UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIAS MATEMÁTICAS

FACULTAD DE CIENCIAS

EL ANILLO DE LOS ENTEROS CUÁNTICOS

T E S I S

QUE PARA OBTENER EL GRADO ACADÉMICO DE

MAESTRO EN CIENCIAS

P R E S E N T A :

YUVAL MATARASSO POZAICER

DIRECTORA DE TESIS: DRA. RITA ESTHER ZUAZUA VEGA

MÉXICO, D.F. ENERO 2010

EL ANILLO DE LOS ENTEROS CUÁNTICOS

Yuval Matarasso Pozaicer

INDICE

Introducción 4

Capítulo 0: Definiciones elementales y propiedades básicas de los enteros cuánticos 6

Notación y definiciones básicas 7

Propiedades de los enteros cuánticos 9

Capítulo I: Estructura multiplicativa de los enteros cuánticos 11

Sucesiones de polinomios que son compatibles con el producto cuántico 14

Ecuaciones funcionales aritméticas 24

Existencia de soluciones 29

Capítulo II: Estructura aditiva cuadrática de los enteros cuánticos. 39

Reglas aditivas cuánticas. 40

Identidades cero cuadráticas 43

Reglas aditivas cuadráticas 46

Ecuaciones funcionales asociadas a las reglas aditivas cuadráticas 52

Capítulo III: Estructura aditiva lineal de los enteros cuánticos . . . 59

Reglas aditivas lineales. 60

La regla aditiva cuántica fundamental 64

Capítulo IV: Estructura de anillo de los enteros cuánticos 72

Adición y Multiplicación 73

Unicidad de los enteros cuánticos 78

El anillo de los enteros cuánticos y la teoría aditiva de los números 80

Conclusiones: 83

Bibliografía: 85

INTRODUCCIÓN

Para el presente trabajo he escogido un tema, de cierta manera, novedoso y poco tratado en los libros de texto y en las aplicaciones de la matemática. **Los enteros cuánticos**.

La decisión de analizar este tema es por varias razones, la primera y más importante es porque la teoría de los números y en particular la teoría aditiva de los números es una rama de las matemáticas la cual me parece fascinante. Desde mis estudios de licenciatura, esta rama de las matemáticas me cautivó. El tema que escogí para realizar mi tesis de licenciatura fue "Los problemas de Waring en la teoría aditiva de los números". Con este trabajo comprendí que esta disciplina matemática tiene mucho trabajo que descubrir, mejorar y aplicar. Así que, una vez comprendidos los temas más básicos de la teoría de los números y analizado el pasado de esta rama, decidí dar un salto hacia la actualidad y futuro de la teoría aditiva de los números.

Otra razón que me motivó para la elección del tema es que no hay mucha información sobre esto. Si uno trata de investigar ¿Qué son los enteros cuánticos? ¿Dónde se aplican? ¿Para qué sirven?, etc. lo único que encuentra es una serie de artículos, escritos principalmente por Melvyn B. Nathanson. Así que la curiosidad de comprender por qué hay tan poca información sobre el tema despertó en mi una necesidad de adentrarme más en los estudios de este autor y de esta manera poder dar respuesta a todas las preguntas antes citadas.

Para poder realizar el presente trabajo de tesis, se analizaron cuatro de los artículos de Nathanson:

- ✓ Nathanson [1].
- ✓ Kontorovich y Nathanson [2].
- ✓ Nathanson [3].
- ✓ Nathanson [4].

Los objetivos, a grandes rasgos, de estos artículos son ir construyendo poco a poco el concepto de entero cuántico, dar operaciones binarias (suma y multiplicación) "bien definidas" para este conjunto de polinomios y así poder llegar al objetivo principal que es darle estructura de anillo a los enteros cuánticos.

El presente trabajo se divide en cinco capítulos:

Capítulo 0: Se dan las definiciones y notaciones elementales que se utilizarán durante el trabajo, así mismo algunas propiedades básicas de los enteros cuánticos.

Capítulo I: Se analiza la estructura multiplicativa de los enteros cuánticos. Esto se hace mediante el concepto de ecuaciones funcionales aritméticas y sucesiones de polinomios compatibles con el producto cuántico. Este capítulo está basado en el artículo Nathanson [1] y contiene varios resultados concentrados en la construcción y clasificación de sucesiones de polinomios que satisfacen la ecuación funcional multiplicativa, así mismo problemas abiertos provenientes de la ecuación funcional.

Capítulo II: Se estudia la estructura aditiva de los enteros cuánticos enfocándonos principalmente en la estructura cuadrática. Para ello se analizan las reglas aditivas cuadráticas, las reglas aditivas cuánticas y las identidades cero cuadráticas. Al igual que en la estructura multiplicativa, se introduce el concepto de ecuaciones funcionales asociadas a las reglas aditivas cuadráticas y se da una clasificación completa de estas reglas.

Capítulo III: Similarmente que en el capítulo II, se analizará la estructura aditiva de los enteros cuánticos pero desde una perspectiva lineal. Abordaremos los conceptos de reglas aditivas lineales y la regla aditiva cuántica fundamental. En este capítulo determinaremos todas las reglas aditivas cuánticas y calcularemos todas las soluciones de las correspondientes ecuaciones funcionales.

Capítulo IV: Las definiciones y resultados de este capítulo nos guían para construir el anillo de los enteros cuánticos y el campo de los números racionales cuánticos. Por último vincularemos el anillo de los enteros cuánticos con la teoría aditiva de los números, con esto, se verá que la adición y multiplicación de enteros cuánticos son equivalentes a la descomposición elemental de intervalos de enteros en teoría aditiva de los números.

CAPÍTULO 0

Definiciones elementales y propiedades básicas de los enteros cuánticos.

1. Notación y definiciones básicas.

El objetivo de este capítulo es dar las nociones preliminares sobre los enteros cuánticos así como las definiciones elementales y algunos resultados básicos que se utilizarán durante toda la tesis.

Notación: $\mathbb{N}=\{1,2,3,...\}$ y $\mathbb{N}_0=\mathbb{N}\cup\{0\}$.

Ahora, definamos el concepto de entero cuántico.

Definición 0.1: Para cada $n\in\mathbb{N}$, el polinomio $[n]_q=1+q+q^2+...+q^{n-1}\in K[q]$ es llamado **el entero cuántico *n***.

Ejemplos:

Si $n=1$, entonces $[1]_q=1$

Si $n=2$, entonces $[2]_q=1+q$

Si $n=3$, entonces $[3]_q=1+q+q^2$

⋮ ⋮

Para *n* en general tenemos la definición 0.1, es decir:

$$[n]_q=1+q+q^2+...+q^{n-1}.$$

Observación: Con la multiplicación usual de polinomios tenemos que:

$$[m]_q[n]_q\neq[mn]_q \quad \forall\ m\neq 1, n\neq 1.$$

Ejemplo: Sean $n=2$ y $m=3$, de esta manera tenemos que:

$$[m]_q=[3]_q=1+q+q^2 \text{ y } [n]_q=[2]_q=1+q.$$

Entonces:

$$[m]_q[n]_q=\left(1+q+q^2\right)(1+q)=q^3+2q^2+2q+1.$$

Por otro lado tenemos que:

$$[mn]_q=[6]_q=1+q+q^2+q^3+q^4+q^5.$$

Por lo tanto $[m]_q[n]_q\neq[mn]_q$. □

Esta observación nos dice que la multiplicación usual de polinomios no nos funciona como producto entre enteros cuánticos, así que queremos definir un nuevo producto de polinomios de tal manera que se cumpla la igualdad:

$$[m]_q \cdot [n]_q = [mn]_q .$$

Esto lo haremos en el capítulo I el cual se dedica a la estructura multiplicativa de los enteros cuánticos.

2. Propiedades de los enteros cuánticos.

A continuación presentaremos un lema que va a ser de gran utilidad para poder presentar un par de ejemplos de reglas aditivas cuadráticas y para poder probar varios teoremas que se irán presentando durante todo el trabajo.

Lema 0.2: Sean n y m enteros positivos cualesquiera, entonces:

a) $q[n]_q = [n+1]_q - 1$

b) $q^s [n]_q = [n+s]_q - [s]_q \quad \forall\, s \in \mathbb{N}$

c) $[m]_q \cdot [n]_q = \sum_{i=n}^{n+m-1} [i]_q - \sum_{j=1}^{m-1} [j]_q$

Demostración:

a) $q[n]_q = q\left(1 + q + q^2 + \ldots + q^{n-1}\right) = q + q^2 + q^3 + \ldots + q^{n-1} + q^n = [n+1]_q - 1$

Por lo tanto se tiene que $\boxed{q[n]_q = [n+1]_q - 1}$. □

b) La prueba de este inciso se hará por inducción sobre s:

- Base de la inducción: Si $s = 1$, entonces lo que tenemos que probar es $q^1 [n]_q = [n+1]_q - [1]_q$, es decir, $q[n]_q = [n+1]_q - 1$ que es el inciso a) el cual ya está demostrado.

- Hipótesis de inducción: Supongamos que el resultado es válido para $s-1$, es decir, supongamos que se cumple que:

$$q^{s-1} [n]_q = \left[n + (s-1)\right]_q - [s-1]_q .$$

- Paso inductivo: Probemos el resultado para s:

$$\begin{aligned} q^s [n]_q = q \cdot q^{s-1} [n]_q &\overset{\text{H.I}}{=} q\left(\left[n + (s-1)\right]_q - [s-1]_q\right) \\ &= q[n+s-1]_q - q[s-1]_q \overset{\text{B.I}}{=} [n+s]_q - 1 - [s]_q + 1 \\ &= [n+s]_q - [s]_q . \end{aligned}$$

Por lo tanto $\boxed{q^s [n]_q = [n+s]_q - [s]_q}$. □

c) $[m]_q \cdot [n]_q = \left(1 + q + q^2 + \ldots + q^{m-1}\right) \cdot [n]_q$

$= [n]_q + q \cdot [n]_q + q^2 \cdot [n]_q + \ldots + q^{m-1} \cdot [n]_q$

$= [n]_q + [n+1]_q - [1]_q + [n+2]_q - [2]_q + \ldots + [n+m-1]_q - [m-1]_q$ por a) y b)

$= \left([n]_q + [n+1]_q + [n+2]_q + \ldots + [n+m-1]_q\right) - \left([1]_q + [2]_q + \ldots + [m-1]_q\right)$

$= \sum_{i=n}^{n+m-1} [i]_q - \sum_{j=1}^{m-1} [j]_q .$

Por lo tanto $\boxed{[m]_q \cdot [n]_q = \sum_{i=n}^{n+m-1} [i]_q - \sum_{j=1}^{m-1} [j]_q}$. □

CAPÍTULO I

ESTRUCTURA MULTIPLICATIVA DE LOS ENTEROS CUANTICOS.

Consideremos los enteros cuánticos $[n]_q = 1+q+q^2+...+q^{n-1}$ y $[m]_q = 1+q+q^2+...+q^{m-1}$ con grado $n-1$ y $m-1$, respectivamente, su producto es un polinomio de grado $m+n-2$. Por otro lado, el entero cuántico $[mn]_q = 1+q+q^2+...+q^{mn-1}$ tiene grado $mn-1$. Es decir, la multiplicación usual de polinomios no es una buena multiplicación para los enteros cuánticos ya que $[m]_q[n]_q \neq [mn]_q \ \forall\ m \neq 1, n \neq 1$, como ya hemos visto en el capítulo 0.

En este capítulo daremos una multiplicación para los enteros cuánticos, denotada como $\otimes_q$ que satisface la ecuación $[m]_q \otimes_q [n]_q = [mn]_q$ y nos permitirá, como veremos en el capítulo IV, darle al conjunto de los enteros cuánticos estructura de anillo.

Definición I.1: Sea $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios con coeficientes en un campo. Se define la multiplicación $\otimes_q$ de polinomios en $\mathcal{F}$ de la siguiente forma:

$$\boxed{f_m(q) \otimes_q f_n(q) = f_m(q) f_n(q^m)}.$$

Definición I.2: Si una sucesión de polinomios $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ satisface la ecuación funcional

$$f_{mn}(q) = f_m(q) \otimes_q f_n(q) = f_m(q) f_n(q^m) \ \forall\ m,n \in \mathbb{N} \quad \ldots (1)$$

entonces diremos que $\mathcal{F}$ es **compatible con el producto cuántico**.

Observemos que si una sucesión de polinomios $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es solución de la ecuación (1), entonces el producto $\otimes_q$ es conmutativo en $\mathcal{F}$ dado que $f_{mn}(q) = f_{nm}(q)$ por la conmutatividad de los naturales, así tenemos la siguiente ecuación:

$$f_m(q) f_n(q^m) = f_n(q) f_m(q^n) \ \forall\ m,n \in \mathbb{N} \quad \ldots (2)$$

Claramente, la sucesión constante $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ definida por $f_n(q) = 1\ \forall\ n \in \mathbb{N}$ satisface la ecuación funcional (1). Veamos dos ejemplos de sucesiones no triviales que también la satisfacen.

1) La sucesión $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ definida por $f_n(q) = q^{n-1}\ \forall\ n \in \mathbb{N}$.
Sustituyendo en la ecuación funcional (1) tenemos:

$$f_{mn}(q) = q^{mn-1} = q^{m-1+mn-m} = q^{m-1+m(n-1)} = q^{m-1} q^{m(n-1)} = f_m(q) f_n(q^m)$$

Por lo tanto,

$$f_{mn}(q) = f_m(q) f_n(q^m).$$

2) La sucesión $\mathcal{F} = \left\{ f_n(q) \right\}_{n=1}^{\infty}$ definida por $f_n(q) = [n]_q \ \forall n \in \mathbb{N}$ (la sucesión de enteros cuánticos.)
Sean $m, n \in \mathbb{N}$, entonces:

$$\begin{aligned}
[m]_q \otimes_q [n]_q &= f_m(q) \otimes_q f_n(q) \\
&= f_m(q) \cdot f_n\left(q^m\right) \\
&= \left(1 + q + q^2 + \ldots + q^{m-1}\right) \cdot \left(1 + q^m + \left(q^m\right)^2 + \ldots + \left(q^m\right)^{n-1}\right) \\
&= \left(1 + q + q^2 + \ldots + q^{m-1}\right) \cdot \left(1 + q^m + q^{2m} + \ldots + q^{m(n-1)}\right) \\
&= 1 + q + \ldots + q^{m-1} + q^m + q^{m+1} + \ldots + q^{2m-1} + q^{2m} + \ldots + q^{mn-1} \\
&= [mn]_q .
\end{aligned}$$

Por lo tanto, la sucesión de enteros cuánticos es compatible con el producto cuántico, es decir, la ecuación funcional (1) nos da una "buena" multiplicación para el conjunto de los enteros cuánticos.

1. Sucesiones de polinomios que son compatibles con el producto cuántico.

Estamos interesados en determinar todas las sucesiones de polinomios $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ que satisfagan la ecuación funcional $f_{mn}(q)=f_m(q)\otimes_q f_n(q)=f_m(q)f_n(q^m)\ \forall m,n\in\mathbb{N}$. Este problema no se ha resuelto, sin embargo, el resultado principal de esta sección, el teorema I.13, nos caracteriza las sucesiones de polinomios que satisfacen la ecuación funcional (1) en términos de ciertos semigrupos.

Definición I.3: Un **semigrupo multiplicativo** de números naturales (por brevedad, un **semigrupo**), es un conjunto $S\subseteq\mathbb{N}$ tal que $1\in S$ y si $m\in S$ y $n\in S\Rightarrow m\cdot n\in S$.

Por ejemplo, para cualquier entero positivo n_0, el conjunto $\{1\}\cup\{n\geq n_0\}$ es un semigrupo.

Otro ejemplo de semigrupo multiplicativo es el siguiente: Sea *P* un conjunto de números primos y denotemos por $S(P)$ el conjunto formado por el 1, unión con todos los enteros positivos tales que todos sus factores primos pertenecen a *P*. Evidentemente, $S(P)$ es un semigrupo multiplicativo de $\mathbb{N}$.

Definición I.4: Un semigrupo de la forma $S(P)$, donde *P* es un conjunto de primos es llamado un **semigrupo primo**.

Observaciones:

1) Si $P=\varnothing$, entonces $S(P)=\{1\}$.
2) Si $P=\{p\}$, entonces $S(P)=\{p^k\ /\ k\in\mathbb{N}_0\}$.

Definición I.5: Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de funciones. El **soporte de $\mathcal{F}$** es el conjunto definido como: $\operatorname{supp}(\mathcal{F})\doteq\{n\in\mathbb{N}\ /\ f_n(q)\neq 0\}$.
La sucesión cero o trivial es aquella tal que su soporte es el conjunto vacío. Si $\operatorname{supp}(\mathcal{F})\neq\varnothing$, se dice que la sucesión es **no-cero**.

Como nos muestra el siguiente lema, las sucesiones no-cero que satisfacen la ecuación funcional (1) están totalmente determinadas por su valor en $n=1$.

Lema I.6: Si la sucesión $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ satisface la ecuación funcional (1), entonces $\mathcal{F}$ es no-cero si y sólo si $f_1(q)=1$.

Demostración:

$\Rightarrow$] Supongamos que $\mathcal{F}$ cumple con la ecuación (1) y es no-cero, entonces $f_1(q) = f_1(q) \otimes_q f_1(q) = f_1(q) f_1(q)$, por lo tanto $f_1(q) = 1$ ó $f_1(q) = 0$.
Si $f_1(q) = 0$, entonces $f_n(q) = f_1(q) \otimes_q f_n(q) = f_1(q) f_n(q) = 0 \ \forall n \in \mathbb{N}$, es decir, $\mathcal{F}$ es la sucesión trivial, lo cual es una contradicción, por lo que $f_1(q) = 1$.

$\Leftarrow$] Trivialmente si $f_1(q) = 1$, la sucesión es no-cero. □

Definición I.7: Para cada entero positivo *n*, sea $\Omega(n)$ el número de factores primos (no necesariamente distintos) de *n*.

Ejemplo: Si $n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$, entonces $\Omega(n) = r_1 + \ldots + r_k$.

El siguiente teorema nos demuestra que el soporte de las sucesiones de funciones que son compatibles con el producto cuántico es siempre un semigrupo primo $S(P)$, que además determina por completo los valores de la sucesión.

Teorema I.8: Sea $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión no-cero de polinomios compatible con el producto cuántico, entonces el soporte de $\mathcal{F}$ es un semigrupo primo. Además, si $\text{supp}(\mathcal{F}) = S(P)$, entonces la sucesión $\mathcal{F}$ está completamente determinada por el conjunto de polinomios $\mathcal{F}_P = \{f_p(q)\}_{p \in P}$.

Demostración:

Como la sucesión $\mathcal{F}$ es no trivial, por el lema I.6, $f_1(q) = 1$, por lo que $1 \in \text{supp}(\mathcal{F})$. Ahora, si $n, m \in \text{supp}(\mathcal{F})$, entonces $f_n(q) \neq 0$ y $f_m(q) \neq 0$, por lo que de la ecuación funcional (1), tenemos que $f_{mn}(q) \neq 0$ y $n \cdot m = m \cdot n \in \text{supp}(\mathcal{F})$.

Con lo anterior, hemos demostrado que el $\text{supp}(\mathcal{F})$ es un semigrupo.

A continuación probaremos que si P es el conjunto de números primos en el $\text{supp}(\mathcal{F})$, entonces $\text{supp}(\mathcal{F}) = S(P)$.

$\supseteq$] Sea $n \in S(P)$. Supongamos que *n* se factoriza como $n = p_1 \cdot \ldots \cdot p_k$ con $p_i \in P \ \forall i = 1, \ldots, k$. Como cada $p_i \in \text{supp}(\mathcal{F})$, es decir, $f_{p_i}(q) \neq 0 \ \forall i = 1, \ldots, k$, entonces tomando los productos de los primos dos a dos, se tiene que $f_n(q) = f_{p_1 \cdot p_2 \cdot \ldots \cdot p_k}(q) \neq 0$. Por lo tanto $n \in \text{supp}(\mathcal{F})$ y $\therefore S(P) \subseteq \text{supp}(\mathcal{F})$.

$\subseteq$] Supongamos que $n \in \text{supp}(\mathcal{F})$, *i.e.*, $f_n(q) \neq 0$ y sea p un primo que divide a n, entonces existe un entero positivo m tal que $n = p \cdot m$. Ahora bien, por la ecuación funcional (1) tenemos que $f_n(q) = f_{p \cdot m}(q) = f_p(q) f_m(q^p) \neq 0$. En particular $f_p(q) \neq 0$. Por lo tanto, hemos demostrado que para todo p primo que divide a n, $p \in \text{supp}(\mathcal{F})$ y $p \in P$ por definición, por lo tanto, $n \in S(P)$ y $\therefore \text{supp}(\mathcal{F}) \subseteq S(P)$.

Para terminar la prueba del teorema veremos que la sucesión $\mathcal{F}$ está completamente determinada por la subsucesión $\mathcal{F}_P = \{f_p(q)\}_{p \in P}$. La prueba se hará por inducción en $\Omega(n)$ para $n \in \text{supp}(\mathcal{F})$.

- Base de la inducción: Si $\Omega(n) = 1$, entonces $n = 1$ ó n es un número primo, en cualquier caso $n \in P$ y $\therefore f_p(q) \in \mathcal{F}_P$.
- Hipótesis de inducción: Supongamos que el teorema se cumple para todo $\forall m \in \text{supp}(\mathcal{F})$, tal que $\Omega(m) \leq k$.
- Paso inductivo: Sea $n \in \text{supp}(\mathcal{F})$ y supongamos que $\Omega(n) = k+1$, entonces $n = p \cdot m$ con $p \in P$, $m \in \text{supp}(\mathcal{F})$. Como la sucesión es compatible con el producto cuántico, $f_n(q) = f_p(q) f_m(q^p)$. Por la hipótesis de inducción, como $\Omega(m) = k$, $f_m(q^p)$ está totalmente determinada por la sucesión $\mathcal{F}_P = \{f_p(q)\}_{p \in P}$ y en consecuencia también lo está $f_n(q)$. □

El teorema anterior nos da una forma de asociarle a una sucesión de polinomios que satisface la ecuación funcional (1), un semigrupo primitivo. Inversamente, el teorema siguiente nos da una manera de asociarle a un conjunto arbitrario de números primos, una sucesión de polinomios que es compatible con el producto cuántico.

Teorema I.9: Sea P un conjunto de números primos y $S(P)$ el semigrupo generado por P. Definamos la sucesión $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ mediante:

$$f_n(q) = \begin{cases} [n]_q & \text{si} \quad n \in S(P) \\ 0 & \text{si} \quad n \notin S(P) \end{cases}$$

entonces la sucesión $\mathcal{F}$ satisface la ecuación funcional (1) y $\text{supp}(\mathcal{F}) = S(P)$.

Demostración:

Como el entero cuántico n es diferente de cero para toda n, por definición $\text{supp}(\mathcal{F}) = S(P)$.
Por el ejemplo 2 de la sección anterior, tenemos que la sucesión de enteros cuánticos satisface la ecuación funcional (1), por lo tanto si n y m están en $S(P)$ no hay nada que demostrar. Si n ó m

no están en $S(P)$, entonces $f_n(q)=0$ ó $f_m(q)=0$ y su producto $n\cdot m$ no está en $S(P)$, por lo tanto, $f_{mn}(q)=0$ y $\mathcal{F}$ es compatible con el producto cuántico. □

Hemos visto entonces que todo semigrupo primo $S(P)$ es el soporte de una sucesión de polinomios que satisfacen la ecuación funcional (1).

Los siguientes tres lemas nos servirán para demostrar el resultado principal de este capítulo que es el teoremaI.13, el cual nos da un método para construir soluciones de la ecuación funcional (1) con soporte $S(P)$ para cualquier conjunto *P* de números primos.

