On Quantum Integers and Rationals

Bernard Le Stum, Adolfo Quirós

On quantum state of numbers

Bernard Le Stum & Adolfo Quirós*

Version of October 25, 2013

Abstract

We introduce the notions of quantum characteristic and quantum flatness for arbitrary rings. More generally, we develop the theory of quantum integers in a ring and show that the hypothesis of quantum flatness together with positive quantum characteristic generalizes the usual notion of prime positive characteristic. We also explain how one can define quantum rational numbers in a ring and introduce the notion of twisted powers. These results play an important role in many different areas of mathematics and will also be quite useful in a subsequent work of the authors.

Contents

Introduction

Quantum mathematics is obtained by making a *small* perturbation q on a usual mathematical object giving rise to its *q-analog*. Alternatively, one may consider the full collection of objects obtained for different values of q, giving rise to different *q-states* of the same usual object. We are interested here in the perturbations of the unit of a ring. And by *small*, we mean that q is a non trivial root of unity. Actually, the same process works for any perturbations q, which can be *big* (q transcendental) or even *trivial* ($q = 1$). One should not use the word *quantum* in this more general situation and instead say *twisted* for example. But we will not do this here because we are actually interested in the former case in the end.

Applying this principle to a usual number, we may consider the various quantum states of the realizations of this number. More precisely, if R is a ring with unit 1, one defines for any $q \in R$, the q-states of the first natural integers as follows:

$$(0)_q = 0, \quad (1)_q = 1, \quad (2)_q = 1 + q, \quad (3)_q = 1 + q + q^2, \quad \dots.$$

*Supported by grants MTM2009-07291 from Ministerio de Ciencia e Innovación (Spain) and MTM2012-35849 from Ministerio de Economía y Competitividad (Spain)

When $R = \mathbb{Z}$ is the ring of integers and $q = 1$, we recover usual natural numbers ; but if we allow some other $q > 0$, we get the so called q-integers in $\mathbb{Z}$. These q-integers may be used to develop q-combinatorics. For example the q-analog of a binomial coefficient will count the number of rational points of the corresponding Grassmanian over a finite field with q elements ([9], Theorem 7.1).

When $R = \mathbb{Z}[t]$ is the polynomial ring over the integers and $q = t$, then the q-analog of binomial coefficients are given by the *Gaussian polynomials* (these rational functions do live inside $\mathbb{Z}[t]$):

$$\binom{n}{k}_t := \frac{(1-t^n)(1-t^{n-1})\cdots(1-t^{n-k+1})}{(1-t^k)(1-t^{k-1})\cdots(1-t)} \in \mathbb{Q}(t).$$

This case is very important in the theory of integer partitions (Ramanujan generating q-series). See, for example, chapter 3 of [1] or section 1.8 in [16].

Note that we can consider the case $R = \mathbb{Z}[t]$ or $\mathbb{Q}(t)$, and $q = t$, as the generic situation and many formulas that will be valid for any ring R and any q can be recovered from this particular case.

When $R = \mathbb{C}$ and $q \neq 1$, we may more generally define the q-state of any complex number a once we make the choice of a branch of the logarithm that is defined at q:

$$(a)_q = \frac{1 - \exp(a \log(q))}{1-q} \in \mathbb{C}$$

(when $R = \mathbb{R}$ and $q > 0$, we can use the usual logarithm). When $|q| \neq 1$, we enter the realm of q-difference equations (see [4] for example). When q is a non trivial root of unity, then we get the numbers that appear in the theory of quantum groups (see [10] for example). Actually, the subjects in which q-analogs are fruitful keep expanding, from q-hypergeometric series (see [6] for a thorough treatment of q-Calculus or [9] for a more concise introduction) to Number Theory [2] or even Multiple q-Zeta Values [3].

Note that if R is a ring of characteristic $p > 0$ and $q = 1$, we will have $(p)_q = 0$. Also, if q is a primitive p-th root of unity for some integer $p \geq 2$, we will have $(p)_q = 0$ whatever the characteristic of R is. Therefore, it appears that from a quantum point of view, roots of unity and positive characteristic share a common property. Starting from this consideration, one may want to lift to characteristic zero some results that are already known in characteristic $p > 0$ at the cost of replacing usual mathematical objects by their q-analog where q is a root of unity. Michel Gros and the first author have been successful in doing this in [7] but we want to investigate this relation in more details in the future. For example, the three of us are developing a quantum confluence theory and will introduce quantum divided powers.

The purpose of this article is to present many properties of quantum numbers in a complete and general form with full proofs. Most - if not all - formulas can be found elsewhere in the literature (and this is particularly true for the formulas of section 2 that have been well known for a long time). However, they are usually stated with unnecessary hypothesis and their proofs often do not extend to the general case. We wish that our presentation will provide a quick and easy reference for the mathematical community.

In section 1, we define quantum integers (or more precisely, the quantum states of an integer) in a ring and study how the choice of the data will affect the behavior of those quantum integers. In particular, we introduce the notion of quantum characteristic and quantum flatness.

In section 2, we define quantum factorials and quantum binomial coefficients. Then we state and prove some classical results on binomial coefficients with a special emphasis on Lucas formula: it is valid under the assumptions of finite quantum characteristic and quantum flatness.

In section 3, we define the quantum state of a rational number. This seems new to us. Instead of choosing a branch of the logarithm as in the complex case, one need to make a compatible choice of roots. We will explain this in detail.

In section 4, we consider a commutative algebra endowed with an endomorphism and introduce the notion of twisted powers. We show that in the case of a dilatation, we recover some of the formulas that were obtained in the previous sections.

We wish to thank Michel Gros with whom we had many conversations related to the notions that are developed here.

Throughout this article, R denotes an associative ring with unit and q is an element of R.

1 Quantum integers

Definition 1.1 *If $m \in \mathbb{N}$, the* q-state *(also called* quantum state *when q is part of the data) of m is*

$$(m)_q = \sum_{i=0}^{m-1} q^i \in R.$$

We will also say that $(m)_q$ is a q-integer *(or a* quantum integer*) of R.*

If q is invertible in R and $m \neq 0$, we define the q-state of $-m$ as

$$(-m)_q = -\sum_{i=1}^{m} q^{-i} \in R$$

and we will also call $(-m)_q$ a q-integer*.*

In other words, we have

$$(0)_q = 0, \quad (1)_q = 1, \quad (2)_q = 1+q, \quad \ldots, \quad (m)_q = 1+q+\cdots+q^{m-1}, \quad \ldots$$

and when $q \in R^\times$,

$$(-1)_q = -\frac{1}{q}, \quad (-2)_q = -\frac{1}{q} - \frac{1}{q^2} = -\frac{1+q}{q^2}, \quad \ldots,$$
$$(-m)_q = -\frac{1}{q} - \cdots - \frac{1}{q^m} = -\frac{1+q+\cdots+q^{m-1}}{q^m}, \quad \ldots$$

Alternatively, one may define $(m)_q$ by induction on m as follows:

$$(0)_q := 0 \quad \text{and} \quad (m+1)_q := (m)_q + q^m.$$

One may also define $(m)_q := -q^m(-m)_q$ for $m < 0$ when $q \in R^\times$.

Remarks.

1. These formulas take place inside the subring of R generated by q (and q^{-1} if $q \in R^\times$). And this last ring is commutative. In particular, we should not worry to much about R being commutative or not.

2. When $u : R \to R'$ is a ring homomorphism with $u(q) = q'$, we have

   $$\forall m \in \mathbb{N}, \quad (m)_{q'} = u((m)_q)$$

   (and the same result for $m < 0$ when $q \in R^\times$). Using this property, we can reduce many (but not all) proofs, first to the case $R = \mathbb{Z}[t]$ and $q = t$, and then even to the case $R = \mathbb{Q}(t)$ and $q = t$.

3. When $v \in R^\times$, one also defines the *symmetric quantum state* of $n \in \mathbb{Z}$ (see for example section 1.3.3 of [13] or section VI.1 of [10]) by

   $$[n]_v = \frac{v^n - v^{-n}}{v - v^{-1}}.$$

   One can easily check that

   $$[n]_v = \frac{(n)_{v^2}}{v^{n-1}}.$$

   It follows that almost any formula from one theory can be translated into the other one.

Examples. 1. For $R = \mathbb{Q}(t)$ and $q = t$, we have

$$(m)_q = \frac{1 - t^m}{1 - t}.$$

2. When $q = 1_R$ is the unit of R (we will just say $q = 1$ in the future), we have $(m)_q = m1_R$. And the canonical map $\mathbb{Z} \to R$ induces a bijection

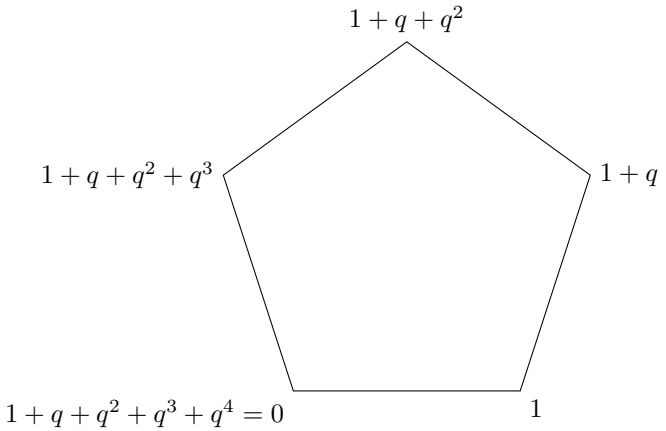
$$\mathbb{Z}/p\mathbb{Z} \longleftrightarrow \{q - \text{integers in } R\}$$

where $p := \text{Char}(R)$.

