colon R \to R'$ be a ring homomorphism and let $M \subset \mathcal{M}_R$ be a subset. If h is injective, then so is the homomorphism*

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

induced by h_q. If h is surjective and M is at most countable, then h_M is surjective.

Proof. For each $f \in M^*$, the R-module $R[q]/(f)$ is free of rank $\deg f$, since f is a monic polynomial. If h is injective, then the natural homomorphism

$$h_f\colon R[q]/(f) \to R[q]/(f) \otimes_R R' = R'[q]/(h(f))$$

is injective. Taking the inverse limit, we see that the induced map h_M is injective.

Suppose h is surjective and M is at most countable. There is a sequence $g_0 | g_1 | \cdots$ in M^* which is cofinal in M^*. Since the topology of $R'[q]$ defined by the $(h(g_n))$ is induced along the surjective homomorphism $h_q\colon R[q] \to R'[q]$ by the topology of $R[q]$ defined by the (g_n), it follows that h_M is surjective. (See, e.g., [8, Theorem 8.1. (ii)].) □

§3.2. Injectivity of the homomorphism $\rho^R_{M,M'}$

Let R be a ring, $I \subset R$ an ideal, and $f, g \in \mathcal{M}_R$. Let $\sqrt{I}$ denote the radical of I. We write $f \overset{I}{\Rightarrow}_R g$, or simply $f \overset{I}{\Rightarrow} g$, if $f \in \sqrt{(g) + I[q]}$, i.e., if $f^m \in (g) + I[q]$ for some $m \geq 0$. For $f, g \in \mathcal{M}_R$, we write $f \Rightarrow_R g$, or simply $f \Rightarrow g$, if we have $f \overset{I}{\Rightarrow}_R g$ for some ideal $I \subset R$ with $\bigcap_{j\geq 0} I^j = (0)$. Then $\Rightarrow_R$ defines a relation on the set $\mathcal{M}_R$. Obviously, $g|f$ implies $f \Rightarrow g$. Note also that if $f \Rightarrow g$, $f|f'$, and $g'|g$, then $f' \Rightarrow g'$.

Proposition 3.1. *Let R be a ring, and $f, g \in \mathcal{M}_R$ with $f \Rightarrow_R g$. Then the homomorphism $\rho^R_{(fg),(f)}\colon R[q]^{(fg)} \to R[q]^{(f)}$ is injective.*

Proof. We first show that if $f \overset{I}{\Rightarrow} g$ and R is I-adically complete, then $\rho^R_{(fg),(f)}$ is an isomorphism. Since $R \simeq R^I$ and f is monic, we have

$$\begin{aligned} R[q]^{(f)} \simeq R^I[q]^{(f)} &= \varprojlim_i (\varprojlim_j R/I^j)[q]/(f^i) \\ &\simeq \varprojlim_i (\varprojlim_j R[q]/((f^i) + I^j[q])) \simeq R[q]^{(f)+I[q]}. \end{aligned}$$

Similarly, $R[q]^{(fg)} \simeq R[q]^{(fg)+I[q]}$. Since $f \overset{I}{\Rightarrow} g$, we have $((f) + I[q])^m \subset (f^m) + I[q] \subset (fg) + I[q]$ for some $m \geq 1$, while we obviously have $(fg) + I[q] \subset (f) + I[q]$. Hence the $((f) + I[q])$-adic topology and the $((fg) + I[q])$-adic topology of $R[q]$ are the same. Hence $\rho^R_{(fg)+I[q],(f)+I[q]}$, which may be identified with $\rho^R_{(fg),(f)}$, is an isomorphism.

Now consider the general case, where we have $f \overset{I}{\Rightarrow}_R g$ and R is I-adically separated. We have a commutative diagram

$$\begin{tikzcd} R[q]^{(fg)} \arrow[r, "\rho^R_{(fg),(f)}"] \arrow[d] & R[q]^{(f)} \arrow[d] \\ R^I[q]^{(fg)} \arrow[r, "\rho^{R^I}_{(fg),(f)}"'] & R^I[q]^{(f)} \end{tikzcd}$$

where vertical arrows are induced by the inclusion $R \subset R^I$, and hence are injective. Let $\bar{I}$ denote the closure of I in R^I. Since R^I is $\bar{I}$-adically complete and clearly $f \overset{\bar{I}}{\Rightarrow}_{R^I} g$, the above-proved case implies that $\rho^{R^I}_{(fg),(f)}$ is an isomorphism. Hence $\rho^R_{(fg),(f)}$ is injective. □

For two subsets $M, M' \subset \mathcal{M}_R$, 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 $M_0 \prec M \subset \mathcal{M}_R$. 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 3.2. *If $M_0 \prec M \subset \mathcal{M}_R$, 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 $M' \subset M''$. □

Theorem 3.1. *If R is a ring and $M_0 \prec M \subset \mathcal{M}_R$, then the homomorphism $\rho^R_{M,M_0}\colon R[q]^M \to R[q]^{M_0}$ is injective.*

Proof. By (3.2) and Lemma 3.2 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 $M \setminus M_0$ is finite. We can further assume 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 3.1, $\rho^R_{(fg),(f)}$ is injective. Since $R[q]^{M_0} = R[q]^{(f)}$ and $R[q]^M = R[q]^{(fg)}$, it follows that ρ^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 $\rho^R_{U \cup \{g\},U}\colon R[q]^{U \cup \{g\}} \to R[q]^U$ is injective. Since ρ^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. □

A subset $M \subset \mathcal{M}_R$ 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 $M' \subset M$ we have $M' \prec M$. The following follows immediately from Theorem 3.1.