Lema I.10: Sea *p* un número primo y $h_p(q)$ un polinomio no-cero. Entonces existe una única sucesión $\mathcal{F}=\left\{f_{p^k}(q)\right\}_{k=0}^{\infty}$ tal que $f_p(q)=h_p(q)$ y $f_{p^k}(q)=f_{p^i}(q)f_{p^j}\left(q^{p^i}\right)$ para toda terna de enteros no negativos (i, j, k) tal que $k=i+j$.

Demostración:

Definamos la sucesión $\mathcal{F}=\left\{f_{p^k}(q)\right\}_{k=0}^{\infty}$ como $f_1(q)=1, f_p(q)=h_p(q)$ e inductivamente para $k\geq 2$:

$$f_{p^k}(q)=f_p(q)f_{p^{k-1}}\left(q^p\right).$$

Demostraremos por inducción sobre *k*, que se satisface la igualdad:

$$f_{p^k}(q)=f_{p^i}(q)f_{p^j}\left(q^{p^i}\right).$$

- Base de la inducción: Si $k=0, 1$ ó 2, usando que $f_1(q)=1$ se tiene la igualdad deseada. Similarmente, si $i=0$ entonces $j=k$, por lo que se tiene que $f_{p^k}(q)=f_{p^i}(q)f_{p^j}\left(q^{p^i}\right)=f_{p^0}(q)f_{p^k}\left(q^{p^0}\right)=f_{p^k}(q)$.

- Hipótesis de inducción: Supongamos que la igualdad se cumple para $k\geq 1$.

- Paso inductivo: Sea $k+1=i+j$ con $i\geq 1$. Entonces:

$$\begin{aligned} f_{p^{k+1}}(q) &= f_p(q)f_{p^k}\left(q^p\right) \\ &= f_p(q)f_{p^{(i-1)+j}}\left(q^p\right) \\ &= \left\{f_p(q)f_{p^{i-1}}\left(q^p\right)\right\}f_{p^j}\left(\left(q^p\right)^{p^{i-1}}\right) \text{ [por hipótesis de inducción]} \\ &= f_{p^i}(q)f_{p^j}\left(q^{p^i}\right). \end{aligned}$$

Por lo tanto, la sucesión $\left\{f_{p^k}(q)\right\}_{k=0}^{\infty}$ así definida satisface el lema.

Unicidad:

Supongamos que la sucesión $\mathcal{G}=\left\{g_{p^k}(q)\right\}_{k=0}^{\infty}$ también satisface la ecuación $g_{p^k}(q)=g_{p^i}(q)g_{p^j}\left(q^{p^i}\right)$ para toda terna de enteros no negativos (i,j,k) tal que $k=i+j$.
Entonces, si $i=j=k=0$, tenemos que $g_1(q)=g_1(q)g_1(q)$, por lo que $g_1(q)=f_1(q)=1$ y como $g_p(q)=h_p(q)=f_p(q)$ se tiene que $f_{p^k}(q)=g_{p^k}(q)$ $\forall k\geq 1$, por lo tanto la sucesión $\mathcal{F}=\left\{f_{p^k}(q)\right\}_{k=0}^{\infty}$ es única. □

Lema I.11: Sea $P=\{p_1,p_2\}$, donde p_1 y p_2 son primos distintos y sea $S(P)$ el semigrupo generado por *P*. Sean $h_{p_1}(q)$ y $h_{p_2}(q)$ polinomios no-cero que satisfacen la siguiente igualdad:

$$h_{p_1}(q)h_{p_2}\left(q^{p_1}\right)=h_{p_2}(q)\,h_{p_1}\left(q^{p_2}\right)$$

entonces existe una única sucesión $\left\{f_n(q)\right\}_{n\in S(P)}$ tal que $f_{p_1}(q)=h_{p_1}(q)$, $f_{p_2}(q)=h_{p_2}(q)$ y $f_{mn}(q)=f_m(q)f_n\left(q^m\right)$ $\forall m,n\in S(P)$.

Demostración:

Por la definición de $S(P)$, cada entero $n\in S(P)$ se puede escribir de manera única como $n=p_1^ip_2^j$ para enteros no negativos *i*, *j*.
Por el Lema I.10, existen y son únicas, las siguientes sucesiones de polinomios $\mathcal{F}_1=\left\{f_{p_1^i}(q)\right\}_{i=0}^{\infty}$ y $\mathcal{F}_2=\left\{f_{p_2^j}(q)\right\}_{j=0}^{\infty}$ que cumplen con que $f_{p_1}(q)=h_{p_1}(q)$ y $f_{p_2}(q)=h_{p_2}(q)$.
Para $n=p_1^ip_2^j$ con *i* y *j* enteros positivos definimos el polinomio $f_n(q)=f_{p_1^i}(q)f_{p_2^j}\left(q^{p_1^i}\right)$ y la sucesión $\left\{f_n(q)\right\}_{n\in S(P)}$. Para demostrar que $f_{mn}(q)=f_m(q)f_n\left(q^m\right)$ $\forall m,n\in S(P)$ como primer paso, demostraremos por inducción sobre $k=i+j$ que $\boxed{f_{p_1^i}(q)f_{p_2^j}\left(q^{p_1^i}\right)=f_{p_2^j}(q)f_{p_1^i}\left(q^{p_2^j}\right)}$ … (3) para todo *i, j* enteros positivos.

Si $i=0$ ó $j=0$ la igualdad se cumple trivialmente. Por lo tanto podemos suponer que $i\geq 1$, $j\geq 1$ y $k\geq 2$.

- Base de la inducción: Si $k=2$ con $i=1=j$:

$$f_{p_1^1}(q)f_{p_2^1}\left(q^{p_1^1}\right)=h_{p_1}(q)h_{p_2}\left(q^{p_1}\right)=h_{p_2}(q)\,h_{p_1}\left(q^{p_2}\right)=f_{p_2^1}(q)f_{p_1^1}\left(q^{p_2^1}\right).$$

- Hipótesis de inducción: Sea $k\geq 2$ y supongamos que el lema se cumple para todos los enteros positivos i,j tales que $i+j\leq k$.

- Paso inductivo: Sea $k+1=i+j+1$. Por el Lema I.10 y la hipótesis de inducción tenemos:

$$\begin{aligned}
f_{p_1^i}(q)f_{p_2^{j+1}}\left(q^{p_1^i}\right)&=f_{p_1^i}(q)f_{p_2^j}\left(q^{p_1^i}\right)f_{p_2}\left(q^{p_1^ip_2^j}\right)\\
&=f_{p_2^j}(q)f_{p_1^i}\left(q^{p_2^j}\right)f_{p_2}\left(q^{p_2^jp_1^i}\right)\left[\text{por la hipótesis de inducción}\right]\\
&=f_{p_2^j}(q)f_{p_2}\left(q^{p_2^j}\right)f_{p_1^i}\left(q^{p_2^{j+1}}\right)\\
&=f_{p_2^{j+1}}(q)f_{p_1^i}\left(q^{p_2^{j+1}}\right).
\end{aligned}$$

Análogamente, $f_{p_1^{i+1}}(q)f_{p_2^j}\left(q^{p_1^{i+1}}\right)=f_{p_2^j}(q)f_{p_1^{i+1}}\left(q^{p_2^j}\right)$.

Ahora sean $m,n\in S(P)$, i,j,k,l enteros positivos tales que $m=p_1^ip_2^j$ y $n=p_1^kp_2^l$. Entonces:

$$\begin{aligned}
f_m(q)f_n\left(q^m\right)&=f_{p_1^i}(q)\left\{f_{p_2^j}\left(q^{p_1^i}\right)f_{p_1^k}\left(q^{p_1^ip_2^j}\right)\right\}f_{p_2^l}\left(q^{p_1^{i+k}p_2^j}\right)\\
&=\left\{f_{p_1^i}(q)f_{p_1^k}\left(q^{p_1^i}\right)\right\}\left\{f_{p_2^j}\left(q^{p_1^{i+k}}\right)f_{p_2^l}\left(q^{p_1^{i+k}p_2^j}\right)\right\}\\
&=f_{p_1^k}(q)\left\{f_{p_1^i}\left(q^{p_1^k}\right)f_{p_2^l}\left(q^{p_1^{i+k}}\right)\right\}f_{p_2^j}\left(q^{p_1^{i+k}p_2^l}\right)\\
&=f_{p_1^k}(q)f_{p_2^l}\left(q^{p_1^k}\right)f_{p_1^i}\left(q^{p_1^kp_2^l}\right)f_{p_2^j}\left(q^{p_1^{i+k}p_2^l}\right)\\
&=f_n(q)f_m\left(q^n\right).
\end{aligned}$$

Para ver la unicidad de $\mathbb{F}$, si se satisface la ecuación $f_{mn}(q)=f_m(q)f_n\left(q^m\right)\ \forall m,n\in S(P)$ tomando $s=p_1^ip_2^j$ y $n=p_2^j$ tenemos que $f_s=f_{p_1^ip_2^j}(q)=f_{p_1^i}(q)f_{p_2^j}\left(q^{p_1^i}\right)$. Por lo que la sucesión de polinomios $\left\{f_n(q)\right\}_{n\in S(P)}$ es única. □

Lema I.12: Sea $P=\{p_1,p_2,...,p_r\}$ un conjunto de *r* números primos y sea $S(P)$ el semigrupo generado por *P*. Sean $h_{p_1}(q),...,h_{p_r}(q)$ polinomios no-cero tales que $h_{p_i}(q)h_{p_j}(q^{p_i})=h_{p_j}(q)\,h_{p_i}(q^{p_j})$ … (4) para $i,j=1,...,r$. Entonces existe una única sucesión de polinomios $\{f_n(q)\}_{n\in S(P)}$ tal que $f_{p_i}(q)=h_{p_i}(q)\ \forall i=1,...,r$ y para toda $m,n\in S(P)$, $f_{mn}(q)=f_m(q)f_n(q^m)$ … (5).

Demostración: (Por inducción sobre *r*)

- Base de la inducción: Si $r=1$ ó $r=2$ se tiene el resultado por los lemas I.10 y I.11.
- Hipótesis de inducción: Sea $r\geq 1$ y supongamos que el Lema I.12 se cumple para todo conjunto de $r-1$ primos.
- Paso inductivo: Sea $P'=P\setminus\{p_r\}=\{p_1,...,p_{r-1}\}$, por la hipótesis de inducción existe una única sucesión $\{f_n(q)\}_{n\in S(P')}$ tal que $f_{p_i}(q)=h_{p_i}(q)\ \forall i=1,...,r-1$ y $f_{m'n'}(q)=f_{m'}(q)f_{n'}(q^{m'})\ \forall\ m',n'\in S(P')$.

  Para cada $n\in S(P)\setminus S(P')$, *n* se puede escribir de manera única como $n=n'\cdot p_r^{a_r}$; donde $n'\in S(P')$ y a_r es un entero positivo.

  Definimos $f_{p_r^{a_r}}(q)$ por el Lema I.10 y $f_{n'p_r^{a_r}}(q)=f_{n'}(q)f_{p_r^{a_r}}(q^{n'})$ … (6).

  Primero probaremos la igualdad $f_{n'}(q)f_{p_r^{a_r}}(q^{n'})=f_{p_r^{a_r}}(q)f_{n'}(q^{p_r^{a_r}})$ … (7) para todo $n'\in S(P')$ y $a_r\in\mathbb{N}$.

  Si $n'=p_s^{a_s}$ para algún primo $p_s\in P'$, entonces es claro que la igualdad (7) se cumple gracias al Lema I.11, puesto que:

  $f_{p_s^{a_s}}(q)f_{p_r^{a_r}}(q^{p_s^{a_s}})=f_{p_r^{a_r}}(q)f_{p_s^{a_s}}(q^{p_r^{a_r}})$ que es exactamente la igualdad (3).

  Sea $n'=n''\cdot p_s^{a_s}$, donde $n''\in S(P\setminus\{p_s,p_r\})$. Entonces por hipótesis de inducción tenemos que $f_{n''}(q)f_{p_r^{a_r}}(q^{n''})=f_{p_r^{a_r}}(q)f_{n''}(q^{p_r^{a_r}})$.

  Entonces:

$$\begin{aligned}
f_{n'}(q)f_{p_r^{a_r}}(q^{n'}) &= f_{n''}(q)\left\{f_{p_s^{a_s}}(q^{n''})f_{p_r^{a_r}}(q^{n''p_s^{a_s}})\right\}\ [n'=n''p_s^{a_s}]\\
&= \left\{f_{n''}(q)f_{p_r^{a_r}}(q^{n''})\right\}f_{p_s^{a_s}}(q^{n''p_r^{a_r}})\ [\text{por (4)}]\\
&= f_{p_r^{a_r}}(q)\left\{f_{n''}(q^{p_r^{a_r}})f_{p_s^{a_s}}(q^{n''p_r^{a_r}})\right\}\ [\text{nuevamente por (4)}]\\
&= f_{p_r^{a_r}}(q)f_{n'}(q^{p_r^{a_r}})\ [\text{por (6)}].
\end{aligned}$$

Por lo tanto, la ecuación (7) se satisface.

Ahora probaremos la ecuación (5). Para esto, sean $m,n \in S(P)$, entonces $n = n' p_r^{a_r}$ y $m = m' p_r^{b_r}$, donde $m', n' \in S(P')$ y $a_r, b_r \in \mathbb{N}$. Si aplicamos la ecuación (7) y la hipótesis de inducción resulta que:

$$\begin{aligned} f_m(q) f_n(q^m) &= f_{m'}(q)\left\{f_{p_r^{a_r}}(q^{m'}) f_{n'}(q^{m' p_r^{b_r}})\right\} f_{p_r^{a_r}}(q^{m'n' p_r^{b_r}}) \\ &= \left\{f_{m'}(q) f_{n'}(q^{m'})\right\}\left\{f_{p_r^{b_r}}(q^{m'n'}) f_{p_r^{a_r}}(q^{m'n' p_r^{b_r}})\right\} \text{ [por (5)]} \\ &= f_{n'}(q)\left\{f_{m'}(q^{n'}) f_{p_r^{a_r}}(q^{m'n'})\right\} f_{p_r^{b_r}}(q^{m'n' p_r^{a_r}}) \text{ [por (2) y la hipótesis de inducción]} \\ &= f_{n'}(q) f_{p_r^{a_r}}(q^{n'}) f_{m'}(q^{n' p_r^{a_r}}) f_{p_r^{b_r}}(q^{m'n' p_r^{a_r}}) \\ &= f_n(q) f_m(q^n). \end{aligned}$$

Por lo tanto, la ecuación (5) se cumple.

Unicidad:

Si sustituimos en la ecuación (5) $m = n'$ y $n = p_r^{a_r}$ tenemos que:
$f_{n'}(q) f_{p_r^{a_r}}(q^{n'}) = f_{p_r^{a_r}}(q) f_{n'}(q^{p_r^{a_r}}) = f_{n' p_r^{a_r}}(q)$ que resulta ser exactamente la ecuación (6).
Por lo tanto la sucesión $\{f_n(q)\}_{n \in S(P)}$ es única. □

Procederemos a continuación a ver el teorema principal de este capítulo.

Teorema I.13: Sea *P* un conjunto de números primos. Para cada $p \in P$, sea $h_p(q)$ un polinomio no-cero tal que $h_{p_1}(q) h_{p_2}(q^{p_1}) = h_{p_2}(q) h_{p_1}(q^{p_2}) \ \forall\, p_1, p_2 \in P$. Entonces existe una única sucesión $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ con $\operatorname{supp}(\mathcal{F}) = S(P)$ tal que $\mathcal{F}$ satisface la ecuación funcional $f_{mn}(q) = f_m(q) \otimes_q f_n(q) = f_m(q) f_n(q^m)$ para todo *m, n* en los naturales. Además para todo *p* en *P* se tiene que $f_p(q) = h_p(q)$.

Demostración:

i) Si *P* es un conjunto finito de números primos, entonces por el Lema I.12, existe la sucesión $\mathcal{F} = \{f_n(q)\}_{n \in S(P)}$ y definiendo $f_n(q) = 0$ para $n \notin S(P)$ se tiene determinada de manera única la sucesión $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ que realiza el teorema.

ii) Si P es infinito, escribimos $P=\{p_i\}_{i=1}^{\infty}$. Para cada entero positivo r, sea $P_r=\{p_i\}_{i=1}^{r}$ y aplicando el Lema I.12 tenemos un conjunto de sucesiones de la forma $\{f_n(q)\}_{n\in S(\Pr)}$.

Como $P_1\subseteq\ldots\subseteq P_r\subseteq P_{r+1}\subseteq\ldots\subseteq P$ y $S(P_1)\subseteq\ldots\subseteq S(P_r)\subseteq S(P_{r+1})\subseteq\ldots\subseteq S(P)$, entonces $\{f_n(q)\}_{n\in S(P_1)}\subseteq\ldots\subseteq\{f_n(q)\}_{n\in S(P_r)}\subseteq\ldots$

Lo que nos permite definir la sucesión:

$$\{f_n(q)\}_{n\in S(P)}=\bigcup_{r=1}^{\infty}\{f_n(q)\}_{n\in S(P_r)}.$$

Haciendo $f_n(q)=0$ para toda $n\notin S(P)$, tenemos determinada de manera única la sucesión $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ que por construcción satisface la ecuación funcional $f_{mn}(q)=f_m(q)\otimes_q f_n(q)=f_m(q)f_n(q^m)$ y $f_p(q)=h_p(q)\ \forall\ p\in P$. □

Ejemplo: Sea $P=\{2,5,7\}$, y los polinomios:

$$\begin{aligned}h_2(q)&=1-q+q^2\\ h_5(q)&=1-q+q^3-q^4+q^5-q^7+q^8\\ h_7(q)&=1-q+q^3-q^4+q^6-q^8+q^9-q^{11}+q^{12}.\end{aligned}$$

Un cálculo simple pero largo nos demuestra que $h_{p_1}(q)h_{p_2}(q^{p_1})=h_{p_2}(q)\,h_{p_1}(q^{p_2})$ para cada par de primos $p_1,p_2\in P$.

Veamos por ejemplo el caso $p_1=2$ y $p_2=5$.

Por un lado,

$$\begin{aligned}h_2(q)h_5(q^2)&=(1-q+q^2)(1-q^2+q^6-q^8+q^{10}-q^{14}+q^{16})\\ &=q^{18}-q^{17}+q^{15}-q^{14}+q^{12}-q^{11}+q^9-q^7+q^6-q^4+q^3-q+1.\end{aligned}$$

Por otro lado,

$$\begin{aligned}h_5(q)\,h_2(q^5)&=(1-q+q^3-q^4+q^5-q^7+q^8)(1-q^5+q^{10})\\ &=q^{18}-q^{17}+q^{15}-q^{14}+q^{12}-q^{11}+q^9-q^7+q^6-q^4+q^3-q+1.\end{aligned}$$

Observemos además que los polinomios dados son cocientes de enteros cuánticos. Explícitamente,

$$h_2(q)=\frac{[2]_{q^3}}{[2]_q}=\frac{1+q^3}{1+q}=q^2-q+1=1-q+q^2.$$

$$h_5(q)=\frac{[5]_{q^3}}{[5]_q}=\frac{1+q^3+q^6+q^9+q^{12}}{1+q+q^2+q^3+q^4}=q^3-q-q^4+q^5-q^7+q^8+1.$$

$$h_7(q)=\frac{[7]_{q^3}}{[7]_q}=\frac{1+q^3+q^6+q^9+q^{12}+q^{15}+q^{18}}{1+q+q^2+q^3+q^4+q^5+q^6}=q^3-q-q^4+q^6-q^8+q^9-q^{11}+q^{12}+1.$$

Haciendo $f_2(q)=h_2(q)=\frac{[2]_{q^3}}{[2]_q}$, $f_5(q)=h_5(q)=\frac{[5]_{q^3}}{[5]_q}$ y $f_7(q)=h_7(q)=\frac{[7]_{q^3}}{[7]_q}$, por el teorema I.13 sabemos que existe una única sucesión de polinomios $\mathfrak{F}=\{f_n(q)\}_{n=1}^{\infty}$ que satisface la ecuación funcional $f_{mn}(q)=f_m(q)\otimes_q f_n(q)=f_m(q)f_n(q^m)$ para todo *m, n* en los naturales. Observemos que en el ejemplo, $f_n(q)=\frac{[n]_{q^3}}{[n]_q}$ $\forall n\in S(P)$ y $\operatorname{gr}(f_n)=2(n-1)$ $\forall n\in S(P)$.

2. ECUACIONES FUNCIONALES ARITMÉTICAS

El resultado principal de esta sección es el teorema I.18, el cual nos da una sucesión de polinomios que satisfacen la ecuación funcional $f_{mn}(q)=f_m(q)\otimes_q f_n(q)=f_m(q)f_n(q^m)\ \forall m,n\in\mathbb{N}$. A similitud de la sección anterior, el concepto de semigrupo primo será reemplazado por el de función aritmética.

Definición I.14: Una **función aritmética** es una función cuyo dominio es el conjunto de los números naturales $\mathbb{N}$. El soporte de la función aritmética δ es $\operatorname{supp}(\delta)=\{n\in\mathbb{N}/\delta(n)\neq 0\}$.

Lema I.15: Sea *S* un semigrupo de números naturales y $\delta(n)$ una función aritmética con valores en los números complejos que satisface la ecuación funcional:

$$\delta(mn)=\delta(m)+m\delta(n)\ \forall m,n\in S.$$

Entonces existe un número complejo *t* tal que $\delta(n)=t(n-1)\ \forall n\in S$.

Demostración:

Sea $\delta(n)$ una solución de la ecuación funcional dada. Si $m=n=1$ tenemos que $\delta(1\cdot 1)=\delta(1)+1\cdot\delta(1)$. Por lo tanto, $\delta(1)-\delta(1)=\delta(1)$ y $\delta(1)=0$.
Para cualesquiera $m,n\in S\setminus\{1\}$, $\delta(m)+m\delta(n)=\delta(mn)=\delta(nm)=\delta(n)+n\delta(m)$ por la conmutatividad de los naturales.

La igualdad $\delta(m)+m\delta(n)=\delta(n)+n\delta(m)$ implica que $m\delta(n)-\delta(n)=n\delta(m)-\delta(m)$, de donde se tiene que $\delta(n)(m-1)=\delta(m)(n-1)$ y $\dfrac{\delta(n)}{n-1}=\dfrac{\delta(m)}{m-1}$. Si hacemos $t=\dfrac{\delta(m)}{m-1}$ llegamos a que $\delta(n)=t(n-1)\ \forall n\in S$.

Claramente *t* es un número complejo ya que δ es una función que toma valores complejos. □

Observación: Si $\delta(n)=0$ para alguna $n\in S\setminus\{1\}$, entonces $\delta(n)=0\ \forall n\in S$.

Lema I.16: Sea $\mathbb{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios no-cero que satisfacen la ecuación funcional $f_{mn}(q)=f_m(q)f_n(q^m)$. Entonces existe un número racional no negativo *t* tal que para toda *n* en el soporte de $\mathbb{F}$ se tiene que $\operatorname{gr}(f_n)=t(n-1)$.

Demostración:

Sea $S=\text{supp}(\mathcal{F})$. La ecuación funcional $f_{mn}(q)=f_m(q)f_n(q^m)$, implica que $\text{gr}(f_{mn})=\text{gr}(f_m)+m\,\text{gr}(f_n)\ \forall m,n\in S$. Por lo tanto $\text{gr}(f_n)$ es una función aritmética que toma valores en los naturales y satisface las hipótesis del lema I.15, por lo que existe un complejo, que resulta ser un racional $t=\dfrac{\text{gr}(f_m)}{m-1}$ tal que $\text{gr}(f_n)=t(n-1)\ \forall n\in S$. □

Observemos que el número *t* es un número racional pero no necesariamente es un número entero.