3. For $R = \mathbb{C}$ and $q = e^{\frac{2\pi\sqrt{-1}}{p}}$ with $p \in \mathbb{N} \setminus \{0\}$, we obtain again a bijection

$$\mathbb{Z}/p\mathbb{Z} \longleftrightarrow \{q - \text{integers in } R\}.$$

This is illustrated in the case $p = 5$ as follows:



The following result is immediate but very important:

Lemma 1.2 *For all $m \in \mathbb{N}$ (or $m \in \mathbb{Z}$ when $q \in R^\times$), we have*

$$(1 - q)(m)_q = 1 - q^m.$$

In particular, if $1 - q$ is invertible in R, we have

$$(m)_q = \frac{1 - q^m}{1 - q}. \tag{1}$$

Proof For $m \in \mathbb{N}$, we have

$$(1 - q)(m)_q = (1 - q)\sum_{i=0}^{m-1} q^i = \sum_{i=0}^{m-1} q^i - \sum_{i=1}^{m} q^i = 1 - q^m,$$

and when $q \in R^\times$,

$$(1 - q)(-m)_q = -(1 - q)\sum_{i=1}^{m} q^{-i} = -\sum_{i=1}^{m} q^{-i} + \sum_{i=0}^{m-1} q^{-i} = 1 - q^{-m}. \quad \square$$

Note that the condition of the second assertion in the lemma implies that $q \neq 1$. Conversely, if $q \neq 1$ and q belongs to some subfield K of R, then the condition is fulfilled. This will often be the case in practice and formula (1) is frequently used as an alternative definition for q-integers.

Proposition 1.3 *For all $m, n \in \mathbb{N}$ (or $\mathbb{Z}$ when $q \in R^\times$), we have*

$$(m+n)_q = (m)_q + q^m (n)_q \tag{2}$$

and

$$(mn)_q = (m)_q (n)_{q^m}. \tag{3}$$

Proof Pulling back along the canonical map $\mathbb{Z}[t] \to R$ (or $\mathbb{Z}[t, t^{-1}] \to R$ when $q \in R^\times$) that sends t to q, we may first assume that $R = \mathbb{Z}[t]$ (or $R = \mathbb{Z}[t, t^{-1}]$ in the second case) and $q = t$. Then, pushing through the embedding of R into $\mathbb{Q}(t)$, we may actually assume that $R = \mathbb{Q}(t)$ (and still $q = t$). Then, the formulas read

$$\frac{1-t^{m+n}}{1-t} = \frac{1-t^m}{1-t} + t^m \times \frac{1-t^n}{1-t}$$

and

$$\frac{1-t^{mn}}{1-t} = \frac{1-t^m}{1-t} \times \frac{1-(t^m)^n}{1-t^m} \quad \text{for } m \neq 0.$$

Of course, for $m = 0$, we have $(mn)_q = (0)_q = 0$ and also $(m)_q (n)_{q^m} = (0)_q (n)_1 = 0 \times n = 0$. □

Definition 1.4 *The* q-characteristic *(or* quantum characteristic *when q is fixed) of R is the smallest positive integer p such that $(p)_q = 0$ if it exists and 0 otherwise. We will then write* $q-\mathrm{char}(R) = p$.

Examples.

1. Assume that $q = 1$. Then, the quantum characteristic is the *usual* characteristic of the ring R.
2. If $R = K[t]$ is a polynomial ring over a commutative ring K, and $q = t$, then $q-\mathrm{char}(R) = 0$.
3. If $R = \mathbb{C}$ and $q = e^{\frac{2\pi\sqrt{-1}}{p}}$, then the q-characteristic of R is p.
4. Assume $R = \mathbb{Z}/n\mathbb{Z}$ and $1 \neq q = \bar{m} \in R$. Then the reader can check that

$$q-\mathrm{char}(R) > 0 \Leftrightarrow q \in R^\times.$$

More precisely, one shows that the q-characteristic of R is the order of m in $(\mathbb{Z}/(m-1)n\mathbb{Z})^\times$.

Proposition 1.5 *Let p be a positive integer. If $q-\mathrm{char}(R) = p$, then q is a p-th a root of unity. In particular, q is invertible.*

Proof We have $1 - q^p = (1-q)(p)_q$. Thus, if $(p)_q = 0$, we have $q^p = 1$ and q is a root of unity. □

Proposition 1.6 *If $q-\mathrm{char}(R) = p$, then the set of $m \in \mathbb{N}$ such that $(m)_q = 0$ is exactly the monoid $p\mathbb{N}$.*

If we allow $m < 0$ when $q \in R^\times$, then we get $p\mathbb{Z}$.

Proof When $p = 0$, this is clear. If $p > 0$, we can always write $m = np + r$ with $0 \leq r < p$ and $n \in \mathbb{N}$. Using proposition 1.3, one sees that

$$(m)_q = q^r (np)_q + (r)_q = q^r (n)_{q^p} (p)_q + (r)_q = (r)_q$$

and therefore

$$(m)_q = 0 \Leftrightarrow (r)_q = 0 \Leftrightarrow r = 0 \Leftrightarrow m \in p\mathbb{N}. \quad \square$$

Proposition 1.7 *Assume that* $q-\mathrm{char}(R) = p > 0$. *Then we have*

1. *If* $m, n \in \mathbb{Z}$ *satisfy* $m \equiv n \mod p$, *then* $(m)_q = (n)_q$.
2. *If* $m \in \mathbb{Z}$ *is prime with* p, *then* $(m)_q$ *is invertible.*

Proof We will use both the fact that $(p)_q = 0$ and its immediate consequence $q^p = 1$. For the first assertion, we may write $m = pv + n$ with $v \in \mathbb{Z}$. We obtain

$$(m)_q = (pv + n)_q = (p)_q(v)_{q^p} + q^{pv}(n)_q = (n)_q.$$

For the second one, we may write $mu = pv + 1$ with $u, v \in \mathbb{Z}$ and we get

$$(m)_q(u)_{q^m} = (mu)_q = (pv + 1)_q = (p)_q(v)_{q^p} + q^{pv}(1)_q = 1. \quad \square$$

For further use, we prove the following:

Lemma 1.8 *Let* $m \in \mathbb{N} \setminus \{0\}$. *Assume* R *has no* $(m)_q$*-torsion. Then, we have* $(m)_q = 0$ *if and only if one of the following conditions is fulfilled:*

1. q *is a non trivial* m*-th root of unity.*
2. $\mathrm{Char}(R) \mid m$ *and* $q = 1$.

In both cases, q *is an* m*-th root of unity and, in particular, it is invertible.*

Note that the lemma is also valid for $m < 0$ when $q \in R^\times$.

Proof Our hypothesis means that

$$(m)_q a = 0 \Leftrightarrow ((m)_q = 0 \text{ or } a = 0).$$

Since $(m)_q(1 - q) = 1 - q^m$, we see that q is an m-th root of unity if and only if $(m)_q = 0$ or $q = 1$. In the case $q \neq 1$, we obtain that $(m)_q = 0$ if and only if q is an m-th root of unity. When $q = 1$, the quantum state of m is m itself, but seen as an element of R. In particular, $(m)_1 = 0$ if and only if $p \mid m$ where $p = \mathrm{Char}(R)$. $\square$

Definition 1.9
1. *The ring* R *is said to be* q-flat *(or* quantum-flat *when the reference to* q *is clear) if* R *has no* $(m)_q$*-torsion for any* $m \in \mathbb{N}$.
2. *The ring* R *is said to be* q-divisible *(or* quantum-divisible *when the reference to* q *is clear) if* $(m)_q \in R^\times$ *whenever* $(m)_q \neq 0$.

Saying that R is q-flat means that

$$\forall m \in \mathbb{N}, a \in R, \quad (m)_q a = 0 \Leftrightarrow ((m)_q = 0 \text{ or } a = 0).$$

Note that the condition will then also hold for $m < 0$ when $q \in R^\times$.

Of course, q-divisibility always implies q-flatness.

Examples.
1. If R is an integral domain (resp. a field), it is q-flat (resp. q-divisible) whatever q is. In particular, if $R = \mathbb{C}$ and $q = e^{\frac{2\pi\sqrt{-1}}{p}}$, then R is q-divisible (and therefore q-flat).
2. Assume that $q = 1$. Then, quantum-flat means either that R has no $\mathbb{Z}$-torsion (in which case $\mathrm{Char}(R) = 0$) or else that R is an $\mathbb{F}_p$-algebra for some prime p (and then $\mathrm{Char}(R) = p > 0$). And quantum-divisible means that R is an algebra over a field (whose characteristic is is the characteristic of R).

3. If $R = K[t]$ is a polynomial ring over a commutative ring K, and $q = t$, then R is q-flat. But R is clearly *not* q-divisible.

4. If $q = -1$, then R is q-divisible because $(m)_q$ only takes values 0 and 1 (and same for $q = 0$).

The flatness condition might sound odd but the quantum characteristic can have a rather strange behavior in general as the following examples show:

Examples. 1. If q is the image of X in $R = \mathbb{Q}[X]/(X^2 - 1)$ then q is a primitive square root of unity but $q-\mathrm{char}(R) = \mathrm{Char}(R) = 0$.

2. If q is the image of X in $R = \mathbf{F}_2[X]/(X^2 - 1)$ then q is a primitive square root of unity but $q-\mathrm{char}(R) = 4$ and $\mathrm{Char}(R) = 2$.

3. If $q = 1$ and $R = \prod \mathbb{Z}/n\mathbb{Z}$ then $q-\mathrm{char}(R) = \mathrm{Char}(R) = 0$ but R has $(m)_q$-torsion for all $m \neq 0$.

However, things get better under quantum flatness hypothesis:

Proposition 1.10 *Assume that R is q-flat and let p be a positive integer. Then $q-\mathrm{char}(R) = p$ if and only if one of the following conditions is satisfied.*

1. *q is a non-trivial primitive p-th root of unity.*

2. *$q = 1$ and $\mathrm{Char}(R) = p$.*

In both cases, q is a p-th root of unity and, in particular, it is invertible.