Corollary 3.1. *If R is a ring, and $M \subset \mathcal{M}_R$ is a $\Rightarrow_R$-connected subset, then for any nonempty subset $M' \subset M$ the homomorphism $\rho^R_{M,M'}\colon R[q]^M \to R[q]^{M'}$ is injective.*

§4. Injectivity of $\rho^R_{S,S'}$

If R a ring, and $S \subset \mathbb{N}$ is a subset, then the completion $R[q]^S$ defined in the introduction can be identified with $R[q]^{\Phi_S}$. If $S' \subset S$, then we set

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

In this section, we will study injectivity of $\rho^R_{S,S'}$.

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*

$$\Phi_{p^e n}(q) \equiv \Phi_n(q)^d \pmod{(p)}, \tag{4.1}$$

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

$$p \in (\Phi_n(q), \Phi_{p^e n}(q)) \tag{4.2}$$

in $\mathbb{Z}[q]$.

(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 $\mathbb{Z}[q]$.*

Proof. (4.2) follows from $p \equiv \sum_{i=0}^{p-1} q^{ip^{e-1}n} \mod (\Phi_n(q))$, and

$$\sum_{i=0}^{p-1} q^{ip^{e-1}n} = \frac{q^{p^e n} - 1}{q^{p^{e-1}n} - 1} \in (\Phi_{p^e n}(q)).$$

The other assertions are more familiar. □

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

For a ring $R \neq \{0\}$, let $\Leftrightarrow_R$ denote the binary relation on $\mathbb{N}$ such that, for $m, n \in \mathbb{N}$, we have $m \Leftrightarrow_R n$ if and only if R is $(c_{m,n})$-adically separated. Note that we have $m \Leftrightarrow_R n$ if and only if n/m is either 1 or an integer-power of a prime p such that R is p-adically separated. Note also that the binary relation $\Leftrightarrow_R$ is reflexive and symmetric, but not transitive in general.

Lemma 4.2. (1) *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., $\Phi_m(q) \overset{(c_{m,n})}{\Rightarrow}_R \Phi_n(q)$.*

(2) *We have $m \Leftrightarrow_R n$ if and only if we have $\Phi_m(q) \Rightarrow_R \Phi_n(q)$.*

Proof. (1) and the "only if" part of (2) follows easily from Lemma 4.1. We will show the "if" part of (2). The case $c_{m,n} = 0$ is obvious, and the case $c_{m,n} = 1$ follows easily from Lemma 4.1 (2).

Suppose that $c_{m,n} = p$ is a prime, and $\Phi_m(q) \Rightarrow_R \Phi_n(q)$ holds. Thus, there is an ideal I in R such that R is I-adically separated, and $\Phi_m(q)^i \in (\Phi_n(q)) + I[q]$ in $R[q]$ for some $i \geq 0$. Hence, by (4.2), we have $p^i \in (\Phi_n(q)) + I[q]$ in $R[q]$. Since $\Phi_n(q)$ is a monic polynomial, it follows that $p^i \in I$. Since R is I-adically separated, R is also p-adically separated and we have the assertion. □

A subset $S \subset \mathbb{N}$ is said to be $\Leftrightarrow_R$-connected if S is not empty and for each $n, n' \in S$ there is a sequence $n = n_0 \Leftrightarrow_R n_1 \Leftrightarrow_R \cdots \Leftrightarrow_R n_r = n'$ $(r \geq 0)$ in S. Note that $S \subset \mathbb{N}$ is $\Leftrightarrow_R$-connected if and only if Φ_S is $\Rightarrow_R$-connected. The following follows immediately from Theorem 3.1, Corollary 3.1, and Lemma 4.2.

Theorem 4.1. *Let R be a ring and let $S' \subset S \subset \mathbb{N}$. Suppose that 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 $\rho^R_{S,S'}\colon R[q]^S \to R[q]^{S'}$ is injective. More particularly, for any nonempty subset $S' \subset \mathbb{N}$ the homomorphism $\rho^{\mathbb{Z}}_{\mathbb{N},S'}\colon \mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Z}[q]^{S'}$ is injective.

We remark that the special case of Theorem 4.1 where $R = \mathbb{Z}$, $S = \mathbb{N}$, and $S' = \{1\}$ is obtained also by P. Vogel. Another proof of a special case of Theorem 4.1 is sketched in Remark 5.1.