Definición I.17: Una función aritmética $\lambda(n)$ es **completamente multiplicativa** si $\lambda(mn)=\lambda(m)\lambda(n)\ \forall m,n\in\mathbb{N}$. Una función es **completamente multiplicativa en un semigrupo *S*** si $\lambda(n)$ es una función definida en *S* y $\lambda(mn)=\lambda(m)\lambda(n)\ \forall m,n\in S$.

Teorema I.18: Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios no-cero tales que satisfacen la ecuación funcional $f_{mn}(q)=f_m(q)f_n(q^m)$. Entonces existe una función aritmética completamente multiplicativa $\lambda(n)$, un número racional no negativo *t* y una sucesión no-cero de polinomios $\mathcal{G}=\{g_n(q)\}_{n=1}^{\infty}$ tal que $f_n(q)=\lambda(n)q^{t(n-1)}g_n(q)\ \forall n\in\mathbb{N}$. Además:

i) La sucesión $\mathcal{G}$ satisface la ecuación funcional $g_{mn}(q)=g_m(q)g_n(q^m)$.

ii) $\text{supp}(\mathcal{F})=\text{supp}(\mathcal{G})=\text{supp}(\lambda)$.

iii) $g_n(0)=1\ \forall n\in\text{supp}(\mathcal{G})$.

El número *t*, la función aritmética $\lambda(n)$ y la sucesión $\mathcal{G}$ son únicos.

Demostración:

Primero vamos a construir $\lambda(n)$ y $\mathcal{G}=\{g_n(q)\}_{n=1}^{\infty}$.

Para cada $n\in\text{supp}(\mathcal{F})$ $(f_n(q)\neq 0)$ existe un único entero no negativo $\delta(n)$ y un polinomio $g'_n(q)$ tal que $g'_n(0)\neq 0$ y $f_n(q)=q^{\delta(n)}g'_n(q)$.

Definimos $\boxed{\lambda(n)=g'_n(0)}$, es decir, el término constante de $g'_n(q)$. Si dividimos $g'_n(q)$ entre $\lambda(n)$, podemos escribir $g'_n(q)=\lambda(n)g_n(q)$, donde $g_n(q)$ es un polinomio con término constante $g_n(0)=1$ y así acabamos de probar el punto *iii)*.

Como $g'_n(q)=\lambda(n)g_n(q)$ y $\lambda(n)\neq 0$ entonces definimos $\boxed{g_n(q)=\frac{g'_n(q)}{\lambda(n)}}$ y con esta definición ya podemos construir la sucesión $\mathcal{G}=\{g_n(q)\}_{n=1}^{\infty}$.

Ahora bien, si $n\notin \operatorname{supp}(\mathcal{F})$, definimos $g_n(q)=0$ y $\lambda(n)=0$.

Ahora probaremos el punto *ii)*, es decir, $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})=\operatorname{supp}(\lambda)$, para esto primero veamos que $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})$.

$\subseteq]$ Sea $n\in\operatorname{supp}(\mathcal{F})$, entonces $f_n(q)\neq 0$ y $f_n(q)=q^{\delta(n)}g'_n(q)$ lo cual implica que $q^{\delta(n)}\neq 0$ y $g'_n(q)\neq 0$. Como $g_n(q)=\frac{g'_n(q)}{\lambda(n)}$, entonces $g_n(q)\neq 0$. Por lo tanto $n\in\operatorname{supp}(\mathcal{G})$.

$\therefore\ \operatorname{supp}(\mathcal{F})\subseteq\operatorname{supp}(\mathcal{G})$.

$\supseteq]$ Supongamos lo contrario, es decir, supongamos que $\operatorname{supp}(\mathcal{G})\not\subseteq\operatorname{supp}(\mathcal{F})$, entonces existe un natural $n\in\operatorname{supp}(\mathcal{G})$ tal que $n\notin\operatorname{supp}(\mathcal{F})$. Como $n\in\operatorname{supp}(\mathcal{G})$, entonces $g_n(q)\neq 0$ pero por otro lado, como $n\notin\operatorname{supp}(\mathcal{F})$, entonces $g_n(q)=0$ lo cual es una contradicción.

$\therefore\ \operatorname{supp}(\mathcal{G})\subseteq\operatorname{supp}(\mathcal{F})$.

Por lo tanto tenemos que $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})$.

Ahora probemos la otra igualdad, es decir, $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\lambda)$.

$\subseteq]$ Sea $n\in\operatorname{supp}(\mathcal{F})$, entonces $f_n(q)=q^{\delta(n)}g'_n(q)$ con $g'_n(q)\neq 0$. Por definición $\lambda(n)=g'_n(0)\neq 0$ lo cual implica que $\lambda(n)\neq 0$. Así, $n\in\operatorname{supp}(\lambda)$.

$\therefore\ \operatorname{supp}(\mathcal{F})\subseteq\operatorname{supp}(\lambda)$.

$\supseteq]$ Supongamos lo contrario, es decir, supongamos que $\operatorname{supp}(\lambda)\not\subseteq\operatorname{supp}(\mathcal{F})$, entonces existe un natural $n\in\operatorname{supp}(\lambda)$ tal que $n\notin\operatorname{supp}(\mathcal{F})$. Como $n\in\operatorname{supp}(\lambda)$, entonces $\lambda(n)\neq 0$ pero por otro lado, como $n\notin\operatorname{supp}(\mathcal{F})$, entonces $\lambda(n)=0$ lo cual es una contradicción.

$\therefore\ \operatorname{supp}(\lambda)\subseteq\operatorname{supp}(\mathcal{F})$.

Por lo tanto tenemos que $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\lambda)$.

Así, si juntamos ambas igualdades resulta que $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})=\operatorname{supp}(\lambda)$ que es lo que queríamos probar.

Ahora veamos que la sucesión $\left\{\lambda(n)q^{\delta(n)}g_n(q)\right\}_{n=1}^{\infty}$ satisface la ecuación funcional (1):

Por la manera de construir $g_n(q)$ y $\lambda(n)$, si tomamos $m,n\notin \operatorname{supp}(\mathcal{F})$ la ecuación funcional (1) se satisface trivialmente.

Sean $m,n\in \operatorname{supp}(\mathcal{F})$, como el soporte de $\mathcal{F}$ es un semigrupo tenemos entonces que $mn\in \operatorname{supp}(\mathcal{F})$ y por lo tanto $f_{mn}(q)=q^{\delta(mn)}g'_{mn}(q)$.

$$\begin{aligned}\lambda(mn)q^{\delta(mn)}g_{mn}(q)&=\frac{\lambda(mn)q^{\delta(mn)}g'_{mn}(q)}{\lambda(mn)}\\&=q^{\delta(mn)}g'_{mn}(q)\\&=f_{mn}(q)\\&=f_m(q)f_n(q^m)\ \text{(pues } \left\{f_n(q)\right\}_{n=1}^{\infty}\ \text{satisface (1))}\\&=q^{\delta(m)}g'_m(q)q^{m\delta(n)}g'_n(q^m)\\&=q^{\delta(m)}\lambda(m)g_m(q)q^{m\delta(n)}\lambda(n)g_n(q^m)\\&=\lambda(m)q^{\delta(m)}g_m(q)\lambda(n)q^{m\delta(n)}g_n(q^m).\end{aligned}$$

Por lo tanto $\left\{\lambda(n)q^{\delta(n)}g_n(q)\right\}_{n=1}^{\infty}$ satisface la ecuación (1).

Así, para toda $m,n\in \operatorname{supp}(\mathcal{F})$:

$$\begin{aligned}\lambda(mn)q^{\delta(mn)}g_{mn}(q)&=\lambda(m)q^{\delta(m)}g_m(q)\lambda(n)q^{m\delta(n)}g_n(q^m)\\&=\lambda(m)\lambda(n)q^{\delta(m)+m\delta(n)}g_m(q)g_n(q^m).\end{aligned}$$

Los polinomios $g_m(q)$, $g_n(q)$ y $g_{mn}(q)$ tienen termino constante 1, entonces para toda $m,n\in \operatorname{supp}(\mathcal{F})$ tenemos que:

$$q^{\delta(mn)}=q^{\delta(m)+m\delta(n)}\ ,\ \lambda(mn)=\lambda(m)\lambda(n)\ \text{y}\ g_{mn}(q)=g_m(q)g_n(q^m).$$

De $q^{\delta(mn)}=q^{\delta(m)+m\delta(n)}$ tenemos que $\delta(mn)=\delta(m)+m\delta(n)\ \forall m,n\in \operatorname{supp}(\mathcal{F})$. Por el Lema I.15, existe un número racional no negativo *t* tal que $\delta(n)=t(n-1)$ y de esta manera tenemos que $f_n(q)=q^{\delta(n)}g'_n(q)=q^{t(n-1)}\lambda(n)g_n(q)=\lambda(n)q^{t(n-1)}g_n(q)\ \forall n\in\mathbb{N}$.

De $\lambda(mn)=\lambda(m)\lambda(n)$ se tiene que $\lambda(n)$ es una función aritmética completamente multiplicativa con soporte $\operatorname{supp}(\mathcal{F})$.

Por último, de $g_{mn}(q) = g_m(q)\, g_n(q^m)$ se sigue que la sucesión $\mathcal{G} = \{g_n(q)\}_{n=1}^{\infty}$ satisface la ecuación funcional (1). □

Observemos que por el Teorema I.18, la clasificación de soluciones de la ecuación funcional (1) se reduce a la clasificación de sucesiones de polinomios $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ con término constante $f_n(0) = 1 \ \forall\, n \in \operatorname{supp}(\mathcal{F})$.

3. EXISTENCIA DE SOLUCIONES

El siguiente teorema nos permite, dada una sucesión de polinomios $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ que satisface la ecuación funcional (1), construir nuevas sucesiones que también son compatibles con el producto cuántico.

Teorema I.19: Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios no-cero que satisface la ecuación funcional (1). Entonces las siguientes sucesiones de polinomios son compatibles con el producto cuántico.

i) La sucesión $\{f_n(\psi(q))\}_{n=1}^{\infty}$, donde $\psi(q)$ es un polinomio tal que $\psi(q)^m=\psi(q^m)$ para todo entero $m\in\mathrm{supp}(\mathcal{F})$.

ii) La sucesión $\{f_n(q^t)\}_{n=1}^{\infty}$, para todo entero positivo *t*.

iii) La sucesión de polinomios recíprocos $\{q^{\mathrm{gr}(f_n)}f_n(q^{-1})\}_{n=1}^{\infty}$.

Demostración:

Supongamos que $\psi(q)^m=\psi(q^m)$ para todo $m\in\mathrm{supp}(\mathcal{F})$. Como $f_{mn}(q)=f_m(q)f_n(q^m)$ para todo *m, n* en el soporte de $\mathcal{F}$. Reemplazando *q* por $\psi(q)$ tenemos la siguiente igualdad:

$$f_{mn}(\psi(q))=f_m(\psi(q))f_n(\psi(q)^m)\quad\forall m,n\in\mathrm{supp}(\mathcal{F}).$$

Lo que demuestra el primer inciso del teorema.

Para demostrar el segundo inciso, observemos que $(q^t)^m=(q^m)^t\ \forall t\in\mathbb{Z}$, si en *i)* hacemos $\psi(q)=q^t$ tenemos que $\psi(q)^m=(q^t)^m=(q^m)^t=\psi(q^m)$ y por lo tanto la $\{f_n(q^t)\}_{n=1}^{\infty}$ es compatible con el producto cuántico para todo entero positivo *t*.

Finalmente, si consideramos el polinomio recíproco de $f(q)$, $f(q)=q^{\mathrm{gr}(f)}f(q^{-1})$, entonces:

$$\begin{aligned}f_{mn}(q)&=q^{\mathrm{gr}(f_{mn})}f_{mn}(q^{-1})\\&=q^{\mathrm{gr}(f_m)+m\,\mathrm{gr}(f_n)}f_m(q^{-1})f_n(q^{-m})\\&=q^{\mathrm{gr}(f_m)}q^{m\,\mathrm{gr}(f_n)}f_m(q^{-1})f_n(q^{-m})\\&=q^{\mathrm{gr}(f_m)}f_m(q^{-1})q^{m\,\mathrm{gr}(f_n)}f_n(q^{-m})\\&=f_m(q)f_n(q^m).\end{aligned}$$

Lo cual demuestra el último inciso del teorema. □

Ejemplo: Consideremos $[n]_{q^t} = 1 + q^t + q^{2t} + \ldots + q^{(n-1)t}$, podemos observar que $\left\{[n]_{q^t}\right\}_{n=1}^{\infty}$ es solución de (1) con soporte $\mathbb{N}$.

El entero cuántico $[n]_q$ es un polinomio auto recíproco puesto que:

$$\begin{aligned}
[n]_q &= q^{\mathrm{gr}\left([n]_q\right)}[n]_{q^{-1}} \\
&= q^{n-1}\left(1 + q^{-1} + q^{-2} + \ldots + q^{-(n-1)}\right) \\
&= q^{n-1} + q^{n-2} + q^{n-3} + \ldots + q^0 \\
&= 1 + q + q^2 + \ldots + q^{n-1} \\
&= [n]_q .
\end{aligned}$$

De la misma manera se observa que $[n]_{q^t}$ es auto recíproco para todos los enteros positivos *t*. El polinomio recíproco del polinomio q^{n-1} es 1.

Observación: Aunque pareciera que los polinomios $\psi(q) = q^t$ son los únicos que generan soluciones de la ecuación funcional $f_{mn}(q) = f_m(q) \otimes_q f_n(q) = f_m(q) f_n\left(q^m\right) \; \forall m, n \in \mathbb{N}$, no lo son. Veamos esta afirmación con un ejemplo:

Tomemos un número primo cualquiera *p* y consideremos todos los polinomios con coeficientes en el campo $\mathbb{Z}/p\mathbb{Z}$. Sea $\mathcal{F} = \left\{f_n(q)\right\}_{n=1}^{\infty}$ solución de la ecuación funcional (1) y tal que $\mathrm{supp}\left(\mathcal{F}\right) = S\left(\{p\}\right) = \left\{p^k / k \in \mathbb{N}_0\right\}$. Ahora bien, si aplicamos el automorfismo de Frobenius ($z \mapsto z^p$) notamos que $\psi(q)^m = \psi\left(q^m\right)$ se cumple para todo polinomio $\psi(q)$ y para toda $m \in \mathrm{supp}\left(\mathcal{F}\right)$.

Así, acabamos de mostrar soluciones de la ecuación funcional (1) que están generadas por polinomios tales que $\psi(q)^m = \psi\left(q^m\right)$ para $m \in \mathrm{supp}\left(\mathcal{F}\right)$.

Ahora presentaremos un resultado que nos da condiciones necesarias y suficientes para que una sucesión de polinomios sea compatible con el producto cuántico. Pero antes recordemos la definición de raíz de la unidad.

Definición: Las **raíces *d*-ésimas de la unidad**, o números de de Moivre, son todos los números complejos que resultan 1 cuando son elevados a una potencia dada *d*. Se puede demostrar que están localizados en el círculo unitario del plano complejo y que en ese plano forman los vértices de un polígono regular de *d* lados con un vértice sobre 1.

Teorema I.20: Sea *P* un conjunto no vacío de números primos y $S(P)$ el semigrupo multiplicativo generado por *P*. Sea *d* el máximo común divisor del conjunto $\{p-1 : p \in P\}$. Para $\zeta \neq 0$, sea $f_n(q) = \sum_{i=0}^{n-1} \zeta^i q^i = [n]_{\zeta q}$ para $n \in S(P)$, y sea $f_n(q) = 0$ para $n \notin S(P)$. Si ζ es una *d*-ésima raíz de la unidad, entonces la sucesión de polinomios $\mathbb{F} = \{f_n(q)\}_{n=1}^{\infty}$ satisface la ecuación funcional (1). Inversamente, si $\mathbb{F}$ es compatible con el producto cuántico entonces ζ es una *d*-ésima raíz de la unidad.

Demostración:

$\Rightarrow$] Sea ζ una *d*-ésima raíz de la unidad, y $\psi(q) = \zeta q$. Como *d* es el máximo común divisor del conjunto $\{p-1 : p \in P\}$, entonces $d \mid p-1 \ \forall p \in P$, *i.e.*, $p \equiv 1 \pmod{d}$ para toda $p \in P$. Ahora, si $m \in S(P)$ tenemos que $m = p_1 p_2 ... p_r$; donde $p_i \in P \ \forall i = 1,...,r$. Entonces $m \equiv 1 \pmod{d}$ para toda $m \in S(P)$. Por lo tanto, si $m \in S(P)$, entonces $\psi(q)^m = (\zeta q)^m = \zeta^m q^m = \zeta q^m = \psi(q^m)$ ya que ζ es una *d*-ésima raíz de la unidad.

Por el inciso *i)* del teorema I.19, se sigue que la sucesión de polinomios $\mathbb{F} = \{f_n(q)\}_{n=1}^{\infty}$ donde $f_n(q) = [n]_{\zeta q} = \sum_{i=0}^{n-1} \zeta^i q^i$ para $n \in S(P)$ y $f_n(q) = 0$ para $n \notin S(P)$, satisface la ecuación funcional (1).

$\Leftarrow$] Supongamos que $\mathbb{F}$ es compatible con el producto cuántico. Sean $m, n \in S(P) \setminus \{1\}$.
Entonces:

$$f_m(q) f_n(q^m) = \left(\sum_{i=0}^{m-1} \zeta^i q^i \right) \left(\sum_{j=0}^{n-1} \zeta^j q^{mj} \right) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \zeta^{i+j} q^{i+mj},$$

$$f_{mn}(q) = \sum_{k=0}^{mn-1} \zeta^k q^k = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \zeta^{i+mj} q^{i+mj}.$$

Y además para todo *m, n* en los naturales, la sucesión de polinomios $\mathbb{F}$ satisface la ecuación funcional $f_{mn}(q) = f_m(q) f_n(q^m)$, entonces $\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \zeta^{i+j} q^{i+mj} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \zeta^{i+mj} q^{i+mj}$, lo cual implica que $\zeta^{i+j} = \zeta^{i+mj}$ para $0 \le i \le m-1$ y $0 \le j \le n-1$. Entonces $\zeta^{j(m-1)} = 1$ y $\zeta^{m-1} = 1 \ \forall m \in S(P)$. Así, ζ es una *l*-ésima raíz de la unidad para algún entero positivo *l*, y *l* divide a $m-1$ para toda $m \in S(P)$. Por lo tanto, *l* divide a *d*, el máximo común divisor de los enteros $m-1$, y entonces ζ es una *d*-ésima raíz de la unidad. □

Recordemos la definición de sucesión producto.

Definición I.21: Sean $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ y $\mathcal{G}=\{g_n(q)\}_{n=1}^{\infty}$ dos sucesiones de polinomios. Definimos la **sucesión producto** como $\mathcal{FG}=\{f_n g_n(q)\}_{n=1}^{\infty}$ donde $f_n g_n(q)=f_n(q)g_n(q)$.

El siguiente teorema nos muestra que si tenemos dos sucesiones compatibles con el producto cuántico, su sucesión producto también lo es.

Teorema I.22: Sean $\mathcal{F}$ y $\mathcal{G}$ sucesiones no-cero de polinomios compatibles con el producto cuántico, entonces la sucesión producto $\mathcal{FG}$ también es compatible. Inversamente, si $\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})$ y si $\mathcal{F}$ y $\mathcal{FG}$ satisfacen la ecuación funcional (1), entonces $\mathcal{G}$ también la satisface. Además, el conjunto de todas las soluciones de la ecuación funcional (1) es un semigrupo abeliano y para todo semigrupo primo $S(P)$, el conjunto $\Gamma(P)$ de todas las sucesiones de funciones $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ compatibles con el producto cuántico tales que $\operatorname{supp}(\mathcal{F})=S(P)$ es un semigrupo abeliano con cancelación.

Demostración:

$\Rightarrow$] Si $\mathcal{F}$ y $\mathcal{G}$ ambas satisfacen (1), tenemos que:

$$\begin{aligned} f_{mn}g_{mn}(q) &= f_{mn}(q)g_{mn}(q) \\ &= f_m(q)f_n(q^m)g_m(q)g_n(q^m) \\ &= f_m g_m(q)f_n g_n(q^m). \end{aligned}$$

Entonces $\mathcal{FG}$ satisface (1).

$\Leftarrow$] Si $m,n\in\operatorname{supp}(\mathcal{F})=\operatorname{supp}(\mathcal{G})$, tenemos $f_{mn}(q)g_{mn}(q)=f_m(q)g_m(q)f_n(q^m)g_n(q^m)$ y $f_{mn}(q)=f_m(q)f_n(q^m)$, entonces $g_{mn}(q)=g_m(q)g_n(q^m)$.
La multiplicación de sucesiones que satisfacen (1) es asociativa y conmutativa. Para todo semigrupo primo $S(P)$, definimos la sucesión $\mathcal{I}_P=\{I_n(q)\}_{n=1}^{\infty}$ mediante $I_n(q)=1$ para $n\in S(P)$ y $I_n(q)=0$ para $n\notin S(P)$. Entonces es claro que $\mathcal{I}_P\in\Gamma(P)$ y $\mathcal{I}_P\mathcal{F}=\mathcal{F}$ para toda $\mathcal{F}\in\Gamma(P)$.
Si $\mathcal{F},\mathcal{G},\mathcal{H}\in\Gamma(P)$ y $\mathcal{FG}=\mathcal{FH}$, entonces $\mathcal{G}=\mathcal{H}$. Así, $\Gamma(P)$ es un semigrupo con cancelación. □

Con la misma idea con la que construimos la sucesión producto, podemos definir las **sucesiones de funciones racionales** y dar una interpretación de dichas sucesiones en términos de la ecuación funcional (1) que es la parte central de este capítulo.

Definición I.23: Sea $S(P)$ un semigrupo primo, y sean $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ y $\mathcal{G}=\{g_n(q)\}_{n=1}^{\infty}$ dos sucesiones de polinomios con soporte $S(P)$. Definimos la **sucesión de funciones racionales** $\mathcal{F}/\mathcal{G}$ mediante $\frac{\mathcal{F}}{\mathcal{G}}=\left\{\frac{f_n}{g_n}(q)\right\}_{n=1}^{\infty}$; donde $\frac{f_n}{g_n}(q)=\frac{f_n(q)}{g_n(q)}$ si $n\in S(P)$ y $\frac{f_n}{g_n}(q)=0$ si $n\notin S(P)$.

Lema I.24: Si $\mathcal{F}$ y $\mathcal{G}$ son sucesiones de funciones compatibles con el producto cuántico, entonces la sucesión $\mathcal{F}/\mathcal{G}$ de funciones racionales también es compatible.

Demostración:

Si $n\in\operatorname{supp}(\mathcal{F}/\mathcal{G})$, entonces $\frac{f_n(q)}{g_n(q)}\neq 0$ lo cual implica que $f_n(q)\neq 0$, es decir, $n\in\operatorname{supp}(\mathcal{F})$, pero $\operatorname{supp}(\mathcal{F})=S(P)$. Por lo tanto $\operatorname{supp}(\mathcal{F}/\mathcal{G})\subseteq S(P)$. Inversamente, si $n\in\operatorname{supp}(\mathcal{F})=S(P)$, entonces $f_n(q)\neq 0$ y $g_n(q)\neq 0$ (pues el soporte de $\mathcal{G}$ también es $S(P)$) entonces $\frac{f_n(q)}{g_n(q)}\neq 0$, es decir, $n\in\operatorname{supp}(\mathcal{F}/\mathcal{G})$. Por lo tanto $S(P)\subseteq\operatorname{supp}(\mathcal{F}/\mathcal{G})$.