Proof It follows from lemma 1.8 that $(p)_q = 0$ and that either q is a non-trivial root of unity or else that $q = 1$ and $\mathrm{Char}(R) > 0$. In the first case, q is a primitive p-th root of unity if and only if p is the smaller positive integer m such that q is an m-th root of unity. In the second case, $\mathrm{Char}(R) = p$ if and only if p is the smaller positive integer m such that $\mathrm{Char}(R) \mid m$. Therefore, the assertion follows from lemma 1.8 and the very definition of quantum characteristic. □

When the quantum characteristic is even, we can do a little better:

Proposition 1.11 *If R is q-flat and $q-\mathrm{char}(R) = 2k > 0$, then $q^k = -1$.*

Proof Since $(k)_q(2)_{q^k} = (2k)_q = 0$ and R is q-flat, we must have $1 + q^k = (2)_{q^k} = 0$. □

Remarks. The fact that R is q-flat is crucial as the following example shows: if $R = \mathbb{Z}/8\mathbb{Z}$ and $q = 3$, we have $q-\mathrm{char}(R) = 4$ but $q^2 = 1 \neq -1$.

Proposition 1.12 *If R has no $\mathbb{Z}$-torsion and $q-\mathrm{char}(R) = p > 0$, then q is a primitive p-th root of unity.*

Proof Since $(p)_q = 0$, lemma 1.8 tells us that q is a p-th root of unity. Assume that q is not primitive. Then, there exists $1 \leq m < p$ with $p = mn$ such that $q^m = 1$. It follows from (3) that

$$0 = (p)_q = (m)_q(n)_1 = n(m)_q.$$

Since R has no $\mathbb{Z}$-torsion, necessarily $(m)_q = 0$ and this contradicts the minimality of p. □

Proposition 1.13 *If $q-\mathrm{char}(R)$ is a prime number p, then R is q-divisible (and therefore also q-flat).*

Proof It follows from proposition 1.7 that $(m)_q = 0$ when m is a multiple of p and that $(m)_q$ is invertible otherwise. $\square$

Remarks. The condition m prime to p in the second statement of proposition 1.7 is necessary even if R is q-flat as the following example shows. If $R = \mathbb{Z}[\sqrt{-1}]$ and $q = \sqrt{-1}$, we have $q-\mathrm{char}(R) = 4$ and $(2)_q = 1 + \sqrt{-1} \notin R^\times$.

Lemma 1.14 *If $\chi_m \in \mathbb{Z}[t]$ denotes the m-th cyclotomic polynomial, we have whenever $n > 0$,*

$$(n)_q = \prod_{m|n, m\neq 1} \chi_m(q).$$

Proof We may assume that $R = \mathbb{Z}[t]$ and that $q = t$. Then our assertion follows from the classical formula

$$1 - t^n = \prod_{n=md} \chi_m. \quad \square$$

When R is q-flat, the next result may be used to reduce some proofs to the case $R = \mathbb{C}$ and $q = e^{\frac{2\pi\sqrt{-1}}{p}}$:

Proposition 1.15 *Assume that R is q-flat with $q-\mathrm{char}(R) = p > 0$ and let $\zeta \in \mathbb{Q}^{\mathrm{alg}}$ be a primitive p-th root of unity. Then, there exists a unique ring homomorphism $\mathbb{Z}[\zeta] \to R$ that sends ζ to q.*

Proof Let us consider the unique ring homomorphism $u : \mathbb{Z}[t] \to R$ that sends t to q. With the notations of lemma 1.14 we see that if $1 < n < p$, then R has no $\chi_n(q)$-torsion (use the formula). The same formula applied to the case $n = p$ then implies that $\chi_p(q) = 0$. It follows that $\ker u$ contains the cyclotomic polynomial χ_p and factors therefore through $\mathbb{Z}[\zeta] := \mathbb{Z}[t]/\chi_p$. $\square$

It will be quite important to understand the behavior of quantum characteristic, quantum flatness and quantum divisibility under the rising of q to some power.

Proposition 1.16 *Assume $q-\mathrm{char}(R) = p > 0$ and let $k \in \mathbb{N}$ be such that $p \nmid k$ and R has no $(k)_q$-torsion.*

1. *If R is q-flat (resp. q-divisible), then R is q^k-flat (resp. q^k-divisible).*
2. *If $d = (p, k)$ denotes the greatest common divisor of p and k, then $q^k-\mathrm{char}(R) = p/d$.*

Note that the condition $p \nmid k$ is equivalent to $(k)_q \neq 0$ and that both hypothesis on k are satisfied when $(k)_q \in R^\times$.

Proof We let $m \in \mathbb{N}$. Recall that $(km)_q = (k)_q (m)_{q^k}$. Since we assume that R has no $(k)_q$-torsion and that $(k)_q \neq 0$, we see that $(km)_q = 0$ is equivalent to $(m)_{q^k} = 0$. But $(km)_q = 0$ means exactly that $p \mid km$ and this happens if and only if $p/d \mid m$. Thus, we obtain the expected formula for the q^k-characteristic.

Now, we let $a \in R$ with $a \neq 0$. If R is q-flat and $(m)_{q^k} a = 0$, then we will have $(km)_q a = 0$ which implies that $(km)_q = 0$. And we just saw that $(km)_q = 0$ if and only if $(m)_{q^k} = 0$. Thus we see that R is q^k-flat.

Assume now that R is q-divisible. We know that $(m)_{q^k} \neq 0$ if and only if $(km)_q \neq 0$, but then necessarily $(km)_q \in R^\times$ and therefore also $(m)_{q^k} \in R^\times$ because of the above equality $(km)_q = (k)_q (m)_{q^k}$ again. And we see that R is q^k-divisible. $\square$

Remarks. 1. The condition $p \nmid k$ in the proposition is really necessary because otherwise R might be q-divisible but not even q^k-flat. This is the case for example if $R = \mathbb{Z}/4\mathbb{Z}$, $q = -1$ and $k = 2$.

2. Note also that if $p \mid k$, then $q^k-\mathrm{char}(R)$ is the usual characteristic of R. In particular, it may be equal to 0 whatever p is.

3. Finally, the converse implications are false in general: if $R = \mathbb{Z}[\sqrt{-1}]$, $q = \sqrt{-1}$ and $k = 2$, we see that R is q^k-divisible but not q-divisible.

The last result of this section shows the relation between the dynamics of affine endomorphisms and quantum numbers.

Proposition 1.17 *Assume R is a commutative ring. Let A be an R-algebra and σ an R-endomorphism of A. Assume that $\sigma(x) = qx+h$ with $q, h \in R$. Then, for all $n \in \mathbb{N}$ (or even $n \in \mathbb{Z}$ when $q \in R^\times$ and σ is bijective), we have*

1. $\sigma^n(x) = q^n x + (n)_q h$
2. $x - \sigma^n(x) = (n)_q(x - \sigma(x))$

Proof By induction on $n \in \mathbb{N}$, we have

$$\sigma^{n+1}(x) = \sigma(q^n x + (n)_q h) = q^n(qx + h) + (n)_q h)$$

$$= q^{n+1}x + ((n)_q + q^n)h = q^{n+1}x + (n+1)_q h$$

and the case of a non-negative integer is settled. Moreover, it follows that, when $q \in R^\times$ and σ is bijective, we have

$$x = \sigma^{-n}(q^n x + (n)_q h) = q^n \sigma^{-n}(x) + (n)_q h$$

and therefore,

$$\sigma^{-n}(x) = q^{-n}x - q^{-n}(n)_q h = q^{-n}x + (-n)_q h.$$

It remains to prove the second assertion. We have:

$$x - \sigma^n(x) = x - q^n x - (n)_q h = (1 - q^n)x - (n)_q h = (n)_q(1 - q)x - (n)_q h$$

$$= (n)_q(x - qx - h) = (n)_q(x - \sigma(x)). \quad \square$$

Remarks. Even if we are only interested in commutative rings, non commutative ones might show up. This is the case for example if R is commutative, $A = R[x]$ denotes the polynomial ring in the variable x over R and we consider the ring S of R-endomorphisms of A. In particular, if $q \in R$, there exists a unique $\sigma \in S$ such that $\sigma(x) = qx$. Then, in this case, we have $\sigma-\mathrm{char}(S) = q-\mathrm{char}(R)$.

2 Quantum binomial coefficients

Recall that we work over a fixed ring R and with a fixed $q \in R$.

Definition 2.1 *The q-*factorial *(or* quantum factorial*) of $m \in \mathbb{N}$ is*

$$(m)_q! := \prod_{i=0}^{m-1} (m - i)_q.$$

Of course, since $(1)_q = 1$, we could stop at $i = m-2$ as well.

In other words, we have

$$(0)_q! = (1)_q! = 1, \quad (2)_q! = (2)_q = 1+q, \quad (3)_q! = (3)_q(2)_q = 1+2q+2q^2+q^3,$$

and for bigger m,

$$(m)_q! := (m)_q(m-1)_q \cdots (3)_q(2)_q.$$

Examples. 1. If $q = 1$ and $\mathbb{Z} \subset R$, then $(m)_q! = m!$ is the usual factorial.

2. More generally, when $q = 1$, we have $(m)_q! = m!1_R$. In particular, we see that $(m)_q! = 0$ for $m \geq p$ when $q = 1$ and $\mathrm{Char}(R) = p > 0$.