For each $n \in \mathbb{N}$, set $\langle n\rangle = \{m \in \mathbb{N} \mid m|n\}$. Since $\prod \Phi_{\langle n\rangle} = \prod_{m|n} \Phi_m(q) = q^n - 1$, we have

$$R[q]^{\langle n\rangle} = R[q]^{(q^n-1)} = \varprojlim_j R[q]/(q^n-1)^j.$$

Note that the set $\langle n\rangle$ is $\Leftrightarrow_R$-connected if and only if for each prime factor p of n the ring R is p-adically separated.

A $\Leftrightarrow_R$-connected subset $S \subset \mathbb{N}$ is called *R-admissible* if $n \in S$ implies $\langle n\rangle \subset S$, and $a, b \in S$ implies $\exists c \in S$ such that $a|c$, $b|c$. 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 $R[q]^S \simeq \varprojlim_{n\in S} R[q]^{\langle n\rangle}$. The following follows easily from Theorem 4.1.

Corollary 4.1. *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 $\rho^R_{\langle n\rangle,\langle m\rangle}\colon R[q]^{\langle n\rangle} \to R[q]^{\langle m\rangle}$ is injective. Hence $R[q]^S$ can be regarded as the intersection $\bigcap_{n\in S} R[q]^{\langle n\rangle}$, where the $R[q]^{\langle n\rangle}$, $n \in S$, are regarded as R-subalgebras of $R[q]^{\langle 1\rangle} = R[[q-1]]$.*

In particular, if $m, n \in \mathbb{N}$ and $m|n$, then $\rho^{\mathbb{Z}}_{\langle n\rangle,\langle m\rangle}\colon \mathbb{Z}[q]^{\langle n\rangle} \to \mathbb{Z}[q]^{\langle m\rangle}$ 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 7.4 that if $m|n$ and $m \neq n$, then $\rho^{\mathbb{Z}}_{\langle n\rangle,\langle m\rangle}$ 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 $Z^R_S = \{\zeta \in Z^R \mid \operatorname{ord}\zeta \in S\}$. 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

$$\rho^R_{Z,Z'} = \rho^R_{M_Z,M_{Z'}}\colon R[q]^Z \to R[q]^{Z'}.$$

(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 $N_Z = \{\operatorname{ord}\zeta \mid \zeta \in Z\}$, and in particular set $N_R = N_{Z^R}$. If $S \subset N_R$, then we have

$$R[q]^S \simeq R[q]^{Z^R_S}.$$

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. $\operatorname{ord}(\zeta^{-1}\zeta')$ *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).

It is straightforward to prove that (2) implies (1), and that (2) and (3) are equivalent. □

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 at least one of the conditions in Lemma 5.1 holds. The following theorem follows immediately from Corollary 3.1.

Theorem 5.1. *Let R be an integral domain of characteristic 0 and let $Z \subset Z^R$ be a $\Leftrightarrow_R$-connected subset. Then for any nonempty subset $Z' \subset Z$ the homomorphism $\rho^R_{Z,Z'}\colon\ R[q]^Z \to R[q]^{Z'}$ is injective.*

Lemma 5.2. *Let R be an integral domain of characteristic 0, and $Z \subset Z^R$. We have the following.*

1. *If Z is $\Leftrightarrow_R$-connected, then N_Z is $\Leftrightarrow_R$-connected.*

2. *Suppose that if $\zeta \in Z$, $\zeta' \in Z^R$ and $\operatorname{ord}\zeta = \operatorname{ord}\zeta'$, then $\zeta' \in Z$. Then if N_Z is $\Leftrightarrow_R$-connected, then Z is $\Leftrightarrow_R$-connected.*

Proof. The first assertion follows from the fact that if $\zeta,\zeta' \in Z^R$, then $\zeta \Leftrightarrow_R \zeta'$ implies $\operatorname{ord}\zeta \Leftrightarrow_R \operatorname{ord}\zeta'$.

The second assertion follows from the fact that if $\operatorname{ord}\zeta \Leftrightarrow_R \operatorname{ord}\zeta'$ holds, then we have $\zeta^a \Leftrightarrow_R (\zeta')^{a'}$ for some $a,a' \in \mathbb{Z}$ such that $(a,\operatorname{ord}\zeta)=1$, $(a',\operatorname{ord}\zeta')=1$. □

Remark 5.1. We sketch below another proof using Theorem 5.1 of the special case of Theorem 4.1 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 $Z^{\bar{k}}_S$. In view of Lemma 3.1, it suffices to see that $\rho^{\tilde{R}}_{S,S'}$ is injective. Since S is $\Leftrightarrow_R$-connected, it is also $\Leftrightarrow_{\tilde{R}}$-connected, and hence Z_S is $\Leftrightarrow_{\tilde{R}}$-connected by Lemma 5.2. By Theorem 5.1, the homomorphism $\rho^{\tilde{R}}_{S,S'} = \rho^{\tilde{R}}_{Z_S,Z_{S'}}$ is injective.