Combinando ambas contenciones tenemos que el soporte de $\mathcal{F}/\mathcal{G}$ es igual a $S(P)$.

Ahora probemos que la sucesión $\mathcal{F}/\mathcal{G}$ satisface la ecuación (1) siempre que $\mathcal{F}$ y $\mathcal{G}$ la satisfagan:

$$\frac{f_{mn}}{g_{mn}}(q)=\frac{f_{mn}(q)}{g_{mn}(q)}=\frac{f_m(q)f_n(q^m)}{g_m(q)g_n(q^m)}\quad\text{(pues }\{f_n(q)\}_{n=1}^{\infty}\text{ y }\{g_n(q)\}_{n=1}^{\infty}\text{ cumplen (1))}$$

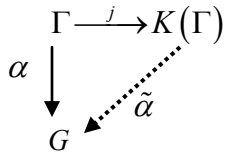
$$=\frac{f_m(q)}{g_m(q)}\cdot\frac{f_n(q^m)}{g_n(q^m)}$$

$$=\frac{f_m}{g_m}(q)\cdot\frac{f_n}{g_n}(q^m).$$

Por lo tanto $\frac{f_{mn}}{g_{mn}}(q)=\frac{f_m}{g_m}(q)\cdot\frac{f_n}{g_n}(q^m)$ es decir, $\mathcal{F}/\mathcal{G}$ satisface la ecuación (1). □

Para continuar, recordemos el concepto de "grupo de Grothendieck."

Definición I.25: Si Γ es un semigrupo abeliano con cancelación, entonces existe un grupo abeliano $K(\Gamma)$ y un homomorfismo inyectivo entre semigrupos $j:\Gamma\to K(\Gamma)$ tal que si *G* es cualquier grupo abeliano y α un homomorfismo de semigrupos de Γ en *G*, entonces existe un único homomorfismo de grupos $\tilde{\alpha}$ de $K(\Gamma)$ en *G* tal que $\tilde{\alpha}j=\alpha$. El grupo $K(\Gamma)$ es llamado **el grupo de Grothendieck del semigrupo Γ**. Diagramáticamente tenemos:



Teorema I.26: Sea $S(P)$ un semigrupo primo, y $\Gamma(P)$ un semigrupo con cancelación cuyos elementos son polinomios que son solución de la ecuación funcional (1) y tienen soporte $S(P)$. El grupo de Grothendieck de $\Gamma(P)$ es el grupo de todas las sucesiones de funciones racionales $\mathcal{F}/\mathcal{G}$, donde $\mathcal{F}$ y $\mathcal{G}$ pertenecen a $\Gamma(P)$.

Demostración:

Sea $K(\Gamma(P))$ el conjunto de todas las sucesiones de funciones racionales de la forma $\mathcal{F}/\mathcal{G}$, donde $\mathcal{F}$ y $\mathcal{G}$ están en $\Gamma(P)$. Claramente es un grupo abeliano ya que tanto $\mathcal{F}$ como $\mathcal{G}$ son sucesiones de polinomios. Demostraremos que $K(\Gamma(P))$ satisface la definición I.25, es decir, es el grupo de Grothendieck de Γ(P).

Sea $j:\Gamma(P)\to K(\Gamma(P))$ una inmersión de $\Gamma(P)$ en $K(\Gamma(P))$ con regla de correspondencia: $\mathcal{F}\mapsto \mathcal{F}/\mathcal{J}_P$, donde $\mathcal{J}_P=\{I_n(q)\}_{n=1}^{\infty}$ se define mediante $I_n(q)=\begin{cases}1 & \text{si } n\in S(p)\\ 0 & \text{si } n\notin S(p)\end{cases}$ y sea $\alpha:\Gamma(P)\to G$ un homomorfismo de grupos.

Entonces definimos la función $\tilde{\alpha}:K(\Gamma(P))\to G$ de la siguiente manera:

$$\tilde{\alpha}\left(\frac{\mathcal{F}}{\mathcal{G}}\right)=\frac{\alpha(\mathcal{F})}{\alpha(\mathcal{G})}.$$

Si $\mathcal{F}/\mathcal{G}=\mathcal{F}_1/\mathcal{G}_1$, entonces $\mathcal{F}\mathcal{G}_1=\mathcal{F}_1\mathcal{G}$. Como α es un homomorfismo de semigrupos, tenemos que $\alpha(\mathcal{F})\alpha(\mathcal{G}_1)=\alpha(\mathcal{F}_1)\alpha(\mathcal{G})$ y entonces $\frac{\alpha(\mathcal{F})}{\alpha(\mathcal{G})}=\frac{\alpha(\mathcal{F}_1)}{\alpha(\mathcal{G}_1)}$. Por lo tanto $\tilde{\alpha}\left(\frac{\mathcal{F}}{\mathcal{G}}\right)=\tilde{\alpha}\left(\frac{\mathcal{F}_1}{\mathcal{G}_1}\right)$ y así, tenemos que $\tilde{\alpha}:K(\Gamma(P))\to G$ es un homomorfismo de grupos bien-definido, y además $\tilde{\alpha}j=\alpha$ ya que:

$\tilde{\alpha}j(\mathcal{F})=\tilde{\alpha}(j(\mathcal{F}))=\tilde{\alpha}\left(\frac{\mathcal{F}}{\mathcal{J}_P}\right)=\frac{\alpha(\mathcal{F})}{\alpha(\mathcal{J}_P)}=\alpha(\mathcal{F})$ (esto se cumple ya que α es un homomorfismo).

Por lo tanto, el grupo $K(\Gamma(P))$ es el grupo de Grothendieck de $\Gamma(P)$. □

Al momento no sabemos si toda sucesión de funciones racionales que satisfaga la ecuación funcional (1) y que tenga soporte $S(P)$ pertenece al grupo $K(\Gamma(P))$.

Recordemos que si $\mathcal{F}$ es una sucesión de polinomios no constantes que satisfacen (1), entonces existe un número racional positivo *t* tal que $\mathrm{gr}(f_n) = t(n-1)$ es un entero positivo para toda $n \in \mathrm{supp}(\mathcal{F})$. En particular, si $\mathrm{supp}(\mathcal{F}) = \mathbb{N}$, o si $2 \in \mathrm{supp}(\mathcal{F})$, o, más general, si $\{n-1 / n \in \mathrm{supp}(\mathcal{F})\}$ es un conjunto de enteros primos relativos, entonces *t* es un entero positivo.

Hemos llegado al último resultado de este artículo y por ende, al resultado que resume toda la información vertida desde el inicio y la conclusión que estábamos esperando, es decir, bajo qué condiciones los enteros cuánticos son la única solución de la ecuación funcional (1).

Teorema I.27: Sea $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios que satisface la ecuación funcional $f_{mn}(q) = f_m(q) f_n(q^m)$ para todos los enteros positivos *m* y *n*. Si $\mathrm{gr}(f_n) = n-1$ y $f_n(0) = 1$ para toda $n \in \mathrm{supp}(\mathcal{F})$, y si $\mathrm{supp}(\mathcal{F})$ contiene al 2 y algún entero impar mayor que 1, entonces $f_n(q) = [n]_q$ para toda $n \in \mathrm{supp}(\mathcal{F})$.

Demostración:

La prueba se hará en tres partes:

i) Veremos que el teorema se cumple para toda potencia de 2 (por inducción).
ii) Veremos que el teorema se cumple para todos los enteros impares (por inducción).
iii) Combinando (*i*) y (*ii*), el teorema se cumple para todos los números enteros.

i) Por demostrar que $f_{2^k}(q) = [2^k]_q \ \forall k \in \mathbb{N}$

- Base de la inducción: Como $2 \in \mathrm{supp}(\mathcal{F})$, tenemos que $\mathrm{gr}(f_2) = 2-1 = 1$ y $f_2(0) = 1$, por lo tanto $f_2(q) = 1 + aq$ para alguna $a \neq 0$. Lo que hace falta probar para que $f_2(q) = [2]_q$ es que $a = 1$.

  Por hipótesis, existe un entero impar mayor que 1 en el soporte de $\mathcal{F}$, así podemos suponer que este entero es $n = 2r+1 \geq 3$ para algún entero positivo *r*. Entonces $f_n(q) = 1 + \sum_{j=1}^{n-1} b_j q^j$ con $b_{n-1} \neq 0$.

  Así, resulta que:

$$f_n(q)f_2(q^n)=\left(1+\sum_{j=1}^{n-1}b_jq^j\right)\left(1+aq^n\right)$$
$$=1+\sum_{j=1}^{n-1}b_jq^j+aq^n+aq^n\sum_{j=1}^{n-1}b_jq^j$$
$$=1+\sum_{j=1}^{n-1}b_jq^j+aq^n+\sum_{j=1}^{n-1}ab_jq^{n+j}$$
$$=1+b_1q+b_2q^2+\ldots+b_{n-1}q^{n-1}+aq^n+ab_1q^{n+1}+ab_2q^{n+2}+\ldots+ab_{n-1}q^{2n-1}.$$

Y además:

$$f_2(q)f_n(q^2)=\left(1+aq\right)\left(1+\sum_{j=1}^{n-1}b_jq^{2j}\right)$$
$$=1+aq+\sum_{j=1}^{n-1}b_jq^{2j}+aq\sum_{j=1}^{n-1}b_jq^{2j}$$
$$=1+aq+\sum_{j=1}^{n-1}b_jq^{2j}+\sum_{j=1}^{n-1}ab_jq^{2j+1}$$
$$=1+aq+\sum_{j=1}^{2r}b_jq^{2j}+\sum_{j=1}^{2r}ab_jq^{2j+1}\quad\left(\text{Pues } n=2r+1\Rightarrow n-1=2r\right)$$
$$=1+aq+b_1q^2+\cdots+b_{r+1}q^{2(r+1)}+\cdots+b_{2r}q^{4r}+ab_1q^3+\cdots+ab_{r+1}q^{2(r+1)+1}+\cdots+ab_{2r}q^{4r+1}$$
$$=1+aq+b_1q^2+\cdots+b_{r+1}q^{n+1}+ab_{r+1}q^{n+2}+\cdots$$

Esto es ya que $n=2r+1\Rightarrow r=\dfrac{n-1}{2}$. Por lo tanto $2\left(r+1\right)=n+1$ y $2\left(r+1\right)+1=n+2$.

Observemos que en la última igualdad lo que estamos haciendo es reacomodar los términos ya que sólo vamos a fijarnos en los términos de grado $1,\ 2,\ n+1$ y $n+2$.

Como $2,n\in\operatorname{supp}\left(\mathcal{F}\right)$, entonces por hipótesis resulta que:

$$f_n(q)f_2(q^n)=f_2(q)f_n(q^2)\ \ldots(8)$$

Así, los polinomios son iguales término a término. Si nos fijamos en los términos de grado $1,\ 2,\ n+1$ y $n+2$, resulta que:

Grado 1: $a=b_1$; Grado 2: $b_1=b_2$. Por lo tanto $\boxed{a=b_1=b_2}$

Grado $n+1$: $ab_1=b_{r+1}$. Por lo tanto $\boxed{b_{r+1}=ab_1=a\cdot a=a^2}$

Grado $n+2$: $ab_2=a^2=ab_{r+1}$

Si igualamos el resultado de grado $n+1$ y de grado $n+2$ resulta que:

$ab_{r+1} = b_{r+1}$ pero $a \neq 0$. Por lo tanto $a = 1$. Así, resulta que $f_2(q) = 1 + q = [2]_q$

De esta manera acabamos de probar la base inductiva.

- Hipótesis de inducción: Supongamos que el resultado es válido para $k-1$, *i.e.*, $f_{2^{k-1}}(q) = \left[2^{k-1}\right]_q$ para algún entero $k \geq 2$.

- Paso inductivo: Queremos demostrar que $f_{2^k}(q) = \left[2^k\right]_q$.

$$\begin{aligned} f_{2^k}(q) &= f_{2^{k-1}\cdot 2} = f_{2^{k-1}}(q) f_2\left(q^{2^{k-1}}\right) \\ &= \left(1 + q + q^2 + \ldots + q^{2^{k-1}-1}\right)\left(1 + q^{2^{k-1}}\right) \text{ (aplicando la base y la hipótesis de inducción)} \\ &= 1 + q + q^2 + \ldots + q^{2^{k-1}-1} + q^{2^{k-1}} + q^{2^{k-1}+1} + \ldots + q^{2^{k-1}+2^{k-1}-1} \\ &= 1 + q + q^2 + \ldots + q^{2^k-1} = \left[2^k\right]_q. \end{aligned}$$

Por lo tanto $f_{2^k}(q) = \left[2^k\right]_q \ \forall k \in \mathbb{N}$.

ii) Por demostrar que $f_n(q) = [n]_q$ para todo entero impar *n*.

Antes de comenzar con la demostración de esta parte, observemos lo siguiente:

Como $n \in \operatorname{supp}(\mathcal{F})$ es impar, podemos suponer que $n = 2r+1$ con $n \geq 3$. Ahora bien, la ecuación (8) implica que:

$$1 + \sum_{j=1}^{n-1} b_j q^j + aq^n + \sum_{j=1}^{n-1} ab_j q^{n+j} = 1 + aq + \sum_{j=1}^{2r} b_j q^{2j} + \sum_{j=1}^{2r} ab_j q^{2j+1}.$$

Si nos fijamos solamente en esta igualdad hasta el término de grado *n* resulta que:

$$1 + \sum_{j=1}^{n-1} b_j q^j + aq^n = 1 + aq + \sum_{j=1}^{2r} b_j q^{2j} + \sum_{j=1}^{2r} ab_j q^{2j+1}.$$

Reacomodando y recordando que $a = 1$ tenemos que:

$$1 + b_1 q + \sum_{j=2}^{n-1} b_j q^j + q^n = 1 + q + \sum_{j=1}^{2r} b_j q^{2j} + \sum_{j=1}^{2r} ab_j q^{2j+1}.$$

Por lo tanto tenemos que:

$$\boxed{1 + b_1 q + \sum_{j=2}^{n-1} b_j q^j + q^n = 1 + q + \sum_{j=1}^{2r} b_j \left(q^{2j} + q^{2j+1}\right)}.$$

Comparando término a término con los grados: 1, $n-1$ y n resulta que:
Grado 1: $b_1 = 1$; Grado $n-1$: $b_{n-1} = b_r$; Grado n: $1 = b_r$.

Entonces $1 = b_1 = b_r = b_{n-1}$.

Ahora bien, si expandimos las series resulta que:

$$1 + b_1 q + b_2 q^2 + \ldots + b_{n-1} q^{n-1} + q^n = 1 + q + b_1 \left(q^2 + q^3 \right) + b_2 \left(q^4 + q^5 \right) + \ldots + b_r \left(q^{n-1} + q^n \right).$$

Por lo tanto $b_i = b_{2i} = b_{2i+1} \ \forall i = 1, \ldots, r-1$.

Después de todas estas observaciones ya podemos probar (*ii*):

- Si $n = 3$ entonces $r = 1$. Así, $b_1 = b_2 = 1$ y como $f_3(q) = 1 + b_1 q + b_2 q^2$ entonces resulta que $f_3(q) = [3]_q$.
- Si $n = 5$, entonces $r = 2$ y $b_1 = b_2 = b_3 = b_4 = 1$, por lo tanto $f_5(q) = [5]_q$.
- Para $n \geq 7$ tenemos que $r \geq 3$. Supongamos que $1 \leq k \leq r-2$ y $b_i = 1$ para $i = 1, \ldots, 2k-1$. Es claro que $k \leq 2k-1$ entonces $1 = b_k = b_{2k} = b_{2k+1}$.

Si aplicamos inducción sobre *k* se sigue que:

$b_i = 1$ para $i = 1, \ldots, n-1$, y $f_n(q) = [n]_q$ para todo entero impar $n \in \operatorname{supp}(\mathcal{F})$.

iii) Sea $m \in \operatorname{supp}(\mathcal{F})$ cualquier entero, entonces $m = 2^k n$, donde *n* es impar y $k \geq 0$, entonces:

$$f_m(q) = f_{2^k n}(q) = f_{2^k}(q) f_n\left(q^{2^k}\right) = \left[2^k\right]_q [n]_{q^{2k}} = \left[2^k n\right]_q \qquad \square$$

Corolario: Sea $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios que satisface la ecuación funcional $f_{mn}(q) = f_m(q) f_n\left(q^m\right)$ para todos los enteros positivos *m* y *n*. Si $\operatorname{gr}(f_n) = n-1$ y $f_n(0) = 1$ para todo entero *n*, entonces $f_n(q) = [n]_q$ para toda *n*.

Terminamos este capítulo formulando el siguiente problema que se plantea Nathanson en [1].

Sea $t \geq 2$, y $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios que satisface la ecuación funcional (1) tal que $f_n(q)$ tiene grado $t(n-1)$ y $f_n(0) = 1 \ \forall n \in \mathbb{N}$. ¿$\mathcal{F}$ está construida mediante enteros cuánticos? Más preciso, ¿existen enteros positivos $t_1, \ldots, t_k$ y enteros $u_1, \ldots, u_k$ tales que $t = t_1 u_1 + \ldots + t_k u_k$ y, para cada $n \in \mathbb{N}$, $f_n(q) = \prod_{i=1}^{k} \left([n]_{q^{t_i}} \right)^{u_i}$?

CAPITULO II

ESTRUCTURA ADITIVA CUADRÁTICA DE LOS ENTEROS CUÁNTICOS.

Una **regla aditiva cuadrática para enteros cuánticos** consiste de una terna de sucesiones de polinomios $\mathscr{R}' = \{r'_n(q)\}_{n=1}^{\infty}$, $\mathscr{S}' = \{s'_n(q)\}_{n=1}^{\infty}$, $\mathscr{T}' = \{t'_{m,n}(q)\}_{m,n=1}^{\infty}$ tales que para todo par de enteros *m, n* se satisface que $[m+n]_q = r'_n(q)[m]_q + s'_m(q)[n]_q + t'_{m,n}(q)[m]_q[n]_q$. En este capítulo se da una clasificación completa de las reglas aditivas cuadráticas, y también se consideran sucesiones de polinomios $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ que satisfacen la ecuación funcional

$$f_{m+n}(q) = r'_n(q) f_m(q) + s'_m(q) f_n(q) + t'_{m,n} f_m(q) f_n(q).$$

1. REGLAS ADITIVAS CUÁNTICAS

Sea $K[q]$ el anillo de polinomios con coeficientes en un campo *K*. Para todo entero positivo *n*, tenemos el polinomio $[n]_q = 1 + q + q^2 + ... + q^{n-1} \in K[q]$. Si $n = 0$ definimos $[0]_q = 0$. Equivalentemente, $[n]_q = \dfrac{1-q^n}{1-q}$.

Es claro que la suma ordinaria de polinomios no es una "buena" suma para los enteros cuánticos ya que $[m]_q + [n]_q \neq [m+n]_q$. Nuestro objetivo es encontrar una operación binaria $\oplus$ tal que para todo para de enteros positivos *m, n* se cumpla que $[m]_q \oplus [n]_q = [m+n]_q$. Con ello en mente, para cada par de enteros positivos *m, n* consideremos una función

$$\Phi_{m,n} : K[q] \times K[q] \to K[q].$$

Dada la sucesión de funciones $\{\Phi_{m,n}\}_{m,n=1}^{\infty}$ podemos definir una operación binaria $\oplus$ en los elementos de una sucesión arbitraria de polinomios en $K[q]$, $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ de la siguiente forma:

$$f_m(q) \oplus f_n(q) = \Phi_{m,n}(f_m(q), f_n(q)).$$

La operación binaria definida por $\{\Phi_{m,n}\}_{m,n=1}^{\infty}$ es llamada una **regla aditiva polinomial**. Una regla aditiva polinomial **está bien definida** en la sucesión $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ si para todos los enteros positivos *m, n, r* y *s* tales que $m+n = r+s$ se cumple que:

$$f_m(q) \oplus f_n(q) = f_r(q) \oplus f_s(q).$$

Observación: Si $\oplus$ está bien definida en la sucesión $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$, entonces claramente la operación binaria $\oplus$ es conmutativa.

Definición II.1: Un **regla aditiva cuántica** es una regla aditiva polinomial que está bien definida en la sucesión de enteros cuánticos y tal que para todo par de enteros positivos *m* y *n* satisface la ecuación $[m]_q \oplus [n]_q = [m+n]_q$.

Ejemplo: Para todo par de polinomios $a(q), b(q) \in K[q]$. Sea:

$$\Phi_{m,n}(a(q), b(q)) = a(q) + q^m b(q).$$

Esta sucesión de funciones define una regla aditiva cuántica ya que:

$$\begin{aligned}\Phi_{m,n}([m]_q, [n]_q) &= [m]_q + q^m [n]_q = (1+q+\ldots+q^{m-1}) + q^m (1+q+\ldots+q^{n-1}) \\ &= (1+q+\ldots+q^{m-1}) + (q^m + q^{m+1} + \ldots + q^{m+n-1}) \\ &= 1+q+\ldots+q^{m-1}+q^m+q^{m+1}+\ldots+q^{(m+n)-1} = [m+n]_q.\end{aligned}$$

Proposición II.2**:** La sucesión de polinomios $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ satisface la ecuación funcional $f_{m+n}(q) = f_m(q) + q^m f_n(q)$ si y sólo si existe un polinomio $h(q)$ tal que $f_n(q) = [n]_q h(q)$ para toda *n*.

Demostración:

$\Rightarrow$] Por inducción sobre *n*:

Supongamos que $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ es solución de la ecuación funcional aditiva $f_{m+n}(q) = f_m(q) + q^m f_n(q)$.

- Base Inductiva: Si $n=1$, definimos $h(q) = f_1(q)$ y entonces $[n]_q h(q) = [1]_q f_1(q) = f_1(q)$. Por lo tanto $f_1(q) = h(q)[1]_q$.

.

- Hipótesis Inductiva: Para $n \geq 2$, supongamos que $f_{n-1}(q) = h(q)[n-1]_q$.

- Paso Inductivo: Por hipótesis $f_n(q) = f_1(q) + q^1 f_{n-1}(q)$, aplicando la hipótesis de inducción, tenemos que:

$$
\begin{aligned}
f_n(q) &= f_1(q) + q^1 f_{n-1}(q) \\
&\overset{H.I}{=} h(q)[1]_q + qh(q)[n-1]_q \\
&= h(q)\left([1]_q + q[n-1]_q\right) \\
&= h(q)\left(1 + q\left(1 + q + q^2 + \ldots + q^{n-2}\right)\right) \\
&= h(q)\left(1 + q + q^2 + \ldots + q^{n-1}\right) \\
&= h(q)[n]_q .
\end{aligned}
$$

Por lo tanto, $f_n(q) = h(q)[n]_q \quad \forall n \in \mathbb{N}$.

$\Leftarrow]$ Si existe un polinomio $h(q)$ tal que $f_n(q) = [n]_q h(q)$ para toda *n*, tenemos que $f_{m+n}(q) = [m+n]_q h(q)$, como $[m+n]_q = [m]_q + q^m [n]_q$, sustituyendo tenemos que:

$$
f_{m+n}(q) = [m+n]_q h(q) = [m]_q h(q) + q^m [n]_q h(q) = f_m(q) + q^m f_n(q). \qquad \square
$$

2. IDENTIDADES CERO CUADRÁTICAS

Definición II.3: Una **identidad cero cuadrática** consiste de tres sucesiones de polinomios $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$, $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ y $\mathcal{W}' = \{w'_{m,n}(q)\}_{m,n=1}^{\infty}$ tales que:

$$u'_n(q)[m]_q + v'_m(q)[n]_q + w'_{m,n}(q)[m]_q[n]_q = 0 \ \ \forall m,n \in \mathbb{Z}^+.$$

Una **identidad cero lineal** consiste de dos sucesiones de polinomios $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ tales que:

$$u'_n(q)[m]_q + v'_m(q)[n]_q = 0 \ \ \forall m,n \in \mathbb{Z}^+.$$

El siguiente teorema nos da una caracterización para las identidades cero cuadráticas y como corolario tendremos una caracterización para las identidades cero lineales que se trabajarán a fondo en el capítulo III.