3. When $R = \mathbb{Q}(t)$ and $q = t$, we have

$$(m)_q! = \frac{(1-t^m)(1-t^{m-1})\cdots(1-t^2)(1-t)}{(1-t)^m}$$

4. If $R = \mathbb{C}$ and $q = e^{2\pi\sqrt{-1}/p}$ with p an integer ≥ 2, we have

$$(m)_q! = \begin{cases} \frac{(1-e^{2m\pi\sqrt{-1}/p})(1-e^{2(m-1)\pi\sqrt{-1}/p})\cdots(1-e^{2\pi\sqrt{-1}/p})}{(1-e^{2\pi\sqrt{-1}/p})^m} & \text{if} \quad m < p \\ 0 & \text{if} \quad m \geq p. \end{cases}$$

Proposition 2.2 *If $q-\mathrm{char}(R) = p$, then $(m)_q! = 0$ for $m \geq p$.*

Proof Immediate consequence of the definition. □

Proposition 2.3 *For all $m \in \mathbb{N}$, we have*

$$(1-q)^m(m)_q! = \prod_{i=0}^{m-1}(1-q^{m-i}).$$

In particular, if $1-q$ is invertible in R, we have

$$(m)_q! = \frac{(1-q^m)(1-q^{m-1})\cdots(1-q^2)(1-q)}{(1-q)^m}.$$

Proof Follows from lemma 1.2. □

Proposition 2.4 *If $\chi_m \in \mathbb{Z}[t]$ denotes the m-th cyclotomic polynomial, we have for all $n \in \mathbb{N}$,*

$$(n)_q! = \prod_{m \neq 1} \chi_m(q)^{[\frac{n}{m}]}$$

where $[\frac{n}{m}]$ is the integer part of $\frac{n}{m}$.

Proof We saw in lemma 1.14 that we have for all $k \in \mathbb{N}$,

$$(k)_q = \prod_{m|k, m\neq 1} \chi_m(q).$$

On the other hand, one easily sees that for all $m \in \mathbb{N}$, we have

$$\#\{k \leq n, m \mid k\} = \left[\frac{n}{m}\right],$$

and the formula follows. □

Definition 2.5 *The* q-binomial coefficients *(or* quantum binomial coefficients*) are defined by induction for* $k, n \in \mathbb{N}$ *via* Pascal identities

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q$$

with

$$\binom{0}{k}_q = \begin{cases} 1 \text{ if } k = 0 \\ 0 \text{ otherwise.} \end{cases}$$

Remarks. If we want to use the "symmetric quantum state" (as it is usually the case in quantum group theory),

$$[n]_v := \frac{v^n - v^{-n}}{v - v^{-1}},$$

then we will have

$$[n]_v! = \frac{1}{v^{\frac{n(n-1)}{2}}}(n)_{v^2}! \quad \text{and} \quad \begin{bmatrix} n \\ k \end{bmatrix}_v = \frac{1}{v^{\frac{n(n-k)}{2}}}\binom{n}{k}_{v^2}.$$

Examples. When $R = \mathbb{Z}$ and q is a power of a prime p, then $\binom{n}{k}_q$ is the number of rational points of the Grassmanian $\mathbb{G}(n, k, q)$. Said differently, this is the number of vector subspaces of dimension k in a vector space of dimension n over a field with q elements. This is easily checked (see also [9], Theorem 7.1).

Proposition 2.6 *We have for all* $n, k \in \mathbb{N}$,

$$\binom{n}{k}_q \prod_{i=0}^{k-1}(k-i)_q = \prod_{i=0}^{k-1}(n-i)_q.$$

In particular, if $q-\mathrm{char}(R) = 0$ *and* R *is* q*-divisible, then*

$$\binom{n}{k}_q = \frac{(n)_q!}{(k)_q!(n-k)_q!}. \tag{4}$$

Proof In order to prove the first assertion, we may first assume that $R = \mathbb{Z}[t]$ and $q = t$, and then specialize to any R and q. We may even assume that $R = \mathbb{Q}(t)$. In particular, all non zero q-integers will be invertible in R and it is therefore sufficient to prove the second assertion. We can use lemma 1.2 in order to show that the right member of equality (4) satisfies the induction property of the left member. This works as follows:

$$\frac{(n-1)_q!}{(k-1)_q!(n-k)_q!} + q^k \frac{(n-1)_q!}{(k)_q!(n-k-1)_q!}$$

$$= \frac{((k)_q + q^k(n-k)_q)(n-1)_q!}{(k)_q!(n-k)_q!} = \frac{(n)_q!}{(k)_q!(n-k)_q!}. \quad \square$$

Corollary 2.7 *We have for all* $n, k \in \mathbb{N}$,

$$\binom{n}{n-k}_q = \binom{n}{k}_q.$$

Proof We may assume as above than $R = \mathbb{Q}(t)$ and $q = t$ and use formula (4). $\square$

Corollary 2.8 *We have for all $k, n \in \mathbb{N}$,*

$$(1-q^k)(1-q^{k-1})\cdots(1-q)\binom{n}{k}_q = (1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1}).$$

In particular, if $1-q^i$ is invertible for all $0 < i \leq k$, we will have

$$\binom{n}{k}_q = \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})\cdots(1-q)}. \quad \square$$

Remarks. 1. The rational function

$$\frac{(1-t^n)(1-t^{n-1})\cdots(1-t^{n-k+1})}{(1-t^k)(1-t^{k-1})\cdots(1-t)} \in \mathbb{Q}(t)$$

actually lives in $\mathbb{Z}[t]$ and is called a *Gaussian polynomial*. It is identical to the binomial coefficient $\binom{n}{k}_t$.

2. One may prove many properties of quantum binomial coefficients by reducing to the case $R = \mathbb{Q}(t)$ and $q = t$ and using various references in the literature (see for example [10], section IV.2).

3. Actually, one may as well assume that $R = \mathbb{C}$ because it is always possible to embed $\mathbb{Q}(t)$ into $\mathbb{C}$ by sending t to any transcendental $q \in \mathbb{C}$.

One may also define the quantum binomial coefficients as a product as we can see for example in [11]:

Corollary 2.9 *We have for all $n \in \mathbb{N}$,*

$$\binom{n}{k}_q = \prod_{[\frac{n}{m}]>[\frac{k}{m}]+[\frac{n-k}{m}]} \chi_m(q)$$

where $\chi_m \in \mathbb{Z}[t]$ denotes the m-th cyclotomic polynomial and $[r]$ denotes the integer part of a real number r.

The condition under the product says that the sum of the rests in the euclidean division of k and $n-k$ by m is at least equal to m.

Proof We may assume that $q-\mathrm{char}(R) = 0$ and R is q-divisible. Then, formula (4) and proposition 2.4 give

$$\binom{n}{k}_q = \prod_{m\neq 1} \chi_m(q)^{[\frac{n}{m}]-[\frac{k}{m}]-[\frac{n-k}{m}]}$$

and we have $[\frac{n}{m}]-[\frac{k}{m}]-[\frac{n-k}{m}] = 0$ unless $[\frac{n}{m}] > [\frac{k}{m}]+[\frac{n-k}{m}]$ in which case $[\frac{n}{m}]-[\frac{k}{m}]-[\frac{n-k}{m}] = 1$. Note that this never happens when $m = 1$. $\square$

Proposition 2.10 *We have*

$$\forall n, j, k \in \mathbb{N}, \quad \binom{n}{j}_q \binom{j}{k}_q = \binom{n}{k}_q \binom{n-k}{n-j}_q.$$

Proof We may assume that $R = \mathbb{Q}(t)$ and $q = t$ and our formula reads

$$\frac{(n)_t!}{(j)_t!(n-j)_t!} \quad \frac{(j)_t!}{(k)_t!(j-k)_t!} = \frac{(n)_t!}{(k)_t!(n-k)_t!} \quad \frac{(n-k)_t!}{(n-j)_t!(j-k)_t!}. \quad \square$$

We can also state and prove the *quantum Chu-Vandermonde identity*:

Lemma 2.11 *We have*

$$\forall n,m,k\in\mathbb{N},\quad \binom{n+m}{k}_q=\sum_{i=0}^{k}q^{i(m-k+i)}\binom{n}{i}_q\binom{m}{k-i}_q.$$

Recall that, with our conventions, we have $\binom{n}{i}_q=0$ for $i>n$ and $\binom{m}{k-i}_q=0$ for $k-i>m$.

Proof This is shown to be true by induction on m. We will have

$$\binom{n+m}{k}_q=\binom{n+m-1}{k-1}_q+q^k\binom{n+m-1}{k}_q$$

$$=\sum_{i=0}^{k-1}q^{i(m-k+i)}\binom{n}{i}_q\binom{m-1}{k-1-i}_q+q^k\sum_{i=0}^{k}q^{i(m-1-k+i)}\binom{n}{i}_q\binom{m-1}{k-i}_q$$

$$=\sum_{i=0}^{k}q^{i(m-k+i)}\binom{n}{i}_q\left(\binom{m-1}{k-1-i}_q+q^{k-i}\binom{m-1}{k-i}_q\right)$$

$$=\sum_{i=0}^{k}q^{i(m-k+i)}\binom{n}{i}_q\binom{m}{k-i}_q.\quad\square$$

Lemma 2.12 *Assume $q-\mathrm{char}(R)=p>0$ and R is q-flat, then*

$$\binom{p}{k}_q=\begin{cases}1 & \text{if } k=0 \text{ or } k=p\\ 0 & \text{otherwise.}\end{cases}\qquad\square$$

Proof We may assume $0<k<p$. Since $q-\mathrm{char}(R)=p>0$, we will have

$$(k)_q(k-1)_q\cdots(2)_q\binom{p}{k}_q=(p)_q(p-1)_q\cdots(p-k+1)_q=0.$$

And since we assume that R is q-flat, we must have

$$\binom{p}{k}_q=0.\quad\square$$

Remarks. The condition will always be satisfied when p is prime. Actually, when $q=1$, the flatness condition is equivalent to p being prime. However, this is not necessary in general.

Examples.