Theorem 5.2. *Let R be an integral domain of characteristic 0, $S \subset \mathbb{N}$ 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 ζ be a primitive nth root of unity in the algebraic closure of the quotient field of R, which may or may not be contained in R. Then the homomorphism*

$$\sigma^R_{S,\zeta}\colon\ R[q]^S \to R[\zeta][[q-\zeta]]$$

induced by $R[q] \subset R[\zeta][q]$ is injective. (*Note that if $\zeta \in R$ then we have $R[\zeta] = R$.*)

In particular, for any root ζ of unity the homomorphism $\sigma^{\mathbb{Z}}_{\mathbb{N},\zeta}\colon\ \mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Z}[\zeta][[q-\zeta]]$ is injective.

Proof. By Lemma 3.1, the homomorphism $R[q]^S \to R[\zeta][q]^S$ is injective. Hence we may assume $\zeta \in R$ without loss of generality.

The homomorphism $\sigma^R_{S,\zeta}$ is the composition of the following two homomorphisms

$$R[q]^S \xrightarrow{\rho^R_{S,\{n\}}} R[q]^{\{n\}} \xrightarrow{\rho^R_{\{n\},(q-\zeta)}} R[[q-\zeta]].$$

The first arrow $\rho^R_{S,\{n\}}$ is injective by Theorem 4.1. Hence it suffices to prove that $\rho^R_{\{n\},(q-\zeta)}$ is injective.

For each m with $m|n$, set $Z_m = Z^R_{\{m\}} = \{\zeta \in Z^R \mid \operatorname{ord}\zeta = m\}$. By $R[q]^{\{n\}} \simeq R[q]^{Z_n}$ and Theorem 5.1, it suffices to prove that the set Z_n is $\Leftrightarrow_R$-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 $p_1,\dots,p_r$ are distinct primes and $e_1,\dots,e_r \geq 1$. There is a bijection

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

It suffices to show that if $(\xi_1,\dots,\xi_r),(\xi'_1,\dots,\xi'_r) \in Z_{p_1^{e_1}} \times \cdots \times Z_{p_r^{e_r}}$ satisfies $\xi_j = \xi'_j$ for all $j \in \{1,\dots,r\} \setminus \{i\}$ and $\xi_i \neq \xi'_i$ for some i, then we have $\xi_1\cdots\xi_r \Leftrightarrow_R \xi'_1\cdots\xi'_r$, which is equivalent to that $\xi_i \Leftrightarrow_R \xi'_i$. Since $Z_2 = \{-1\}$ contains only one element, the case $p_i = 2$ and $e_i = 1$ does not occur. We have $(\xi_i - \xi'_i) \subset \sqrt{(p_i)}$, and hence $\xi_i \Leftrightarrow_R \xi'_i$. □

Corollary 5.1. *Let R be an integral domain of characteristic 0, and $S \subset \mathbb{N}$ a $\Leftrightarrow_R$-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, $\mathbb{Z}[q]^S$ is an integral domain for any nonempty subset $S \subset \mathbb{N}$.

Proof. The result follows from Theorem 5.2 and the fact that the formal power series ring $R[\zeta][[q-\zeta]]$ is an integral domain. □

§6. Values at Roots of Unity

Let R be a subring of the field $\bar{\mathbb{Q}}$ of algebraic numbers and let $S \subset \mathbb{N}$. For $T \subset S$, set

$$P_T(R) = \prod_{n \in T} R[q]/(\Phi_n(q)),$$

and let

$$\epsilon^R_{S,T} \colon\ R[q]^S \to P_T(R)$$

be induced by the homomorphism $R[q] \to P_T(R)$, $f(q) \mapsto (f(q) \bmod (\Phi_n(q)))_{n \in T}$.

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

Proof. Suppose to the contrary that there is a nonzero element $a \in R[q]^S$ with $\epsilon^R_{S,T}(a) = 0$. By Theorem 4.1, $\rho^R_{S,\{n\}}$ is injective, and therefore we have $\rho^R_{S,\{n\}}(a) \neq 0$. Hence we can write $\rho^R_{S,\{n\}}(a) = \sum_{j=l}^{\infty} a_j \Phi_n(q)^j$, where $l \geq 0$ and $a_j \in R[q]$ for $j \geq l$ with $a_l \notin (\Phi_n(q))$.

Now observe that there are infinitely many elements $m_1, m_2, \ldots \in T$ with $m_i \Leftrightarrow_R n$ 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 $\epsilon^R_{S,T}(a) = 0$ that $\Phi_{m_i}(q)|a$ in $R[q]^S$ for each i.