Teorema II.4: Las sucesiones de polinomios $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$, $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ y $\mathcal{W}' = \{w'_{m,n}(q)\}_{m,n=1}^{\infty}$ satisfacen la identidad cero cuadrática:

$$u'_n(q)[m]_q + v'_m(q)[n]_q + w'_{m,n}(q)[m]_q[n]_q = 0 \ \ \forall m,n \in \mathbb{Z}^+$$

si y sólo si existen sucesiones $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ tales que para todo par de enteros positivos *m, n* se satisfacen las siguientes tres igualdades:

$$u'_n(q) = u_n(q)[n]_q$$
$$v'_m(q) = v_m(q)[m]_q$$
$$w'_{m,n}(q) = -\left(u_n(q) + v_m(q)\right).$$

Demostración:

$\Rightarrow$] Supongamos que $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$, $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ y $\mathcal{W}' = \{w'_{m,n}(q)\}_{m,n=1}^{\infty}$ nos dan una identidad cero cuadrática.

Definamos $\boxed{u_n(q) = -\left(v'_1(q) + w'_{1,n}(q)\right)}$ y $\boxed{v_m(q) = -\left(u'_1(q) + w'_{m,1}(q)\right).}$

Para $m = 1$, en la identidad cero cuadrática tenemos que:

$$u'_n(q)[1]_q + v'_1(q)[n]_q + w'_{1,n}(q)[n]_q[1]_q = 0.$$

Por lo tanto, $u_n'(q)+v_1'(q)[n]_q+w_{1,n}'(q)[n]_q=0$, despejando $u_n'(q)$ tenemos la primera igualdad $u_n'(q)=-\left(v_1'(q)+w_{1,n}'(q)\right)[n]_q=u_n(q)[n]_q$.

Si ahora sustituimos $n=1$ en la identidad cero cuadrática, tenemos que:

$$u_1'(q)[m]_q+v_m'(q)[1]_q+w_{m,1}'(q)[m]_q[1]_q=0.$$

Lo cual implica que $v_m'(q)=-\left(u_1'(q)+w_{m,1}'(q)\right)[m]_q=v_m(q)[m]_q$.

Para obtener la última igualdad, sustituyendo los polinomios $u_n'(q)$ y $v_m'(q)$ en la identidad cero cuadrática, tenemos que:

$$u_n(q)[n]_q[m]_q+v_m(q)[m]_q[n]_q+w_{m,n}'(q)[m]_q[n]_q=0.$$

Equivalentemente $u_n(q)+v_m(q)+w_{m,n}'(q)=0$, por lo que $w_{m,n}'(q)=-\left(u_n(q)+v_m(q)\right)$.

$\Leftarrow]$ Si suponemos que tenemos las sucesiones de polinomios $\mathcal{U}=\{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}=\{v_m(q)\}_{m=1}^{\infty}$ tales que:

$$u_n'(q)=u_n(q)[n]_q$$
$$v_m'(q)=v_m(q)[m]_q \text{ y}$$
$$w_{m,n}'(q)=-\left(u_n(q)+v_m(q)\right)$$

entonces, $u_n(q)[n]_q[m]_q+v_m(q)[m]_q[n]_q+w_{m,n}'(q)[n]_q[m]_q=0.$

Con lo cual tenemos la identidad cuadrática cero:

$$u_n'(q)[m]_q+v_m'(q)[n]_q+w_{m,n}'(q)[m]_q[n]_q=0 \ \ \forall m,n\in\mathbb{Z}^+. \qquad \square$$

Corolario: Las sucesiones de polinomios $\mathcal{U}'=\{u_n'(q)\}_{n=1}^{\infty}$ y $\mathcal{V}'=\{v_m'(q)\}_{m=1}^{\infty}$ satisfacen la identidad cero lineal $u_n'(q)[m]_q+v_m'(q)[n]_q=0$ para todo entero positivo *m* y *n* si y sólo si existe un polinomio $z(q)$ tal que para todo entero positivo *m* y *n*:

$$u_n'(q)=z(q)[n]_q \quad \text{y}$$
$$v_m'(q)=-z(q)[m]_q.$$

Demostración:

$\Rightarrow$] Es claro que la identidad cero lineal $u'_n(q)[m]_q + v'_m(q)[n]_q = 0$ es una identidad cero cuadrática con $w'_{m,n}(q) = 0$ para toda *m* y *n*. Así, gracias al Teorema II.4 se sigue que existen polinomios $u_n(q)$ y $v_m(q)$ tales que $w'_{m,n}(q) = -\left(u_n(q) + v_m(q)\right) = 0$. Entonces existe un polinomio $z(q)$ tal que $u_n(q) = -v_m(q) = z(q)$, $u'_n(q) = z(q)[n]_q$ y $v'_m(q) = -z(q)[m]_q$ para todo entero positivo *m* y *n* que es lo que queríamos probar.

$\Leftarrow$] Si suponemos que existe un polinomio $z(q)$ tal que las sucesiones $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ satisfacen $u'_n(q) = z(q)[n]_q$ y $v'_m(q) = -z(q)[m]_q$, entonces:

$$u'_n(q)[m]_q + v'_m(q)[n]_q = z(q)[n]_q[m]_q - z(q)[m]_q[n]_q = 0,$$

que es la identidad cero lineal $u'_n(q)[m]_q + v'_m(q)[n]_q = 0 \ \forall m,n \in \mathbb{Z}^+$ y es lo que queríamos probar. □

Teorema II.5: Sean $\mathcal{U}' = \{u'_n(q)\}_{n=1}^{\infty}$, $\mathcal{V}' = \{v'_m(q)\}_{m=1}^{\infty}$ y $\mathcal{W}' = \{w'_{m,n}(q)\}_{m,n=1}^{\infty}$ sucesiones de polinomios que satisfacen la identidad cuadrática cero:

$$u'_n(q)[m]_q + v'_m(q)[n]_q + w'_{m,n}(q)[m]_q[n]_q = 0 \ \forall m,n \in \mathbb{Z}.$$

Si $\mathrm{gr}\left(u'_n(q)\right) < n-1$, entonces $u'_n(q) = 0$. Similarmente, si $\mathrm{gr}\left(v'_m(q)\right) < m-1$, entonces $v'_m(q) = 0$.

Demostración:

Supongamos que $\mathrm{gr}\left(u'_n(q)\right) < n-1$ con $u'_n(q) \neq 0$, por el teorema anterior, existe una sucesión de polinomios $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ tal que $u'_n(q) = u_n(q)[n]_q \neq 0 \ \forall n \in \mathbb{Z}^+$.

Como $\mathrm{gr}\left([n]_q\right) = n-1$ y $\mathrm{gr}(u_n) \geq 0$, $\mathrm{gr}\left(u'_n(q)\right) = \mathrm{gr}\left([n]_q\right) + \mathrm{gr}\left(u_n(q)\right) \geq n-1$, lo cual es una contradicción. Por lo tanto $u'_n(q) = 0$.

De una manera análoga se demuestra que si $\mathrm{gr}\left(v'_m(q)\right) < m-1$ entonces $v'_m(q) = 0$ □

3. REGLAS ADITIVAS CUADRÁTICAS

Definición II.6: Una regla aditiva cuántica es **cuadrática** si existen tres sucesiones de polinomios $\mathcal{R}' = \{r'_n(q)\}_{n=1}^{\infty}$, $\mathcal{S}' = \{s'_n(q)\}_{n=1}^{\infty}$ y $\mathcal{T}' = \{t'_{m,n}(q)\}_{m,n=1}^{\infty}$ tales que:

$$[m+n]_q = r'_n(q)[m]_q + s'_m(q)[n]_q + t'_{m,n}(q)[m]_q[n]_q \quad \forall\, m,n \in \mathbb{N}.$$

A continuación presentaremos algunos ejemplos de reglas aditivas cuadráticas:

1) $[m+n]_q = [m]_q + [n]_q + (q-1)[m]_q[n]_q$.

Demostración:

Utilizando los resultados del lema 0.2 del capítulo cero, tenemos que

$$\begin{aligned}
[m]_q + [n]_q + (q-1)[m]_q[n]_q &= [m]_q + [n]_q + q[m]_q[n]_q - [m]_q[n]_q \\
&= [m]_q + [n]_q + q\left(\sum_{i=n}^{n+m-1}[i]_q - \sum_{j=1}^{m-1}[j]_q\right) - \left(\sum_{i=n}^{n+m-1}[i]_q - \sum_{j=1}^{m-1}[j]_q\right) \\
&= [m]_q + [n]_q + q\sum_{i=n}^{n+m-1}[i]_q - q\sum_{j=1}^{m-1}[j]_q - \sum_{i=n}^{n+m-1}[i]_q + \sum_{j=1}^{m-1}[j]_q \\
&= [m]_q + [n]_q + \sum_{i=n}^{n+m-1}\left([i+1]_q - 1\right) - \sum_{j=1}^{m-1}\left([j+1]_q - 1\right) - \sum_{i=n}^{n+m-1}[i]_q + \sum_{j=1}^{m-1}[j]_q \\
&= [m]_q + [n]_q + \sum_{i=n}^{n+m-1}[i+1]_q - \sum_{i=n}^{n+m-1}1 - \sum_{j=1}^{m-1}[j+1]_q + \sum_{j=1}^{m-1}1 - \sum_{i=n}^{n+m-1}[i]_q + \sum_{j=1}^{m-1}[j]_q \\
&= [m]_q + [n]_q + [m+n]_q - m - [m]_q + m - 1 - [n]_q + [1]_q \\
&= [m+n]_q .
\end{aligned}$$

Por lo tanto, $[m+n]_q = [m]_q + [n]_q + (q-1)[m]_q[n]_q$. □

2) $[m+n]_q = q^n[m]_q + q^m[n]_q - (q-1)[m]_q[n]_q$.

Demostración:

Nuevamente por el lema 0.2 del capítulo cero se tiene que:

$$\begin{aligned} q^n[m]_q + q^m[n]_q - (q-1)[m]_q[n]_q &= q^n[m]_q + q^m[n]_q - \left([m+n]_q - [m]_q - [n]_q\right) \\ &= [m+n]_q - [n]_q + [m+n]_q - [m]_q - [m+n]_q + [m]_q + [n]_q \\ &= [m+n]_q . \end{aligned}$$

Por lo tanto, $[m+n]_q = q^n[m]_q + q^m[n]_q - (q-1)[m]_q[n]_q$. □

Observación: Sean $(\mathcal{R}', \mathcal{S}', \mathcal{T}')$ y $(\mathcal{R}'', \mathcal{S}'', \mathcal{T}'')$ dos ternas de sucesiones que determinan una regla aditiva cuadrática. Entonces:

$$\left(r_n'(q) - r_n''(q)\right)[m]_q + \left(s_m'(q) - s_m''(q)\right)[n]_q + \left(t_{m,n}'(q) - t_{m,n}''(q)\right)[m]_q[n]_q = 0.$$

Es decir, las sucesiones $\mathcal{U}' = \mathcal{R}' - \mathcal{R}''$, $\mathcal{V}' = \mathcal{S}' - \mathcal{S}''$ y $\mathcal{W}' = \mathcal{T}' - \mathcal{T}''$ determinan una identidad cero cuadrática.

Por otro lado, si la terna de sucesiones $(\mathcal{U}', \mathcal{V}', \mathcal{W}')$ es una identidad cero cuadrática, entonces para todo escalar λ la terna de sucesiones $(\mathcal{R}' + \lambda\mathcal{U}', \mathcal{S}' + \lambda\mathcal{V}', \mathcal{T}' + \lambda\mathcal{W}')$ también determinan una regla aditiva cuadrática.

En conclusión, para generar a todas las reglas aditivas cuadráticas es suficiente con que consideremos una regla aditiva cuadrática fija y las identidades cero cuadráticas.

El siguiente resultado es similar al Teorema II.4 de la sección anterior y nos caracterice las reglas aditivas cuadráticas.

Teorema II.7: Las sucesiones de polinomios $\mathcal{R}' = \{r_n'(q)\}_{n=1}^{\infty}$, $\mathcal{S}' = \{s_n'(q)\}_{n=1}^{\infty}$ y $\mathcal{T}' = \{t_{m,n}'(q)\}_{m,n=1}^{\infty}$ determinan una regla aditiva cuadrática si y sólo si existen sucesiones de polinomios $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ tales que:

$$\begin{aligned} r_n'(q) &= u_n(q)[n]_q + 1 - \delta_n \\ s_m'(q) &= v_m(q)[m]_q + 1 - \delta_m \qquad \text{y} \\ t_{m,n}'(q) &= q - 1 - u_n(q) - v_m(q) + \delta_m + \delta_n, \end{aligned}$$

donde $\delta_n = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2. \end{cases}$

Demostración:

$\Rightarrow]$ Sean $\mathscr{R}'$, $\mathscr{S}'$ y $\mathscr{T}'$ sucesiones de polinomios tales que para todo par de enteros positivos *m, n* se cumple que $[m+n]_q = r'_n(q)[m]_q + s'_m(q)[n]_q + t'_{m,n}(q)[m]_q[n]_q$.

Por el algoritmo de la división para polinomios, para toda $n \geq 1$ existen polinomios $u_n(q)$ y $r_n(q)$ tales que $r'_n(q) = u_n(q)[n]_q + r_n(q)$ con $\operatorname{gr}(r_n(q)) \leq \operatorname{gr}([n]_q) - 1 = n - 2.$

De manera similar, para cada $m \geq 1$ existen polinomios $v_m(q)$ y $s_m(q)$ tales que $s'_m(q) = v_m(q)[m]_q + s_m(q)$ y $\operatorname{gr}(s_m(q)) \leq \operatorname{gr}([m]_q) - 1 = m - 2.$

Si definimos los polinomios:

$$u'_n(q) = u_n(q)[n]_q$$
$$v'_m(q) = v_m(q)[m]_q$$
$$w'_{m,n}(q) = -(u_n(q) + v_m(q)),$$

claramente se tiene que $u'_n(q)[m]_q + v'_m(q)[n]_q + w'_{m,n}(q)[m]_q[n]_q = 0,$ es decir, determinan una identidad cero cuadrática.

Sea $t_{m,n}(q) = t'_{m,n}(q) - w'_{m,n}(q) = t'_{m,n}(q) + u_n(q) + v_m(q)$. Si a la regla aditiva cuadrática dada le restamos la identidad cero cuadrática definida, tenemos la nueva regla aditiva cuadrática:

$$\begin{aligned}[m+n]_q &= (r'_n(q) - u'_n(q))[m]_q + (s'_m(q) - v'_m(q))[n]_q + (t'_{m,n}(q) - w'_{m,n}(q))[m]_q[n]_q \\ &= r_n(q)[m]_q + s_m(q)[n]_q + t_{m,n}(q)[m]_q[n]_q.\end{aligned}$$

Recordemos que el $\operatorname{gr}([m+n]_q) = m + n - 1$. Por otro lado, con la información dada podemos deducir que:

$$gr(r_n(q)[m]_q) \leq m + n - 3$$
$$gr(s_m(q)[n]_q) \leq m + n - 3$$
$$gr(t_{m,n}(q)[m]_q[n]_q) \geq m + n - 2,$$

lo cual implica que $\operatorname{gr}(t_{m,n}(q)) = 1$. Más aún, $t_{m,n}(q)$ es un polinomio mónico, ya que los enteros cuánticos $[m]_q$, $[n]_q$ y $[m+n]_q$ son polinomios mónicos.

Para continuar con la demostración del teorema consideraremos cuatro casos.

Caso 1: Si $m=n=1$, entonces $[m]_q=1=[n]_q$ y $[m+n]_q=[2]_q=1+q$.
Sustituyendo en la regla aditiva cuadrática tenemos que:

$$[2]_q=r_1(q)(1)+s_1(q)(1)+t_{1,1}(q)(1)(1)=r_1(q)+s_1(q)+t_{1,1}(q).$$

Como $\text{gr}(r_n(q))\le n-2$ y $\text{gr}(s_m(q))\le m-2$, llegamos a que $r_1(q)=s_1(q)=0$. Entonces,
$q+1=[2]_q=0(1)+0(1)+t_{1,1}(q)(1)=t_{1,1}(q).$
Por lo tanto $\boxed{t_{1,1}(q)=q+1}$.

Caso 2: Si $m=1$ y $n\ge 2$, entonces $[n+1]_q=r_n(q)(1)+s_1(q)[n]_q+t_{1,n}(q)(1)[n]_q$, por la regla aditiva cuadrática dada. Nuevamente como $\text{gr}(s_m(q))\le m-2$, entonces $s_1(q)=0$, con lo que obtenemos la igualdad $[n+1]_q=r_n(q)+t_{1,n}(q)[n]_q$.

Ahora bien, como $\text{gr}(t_{m,n}(q))=1$ y $t_{m,n}(q)$ es un polinomio mónico, existe $a\in\mathbb{R}$ tal que $t_{1,n}(q)=q+a$. Entonces, $[n+1]_q=r_n(q)+(q+a)[n]_q$.

Si nos fijamos en los términos de grado $n-1$ tenemos que $q^{n-1}=q^{n-1}+aq^{n-1}$, por lo que $a=0$ y $[n+1]_q=r_n(q)+q[n]_q=r_n(q)+(q+q^2+...+q^n)$ lo cual implica que $\boxed{r_n(q)=1 \text{ si } n\ge 2.}$

Caso 3: Si $m\ge 2$ y $n=1$, $[m+1]_q=r_1(q)[m]_q+s_m(q)(1)+t_{m,1}(q)[m]_q(1)$.
Como $\text{gr}(r_n(q))\le n-2$ entonces $r_1(q)=0$ y $[m+1]_q=s_m(q)+t_{m,1}(q)[m]_q$. Dado que $\text{gr}(t_{m,n}(q))=1$ y $t_{m,n}(q)$ es un polinomio mónico, existe $a\in\mathbb{R}$ tal que $t_{m,1}(q)=q+a$. Entonces, $[m+1]_q=s_m(q)+(q+a)[m]_q$.

Comparando los términos de grado $m-1$ tenemos que $q^{m-1}=q^{m-1}+aq^{m-1}$, lo que implica que $a=0$. Por lo que $[m+1]_q=s_m(q)+q[m]_q=s_m(q)+(q+q^2+...+q^n)$ y por lo tanto: $\boxed{s_m(q)=1 \text{ si } m\ge 2.}$

Caso 4: Si $m\ge 2$ y $n\ge 2$, por los casos 2 y 3, tenemos que $r_n(q)=1$ y $s_m(q)=1$. Además como $\text{gr}(t_{m,n}(q))=1$ y $t_{m,n}(q)$ es un polinomio mónico, existe $a\in\mathbb{R}$ tal que $t_{m,n}(q)=q+a$.

Entonces la regla aditiva cuadrática se ve como $[m+n]_q=[m]_q+[n]_q+(q+a)[m]_q[n]_q$.

Comparando los términos de grado $m+n-2$, llegamos a que:

$$q^{m+n-2} = q\left(q^{m-1}\right)\left(q^{n-2}\right) + q\left(q^{m-2}\right)\left(q^{n-1}\right) + a\left(q^{m-1}\right)\left(q^{n-1}\right).$$

Es decir, $1 = 2 + a$, lo cual implica que $a = -1$ y $t_{m,n} = q + a = q - 1,$ de donde concluimos que $\boxed{t_{m,n}(q) = q - 1 \ \forall\ m,n \geq 2.}$

Los resultados obtenidos hasta ahora son los siguientes:

$$\begin{aligned} &t_{1,1}(q) = q + 1, \\ &t_{1,n}(q) = q \ \ \forall n \geq 2, \\ &t_{m,1}(q) = q \ \forall m \geq 2 \qquad \text{y} \\ &t_{m,n}(q) = q - 1 \ \forall m,n \geq 2. \end{aligned}$$

Para concluir con la primera parte de la demostración, definamos la función $\delta_n = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2 \end{cases}$.

Sabemos que $r_n'(q) = u_n(q)[n]_q + r_n(q)$. Si $n = 1$ entonces $r_1(q) = 0 = 1 - \delta_n$ y $r_n(q) = 1 = 1 - \delta_n$ para $n \geq 2.$ Por lo tanto $\boxed{r_n'(q) = u_n(q)[n]_q + 1 - \delta_n}$.

Análogamente, $s_m'(q) = v_m(q)[m]_q + s_m(q)$. Pero ya vimos que $s_1(q) = 0 = 1 - \delta_m$ y, para $m \geq 2$, $s_m(q) = 1 = 1 - \delta_m$. Por lo tanto $\boxed{s_m'(q) = v_m(q)[m]_q + 1 - \delta_m}$.

Para $t_{m,n}'(q) = t_{m,n}(q) - u_n(q) - v_m(q)$ tenemos que considerar las siguientes cuatro posibilidades:

$$\begin{aligned} &\text{Si } m = n = 1, \text{ entonces } t_{m,n}(q) = q + 1 = q - 1 + \delta_m + \delta_n. \\ &\text{Si } m = 1 \text{ y } n \geq 2, \text{ entonces } t_{m,n}(q) = q = q - 1 + \delta_m + \delta_n. \\ &\text{Si } m \geq 2 \text{ y } n = 1, \text{ entonces } t_{m,n}(q) = q = q - 1 + \delta_m + \delta_n. \\ &\text{Si } m,n \geq 2, \text{ entonces } t_{m,n}(q) = q - 1 = q - 1 + \delta_m + \delta_n. \end{aligned}$$

Por lo tanto $\boxed{t_{m,n}'(q) = q - 1 - u_n(q) - v_m(q) + \delta_m + \delta_n}$.

$\Leftarrow]$ Ahora partimos de que:

$$\begin{aligned} r_n'(q)[m]_q + s_m'(q)[n]_q + t_{m,n}'(q)[m]_q[n]_q = &\left(u_n(q)[n]_q + 1 - \delta_n\right)[m]_q + \left(v_m(q)[m]_q + 1 - \delta_m\right)[n]_q \\ &+ \left(q - 1 - u_n(q) - v_m(q) + \delta_m + \delta_n\right)[m]_q[n]_q. \end{aligned}$$

Equivalentemente,

$$r_n'(q)[m]_q + s_m'(q)[n]_q + t_{m,n}'(q)[m]_q[n]_q = (1 - \delta_n)[m]_q + (1 - \delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q[n]_q.$$

Queremos demostrar que tenemos una regla aditiva cuadrática, es decir que:

$$(1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q [n]_q = [m+n]_q .$$

Consideremos los siguientes casos:

Caso 1: Si $n = m = 1$, entonces $\delta_m = \delta_n = 1$ y:

$$(1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q [n]_q = q + 1 = [2]_q = [m+n]_q .$$

Caso 2: Si $n \geq 2$ y $m \geq 2$, entonces $\delta_m = \delta_n = 0$ y de esta manera tenemos que:
$(1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q [n]_q = [m]_q + [n]_q + (q-1)[m]_q [n]_q = [m+n]_q$
Como ya observamos en el ejemplo 1).

Caso 3: Si $n = 1$ y $m \geq 2$, entonces $\delta_n = 1$ y $\delta_m = 0$ y de esta manera tenemos que:

$$\begin{aligned}(1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q [n]_q &= [n]_q + q[m]_q [n]_q \\ &= 1 + q[m]_q = [m+1]_q = [m+n]_q .\end{aligned}$$

Caso 4: El caso $n \geq 2$ y $m = 1$ es análogo al caso anterior.