1. Assume $R=\mathbb{C}$ and $q=e^{\frac{2\sqrt{-1}\pi}{p}}$ with $p\in\mathbb{N}$ (not necessary prime) and $p\geq 2$. Then we have $\binom{p}{k}_q=0$ for $0<k<p$.
2. Assume R is an $\mathbb{F}_p$-algebra for some prime number p. Then $\binom{p}{k}=0$ for $0<k<p$.
3. Assume $R=\mathbb{Z}/4\mathbb{Z}$ and $q=1$. Then we have $\binom{4}{2}_q=2\neq 0$.

We can now prove the *quantum Lucas theorem* (see also lemma 24.1.2 of [13]):

Proposition 2.13 *Assume $q-\mathrm{char}(R) = p > 0$ and R is q-flat. Let $n, k, i, j \in \mathbb{N}$ with $i, j < p$. Then, we have*

$$\binom{np+i}{kp+j}_q = \binom{n}{k}\binom{i}{j}_q.$$

With our convention, it means in particular that

$$\binom{np+i}{kp+j}_q = 0 \quad \text{if } 0 \leq i < j < p.$$

Proof We proceed by induction on n and i, and we use the quantum Pascal identity

$$\binom{np+i}{kp+j}_q = \binom{np+i-1}{kp+j-1}_q + q^{kp+j}\binom{np+i-1}{kp+j}_q. \tag{5}$$

We only do the non trivial cases.

Assume first that $n, k > 0$ but $i = j = 0$. Then the formula reads

$$\binom{np}{kp}_q = \binom{(n-1)p+p-1}{(k-1)p+p-1}_q + q^{kp}\binom{(n-1)p+p-1}{kp}_q$$

$$= \binom{n-1}{k-1}\binom{p-1}{p-1}_q + \binom{n-1}{k}\binom{p-1}{0}_q = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

as expected.

Assume now that $n, j > 0$ but $i = 0$. Then formula (5) reads

$$\binom{np}{kp+j}_q = \binom{(n-1)p+p-1}{kp+j-1}_q + q^{kp+j}\binom{(n-1)p+p-1}{kp+j}_q$$

$$= \binom{n-1}{k}\binom{p-1}{j-1}_q + q^j\binom{n-1}{k}\binom{p-1}{j}_q = \binom{n-1}{k}\left(\binom{p-1}{j-1}_q + q^j\binom{p-1}{j}_q\right)$$

$$= \binom{n-1}{k}\binom{p}{j}_q = 0$$

thanks to lemma 2.12.

Now, if $i, j > 0$, the formula reads

$$\binom{np+i}{kp+j}_q = \binom{n}{k}\binom{i-1}{j-1}_q + q^j\binom{n}{k}\binom{i-1}{j}_q$$

$$= \binom{n}{k}\left(\binom{i-1}{j-1}_q + q^j\binom{i-1}{j}_q\right) = \binom{n}{k}\binom{i}{j}_q.$$

Finally, in the case $i, k > 0$ but $j = 0$, formula (5) gives

$$\binom{np+i}{kp}_q = \binom{np+i-1}{kp-1}_q + q^{kp}\binom{np+i-1}{kp}_q$$

$$= \binom{np+i-1}{(k-1)p+p-1}_q + \binom{np+i-1}{kp}_q = \binom{n}{k-1}\binom{i-1}{p-1}_q + \binom{n}{k}\binom{i-1}{0}_q$$

$$= \binom{n}{k-1} \times 0 + \binom{n}{k} \times 1 = \binom{n}{k} = \binom{n}{k}\binom{i}{0}_q$$

because $0 \leq i-1 < p-1 < p$. $\square$

Remarks. 1. We recover the usual Lucas theorem in arithmetics from the case $R = \mathbb{F}_p$ and $q = 1$ of the proposition: if $n = \sum a_i p^i$ and $k = \sum b_i p^i$ denote the p-adic expansions of n and k (p a *prime* number), we have

$$\binom{n}{k} \equiv \prod_i \binom{a_i}{b_i} \mod p.$$

2. In the case where $R = \mathbb{C}$ is the field of complex numbers and $q = \zeta$ is a primitive p-th root of unity, we recover proposition 2.1 of [8].

3. Using proposition 1.15, one can also derive the quantum Lucas theorem from the case $R = \mathbb{C}$. This gives a proof of the classical Lucas theorem using the theory of complex functions.

Finally, we prove the binomial quantum formula:

Proposition 2.14 *Assume that R is commutative and let A be a commutative R-algebra. Then, we have*

$$\forall n \in \mathbb{N}, \quad \prod_{i=0}^{n-1} (q^i x + y) = \sum_{k=0}^{n} q^{\frac{k(k-1)}{2}} \binom{n}{k}_q x^k y^{n-k}.$$

Proof By induction on n, we see that

$$\prod_{i=0}^{n-1} (q^i x + y) = \left(\sum_{k=0}^{n-1} q^{\frac{k(k-1)}{2}} \binom{n-1}{k}_q x^k y^{n-1-k} \right) (q^{n-1} x + y)$$

$$= \left(\sum_{k=0}^{n-1} q^{\frac{k(k-1)}{2}+n-1} \binom{n-1}{k}_q x^{k+1} y^{n-1-k} \right) + \left(\sum_{k=0}^{n-1} q^{\frac{k(k-1)}{2}} \binom{n-1}{k}_q x^k y^{n-k} \right)$$

$$= \left(\sum_{k=1}^{n} q^{\frac{(k-1)(k-2)}{2}+n-1} \binom{n-1}{k-1}_q x^k y^{n-k} \right) + \left(\sum_{k=0}^{n-1} q^{\frac{k(k-1)}{2}} \binom{n-1}{k}_q x^k y^{n-k} \right)$$

$$= \left(\sum_{k=0}^{n} q^{\frac{k(k-1)}{2}} \left(q^{n-k} \binom{n-1}{k-1}_q + \binom{n-1}{k}_q \right) x^k y^{n-k} \right)$$

$$= \sum_{k=0}^{n} q^{\frac{k(k-1)}{2}} \binom{n}{k}_q x^k y^{n-k}. \quad \square$$

Remarks. If instead of assuming A commutative, we make the supposition that $yx = qxy$ (*quantum plane identity*), then the formula becomes even nicer:

$$\forall n \in \mathbb{N}, \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k}_q x^k y^{n-k}$$

(see proposition IV.2.2 of [10] for example).

3 Quantum rational numbers

We are going to define the quantum states of a rational number. We might call them quantum rational numbers (as in [14]) but they should not be confused with the quantum rational numbers that appear in quantum physics (see in chapter 6 of [15] for example).

We start with some generalities about roots in monoids, generalizing divisibility in additive (commutative) monoids. In the end, we will apply these considerations to the multiplicative monoid of R.

We recall that a monoid S is a set endowed with a law which is associative with unit. Usually, this law is written multiplicatively, but we might also use the addition when the law is commutative.

Definition 3.1 *Let S be a monoid. A family $\{s_n\}_{n\in D}$ with $\emptyset \neq D \subset \mathbb{N}\setminus\{0\}$ is a* system of roots *in S if it satisfies:*

$$\forall n, n' \in D, \forall m, m' \in \mathbb{N}, \quad m'n = mn' \Rightarrow s_{n'}^{m'} = s_n^m.$$

In other words, we require that s_n^m only depends on $r := \frac{m}{n} \in \mathbb{Q}$ when $n \in D$ and $m \in \mathbb{N}$. In particular, $s := s_n^n$ does not depend on $n \in D$ and we will also call $\{s_n\}_{n\in D}$ a *system of roots of s*.

We specialize a little bit the definition:

Definition 3.2 *Let S be a monoid and $\underline{s} := \{s_n\}_{n\in D}$ a system of roots of $s \in S$.*

1. *In the case $D := \{p\}$, we will call s_p a* p-th root of s.
2. *In the case $D := \{p^i, i \in \mathbb{N}\}$, we will call $\underline{s}$ a* system of p-th roots of s.
3. *In the case $D = \mathbb{N}\setminus\{0\}$, we will call $\underline{s}$ a* complete system of roots of s.

For p-th roots, or more generally, for systems of p-th roots, there exists a simpler alternative definition:

Proposition 3.3 *Let S be a monoid and $s \in S$.*

1. *If $p \in \mathbb{N}\setminus\{0\}$, giving a p-th root of s is equivalent to giving an element $s_1 \in S$ such that $s = s_1^p$.*
2. *If $p \in \mathbb{N}\setminus\{0\}$, giving a system of p-th roots of s is equivalent to giving a sequence $\{s_i\}_{i\in\mathbb{N}}$ of $s_i \in S$ such that $s_0 = s$ and $s_{i+1}^p = s_i$.*

Proof In the first assertion, the condition of the definition is void and we have $s_p^p = s$. Thus, we obtain the result after a renumbering $s_p \rightsquigarrow s_1$.

For the second assertion, one easily checks that the condition in the definition is implied by

$$\forall i \in \mathbb{N}, \quad s_{p^{i+1}}^p = s_{p^i}.$$

And the result therefore follows also from a renumbering $s_{p^i} \rightsquigarrow s_i$. □

Any monoid S has a *natural preorder* (reflexive and transitive relation) given by

$$s \leq s' \quad \Leftrightarrow \quad \exists m \in \mathbb{N}, s' = s^m.$$

For example, the natural preorder on the additive monoid $\mathbb{N}$ is given by divisibility (and not the usual order on $\mathbb{N}$). Note that any morphism of monoids preserves the preorder. Finally, recall that a preordered set is *inductive* (or *directed*) if any couple has an upper bound:

$$\forall s, s' \in S, \quad \exists s'' \in S \quad s \leq s'' \text{ and } s' \leq s''.$$

Remarks.

1. When the index set D is inductive (for divisibility), the condition of definition 3.1 is equivalent to
$$\forall n, n' \in D, \forall m \in \mathbb{N}, \quad n = mn' \Rightarrow s_{n'} = s_n^m.$$
2. When D is inductive, the family $\{s_n\}_{n\in D}$ is inductive for the *reverse* preorder.
3. In the special cases above, the index set is inductive (and therefore, the system of roots is inductive for the reverse preorder).