We claim that we have $\Phi_{m_1}(q) \cdots \Phi_{m_k}(q)|a$ in $R[q]^S$ for each $k \geq 0$. We will prove this claim by induction on k. Since the case $k = 0$ is trivial, suppose $k \geq 1$. By assumption, we have $\Phi_{m_1}(q) \cdots \Phi_{m_{k-1}}(q)|a$ in $R[q]^S$. Since $m_k \in S$, there are $b(q) \in R[q]$ and $c \in R[q]^S$ such that

$$a = \Phi_{m_1}(q) \cdots \Phi_{m_{k-1}}(q)(b(q) + \Phi_{m_k}(q)c). \tag{6.1}$$

Since $\Phi_{m_k}|a$, we have $\Phi_{m_k}(q)|\Phi_{m_1}(q)\cdots\Phi_{m_{k-1}}(q)b(q)$ in $R[q]^S$. Hence we have

$$\Phi_{m_1}(\zeta_{m_k})\cdots\Phi_{m_{k-1}}(\zeta_{m_k})b(\zeta_{m_k})=0$$

in R. Since $\Phi_{m_j}(\zeta_{m_k})\neq 0$ for $j=1,\dots,k-1$, it follows that $b(\zeta_{m_k})=0$, and hence $\Phi_{m_k}(q)|b(q)$. By (6.1), we obtain the claim.

It follows from the above claim that we have $\Phi_{m_1}(q)\cdots\Phi_{m_k}(q)|\rho^R_{S,\{n\}}(a)$ in $R[q]^{\{n\}}$. By (4.1) 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 $k\geq 0$, $\bar{a}_l=a_l$ 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 $\bar{a}_l$ 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 $k\geq 0$. Since R is a subring of $\bar{\mathbb{Q}}$ and each p_i is a non-unit in R, it follows that the coefficients of $\bar{a}_l$ are zero. Consequently, we have $a_l\in(\Phi_n(q))$. □

Proposition 6.1. *Let R be a subring of $\bar{\mathbb{Q}}$, 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 $\mathrm{id}_{R[q]}$ induces an isomorphism $R[q]^S\simeq\varprojlim_j R[q]/I^j$.*

Proof. Suppose to the contrary that there is a nonzero ideal I in $R[q]$ such that $\mathrm{id}_{R[q]}$ induces an isomorphism $R[q]^S\simeq\varprojlim_j R[q]/I^j$. Let $f(q)\in I$ be a nonzero element. Since S is infinite, there is an $m\in S$ such that for each $j\geq 0$, we have $f(q)^j\notin\Phi_m(q)\bar{\mathbb{Q}}[q]$ and hence $f(q)^j\notin\Phi_m(q)R[q]$. Hence the ideals $I^j\subset R$, $j\geq 0$, are not cofinal in the ideals $(g(q))\subset R[q]$, $g(q)\in\Phi^*_S$. This contradicts the assumption. □

Let R be a subring of $\bar{\mathbb{Q}}$, and let $Z\subset Z^{\bar{\mathbb{Q}}}$ 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 $Z\subset Z^{\bar{\mathbb{Q}}}_S$, then let

$$\epsilon^R_{S,Z}\colon\ R[q]^S\to P_Z(R)$$

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

Theorem 6.2. *Let R be a subring of $\bar{\mathbb{Q}}$, and let $S\subset\mathbb{N}$ and $Z\subset Z^{\bar{\mathbb{Q}}}_S$ be subsets. Suppose that there is an element $n\in S$ such that for infinitely many*

$\zeta \in Z$ we have $\operatorname{ord}\zeta \Leftrightarrow_R n$. Then the homomorphism $\epsilon^R_{S,Z}\colon R[q]^S \to P_Z(R)$ is injective.

In particular, if R is a subring of the ring of algebraic integers, and $Z \subset Z^{\bar{\mathbb{Q}}}$ is a subset containing infinitely many elements of prime power order, then $\epsilon^R_{S,Z}\colon R[q]^S \to P_Z(R)$ is injective.

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

Conjecture 6.1. *For any infinite subset $Z \subset Z^{\bar{\mathbb{Q}}}$, the homomorphism $\epsilon^{\mathbb{Z}}_{\mathbb{N},Z}\colon \mathbb{Z}[q]^{\mathbb{N}} \to P_Z(\mathbb{Z})$ is injective.*

If $Z' \subset Z \subset Z^R$, then we have a homomorphism

$$\epsilon^R_{Z,Z'}\colon R[q]^Z \to P_{Z'}(R),$$

induced by $R[q] \to P_{Z'}(R)$, $f(q) \mapsto (f(\zeta))_\zeta$.

Theorem 6.3. *Let R be a subring of $\bar{\mathbb{Q}}$, 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 $\epsilon^R_{Z,Z'}\colon R[q]^Z \to P_{Z'}(R)$ is injective.*

Proof. The proof is similar to that of Theorem 6.1 with the cyclotomic polynomials replaced with the polynomials $q - \zeta$, where ζ is a root of unity. The details are left to the reader. □

§7. Remarks

§7.1. Units in $\mathbb{Z}[q]^S$

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

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

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

where $(q)_n = (1-q)(1-q^2)\cdots(1-q^n)$.