Con lo anterior queda demostrado el teorema. □

Definición II.8: La forma aditiva cuadrática definida como:

$$[m+n]_q = (1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (\delta_m + \delta_n + q - 1)[m]_q [n]_q ,$$

se conoce como la **forma aditiva cuadrática fundamental.**

4. ECUACIONES FUNCIONALES ASOCIADAS A LAS REGLAS ADITIVAS CUADRÁTICAS

Sean $\mathscr{R}'$, $\mathscr{S}'$ y $\mathscr{T}'$ sucesiones que definen una regla cuadrática para la adición cuántica, es decir, $\mathscr{R}' = \{r'_n(q)\}_{n=1}^{\infty}$, $\mathscr{S}' = \{s'_m(q)\}_{m=1}^{\infty}$ y $\mathscr{T}' = \{t'_{m,n}(q)\}_{m,n=1}^{\infty}$ son sucesiones de polinomios en $K[q]$ tales que para todo par de enteros positivos *m* y *n*:

$$[m+n]_q = r'_n(q)[m]_q + s'_m(q)[n]_q + t'_{m,n}(q)[m]_q[n]_q .$$

Sea $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios y definimos la operación aditiva $\oplus : \mathscr{F} \times \mathscr{F} \to K[q]$ mediante la siguiente regla:

$$f_m(q) \oplus f_n(q) = r'_n(q) f_m(q) + s'_m(q) f_n(q) + t'_{m,n}(q) f_m(q) f_n(q).$$

Definición II.9: Si una sucesión de polinomios $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ satisface que para todo entero positivo *m* y *n*, se cumple que $f_{m+n}(q) = f_m(q) \oplus f_n(q)$ diremos que la sucesión **está asociada** a una forma aditiva cuadrática.

En esta sección estamos interesados en estudiar las sucesiones $\mathscr{F}$ de polinomios asociadas a formas aditivas cuadráticas.

Además de la solución trivial o cero dada por la sucesión $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ con $f_n(q) = 0 \ \forall n \in \mathbb{N}$, sabemos de la sección anterior que la sucesión definida por los enteros cuánticos, $f_n(q) = [n]_q \ \ \forall n \in \mathbb{N}$ está asociada a una forma aditiva cuadrática.

Observación: Notemos que si una sucesión de polinomios $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ está asociada a una forma aditiva cuadrática, entonces $\mathscr{F} = \{f_n(q)\}_{n=1}^{\infty}$ está totalmente determinada por su valor en el polinomio $f_1(q) = h(q)$.

Demostración:

En la ecuación:

$$f_m(q) \oplus f_n(q) = r'_n(q) f_m(q) + s'_m(q) f_n(q) + t'_{m,n}(q) f_m(q) f_n(q) = f_{m+n}(q),$$

consideremos $m = 1,$ entonces:

$$
\begin{aligned}
f_n(q) &= f_{1+(n-1)}(q) = f_1(q) \oplus f_{n-1}(q) \\
&= h(q) \oplus f_{n-1}(q) \\
&= r'_{n-1}(q)h(q) + s'_1(q)f_{n-1}(q) + t'_{1,n-1}(q)h(q)f_{n-1}(q) \quad \forall n \geq 2 \ .
\end{aligned}
$$ □

Para finalizar este capítulo, calcularemos soluciones de las ecuaciones funcionales asociadas a las siguientes tres reglas aditivas cuadráticas:

1) La forma aditiva cuadrática fundamental.

2) $[m+n]_q = [m]_q + [n]_q + (q-1)[m]_q[n]_q$.

3) $[m+n]_q = q^n[m]_q + q^m[n]_q - (q-1)[m]_q[n]_q$.

Veremos que para cada una de estas tres reglas aditivas cuadráticas existe una solución de la ecuación funcional asociada con $f_1(q) = h(q)\ \forall h(q) \in K[q]$.

1) Soluciones de la forma aditiva cuadrática fundamental.

La regla aditiva cuadrática fundamental es:

$$[m+n]_q = (1-\delta_n)[m]_q + (1-\delta_m)[n]_q + (q-1+\delta_m+\delta_n)[m]_q[n]_q .$$

La ecuación funcional asociada es

$$f_{m+n}(q) = (1-\delta_n)f_m(q) + (1-\delta_m)f_n(q) + (q-1+\delta_m+\delta_n)f_m(q)f_n(q).$$

Si $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es una solución de esta ecuación con $f_1(q) = h(q)$, entonces sustituyendo $m = n = 1$, tenemos que $f_2(q) = (q+1)h(q)^2$.

Ahora bien, para hallar $f_n(q)$, hacemos $m = n-1$ y $n = 1$ en la ecuación funcional asociada y de esta manera obtenemos:

$$
\begin{aligned}
f_n(q) = f_{(n-1)+1}(q) &= (1-\delta_1)f_{n-1}(q) + (1-\delta_{n-1})f_1(q) + (q-1+\delta_{n-1}+\delta_1)f_{n-1}(q)f_1(q) \\
&= f_1(q) + qf_{n-1}(q)f_1(q) \\
&= h(q) + qh(q)f_{n-1}(q).
\end{aligned}
$$

Ahora hallemos $f_{n-1}(q)$. Para esto sustituimos $m = n-2$ y $n = 1$ en la ecuación funcional asociada y de esta manera tenemos que:

$$f_{n-1}(q) = f_{(n-2)+1}(q) = (1-\delta_1) f_{n-2}(q) + (1-\delta_{n-2}) f_1(q) + (q-1+\delta_{n-2}+\delta_1) f_{n-2}(q) f_1(q)$$
$$= f_1(q) + q f_{n-2}(q) f_1(q)$$
$$= h(q) + q h(q) f_{n-2}(q).$$

Ahora bien, si combinamos los dos resultados anteriores tenemos que:

$$f_n(q) = h(q) + q h(q) f_{n-1}(q)$$
$$= h(q) + q h(q)\left[h(q) + q h(q) f_{n-2}(q)\right]$$
$$= h(q) + q h(q)^2 + q^2 h(q)^2 f_{n-2}(q).$$

Generalizando este resultado tenemos que:

$$f_n(q) = h(q) + q h(q) f_{n-1}(q)$$
$$= h(q) + q h(q)^2 + q^2 h(q)^3 + \ldots + q^{n-3} h(q)^{n-2} + \left(q^{n-2} + q^{n-1}\right) h(q)^n$$
$$= \frac{h(q)\left(1-(q h(q))^n\right)}{1-q h(q)} + q^{n-2} h(q)^{n-1}\left(h(q)-1\right) \qquad \forall\ n \geq 3.$$

2) Soluciones de la ecuación funcional asociada a la forma aditiva cuadrática

$$[m+n]_q = [m]_q + [n]_q - (1-q)[m]_q [n]_q.$$

Para la regla aditiva cuadrática $[m+n]_q = [m]_q + [n]_q - (1-q)[m]_q [n]_q$, La ecuación funcional asociada es $f_{m+n}(q) = f_m(q) + f_n(q) - (1-q) f_m(q) f_n(q)$.

Primero veamos qué pasa con $f_2(q)$, para esto, en la ecuación funcional asociada sustituimos $m = n = 1$. De esta manera obtenemos:

$$f_2(q) = f_{1+1}(q) = f_1(q) + f_1(q) - (1-q) f_1(q) f_1(q)$$
$$= 2h(q) - h(q)^2 + q h(q)^2$$
$$= 2h(q) - h(q)^2 (1-q).$$

Si multiplicamos la última igualdad por el factor $(1-q)$ tenemos que:

$$\begin{aligned} f_2(q)(1-q) &= 2h(q)(1-q) - h(q)^2(1-q)^2 \\ &= 2h(q)(1-q) - h(q)^2(1-q)^2 + (1-1) \\ &= 1 - \left(1 - 2h(q)(1-q) + h(q)^2(1-q)^2\right) \\ &= 1 - \left(1 - (1-q)h(q)\right)^2. \end{aligned}$$

Por lo tanto $f_2(q) = \dfrac{1-\left(1-(1-q)h(q)\right)^2}{(1-q)}$.

Ahora veamos lo que sucede con $f_3(q)$, para esto, en la ecuación funcional asociada sustituimos $m=2$ y $n=1$. De esta manera obtenemos:

$$\begin{aligned} f_3(q) = f_{2+1}(q) &= f_2(q) + f_1(q) - (1-q) f_2(q) f_1(q) \\ &= f_2(q) + h(q) - (1-q) h(q) f_2(q) \\ &= f_2(q)\left(1 - (1-q)h(q)\right) + h(q). \end{aligned}$$

Si multiplicamos la última igualdad por el factor $(1-q)$ y sustituimos el valor de $f_2(q)$, tenemos que:

$$\begin{aligned} f_3(q)(1-q) &= f_2(q)\left(1-(1-q)h(q)\right)(1-q) + h(q)(1-q) \\ &= \left(1 - \left(1-(1-q)h(q)\right)^2\right)\left(1-(1-q)h(q)\right) + h(q)(1-q) \\ &= \left(1-(1-q)h(q)\right) - \left(1-(1-q)h(q)\right)^3 + h(q)(1-q) \\ &= 1 - (1-q)h(q) + h(q)(1-q) - \left(1-(1-q)h(q)\right)^3 \\ &= 1 - \left(1-(1-q)h(q)\right)^3. \end{aligned}$$

Por lo tanto $f_3(q) = \dfrac{1-\left(1-(1-q)h(q)\right)^3}{(1-q)}$.

Generalizando este resultado tenemos que las soluciones de la ecuación funcional asociada a la forma aditiva $[m+n]_q = [m]_q + [n]_q - (1-q)[m]_q[n]_q$ son:

$$f_n(q) = \frac{1-\left(1-(1-q)h(q)\right)^n}{1-q}.$$

3) **Soluciones de la ecuación funcional asociada a la forma aditiva cuadrática**

$$[m+n]_q = q^n [m]_q + q^m [n]_q + (1-q)[m]_q [n]_q .$$

Para esta regla aditiva cuadrática, la ecuación funcional asociada es:

$$f_{m+n}(q) = q^n f_m(q) + q^m f_n(q) + (1-q) f_m(q) f_n(q).$$

Primero veamos qué pasa con $f_2(q)$, para esto, en la ecuación funcional asociada sustituimos $m = n = 1$. De esta manera obtenemos:

$$\begin{aligned} f_2(q) = f_{1+1}(q) &= q f_1(q) + q f_1(q) + (1-q) f_1(q) f_1(q) \\ &= 2q h(q) + (1-q) h(q)^2 . \end{aligned}$$

Si multiplicamos la última igualdad por el factor $(1-q)$ tenemos que:

$$\begin{aligned} f_2(q)(1-q) &= 2q h(q)(1-q) + (1-q)^2 h(q)^2 \\ &= 2q h(q)(1-q) + (1-q)^2 h(q)^2 + (q^2 - q^2) \\ &= q^2 + 2q h(q)(1-q) + (1-q)^2 h(q)^2 - q^2 \\ &= (q + (1-q) h(q))^2 - q^2 . \end{aligned}$$

Por lo tanto $f_2(q) = \dfrac{(q + (1-q) h(q))^2 - q^2}{(1-q)}$.

Ahora veamos lo que sucede con $f_3(q)$, para esto, en la ecuación funcional asociada sustituimos $m = 2$ y $n = 1$. De esta manera obtenemos:

$$\begin{aligned} f_3(q) = f_{2+1}(q) &= q f_2(q) + q^2 f_1(q) + (1-q) f_2(q) f_1(q) \\ &= q f_2(q) + q^2 h(q) + (1-q) h(q) f_2(q) \\ &= f_2(q)(q + (1-q) h(q)) + q^2 h(q). \end{aligned}$$

Si multiplicamos la última igualdad por el factor $(1-q)$ y sustituimos el valor de $f_2(q)$, tenemos que:

$$
\begin{aligned}
f_3(q)(1-q) &= f_2(q)\big(q+(1-q)h(q)\big)(1-q)+q^2h(q)(1-q)\\
&= \Big(\big(q+(1-q)h(q)\big)^2-q^2\Big)\big(q+(1-q)h(q)\big)+q^2h(q)(1-q)\\
&= \big(q+(1-q)h(q)\big)^3-q^2\big(q+(1-q)h(q)\big)+q^2h(q)(1-q)\\
&= \big(q+(1-q)h(q)\big)^3-q^3-q^2h(q)(1-q)+q^2h(q)(1-q)\\
&= \big(q+(1-q)h(q)\big)^3-q^3.
\end{aligned}
$$

Por lo tanto $f_3(q)=\dfrac{\big(q+(1-q)h(q)\big)^3-q^3}{(1-q)}$.

Generalizando este resultado tenemos que las soluciones de la ecuación funcional asociada a la forma aditiva $[m+n]_q=q^n[m]_q+q^m[n]_q+(1-q)[m]_q[n]_q$ son:

$$f_n(q)=\frac{\big(q+(1-q)h(q)\big)^n-q^n}{1-q}.$$

A continuación haremos una discusión sobre la ecuación funcional general asociada a una regla aditiva cuadrática.

Por el Teorema II.7 de la sección anterior, tenemos que la forma general de una regla aditiva cuadrática es:

$$
\begin{aligned}
r_n'(q)[m]_q+s_m'(q)[n]_q+t_{m,n}'(q)[m]_q[n]_q &= \Big(u_n(q)[n]_q+1-\delta_n\Big)[m]_q+\Big(v_m(q)[m]_q+1-\delta_m\Big)[n]_q\\
&\quad+\big(q-1-u_n(q)-v_m(q)+\delta_m+\delta_n\big)[m]_q[n]_q\\
&= [m+n]_q.
\end{aligned}
$$

Por lo tanto, la ecuación funcional general asociada a la regla aditiva cuadrática cuántica es:

$$f_{m+n}(q)=\Big(u_n(q)[n]_q+1-\delta_n\Big)f_m(q)+\Big(v_m(q)[m]_q+1-\delta_m\Big)f_n(q)+\big(q-1-u_n(q)-v_m(q)+\delta_m+\delta_n\big)f_m(q)f_n(q).$$

Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una solución de la ecuación funcional general, la cual está generada por el polinomio $f_1(q)=h(q)$. Haciendo $m=n=1$, tenemos:

$$f_2(q)=\big(u_1(q)+v_1(q)\big)h(q)+\big(q+1-u_1(q)-v_1(q)\big)h(q)^2.$$

Ahora, si hacemos $m=1$ y $n=2$, entonces:

$$\begin{aligned} f_3(q) &= f_{1+2}(q) \\ &= \big(u_2(q)(q+1)+1\big)h(q) + v_1(q)f_2(q) + \big(q-u_2(q)-v_1(q)\big)h(q)f_2(q). \end{aligned}$$

Similarmente, con $m=2$ y $n=1$, llegamos a que:

$$\begin{aligned} f_3(q) &= f_{2+1}(q) \\ &= u_1(q)f_2(q) + \big(v_2(q)(q+1)+1\big)h(q) + \big(q-u_1(q)-v_2(q)\big)f_2(q)h(q). \end{aligned}$$

Si restamos las dos últimas ecuaciones tenemos la igualdad:

$$0 = \Big(\big(u_1(q)-v_1(q)\big)-\big(u_2(q)-v_2(q)\big)\Big)f_2(q)h(q) + \big(u_2(q)-v_2(q)\big)(q+1)h(q) + \big(v_1(q)-u_1(q)\big)f_2(q).$$

Reemplazando $f_2(q)$ por su valor y simplificando llegamos a que el polinomio $h(q)$ debe de satisfacer la ecuación:

$$\begin{aligned} 0 = {} & \big(u_2-v_2-u_1+v_1\big)\big(q+1-u_1-v_1\big)h(q)^3 \\ & + \Big(\big(u_2-v_2\big)\big(u_1+v_1\big)+\big(q+1\big)\big(u_1-v_1\big)-2\big(u_1^2-v_1^2\big)\Big)h(q)^2 \\ & + \Big(u_1^2-v_1^2-\big(u_2-v_2\big)\big(q+1\big)\Big)h(q). \end{aligned}$$

Equivalentemente, $h(q)$ es una raíz del polinomio cúbico:

$$\begin{aligned} 0 = {} & \big(u_2-v_2-u_1+v_1\big)\big(q+1-u_1-v_1\big)x^3 \\ & + \Big(\big(u_2-v_2\big)\big(u_1+v_1\big)+\big(q+1\big)\big(u_1-v_1\big)-2\big(u_1^2-v_1^2\big)\Big)x^2 \\ & + \Big(u_1^2-v_1^2-\big(u_2-v_2\big)\big(q+1\big)\Big)x. \end{aligned}$$

Claramente $x=0$ y $x=1$ son soluciones de esta ecuación. Dividiendo entre $x(x-1)$ obtenemos:

$$\big(u_2-v_2-u_1+v_1\big)\big(q+1-u_1-v_1\big)x - \Big(u_1^2-v_1^2-\big(u_2-v_2\big)\big(q+1\big)\Big) = 0.$$

Para los ejemplos de reglas aditivas cuadráticas estudiadas, vemos que los coeficientes en esta ecuación son ambos cero y todo polinomio $h(q)$ es una solución.

CAPÍTULO III

ESTRUCUTRA ADITIVA LINEAL DE LOS ENTEROS CUÁNTICOS

Dadas dos sucesiones de polinomios $\mathcal{U}=\{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}=\{v_m(q)\}_{m=1}^{\infty}$ decimos que definen una **regla aditiva lineal** $\oplus$ en una sucesión de polinomios $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ si se satisface que para todo par de enteros *m, n*, se cumple que:

$$f_m(q)\oplus f_n(q)=u_n(q)f_m(q)+v_m(q)f_n(q).$$

Una regla aditiva lineal es **cuántica** si $[m]_q\oplus[n]_q=[m+n]_q$ para todo par de enteros positivos *m* y *n*. En este capítulo se dará una caracterización para las reglas aditivas cuánticas y se estudiarán las soluciones de las correspondientes ecuaciones funcionales.

1. REGLAS ADITIVAS LINEALES.

Definición III.1: Dos sucesiones infinitas dobles de polinomios $\mathcal{U}=\{u_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}=\{v_{m,n}(q)\}_{m,n=1}^{\infty}$ determinan una **regla aditiva cuántica lineal** si para todo par de enteros positivos *m, n* se cumple que:

$$[m+n]_q=u_{m,n}(q)[m]_q+v_{m,n}(q)[n]_q \quad ...(1)$$

Observación: Si las sucesiones $\mathcal{U}$ y $\mathcal{V}$ satisfacen una regla aditiva cuántica lineal entonces la sucesión $\mathcal{U}$ determina a la sucesión $\mathcal{V}$ y viceversa. Sin embargo, no se sabe para qué sucesiones $\mathcal{U}$ existe una sucesión $\mathcal{V}$ de tal manera que ambas definan la ecuación anterior.

Definición III.2: Una **identidad cero lineal** está definida por dos sucesiones de polinomios $\mathcal{S}=\{s_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{T}=\{t_{m,n}(q)\}_{m,n=1}^{\infty}$ tales que $s_{m,n}(q)[m]_q+t_{m,n}(q)[n]_q=0$ para todos los enteros positivos *m* y *n*.

En el capítulo anterior hemos visto que tenemos la regla aditiva lineal:

$$[m+n]_q=[m]_q+q^m[n]_q \quad ...(2)$$

Por conmutatividad, $[m]_q+q^m[n]_q=[m+n]_q=[n+m]_q=[n]_q+q^n[m]_q \;\forall\, m,n\in\mathbb{Z}^+$, por lo que:

$$(1-q^n)[m]_q+(q^m-1)[n]_q=0 \quad ...(3)$$

Sumando las dos ecuaciones anteriores se tiene que:

$$[m+n]_q = (2-q^n)[m]_q + (2q^m - 1)[n]_q \ \ldots (4)$$

A continuación veremos cómo podemos obtener una nueva regla aditiva a partir de reglas aditivas ya conocidas:

Primero tomamos la igualdad (2) y la multiplicamos por 4 obteniendo:

$$4[m+n]_q = 4[m]_q + 4q^m [n]_q \ \ldots (5)$$

Ahora, multiplicamos la ecuación (4) por 3 y se obtiene:

$$\begin{aligned} 3[m+n]_q &= 3(2-q^n)[m]_q + 3(2q^m - 1)[n]_q \\ &= 6[m]_q - 3q^n [m]_q + 6q^m [n]_q - 3[n]_q \\ &= 6[m+n]_q - 3q^n [m]_q - 3[n]_q \text{ utilizando la ecuación (2).} \end{aligned}$$

Por lo tanto tenemos que:

$$3[m+n]_q = 3q^n [m]_q + 3[n]_q \ \ldots (6)$$

Por último, restando las ecuaciones (5) y (6) se tiene que:

$$\begin{aligned} [m+n]_q &= 4[m]_q + 4q^m [n]_q - 3q^n [m]_q - 3[n]_q \\ &= (4-3q^n)[m]_q + (4q^m - 3)[n]_q . \end{aligned}$$

Es decir,

$$[m+n]_q = (4-3q^n)[m]_q + (4q^m - 3)[n]_q .$$

La cual es una nueva regla aditiva.

Este proceso de construir nuevas reglas aditivas a partir de reglas antiguas queda descrito en el siguiente teorema.

Teorema III.3:

a) Sean $\mathcal{U}^i = \left\{u_{m,n}^{(i)}(q)\right\}_{m,n=1}^{\infty}$ y $\mathcal{V}^i = \left\{v_{m,n}^{(i)}(q)\right\}_{m,n=1}^{\infty}$ dos sucesiones de polinomios que determinan una regla aditiva cuántica con $i = 1,..,k$. Si $\alpha_1,...,\alpha_k$ son elementos del correspondiente anillo de coeficientes tales que $\alpha_1 + ... + \alpha_k = 1$, y si las sucesiones $\mathcal{U} = \left\{u_{m,n}(q)\right\}_{m,n=1}^{\infty}$ y $\mathcal{V} = \left\{v_{m,n}(q)\right\}_{m,n=1}^{\infty}$ están definidas, para todo par de enteros positivos *m, n* por:

$$u_{m,n}(q)=\sum_{i=1}^{k}\alpha_i u_{m,n}^{(i)}(q)$$
$$v_{m,n}(q)=\sum_{i=1}^{k}\alpha_i v_{m,n}^{(i)}(q),$$

entonces $\mathcal{U}$ y $\mathcal{V}$ determinan una regla aditiva cuántica lineal.

b) Si $\mathcal{U}=\{u_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}=\{v_{m,n}(q)\}_{m,n=1}^{\infty}$ son sucesiones de polinomios que determinan una regla aditiva cuántica lineal, y si $\mathcal{S}=\{s_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{T}=\{t_{m,n}(q)\}_{m,n=1}^{\infty}$ son sucesiones de polinomios que determinan una identidad cero lineal, entonces las sucesiones $\mathcal{U}+\mathcal{S}=\{u_{m,n}(q)+s_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}+\mathcal{T}=\{v_{m,n}(q)+t_{m,n}(q)\}_{m,n=1}^{\infty}$ determinan una regla aditiva cuántica.