Definition 3.4 *Let N be a submonoid of the additive monoid $\mathbb{Q}_{\geq 0}$. A denominator for N is an element $n \in \mathbb{N} \setminus \{0\}$ such that $\frac{1}{n} \in N$. A subset $D \subset \mathbb{N} \setminus \{0\}$ is a* full set of denominators *for N if $\frac{1}{D} := \{\frac{1}{n}, n \in D\}$ is a set of generators for N.*

If $E \subset N$ is a set of generators for an additive (commutative) monoid N, we will write $N = \mathbb{N}E$. Thus, we see that D is a full set of denominators for N if $N = \mathbb{N}\frac{1}{D}$.

Recall also that if N is an additive monoid, there exists a smallest abelian group $\pm N$ that contains N. More precisely, the forgetful functor from abelian groups to commutative monoids has a left adjoint $N \mapsto \pm N$. Note that when N is a submonoid of $\mathbb{Q}_{\geq 0}$, we may assume $\pm N \subset \mathbb{Q}$, and then we have $N = \pm N \cap \mathbb{Q}_{\geq 0}$.

Examples. 1. For $D := \{p\}$ with $p \in \mathbb{N} \setminus \{0\}$, we have

$$\mathbb{N}\frac{1}{D} = \mathbb{N}\frac{1}{p} := \{\frac{m}{p}, \quad m \in \mathbb{N}\}$$

and

$$\pm\mathbb{N}\frac{1}{D} = \mathbb{Z}\frac{1}{p} := \{\frac{m}{p}, \quad m \in \mathbb{Z}\}.$$

2. If $D := \{p^i, i \in \mathbb{N}\}$ with $p \in \mathbb{N} \setminus \{0\}$, then

$$\mathbb{N}\frac{1}{D} = \mathbb{N}\left[\frac{1}{p}\right] := \{r \in \mathbb{Q}_{\geq 0}, \exists i \in \mathbb{N}, p^i r \in \mathbb{N}\}$$

and

$$\pm\mathbb{N}\frac{1}{D} = \mathbb{Z}\left[\frac{1}{p}\right] := \{r \in \mathbb{Q}, \exists i \in \mathbb{N}, p^i r \in \mathbb{Z}\}.$$

3. If $D = \mathbb{N} \setminus \{0\}$, then $\mathbb{N}\frac{1}{D} = \mathbb{Q}_{\geq 0}$ and $\pm\mathbb{N}\frac{1}{D} = \mathbb{Q}$.

Lemma 3.5 *If m, n are two denominators for a submonoid N of $\mathbb{Q}_{\geq 0}$, then their least common multiple p is also a denominator for N.*

Proof We are given two denominators m, n of N. Let us denote by d their greatest common divisor and by p their least common multiple. We can write $d = um + vn$ with $u, v \in \mathbb{Z}$ and it follows that $\frac{1}{p} = \frac{u}{n} + \frac{v}{m} \in \pm N$ and therefore $\frac{1}{p} \in N$. $\square$

Proposition 3.6 *A submonoid $N \subset \mathbb{Q}_{\geq 0}$ has a full set of denominators if and only if $N = \{0\}$ or $1 \in N$. If this is the case, it has a full inductive set of denominators. Actually, if $1 \in N$, the set*

$$D := \{n \in \mathbb{N} \setminus \{0\}, \frac{1}{n} \in N\}$$

of all denominators of N is a full inductive set of denominators for N.

Of course, the condition $1 \in N$ is equivalent to $\mathbb{N} \subset N$.

Proof The condition is necessary. More precisely, there exists $n \in D$ and we have $1 = n \times \frac{1}{n} \in N$. In order to check that the condition is also sufficient, we only have to prove the last assertion.

Let us assume that $1 \in N$. If $r \in N$, we can write $r = \frac{m}{n}$ with $m, n \in \mathbb{N}$ coprime and $n \neq 0$. Thus, there exists $u, v \in \mathbb{Z}$ with $um + vn = 1$ and it follows that $\frac{1}{n} = ur + v \in \pm N$. Therefore, we can write $r = m \times \frac{1}{n}$ with $m \in \mathbb{N}$ and $\frac{1}{n} \in \pm N \cap \mathbb{Q}_{\geq 0} = N$. It means that all denominators make a full set of denominators. We still have to show that this is an inductive set. Actually, this follows from lemma 3.5. $\square$

Proposition 3.7 *1. If a submonoid $N \subset \mathbb{Q}_{\geq 0}$ has a finite full set of denominators D, then $N = \mathbb{N}\frac{1}{p}$ for some $p \in \mathbb{N}$.*

2. If D is a full inductive set of denominators for a submonoid N of $\mathbb{Q}_{\geq 0}$, then

$$N = \cup_{n\in D}\mathbb{N}\frac{1}{n} \simeq \varinjlim_{n\in D} \mathbb{N}\frac{1}{n}.$$

Note that the second assertion means that any $r \in N$ may be written on the form $r = \frac{m}{n}$ with $m \in \mathbb{N}$ and $n \in D$.

Proof We prove the first assertion. Let D be a finite set of positive integers and p the least common multiple of all elements of D. Clearly, we have $N \subset \mathbb{N}\frac{1}{p}$ and it only remains to check that $\frac{1}{p} \in N$. By induction, this will easily follow from the case $D = \{m, n\}$. And we can use lemma 3.5.

In order to prove the second assertion, it is sufficient to check that $\cup_{n\in D}\mathbb{N}\frac{1}{n}$ is a submonoid of $\mathbb{Q}_{\geq 0}$. But, since D is inductive, if $n, n' \in D$, there exists $n'' \in D$ such that $n = dn''$ and $n' = d'n''$ with $d, d' \in \mathbb{N}$. Therefore, if $m, n \in \mathbb{N}$, we have

$$\frac{m}{n} + \frac{m'}{n'} = \frac{md + m'd'}{n''} \in \mathbb{N}\frac{1}{n''}. \quad \square$$

Proposition 3.8 *Let N be a submonoid of the additive monoid $\mathbb{Q}_{\geq 0}$ that contains $\mathbb{N}$, S a (multiplicative) monoid and $s \in S$.*

1. If

$$\begin{array}{ccc} N & \longrightarrow & S \\ r & \longmapsto & s^r \end{array} \tag{6}$$

is a morphism of monoids that sends 1 to s and D is a full set of denominators for N, then the sequence $\{s^{\frac{1}{n}}\}_{n\in D}$ is a system of roots of s.

2. Conversely, if D is a full inductive set of denominators for N and $\{s_n\}_{n\in D}$ is a system of roots for s, there exists a unique map (6) with $s^{\frac{1}{n}} = s_n$ for all $n \in D$.

Moreover, the map (6) extends uniquely to $\pm N$ if and only if s is invertible in S.

Proof Under the hypothesis of the first assertion, one easily checks that the conditions for a system of roots are satisfied. More precisely, we have for all $n \in D$, $(s^{\frac{1}{n}})^n = s$. Moreover, if $r = \frac{m}{n}$ with $n \in D$, then $(s^{\frac{1}{n}})^m = s^r$ will only depend on r.

Using proposition 3.7 and uniqueness, the second assertion will follow from the case $D = \{p\}$ which in turn follows from the fact that $\mathbb{N}\frac{1}{p}$ is isomorphic to $\mathbb{N}$ as an abstract monoid.

Finally, if s is invertible and $\frac{1}{s}$ denotes its inverse, one can extend the map (6) to $\pm N$ by sending $-r$ to $(\frac{1}{s})^r$. Of course, one must check that this defines a morphism of monoids. This is left to the reader. Conversely, if the maps extends to $\pm N$, the image of -1 must be an inverse for s. $\square$

Corollary 3.9 *If we are given a system of p-th roots s_{p^i} of s for* all *prime p, this will extend uniquely to a complete system of roots of s.*

Proof Uniqueness follows from the fact that $\sum_p \mathbb{N}\left[\frac{1}{p}\right] = \mathbb{Q}_{\geq 0}$ (i.e. $\mathbb{Q}_{\geq 0}$ is the smallest submonoid containing all $\mathbb{N}\left[\frac{1}{p}\right]$ for p prime). Existence follows from the fact that $\mathbb{N}[\frac{1}{p_1}] \cap \mathbb{N}[\frac{1}{p_2}] = \mathbb{N}$ for p_1, p_2 distinct primes. Details are left to the reader. $\square$

As we said above, we want to apply the theory to the multiplicative monoid of our ring R and the element q.

Examples. For $R = \mathbb{C}$ and $q = \rho e^{\sqrt{-1}\theta}$, we can consider the morphism of groups

$$\begin{aligned} \mathbb{Q} &\longrightarrow \mathbb{C}^\times \\ r &\longmapsto \rho^r e^{\sqrt{-1}r\theta}. \end{aligned}$$

It provides us with a complete system of roots of q. More generally, if K is algebraically closed, there always exists a complete system of roots of $q \in K$.

Recall that if K is a commutative ring, the forgetful functor from K-algebras to monoids has a left inverse. Actually, if N is an additive monoid, the associated K-algebra is the free module on the abstract basis $\{t^r\}_{r\in N}$ and multiplication is given by $t^{r_1}t^{r_2} = t^{r_1+r_2}$.

When N is a submonoid of $\mathbb{Q}_{\geq 0}$ with set of denominators D, we will denote the K-algebra of N by $K[t^{\frac{1}{D}}]$ (even if it actually only depends only on N and not on D). This is the ring of *Puiseux polynomials* with denominators in D. Note that

$$K[t^{\frac{1}{D}}] = \varinjlim_{n\in D} K[t^{\frac{1}{n}}]$$

when D is inductive. Actually, the map

$$\begin{aligned} K[t] &\longrightarrow K[t^{\frac{1}{n}}] \\ t &\longmapsto t^{\frac{1}{n}} \end{aligned}$$

is obviously an isomorphism and we could as well write

$$K[t^{\frac{1}{D}}] = \varinjlim_{t\mapsto t^n, n\in D} K[t].$$

We will also denote the K-algebra of $\pm N$ by $K[t^{\pm\frac{1}{D}}]$ and, when K is a field, we will denote by $K(T^{\frac{1}{D}})$ the fraction field of $K[t^{\frac{1}{D}}]$.