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

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

$$\mathbb{Z}[q]^S \simeq \varprojlim_{f\in\Phi^*_S} \mathbb{Z}[q,q^{-1}]/(f),$$

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

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

It is well known that $U(\mathbb{Z}[q,q^{-1}]) = \{\pm q^i \mid i \in \mathbb{Z}\}$. If we regard $\mathbb{Z}[q]^{\mathbb{N}}$ and the $\mathbb{Z}[q]^{\langle n\rangle}$ as subrings of $\mathbb{Z}[q]^{\langle 1\rangle} = \mathbb{Z}[[q-1]]$ as in Corollary 4.1, then we have

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

Conjecture 7.1. *We have $U(\mathbb{Z}[q]^{\mathbb{N}}) = \{\pm q^i \mid i \in \mathbb{Z}\}$.*

Remark 7.1. One might expect that Conjecture 7.1 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 $\gamma_m = \sum_{i=0}^{m-1}(-1)^i q^i \in \mathbb{Z}[q]$, 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 [14]. 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 $\mathbb{Z}[q]^{\langle n\rangle}$, it follows that γ_m is a unit in $\mathbb{Z}[q]^{\langle n\rangle}$. Set $S = \{n \in \mathbb{N} \mid (n,2m)=1\}$. Then it is straightforward to check that γ_m defines a unit in $\mathbb{Z}[q]^S$ (hence also in $\mathbb{Z}[q]^{S'}$ for any $S' \subset S$). Consequently, we have $U(\mathbb{Z}[q]^S) \supsetneq \{\pm q^i \mid i \in \mathbb{Z}\}$.

§7.2. A localization of $\mathbb{Z}[q]^{\mathbb{N}}$

In some applications, it will be natural to consider the following type of localization of $\mathbb{Z}[q]^{\mathbb{N}}$. Recall from Proposition 5.1 that $\mathbb{Z}[q]^{\mathbb{N}}$ is an integral domain. Let $Q(\mathbb{Z}[q]^{\mathbb{N}})$ denote the quotient field of $\mathbb{Z}[q]^{\mathbb{N}}$. We will consider the $\mathbb{Z}[q]^{\mathbb{N}}$-subalgebra $\mathbb{Z}[q]^{\mathbb{N}}[\Phi_{\mathbb{N}}^{-1}]$ of $Q(\mathbb{Z}[q]^{\mathbb{N}})$ generated by the elements $\Phi_n(q)^{-1}$ for

$n \in \mathbb{N}$. Alternatively, $\mathbb{Z}[q]^{\mathbb{N}}[\Phi_{\mathbb{N}}^{-1}]$ may be defined as the subring of $Q(\mathbb{Z}[q]^{\mathbb{N}})$ consisting of the fractions $f(q)/g(q)$ with $f(q) \in \mathbb{Z}[q]^{\mathbb{N}}$ and $g(q) \in \Phi_{\mathbb{N}}^{*}$. Similarly, let $\mathbb{Z}[q,q^{-1}][\Phi_{\mathbb{N}}^{-1}]$ denote the $\mathbb{Z}[q,q^{-1}]$-subalgebra of the quotient field $\mathbb{Q}(q)(\subset Q(\mathbb{Z}[q]^{\mathbb{N}}))$ 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 $\mathbb{Q}(q)$ consisting of the fractions $f(q)/g(q)$ with $f(q) \in \mathbb{Z}[q,q^{-1}]$ and $g(q) \in \Phi_{\mathbb{N}}^{*}$.

Proposition 7.2. *We have* $\mathbb{Z}[q]^{\mathbb{N}}[\Phi_{\mathbb{N}}^{-1}] = \mathbb{Z}[q]^{\mathbb{N}} + \mathbb{Z}[q,q^{-1}][\Phi_{\mathbb{N}}^{-1}]$.

Proof. The inclusion $\supset$ is obvious; we will show the other inclusion. Since

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

it suffices to show that for each $f(q) \in \Phi_{\mathbb{N}}^{*}$ we have

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

By multiplying $f(q)$, we need to show that

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

which follows from $\mathbb{Z}[q]^{\mathbb{N}} \simeq \varprojlim_{g(q)\in\Phi_{\mathbb{N}}^{*}} \mathbb{Z}[q,q^{-1}]/(f(q)g(q))$. □

Proposition 7.3. *We have*

$$\mathbb{Z}[q]^{\mathbb{N}} \cap \mathbb{Z}[q,q^{-1}][\Phi_{\mathbb{N}}^{-1}] = \mathbb{Z}[q,q^{-1}].$$

Proof. The inclusion $\supset$ is obvious; we will show the other inclusion. Suppose that $f(q) = g(q)/h(q) \in \mathbb{Z}[q]^{\mathbb{N}} \cap \mathbb{Z}[q,q^{-1}][\Phi_{\mathbb{N}}^{-1}]$, where $g(q) \in \mathbb{Z}[q,q^{-1}]$ and $h(q) \in \Phi_{\mathbb{N}}^{*}$. We may assume that $h(q)$ is minimal in degree. Thus there is no $n \in \mathbb{N}$ such that $g(q)$ and $h(q)$ have a common divisor $\Phi_n(q)$.