Demostración:

a) Como $\mathcal{U}^i=\{u_{m,n}^{(i)}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}^i=\{v_{m,n}^{(i)}(q)\}_{m,n=1}^{\infty}$ determinan una regla aditiva cuántica para toda $i=1,..,k$, entonces $[m+n]_q=u_{m,n}^{i}(q)[m]_q+v_{m,n}^{i}(q)[n]_q\ \forall i=1,...,k$. Lo que queremos probar es que $\mathcal{U}$ y $\mathcal{V}$ determinan una regla aditiva cuántica, es decir,

$$[m+n]_q=u_{m,n}(q)[m]_q+v_{m,n}(q)[n]_q .$$

Por hipótesis sabemos que $u_{m,n}(q)=\sum_{i=1}^{k}\alpha_i u_{m,n}^{(i)}(q)$ y $v_{m,n}(q)=\sum_{i=1}^{k}\alpha_i v_{m,n}^{(i)}(q)$ y que $\alpha_1+...+\alpha_k=1$; entonces:

$$\begin{aligned}
u_{m,n}(q)[m]_q+v_{m,n}(q)[n]_q &=\left(\sum_{i=1}^{k}\alpha_i\cdot u_{m,n}^{i}(q)\right)[m]_q+\left(\sum_{i=1}^{k}\alpha_i\cdot v_{m,n}^{i}(q)\right)[n]_q\\
&=\alpha_1\cdot u_{m,n}^{1}(q)\cdot[m]_q+...+\alpha_k\cdot u_{m,n}^{k}(q)\cdot[m]_q+\alpha_1\cdot v_{m,n}^{1}(q)\cdot[n]_q+...+\alpha_k\cdot v_{m,n}^{k}(q)\cdot[n]_q\\
&=\alpha_1\left(u_{m,n}^{1}(q)\cdot[m]_q+v_{m,n}^{1}(q)\cdot[n]_q\right)+...+\alpha_k\left(u_{m,n}^{k}(q)\cdot[m]_q+v_{m,n}^{k}(q)\cdot[n]_q\right)\\
&=\alpha_1\left([m+n]_q\right)+...+\alpha_k\left([m+n]_q\right)\\
&=(\alpha_1+...+\alpha_k)\left([m+n]_q\right)=(1)\left([m+n]_q\right)=[m+n]_q .
\end{aligned}$$

Por lo tanto $\boxed{[m+n]_q=u_{m,n}(q)[m]_q+v_{m,n}(q)[n]_q}$, es decir, $\mathcal{U}$ y $\mathcal{V}$ determinan una regla aditiva cuántica. □

b) Por hipótesis sabemos que $\mathcal{U}=\{u_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}=\{v_{m,n}(q)\}_{m,n=1}^{\infty}$ determinan una regla aditiva cuántica, es decir, $[m+n]_q = u_{m,n}(q)[m]_q + v_{m,n}(q)[n]_q$. También sabemos que $\mathcal{S}=\{s_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{T}=\{t_{m,n}(q)\}_{m,n=1}^{\infty}$ determinan una identidad cero, es decir, $s_{m,n}(q)[m]_q + t_{m,n}(q)[n]_q = 0$. Lo que queremos probar es que $\mathcal{U}+\mathcal{S}=\{u_{m,n}(q)+s_{m,n}(q)\}_{m,n=1}^{\infty}$ y $\mathcal{V}+\mathcal{T}=\{v_{m,n}(q)+t_{m,n}(q)\}_{m,n=1}^{\infty}$ determinan una regla aditiva cuántica, *i.e.*, $[m+n]_q = \big(u_{m,n}(q)+s_{m,n}(q)\big)[m]_q + \big(v_{m,n}(q)+t_{m,n}(q)\big)[n]_q$.

Vamos a aplicar las hipótesis para poder llegar a la conclusión deseada:

$$\begin{aligned}\big(u_{m,n}(q)+s_{m,n}(q)\big)[m]_q + \big(v_{m,n}(q)+t_{m,n}(q)\big)[n]_q &= u_{m,n}(q)[m]_q + s_{m,n}(q)[m]_q + v_{m,n}(q)[n]_q + t_{m,n}(q)[n]_q \\ &= \big(u_{m,n}(q)[m]_q + v_{m,n}(q)[n]_q\big) + \big(s_{m,n}(q)[m]_q + t_{m,n}(q)[n]_q\big) \\ &= [m+n]_q + 0 = [m+n]_q .\end{aligned}$$

Por lo tanto $\boxed{[m+n]_q = \big(u_{m,n}(q)+s_{m,n}(q)\big)[m]_q + \big(v_{m,n}(q)+t_{m,n}(q)\big)[n]_q}$, es decir, $\mathcal{U}+\mathcal{S}$ y $\mathcal{V}+\mathcal{T}$ determinan una regla aditiva cuántica. □

2. LA REGLA ADITIVA CUÁNTICA FUNDAMENTAL.

El objetivo de esta sección es clasificar todas las identidades cero lineales y todas las reglas aditivas lineales cuánticas. Para esto, consideraremos sucesiones que dependan únicamente de *m* ó *n*.

Teorema III.4:

a) Sean $\mathfrak{S}=\{s_n(q)\}_{n=1}^{\infty}$ y $\mathcal{T}=\{t_m(q)\}_{m=1}^{\infty}$ dos sucesiones de polinomios. Entonces, $s_n(q)[m]_q+t_m(q)[n]_q=0\ \forall\ m,n\in\mathbb{Z}^+$ si y sólo si existe un polinomio $z(q)$ tal que $s_n(q)=z(q)[n]_q\ \forall\ n\geq 1$ y $t_m(q)=-z(q)[m]_q\ \forall\ m\geq 1$.

b) Si $s_m(q)[m]_q+t_m(q)[n]_q=0\ \forall\ m,n\in\mathbb{Z}^+$ ó $s_m(q)[m]_q+t_n(q)[n]_q=0\ \forall\ m,n\in\mathbb{Z}^+$, entonces $s_n(q)=t_n(q)=0\ \forall n\in\mathbb{Z}^+$.

Demostración:

a) $\Rightarrow$] Supongamos que las sucesiones $\mathfrak{S}$ y $\mathcal{T}$ satisfacen la identidad $s_n(q)[m]_q+t_m(q)[n]_q=0$. Como esto se cumple para todos los enteros positivos *m* y *n*, en particular se cumple para $m=n=1$, entonces tenemos que:

$$s_1(q)+t_1(q)=s_1(q)[1]_q+t_1(q)[1]_q=0.$$

Definimos $\boxed{z(q)=s_1(q)=-t_1(q)}$.

Con esta definición tenemos que para todo entero positivo *n* y $m=1$, $s_n(q)[1]_q+t_1(q)[n]_q=s_n(q)-z(q)[n]_q=0$. Si despejamos el término $s_n(q)$ tenemos que $s_n(q)=z(q)[n]_q\ \forall\ n\geq 1$.

Análogamente, si ahora consideramos cualquier entero positivo *m* y $n=1$ tenemos: $s_1(q)[m]_q+t_m(q)[1]_q=z(q)[m]_q+t_m(q)=0$. Si despejamos el término $t_m(q)$ tenemos que $t_m(q)=-z(q)[m]_q\ \forall\ m\geq 1$.

$\Leftarrow$] Supongamos que existe un polinomio $z(q)$ tal que $s_n(q)=z(q)[n]_q\ \forall\ n\geq 1$ y $t_m(q)=-z(q)[m]_q\ \forall\ m\geq 1$. Entonces:
$s_n(q)[m]_q+t_m(q)[n]_q=z(q)[n]_q[m]_q-z(q)[m]_q[n]_q=0$ y esto se cumple para todos los enteros positivos *m* y *n*.
Por lo tanto, $s_n(q)[m]_q+t_m(q)[n]_q=0\ \forall\ m,n\in\mathbb{Z}^+$. □

b) Caso 1: Supongamos que $s_m(q)[m]_q + t_m(q)[n]_q = 0 \ \forall\ m,n \in \mathbb{Z}^+$, entonces $t_m(q)[n]_q = -s_m(q)[m]_q$. Pero como la igualdad $s_m(q)[m]_q + t_m(q)[n]_q = 0$ se cumple para toda n y toda m, en particular se cumple para toda m y toda $n+1$, *i.e.*, $s_m(q)[m]_q + t_m(q)[n+1]_q = 0$, entonces $t_m(q)[n+1]_q = -s_m(q)[m]_q$. Igualando las dos expresiones resulta que:
$t_m(q)[n]_q = -s_m(q)[m]_q = t_m(q)[n+1]_q = t_m(q)\left([n]_q + q^n\right)$ y esto implica que $t_m(q)[n]_q = t_m(q)[n]_q + t_m(q)q^n$, entonces $t_m(q)q^n = 0$, pero $q^n \neq 0 \ \forall n \geq 0$ por lo tanto $t_m(q) = 0$ para toda m. Además, como $t_m(q)[n]_q = -s_m(q)[m]_q$, entonces también $s_m(q) = 0$ para toda m.

Por lo tanto $s_m(q) = t_m(q) = 0$ para toda m.

Caso 2 (Por contradicción): Supongamos que $s_m(q)[m]_q + t_n(q)[n]_q = 0 \ \forall\ m,n \in \mathbb{Z}^+$, entonces $s_m(q)[m]_q = -t_n(q)[n]_q \ \forall\ m,n \in \mathbb{Z}^+$.

Así, si suponemos que $s_m(q) \neq 0$ para alguna m, entonces $t_n(q) \neq 0$ para toda n y $s_m(q) \neq 0$ para toda m.

Si nos fijamos en los grados de los polinomios tenemos que:
$\mathrm{gr}\left(s_m(q)[m]_q\right) = \mathrm{gr}\left(t_n(q)[n]_q\right)$, entonces $\mathrm{gr}\left(s_m(q)\right) + m - 1 = \mathrm{gr}\left(t_n(q)\right) + n - 1 \geq n - 1.$

Por lo tanto $\mathrm{gr}(s_m) \geq n - m \ \forall n \in \mathbb{Z}^+$ lo cual es un absurdo, ya que es para todo entero positivo n, así si hacemos $n = m + \mathrm{gr}\left(s_m(q)\right) + 1$ tenemos que $\mathrm{gr}\left(s_m(q)\right) \geq \mathrm{gr}\left(s_m(q)\right) + 1$ lo cual es imposible.

Por lo tanto, $\mathcal{S}$ y $\mathcal{T}$ son sucesiones cero. □

El siguiente teorema nos muestra cuando dos sucesiones de polinomios definen una regla aditiva cuántica lineal.

Teorema III.5: Las sucesiones $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ definen una regla aditiva cuántica lineal si y sólo si existe un polinomio $z(q)$ tal que:

$$u_n(q) = 1 + z(q)[n]_q \ \forall n \in \mathbb{Z}^+ \text{ y } v_m(q) = q^m - z(q)[m]_q \ \forall m \in \mathbb{Z}^+.$$

Más aún, $z(q) = u_1(q) - 1 = q - v_1(q)$.

Demostración:

$\Rightarrow$] Sean $\mathcal{U}=\{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}=\{v_m(q)\}_{m=1}^{\infty}$ solución de la ecuación

$$[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q \ .$$

Definimos $\boxed{z(q)=u_1(q)-1}$.

Como la ecuación $[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q$ se cumple para todos los enteros positivos, entonces en particular se cumple para $n=1=m$. Entonces:
$1+q=[2]_q=[1+1]_q=u_1(q)+v_1(q)=1+z(q)+v_1(q)$ ya que si $z(q)=u_1(q)-1$ entonces $u_1(q)=1+z(q)$.

Por lo tanto $1+q=1+z(q)+v_1(q)$, lo cual implica que $v_1(q)=q-z(q)$. Así, para todo entero positivo *m*, tenemos que $[m+1]_q=u_1(q)[m]_q+v_m(q)$, entonces:

$$\begin{aligned} v_m(q) &= [m+1]_q - u_1(q)[m]_q \\ &= q^m + [m]_q - u_1(q)[m]_q \\ &= q^m + (1-u_1)[m]_q \\ &= q^m - z(q)[m]_q \ . \end{aligned}$$

Por lo tanto $\boxed{v_m(q)=q^m-z(q)[m]_q}$.

Análogamente, para todo entero positivo *n*, tenemos que $[n+1]_q=[1+n]_q=u_n(q)+v_1(q)[n]_q$ entonces:

$$\begin{aligned} u_n(q) &= [n+1]_q - v_1(q)[n]_q \\ &= 1+q[n]_q - (q-z(q))[n]_q \\ &= 1+q[n]_q - q[n]_q + z(q)[n]_q \\ &= 1+z(q)[n]_q \ . \end{aligned}$$

Por lo tanto $\boxed{u_n(q)=1+z(q)[n]_q}$.

$\Leftarrow$] Sea $z(q)$ cualquier polinomio y definamos las sucesiones $\mathcal{U}=\{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V}=\{v_m(q)\}_{m=1}^{\infty}$ mediante las hipótesis del teorema, es decir, mediante las igualdades $u_n(q)=1+z(q)[n]_q$ y $v_m(q)=q^m-z(q)[m]_q$. Entonces:

$$\begin{aligned} u_n(q)[m]_q + v_m(q)[n]_q &= \left(1+z(q)[n]_q\right)[m]_q + \left(q^m - z(q)[m]_q\right)[n]_q \\ &= [m]_q + z(q)[n]_q[m]_q + q^m[n]_q - z(q)[m]_q[n]_q \\ &= [m]_q + q^m[n]_q \\ &= \left(1+q+q^2+\ldots+q^{m-1}\right) + \left(q^m + q^{m+1} + \ldots + q^{m+n-1}\right) \\ &= [m+n]_q . \end{aligned}$$

Por lo tanto $[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q \ \forall\ m,n \in \mathbb{Z}^+$ □

Para entender mejor este último teorema, vamos a dar un ejemplo:

Ejemplo: La ecuación $[m+n]_q = \left(4-3q^n\right)[m]_q + \left(4q^m - 3\right)[n]_q$ se puede reescribir de la siguiente manera:

$$\begin{aligned} [m+n]_q &= \left(4-3q^n\right)[m]_q + \left(4q^m-3\right)[n]_q \\ &= \left(1+z(q)[n]_q\right)[m]_q + \left(q^m - z(q)[m]_q\right)[n]_q . \end{aligned}$$

Donde $z(q) = 3-3q$.

Demostración:

Primero desarrollemos los términos $1+z(q)[n]_q$ y $q^m - z(q)[m]_q$ para $z(q) = 3-3q$:

$$\begin{aligned} 1+z(q)[n]_q &= 1+(3-3q)[n]_q \\ &= 1+3[n]_q - 3q[n]_q \\ &= 1+3\left(1+q+q^2+\ldots+q^{n-1}\right) - 3q\left(1+q+q^2+\ldots+q^{n-1}\right) \\ &= 1+\left(3+3q+3q^2+\ldots+3q^{n-1}\right) + \left(-3q-3q^2-3q^3-\ldots-3q^n\right) \\ &= 1+3-3q^n = 4-3q^n . \end{aligned}$$

Por lo tanto $\boxed{1+z(q)[n]_q = 4-3q^n}$.

$$\begin{aligned} q^m - z(q)[m]_q &= q^m - (3-3q)[m]_q \\ &= q^m - 3[m]_q + 3q[m]_q \\ &= q^m - 3\left(1+q+q^2\ldots+q^{m-1}\right) + 3q\left(1+q+q^2\ldots+q^{m-1}\right) \\ &= q^m + \left(-3-3q-3q^2-\ldots-3q^{m-1}\right) + \left(3q+3q^2+3q^3\ldots+3q^m\right) \\ &= q^m - 3 + 3q^m = 4q^m - 3. \end{aligned}$$

Por lo tanto $\boxed{q^m - z(q)[m]_q = 4q^m - 3}$.

Por lo tanto obtenemos:

$$\begin{aligned}\left(1+z(q)[n]_q\right)[m]_q + \left(q^m - z(q)[m]_q\right)[n]_q &= \left(4-3q^n\right)[m]_q + \left(4q^m - 3\right)[n]_q \\ &= [m+n]_q .\end{aligned}$$

□

Teorema III.6: Sean $\mathcal{U} = \{u_m(q)\}_{m=1}^{\infty}$ y $\mathcal{V} = \{v_n(q)\}_{n=1}^{\infty}$ sucesiones de polinomios. Entonces:

$$[m+n]_q = u_m(q)[m]_q + v_m(q)[n]_q \quad \forall\ m,n \in \mathbb{Z}^+,$$

si y sólo si $u_m(q) = 1$ y $v_m(q) = q^m$ para toda m.

Demostración:

$\Rightarrow$] Supongamos que se cumple la ecuación $[m+n]_q = u_m(q)[m]_q + v_m(q)[n]_q$, como ésta se cumple para todos los enteros positivos m y n, podemos hacer $n = 1$ y obtenemos:

$$[m+1]_q = u_m(q)[m]_q + v_m(q)[1]_q = u_m(q)[m]_q + v_m(q).$$

De la misma manera, hagamos ahora $n = 2$ y resulta:

$$[m+2]_q = u_m(q)[m]_q + v_m(q)[2]_q = u_m(q)[m]_q + (1+q)v_m(q).$$

Ahora bien, si restamos estas últimas dos ecuaciones resulta que:

$$[m+2]_q - [m+1]_q = u_m(q)[m]_q + (1+q)v_m(q) - u_m(q)[m]_q - v_m(q).$$

Entonces tenemos que $q^{m+1} = v_m(q) + qv_m(q) - v_m(q) = qv_m(q)$, es decir, $q^{m+1} = qv_m(q)$.
Por lo tanto $\boxed{v_m(q) = q^m}$.

Ahora, si en la ecuación $[m+1]_q = u_m(q)[m]_q + v_m(q)$ despejamos $u_m(q)[m]_q$ resulta:

$$u_m(q)[m]_q = [m+1]_q - v_m(q) = [m+1]_q - q^m = [m]_q .$$

Es decir, $u_m(q)[m]_q = [m]_q$.
Por lo tanto $\boxed{u_m(q) = 1}$ para toda m.

$\Leftarrow]$ Supongamos que $u_m(q)=1$ y $v_m(q)=q^m$ para toda *m*, entonces:

$$\begin{aligned} u_m(q)[m]_q + v_m(q)[n]_q &= 1\cdot[m]_q + q^m\cdot[n]_q \\ &= [m]_q + q^m[n]_q \\ &= \left(1+q+\ldots+q^{m-1}\right)+q^m\left(1+q+\ldots+q^{n-1}\right) \\ &= 1+q+\ldots+q^{m-1}+q^m+q^{m+1}+\ldots+q^{m+n-1} \\ &= [m+n]_q . \end{aligned}$$

Por lo tanto $[m+n]_q = u_m(q)[m]_q + v_m(q)[n]_q \ \forall\ m,n\in\mathbb{Z}^+$. □

El teorema anterior da condiciones necesarias y suficientes para que suceda que $[m+n]_q = u_m(q)[m]_q + v_m(q)[n]_q \ \forall\ m,n\in\mathbb{Z}^+$. Es decir, el subíndice de *u* y *v* tiene que ser el mismo (a saber, *m*).

A continuación presentaremos un lema en el cual se observará que si tenemos distintos subíndices en *u* y *v* (*m* y *n* respectivamente), el teorema NO se cumple.

Lema III.7: NO existen sucesiones de polinomios $\mathcal{U}=\{u_m(q)\}_{m=1}^{\infty}$ y $\mathcal{V}=\{v_n(q)\}_{n=1}^{\infty}$ tales que:

$$[m+n]_q = u_m(q)[m]_q + v_n(q)[n]_q \ \forall\ m,n\in\mathbb{Z}^+.$$

Demostración:

Esta prueba la haremos por reducción al absurdo:

Supongamos que SI existen sucesiones de polinomios $\mathcal{U}=\{u_m(q)\}_{m=1}^{\infty}$ y $\mathcal{V}=\{v_n(q)\}_{n=1}^{\infty}$ tales que:

$$[m+n]_q = u_m(q)[m]_q + v_n(q)[n]_q \ \forall\ m,n\in\mathbb{Z}^+.$$

Como esto se cumple para toda *n*, entonces se cumple para $n=1$ y $n=2$, es decir:

$$[m+1]_q = u_m(q)[m]_q + v_1(q)[1]_q = u_m(q)[m]_q + v_1(q).$$

Lo cual implica que $u_m(q)[m]_q = [m+1]_q - v_1(q).$

Y también:

$$[m+2]_q = u_m(q)[m]_q + v_2(q)[2]_q = [m+1]_q - v_1(q) + (1+q)v_2(q).$$

Haciendo un poco de álgebra en la expresión $[m+2]_q = [m+1]_q - v_1(q) + (1+q)v_2(q)$ resulta que:

$$[m+2]_q - [m+1]_q = (1+q)v_2(q) - v_1(q)$$
$$\left(1+q+q^2+\ldots+q^{m-1}+q^m+q^{m+1}\right) - \left(1+q+q^2+\ldots+q^{m-1}+q^m\right) = (1+q)v_2(q) - v_1(q)$$
$$q^{m+1} = (1+q)v_2(q) - v_1(q)$$

Por lo tanto $q^{m+1} = (1+q)v_2(q) - v_1(q)\ \forall m \in \mathbb{Z}^+$ lo cual es un absurdo. □

El siguiente resultado, el cual es el último de este capítulo, demuestra que la sucesión de enteros cuánticos es esencialmente la única solución de la correspondiente ecuación funcional.

Teorema III.8: Sean $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ sucesiones de polinomios tales que $[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q$ para todos los enteros positivos m y n. Entonces $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es una solución de la ecuación funcional $f_{m+n}(q) = u_n(q)f_m(q) + v_m(q)f_n(q)$ si y sólo si existe un polinomio $h(q)$ tal que $f_n(q) = h(q)[n]_q\ \forall\ n \geq 1$.

Demostración:

$\Rightarrow$] Supongamos que $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ son sucesiones de polinomios tales que $[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q$ para todos los enteros positivos m y n y que $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es una solución de la ecuación funcional $f_{m+n}(q) = u_n(q)f_m(q) + v_m(q)f_n(q)$. Lo que queremos probar es que existe un polinomio $h(q)$ tal que $f_n(q) = h(q)[n]_q\ \forall\ n \geq 1$. Esto lo haremos por inducción sobre n:

- Base de la inducción: Para $n = 1$ definimos $h(q) = f_1(q)$. De esta manera $f_1(q) = h(q)[1]_q = h(q)$.

- Hipótesis de inducción: Supongamos que $f_n(q) = h(q)[n]_q$.

- Paso inductivo: Gracias al Teorema III.5, tenemos que existe un polinomio $z(q)$ tal que $u_n(q) = 1 + z(q)[n]_q\ \forall n \in \mathbb{Z}^+$ y $v_m(q) = q^m - z(q)[m]_q\ \forall m \in \mathbb{Z}^+$, entonces:

$$\begin{aligned} f_{n+1}(q) = f_{1+n}(q) &= u_1(q) f_n(q) + v_n(q) f_1(q) \\ &= \left(1 + z(q)[1]_q\right) h(q)[n]_q + \left(q^n - z(q)[n]_q\right) h(q) \\ &= h(q)\left([n]_q + z(q)[n]_q + q^n - z(q)[n]_q\right) \\ &= h(q)\left([n]_q + q^n\right) = h(q)[n+1]_q . \end{aligned}$$

Por lo tanto $f_{n+1}(q) = h(q)[n+1]_q$.

Así, resulta que $f_n(q) = h(q)[n]_q \ \ \forall\, n \geq 1$.