The K-algebra $K[t^{\frac{1}{D}}]$ has the following universal property:

Proposition 3.10 *Assume that R is a K-algebra and that we are given a system of roots of q indexed by D in R. Then, there exists a unique morphism of K-algebras*

$$\begin{aligned} K[t^{\frac{1}{D}}] &\longrightarrow R \\ t^r &\longmapsto q^r. \end{aligned}$$

When $q \in R^\times$, it extends uniquely to $K[t^{\pm\frac{1}{D}}]$.

Proof The morphism of monoids $N \to R$ will extend uniquely to a morphism of K-algebras. The same result holds with $\pm N$ when $q \in R^\times$. $\square$

Definition 3.11 *A system $\{q_n\}_{n\in D}$ of roots of q is said to be* admissible *if*

$$\forall n \in D, \quad (n)_{q_n} \in R^\times.$$

Examples.

1. If $1 - q \in R^\times$, then any system of roots of q is admissible because

$$(1 - q_n)(n)_{q_n} = 1 - q_n^n = 1 - q.$$

   This applies in particular when R is a field and $q \neq 1$, or more generally when R contains a field K and $q \in K$ with $q \neq 1$.

2. A non trivial system of roots of 1 *cannot* be admissible: we will have $(n)_{q_n} = 0$ for all $n \in D$.

3. Assume $R = \mathbb{Z}[\sqrt{-1}]$ and $q = -1$. Then the square roots of q are not admissible because $1 \pm \sqrt{-1}$ is not invertible in R.

Definition 3.12 *Let $D \subset \mathbb{N}\backslash\{0\}$ be a full inductive set of denominators for a submonoid $N \subset \mathbb{Q}_{\geq 0}$. Let $\{q_n\}_{n\in D}$ be an admissible system of roots of q in R. If $r = \frac{m}{n} \in N$ with $m \in \mathbb{N}$ and $n \in D$, then the q-*state *(or* quantum state*) of r is*

$$(r)_q := \frac{(m)_{q_n}}{(n)_{q_n}}.$$

*If $q \in R^\times$ and $r \in \pm N$, then the q-*state *(or* quantum state *) of r is defined by the same formula.*

Note that we must verify that this definition makes sense. More precisely, since D is assumed to be inductive, we must check that if $k \in \mathbb{N}$ is such that $kn \in D$, we also have

$$(r)_q = \frac{(km)_{q_{kn}}}{(kn)_{q_{kn}}}.$$

But we know from proposition 1.3 that

$$(km)_{q_{kn}} = (k)_{q_{kn}}(m)_{q_n} \quad \text{and} \quad (kn)_{q_{kn}} = (k)_{q_{kn}}(n)_{q_n}.$$

Following proposition 3.8, we will sometimes write $q^{\frac{m}{n}} := q_n^m$. Then, the formula reads

$$\left(\frac{m}{n}\right)_q := \frac{\sum_{i=0}^{m-1} q^{\frac{i}{n}}}{\sum_{i=0}^{n-1} q^{\frac{i}{n}}},$$

and for example, we will have

$$\left(\frac{1}{2}\right)_q = \frac{1}{1+q^{\frac{1}{2}}}, \quad \left(\frac{1}{3}\right)_q = \frac{1}{1+q^{\frac{1}{3}}+q^{\frac{2}{3}}}, \quad \left(\frac{2}{3}\right)_q = \frac{1+q^{\frac{1}{3}}}{1+q^{\frac{1}{3}}+q^{\frac{2}{3}}}, \quad \dots$$

Also, if $q \in R^\times$, we will have

$$\left(-\frac{m}{n}\right)_q := -\frac{\sum_{i=1}^{m} q^{-\frac{i}{n}}}{\sum_{i=0}^{n-1} q^{\frac{i}{n}}},$$

and in particular

$$\left(-\frac{1}{2}\right)_q = -\frac{1}{q^{\frac{1}{2}}+q}, \quad \left(-\frac{1}{3}\right)_q = -\frac{1}{q^{\frac{1}{3}}+q^{\frac{2}{3}}+q}, \quad \dots$$

Propositions 1.3 and 1.8 generalize as follows:

Proposition 3.13 *Assume that we are given an admissible system of roots of q indexed by an inductive set of denominators D of a submonoid N of $\mathbb{Q}_{\geq 0}$. Then, for all $r \in N$ (or $r \in \pm N$ when $q \in R^\times$), we have*

$$(1-q)(r)_q = 1 - q^r.$$

In particular, if $1-q$ is invertible in R, we have

$$(r)_q = \frac{1-q^r}{1-q}.$$

Proof If we write $r = \frac{m}{n}$ with $m \in N$ and $n \in D$, we have

$$(1-q)(r)_q = \left((1-q^{\frac{1}{n}})(n)_{q^{\frac{1}{n}}}\right)\left(\frac{(m)_{q^{\frac{1}{n}}}}{(n)_{q^{\frac{1}{n}}}}\right)$$

$$= (1-q^{\frac{1}{n}})(m)_{q^{\frac{1}{n}}} = 1 - (q^{\frac{1}{n}})^m = 1 - q^r. \quad \square$$

Proposition 3.14 *Assume that we are given an admissible system of roots of q indexed by an inductive set of denominators of a submonoid N of $\mathbb{Q}_{\geq 0}$. For all $r_1, r_2 \in N$ (or $\pm N$ when $q \in R^\times$), we have*

$$(r_1 + r_2)_q = (r_1)_q + q^{r_1}(r_2)_q$$

and

$$(r_1 r_2)_q = (r_1)_q (r_2)_{q^{r_1}}.$$

Proof We easily reduce to the case $R = \mathbb{Q}(t^{\frac{1}{D}})$ and $q = t$ in which case, proposition 3.13 tells us that

$$(r)_q = \frac{1 - q^r}{1 - q}$$

whenever $r \in N$ (or $\pm N$ when $q \in R^\times$). Then, the formulas are easily checked exactly as in the the proof of proposition 1.8 (integer case). □

Remarks. (see definition 2.1 of [5] for example) If $q \in \mathbb{R}_{>0}$ is not equal to 1, one defines the *q-analog* (or *quantum analog*) of a real number a as

$$(a)_q = \frac{1 - q^a}{1 - q}$$

This is compatible with the above definition of the q-state of r when $a = r \in \mathbb{Q}$. More generally, if we choose a branch of the logarithm which is defined at a complex number $q \neq 1$, we may define the quantum analog of a complex number a with the same formula and the convention $q^a = \exp(a \ln(q))$. There are analogous results over ultrametric fields.

4 Twisted powers

We assume here that R is commutative and we fix a commutative R-algebra A endowed with an R-algebra endomorphism σ.

Definition 4.1 *If $x \in A$ and $n \in \mathbb{N}$, the* n-th twisted power *of x (with respect to σ) is*

$$x^{(n)_\sigma} := \prod_{i=0}^{n-1} \sigma^i(x).$$

In other words, we have

$$x^{(0)_\sigma} = 1, \quad x^{(1)_\sigma} = x, \quad x^{(1)_\sigma} = x\sigma(x), \quad \ldots, \quad x^{(n)_\sigma} = x\sigma(x)\cdots\sigma^{n-1}(x), \quad \ldots$$

The twisted powers can also be defined inductively by

$$x^{(n+1)_\sigma} = x^{(n)_\sigma}\sigma^n(x) = x\sigma(x^{(n)_\sigma}).$$

Examples.

1. When $\sigma(x) = x$, we have $x^{(n)_\sigma} = x^n$. In particular, in the case $\sigma = \mathrm{Id}_A$, twisted powers are just usual powers.
2. (a) If $\sigma(x) = x - 1$, we obtain the *falling Pochhammer symbol* of x:

$$x^{(n)_\sigma} = x(x-1)\cdots(x-n+1).$$

When R is a $\mathbb{Q}$-algebra, it is then common to extend the usual binomial coefficients by writing

$$\binom{x}{n} := \frac{x^{(n)_\sigma}}{n!}.$$

(b) If $\sigma(x) = x + 1$, we obtain the *rising Pochhammer symbol* of x:

$$x^{(n)_\sigma} = x(x+1)\cdots(x+n-1)$$

and:

$$\frac{x^{(n)_\sigma}}{n!} = \binom{x+n-1}{n}$$

when R is a $\mathbb{Q}$-algebra.

3. More generally, if $\sigma(x) = x - h$ (resp. $\sigma(x) = x + h$) with $h \in R^\times$ and R is a $\mathbb{Q}$-algebra, we will have the identity

$$\frac{x^{(n)_\sigma}}{n!} = h^n \binom{x/h}{n} \quad (\text{resp.} \quad \frac{x^{(n)_\sigma}}{n!} = h^n \binom{(x+n-1)/h}{n}).$$

4. Assume now that $\mathrm{Char}(R) = p > 0$ and $\sigma(x) = x + h$ with $h \in R$. Then

$$x^{(p)_\sigma} = x^p - h^{p-1}x.$$

When $h = 1$, this is exactly the *Artin-Schreier* map.

5. If $\sigma(x) = qx$ with $q \in R$, then

$$(1-x)^{(p)_\sigma} = (1-x)(1-qx)\cdots(1-q^{p-1}x)$$

is the *q-Pochhammer symbol* of x.