Suppose that $h(q) \neq 1$. Choose $n \in \mathbb{N}$ such that $\Phi_n(q)|h(q)$ in $\mathbb{Z}[q]$. Let $\zeta_n \in \bar{\mathbb{Q}}$ denote a primitive nth root of unity. By applying the homomorphism

$$\sigma^{\mathbb{Z}}_{\mathbb{N},\{\zeta_n\}}\colon\ \mathbb{Z}[q]^{\mathbb{N}} \to \mathbb{Z}[\zeta_n], \quad a(q) \mapsto a(\zeta_n)$$

to the both sides of the identity $g(q) = f(q)h(q)$ in $\mathbb{Z}[q]^{\mathbb{N}}$, we obtain $g(\zeta_n) = f(\zeta_n)h(\zeta_n) = 0$. Hence $g(q)$ is divisible by $\Phi_n(q)$ in $\mathbb{Z}[q,q^{-1}]$, which contradicts the assumption that $g(q)$ and $h(q)$ do not have a common divisor. Hence we have $h(q) = 1$, and it follows that $f(q) \in \mathbb{Z}[q,q^{-1}]$. □

§7.3. Modules

We can define cyclotomic completions also for any $\mathbb{Z}$-module, 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

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

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 $A[q]^S$.

For example, Theorem 4.1 may be generalized as follows. Let $\Leftrightarrow_A$ denote the relation on $\mathbb{N}$ such that $m \Leftrightarrow_A n$ if and only if either we have $A = 0$, or m/n is an integer power of a prime p such that A is p-adically separated.

Theorem 7.1. *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 $S' \ni n' \Leftrightarrow_A \cdots \Leftrightarrow_A n$ in S. Then the homomorphism $\rho^A_{S,S'}\colon A[q]^S \to A[q]^{S'}$ induced by $\mathrm{id}_{A[q]}$ is injective.*

Proof. One way to prove Theorem 7.1 is to modify Section 3 and the proof of Theorem 4.1. We roughly sketch the necessary modifications. Section 3 is generalized as follows. For two elements $f, g \in \mathcal{M}_R$ and an R-module, we write $f \Rightarrow_A g$ if $f \overset{I}{\Rightarrow}_A g$ for some ideal I such that A is I-adically separated. Then Proposition 3.1 with R replaced by an R-module A holds. Generalizations of Theorem 3.1 and Corollary 3.1 to R-modules is straightforward. Theorem 7.1 follows immediately from the generalized version of Corollary 3.1.

Alternatively, we can use Theorem 4.1 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 $m \Leftrightarrow_A n$ if and only if $m \Leftrightarrow_{A'} n$. Hence we can apply Theorem 4.1 to obtain the injectivity of $\rho^{A'}_{S,S'}$. We can identify $\rho^{A'}_{S,S'}$ with the direct product

$$\rho^{\mathbb{Z}}_{S,S'} \oplus \rho^A_{S,S'}\colon \mathbb{Z}[q]^S \oplus A[q]^S \to \mathbb{Z}[q]^{S'} \oplus A[q]^{S'}.$$

Hence $\rho^A_{S,S'}$ is injective. □

§7.4. Non-surjectivity of $\rho^{\mathbb{Z}}_{\mathbb{N},\{n\}}$

Proposition 7.4. *We have the following.*

1. *If $m, n \in \mathbb{N}$, $m \Leftrightarrow_{\mathbb{Z}} n$, and $m \neq n$, then the homomorphism $\rho^{\mathbb{Z}}_{\{m,n\},\{m\}}$ is* not *surjective.*

2. *If $m|n$ and $m \neq n$, then the homomorphism $\rho^{\mathbb{Z}}_{\langle n\rangle,\langle m\rangle}$ is* not *surjective.*
3. *For each nonempty, finite subset $S \subset \mathbb{N}$, the homomorphism $\rho^{\mathbb{Z}}_{\mathbb{N},S}$ 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.

$$\begin{tikzcd}
\mathbb{Z}[q]^{\{m,n\}} \arrow[r, "\rho^{\mathbb{Z}}_{\{m,n\},\{m\}}"] \arrow[d] & \mathbb{Z}[q]^{\{m\}} \arrow[d, "b"] \\
\mathbb{Z}[q]/(\Phi_n(q)) \arrow[r, "c"'] & \mathbb{Z}_p[q]/(\Phi_n(q))
\end{tikzcd}$$

It follows from $\mathbb{Z}_p[q]/(\Phi_n(q)) \simeq \varprojlim_j \mathbb{Z}[q]/(\Phi_n(q), p^j)$, $\Phi_m(q) \in \sqrt{(\Phi_n(q), p)}$, and $p \in (\Phi_m(q), \Phi_n(q))$ (which follows from (4.2)) that b is a well-defined, surjective homomorphism. Since c is not surjective, $\rho^{\mathbb{Z}}_{\{m,n\},\{m\}}$ 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 $\mathbb{Z}[q] \simeq \mathbb{Z}[q^m] \otimes_{\mathbb{Z}[q^m]} \mathbb{Z}[q]$. Thus the case $m = 1$ implies the non-surjectivity of $\rho^{\mathbb{Z}}_{\langle pm\rangle,\langle m\rangle}$.