$\Leftarrow$] Supongamos que $\mathcal{U} = \{u_n(q)\}_{n=1}^{\infty}$ y $\mathcal{V} = \{v_m(q)\}_{m=1}^{\infty}$ son sucesiones de polinomios tales que $[m+n]_q = u_n(q)[m]_q + v_m(q)[n]_q$ para todos los enteros positivos *m* y *n* y que existe un polinomio $h(q)$ tal que $f_n(q) = h(q)[n]_q \ \ \forall\, n \geq 1$. Lo que queremos probar es que $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es una solución de la ecuación funcional $f_{m+n}(q) = u_n(q) f_m(q) + v_m(q) f_n(q)$. Entonces:

$$\begin{aligned} u_n(q) f_m(q) + v_m(q) f_n(q) &= u_n(q) h(q)[m]_q + v_m(q) h(q)[n]_q \\ &= h(q)\left(u_n(q)[m]_q + v_m(q)[n]_q\right) \\ &= h(q)[m+n]_q \\ &= f_{m+n}(q). \end{aligned}$$

Por lo tanto $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es una solución de la ecuación funcional $f_{m+n}(q) = u_n(q) f_m(q) + v_m(q) f_n(q)$. □

Observación: Nosotros sabemos que $[n]_q = 1 + q + q^2 + \ldots + q^{n-1}$ lo cual quiere decir que los enteros cuánticos no son otra cosa más que polinomios. Si observamos con cuidado todo el trabajo realizado en este capítulo podremos darnos cuenta de que la única propiedad que utilizamos de los polinomios es la función grado. Esto implica que los teoremas III.5 y III.8 se cumplen en cualquier álgebra que contenga enteros cuánticos. Algunos ejemplos de estas álgebras son: los polinomios, las funciones racionales, las series de potencias, las series de Laurent con coeficientes en un anillo o en un campo, etc.

Con todo esto, hacemos referencia a que los enteros cuánticos no son más que polinomios y así tenemos una infinidad de ejemplos en donde aparecen estos.

CAPÍTULO IV

ESTRUCTURA DE ANILLO DE LOS ENTEROS CUÁNTICOS

En los capítulos anteriores hemos visto como definir una operación aditiva y una multiplicativa en el conjunto de los enteros cuánticos de tal manera que $[m]_q \oplus_q [n]_q = [m+n]_q$ y $[m]_q \otimes_q [n]_q = [mn]_q$. Estas definiciones nos sirven para demostrar que tenemos una estructura de anillo para los enteros cuánticos y de campo para los números racionales cuánticos.

Finalizaremos observando que las reglas aditiva y multiplicativa definidas en el anillo de los enteros cuánticos son equivalentes a la descomposición elemental de intervalos de enteros en la teoría aditiva de los números.

1. ADICIÓN Y MULTIPLICACIÓN

Sean $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ los conjuntos de enteros positivos, enteros y números racionales respectivamente.

Recordemos brevemente la definición de anillo.

Definición IV.1: Sea *A* un conjunto no vacio con dos elementos distinguidos (*n* y *m*) y sean + y * dos operaciones binarias. Diremos que $(A,+,*,n,m)$ es un **anillo** si se cumplen las siguientes condiciones:

1) *A* es cerrado bajo + y bajo *.
2) + es conmutativa.
3) + y * son asociativas.
4) *n* es neutro en + y *m* es neutro en *.
5) Existen inversos para +.
6) * es distributiva respecto de +.

Además, si la operación * es conmutativa, entonces diremos que $(A,+,*,n,m)$ es un **anillo conmutativo.**

Definición IV.2: El número cuántico $[x]_q$ se define como la siguiente función en las variables *x* y *q*:

$$[x]_q = \frac{1-q^x}{1-q}.$$

Si *x* es un entero *n*, entonces tenemos la definición usual de entero cuántico,

$$[n]_q = \frac{1-q^n}{1-q} = 1+q+\ldots+q^{n-1}.$$

Para *n* en los enteros negativos, tenemos:

$$\begin{aligned}\left[-n\right]_q &= \frac{1-q^{-n}}{1-q} = -\frac{1-q^n}{q^n\left(1-q\right)} \\ &= -\frac{1}{q^n}\left[n\right]_q = -q^{-1}\left[n\right]_{q^{-1}} \\ &= -\left(\frac{1}{q}+\frac{1}{q^2}+\ldots+\frac{1}{q^n}\right).\end{aligned}$$

Definimos a $\left[\mathbb{Z}\right]_q = \left\{\left[n\right]_q / n \in \mathbb{Z}\right\}$ como **el conjunto de los enteros cuánticos**.

Teorema IV.3: Los enteros cuánticos tienen estructura de anillo.

Demostración:

Definamos en $\left[\mathbb{Z}\right]_q$ la siguiente operación aditiva:

$$\left[n\right]_q \oplus_q \left[m\right]_q = \left[n\right]_q + q^n\left[m\right]_q .$$

Entonces,

$$\begin{aligned}\left[n\right]_q \oplus_q \left[m\right]_q &= \left[n\right]_q + q^n\left[m\right]_q \\ &= \frac{1-q^n}{1-q} + q^n \cdot \frac{1-q^m}{1-q} \\ &= \frac{1-q^{n+m}}{1-q} \\ &= \left[n+m\right]_q .\end{aligned}$$

Similarmente, definimos la siguiente operación multiplicativa:

$$\left[n\right]_q \otimes_q \left[m\right]_q = \left[n\right]_q \cdot \left[m\right]_{q^n}$$

Entonces,

$$\begin{aligned}\left[n\right]_q \otimes_q \left[m\right]_q &= \left[n\right]_q \cdot \left[m\right]_{q^n} \\ &= \frac{1-q^n}{1-q} \cdot \frac{1-q^{nm}}{1-q^n} \\ &= \frac{1-q^{nm}}{1-q} \\ &= \left[nm\right]_q .\end{aligned}$$

Por lo tanto, las ecuaciones:

$$[n]_q \oplus_q [m]_q = [n+m]_q \qquad \text{y} \qquad [n]_q \otimes_q [m]_q = [nm]_q$$

nos dan una estructura de anillo conmutativo en el conjunto $[\mathbb{Z}]_q = \{[n]_q / n \in \mathbb{Z}\}$. □

Para continuar, recordemos la definición de isomorfismo de anillos.

Definición IV.4: Sean *R* y *S* dos anillos y *f* una aplicación de *R* en *S*, es decir, $f : R \to S$. Diremos que ***f* es un isomorfismo** si se cumplen las siguientes condiciones:

1) f es biyectiva.
2) $f(x+y) = f(x) + f(y) \quad \forall\ x, y \in R.$
3) $f(x \cdot y) = f(x) \cdot f(y) \quad \forall\ x, y \in R.$
4) $f(1) = 1$

Lema IV.5: La aplicación $f : \mathbb{Z} \to [\mathbb{Z}]_q$ con regla de correspondencia, $f(n) = [n]_q \quad \forall\ n \in \mathbb{Z}$ es un isomorfismo de anillos.

Demostración:

Para demostrar que *f* es un isomorfismo debemos de comprobar que se cumplen las cuatro condiciones de la definición IV.4:

1) Sean $a, b \in \mathbb{Z}$ y supongamos que $f(a) = f(b)$. Lo que se quiere probar es que $a = b$.
   Por definición tenemos que $f(a) = 1 + q + q^2 + ... + q^{a-1}$ y $f(b) = 1 + q + q^2 + ... + q^{b-1}$.
   Pero por hipótesis $f(a) = f(b)$, entonces tenemos una igualdad de polinomios. De este hecho podemos deducir que los polinomios $f(a)$ y $f(b)$ son del mismo grado, es decir, $a - 1 = b - 1$. De esta última igualdad se deduce que $a = b$. Por lo tanto *f* es inyectiva.
   La suprayectividad se da trivialmente gracias a la regla de correspondencia de la función *f*.
   Por lo tanto *f* es biyectiva.

2) Por el teorema IV.3 sabemos que $[n]_q \oplus_q [m]_q = [n+m]_q \ \forall\ n, m \in \mathbb{Z}$. Es decir, en términos de la aplicación *f* se tiene que:

$$f(n) + f(m) = f(n+m) \quad \forall\ n, m \in \mathbb{Z}.$$

3) Nuevamente, gracias al teorema IV.3 tenemos que $[n]_q \otimes_q [m]_q = [nm]_q$. Esta igualdad en términos de la aplicación *f* quedaría escrita como:

$$f(n)\cdot f(m) = f(n\cdot m) \;\; \forall \; n,m \in \mathbb{Z}.$$

4) Si $n=1$, entonces $f(1)=[1]_q$. Pero sabemos que $[1]_q = 1$.
Por lo tanto $f(1)=1$.

Por lo tanto, *f* es un isomorfismo de anillos y así $\mathbb{Z}$ y $[\mathbb{Z}]_q$ son isomorfos. □

Definición IV.5: Para un número racional $\frac{m}{n}$, se define **el número racional cuántico** $\left[\frac{m}{n}\right]_q$ como:

$$\left[\frac{m}{n}\right]_q = \frac{1-q^{\frac{m}{n}}}{1-q} = \frac{1-\left(q^{\frac{1}{n}}\right)^m}{1-\left(q^{\frac{1}{n}}\right)^n} = \frac{\dfrac{1-\left(q^{\frac{1}{n}}\right)^m}{1-q^{\frac{1}{n}}}}{\dfrac{1-\left(q^{\frac{1}{n}}\right)^n}{1-q^{\frac{1}{n}}}} = \frac{[m]_{q^{\frac{1}{n}}}}{[n]_{q^{\frac{1}{n}}}}.$$

Las identidades $[n]_q \oplus_q [m]_q = [n+m]_q$ y $[n]_q \otimes_q [m]_q = [nm]_q$ implican que la adición y la multiplicación de números racionales cuánticos son operaciones que están bien definidas y nos permiten darles una estructura de campo.

Definición IV.6: Se define **el campo de los números racionales cuánticos** como el conjunto:

$$[\mathbb{Q}]_q = \left\{ \left[\frac{m}{n}\right]_q / \frac{m}{n} \in \mathbb{Q} \right\}.$$

Si consideramos a $[x]_q$ como una función de variables reales *x* y *q*, entonces $\lim_{q\to 1}[x]_q = x$ para todo número real *x*.

Como las definiciones que hemos visto son de índole formal, tenemos el siguiente teorema el cual generaliza los resultados de los enteros cuánticos para cualquier anillo *R*.

Teorema IV.7: Para cualquier anillo R, no necesariamente conmutativo, el conjunto $[R]_q = \{[x]_q / x \in R\}$ es un anillo con la operación aditiva $[x]_q \oplus_q [y]_q = [x]_q + q^x [y]_q$ y la multiplicación de elementos definida por la regla $[x]_q \otimes_q [y]_q = [x]_q [y]_{q^x}$. El morfismo de R a $[R]_q$ definido mediante $x \mapsto [x]_q$ es un isomorfismo de anillos.

2. UNICIDAD DE LA ARITMÉTICA CUÁNTICA.

Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de polinomios en la variable q que satisface las reglas de adición y multiplicación para enteros cuánticos, es decir, $\mathcal{F}$ satisface la ecuación funcional aditiva para todos los enteros positivos m y n:

$$f_{m+n}(q)=f_m(q)+q^m f_n(q)$$

y la ecuación funcional multiplicativa para todos los enteros positivos m y n:

$$f_{mn}(q)=f_m(q)f_n(q^m).$$

Nathanson [1] demuestra que hay una gran variedad de sucesiones de polinomios que satisfacen la ecuación funcional multiplicativa $f_{mn}(q)=f_m(q)f_n(q^m)$. No se tiene una clasificación completa de las soluciones de esta ecuación, pero sí una descripción simple de todas las soluciones de la ecuación funcional aditiva $f_{m+n}(q)=f_m(q)+q^m f_n(q)$.

Teorema IV.8: Sea $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ una sucesión de funciones que satisface la ecuación funcional aditiva $f_{m+n}(q)=f_m(q)+q^m f_n(q)$. Sea $h(q)=f_1(q)$, entonces:

$$f_n(q)=h(q)[n]_q \quad \forall\, n\in\mathbb{N}.$$

Inversamente, para cualquier función $h(q)$, la sucesión de funciones $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ definida por $f_n(q)=h(q)[n]_q$ es una solución de $f_{m+n}(q)=f_m(q)+q^m f_n(q)$. En particular, si $h(q)$ es un polinomio en q, entonces $h(q)[n]_q$ es un polinomio en q para todo entero positivo n, y toda solución polinomial de $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ es de esta forma.

Demostración:

$\Rightarrow$] (Por inducción / n)

Supongamos que $\mathcal{F}=\{f_n(q)\}_{n=1}^{\infty}$ es solución de la ecuación funcional aditiva $f_{m+n}(q)=f_m(q)+q^m f_n(q)$.

- Base Inductiva: Si $n=1$, definimos $h(q)=f_1(q)$ y entonces $[n]_q\,h(q)=[1]_q\,f_1(q)=f_1(q)$.
  Por lo tanto $f_1(q)=h(q)[1]_q$.
- Hipótesis Inductiva: Para $n\geq 2$, supongamos que $f_{n-1}(q)=h(q)[n-1]_q$.

- Paso Inductivo: Gracias a la ecuación $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ tenemos que:

$$\begin{aligned} f_n(q) &= f_1(q)+q^1 f_{n-1}(q) \\ &\overset{H.I}{=} h(q)[1]_q + qh(q)[n-1]_q \\ &= h(q)\left([1]_q + q[n-1]_q\right) \\ &= h(q)\left(1+q\left(1+q+q^2+...+q^{n-2}\right)\right) \\ &= h(q)\left(1+q+q^2+...+q^{n-1}\right) \\ &= h(q)[n]_q . \end{aligned}$$

Por lo tanto $f_n(q)=h(q)[n]_q \quad \forall n\in\mathbb{N}$.

$\Leftarrow$] Si multiplicamos la ecuación $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ por $h(q)$, obtenemos: $h(q)[m+n]_q = h(q)[m]_q + q^m h(q)[n]_q$. Esto quiere decir que la sucesión $\left\{h(q)[n]_q\right\}_{n=1}^{\infty}$ es solución de la ecuación funcional aditiva $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ para cualquier función $h(q)$. □

Ahora podemos probar que la sucesión de enteros cuánticos es la única solución no trivial de las ecuaciones funcionales aditivas y multiplicativas $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ y $f_{mn}(q)=f_m(q)f_n(q^m)$.

Teorema IV.9: Sea $\mathcal{F}=\left\{f_n(q)\right\}_{n=1}^{\infty}$ una sucesión de funciones que satisfacen las dos ecuaciones $f_{m+n}(q)=f_m(q)+q^m f_n(q)$ y $f_{mn}(q)=f_m(q)f_n(q^m)$. Entonces $f_n(q)=0\ \forall n\in\mathbb{N}$ ó $f_n(q)=[n]_q \ \forall n\in\mathbb{N}$.

Demostración:

La ecuación funcional multiplicativa implica que $f_1(q)=f_1(q)^2$, entonces $f_1(q)=0$ ó $f_1(q)=1$. Como $\mathcal{F}=\left\{f_n(q)\right\}_{n=1}^{\infty}$ también satisface la ecuación funcional aditiva, se sigue del teorema IV.8 que $f_n(q)=0\ \forall n\in\mathbb{N}$ ó $f_n(q)=[n]_q \ \forall n\in\mathbb{N}$. □

3. EL ANILLO DE LOS ENTEROS CUÁNTICOS Y LA TEORÍA ADITIVA DE LOS NÚMEROS.

En esta sección mostraremos la estrecha relación entre las reglas aditivas y multiplicativas de los enteros cuánticos y algunos resultados de teoría aditiva de los números.

Definición IV.10: Sean A y B dos conjuntos de enteros, y sea m un número entero. Entonces definimos:

1) La **dilatación de *A*** como: $m * A = \{ma / a \in A\}$
2) La **traslación de *A* con respecto a m** como: $m + A = \{m + a \ / a \in A\}$
3) El **conjunto suma** como: $A + B = \{a + b \ / a \in A, b \in B\}$

Observación: Escribimos $A \oplus B = C$ si $A + B = C$ y todo entero en C se puede escribir de manera única de la forma $a + b$ para alguna $a \in A$ y $b \in B$.

Uno de los intereses de la teoría aditiva de los números es estudiar el problema de cómo escribir a los números enteros como combinación de otros enteros. Por ejemplo, particiones de $\mathbb{Z}$ en unión disjunta de subconjuntos o la descomposición de números enteros en suma de conjuntos de enteros.

Notación: Sea $[n]$ el conjunto de los primeros n enteros no negativos, es decir:

$$[n] = \{0,1,2,...,n-1\}.$$

Con esta notación tenemos la siguiente partición:

$$[m+n] = [m] \cup (m + [n]), \text{ donde } [m] \cap (m + [n]) = \varnothing.$$

Y la descomposición en suma directa:

$$[mn] = [m] \oplus m * [n].$$

Si $m_1,...,m_r$ son enteros positivos, entonces, por inducción, tenemos la partición:

$$[m_1 + m_2 + ... + m_r] = \bigcup_{j=1}^{r} \left(\sum_{i=1}^{j-1} m_i + [m_j] \right)$$

en conjuntos disjuntos dos a dos, y la descomposición en suma directa:

$$[m_1 m_2 \cdots m_r] = \bigoplus_{j=1}^{r} \left(\prod_{i=1}^{j-1} m_i * [m_j] \right).$$

Para cada conjunto finito A de enteros, asociamos el polinomio de Laurent:

$$F_A(q) = \sum_{a \in A} q^a$$

esto es llamado la **función generadora de *A***. Por las definiciones de dilatación, traslación y suma de conjuntos, tenemos las identidades de funciones generadoras:

$$\begin{aligned} F_{m*A}(q) &= F_A(q^m) \\ F_{m+A}(q) &= q^m F_A(q) \\ F_{A \oplus B}(q) &= F_A(q) F_B(q). \end{aligned}$$

Si $A \cap B = \varnothing$, entonces $F_{A \cup B}(q) = F_A(q) + F_B(q)$.

La función generadora para el conjunto $[n]$ es el entero cuántico $[n]_q$, ya que:

$$F_{[n]}(q) = 1 + q + q^2 + \ldots + q^{n-1} = [n]_q .$$

Reescribiendo la identidad (partición) $[m+n] = [m] \cup (m + [n])$ en términos de funciones generadoras tenemos:

$$\begin{aligned} [m+n]_q &= F_{[m+n]}(q) \\ &= F_{[m] \cup (m+[n])}(q) \\ &= F_{[m]}(q) + F_{m+[n]}(q) \\ &= F_{[m]}(q) + q^m F_{[n]}(q) \\ &= [m]_q + q^m [n]_q . \end{aligned}$$

La descomposición de suma de conjuntos $[mn] = [m] \oplus m*[n]$ del intervalo $[mn]$ es:

$$\begin{aligned} [mn]_q &= F_{[mn]}(q) \\ &= F_{[m] \oplus m*[n]}(q) \\ &= F_{[m]}(q) F_{m*[n]}(q) \\ &= F_{[m]}(q) F_{[n]}(q^m) \\ &= [m]_q [n]_{q^m} . \end{aligned}$$

Similarmente, las identidades de teoría aditiva de números $\left[m_1+m_2+\ldots+m_r\right]=\bigcup_{j=1}^{r}\left(\sum_{i=1}^{j-1}m_i+\left[m_j\right]\right)$ y $\left[m_1m_2\cdots m_r\right]=\bigoplus_{j=1}^{r}\left(\prod_{i=1}^{j-1}m_i*\left[m_j\right]\right)$ satisfacen la identidad de enteros cuánticos:

$$\left[m_1+m_2+\ldots+m_r\right]_q=\sum_{j=1}^{r}q^{\sum_{i=1}^{j-1}m_i}\left[m_j\right]_q$$

y

$$\left[m_1m_2\cdots m_r\right]_q=\prod_{j=1}^{r}\left[m_j\right]_{q^{\prod_{i=1}^{j-1}m_i}}.$$

En este sentido, observamos que las reglas de adición y multiplicación de enteros cuánticos son equivalentes a las afirmaciones elementales en la teoría aditiva de los números.

CONCLUSIONES

Como se mencionó en la introducción, la estructura de anillo de los enteros cuánticos es la parte central de este trabajo. Sin embargo, toda la información aquí vertida es de gran valor. Desde la construcción de la adición y multiplicación cuántica hasta los resultados más específicos y complejos de estos números.

En la tesis se presentan soluciones ya existentes, pero rescritas para una mejor comprensión, y en algunos casos la demostración es propia de este trabajo. Con esto se quiere lograr obtener un texto de fácil comprensión para que todo aquel interesado en el tema tenga una base que le sirva como introducción a los enteros cuánticos.

Algunas de las aplicaciones directas que tienen los enteros cuánticos son probadas por Borisov, Nathanson y Wang en [5]. Ellos probaron que las únicas soluciones de $f_m(q) * f_n(q) = f_{mn}(q)$ en el campo $\mathbb{Q}(q)$ de funciones racionales con coeficientes racionales son en esencia cocientes de productos de enteros cuánticos.

También probaron que existe un conjunto finito *R* de enteros positivos y un conjunto $\{t_r\}_{r\in R}$ de enteros tales que, para toda $n \in \operatorname{supp}(\mathcal{F})$, $f_n(q) = \lambda(n) q^{t_0(n-1)} \prod_{r\in R} [n]_{q^r}^{t_r}$; donde $\lambda(n)$ es una función aritmética completamente multiplicativa y t_0 es un número racional tal que $t_0(n-1) \in \mathbb{Z}$ para toda $n \in \operatorname{supp}(\mathcal{F})$.

Nathanson en [7] también probó que si $\mathcal{F} = \{f_n(q)\}_{n=1}^{\infty}$ es cualquier solución de la ecuación funcional $f_m(q) * f_n(q) = f_{mn}(q)$ en polinomios o series formales de potencias con coeficientes en un campo, y si $f_n(0) = 1 \; \forall n \in \operatorname{supp}(\mathcal{F})$, entonces existe una serie formal de potencias $F(q)$ tal que $\lim_{\substack{n\to\infty \\ n\in\operatorname{supp}(\mathcal{F})}} f_n(q) = F(q)$.

Cheung y Kac en [6] observan que los enteros cuánticos (vistos como polinomios) aparecen en muchos contextos, uno de ellos, en el cálculo cuántico. Por ejemplo, la *q*-ésima derivada de $f(x) = x^n$ es:

$$f'(x) = \frac{f(qx) - f(x)}{qx - x} = [n]_q \, x^{n-1}.$$

Los enteros cuánticos también se ubican en el estudio de grupos cuánticos, tema estudiado por Kassel en [8].

Desde el inicio del trabajo, quedó manifiesto que nunca se tuvo la intención de rescribir la obra de Nathanson, pero sí darla a conocer, porque estos trabajos que ha realizado, desde mi punto de vista son poco conocidos y reconocidos dentro de la matemática, de esta manera esperamos que esta tesis de un panorama global sobre Nathanson y sus artículos sobre los fascinantes enteros cuánticos, y que así el lector conozca un poco sobre el trabajo actual de este gran matemático.

BIBLIOGRAFÍA

[1] Melvyn B. Nathanson. "A functional equation arising from multiplication of quantum integers". Journal of Number Theory 103 (2003), pp. 214-233.

[2] Alex V. Kontorovich, Melvyn B. Nathanson. "Quadratic addition rules for quantum integers". Journal of Number Theory 117 (2006), pp. 1-13.

[3] Melvyn B. Nathanson. "Linear quantum addition rules". Journal of Combinatorial Number Theory 7(2) (2007), #A27.

[4] Melvyn B. Nathanson. "Additive number theory and the ring of quantum integers". www.arXiv.org:-math.NT/0204006.

[5] Alexander Borisov, Melvyn B. Nathanson and Yang Wang. "Quantum integers and cyclotomy". Journal of Number Theory 109 (2004), pp. 120-135.

[6] Victor Kac and Pokman Cheung. "Quantum Calculus". Universitext, Springer-Verlag, New York, 1995.

[7] Melvyn B. Nathanson. "Formal power series arising from multiplication of quantum integers". Unusual applications of number theory, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 64, Amer. Math. Soc., Providence, RI, 2004, pp. 145-167.

[8] Christian Kassel. "Quantum groups". Graduate Texts in Math., vol. 155, Springer-Verlag, New York, 1995.