6. If $y \in A$ satisfies $\sigma(y) = qy$ with $q \in R$, we may endow the polynomial ring $A[\xi]$ with the endomorphism $\sigma(\xi) = \xi + y$. Then, we will have

$$\forall n \in \mathbb{N}, \quad \xi^{(n)_\sigma} = \xi(\xi+y)\cdots(\xi+(n-1)_q y).$$

These twisted powers play an important role in the theory of q-difference equations.

Proposition 4.2 *Assume $\sigma(x) = qx$ with $q \in R$. Then, we have the following:*

1. $x^{(n)_\sigma} = q^{\frac{n(n-1)}{2}} x^n$.
2. *If $q-\mathrm{char}(R) = p$ is an* odd *integer, then $x^{(p)_\sigma} = x^p$.*
3. *If R is q-flat and $q-\mathrm{char}(R) = p > 0$, then $x^{(p)_\sigma} = (-1)^{p-1}x^p$.*

Proof We have for all $i \in \mathbb{N}$, $\sigma^i(x) = q^i x$ and therefore

$$x^{(n)_\sigma} = \prod_{i=0}^{n-1} q^i x = q^{\frac{n(n-1)}{2}} x^n.$$

If $q-\mathrm{char}(R) = p$, we have $q^p = 1$. Therefore, if $p = 2k+1$, we obtain

$$x^{(p)_\sigma} = q^{\frac{p(p-1)}{2}} x^p = q^{kp} x^p = x^p.$$

Finally, assume that R is q-flat and $q-\mathrm{char}(R) = p > 0$. For p odd, we just proved the formula. On the other hand, if $p = 2k$, we know from proposition 1.11 that $q^k = -1$. It follows that

$$x^{(p)_\sigma} = q^{k(p-1)} x^p = (-1)^{p-1} x^p. \quad \square$$

Lemma 4.3 *We have*

1. $\forall x \in A, \forall n, m \in \mathbb{N}, \quad x^{(n)_\sigma} \sigma^n(x^{(m)_\sigma}) = x^{(n+m)_\sigma}$
2. $\forall x, y \in A, \forall n \in \mathbb{N} \quad (xy)^{(n)_\sigma} = x^{(n)_\sigma} y^{(n)_\sigma}$
3. $\forall x \in A, \forall n, k \in \mathbb{N} \quad \sigma^k(x^{(n)_\sigma}) = \sigma^k(x)^{(n)_\sigma}$

Proof All the equalities follow from the fact that σ is a ring endomorphism. More precisely, we have

$$x^{(n)_\sigma} \sigma^n(x^{(m)_\sigma}) = \prod_{i=0}^{n-1} \sigma^i(x) \sigma^n \left(\prod_{j=0}^{m-1} \sigma^j(x) \right)$$

$$= \prod_{i=0}^{n-1} \sigma^i(x) \prod_{j=0}^{m-1} \sigma^{n+j}(x) = \prod_{i=0}^{m+n-1} \sigma^i(x) = x^{(n+m)_\sigma}.$$

Also,

$$(xy)^{(n)_\sigma} = \prod_{i=0}^{n-1} \sigma^i(xy) = \prod_{i=0}^{n-1} \sigma^i(x)\sigma^i(y) = \prod_{i=0}^{n-1} \sigma^i(x) \prod_{i=0}^{n-1} \sigma^i(y) = x^{(n)_\sigma} y^{(n)_\sigma}.$$

And finally,

$$\sigma^k(x^{(n)_\sigma}) = \sigma^k(\prod_{i=0}^{n-1} \sigma^i(x)) = \prod_{i=0}^{n-1} \sigma^{i+k}(x) = \sigma^k(x)^{(n)_\sigma}. \quad \square$$

There is also a formula for moving from σ to σ^m that is quite useful:

Proposition 4.4 *We have*

$$\forall x \in A, n, m \in \mathbb{N}, \quad \left(x^{(n)_{\sigma^m}}\right)^{(m)_\sigma} = \left(x^{(n)_\sigma}\right)^{(m)_{\sigma^n}} = x^{(mn)_\sigma}$$

Proof We simply do the computations. We have

$$\left(x^{(n)_{\sigma^m}}\right)^{(m)_\sigma} = \prod_{i=0}^{m-1} \sigma^i \left(\prod_{j=0}^{n-1} (\sigma^m)^j(x) \right)$$

$$= \prod_{i=0}^{m-1} \prod_{j=0}^{n-1} \sigma^{mj+i}(x) = \prod_{k=0}^{mn-1} \sigma^k(x) = x^{(mn)_\sigma}.$$

And

$$\left(x^{(n)_\sigma}\right)^{(m)_{\sigma^n}} = \prod_{i=0}^{m-1} (\sigma^n)^i \left(\prod_{j=0}^{n-1} \sigma^j(x) \right)$$

$$= \prod_{i=0}^{m-1} \prod_{j=0}^{n-1} \sigma^{ni+j}(x) = \prod_{k=0}^{mn-1} \sigma^k(x) = x^{(mn)_\sigma}. \quad \square$$

The *twisted binomial formula* reads as follows:

Proposition 4.5 *Assume that $x, y \in A$ satisfy $\sigma(x) = qx$ with $q \in R$, and $\sigma(y) = y$. Then, we have*

$$\forall n \in \mathbb{N}, \quad (x+y)^{(n)_\sigma} = \sum_{k=0}^{n} \binom{n}{k}_q x^{(k)_\sigma} y^{(n-k)_\sigma}.$$

Proof This is exactly the formula of proposition 2.14. $\square$

We can also state the *Frobenius property*:

Corollary 4.6 *Let $q \in R$. Assume $q-\mathrm{char}(R) = p > 0$ and R is q-flat. Assume that $x, y \in A$ satisfy $\sigma(x) = qx$ and $\sigma(y) = y$. Then, we have*

$$\forall n \in \mathbb{N}, \quad (x+y)^{(p)_\sigma} = x^{(p)_\sigma} + y^{(p)_\sigma}$$

Proof Follows from lemma 2.12. □

Note that one can also recover the quantum Lucas theorem (proposition 2.13) as a corollary of proposition 4.5 as explained for example in lemma 1 of [12].

We also want to mention that one can consider the notion of twisted powers of an ideal (products and images are always meant as ideals):

Definition 4.7 *If $\mathfrak{a} \subset A$ is an ideal, the* twisted powers *of $\mathfrak{a}$ are defined as*

$$\mathfrak{a}^{(n)_\sigma} := \prod_{i=0}^{n-1} \sigma^i(\mathfrak{a}).$$

And the twisted completion *of A along $\mathfrak{a}$ is*

$$\hat{A}^\sigma := \varprojlim A/\mathfrak{a}^{(n)_\sigma}$$

Again, it means that

$$\mathfrak{a}^{(0)_\sigma} := A, \quad \mathfrak{a}^{(1)_\sigma} := \mathfrak{a}, \quad \text{and} \quad \mathfrak{a}^{(n)_\sigma} = \mathfrak{a}\sigma(\mathfrak{a}) \cdots \sigma^{n-1}(\mathfrak{a}).$$

Of course, when $\mathfrak{a}$ is a principal ideal, say $\mathfrak{a} = (x)$, we will have $\mathfrak{a}^{(n)_\sigma} = (x^{(n)_\sigma})$.

Examples. 1. If $\sigma = \mathrm{Id}_A$ these are just usual powers and usual completion.

2. If $R = \mathbb{Q}$, $A = \mathbb{Q}[x]$ and $\sigma(x) = x + h$ with $h \neq 0$, then $\hat{A}^\sigma \simeq \mathbb{Q}[x]^{\mathbb{N}}$ and the canonical map $A \to \hat{A}^\sigma$ sends x to $(x - ih)_{i \in \mathbb{N}}$.

References

[1] George E. Andrews. *The theory of partitions*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976. Encyclopedia of Mathematics and its Applications, Vol. 2.

[2] Alexander Borisov, Melvyn B. Nathanson, and Yang Wang. Quantum integers and cyclotomy. *J. Number Theory*, 109(1):120–135, 2004.

[3] David M. Bradley. Multiple q-zeta values. *J. Algebra*, 283(2):752–798, 2005.

[4] L. Di Vizio, J.-P. Ramis, J. Sauloy, and C. Zhang. Équations aux q-différences. *Gaz. Math.*, (96):20–49, 2003.

[5] Thomas Ernst. A method for q-calculus. *J. Nonlinear Math. Phys.*, 10(4):487–525, 2003.

[6] Thomas Ernst. *A comprehensive treatment of q-calculus*. Birkhäuser/Springer Basel AG, Basel, 2012.

[7] Michel Gros and Bernard Le Stum. Une neutralisation explicite de l'algèbre de Weyl complétée. *Communications in Algebra*, 2013.

[8] Victor J. W. Guo and Jiang Zeng. Some arithmetic properties of the q-Euler numbers and q-Salié numbers. *European J. Combin.*, 27(6):884–895, 2006.

[9] Victor Kac and Pokman Cheung. *Quantum calculus*. Universitext. Springer-Verlag, New York, 2002.

[10] Christian Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[11] Donald E. Knuth and Herbert S. Wilf. The power of a prime that divides a generalized binomial coefficient. *J. Reine Angew. Math.*, 396:212–219, 1989.

[12] Peter Littelmann. Contracting modules and standard monomial theory for symmetrizable Kac-Moody algebras. *J. Amer. Math. Soc.*, 11(3):551–567, 1998.

[13] George Lusztig. *Introduction to quantum groups*. Modern Birkhäuser Classics. Birkhäuser/Springer, New York, 2010. Reprint of the 1994 edition.

[14] M. B. Nathanson. Additive number theory and the ring of quantum integers. In *General theory of information transfer and combinatorics*, volume 4123 of *Lecture Notes in Comput. Sci.*, pages 505–511. Springer, Berlin, 2006.

[15] Heinrich Saller. *Operational quantum theory. I.* Operational Physics. Springer, New York, 2006. Nonrelativistic structures.

[16] Richard P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.