(3) The homomorphism $\rho^{\mathbb{Z}}_{\mathbb{N},S}$ factors as follows.

$$\mathbb{Z}[q]^{\mathbb{N}} \overset{\rho^{\mathbb{Z}}_{\mathbb{N},\langle n\rangle}}{\longrightarrow} \mathbb{Z}[q]^{\langle n\rangle} \overset{\rho^{\mathbb{Z}}_{\langle n\rangle,\langle m\rangle}}{\longrightarrow} \mathbb{Z}[q]^{\langle m\rangle} \overset{\rho^{\mathbb{Z}}_{\langle m\rangle,S}}{\longrightarrow} \mathbb{Z}[q]^S,$$

where $m \in \mathbb{N}$ is the least common multiple of the elements of S, and $n \in \mathbb{N}$ is any element such that $m|n$ and $m \neq n$. By (2) above, $\rho^{\mathbb{Z}}_{\langle n\rangle,\langle m\rangle}$ is not surjective. Since the set $\langle m\rangle$ is $\Leftrightarrow_{\mathbb{Z}}$-connected, it follows from Theorem 4.1 that $\rho^{\mathbb{Z}}_{\langle m\rangle,S}$ is injective. Hence $\rho^{\mathbb{Z}}_{\mathbb{N},S}$ is not surjective. □

§7.5. The ring $\mathbb{Q}[q]^S$

The structure of $\mathbb{Q}[q]^S$ for $S \subset \mathbb{N}$ 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 $(\Phi_m(q)^i, \Phi_n(q)^j) = (1)$ in $\mathbb{Q}[q]$ 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

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

Since each $\mathbb{Q}[q]^{\{n\}}$ is not zero, it follows that $\mathbb{Q}[q]^S$ is not an integral domain if $|S| > 1$. It also follows that $\rho^{\mathbb{Q}}_{S,S'}\colon \mathbb{Q}[q]^S \to \mathbb{Q}[q]^{S'}$ is not injective (but surjective) for each $S' \subsetneq S$. Since for each $n \in S$ the (surjective) homomorphism $\mathbb{Q}[q]^{\{n\}} \to \mathbb{Q}[q]/(\Phi_n(q))$ is not injective, the homomorphism $\epsilon^{\mathbb{Q}}_{S,S}\colon \mathbb{Q}[q]^S \to P_S(\mathbb{Q})$ is not injective.

Acknowledgements

The author would like to thank the anonymous referee for helpful comments.

References

[1] Habiro, K., On the quantum sl_2 invariants of knots and integral homology spheres, *Invariants of knots and 3-manifolds* (*Kyoto, 2001*), 55-68 Geom. Topol. Monogr., 4, Geom. Topol. Publ., Coventry, 2002.

[2] ———, An integral form of the quantized enveloping algebra of sl_2 and its completions, *Preprint.*

[3] ———, in preparation.

[4] Lawrence, R. J., Asymptotic expansions of Witten-Reshetikhin-Turaev invariants for some simple 3-manifolds, *J. Math. Phys.*, **36** (1995), 6106–6129.

[5] ———, Witten-Reshetikhin-Turaev invariants of 3-manifolds as holomorphic functions, *Geometry and physics (Aarhus, 1995)*, 363–377, Lecture Notes in Pure and Appl. Math., 184, Dekker, New York, 1997.

[6] Lawrence, R. J. and Zagier, D., Modular forms and quantum invariants of 3-manifolds, *Asian J. Math.*, **3** (1999), 93–107.

[7] Le, T. T. Q., Quantum invariants of 3-manifolds: integrality, splitting, and perturbative expansion, *Topology Appl.*, **127** (2003), 125–152.

[8] Matsumura, H., *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, 8, Cambridge University Press, Cambridge, 1986.

[9] Murakami, H., Quantum SU(2)-invariants dominate Casson's SU(2)-invariant, *Math. Proc. Cambridge Philos. Soc.*, **115** (1994), 253–281.

[10] Ohtsuki, T., A polynomial invariant of integral homology 3-spheres, *Math. Proc. Cambridge Philos. Soc.*, **117** (1995), 83–112.

[11] Ohtsuki, T. (ed.), Problems on invariants of knots and 3-manifolds, *Invariants of knots and 3-manifolds* (*Kyoto, 2001*), 377-572 Geom. Topol. Monogr., 4, Geom. Topol. Publ., Coventry, 2002.

[12] Reshetikhin, N. and Turaev, V. G., Invariants of 3-manifolds via link polynomials and quantum groups, *Invent. Math.*, **103** (1991), 547–597.

[13] Rozansky, L., On p-adic properties of the Witten-Reshetikhin-Turaev invariant, *Preprint*, math.QA/9806075.

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

[15] Witten, E., Quantum field theory and the Jones polynomial, *Comm. Math. Phys.*, **121** (1989), 351–399.

[16] Zagier, D., Vassiliev invariants and a strange identity related to the Dedekind eta-function, *Topology*, **40** (2001), 945–960.